В.В. Скобелев
В.Г. Скобелев

АНАЛИЗ ШИФРСИСТЕМ

ИПММ НАНУ

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ И МЕХАНИКИ

В.В. Скобелев , В.Г. Скобелев

АНАЛИЗ ШИФРСИСТЕМ

Донецк

2009

УДК 004.4+519.7+681.3

Рецензенты:

Д.т.н., профессор, зав. кафедрой защиты информации и криптографии Томского государственного университета *Г.П. Агибалов*

Д.ф.-м.н., с.н.с., зав. кафедрой КММТ ИКТ Национального авиационного университета *Н.М. Глазунов*

Д.т.н., профессор, профессор кафедры авиационных радиотехнических систем навигации и посадки Харьковского университета ВВС им. И. Кожедуба *П.Ю. Костенко*

Анализ шифрсистем
В.В. Скобелев, В.Г. Скобелев. ИПММ НАН Украины, Донецк, 2009. – 479с.

ISBN 978-966-02-5126-7

Монография посвящена разработке математических моделей и методов, предназначенных для решения задач современной криптологии с позиции дискретной математики, теории булевых функций, теории автоматов, теории систем и современной алгебры. Решен ряд модельных задач современной криптографии методами дискретной математики и методами теории хаотических динамических систем. Исследованы классы линейных и нелинейных автоматов над конечным кольцом. Решен ряд задач квантовой криптографии.

Для специалистов в областях дискретной математики, computer science, защиты информации и теории квантовых вычислений, а также для студентов и аспирантов, специализирующихся в этих областях.

Утверждено к печати Ученым советом Института прикладной математики и механики НАН Украины

Аналіз шифрсистем
В.В. Скобелєв, В.Г. Скобелєв. ІПММ НАН України, Донецьк, 2009. – 479с. (на російській мові)

ISBN 978-966-02-5126-7

Монографія присв'ячена розробці математичних моделей та методів, які призначені для вирішення задач сучасної криптології з позиції дискретної математики, теорії булевих функцій, теорії автоматів, теорії систем та сучасної алгебри. Вирішено низку модельних задач сучасної криптографії методами дискретної математики та методами теорії хаотичних динамічних систем. Досліджено класи лінійних та нелінійних автоматів над скінченим кільцем. Вирішено низку задач квантової криптографії.

Для спеціалістів в галузях дискретної математики, computer science, захисту інформації та теорії квантових обчислень, а також для студентів та аспирантів, які спеціалізуються у цих галузях.

ISBN 978-966-02-5126-7

ПРЕДИСЛОВИЕ

На современном этапе развития общества стремительное проникновение информационных технологий во все сферы жизнедеятельности человека превратило информацию в товар (часто, в стратегический товар) и выдвинуло проблему ее защиты в число наиболее актуальных проблем. Интенсификация исследований, направленных на решение этой многогранной и сложной проблемы, привела к формированию ряда научных направлений, среди которых современная криптология (до последнего времени полностью закрытое направление исследований) играет одну из центральных ролей.

Для криптологии (как и для любого научного направления, предназначенного для решения практических задач, определяемых современным состоянием технических средств) характерно использование (часто недостаточно проработанных именно с позиции решения задач криптологии) моделей и методов из различных разделов математики. К ним относятся такие классические разделы математики со своей сложившейся тематикой исследований, как комбинаторный анализ, теория булевых функций, теория автоматов, теория алгоритмов, конечные алгебраические системы. Более того, в криптологии начинают интенсивно использоваться модели и методы из таких формируемых в настоящее время разделов математики, как теория детерминированного хаоса динамических систем, теория фракталов и теория квантовых алгоритмов.

Широкий спектр недостаточно теоретически проработанных с позиции криптологии, часто плохо сравнимых друг с другом моделей и методов, приводит к тому то, что одним из основных методов анализа и синтеза криптографических алгоритмов является статистический анализ их качества. Упущения, допускаемые в процессе синтеза криптографических алгоритмов, а также интенсивное развитие средств вычислительной техники являются основной причиной достаточно частого пересмотра криптографических стандартов во всем мире. Понимание этой ситуации стимулировало разработку математических основ современной криптологии. По-видимому, наиболее впечатляющими результатами, полученными в этом направлении, являются развитие в течение последнего двадцатилетия теории булевых функций и теории эллиптических кривых над конечными полями. Именно разработке математических основ современной криптологии и посвящена настоящая монография.

Предметом исследования в настоящей монографии является дескриптивный, метрический и алгоритмический анализ комбинаторно-алгебраических моделей и методов, предназначенных для решения задач современной криптологии.

Монография состоит из восьми разделов.

Раздел 1 представляет собой развернутое введение. В нем изложен необходимый математический аппарат, проведен ретроспективный анализ предмета исследования, охарактеризованы задачи, модели и методы, исследуемые в монографии.

В разделе 2 на основе свойств комбинаторных структур дискретной математики исследуется решение следующих модельных задач криптографии: разрушение частот в исходном тексте на основе регулярных комбинаторных структур, «диффузия информации» на основе подгрупп симметрической группы подстановок, построение вычислительно стойкого нестационарного секретного замка, построение вычислительно стойких нестационарных поточных шифров.

В разделе 3 в терминах симметрической группы исследуются особенности применения одномерных хаотических отображений к решению следующих модельных задач криптографии: построение нестационарного шифра на основе отображения «зуб пилы» и на основе кодируемых циклических аттракторов одномерных кусочно-линейных отображений, организация многопользовательского доступа к каналу связи на основе циклических аттракторов ансамбля одномерных кусочно-линейных отображений.

В разделе 4 исследуются задачи обнаружения и локализации неисправностей в схемах, реализующих матричные, послойные и рекурсивные блоки управляемых перестановок, а также в схеме, реализующей управляемую подстановочную операцию.

Разделы 5 и 6 посвящены систематическому исследованию нового класса конечных автоматов, а именно: конечных автоматов над кольцом Z_{p^k} (p – простое число, а $k \in \mathbf{N}$).

В разделе 5 систематически исследуются линейные автоматы с лагом 1 над кольцом Z_{p^k}. Выделены подмножества автоматов, представляющих собой поточные шифры. Охарактеризованы основные нетривиальные подмножества автоматов, а также оценены мощности этих подмножеств. Установлены критерии эквивалентности автоматов, а также охарактеризованы классы эквивалентных состояний автомата. Решены задачи параметрической идентификации автомата и идентификации начального состояния автомата. Охарактеризованы множества неподвижных точек словарных функций, реализуемых инициальными автоматами. Построены канонические формы автоматов. Исследована вариация поведения автомата. Охарактеризованы линейные одномерные автоматы с лагом l.

Раздел 6 представляет собой логическое продолжение исследований, представленных в разделе 5. В нем систематически исследуются нелинейные автоматы с лагом 1 над кольцом Z_{p^k}, для которых «нелинейность» характеризуется тем, что изменение значений переменных состояний и выходных переменных представлено алгебраической суммой квадратичной и линейной форм от переменных состояний с линейной формой от входных переменных. Выделены и охарактеризованы подмножества автоматов, представляющих собой поточные шифры. Охарактеризованы классы эквивалентных состояний автоматов. Решены задачи параметрической идентификации автомата и идентификации начального состояния автомата. Исследована вариация поведения автомата. Исследованы также два типа нелинейных автоматов (Guckenheimer and Holmes автомат и free-running автомат), которые не укладываются в рамки указанных выше моделей, а также обладают нетривиальными группами симметрий. Решена задача построения поточного шифра на основе управления семейством легко-вычислимых перестановок посредством псевдофрактала, а также охарактеризован один из классов семейств легко вычислимых перестановок, применяемых при построении таких шифров.

Раздел 7 посвящен решению задач квантовой криптографии. Построен и исследован квантовый алгоритм с оракулом, предназначенный для решения задачи идентификации булевой вектор-функции, являющейся модельной задачей современного криптоанализа. Исследована вычислительная стойкость квантового протокола передачи ключа в предположении, что криптоаналитик может управлять вероятностями выбора базисных векторов, предназначенных для измерения кубита, а также одновременным изменением базисов отправителя и адресата. Построен вычислительно стойкий квантовый шифр, основанный на классическом квантовом алгоритме плотного кодирования.

В разделе 8 построена и охарактеризована многоосновная алгебраическая система, предназначенная для унифицированного представления современных шифрсистем.

Монография написана в замкнутой форме, т.е. определяются все понятия, кроме общепринятых понятий.

Представленные в монографии результаты получены авторами в соответствии с планами научных исследований, проводимых в ИПММ НАН Украины в рамках следующих тем:

1.1.4.10 «Алгебраїчні, комбінаторні, логічні та еволюційні методи дослідження дискретних та безперервних систем та їх застосування до задач ідентифікації та керування» (2004-2008 гг.);

1.1.4.14 «Логічний підхід до керування динамічними системами» (2004-2006 гг.);

III-13-07 «Обернені задачі теорії керування і сучасні комунікаційні технології» (с 2007 г.).

Основные результаты, представленные в монографии, были апробированы на научных семинарах в ИК НАН Украины, ХНУРЭ, ИПММ НАН Украины и на следующих международных конференциях:

V-VII Международные конференции «Идентификация систем и задачи управления» (SICPRO'06, SICPRO'07 и SICPRO'08) (РФ, г. Москва, ИПУ РАН);

IV Международная конференция «Параллельные вычисления и задачи управления (PACO'2008) (РФ, г. Москва, ИПУ РАН);

III-VII Сибирские научные школы-семинары с международным участием «Компьютерная безопасность и криптография» (SIBERCRYPT'04 (РФ, г. Иркутск, ТГУ и ИДСТУ СО РАН), SIBERCRYPT'05 (РФ, г. Томск, ТГУ), SIBERCRYPT'06 (РФ, г. Шушенское, ТГУ), SIBERCRYPT'07 (РФ, г. Горно-Алтайск, ТГУ и ГАГУ), SIBERCRYPT'08 (РФ, г. Красноярск, ТГУ и СГАЭУ);

IX-й Международный семинар «Дискретная математика и ее приложения» (ДМ-07) (РФ, г. Москва, МГУ, 2007 г.);

VI-VIII Международные научно-практические конференции «Информационная безопасность» (ИБ'04, ИБ'05 и ИБ'06) (РФ, г. Таганрог, ТРТУ);

IXth International Conference «CADSM 2007» (г. Поляна, Национальный технический университет «Львівська політехніка»);

Международная конференция «Моделирование-2008») (г. Киев, ИПМЭ НАН Украины);

IX Международная конференция «Системный анализ и информационные технологии» (SAIT'08) (г. Киев, Национальный технический университет «Київський політехнічний інститут»);

3-й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития» (МРФ-2008) (г. Харьков, ХНУРЭ).

Многие результаты, представленные в настоящей монографии, были опубликованы авторами ранее (см. список литературы). Однако настоящая монография – это первая попытка систематически представить все эти результаты с единых позиций.

Вклад авторов в работу над монографией следующий.

В.В. Скобелевым написаны п.1.4, пп.2.1-2.3, п.6.6, а также раздел 5.

В.Г. Скобелевым написаны пп.1.1-1.3, п.1.6, п.1.8, пп.2.5-2.7, пп.6.1-6.5, а также разделы 3, 4, 7 и 8.

Совместно авторами написаны п.1.5, п.1.7 (утверждения 1.6, 1.7 и следствия 1.8, 1.9 принадлежат В.В. Скобелеву) и п.2.4 (теорема 2.4 принадлежит В.В. Скобелеву).

Монография предназначена для специалистов в областях криптологии, квантовых вычислений, теории автоматов и дискретной математики, а также для студентов и аспирантов, специализирующихся в этих областях. Она также может быть использована преподавателями при разработке спецкурсов. Часть материала из разделов 1, 2, 6 и 7 использовалась В.Г. Скобелевым при чтении курсов лекций «Введение в криптологию» и «Математические основы криптографии» в Донецком национальном университете для студентов направления 6.080.200 «Прикладна математика», а также при чтении курса лекций «Захист інформації в телекомунікаційних мережах і системах» в Донец-

ком национальном техническом университете для студентов специальности 7.09.24.01 «Телекомунікаційні мережи і системи».

Авторы считают своим долгом выразить следующие благодарности.

В.Г. Скобелев выражает искреннюю благодарность своим научным руководителям на стадии кандидатской диссертации, профессору **А.М. Богомолову** и академику РАЕН В.Б. Кудрявцеву, чьи усилия и терпение, во многом, сформировали сегодняшние позиции и точки зрения автора на исследуемые в монографии проблемы, профессорам Г.П. Агибалову, И.Д. Горбенко и П.Ю. Костенко за полезные обсуждения большинства из представленных в монографии результатов, декану математического факультета ДонНУ профессору В.И. Сторожеву, обеспечившего возможность привлечения студентов и аспирантов ДонНУ к исследованиям в области разработки математических основ криптологии, а также директору ИПММ НАН Украины члену-корреспонденту НАН Украины А.М. Ковалеву, по инициативе которого автор с 2003 г. занялся систематическими исследованиями в области разработки математических основ криптологии.

Оба автора выражают искреннюю благодарность профессору **Ю.В. Капитоновой** и члену-корреспонденту НАН Украины А.А. Летичевскому за поддержку и полезные обсуждения результатов, связанных с исследованием автоматов над конечным кольцом.

Написание любой книги требует больших затрат сил и времени. Оба автора выражают искреннюю благодарность жене и маме, Скобелевой Галине, за ее терпение и поддержку в процессе работы над монографией.

Безусловно, что за все недостатки ответственность несут только авторы, которые будут благодарны за любые конструктивные замечания, касающиеся содержания книги.

АВТОРЫ

Январь, 2009 г., г. Донецк

СОДЕРЖАНИЕ

1. ПРОБЛЕМЫ, МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Цель настоящего раздела состоит в том, чтобы очертить предмет и объект исследования, представить математический аппарат, используемый в дальнейшем. Раздел логически подразделен на две части.

В первой части раздела (пп.1.1-1.3) дан системный анализ проблемы защиты информации и методов ее решения. В п.1.1 система информационной безопасности охарактеризована как подсистема комплексной системы безопасности организации. Выделены основные типы противников систем информационной безопасности и проблемы, связанные с компьютерной безопасностью. В п.1.2 охарактеризованы проблемы, возникающие в процессе передачи информации по каналу связи. П.1.3 содержит ретроспективный анализ криптологии.

Вторая часть раздела (пп.1.4-1.8) содержит математический аппарат, необходимый для дальнейшего изложения. В п.1.4-1.6 представлен классический математический аппарат криптологии, приведены основные понятия, определения и конструкции алгебры (п.1.4), теории автоматов (п.1.5) и теории булевых функций (п.1.6). В пп.1.7 и 1.8 представлен математический аппарат, связанный с перспективными направлениями криптологии, приведены основные понятия, определения и конструкции теории динамического хаоса (п.1.7) и квантовых вычислений (п.1.8).

1.1. Системный анализ проблемы защиты информации.

Актуальность, многогранность и стратегическое значение проблемы защиты информации на современном этапе компьютеризации общества выделили разработку моделей и методов обеспечения компьютерной и информационной безопасности в виде отдельного направления исследований. В [18,40,51,53,56,66,75,132,150,151,203,210,228,231,232,241] исследованы различные аспекты этой тематики. Ниже дан краткий системный анализ проблемы защиты информации в свете этих публикаций.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности, поддержку целостности, доступности и конфиденциальности информации. Этот комплекс мероприятий используется в течение всего жизненного цикла информации, т.е. на этапах ввода, хранения, обработки и передачи данных. При этом:

целостность информации – это гарантия возможности ее модификации только теми лицами, которые имеют на это право;

доступность информации – это гарантия того, что «злоумышленник» не сможет помешать работе законных пользователей;

конфиденциальность информации – это предотвращение несанкционированного доступа к ней.

Итак, *информационная безопасность* – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий чреватых нанесением ущерба владельцам, пользователям информации или поддерживающей инфраструктуры. Проблема защиты компьютерной информации от несанкционированного доступа систематически исследована в [231]. В настоящее время на государственном уровне разра-

ботаны четкие критерии защиты информации в компьютерных сетях от несанкционированного доступа (см., напр., [125, 221]).

Рассмотрим организацию как систему, в которой выделены объекты, подвергающиеся угрозам. К ним относятся руководство, персонал и ресурсы (материально-технические, финансовые и информационные). Для материально-технических и финансовых ресурсов достаточно хорошо проработаны методы учета, контроля и аудита.

Стратегическое значение информационных ресурсов для существования организации и части взаимодействующей с ней внешней среды, отсутствие хорошо проработанных методов защиты обуславливают необходимость выделения системы информационной безопасности в виде отдельной подсистемы комплексной системы безопасности организации. Отметим, что по своей значимости источники угроз для информационных ресурсов организации разбиваются на:

1) непреднамеренные ошибки пользователей и лиц, обслуживающих информационные системы (на их долю приходится около 65% потерь);
2) кражи и подлоги;
3) действия обиженных сотрудников;
4) стихийные бедствия (пожары, наводнения, перебои с электропитанием и т.д.).

Роль, место и объекты взаимодействия для комплексной системы безопасности организации схематически показаны на рис. 1.1. Классификация потенциально возможных угроз для организации приведена на рис. 1.2. Угрозы, направленные непосредственно против системы управления организацией, которая, как известно, имеет стратегическое значение, и существенно опирается на информационные ресурсы, представлены на рис. 1.3.

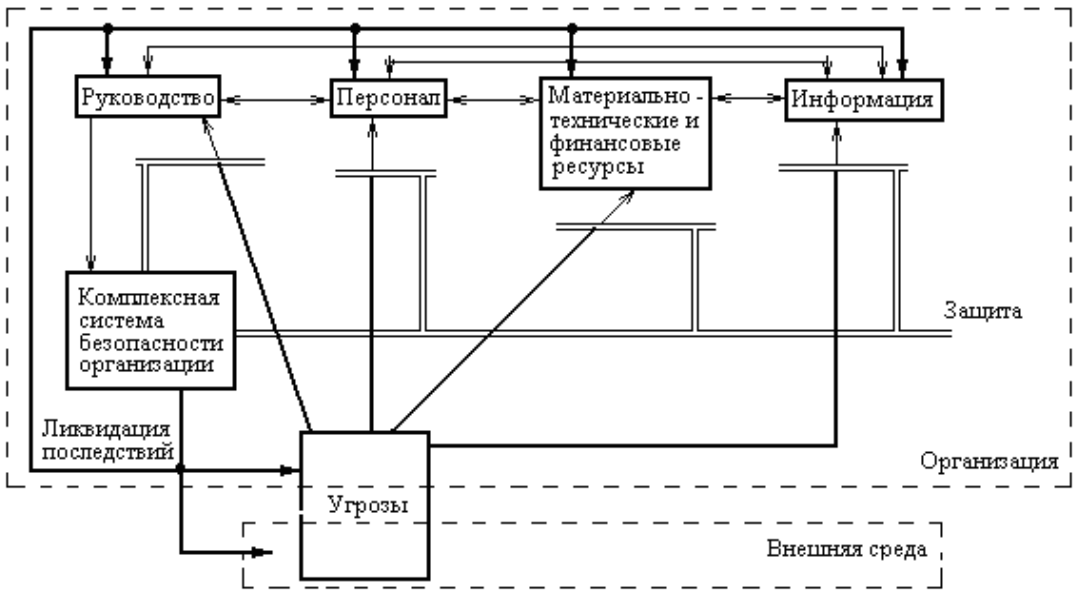


Рис.1.1. Взаимодействия комплексной системы безопасности организации.

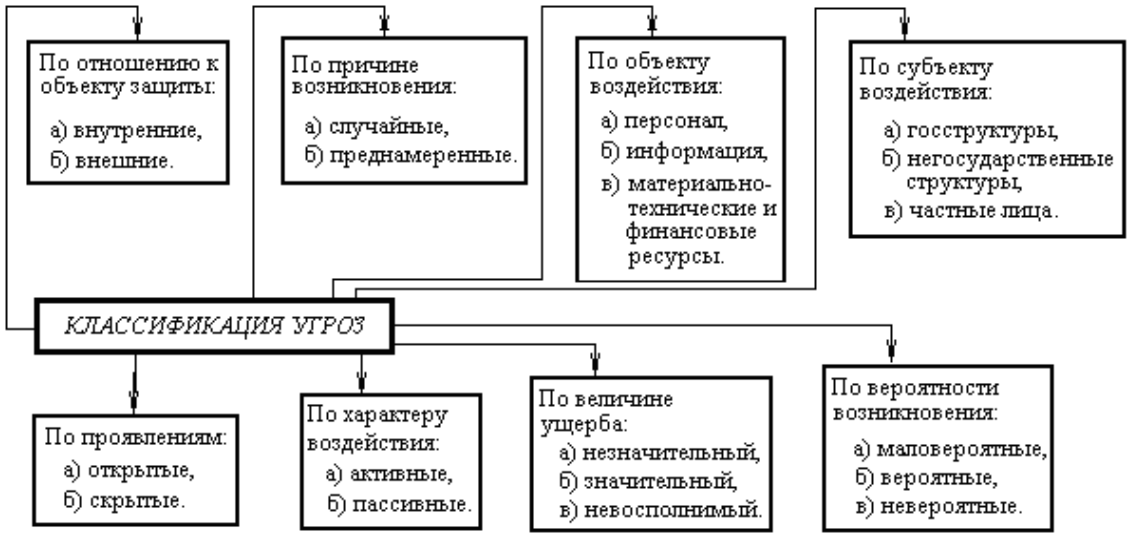


Рис.1.2. Классификация угроз организации.

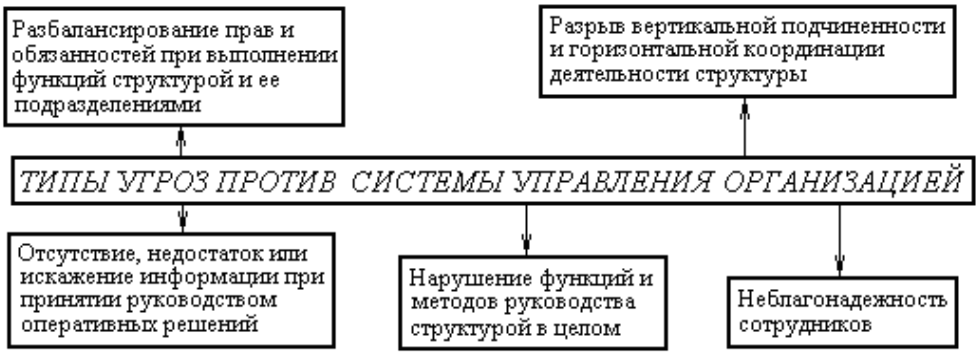


Рис.1.3. Типы угроз, направленных против системы управления организацией.

Концептуальный подход к обеспечению безопасности организации основан на законодательстве, нормативных актах и включает:

1) принципы реализации специальных мер;
2) цели и задачи защиты от угроз;
3) правовые основы защиты;
4) определение видов угроз;
5) основные направления системы безопасности.

Цели защиты от угроз включают в себя выявление, предотвращение, нейтрализацию, пресечение, локализацию, отражение и уничтожение угроз, а задачи защиты от угроз − планирование и проведение мероприятий, а также восстановительных работ на объекте защиты, формирование и использование сил и средств обеспечения безопасности.

Подчеркнем, что меры информационной безопасности на управленческом уровне должны включать в себя разработку и реализацию политики информационной безопасности организации, т.е. документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов, на контроль деятельности персонала, на эффективное

управление рисками, связанными с использованием информационных технологий.

Таким образом, на уровне концептуального подхода обеспечения комплексной системы безопасности естественно выделяются направления, представленные на рис. 1.4.

Рис.1.4. Направления обеспечения комплексной системы безопасности организации.

Рассмотрим подробнее проблему защиты информационных ресурсов организации.

Особенность защиты компьютерной информации − доминирование зарубежного аппаратно-программного обеспечения, часто не имеющего сертификатов безопасности, компьютерной техники и зарубежных программных продуктов (что недопустимо в органах управления государством и в органах, обеспечивающих жизнедеятельность и безопасность государства). Опасность при использовании зарубежного оборудования − это возможность наличия в нем аппаратных закладных устройств, что открывает неограниченные возможности для «утечки» информации и манипулирования таким оборудованием. Математический анализ таких устройств содержится в [37].

Выделяют следующие типы компьютерных преступлений:

1) кража компьютерного времени, программ, информации или оборудования;
2) мошенничество и злоупотребления;
3) ввод неавторизованной информации;

4) создание неавторизованных файлов;
5) манипуляция с разрешенной для ввода информацией;
6) неправильное использование файлов с информацией;
7) обход внутренних мер защиты;
8) разработка программ для неслужебного использования;
9) манипулирование или неправильное использование возможностей по проведению работ на компьютере.

В связи с этим можно выделить пять типов механизмов обеспечения информационной безопасности организации, представленных на рис. 1.5, а в качестве основных работ по защите информационных ресурсов организации руководствоваться схемой, представленной на рис. 1.6.

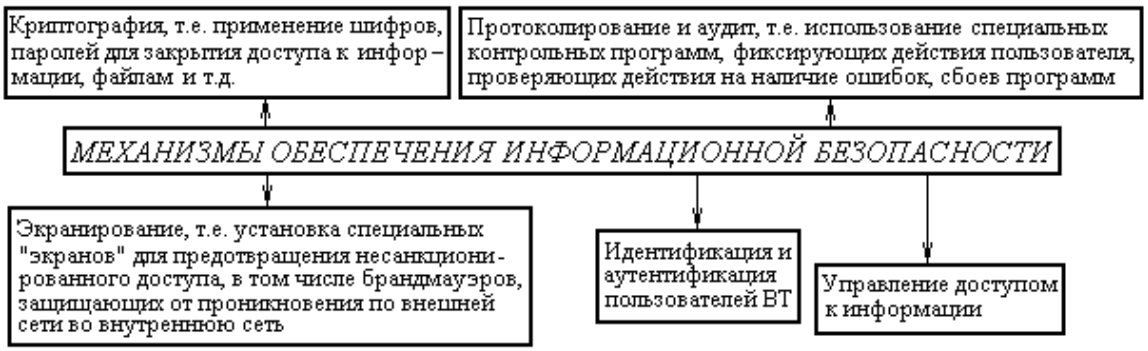


Рис. 1.5. Механизмы обеспечения информационной безопасности организации.

Рис. 1.6. Основные направления работ по защите информационных ресурсов организации.

Для того чтобы система защиты информационных ресурсов организации была эффективной, весь комплекс рассмотренных выше мероприятий должен быть направлен на защиту:

1) информации, составляющей государственную тайну (в соответствии с *перечнем сведений, подлежащих засекречиванию*);
2) информации, составляющей служебную тайну;
3) информации, защищенной патентным или авторским правом;
4) информации, составляющей коммерческую тайну.

Охарактеризуем нарушителей информационной безопасности в соответствии с их целями, уровнем доступа к компьютерной сети, квалификацией, имеющимися ресурсами и степенью принятия риска. Можно выделить следующие пять типов нарушителей.

1-й тип нарушителей − это *хакеры*. Как правило, они являются внешними лицами по отношению к атакуемой компьютерной сети. Характеризуются тем, что:

1) имеют более высокую квалификацию, чем проектировщики программных систем;
2) располагают значительным временем
3) имеют ограниченные финансовые ресурсы;
4) не принимают во внимание риск, связанный с их деятельностью.

Целью хакера является взлом системы защиты информации корпоративной компьютерной системы и/или вывод ее (или вообще, всей корпоративной компьютерной системы) из строя без получения материальных выгод.

Эффективный инструмент взлома, созданный хакерами для автоматизации процесса вторжения в компьютерные системы, подключенные к *INTERNET*, это программы, называемые *эксплоитами*. Они предназначены для вывода сервера из строя, за счет создания аварийной ситуации (типа «отказ в обслуживании»).

Так как хакеры рассматривают взламываемую систему с позиции нападающего на «единое целое», то они понимают атаки намного лучше, чем проектировщики этих систем. А поскольку программные системы достаточно «хрупкие», то ни одну программную систему защиты информации, взломанную хакером, недопустимо применять в органах государственного управления и в органах, обеспечивающих жизнедеятельность и безопасность государства.

2-й тип нарушителей − это *преступники-одиночки* (на их долю приходится наибольшая часть компьютерных преступлений). Как правило, они являются внешними лицами по отношению к атакуемой компьютерной сети. Характеризуются тем, что:

1) имеют ограниченные финансовые ресурсы;
2) имеют не всегда достаточный доступ к атакуемой системе;

3) у них недостаточно хорошо организована экспертиза, из-за чего они часто попадаются, совершив элементарную ошибку;

4) часто действуют с достаточно высокой степенью риска.

Целью преступника-одиночки является либо обычное мошенничество, либо взлом системы защиты информации корпоративной компьютерной системы для получения незаконных финансовых ресурсов за счет выявленных им недостатков в атакуемой системе.

Средства, необходимые для поимки преступника-одиночки и доказательства его вины часто значительно превышают похищаемые средства. Поэтому, а также из-за боязни «подмочить репутацию», банки обычно не предают огласке указанные преступления, так что в реальности число преступлений, совершаемых преступниками-одиночками, может существенно превосходить официальную статистику.

3-й тип нарушителей − это *злонамеренные посвященные лица*. Характеризуются тем, что:

1) являются легальными пользователями атакуемой системы;

2) имеют высокий уровень доступа в этой системе;

3) осведомлены о том как, кем и когда будет производиться расследование при обнаружении незаконных действий;

4) минимизируют риск, связанный с их деятельностью.

Целью злонамеренного посвященного лица является использование служебного положения для получения незаконных финансовых ресурсов или использование корпоративной компьютерной системы для реализации своей деятельности, не связанной с легальной деятельностью организации.

Опасность от действий злонамеренных посвященных лиц обусловлена тем, что они в момент атаки на систему информационной безопасности рассматриваются последней как лица, заслуживающие доверия. Кроме того, они имеют возможность использовать ресурсы системы информационной безопасности против нее же самой, а также хорошо осведомлены о недостатках применяемой системы информационной безопасности.

4-й тип нарушителей − это *организованная преступность*. Характеризуется тем, что:

1) располагает значительными финансовыми ресурсами;

2) имеет потенциальную возможность доступа к любой информации;

3) имеет возможность непосредственного подкупа сотрудников и возможность опосредственного подкупа высокопоставленных лиц атакуемой организации за счет их приглашения в качестве консультантов или участников будущих проектов;

4) осуществляет тщательную экспертизу последствий своих действий и оценку риска.

Целью организованной преступности является эффективная автоматизация деятельности и максимальное расширение рынка за счет киберпространства.

Организованная преступность использует следующие схемы:

1) атаки на банки, предназначенные для крупномасштабного похищения средств из банков;

2) отмывание денег, т.е. легализация доходов за счет многоходовых переводов средств с одних счетов на другие, в том числе осуществляя на электронном уровне фиктивные покупки и продажи, что легко сделать из-за анонимности банковских электронных денег;

3) присвоение личности за счет замены расположенных на чужих веб-сайтах телефонных номеров на свои (для организации эскорт-услуг, тотализаторов и т.д.) и за счет создания «липовых» веб-сайтов, мало чем отличающихся от веб-сайтов легальных фирм, которые при необходимости можно уничтожить в считанные секунды;

4) кража конфиденциальной информации о клиентах для шантажа, лоббирования своих интересов или для получения непосредственной материальной выгоды;

5) пиратство, т.е. массовый перехват и перепродажа номеров сотовых телефонов, а также массовое изготовление и продажа незаконно сделанных копий (программного обеспечения, видео-продукции), что наносит ощутимый урон легальным производителям.

5-й тип нарушителей − это *компьютерные террористы*. Характеризуются тем, что:

1) имеют недостаточные финансовые ресурсы;
2) часто имеют достаточно низкую квалификацию;
3) идут на любой риск.

Цель компьютерных террористов является дестабилизация или разрушение атакуемой системы без материальных выгод для себя.

Действия компьютерных террористов при наличии достаточного источника финансирования могут по своим последствиям значительно превзойти действия обычных террористов (атакам могут подвергнуться системы управления государственных органов, министерства обороны, ядерных электростанций, аэропортов, железнодорожного транспорта и т.д.).

Пиратство и его последствия стимулировали разработку методов защиты программного обеспечения (см., напр., [133,223,242]). Эта проблема является актуальной как для коммерческих, так и стратегических применений вычислительной техники и включает в себя:

1) защиту интеллектуальной собственности;

2) защиту от анализа функций программы в среде исполнения программы пользователем;

3) защиту от незаконного копирования и использования программного обеспечения.

В настоящее время разработаны следующие методы борьбы с нелегальным использованием программного обеспечения (хотя удовлетворительное решение этой проблемы отсутствует до сих пор):

1) привязка кода к аппаратному обеспечению, электронному ключу или доверенному серверу;

2) контроль целостности кода с хранением контрольных данных в специальных хранилищах;

3) шифрование всего кода или некоторых его блоков;

4) использование эмулятора кода;

5) запутывание кода за счет его «замусоривания» (т.е. вставки в код бессмысленных инструкций, не изменяющих функционирования программы), а также за счет перемешивания блоков команд с сохранением логики выполнения.

Рассмотрим проблемы компьютерной безопасности.

Выделяют следующие три уровня, каждый из которых порождает свои собственные проблемы обеспечения информационной безопасности.

Уровень 1 − это *изолированный компьютер, применяемый для совместного использования*. Такая ситуация приняла массовый характер, начиная с 70-х годов прошлого века. При этом возникла необходимость решения следующих трех проблем:

Проблема 1. Если системой пользуется большая группа людей, у каждого из которых есть определенные права использовать определенные программы и видеть определенные данные, то, как можно эффективно реализовать правила контроля доступа?

Проблема 2. Как удостовериться в том, что используемые программы исправны, не были модифицированы, что данные не были изменены несанкционированным образом?

Проблема 3. Как обеспечить выполнение правил лицензирования создаваемого программного обеспечения?

Проблемы 1-3 определили необходимость решения следующих пяти задач защиты информации:

1) контроль санкционированного и несанкционированного доступа к компьютеру и содержащейся в нем информации;

2) управление учетными записями и привилегиями пользователей;

3) защита от несанкционированного копирования информации;

4) защита от вирусов, т.е. от программ, которые могут «заражать» другие программы путем их модификации;

5) защита баз данных.

Уровень 2 − это *компьютер, подключенный к локальной сети*. Такая ситуация приняла массовый характер, начиная с 80-ых годов прошлого века. В дополнение к проблемам 1-3 возникла необходимость решения следующей проблемы:

Проблема 4. Как обеспечить правильную работу с большой базой данных, к которой различные люди имеют различный доступ?

Эта проблема привела к формированию формальной модели контроля доступа, содержащей следующие три категории:

1) *субъекты*;
2) *объекты*;
3) *право доступа*.

Субъект (его часто отождествляют с понятием процесс, представляющий пользователя) представляет собой сущность, которая может получать те или иные права доступа к объектам, объект представляет собой сущность, доступ к которой контролируется, а право доступа представляет собой способ доступа субъекта к объекту.

Формальная модель контроля доступа представляет собой систему

$$S = (S, O, R),$$

где S и O – конечное множество, соответственно, субъектов и объектов, а $R = \{\rho_i \mid i = 1, \ldots, n\}$ — это множество таких бинарных отношений $\rho_i \subseteq S \times O \quad (i = 1, \ldots, n)$, что $\rho_i \quad (i = 1, \ldots, n)$ определяет i-й вид доступа субъектов к объектам.

Контроль доступа может быть реализован одним из следующих двух способов:

1) определяется, что и как разрешается делать субъектам, т.е. для каждого субъекта $s \in S$ строится вектор $O(s) = (\rho_1(s), \ldots, \rho_n(s))$;

2) определяется, что, кому и как, разрешается делать с объектами, т.е. для каждого объекта $o \in O$ строится вектор $S(o) = (\rho_1^{-1}(o), \ldots, \rho_n^{-1}(o))$.

Ясно, что каждый из этих способов имеет свои сильные и слабые стороны, так как они представляют собой два различных взгляда на одну и ту же проблему.

Попытки построения формальных моделей контроля доступа стимулировали в 70-е – 80-е годы XX столетия интенсивную разработку теоретических моделей обеспечения информационной безопасности. Был разработан ряд таких моделей, каждая из которых представляет собой многоуровневую систему. Рассмотрим кратко наиболее известные из таких моделей.

Модель безопасности Белла-ЛаПадула [241] представляет собой модель автоматного типа, в которой формализованы определения субъекта, объекта, операции доступа и развит математический аппарат для действий с этими понятиями. В основе этой модели лежит

Принцип 1. Пользователи могут читать только документы, уровень секретности которых не превышает уровень их допуска, и не могут создавать документы ниже уровня своего допуска.

Важное понятие модели Белла-ЛаПадула − это *обязательный* (или *мандатный*) *допуск*, реализованный в ряде ОС.

Основные недостатки модели Белла-ЛаПадула состоят в следующем:

1) обеспечение конфиденциальности в ущерб всему остальному;

2) не проработаны задачи повышения уровня секретности совокупности данных по сравнению с уровнями секретности отдельных компонент и понижения уровней секретности отдельных компонент данных по сравне-

нию с уровнем секретности этих данных, а также задача рассекречивания информации;

3) не проработаны ситуации, когда пользователи должны работать с данными, которые они не имеют права видеть.

Отметим, что до сих пор большинство формальных моделей высокозащищенных компьютерных систем строится на основе модели Белла-ЛаПадула, модели системы военных сообщений, субъектно-ориентированной модели изолированной программной среды, а также графов доступа и информационных потоков, определенных в модели *Take-Grant* (см., напр., [51-57,232,252]).

Информационный поток от объекта-источника к объекту-приемнику − это преобразование информации в объекте-приемнике, реализуемое с использованием доступов субъектов к объектам и зависящее от информации в объекте-источнике. Классификация информационных потоков на потоки по памяти (т.е. реализация которых требует пренебрежимо малое время) и потоки по времени (т.е. для реализации которых необходим некоторый интервал времени) приводит к автоматной модели обеспечения безопасности компьютерной системы, изображенной на рис. 1.7.

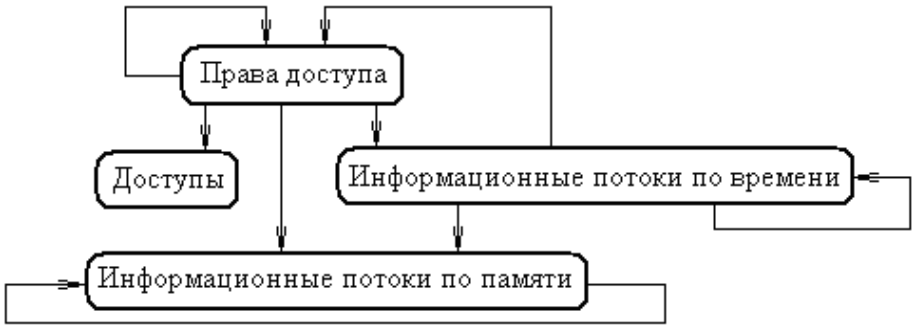


Рис. 1.7. Система безопасности информационных потоков.

Рассмотрим математический аппарат, на основе которого строятся системы мандатного разграничения доступа [51-57]. Пусть O − множество объектов, S $(S \subseteq O)$ − множество субъектов, а $R = \{read, write, append\}$, где *read* и *write* − доступ или информационный поток, соответственно, на чтение и запись, а *append* − доступ на запись в конец объекта.

Текущие доступы и информационные потоки представляются размеченным орграфом $G = (O, E \cup F)$, где O и $E \cup F$ − множество, соответственно, вершин и дуг. Элементы множества E $(E \subseteq S \times O)$ — *реальные* дуги — представляют права доступа. Элементы множества F $(F \subseteq O \times O)$ — *мнимые* дуги — представляют информационные потоки. Каждая реальная дуга помечена непустым подмножеством множества R, а каждая мнимая дуга − непустым подмножеством множества $\{read, write\}$.

Пусть $(L,\leq_L)$ − решетка уровней конфиденциальности. Для каждого момента времени определяются функция $f_S : S \to L$ − уровень доступа субъекта, функция $f_O : O \to L$ − уровень конфиденциальности объекта и функция $f_C : S \to L$ − текущий уровень доступа субъекта. Требуется, чтобы условие $f_C(s) \leq_L f_S(s)$ было выполнено для всех $s \in S$.

Состояние компьютерной системы в каждый момент времени представляется орграфом G и тройкой функций (f_S, f_O, f_C).

Доступ $(s,o,r) \in S \times O \times R$ удовлетворяет:

1) ss-свойству, если $r = append$ или $f_S(s) \geq_L f_O(o)$ при условии, что $r \in \{read, write\}$;

2) $*$-свойству, если $f_O(o) \geq_L f_S(s)$ при условии, что $r = append$, $f_S(s) \geq_L f_O(o)$ при условии, что $r = read$ и $f_C(s) \geq_L f_O(o)$ при условии, что $r = write$.

Компьютерная система соответствует требованиям безопасности модели Белла-ЛаПадула, если все ее состояния при всех возможных ее реализациях удовлетворяют ss-свойству и $*$-свойству.

В терминах введенных понятий и разрабатываются методы предотвращения возникновения запрещенных информационных потоков.

Модель безопасности «*Китайская стена*» предназначена для автоматизации брокерской деятельности, т.е. когда имеется достаточно большое число пользователей, которые не доверяют друг другу и каждому из которых необходимо обеспечить конфиденциальность. Отметим, что аналогичные ситуации возникают при автоматизации деятельности разведки и правоохранительных органов [280].

Модель безопасности Кларка-Уилсона предназначена для автоматизации бухгалтерских операций, т.е. когда с данными можно работать только по предписанным правилам (например, каждому кредиту сопоставляется равный ему дебит, и вся информация записывается в аудиторский файл).

В этой модели обеспечение конфиденциальности данных реализовано на основе симбиоза следующих двух принципов, определяющих понятие целостности данных.

Принцип 2. Обеспечивается внутреннее соответствие данных, определяемое исключительно в терминах внутреннего состояния системы.

Принцип 3. Обеспечивается внешнее соответствие данных, определяемое исключительно в терминах свойств системы по отношению к внешнему миру.

Следует отметить, что на практике все теоретические разработки оказались бесполезными для создания эффективных и экономичных ОС. Проектировщики снабжали разрабатываемые ОС своими собственными встроенными средствами обеспечения безопасности, созданными независимо от рассмотренных выше теоретических исследований. Именно опыт эксплуа-

тации разработанных в то время ОС привел к ясному пониманию того, что в процессе разработки встроенных средств обеспечения информационной безопасности для компьютерных систем необходимо придерживаться следующих двух принципов.

Принцип 4. Встроенные средства обеспечения информационной безопасности целесообразно размещать на как можно более низких уровнях, т.е. на аппаратном уровне или на уровне ОС.

Принцип 5. Встроенные средства обеспечения информационной безопасности образуют *ядро*, реализующее концепцию *монитора обращений*, т.е. абстрактного программного устройства, предназначенного для управления файлами и памятью.

Значение принципа 4 состоит в том, что уровень ОС обеспечивает большое быстродействие и простоту введения дополнительных средств обеспечения информационной безопасности. Если средства обеспечения информационной безопасности реализованы на уровне ОС, то возможность проведения «атаки уровнем ниже» весьма проблематична. Если же средства обеспечения информационной безопасности реализованы на аппаратном уровне, то возможность проведения «атаки уровнем ниже» практически неосуществима.

Значение принципа 5 состоит в том, что он дает возможность реализовать с «чистого листа» теоретическую модель информационной безопасности, что было успешно проиллюстрировано в конце 60-х годов прошлого столетия фирмами *Bell Labs* и *Honeywell* в процессе разработки ОС *Multics*, в которой была частично реализована модель Белла-ЛаПадулы.

Следует отметить, что до сих пор отсутствует глубокая проработка концепции ядра, образованного встроенными средствами обеспечения информационной безопасности. Из-за этого наблюдается тенденция «разбухания ядра» при переходе к новым модификациям ОС. В результате анализ эффективности ядра становится практически неосуществимым.

Тем не менее, именно концепция ядра, образованного встроенными средствами обеспечения информационной безопасности стимулировала разработку международных стандартов, содержащих критерии оценки безопасности информационных технологий. Такие стандарты разработаны в различных странах. В настоящее время прилагаются значительные усилия к их взаимному признанию и согласованию. Одним из первых таких шагов является появление стандартов *ISO* (*International Organization for Standardization*). Анализ алгоритмов современного стандарта *ISO/IEC 9797-1* содержится в [44].

Уровень 3 − это *компьютер*, *подключенный к INTERNET*. Такая ситуация стала массовой, начиная с 90-х годов прошлого века. В дополнение к проблемам 1-4 возникла необходимость решения принципиально новых задач предотвращения атак через *INTERNET* [73,127,150,151,203]. Рассмотрим кратко основные типы таких атак.

I. *Атаки, осуществляемые посредством разрушительных программ*, т.е. программ, предназначенных для нарушения нормального функционирования компьютера. Такие программы состоят из механизма распространения и полезной нагрузки, предназначенной для нанесения удара. Диапазон наносимых ударов включает в себя вывод повторяющихся сообщений на экран, переформатирование жесткого диска, изменение установок компьютера, изменение контроля доступа к компьютеру, кражу информации (например, пароля или секретного ключа) и передачу ее по *e-mail* и т.д. Механизмы распространения дают возможность выделить следующие три класса разрушительных программ.

1-й класс разрушительных программ − это *компьютерные вирусы*, т.е. фрагменты кода, которые, прикрепляясь к другим программам, создают свои копии. В настоящее время выделяют следующие три типа вирусов:

1. *Файловый вирус*. При запуске инфицированной программы вирус размещается в памяти так, чтобы «заразить» другие приложения, запускаемые пользователем. Именно так вирус распространяется по компьютеру. Эти вирусы относятся к 1-му поколению вирусов. Их «вымирание» вызвало появление ОС *Windows 3.1*. Файловые вирусы просто рушили эту ОС, и, как следствие, они не могли распространяться.

2. *Загрузочный вирус*. Размещается на специальном участке диска или дискеты, информация с которого загружается в память при загрузке компьютера. При внедрении в память компьютера «заражает» соответствующие секторы всех жестких дисков и дискет, вставленных в дисковод. Эти вирусы относятся ко 2-му поколению вирусов. Их «вымирание» вызвало появление ОС *Windows 95* и переход от к *CD ROM* при загрузке.

3. *Макровирус*. Представляет собой программу, написанную на языке сценариев и предназначенную для заражения файлов. Распространяется в процессе обмена данными (в том числе и через *e-mail*). Эти вирусы относятся к 3-му поколению вирусов. За ними настоящее и, как считают специалисты, будущее.

Основная опасность макровируса – это способность существовать в различных ОС. Объектами атаки макровирусов являются не только компьютеры, но и периферийные и встроенные системы. Некоторые макровирусы предназначены для воздействия на принтеры, другие воздействуют на сотовую связь. Сложность борьбы с макровирусами обусловлена тем, что в настоящее время получили широкое распространение *полиморфные вирусы*, т.е. изменяющиеся при каждом инфицировании. Их опасность состоит в том, что *антивирусные программы*, выискивая вирусы, сканируют файлы, осуществляя поиск «отпечатков», т.е. фрагментов кода, помещенных в специальную базу данных. Более того, в настоящее время получают распространение *зашифрованные вирусы*. В них «отпечатки» скрываются с помощью криптографических методов, что существенно затрудняет обнаружение таких вирусов антивирусными программами.

2-й класс разрушительных программ − это *черви*, т.е. самовоспроизводящиеся программы, которые существуют самостоятельно, «блуждают» по компьютерным сетям, причиняя те или иные повреждения. Как правило, червь приходит по *e-mail* в виде вложения в собственное сообщение. При его запуске он рассылает свои копии по всем адресам *e-mail*, находящимся в книге *Outlook Express*. Опасность червей состоит в том, что часто они подсоединяют зараженный компьютер к серверам типа *IRC*, посредством которых пользователи общаются в реальном времени, что дает возможность автору червя получать информацию из зараженного компьютера.

3-й класс разрушительных программ − это *троянские кони* (или *логические бомбы*) т.е. разрушительные фрагменты, встроенные в обычные программы, которые активизируются по специальному сигналу. Для троянского коня, следящего за буфером клавиатуры, «специальным сигналом» может быть появление комбинации, которая возможно является паролем (т.е. правильное количество цифр), идентификатором платежной ведомости или номером кредитной карты (т.е. правильное количество цифр плюс контрольная сумма). Действие троянского коня может состоять в пересылке крупных сумм денег на специальный счет, в соединении абонента с большим числом абонентов, в предоставлении удаленному пользователю несанкционированного доступа к компьютеру, в пересылке имеющихся в компьютере паролей по специальному адресу, в уничтожении файлов, в перезагрузке компьютера и т.д.

II. *Атаки на пакеты, передаваемые через INTERNET*. Сообщения, передаваемые через *INTERNET*, представляются в виде пакетов, которые пересылаются *маршрутизатором* (т.е. устройством, обеспечивающим соединение локальной сети с *INTERNET*) по специальным *маршрутам* (иными словами, *трафикам*), причем число маршрутов между отдаленными пунктами невелико. Предполагается, что маршрутизатор считывает только адрес получателя. Существует следующие два типа атак на пакеты, передаваемые через *INTERNET*.

1-й тип − это *пассивная атака*. Хакер, подсоединившись к маршрутизатору с помощью специальных программ (*анализаторов пакетов*), сканирует проходящие по маршруту пакеты с целью получения интересующей его информации, включая пароли пользователя. Анализаторы пакетов малы по объему, не проявляют себя (так как они только считывают информацию). Поэтому их обнаружение является сложной задачей.

2-й тип − это *активная атака*. К ним относятся:

1. *Подмена адреса* в заголовке пакета (*IP-spoofing*) с целью взломать аутентификацию источника пакета. После этого нападающий отправляет свой пакет адресату в надежде, что последний поверит, что пакет пришел от легального отправителя.

2. *Атака на маршрутизацию*, состоящая в том, что нападающий сообщает двум узлам *INTERNET* о том, что кратчайший маршрут между ними

проходит через его компьютер, что дает возможность сканировать отдельные узлы *INTERNET*.

В настоящее время значительное внимание уделяется разработке средств, предназначенных для защиты от атак на пакеты. К ним относятся:

1) программы типа *SSH*, предназначенные для шифрования пакетов и аутентификации внешних связей пользователя через сеть;

2) протоколы типа *SSL*, предназначенные для шифрования пакетов и идентификации подлинности трафика;

3) протокол *IPSec*, предназначенный для защиты обмена данными в локальных сетях, в корпоративных сетях и в *INTERNET*.

Отметим, что область применения протокола *IPSec* [103,203] включает в себя защищенный доступ к филиалу организации через *INTERNET*, защищенный удаленный доступ через *INTERNET*, защищенное внутри сетевое и межсетевое взаимодействие с партнерами, а также усиление защиты электронных коммерческих операций.

III. *Атаки на DNS* (*Domain Name System*), т.е. на распределенную базу данных, предназначенную для установления соответствия между *числовыми IP-адресами*, применяемыми при отправке пакетов по сети и *доменными именами*, созданными для удобства запоминания в указателях информационного ресурса или адресах *e-mail*. Компьютер, получив имя домена, запрашивает сервер службы доменных имен для перевода этого имени в *IP-адрес*, определяющий пункт назначения отправляемого сообщения. Если *DNS* взломан и сфальсифицирован, то пересылка сообщений осуществляется в соответствии с этой фальсификацией. В настоящее время отсутствует какая-либо защита *DNS*. По-видимому, эффективное решение этой проблемы ─ аутентификация на основе методов криптографии.

IV. *Атаки типа* «*отказ в обслуживании*». Предназначены для вывода компьютера или сети из строя за счет создания условий, при которых возникает нехватка временных и/или емкостных ресурсов. Основные виды таких атак – следующие:

1. *Атака синхронизации* (*SYN flooding*). Состоит в том, что на *INTERNET*-провайдер интенсивно подаются сообщения, в которых указан обратный адрес несуществующих компьютеров. Попытки *INTERNET*-провайдера связаться с этими компьютерами, прежде чем разорвать связь, приводит к паузам, недопустимым при его нормальном функционировании. В конечном итоге это приводит к аварийному отказу.

2. *Атака подпиской*. Состоит в том, что «жертва» подписывается на всевозможные каталоги. В результате «жертва» получает ежедневно настолько большое число сообщений, что выявить среди них действительно нужную информацию весьма трудоемко.

3. *Бомбежка почтой*. Состоит в отправке на сервер настолько большого числа сообщений, чтобы превысить его емкостные возможности. В конечном итоге и приводит к аварийному отказу.

Для борьбы с атаками подпиской и бомбежкой почтой предпринимаются применяется «фильтрация» *INTERNET*-провайдера или персонального компьютера с помощью специальных программ (их называют *антиспам*). При этом возникают следующие две проблемы:

1) *антиспам* достаточно быстро *стареет*, что проявляется в том, что интенсивно возрастает количество пропускаемого им спама;

2) существует опасность «фильтрации» легальной информации, что в конечном итоге приводит к ее потере.

Эффективное решение этих проблем в настоящее время отсутствует.

Отметим, что в настоящее время интенсивно разрабатываются системы, обеспечивающие защищенные многоцелевые расширения электронной почты, в том числе, системы, предназначенные для обеспечения электронного документооборота [71,114,203].

1.2. Проблемы передачи информации по каналу связи.

В процессе передачи информации по каналу связи могут возникнуть проблемы, вызванные техническим несовершенством носителей информации и передающей аппаратуры, а также проблемы, связанные с действиями *криптоаналитика*, т.е. «злонамеренными» действиями одного или нескольких лиц, направленными на несанкционированный доступ, искажение, уничтожение передаваемой информации или вообще на вывод из строя системы передачи информации. Рассмотрим эти проблемы.

Техническое несовершенство носителей информации и передающей аппаратуры приводит к появлению *ошибок*. Разработка методов *контроля* (т.е. обнаружения или исправления) ошибок − предмет исследования *теории кодирования* [21]. Суть таких методов состоит в следующем.

В терминах формальной модели определяется класс M ошибок, которые могут возникать в процессе передачи информации. В соответствии с поставленной целью (т.е. обнаружение или исправление любой ошибки, принадлежащей классу M) конструируются:

1) алгоритм $\mathsf{A}_{\mathsf{M}}^{вн.изб.}$ внесения избыточности в передаваемую информацию за счет специальным образом подобранного увеличения ее объема;

2) алгоритм $\mathsf{A}_{\mathsf{M}}^{кнтр.}$ обнаружения или исправления любой ошибки, принадлежащей классу M в переданной избыточной информации.

Доказывается *корректность* пары алгоритмов $\mathsf{A}_{\mathsf{M}}^{вн.изб.}$ и $\mathsf{A}_{\mathsf{M}}^{кнтр.}$, а также оценивается их *временна́я сложность*. Реализацию алгоритма $\mathsf{A}_{\mathsf{M}}^{вн.изб.}$ называют *кодером*, а реализацию алгоритма $\mathsf{A}_{\mathsf{M}}^{кнтр.}$ – *декодером*. Источник информации снабжается кодером, а адресат – декодером (рис. 1.8).

Рассмотрим, как решается задача внесения в передаваемую двоичную последовательность избыточности для контроля ошибок, возникающих в процессе передачи информации по каналу связи из-за технического несовершенства носителей информации и передающей аппаратуры.

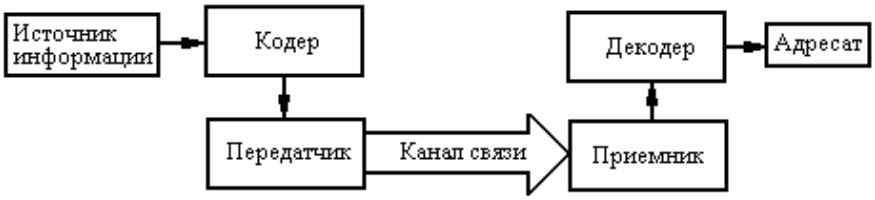


Рис. 1.8. Схема передачи информации, рассматриваемая при построении кодов, контролирующих ошибки.

Введем необходимые понятия и определения.

Пусть $\mathbf{E} = \{0,1\}$. *Блоковым* (n,k)*-кодом* $(n > k)$ называется инъекция $f : \mathbf{E}^k \to \mathbf{E}^n$. Последовательность $f(\mathbf{x}) \in \mathbf{E}^n$ $(\mathbf{x} \in \mathbf{E}^k)$ — *кодовая последовательностью* (или *кодовое слово*) для *информационной последовательности* $\mathbf{x}$. При использовании блокового (n,k)-кода передача по каналу связи информации, представленной двоичной последовательностью, осуществляется следующим образом.

В передаваемой последовательности выделяется очередная информационная последовательность (при необходимости последний фрагмент дополняется фиксированными символами до длины k). Посредством алгоритма $\mathsf{A}_{\mathsf{M}}^{вн.изб.}$, реализующего отображение f, информационная последовательность преобразуется в кодовую последовательность длины n, которая и передается по каналу связи. Величина $v_f = k \cdot n^{-1}$ называется *скоростью передачи информации*. Блоковый код f называется *высокоскоростным*, если $v_f \to 1$ $(k \to \infty)$ и *низкоскоростным*, если $v_f \to 0$ $(k \to \infty)$.

Под *ошибкой* в процессе передачи информации будем понимать изменение значений некоторых бит кодовой последовательности $f(\mathbf{x}) \in \mathbf{E}^n$ $(\mathbf{x} \in \mathbf{E}^k)$ на противоположные значения. Этот класс ошибок не исчерпывает всех ошибок, исследуемых в теории кодирования. Однако в настоящее время его принято считать *элементарным*, так как для него получены наиболее сильные результаты.

Расстоянием по Хеммингу между двоичными последовательностями $\mathbf{x} = x_1 \ldots x_n$ и $\mathbf{y} = y_1 \ldots y_n$ называется величина

$$\rho(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{n} (x_i \oplus y_i),$$

где $\oplus$ – сумма по модулю 2. Ясно, что $\rho(\mathbf{x},\mathbf{y})$ – это количество позиций, в которых последовательности $\mathbf{x}$ и $\mathbf{y}$ различаются друг от друга.

Минимальным расстоянием кода f называется величина

$$d_f^{\min} = \min_{\substack{\mathbf{x},\mathbf{y} \in \mathbf{E}^k \\ \mathbf{x} \neq \mathbf{y}}} \rho(f(\mathbf{x}), f(\mathbf{y})).$$

Эта величина являющаяся мерой различия двух наиболее близких кодовых последовательностей, следующим образом характеризует код f.

Теорема 1.1. Блоковый (n,k)-код f в процессе передачи информационной последовательности $x_1 \dots x_k$ дает возможность обнаружить

$$r_f^{обн} = d_f^{\min} - 1$$

ошибок и исправить

$$r_f^{испр} = 0{,}5 \cdot \lfloor d_f^{\min} - 1 \rfloor$$

ошибок.

Истинность этой теоремы обосновывает рис. 1.9.

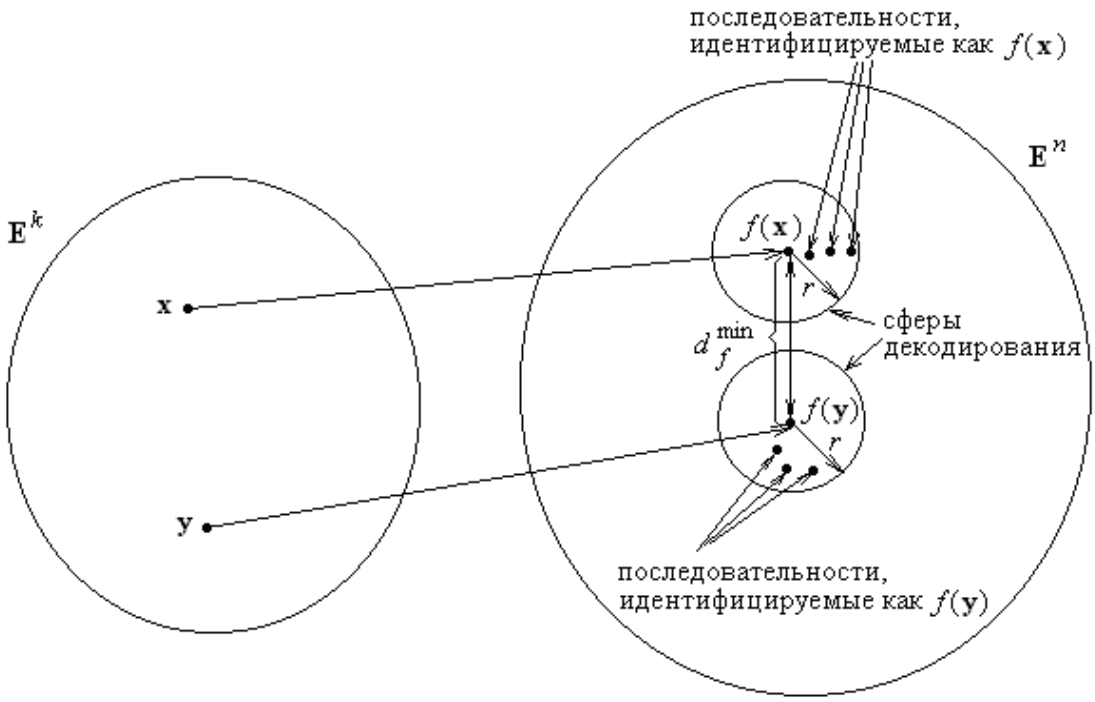


Рис. 1.9. Сферы декодирования радиуса $r = r_f^{испр}$ обеспечивают возможность исправления r ошибок.

Наиболее хорошо изучен класс *линейных* (n,k)*-кодов*. Для них множества $\mathbf{E}^k$ и $\mathbf{E}^n$ наделяются структурой линейного пространства над полем Галуа $\mathbf{GF}(2) = (\mathbf{Z}_2, \oplus, \circ)$ ($a \oplus b = a + b \pmod 2$, $a \circ b = a \cdot b \pmod 2$), а отображение $f : \mathbf{E}^k \to \mathbf{E}^n$ определяется равенством $\mathbf{y} = \mathbf{x} \circ G$, где булева $k \times n$-матрица G называется *порождающей матрицей* кода f. Для линейного блокового (n,k)-кода f истинна оценка Синглтона $d_f^{\min} \le n - k + 1$. Линейные блоковые коды, для которых в этой формуле имеет место знак равенства, называются *кодами с максимальным расстоянием*.

При решении задач теории кодирования и задач защиты информации важную роль играют линейные блоковые коды, называемые *кодами Рида-Маллера*. В классическом случае код Рида-Маллера r-го порядка длины 2^m определяется как линейный блоковый код f, порождающая матрица которого имеет вид $G = (G_0 G_1 \dots G_r)^T$, где:

1) G_0 − это вектор размерности 2^m, состоящий из одних единиц;

2) G_1 − это $m \times 2^m$-матрица, столбцы которой − все двоичные последовательности длины m;

3) G_i $(i = 2,\ldots,r)$ − это $\binom{m}{i} \times 2^m$-матрица, строками которой являются всевозможные покомпонентные произведения i строк матрицы G_1.

Отметим, что код Рида-Маллера r-го порядка длины 2^m это (n,k)-код f, для которого $n = 2^m$, $k = \sum_{i=0}^{r} \binom{m}{i}$ и $d_f^{\min} = 2^{m-r}$.

Существенная характеристика блоковых кодов состоит в том, что кодовая последовательность для очередной информационной последовательности $\mathbf{x}$ $(\mathbf{x} \in \mathbf{E}^k)$ не зависит от того, какие информационные последовательности были закодированы ранее. Это означает, что кодер и декодер для блокового кода может быть реализован с помощью *комбинационных схем*, т.е. *схем без памяти*.

Другой важный класс кодов − это *древовидные коды*. Для них кодер и декодер реализуются с помощью конечных автоматов, т.е. *схем с памятью*. Это означает, что кодовая последовательность для очередной информационной последовательности существенно зависит от того, какие информационные последовательности были закодированы ранее.

Формально, *древовидный* (n,k)*-код* — это словарная функция $f : (\mathbf{E}^k)^+ \to (\mathbf{E}^n)^+$ $(n > k)$, реализуемая инициальным конечным автоматом (такие словарные функции называются *ограниченно детерминированными функциями* или *о.д.-функциями*) и являющаяся *инъекцией*, т.е. $f(\mathbf{x}_1) \neq f(\mathbf{x}_2)$ для всех $\mathbf{x}_1, \mathbf{x}_2 \in (\mathbf{E}^k)^+$ $(\mathbf{x}_1 \neq \mathbf{x}_2)$. Конечные автоматы, реализующие о.д.-функции, являющиеся инъекциями — это *автоматы без потери информации* (*БПИ-автоматы*). Для древовидных кодов имеются отличия в терминологии по сравнению с блоковыми кодами. Элементы $\mathbf{x} \in \mathbf{E}^k$ и $\mathbf{y} \in \mathbf{E}^n$ называются *кадрами*, соответственно, информационных и кодовых символов. Последовательности кадров информационных символов $\mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_r \in (\mathbf{E}^k)^+$ соответствует такая последовательность кадров кодовых символов $\mathbf{y}_1\mathbf{y}_2\ldots\mathbf{y}_r \in (\mathbf{E}^n)^+$, что $\mathbf{y}_1 = f(\mathbf{x}_1)$ и $\mathbf{y}_i = f(\mathbf{x}_1\ldots\mathbf{x}_i) \setminus f(\mathbf{x}_1\ldots\mathbf{x}_{i-1})$ $(i = 2,\ldots,r)$, где "\" – операция левого деления слов, т.е. если b − начальный отрезок слова a, то $a \setminus b$ – это слово, полученное из слова a вычеркиванием его начального отрезка b.

Часто рассматриваются древовидные коды, удовлетворяющие условию: каждый кадр кодовых символов, начиная с $(l+1)$-го, полностью определяется фрагментом длины l последовательности кадров информационных

символов, поступивших на вход в течение последних l моментов времени (конечные автоматы, реализующие такие о.д.-функции − это *автоматы с конечной памятью*). Такой код называется *скользящим блоковым* $(n \cdot l, k \cdot l)$*-кодом*, а число $\nu = k \cdot l$ − *длиной кодового ограничения*. Общая схема кодера для скользящего блокового кода изображена на рис. 1.10.

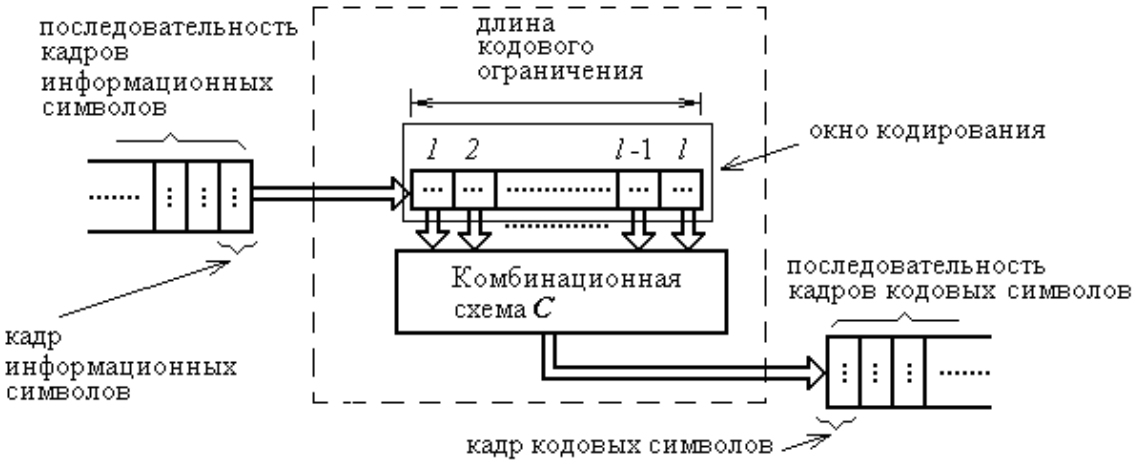


Рис. 1.10. Кодер скользящего блокового $(n \cdot l, k \cdot l)$-кода.

Отметим следующие два обстоятельства относительно рис. 1.10. Во-первых, схема $\boldsymbol{C}$ − это обычный кодер блокового кода. Во-вторых, символы, образующие кадр информационных символов, заносятся в кодер параллельно, а символы, образующие кадр кодовых символов, покидают кодер параллельно. Иногда предполагается, что символы, образующие кадр, поступают на кодер (или декодер) и покидают его последовательно, один за другим. В этом случае *скорость древовидного* (n,k)*-кода* f определяется величиной $v_f = k \cdot n^{-1}$. На языке теории алгоритмов это означает, что в этом случае исследование древовидных кодов осуществляется на основе *логарифмического веса* [15,89,141].

Структура кодеров и декодеров часто представляется в терминах *регистров сдвига*. Рассмотрим это понятие более подробно.

l*-разрядный регистр сдвига* − это синхронная схема, состоящая из последовательно соединенных l ячеек памяти (рис. 1.11.а).

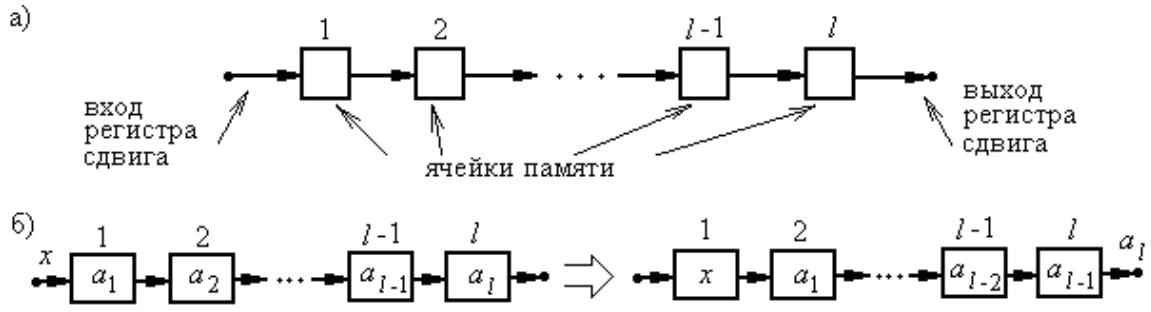


Рис. 1.11. *l*-разрядный регистр сдвига: а) общий вид; б) функционирование за один такт.

При подаче на вход символа $x \in \mathbf{E}$ происходят следующие действия (рис. 1.11.б). Содержимое каждой из ячеек памяти с номерами $1,\ldots,l-1$ сдвигается на одну ячейку вправо. Содержимое ячейки памяти с номером l «выталкивается» из регистра на его выход. В ячейку памяти с номером 1 записывается символ x.

Часто применяется *мультипликатор на скаляр* $\alpha \in \mathbf{E}$ (рис. 1.12.а). Если $\alpha = 1$ (рис.1.12.б), то символ из узла u транспортируется в узел v, а если $\alpha = 0$ (рис.1.12.в), то отсутствует связь между узлами u и v.

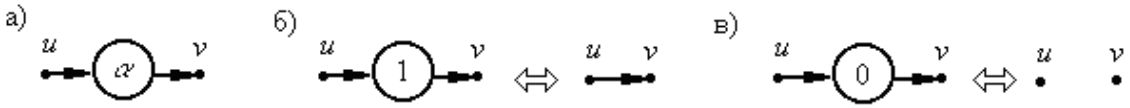


Рис. 1.12. Элемент схемы: а) умножитель на скаляр α; б) интерпретация при $\alpha = 1$; в) интерпретация при $\alpha = 0$.

Рассмотрим основные схемы, построенные на основе регистров сдвига и применяемые при построении кодеров и декодеров для кодов, контролирующих ошибки.

l-разрядный регистр сдвига с линейной обратной связью изображен на рис. 1.13.а. Пусть в ячейки с номерами $1,\ldots,l$ записаны, соответственно, символы $a_{l-1}, a_{l-2}, \ldots, a_1, a_0$, где $a_i \in \mathbf{E}$ $(i = 0,1,\ldots l-1)$.

Реакция схемы – бесконечная двоичная последовательность $b_0, b_1, \ldots, b_i, \ldots$ определяется начальными условиями $b_i = a_i$ $(i = 0,1,\ldots l-1)$ и рекуррентным выражением

$$b_i = \bigoplus_{j=1}^{l} \alpha_j \circ b_{i-j} \quad (i \geq l).$$

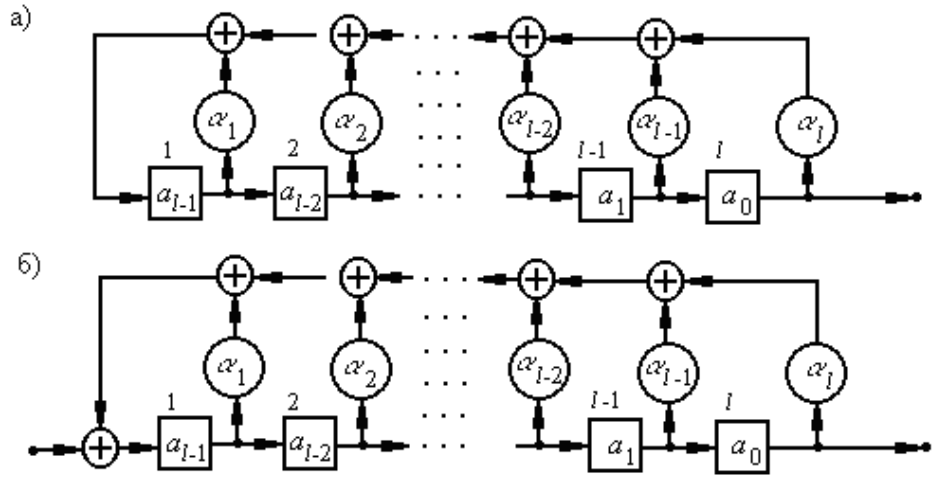


Рис. 1.13. Схемы, построенные на основе регистров сдвига: а) l-разрядный регистр сдвига с линейной обратной связью; б) l-разрядный авторегрессионный фильтр.

2. *l-разрядный авторегрессионный фильтр* изображен на рис. 1.13.б. Пусть в ячейки памяти с номерами $1,\ldots,l$ предварительно записаны, соответственно, символы $a_{l-1}, a_{l-2}, \ldots, a_1, a_0$, где $a_i \in \mathbf{E}$ $(i = 0,1,\ldots l-1)$, а на вход

схемы последовательно, бит за битом, поступает бесконечная двоичная последовательность $\gamma_0, \gamma_1, \ldots, \gamma_i, \ldots$.

Реакция схемы − бесконечная двоичная последовательность $b_0, b_1, \ldots, b_i, \ldots$ определяется начальными условиями $b_i = a_i$ $(i = 0,1,\ldots l-1)$ и рекуррентным выражением

$$b_i = \bigoplus_{j=1}^{l} \alpha_j \circ b_{i-j} \oplus \gamma_{i-l} \quad (i \geq l).$$

Следующие две схемы реализуют операции умножения и деления на фиксированный ненулевой элемент кольца многочленов $\mathbf{GF}(2)[x]$.

3. *l-разрядный фильтр с конечным импульсным откликом* (*КИО-фильтр*) изображен на рис. 1.14.а.

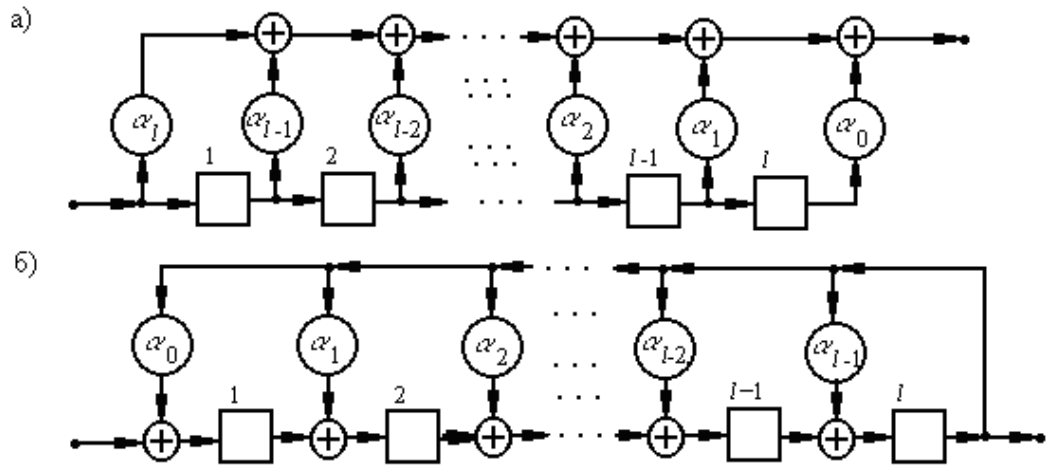


Рис. 1.14. Схемы, построенные на основе регистров сдвига: а) l-разрядный КИО-фильтр; б) схема деления на фиксированный ненулевой многочлен $a(x) \in \mathbf{GF}(2)[x]$.

Пусть в каждую ячейку памяти предварительно записан символ 0, а на вход подается двоичная последовательность $\gamma_k \gamma_{k-1} \ldots \gamma_1 \gamma_0 \underbrace{0\ldots0}_{l \text{ раз}}$.

Реакция схемы − такая двоичная последовательность $b_{l+k} b_{l+k-1} \ldots b_1 b_0$, что

$$b_j = \bigoplus_{i=0}^{k+l-j} \gamma_{j-l+i} \circ \alpha_{l-i} \quad (j = l+k, l+k-1, \ldots, 1, 0), \tag{1.1}$$

где $\gamma_r = 0$, если $r < 0$ и $\alpha_h = 0$, если $h < 0$. Положим

$$a(x) = \bigoplus_{i=0}^{l} \alpha_i \circ x^i, \quad g(x) = \bigoplus_{i=0}^{k} \gamma_i \circ x^i, \quad f(x) = a(x) \circ g(x).$$

Тогда

$$f(x) = \bigoplus_{j=0}^{k+l} b_j \circ x^j,$$

где b_j $(j = l+k, l+k-1, \ldots, 1, 0)$ вычисляются в соответствии с (1.1), т.е. схема реализует операцию умножения любого многочлена $g(x) \in \mathbf{GF}(2)[x]$ на фиксированный многочлен $a(x) \in \mathbf{GF}(2)[x]$.

4. Рассмотрим схему, изображенную на рис. 1.14.б. Пусть в каждую ячейку памяти предварительно записан символ 0, а на вход подается двоичная последовательность $b_k b_{k-1} \dots b_1 b_0$.

Реакция схемы − двоичная последовательность $\underbrace{0 \dots 0}_{l \text{ раз}} \beta_{k-l} \beta_{k-l-1} \dots \beta_1 \beta_0$, а финальное содержимое ячеек памяти – двоичная последовательность $\gamma_{l-1}, \gamma_{l-2}, \dots \gamma_1, \gamma_0$, где γ_j $(j = l-1, l-2, \dots, 1, 0)$ – это число, записанное в ячейке с номером $j+1$.

Положим

$$f(x) = \bigoplus_{i=0}^{k} b_i \circ x^i, \quad a(x) = \bigoplus_{j=0}^{l-1} \alpha_j \circ x^j \oplus x^l, \quad g(x) = \bigoplus_{j=0}^{k-l} \beta_j \circ x^j, \quad r(x) = \bigoplus_{j=0}^{l-1} \gamma_j \circ x^j.$$

Тогда

$$f(x) = a(x) \circ g(x) \oplus r(x),$$

т.е. схема реализует операцию деления (с остатком) любого многочлена $f(x) \in \mathbf{GF}(2)[x]$ на фиксированный ненулевой многочлен $a(x)$.

Кодер скользящего блокового $(n \cdot l, k \cdot l)$-кода часто реализуется с помощью n наборов КИО-фильтров (рис. 1.15). При этом:

каждый набор КИО-фильтров содержит не более чем k элементов, причем оценка k достигается хотя бы для одного набора КИО-фильтров;

разрядность каждого КИО-фильтра не превосходит числа l, причем разрядность l достигается хотя бы на одном КИО-фильтре.

Каждый КИО-фильтр реализует операцию умножения на некоторый элемент кольца многочленов $\mathbf{GF}(2)[x]$, являющийся многочленом степени не выше, чем l. Эти многочлены называются *порождающими многочленами* древовидного $(n \cdot l, k \cdot l)$-кода.

Пусть $g_{1j}(x), \dots, g_{kj}(x)$ $(j = 1, \dots, n)$ − порождающие многочлены скользящего блокового $(n \cdot l, k \cdot l)$-кода f, определяемые j-м набором КИО-фильтров. *Порождающей матрицей* кода f называется $k \times n$-матрица

$$G(x) = \begin{pmatrix} g_{11}(x) & \dots & g_{1n}(x) \\ \vdots & \ddots & \vdots \\ g_{k1}(x) & \dots & g_{kn}(x) \end{pmatrix}.$$

Представим последовательность кадров информационных символов $\mathbf{x}_1 \mathbf{x}_2 \dots \mathbf{x}_r \in (\mathbf{E}^k)^+$ вектором-строкой $\mathbf{d}(x) = (d_1(x), \dots, d_k(x))$, где $d_i(x) \in \mathbf{GF}(2)[x]$ $(i = 1, \dots, k)$ − многочлен степени не выше, чем $r-1$, коэффициенты которого – i-е координаты векторов $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_r$. Кодирование этой последовательности кадров информационных символов посредством кода f может быть представлено в виде

$$\mathbf{c}(x) = \mathbf{d}(x) \circ G(x).$$

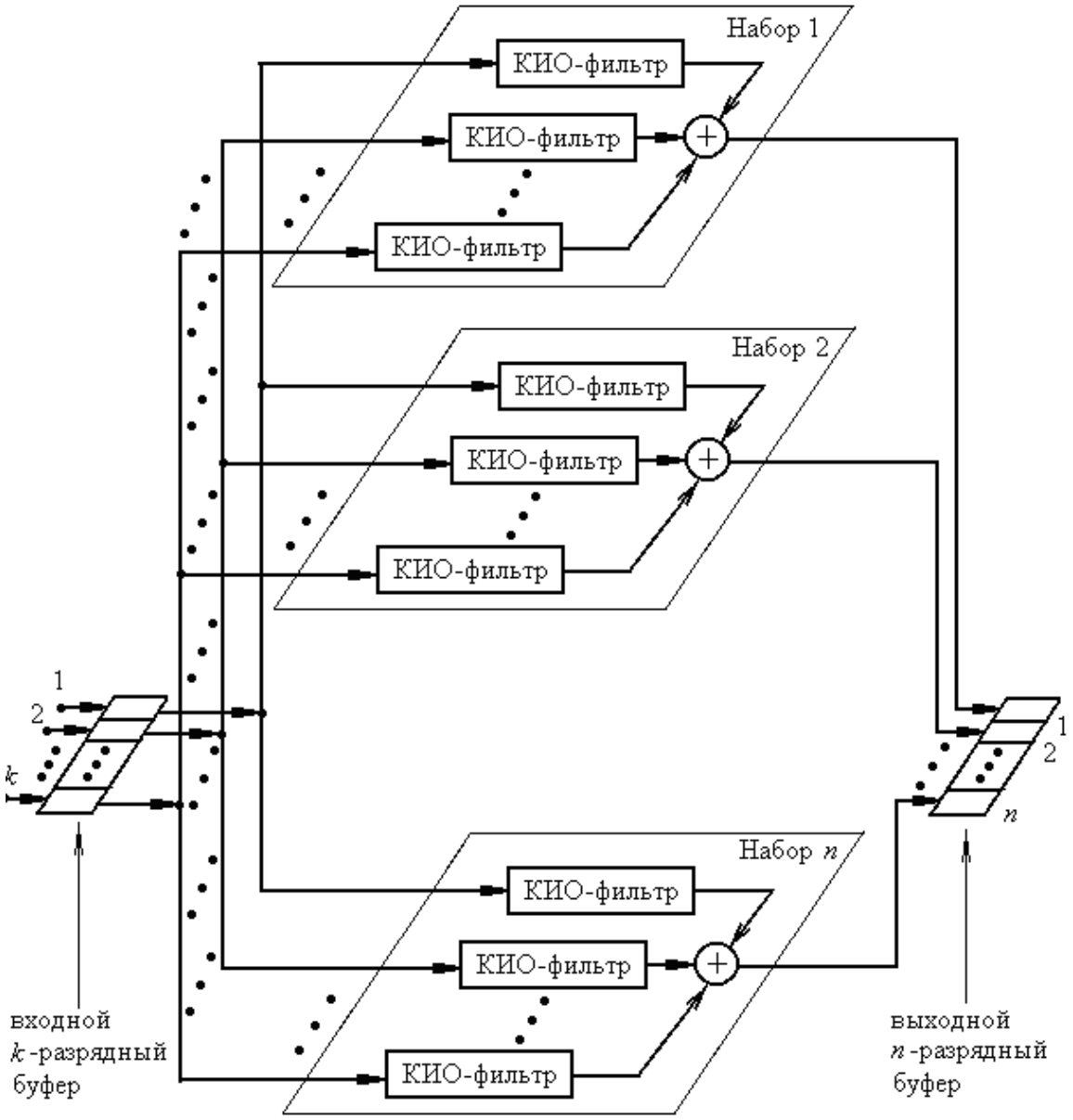


Рис. 1.15. Кодер скользящего блокового $(n \cdot l\,,\, k \cdot l\,)$-кода, построенный на основе наборов КИО-фильтров.

Проверочной матрицей кода f называется такая $(n-k)\times n$-матрица

$$H(x)=\begin{pmatrix} h_{11}(x) & \dots & h_{1n}(x) \\ \vdots & \ddots & \vdots \\ h_{n-k,1}(x) & \dots & h_{n-k,n}(x) \end{pmatrix},$$

над кольцом многочленов $\mathbf{GF}(2)[x]$, что

$$G(x)\circ H^{T}(x)=\mathbf{0}.$$

Пусть в результате передачи по каналу связи кода $\mathbf{c}(x)$ на входе декодера получена последовательность

$$\mathbf{v}(x)=(v_1(x),\dots,v_k(x)),$$

где $v_i(x)\in \mathbf{GF}(2)[x]$ $(i=1,\dots,k)$ − многочлен степени не выше, чем $r-1$.

Для контроля ошибок применяется *вектор синдромных многочленов*

$$\mathbf{s}(x) = \mathbf{v}(x) \circ H^T(x).$$

Итак, построение древовидных кодов сводится к поиску матриц $G(x)$ и $H(x)$, обеспечивающих заданный уровень контроля ошибок и требуемую скорость обработки информации.

Рассмотрим теперь проблемы, связанные с действиями *криптоаналитика*, т.е. действиями одного или нескольких лиц, направленными на несанкционированный доступ, искажение, уничтожение передаваемой информации или на вывод из строя системы передачи информации. Решение всего спектра задач, связанных с этой ситуацией и составляет предмет исследования современной *криптологии*.

Центральное понятие криптологии − *шифр*, т.е. алгоритм, преобразующий информацию к виду, скрывающему ее суть. Весь комплекс задач криптологии естественно разбивается на следующие два класса:

1) задачи разработки методов построения «хороших» шифров;
2) задачи разработки методов «взлома» шифров.

В этом контексте слово «хороший» имеет следующий смысл. Для легального пользователя применение соответствующего алгоритма не составляет труда, т.е. осуществляется с *линейной* (или близкой к ней) *временной* и *емкостной сложностью*. В тоже время для криптоаналитика сложность «взлома» шифра превышает все имеющиеся в его распоряжении вычислительные и временные ресурсы. В терминах теории алгоритмов это означает, что в настоящее время не известен (либо доказано, что не существует) алгоритм, осуществляющий «взлом» шифра с *полиномиальной временной* и *емкостной сложностью*.

Осмысленная информация обладает тем свойством, что слова и фрагменты фраз внутри потока текста или структуры изображения имеют многочисленные повторения. Повторяющуюся последовательность символов можно заменить коротким кодом, что уменьшает объем передаваемой по каналу связи информации и вероятность ее искажения. С этой целью созданы *архиваторы* (или пакеты сжатия данных).

Итак, в процессе передачи информации по каналу связи являются существенными следующие три составляющие: кодирование, шифрование и сжатие данных. Ясно, что кодирование информации посредством кода, контролирующего ошибки необходимо выполнить именно на последнем этапе. Таким образом, при организации процесса передачи информации по каналу связи возможны следующие две схемы (рис. 1.16):

сжатие данных → *шифрование* → *кодирование*
шифрование → *сжатие данных* → *кодирование.*

Возникает вопрос:

Равноправны ли эти схемы с позиции защиты информации?

Ответ на этот вопрос определяется следующими обстоятельствами.

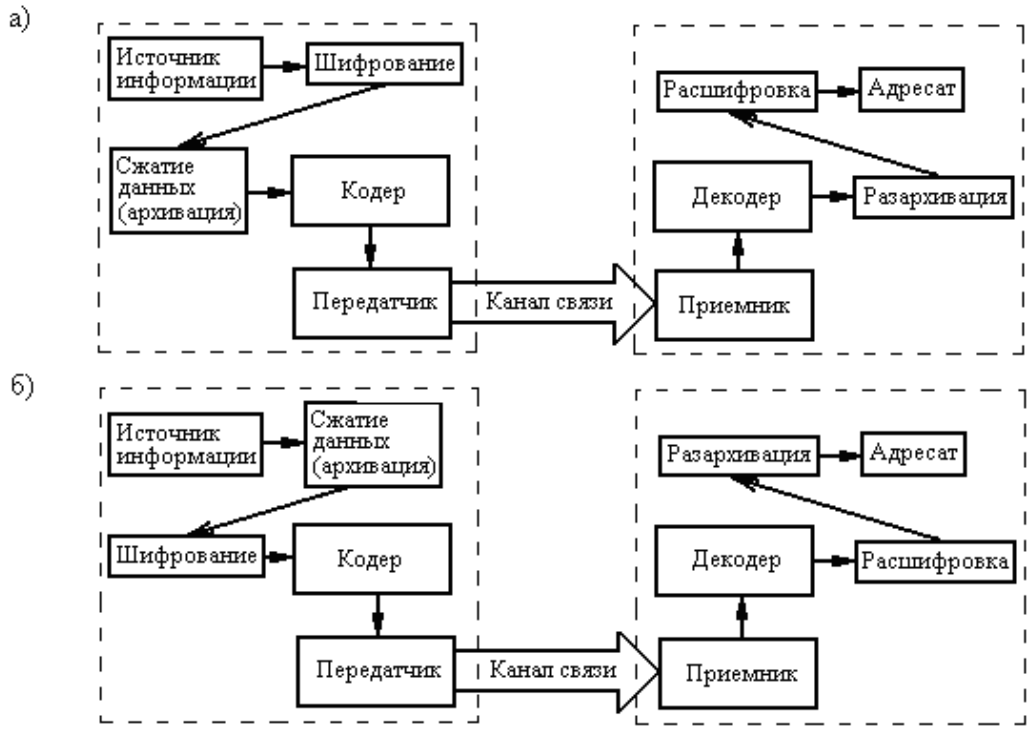


Рис. 1.16. Передача информации по каналу связи по схеме: а) шифрование → архивация; б) архивация → шифрование.

Во-первых, любой естественный язык обладает присущей ему внутренней избыточностью. Это означает, что если взять любой осмысленный текст и внести в него небольшие «помехи» (например, изменить или удалить некоторые буквы), то не составит большого труда восстановить исходный текст. Ясно, что с позиции защиты информации естественно максимально снизить ее избыточность

Во-вторых, осмысленная информация имеет значительно больше повторений, чем преобразованная информация. Поэтому большая степень сжатия достигается на сжатии осмысленной информации. При этом сама процедура сжатия информации снижает избыточность информации по сравнению с исходными данными.

Следовательно, более предпочтительной является схема

сжатие данных → шифрование → кодирование.

Всюду в дальнейшем предполагается, что передача информации по каналу связи осуществляется именно в соответствии с этой схемой.

1.3. Криптология: ретроспективный анализ.

Попытки обеспечения конфиденциальности передаваемой информации известны с древних времен. Более трех тысяч лет тому назад получил распространение следующий способ, основанный на *сокрытии самого факта передачи информации* (такие способы защиты информации в настоящее время называют *стеганографическими*). Голова гонца (как правило, раба) выбривалась. На ней несмывающейся краской наносилось сообщение. По-

сле того, как волосы отрастали, гонец отправлялся в путь. После достижения цели голова гонца выбривалась, а сообщение считывалось адресатом. Уязвимость этого способа передачи информации состоит в том, что гонец мог погибнуть, мог быть захвачен в плен и т.д. Это обстоятельство заставило обеспечивать конфиденциальность передаваемой информации более тонкими методами, такими, как изобретенный в Спарте (*IX-VIII век до н.э.*) шифр *Сциталла*. Его суть состоит в том, что для шифрования применялся цилиндр определенного диаметра (т.е. первое устройство для шифрования). На него наматывалась тонкая полоса пергамента. Текст наносился на полосу пергамента построчно по образующей цилиндра. Затем полоса пергамента сматывалась, и отправлялась адресату. Последний наматывал полосу на цилиндр такого же диаметра и читал текст вдоль оси цилиндра. Этот шифр основан на перестановке букв исходного текста. С ним связано и создание первого дешифратора – *Антисциталлы* (изобретение приписывают Аристотелю (*IV век до н.э.*)). Антисцитала − это конусообразное копье, на которое перехваченная полоса пергамента наматывалась, и передвигалась вдоль оси до тех пор, пока не появлялся осмысленный текст. Тем самым определялся диаметр цилиндра, с помощью которого осуществлялось чтение перехваченного сообщения.

Рассмотрим некоторые шифры, оказавшие существенное влияние на формирование моделей и методов современной криптологии [8,148,234].

Шифр Полибия (*II век до н.э.*). Символы алфавита, применяемого для представления сообщения, размещаются в виде прямоугольной таблицы $\mathsf{T}_{пл}$. Шифрование состоит в замене каждого символа x сообщения упорядоченной парой чисел (i, j), где i и j – номера, соответственно, строки и столбца таблицы $\mathsf{T}_{пл}$, на пересечении которых расположен символ x. Расшифровка основана на последовательном просмотре шифртекста, выделении очередной пары чисел (i, j) и замены ее символом x, расположенном в таблице $\mathsf{T}_{пл}$ на пересечении i-й строки и j-го столбца.

Шифр Тритемия (1518г.). Пусть передаваемые сообщения представлены в n-буквенном алфавите X. Таблица Тритемия – это квадратная таблица $\mathsf{T}_{тр}$ размера $n \times n$, строки которой занумерованы числами $1,2,\ldots,n$, а столбцы – элементами алфавита X, причем i-я строка $(i = 1,2,\ldots,n)$ таблицы $\mathsf{T}_{тр}$ – это алфавит X, сдвинутый циклически на i позиций влево. Каждая $2 \times n$-матрица M_i $(i = 1,2,\ldots,n)$, у которой 1-я строка – это номера столбцов таблицы $\mathsf{T}_{тр}$, а 2-я строка – это i-я строка таблицы $\mathsf{T}_{тр}$, определяет *перестановку* f_i элементов множества X, причем, если $i \neq j$ $(i, j = 1,2,\ldots,n)$, то перестановки – различные. Шифрование состоит в замене j-го символа $(j = 1,2,\ldots)$ сообщения его образом при перестановке

$$F(j)=\begin{cases} f_{j\,(\mathrm{mod}\,n)}\ , & \textit{если число } j \textit{ не кратно числу } n \\ f_n\ , & \textit{если число } j \textit{ кратно числу } n \end{cases}.$$

Расшифровка состоит в замене j-го символа $(j=1,2,\ldots)$ шифртекста его прообразом при перестановке $F(j)$, т.е. применяется перестановка $F^{-1}(j)$.

Отметим, что шифр Тритемия представляет собой обобщение *шифра Цезаря* (*I век до н.э.*). В последнем применяется только фиксированная i-я строка таблицы T_{mp}.

Шифр Альберти (1466г.). Основан на применении *шифровального диска,* состоящего из двух соосных дисков различных размеров (рис. 1.17). Больший диск – неподвижный, а меньший допускает вращение вокруг своего центра.

Пусть передаваемые сообщения представлены в n-буквенном алфавите X, а шифртексты – в n-буквенном алфавите Y, Шифровальный диск разбивался на n секторов. В каждый сектор большего диска вписано по одному символу алфавита X, а в каждый сектор меньшего диска – по одному символу алфавита Y. Корреспонденты договаривались об *индексной букве*, т.е. букве подвижного диска, принимаемой за точку отсчета. Шифрование осуществляется следующим образом. Сообщение разбивается на отдельные фрагменты. При обработке очередного фрагмента отправитель выставлял индексную букву против фиксированной заранее буквы неподвижного диска, а затем заменял символы алфавита X соответствующими символами алфавита Y. По завершению процесса шифрования очередного фрагмента сообщения положение индексной буквы изменялось, шифровался следующий фрагмент сообщения и т.д. Отправитель пересылал адресату шифртекст и информацию о положениях индексной буквы, соответствующих каждому фрагменту шифртекста. Расшифровка сводилась к выставлению индексной буквы и замене символов алфавита Y соответствующими символами алфавита X.

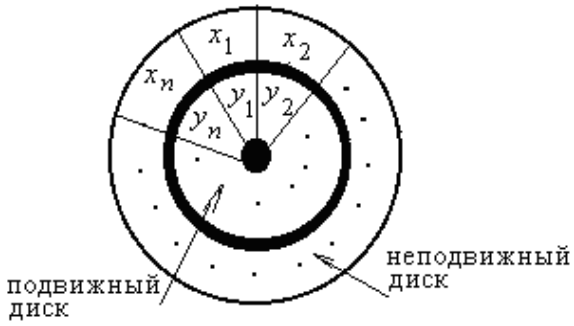


Рис. 1.17. Шифровальный диск.

Отметим следующие три обстоятельства.

Во-первых, в шифре Альберти, по-видимому, впервые реализован прототип современного понятия *сеансовый* (т.е. временный) *ключ*, роль которого играла последовательность индексных букв.

Во-вторых, шифр Альберти основан на *подстановке* вместо букв одного алфавита букв другого алфавита.

В-третьих, шифровальный диск дает возможность представить в неявном виде таблицу Тритемия. Для этого достаточно положить $X=Y$ и записать на каждом диске в одном и том же порядке символы алфавита X.

Шифры Виженера (*XVI век*). Основаны на таблице Виженера $\mathsf{T}_{вж}$, которая отличается от таблицы $\mathsf{T}_{тр}$ только тем, что в таблице $\mathsf{T}_{вж}$ строки и столбцы занумерованы элементами алфавита X. В этих шифрах впервые реализовано понятие «сеансовый ключ, существенно зависящий от передаваемого сообщения».

Пусть сообщение − это последовательность

$$\alpha_1\alpha_2\ldots\alpha_m,$$

где $\alpha_i \in X \quad (i=1,\ldots,m)$. Отправитель и адресат заранее договаривались о *пароле*, т.е. последовательности

$$\beta_1\ldots\beta_k$$

символов алфавита X.

Известны следующие два шифра Виженера.

1-й шифр Виженера. При шифровании формируются исходный текст

$$T=\alpha_1\ldots\alpha_m\beta_1\ldots\beta_k=\underbrace{\mu_1\ldots\mu_m}_{\text{сообщение}}\underbrace{\mu_{m+1}\ldots\mu_{m+k}}_{\text{пароль}}$$

и сеансовый ключ

$$K=\beta_1\ldots\beta_k\alpha_1\ldots\alpha_m=\underbrace{\nu_1\ldots\nu_k}_{\text{пароль}}\underbrace{\nu_{k+1}\ldots\nu_{m+k}}_{\text{сообщение}}.$$

Шифрование исходного текста осуществляет

Алгоритм 1.1.

Шаг 1. $i:=1$.

Шаг 2. $\gamma_i:=\delta$, где δ – символ алфавита X, расположенный в таблице $\mathsf{T}_{вж}$ на пересечении μ_i-ой строки и ν_i-го столбца, $i:=i+1$.

Шаг 3. Если $i\le m+k$, то переход к шагу 2, иначе – *конец*.

Расшифровку шифртекста $\gamma_1\ldots\gamma_{m+k}$ осуществляет

Алгоритм 1.2.

Шаг 1. $i:=1$.

Шаг 2. В ν_i-м столбце таблицы $\mathsf{T}_{вж}$ осуществляется поиск элемента γ_i.

Шаг 3. $\nu_{i+k}:=\delta$, где δ – номер строки таблицы $\mathsf{T}_{вж}$, на пересечении которой с ν_i-м столбцом расположен элемент γ_i, $i:=i+1$.

Шаг 4. Если $i\le m$, то переход к шагу 2, иначе – переход к шагу 5.

Шаг 5. $\alpha_1\alpha_2\ldots\alpha_m:=\nu_1\ldots\nu_m$ и *конец*.

Финальный отрезок

$$\gamma_{n+1}\cdots\gamma_{n+k}$$

шифртекста представляет собой «подпись» отправителем зашифрованной информации, если под «подписью» понимать зашифрованный пароль.

Таким образом, в шифрах Виженера впервые заложен механизм *аутентификации* (т.е. распознавания подлинности) пользователя и информации. Ее осуществляет

Алгоритм 1.3.

Шаг 1. $i := 1$.

Шаг 2. В ν_{m+i}-м столбце таблицы $\mathsf{T}_{вж}$ осуществляется поиск элемента γ_{m+i}.

Шаг 3. $\kappa_i := \delta$, где δ – номер строки таблицы $\mathsf{T}_{вж}$, на пересечении которой с ν_{m+i}-м столбцом расположен элемент γ_{m+i}, $i := i + 1$.

Шаг 4. Если $i \le k$, то переход к шагу 2, иначе – переход к шагу 5.

Шаг 5. Если $\kappa_1 \dots \kappa_k = \beta_1 \dots \beta_k$, то информацию принять и *конец*, иначе, информацию отвергнуть и *конец*.

2-й шифр Виженера (*шифр с автоключом*). Отличается от 1-го шифра Виженера тем, что *сеансовый ключ* имеет вид

$$K = \beta_1 \dots \beta_k \gamma_1 \gamma_2 \dots \gamma_m \ (= \nu_1 \dots \nu_{k+m}),$$

т.е. сеансовый ключ формируется в процессе шифрования исходного текста.

Шифрование осуществляется в соответствии с алгоритмом 1.1. Так как адресат располагает паролем, то он располагает и сеансовым ключом. Расшифровка осуществляется в соответствии с алгоритмом 1.2, а аутентификация − посредством алгоритма 1.3.

Стеганографическая маскировка на основе трафарета. Этот шифр получил распространение в Европе в XVI-XIX веках. Трафарет − это прямоугольник размера $k \times l$, в котором вырезано несколько прямоугольников размера 1×1.

Шифрование осуществлялось следующим образом. Трафарет накладывался на лист бумаги. В вырезы последовательно, буква за буквой, вписывалась информация, которую было необходимо передать адресату. После этого трафарет снимался с листа бумаги. В свободные позиции дописывалась буквы так, чтобы получился «безобидный текст». Если места для записи информации не хватало, то трафарет накладывался на новое место листа, и описанная выше процедура повторялась. Полученный «безобидный текст» отправлялся адресату.

Адресат накладывал трафарет на полученное сообщение, и считывал информацию. Вся «маскировка» закрывалась трафаретом.

Шифр на основе поворотной решетки (*XVI век*). Идея *поворотной решетки*, как средства шифрования, принадлежит итальянскому математику *Д. Кардано*. Такая решетка − это квадрат размера $k \times k$, в котором так вырезаны квадратики размера 1×1, что при поворотах решетки на угол $90^\circ \cdot l$ $(l = 0,1,2,3)$ каждая клетка квадрата размера $k \times k$ оказывалась под вырезом не более одного раза.

Для того чтобы обеспечить однозначность процесса преобразования информации одна из сторон поворотной решетки помечалась, а ее исходное положение и направление поворота решетки заранее фиксировалось.

Шифрование осуществлялось следующим образом. Решетка накладывалась в исходном положении на лист бумаги. В вырезы последовательно, буква за буквой, вписывалась информация, которую необходимо передать адресату. После заполнения всех вырезов, решетка поворачивалась на угол 90°, и описанная процедура повторялась. После 3-х поворотов решетка снималась и незаполненные позиции (если таковые имелись) квадрата размера $k \times k$ заполнялись произвольными символами используемого алфавита. Если места для записи информации не хватало, то решетка накладывалась на новое место листа, и описанная выше процедура повторялась. Если при заполнении последнего квадрата размера $k \times k$ вся информация оказывалась записанной, но не все вырезы в решетке были полностью использованы, то в свободные позиции записывалась заранее обговоренная последовательность символов − *финальный маркер*, фиксирующий завершение информационной последовательности. Шифртекст отправлялся адресату.

Адресат повторял все действия отправителя с той лишь разницей, что вместо «записи» осуществлял «считывание» информации.

Поворотная решетка размера $k \times k$ называется *полной*, если после обработки посредством ее квадрата размера $k \times k$ отсутствуют незаполненные позиции в случае, когда k – четное число и имеется в точности одна незаполненная позиция, расположенная в центре квадрата в случае, когда k – нечетное число.

Известно, что число полных поворотных решеток размера $k \times k$ равно

$$n(k) = 4^{\lfloor 0.25 \cdot k^2 \rfloor}. \qquad (1.2)$$

Шифр Арджента (*XVII век*). Основан на *таблице Арджента*. В ней были совмещены следующие три идеи:

для наиболее часто встречаемых символов исходного алфавита используется несколько шифр-обозначений (из-за чего частотный анализ шифртекста практически неосуществим);

используются шифр-обозначения различной длины;

шифр-обозначения применяются для часто встречаемых сочетаний букв, слогов, слов и целых фраз.

В результате реализации последней идеи «алфавит» X, нумерующий столбцы таблицы Арджента, содержал порядка 1200 символов.

Шифрование осуществлялось посредством последовательной замены каждого символа $x \in X$ сообщения любым его шифр-обозначением.

Такой подход приводит к *неоднозначности шифрования*, так как для одного и того же сообщения могут быть получены различные шифртексты, причем различной длины. Однако эта неоднозначность не влияет на корректность и сложность процесса расшифровки.

Адресат, последовательно просматривал шифртекст, осуществляя поиск очередного шифр-обозначения в столбцах таблицы Арджента. Обнаружив его, он заменял его символом $x \in X$, нумерующим этот столбец.

Шифр с вариацией размера «окна» шифрования. В XVII веке *А. Ришелье* применил шифр, для которого длина шифруемого блока исходного текста варьировалась заранее предписанным способом. Для этого в качестве *сеансового ключа* фиксировалась последовательность перестановок

$$f_0,\ldots, f_{k-1},$$

где f_i $(i = 0,1,\ldots,k-1)$ – это перестановка элементов множества $\{1,\ldots,l_i\}$.

Шифрование осуществлялось следующим образом. Исходный текст разбивался на блоки, длины которых образовывали начальный отрезок бесконечной периодической последовательности

$$l_0,l_1,\ldots,l_{k-1},l_0,l_1,\ldots,l_{k-1},\ldots.$$

При необходимости последний блок дополнялся финальным маркером до требуемой длины. Шифрование j-го $(j = 1,2,\ldots)$ блока

$$x_1\ldots x_{l_{(j-1)(\mathrm{mod}\,k)}}$$

исходного текста состояло в его замене на блок

$$x_{f_i^{-1}(1)}\ldots x_{f_i^{-1}(l_{(j-1)(\mathrm{mod}\,k)})},$$

где

$$i \equiv (j-1)\,(\mathrm{mod}\,k).$$

Адресат разбивал шифртекст на блоки, длины которых образовывали начальный отрезок последовательности

$$l_0,l_1,\ldots,l_{k-1},l_0,l_1,\ldots,l_{k-1},\ldots.$$

Расшифровка j-го $(j = 1,2,\ldots)$ блока

$$y_1y_2\ldots y_{l_{(j-1)(\mathrm{mod}\,k)}}$$

шифртекста состояла в его замене на блок

$$y_{f_i(1)}\ldots y_{f_i(l_{(j-1)(\mathrm{mod}\,k)})},$$

где

$$i \equiv (j-1)\,(\mathrm{mod}\,k).$$

Шифр Вернама (1917г.). Этот шифр предназначен для шифрования телеграфных сообщений. В нем впервые реализованы следующие три принципа:

информация представлена двоичной последовательностью

$$\mathbf{p} = \alpha_1\ldots\alpha_n;$$

сеансовый ключ − заранее заданная двоичная последовательность

$$\mathbf{q} = \beta_1\ldots\beta_n;$$

последовательность $\mathbf{q}$ − *гамма*, т.е. $\mathbf{q}$ «накладывается» на информацию посредством поразрядной операции $\oplus$ (рис. 1.18.а).

Итак, шифртекст имеет вид

$$\mathbf{w} = \mathbf{p} \oplus \mathbf{q} = \gamma_1\ldots\gamma_n,$$

где

$$\gamma_i = \alpha_i \oplus \beta_i \quad (i = 1,\ldots,n).$$

Адресат осуществляет расшифровку посредством наложения гаммы на шифртекст (рис. 1.18.б), т.е. руководствуясь правилом

$$\mathbf{p} = \mathbf{w} \oplus \mathbf{q}\,.$$

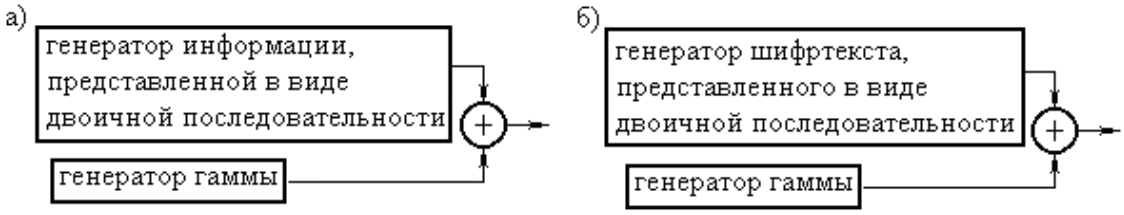


Рис. 1.18. Шифр Вернама: а) шифрование; б) расшифровка.

Отметим следующие две характеристики шифра Вернама:

1) высокая скорость процессов шифрования и расшифровки информации для легального пользователя;

2) сложность «взлома» шифра полностью определяется сложностью идентификации гаммы.

Охарактеризуем теперь современную криптологию. Это направление исследований находится на стыке *математики*, *прикладной математики* и *Computer Science* [8,17,26,59,148,203,226-229,234,287].

Предметом исследования криптологии являются математические модели, методы и алгоритмы (в том числе их программные, аппаратные и аппаратно/программные реализации), предназначенные для защиты информации в процессе ее передачи по каналу связи и в процессе ее хранения от действий человека, направленных на несанкционированный доступ, искажение или уничтожение информации. Человек, для которого предназначена информация − *легальный пользователь*, а человек, осуществляющий несанкционированный доступ, искажение или уничтожение информации – *криптоаналитик*. Итак, исследования в рамках криптологии осуществляются в среде взаимодействия этих двух лиц. Общий вид такого взаимодействия изображен на рис. 1.19. Все многообразие конкретных типов взаимодействий «легальный пользователь – криптоаналитик» получается из этой схемы в результате детализации или удаления тех или иных связей или их преобразованием в односторонние связи.

Необходимыми составляющими процесса исследования любых систем являются *анализ* и *синтез* [74,111,118]. Основными задачами анализа являются следующие задачи:

1. *Верификация*, т.е. доказательство того, что разработанная модель, метод или алгоритм выполняют свое предназначение согласно выдвинутым требованиям.

2. *Доказательство корректности* разработанного алгоритма, т.е. того, что через конечное число шагов всегда будет вычислено именно то, что требуется.

3. *Анализ сложности* разработанного алгоритма, т.е. теоретическая оценка эффективности любой его реализации.

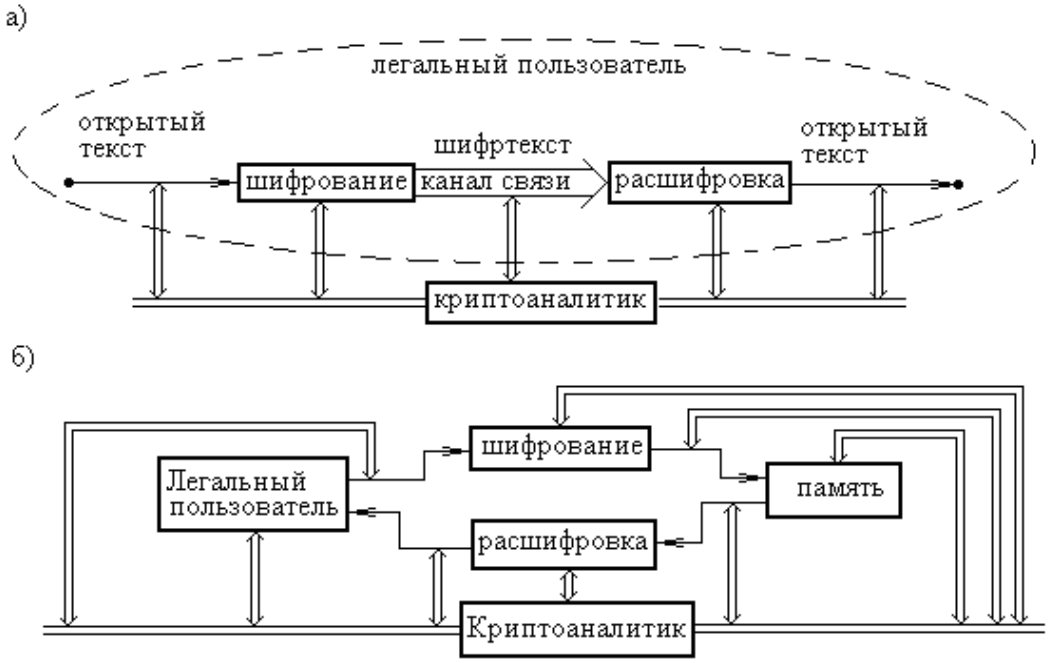


Рис. 1.19. Общий вид взаимодействия "легальный пользователь-криптоаналитик": а) в процессе передачи информации; б) в процессе хранения информации.

В криптологии важную роль также играют следующие задачи анализа:

4. *Анализ сложности идентификации* структуры, параметров или настройки систем, используемых легальными пользователями.

5. *Анализ сложности эмулирования поведения* систем, используемых легальными пользователями.

Основными задачами синтеза являются следующие задачи:

6. *Обеспечение требуемого быстродействия* реализации алгоритма.

7. *Обеспечение требуемого уровня надежности* реализации алгоритма относительно помех и сбоев в процессе ее функционирования.

8. *Обеспечение требуемого уровня* «*живучести*» реализации алгоритма при неисправностях в процессе ее функционирования.

Последней задаче уделяется мало внимания в криптологии. Хотя эта задача может быть решена стандартными методами технической диагностики [131], такой подход имеет высокую сложность. Учет структуры и характеристик конструкций, применяемых в криптологии, дает возможность решить эту задачу значительно проще.

В криптологии важную роль также играет следующая задача синтеза:

9. *Обеспечение требуемого уровня устойчивости* реализации алгоритма относительно попыток вмешательства криптоаналитика в ее функционирование (такую устойчивость алгоритма называют *имитостойкостью* алгоритма шифрования информации).

Наличие взаимодействия «легальный пользователь – криптоаналитик» приводит к тому, что в криптологии существует двойственный подход к задачам 4,5,7-9: цель легального пользователя – высокие оценки сложности решения задач 4 и 5 и положительное решение задач 7-9, а цель криптоаналитика – низкие оценки сложности решения задач 4,5 и отрицательное решение для задач 7-9. С учетом этой двойственности можно выделить следующие три составные части криптологии:

1. *Криптография*. Ее цель − разработка и реализация «хороших» моделей и методов шифрования информации.

2. *Криптоанализ*. Его цель − разработка и реализация моделей и методов «взлома» шифров и дестабилизации функционирования систем передачи и хранения информации в шифрованном виде.

3. *Стеганография*. Ее цель − разработка и реализация моделей и методов скрытия одних сообщений в других так, что скрывается существование секретного сообщения.

Замечание 1.1. Часто к криптологии относят только криптографию и криптоанализ. Такой подход, по-видимому, методологически не корректен в силу следующих причин.

Во-первых, стеганографические методы применялись для шифрования информации на протяжении всей истории человечества с момента появления письменности.

Во-вторых, шифры, основанные на детерминированном хаосе динамических систем и шифры, основанные на методах фрактальной геометрии, приводят к появлению «эффекта сбоя» в процессе передачи графических или звуковых объектов, что, по своей сути, представляет собой стеганографический эффект.

В-третьих, в последнее время возрос интерес к разработке семантических шифров в форме осмысленного текста постороннего содержания [110].

Чтобы избежать неточностей в процессе анализа основных понятий криптологии, будем использовать следующую формальную модель.

Определение 1.1. Назовем шифром систему

$$\mathsf{S} = (E, D, \mathsf{M}, \mathsf{C}, \mathsf{K}_1, \mathsf{K}_2),$$

где E – алгоритм шифрования, D – алгоритм расшифровки, M – множество открытых текстов, C – множество шифртекстов, K_1 – множество ключей, применяемых для шифрования, а K_2 – множество ключей, применяемых для расшифровки информации.

Ключ $K_1 \in \mathsf{K}_1$ − это параметр, осуществляющий такую настройку алгоритма E, что алгоритм E_{K_1} реализует биекцию множества M на множество C. Аналогичным образом, ключ $K_2 \in \mathsf{K}_2$ − это параметр, осуществляющий такую настройку алгоритма D, что алгоритм D_{K_2} реализует биекцию множества C на множество M.

Условие согласованности шифра S между двумя пользователями состоит в том, что существует такая биекция $\kappa : \mathsf{K}_1 \to \mathsf{K}_2$, что

$$M = D_{\kappa(K_1)}(E_{K_1}(M)) \quad (K_1 \in \mathsf{K}_1, M \in \mathsf{M})$$

и

$$C = E_{\kappa^{-1}(K_2)}(D_{K_2}(C)) \quad (K_2 \in \mathsf{K}_2, C \in \mathsf{C}).$$

Рассмотрим классификацию шифров.

Определение 1.2. Шифр $\mathsf{S} = (E, D, \mathsf{M}, \mathsf{C}, \mathsf{K}_1, \mathsf{K}_2)$ называется:

1) симметричным шифром, если κ и κ^{-1} – легко вычислимые функции;

2) асимметричным шифром, если κ (а также κ^{-1}) зависит от таких фиксируемых одним из пользователей параметров $a_1, \ldots, a_k$, что:

а) если значения $a_1, \ldots, a_k$ известны, то $\kappa_{a_1,\ldots,a_k}$ и $\kappa^{-1}_{a_1,\ldots,a_k}$ – легко вычислимые функции;

б) если значения некоторых параметров $a_1, \ldots, a_k$ не известны, то либо $\kappa_{a_1,\ldots,a_k}$, либо $\kappa^{-1}_{a_1,\ldots,a_k}$ не является легко вычислимой функцией или не известен полиномиальный алгоритм для его вычисления.

Из определения 1.2 вытекает, что для симметричного шифра существует алгоритм, который по любому заданному ключу $K_1 \in \mathsf{K}_1$ вычисляет ключ $K_2 = \kappa(K_1)$ с полиномиальной сложностью, а также существует алгоритм, который по любому заданному ключу $K_2 \in \mathsf{K}_2$ вычисляет ключ $K_1 = \kappa^{-1}(K_2)$ с полиномиальной сложностью. Поэтому считают, что симметричный шифр «взломан», если ключ $K_1 \in \mathsf{K}_1$ или соответствующий ему ключ $K_2 \in \mathsf{K}_2$ становятся известными. Это означает, что для симметричного шифра $K_1 \in \mathsf{K}_1$ и $K_2 \in \mathsf{K}_2$ являются *секретными ключами*. Для асимметричного шифра *секретным ключом* являются параметры $a_1, \ldots, a_k$. Остальные параметры, если таковые имеются, являются *открытым ключом*.

Определение 1.3. Шифр $\mathsf{S} = (E, D, \mathsf{M}, \mathsf{C}, \mathsf{K}_1, \mathsf{K}_2)$ называется:

1) блочным шифром, если открытый текст разбивается на блоки одинаковой длины l (при необходимости последний блок дополняется финальным маркером для достижения длины l) и каждый блок, независимо от остальных блоков, обрабатывается с помощью одного и того же алгоритма;

2) поточным шифром, если открытый текст так разбивается на отдельные символы, что обработка полученного слова осуществляется инициальным конечным БПИ-автоматом.

Замечание 1.2. В настоящее время нет поточных асимметричных шифров, приемлемых для эффективного промышленного применения.

Пример 1.1. В 1977г. Р. Ривест, А. Шамир и Л. Адлеман предложили следующий шифр, ныне известный как *RSA* [297].

Случайным образом выбираются два *простых* числа p и q, а также число e, взаимно простое с числом $(p-1)\cdot(q-1)$. Положим

$$n = p \cdot q$$

и вычислим такое число d, что

$$d \cdot e \equiv 1 (\mathrm{mod}\,(p-1)\cdot(q-1)).$$

Шифрование двоичной последовательности осуществляется следующим образом: выделяем очередной фрагмент m длины $\lfloor \log n \rfloor$, и полагаем

$$c = m^e \ (\mathrm{mod}\, n).$$

Расшифровка осуществляется в соответствии с формулой

$$m = c^d \ (\mathrm{mod}\, n).$$

Параметры p и q – секретный ключ. В настоящее время временная сложность наилучшего из известных алгоритмов разложения числа n на два простых множителя равна

$$T = O(e^{c\cdot\sqrt[3]{n}}) \quad (n \to \infty),$$

где c – положительная константа. Следовательно, *RSA* – асимметричный шифр. Возможны следующие два варианта его применения.

Пусть $K_1 = e$ – открытый ключ, а $K_2 = d$ – закрытый ключ. Быстро зашифровать двоичную последовательность может любой пользователь. Однако осуществить быструю расшифровку могут только те пользователи, которым известен секретный ключ.

Пусть $K_2 = d$ – открытый ключ, а $K_1 = e$ – закрытый ключ. Быстро расшифровать двоичную последовательность может любой пользователь. Однако осуществить быстрое шифрование могут только те пользователи, которым известен секретный ключ.

С учетом различных типов преобразования информации в настоящее время принято выделять классы шифров, представленные на рис. 1.20.

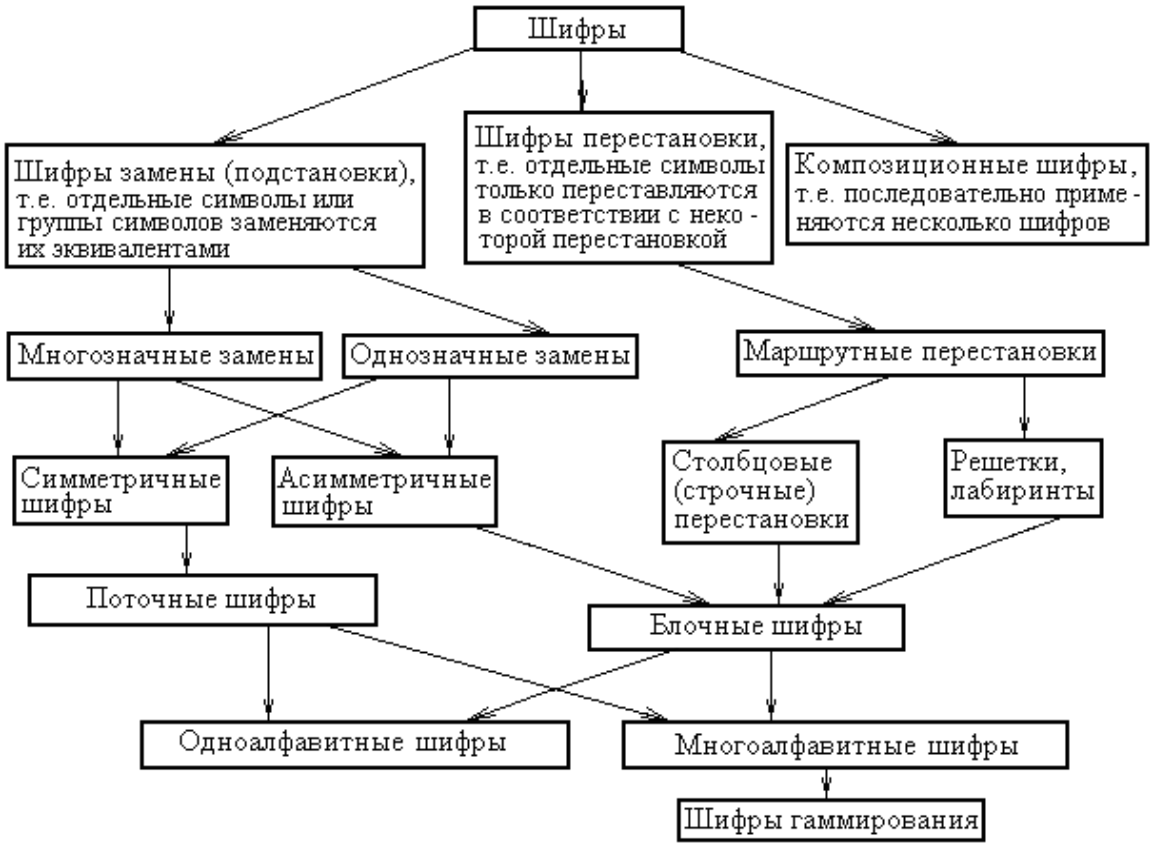


Рис. 1.20. Классы шифров.

Рассмотрим, что нужно сделать для того, чтобы шифр можно было эффективно применить для защиты информации.

Во-первых, необходимо решить *задачу управления ключами*, т.е. осуществить генерацию ключей и распределить их между пользователями. Для этого предназначена *система управления ключами*.

Во-вторых, при получении информации необходимо убедиться в том, что она не была искажена в процессе ее пересылки (т.е. проверить ее *целостность*), а отправитель – именно тот за кого он себя выдает (т.е. установить *авторство*). Комплексное решение этих задач обеспечивает *система аутентификации* информации и пользователя.

В-третьих, такая информация, как *электронный документ*, должна иметь *подпись* соответствующего лица. При этом необходимо предотвратить конфликты, связанные с попытками отказа от авторства информации, от факта ее получения адресатом и от времени отправления или получения информации. Комплексное решение этих задач обеспечивает *система электронной цифровой* подписи (ЭЦП). Иногда подсистема установки метки времени выделяется в отдельную систему.

В-четвертых, при взаимодействии локальной компьютерной сети с *Internet* необходимо обеспечить защиту ресурсов и файлов каждого пользователя, электронной почты, обмена данными в локальных, корпоративных и глобальных сетях. Решение этой задачи включает в себя криптографическую защиту информации при внутри сетевом и межсетевом взаимодействии, а также защиту информации на уровне удаленного доступа к ней через *Internet*. Специальные шифры применяются для защиты систем мониторинга системным администратором от атак со стороны внутренних пользователей сети. Для защиты от атак со стороны внешних пользователей применяются системы, называемые *брандмауэрами* или *фарэволами*.

Цель криптоанализа состоит в разработке и реализации методов «взлома» шифров или дестабилизации систем передачи и хранения информации в шифрованном виде. Действия криптоаналитика, направленные на «взлом» шифра, называют *атакой*. В 1883г. Керкгоффс сформулировал следующие требования, которым должен удовлетворять любой шифр (их в формализованном виде применяют в настоящее время, так как их нарушение заведомо облегчает действия криптоаналитика):

1) шифр не раскрываем теоретически или практически;
2) компрометация шифра не должна причинять неудобств легальным пользователям;
3) секретный ключ запоминается без каких-либо записей;
4) шифртекст должен быть представлен в такой форме, чтобы его можно было передать по телеграфу;
5) аппаратура шифрования должна быть портативной и такой, чтобы ее мог обслужить один человек;
6) шифр прост в эксплуатации.

Отметим следующие обстоятельства.

Фраза «теоретическая не раскрываемость шифра» означает, что апостериорная информация криптоаналитика равна его априорной информации. Шифры, удовлетворяющие этому условию, называются *абсолютно стойкими* (или *совершенными*) шифрами [72,227].

Для них истинны следующие два положения:

если множество открытых текстов бесконечное, то не существует алгоритм, осуществляющий «взлом» шифра;

если множество открытых текстов конечное, то вне зависимости от предыдущего опыта криптоаналитика, основанного на внешнем наблюдении шифра, любой алгоритм «взлома» шифра – это перебор вариантов, формирующий достаточно большое по мощности множество возможных открытых текстов, причем апостериорные вероятности этих открытых текстов равны их априорным вероятностям.

К совершенным шифрам относится шифр Вернама при использовании случайной равновероятной гаммы. Схемы вероятностного шифрования исследованы в [3,45,86], а обзор математических моделей датчиков шума содержится в [207].

Фраза «практическая не раскрываемость шифра» означает, что любой алгоритм его «взлома» имеет экспоненциальную временную сложность. Такие шифры называют *вычислительно стойкими*.

Так как доказательство того, что любой алгоритм решения данной задачи имеет экспоненциальную временную сложность − одна из наиболее сложных проблем дискретной математики, то в криптографии часто используют ослабленное требование, состоящее в том, что любой известный в настоящее время алгоритм решения данной задачи имеет экспоненциальную временную сложность.

3. Фраза «компрометация шифра не должна причинять неудобств ее легальным пользователям» означает, что шифр известен криптоаналитику, а стойкость шифра полностью определяется секретностью ключа шифрования. Поэтому под *атакой* (за исключением «взлома» стратегических шифров) понимаются действия криптоаналитика, направленные на восстановление исходного текста или ключа.

Сложность «взлома» шифра характеризуют либо сложностью вычисления ключа, либо сложностью *дедукции*, понимаемой как вычисление альтернативного алгоритма шифрования (полная дедукция) или вычисление части информации о ключе или об исходном тексте (информационная дедукция) или вычисление части исходного текста (частичная дедукция).

Атаки, направленные на «взлом» шифра делят на *пассивные* атаки (криптоаналитик наблюдает, но не изменяет передаваемые по каналу связи сообщения, может перехватить часть из них и подвергнуть криптоанализу) и *активные* атаки (криптоаналитик может вмешиваться в процесс переда-

чи информации по каналу связи, т.е. удалять, добавлять или изменять эту информацию). Выделяют следующие типы пассивных атак.

1. *Атака на основе шифртекста*. По заданному множеству шифртекстов требуется найти соответствующие открытые тексты, либо алгоритм, восстанавливающий открытый текст по любому шифртексту.

2. *Атака на основе известного открытого текста*. По заданному множеству пар (открытый текст, шифртекст) требуется найти либо ключи шифрования или ключи расшифровки, либо алгоритм, восстанавливающий открытый текст по любому шифртексту, либо алгоритм, восстанавливающий шифртекст по любому открытому тексту.

3. *Атака на основе заранее подобранного текста*. Отличается от 2-й атаки только тем, что открытые тексты, либо шифртексты заранее сформированы криптоаналитиком.

4. *Атака на основе адаптивно подбираемого текста*. Отличается от 3-й атаки только тем, что открытые тексты, либо шифртексты формируется криптоаналитиком на основе реакции шифрсистемы на его предыдущие воздействия.

5. *Бандитский криптоанализ*. Криптоаналитик завладевает ключами на основе прямой кражи, шантажа или подкупа.

Атаки 1-4 допускают естественную интерпретацию в терминах *теории экспериментов с конечными автоматами*. Представим шифрсистему конечным автоматом, а ключ будем интерпретировать как *инициализацию* автомата, т.е. выбор его начального состояния. Выделяют следующие типы экспериментов с автоматом:

а) *пассивный эксперимент*, если экспериментатор наблюдает выход (возможно, и вход) автомата, но не может воздействовать на его вход;

б) *безусловный эксперимент*, если воздействия экспериментатора на автомат формируются им до начала эксперимента, а заключения экспериментатора делаются только по завершению эксперимента;

в) *условный эксперимент*, если очередное воздействие экспериментатора на автомат формируется на основе предыдущих воздействий и реакций на них автомата;

г) *простой эксперимент*, если участвует один экземпляр автомата;

д) r*-кратный* ($r \geq 2$) *эксперимент*, если участвует r экземпляров автомата, возможно при различной инициализации.

Таким образом, атака на основе шифртекста (соответственно, на основе известного открытого текста) представляет собой пассивный простой или кратный безусловный эксперимент, в котором экспериментатору для наблюдения доступен только выход (рис. 1.21.а) (соответственно, вход и выход (рис. 1.21.б)) автомата. Атака на основе заранее подобранного текста – это простой или кратный безусловный эксперимент (рис. 1.21.в). Атака на основе адаптивно подбираемого текста – это простой или кратный условный эксперимент (рис. 1.21.г).

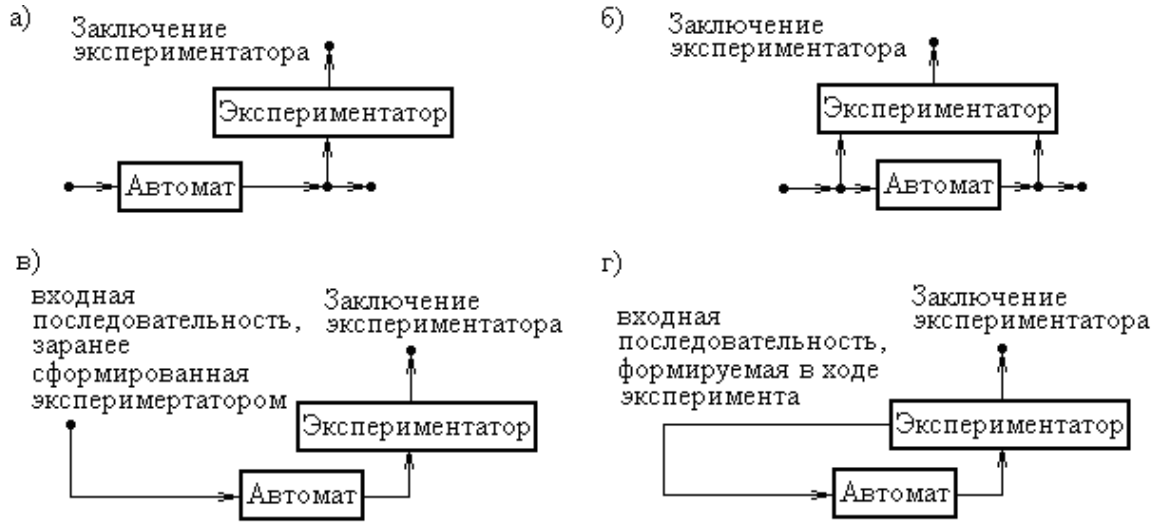


Рис. 1.21. Интерпретация пассивных криптоатак в терминах теории экспериментов с конечными автоматами.

Понятие «активная атака» в настоящее время не так хорошо формализовано, как понятие «пассивная атака». Тем не менее, выделяют следующие типы активных атак:

Атака имитации. Криптоаналитик, представляясь легальным пользователем, пересылает по каналу связи созданный им «шифртекст» и рассчитывает на то, что адресат воспримет это сообщение как подлинное (т.е. аутентичное как по пользователю, так и по информации).

Атака подмены. Криптоаналитик наблюдает пересылаемые по каналу связи сообщения легального пользователя, «изымает» часть из них, заменяет их поддельными и рассчитывает на то, что адресат воспримет это сообщение как подлинное (т.е. аутентичное по информации).

Понятие «активная атака» дает возможность представить *имитостойкость* шифра S вектором

$$(p_1(\mathsf{S}), p_2(\mathsf{S})),$$

где $p_1(\mathsf{S})$ и $p_2(\mathsf{S})$ есть вероятность, соответственно, имитации и подмены. Проявляется следующий *принцип двойственности*. Цель разработчика − это выбор такого шифра S_0, что $p_1(\mathsf{S}_0)$ и $p_2(\mathsf{S}_0)$ принимают как можно меньшие значения. Цель криптоаналитика при активной атаке на шифр S_0 – это выбор действий, гарантирующих ему достижение таких вероятностей имитации p_1 и подмены p_2, что величины $p_1(\mathsf{S}_0) - p_1$ и $p_2(\mathsf{S}_0) - p_2$ принимают как можно меньшие значения.

Множество применяемых криптоаналитиком методов можно разбить на поиск алгебраических и поиск статистических закономерностей.

При поиске алгебраических закономерностей каждое входящее в шифр S множество M, C, K_1 и K_2 рассматривается как алгебраическая система и выделяются взаимосвязи между ними методами современной алгебры, т.е. на уровне гомоморфизмов и изоморфизмов алгебраических систем.

При поиске статистических закономерностей применяется стандартная теория статистических решений с учетом статистических характеристик естественного языка.

Проиллюстрируем некоторые особенности криптоанализа на следующем примере.

Пример 1.2. Рассмотрим следующий шифр S.

Пусть $\mathsf{G} = (G, \circ)$ − конечная группа, где

$$G = \{g_1, \ldots, g_l\}.$$

Информация представляется последовательностью

$$\mathbf{p} = \alpha_0 \ldots \alpha_n \in G^+.$$

Сеансовый ключ − это «гамма»

$$\mathbf{q} = \beta_0 \beta_1 \beta_2 \ldots = \delta_1 \ldots \delta_k \delta_1 \ldots \delta_k \ldots \in G^+,$$

которая накладывается на информацию посредством поразрядной групповой операции $\circ$, т.е. шифртекст имеет вид

$$\mathbf{w} = \mathbf{p} \circ \mathbf{q} = \gamma_1 \ldots \gamma_n,$$

где

$$\gamma_i = \alpha_i \circ \beta_{i \,(\mathrm{mod}\, k)} \quad (i = 0,1,\ldots,n).$$

Такой шифр называют иногда шифром Вернама.

Криптоанализ шифра S может быть осуществлен в соответствии со следующей двухэтапной схемой: на 1-м этапе вычисляется период k сеансового ключа $\mathbf{q}$, а на 2-м этапе – сеансовый ключ $\mathbf{q}$.

1-й этап осуществляется в соответствии с методом *Ф. Казиски* (1863г.), основанном на следующем свойстве: два одинаковых отрезка открытого текста, отстоящие друг от друга на расстоянии k, зашифрованы одинаково.

Индексом совпадения в последовательности $\mathbf{p}$ называется вероятность того, что совпадают два случайно выбранных элемента этой последовательности. Этот индекс вычисляется в соответствии с формулой

$$I(\mathbf{p}) = (n \cdot (n-1))^{-1} \cdot \sum_{i=1}^{l} \mu_i \cdot (\mu_i - 1),$$

где μ_i $(i = 1,\ldots,l)$ – число вхождений элемента $g_i \in G$ в последовательность $\mathbf{p}$.

Пусть p_i $(i = 1,\ldots,l)$ − вероятность появления элемента $g_i \in G$ в осмысленном тексте. Тогда

$$I(\mathbf{p}) \approx \sum_{i=1}^{l} p_i^2$$

для любого осмысленного текста $\mathbf{p}$. С помощью этой формулы могут быть подсчитаны индексы совпадения I_o в осмысленном тексте для любого естественного языка.

Вычисление периода k сеансового ключа $\mathbf{q}$ осуществляется следующим образом. Представим шифртекст $\mathbf{w}$ в виде матрицы

$$A_m = \begin{pmatrix} \gamma_1 & \cdots & \gamma_m \\ \gamma_{m+1} & \cdots & \gamma_{2m} \\ \vdots & \ddots & \vdots \end{pmatrix} = (\mathbf{y}_1, \ldots, \mathbf{y}_m).$$

Если $m = k$, то

$$I(\mathbf{y}_j) \approx I_o$$

для каждого столбца $\mathbf{y}_j$ $(j = 1,\ldots,m)$ матрицы A_m, так как каждый столбец $\mathbf{y}_j$ $(j = 1,\ldots,m)$ матрицы A_k – это результат применения фиксированной циклической перестановки f, определенной на множестве G. Если же $m \neq k$, то

$$I(\mathbf{y}_j) \approx I_{сл},$$

где $I_{сл}$ – индекс совпадения в случайном тексте используемого естественного языка.

Так как для любого естественного языка

$$I_o \neq I_{сл},$$

то вычисление периода k сеансового ключа $\mathbf{q}$ не составляет труда.

2-й этап осуществляется следующим образом. *Взаимным индексом совпадения* в последовательностях

$$\mathbf{p}_1 = \alpha_0^{(1)} \ldots \alpha_{n_1}^{(1)} \in G^+$$

и

$$\mathbf{p}_2 = \alpha_0^{(2)} \ldots \alpha_{n_2}^{(2)} \in G^+$$

называется вероятность того, что случайно выбранный элемент последовательности $\mathbf{p}_1$ совпадает со случайно выбранным элементом последовательности $\mathbf{p}_2$. Этот индекс вычисляется в соответствии с формулой

$$J(\mathbf{p}_1, \mathbf{p}_2) = (n_1 \cdot n_2)^{-1} \cdot \sum_{i=1}^{l} \mu_i^{(1)} \cdot \mu_i^{(2)},$$

где $\mu_i^{(j)}$ $(i = 1,\ldots,l;\ j = 1,2)$ – число вхождений элемента $g_i \in G$ в последовательность $\mathbf{p}_j$. Так как период k сеансового ключа $\mathbf{q}$ известен, то известна матрица

$$A_k = (\mathbf{y}_1,\ldots,\mathbf{y}_k).$$

Рассмотрим анализ матрицы A_k в случае, когда

$$\mathsf{G} = (\mathbf{Z}_l, \oplus),$$

где

$$a \oplus b = a + b \,(\mathrm{mod}\, l)$$

для всех $a, b \in \mathbf{Z}_l$. Каждый столбец $\mathbf{y}_i$ $(i = 1,\ldots,m)$ получен в результате применения циклической перестановки

$$f_i = \begin{pmatrix} 0 & 1 & 2 & \ldots & l-\delta_i & \ldots & l-1 \\ \delta_i & \delta_i+1 & \delta_i+2 & \ldots & 0 & \ldots & \delta_i-1 \end{pmatrix}.$$

Следовательно

$$J(\mathbf{y}_i, \mathbf{y}_j) \approx \sum_{h=0}^{l-1} p_{(h-\delta_i)\,(\mathrm{mod}\, l)} \cdot p_{(h-\delta_j)\,(\mathrm{mod}\, l)} = \sum_{h=0}^{l-1} p_h \cdot p_{(h+(\delta_i-\delta_j))\,(\mathrm{mod}\, l)},$$

где p_h – вероятность появления элемента h в открытом тексте.

Пусть $\mathbf{y}_j^{\delta}$ $(\delta = 0,1,\ldots,l-1)$ – столбец, полученный в результате прибавления (по модулю l) элемента δ к каждому элементу столбца $\mathbf{y}_j$. Вычислим значения

$$J(\mathbf{y}_i, \mathbf{y}_j^{\delta}) \quad (1 \le i < j \le k;\ 0 \le \delta \le l-1).$$

Если

$$\delta = (\delta_i - \delta_j) \pmod l,$$

то $J(\mathbf{y}_i, \mathbf{y}_j^{\delta})$ близко к взаимному индексу совпадения при сдвиге на величину 0 для используемого естественного языка. Если же

$$\delta \neq (\delta_i - \delta_j) \pmod l,$$

то $J(\mathbf{y}_i, \mathbf{y}_j^{\delta})$ существенно отличается от этого индекса, т.е. вычисление сеансового ключа сводится к поиску решений системы линейных уравнений

$$(\delta_i - \delta_j) \pmod l = a_{ij} \quad (1 \le i < j \le k).$$

Выше было отмечено, что стеганографические методы обеспечения конфиденциальности информации известны с глубокой древности. В эпоху Возрождения к ним добавилось использование *симпатических чернил*, т.е. химикатов, растворами которых конфиденциальная информация наносилась между строчек безобидного письма. При высыхании секретный текст становился невидимым. Чтобы его проявить, необходимо было либо нагреть письмо, либо обработать его соответствующим химикатом. Во времена холодной войны (1945-1990гг.) разведки следующим образом использовали легальные радиостанции для секретной передачи информации своим агентам. Осуществлялся запуск магнитофонной записи безобидной передачи (новости, прогноз погоды, литературная передача или песня) на значительно меньшей скорости и на нее накладывался секретный текст, записанный с помощью азбуки Морзе. В эфир эта запись шла на обычной скорости, в результате чего записанный секретный текст не воспринимался ухом. Для получения информации агент записывал передачу на магнитофон, а затем прокручивал ее на требуемой скорости. В настоящее время под *стеганографией* [47,88,142] понимают разработку методов и технических средств, предназначенных для незаметного и надежного скрытия одних битовых последовательностей в других. Это направление имеет следующие области применения:

1) электронная коммерция, т.е. контроль процессов копирования и распространения мультимедийной информации;

2) скрытая аннотация документов (медицинские снимки, объекты в картографии, мультимедийные базы данных);

3) аутентификация для систем видео наблюдения, голосовой почты, электронного конфиденциального делопроизводства;

4) скрытая связь в военной и разведывательной деятельности.

В связи с этим в стеганографии выделяют разработку методов встраивания информации с целью ее скрытой передачи, разработку технических средств встраивания *цифровых водяных знаков* (ЦВЗ) для защиты мультимедийной информации от копирования и несанкционированного использования, а также разработку технических средств встраивания *идентификационных номеров*, *невидимых подписей*, *заголовков* и т.д.

Рассмотрим задачу встраивания информации в bmp-файл с целью ее скрытой передачи.

Исходный файл называется *пустым контейнером*, а файл, содержащий скрываемую информацию – *стего-контейнером*. При *полутоновом* изображении каждому пикселю соответствует 1 байт, определяющий оттенок серого цвета, а при цветном изображении − три байта (*RGB-компонента*), определяющих его цвет. Под *младшим значащим битом* (LSB) понимают бит, который несет меньше всего информации (рис. 1.22).

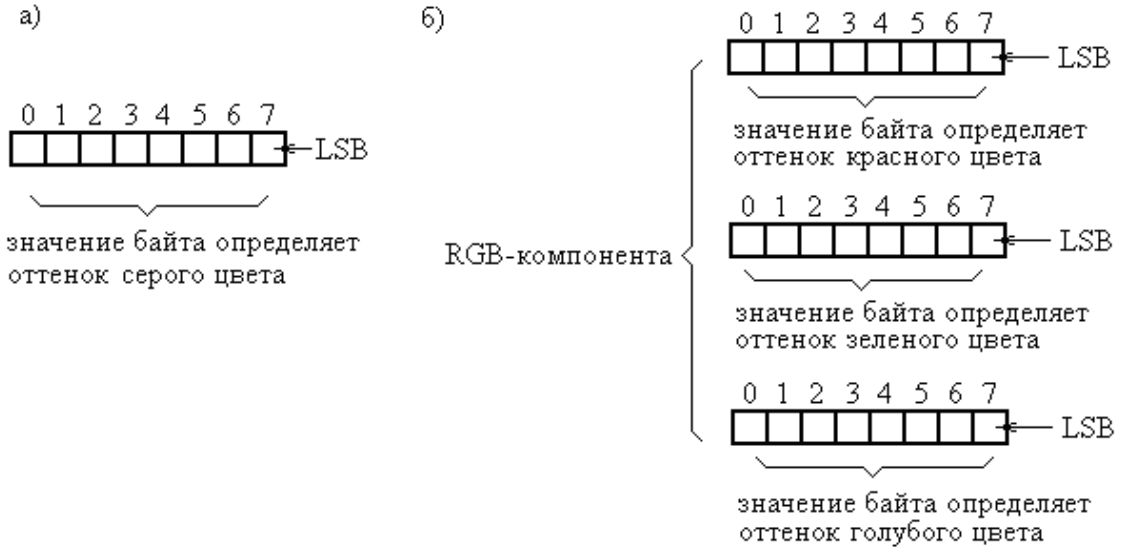


Рис. 1.22. Представление пикселя в *bmp*-файле при: а) полутоновом изображении; б) цветном изображении.

Встраивание информации − это преобразование пустого контейнера в стегоконтейнер за счет изменения значений некоторых LSB в соответствии с тем или иным алгоритмом. Выделяют три типа пустых контейнеров: *выбранный* (т.е. контейнер подбирается в соответствии со структурой передаваемого сообщения), *случайный* (контейнер выбирается случайным образом, что наиболее типично на практике) и *навязанный* (например, лицо, представляющее контейнер, подозревая о возможности скрытой переписки, принимает усилия для ее предотвращения).

В стегоанализе выделяют *пассивные атаки*, предназначенные только для обнаружения самого факта скрытой передачи информации и *активные атаки*, предназначенные для уничтожения сообщения при его обнаружении. Наиболее простая пассивная атака состоит в следующем. Вычисляется и хранится в качестве эталона распределение значений байтов пустого контейнера. При анализе контейнера достаточно вычислить распределение значений байтов и сравнить его с эталоном. Поэтому любой алгоритм встраивания информации в bmp-файл с целью ее скрытой передачи не должен изменять распределение значений байтов в стегоконтейнере по сравнению с распределением этих значений в эталоне.

Пример 1.3. В [135] предложен следующий метод шифрования битовой последовательности $\mathbf{p}$. В пустом контейнере (bmp-файле) выделены две такие системы

$$\mathsf{X}_j = \{X_0^{(j)}, X_1^{(j)}, \ldots, X_{255}^{(j)}\} \quad (j = 1,2)$$

множеств байтов, что:

1) для всех $i = 0,1,\ldots,255$ каждый элемент множества $X_i^{(j)}$ $(j = 1,2)$ – это байт, в котором записано двоичное представление числа i;

2) $X_i^{(1)} \cap X_i^{(2)} = \varnothing$ для всех $i = 0,1,\ldots,255$;

3) $|X_i^{(1)}| \approx |X_{i+1}^{(2)}|$ для каждого четного $i \in \{0,1,\ldots,255\}$ и $|X_i^{(1)}| \approx |X_{i-1}^{(2)}|$ для каждого нечетного $i \in \{0,1,\ldots,255\}$.

Алгоритм встраивания информации состоит в следующем. Для очередного бита b последовательности $\mathbf{p}$ выбирается значение $i \in \{0,1,\ldots,255\}$ и очередной байт $B_1 \in X_i^{(1)}$. В LSB байта B_1 заносится бит b. Если произошло инвертирование LSB, то выбирается очередной байт $B_2 \in X$, где $X = X_{i+1}^{(2)}$, если i – четное число и $X = X_{i-1}^{(2)}$, если i – нечетное число. LSB байта B_2 инвертируется. Этот метод не изменяет распределение значений байтов в стегоконтейнере по сравнению с их распределением в эталоне.

В стеганографии (по аналогии с криптографией) для повышения уровня сокрытия информации, используется понятие *сеансовый ключ*. Выделяют стегосистемы с *секретным ключом* и стегосистемы с *открытым ключом*. Обобщенная модель стегосистемы изображена на рис. 1.23, а ее детализация, представляющая типичную структурную схему стегосистемы ЦВЗ, изображена на рис. 1.24.

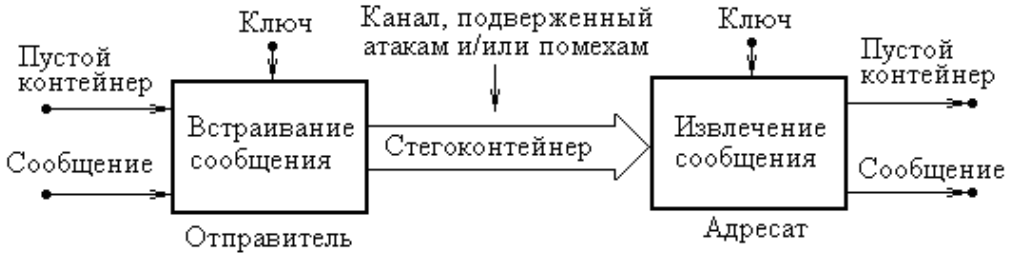


Рис. 1.23. Обобщенная модель стегосистемы.

Проектирование стегосистем основано на следующих принципах:

1) знание стегоаналитиком факта наличия сообщения в каком-либо контейнере не должно помочь ему при обнаружении сообщений в других контейнерах;

2) стегоконтейнер визуально неотличим от пустого контейнера;

3) стегосистема имеет низкую вероятность ложного обнаружения скрытого сообщения в контейнере, его не содержащем;

4) обеспечивается требуемая пропускная способность стегосистемы;

5) стегосистема имеет приемлемую вычислительную сложность реализации.

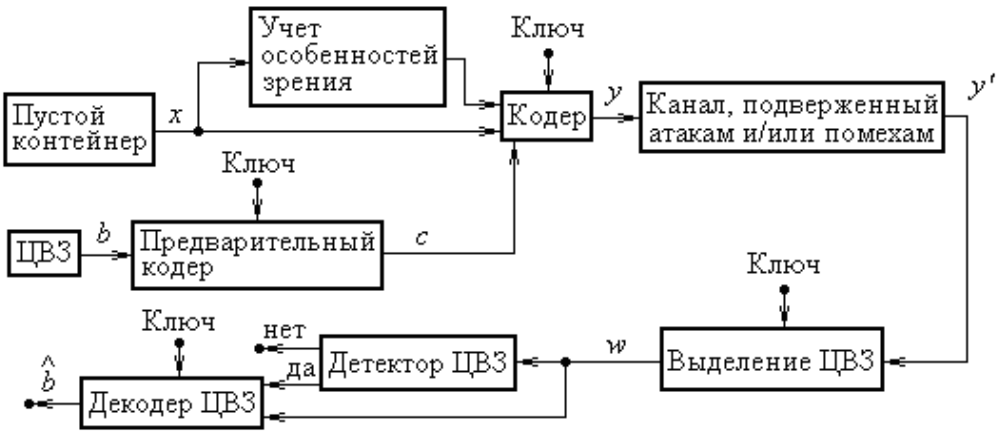


Рис. 1.24. Структурная схема типичной стегосистемы ЦВЗ.

Отметим, что ЦВЗ, в зависимости о приложения, должен быть либо устойчив, либо неустойчив к преднамеренным или случайным воздействиям, а также должна быть предусмотрена возможность внесения в стегоконтейнер дополнительных ЦВЗ.

Рассмотрим теперь кратко современные шифры.

Вначале рассмотрим блочные шифры.

Каждый блочный шифр основан на разбиении двоичной последовательности на блоки длины l и независимой обработке каждого блока посредством одного и того же алгоритма. Для оптимизации скорости обработки информации (в зависимости от разрядности процессоров) число l выбирается кратным 32 или 64. Всюду в дальнейшем l – *четное число*. Общий вид блочного симметричного шифра представлен на рис. 1.25.

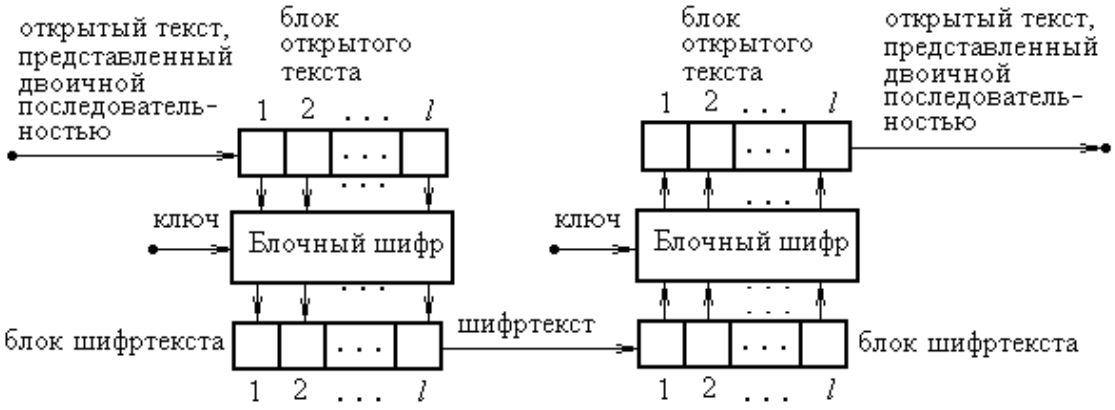


Рис. 1.25. Общий вид симметричного блочного шифра.

В основе ряда блочных шифров лежит *сеть Фейстеля*.

В 1973 г. *Х. Фейстель* предложил следующий алгоритм преобразования блока информации $M \in \mathbf{E}^l$. Пусть $\mathsf{K} = \mathbf{E}^h$ – множество ключей. Зафиксируем отображение $f : \mathbf{E}^{0.5 \cdot l} \times \mathbf{E}^h \to \mathbf{E}^{0.5 \cdot l}$. Представим M в виде $M = A \uparrow\uparrow B$, где $A, B \in \mathbf{E}^{0.5 \cdot l}$, а $\uparrow\uparrow$ – операция сцепления двоичных последовательностей.

F -функцией называется отображение $F_f : \mathbf{E}^{0.5 \cdot l} \times \mathbf{E}^{0.5 \cdot l} \to \mathbf{E}$, определяемое равенством

$$F_f(M) = B \uparrow\uparrow (A \oplus f(B,K))$$

для каждого значения ключа $K \in K$ (рис. 1.26).

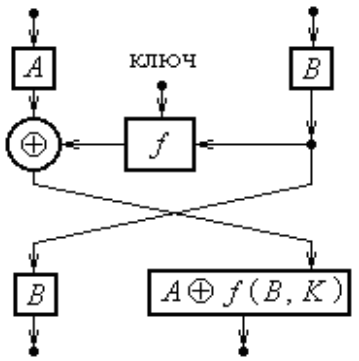


Рис. 1.26. Схема, реализующая *F*- функцию.

Так как

$$A \oplus f(B,K) \oplus f(B,K) = A,$$

то F_f *– биекция*.

Для реализации F_f^{-1} достаточно поменять местами входы и выходы на рис. 1.26.

Сетью Фейстеля называется любая схема, реализующая конечный итерационный процесс, каждый шаг (*раунд*) которого основан на вычислении F -функции, т.е. сеть Фейстеля − это последовательное соединение схем, изображенных на рис. 1.26, возможно снабженных дополнительной логикой.

1. *Алгоритм DES***.** В 1976г. *Национальное бюро стандартов* (*NBS*) США, ныне *Национальный институт стандартов и технологии* (*NIST*), приняло *DES* (*Data Encryption Standard*) в качестве федерального стандарта криптографического алгоритма и разрешило его использование во всех несекретных правительственных каналах связи. Необходимость этих действий была вызвана тем, что фирмы выпускали на рынок криптографические продукты, созданные на основе своих собственных, часто несовместимых друг с другом, секретных разработок. В 1981г. Американский национальный институт стандартизации *ANSI* одобрил *DES* под именем *DEA* (*Data Encryption Algorithm*) в качестве стандарта для частного сектора. Было решено, что применимость этого стандарта будет пересматриваться каждые 5 лет. С тех пор появились многочисленные программные и аппаратные реализации различных вариантов и модификаций *DES*.

За основу разработки *DES* были приняты следующие критерии:

1) высокий уровень защиты;
2) детальное и понятное описание алгоритма;
3) надежность алгоритма опирается только на ключ;
4) доступность алгоритма всем пользователям;
5) адаптация алгоритма к различным применениям;
6) возможность экономически выгодной аппаратной реализации алгоритма;
7) эффективность алгоритма в использовании;
8) алгоритм должен предоставлять возможности проверки;
9) алгоритм должен быть разрешен для экспорта.

Базовый вариант *DES* применяется к 64-битовому блоку данных, и использует 56-битовый ключ − 64-битовое число, каждый 8-й бит которого предназначен для контроля на четность и игнорируется в процессе применения ключа. Алгоритм *DES* (рис. 1.27) реализует *рассеивание* и *перемешивание* информации 16-и раундовой сетью Фейстеля.

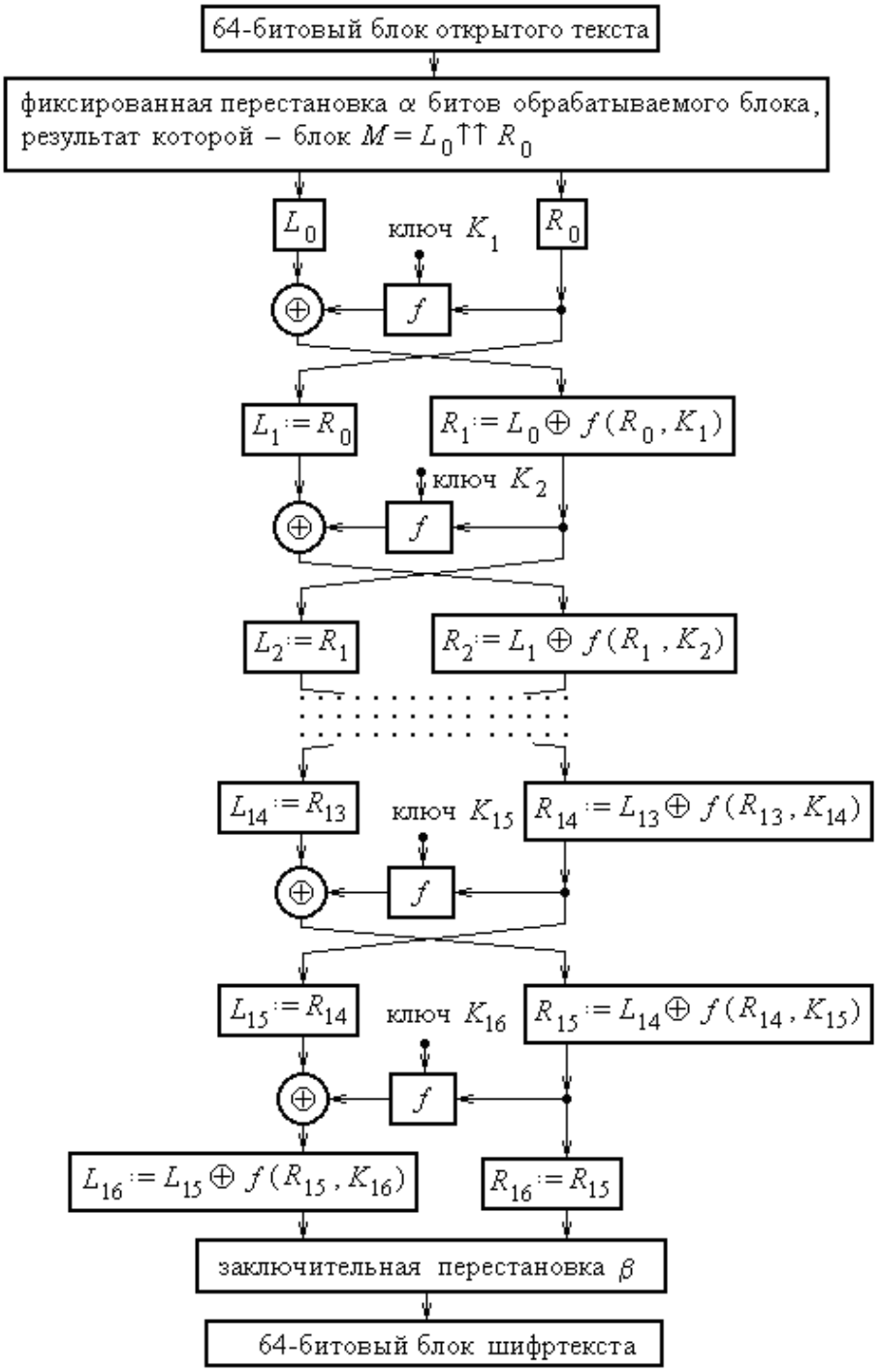


Рис. 1.27. Схема алгоритма *DES*.

Перестановки α и β предназначены для облегчения загрузки данных в микросхему при аппаратной реализации алгоритма *DES*. Они отсутствует во многих программных реализациях *DES*, и совершенно не влияют на стойкость алгоритма *DES*.

Детализация F-функции F_f, применяемой в алгоритме *DES*, изображена на рис. 1.28.

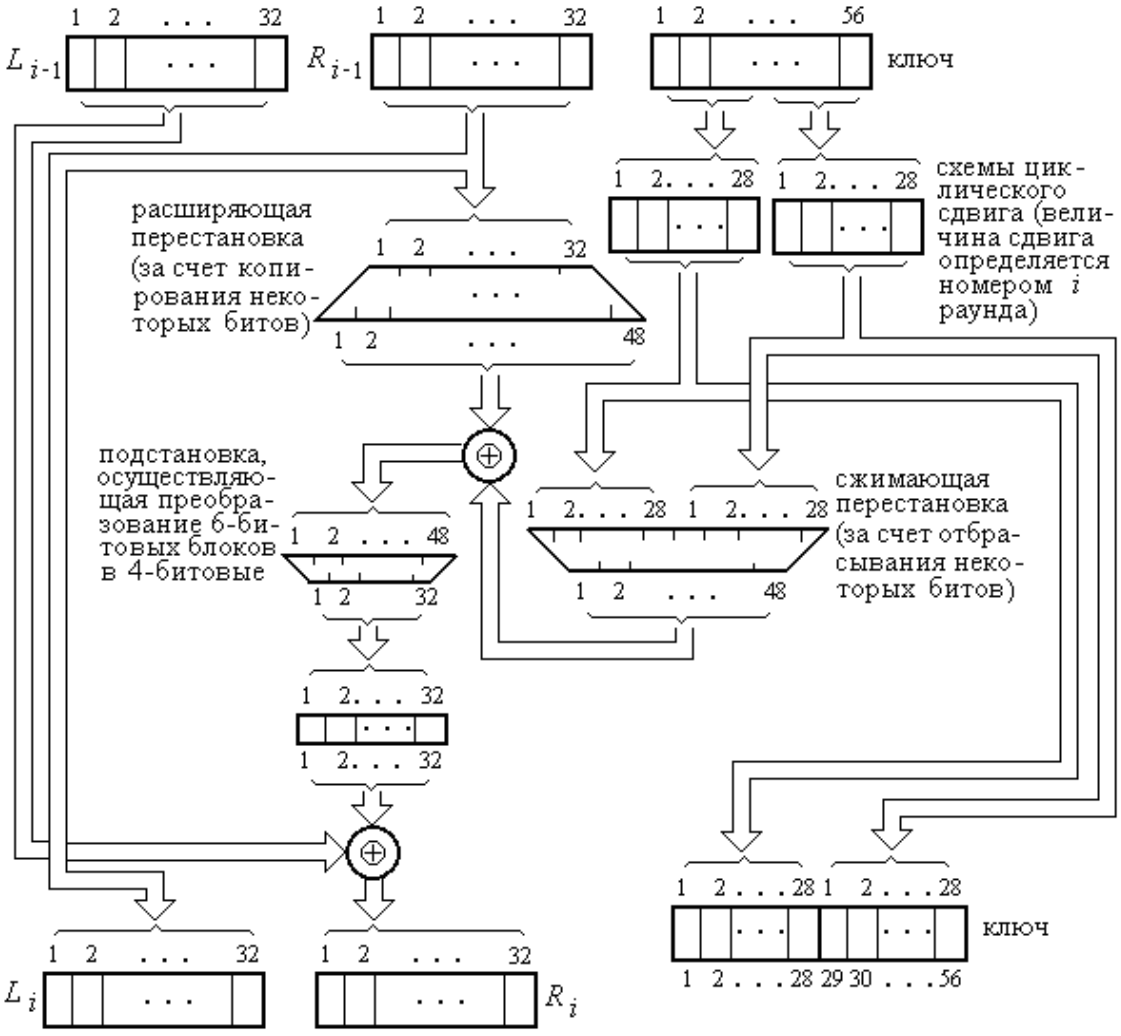


Рис. 1.28. Детализация отображения f для F-функции, применяемой на i-м раунде (i =1,..., 16) алгоритма DES.

Вначале 64-битовый ключ за счет отбрасывания каждого 8-го бита сжимается до 56-битового ключа $\gamma_1^{(1)} \ldots \gamma_{56}^{(1)}$.

Ключ K_i $(i = 1,\ldots,16)$ формируется из этой последовательности следующим образом. Последовательность $\gamma_1^{(i)} \ldots \gamma_{56}^{(i)}$ разбивается на две 28-битовые последовательности, к каждой из которых применяется циклический сдвиг влево. Величина этого сдвига для i-го раунда $(i = 1,\ldots,16)$ определяется таблицей 1.1.

Таблица 1.1.

раунд	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
величина сдвига	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

В результате последовательность $\gamma_1^{(i)} \dots \gamma_{56}^{(i)}$ преобразуется в последовательность $\gamma_1^{(i+1)} \dots \gamma_{56}^{(i+1)}$. К этой последовательности применяется сжимающая перестановка, формирующая 48-битовую последовательность $\mu_1^{(i)} \dots \mu_{48}^{(i)}$, которая и является ключом K_i.

Величины циклических сдвигов и сжимающая перестановка экспериментально подобраны так, что множества битов последовательности $\gamma_1^{(1)} \dots \gamma_{56}^{(1)}$, используемые в различных раундах – различные и каждый бит используется в 14-и раундах из 16-и.

Расширяющая перестановка преобразует блок $R_{i-1} = \delta_1^{(i-1)} \dots \delta_{32}^{(i-1)}$ $(i = 1,\dots,16)$ в блок $\nu_1^{(i-1)} \dots \nu_{48}^{(i-1)}$ и выбрана так, что $\nu_1^{(i-1)} = \delta_{32}^{(i-1)}$, $\nu_{1+12\cdot h}^{(i-1)} = \delta_{8\cdot h}^{(i-1)}$ и $\nu_{12\cdot h}^{(i-1)} = \delta_{1+8\cdot h}^{(i-1)}$ при $h = 1,2,3$, $\nu_{48}^{(i-1)} = \delta_1^{(i-1)}$ и для $h = 0,1,2,3$, если $j = 2,\dots,6$, то $\nu_{j+12\cdot h}^{(i-1)} = \delta_{j-1+8\cdot h}^{(i-1)}$, а если $j = 7,\dots,11$, то $\nu_{j+12\cdot h}^{(i-1)} = \delta_{j-3+8\cdot h}^{(i-1)}$.

После поразрядного сложения по модулю 2 сжатого ключа $\mu_1^{(i)} \dots \mu_{48}^{(i)}$ с расширенным блоком $\nu_1^{(i-1)} \dots \nu_{48}^{(i-1)}$ получен блок $\kappa_1 \dots \kappa_{48}$, над которым выполняется операция *подстановки*, реализованная следующим образом. Последовательность $\kappa_1 \dots \kappa_{48}$ разбивается на восемь 6-битовых *S-блоков* $\kappa_{1+6\cdot j} \dots \kappa_{6+6\cdot j}$ $(j = 0,1,\dots,7)$. Для преобразования j-го S-блока $(j = 0,1,\dots,7)$ применяется подстановка f_j. Эта подстановка представлена таблицей T_j, состоящей из 16-и столбцов и 4-х строк, где каждая строка таблицы T_j – это перестановка множества чисел $\{0,1,\dots,15\}$. S-блок $\kappa_{1+6\cdot j} \dots \kappa_{6+6\cdot j}$ $(j = 0,1,\dots,7)$ преобразуется в 4-битовую последовательность, являющуюся двоичным представлением числа, расположенного в таблице T_j на пересечении строки с номером $\kappa_{1+6\cdot j}\kappa_{6+6\cdot j}$ и столбца с номером $\kappa_{2+6\cdot j}\kappa_{3+6\cdot j}\kappa_{4+6\cdot j}\kappa_{5+6\cdot j}$. Таблицы T_j $(j = 0,1,\dots,7)$ имеют вид:

Таблица 1.2 (Таблица T_0)**.**

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Таблица 1.3 (Таблица T_1).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Таблица 1.4 (Таблица T_2).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Таблица 1.5 (Таблица T_3).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Таблица 1.6 (Таблица T_4).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Таблица 1.7 (Таблица T_5).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Таблица 1.8 (Таблица T_6).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Таблица 1.9 (Таблица T_7).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Рассмотрим кратко некоторые модификации алгоритма *DES*.

Алгоритм *EDE*3 (1985г.) имеет вид

$$EDE3_{K_1,K_2,K_3}(M) = DES_{K_3}(DES^{-1}_{K_2}(DES_{K_1}(M))).$$

Так как

$$EDE3_{K,K,K}(M) = DES_K(M)$$

для любого 56-битового ключа K и любого 64-битового блока M открытого текста, т.е. *EDE*3 совместим с *DES*.

Производительность алгоритма *EDE*3 в три раза меньше, чем производительность алгоритма *DES*, что сужает область применения *EDE*3.

Алгоритм *DESX* (1984г.) имеет вид

$$DESX_{K,K_1,K_2}(M) = K_2 \oplus DES_K(K_1 \oplus M),$$

где 64-битовые ключи K_1 и K_2 предназначены для *зашумления* информации. Этот алгоритм более устойчив к ряду атак, чем *EDE*3.

Производительность алгоритма *DESX* такая же, как и производительность алгоритма *DES*.

Алгоритм *DES-PEP* имеет вид

$$DES-PEP_{K,K_1,K_2}(M) = K_2 \circ DES_K(K_1 \circ M),$$

где операция $\circ$ определена равенством

$$(L \uparrow\uparrow R) \circ (L' \uparrow\uparrow R') = ((L+L') \pmod{2^{32}}) \uparrow\uparrow ((R+R') \pmod{2^{32}}).$$

Этот алгоритм более устойчив к ряду атак, чем алгоритм *DESX*.

Производительность алгоритма *DES-PEP* такая же, как и производительность алгоритма *DES*.

2. *Алгоритм ГОСТ 28147-89* [46]. Этот шифр принят в СССР в 1989г. Является стандартом шифрования в России. Носит обязательный характер для государственных органов и организаций, чья деятельность связана с обеспечением информационной безопасности государства. Алгоритм разрабатывался с учетом недостатков, выявленных в процессе эксплуатации алгоритма *DES* и его модификаций. Алгоритм построен на основе 32-раундовой сети Фейстеля, осуществляет шифрование 64-битового блока открытого текста, разбитого на два 32-битовых блока, записанных в инверсном порядке и использует 256-битовый ключ K, представленный в виде восьми 32-разрядных двоичных чисел, т.е.

$$K = K_7 \uparrow\uparrow K_6 \uparrow\uparrow \ldots \uparrow\uparrow K_1 \uparrow\uparrow K_0.$$

Предусмотрены три режима шифрования.

Базовый режим шифрования (рис.1.29) осуществляется в соответствии с формулами ([+] – операция сложения по $\bmod 2^{32}$):

$$L_i := R_{i-1} \quad (i = 1,\ldots,31),$$

$$\begin{cases} R_i := \mathbf{R}(\mathbf{S}(R_{i-1}\,[+]\,K_{(i-1)\,(\bmod 8)})) \oplus L_{i-1}, \ \textit{если} \ \ i = 1,\ldots,24 \\ R_i := \mathbf{R}(\mathbf{S}(R_{i-1}\,[+]\,K_{(32-i)\,(\bmod 8)})) \oplus L_{i-1}, \ \textit{если} \ \ i = 25,\ldots,31 \end{cases},$$

$$\begin{cases} L_{32} := \mathbf{R}(\mathbf{S}(R_{31}\,[+]\,K_0)) \oplus L_{31} \\ R_{32} := R_{31} \end{cases}.$$

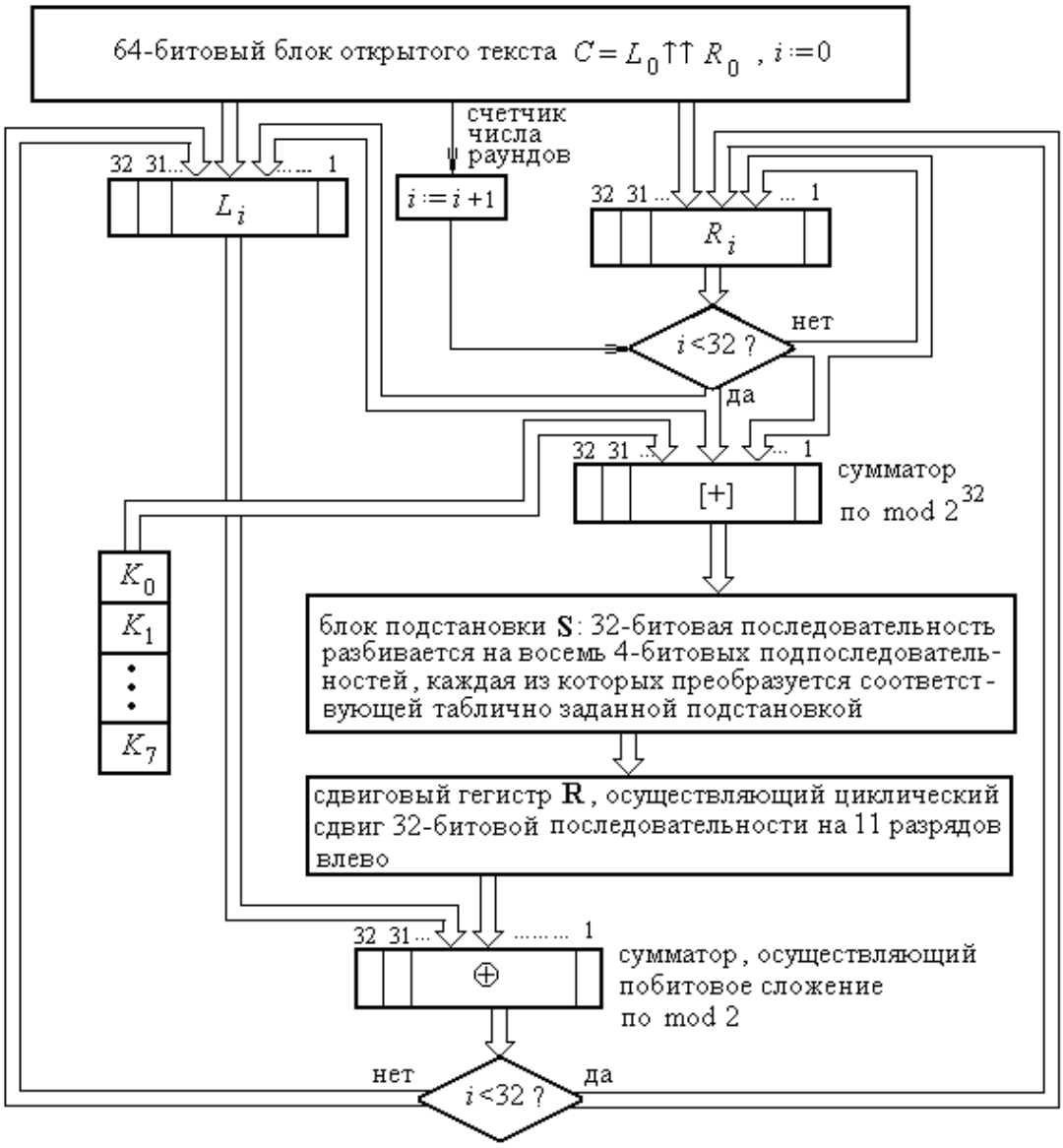


Рис. 1.29. Базовый режим работы алгоритма *ГОСТ 28147-89*.

Второй режим шифрования – это режим гаммирования. Открытый текст разбивается на 64-битовые блоки $M^{(1)} \uparrow\uparrow \ldots \uparrow\uparrow M^{(m)}$. При необходимости последний блок дополняется финальным маркером.

Шифрование осуществляется поразрядным сложением по $\mathrm{mod}\,2$ этих блоков с соответствующими 64-битовыми блоками гаммы

$$\Gamma^{(1)} \uparrow\uparrow \ldots \uparrow\uparrow \Gamma^{(m)},$$

т.е.

$$C^{(i)} = M^{(i)} \oplus \Gamma^{(i)} \quad (i = 1,\ldots,m).$$

Гамма $\Gamma^{(1)} \uparrow\uparrow \ldots \uparrow\uparrow \Gamma^{(m)}$ вырабатывается в соответствии с формулой

$$\Gamma^{(i)} = E_K((Y^{(i-1)}\,[+]\,c_2) \uparrow\uparrow (Z^{(i-1)}\,\{+\}\,c_1)) \quad (i = 1,\ldots,m),$$

где E_K – базовый режим шифрования алгоритма *ГОСТ 28147-89*, $\{+\}$ – операция сложения по $\mathrm{mod}\,(2^{32}-1)$, а c_1 и c_2 – константы, представление которых в 16-ричной системе счисления имеет вид $c_1 = 01010104$ и $c_2 = 01010101$.

Последовательности $Y^{(j)} \uparrow\uparrow Z^{(j)}$ $(j = 0,1,\ldots,m-1)$ вычисляются следующим образом

$$Y^{(0)} \uparrow\uparrow Z^{(0)} = E_K(S),$$

где 64-битовая последовательность S (*синхропосылка*) не является секретным ключом (ее наличие необходимо как у отправителя, так и у адресата) и

$$Y^{(i)} \uparrow\uparrow Z^{(i)} = (Y^{(i-1)}\,[+]\,c_2) \uparrow\uparrow (Z^{(i-1)}\,\{+\}\,c_1) \quad (i = 1,\ldots,m-1).$$

Третий режим шифрования – это режим гаммирования с обратной связью. Отличается от 2-го режима только тем, что гамма вырабатывается в соответствии с формулами

$$\Gamma^{(1)} = E_K(S)$$

и

$$\Gamma^{(i)} = E_K(C^{(i-1)}) \quad (i = 2,3,\ldots).$$

3. *Алгоритм AES***.** В 1996 г. *NIST* объявил конкурс на разработку нового национального стандарта шифрования – *AES* (*Advanced Encryption Standard*), который должен в XXI веке заменить стандарт *DES*. Подведение итогов конкурса состоялось 2-го октября 2000г. Победитель конкурса − алгоритм *Rijndael*. Этот алгоритм основан на преобразованиях в конечных алгебраических системах (а не на сетях Фейстеля) и допускает независимый выбор длины блока данных и ключа, равной 128, 192 или 256 бит.

Пусть n_B и n_K − длины блока, соответственно, данных и ключа, деленные на 32. Шифруемый блок данных C последовательно, байт за байтом, записывается (по строкам) в двумерный массив состояния блока данных

$$M_C = \begin{pmatrix} c_{11} & \cdots & c_{1n_B} \\ \vdots & \ddots & \vdots \\ c_{41} & \cdots & c_{4n_B} \end{pmatrix},$$

где $c_{ij} \in \mathbf{GF}^8(2)$ $(i=1,\ldots,4;\ j=1,\ldots,n_B)$, а ключ представляется одномерным массивом

$$K = k_1 \ldots k_{n_K},$$

где $k_j \in \mathbf{GF}^{32}(2)$ $(j=1,\ldots,n_K)$.

Шифрование представляет собой итерационный процесс преобразования состояний блока данных и ключа. Число n итераций (раундов) определяется таблицей 1.10.

Таблица 1.10.

n_K / n_B	4	6	8
4	10	12	14
6	12	12	14
8	14	14	14

Каждый раунд, кроме последнего раунда, состоит из четырех процедур: *подстановка*, *сдвиг*, *перемешивание* и *гаммирование*. На последней итерации *перемешивание* не выполняется. Рассмотрим эти процедуры.

Процедура подстановка (*SubByte*). Каждый элемент массива M_C интерпретируется как элемент поля Галуа

$$\mathbf{GF}(2^8) = \mathbf{GF}(2)[x]/(x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1),$$

т.е. $c_{ij} = \alpha_7\alpha_6 \ldots \alpha_1\alpha_0$ $(i=1,\ldots,4;\ j=1,\ldots,n_B)$ – это набор коэффициентов многочлена

$$c_{ij}(x) = \alpha_7 \circ x^7 \oplus \alpha_6 \circ x^6 \oplus \ldots \oplus \alpha_1 \circ x \oplus \alpha_0 \quad (i=1,\ldots,4;\ j=1,\ldots,n_B).$$

Процедура *подстановка* состоит из следующих двух шагов:

Шаг 1. Конструируется массив состояния блока данных

$$M_C^{(1)} = \begin{pmatrix} c_{11}^{(1)} & \cdots & c_{1n_B}^{(1)} \\ \vdots & \ddots & \vdots \\ c_{41}^{(1)} & \cdots & c_{4n_B}^{(1)} \end{pmatrix},$$

где $c_{ij}^{(1)}$ $(i=1,\ldots,4;\ j=1,\ldots,n_B)$ – это набор коэффициентов такого многочлена $c_{ij}^{(1)}(x)$, что

$$c_{ij}^{(1)}(x) = \begin{cases} (c_{ij}(x))^{-1}, \ \textit{если} \ c_{ij}(x) \not\equiv 0 \\ c_{ij}(x), \ \textit{если} \ c_{ij}(x) \equiv 0 \end{cases} \quad (i=1,\ldots,4;\ j=1,\ldots,n_B).$$

Шаг 2. Конструируется такой массив состояния блока данных

$$M_C^{(2)} = \begin{pmatrix} c_{11}^{(2)} & \cdots & c_{1n_B}^{(2)} \\ \vdots & \ddots & \vdots \\ c_{41}^{(2)} & \cdots & c_{4n_B}^{(2)} \end{pmatrix},$$

что $c_{ij}^{(2)}$ $(i=1,\ldots,4;\ j=1,\ldots,n_B)$ – это набор коэффициентов многочлена

$$c_{ij}^{(2)}(x)=(x^7\oplus x^6\oplus x^2\oplus x)\oplus u_{ij}(x),$$

где

$$u_{ij}(x)=c_{ij}^{(1)}(x)\circ(x^7\oplus x^6\oplus x^5\oplus x^4\oplus 1)\,(\mathrm{mod}\,(x^8\oplus 1)),$$

а $\oplus$ и $\circ$ – операции в кольце многочленов $\mathbf{GF}(2)[x]$.

Процедура сдвиг (*ShiftRow*). Применяется к строкам массива $M_C^{(2)}$. Имеет вид: 1-я строка не изменяется, а 2-я, 3-я и 4-я строки циклически сдвигаются влево на число позиций i_2, i_3 и i_4, определяемые в соответствии с таблицей 1.11.

Таблица 1.11.

n_B	i_2	i_3	i_4
4	1	2	3
6	1	2	3
8	1	3	4

В результате получаем массив состояния блока данных

$$M_C^{(3)}=\begin{pmatrix} c_{11}^{(3)} & \cdots & c_{1n_B}^{(3)} \\ \vdots & \ddots & \vdots \\ c_{41}^{(3)} & \cdots & c_{4n_B}^{(3)} \end{pmatrix}.$$

Процедура перемешивание (*MixColumn*). Массив $M_C^{(3)}$ преобразуется в массив состояния блока данных

$$M_C^{(4)}=\begin{pmatrix} c_{11}^{(4)} & \cdots & c_{1n_B}^{(4)} \\ \vdots & \ddots & \vdots \\ c_{41}^{(4)} & \cdots & c_{4n_B}^{(4)} \end{pmatrix}$$

по формуле

$$\begin{pmatrix} c_{1j}^{(4)} \\ c_{2j}^{(4)} \\ c_{3j}^{(4)} \\ c_{4j}^{(4)} \end{pmatrix}=\begin{pmatrix} '02' & '03' & '01' & '01' \\ '01' & '02' & '03' & '01' \\ '01' & '01' & '02' & '03' \\ '03' & '01' & '01' & '02' \end{pmatrix}\circ\begin{pmatrix} c_{1j}^{(3)} \\ c_{2j}^{(3)} \\ c_{3j}^{(3)} \\ c_{4j}^{(3)} \end{pmatrix}.$$

Процедура гаммирования (*AddRoundKey*). Для раунда с номером $h\in\{1,\ldots,n\}$ осуществляется по формуле

$$M_C:=M_c^{(4)}\oplus M_K^{(h)}\ \ (h=1,\ldots,n),$$

где $\oplus$ − операция поразрядного сложения по $\mathrm{mod}\,2$, а массив $M_K^{(h)}$ $(h=1,\ldots,n)$ − раундовый ключ.

Раундовые ключи получаются из ключа шифрования K. Вначале ключ K расширяется в массив

$$K_{ext} = k_1^{(1)} \ldots k_{n_B \cdot (n+1)}^{(1)},$$

где $k_j^{(1)}$ $(j = 1, \ldots, n_B \cdot (n+1))$ − 4-х байтовое слово.

Процедура расширения ключа выполняется следующим образом. Первые n_K элементов массива K_{ext} заполняются ключом шифрования K. Если $n_K \in \{4,6\}$, то каждый последующий элемент $k_j^{(1)}$ − результат поразрядного сложения элементов $k_{j-1}^{(1)}$ и $k_{j-n_K}^{(1)}$ по $\bmod 2$. Для элементов, номер которых кратен n_K, перед выполнением этой операции к элементу $k_{j-1}^{(1)}$ применяется циклический сдвиг байтов, прибавляется раундовая константа, а затем применяется процедура *SubByte*. Если $n_K = 8$, то процедура расширения ключа отличается только тем, что циклический сдвиг байтов, прибавление раундовой константы и процедура *SubByte* применяются при вычислении элементов, номер которых кратен четырем.

Раундовые ключи берутся из расширенного ключа следующим образом: 1-й раундовый ключ содержит первые n_B элементов, 2-й раундовый ключ − следующие n_B элементов и т.д.

По-видимому, три рассмотренных выше блочных шифра и работа [59] оказали основное влияние на формирование математических методов анализа и синтеза современных блочных шифров. Это влияние проявляется при разработке общих принципов проектирования блочных шифров [123,214,269], при разработке методов анализа вычислительной стойкости блочных шифров [7,33,209,213,240,270], при разработке методов анализа и отбора случайных подстановок [38,64,65,249,290], при разработке методов построения и анализа S-блоков [34,235,236], а также при конструировании кандидатов, представленных на разрабатываемые в настоящее время стандарты блочных шифров [35,39,41-43,134].

Для современных блочных шифров вычислительная стойкость характеризуется по отношению их устойчивости, по крайней мере, к следующим типам атак:

1) *атака грубой силы*, состоящая в том, что криптоаналитик осуществляет полный перебор ключей;

2) *линейный криптоанализ*, состоящий в том, что осуществляются попытки замены преобразований, описывающих алгоритм шифрования, их приближениями в классе линейных функций (методы линейного криптанализа *DES*-подобных алгоритмов исследованы в [284]);

3) *дифференциальный криптоанализ*, состоящий в том, что криптоаналитик имеет для анализа либо несколько шифртекстов, о которых известно, что они получены на одном и том же ключе, а также ему известна информация о том, как различаются между собой (неизвестные) открытые

тексты, либо криптоаналитику известны результаты шифрования одного и того же открытого текста на различных неизвестных ключах, а также ему известна информация о том, как различаются между собой эти ключи (методы дифференциального криптанализа *DES*-подобных алгоритмов исследованы в [250]);

4) *интегральный криптоанализ*, состоящий в том, что криптоаналитик располагает достаточным множеством шифртекстов, полученных при шифровании подобранных открытых текстов на одном и том же секретном ключе;

5) *интерполяционная атака*, состоящая в том, что шифртекст представляется в виде полинома от открытого текста;

6) *слайд-атака*, состоящая в том, что алгоритм шифрования E представляется в виде итерации некоторого преобразования F;

7) *атака на связанных ключах*, состоящая в том, что криптоаналитик располагает результатами шифрования известных или подобранных текстов не только при использовании неизвестного ключа K, но и при использовании ключа $K_1 = f(K)$, где f − функция, известная криптоаналитику.

Следует отметить, что в последнее время в криптографии наблюдается устойчивая тенденция перехода от чисто комбинаторных конструкций к конечным алгебраическим системам. В этой связи большое значение имеет разработка теоретико-числовых и алгебраических методов анализа и синтеза асимметричных шифрсистем [143,237,260,275,291,292,311].

Особо следует выделить применение эллиптических кривых [77,78,102] к разработке методов анализа и синтеза ЭЦП. В настоящее время этому направлению уделяется значительное внимание [20,23-25,63,271] и, по-видимому, оно является одним из наиболее перспективных направлений в криптографии с открытым ключом.

Охарактеризуем наиболее часто используемые режимы применения блочных шифров в современных системах защиты информации [17] (E_K и D_K − соответствующие друг другу алгоритм, соответственно, шифрования и расшифровки, M − шифруемый блок, а C − результат шифрования блока M).

1. Режим *электронной кодировочной книги* (*ECB − Electronic Code Book*). В этом режиме каждый блок исходного текста шифруется независимо от других блоков (рис. 1.30).

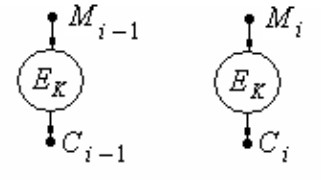


Рис. 1.30. Режим *ECB*.

Результаты шифрования и расшифровки связаны между собой соотношениями

$$C_i = E_K(M_i)$$

и

$$M_i = D_K(C_i).$$

Стойкость режима *ECB* равна стойкости блочно-

го шифра, лежащего в его основе. Скорость шифрования для *ECB* равна скорости исходного блочного шифра. Структура исходного текста сохраняется. Исходным текстом легко манипулировать путем удаления, повторения и перестановки блоков.

Режим *ECB* допускает простое распараллеливание вычислений.

При атаке на шифртекст, состоящей в изменении его криптоаналитиком, с ошибками будут расшифрованы только те блоки, которых коснулось изменение.

2. Режим *сцепления блоков шифртекста* (*CBC − Cipher Block Chaining*). Каждый блок исходного текста складывается поразрядно по $\mathrm{mod}\,2$ с предыдущим блоком шифртекста, а затем шифруется (рис. 1.31). Для 1-го блока исходного текста используется *синхропосылка* (или *начальный вектор*), передаваемая в канал связи в открытом виде.

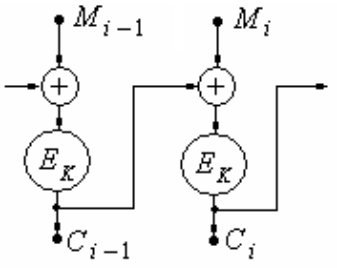


Рис. 1.31. Режим *CBC*.

Результаты шифрования и расшифровки связаны соотношениями

$$C_i = E_K(M_i \oplus C_{i-1})$$

и

$$M_i = D_K(C_i) \oplus C_{i-1}.$$

Стойкость режима *CBC* равна стойкости блочного шифра, лежащего в его основе. Скорость шифрования для *CBC* равна скорости исходного блочного шифра. Структура исходного текста скрывается за счет сложения предыдущего блока шифртекста с очередным блоком открытого текста. Невозможно манипулирование исходным текстом, кроме удаления блоков из начала или конца шифртекста. Простого способа распараллеливания вычислений для режима *CBC* нет.

При атаке на шифртекст, состоящей в изменении криптоаналитиком одного блока, с ошибками будут расшифрованы только два блока.

Известны следующие две модификации режима *CBC*.

Режим *сцепления блоков шифртекста с распространением* (*PCBC − Propagating CBC*). Отличается от *CBC* тем, что каждый блок исходного текста складывается поразрядно по $\mathrm{mod}\,2$ с предыдущими блоками, как исходного текста, так и шифртекста. Результаты шифрования и расшифровки связаны между собой соотношениями

$$C_i = E_K(M_i \oplus C_{i-1} \oplus M_{i-1})$$

и

$$M_i = D_K(C_i) \oplus C_{i-1} \oplus M_{i-1}.$$

Режим *сцепления блоков шифртекста с контрольной суммой* (*CBCC − CBC with Checksum*). Отличается от *CBC* тем, что последний блок исходного текста перед шифрованием складывается поразрядно по $\mathrm{mod}\,2$ со всеми предыдущими блоками исходного текста, что дает возможность контроли-

ровать целостность передаваемого текста с небольшими накладными расходами.

3. Режим *обратной связи по шифртексту* (*CFB − Cipher Feedback*). Каждый блок исходного текста складывается поразрядно по $\mathrm{mod}\,2$ с еще раз зашифрованным предыдущим блоком шифртекста, а затем шифруется (рис. 132). Для 1-го блока исходного текста используется *синхропосылка* , передаваемая в канал связи в открытом виде.

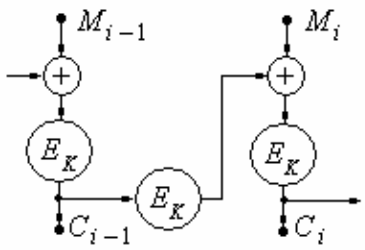


Рис. 1.32. Режим *CFB*.

Результаты шифрования и расшифровки связаны соотношениями

$$C_i = M_i \oplus E_K(C_{i-1})$$

и

$$M_i = E_K(C_{i-1}) \oplus C_i .$$

Стойкость режима *CFB* равна стойкости блочного шифра, лежащего в его основе. Скорость шифрования для *CFB* равна скорости исходного блочного шифра. Структура исходного текста скрывается за счет сложения зашифрованного предыдущего блока шифртекста с очередным блоком открытого текста. Невозможно манипулирование с исходным текстом посредством удаления блоков из начала или конца шифртекста. Простого способа распараллеливания вычислений для режима *CFB* нет.

В режиме *CFB* если два блока шифртекста идентичны, то идентичны и результаты их шифрования, что приводит к утечке информации об исходном тексте.

4. Режим *обратной связи по выходу* (*OFB − Outputipher Feedback*). Отличается от *CFB* тем, что величины, складываемые поразрядно по $\mathrm{mod}\,2$ с блоками исходного текста, генерируются независимо от исходного текста и шифртекста (рис. 1.33). Для начала процесса шифрования используется синхропосылка.

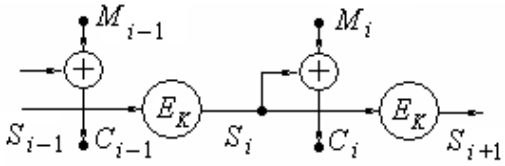


Рис. 1.33. Режим *OFB*.

Результаты шифрования и расшифровки связаны соотношениями

$$C_i = M_i \oplus S_i$$

и

$$M_i = C_i \oplus S_i ,$$

где $S_i = E_K(S_{i-1})$.

При атаке на шифртекст, состоящей в изменении его криптоаналитиком, с ошибками будут расшифрованы только те блоки, которых коснулось изменение. Возможна манипуляция исходным текстом посредством изменения шифртекста.

Существует несколько модификаций *OFB*. Отметим одну из них, известную как режим *обратной связи по выходу с нелинейной функцией* (*OFBNF − OFB with NonLinear Function*). Эта модификация отличается от *OFB* тем, что ключ, применяемый для шифрования очередного блока ис-

ходного текста − результат шифрования посредством исходного блочного шифра ключа, применяемого для шифрования предыдущего блока исходного текста, т.е. $K_i = E_K(K_{i-1})$.

Ясно, что ключевая последовательность может быть вычислена заранее, до начала процесса шифрования.

Рассмотрим теперь поточные шифры.

1. *Шифр RC4*. Этот поточный шифр с переменной длиной ключа был разработан в 1987г. Р. Ривестом для компании *RSA Data Security, Inc*. В 1994г. этот шифр был опубликован в Интернете. С тех пор стал доступным для исследования. Структура шифра *RC4* изображена на рис. 1.34.

Шифр *RC4* функционирует в режиме *OFB*, т.е. ключевая последовательность не зависит от исходного текста.

В шифре RC4 используется 8-и разрядный S-блок, таблица замен имеет размерность 8×256 и является перестановкой двоичных чисел от 0 до 256, зависящей от ключа. Применяются два счетчика Q_1 и Q_2 с нулевым начальным состоянием.

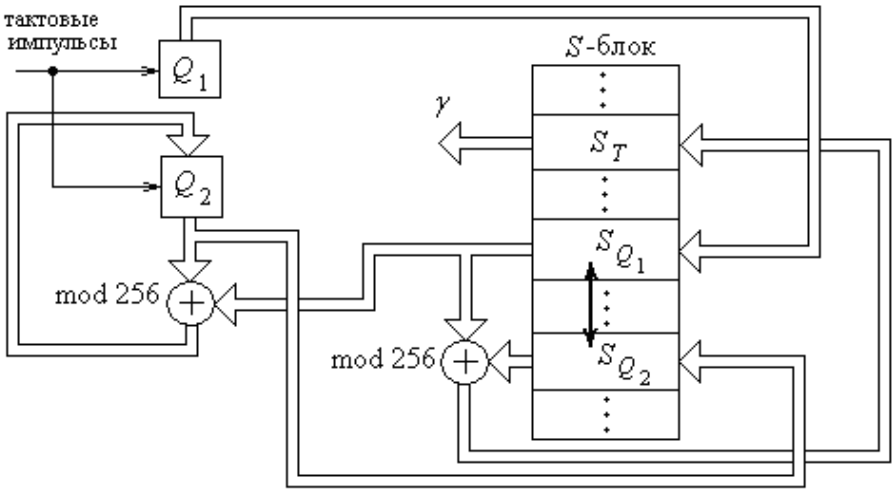


Рис. 1.34. Схема генератора псевдослучайных кодов *RC4*.

Генерация очередного байта γ гаммы осуществляется следующим образом:

Шаг 1. $Q_1 := (Q_1 + 1) \pmod{256}$.

Шаг 2. $Q_2 := (Q_2 + S_{Q_1}) \pmod{256}$.

Шаг 3. Ячейки таблицы замен S-блока с адресами Q_1 и Q_2 обмениваются своим содержимым: $S_{Q_1} \leftrightarrow S_{Q_2}$.

Шаг 4. $T := (S_{Q_1} + S_{Q_2}) \pmod{256}$.

Шаг 5. $\gamma := S_T$.

Инициализация таблицы замен S-блока осуществляется следующим образом:

Шаг 1. $S_i := i$ для всех $i = 0,1,\ldots,255$ (т.е. в каждую ячейку таблицы замен S-блока записывается ее собственный адрес).

Шаг 2. Заполняется байтами ключа другая 256-байтовая таблица $K = k_0 k_1 \ldots k_{255}$ (при необходимости ключ может повторяться несколько раз до заполнения всего массива).

Шаг 3. $i := 0,\ j := 0$.

Шаг 4. $j := (j + S_i + k_i) \pmod{256}$.

Шаг 5. Ячейки таблицы замен S-блока с адресами i и j обмениваются своим содержимым: $S_i \leftrightarrow S_j$, $i := i + 1$.

Шаг 6. Если $i \le 255$, то переход к шагу 4, иначе конец.

Число состояний *RC4* приблизительно равно $2^{1700} \cdot 256! \cdot (256)^2$. Таблица замен S-блока медленно изменяется при использовании генератора. Счетчик Q_1 обеспечивает изменение каждого элемента таблицы, а счетчик Q_2 гарантирует, что элементы таблицы изменяются случайным образом. Практика показала, что скорость шифрования посредством *RC4* примерно в 10 раз выше скорости программной реализации *DES*.

2. *Шифр A5*. Этот поточный шифр применяется в *GSM* (*Group Special Mobile*) для закрытия связи между абонентом и базовой станцией. Является европейским стандартом для цифровых сотовых телефонов.

Структура шифра *A5* изображена на рис. 1.35.

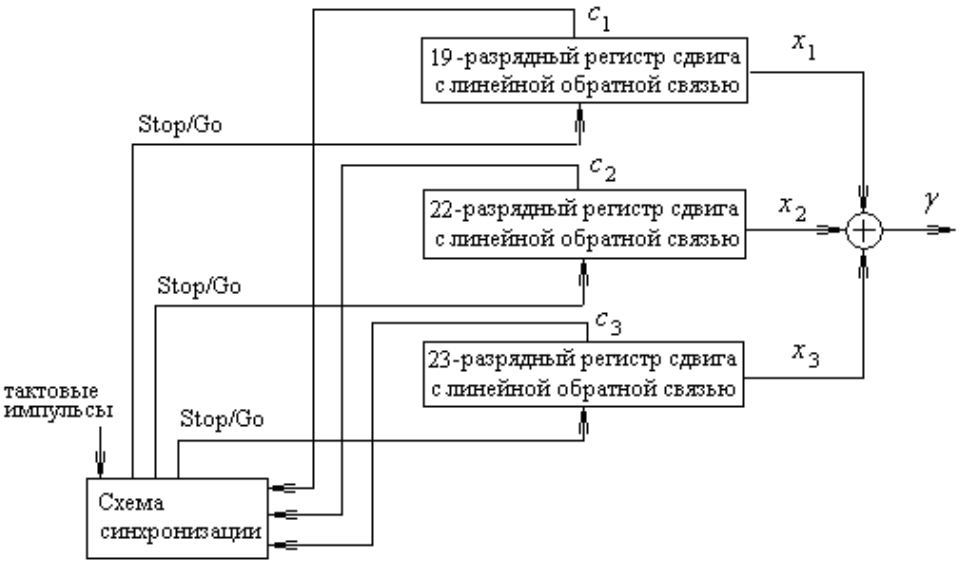


Рис. 1.35. Шифрсистема *A5*.

Образующие многочлены для регистров сдвига с линейной обратной связью имеют небольшое число ненулевых коэффициентов (такие многочлены называются *прореженными*). Начальное заполнение регистров является секретным сеансовым ключом.

Биты c_1, c_2 и c_3 используются для управления синхронизацией регистров сдвига. Если $c_1 = c_2 = c_3$, то сдвигаются все три регистра. В противном случае сдвигаются те два регистра i и j, для которых $c_i = c_j$. Таким образом, в каждом такте сдвигаются, по крайней мере, два регистра.

Установлено, что примерно 40% ключей приводят к циклу, длина которого наименьшая из всех возможных длин и равна $\frac{4}{3} \cdot (2^{23} - 1)$ бит.

Криптанализ шифра *A5* показал, что для определения начального заполнения регистров при известных 64 битах гаммы требуется перебор примерно 2^{40} вариантов.

3. *Шифр CHAMELEON*. Этот поточный шифр разработан Р. Андерсоном (1997г.). Представляет собой 2-х уровневую схему (рис. 1.36): 1-й уровень − это генератор псевдослучайных 64-разрядных кодов, а 2-й уровень − это *S*-блок, таблица замен которого имеет объем 512Кб и состоит из 2^{16} 64-разрядных слов.

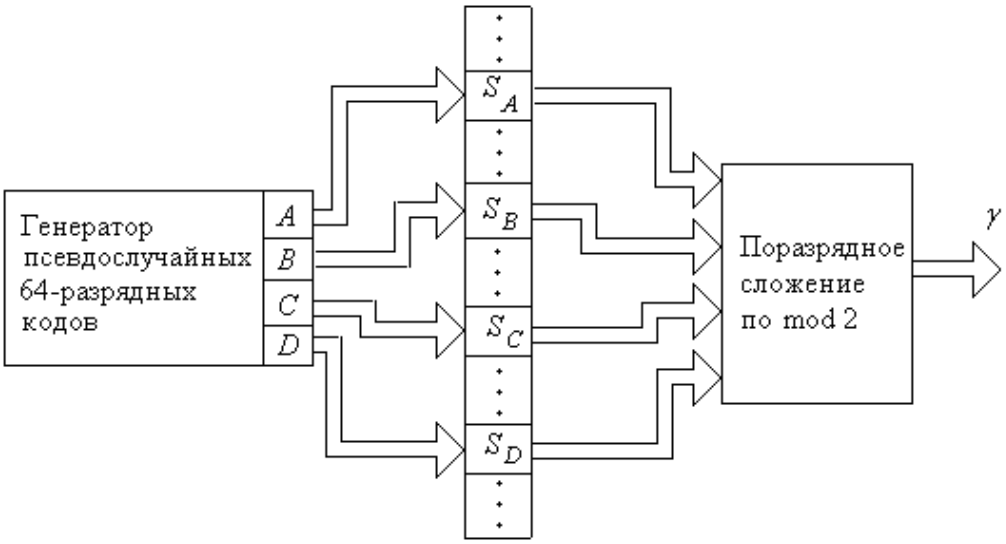


Рис. 1.36. Схема генератора *CHAMELEON*.

Ключевая информация − это начальное заполнение генератора псевдослучайных кодов и содержимое таблицы замен. Выход Q генератора псевдослучайных кодов рассматривается как совокупность четырех 16-и разрядных слов A, B, C и D, т.е.

$$Q = A \cdot 2^{48} + B \cdot 2^{32} + C \cdot 2^{16} + D.$$

Пусть S_i − содержимое блока замены с адресом i. Очередной элемент 64-разрядной гаммы вычисляется в соответствии с формулой

$$\gamma = S_A \oplus S_B \oplus S_C \oplus S_D.$$

Для шифра *CHAMELEON* изменение одного бита в ячейке таблицы замен приводит к изменению четырех бит на 512Кб сформированной гаммы.

Изменения гаммы находятся на тех же местах слова, что и измененные биты слова S_i.

То обстоятельство, что незначительные изменения в ключе вызывают незначительные изменения в гамме, а также высокая криптостойкость шифра *CHAMELEON* делают его весьма привлекательным для коммерческих приложений.

Во-первых, в цифровой продукции можно помещать знаки авторских прав в самых младших битах.

Во-вторых, несложно организовать следующую защиту интеллектуальной собственности в платном телевидении.

Для большого числа пользователей транслируется один и тот же шифр, а у каждого пользователя имеются незначительно отличающиеся ключи расшифровки (которые дают незначительно различающиеся открытые тексты).

В результате появляется возможность определения нарушителей, пытающихся незаконно тиражировать материал, предназначенный для индивидуального использования.

4. *Шифр SOLITAIRE*. Этот поточный алгоритм разработан Б. Шнайером (1999г.).

Для того чтобы изложить идею алгоритма предположим, что алфавит, на котором написаны сообщения, состоит из 26-и строчных букв английского алфавита (обобщение алгоритма для алфавита произвольной мощности сделать несложно).

Каждой букве ставится в соответствие целое число от 0 до 25, т.е. открытый текст имеет вид

$$m_1 \dots m_k \in \mathbf{Z}_{26}^k.$$

Шифр генерирует ключевую последовательность (гамму)

$$\gamma_1 \dots \gamma_k \in \mathbf{Z}_{26}^k.$$

Шифртекст $c_1 \dots c_k \in \mathbf{Z}_{26}^k$ формируется в соответствии с формулой

$$c_i = (m_i + \gamma_i) \,(\mathrm{mod}\, 26),$$

а расшифровка осуществляется в соответствии с формулой

$$m_i = (c_i - \gamma_i) \,(\mathrm{mod}\, 26).$$

Для формирования гаммы используется колода карт, состоящая из 52-х карт и двух джокеров α и β. Таким образом, существует

$$54! \approx 2.3 \cdot 10^{71}$$

различных состояний колоды карт.

Каждой карте следующим образом ставится в соответствие целое число от 1 до 53:

«пики»: картам туз, двойка,…, король соответствуют числа

$$1, 2, \dots, 13,$$

т.е. значение карты не меняется;

«трефы»: картам туз, двойка,…, король соответствуют числа

$$14, 15, \dots, 26,$$

т.е. к значению карты прибавляется число 13;

«бубны»: картам туз, двойка,…, король соответствуют числа

$$27, 28, \dots, 39,$$

т.е. к значению карты прибавляется число 26;

«черви»: картам туз, двойка,…, король соответствуют числа

$$40, 41, \dots, 39,$$

т.е. к значению карты прибавляется 39;

джокерам α и β ставится в соответствие число 53.

Секретный ключ шифра − начальное состояние колоды карт.

Разложим карты лицевой стороной вверх. Джокер, расположенный левее назовем 1-м джокером, а джокер, расположенный правее − 2-м джокером.

Генерация гаммы $\gamma_1 \dots \gamma_k \in \mathbf{Z}_{26}^k$ осуществляется последовательно, символ за символом. Вычисление очередного символа γ_i $(i = 1, \dots, k)$ осуществляется следующим образом:

Шаг 1. Переместим джокер α вправо через одну карту циклически, т.е. если джокер α − последняя карта, то перемещаем его за 1-ю карту.

Шаг 2. Переместим джокер β вправо через две карты циклически, т.е. если джокер β − последняя карта, то перемещаем его за 2-ю карту, а если джокер β − предпоследняя карта, то перемещаем его за 1-ю карту.

Шаг 3. Меняем местами карты, расположенные левее 1-го джокера с картами, расположенными правее 2-го джокера.

Шаг 4. Возьмем последнюю (т.е. самую правую) карту и преобразуем ее в соответствующее ей натуральное число n. Меняем местами первые n карт со следующими $53 - n$ картами.

Шаг 5. Возьмем первую (т.е. самую левую) карту и преобразуем ее в соответствующее ей натуральное число l.

Шаг 6. Если $(l+1)$-я карта − джокер, то переход к шагу 1, иначе переход к шагу 7.

Шаг 7. Фиксируем число h, соответствующее $(l+1)$-й карте.

Шаг 8. $\gamma_i := h \pmod{26}$.

Итак, каждый поточный шифр основан на последовательном, посимвольном, преобразовании входного потока данных в шифртекст посредством конечного БПИ-автомата. Поточные шифры осуществляют поэлементное шифрование потока данных практически без задержки. Поэтому их основное достоинство − высокая скорость преобразования информации, соизмеримая со скоростью поступления входной информации. Из-за этого обстоятельства именно поточные шифры наиболее пригодны для шифрования потоков данных в различных сетях передачи данных.

Все современные поточные шифры являются шифрами гаммирования. Основой любого современного поточного шифра является генератор *ключевой последовательности* (*генератор бегущего ключа*)

$$k_1 \ldots k_i \ldots.$$

Шифрование исходного текста

$$m_1 \ldots m_i \ldots$$

осуществляется в соответствии с формулой

$$c_i = m_i \oplus k_i,$$

а расшифровка — в соответствии с формулой

$$m_i = c_i \oplus k_i.$$

Стойкость поточного шифра полностью зависит от генератора ключевой последовательности. Если генератор выдает периодическую последовательность небольшого периода, то стойкость шифра невелика. Если же генератор выдает случайную последовательность бит, то получим *одноразовый блокнот* с идеальной стойкостью. Стойкость современных поточных шифров расположена примерно посередине между этими крайними случаями.

Существенным для поточных шифров является следующее обстоятельство. Если каждый раз генератор будет выдавать одну и ту же ключевую последовательность, то взломать такой шифр несложно.

Действительно, перехватив два шифртекста и сложив их поразрядно по $\mathrm{mod}\,2$, криптоаналитик получит два сложенных поразрядно по $\mathrm{mod}\,2$ исходных текста. Далее применяется техника, аналогичная той, которая изложена в примере 1.2.

Взлом поточного шифра вообще тривиален, если криптоаналитик перехватит исходный текст и соответствующий ему шифртекст, так как, сложив их поразрядно по $\mathrm{mod}\,2$, криптоаналитик получит ключевую последовательность.

Из-за указанного обстоятельства все современные потоковые шифры основаны на использовании специального ключа, от которого зависит выход генератора ключевой последовательности, что делает рассмотренный выше криптоанализ неосуществимым.

Таким образом, любой генератор ключевой последовательности − это конечный автомат, состоящий из трех блоков:

1) блок памяти, хранящий информацию о состоянии генератора ключевой последовательности;

2) блок, реализующий выходную функцию, который генерирует очередной элемент ключевой последовательности в зависимости от состояния генератора ключевой последовательности;

3) блок, реализующий функцию переходов генератора ключевой последовательности, который вычисляет состояние, в которое генератор ключевой последовательности перейдет на следующем шаге.

По-видимому, наибольшее распространение получили генераторы псевдослучайных двоичных последовательностей, построенные на основе регистров сдвига с линейными обратными связями.

Выбор именно таких генераторов обусловлен следующими обстоятельствами:

1) простая аппаратная и программная реализация;
2) высокое быстродействие;
3) близкие к идеальным статистические свойства формируемых последовательностей;
4) высокая достоверность контроля при обнаружении случайных искажений в двоичных последовательностях;
5) формирование последовательностей произвольной длины, последовательностей с предпериодом, последовательностей с произвольным законом распределения;
6) формирование последовательностей *максимальной длины*.

Для достижения последнего свойства в качестве образующего многочлена l-разрядного регистра сдвига с линейной обратной связью выбирают *примитивный многочлен* $\varphi(x)$, т.е. многочлен степени l, который не делит ни один многочлен вида $x^n \oplus 1 \quad (n \le 2^l - 1)$. В этом случае l-разрядный регистр сдвига с линейной обратной связью при любом ненулевом начальном состоянии генерирует двоичную последовательность максимальной длины 2^l.

Методам синтеза генераторов псевдослучайных двоичных последовательностей и методам анализа их характеристик посвящены многочисленные публикации (см., напр., [6,8,17,73,218,229]). В [136] изложены принципы системного подхода к сертификации генераторов псевдослучайных чисел в системах защиты информации.

При использовании поточных шифров искажение (но не потеря) отдельных битов шифртекста приводит только к локальным потерям: все знаки шифртекста, принятые без искажений будут расшифрованы правильно. Однако ситуация становится иной, если потерян хотя бы один бит шифртекста. В этом случае нарушается *синхронизация* систем шифрования и расшифровки, из-за чего вся оставшаяся часть шифртекста будет расшифрована неправильно.

Решение этой проблемы достигается за счет внедрения в поточный шифр специальной процедуры, предназначенной для восстановления синхронности функционирования отправителя и адресата. Одно из таких решений достигается вставкой в передаваемое сообщение специальных *маркеров*. В результате, из-за пропущенного бита шифртекста неправильная расшифровка будет осуществляться только до появления очередного маркера. Второе решение состоит в повторной инициализации состояний шифров отправителя и адресата при некотором предварительно согласо-

ванном условии. Третье решение состоит в построении самосинхронизирующегося шифра, в котором каждый шифруемый бит информации зависит только от ключа и от последних m бит шифртекста. Именно такие шифры в настоящее время наиболее часто применяются в дипломатических, военных и промышленных сетях связи.

Любой современный поточный шифр может быть представлен в виде двух взаимодействующих блоков: *управляющего блока* и *шифрующего блока*.

Управляющий блок вырабатывает последовательность номеров шифрующих преобразований, т.е. управляет процедурой шифрования. Эту последовательность называют *управляющей последовательностью* (или *управляющей гаммой*).

Шифрующий блок реализует алгоритм шифрования очередного символа открытого текста в соответствии с очередным символом управляющей гаммы.

Управляющий и шифрующий блоки любого поточного шифра должны удовлетворять ряду требований, нарушение которых приводит к появлению аналитических или статистических зависимостей, снижающих стойкость алгоритма шифрования.

К управляющему блоку предъявляются следующие требования:

1) период управляющей гаммы превышает максимальную длину шифруемых сообщений;

2) статистические свойства управляющей гаммы близки к свойствам случайной равновероятной последовательности;

3) в управляющей гамме отсутствуют простые аналитические зависимости между близко расположенными элементами;

4) алгоритм генерации элементов управляющей гаммы обеспечивает высокую сложность идентификации секретного ключа.

К шифрующему блоку предъявляются следующие требования:

1) применение алгоритма шифрования носит универсальный характер, и не зависит от вида шифруемой информации;

2) способ построения шифрующего блока обеспечивает стойкость шифра при перекрытиях управляющей гаммы, в частности, при повторном использовании ключей.

Разработка математических методов анализа и синтеза поточных шифров — одно из наиболее интенсивно развиваемых направлений современной криптографии [8,14,17,73,140,228,256,257,261,286,303]. Однако успехи здесь намного скромнее, чем в ситуации с блочными шифрами. По-видимому, это обусловлено высокой сложностью решения задач теории автоматов и отсутствием системной проработки ее разделов, предназначенных именно для решения задач защиты информации. Анализ современного состояние развития блочных и поточных шифров содержится в [251].

Отметим, что вычислительная стойкость современных поточных шифров характеризуется по отношению их устойчивости, по крайней мере, к следующим типам атак (см., напр., [8]):

1) атака грубой силы;

2) атаки, направленные на получение оценок вероятностных характеристик гаммы (в частности возможность применения методов оценки вероятностей элементов не равновероятной гаммы по шифртексту);

3) атаки, направленные на поиск приближений уравнений гаммообразования в классе линейных функций;

4) атаки, осуществляющие поиск комбинаторных зависимостей между элементами гаммы.

Любой шифр представляет собой только часть системы защиты информации. Для эффективного использования последней необходимо организовать взаимодействие удаленных абонентов сети по открытым каналам связи. Именно для достижения этой цели предназначены *криптографические протоколы*.

Существенным для криптографического протокола является то, что он является интерактивным, т.е. предусматривает многораундовый обмен сообщениями между участниками, и включает в себя:

1) распределенный алгоритм, т.е. характер и последовательность действий каждого участника;

2) спецификацию форматов пересылаемых сообщений;

3) спецификацию синхронизации действий участников;

4) описание действий при возникновении сбоев.

Отметим следующие два обстоятельства.

Во-первых, возможны атаки на криптографический протокол со стороны внешнего криптоаналитика. Такие атаки делятся на *пассивные* и *активные* атаки. Пассивная атака состоит в том, что криптоаналитик, не вмешиваясь в протокол, «прослушивает» его с целью получения информации. Активная атака состоит в том, что криптоаналитик, представляясь тем или иным участником, вмешивается в протокол, пытаясь изменить его к собственной выгоде.

Во-вторых, некоторые участники протокола − *мошенники* могут «обманывать» других участников или вообще не следовать протоколу. Мошенники также делятся на *пассивных* и *активных* мошенников. Пассивные мошенники исполняют протокол, но пытаются получить больше информации, чем предусмотрено протоколом. Активные мошенники нарушают нормальное исполнение протокола с целью получения выгоды для себя. Поэтому криптографический протокол должен быть разработан так, чтобы предотвращать «утечку» информации и вовремя обнаруживать «вмешательства» в нормальное исполнение протокола.

В силу указанных обстоятельств на разработку криптографических протоколов существенное влияние оказало исследование *интерактивной системы доказательств* и *доказательств с нулевым разглашением*.

Интерактивная система доказательств − это протокол (P,V,S) взаимодействия двух абонентов: доказывающего P и проверяющего V. Задача состоит в том, что абонент P хочет доказать абоненту V, что утверждение S истинно. Существуют два варианта интерактивной системы доказательств.

В 1-м варианте предполагается, что:

1) абонент V не может самостоятельно проверить утверждение S;

2) абонент V не может быть противником;

3) абонент P может быть противником, пытающимся доказать истинность ложного утверждения S.

Протокол (P,V,S) должен удовлетворять условию *полноты* (если S − истинное утверждение, то абонент P убедит абонента V признать этот факт) и условию *корректности* (если S − ложное утверждение, то абонент P не сможет убедить абонента V в том, что утверждение S истинно).

Во 2-м варианте предполагается, что выполнены 1-е и 3-е условия, а 2-е условие заменяется условием: абонент V может быть противником, который хочет получить информацию об утверждении S.

В этом случае требуется, чтобы протокол (P,V,S) удовлетворял условиям полноты, корректности и условию *нулевого разглашения* (в результате работы протокола абонент V не увеличивает своих знаний об утверждении S).

Отметим, что доказательства с нулевым разглашением играют существенную роль при реализации протоколов аутентификации клиентов банка, при создании электронных не поддающихся подделке удостоверений личности и т.д.

Из-за возможного наличия мошенников вытекает, что не все участники криптографических протоколов доверяют друг другу. С этой точки зрения в настоящее время выделяют следующие типы криптографических протоколов.

1. *Протоколы с посредником*, т.е. незаинтересованной стороной, которой доверено довести до конца исполнение протокола. Слово «доверено» означает, что все участники протокола уверены, что посредник выполнит свою часть протокола, воспринимают его слова за истину, а также признают правильными все его действия. Однако при использовании компьютерных посредников возникают следующие проблемы:

1) сложно доверять безликому посреднику, находящемуся где-то в компьютерной сети;

2) кем-то должны покрываться расходы на поддержку компьютерного посредника;

3) всем протоколам с посредником свойственна врожденная задержка;

4) компьютерный посредник − это узкое место при крупномасштабных реализациях протокола;

5) компьютерный посредник является потенциальной мишенью для атак хакеров.

2. *Протоколы с арбитром*, т.е. посредником, который принимает участие в исполнении протокола только тогда, когда возникают разногласия между участниками протокола. Это означает, что протокол с арбитром разбивается на два протокола более низкого уровня. Первый протокол является протоколом без посредника. Он исполняется в тех случаях, когда все участники доверяют друг другу, а также намерены выполнять протокол. Второй протокол является протоколом с посредником. Он исполняется только в тех случаях, когда между участниками возникает недоверие или разногласия. Протоколы с арбитром обеспечивают решение ряда проблем, возникающих для протокола с посредником.

3. *Самодостаточные протоколы*. Эти протоколы не требуют посредника. Они построены так, что любая попытка мошенничества со стороны участников сразу же будет обнаружена, а исполнение протокола прекратится. Этот тип протоколов намного более эффективен, чем предыдущие два. К сожалению, самодостаточные протоколы существуют не для всех ситуаций.

4. *Протоколы разделения секрета*. Такой протокол (его также называют *схемой разделения секрета* или *СРС*) обеспечивают доступ не доверяющим друг другу участникам к секретной информации только при одновременном предъявлении ими своих полномочий. Любая *СРС* предполагает, что выделен один участник D − *дилер*, распределяющий части секрета ζ между множеством S тех участников, которым разрешен доступ к этой информации. Эти части секрета распределяются так, что восстановить секрет ζ могут только все участники, принадлежащие множеству S при их совместном действии. Кроме того, ни один участник, не принадлежащий множеству S, не получает никакой информации о значении ζ. Подчеркнем, что любая *СРС* содержит две стадии: *стадию распределения секрета* и *стадию восстановления секрета*.

Эффективность и надежность криптографической защиты информации в компьютерных сетях во многом зависит от эффективности и надежности подсистемы управления криптографическими ключами, так как успешная атака криптоаналитика на эту подсистему может не только дестабилизировать работу всей сети, но и вызвать широкомасштабную утечку информации.

Понятие «управление криптографическими ключами» включает в себя разработку протоколов, предназначенных для решения следующих задач:

1) генерация криптографических ключей;

2) распределение криптографических ключей;

3) хранение криптографических ключей;
4) замена криптографических ключей;
5) депонирование криптографических ключей;
6) уничтожение криптографических ключей.

Сложность комплексного решения этих задач обусловлена не только сложностью среды, но и существенными отличиями криптографических ключей по их предназначению и времени жизни. Выделяют следующие три группы криптографических ключей:

1) *мастер-ключи* (их обозначают K_m) сети, серверов, компьютеров и терминалов, которые используются для шифрования и генерации ключей;

2) *ключи шифрования ключей* (их обозначают K_F), которые предназначены для шифрования других ключей при их распределении;

3) *сеансовые ключи* (их обозначают $K_{A,B}$), которые используются для шифрования данных в сеансе связи между пользователями A и B сети.

Для генерации мастер-ключей используют физические генераторы случайных последовательностей, а распределяются и устанавливаются эти ключи специальным образом. Для генерации ключей шифрования ключей и сеансовых ключей используются как физические генераторы, так и псевдослучайные методы с секретными параметрами. В последнем случае для генерации ключей часто применяется стандартная шифрсистема.

Задача распределения сеансовых ключей между участниками информационного обмена в сети решается двумя способами:

1) прямой обмен сеансовыми ключами между пользователями сети;
2) с использованием центров распределения ключей.

Целесообразность создания центров распределение ключей обусловлена следующим. В сети, содержащей n пользователей, число обменов сеансовыми ключами может достигать величины $0.5 \cdot n \cdot (n-1)$. С учетом времени, необходимого для совершения одного обмена, отсюда вытекает, что непроизводительная нагрузка, как на пользователей, так и на сеть становится ощутимой. Поэтому для повышения эффективности работы сети удобнее создать центральный сервер или несколько таких серверов, предназначенных для распределения ключей.

Очевидно, что секретные ключи не должны храниться в явном виде, так как в этом случае они могут быть просто считаны криптоаналитиком. Поэтому любая информация об используемых ключах должна храниться в зашифрованном виде. Именно поэтому вводится иерархия ключей. Такая иерархия может быть либо двухуровневой

ключи шифрования ключей $\rightarrow$ *сеансовые ключи*,

либо трехуровневой

мастер-ключи $\rightarrow$ *ключи шифрования ключей* $\rightarrow$ *сеансовые ключи*.

Каждый из указанных выше типов ключей различается по последствиям компрометации, времени жизни и способам формирования.

Как правило, в каждом компьютере используется один мастер-ключ. Он должен храниться в модуле системы защиты информации, защищенном от считывания, записи и разрушающих воздействий. Мастер-ключ распространяется неэлектронным способом, исключающим его компрометацию. Кроме того, в системе защиты информации должен существовать способ проверки аутентичности мастер-ключа. Один из способов такой проверки имеет вид, представленный на рис. 1.37.

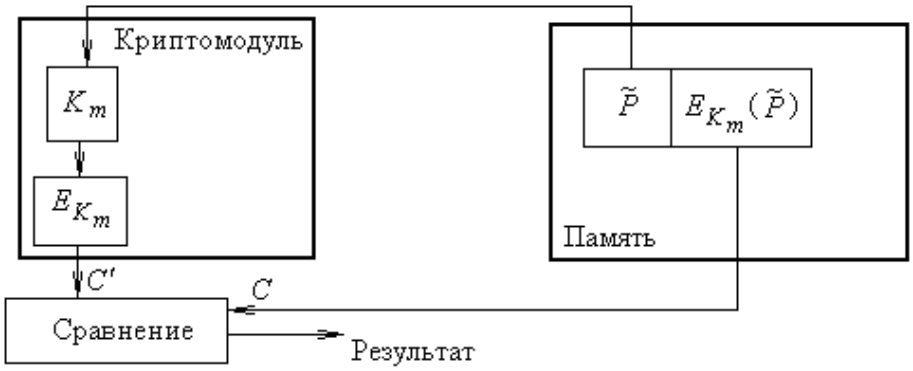


Рис. 1.37. Схема аутентификации мастер-ключа.

В памяти компьютера хранится пара $(\tilde{P}, C)$, где $\tilde{P}$ фиксированный массив данных, а $C = E_{K_m}(\tilde{P})$ − результат его шифрования на мастер-ключе K_m. Каждый раз, когда требуется проверка аутентичности мастер-ключа, массив $\tilde{P}$ считывается из памяти и подается на вход криптомодуля. Полученный шифртекст сравнивается с шифртекстом, хранящимся в памяти. При положительном результате аутентичность мастер ключа считается установленной. При отрицательном результате считается, что мастер-ключ сфальсифицирован.

Ключи шифрования ключей могут храниться в соответствии с описанной выше схемой хранения мастер-ключа, либо в соответствии с рассмотренной ниже схемой хранения сеансового ключа.

При генерации сеансового ключа K_s пользователь получает шифртекст $E_{K_m}(K_s)$ (рис. 1.38).

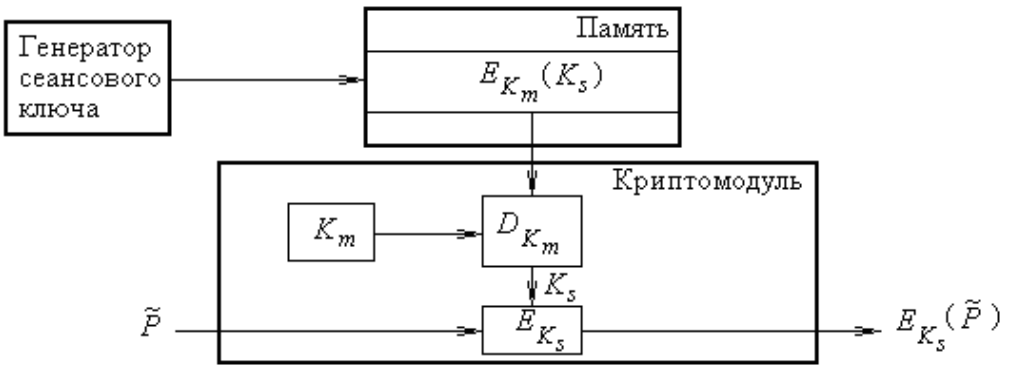


Рис. 1.38. Схема защиты сеансового ключа.

Этот шифртекст может храниться в памяти.

При шифровании сообщения $\tilde{P}$ это сообщение и шифртекст $E_{K_m}(K_s)$ подаются на вход криптомодуля. Последний вначале «восстанавливает» сеансовый ключ K_s, а затее осуществляет шифрование сообщения $\tilde{P}$.

Ясно, что проще всего хранить сеансовые ключи криптосистемы с одним пользователем. В этом случае возможны следующие три варианта, перечисленные в порядке возрастания их надежности:

1) запоминается пароль p, а (при необходимости) автоматическое получение ключа осуществляется с использованием хэш-функции h, т.е.

$$k_s = h(p);$$

2) запоминается начальное заполнение генератора, формирующего сеансовый ключ, и при необходимости получения очередного сеансового ключа этот генератор запускается;

3) используется пластиковый ключ (*ROM-key*).

Отметим, что любой ключ должен использоваться в течение ограниченного промежутка времени, длительность которого зависит от следующих трех факторов:

1) частоты использования ключа;

2) величины ущерба от компрометации ключа, которая зависит от «ценности» защищаемой информации;

3) объема и характера защищаемой информации.

При этом следует принимать во внимание, что:

1) чем дольше используется ключ, тем больше вероятность его компрометации;

2) чем дольше используется ключ, тем больший потенциальный ущерб может нанести его компрометация;

3) чем больше объем информации, зашифрованной на одном ключе, тем легче криптоаналитику осуществить атаку на этот ключ;

4) при длительном использовании ключа у криптоаналитика может возникнуть дополнительный стимул для вскрытия ключа, если его затраты будут перекрыты выгодой, полученной от вскрытия ключа.

В заключение отметим, что в настоящее время уделяется большое внимание проблеме анализа безопасности криптографических протоколов, предназначенных для обмена сеансовыми ключами. Многообразие математических моделей и методов, применяемых для построения таких протоколов [8,17,73,117,218,225,228,238285,288,293], существенно усложняют системную проработку этой проблемы.

По-видимому, такая ситуация вызвана прежде всего тем, что в настоящее время отсутствует достаточно детализированная формальная модель взаимодействия «криптосистема − внешняя среда». Одна из первых попыток построения такой модели предпринята в [282].

1.4. Арифметические и алгебраические основы криптологии.

Теоретико-числовые и алгебраические методы представляют собой мощный математический аппарат анализа и синтеза современных шифров [8,17,73,218,229]. Более того, практически все схемы, представленные в проектах NESSIE и CRYPTREC в качестве кандидата на новый стандарт поточного шифра, основаны на использовании автоматов над полем $\mathbf{GF}(2^k)$ $(k = 16, 32)$.

Рассмотрим вначале основные понятия и определения теории чисел, используемые в последующих разделах (см., напр., [27,78,115,218,224]).

Запись $a \equiv b \pmod m$ $(a, b \in \mathbf{Z}, m \in \mathbf{N})$ называется *сравнением по модулю* m и означает утверждение о том, что числа a и b имеют один и тот же остаток при делении на число m. Так как $a \equiv b \pmod 1$ для любых чисел $a, b \in \mathbf{Z}$, то всюду ниже предполагается, что $m \geq 2$. Истинны следующие утверждения ((a,b) − НОД чисел a и b, $[a,b]$ − НОК чисел a и b, а $b \mid a$ − утверждение «число b − делитель числа a»):

1) $a \equiv a \pmod m$;
2) $a \equiv b \pmod m$ тогда и только тогда, когда $b \equiv a \pmod m$;
3) если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, то $a \equiv c \pmod m$;
4) если $a \equiv b \pmod m$, то $(a, m) = (b, m)$;
5) если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a + c \equiv b + d \pmod m$;
6) если $a \equiv b \pmod m$, то $a + c \equiv b + c \pmod m$ для любого числа $c \in \mathbf{Z}$;
7) если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a \cdot c \equiv b \cdot d \pmod m$;
8) если $a \equiv b \pmod m$, то $a \cdot c \equiv b \cdot c \pmod m$ для любого числа $c \in \mathbf{Z}$;
9) если $a \cdot c \equiv b \cdot c \pmod m$ $(c \in \mathbf{Z} \setminus \{0\})$ и $(|c|, m) = 1$, то $a \equiv b \pmod m$;
10) если $a \cdot c \equiv b \cdot c \pmod{m \cdot c}$ $(c \in \mathbf{N})$, то $a \equiv b \pmod m$;
11) если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1, m_2]}$;
12) если $a \equiv b \pmod m$, $c \mid a$ и $c \mid m$, то $c \mid b$;
13) если $a \equiv b \pmod m$ и $m = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ − каноническое разложение числа m, то $a \equiv b \pmod{p_i^j}$ $(j = 1, \ldots, k_i)$ для всех $i = 1, \ldots, l$.

Для любого модуля m бинарное отношение $\equiv$ определяет разбиение множества $\mathbf{Z}$ на m классов эквивалентных элементов (их называют *классы вычетов по модулю* m).

Взяв по одному представителю из каждого класса, получим *полную систему вычетов по модулю* m.

Если взять по одному представителю из всех классов, содержащих взаимно-простые с модулем m числа, то получим *приведенную систему вычетов по модулю* m.

Истинны следующие два утверждения:

1) для любых чисел $a,b\in\mathbf{Z}$, если $(a,m)=1$ и x пробегает полную систему вычетов по модулю m, то $a\cdot x+b$ пробегает полную систему вычетов по модулю m;

2) для любого числа $a\in\mathbf{Z}$, если $(a,m)=1$ и x пробегает приведенную систему вычетов по модулю m, то $a\cdot x$ пробегает приведенную систему вычетов по модулю m.

Как правило, полная система вычетов по модулю m отождествляется с множеством $\mathbf{Z}_m$, а приведенная система вычетов по модулю m − с множеством

$$\mathbf{Z}_{m-rd}=\{a\in\mathbf{Z}_m\mid(a,m)=1\}.$$

Количество элементов приведенной системы вычетов по модулю m равно значению *функции Эйлера* $\varphi(m)$ ($\varphi(m)$ − это число элементов множества $\mathbf{Z}_m$, взаимно-простых с числом m). Известно, что

$$\varphi(1)=1$$

и для всех $m\geq 2$, если $m=p_1^{k_1}\cdot\ldots\cdot p_l^{k_l}$ − каноническое разложение числа m, то

$$\varphi(m)=(p_1^{k_1}-p_1^{k_1-1})\cdot\ldots\cdot(p_l^{k_l}-p_l^{k_l-1}).$$

Отметим следующие свойства функции Эйлера:

1) если $(m_1,m_2)=1$ $(m_1,m_2\in\mathbf{N})$, то

$$\varphi(m_1\cdot m_2)=\varphi(m_1)\cdot\varphi(m_2);$$

2) (*теорема Эйлера*) если $(a,m)=1$ $(a\in\mathbf{Z},m\in\mathbf{N})$, то

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m).$$

Из теоремы Эйлера вытекает *малая теорема Ферма*: для любого простого числа p если $(a,p)=1$ $(a\in\mathbf{Z},m\in\mathbf{N})$, то

$$a^{p-1}\equiv 1(\mathrm{mod}\,p).$$

Рассмотрим методы решения простейших сравнений.

Решением сравнения по модулю m с одним неизвестным называются классы вычетов по модулю m, элементы которых удовлетворяют этому сравнению.

Рассмотрим линейное сравнение

$$a\cdot x\equiv b(\mathrm{mod}\,m)\quad(a\in\mathbf{Z}_m). \tag{1.3}$$

Решения этого сравнения находятся следующим образом:

1) если $a\in\mathbf{Z}_{m-rd}$, то сравнение (1.3) имеет единственное решение

$$x\equiv a^{\varphi(m)-1}\cdot b(\mathrm{mod}\,m);$$

2) если $(a,m)=d$ $(d>1)$ и $d\mid b$, то сравнение (1.3) имеет d решений

$$x_1,x_1+(d^{-1}\cdot m),\ldots,x_1+(d-1)\cdot(d^{-1}\cdot m),$$

где

$$x_1\equiv(d^{-1}\cdot a)^{\varphi(d^{-1}\cdot m)-1}\cdot(d^{-1}\cdot b)(\mathrm{mod}\,(d^{-1}\cdot m));$$

3) если $(a,m)=d$ $(d>1)$ и $d \nmid b$, то сравнение (1.3) не имеет решений.

Рассмотрим систему линейных сравнений

$$\begin{cases} a_1 \cdot x \equiv b_1 \pmod{m_1} \\ \quad\vdots \\ a_n \cdot x \equiv b_n \pmod{m_n} \end{cases}, \quad (a_1,\ldots,a_n \in \mathbf{N}). \tag{1.4}$$

где $a_i \in \mathbf{Z}_{m_i}$ $(i=1,\ldots,n)$.

Решениями системы (1.4) называются классы вычетов по модулю $[m_1,\ldots,m_n]$, элементы которых удовлетворяют этой системе.

Система (1.4) заведомо не имеет решений в случае, когда условие «если $(a_i,m_i)=d_i$, то $d_i \mid b_i$» не выполнено, по крайней мере, для одного $i \in \{1,\ldots,n\}$. Если же указанное условие выполнено для всех $i \in \{1,\ldots,n\}$, то поиск решений системы (1.4) сводится к решению $\prod_{i=1}^{n} d_i$ систем сравнений

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ \quad\vdots \\ x \equiv c_n \pmod{m_n} \end{cases}, \tag{1.5}$$

где

$$x \equiv c_i \pmod{m_i} \quad (i=1,\ldots,n)$$

является решением сравнения

$$a_i \cdot x \equiv b_i \pmod{m_i}.$$

Решение системы (1.5) сводится к последовательной замене системы двух сравнений

$$\begin{cases} x \equiv e_1 \pmod{k_1} \\ x \equiv e_2 \pmod{k_2} \end{cases} \tag{1.6}$$

ее решением.

Система (1.6) имеет решения по модулю $[k_1,k_2]$ тогда и только тогда, когда $(k_1,k_2) \mid (e_2-e_1)$. Это решение − единственное и имеет вид

$$x \equiv e_1 + k_1 \cdot t \pmod{[k_1,k_2]},$$

где t − единственное решение сравнения

$$\frac{k_1}{(k_1,k_2)} \cdot t \equiv \frac{e_2-e_1}{(k_1,k_2)} \left(\mathrm{mod}\ \frac{k_2}{(k_1,k_2)} \right).$$

Отметим, что если модули $m_1,\ldots,m_n$ − попарно взаимно простые числа, то единственное решение системы (1.5) может быть найдено следующим образом.

Теорема 1.2 (*китайская теорема об остатках*). При попарно взаимно простых модулях $m_1,\ldots,m_n$ система сравнений (1.5) имеет единственное решение

$$x \equiv \sum_{i=1}^{n}\left(\prod_{j=1}^{i-1} m_j\right)\cdot x_i \cdot \left(\prod_{j=i+1}^{n} m_j\right)\cdot c_i \ (\mathrm{mod}\,[m_1,\ldots,m_n]),$$

где x_i $(i=1,\ldots,n)$ − единственное решение сравнения

$$\left(\prod_{j=1}^{i-1} m_j\right)\cdot\left(\prod_{j=i+1}^{n} m_j\right)\cdot x_i \equiv 1 (\mathrm{mod}\, m_i).$$

Пусть $(a,m)=1$. Число a *принадлежит показателю* δ *по модулю* m, если δ − такое наименьшее натуральное число, что

$$a^{\delta} \equiv 1 (\mathrm{mod}\, m).$$

Истинны следующие утверждения:

1) числа $1, a,\ldots,a^{\delta-1}$ попарно несравнимы по модулю m;

2) $a^{n_1} \equiv a^{n_2} (\mathrm{mod}\, m)$ $(n_1, n_2 \in \mathbf{N})$ тогда и только тогда, когда $n_1 \equiv n_2 (\mathrm{mod}\,\delta)$;

3) $\delta \mid \varphi(m)$.

Число a, принадлежащее показателю $\varphi(m)$, называется *первообразным корнем по модулю* m. Истинны следующие утверждения:

1) первообразный корень по модулю m существует тогда и только тогда, когда

$$m \in \{2,4\} \cup \{p^n, 2\cdot p^n \mid p - \textit{нечетное простое число},\ n \in \mathbf{N}\};$$

2) если $(a,m)=1$ и $p_1,\ldots p_k$ − все различные простые делители числа $\varphi(m)$, то a − первообразный корень по модулю m тогда и только тогда, когда ложны все сравнения

$$a^{p_i^{-1}\cdot\varphi(m)} \equiv 1 (\mathrm{mod}\, m) \quad (i=1,\ldots,k);$$

3) если a − первообразный корень по модулю m, а число k принимает последовательно значения $0,1,\ldots,\varphi(m)-1$, то число a^k пробегает приведенную систему вычетов по модулю m.

Зафиксируем модуль

$$m \in \{2,4\} \cup \{p^n, 2\cdot p^n \mid p - \textit{нечетное простое число},\ n \in \mathbf{N}\}$$

и первообразный корень $a \in \mathbf{Z}_{m-rd}$ по модулю m. Число $k \in \mathbf{Z}_{\varphi(m)}$ называется *индексом* (или *дискретным логарифмом*) *числа* $b \in \mathbf{Z}_{m-rd}$ *по модулю* m, если

$$b \equiv a^k (\mathrm{mod}\, m).$$

В этом случае используют обозначение

$$k = ind_a b.$$

Истинны следующие утверждения:

1) $ind_a(b \cdot c) \equiv (ind_a b + ind_a c) \pmod{\varphi(m)}$ $(b, c \in \mathbf{Z}_{m-rd})$;

2) $ind_a b^l \equiv (l \cdot ind_a b) \pmod{\varphi(m)}$ $(b \in \mathbf{Z}_{m-rd})$;

3) если $b, l \in \mathbf{Z}_{m-rd}$, то сравнение

$$l^k \equiv b \pmod{m}$$

эквивалентно сравнению

$$k \cdot ind_a l \equiv ind_a b \pmod{\varphi(m)}.$$

Из последнего утверждения вытекает, что:

2) если $b \in \mathbf{Z}_{m-rd}$, то степенное сравнение

$$x^k \equiv b \pmod{m} \tag{1.7}$$

эквивалентно сравнению

$$k \cdot ind_a x \equiv ind_a b \pmod{\varphi(m)} \tag{1.8}$$

и, следовательно, степенное сравнение (1.7) имеет решения тогда и только тогда, когда $(k, \varphi(m)) \mid ind_a b$;

2) если $b, c \in \mathbf{Z}_{m-rd}$, то показательное сравнение

$$c^x \equiv b \pmod{m} \tag{1.9}$$

эквивалентно сравнению

$$x \cdot ind_a c \equiv ind_a b \pmod{\varphi(m)} \tag{1.10}$$

и, следовательно, сравнение (1.9) имеет решения тогда и только тогда, когда выполнено условие $(ind_a c, \varphi(m)) \mid ind_a b$.

При наличии таблицы индексов решение сравнений (1.7) и (1.9) сводится к решению сравнений, соответственно, (1.8) и (1.10). Однако в явном виде эти таблицы могут быть построены только для небольших значений модуля m.

При больших значениях модуля m работа с таблицей индексов сводится к последовательной генерации чисел $a^l \pmod{m}$ для всех $l \in \mathbf{Z}_{\varphi(m)}$.

Высокая сложность решения сравнений (1.7) и (1.9) делает привлекательным их использование при решении задач защиты информации.

Действительно, зафиксируем модуль

$$m \in \{2,4\} \cup \{p^n, 2 \cdot p^n \mid p - \textit{нечетное простое число}, \ n \in \mathbf{N}\}$$

и первообразный корень $a \in \mathbf{Z}_{m-rd}$ по модулю m.

Выберем в качестве секретного ключа упорядоченную пару чисел (a, k) $(k \in \mathbf{Z}_{\varphi(m)})$, а в качестве открытого ключа − число $b \in \mathbf{Z}_{m-rd}$, являющееся решением сравнения

$$b \equiv a^k \pmod{m}.$$

Идентификацию секретного ключа можно осуществить в два этапа.

На 1-м этапе осуществляется поиск множества всех упорядоченных пар чисел (α, κ), являющихся возможными кандидатами на секретный ключ, где $\alpha \in \mathbf{Z}_{m-rd}$ − первообразный корень модулю m и $\kappa = ind_{\alpha} b$.

На 2-м этапе истинный секретный ключ (a,k) выделяется из этого множества с помощью дополнительной информации.

Даже если известно в точности одно из чисел a или k, поиск секретного ключа (a,k) при больших значениях модуля m имеет высокую сложность, так как таблицы индексов отсутствуют в явном виде.

Отметим, что если секретным ключом является упорядоченная тройка чисел (a,k,m), то сложность его идентификация существенно выше, чем в рассмотренном случае.

Высокая сложность поиска решений степенного сравнения (1.7) обосновывает актуальность поиска эффективного критерия существования этих решений. Рассмотрим такой критерий для сравнения 2-й степени, имеющего нетривиальные приложения при решении задач защиты информации.

Число $b \in \mathbf{Z}_{m-rd}$ называется *квадратичным вычетом по модулю* m, если сравнение

$$x^2 \equiv b \,(\mathrm{mod}\, m). \qquad (1.11)$$

имеет решения и *квадратичным невычетом по модулю* m, если сравнение (1.11) не имеет решений.

Замечание 1.3. Если

$$m \in \{p^n, 2 \cdot p^n \mid p - \textit{нечетное простое число},\ n \in \mathbf{N}\},$$

то число квадратичных вычетов по модулю m, а также число квадратичных невычетов модулю m равно $0.5 \cdot \varphi(m)$.

Действительно, пусть $a \in \mathbf{Z}_{m-rd}$ − первообразный корень по модулю m. Тогда:

1) множество квадратичных вычетов по модулю m имеет вид

$$\{b \in \mathbf{Z}_{m-rd} \mid b \equiv a^{2 \cdot k} \,(\mathrm{mod}\, m) \ \textit{для некоторого}\ k \in \mathbf{Z}_{0.5 \cdot \varphi(m)}\};$$

3) множество квадратичных невычетов по модулю m имеет вид

$$\{b \in \mathbf{Z}_{m-rd} \mid b \equiv a^{2 \cdot k+1} \,(\mathrm{mod}\, m) \ \textit{для некоторого}\ k \in \mathbf{Z}_{0.5 \cdot \varphi(m)}\}.$$

Пусть m − нечетное число, а разложение числа m на простые множители имеет вид $m = p_1 \cdot \ldots \cdot p_l$.

Число $b \in \mathbf{Z}_{m-rd}$ принадлежит множеству квадратичных вычетов по модулю m тогда и только тогда, когда для всех $i = 1, \ldots, l$

$$\left(\frac{b}{p_i}\right) = 1,$$

где $\left(\frac{b}{p}\right)$ (p − простое нечетное число, $b \in \mathbf{Z}$, $(b,p) = 1$) — *символ Лежандра*.

Формально символ Лежандра определяется равенством

$$\left(\frac{b}{p}\right)=\begin{cases} 1, \textit{ если сравнение } x^2 \equiv b \pmod p \textit{ имеет решения} \\ -1, \textit{ если сравнение } x^2 \equiv b \pmod p \textit{ не имеет решений} \end{cases},$$

а для упрощения его вычисления используют следующие равенства

$$\left(\frac{b\cdot c}{p}\right)=\left(\frac{b}{p}\right)\cdot\left(\frac{c}{p}\right),$$

$$\left(\frac{b}{p}\right)\equiv b^{0.5\cdot(p-1)} \pmod p,$$

$$\left(\frac{q}{p}\right)=(-1)^{0.25\cdot(p-1)\cdot(q-1)}\cdot\left(\frac{p}{q}\right) \ (q \text{ − простое нечетное число}).$$

Поиск решения произвольного полиномиального сравнения

$$\sum_{i=0}^{n} a_i \cdot x^i \equiv 0 \pmod m, \tag{1.12}$$

где $a_i \in \{0,1,\ldots,m-1\}$ $(i=0,1,\ldots,n)$, значительно сложнее, чем поиск решения рассмотренного выше степенного сравнения (1.7). Все известные методы решения сравнения (1.12) сводятся к решению специально построенной системы полиномиальных диофантовых уравнений (см., напр., [70]).

Высокая сложность решения диофантовых уравнений с параметрами является теоретической предпосылкой для высокой сложности идентификации секретного ключа, построенного на основе этих решений. Проиллюстрируем некоторые особенности решения диофантовых уравнений с параметрами.

Пример 1.4. В [152] рассмотрено диофантово уравнение с параметрами

$$x_1+\ldots+x_n = k\cdot x_1\cdot\ldots\cdot x_n, \tag{1.13}$$

где $k\in\mathbf{Z}$ и $n\in\mathbf{N}$.

Обозначим через $S(n,k)$ $(k\in\mathbf{Z}, n\in\mathbf{N})$ множество решений уравнения (1.13), т.е.

$$S(n,k)=\{(\alpha_1,\ldots,\alpha_n)\in\mathbf{Z}^n \mid \alpha_1+\ldots+\alpha_n = k\cdot\alpha_1\cdot\ldots\cdot\alpha_n\}.$$

Исследуем множество $S(n,k)$ в зависимости от значений параметров $k\in\mathbf{Z}$ и $n\in\mathbf{N}$.

Утверждение 1.1. Для всех $n\in\mathbf{N}$

$$S(n,k)\neq\varnothing$$

при всех значениях $k\in\mathbf{Z}$.

Доказательство. Так как

$$(\underbrace{0,\ldots,0}_{n\ раз})\in S(n,k)$$

для всех $k\in\mathbf{Z}$ и $n\in\mathbf{N}$, то

$$S(n,k)\neq\varnothing.$$

Утверждение доказано.

Рассмотрим следующие три случая.

Случай 1. $n=1$. Уравнение (1.13) принимает следующий вид

$$x_1 = k \cdot x_1 \quad (k \in \mathbf{Z}). \tag{1.14}$$

Теорема 1.3. Истинны равенства

$$S(1,k) = \begin{cases} \mathbf{Z}, \ \textit{если} \ \ k=1 \\ \{0\}, \ \textit{если} \ \ k=2,3,\ldots \end{cases}.$$

Доказательство. Пусть $k=1$. Тогда уравнение (1.14) имеет вид $x_1 = x_1$. Последнее равенство истинно для всех $x_1 \in \mathbf{Z}$. Следовательно, $S(1,1) = \mathbf{Z}$.

Пусть $k = 2,3,\ldots$. Тогда

$$x_1 = k \cdot x_1 \Leftrightarrow (1-k) \cdot x_1 = 0 \Leftrightarrow x_1 = 0 \Leftrightarrow S(1,k) = \{0\}.$$

Теорема доказана.

Следствие 1.1. Истинны равенства

$$|\, S(1,k)\,| = \begin{cases} \infty, \ \textit{если} \ \ k=1 \\ 1, \ \textit{если} \ \ k=2,3,\ldots \end{cases}.$$

Случай 2. $n=2$. Уравнение (1.13) принимает следующий вид

$$x_1 + x_2 = k \cdot x_1 \cdot x_2 \quad (k \in \mathbf{Z}). \tag{1.15}$$

Теорема 1.4. Истинны равенства

$$S(2,k) = \begin{cases} \{(l,-l) \mid l \in \mathbf{Z}\}, \ \textit{если} \ \ k=0 \\ \{(0,0)\}, \ \textit{если} \ \ |\,k\,| \geq 3 \\ \{(0,0),(-2,-2)\}, \ \textit{если} \ \ k=-1 \\ \{(0,0),(2,2)\}, \ \textit{если} \ \ k=1 \\ \{(0,0),(-1,-1)\}, \ \textit{если} \ \ k=-2 \\ \{(0,0),(1,1)\}, \ \textit{если} \ \ k=2 \end{cases}.$$

Доказательство. 1. Предположим, что $k=0$. Решая уравнение (1.15), получим

$$x_1 + x_2 = 0 \Leftrightarrow x_2 = -x_1 \Leftrightarrow S(2,0) = \{(l,-l) \mid l \in \mathbf{Z}\}.$$

2. Предположим, что $k \neq 0$. Тогда для любого решения (x_1, x_2) уравнения (1.15)

$$x_1 = 0 \Leftrightarrow x_2 = 0.$$

Следовательно, при любом значении $k \neq 0$, если уравнение (1.15) имеет такое решение (x_1, x_2), что

$$(x_1, x_2) \neq (0,0),$$

то $x_1 \neq 0$ и $x_2 \neq 0$.

Предположим, что (x_1, x_2) – такое решение уравнения (1.15), что $x_1 \neq 0$ и $x_2 \neq 0$. Преобразуем уравнение (1.15) к виду

$$x_2 = x_1 \cdot (k \cdot x_2 - 1). \tag{1.16}$$

Если $k \cdot x_2 - 1 = 0$, то $k \cdot x_2 = 1$ и $x_2 = 0$. Получено противоречие.

Следовательно,

$$k \cdot x_2 - 1 \neq 0.$$

Так как $x_1 \neq 0$, $x_2 \neq 0$, $k \cdot x_2 - 1 \neq 0$ $(k \neq 0)$ и $x_1, x_2 \in \mathbf{Z}$, то из (1.16) вытекает, что

$$|k \cdot x_2 - 1| = 1.$$

Следовательно, либо

$$k \cdot x_2 - 1 = -1 \Leftrightarrow k \cdot x_2 = 0,$$

либо

$$k \cdot x_2 - 1 = 1 \Leftrightarrow k \cdot x_2 = 2.$$

Равенство $k \cdot x_2 = 0$ противоречит условию $k \neq 0$ и $x_2 \neq 0$. Следовательно,

$$k \cdot x_2 = 2. \qquad (1.17)$$

Из условия $k \neq 0$ вытекает, что целочисленные решения уравнения (1.17) существуют тогда и только тогда, когда $k \in \{-1,1,-2,2\}$.

Следовательно,

$$S(2,k) = \{(0,0)\}$$

для всех таких $k \in \mathbf{Z}$, что $|k| \geq 3$.

Пусть $k \in \{-1,1,-2,2\}$.

Если $k = 1$, то $x_2 = 2$. Подставив эти значения в уравнение (1.16), получим $x_1 = 2$, т.е. $(x_1, x_2) = (2,2)$ – решение уравнения (1.16). Следовательно,

$$S(2,1) = \{(0,0),(2,2)\}.$$

Если $k = -1$, то $x_2 = -2$. Подставив эти значения в уравнение (1.16), получим $x_1 = -2$, т.е. $(x_1, x_2) = (-2,-2)$ – решение уравнения (1.16). Следовательно,

$$S(2,-1) = \{(0,0),(-2,-2)\}.$$

Если $k = 2$, то $x_2 = 1$. Подставив эти значения в уравнение (1.16), получим $x_1 = 1$, т.е. $(x_1, x_2) = (1,1)$ – решение уравнения (1.16). Следовательно,

$$S(2,2) = \{(0,0),(1,1)\}.$$

Если $k = -2$, то $x_2 = -1$. Подставив эти значения в уравнение (1.16), получим $x_1 = -1$, т.е. $(x_1, x_2) = (-1,-1)$ – решение уравнения (1.16). Следовательно,

$$S(2,-2) = \{(0,0),(-1,-1)\}.$$

Теорема доказана.

Следствие 1.2. Если $n = 2$, то

$$|S(2,k)| = \begin{cases} \infty, \ \textit{если} \ k = 0 \\ 1, \ \textit{если} \ |k| \geq 3 \\ 2, \ \textit{если} \ k \in \{-1,1,-2,2\} \end{cases}.$$

Случай 3. $n \geq 3$. Для каждого значения $j = 1,\ldots,n$ положим

$$S_j(n,k) = \{(\alpha_1,\ldots\alpha_n) \in \mathbf{Z}^n \mid \alpha_j = 0, \ \sum_{i=1}^{n} \alpha_i = 0\}.$$

Ясно, что для всех $k \in \mathbf{Z}$ истинно включение

$$S(n,k) \supseteq \bigcup_{j=1}^{n} S_j(n,k). \qquad (1.18)$$

Утверждение 1.2. Для всех $n \geq 3$ при всех значениях $k \in \mathbf{Z}$

$$|S_j(n,k)| = \infty \quad (j = 1,\ldots,n).$$

Доказательство. Пусть $j = 1$. Положим

$$\mathbf{a}_1(l) = (0,-(n-2)\cdot l, \underbrace{l,\ldots,l}_{n-2 \text{ раз}}) \quad (l \in \mathbf{Z}).$$

Так как $\mathbf{a}_1(l) \in S_1(n,k)$ для всех значений $l \in \mathbf{Z}$, то

$$|S_1(n,k)| = \infty.$$

Пусть $j \in \{2,\ldots,n\}$. Положим

$$\mathbf{a}_j(l) = (-(n-2)\cdot l, \underbrace{l,\ldots,l}_{j-2 \text{ раз}}, 0, \underbrace{l,\ldots,l}_{n-j \text{ раз}}) \quad (l \in \mathbf{Z}).$$

Так как $\mathbf{a}_j(l) \in S_j(n,k)$ $(j = 2,\ldots,n)$ для всех значений $l \in \mathbf{Z}$, то

$$|S_j(n,k)| = \infty.$$

Утверждение доказано.

Следствие 1.3. Для всех $n \geq 3$ при всех значениях $k \in \mathbf{Z}$

$$|S(n,k)| = \infty.$$

Следствие 1.3 вытекает из утверждения 1.2 и включения (1.18).

Следующие теоремы дают возможность усилить включение (1.18) для ряда специальных случаев.

Теорема 1.5. Если $n \geq 3$ и $|k| > n$ $(k \in \mathbf{Z})$, то

$$S(n,k) = \bigcup_{j=1}^{n} S_j(n,k). \tag{1.19}$$

Доказательство. Предположим, что

$$S(n,k) \supset \bigcup_{j=1}^{n} S_j(n,k). \tag{1.20}$$

Тогда существует такое решение $(\gamma_1,\ldots,\gamma_n) \in S(n,k)$, что $\gamma_j \neq 0$ для всех $j = 1,\ldots,n$. При этом

$$|\gamma_1 + \ldots + \gamma_n| \leq n \cdot \max_{j=1,\ldots,n} |\gamma_j|$$

и

$$|k \cdot \gamma_1 \cdot \ldots \cdot \gamma_n| \geq |k| \cdot \max_{j=1,\ldots,n} |\gamma_i| > n \cdot \max_{j=1,\ldots,n} |\gamma_i|.$$

Отсюда вытекает, что

$$|\gamma_1 + \ldots + \gamma_n| \neq |k \cdot \gamma_1 \cdot \ldots \cdot \gamma_n|$$

и, следовательно,

$$\gamma_1 + \ldots + \gamma_n \neq k \cdot \gamma_1 \cdot \ldots \cdot \gamma_n,$$

т.е. $(\gamma_1,\ldots,\gamma_n) \notin S(n,k)$. Получено противоречие. Следовательно, включение (1.20) ложное, т.е. истинна формула

$$S(n,k) \not\supset \bigcup_{j=1}^{n} S_j(n,k). \tag{1.21}$$

Из (1.18) и (1.21) вытекает, что равенство (1.19) − истинное.

Теорема доказана.

Теорема 1.6. Пусть $n \geq 3$ и $|k| \leq n \ \ (k \in \mathbf{Z})$. Если

$$\begin{cases} n+k \equiv 0 \,(\mathrm{mod}\, 2) \\ n-k \equiv 0 \,(\mathrm{mod}\, 4) \end{cases}, \tag{1.22}$$

или

$$\begin{cases} n-k \equiv 0 \,(\mathrm{mod}\, 2) \\ n+k \equiv 2 \,(\mathrm{mod}\, 4) \end{cases}, \tag{1.23}$$

то

$$S(n,k) \supset \bigcup_{j=1}^{n} S_j(n,k). \tag{1.24}$$

Доказательство. Пусть

$$\mathbf{a} = (\underbrace{1,\ldots,1}_{u \text{ раз}}, \underbrace{-1,\ldots,-1}_{v \text{ раз}}), \tag{1.25}$$

где

$$u+v=n \ \ (u,v \in \mathbf{Z}_+).$$

Подставив (1.25) в уравнение (1.13), получим

$$u-v=k\cdot(-1)^v.$$

Таким образом, $\mathbf{a} \in S(n,k)$ тогда и только тогда, когда

$$\begin{cases} u+v=n \\ u-v=k \\ v \equiv 0 \,(\mathrm{mod}\, 2) \\ u,v \in \mathbf{Z}_+ \end{cases} \Leftrightarrow \begin{cases} u=0.5\cdot(n+k) \\ v=0.5\cdot(n-k) \\ v \equiv 0 \,(\mathrm{mod}\, 2) \\ u,v \in \mathbf{Z}_+ \end{cases} \Leftrightarrow \begin{cases} n+k \equiv 0 \,(\mathrm{mod}\, 2) \\ n-k \equiv 0 \,(\mathrm{mod}\, 4) \end{cases},$$

или

$$\begin{cases} u+v=n \\ u-v=-k \\ v \equiv 1 \,(\mathrm{mod}\, 2) \\ u,v \in \mathbf{Z}_+ \end{cases} \Leftrightarrow \begin{cases} u=0.5\cdot(n-k) \\ v=0.5\cdot(n+k) \\ v \equiv 1 \,(\mathrm{mod}\, 2) \\ u,v \in \mathbf{Z}_+ \end{cases} \Leftrightarrow \begin{cases} n+k \equiv 2 \,(\mathrm{mod}\, 4) \\ n-k \equiv 0 \,(\mathrm{mod}\, 2) \end{cases}.$$

Итак, $\mathbf{a} \in S(n,k)$ тогда и только тогда, когда истинно (1.22) или (1.23). А так как

$$\mathbf{a} \notin \bigcup_{j=1}^{n} S_j(n,k),$$

то включение (1.24) − истинное.

Теорема доказана.

Полученные результаты дают возможность получить достаточно полное представление о структуре множества $S(n,k) \ \ (k \in \mathbf{Z}, n \in \mathbf{N})$.

В то же время остается открытым вопрос: что имеет место − равенство (1.19) или включение (1.24) в случае, когда $n \geq 3$, $|k| \leq n \ \ (k \in \mathbf{Z})$ и $n+k \equiv 1 \,(\mathrm{mod}\, 2)$?

Рассмотрим теперь кратко основные понятия и определения современной алгебры, используемые в последующих разделах (см., напр., [16,97,104,112,218]).

Бинарной операцией, определенной на множестве X, называется любое отображение $\circ : X \times X \to X$. Результат применения операции $\circ$ к элементам $x, y \in X$ обозначается через $x \circ y$. Бинарная операция $\circ$ называется:

1) *ассоциативной операцией*, если

$$(x \circ y) \circ z = x \circ (y \circ z) \quad (x, y, z \in X);$$

2) *коммутативной операцией*, если

$$x \circ y = y \circ x \quad (x, y \in X).$$

Полугруппой называется такая алгебраическая система $\mathsf{X} = (X, \circ)$, что $\circ$ – ассоциативная операция. Полугруппа $\mathsf{X} = (X, \circ)$ называется *коммутативной полугруппой*, если $\circ$ – коммутативная операция.

Полугруппы $\mathsf{X} = (X, \circ_{\mathsf{X}})$ и $\mathsf{Y} = (Y, \circ_{\mathsf{Y}})$ называются *изоморфными*, если существует такая биекция $f : X \to Y$, что $f(x_1 \circ_{\mathsf{X}} x_2) = f(x_1) \circ_{\mathsf{Y}} f(x_2)$ для всех $x_1, x_2 \in X$. Само отображение f называется *изоморфизмом* полугрупп X и Y.

Полугруппа $\mathsf{Y} = (Y, \circ_{\mathsf{Y}})$ называется *гомоморфным образом* полугруппы $\mathsf{X} = (X, \circ_{\mathsf{X}})$, если существует такая сюръекция $f : X \to Y$, что $f(x_1 \circ_{\mathsf{X}} x_2) = f(x_1) \circ_{\mathsf{Y}} f(x_2)$ для всех $x_1, x_2 \in X$. Само отображение f называется *гомоморфизмом* полугруппы X на полугруппу Y.

Для алгебраической системы $\mathsf{X} = (X, \circ)$ ($\circ$ − бинарная операция) элемент $e_л \in X$ называется *левым нейтральным элементом*, если $e_л \circ x = x$ для всех $x \in X$, а элемент $e_п \in X$ называется *правым нейтральным элементом*, если $x \circ e_п = x$ для всех $x \in X$. Если в алгебраической системе $\mathsf{X} = (X, \circ)$ существуют и левый, и правый нейтральные элементы, то они совпадают между собой. В этом случае говорят, что в алгебраической системе $\mathsf{X} = (X, \circ)$ существует *нейтральный элемент*.

Итак, $e \in X$ – нейтральный элемент алгебраической системы $\mathsf{X} = (X, \circ)$ тогда и только тогда, когда для всех $x \in X$

$$e \circ x = x \circ e = x.$$

В любой алгебраической системе $\mathsf{X} = (X, \circ)$ может существовать не более одного нейтрального элемента.

Нейтральный элемент алгебраической системы $\mathsf{X} = (X, \circ)$ часто называется *единицей*, а, в случае, когда операция обозначается тем или иным вариантом знака «плюс» – *нулем*. В последнем случае говорят, что используется *аддитивная запись*.

Полугруппа, в которой существует нейтральный элемент, называется *моноидом* (или *полугруппой с единицей*).

В моноиде $\mathsf{X} = (X, \circ)$ элемент $x \in X$ называется (через e обозначен нейтральный элемент моноида X):

1) *обратимым слева*, если существует такой элемент $x_л^{-1} \in X$, что

$$x_л^{-1} \circ x = e;$$

2) *обратимым справа*, если существует такой элемент $x_п^{-1} \in X$, что

$$x \circ x_п^{-1} = e.$$

Элементы $x_л^{-1}$ и $x_п^{-1}$ называются, соответственно, *левым* и *правым обратными элементами* для элемента x. Если в моноиде $\mathsf{X} = (X, \circ)$ для элемента $x \in X$ существуют левый обратный элемент $x_л^{-1} \in X$ и правый обратный элемент $x_п^{-1} \in X$, то они совпадают, т.е. $x_л^{-1} = x_п^{-1}$. В этом случае говорят, что в моноиде $\mathsf{X} = (X, \circ)$ для элемента $x \in X$ существует *обратный элемент*.

Итак, $x^{-1} \in X$ – обратный элемент для элемента $x \in X$ в моноиде $\mathsf{X} = (X, \circ)$ тогда и только тогда, когда

$$x^{-1} \circ x = x \circ x^{-1} = x.$$

В любом моноиде $\mathsf{X} = (X, \circ)$ для каждого элемента $x \in X$ может существовать не более одного обратного элемента.

В случае, когда обозначения операции используется аддитивная запись, вместо словосочетания *обратный элемент* используется словосочетание *противоположный элемент*.

Группой называется моноид $\mathsf{G} = (G, \circ)$, в котором для каждого элемента $g \in G$ существует обратный элемент $g^{-1} \in G$. Группа G называется *коммутативной* (или *абелевой*) *группой*, если $\circ$ – коммутативная операция. Для абелевых групп, обычно, используется аддитивная запись.

Группа $\mathsf{G} = (G, \circ)$ называется *конечной группой*, если G – конечное множество и *бесконечной группой*, если G – бесконечное множество. В том случае, когда $|G| = n$, говорят, что G – группа *порядка* n.

Конечную группу $\mathsf{G} = (G, \circ)$ можно задать *таблицей Кэли*, т.е. квадратной таблицей, строки и столбцы которой занумерованы элементами множества G, а в клетке расположенной на пересечении строки g_1 и столбца g_2, записан элемент $g_1 \circ g_2$.

Группы $\mathsf{G} = (G, \circ_{\mathsf{G}})$ и $\mathsf{H} = (H, \circ_{\mathsf{H}})$ называются *изоморфными*, если существует такая биекция $f : G \to H$, что $f(g_1 \circ_{\mathsf{G}} g_2) = f(g_1) \circ_{\mathsf{H}} f(g_2)$ для всех $g_1, g_2 \in G$. Само отображение f называется *изоморфизмом* групп G и H. При изоморфизме f:

1) нейтральный элемент e_{G} группы G переходит в нейтральный элемент e_{H} группы H;

2) элемент g^{-1}, обратный элементу g в группе G, переходит в элемент $(f(g))^{-1}$, обратный элементу $f(g)$ в группе H.

Группа $\mathsf{H}=(H,\circ)$ называется *подгруппой* группы $\mathsf{G}=(G,\circ)$, если $H\subseteq G$. Запись $\mathsf{H}\le\mathsf{G}$ означает утверждение «H – подгруппа группы G».

Если $H=\{e\}$ или $H=G$, то $\mathsf{H}=(H,\circ)$ – *несобственная* подгруппа группы $\mathsf{G}=(G,\circ)$. В остальных случаях $\mathsf{H}=(H,\circ)$ – *собственная* подгруппа группы $\mathsf{G}=(G,\circ)$.

Подстановкой на множестве X называется любая биекция $F: X\to X$. Множество $\mathsf{S}(X)$ всех подстановок на множестве X, вместе с операцией их суперпозиции является группой. В том случае, когда $X=\{1,\ldots,n\}$ эта группа называется симметрической группой и обозначается $\mathsf{S}(n)$.

Для конечных групп симметрическая группа $\mathsf{S}(n)$ играет исключительную роль, которая характеризуется следующим образом.

Теорема 1.7 (*Теорема Кэли*). Любая конечная группа $\mathsf{G}=(G,\circ)$ изоморфна подгруппе группы $\mathsf{S}(n)$ при подходящем выборе числа n.

Таким образом, симметрическая группа $\mathsf{S}(n)$ $(n\in\mathbf{N})$ обеспечивает унифицированное представление конечных групп.

Пусть $\mathsf{H}=(H,\circ)$ – подгруппа группы $\mathsf{G}=(G,\circ)$. Для любого элемента $g\in G$ множество

$$g\circ H=\{g\circ h\mid h\in H\}$$

называется *левым смежным классом группы* G *по подгруппе* H, а множество

$$H\circ g=\{h\circ g\mid h\in H\}$$

называется *правым смежным классом группы* G *по подгруппе* H. При этом

$$\pi^{л}_{\mathsf{H}}=\{g\circ H\mid g\in G\}$$

и

$$\pi^{п}_{\mathsf{H}}=\{g\circ H\mid g\in G\}$$

являются разбиениями множества G, т.е. любые два левых (соответственно, правых) смежных класса либо не пересекаются, либо совпадают.

Если G − конечная группа, то разбиения $\pi^{л}_{\mathsf{H}}$ и $\pi^{п}_{\mathsf{H}}$ содержат одно и то же число блоков. Это число блоков называется *индексом* подгруппы H в группе G. Имеет место

Теорема 1.8 (*теорема Лагранжа*). Порядок и индекс любой подгруппы H конечной группы G являются делителями порядка группы G.

Подгруппа $\mathsf{H}=(H,\circ)$ группы $\mathsf{G}=(G,\circ)$ называется *нормальной подгруппой*, если $g\circ H=H\circ g$ для любого элемента $g\in G$. Запись $\mathsf{H}\lhd\mathsf{G}$ означает утверждение «H − нормальная подгруппа группы G».

Если $\mathsf{H} \lhd \mathsf{G}$, то множество $\{g \circ H \mid g \in G\}$ называется множеством смежных классов группы G по подгруппе H. Это множество является группой, если операцию $*$ композиции смежных классов определить равенством

$$(g_1 \circ H) * (g_2 \circ H) = (g_1 \circ g_2) \circ H .$$

Такая группа называется *фактор-группой* группы G по подгруппе H и обозначается G/H.

Группа $\mathsf{H} = (H, \circ_{\mathsf{H}})$ – *гомоморфный образ* группы $\mathsf{G} = (G, \circ_{\mathsf{G}})$, если существует такая сюръекция $f : G \to H$, что $f(g_1 \circ_{\mathsf{G}} g_2) = f(g_1) \circ_{\mathsf{H}} f(g_2)$ для всех $g_1, g_2 \in G$. Само отображение f называется *гомоморфизмом* группы G на группу H.

Известно, что существует следующая связь между гомоморфизмами групп и нормальными подгруппами (через e_{H} обозначен нейтральный элемент группы H).

Теорема 1.9. Сюръекция $f : G \to H$ является гомоморфизмом группы $\mathsf{G} = (G, \circ_{\mathsf{G}})$ на группу $\mathsf{H} = (H, \circ_{\mathsf{H}})$ тогда и только тогда, когда $(f^{-1}(e_{\mathsf{H}}), \circ_{\mathsf{G}})$ – нормальная подгруппа группы G.

При этом множество $f^{-1}(e_{\mathsf{H}})$ называется *ядром гомоморфизма* f и обозначается $\ker f$.

В группе $\mathsf{G} = (G, \circ)$ для любого элемента $g \in G$ полагают

$$g^0 = e,$$

а также для всех $n \in \mathbf{N}$

$$g^n = \underbrace{g \circ \ldots \circ g}_{n \text{ раз}}$$

и

$$g^{-n} = (g^{-1})^n .$$

Циклической подгруппой группы G, порожденной элементом $g \in G$, называется группа $(\langle g \rangle, \circ)$, где $\langle g \rangle = \{g^l \mid l \in \mathbf{Z}\}$. Элемент g называется *образующим элементом* циклической группы $(\langle g \rangle, \circ)$. Говорят, что $g \in G$ − элемент *бесконечного порядка*, если $\langle g \rangle$ − бесконечное множество и $g \in G$ − элемент *порядка* n, если $|\langle g \rangle| = n$. В последнем случае n − это такое наименьшее натуральное число, что $g^n = e$.

Для циклических групп истинны следующие утверждения:

1) любая циклическая группа является абелевой группой;
2) каждая подгруппа циклической группы − циклическая группа;
3) в циклической группе $(\langle g \rangle, \circ)$ порядка n элемент g^k порождает подгруппу порядка $(n,k)^{-1} \cdot n$, где (n,k) — НОД чисел n и k;

4) в циклической группе $(\langle g\rangle,\circ)$ порядка n для каждого делителя d числа n существует единственная подгруппа порядка d и единственная подгруппа индекса d;

5) в циклической группе порядка n для каждого делителя d числа n существует в точности $\varphi(d)$ элементов порядка d;

6) в циклической группе порядка n существует в точности $\varphi(n)$ образующих элементов.

Группы подстановок, определенных на множестве X естественно приводят к *функциональным уравнениям*. Высокая сложность решения таких уравнений делает весьма привлекательным их применение при решении задач защиты информации.

Проиллюстрируем некоторые особенности решения функциональных уравнений на основе метода подстановок, развитого в [304].

Пример 1.5. Рассмотрим функциональное уравнение

$$\sum_{i=0}^{r} a_i(x_1,\ldots,x_n)\cdot f(f_{i1}(x_1),\ldots,f_{in}(x_n)) = b(x_1,\ldots,x_n), \tag{1.26}$$

где $b, a_i, f_{i1},\ldots,f_{in}$ $(i=0,1,\ldots,r)$ – заданные функции.

Всюду в дальнейшем предполагается, что

$$\{f_{ij} \mid i=0,1,\ldots,r\} \subseteq G_j \quad (j=1,\ldots,n),$$

где $\mathsf{G}_j = (G_j,\circ)$ $(j=1,\ldots,n)$ – конечная группа преобразований такого множества X, что

$$\varnothing \neq X^n \subseteq Dom\, b \cap \left(\bigcap_{i=0}^{r} Dom\, a_i\right) \subseteq \mathbf{R}^n,$$

а операция композиции $\circ$ – это операция суперпозиции функций, т.е. элемент $\alpha\circ\beta \in G_j$ $(\alpha,\beta\in G_j)$ определяется равенством

$$(\alpha\circ\beta)(x) = \alpha(\beta(x)) \quad (x\in X).$$

Положим

$$\mathsf{G} = \mathsf{G}_1\times\ldots\times\mathsf{G}_n = (G,\circ).$$

Уравнение, полученное из (1.26) в результате подстановки вместо переменных $x_1,\ldots,x_n$ соответственно функций $\gamma_1(x_1),\ldots,\gamma_n(x_n)$ $((\gamma_1,\ldots,\gamma_n)\in G)$ назовем *композицией уравнения* (1.26) *с элементом* $(\gamma_1,\ldots,\gamma_n)$ *группы* G.

Построим композиции уравнения (1.26) с каждым элементом группы G. Получим систему из

$$m = \prod_{j=1}^{n} |G_j|$$

алгебраических уравнений

$$\begin{aligned}\sum_{i=0}^{r} a_i(\gamma_1(x_1),\ldots,\gamma_n(x_n))\cdot f(f_{i1}(\gamma_1(x_1)),\ldots,f_{in}(\gamma_n(x_n))) = \\ = b(\gamma_1(x_1),\ldots,\gamma_n(x_n)) \quad ((\gamma_1,\ldots,\gamma_n)\in G).\end{aligned} \tag{1.27}$$

Перепишем систему (1.27) в виде

$$\sum_{j=1}^{m} c_{ij}(x_1,\ldots,x_n)\cdot f(\delta_{1ij}(x_1),\ldots,\delta_{nij}(x_n)) = d_i(x_1,\ldots,x_n) \quad (i=1,\ldots,m), \qquad (1.28)$$

где

$$\delta_{k1j} = \delta_{k2j} = \ldots = \delta_{kmj} \quad (k=1,\ldots,n;\ j=1,\ldots,m),$$

причем

$$\delta_{1i1} = \delta_{2i1} = \ldots = \delta_{mi1} = e \quad (i=1,\ldots,m),$$

а e – тождественное преобразование множества X.

Положим

$$\Delta(x_1,\ldots,x_n) = \begin{vmatrix} c_{11}(x_1,\ldots,x_n) & \ldots & c_{1m}(x_1,\ldots,x_n) \\ \vdots & \ddots & \vdots \\ c_{m1}(x_1,\ldots,x_n) & \ldots & c_{mm}(x_1,\ldots,x_n) \end{vmatrix}$$

и

$$\Delta_1(x_1,\ldots,x_n) = \begin{vmatrix} d_1(x_1,\ldots,x_n) & c_{12}(x_1,\ldots,x_n) & \ldots & c_{1m}(x_1,\ldots,x_n) \\ \vdots & \vdots & \ddots & \vdots \\ d_m(x_1,\ldots,x_n) & c_{m2}(x_1,\ldots,x_n) & \ldots & c_{mm}(x_1,\ldots,x_n) \end{vmatrix}.$$

Назовем систему (1.28):

1) *невырожденной*, если для всех $(x_1,\ldots,x_n)\in X^n$

$$\Delta(x_1,\ldots,x_n)\neq 0;$$

2) *несовместной*, если для всех $(x_1,\ldots,x_n)\in X^n$

$$\Delta(x_1,\ldots,x_n)\equiv 0$$

и

$$\Delta_1(x_1,\ldots,x_n)\neq 0.$$

Теорема 1.10. Если система (1.28) невырожденная, то на множестве X^n общее решение функционального уравнения (1.26) определяется формулой

$$f(x_1,\ldots,x_n) = \frac{\Delta_1(x_1,\ldots,x_n)}{\Delta(x_1,\ldots,x_n)}. \qquad (1.29)$$

Доказательство. Предположим, что система (1.28) невырожденная.

Тогда система (1.28) имеет единственное решение $f(x_1,\ldots,x_n)$, причем $f(x_1,\ldots,x_n)$ определяется формулой (1.29)

Подставим это решение в систему (1.28). Каждое уравнение превращается в тождество. Уравнение (1.26) является уравнением системы (1.28), так как оно соответствует композиции уравнения (1.26) с элементом $(\underbrace{e,\ldots,e}_{n\ раз})$ группы G.

Следовательно, решение системы (1.28) удовлетворяет уравнению (1.26).

Покажем, что уравнение (1.26) имеет единственное решение на множестве X^n. Предположим противное, т.е. что на множестве X^n уравнение (1.26) имеет, по крайней мере, два различных решения $f(x_1,\ldots,x_n)$ и $g(x_1,\ldots,x_n)$.

Подставим эти решения в уравнение (1.26). Получим тождества

$$\sum_{i=0}^{r} a_i(x_1,\ldots,x_n)\cdot f(f_{i1}(x_1),\ldots,f_{in}(x_n)) \equiv b(x_1,\ldots,x_n)$$

и

$$\sum_{i=0}^{r} a_i(x_1,\ldots,x_n)\cdot g(f_{i1}(x_1),\ldots,f_{in}(x_n)) \equiv b(x_1,\ldots,x_n).$$

Вычтем из 1-го тождества 2-е тождество. Получим тождество

$$\sum_{i=0}^{r} a_i(x_1,\ldots,x_n)\cdot (f(f_{i1}(x_1),\ldots,f_{in}(x_n)) - g(f_{i1}(x_1),\ldots,f_{in}(x_n))) \equiv 0$$

Построим композиции этого тождества с каждым элементом группы G. Получим систему, из m тождеств

$$\begin{aligned}\sum_{i=0}^{r} a_i(\gamma_1(x_1),\ldots,\gamma_n(x_n))\cdot (f(f_{i1}(\gamma_1(x_1)),\ldots,f_{in}(\gamma_n(x_n))) - \\ - g(f_{i1}(\gamma_1(x_1)),\ldots,f_{in}(\gamma_n(x_n)))) \equiv 0 \ \ ((\gamma_1,\ldots,\gamma_n)\in G).\end{aligned} \tag{1.30}$$

Система (1.30) имеет тот же определитель, что и система (1.28). Следовательно, система (1.30) невырожденная. А так как система (1.30) однородная, то

$$f(x_1,\ldots,x_n) \equiv g(x_1,\ldots,x_n) \ \ ((x_1,\ldots,x_n)\in X^n).$$

Получено противоречие. Следовательно, предположение − ложное, т.е. уравнение (1.26) имеет единственное решение на множестве X^n.

Теорема доказана.

Следствие 1.4. Если система (1.28) несовместная, то функциональное уравнение (1.26) на множестве X^n не имеет решений.

Доказательство. По своему построению, система (1.28) является следствием уравнения (1.26) на множестве X^n. Следовательно, на множестве X^n любое решение уравнения (1.26) является также и решением системы (1.28).

Следствие доказано.

Рассмотрим решение уравнения (1.26) для некоторых классических конечных групп преобразований $\mathsf{G}=(G,\circ)$ в случае, когда $n=1$, а коэффициенты при неизвестной функции − постоянные. В этом случае уравнение (1.27) имеет вид

$$a_0\cdot f(x)+a_1\cdot f(f_1(x))+\ldots+a_r\cdot f(f_r(x)) = b(x), \tag{1.31}$$

где $\{f_1,\ldots,f_r\}\subseteq G$.

Предположим, что в уравнении (1.31) функции $f_1,\ldots,f_r$ − последовательные элементы конечной циклической группы G преобразований множества X. Требование о том, что элементы группы − *последовательные* выбрано с целью упрощения изложения и не влияет на общность рассуждений.

Таким образом, считаем, что выполнены следующие три условия:

1) $f_j = \underbrace{\varphi\circ\ldots\circ\varphi}_{j\ раз}$ $(j=1,2,\ldots)$ для заданной функции φ;

2) $Val\,\varphi = Dom\,\varphi = X \subseteq Dom\,b \subseteq \mathbf{R}$;

3) существует такое $k\in\mathbf{N}$ $(k\ge r)$, что $f_{k+1}=e$ и $f_j\neq e$ для всех $j=1,\ldots,k$.

Для уравнения (1.31) система (1.28) имеет вид

$$\begin{cases} a_0 \cdot f(x) + a_1 \cdot f(f_1(x)) + \ldots + a_r \cdot f(f_r(x)) = b(x) \\ a_0 \cdot f(f_1(x)) + a_1 \cdot f(f_2(x)) + \ldots + a_r \cdot f(f_{r+1}(x)) = b(f_1(x)) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 \cdot f(f_{k-r}(x)) + a_1 \cdot f(f_{k-r+1}(x)) + \ldots + a_r \cdot f(f_k(x)) = b(f_{k-r}(x)) \\ a_0 \cdot f(f_{k-r+1}(x)) + a_1 \cdot f(f_{k-r+2}(x)) + \ldots + a_{r-1} \cdot f(f_k(x)) + \\ \qquad + a_r \cdot f(x) = b(f_{k-r+1}(x)) \\ a_0 \cdot f(f_{k-r+2}(x)) + a_1 \cdot f(f_{k-r+3}(x)) + \ldots + a_{r-1} \cdot f(x) + \\ \qquad + a_r \cdot f(f_1(x)) = b(f_{k-r+2}(x)) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 \cdot f(f_k(x)) + a_1 \cdot f(x) + \\ \qquad + a_2 \cdot f(f_1(x)) + \ldots + a_r \cdot f(f_{r-1}(x)) = b(f_k(x)). \end{cases} \tag{1.32}$$

При малых значениях r решения уравнения (1.32) могут быть найдены в явном виде для любых $k \in \mathbf{N}$.

Рассмотрим специальный случай, когда $r = 1$.

Теорема 1.11. Пусть в функциональном уравнении

$$a_0 \cdot f(x) + a_1 \cdot f(\varphi(x)) = b(x) \tag{1.33}$$

$\varphi(x)$ и $b(x)$ такие заданные функции, что $Val\,\varphi = Dom\,\varphi = X \subseteq Dom\,b$ и существует такое число k, что $\underbrace{\varphi \circ \ldots \circ \varphi}_{k+1\ раз} = e$ и $\underbrace{\varphi \circ \ldots \circ \varphi}_{j\ раз} \neq e$ $(j = 1, \ldots, k)$. Положим

$$F(x) = \sum_{i=0}^{k} (-1)^{k-i} a_0^i a_1^{k-i} b(f_{k-i}(x)),$$

где $f_j = \underbrace{\varphi \circ \ldots \circ \varphi}_{j\ раз}$ $(j = 01, \ldots)$. На множестве X уравнение (1.33):

1) не имеет решений, если функция $F(x)$ $(x \in X)$ не равна тождественно нулю и либо k чётное число и $a_0 = -a_1$, либо k нечётное число и $|a_0| = |a_1|$;

2) имеет общее решение, определяемое формулой

$$f(x) = \frac{F(x)}{a_0^{k+1} + (-1)^k \cdot a_1^{k+1}}, \tag{1.34}$$

если либо k чётное число и $a_0 \neq a_1$, либо k нечётное число и $|a_0| \neq |a_1|$.

Доказательство. Для уравнения (1.33) система (1.32) имеет следующий вид

$$\begin{cases} a_0 \cdot f(x) + a_1 \cdot f(f_1(x)) = b(x) \\ a_0 \cdot f(f_1(x)) + a_1 \cdot f(f_2(x)) = b(f_1(x)) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 \cdot f(f_{k-1}(x)) + a_1 \cdot f(f_k(x)) = b(f_{k-1}(x)) \\ a_0 \cdot f(f_k(x)) + a_1 \cdot f(x) = b(f_k(x)). \end{cases} \tag{1.35}$$

Непосредственными вычислениями находим, что для системы (1.35)

$$\Delta(x)=\begin{vmatrix} a_0 & a_1 & 0 & \dots & 0 & 0 \\ 0 & a_0 & a_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_0 & a_1 \\ a_1 & 0 & 0 & \dots & 0 & a_0 \end{vmatrix} = a_0^{k+1} + (-1)^k a_1^{k+1}$$

и

$$\Delta_1(x)=\begin{vmatrix} b(x) & a_1 & 0 & \dots & 0 & 0 \\ b(f_1(x)) & a_0 & a_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b(f_{k-1}(x)) & 0 & 0 & \dots & a_0 & a_1 \\ b(f_k(x)) & 0 & 0 & \dots & 0 & a_0 \end{vmatrix} = G(x).$$

Следовательно, $\Delta(x)=0$ тогда и только тогда, когда либо k чётное число и $a_0=-a_1$, либо k нечётное и $|a_0|=|a_1|$.

Пусть $\Delta(x)=0$, а функция $F(x)$ $(x\in X)$ не равна тождественно нулю. Тогда система (1.35) несовместная. В силу следствия 1.4 на множестве X уравнение (1.33) не имеет решений, что и требовалось доказать.

Пусть $\Delta(x)\neq 0$. Тогда либо k четное число и $a_0\neq a_1$, либо k нечетное число и $|a_0|\neq|a_1|$.

В этом случае система (1.35) невырожденная. Из теоремы 1.10 вытекает, что на множестве X общее решение уравнения (1.33) определяется формулой (1.29). Непосредственная подстановка в (1.29) значений $\Delta(x)$ и $\Delta_1(x)$ приводит к формуле (1.34), что и требовалось доказать.

Теорема доказана.

В теореме 1.11 ничего не сказано о решениях уравнения (1.33), если $F(x)\equiv 0$ $(x\in X)$ и либо k чётное число и $a_0=-a_1$, либо k нечётное число и $|a_0|=|a_1|$. Несложно показать, что в этом случае уравнение (1.33) может иметь существенно отличающиеся друг от друга решения, причем они не могут быть найдены из системы (1.35).

Предположим теперь, что в уравнении (1.31) функции $f_1,\dots,f_r$ являются порождающими элементами абелевой группы $\mathsf{G}=(G,\circ)$ преобразований множества X, в которой каждый элемент имеет порядок k.

Таким образом, считаем, что выполнены следующие условия:

1) $Dom\ f_i = Val\ f_i = X \subseteq Dom\, b$ $(i=1,\dots,r)$;

2) $f_i \circ f_j = f_j \circ f_i$ для всех $i,j=1,\dots,r$;

3) $\underbrace{f_i\circ\dots\circ f_i}_{k\text{ раз}} = e$ и $\underbrace{f_i\circ\dots\circ f_i}_{j\text{ раз}} \neq e$ $(j=1,\dots,k-1)$ для всех $i=1,\dots,r$;

4) $f_i \circ f_j \neq e$ $(i,j=1,\dots,r)$ при $i\neq j$.

Итак,

$$G = \{ f_{i_1}^{\alpha_1} \circ \ldots \circ f_{i_l}^{\alpha_l} \mid 1 \le i_1 < \ldots < i_l \le r \ (l = 0,1,\ldots,r); \\ \alpha_j = 0,1,\ldots,k-1 \ (j = 1,\ldots,l) \}.$$

Ясно, что группа $\mathsf{G} = (G,\circ)$ изоморфна *элементарной абелевой группе* порядка k^r. Последняя определяется равенством

$$\mathsf{Z}_{k^r} = \underbrace{\mathsf{Z}_k \times \ldots \times \mathsf{Z}_k}_{r \text{ раз}},$$

где в циклической группе $\mathsf{Z}_k = (\mathbf{Z}_k, \oplus)$ порядка k операция $\oplus$ определена равенством

$$a \oplus b = a + b \pmod{k} \quad (a,b \in \mathbf{Z}_k).$$

Изоморфизм между группами G и Z_{k^r} устанавливается формулой

$$f_{i_1}^{\alpha_1} \circ \ldots \circ f_{i_l}^{\alpha_l} \leftrightarrow (\beta_1,\ldots,\beta_r),$$

где

$$\beta_j = \begin{cases} \alpha_m, \text{ если } j = i_m \ (m = 1,\ldots,l) \\ 0, \text{ если } j \in \{1,\ldots,r\} \setminus \{i_1,\ldots,i_l\} \end{cases}.$$

Для уравнения (1.31) система (1.28) состоит из k^r уравнений. При малых значениях k и r решения уравнения (1.31) могут быть найдены в явном виде.

Рассмотрим специальный случай, когда $k = r = 2$.

Теорема 1.12. Пусть в функциональном уравнении

$$a_0 \cdot f(x) + a_1 \cdot f(f_1(x)) + a_2 \cdot f(f_2(x)) = b(x) \qquad (1.36)$$

заданные функции $f_1(x)$, $f_2(x)$ и $b(x)$ удовлетворяют следующим трем условиям:

1) $Dom\ f_i = Val\ f_i = X \subseteq Dom\ b \ (i = 1,2)$;

2) $f_1 \circ f_2 = f_2 \circ f_1 \ne e$;

3) $f_i \circ f_i = e \ (i = 1,2)$.

Положим

$$A = a_0^4 + a_1^4 + a_2^4 - 2a_0^2a_1^2 - 2a_0^2a_2^2 - 2a_1^2a_2^2,$$

$$H(x) = (a_0^3 - a_0 \cdot a_1^2 - a_0 \cdot a_2^2) \cdot b(x) + (a_1^3 - a_0^2 \cdot a_1 - a_1 \cdot a_2^2) \cdot f(f_1(x)) + \\ + (a_2^3 - a_0^2 \cdot a_2 - a_1^2 \cdot a_2) \cdot b(f_2(x)) + 2 \cdot a_0 \cdot a_1 \cdot a_2 \cdot b(f_{12}(x)),$$

где $f_{12} = f_1 \circ f_2$. На множестве X уравнение (1.36):

1) не имеет решений, если $A = 0$ и функция $H(x)$ $(x \in X)$ не равна тождественно нулю;

2) имеет общее решение, определяемое формулой

$$f(x) = \frac{H(x)}{A}, \qquad (1.37)$$

если $A \ne 0$.

Доказательство. Для уравнения (1.36) система (1.28) имеет следующий вид

$$\begin{cases} a_0 f(x) + a_1 f(f_1(x)) + a_2 f(f_2(x)) = b(x) \\ a_1 f(x) + a_0 f(f_1(x)) + a_2 f(f_{12}(x)) = b(f_1(x)) \\ a_2 f(x) + a_0 f(f_2(x)) + a_1 f(f_{12}(x)) = b(f_2(x)) \\ a_2 f(f_1(x)) + a_1 f(f_2(x)) + a_0 f(f_{12}(x)) = b(f_{12}(x)). \end{cases} \tag{1.38}$$

Непосредственными вычислениями находим, что для системы (1.38)

$$\Delta(x) = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ a_1 & a_0 & 0 & a_2 \\ a_2 & 0 & a_0 & a_1 \\ 0 & a_2 & a_1 & a_0 \end{vmatrix} = A$$

и

$$\Delta_1(x) = \begin{vmatrix} b(x) & a_1 & a_2 & 0 \\ b(f_1(x)) & a_0 & 0 & a_2 \\ b(f_2(x)) & 0 & a_0 & a_1 \\ b(f_{12}(x)) & a_2 & a_1 & a_0 \end{vmatrix} = H(x).$$

Пусть $A = 0$ и функция $H(x)$ $(x \in X)$ не равна тождественно нулю. Тогда система (1.38) несовместная. В силу следствия 1.4, на множестве X уравнение (1.36) не имеет решений, что и требовалось доказать.

Пусть $A \neq 0$. В этом случае система (1.38) невырожденная. Из теоремы 1.10 вытекает, что на множестве X общее решение уравнения (1.36) определяется формулой (1.29). Непосредственная подстановка в (1.29) значений $\Delta(x)$ и $\Delta_1(x)$ приводит к формуле (1.37), что и требовалось доказать.

Теорема доказана.

Итак, показано, что сведение функционального уравнения (1.26) к системе (1.28) дает возможность эффективно найти его общее решение в случаях, когда система (1.28) невырожденная или несовместная.

Расчетные формулы облегчают вычисление общих решений для конкретных типов уравнений и специальных групп преобразований.

Часто возникает необходимость рассматривать множество X, на котором определены две бинарные операции, связанные друг с другом теми или иными соотношениями (аксиомами).

Кольцом называется такая алгебраическая система

$$\mathsf{K} = (X, \Diamond, \circ),$$

что $(X, \Diamond)$ – абелева группа, $(X, \circ)$ – полугруппа, а операции $\Diamond$ и $\circ$ связаны дистрибутивными законами:

$$(x_1 \Diamond x_2) \circ x_3 = (x_1 \circ x_3) \Diamond (x_1 \circ x_3),$$

$$x_3 \circ (x_1 \Diamond x_2) = (x_3 \circ x_1) \Diamond (x_3 \circ x_2).$$

Группа $(X,\lozenge)$ называется *аддитивной группой* кольца K, а полугруппа $(X,\circ)$ – *мультипликативной полугруппой* кольца K. В соответствии с этой терминологией операция $\circ$ имеет более высокий приоритет, чем операция $\lozenge$. Поэтому законы дистрибутивности записываются в виде

$$(x_1 \lozenge x_2) \circ x_3 = x_1 \circ x_3 \lozenge x_1 \circ x_3,$$
$$x_3 \circ (x_1 \lozenge x_2) = x_3 \circ x_1 \lozenge x_3 \circ x_2.$$

Для нейтрального элемента $e_\lozenge$ абелевой группы $(X,\lozenge)$ кольца K истинны равенства

$$e_\lozenge \circ x = x \circ e_\lozenge = e_\lozenge \quad (x \in X),$$

т.е. элемент $e_\lozenge$ кольца K играет ту же роль, что и число 0 при умножении чисел. Поэтому нейтральный элемент $e_\lozenge$ абелевой группы $(X,\lozenge)$ называется *нулем* кольца K.

В том случае, когда мультипликативная полугруппа $(X,\circ)$ кольца $\mathsf{K} = (X,\lozenge,\circ)$ – моноид, для нейтрального элемента $e_\circ$ моноида $(X,\circ)$ истинны равенства

$$e_\circ \circ x = x \circ e_\circ = x \quad (x \in X),$$

т.е. элемент $e_\circ$ кольца K играет ту же роль, что и число 1 при умножении чисел. Поэтому нейтральный элемент $e_\circ$ называется *единицей*, а кольцо K – *кольцом с единицей*. В таком кольце циклическая подгруппа аддитивной группы, порожденная элементом $e_\circ$, изоморфна либо группе $(\mathbf{Z},+)$, либо группе $(\mathbf{Z}_m,\oplus)$ (где $a \oplus b = a + b \pmod m$ для всех $a,b \in \mathbf{Z}_m$) при некотором значении $m \in \mathbf{N}$. В первом случае говорят, что K – *кольцо характеристики нуль*, а во втором случае, что K – *кольцо характеристики* m.

Кольцо $\mathsf{L} = (Y,\lozenge,\circ)$ — *подкольцо* кольца $\mathsf{K} = (X,\lozenge,\circ)$, если $Y \subseteq X$.

Центром кольца $\mathsf{K} = (X,\lozenge,\circ)$ называется множество

$$cntr\ X = \{a \in X \mid a \circ x = x \circ a \ \textit{для всех}\ x \in X\}.$$

Для любого кольца $\mathsf{K} = (X,\lozenge,\circ)$ алгебраическая система $(cntr\ K,\lozenge,\circ)$ является подкольцом кольца K.

Если мультипликативная полугруппа $(X,\circ)$ кольца $\mathsf{K} = (X,\lozenge,\circ)$ – коммутативная полугруппа, то K называется *коммутативным кольцом*.

Элементы $a,b \in X \setminus \{e_\lozenge\}$ коммутативного кольца $\mathsf{K} = (X,\lozenge,\circ)$ называются *делителями нуля*, если

$$a \circ b = e_\lozenge.$$

Коммутативное кольцо с единицей, в котором отсутствуют делители нуля, называется *областью целостности*.

Пусть $\mathsf{K} = (X,\lozenge,\circ)$ – коммутативное кольцо с единицей. Элемент $x \in X$ называется *обратимым* элементом кольца K, если существует такой элемент $x^{-1} \in X$, что $x \circ x^{-1} = e_\circ$. Сам элемент x^{-1} называется *обратным* эле-

ментом для элемента x. Пусть X_{inv} – множество всех обратимых элементов кольца K. Тогда $(X_{inv},\circ)$ – группа. Эта группа называется *мультипликативной группой* кольца K.

Область целостности $\mathsf{K}=(X,\Diamond,\circ)$ называется *евклидовым кольцом*, если существует такое отображение $\nu: X\setminus\{e_\Diamond\}\to\mathbf{Z}_+$, называемое *нормой*, что:

1) $\nu(a\circ b)\geq\nu(a)$ для всех $a,b\in X\setminus\{e_\Diamond\}$;

2) для любых $a\in X$ и $b\in X\setminus\{e_\Diamond\}$ существуют такие элементы $q,r\in X$, что $a=b\circ q\Diamond r$, где либо $q=e_\Diamond$, либо $\nu(r)<\nu(b)$.

Известно, что в любом евклидовом кольце $\mathsf{K}=(X,\Diamond,\circ)$:

1) $\nu(a\circ b)=\nu(a)$ $(a,b\in X\setminus\{e_\Diamond\})$ тогда и только тогда, когда $b\in X^{inv}$;

2) $\nu(a)=\nu(e_\circ)$ $(a\in X\setminus\{e_\Diamond\})$ тогда и только тогда, когда $a\in X^{inv}$.

Отметим, что наличие нормы в евклидовом кольце дает возможность построить для него теории делимости, аналогичную теории делимости целых чисел.

Для любого числа $m\in\mathbf{N}$ евклидовым кольцом является алгебраическая система $\mathsf{Z}_m=(\mathbf{Z}_m,\oplus,\circ)$, где операции $\oplus$ и $\circ$ определены равенствами

$$a\oplus b=a+b\,(\mathrm{mod}\,m)$$

и

$$a\circ b=a\cdot b\,(\mathrm{mod}\,m)$$

для всех $a,b\in\mathbf{Z}_m$.

В кольце Z_m через Θ обозначается операция, обратная операции $\oplus$, т.е. $a\Theta b=c$ тогда и только тогда, когда $a=b\oplus c$.

Сложность решения уравнений над кольцом Z_m $(m\in\mathbf{N})$ совпадает со сложностью решения сравнений по модулю m, которая, как известно, является достаточно высокой. Это обстоятельство делает привлекательным применение колец Z_m $(m\in\mathbf{N})$ при решении задач защиты информации [154-163,175,179,182-187,189,204-206].

Кольца $\mathsf{K}_1=(X,\Diamond_{\mathsf{K}_1},\circ_{\mathsf{K}_1})$ и $\mathsf{K}_2=(Y,\Diamond_{\mathsf{K}_2},\circ_{\mathsf{K}_2})$ – называются *изоморфными*, если существует такая биекция $f: X\to Y$, что $f(x_1\Diamond_{\mathsf{K}_1}x_2)=f(x_1)\Diamond_{\mathsf{K}_2}f(x_2)$ и $f(x_1\circ_{\mathsf{K}_1}x_2)=f(x_1)\circ_{\mathsf{K}_2}f(x_2)$ для всех $x_1,x_2\in X$. Само отображение f называется *изоморфизмом* колец K_1 и K_2.

Содержательно изоморфизм двух колец означает, что изоморфны аддитивные группы колец, а также изоморфны мультипликативные полугруппы колец, причем эти изоморфизмы устанавливает одно и то же отображение f.

Идеалом кольца $\mathsf{K}=(X,\Diamond,\circ)$ называется такое его подкольцо $\mathsf{J}=(Y,\Diamond,\circ)$, что $x\circ y\in Y$ и $y\circ x\in Y$ для всех $x\in Y$ и $y\in X$. Так как $(X,\Diamond)$ − абелева группа, то $(Y,\Diamond)\lhd(X,\Diamond)$.

Рассмотрим фактор-группу

$$(X,\Diamond)/(Y,\Diamond)=(\{x\Diamond Y \mid x\in X\},\☺),$$

где операция ☺ сложения смежных классов определена равенством

$$(x_1\Diamond Y)\☺(x_2\Diamond Y)=(x_1\Diamond x_2)\Diamond Y \quad (x_1,x_2\in X).$$

Определим на множестве $\{x\Diamond Y \mid x\in X\}$ смежных классов операцию ☹ умножения равенством

$$(x_1\Diamond Y)\☹(x_2\Diamond Y)=(x_1\circ x_2)\Diamond Y \quad (x_1,x_2\in X).$$

В результате построено кольцо $(\{x\Diamond Y \mid x\in X\},\☺,\☹)$. Это кольцо называется фактор-кольцом кольца K по идеалу J и обозначается K/J. Элементы множества $\{x\Diamond Y \mid x\in X\}$ называются *классами вычетов* по модулю идеала J.

Идеал $\mathsf{J}=(Y,\Diamond,\circ)$ кольца $\mathsf{K}=(X,\Diamond,\circ)$ называется:

1) *простым идеалом*, если $x_1\circ x_2\in Y$ влечет, что $x_1\in Y$ или $x_2\in Y$;

2) *максимальным идеалом*, если он не содержится ни в каком большем идеале, за исключением самого кольца K;

3) *главным идеалом, порожденным элементом* $a\in X$, если

$$Y=\{a\circ x \mid x\in X\}.$$

Имеет место

Теорема 1.13. Фактор-кольцо K/J является областью целостности тогда и только тогда, когда J − простой идеал кольца K.

Отметим, что в коммутативном кольце с единицей каждый максимальный идеал является простым идеалом, а в евклидовом кольце каждый идеал является главным идеалом.

Кольцо $\mathsf{L}=(Y,\Diamond_{\mathsf{L}},\circ_{\mathsf{L}})$ – *гомоморфный образ* кольца $\mathsf{K}=(X,\Diamond_{\mathsf{K}},\circ_{\mathsf{K}})$, если существует такая сюръекция $f: X\to Y$, что $f(x_1\Diamond_{\mathsf{K}} x_2)=f(x_1)\Diamond_{\mathsf{L}} f(x_2)$ и $f(x_1\circ_{\mathsf{K}} x_2)=f(x_1)\circ_{\mathsf{L}} f(x_2)$ для всех $x,y\in X$. Само отображение f называется *гомоморфизмом* кольца K на кольцо L.

Существует следующая связь между гомоморфизмами колец и идеалами колец (через e_{L} обозначен нуль кольца L).

Теорема 1.14. Сюръекция $f: X\to L$ является гомоморфизмом кольца $\mathsf{K}=(X,\Diamond_{\mathsf{K}},\circ_{\mathsf{K}})$ на кольцо $\mathsf{L}=(Y,\Diamond_{\mathsf{L}},\circ_{\mathsf{L}})$ тогда и только тогда, когда $(f^{-1}(e_{\mathsf{L}}),\Diamond_{\mathsf{K}},\circ_{\mathsf{K}})$ − идеал кольца K.

Множество $f^{-1}(e_{\mathsf{L}})$ называется *ядром* гомоморфизма f и обозначается $Ker\ f$.

Таким образом, в теории колец идеалы играют ту же роль, что и нормальные группы в теории групп.

Абелева группа $\mathsf{G} = (G, \Diamond_{\mathsf{G}})$ для которой зафиксировано непустое множество Φ отображений множества G в себя называется Φ-*операторной группой,* если

$$\varphi(a \Diamond_{\mathsf{G}} b) = \varphi(a) \Diamond_{\mathsf{G}} \varphi(b)$$

для всех $\varphi \in \Phi$ и $a, b \in G$. Множество Φ называется *областью операторов*. Предположим, что область операторов – кольцо $\mathsf{K} = (X, \Diamond_{\mathsf{K}}, \circ_{\mathsf{K}})$. Тогда K-операторная группа G называется K-*модулем*, если равенства

$$(\alpha \Diamond_{\mathsf{K}} \beta)(a) = \alpha(a) \Diamond_{\mathsf{G}} \beta(a)$$

и

$$(\alpha \circ_{\mathsf{K}} \beta)(a) = \alpha(\beta(a))$$

истинны для всех $a \in G$ и $\alpha, \beta \in X$.

Говорят, что K-модуль G – *конечный,* если существуют такие элементы $g_1, \ldots g_l \in G$ (они называются *базисом*), что любой элемент $g \in G$ может быть представлен в виде

$$g = \lambda_1(g_1) \Diamond_{\mathsf{G}} \ldots \Diamond_{\mathsf{G}} \lambda_l(g_l)$$

при некоторых $\lambda_1, \ldots, \lambda_l \in X$.

Если в этом представлении операторы $\lambda_1, \ldots, \lambda_l \in X$ однозначно определяются элементом $g \in G$, то G называется *модулем линейных форм*.

Зафиксируем кольцо $\mathsf{Z}_m = (\mathbf{Z}_m, \oplus, \circ)$. Абелева группа $\mathsf{G} = (\mathbf{Z}_m^n, \oplus)$, где

$$(x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$$

для всех $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbf{Z}_m^n$ является Z_m-модулем, если действие оператора $a \in \mathbf{Z}_m$ на элемент $(x_1, \ldots, x_n) \in \mathbf{Z}_m^n$ определить равенством

$$a(x_1, \ldots, x_n) = (a \circ x_1, \ldots, a \circ x_n).$$

Более того, G является модулем линейных форм. Его базисом являются, например, элементы

$$\mathbf{e}_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, 1, \underbrace{0, \ldots, 0}_{n-i \text{ раз}}) \quad (i = 1, \ldots, n).$$

В дальнейшем вместо записи $a(x_1, \ldots, x_n)$ будем использовать запись $a \circ (x_1, \ldots, x_n)$.

Полем называется такое кольцо $\mathsf{K} = (X, \Diamond, \circ)$, что $(X \setminus \{e_\Diamond\}, \circ)$ – абелева группа. Имеет место

Теорема 1.15. Для любого коммутативного кольца K с единицей и для любого идеала K/J кольца K фактор-кольцо K/J является полем тогда и только тогда, когда K/J − максимальный идеал.

В дальнейшем рассматриваем только *конечные поля*, т.е. такие поля, что X – конечное множество. Эти поля называют *полями Галуа*.

Существует 2 типа полей Галуа: 1-й тип полей Галуа – это поля вида $\mathbf{GF}(p) = \mathsf{Z}_p$, где p – простое число, а 2-й тип полей Галуа – это поля, основанные на кольцах многочленов над полем $\mathbf{GF}(p)$.

Выясним структуру таких полей.

Многочленом от переменной x над полем $\mathbf{GF}(p)$ называется запись

$$f(x) = \bigoplus_{i=0}^{n} a_i \circ x^i \quad (n \in \mathbf{Z}_+),$$

где $a_i \in \mathbf{Z}_p$ $(i = 0,1,\ldots,n)$. Если $a_n \neq 0$, то $f(x)$ – *многочлен n-й степени*, а если $a_n = 1$, то $f(x)$ – *приведенный многочлен*.

Сумма и произведение многочленов

$$f(x) = \bigoplus_{i=0}^{n} a_i \circ x^i$$

и

$$g(x) = \bigoplus_{i=0}^{m} b_i \circ x^i$$

определяются равенствами

$$f(x) \oplus g(x) = \bigoplus_{i=0}^{\max\{n,m\}} (a_i \oplus b_i) \circ x^i$$

и

$$f(x) \circ g(x) = \bigoplus_{i=0}^{n+m} (\bigoplus_{j=0}^{i} a_j \circ b_{i-j}) \circ x^i,$$

где $a_k = 0$ при всех $k > n$ и $b_l = 0$ при всех $l > m$.

Множество всех многочленов от переменной x над полем $\mathbf{GF}(p)$ с определенными выше операциями сложения и умножения многочленов образует *кольцо*, которое обозначается $\mathbf{GF}(p)[x]$. Элементы этого кольца обладают многими свойствами, аналогичным свойствам многочленов с действительными коэффициентами. Рассмотрим кратко эти свойства.

Многочлен $g(x)$ − *делитель* многочлена (обозначается $g(x) \mid f(x)$), если существует такой многочлен $h(x)$, что

$$f(x) = g(x) \circ h(x).$$

Многочлен $f(x)$ – *неприводимый* многочлен, если

$$g(x) \mid f(x) \Rightarrow (\exists \alpha \in \mathbf{Z}_p)(g(x) = \alpha \circ f(x) \ \vee \ g(x) = \alpha).$$

Приведенный неприводимый многочлен называется *простым* многочленом.

Наибольшим общим делителем многочленов $f(x)$ и $g(x)$ (обозначается $(f(x), g(x))$) называется такой приведенный многочлен $h(x)$ наибольшей степени, что $h(x) \mid f(x)$ и $h(x) \mid g(x)$.

Вычисление многочлена $(f(x), g(x))$ можно осуществить с помощью *алгоритма Евклида* (отличающегося от обычного алгоритма Евклида только тем, что все действия выполняются в поле $\mathbf{GF}(p)$).

Суть алгоритма Евклида состоит в следующем.

Вначале из многочленов $f(x)$ и $g(x)$ выбирается тот, степень которого не меньше, чем степень другого. Выбранный многочлен делится на оставшийся многочлен. Если деление произошло без остатка, то делитель посредством умножения на соответствующий элемент поля $\mathbf{GF}(p)$ преобразуется в приведенный многочлен. Полученный многочлен и является $(f(x), g(x))$. Если же деление произошло с остатком, то делитель делится на остаток.

Эта процедура повторяется до тех пор, пока не произойдет деление без остатка. Последний отличный от нуля остаток посредством умножения на соответствующий элемент поля $\mathbf{GF}(p)$, преобразуется в приведенный многочлен.

Полученный многочлен и является $(f(x), g(x))$.

Многочлены $f(x)$ и $g(x)$ называются *взаимно простыми*, если

$$(f(x), g(x)) = 1.$$

Имеет место

Теорема 1.16. В кольце $\mathbf{GF}(p)[x]$ любой ненулевой многочлен $f(x)$ однозначно (с точностью до порядка следования сомножителей) раскладывается в произведение элемента поля $\mathbf{GF}(p)$ и простых многочленов.

Корнем многочлена $f(x)$ называется такой элемент $\alpha \in \mathbf{GF}(p)$, что

$$f(\alpha) = 0.$$

Имеет место

Теорема 1.17. В кольце $\mathbf{GF}(p)[x]$ элемент $\alpha \in \mathbf{GF}(p)$ является корнем многочлена $f(x)$ тогда и только тогда, когда $(x \Theta \alpha) \mid f(x)$.

Зафиксируем приведенный многочлен $h(x)$. Остаток $r(x)$ от деления многочлена $f(x)$ на многочлен $h(x)$ называется *вычетом многочлена* $f(x)$ *по модулю многочлена* $h(x)$. Запись

$$f(x) \equiv g(x) \pmod{h(x)}$$

означает, что многочлены $f(x)$ и $g(x)$ при делении на многочлен $h(x)$ дают один и тот же остаток.

Это отношение – эквивалентность на множестве всех многочленов над полем $\mathbf{GF}(p)$. Следовательно, оно определяет *разбиение* $\pi_{h(x)}$ множества всех многочленов над полем $\mathbf{GF}(p)$ *на классы вычетов по модулю* $h(x)$.

Обозначим через $[f(x)]_{h(x)}$ блок разбиения $\pi_{h(x)}$, содержащий многочлен $f(x)$.

Определим на блоках разбиения $\pi_{h(x)}$ операции сложения и умножения равенствами

$$[f(x)]_{h(x)} \oplus [g(x)]_{h(x)} = [f(x) \oplus g(x)]_{h(x)},$$
$$[f(x)]_{h(x)} \circ [g(x)]_{h(x)} = [f(x) \circ g(x)]_{h(x)}.$$

Несложно убедиться в том, что алгебраическая система $(\pi_{h(x)}, \oplus, \circ)$ является кольцом. Это кольцо называется *кольцом многочленов по модулю* $h(x)$ *над полем* $\mathbf{GF}(p)$ и обозначается $\mathbf{GF}(p)[x]/(h(x))$.

Имеет место

Теорема 1.18. Для любого простого числа p кольцо $\mathbf{GF}(p)[x]/(h(x))$ многочленов по модулю приведенного многочлена $h(x)$ является полем тогда и только тогда, когда $h(x)$ – простой многочлен.

Если $h(x)$ – простой многочлен степени n, то поле $\mathbf{GF}(p)[x]/(h(x))$ содержит в точности p^n элементов (так как в кольце $\mathbf{GF}(p)[x]$ существует именно столько различных многочленов степени не выше, чем $n-1$). По этой причине (принимая во внимание изоморфизм полей) поле $\mathbf{GF}(p)[x]/(h(x))$ кратко обозначается $\mathbf{GF}(p^n)$.

Итак, выделены поля Галуа вида $\mathbf{GF}(p)$ и вида $\mathbf{GF}(p^n)$, где p – простое число и $n \in \mathbf{N}$. Других (с точностью до изоморфизма) полей Галуа нет. Отметим, что $\mathbf{GF}(p)$ и $\mathbf{GF}(p^n)$ – это поля характеристики p.

Важное свойство полей Галуа устанавливает

Теорема 1.19. Группа ненулевых элементов любого поля Галуа по умножению является циклической группой.

Эта теорема обосновывает следующее понятие.

Элемент α поля Галуа $\mathbf{GF}(q)$, где

$$q \in \{p^n \mid p \text{ простое число и } n \in \mathbf{N}\}$$

называется *примитивным* элементом, если все элементы поля $\mathbf{GF}(q)$, за исключением нуля, могут быть представлены в виде степеней элемента α.

Значение примитивного элемента состоит в том, что *умножение* в поле Галуа $\mathbf{GF}(q)$ сводится к сложению по модулю q показателей степеней примитивного элемента.

Существуют полученные с помощью ЭВМ списки примитивных многочленов над полями Галуа. Эти списки приведены во многих книгах, в которых математическим аппаратом исследования являются конечные поля.

Зафиксируем поле $\mathbf{GF}(p)$ (где p – простое число). Пусть $f(x)$ − неприводимый многочлен степени n над полем $\mathbf{GF}(p)$. Поле $\mathbf{GF}(p^n)$ является наименьшим полем, в котором многочлен $f(x)$ раскладывается на линейные множители.

Это поле называется *полем разложения* многочлена $f(x)$.

В поле $\mathbf{GF}(p^n)$ n-элементное множество корней многочлена $f(x)$ имеет вид

$$S = \{\beta, \beta^p, \ldots, \beta^{p^{n-1}}\},$$

где β − произвольный корень многочлена $f(x)$ в поле $\mathbf{GF}(p^n)$. При этом все элементы множества S, рассматриваемые как элементы мультипликативной группы поля $\mathbf{GF}(p^n)$, имеют один и тот же порядок. Это число называется *порядком многочлена* $f(x)$ и представляет собой такое наименьшее число $l \in \mathbf{N}$, что $(x^l \Theta 1) \mid f(x)$.

Высокая сложность решения нелинейных систем многостепенных многопеременных уравнений над полем Галуа (эта задача является NP-полной уже в случае квадратных уравнений) делает привлекательным использование таких систем при разработке современных шифров.

В настоящее известны попытки применения методов решения нелинейных систем полиномиальных уравнений над полем Галуа в процессе криптоанализа симметричных блочных и поточных шифров [258-261]. Обзор таких методов содержится в [5].

Рассмотрим следующее применение полей Галуа к решению задач защиты информации.

Естественным обобщением l-разрядного регистра сдвига с линейной обратной связью над полем $\mathbf{GF}(2)$, рассмотренного в п.1.2 (см. рис. 1.13.а), является его аналог над полем Галуа $\mathbf{GF}(q)$, где

$$q \in \{p^n \mid p \text{ простое число и } n \in \mathbf{N}\}.$$

Реакция такой схемы − (бесконечная) последовательность

$$b_0, b_1, \ldots, b_i, \ldots$$

элементов поля $\mathbf{GF}(q)$, определяемая начальными условиями

$$b_i = a_i \quad (i = 0,1,\ldots l-1)$$

и рекуррентным выражением

$$b_{l+k} = \bigoplus_{j=1}^{l} \alpha_j \circ b_{l+k-j} \quad (k \in \mathbf{Z}_0). \tag{1.39}$$

Эта последовательность $b_0, b_1, \ldots, b_i, \ldots$ называется *линейной рекуррентой* l-го порядка над полем Галуа $\mathbf{GF}(q)$.

Положим

$$\mathbf{s}_k = (b_k, \ldots, b_{l+k-1}) \quad (k \in \mathbf{Z}_0).$$

Тогда (1.39) можно записать в следующем матричном виде

$$\mathbf{s}_{k+1} = \mathbf{s}_k \circ A \quad (k \in \mathbf{Z}_0), \tag{1.40}$$

где

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_1 \\ 1 & 0 & \dots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \alpha_l \end{pmatrix}.$$

Из (1.40) вытекает, что

$$\mathbf{s}_{k+1} = \mathbf{s}_0 \circ A^{k+1} \quad (k \in \mathbf{Z}_0), \tag{1.41}$$

Пусть A − невырожденная матрица (критерий для этого − условие $\alpha_1 \neq 0$). Тогда A − элемент конечной группы

$$\mathsf{GL}_l(\mathbf{GF}(q)) = (X_l, \circ),$$

где X_l − множество всех невырожденных $l \times l$-матриц над полем $\mathbf{GF}(q)$, а $\circ$ − операция умножения матриц.

Из (1.41) вытекает, что $\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \dots$ − периодическая последовательность, причем ее период не превосходит порядок элемента A группы $\mathsf{GL}_l(\mathbf{GF}(q))$.

Пусть Θ − операция в поле $\mathbf{GF}(q)$, обратная операции $\oplus$, а $E \in X_l$ − единичная матрица.

Характеристический многочлен

$$f(x) = \det(x \circ E \Theta A)$$

матрицы A имеет вид

$$f(x) = x^l \Theta \alpha_l \circ x^{l-1} \Theta \dots \Theta \alpha_2 \circ x^1 \Theta \alpha_1.$$

Истинны следующие утверждения:

1) характеристический многочлен $f(x)$ матрицы A является минимальным многочленом матрицы A;

2) если характеристический многочлен $f(x)$ матрицы A − неприводимый многочлен, то его порядок совпадает с порядком матрицы A, рассматриваемой как элемент группы $\mathsf{GL}_l(\mathbf{GF}(q))$;

3) если $\mathbf{s}_0 \neq \mathbf{0}$, то период линейной рекурренты с неприводимым характеристическим многочленом $f(x)$ равен порядку многочлена $f(x)$.

Эти утверждения представляют собой основу для построения и анализа генераторов псевдослучайных последовательностей при решении задач защиты информации (см., напр., [4,6,7,136,218,229,313]).

Отметим, что в последнее время уделяется большое внимание исследованию линейных и полилинейных рекуррент над конечными кольцами (см., напр., [211,212,278,279]).

1.5. Конечные автоматы.

В пп.1.2 и 1.3 было показано, что модели и методы теории конечных автоматов играют существенную роль в процессе решения задач защиты информации. Рассмотрим основные понятия и определения этой теории (см., напр., [30,31,98,208,265]), используемые в последующих разделах. Так как рассматриваются только конечные автоматы, то всюду в дальнейшем в словосочетании «конечный автомат» слово «конечный» будем опускать.

Автоматом называется система

$$M = (Q, X, Y, \delta, \lambda),$$

где Q, X и Y − непустые конечные множество *состояний*, *входной* и *выходной* алфавиты, а $\delta : Q \times X \to Q$ и $\lambda : Q \times X \to Y$ − функции *переходов* и *выходов*.

Если представляют интерес только переходы состояний, то автомат определяется как тройка объектов

$$M = (Q, X, \delta),$$

т.е. выходной алфавит и функция выходов опускаются.

Автомат $M = (Q, X, Y, \delta, \lambda)$ называется *автономным* автоматом, если $|X| = 1$. Отметим, что решения многих задач теории автоматов в предположении, что исследуемый автомат является автономным, существенно отличаются от решения этих же задач в предположении, что $|X| = 2$. В свою очередь, решения многих задач теории автоматов в предположении, что $|X| = 2$ существенно отличаются от решения этих же задач в предположении, что $|X| \geq 3$.

Обозначим через A^+ множество всех непустых слов в алфавите A, т.е. $A^+ = \bigcup_{i=1}^{\infty} A^i$, а через A^* − множество всех слов в алфавите A, включая и *пустое* слово Λ, т.е. $A^* = \{\Lambda\} \cup A^+$. Длина $d(w)$ слова $w \in A^*$ определяется следующим образом: $d(\Lambda) = 0$ и $d(w) = i$ для всех $w \in A^i$ $(i \in \mathbf{N})$.

Расширим функции переходов $\delta : Q \times X \to Q$ и выходов $\lambda : Q \times X \to Y$ автомата M до функций $\tilde{\delta} : Q \times X^* \to Q$ и $\tilde{\lambda} : Q \times X^* \to Y^*$ равенствами

$$\tilde{\delta}(q, \Lambda) = q, \quad \tilde{\lambda}(q, \Lambda) = \Lambda$$

и

$$\tilde{\delta}(q, wx) = \delta(\tilde{\delta}(q, w), x),$$
$$\tilde{\lambda}(q, wx) = \tilde{\lambda}(q, w)\lambda(\tilde{\delta}(q, w), x)$$

для всех $q \in Q$, $w \in X^*$ и $x \in X$.

Автомат $M = (Q, X, Y, \delta, \lambda)$ функционирует в дискретном времени, принимающем целые неотрицательные значения. Это функционирование

представляется с помощью рекуррентных соотношений. Рассмотрим существующие подходы к выбору таких соотношений.

В [208] предполагается, что:

1) рекуррентные соотношения, определяющие функционирование автомата Мили $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_t) \\ y_t=\lambda(q_t,x_t) \end{cases} \quad (t\in \mathbf{N});$$

2) рекуррентные соотношения, определяющие функционирование автомата Мура $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_t) \\ y_t=\lambda(q_{t+1}) \end{cases} \quad (t\in \mathbf{N});$$

3) рекуррентные соотношения, определяющие функционирование автомата с задержкой $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_t) \\ y_t=\lambda(q_t) \end{cases} \quad (t\in \mathbf{N}).$$

В [31] предполагается, что:

1) рекуррентные соотношения, определяющие функционирование автомата *первого рода* (автомата Мили) $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_{t+1}) \\ y_{t+1}=\lambda(q_t,x_{t+1}) \end{cases} \quad (t\in \mathbf{Z}_+);$$

2) рекуррентные соотношения, определяющие функционирование автомата *второго рода* $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_{t+1}) \\ y_{t+1}=\lambda(q_{t+1},x_{t+1}) \end{cases} \quad (t\in \mathbf{Z}_+);$$

3) рекуррентные соотношения, определяющие функционирование автомата Мура $M=(Q,X,Y,\delta,\lambda)$, имеют вид

$$\begin{cases} q_{t+1}=\delta(q_t,x_{t+1}) \\ y_{t+1}=\lambda(q_{t+1}) \end{cases} \quad (t\in \mathbf{Z}_+).$$

При исследовании автоматов в последующих разделах книги будем следовать именно подходу, предложенному в [31].

В [101,264,267] введено и исследовано понятие «*автомат без потери информации*» (БПИ-автомат). Автомат $M=(Q,X,Y,\delta,\lambda)$ называется:

1) БПИ-автоматом 1-го типа, если для всех $q\in Q$ и $w\in X^+$ пара $(q,\tilde{\lambda}(q,w))$ дает возможность идентифицировать входное слово w;

2) БПИ-автоматом 2-го типа, если для всех $q\in Q$ и $w\in X^+$ пара $(\tilde{\delta}(q,w),\tilde{\lambda}(q,w))$ дает возможность идентифицировать входное слово w.

Обобщением этих понятий являются БПИ-автоматы порядка n $(n \in \mathbf{N})$. Для них идентификация входного слова осуществляется с задержкой в n тактов. Эти автоматы определяются следующим образом.

Автомат $M = (Q, X, Y, \delta, \lambda)$ называется:

1) БПИ-автоматом 1-го типа порядка n $(n \in \mathbf{Z}_+)$, если для всех $q \in Q$, $x \in X$ и всех таких $w \in X^+$, что $d(w) = n$, пара $(q, \tilde{\lambda}(q, xw))$ дает возможность идентифицировать входной символ x;

2) БПИ-автоматом 2-го типа порядка n $(n \in \mathbf{Z}_+)$, если для всех $q \in Q$, $x \in X$ и всех таких $w \in X^+$, что $d(w) = n$, пара $(q, \tilde{\lambda}(q, wx))$ дает возможность идентифицировать входной символ x и состояние $\tilde{\delta}(q, w)$.

Ясно, что БПИ-автомат 1-го типа – это БПИ-автомат 1-го типа порядка 0, а БПИ-автомат 2-го типа – это БПИ-автомат 2-го типа порядка 0.

В [191,192] содержится исследование обобщения понятия «БПИ-автомат» на случай, когда входной и выходной алфавиты автомата являются декартовыми произведениями множеств, т.е. $X = \underset{i=1}{\overset{n}{\times}} X_i$ и $Y = \underset{j=1}{\overset{m}{\times}} Y_j$.

При использовании БПИ-автомата в качестве поточного шифра естественно возникает задача построения обратного автомата, осуществляющего расшифровку. В [101] эта задача решена для БПИ-автоматов порядка n $(n \in \mathbf{N})$. Доказано существование обратных автоматов, осуществляющих идентификацию входного слова с задержкой на n тактов. Предложены алгоритмы построения таких автоматов. Отметим, что обратный автомат, построенный в соответствии с таким алгоритмом, может иметь число состояний, существенно превышающее число состояний исходного автомата.

Пусть Q_0 $(\varnothing \neq Q_0 \subseteq Q)$ – множество *допустимых начальных состояний*, т.е. перед подачей входного слова автомат M находится в некотором состоянии $q \in Q_0$. Упорядоченная пара (M, Q_0) называется *слабоинициальным* автоматом. Если $|Q_0| = 1$, т.е. $Q_0 = \{q_0\}$ $(q_0 \in Q)$, то пишут просто (M, q_0) и говорят, что задан *инициальный* автомат.

Каждый инициальный автомат (M, q_0) реализует *ограниченно-детерминированную функцию* (о.-д. функцию) $f_{(M,q_0)} : X^* \to Y^*$, где

$$f_{(M,q_0)}(w) = \tilde{\delta}(q_0, w) \quad (w \in X^*).$$

Эта функция удовлетворяет следующим двум условиям:

1) отображение $f_{(M,q_0)}$ сохраняет *длины* слов, т.е. $d(w) = d(f_{(M,q_0)}(w))$ для любого входного слова $w \in X^*$;

2) отображение $f_{(M,q_0)}$ согласовано с начальными отрезками слов, т.е. если $w_1 = ww_2$ и $w_3 = ww_4$ $(w, w_2, w_4 \in X^*)$, то у выходных слов $f_{(M,q_0)}(w_1)$ и $f_{(M,q_0)}(w_3)$ совпадают начальные отрезки длины $d(w)$.

Предположим, что инициальный автомат (M, q_0) реализует обратимую о.-д. функцию $f_{(M,q_0)}$, т.е. $f_{(M,q_0)}$ – инъекция. Тогда отображение $f_{(M,q_0)}$ представляет собой поточный шифр, осуществляющий шифрование сообщения, представленного элементом свободной полугруппы X^*, в шифртекст, представленный элементом свободной полугруппы Y^*. Расшифровка сообщений осуществляется посредством любого такого отображения $g: Y^* \to X^*$, что $g|_{Val\, f_{(M,q_0)}} = f^{-1}_{(M,q_0)}$.

Такая интерпретация допускает следующие два обобщения:

1. Пусть для автомата $M = (Q, X, Y, \delta, \lambda)$ существует такое подмножество состояний Q_0 $(\varnothing \neq Q_0 \subseteq Q)$, что для всех $q_0 \in Q_0$ о.-д. функция $f_{(M,q_0)}$ – инъекция. В качестве поточного шифра может быть выбрано однопараметрическое семейство о.-д. функций $\{f_{(M,q_0)}\}_{q_0 \in Q_0}$.

При этом начальное состояние $q_0 \in Q_0$ – секретный сеансовый ключ.

2. Пусть однопараметрическое семейство автоматов

$$\mathsf{M} = \{M_i = (Q_i, X, Y, \delta_i, \lambda_i)\}_{i \in I}$$

удовлетворяет условию: для каждого $i \in I$ существует такое подмножество состояний $Q_0^{(i)}$ $(\varnothing \neq Q_0^{(i)} \subseteq Q^{(i)})$, что для всех $q_0^{(i)} \in Q_0^{(i)}$ о.-д. функция $f_{(M_i, q_0^{(i)})}$ – инъекция. В качестве поточного шифра может быть выбрано двухпараметрическое семейство о.-д. функций $\{f_{(M_i, q_0^{(i)})}\}_{i \in I, q_0^{(i)} \in Q_0^{(i)}}$.

При этом автомат M_i $(i \in I)$ – секретный ключом средней длительности, а начальное состояние $q_0^{(i)} \in Q_0^{(i)}$ – секретный сеансовый ключ.

Представление поточного шифра слабоинициальным автоматом (или семейством слабоинициальных автоматов) дает возможность формально охарактеризовать сложность и точность действий криптоаналитика посредством оценки числа прообразов выходной последовательности, которая может быть реализована автоматом. Исследованию этой задачи, как задачи теории автоматов, посвящены работы [67,119-122,149].

Пусть $M = (Q, X, Y, \delta, \lambda)$ $(|X| = |Y|)$ – такой автомат, что семейство о.-д. функций $\{f_{(M,q_0)}\}_{q_0 \in Q}$ состоит из инъекций. Тогда автомат M является БПИ-автоматом 1-го типа. Для построения обратного автомата M^{-1} достаточно в автоматном графе автомата M поменять местами входы и выходы. Это означает, что:

1) автоматы M и M^{-1} имеют одно и то же множество состояний Q;

2) при шифровании любого входного слова $w \in X^+$ инициальным автоматом (M, q_0), а также при расшифровке выходного слова $\tilde{\lambda}(q_0, w)$ автоматом (M^{-1}, q_0) оба автомата «движутся» по одной и той же траектории в пространстве состояний.

Зафиксируем автоматы $M_1 = (Q_1, X, Y, \delta_1, \lambda_1)$ и $M_2 = (Q_2, X, Y, \delta_2, \lambda_2)$.

Состояния $q_1 \in Q_1$ и $q_2 \in Q_2$ называются *эквивалентными*, если

$$f_{(M_1, q_1)}(w) = f_{(M_2, q_2)}(w)$$

для любого входного слова $w \in X^+$. Эквивалентные состояния $q_1, q_2 \in Q$ $(q_1 \neq q_2)$ автомата $M = (Q, X, Y, \delta, \lambda)$ называются *близнецами* [90], если

$$\delta(q_1, x) = \delta(q_2, x)$$

для всех $x \in X$.

Автоматы M_1 и M_2 — *эквивалентные*, если для каждого состояния $q_1 \in Q_1$ существует эквивалентное ему состояние $q_2 \in Q_2$, и для каждого состояния $q_2 \in Q_2$ существует эквивалентное ему состояние $q_1 \in Q_1$.

Выделяют следующие специальные случаи эквивалентных автоматов:

1) автоматы M_1 и M_2 называются *изоморфными*, если существует такая биекция $\varphi: Q_1 \to Q_2$, что q_1 и $\varphi(q_1)$ – эквивалентные состояния для всех $q_1 \in Q_1$, причем

$$\varphi(\delta_1(q_1, x)) = \delta_2(\varphi(q_1), x)$$

для всех $x \in X$;

2) автомат M_2 – *гомоморфный образ* автомата M_1, если существует такая сюръекция $\varphi: Q_1 \to Q_2$, что q_1 и $\varphi(q_1)$ – эквивалентные состояния для всех $q_1 \in Q_1$, причем

$$\varphi(\delta_1(q_1, x)) = \delta_2(\varphi(q_1), x)$$

для всех $x \in X$.

Автомат $M = (Q, X, Y, \delta, \lambda)$ называется *приведенным* автоматом, если любые два его различных состояния $q_1, q_2 \in Q$ не являются эквивалентными. Если автомат M не является приведенным, то существует такое нетривиальное отношение эквивалентности $\equiv$ на множестве состояний Q, что при переходе к фактор-множеству $Q/_{\equiv}$ получается автомат $M/_{\equiv}$, являющийся гомоморфным образом автомата M. При этом, если отношение эквивалентности $\equiv$ выбрано так, что $q_1 \equiv q_2$ $(q_1, q_2 \in Q)$ тогда и только тогда, когда q_1 и q_2 – эквивалентные состояния, то $M/_{\equiv}$ – приведенный автомат. Отсюда вытекает, что в любом множестве всех эквивалентных друг другу автоматов существует единственный (с точностью до обозначения состояний) приведенный автомат.

Проблемы, возникающие при экспериментальном анализе поведения автомата, исследуются в разделе теории автоматов, известном под именем *теория экспериментов с автоматами*. Впервые этот раздел систематически изложен в [30]. *Эксперимент* с автоматом состоит в подаче на автомат входных слов и анализе соответствующих реакций автомата. Многообразие экспериментов с автоматом определяется:

1) объектом идентификации, т.е. состояние слабоинициального автомата, автомат, принадлежащий заданному классу автоматов, обнаружение или локализация неисправностей в автомате и т.д.;

2) числом экземпляров (копий) автомата, используемых в процессе эксперимента, т.е. простой эксперимент, если используется единственный экземпляр автомата и кратный эксперимент, если используется не менее двух копий автомата;

3) способом исполнения эксперимента, т.е. безусловный эксперимент, если при каждой реализации эксперимента подаются одни и те же входные слова и адаптивный (или условный) эксперимент, если каждый входной символ, начиная со второго, формируется в зависимости от реакции на предыдущие символы.

В [30] показано, что большинство экспериментов с автоматами сводится к экспериментам по идентификации состояний автомата. При этом могут быть выделены следующие три основных типа экспериментов по идентификации состояний автомата:

1) *диагностический* эксперимент, т.е. эксперимент, предназначенный для идентификации начального состояния заданного слабоинициального автомата;

2) *установочный* эксперимент, т.е. эксперимент, предназначенный для идентификации финального состояния заданного слабоинициального автомата;

3) *синхронизирующий* эксперимент, т.е. эксперимент, предназначенный для перевода всех начальных состояний заданного слабоинициального автомата в одно и то же состояние.

Слова, подаваемые на автомат в процессе этих экспериментов, получили название, соответственно, *диагностические*, *установочные* и *синхронизирующие*. Формально эти слова определяются следующим образом.

Для заданного слабоинициального автомата (M, Q_0) $(|Q_0| \geq 2)$ входное слово $w \in X^+$ называется:

1) *диагностическим* словом, если

$$\tilde{\lambda}(q', w) = \tilde{\lambda}(q'', w) \Rightarrow q' = q''$$

для всех $q', q'' \in Q_0$;

2) *установочным* словом, если

$$\tilde{\lambda}(q', w) = \tilde{\lambda}(q'', w) \Rightarrow \tilde{\delta}(q', w) = \tilde{\delta}(q'', w)$$

для всех $q', q'' \in Q_0$;

3) *синхронизирующим* словом, если

$$\tilde{\delta}(q', w) = \tilde{\delta}(q'', w)$$

для всех $q', q'' \in Q_0$.

Таким образом, реакции на диагностические и установочные слова дают возможность идентифицировать, соответственно, начальное и финаль-

ное состояние слабоинициального автомата (M, Q_0). Синхронизирующее слово переводит все начальные состояния слабоинициального автомата в одно и то же финальное состояние. Следовательно, синхронизирующее слово идентифицирует финальное состояние слабоинициального автомата.

В определении синхронизирующих слов вообще не задействована функция выходов. Поэтому при их построении и анализе рассматривают, как правило, автоматы без выхода.

Для краткости, диагностические, установочные и синхронизирующие слова будем называть *идентифицирующими*.

Среди идентифицирующих слов выделяются *минимальные* (по длине) и *неприводимые* (или *неизбыточные*) идентифицирующие слова. Последние характеризуются тем, что при вычеркивании в них хотя бы одной буквы теряется свойство «быть идентифицирующим словом». Для минимизации сложности исполнения эксперимента предпочтительно подавать на автомат минимальные слова, так как именно эти слова характеризуют *внутреннюю сложность* экспериментов, предназначенных для идентификации состояний автомата.

В [49] показано, что диагностические слова используются при исследовании *наблюдаемости*, а установочные и синхронизирующие слова – при исследовании *управляемости* дискретных систем, представленных моделями с конечным числом состояний.

Таким образом, разработка методов построения минимальных и неприводимых идентифицирующих слов и оценка длин минимальных таких слов являются актуальными для решения *проблем анализа контроллепригодности дискретных систем*, а также при решении проблем анализа и синтеза *систем дискретных событий*, интерес к которым резко возрос за последнее время (см., напр., [312]).

В [30] для заданного слабоинициального автомата предложены методы поиска всех минимальных диагностических и установочных слов, основанные на *восстановлении начальных отрезков*. В [309] для заданного слабоинициального автомата предложен метод построения акцептора, представляющего множество всех диагностических слов, тем самым обоснована возможность использование техники *восстановления финальных отрезков* при построении идентифицирующих слов для заданного слабоинициального автомата.

В [167] систематически изложены методы построения для заданного слабоинициального автомата множеств минимальных и неприводимых идентифицирующих слов, основанные на восстановлении либо начальных отрезков, либо финальных отрезков, методы двухстороннего восстановления этих слов, а также методы построения автоматов-экспериментаторов.

Обозначим через $D(M, Q_0)$, $H(M, Q_0)$ и $S(M, Q_0)$ множество всех, соответственно, диагностических, установочных и синхронизирующих слов

для слабоинициального автомата (M,Q_0) $(|Q_0|\geq 2)$. Истинны следующие включения $D(M,Q_0)\subseteq H(M,Q_0)$ и $S(M,Q_0)\subseteq H(M,Q_0)$.

Пусть $U(M,Q_0)\in\{D(M,Q_0),H(M,Q_0),S(M,Q_0)\}$. Обозначим через $U^{\min}(M,Q_0)$ и $U^{ir}(M,Q_0)$ множество всех, соответственно, минимальных и неприводимых слов, принадлежащих множеству $U(M,Q_0)$. Истинны следующие включения $U^{\min}(M,Q_0)\subseteq U^{ir}(M,Q_0)$ $(U\in\{D,H,S\})$.

Обозначим через $L^d(M,Q_0)$, $L^h(M,Q_0)$ и $L^s(M,Q_0)$ длину минимального, соответственно, диагностического, установочного и синхронизирующего слова для слабоинициального автомата (M,Q_0). Если для слабоинициального автомата (M,Q_0) диагностическое установочное или синхронизирующее слово не существует, то считаем, что, соответственно, $L^d(M,Q_0)=0$, $L^h(M,Q_0)=0$ или $L^s(M,Q_0)=0$.

Пусть A_{kmn} – множество всех автоматов $M=(Q,X,Y,\delta,\lambda)$, имеющих фиксированные множество состояний $Q=\{q_1,\ldots,q_k\}$, входной алфавит $X=\{x_1,\ldots,x_m\}$ и выходной алфавит $Y=\{y_1,\ldots,y_n\}$.

Определим отображения $L^u_{kmn}:\{2,\ldots,k\}\to\mathbf{Z}_+$ $(u\in\{d,h,s\})$ равенством

$$L^u_{kmn}(r)=\max L^u(M,Q_0)\quad (r\in\{2,\ldots,k\}),$$

где максимум берется по всем автоматам $M\in\mathsf{A}_{kmn}$ и всем таким множествам допустимых начальных состояний $Q_0\subseteq Q$, что $|Q_0|=r$. Положим

$$L^u_{kmn}=\max_{r\in\{2,\ldots,k\}}L^u_{kmn}(r).$$

Отметим, что $L^d_{kmn}(r)$, $L^h_{kmn}(r)$, $L^s_{kmn}(r)$, L^d_{kmn}, L^d_{kmn} и L^d_{kmn} представляют собой *функции Шеннона*, характеризующие сложность построения минимальных идентифицирующих слов.

Исследованию длин минимальных идентифицирующих слов для слабоинициального автомата посвящен ряд работ.

В [266] установлена точная оценка максимальной длины минимального установочного слова

$$L^h_{kmn}(r)=0.5\cdot(2k-r)\cdot(r-1)\quad (r\in\{2,\ldots,k\}).$$

В [272] доказано, что в специальном случае, когда $Q_0=Q$, истинна следующая верхняя оценка длины минимального синхронизирующего слова

$$L^s_{kmn}(k)\leq 0.5\cdot k\cdot(k-1)^2.$$

Имеется много невыясненных моментов, связанных с оценками длин минимальных диагностических слов.

В [30] и в [309] установлены, соответственно верхние оценки

$$L^d_{kmn}(r)\leq(r-1)\cdot k^r\quad (r\in\{2,\ldots,k\})$$

и

$$L^{d}_{kmn}(r) \le k! \quad (r \in \{2,\ldots,k\}).$$

В [190] доказано, что истинна верхняя оценка

$$L^{d}_{kmn}(r) \le \begin{cases} (r-1)\cdot k^{0.5\cdot k\cdot(1+\varepsilon)}, & \textit{если } r \in \{2,\ldots,k-1\} \\ \binom{k}{0.5\cdot k}\cdot k^{2}, & \textit{если } r = k \end{cases},$$

где $\varepsilon \to 0$ при $r \to \infty$, а также нижняя оценка

$$L^{d}_{kmn}(r) \ge \begin{cases} \binom{k-1}{r-1}, & \textit{если } r \in \{2,\ldots,\lfloor 0.5k \rfloor\} \\ \binom{k\text{-}2}{\lfloor 0.5\cdot(k\text{-}2)\rfloor}, & \textit{если } r \in \{\lfloor 0.5k \rfloor+1,\ldots,k-1\}. \\ 3^{\left\lfloor \frac{1}{6}\cdot k \right\rfloor}, & \textit{если } r = k \end{cases}$$

В [144,145] доказано, что в специальном случае, когда $Q_0 = Q$, истинна следующая асимптотически точная оценка

$$\log_3 L^{d}_{kmn}(k) \sim \frac{k}{6} \quad (k \to \infty).$$

Работы [144,145,190] объединяет то, что используемые в них автоматы имеют входной алфавит, мощность которого, фактически, совпадает с длиной минимального идентифицирующего слова. Поэтому установленная в этих работах длина минимального идентифицирующего слова не превосходит память, необходимую для хранения автоматной таблицы.

Следующий пример показывает, что более тонкий комбинаторный анализ допустимой структуры графа переходов слабоинициального автомата, развитый в [164,166], дает возможность получить результаты совершенно иного уровня.

Пример 1.6. Сложность поиска минимальных идентифицирующих слов для слабоинициального автомата характеризуется более точно не функцией Шеннона L^{u}_{kmn} $(u \in \{d,h,s\})$, а отношением

$$L^{u}_{отн}(k,m,n) = \frac{L^{u}_{kmn}}{k\cdot m}, \tag{1.42}$$

где произведение $k\cdot m$ характеризует *объем памяти*, необходимой для хранения таблицы автомата, т.е. характеризует *сложность* исследуемой модели. Отметим, что ограничения значений m величиной $O(k)$ $(k \to \infty)$ дает возможность оценивать *сложность* поиска минимальных идентифицирующих слов, как функцию только от числа k состояний автомата.

Будем говорить, что состояния q_1 и q_2 автомата $M=(Q,X,Y,\delta,\lambda)\in \mathsf{A}_{kmn}$ являются x*−совместимыми* $(x\in X)$, если $\delta(q_1,x)=\delta(q_2,x)$ и $\lambda(q_1,x)=\lambda(q_2,x)$.

Теорема 1.20. Если $n=\left\lfloor \frac{1}{6}\cdot(\sqrt{24\cdot k-23}+1)\right\rfloor+1$, то истинна следующая оценка

$$L^d_{k2n}\geq e^{O(\sqrt{k})}\ \ (k\to\infty). \tag{1.43}$$

Доказательство. Для доказательства теоремы нам понадобится

Лемма 1.1. Для всех $k\geq 2$ и $r\in\{2,\ldots,\left\lfloor \frac{1}{6}\cdot(\sqrt{24\cdot k-23}+1)\right\rfloor\}$, то

$$L^d_{k2r}(r)>\max[l+1,\ldots,l+r-1], \tag{1.44}$$

где максимум берется по всем $l\in\{1,\ldots,\lfloor 0.5\cdot(r-1)^{-1}\cdot(2\cdot(k-1)-r\cdot(r-1))\rfloor\}$.

Доказательство. Для доказательства леммы достаточно построить такой слабоинициальный автомат (M,Q_0) $(M\in \mathsf{A}_{k2r},\ Q_0\subseteq Q,\ |Q_0|=r\geq 2)$, что

$$L^d(M,Q_0)=[l+1,\ldots,l+r-1]+1. \tag{1.45}$$

Выберем такие попарно непересекающиеся подмножества $W_1,\ldots,W_{r-1}$ множества $Q\setminus\{q_1\}$, что

$$W_i=\{q_{g(i)+j}\mid j=0,1,\ldots,l+i-1\}\quad (i=1,\ldots,r-1),$$

где

$$g(i)=2+l\cdot(i-1)+0.5\cdot i\cdot(i-1).$$

Нетрудно убедиться в том, что существование таких подмножеств гарантируется выбранными значениями чисел r и l.

Пусть $M\in \mathsf{A}_{k2r}$ − такой автомат, что

$$\delta(q_u,x_v)=\begin{cases} q_{u+1},\ \textit{если}\ v=1\ \textit{и}\ q_u\in W_i\setminus\{q_{g(i+1)-1}\}\ (i=1,\ldots,r-1)\\ q_{g(i)},\ \textit{если}\ v=1\ \textit{и}\ u=g(i+1)-1\ (i=1,\ldots,r-1)\\ q_1,\ \textit{если}\ v=2\ \textit{и}\ q_u\in\bigcup_{i=1}^{r-1}W_i\\ q_1,\ \textit{если}\quad v\in\{1,2\}\quad \textit{и}\ u=1, \end{cases} \tag{1.46}$$

$$\lambda(q_u,x_v)=\begin{cases} y_1,\ \textit{если}\ v=1\ \textit{и}\ q_u\in\bigcup_{i=1}^{r-1}W_i\\ y_1,\ \textit{если}\ v=2\ \textit{и}\ q_u\in W_i\setminus\{q_{g(i+1)-1}\}\ (i=1,\ldots,r-1)\\ y_{i+1},\ \textit{если}\ v=2\ \textit{и}\ u=g(i+1)-1\ (i=1,\ldots,r-1)\\ y_1,\ \textit{если}\quad v\in\{1,2\}\ \textit{и}\ u=1. \end{cases} \tag{1.47}$$

Положим $Q_0=\{q_1,q_{g(1)},\ldots,q_{g(r-1)}\}$. Из (1.46) и (1.47) вытекает, что:

1) состояние q_1 и любое состояние $q\in W_i\setminus\{q_{g(i+1)-1}\}$ $(i=1,\ldots,r-1)$ являются x_1−совместимыми;

2) входной символ x_2 попарно различает состояния $q_1,q_{g(2)-1},\ldots,q_{g(r)-1}$;

3) множество Q_0 переходит в множество $\{q_1, q_{g(2)-1}, \ldots, q_{g(r)-1}\}$ только под действием слов вида x_1^{α}, где α – общее кратное чисел $l+1, \ldots, l+r-1$.

Следовательно, единственным минимальным диагностическим словом для слабоинициального автомата (M, Q_0) является слово $x_1^{\alpha_0} x_2$, где

$$\alpha_0 = [l+1, \ldots, l+r-1].$$

Таким образом, для слабоинициального автомата (M, Q_0) истинно равенство (1.45).

Лемма доказана.

Из (1.44) вытекает, что при $l = r-1$

$$L^d_{k2r}(r) > [r, \ldots, 2\cdot(r-1)] = [1, \ldots, 2\cdot(r-1)]. \quad (1.48)$$

Известно, что (см., напр., [137]) при $x \geq 2$

$$e^{c_1 x} < [1, \ldots, x] < e^{c_2 x}, \quad (1.49)$$

где c_1, c_2 $(0 < c_1 < c_2)$ – константы. Из (1.59) вытекает, что

$$L^d_{k2r}(r) > e^{c(r-1)}, \quad (1.50)$$

где c $(c > 0)$ – константа. Полагая $r = O(\sqrt{k})$ $(k \to \infty)$ в (1.50), получим (1.43).

Теорема доказана.

Для функции переходов δ автомата $M = (Q, X, Y, \delta, \lambda)$ и входного символа $x \in X$ определим отображение $\delta_x : Q \to Q$ равенством

$$\delta_x(q) = \delta(q, x) \quad (q \in Q).$$

Отметим, что автомат M, построенный в процессе доказательства леммы 1.1, обладает тем свойством, что сужение $\delta_{x_1}\big|_{W_1 \cup \ldots \cup W_{r-1}}$ отображения δ_{x_1} является на множестве $W_1 \cup \ldots \cup W_{r-1}$ подстановкой, состоящей из циклов длины $l+1, \ldots, l+r-1$.

Следствие 1.5. Если $n = \left\lfloor \frac{1}{6} \cdot (\sqrt{24\cdot k - 23} + 1) \right\rfloor + 1$, то

$$L^d_{отн}(k, 2, n) \geq e^{O(\sqrt{k} - \ln k)} \quad (k \to \infty). \quad (1.51)$$

Доказательство. Положим $m = 2$ в равенстве (1.42) и подставим (1.43) в (1.42). Получим (1.51).

Следствие доказано.

Теорема 1.21. Истинно следующее асимптотическое неравенство

$$L^s_{k2n} \geq e^{O(\sqrt{k})} \quad (k \to \infty). \quad (1.52)$$

Доказательство. Для доказательства теоремы нам понадобится

Лемма 1.2. Для всех $k \geq 2$ и $r \in \{2, \ldots, \left\lfloor \frac{1}{6} \cdot (\sqrt{24\cdot k - 47} + 1) \right\rfloor\}$

$$L^s_{k2n}(r) > \max [l+1, \ldots, l+r-1], \quad (1.53)$$

где максимум берется по всем $l \in \{1, \ldots, \lfloor 0.5 \cdot (r-1)^{-1} \cdot (2\cdot(k-2) - r\cdot(r-1)) \rfloor\}$.

Доказательство. Для доказательства леммы достаточно построить такой слабоинициальный автомат (M, Q_0) $(M \in A_{k2n},\ Q_0 \subseteq Q,\ |Q_0| = r \geq 2)$, что

$$L^s(M, Q_0) = [l+1, \ldots, l+r-1] + 1. \tag{1.54}$$

Выберем такие попарно непересекающиеся подмножества $U_1, \ldots, U_{r-1}$ множества $Q \setminus \{q_1\}$, что

$$U_i = \{q_{h(i)+j} \mid j = 0,1,\ldots,l+i-1\} \quad (i = 1,\ldots,r-1),$$

где

$$h(i) = g(i) + 1,$$

а g – отображение, построенное в процессе доказательства леммы 1.1. Нетрудно убедиться в том, что существование таких подмножеств гарантируется выбранными значениями r и l.

Так как речь идет о синхронизирующем слове, то рассматриваем автомат M как автомат без выхода. Определим его функцию переходов равенством

$$\delta(q_u, x_v) = \begin{cases} q_{u+1}, \text{ если } v = 1 \text{ и } q_u \in U_i \setminus \{q_{h(i+1)-1}\} \ (i = 1,\ldots,r-1) \\ q_{h(i)}, \text{ если } v = 1 \text{ и } u = h(i+1) - 1 \ (i = 1,\ldots,r-1) \\ q_2, \text{ если } v = 2 \text{ и } q_u \in U_i \setminus \{q_{h(i+1)-1}\} \ (i = 1,\ldots,r-1) \\ q_1, \text{ если } v = 2 \text{ и } u = h(i+1) - 1 \ (i = 1,\ldots,r-1) \\ q_u, \text{ если } v \in \{1,2\} \text{ и } u \in \{1,2\}. \end{cases} \tag{1.55}$$

Положим $Q_0 = \{q_1, q_{h(1)}, \ldots, q_{h(r-1)}\}$. Из (1.55) вытекает, что:

1) состояния q_1 и q_2 не склеиваются никаким входным словом;

2) любое состояние $q \in U_i \setminus \{q_{h(i+1)-1}\}$ $(i = 1,\ldots,r-1)$ под действием входного символа x_2 переходит в состояние q_2;

3) входной символ x_2 склеивает состояния $q_1, q_{h(2)-1}, \ldots, q_{h(r)-1}$;

4) множество Q_0 переходит в множество $\{q_1, q_{h(2)-1}, \ldots, q_{h(r)-1}\}$ только под действием слов вида x_1^{α}, где α – общее кратное чисел $l+1, \ldots, l+r-1$.

Следовательно, единственное минимальное синхронизирующее слово для слабоинициального автомата (M, Q_0) – это слово $x_1^{\alpha_0} x_2$, где

$\alpha_0 = [l+1, \ldots, l+r-1]$.

Таким образом, для слабоинициального автомата (M, Q_0) истинно равенство (1.54).

Лемма доказана.

Из (1.53) вытекает, что если $l = r-1$, то

$$L^s_{k2n}(r) > [r, \ldots, 2\cdot(r-1)] = [1, \ldots, 2\cdot(r-1)] \geq e^{c(r-1)}, \tag{1.56}$$

где c $(c > 0)$ – константа. Полагая $r = O(\sqrt{k})$ $(k \to \infty)$ в (1.56), получим (1.52).

Теорема доказана.

Отметим, что автомат M, построенный в процессе доказательства леммы 1.2, обладает тем свойством, что сужение $\delta_{x_1}\big|_{U_1\cup\ldots\cup U_{r-1}}$ отображения δ_{x_1} является на множестве $U_1\cup\ldots\cup U_{r-1}$ подстановкой, состоящей из циклов длины $l+1,\ldots,l+r-1$.

Следствие 1.6. Истинно следующее асимптотическое неравенство

$$L^s_{отн}(k,2,n)\geq e^{O(\sqrt{k}-\ln k)}\ \ (k\to\infty). \qquad (1.57)$$

Доказательство. Положим $m=2$ в (1.42) и подставим (1.52) в (1.42). Получим (1.57).

Следствие доказано.

Значение следствий 1.5 и 1.6 состоит в следующем.

Пусть A − произвольный алгоритм поиска (возможно, неминимальных) диагностических или синхронизирующих слов для слабоинициального автомата, удовлетворяющий условию: за единицу времени алгоритм A восстанавливает фрагмент слова, длина которого является полиномом от размера автоматной таблицы. Тогда алгоритм A заведомо имеет экспоненциальную (как временную, так и емкостную) *сложность*.

Выше рассматривались *абстрактные* автоматы. Основной метод их исследования – это поиск, основанный на автоматной таблице или автоматном графе. Выделение классов автоматов, для которых функции переходов и выходов могут быть представлены системами алгебраических уравнений, дает возможность эффективно применять при исследовании таких автоматов алгебраические методы. Это, в свою очередь, дает возможность упростить решение ряда фундаментальных задач теории автоматов по сравнению с решением этих же задач в классе всех абстрактных автоматов.

Кроме того, появляется возможность установить внутреннюю связь между теорией динамических систем [74,111], теорией автоматов [30,31,98,208,265] и современной алгеброй [16,97,104]. Эта связь нетривиальная, так как такая чисто комбинаторная задача абстрактной теории автоматов, как контрольный эксперимент [265], для автоматов, представленных системами алгебраических уравнений, является обычной задачей параметрической идентификации, а исследование управляемости и наблюдаемости автоматов, представленных системами алгебраических уравнений сводится к построению установочного и диагностического экспериментов со слабоинициальным автоматом.

В [19,29,116,220] систематически исследованы линейные автоматы над полем Галуа $\mathbf{GF}(p)$, т.е. автоматы вида

$$\begin{cases}\mathbf{q}_{t+1}=A\circ\mathbf{q}_t\oplus B\circ\mathbf{x}_t\\ \mathbf{y}_t=C\circ\mathbf{q}_t\oplus D\circ\mathbf{x}_t\end{cases}\ (t\in\mathbf{N}),$$

где A,B,C,D − фиксированные, соответственно, $n\times n$-матрица, $n\times l$-матрица, $m\times n$-матрица и $m\times l$-матрица над полем Галуа $\mathbf{GF}(p)$, $\mathbf{x}\in\mathbf{Z}_p^l$ − входная переменная, $\mathbf{q}\in\mathbf{Z}_p^n$ − переменная состояния, а $\mathbf{y}\in\mathbf{Z}_p^m$ − выходная

переменная. Для таких автоматов охарактеризованы классы эквивалентных состояний, решены задача минимизации автомата и задача построения канонической формы, исследована управляемость автомата, охарактеризованы генераторы последовательностей элементов поля Галуа $\mathbf{GF}(p)$, получаемые в случае, когда B и D − нулевые матрицы. Методы анализа и синтеза линейных автоматов, развитые в [29,116,220], существенно опираются на модулярное преобразование Лапласа, чем установлена нетривиальная внутренняя связь между теорией таких автоматов и теорией линейных динамических систем [68].

Линейный автомат над полем Галуа $\mathbf{GF}(p)$ называется *автономным* автоматом, если входной символ тождественно равен нулю для всех $t \in \mathbf{N}$. Задача распознавания о.-д. функции, реализуемой автономным линейным автоматом над произвольным полем Галуа решена в [1].

В [2] исследована сложность параметрической идентификации линейного автомата над произвольным полем Галуа. В [87] исследована сложность обнаружения одиночных константных неисправностей для линейных автоматов над полем Галуа $\mathbf{GF}(2^n)$. В [308] рассмотрены задачи анализа управляемости и наблюдаемости для слабоинициальных линейных автоматов над полем $\mathbf{GF}(p)$. Задача построения синхронизирующей последовательности для линейных автоматов над полем $\mathbf{GF}(p)$ решена в [22]. Систематически диагностические, установочные и синхронизирующие эксперименты с линейными автоматами над полем $\mathbf{GF}(p)$ исследованы в [202]. Отдельные аспекты этого исследования представлены в [193-197,199-201].

По-видимому, в [198,202] впервые проработаны основы теории экспериментов с билинейными автоматами над полем $\mathbf{GF}(p)$, т.е. с автоматами вида

$$\begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus (\bigoplus_{i=1}^{l} F_i \circ x_t^{(i)}) \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_t \\ \mathbf{y}_t = C \circ \mathbf{q}_t \oplus (\bigoplus_{i=1}^{l} G_i \circ x_t^{(i)}) \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_t \end{cases} \quad (t \in \mathbf{N}),$$

где $\mathbf{x} = (x^{(1)},\ldots,x^{(l)})^T$ – входная переменная, $\mathbf{y} = (y^{(1)},\ldots,y^{(m)})^T$ – выходная переменная, $\mathbf{q} = (q^{(1)},\ldots,q^{(n)})^T$ – переменная состояния. Предполагается, что A и F_i $(i = 1,\ldots,l)$ – $n \times n$-матрицы, C и G_i $(i = 1,\ldots,l)$ – $m \times n$-матрицы, а B – $n \times l$-матрица.

1.6. Булевы функции.

Модели и методы теории булевых функций [58] играют существенную роль в процессе решения задач защиты информации. Рассмотрим основные понятия и определения этой теории, используемые в последующих разделах (см., напр., [58,105]).

Булевой функцией от n $(n \in \mathbf{N})$ переменных называется отображение $f : \mathbf{E}^n \to \mathbf{E}$, где $\mathbf{E} = \{0,1\}$.

Переменная z – *булева*, если $\mathbf{E}$ – область ее значений. Зафиксируем имена независимых булевых переменных $x_1, \ldots, x_n, \ldots$.

Обозначим через $P_2(n)$ $(n \in \mathbf{N})$ множество всех булевых функций от переменных $x_1, \ldots, x_n$.

В дальнейшем для краткости слово «булева» перед словами «переменная» и «функция» будем опускать, если это не вызывает недоразумений.

Значение функции $f \in P_2(n)$ на наборе $\mathbf{s} \in \mathbf{E}^n$ обозначим через $f(\mathbf{s})$.

Функции $f, g \in P_2(n)$ $(n \in \mathbf{N})$ – *равные* (обозначается $f = g$), если их значения равны при любых значениях переменных $x_1, \ldots, x_n$.

Функция $f \in P_2(n)$ может быть задана таблицей, содержащей $n+1$ столбец. В первых n столбцах представлены значения переменных $x_1, \ldots, x_n$, а в последнем столбце – соответствующее значение функции, т.е. если в первых n клетках строки записан набор $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n$, то в $(n+1)$-й клетке этой же строки записано значение $f(\mathbf{s})$.

Ясно, что такая таблица состоит из 2^n строк. Первые n столбцов таблицы заполняются в соответствии с правилом: набор

$$\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n,$$

записанный в первых n позициях i-ой строки $(i = 1, \ldots, 2^n)$ – это двоичное представление числа $i-1$, т.е.

$$i - 1 = \sum_{i=1}^{n} 2^{n-i} \cdot \sigma_i .$$

В таблицах 1.12 и 1.13 представлены все функции, принадлежащие, соответственно, множествам $P_2(1)$ и $P_2(2)$.

Таблица 1.12.

x_1	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0

Таблица 1.13.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Функции из таблиц 1.12 и 1.13 называются *элементарными функциями*. Они имеют специальные обозначения и имена, которые приведены в таблицах 1.14 и 1.15.

Таблица 1.14.

Функции из Таблицы 1.12	Специальное обозначение	Общепринятое имя функции
f_1	0	Константа нуль
f_2	1	Константа единица
f_3	x_1	Тождественная функция
f_4	$\bar{x}_1$	Отрицание

Таблица 1.15.

Функция из Таблицы 1.13	Специальное обозначение	Общепринятое имя функции
f_1	0	Константа нуль
f_2	$x_1 \wedge x_2$, $x_1 \cdot x_2$, $x_1 \& x_2$	Конъюнкция
f_3	$x_1 \not\Rightarrow x_2$	Отрицание (прямой) импликации
f_4	x_1	Первая проекция
f_5	$x_2 \not\Rightarrow x_1$	Отрицание (обратной) импликации
f_6	x_2	Вторая проекция
f_7	$x_1 \oplus x_2$, $x_1 + x_2$, $x_1 + x_2 (\mathrm{mod}\, 2)$	Сумма по модулю 2
f_8	$x_1 \vee x_2$	Дизъюнкция
f_9	$x_1 \downarrow x_2$	Стрелка Пирса (отрицание дизъюнкции)
f_{10}	$x_1 \sim x_2$	Эквивалентность
f_{11}	$\bar{x}_2$	Отрицание по 2-й проекции
f_{12}	$x_2 \Rightarrow x_1$	(Обратная) импликация
f_{13}	$\bar{x}_1$	Отрицание по 1-й проекции
f_{14}	$x_1 \Rightarrow x_2$	(Прямая) импликация
f_{15}	$x_1 \mid x_2$, $x_1 \uparrow x_2$	Штрих Шеффера (отрицание дизъюнкции)
f_{16}	1	Константа единица

Так как $\mathbf{GF}(2) = (\mathbf{E}, \oplus, \cdot)$ (где точкой обозначена операция конъюнкция), то множество $\mathbf{E}^n$ $(n \in \mathbf{N})$ может рассматриваться как линейное пространство $\mathbf{GF}^n(2)$ над полем $\mathbf{GF}(2)$.

Отметим, что:

1) *вес* вектора $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n$ определяется равенством

$$wt(\boldsymbol{\alpha}) = \sum_{i=1}^{n} \alpha_i ;$$

2) *скалярное произведение* векторов

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n$$

и

$$\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbf{E}^n$$

определяется равенством

$$< \boldsymbol{\alpha}, \boldsymbol{\beta} > = \bigoplus_{i=1}^{n} \alpha_i \cdot \beta_i ;$$

3) *отношение частичного порядка* $\leq_{\mathbf{E}^n}$ на множестве $\mathbf{E}^n$ определяется следующим образом: если $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n$ и $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbf{E}^n$, то

$$\boldsymbol{\alpha} \leq_{\mathbf{E}^n} \boldsymbol{\beta} \Leftrightarrow (\forall i = 1, \ldots, n)(\alpha_i \leq \beta_i) .$$

Ясно, что множество $P_2(n)$ $(n \in \mathbf{N})$ может рассматриваться как линейное пространство $\mathbf{GF}^{2^n}(2)$. Отсюда вытекает, что любая задача теории булевых функций может быть сформулирована в терминах теории линейных пространств над конечным полем.

Для функции $f \in P_2(n)$ $(n \in \mathbf{N})$ переменная x_i $(i = 1, \ldots, n)$ называется *существенной*, если существуют такие отличающиеся друг от друга только по i-ой компоненте наборы

$$\mathbf{s}_0 = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \in \mathbf{E}^n$$

и

$$\mathbf{s}_1 = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n) \in \mathbf{E}^n ,$$

что

$$f(\mathbf{s}_0) \neq f(\mathbf{s}_1) .$$

Обозначим через $P_2^{сущ}(n)$ $(n \in \mathbf{N})$ множество всех $f \in P_2(n)$, для которых каждая из переменных $x_1, \ldots, x_n$ существенная. Известно, что

$$| P_2^{сущ}(n) | = \sum_{i=0}^{n} (-1)^i \cdot \binom{n}{i} \cdot 2^{2^{n-i}} \quad (n \in \mathbf{N}) .$$

Если переменная x_i $(i = 1, \ldots, n)$ не является существенной для функции $f \in P_2(n)$ $(n \in \mathbf{N})$, то x_i – *фиктивная* переменная для функции f. Пусть $i \in \{1, \ldots, n+1\}$. Запись

$$f(x_1,\ldots,x_{n+1}) = g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_{n+1}),$$

означает, что x_i – фиктивная переменная для функции $f \in P_2(n+1)$, а $g \in P_2(n)$ – такая функция, что для всех $\boldsymbol{\sigma} = (\sigma_1,\ldots,\sigma_n) \in \mathbf{E}^n$ истинно равенство

$$f(\sigma_1,\ldots,\sigma_{i-1},x_i,\sigma_i,\sigma_{i+1},\ldots,\sigma_n) = g(\boldsymbol{\sigma}).$$

Для функции $f \in P_2(n)$ $(n \in \mathbf{N})$ положим

$$\mathbf{N}_f = \{\boldsymbol{\sigma} \in \mathbf{E}^n \mid f(\boldsymbol{\sigma}) = 1\}.$$

Число $|\mathbf{N}_f|$ называется весом функции $f \in P_2(n)$ $(n \in \mathbf{N})$, и обозначается $wt(f)$. Пусть $f \in P_2(n+1)$ $(n \in \mathbf{N})$ и $g \in P_2(n)$. Известно, что:

1) если $f(x_1,\ldots,x_{n+1}) = g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_{n+1})$, то $wt(f) = 2 \cdot wt(g)$;

2) если $f(x_1,\ldots,x_{n+1}) = g(x_1,\ldots,x_{n-1},x_n \oplus x_{n+1})$, то $wt(f) = 2 \cdot wt(g)$

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ называется *уравновешенной*, если

$$wt(f) = 2^{n-1}.$$

Отметим, что для любых $f \in P_2(n)$ $(n \in \mathbf{N})$ и $s \in \mathsf{S}(n+1)$ уравновешенной является функция $g \in P_2(n+1)$, определенная равенством

$$g(x_1,\ldots,x_{n+1}) = f(x_{s(1)},\ldots,x_{s(n)}) \oplus x_{s(n+1)}.$$

Рассмотрим два основных представления функций $f \in P_2(n)$ $(n \in \mathbf{N})$.

Первое представление функции $f \in P_2(n)$ $(n \in \mathbf{N})$ – это представление в виде *дизъюнктивной нормальной формы* (ДНФ) и *конъюнктивной нормальной формы* (КНФ).

Пусть x – булева переменная (или булева функция). Положим

$$x^\sigma = \begin{cases} x, \text{ если } \sigma = 1 \\ \bar{x}, \text{ если } \sigma = 0 \end{cases}.$$

Ясно, что $\sigma^\sigma = 1$, $\sigma^{\bar{\sigma}} = 0$ и $\bar{\sigma}^\sigma = 0$, где $\sigma \in \mathbf{E}$.

Каждая функция $f \in P_2(n)$ $(n \in \mathbf{N})$ может быть представлена *совершенной ДНФ* (СДНФ), т.е. в виде

$$f(x_1,\ldots,x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n) \in \mathbf{N}_f} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n},$$

а также *совершенной КНФ* (СКНФ), т.е. в виде

$$f(x_1,\ldots,x_n) = \mathop{\&}_{(\sigma_1,\ldots,\sigma_n) \in \mathbf{E}^n \setminus \mathbf{N}_f} (x_1^{\bar{\sigma}_1} \vee \ldots \vee x_n^{\bar{\sigma}_n}).$$

СДНФ и СКНФ являются специальными случаями следующей конструкции.

Пусть $x_{i_1},\ldots,x_{i_r}$ $(r \in \mathbf{Z}_+)$ – попарно различные переменные и $\sigma_j \in \mathbf{E}$ $(j = 1,\ldots,r)$. Выражение $x_{i_1}^{\sigma_1} \cdot \ldots \cdot x_{i_r}^{\sigma_r}$ $(= \mathop{\&}_{j=1}^{r} x_{i_j}^{\sigma_j})$ называется *элементарной*

конъюнкцией ранга r, а выражение $x_{i_1}^{\sigma_1} \vee \ldots \vee x_{i_r}^{\sigma_r}$ $(= \bigvee\limits_{j=1}^{r} x_{i_j}^{\sigma_j})$ – *элементарной дизъюнкцией ранга* r. По определению $\&\limits_{j=1}^{0} x_{i_j}^{\sigma_j} = 1$ и $\bigvee\limits_{j=1}^{0} x_{i_j}^{\sigma_j} = 0$.

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ представлена:

1) ДНФ, если

$$f(x_1,\ldots,x_n) = \bigvee_{j=1}^{h} K_j,$$

где K_j $(j = 1,\ldots,h)$ – элементарные конъюнкции;

2) КНФ, если

$$f(x_1,\ldots,x_n) = \&_{j=1}^{l} D_j,$$

где D_j $(j = 1,\ldots,l)$ – элементарные дизъюнкции.

От представления функции в виде ДНФ можно перейти к ее представлению в виде КНФ. Для этого достаточно применять дистрибутивный закон $a \cdot b \vee c = (a \vee c) \cdot (b \vee c)$ и тождество $x \vee \bar{x} = 1$. Аналогичным образом, от представления функции в виде КНФ можно перейти к ее представлению в виде ДНФ. Для этого достаточно раскрыть все скобки в соответствии с дистрибутивным законом $a \cdot (b \vee c) = a \cdot b \vee a \cdot c$ и применить тождество $x \cdot \bar{x} = 0$. Принимая во внимание это соответствие между ДНФ и КНФ, в дальнейшем рассматриваем представление функции $f \in P_2(n)$ $(n \in \mathbf{N})$ в виде ДНФ.

Говорят, что ДНФ D *реализует* функцию $f \in P_2(n)$ $(n \in \mathbf{N})$, если $f = D$. При этом, D – *минимальная* ДНФ, если D содержит наименьшее число литералов среди всех ДНФ, реализующих функцию f и D – *кратчайшая* ДНФ, если D содержит наименьшее число элементарных конъюнкций, среди всех ДНФ, реализующих функцию f.

Если K – элементарная конъюнкция ранга r $(r \le n)$, то $\mathbf{N}_K$ – *интервал* r*-го ранга*, определяющий $(n-r)$*-мерную грань* n-мерного единичного куба $\mathbf{E}^n$. Ясно, что ДНФ $D = \bigvee\limits_{i=1}^{h} K_i$ реализует функцию $f \in P_2(n)$ $(n \in \mathbf{N})$ тогда и только тогда, когда $\mathbf{N}_f = \bigcup\limits_{i=1}^{h} \mathbf{N}_{K_i}$. Итак, построение ДНФ, реализующей функцию $f \in P_2(n)$ $(n \in \mathbf{N})$, эквивалентно *покрытию* множества $\mathbf{N}_f$ такими интервалами $\mathbf{N}_{K_1},\ldots,\mathbf{N}_{K_h}$, что $\mathbf{N}_{K_i} \subseteq \mathbf{N}_f$ для всех $i = 1,\ldots,h$.

Элементарная конъюнкция K и интервал $\mathbf{N}_K$ называются *допустимыми* для функции $f \in P_2(n)$ $(n \in \mathbf{N})$, если $\mathbf{N}_K \subseteq \mathbf{N}_f$. Интервал $\mathbf{N}_K$ называется *максимальным* интервалом для функции $f \in P_2(n)$ $(n \in \mathbf{N})$, если $\mathbf{N}_K \subseteq \mathbf{N}_f$ и не существует такой интервал $\mathbf{N}_{\tilde{K}}$, что $\mathbf{N}_K \subset \mathbf{N}_{\tilde{K}} \subseteq \mathbf{N}_f$.

Сокращенной ДНФ называется ДНФ, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$ и соответствующая покрытию множества $\mathbf{N}_f$ всеми максимальными для функции f интервалам. Сокращенная ДНФ функции $f \in P_2(n)$ $(n \in \mathbf{N})$ определяется однозначно. Она обозначается через $D_c(f)$. Значимость ДНФ $D_c(f)$ характеризуется тем, что любая минимальная ДНФ, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$, может быть получена из ДНФ $D_c(f)$ в результате удаления некоторых элементарных конъюнкций. Кроме того, для каждой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ существует кратчайшая ДНФ, которая может быть получена из ДНФ $D_c(f)$ в результате удаления некоторых элементарных конъюнкций.

Рассмотрим методы построения ДНФ $D_c(f)$ для функции $f \in P_2(n)$ $(n \in \mathbf{N})$.

1. Метод Квайна. Исходными данными является СДНФ $D_f^{сов}$ функции $f \in P_2(n)$ $(n \in \mathbf{N})$. Применяются преобразования:

1) *неполное склеивание*, т.е.

$$K \cdot x \vee K \cdot \bar{x} = K \vee K \cdot x \vee K \cdot \bar{x}; \qquad (1.58)$$

2) *элементарное поглощение*, т.е.

$$K \cdot x^{\sigma} \vee K = K. \qquad (1.59)$$

Построение ДНФ $D_c(f)$ осуществляется следующим образом.

Алгоритм 1.4.

Шаг 1. $i := 0$, $D_0 := D_f^{сов}$.

Шаг 2. Строим ДНФ D_i' в соответствии с правилом: выполняем всевозможные преобразования (1.58) над всеми парами элементарных конъюнкций ранга $n - i$, принадлежащих ДНФ D_i.

Шаг 3. Строим ДНФ D_{i+1} в соответствии с правилом: удаляем из ДНФ D_i' все элементарные конъюнкции ранга $n - i$, которые можно исключить в результате преобразования (1.59).

Шаг 4. Если D_i и D_{i+1} состоят из одних и тех же элементарных конъюнкций, то переход к шагу 6, иначе переход к шагу 5.

Шаг 5. $i := i + 1$ и переход к шагу 2.

Шаг 6. $D_c(f) := D_i$ и *конец.*

2. Метод Блейка. Исходными данными является любая ДНФ D, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$. Применяются преобразования:

1) *обобщенное склеивание*, т.е.

$$x \cdot K_1 \vee \bar{x} \cdot K_2 = x \cdot K_1 \vee \bar{x} \cdot K_2 \vee K_1 \cdot K_2; \qquad (1.60)$$

2) *поглощение*, т.е.

$$K_1 \vee K_1 \cdot K_2 = K_1. \qquad (1.61)$$

Построение ДНФ $D_c(f)$ осуществляется в следующим образом.

Алгоритм 1.5.

Шаг 1. $i := 0$, $D_0 := D$.

Шаг 2. Строим ДНФ D_i' в соответствии с правилом: применяем все возможные преобразования (1.60) ко всем парам элементарных конъюнкций, принадлежащих ДНФ D_i (в ДНФ D_i' не записываются произведения *ортогональных* конъюнкций, т.е. таких, что $K_1 \cdot K_2 = 0$).

Шаг 3. Строим ДНФ D_{i+1} в соответствии с правилом: удаляем из ДНФ D_i' все элементарные конъюнкции, которые можно удалить в результате преобразования (1.61).

Шаг 4. Если D_i и D_{i+1} состоят из одних и тех же элементарных конъюнкций, то переход к шагу 6, иначе переход к шагу 5.

Шаг 5. $i := i+1$ и переход к шагу 2.

Шаг 6. $D_c(f) := D_i$ и *конец*.

3. Метод Нельсона. Исходными данными является любая КНФ K, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$. Применяются преобразования:

1) *дистрибутивный закон*, т.е.

$$K_1 \cdot (K_2 \vee K_3) = K_1 \cdot K_2 \vee K_1 \cdot K_3; \qquad (1.62)$$

2) *правила дополнения*, т.е.

$$x \cdot \bar{x} = 0, \quad x \vee \bar{x} = 1; \qquad (1.63)$$

3) *поглощение*, т.е. преобразование (1.61).

Построение ДНФ $D_c(f)$ состоит в последовательном раскрытии скобок в КНФ K в соответствии с (1.62). После каждого раскрытия скобок выполняются все возможные упрощения в соответствии с (1.61) и (1.63).

Покрытие $\{\mathbf{N}_{K_1}, \ldots, \mathbf{N}_{K_h}\}$ множества $\mathbf{N}_f$ $(f \in P_2(n))$ максимальными допустимыми для функции f интервалами называется *неприводимым*, если $\{\mathbf{N}_{K_1}, \ldots, \mathbf{N}_{K_h}\} \setminus \{\mathbf{N}_{K_j}\}$ не является покрытием множества $\mathbf{N}_f$ для каждого $j = 1, \ldots, h$.

Пусть $D(j)$ $(j = 1, \ldots, h)$ – ДНФ, полученная из ДНФ $\bigvee\limits_{\substack{i=1 \\ i \neq j}}^{h} K_i$ в результате вычеркивания всех литералов, входящих в K_j. Ясно, что покрытие $\{\mathbf{N}_{K_1}, \ldots, \mathbf{N}_{K_h}\}$ является неприводимым тогда и только тогда, когда $D(j) \not\equiv 1$ для всех $j = 1, \ldots, h$.

ДНФ $D = \bigvee\limits_{i=1}^{h} K_i$, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$, называется *тупиковой* ДНФ, если $\{\mathbf{N}_{K_1}, \ldots, \mathbf{N}_{K_h}\}$ – неприводимое покрытие множества $\mathbf{N}_f$. Значение тупиковых ДНФ характеризуется тем, что:

1) каждая реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$ минимальная ДНФ является тупиковой ДНФ для функции f;

2) если $D = \bigvee_{i=1}^{h} K_i$ – кратчайшая ДНФ, реализующая функцию $f \in P_2(n)$ $(n \in \mathbf{N})$, то существует кратчайшая тупиковая ДНФ $D = \bigvee_{i=1}^{h} K_i'$, реализующая функцию f, где $\mathbf{N}_{K_i'} \supseteq \mathbf{N}_{K_i}$ для всех $i = 1, \ldots, h$.

Второе представление функции $f \in P_2(n)$ $(n \in \mathbf{N})$ – это ее представление элементом кольца многочленов $\mathbf{GF}(2)[x_1, \ldots, x_n]$, у которого степень по каждой переменной $x_1, \ldots, x_n$ не превосходит единицы.

Пусть $\mathbf{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n$. Положим $\mathbf{x}^{\boldsymbol{\sigma}} = x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$, где

$$x^{\sigma} = \begin{cases} 1, \text{ если } \sigma = 0 \\ x, \text{ если } \sigma = 1 \end{cases}.$$

Полиномом Жегалкина или *алгебраической нормальной формой* (АНФ) для функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется ее представление в виде

$$f(x) = \bigoplus_{\boldsymbol{\sigma} \in \mathbf{E}^n} a_{\boldsymbol{\sigma}} \cdot \mathbf{x}^{\boldsymbol{\sigma}}, \tag{1.64}$$

где $a_{\boldsymbol{\sigma}} \in \mathbf{E}$ $(\boldsymbol{\sigma} \in \mathbf{E}^n)$. Известно, что для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ существует единственное ее представление в виде (1.64), причем

$$a_{\boldsymbol{\sigma}} = \bigoplus_{\boldsymbol{\alpha} \le_{\mathbf{E}^n} \boldsymbol{\sigma}} f(\boldsymbol{\alpha}) \quad (\boldsymbol{\sigma} \in \mathbf{E}^n).$$

Слагаемым в представлении (1.64) называется каждое такое выражение $a_{\boldsymbol{\sigma}} \cdot \mathbf{x}^{\boldsymbol{\sigma}}$, что $a_{\boldsymbol{\sigma}} = 1$. *Алгебраической степенью* функции $f \in P_2(n)$ $(n \in \mathbf{N})$ (обозначается $\deg f$) называется число переменных в самом длинном слагаемом АНФ функции f. Число $\deg f$ называется также *степенью нелинейности* функции f.

Следующий пример показывает, что понятие «степень нелинейности функции f» дает возможность существенно обобщить и представить в терминах булевых функций коды Рида-Маллера [21,105,106], рассмотренные в п.1.2.

Пример 1.7. Для функции $f \in P_2(m)$ $(m \in \mathbf{N})$ положим $\Omega_f = (f(\mathbf{0}), \ldots, f(\mathbf{1}))$.

Множество кодовых слов кода Рида-Маллера r-го порядка $(r \in \mathbf{N})$ длины 2^m $(m \ge r)$ определяется равенством

$$RM(r, m) = \{\Omega_f \mid f \in P_2(m), \deg f \le r\}.$$

Поэтому для любых

$$\tau \in \mathsf{S}(\{0,1, \ldots, r\})$$

и

$$\zeta_i \in \mathsf{S}(\{\Omega_{x_1 \cdot \ldots \cdot x_i}, \ldots, \Omega_{x_{m-i+1} \cdot \ldots \cdot x_m}\}) \quad (i = 1, \ldots, r)$$

порождающая матрица $G(r,m;\tau,\zeta_1,\ldots,\zeta_r)$ кода Рида-Маллера r-го порядка длины 2^m – это матрица

$$G(r,m;\tau,\zeta_1,\ldots,\zeta_r)=(G_{\tau(0)}G_{\tau(1)}\ldots G_{\tau(r)}),$$

где

$$G_0=(\underbrace{1,\ldots,1}_{2^m\ раз})^T$$

и

$$G_i=(\zeta_i(\Omega_{x_1\cdot\ldots\cdot x_i}),\ldots,\zeta_i(\Omega_{x_{m-i+1}\cdot\ldots\cdot x_m}))^T\quad(i=1,\ldots,r).$$

Отметим, что в настоящее время в криптологии, как правило, применяются коды Рида-Маллера 1-го порядка.

Среди функций $f\in P_2(n)$ $(n\in\mathbf{N})$, для которых $\deg f\le 1$, выделяется множество *аффинных* функций

$$P_2^{аф}(n)=\{f\in P_2(n)\mid f(x_1,\ldots,x_n)=b\oplus a_1\cdot x_1\oplus\ldots\oplus a_n\cdot x_n\}$$

и множество *линейных* функций

$$P_2^{лин}(n)=\{f\in P_2^{аф}(n)\mid f(x_1,\ldots,x_n)=a_1\cdot x_1\oplus\ldots\oplus a_n\cdot x_n\}.$$

Любая аффинная функция, принадлежащая множеству $P_2^{аф}(n)$, может быть представлена в виде

$$l_{\mathbf{a},b}(\mathbf{x})=<\mathbf{a},\mathbf{x}>\oplus b,$$

где $\mathbf{x}=(x_1,\ldots,x_n)$, $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbf{E}^n$ и $b\in\mathbf{E}$. Отсюда вытекает, что

$$|P_2^{аф}(n)|=2^{n+1}$$

и

$$|P_2^{лин}(n)|=2^n.$$

Функция $f\in P_2(n)$ $(n\in\mathbf{N})$ называется *функционально разделимой*, если существует такие $k\in\{1,\ldots,n-1\}$, $g\in P_2(n-k+1)$, $h\in P_2(k)$ и $s\in\mathsf{S}(n)$, что

$$f(x_1,\ldots,x_n)=g(h(x_{s(1)},\ldots,x_{s(k)}),x_{s(k+1)},\ldots,x_{s(n)}).$$

Известно, что если $n\to\infty$, то доля функционально разделимых функций стремится к нулю. Отметим, что до сих пор не известен эффективный критерий для возможности представления функции $f\in P_2(n)$ $(n\in\mathbf{N})$ в виде

$$f(A\circ(x_1,\ldots,x_n)^T)=h(x_{s(1)},\ldots,x_{s(k)})\vee g(x_{s(k+1)},\ldots,x_{s(n)}),$$

а также в виде

$$f(A\circ(x_1,\ldots,x_n)^T)=h(x_{s(1)},\ldots,x_{s(k)})\oplus g(x_{s(k+1)},\ldots,x_{s(n)}),$$

где A – невырожденная $n\times n$-матрица над полем $\mathbf{GF}(2)$, а $s\in\mathsf{S}(n)$.

Для функции $f\in P_2(n)$ $(n\in\mathbf{N})$ *преобразованием Фурье* называется функция $\tilde{W}_f:\mathbf{E}^n\to\mathbf{Z}$, определенная равенством

$$\tilde{W}_f(\mathbf{u})=\sum_{\mathbf{x}\in\mathbf{E}^n}f(\mathbf{x})\cdot(-1)^{<\mathbf{x},\mathbf{u}>},$$

а *преобразованием Уолша-Адамара* – функция $W_f : \mathbf{E}^n \to \mathbf{Z}$, определенная равенством

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbf{E}^n} (-1)^{f(\mathbf{x})\oplus<\mathbf{x},\mathbf{u}>} . \qquad (1.65)$$

Из (1.65) вытекает, что:

1) $(-1)^{f(\boldsymbol{\sigma})} = 1 - 2\cdot f(\boldsymbol{\sigma})$ для всех $f \in P_2(n)$ $(n \in \mathbf{N})$ и $\boldsymbol{\sigma} \in \mathbf{E}^n$;

2) для любой функции $l_{\mathbf{a},b} \in P_2^{a\phi}(n)$ истинно равенство

$$W_{l_{\mathbf{a},b}}(\boldsymbol{\sigma}) = \begin{cases} (-1)^b \cdot 2^n, \ \textit{если} \ \boldsymbol{\sigma} = \mathbf{a} \\ 0, \ \textit{если} \ \boldsymbol{\sigma} \neq \mathbf{a} \end{cases};$$

3) для любых функций $g, h \in P_2(n)$ $(n \in \mathbf{N})$, если $f(\mathbf{x}) = g(\mathbf{x}) \oplus h(\mathbf{x})$, то

$$W_f(\boldsymbol{\sigma}) = 2^{-n} \cdot \sum_{\boldsymbol{\alpha}\in\mathbf{E}^n} W_g(\boldsymbol{\alpha}) \cdot W_h(\boldsymbol{\alpha} \oplus \boldsymbol{\sigma}) \quad (\boldsymbol{\sigma} \in \mathbf{E}^n).$$

Для каждого $\boldsymbol{\sigma} \in \mathbf{E}^n$ числа $\widetilde{W}_f(\boldsymbol{\sigma})$ и $W_f(\boldsymbol{\sigma})$ называются, соответственно, *коэффициентами Фурье* и *коэффициентами Уолша-Адамара* функции $f \in P_2(n)$ $(n \in \mathbf{N})$. Эти коэффициенты связаны друг с другом равенством

$$W_f(\boldsymbol{\sigma}) = 2^n \cdot \delta(\boldsymbol{\sigma}) - 2 \cdot \widetilde{W}_f(\boldsymbol{\sigma}) \quad (\boldsymbol{\sigma} \in \mathbf{E}^n), \qquad (1.66),$$

где $\delta : \mathbf{E}^n \to \mathbf{E}$ – *δ-функция Дирака*, определяемая следующим образом

$$\delta(\mathbf{u}) = \begin{cases} 1, \ \textit{если} \ \mathbf{u} = \mathbf{0} \\ 0, \ \textit{если} \ \mathbf{u} \neq \mathbf{0} \end{cases}.$$

Учитывая равенство (1.66), достаточно рассмотреть свойства коэффициентов Уолша-Адамара функции $f \in P_2(n)$ $(n \in \mathbf{N})$.

Зафиксируем константы $\sigma_j \in \mathbf{E}$ $(j = 1,\ldots,k)$, где $k \le n$. Обозначим через $f_{i_1,\ldots,i_k}^{\sigma_1,\ldots,\sigma_k}$ $(f \in P_2(n); 1 \le i_1 < \ldots < i_k \le n)$ функцию, полученную из функции f в результате подстановки вместо переменных $x_{i_1},\ldots,x_{i_k}$, соответственно, констант $\sigma_1,\ldots,\sigma_k$. Функция $f_{i_1,\ldots,i_k}^{\sigma_1,\ldots,\sigma_k}$ называется *подфункцией* функции f.

Известно, что для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$:

1) если $f(x) = \bigoplus_{\boldsymbol{\sigma}\in\mathbf{E}^n} a_{\boldsymbol{\sigma}} \cdot \mathbf{x}^{\boldsymbol{\sigma}}$, то

$$a_{\boldsymbol{\sigma}} = (2^{wt(\boldsymbol{\sigma})-1} - 2^{wt(\boldsymbol{\sigma})-n-1} \cdot \sum_{\boldsymbol{\alpha}\le_{\mathbf{E}^n}\boldsymbol{\sigma}\oplus\mathbf{1}} W_f(\boldsymbol{\alpha})) \,(\mathrm{mod}\, 2);$$

2) $\sum_{\boldsymbol{\alpha}\le_{\mathbf{E}^n}\boldsymbol{\sigma}} W_f(\boldsymbol{\alpha}) = 2^n - 2^{k+1} \cdot wt(f_{i_1,\ldots,i_k}^{0,\ldots,0})$ для любого такого вектора $\boldsymbol{\sigma} \in \mathbf{E}^n$, что $wt(\boldsymbol{\sigma}) = k$ $(k \le n)$ и координаты вектора $\boldsymbol{\sigma}$ равные 1 расположены в позициях $i_1,\ldots,i_k$;

3) $W_f(\mathbf{0}) = 2^n - 2 \cdot wt(f)$;

4) $W_f(\boldsymbol{\sigma}) = W_{f\oplus l_{\boldsymbol{\sigma},0}}(\mathbf{0})$ для всех $\boldsymbol{\sigma} \in \mathbf{E}^n$;

5) $\sum_{\boldsymbol{\sigma}\in\mathbf{E}^n} W_f^2(\boldsymbol{\sigma}) = 2^{2\cdot n}$ (*равенство Парсеваля*);

6) $\max_{\boldsymbol{\sigma}\in\mathbf{E}^n} |W_f(\boldsymbol{\sigma})| \geq 2^{0.5\cdot n}$;

7) $2^{-n}\cdot \sum_{\boldsymbol{\sigma}\in\mathbf{E}^n} W_f(\boldsymbol{\sigma})\cdot(-1)^{<\boldsymbol{\sigma},\boldsymbol{\alpha}>} = (-1)^{f(\boldsymbol{\alpha})}$ (*формула обращения*);

8) $\sum_{\boldsymbol{\sigma}\in\mathbf{E}^n} W_f(\boldsymbol{\sigma})\cdot W_f(\boldsymbol{\sigma}\oplus\boldsymbol{\alpha}) = 0$ для любого $\boldsymbol{\alpha}\in\mathbf{E}^n\setminus\{\mathbf{0}\}$;

9) если существуют такие $k\in\{1,\ldots,n-1\}$ и $s\in \mathsf{S}(n)$, что

$$f(x_1,\ldots,x_n) = h(x_{s(1)},\ldots,x_{s(k)})\oplus g(x_{s(k+1)},\ldots,x_{s(n)}),$$

то для всех $(\sigma_1,\ldots,\sigma_n)\in\mathbf{E}^n$

$$W_f(\sigma_1,\ldots,\sigma_n) = W_h(\sigma_{s(1)},\ldots,\sigma_{s(k)})\cdot W_g(\sigma_{s(k+1)},\ldots,\sigma_{s(n)}).$$

10) если $W_f(\boldsymbol{\sigma})\equiv 0 \pmod{2^k}$ для всех $\boldsymbol{\sigma}\in\mathbf{E}^n$, то $\deg f \leq n-k+1$.

Ортогональное дополнение подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$ – это подпространство, определяемое равенством

$$\mathbf{V}^{\perp} = \{\boldsymbol{\sigma}\in\mathbf{E}^n \mid <\boldsymbol{\sigma},\boldsymbol{\alpha}> = 0 \ \textit{для всех}\ \boldsymbol{\alpha}\in\mathbf{V}\}.$$

Отметим, что

$$\dim\mathbf{V} + \dim\mathbf{V}^{\perp} = n,$$

для любого подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$.

Нетрудно убедиться в том, что для любого подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$

$$\sum_{\boldsymbol{\sigma}\in\mathbf{V}}(-1)^{<\boldsymbol{\sigma},\boldsymbol{\alpha}>} = \begin{cases} 2^{\dim\mathbf{V}}, & \textit{если}\ \boldsymbol{\alpha}\in\mathbf{V}^{\perp} \\ 0, & \textit{если}\ \boldsymbol{\alpha}\in\mathbf{V} \end{cases}.$$

Известно, что для любых $f\in P_2(n)$ $(n\in\mathbf{N})$, $\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbf{E}^n$ и любого подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$ истинно равенство

$$\sum_{\boldsymbol{\sigma}\in\boldsymbol{\alpha}\oplus\mathbf{V}}(-1)^{f(\boldsymbol{\sigma})\oplus<\boldsymbol{\beta},\boldsymbol{\sigma}>} = 2^{\dim\mathbf{V}-n}\cdot(-1)^{<\boldsymbol{\alpha},\boldsymbol{\beta}>}\cdot\sum_{\boldsymbol{\sigma}\in\boldsymbol{\beta}\oplus\mathbf{V}^{\perp}} W_f(\boldsymbol{\sigma})\cdot(-1)^{<\boldsymbol{\alpha},\boldsymbol{\sigma}>}.$$

Из этого равенства вытекает, что для любой функции $f\in P_2(n)$ $(n\in\mathbf{N})$ и для любого подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$ истинны равенства

$$\sum_{\boldsymbol{\sigma}\in\mathbf{V}}(-1)^{f(\boldsymbol{\sigma})} = 2^{\dim\mathbf{V}-n}\cdot\sum_{\boldsymbol{\sigma}\in\mathbf{V}^{\perp}} W_f(\boldsymbol{\sigma})$$

и

$$\sum_{\boldsymbol{\sigma}\in\mathbf{V}^{\perp}} W_f(\boldsymbol{\sigma}) = 2^n - 2^{n-\dim\mathbf{V}+1}\cdot wt(f|_{\mathbf{V}}),$$

где

$$wt(f|_{\mathbf{V}}) = |\{\boldsymbol{\alpha}\in\mathbf{V} \mid \boldsymbol{\alpha}\in\mathbf{N}_f\}|.$$

Матрицей Адамара типа Сильвестра называется $2^n \times 2^n$-матрица H_n $(n \in \mathbf{N})$, определенная следующим образом:

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

и

$$H_n = H_1 \otimes H_{n-1} \quad (n \geq 2),$$

где $\otimes$ – тензорное произведение матриц, т.е.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes A = \begin{pmatrix} a \cdot A & b \cdot A \\ c \cdot A & d \cdot A \end{pmatrix}.$$

Отметим, что

$$H_n = H_n^T = 2^n \cdot H_n^{-1}$$

и

$$H_n \cdot H_n = 2^n \cdot I_{2^n}$$

для всех $n \in \mathbf{N}$, где I_{2^n} – единичная $2^n \times 2^n$-матрица.

Для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ истинно равенство

$$(W_f(\mathbf{0}), \ldots, W_f(\mathbf{1})) = ((-1)^{f(\mathbf{0})}, \ldots, (-1)^{f(\mathbf{1})}) \cdot H_n.$$

Вектор

$$(W_f(\mathbf{0}), \ldots, W_f(\mathbf{1}))$$

называется *спектром* функции $f \in P_2(n)$ $(n \in \mathbf{N})$. Говорят, что функции $f, g \in P_2(n)$ $(n \in \mathbf{N})$ имеют *непересекающиеся спектры*, если

$$W_f(\boldsymbol{\sigma}) \cdot W_g(\boldsymbol{\sigma}) = 0$$

для всех $\boldsymbol{\sigma} \in \mathbf{E}^n$.

Расстояние между функциями $f, g \in P_2(n)$ определяется равенством

$$dist(f, g) = wt(f \oplus g),$$

а расстояние между функцией $f \in P_2(n)$ $(n \in \mathbf{N})$ и множеством функций S $(S \subseteq P_2(n))$ – равенством

$$dist(f, S) = \min_{g \in S} dist(f, g).$$

Известно, что для всех $f \in P_2(n)$ $(n \in \mathbf{N})$ и $\boldsymbol{\sigma} \in \mathbf{E}^n$ истинны равенства

$$dist(f, l_{\boldsymbol{\sigma},0}) = 2^{n-1} - 0.5 \cdot W_f(\boldsymbol{\sigma})$$

и

$$dist(f, l_{\boldsymbol{\sigma},1}) = 2^{n-1} + 0.5 \cdot W_f(\boldsymbol{\sigma}).$$

Нелинейностью функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется число

$$N_f = dist(f, P_2^{аф}(n)).$$

Известно, что для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$:

1) $N_f = 2^{n-1} - 0.5 \cdot \max\limits_{\boldsymbol{\sigma} \in \mathbf{E}^n} |W_f(\boldsymbol{\sigma})|$;

2) $N_f \le 2^{n-1} - 2^{0.5 \cdot n - 1}$;

3) если существуют такие $k \in \{1, \ldots, n-1\}$ и $s \in \mathsf{S}(n)$, что

$$f(x_1, \ldots, x_n) = h(x_{s(1)}, \ldots, x_{s(k)}) \oplus g(x_{s(k+1)}, \ldots, x_{s(n)}),$$

то

$$N_f \ge 2^{n-k} \cdot N_h + 2^k \cdot N_g - 2 \cdot N_h \cdot N_g.$$

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ называется *максимально-нелинейной*, если ее нелинейность N_f достигает максимального значения, т.е.

$$\max_{\boldsymbol{\sigma} \in \mathbf{E}^n} |W_f(\boldsymbol{\sigma})| = \min_{g \in P_2(n)} \max_{\boldsymbol{\sigma} \in \mathbf{E}^n} |W_g(\boldsymbol{\sigma})|.$$

Максимально-нелинейные функции являются *экстремальными* в том смысле, что они наиболее удалены от множества аффинных функций (такие функции называются *глубокими дырами*). Именно по этой причине они представляют особый интерес при построении криптографических отображений.

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ называется *бент-функцией*, если все ее коэффициенты Уолша-Адамара равны $\pm 2^{0.5 \cdot n}$. Обозначим через $P_2^{\textit{бф}}(n)$ $(n \in \mathbf{N})$ множество всех бент-функций $f \in P_2(n)$. Ясно, что:

1) $P_2^{\textit{бф}}(n) \ne \varnothing$ $(n \in \mathbf{N})$ тогда и только тогда, когда n – четное число;

2) при четном значении числа $n \in \mathbf{N}$ множество $P_2^{\textit{бф}}(n)$ совпадает с множеством максимально-нелинейных функций $f \in P_2(n)$.

Пространством k-нелинейности $(k < \deg f)$ функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется подпространство

$$\mathbf{L}_f^{(k)} = \{\boldsymbol{\sigma} \in \mathbf{E}^n \mid \deg D_{\boldsymbol{\sigma}} f(\mathbf{x}) \le k\},$$

где $D_{\boldsymbol{\sigma}} f$ – (*булева*) *производная функции* f *по направлению* $\boldsymbol{\sigma}$ определяется равенством

$$(D_{\boldsymbol{\sigma}} f)(\mathbf{x}) = f(\mathbf{x} \oplus \boldsymbol{\sigma}) \oplus f(\mathbf{x}).$$

Пространство

$$\mathbf{L}_f = \mathbf{L}_f^{(0)} \quad (f \in P_2(n))$$

называется *пространством линейных трансляторов* функции f. Для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$:

1) если $\mathbf{L}_f^{(k)} \ne \mathbf{L}_f^{(k-1)}$, то $\dim \mathbf{L}_f^{(k)} \ge \dim \mathbf{L}_f^{(k-1)} + k + 1$;

2) $\mathbf{L}_f^{(0)} \subseteq \mathbf{L}_f^{(1)} \subseteq \ldots \subseteq \mathbf{L}_f^{(\deg f - 1)} = \mathbf{E}^n$.

Отображением, ассоциированным с функцией $f \in P_2(n)$ $(n \in \mathbf{N})$, называется функция $q_f : \mathbf{E}^n \times \mathbf{E}^n \to \mathbf{E}$, определенная равенством

$$q_f(\mathbf{u}, \mathbf{v}) = D_{\mathbf{u}} D_{\mathbf{v}} f(\mathbf{0}).$$

Подпространство

$$\ker f = \{\mathbf{u} \in \mathbf{E}^n \mid q_f(\mathbf{u}, \mathbf{v}) = 0 \text{ для всех } \mathbf{v} \in \mathbf{E}^n\}$$

называется *ядром* отображения q_f. Отметим, что $\ker f = \mathbf{L}_f$ для всех $f \in P_2(n)$ $(n \in \mathbf{N})$.

Взаимная корреляция между функциями $f, g \in P_2(n)$ $(n \in \mathbf{N})$ – это функция $\Delta_{f,g} : \mathbf{E}^n \to \mathbf{Z}$, определенная равенством

$$\Delta_{f,g}(\mathbf{x}) = \sum_{\boldsymbol{\sigma} \in \mathbf{E}^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \boldsymbol{\sigma})}.$$

Известно, что для любых функций $f, g \in P_2(n)$ $(n \in \mathbf{N})$:

1) $\Delta_{f,g}(\boldsymbol{\sigma}) = \Delta_{g,f}(\boldsymbol{\sigma})$ для всех $\boldsymbol{\sigma} \in \mathbf{E}^n$;

2) $\sum_{\boldsymbol{\sigma} \in \mathbf{E}^n} \Delta^2_{f,g}(\boldsymbol{\sigma}) \le 2^{3 \cdot n}$;

3) $\sum_{\boldsymbol{\sigma} \in \mathbf{V}} \Delta_{f,g}(\boldsymbol{\sigma}) = 2^{-\dim \mathbf{V}^\perp} \cdot \sum_{\boldsymbol{\sigma} \in \mathbf{V}^\perp} W_f(\boldsymbol{\sigma}) \cdot W_g(\boldsymbol{\sigma})$ для любого подпространства $\mathbf{V}$ линейного пространства $\mathbf{GF}^n(2)$;

4) $\Delta_{f,g}(\mathbf{0}) = 2^{-n} \cdot \sum_{\boldsymbol{\sigma} \in \mathbf{E}^n} W_f(\boldsymbol{\sigma}) \cdot W_g(\boldsymbol{\sigma})$;

5) $N\Delta_{f,g} \cdot NW_{f,g} \ge |\max_{\boldsymbol{\sigma} \in \mathbf{E}^n} \Delta_{f,g}(\boldsymbol{\sigma})|$, где

$$N\Delta_{f,g} = |\{\boldsymbol{\sigma} \in \mathbf{E}^n \mid \Delta_{f,g}(\boldsymbol{\sigma}) \ne 0\}|$$

и

$$NW_{f,g} = |\{\boldsymbol{\sigma} \in \mathbf{E}^n \mid W_f(\boldsymbol{\sigma}) \cdot W_g(\boldsymbol{\sigma}) \ne 0\}|;$$

6) $(\Delta_{f,g}(\mathbf{0}), \ldots, \Delta_{f,g}(\mathbf{1})) \cdot H_n = (W_f(\mathbf{0}) \cdot W_g(\mathbf{0}), \ldots, W_f(\mathbf{1}) \cdot W_g(\mathbf{1}))$;

7) $2^n \cdot (\Delta_{f,g}(\mathbf{0}), \ldots, \Delta_{f,g}(\mathbf{1})) = (W_f(\mathbf{0}) \cdot W_g(\mathbf{0}), \ldots, W_f(\mathbf{1}) \cdot W_g(\mathbf{1})) \cdot H_n$.

Функции $f, g \in P_2(n)$ $(n \in \mathbf{N})$ называются:

1) *совершенно некоррелированными*, если $\Delta_{f,g}(\boldsymbol{\sigma}) = 0$ для всех $\boldsymbol{\sigma} \in \mathbf{E}^n$;

2) *некоррелированными порядка* k $(0 \le k \le n)$, если $\Delta_{f,g}(\boldsymbol{\sigma}) = 0$ для всех таких $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n$, что $wt(\boldsymbol{\sigma}) \le k$.

Ясно, что функции $f, g \in P_2(n)$ $(n \in \mathbf{N})$ имеют непересекающиеся спектры тогда и только тогда, когда они совершенно некоррелированы.

Автокорреляцией функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется функция

$$\Delta_f(\mathbf{x}) = \Delta_{f,f}(\mathbf{x}) \quad (\mathbf{x} \in \mathbf{E}^n).$$

Известно, что для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$:

1) $(\Delta_f(\mathbf{0}),\ldots,\Delta_f(\mathbf{1}))\cdot H_n = (W_f^2(\mathbf{0}),\ldots,W_f^2(\mathbf{1}))$;

2) $\Delta_f(\boldsymbol{\sigma}) = W_{D_\sigma f}(\mathbf{0})$ $(\boldsymbol{\sigma} \in \mathbf{E}^n)$;

3) если $n = 2\cdot k$ $(k \in \mathbf{N})$, то функция $f \in P_2(n)$ является бент-функций тогда и только тогда, когда

$$\max_{\boldsymbol{\sigma}\in\mathbf{E}^n} |\Delta_f(\boldsymbol{\sigma})| = 0;$$

4) если $n = 2\cdot k$ $(k \in \mathbf{N})$, то бент-функций является любая функция $f \in P_2(n)$, определенная равенством

$$f(\mathbf{x},\mathbf{y}) = <\tau(\mathbf{y}),\mathbf{x}> \oplus g(\mathbf{y}) \quad (\mathbf{x},\mathbf{y} \in \mathbf{E}^n)$$

где $\tau \in \mathsf{S}(\mathbf{E}^n)$, а $g \in P_2(n)$.

5) если существуют такие $k \in \{1,\ldots,n-1\}$ и $s \in \mathsf{S}(n)$, что

$$f(x_1,\ldots,x_n) = h(x_{s(1)},\ldots,x_{s(k)}) \oplus g(x_{s(k+1)},\ldots,x_{s(n)}),$$

то для всех $(\sigma_1,\ldots,\sigma_n) \in \mathbf{E}^n$

$$\Delta_f(\sigma_1,\ldots,\sigma_n) = \Delta_h(\sigma_{s(1)},\ldots,\sigma_{s(k)})\cdot\Delta_g(\sigma_{s(k+1)},\ldots,\sigma_{s(n)});$$

6) $N\Delta_f \cdot NW_f \geq 2^n$;

Значение последнего неравенства состоит в том, что невозможно одновременно обеспечить небольшое количество нулей функции автокорреляции и небольшое количество нулей в спектре функции $f \in P_2(n)$ $(n \in \mathbf{N})$.

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ называется *частично максимально-нелинейной*, если

$$N\Delta_f \cdot NW_f = 2^n.$$

Множество всех частично максимально-нелинейных функций $f \in P_2(n)$ $(n \in \mathbf{N})$ характеризуется тем, что оно содержит множество всех аффинных функций, множество всех квадратичных функций, а также множество всех максимально-нелинейных функций, принадлежащих множеству $P_2(n)$.

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ – *корреляционно-иммунная* порядка k $(1 \leq k \leq n)$, если

$$wt(f^{\sigma_1,\ldots,\sigma_k}_{i_1,\ldots,i_k}) = 2^{-k}\cdot wt(f).$$

Уравновешенная корреляционно-иммунная порядка k $(1 \leq k \leq n)$ функция называется *k-устойчивой*.

Свойство функции $f \in P_2(n)$ $(n \in \mathbf{N})$ быть «корреляционно-иммунной функцией» означает, что в известном значении функции отсутствует какая-либо информация о значениях некоторого подмножества ее аргументов или о значениях некоторых функций от ее аргументов. Отсюда вытекает, что корреляционно-иммунные функции способны противостоять корреля-

ционным методам их анализа. Поэтому такие функции являются привлекательными при построении криптографических отображений.

Функция $f \in P_2(n)$ $(n \in \mathbf{N})$ удовлетворяет:

1) *критерию SAC*, если $D_{\boldsymbol{\sigma}} f$ – уравновешенная функция для любого такого набора $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n$, что $wt(\boldsymbol{\sigma}) = 1$;

2) *критерию SAC*(k) $(1 \le k < n)$, если $f_{i_1,\ldots,i_k}^{\sigma_1,\ldots,\sigma_k}$ удовлетворяет критерию *SAC* для любого набора $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_k) \in \mathbf{E}^k$ $(1 \le i_1 < \ldots < i_k \le n)$;

3) *критерию PC*(k) $(1 \le k < n)$, если $D_{\boldsymbol{\sigma}} f$ – уравновешенная функция для любого такого набора $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \mathbf{E}^n$, что $1 \le wt(\boldsymbol{\sigma}) \le k$.

Обобщим введенные выше понятия на множество булевых вектор-функций.

Пусть $P_2(n,m)$ $(n,m \in \mathbf{N})$ – множество всех отображений $\mathbf{f} : \mathbf{E}^n \to \mathbf{E}^m$.

Нелинейностью отображения $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n,m)$ $(n,m \in \mathbf{N})$ называется число $N_{\mathbf{f}}$, равное минимальной из нелинейностей функций

$$f(\mathbf{x}) = \bigoplus_{i=1}^{m} c_i \cdot f_i(\mathbf{x}),$$

где минимум берется по всем векторам $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbf{E}^m \setminus \{\mathbf{0}\}$.

Отображение $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n,m)$ $(n,m \in \mathbf{N})$ называется:

1) *уравновешенным*, если

$$|\{\boldsymbol{\sigma} \in \mathbf{E}^n \mid \mathbf{f}(\boldsymbol{\sigma}) = \boldsymbol{\alpha}\}| = 2^{n-m}$$

для любого $\boldsymbol{\alpha} \in \mathbf{E}^m$;

2) (n,m,k)*-устойчивым*, если отображение

$$\tilde{\mathbf{f}} = ((f_1)_{i_1,\ldots,i_k}^{\sigma_1,\ldots,\sigma_k}, \ldots, (f_m)_{i_1,\ldots,i_k}^{\sigma_1,\ldots,\sigma_k})$$

является уравновешенным для любого набора $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_k) \in \mathbf{E}^k$ $(1 \le i_1 < \ldots < i_k \le n)$;

3) *отображением с линейной структурой*, если существует такой вектор $\boldsymbol{\sigma} \in \mathbf{E}^n \setminus \{\mathbf{0}\}$, что

$$D_{\boldsymbol{\sigma}} \mathbf{f}(\boldsymbol{\alpha}) = const$$

для всех $\boldsymbol{\alpha} \in \mathbf{E}^n$ (вектор $\boldsymbol{\sigma}$ называется *линейным транслятором* отображения $\mathbf{f}$, а подпространство $\mathbf{L}_{\mathbf{f}} = \{\boldsymbol{\sigma} \in \mathbf{E}^n \mid D_{\boldsymbol{\sigma}} \mathbf{F} \equiv const\}$ – *подпространством линейности* отображения $\mathbf{f}$).

Отметим, что для отображения $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n,m)$ $(n,m \in \mathbf{N})$:

1) вектор $\boldsymbol{\sigma} \in \mathbf{E}^n \setminus \{\mathbf{0}\}$ является линейным транслятором тогда и только тогда, когда

$$|\Delta_{f_i}(\boldsymbol{\sigma})| = 2^n$$

для всех $i = 1, \ldots, n$;

2) $\dim \mathbf{L}_{\mathbf{F}} = k$ $(1 \le k \le n)$ тогда и только тогда, когда существуют такие $s \in \mathrm{S}(n)$, отображение $\tilde{\mathbf{F}} \in P_2(n-k, m)$, не обладающее линейной структурой, и невырожденная $n \times n$-матрица A над полем $\mathbf{GF}(2)$, что

$$\mathbf{f}(A \circ \mathbf{x}^T) = \bigoplus_{i=1}^{k} \mathbf{a}_i \cdot x_{s(i)} \oplus \tilde{\mathbf{f}}(x_{s(i+1)}, \ldots, x_{s(n)}),$$

где $\mathbf{a}_i \in \mathbf{E}^n$ $(i = 1, \ldots, k)$.

Обозначим через $P_2^{аф}(n, m)$ и $P_2^{лин}(n, m)$ множество, соответственно, всех аффинных и множество всех линейных отображений $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n, m)$. Отметим, что любое отображение $\mathbf{f} \in P_2^{аф}(n, m)$ может быть представлено в виде $\mathbf{f}(\mathbf{x}) = A \circ \mathbf{x}^T \oplus \mathbf{b}$, а любое отображение $\mathbf{f} \in P_2^{лин}(n, m)$ – в виде $\mathbf{f}(\mathbf{x}) = A \circ \mathbf{x}^T$, где A – $m \times n$-матрица над полем $\mathbf{GF}(2)$, $\mathbf{b} = (\beta_1, \ldots, \beta_n) \in \mathbf{E}^m$, а $\mathbf{x} = (x_1, \ldots, x_n)$.

Стандартным приемом построения криптографических нелинейных отображений является *неравномерное движение*. Этот метод основан на конструировании нелинейного отображения из заданного семейства аффинных отображений, и состоит в следующем. Зафиксируем линейное отображение $\mathbf{h} \in P_2^{лин}(n, k)$ $(n, k \in \mathbf{N})$ и семейство аффинных отображений $\mathbf{g}_{\boldsymbol{\sigma}} \in P_2^{аф}(n, m)$ $(\boldsymbol{\sigma} \in \mathbf{E}^k)$. Определим отображение $\mathbf{f} \in P_2(n, m)$ равенством

$$\mathbf{f}(\mathbf{x}) = \mathbf{g}_{\mathbf{h}(\mathbf{x})}(\mathbf{x}) \quad (\mathbf{x} \in \mathbf{E}^n). \tag{1.67}$$

Это отображение называется *линейным разветвлением* с *разветвляющим пространством* $\mathbf{E}^k$ и *разветвляющим отображением* $\mathbf{h}$, а отображения $\mathbf{g}_{\boldsymbol{\sigma}}$ $(\boldsymbol{\sigma} \in \mathbf{E}^k)$ – *разветвляемыми отображениями*. *Индексом линейности* отображения $\mathbf{f}$ называется число $ill(\mathbf{f})$, равное минимальной размерности k разветвляющего пространства среди всех возможных представлений отображения $\mathbf{f}$ в виде (1.67).

Отметим, что число $ill(\mathbf{f})$ характеризует «удаленность» отображения $\mathbf{f}$ от множества $P_2^{аф}(n, m)$.

Известно, что:

1) $\deg f \le ill(f) + 1$ для любой функции $f \in P_2(n)$ $(n \in \mathbf{N})$;

2) $ill(f) \le k$ $(f \in P_2(n))$ тогда и только тогда, когда существуют $s \in \mathrm{S}(n)$ и такая аффинная замена переменных, что функция f может быть представлена в виде

$$f(x_{s(1)}, \ldots, x_{s(n-k)}, y_1, \ldots, y_k) = \bigoplus_{i=1}^{n-k} g_i(y_1, \ldots, y_k) \cdot x_{s(i)} \oplus \tilde{f}(y_1, \ldots, y_k). \tag{1.68}$$

Ясно, что равенство (1.68) может быть переписано в виде

$$f(\mathbf{x}, \mathbf{y}) = <\mathbf{x}, \mathbf{g}(\mathbf{y})> \oplus \tilde{f}(\mathbf{y}). \tag{1.69}$$

Если функция $f \in P_2(n)$ $(n \in \mathbf{N})$ может быть представлена в виде (1.69), то говорят, что функция f может быть задана в виде *линейного разветвления*. Известно, что если истинно равенство (1.69), то для всех $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbf{E}^{n-k} \times \mathbf{E}^k$:

1) $W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2^k \cdot \sum\limits_{\boldsymbol{\sigma} \in \mathbf{g}^{-1}(\boldsymbol{\alpha})} (-1)^{\tilde{f}(\boldsymbol{\sigma}) \oplus <\boldsymbol{\sigma}, \boldsymbol{\beta}>}$;

2) $2^k \cdot \sqrt{|\mathbf{g}^{-1}(\boldsymbol{\alpha})|} \le \max\limits_{\boldsymbol{\beta} \in \mathbf{E}^k} |W_f(\boldsymbol{\alpha}, \boldsymbol{\beta})| \le 2^k \cdot |\mathbf{g}^{-1}(\boldsymbol{\alpha})|$.

В процессе построения криптографических отображений $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n, m)$ $(n, m \in \mathbf{N})$ важную роль играют группы преобразований линейного пространства $\mathbf{E}^n$. Пусть $\mathsf{G}_{\mathbf{E}^n} = (G_{\mathbf{E}^n}, \lozenge)$ – группа всех преобразований пространства $\mathbf{E}^n$, где $\lozenge$ – операция суперпозиции. Известно, что $|G_{\mathbf{E}^n}| = (2^n)!$.

Рассмотренные выше конструкции показывают, что при классификации криптографических отображений $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n, m)$ $(n, m \in \mathbf{N})$ часто используются следующие подгруппы группы $\mathsf{G}_{\mathbf{E}^n}$:

1. *Группа сдвигов* $\mathsf{J}_n = (G_{\mathsf{J}_n}, \lozenge)$, где

$$G_{\mathsf{J}_n} = \{\mathbf{g}_{\boldsymbol{\alpha}}(x_1, \ldots, x_n) = (x_1 \oplus \alpha_1, \ldots, x_n \oplus \alpha_n) \mid \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n\}.$$

Ясно, что

$$|G_{\mathsf{J}_n}| = 2^n.$$

2. *Группа перестановок переменных* $\mathsf{G}_n = (G_{\mathsf{G}_n}, \lozenge)$, где

$$G_{\mathsf{G}_n} = \{\mathbf{g}_s(x_1, \ldots, x_n) = (x_{s(1)}, \ldots, x_{s(n)}) \mid s \in \mathsf{S}(n)\}.$$

Ясно, что

$$|G_{\mathsf{G}_n}| = n!.$$

3. *Группа Джевонса* $\mathsf{D}_n = (G_{\mathsf{D}_n}, \lozenge)$, где

$$G_{\mathsf{D}_n} = \{\mathbf{g}_{\boldsymbol{\alpha}, s}(x_1, \ldots, x_n) =$$

$$= (x_{s(1)} \oplus \alpha_1, \ldots, x_{s(n)} \oplus \alpha_n) \mid \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n, s \in \mathsf{S}(n)\}.$$

Ясно, что

$$|G_{\mathsf{D}_n}| = 2^n \cdot n!.$$

4. *Полная линейная группа* $\mathsf{GL}(\mathbf{E}^n) = (G_{\mathsf{GL}(\mathbf{E}^n)}, \lozenge)$, где

$$G_{\mathsf{GL}(\mathbf{E}^n)} = \{\mathbf{g}_A(\mathbf{x}) = A \circ \mathbf{x}^T \mid A - \textit{невырожденная булева} \quad n \times n - \textit{матрица}\}.$$

Известно, что

$$|G_{\mathsf{GL}(\mathbf{E}^n)}| = \prod_{i=0}^{n-1} (2^n - 2^i).$$

5. *Полная аффинная группа* $\mathsf{GA}(\mathbf{E}^n) = (G_{\mathsf{GA}(\mathbf{E}^n)}, \lozenge)$, где

$$G_{\mathsf{GA}(\mathbf{E}^n)} = \{\mathbf{g}_{A,\mathbf{a}}(\mathbf{x}) =$$

$$= A \circ \mathbf{x}^T \oplus \mathbf{a} \mid A - \textit{невырожденная булева } n \times n - \textit{матрица}, \ \mathbf{a} \in \mathbf{E}^n\}.$$

Ясно, что

$$|G_{\mathsf{GL}(\mathbf{E}^n)}| = 2^n \cdot \prod_{i=0}^{n-1}(2^n - 2^i).$$

Следующий пример показывает, что значение группы $\mathsf{G}_{\mathbf{E}^n} = (G_{\mathbf{E}^n}, \lozenge)$ и ее подгрупп при анализе свойств отображений $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n,m)$ $(n,m \in \mathbf{N})$ определяется еще и тем, что на основании подхода, систематически изложенного в [167], график отображения $\mathbf{f}$ может быть представлен в виде объединения подпространств линейного пространства $\mathbf{E}^{n+m}$.

Пример 1.8. Определим *график* отображения $\mathbf{f} = (f_1, \ldots, f_m) \in P_2(n,m)$ $(n,m \in \mathbf{N})$ равенством

$$graph\,\mathbf{f} = \{(\alpha_1, \ldots, \alpha_{m+n}) \in \mathbf{E}^{n+m} \mid \mathbf{f}(\alpha_1, \ldots, \alpha_n) = (\alpha_{n+1}, \ldots, \alpha_{n+m})\}.$$

Множество $graph\,\mathbf{f}$, как и любое функциональное отношение, обладает следующим свойством: если $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n+m}) \in graph\,\mathbf{f}$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{n+m}) \in graph\,\mathbf{f}$ и $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, то существует такое $j \in \{1, \ldots, n\}$, что $\alpha_j \neq \beta_j$.

Линейной характеристической функцией множества $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ назовем множество

$$\chi_{\mathbf{f}} = \{M_i \mid i = 1, \ldots, k\}$$

таких $(n+m) \times (n+m)$-матриц над полем $\mathbf{GF}(2)$, что для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m}$ равенство

$$\boldsymbol{\sigma} \circ M_i = \mathbf{0},$$

истинно хотя бы для одного значения $i \in \{1, \ldots, k\}$ тогда и только тогда, когда $\boldsymbol{\sigma} \in graph\,\mathbf{f}$.

Положим

$$\chi_{\mathbf{f}}(\boldsymbol{\sigma}) = \{\boldsymbol{\sigma} \circ M_i \mid i = 1, \ldots, k\} \quad (\boldsymbol{\sigma} \in \mathbf{E}^{n+m}).$$

Таким образом,

$$\boldsymbol{\sigma} \in graph\,\mathbf{f} \Leftrightarrow \mathbf{0} \in \chi_{\mathbf{f}}(\boldsymbol{\sigma}) \quad (\boldsymbol{\sigma} \in \mathbf{E}^{n+m}, \mathbf{f} \in P_2(n,m)).$$

Охарактеризуем структуру множества $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$.

Утверждение 1.3. Для любого отображения $\mathbf{f} \in P_2(n,m)$ $(n,m \in \mathbf{N})$ число линейно независимых векторов, принадлежащих множеству $graph\,\mathbf{f}$, не меньше, чем n.

Доказательство. Для любого отображения $\mathbf{f} \in P_2(n,m)$ $(n,m \in \mathbf{N})$ множество $graph\,\mathbf{f}$ содержит элементы

$$\mathbf{e}_i = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, 1, \underbrace{0, \ldots, 0}_{n-i \text{ раз}}, \beta_1, \ldots, \beta_m) \quad (i = 1, \ldots, n), \tag{1.70}$$

где

$$f(\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{n-i\ раз}) = (\beta_1,\ldots,\beta_m).$$

Векторы $\mathbf{e}_1,\ldots,\mathbf{e}_n$ - линейно независимые и их число равно n.

Утверждение доказано.

Пусть $P_2^{(0)}(n)$ $(n \in \mathbf{N})$ – множество всех функций $f \in P_2(n)$, сохраняющих константу 0.

Теорема 1.22. Множество $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ является подпространством линейного пространства $\mathbf{E}^{n+m}$ тогда и только тогда, когда $\mathbf{f} \in (P_2^{(0)}(n) \cap P_2^{лин}(n))^m$.

Доказательство. Множество $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ является подпространством линейного пространства $\mathbf{E}^{n+m}$ тогда и только тогда, когда

$$\mathbf{0} \in graph\,\mathbf{f} \tag{1.71}$$

и

$$\begin{array}{l}(\alpha_1,\ldots,\alpha_{n+m}),(\beta_1,\ldots,\beta_{n+m}) \in graph\,\mathbf{f} \Rightarrow \\ \Rightarrow (\alpha_1 \oplus \beta_1,\ldots,\alpha_{n+m} \oplus \beta_{n+m}) \in graph\,\mathbf{f}\end{array}. \tag{1.72}$$

Соотношение (1.71) эквивалентно равенству $\mathbf{f}(\mathbf{0}) = \mathbf{0}$, которое истинно тогда и только тогда, когда $pr_j\mathbf{f} \in P_2^{(0)}(n)$ для всех $j = 1,\ldots,m$.

Соотношение (1.72) эквивалентно тому, что для всех $(\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n) \in \mathbf{E}^n$

$$pr_j\mathbf{f}(\alpha_1,\ldots\alpha_n) \oplus pr_j\mathbf{f}(\beta_1,\ldots\beta_n) = pr_j\mathbf{f}(\alpha_1 \oplus \beta_1,\ldots,\alpha_n \oplus \beta_n) \quad (j = 1,\ldots,m),$$

т.е. $pr_j\mathbf{f} \in P_2^{лин}(n)$ для всех $j = 1,\ldots,m$.

Итак, множество $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ является подпространством линейного пространства $\mathbf{E}^{n+m}$ тогда и только тогда, когда $pr_j\mathbf{f} \in P_2^{(0)}(n) \cap P_2^{лин}(n)$ для всех $j = 1,\ldots,m$, т.е. когда $\mathbf{f} \in (P_2^{(0)}(n) \cap P_2^{лин}(n))^m$.

Теорема доказана.

Следствие 1.7. Множество $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ является подпространством линейного пространства $\mathbf{E}^{n+m}$ тогда и только тогда, когда $pr_j\mathbf{f} = x_{j1} \oplus \ldots \oplus x_{jr_j}$ для всех $j = 1,\ldots,m$.

Доказательство. Так как

$$P_2^{(\mathbf{0})}(n,m) = (P_2^{(0)}(n))^m = \{\mathbf{f} \in P_2(n,m) \mid \mathbf{f}(\mathbf{0}) = \mathbf{0}\}$$

и

$$P_2^{лин}(n,m) =$$

$$= \{\mathbf{f} \in P_2(n.m) \mid pr_j\,\mathbf{f} = \alpha_j \oplus x_{j1} \oplus \ldots \oplus x_{jr_j}\ \ (\alpha_j \in \mathbf{E})\ \textit{для всех}\ \ j = 1,\ldots,m\},$$

то

$$(P_2^{(0)}(n) \cap P_2^{лин}(n))^m = (P_2^{(0)}(n))^m \cap (P_2^{лин}(n))^m =$$

$$= \{\mathbf{f} \in P_2(n,m) \mid pr_j\,\mathbf{f} = x_{j1} \oplus \ldots \oplus x_{jr_j}\ \ \textit{для всех}\ \ j = 1,\ldots,m\}.$$

Следствие доказано.

Утверждение 1.4. Если множество $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ является подпространством линейного пространства $\mathbf{E}^{n+m}$, то $\dim graph\,\mathbf{f} = n$ и $\dim(graph\,\mathbf{f})^{\perp} = m$.

Доказательство. Пусть $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ – подпространство линейного пространства $\mathbf{E}^{n+m}$. Достаточно доказать, что $\dim graph\,\mathbf{f} = n$.

Из утверждения 1.3 вытекает, что $\dim graph\,\mathbf{f} \geq n$. Покажем, что векторы $\mathbf{e}_1,\ldots,\mathbf{e}_n$, определяемые равенствами (1.70), образуют базис пространства $graph\,\mathbf{f}$. Выберем произвольный вектор

$$\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n,\gamma_1,\ldots,\gamma_m) \in graph\,\mathbf{f}.$$

Пусть среди его первых n компонент ненулевыми будут те, и только те компоненты, которые имеют номера $j_1,\ldots,j_r$ $(1 \leq j_1 < \ldots < j_r \leq n)$. Рассмотрим вектор

$$\boldsymbol{\beta} = \mathbf{e}_{j_1} \oplus \ldots \oplus \mathbf{e}_{j_r} = (\alpha_1,\ldots,\alpha_n,\delta_1,\ldots,\delta_m).$$

Так как $\boldsymbol{\alpha},\boldsymbol{\beta} \in graph\,\mathbf{f}$ и $graph\,\mathbf{f}$ – линейное пространство, то

$$\boldsymbol{\alpha} \oplus \boldsymbol{\beta} = (\underbrace{0,\ldots,0}_{n\ раз},\gamma_1 \oplus \delta_1,\ldots,\gamma_m \oplus \delta_m) \in graph\,\mathbf{f}.$$

А так как (см. теорему 1.22) $\mathbf{f} \in (P_2^{(0)}(n))^m$, то $\gamma_j \oplus \delta_j = 0$ $(j = 1,\ldots,m)$, т.е. $\gamma_j = \delta_j$ $(j = 1,\ldots,m)$. Это означает, что $\boldsymbol{\alpha} \oplus \boldsymbol{\beta} = \mathbf{e}_{j_1} \oplus \ldots \oplus \mathbf{e}_{j_r}$.

Итак, показано, что любой вектор $\boldsymbol{\alpha} \in graph\,\mathbf{f}$ является линейной комбинацией линейно независимых векторов $\mathbf{e}_1,\ldots,\mathbf{e}_n$. Следовательно, векторы $\mathbf{e}_1,\ldots,\mathbf{e}_n$ образуют базис пространства $graph\,\mathbf{f}$. Отсюда вытекает, что $\dim graph\,\mathbf{f} = n$.

Утверждение доказано.

Обозначим через $\mathbf{Lin}(graph\,\mathbf{f})$ $(\mathbf{f} \in P_2(n,m))$ множество всех максимальных по включению подпространств линейного пространства $\mathbf{E}^{n+m}$, содержащихся во множестве $graph\,\mathbf{f}$.

Теорема 1.23. $\mathbf{Lin}(graph\,\mathbf{f}) \neq \varnothing$ $(\mathbf{f} \in P_2(n,m))$ тогда и только тогда, когда $\mathbf{f} \in (P_2^{(0)}(n))^m$.

Доказательство. Пусть $\mathbf{f} \notin (P_2^{(0)}(n))^m$. Тогда $\mathbf{0} \notin graph\,\mathbf{f}$. Следовательно, ни одно подпространство линейного пространства $\mathbf{E}^{n+m}$ не содержится во множестве $graph\,\mathbf{f}$, т.е. $\mathbf{Lin}(graph\,\mathbf{f}) = \varnothing$.

Для дальнейшего доказательства нам понадобится следующая лемма.

Лемма 1.3. Для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m} \setminus \{\mathbf{0}\}$ множество $\mathbf{V} = \{\mathbf{0},\boldsymbol{\sigma}\}$ – подпространство линейного пространства $\mathbf{E}^{n+m}$.

Доказательство. Так как $\mathbf{0} \in graph\,\mathbf{f}$, то условие (4.71) выполнено. А так как $\mathbf{0}+\mathbf{0}=\mathbf{0}$, $\mathbf{0} \oplus \boldsymbol{\sigma} = \boldsymbol{\sigma} \oplus \mathbf{0} = \boldsymbol{\sigma}$ и $\boldsymbol{\sigma} \oplus \boldsymbol{\sigma} = \mathbf{0}$, то выполнено и условие (1.72). Следовательно, $\mathbf{V} = \{\mathbf{0},\boldsymbol{\sigma}\}$ – подпространство линейного пространства $\mathbf{E}^{n+m}$.

Лемма доказана.

Пусть $\mathbf{f} \in (P_2^{(0)}(n))^m$. Тогда $\mathbf{0} \in graph\,\mathbf{f}$. Так как $|\,graph\,\mathbf{f}\,| = 2^n$, то существует ненулевой вектор $\boldsymbol{\sigma} \in graph\,\mathbf{f}$. Множество $\{\mathbf{0}, \boldsymbol{\sigma}\}$ – подпространство линейного пространства $\mathbf{E}^{n+m}$ и удовлетворяет включению $\{\mathbf{0}, \boldsymbol{\sigma}\} \subseteq graph\,\mathbf{f}$. Следовательно, существует максимальное по включению подпространство $\mathbf{V}$ линейного пространства $\mathbf{E}^{n+m}$, удовлетворяющее включениям $\{\mathbf{0}, \boldsymbol{\sigma}\} \subseteq \mathbf{V} \subseteq graph\,\mathbf{f}$.
Так как $\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})$, то $\mathbf{Lin}(graph\,\mathbf{f}) \neq \varnothing$.

Теорема доказана.

Таким образом, множество $\mathbf{Lin}(graph\,\mathbf{f})$ $(\mathbf{f} \in P_2(n,m))$ может быть использовано для исследования свойств множества $graph\,\mathbf{f}$ тогда и только тогда, когда $\mathbf{f} \in (P_2^{(0)}(n))^m$. Следующее утверждение показывает, что исследование множества $graph\,\mathbf{f}$ $(\mathbf{f} \in P_2(n,m))$ *всегда можно свести* к исследованию такого множества $graph\,\mathbf{g}$, что $\mathbf{g} \in (P_2^{(0)}(n))^m$.

Утверждение 1.5. Для каждого отображения $\mathbf{f} \in P_2(n,m)$ $(n,m \in \mathbf{N})$ существует единственный такой вектор $\boldsymbol{\sigma} \in \mathbf{E}^m$, что $\mathbf{g} \in (P_2^{(0)}(n))^m$, где функция $\mathbf{g}$ определена равенством $\mathbf{g}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) \oplus \boldsymbol{\sigma}$.

Доказательство. Пусть $\mathbf{f} \in P_2(n,m)$ $(n,m \in \mathbf{N})$ и $\mathbf{g}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) \oplus \boldsymbol{\sigma}$, где $\boldsymbol{\sigma} \in \mathbf{E}^m$. Соотношение $\mathbf{g} \in (P_2^{(0)}(n))^m$ истинно тогда и только тогда, когда $f(\mathbf{0}) \oplus \boldsymbol{\sigma} = \mathbf{0}$, т.е. когда $\boldsymbol{\sigma} = \mathbf{f}(\mathbf{0})$. Отсюда вытекает, что для любой функции $\mathbf{f} \in P_2(n,m)$ требуемый вектор $\boldsymbol{\sigma} \in \mathbf{E}^m$ существует и единственный.

Утверждение доказано.

Значение утверждения 1.5 состоит в следующем. Пусть $\mathbf{f} \notin (P_2^{(0)}(n))^m$ $(n,m \in \mathbf{N})$. Заменим множество $graph\,\mathbf{f}$ множеством $graph\,\mathbf{g}$, где $\mathbf{g}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) \oplus \mathbf{f}(\mathbf{0})$. Исследуем множество $graph\,\mathbf{g}$ в терминах множества $\mathbf{Lin}(graph\,\mathbf{g})$. Из построения отображения $\mathbf{g}$ вытекает, что множество $graph\,\mathbf{g}$ – это результат *сдвига* множества $graph\,\mathbf{f}$ на вектор $\mathbf{f}(\mathbf{0})$. Указанная биекция дает возможность переформулировать любое утверждение относительно множества $graph\,\mathbf{g}$ в соответствующее утверждение относительно множества $graph\,\mathbf{f}$.

Теорема 1.24. Для любого отображения $\mathbf{f} \in (P_2^{(0)}(n))^m$ $(n,m \in \mathbf{N})$ истинно равенство

$$graph\,\mathbf{f} = \bigcup_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V}. \tag{1.73}$$

Доказательство. Пусть $\mathbf{f} \in (P_2^{(0)}(n))^m$ $(n,m \in \mathbf{N})$. Так как $\mathbf{V} \subseteq graph\,\mathbf{f}$ для любого подпространства $\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})$, то истинно включение

$$graph\,\mathbf{f} \supseteq \bigcup_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V}. \tag{1.74}$$

Докажем, что истинно обратное включение

$$graph\,\mathbf{f} \subseteq \bigcup_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V}. \tag{1.75}$$

Пусть $\boldsymbol{\sigma} \in graph\,\mathbf{f}$. Возможны два случая.

1. Предположим, что $\boldsymbol{\sigma} = \mathbf{0}$. Так как вектор $\mathbf{0}$ является элементом любого подпространства линейного пространства $\mathbf{E}^{n+m}$ и $\mathbf{Lin}(graph\,\mathbf{f}) \neq \varnothing$, то $\mathbf{0} \in \bigcup\limits_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V}$.

2. Предположим, что $\boldsymbol{\sigma} \in graph\,\mathbf{f} \setminus \{\mathbf{0}\}$. В силу леммы 1.3 множество $\{\mathbf{0}, \boldsymbol{\sigma}\}$ – подпространство линейного пространства $\mathbf{E}^{n+m}$. Следовательно, существует максимальное по включению подпространство $\mathbf{V}$ линейного пространства $\mathbf{E}^{n+m}$, удовлетворяющее включениям $\{\mathbf{0}, \boldsymbol{\sigma}\} \subseteq \mathbf{V} \subseteq graph\,\mathbf{f}$. Так как $\boldsymbol{\sigma} \in \mathbf{V}$ и $\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})$, то

$$\boldsymbol{\sigma} \in \bigcup_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V}.$$

Итак, показано, что включение (1.75) – истинное.

Из включений (1.74) и (1.75) вытекает, что истинно равенство (1.73).

Теорема доказана.

Пусть $\mathbf{V}$ - подпространство линейного пространства $\mathbf{E}^{n+m}$, а $\mathbf{e}_1, \ldots, \mathbf{e}_{n+m-\dim \mathbf{V}}$ – базис подпространства $\mathbf{V}^{\perp}$. Обозначим через $E_{\mathbf{V}}$ матрицу порядка $(n+m) \times (n+m-\dim V)$, столбцы которой – это векторы $\mathbf{e}_1, \ldots, \mathbf{e}_{n+m-\dim \mathbf{V}}$.

Теорема 1.25. Для любого отображения $\mathbf{f} \in (P_2^{(0)}(n))^m$ $(n, m \in \mathbf{N})$ линейной характеристической функцией множества $graph\,\mathbf{f}$ является множество матриц

$$\chi_{\mathbf{f}} = \{E_{\mathbf{V}} \mid \mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})\}. \tag{1.76}$$

Доказательство. Пусть $\mathbf{f} \in (P_2^{(0)}(n))^m$ $(n, m \in \mathbf{N})$ и множество матриц $\chi_{\mathbf{f}}$ построено в соответствии с равенством (1.76). Тогда для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m}$

$$\mathbf{0} \in \chi_{\mathbf{f}}(\boldsymbol{\sigma}) \Leftrightarrow (\exists \mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f}))(\boldsymbol{\sigma} \circ E_{\mathbf{V}} = \mathbf{0}). \tag{1.77}$$

По построению, столбцы матрицы $E_{\mathbf{V}}$ образуют базис подпространства $\mathbf{V}^{\perp}$. Следовательно, для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m}$

$$\boldsymbol{\sigma} \circ E_{\mathbf{V}} = \mathbf{0} \Leftrightarrow \boldsymbol{\sigma} \in \mathbf{V}. \tag{1.78}$$

Из (1.77) и (1.78) вытекает, что для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m}$

$$\mathbf{0} \in \chi_{\mathbf{f}}(\boldsymbol{\sigma}) \Leftrightarrow (\exists \mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f}))(\boldsymbol{\sigma} \in \mathbf{V}). \tag{1.79}$$

По условию, $\mathbf{f} \in (P_2^{(0)}(n))^m$. Из теоремы 1.24 и из (1.79) вытекает, что для любого вектора $\boldsymbol{\sigma} \in \mathbf{E}^{n+m}$

$$\mathbf{0} \in \chi_{\mathbf{f}}(\boldsymbol{\sigma}) \Leftrightarrow \boldsymbol{\sigma} \in graph\,\mathbf{f}. \tag{1.80}$$

Из (1.80) вытекает, что $\chi_{\mathbf{f}}$ – линейная характеристическая функция множества $graph\,\mathbf{f}$.

Теорема доказана.

Результаты, представленные в примере 1.8 показывают, что при построении и анализе криптографических отображений целесообразно выделение и анализ таких подгрупп группы $\mathsf{G}_{\mathbf{E}^n} = (G_{\mathbf{E}^n}, \Diamond)$, которые переводят множество $(P_2^{(0)}(n))^m$ в себя.

1.7. Хаотические динамические системы.

На протяжении последнего двадцатилетия были достигнуты значительные успехи в области исследования свойств детерминированного хаоса динамических систем [99,230,295,298], причем большое внимание уделяется применению хаотических динамических систем к решению задач преобразования информации [9,10,60-62,139,263,273,283,289,294]. Рассмотрим основные понятия и определения, связанные с хаотическими динамическими системами, используемые в последующих разделах.

Говоря неформально, *динамическая система* характеризуется таким набором из n *динамических переменных*, характеризующих *состояние* системы, что их значения в любой последующий момент времени получаются из исходного набора значений по определенному правилу, называемому *оператором эволюции* системы.

Динамику (иными словами, *эволюцию*) такой системы можно представить как *движение точки* по *траектории* в n*-мерном фазовом пространстве*.

Динамическую систему, представленную системой дифференциальных уравнений, часто называют *потоком*, а динамическую систему, представленную системой рекуррентных соотношений называют *отображением*. Отметим, что при компьютерном моделировании динамической системы всегда происходит переход от представления системы в виде потока к ее представлению в виде отображения.

Будем рассматривать только *финитные* движения динамической системы, т.е. движения в ограниченной области фазового пространства. Динамическая система называется *хаотической*, если сколь угодно малое изменение начального состояния системы быстро нарастает во времени. Это означает, что сколь угодно малая неточность в задании начального состояния системы делает невозможной предсказуемость ее эволюции на достаточно больших интервалах времени.

Выделим в фазовом пространстве динамической системы некоторую область (ее называют *облаком*). Рассмотрим эволюцию облака. Если с течением времени *объем* облака остается постоянным, то динамическая система называется *консервативной*, а если с течением времени *объем* облака изменяется, то динамическая система называется *диссипативной*.

С физической точки зрения для динамических систем, представленных системой дифференциальных уравнений, *консервативность* означает *сохранение энергии*.

Для диссипативных систем характерно то, что с течением времени облако *съеживается*, и *концентрируется* на одном или нескольких *аттракторах*, т.е. подмножествах фазового пространства, обладающих, как правило, нулевым фазовым объемом.

Наиболее известные примеры аттракторов – это *положение равновесия* и *предельный цикл*, т.е. замкнутая фазовая траектория, к которой с течением времени стремятся все близкие траектории.

Инвариантным множеством называется такое множество точек фазового пространства, что фазовая траектория, стартующая из любой его точки, содержится в этом множестве.

Множество точек фазового пространства, из которых траектории приходят к одному и тому же аттрактору, называется *бассейном* этого аттрактора. Ясно, что бассейн любого аттрактора динамической является инвариантным множеством.

В диссипативных системах хаос часто связан с наличием *странных аттракторов*, представляющих собой фрактальные множества (или, кратко, *фракталы*), т.е. множества, имеющие сложную самоподобную структуру, и притягивающие к себе все траектории, принадлежащие бассейну этого аттрактора.

На развитие теории фракталов существенное влияние оказали теория множеств и теория размерности. Рассмотрим кратко соответствующие понятия и определения (см., напр., [138,216]).

Пусть (M, ρ) – метрическое пространство, $diam(M)$ – диаметр множества M $(M \subset \mathsf{M})$, а $h : \mathbf{R}_+ \to \mathbf{R}_+$ – такая непрерывная возрастающая функция, что

$$h(0) = 0 .$$

Обозначим через F_M такое семейство подмножеств множества M, что для любого множества M $(M \subset \mathsf{M})$ и любого положительного числа ε существует не более чем счетное ε-покрытие $\{G_i\}_{i \in I}$ множества M элементами семейства F_M, т.е.

$$M \subseteq \bigcup_{i \in I} G_i$$

и

$$d(G_i) \le \varepsilon \quad (i \in I) .$$

Положим

$$m_h^\varepsilon(M) = \inf \sum_{i \in I} h(diam(G_i)) \quad (M \subset \mathsf{M}),$$

где нижняя грань берется по всем не более чем счетным ε-покрытиям $\{G_i\}_{i \in I}$ множества M элементами семейства F_M.

Функция h называется *измеряющей* функцией, а $m_h^\varepsilon(M)$ – *внешней приближающей мерой* порядка ε.

Внешняя h-мера Хаусдорфа H_h определяется равенством

$$H_h(M) = \lim_{\varepsilon \to 0^+} m_h^\varepsilon(E) \quad (M \subset \mathsf{M}) .$$

Для любого компактного множества M $(M \subset \mathsf{M})$ при любой внешней h-мере Хаусдорфа H_h равенство $H_h(M) = 0$ истинно тогда и только тогда, когда для каждого положительного числа ε существует такое конечное разложение

$$M = \bigcup_{i=1}^{k(\varepsilon)} M_i$$

множества M, что

$$\sum_{i=1}^{k} h(diam(M_i)) < \varepsilon .$$

Различные семейства F_M и различные функции h могут приводить к различным внешним h-мерам Хаусдорфа.

В дальнейшем, для краткости, в словосочетании «внешняя мера» слово «внешняя» будем опускать.

Важным специальным случаем h-меры Хаусдорфа является *α-мерная мера Хаусдорфа* H_α $(\alpha > 0)$, которая получается, если в качестве семейства F_M выбрать семейство всех непустых подмножеств множества M, а в качестве функции h – функцию

$$h(x) = \gamma(\alpha) \cdot x^\alpha ,$$

где α – положительное число, а $\gamma(\alpha)$ – положительная константа, зависящая только от числа α.

Ясно, что любого множества M $(M \subset \mathsf{M})$ при любой α-мерной мере Хаусдорфа H_α $(\alpha > 0)$ истинно равенство

$$H_\alpha(M) = \lim_{\varepsilon \to 0^+} \gamma(\alpha) \cdot \inf \sum_{i \in I} (diam(G_i))^\alpha ,$$

где нижняя грань берется по всем не более чем счетным ε-покрытиям $\{G_i\}_{i \in I}$ множества M элементами семейства F_M.

Отметим, что к той же самой мере H_α приводит выбор в качестве F_M семейства всех непустых открытых (или всех замкнутых) подмножеств множества M.

К *сферической α-мере Хаусдорфа* (которая также обозначается H_α) приводит выбор в качестве F_M семейства всех замкнутых (либо открытых) шаров в множестве M, а в качестве h – функции

$$h(x) = \frac{\Gamma^\alpha(0.5)}{2^\alpha \cdot \Gamma(1 + 0.5 \cdot \alpha)} \cdot x^\alpha \quad (x \geq 0),$$

где Γ – гамма-функция Эйлера. В этом случае $h(x)$ $(x \geq 0)$ – это объем α-мерного шара диаметра x.

Ясно, что если $\alpha \in \mathbf{N}$, то сферическая α-мера Хаусдорфа совпадает с *α-мерой Лебега*.

Если при определении сферической α-меры Хаусдорфа H_α ограничиться только покрытиями шарами одного и того же диаметра ε, то получим *энтропийную меру* $\overline{H}_\alpha$.

Ясно, что для любого компактного множества M $(M \subset \mathsf{M})$

$$\overline{H}_\alpha(M) = \lim_{\varepsilon \to 0^+} n_M(\varepsilon) \cdot h(\varepsilon) \quad (M \subset \mathsf{M}),$$

где $n_M(\varepsilon)$ – наименьшее число шаров диаметра ε, необходимое для покрытия множества M. Функция $n_M(\varepsilon)$ является неубывающей функцией от аргумента ε. При этом для бесконечного компактного множества M число $n_M(\varepsilon)$ неограниченно возрастает, если $\varepsilon \to 0^+$.

Скорость роста числа $n_M(\varepsilon)$ при $\varepsilon \to 0^+$ характеризует *метрический порядок* компактного множества M, определяемый равенством

$$D(M) = -\lim_{\varepsilon \to 0^+} \frac{\ln n_M(\varepsilon)}{\ln \varepsilon}.$$

Размерность Хаусдорфа-Безиковича множества M $(M \subset \mathsf{M})$ определяется равенством

$$\alpha_0(M) = \sup\{\alpha \mid H_\alpha(M) \neq 0\} \ (= \inf\{\alpha \mid H_\alpha(M) = 0\}.$$

Известно, что:

1) если M_1 и M_2 – геометрически подобные множества, то
$$\alpha_0(M_1) = \alpha_0(M_2);$$
2) если M – конечное или счетное множество, то $\alpha_0(M) = 0$;
3) если $M_1 \subset M_2$, то $\alpha_0(M_1) \le \alpha_0(M_2)$;
4) $\alpha_0(\bigcup\limits_{i \in I} M_i) = \alpha_0(\sup\limits_{i \in I} M_i)$ $(I \subseteq \mathbf{N})$;
5) для любого компактного множества M истинно неравенство
$$D(M) \le \alpha_0(M).$$

Пусть M $(M \subset \mathsf{M})$ – компактное множество. *Топологической размерностью* множества M (обозначается $\dim M$) называется такое наименьшее число $n \in \mathbf{Z}_+$, что для любого положительного числа ε существует такое конечное ε-покрытие множества M замкнутыми множествами, что никакие $n+2$ элемента покрытия не пересекаются.

Известно, что для любого компактного множества M и для любой меры H_α истинно неравенство

$$\dim M \le \alpha_0(M).$$

Компактное множество M $(M \subset \mathsf{M})$ называется *фракталом в широком смысле*, если

$$\dim M < \alpha_0(M)$$

и фракталом в узком смысле, если $\alpha_0(M)$ – дробное число.

Для фрактала M $(M \subset \mathsf{M})$ метрический порядок $D(M)$ называется *фрактальной размерностью*.

Отметим, что при вычислении фрактальной размерности компактного множества $M \subset \mathbf{R}^n$ $(n \in \mathbf{N})$ вместо покрытия множества M шарами диаметра ε часто используют покрытие множества M n-мерными «кубиками» (или «пирамидами») с ребром ε, т.е. в формуле

$$D(M) = -\lim_{\varepsilon \to 0^+} \frac{\ln n_M(\varepsilon)}{\ln \varepsilon},$$

$n_M(\varepsilon)$ – это число n-мерных «кубиков» (соответственно, число «пирамид») с ребром ε, покрывающих множество M.

Выше было отмечено, что часто под «фракталом» понимают «геометрическую фигуру, в которой один и тот же фрагмент повторяется при каждом уменьшении масштаба» (см., напр., [124]). В этой фразе отражено свойство фрактала «быть самоподобным множеством».

Формально это свойство может быть представлено следующим образом.

Множество M_1 $(M_1 \subseteq \mathsf{M})$ *подобно* множеству M_2 $(M_2 \subseteq \mathsf{M})$ *с коэффициентом подобия* r $(r > 0)$ (в этом случае пишут $M_1 \sim^r M_2$), если существует такое отображение $f : M_2 \to M_1$, что для всех $x, y \in M_2$ $(x \neq y)$ истинно равенство

$$\frac{\rho(f(x), f(y))}{\rho(x, y)} = r.$$

Пусть $n \in \mathbf{N}$ $(n > 1)$ и

$$R = (r_1, \ldots, r_n),$$

где $r_i > 0$ $(i = 1, \ldots, n)$. Компактное множество M $(M \subset \mathsf{M})$ называется *самоподобным* множеством (СП-множеством) с *законом самоподобия* (R, n), если

$$M = \bigcup_{i=1}^{n} M_i,$$

где

$$M_i \sim^{r_i} M \quad (i = 1, \ldots, n)$$

и

$$\alpha_0(M_i \cap M_j) < \alpha_0(M)$$

для всех $i, j \in \{1, \ldots, n\}$ $(i \neq j)$.

Если множества $M_1, \ldots, M_n$ попарно не пересекаются, то положительное решение $\alpha_s(M)$ уравнения

$$\sum_{i=1}^{n} r_i^x = 1$$

называется *размерностью самоподобия* (СП-размерностью) множества M.

Известно, что если существует такое число α, что истинно неравенство

$$0 < H_\alpha(M) < \infty,$$

то

$$\alpha_s(M) = \alpha_0(M).$$

В том случае, когда

$$r_1 = \ldots = r_n = r$$

СП-множество M называется *абсолютно самоподобным* множеством (АСП-множеством).

Рассмотрим ряд обобщений понятия «СП-множество».

Пусть $n \in \mathbf{N}$ $(n > 1)$, $m \in \mathbf{Z}_{n+1}$ и

$$R = (r_1, \ldots, r_m),$$

где $r_i > 0$ $(i = 1, \ldots, m)$. Компактное множество M $(M \subset \mathsf{M})$ называется *генетически самоподобным* множеством (ГСП-множеством) с *законом самоподобия*

$$((R, m), (R_j, n_j)\,(j = m+1, \ldots, n)),$$

если

$$M = (\bigcup_{i=1}^{m} M_i) \cup (\bigcup_{j=m+1}^{n} M_j),$$

где

$$M_i \sim^{r_i} M \quad (i = 1, \ldots, m)$$

и M_j $(j = m+1, \ldots, n)$ – СП-множество с законом самоподобия (R_j, n_j).

Если $m = n$, то ГСП-множество M является СП-множеством, а если $m = 0$, то M состоит из конечного числа СП-множеств (в этом случае множество M называется *кусочно-самоподобным* множеством).

Известно, что если

$$\sum_{i=1}^{m} r_i^{\alpha} = 1,$$

$$H_\alpha(M) = \sum_{i=1}^{n} H_\alpha(M_i),$$

$$\alpha_s(M_j) = \alpha_0(M_j) \quad (j = m+1, \ldots, n)$$

и

$$0 < H_{\alpha_0(M)}(M) < \infty,$$

то

$$\alpha_0(M) = \max_{m < j \le n} \{\alpha, \alpha_s(M_j)\}.$$

Компактное множество M $(M \subset \mathsf{M})$ называется N*-самоподобным* множеством (N-СП-множеством), если

$$M = \bigcup_{i=1}^{\infty} M_i ,$$

где

$$M_i \sim^{r_i} M \quad (i \in \mathbf{N})$$

и

$$\alpha_0(M_i \cap M_j) < \alpha_0(M)$$

для всех $i, j \in \{1,\ldots,n\}$ $(i \neq j)$.

Если каждое пересечение $M_i \cap M_j$ $(i, j \in \mathbf{N}, i \neq j)$ – не более чем счетное множество, то положительное решение $\alpha_{Ns}(M)$ уравнения

$$\sum_{i=1}^{\infty} r_i^{\,x} = 1$$

называется *размерностью N-самоподобия* (N-СП-размерностью) множества M.

Отметим, что

$$\alpha_{Ns}(M) = \alpha_0(M).$$

Компактное множество M $(M \subset \mathsf{M})$ называется *почти самоподобным* множеством, если существует такое СП-множество M_1 $(M_1 \subset M)$, что

$$\alpha_0(M \setminus M_1) < \alpha_0(M).$$

Кривая называется *фрактальной*, если ее график – фрактал.

В [107-109] исследованы проблемы, связанные с заданием фрактальных кривых конечными преобразователями. В [215] показано, как фракталы могут быть использованы при построении вычислительно стойких шифров, а в [238] – как фракталы могут быть использованы при построении протоколов обмена ключами.

В настоящее время в приложениях выделяют два класса фракталов: *конструктивные* фракталы и *динамические* фракталы (см., напр., [124]).

Охарактеризуем кратко эти классы фракталов в метрическом пространстве $\mathbf{R}^2$.

Конструктивный фрактал в метрическом пространстве $\mathbf{R}^2$ характеризуется заданием двух множеств: *основы* и *фрагмента*, повторяющегося при каждом уменьшении масштаба. При этом фрагмент применяется для преобразования *текущего состояния* основы, и может использоваться двумя способами.

1-й способ использования фрагмента основан на применении *метода решета*. Этот метод состоит в том, что запускается следующая бесконечная рекурсивная процедура: текущее состояние основы разбивается на части, подобные исходному состоянию основы и из каждого блока этого разбиения удаляются части, подобные фрагменту.

Те точки основы, которые не удаляются в результате применения этой бесконечной рекурсивной процедуры, образуют фрактал.

Ясно, что вычисление текущего состояния основы при небольших значениях числа итераций не является сложным.

Пример 1.9. Наиболее известными фракталами, построение которых основано на применении *метода решета*, являются *салфетка* и *ковер* Серпинского.

Для салфетки Серпинского основой ─ равносторонний треугольник (рис. 1.39.а), а фрагмент – это перевернутый открытый равносторонний треугольник со стороной, длина которой в два раза меньше длины стороны основы (рис. 1.39.б).

На рис. 1.39.в изображено состояние основы, полученное после двух итераций рекурсивной процедуры (черным цветом закрашены удаленные области).

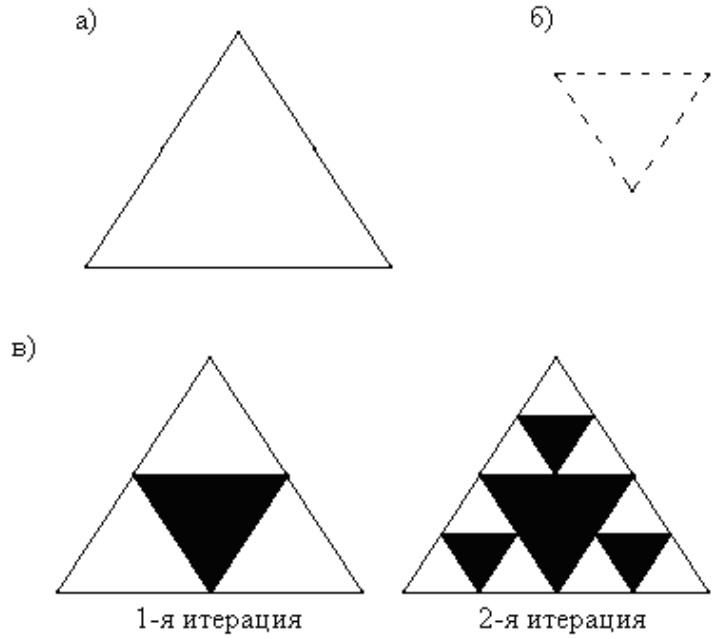


Рис. 1.39. Салфетка Серпинского: а) основа; б) фрагмент; в) результат двух итераций рекурсивной процедуры.

Для ковра Серпинского основа ─ квадрат (рис. 1.40.а), а фрагмент – это открытый квадрат со стороной, длина которой в три раза меньше длины основы (рис. 1.40.б).

На рис. 1.40. в изображено состояние основы, полученное после двух итераций рекурсивной процедуры (черным цветом закрашены удаленные области).

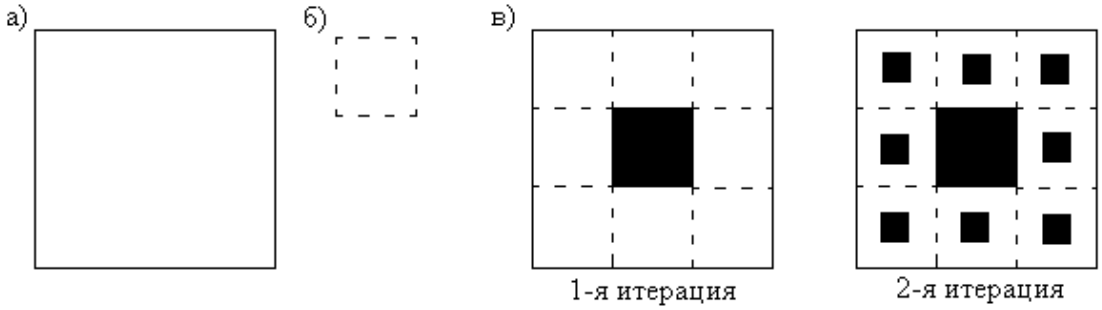


Рис. 1.40. Ковер Серпинского: а) основа; б) фрагмент; в) результат двух итераций рекурсивной процедуры.

2-й способ использования фрагмента. Предполагается, что основа и фрагмент – ломаные линии, причем фрагмент можно так расположить на звене основы, что их концы совпадают. Запускается следующая бесконечная рекурсивная процедура: в текущем состоянии основы (а оно представляет собой ломаную линию) каждое из выбранных звеньев ломанной заменяется ломанной, подобной фрагменту.

Ломаная линия, полученная в результате применения этой бесконечной рекурсивной процедуры, является фракталом.

Пример 1.10. Для *фрактала Леви* основой является отрезок (рис. 1.41.а), фрагмент – это половина квадрата, построенного на этом отрезке, как на диагонали (рис. 1.41.б). На каждой итерации рекурсивной процедуры выбираются все звенья, принадлежащие текущему состоянию основы.

На рис. 1.41.в изображено состояние основы, полученное после пяти итераций рекурсивной процедуры.

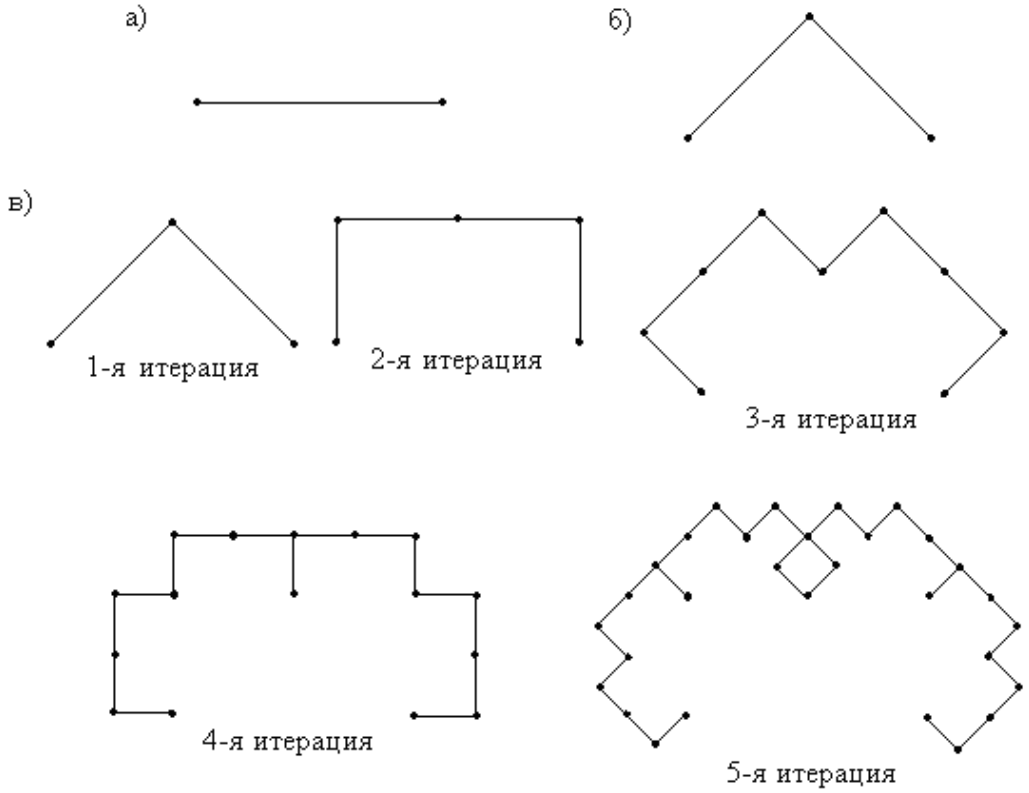


Рис. 1.41. Фрактал Леви: а) основа; б) фрагмент; в) результат пяти итераций рекурсивной процедуры.

Ясно, что на l-й итерации ($l \in \mathbf{N}$) рекурсивной процедуры, применяемой во 2-м способе построения конструктивного фрактала, замена выбранного звена ломаной сводится к удалению этого звена (без его концов) из текущего состояния основы и к применению следующей последовательности преобразований метрического пространства $\mathbf{R}^2$:

Шаг 1. К фрагменту, расположенному так, что его концы лежат на оси *Ox*, применяется преобразование f^{l-1}, где f – «сжатие».

Шаг 2. К образу фрагмента, полученному на шаге 1, применяется преобразование «поворот» на угол φ_l.

Шаг 3. Применяется такое преобразование «сдвиг», что концы фрагмента, полученного на шаге 2, совпадают с концами выбранного звена из текущего состояния основы.

Для того чтобы к ломаной линии с вершинами

$$P_1 = (x_1, y_1), \ldots, P_l = (x_l, y_l)$$

применить преобразование «сжатие», «поворот» или «сдвиг» достаточно вычислить образы этих вершин. При этом для любой точки P плоскости имеет место равенство

$$f^{k+1}(P) = f(f^k(P)) \quad (k \in \mathbf{N}).$$

Кроме того, преобразования «сжатие относительно начала координат», «поворот на угол α против часовой стрелки» и «сдвиг в направлении $\mathbf{h} = (h_1, h_2)$» имеют, соответственно, вид

$$\begin{cases} \tilde{x} = r \cdot x \\ \tilde{y} = r \cdot y \end{cases} (0 < r < 1),$$

$$\begin{cases} \tilde{x} = x \cdot \cos\alpha - y \cdot \sin\alpha \\ \tilde{y} = x \cdot \sin\alpha + y \cdot \cos\alpha \end{cases},$$

и

$$\begin{cases} \tilde{x} = x + h_1 \\ \tilde{y} = y + h_2 \end{cases}.$$

Отсюда вытекает, что вычисление текущего состояния основы при небольших значениях числа итераций не является сложным.

Следует отметить, что при построении конструктивного фрактала 2-м способом иногда к фрагменту более удобно применять последовательность преобразований «сжатие-поворот» относительно начала координат, а затем – преобразование «сдвиг». Преобразование «сжатие-поворот» имеет вид

$$\begin{cases} \tilde{x} = a \cdot x - b \cdot y \\ \tilde{y} = b \cdot x + a \cdot y \end{cases},$$

где число

$$\Delta = a^2 + b^2 < 1$$

характеризует величину сжатия, а угол поворота α определяется из условий

$$\begin{cases} \cos\alpha = \dfrac{a}{\sqrt{a^2 + b^2}} \\ \sin\alpha = \dfrac{b}{\sqrt{a^2 + b^2}} \end{cases}.$$

При построении конструктивного фрактала 2-м способом применяется преобразование «поворот». Поворот на угол α можно производить как по часовой стрелке, так и против часовой стрелки.

Возможность такого выбора является основой для реализации «механизма внесения случайности» в построение конструктивного фрактала 2-м способом.

Действительно, пусть задана случайная (или псевдослучайная) битовая последовательность

$$u_1, u_2, \ldots.$$

На i-й итерации $(i = 1,2,\ldots)$ рекурсивной процедуры, применяемой во 2-м способе построения конструктивного фрактала, будем осуществлять поворот на угол α против часовой стрелке, если $u_i = 0$ и поворот на угол α по часовой стрелке, если $u_i = 1$.

Значимость такого «механизма внесения случайности» в построение конструктивного фрактала 2-м способом обусловлена следующими двумя обстоятельствами.

Во-первых, существенно расширяется множество «геометрических изображений» конструктивных фракталов, построенных 2-м способом.

Во-вторых, даже зная алгоритм, в соответствии с которым осуществляется построение конструктивного фрактала 2-м способом и параметры, используемые при конкретной реализации этого алгоритма, невозможно вычислить результат без знания используемой случайной (или псевдослучайной) битовой последовательности.

Эти два обстоятельства делают весьма привлекательным при решении задач защиты информации применение конструктивных фракталов, построение которых осуществляется 2-м способом.

Если при построении конструктивного фрактала (1-м или 2-м способом) ограничиться конечным числом итераций применяемой рекурсивной процедуры, то построенную фигуру часто называют *конструктивным псевдофракталом*.

Зафиксируем числа $l_1, l_2 \in \mathbf{N}$ и положительные рациональные числа h_1 и h_2. Выделим в $\mathbf{R}^2$ прямоугольник Π с длиной основания $l_1 \cdot h_1$ и высотой $l_2 \cdot h_2$, содержащий конструктивный псевдофрактал Φ.

Построим на прямоугольнике Π прямоугольную сетку S, ячейки которой – прямоугольники с длиной основания h_1 и высотой h_2.

Закрасим черным цветом все ячейки сетки S, пересекающиеся с псевдофракталом Φ, а белым цветом – все ячейки сетки S, непересекающиеся с псевдофракталом Φ.

Зафиксируем прямоугольную область Γ дисплея, содержащую l_1 пикселей по горизонтали и l_2 пикселей по вертикали. Установим такое взаимно-однозначное соответствие между прямоугольной сеткой S и областью

Γ, что ячейка, расположенная в i-м ряду $(i=1,\ldots,l_2)$ и j-м столбце $(j=1,\ldots,l_1)$ сетки S соответствует пикселю области Γ, расположенному на пересечении i-й строки и j-го столбца.

Закрасим каждый пиксель области Γ в тот же цвет, в который закрашена соответствующая ячейка сетки S.

Полученное изображение Γ_Φ назовем *черно-белым представлением конструктивного псевдофрактала* Φ *в области* Γ *дисплея*.

Динамический фрактал в метрическом пространстве $\mathbf{R}^2$ характеризуется заданием комплексного целого или рационального отображения

$$z_{n+1} = f(z_n) \quad (n \in \mathbf{Z}_+), \tag{1.81}$$

где

$$z_n = x_n + i \cdot y_n \in \mathbf{C} \quad (n \in \mathbf{Z}_+),$$

а $i \in \mathbf{C}$ – мнимая единица.

Отметим, что при построении изображения фрактала в метрическом пространстве $\mathbf{R}^2$ от представления (1.81) переходят к системе двух действительных отображений

$$\begin{cases} x_{n+1} = f_1(x_n, y_n) \\ y_{n+1} = f_2(x_n, y_n) \end{cases} \quad (n \in \mathbf{Z}_+). \tag{1.82}$$

В дальнейшем, для упрощения изложения, предполагается, что f – полином, т.е.

$$f(z) = \sum_{j=0}^{k} a_j \cdot z^j \quad (k \in \mathbf{N}),$$

где $a_0, a_1, \ldots, a_k \in \mathbf{C}$ – константы.

Для отображения f число $\omega \in \mathbf{C}$ называется:

1) *неподвижной точкой*, если

$$f(\omega) = \omega;$$

2) *периодической точкой* периода l $(l \in \mathbf{N})$, если l – такое наименьшее натуральное число, что

$$f^l(\omega) = \omega,$$

где

$$f^l = \underbrace{f \circ \ldots \circ f}_{l \text{ раз}}.$$

Если для отображения f число $\omega \in \mathbf{C}$ – периодическая точка периода l, то последовательность комплексных чисел

$$\omega, f(\omega), \ldots, f^{l-1}(\omega)$$

называется *орбитой* периода l.

Пусть для отображения f число $\omega \in \mathbf{C}$ является периодической точкой периода l и

$$\frac{d}{dz} f^{l}(z)|_{z=\omega} = \lambda .$$

Тогда число $\lambda \in \mathbf{C}$ называется:

1) *притягивающей точкой*, если $0 \le \lambda < 1$;
2) *индифферентной точкой*, если $|\lambda| = 1$;
3) *отталкивающей точкой*, если $|\lambda| > 1$.

Множеством Жюлиа $J(f)$ для отображения f называется замыкание множества отталкивающих периодических точек отображения f.

Известно, что множество $J(f)$ является непустым компактным множеством, инвариантным для отображения f, т.е.

$$f(J(f)) = J(f).$$

При этом, как правило, итерации отображения f на множестве $J(f)$ ведут себя хаотически и, более того, множество $J(f)$ обычно является фракталом.

Назовем фрактал $J(f)$ *фракталом Мандельброта*, если $J(f)$ – связное множество, Такое определение обусловлено тем, что для отображения

$$z_{n+1} = z_n^2 + c \quad (n \in \mathbf{Z}_+), \tag{1.83}$$

где

$$c = a + i \cdot b,$$

именно Б. Мандельброт охарактеризовал множество значений параметров (a, b), для которых фрактал Жюлиа $J(f)$ – связное множество.

При построении изображения Φ фрактала Мандельброта для отображения (1.83) (т.е. при построении *псевдофрактала*) переходят к представлению этого отображения в виде (1.82), т.е. к представлению

$$\begin{cases} x_{n+1} = x_n^2 - y_n^2 + a \\ y_{n+1} = 2 \cdot x_n \cdot y_n + b \end{cases} \quad (n \in \mathbf{Z}_+), \tag{1.84}$$

фиксируют значения параметров

$$a \in [-2.5; 1.5],$$

$$b \in [-2; 2],$$

положительное натуральное число R $(R \ge 2)$ и верхнюю границу $k_{\max}$ числа итераций отображения (1.84). Затем на множестве

$$S = [-2.5; 1.5] \times [-2; 2]$$

строят достаточно мелкую прямоугольную сетку, и последовательно перебирают центры ячеек этой сетки.

Если в течение $k_{\max}$ итераций центр $(x_0; y_0) \in S$ ячейки сетки не покидает круг

$$x^2 + y^2 \le R^2, \tag{1.85}$$

то считается, что ячейка сетки, содержащая этот центр, принадлежит псевдофракталу Мандельброта. Эта ячейка сетки закрашивается в черный цвет.

Если же центр сетки $(x_0; y_0) \in S$ покинул круг (1.85) на k-й итерации, где $k < k_{\max}$, то считается, что ячейка сетки, содержащая этот центр, не принадлежит псевдофракталу Мандельброта. Эта ячейка сетки закрашивается в белый цвет.

Черно-белое представление псевдофрактала Φ в области Γ дисплея строится так же, как и черно-белое представление конструктивного псевдофрактала.

Фракталы Ньютона возникают при использовании отображения

$$z_{n+1} = z_n - \frac{f(z)}{\dfrac{df(z)}{dz}} \quad (n \in \mathbf{Z}_+), \tag{1.86}$$

где f – фиксированный полином. В настоящее время этот класс динамических фракталов наименее изучен. Поэтому, как правило, на практике ограничиваются случаем, когда

$$f(z) = z^k - a \quad (k \in \mathbf{N}),$$

где $a \in \mathbf{C}$ – фиксированное число. В этом случае (1.86) принимает вид

$$z_{n+1} = \frac{(k-1) \cdot z_n^k + a}{k \cdot z_n^{k-1}} \quad (n \in \mathbf{Z}_+). \tag{1.87}$$

Известно, что корни уравнения

$$z^k - a = 0$$

являются устойчивыми неподвижными точками отображения (1.87), а граница, разделяющая области притяжения различных корней представляет собой фрактал.

Рассмотрим теперь модельные хаотические динамические системы (см., напр., [99]).

Вначале рассмотрим модельные хаотические отображения.

Среди одномерных хаотических отображений наиболее известными, по-видимому, являются следующие три отображения.

1. Отображение *зуб пилы* имеет вид

$$x_{n+1} = \{2 \cdot x_n\} \quad (n \in \mathbf{Z}_+), \tag{1.88}$$

где $\{a\}$ – дробная часть числа a. Отметим, что (1.88) часто записывается в виде

$$x_{n+1} = 2 \cdot x_n \pmod 1 \quad (n \in \mathbf{Z}_+).$$

Для отображения *зуб пилы* отрезок [0;1] является инвариантным множеством. График сужения отображения (1.88) на отрезок [0;1] изображен на рис. 1.42.а.

Эволюция динамической системы $S_2^{зп}$, представленной этим сужением, показана на рис. 1.42.б.

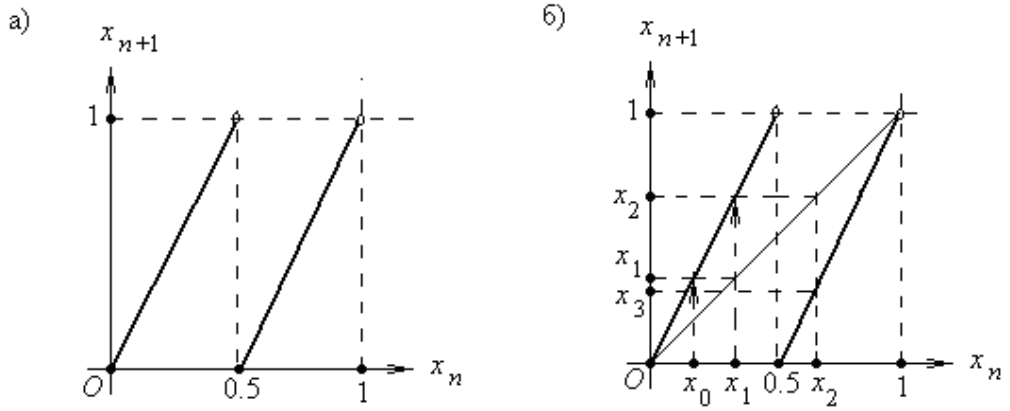


Рис. 1.42. Отображение *зуб пилы*: а) сужение графика на отрезок [0;1]; б) первые три шага эволюции динамической системы, представленной отображением *зуб пилы*.

В дальнейшем предполагается, что для начального состояния x_0 динамической системы $S_2^{зп}$ выполнено условие

$$x_0 \in (0;1).$$

Запишем начальное состояние x_0 динамической системы $S_2^{зп}$ в двоичной системе счисления. Если число x_0 представимо конечной двоичной дробью, т.е.

$$x_0 = 0.\alpha_1 \ldots \alpha_k,$$

где $\alpha_i \in \{0;1\}$ $(i = 1,\ldots,k)$, причем

$$\alpha_k = 1,$$

то считаем, что

$$x_0 = 0.\alpha_1 \ldots \alpha_k 0 \ldots 0 \ldots.$$

Итак, пусть

$$x_0 = 0.\alpha_1 \ldots \alpha_n \ldots,$$

где $\alpha_i \in \{0;1\}$ $(i \in \mathbf{N})$. Так как

$$x_n = 0.\alpha_{n+1}\alpha_{n+2} \ldots$$

для всех $n \in \mathbf{Z}_+$, то динамическая переменная x_n $(n \in \mathbf{Z}_+)$ принимает значение из левой половины отрезка [0;1], если $\alpha_{n+1} = 0$ и из правой половины отрезка [0;1], если $\alpha_{n+1} = 1$.

Зафиксируем случайную (соответственно, псевдослучайную) последовательность

$$\alpha_1, \ldots, \alpha_n, \ldots.$$

Тогда при начальном состоянии

$$x_0 = 0.\alpha_1 \ldots \alpha_n \ldots$$

динамическая переменная x_n $(n \in \mathbf{Z}_+)$ случайно (соответственно, псевдослучайно) принимает значения из левой и правой половин отрезка $[0;1]$.

Охарактеризуем эволюцию динамической системы $S_2^{зп}$ в зависимости от выбора начального состояния $x_0 \in (0;1)$.

Пример 1.11. В [173] показано, что в зависимости от выбора начального состояния

$$x_0 \in (0;1)$$

возникают следующие три принципиально различных типа эволюции динамической системы $S_2^{зп}$:

1. Пусть x_0 – рациональное число, представимое конечной двоичной дробью, т.е.

$$x_0 = 0.\alpha_1 \ldots \alpha_k 00\ldots \quad (k \in \mathbf{N}).$$

Так как $x_n = 0$ для всех $n \geq k$, то неподвижная точка

$$x = 0$$

представляет собой аттрактор, достижимый из начального состояния x_0 за конечное время.

Несложно показать, что этот аттрактор – неустойчивое положение равновесия динамической системы $S_2^{зп}$.

2. Пусть x_0 – рациональное число, представимое бесконечной периодической двоичной дробью, т.е.

$$x_0 = 0.\alpha_1 \ldots \alpha_k (\beta_1 \ldots \beta_l) \quad (k, l \in \mathbf{N}).$$

Так как

$$x_{n+h\cdot l} = x_n$$

для всех $n \geq k$, то цикл, определяемый последовательностью точек

$$x_k, \ldots, x_{k+l-1}$$

представляет собой аттрактор, достижимый из начального состояния x_0 за конечное время.

Несложно показать, что этот аттрактор – неустойчивый предельный цикл динамической системы $S_2^{зп}$.

3. Пусть x_0 – иррациональное число. Тогда число x_0 представляется бесконечной непериодической десятичной дробью. Следовательно, все точки траектории

$$x_0, x_1, \ldots, x_n, \ldots$$

динамической системы $S_2^{зп}$ являются попарно различными. Несложно показать, что существуют такие иррациональные числа

$$x_0 \in (0;1),$$

что траектория

$$x_0, x_1, \ldots, x_n, \ldots$$

динамической системы $S_2^{зп}$ – всюду плотное подмножество отрезка $[0;1]$.

2. *Логистическое* отображение имеет вид

$$x_{n+1} = 1 - \lambda \cdot x_n^2 \quad (n \in \mathbf{Z}_+), \tag{1.89}$$

где λ – положительный параметр, от величины которого зависит характер динамики.

Чаще всего рассматривается случай, когда

$$\lambda = 2,$$

т.е. отображение

$$x_{n+1} = 1 - 2 \cdot x_n^2 \quad (n \in \mathbf{Z}_+). \tag{1.90}$$

Для отображения (1.90) отрезок [–1;1] является инвариантным множеством.

График отображения (1.90) изображен на рис. 1.43.а.

Эволюция динамической системы $S^{лг}$, представленной сужением отображения (1.90) на отрезок [–1;1], показана на рис. 1.43.б.

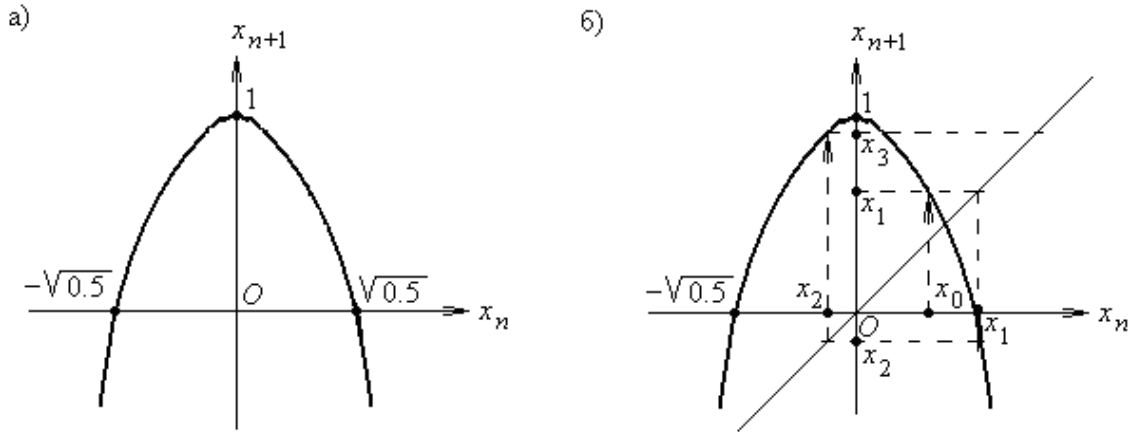


Рис. 1.43. Отображение $x_{n+1} = 1 - 2 \cdot x_n^2$ $(n \in \mathbf{Z}_+)$: а) график; б) первые три шага эволюции динамической системы, представленной этим отображением.

Осуществим в динамической системе $S^{лг}$ замену динамической переменной по формуле

$$x_n = -\cos 2 \cdot \pi \cdot y_n \quad (n \in \mathbf{Z}_+), \tag{1.91}$$

где

$$|y_0| \le 1.$$

Подставив (1.91) в (1.90), получим

$$\cos 2 \cdot \pi \cdot y_{n+1} = \cos 4 \cdot \pi \cdot y_n \quad (n \in \mathbf{Z}_+).$$

Последнее равенство истинно для всех $n \in \mathbf{Z}_+$, если

$$y_{n+1} = 2 \cdot y_n \pmod 1 \quad (n \in \mathbf{Z}_+),$$

т.е. если динамическая переменная y_n $(n \in \mathbf{Z}_+)$ изменяется в соответствии с хаотическим отображением *зуб пилы*.

Отсюда вытекает, что $S^{лг}$ – хаотическая динамическая система.

3. Отображение *тент* имеет вид

$$x_{n+1} = \begin{cases} \alpha^{-1} \cdot x_n, \ \textit{если} \ 0 \le x_n \le \alpha \\ (1-\alpha)^{-1} \cdot (1-x_n), \ \textit{если} \ \alpha < x_n \le 1 \end{cases} \quad (n \in \mathbf{Z}_+), \qquad (1.92)$$

где α $(0 < \alpha < 1)$ – параметр.

Несложно показать, что динамическая система $S_\alpha^{тн}$ $(0 < \alpha < 1)$, представленная отображением (1.92), является хаотической динамической системой.

Чаще всего рассматривается случай, когда

$$\alpha = 0.5,$$

т.е. отображение

$$x_{n+1} = \begin{cases} 2 \cdot x_n, \ \textit{если} \ 0 \le x_n \le 0.5 \\ 2 \cdot (1-x_n), \ \textit{если} \ 0.5 < x_n \le 1 \end{cases} \quad (n \in \mathbf{Z}_+). \qquad (1.93)$$

Иногда отображение (1.92) называют *косым тентом*, если

$$\alpha \ne 0.5 \quad (0 < \alpha < 1),$$

а отображение (1.93) часто называется *симметричным тентом*.

График отображения (1.93) изображен на рис. 1.44.а.

Эволюция динамической системы $S_{0.5}^{тн}$, представленной этим отображением, показана на рис. 1.44.б.

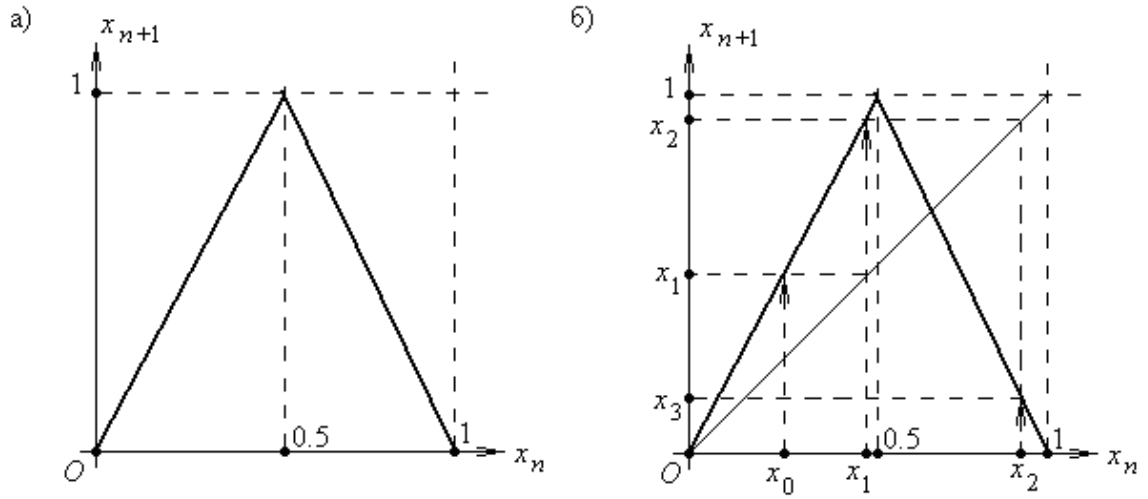


Рис. 1.44. Отображение *симметричный тент*: а) график; б) первые три шага эволюции динамической системы, представленной этим отображением.

Естественным обобщением сужения отображения (1.88) на отрезок [0;1], сужения отображения (1.90) на отрезок [–1;1] и отображения (1.93) являются, соответственно, хаотические отображения

$$x_{n+1}(l) = \{l \cdot x_n(l)\} \quad (n \in \mathbf{Z}_+), \qquad (1.94)$$

$$x_{n+1}(l)=\begin{cases}1-2\cdot l^{2}\cdot(x+1-2\cdot l^{-1}\cdot(i+0.5))^{2},\ \textit{если}\\ \quad x_n\in(-1+2\cdot l^{-1}\cdot i;-1+2\cdot l^{-1}\cdot(i+1))\\ \qquad (i=0,1,\ldots,l-1)\\ \text{-}1,\ \textit{если}\ \ x_n=-1+2\cdot l^{-1}\cdot i\ \ (i=0,1,\ldots,l)\end{cases}\quad (n\in\mathbf{Z}_{+}),\qquad (1.95)$$

и

$$x_{n+1}(l)=\begin{cases}2\cdot l\cdot x_n(l)-2\cdot i,\ \ \textit{если}\\ \quad x_n(l)\in[i\cdot l^{-1};(i+0.5)\cdot l^{-1}]\\ \qquad (i=0,1,\ldots,l-1)\\ -2\cdot l\cdot x_n(l)+2\cdot(i+1),\ \textit{если}\\ \quad x_n(l)\in((i+0.5)\cdot l^{-1};(i+1)\cdot l^{-1})\\ \qquad (i=0,1,\ldots,l-1)\end{cases}\quad (n\in\mathbf{Z}_{+}),\qquad (1.96)$$

где число l – параметр ($l\in\{2,3,\ldots\}$ для отображения (1.84), а $l\in\mathbf{N}$ – параметр для отображений (1.95) и (1.96)).

Параметр l называется *порядком* хаотического отображения, и определяет число элементов, используемых при конструировании отображения.

Так как для каждого из отображений (1.94)-(1.96) число интервалов монотонности равно $2\cdot l$, то при обращении отображения возможны $2\cdot l$ вариантов.

Это обстоятельство делает привлекательным применение отображений (1.94)-(1.969) при построении шифров. Для таких шифров секретным ключом является последовательность интервалов монотонности используемых отображений, а шифртекстом – последовательность рациональных чисел, принадлежащих для отображений (1.94) и (1.96) отрезку [0;1], а для отображения (1.95) – отрезку [–1;1]. Вычислительная стойкость таких шифров основана именно на статистических свойствах используемого хаотического отображения и на неоднозначности его обращения.

В [13,91-96] описанный выше подход к построению шифров в деталях проработан для отображения (1.96). Особо следует отметить, что в этих работах установлена точность вычислений, обеспечивающая корректность процесса расшифровки.

Среди двумерных хаотических отображений, обладающих странным аттрактором, наиболее известным, по-видимому, является отображение *Эно*. Это отображение имеет следующий вид

$$\begin{cases}x_{n+1}=1-a\cdot x_n^{2}-b\cdot y_n\\ y_{n+1}=x_n\end{cases}\quad (n\in\mathbf{Z}_{+}),\qquad (1.97)$$

где a $(a\in\mathbf{R}_{+})$ и b $(b\in\mathbf{R})$ – параметры.

Система (1.97) была исследована М. Эно в 1976г. при значениях параметров $a=1.4$ и $b=-0.3$.

Известно, что если $|b|<1$, то отображение *Эно* – диссипативная динамическая система, а если $|b|=1$, то отображение *Эно* – консервативная динамическая система.

Отметим, что если $b=0$, то отображение *Эно* сводится к *логистическому* отображению.

Рассмотрим теперь модельные хаотические потоки.

1. Система *Лоренца* имеет вид

$$\begin{cases} \dot{x} = \sigma \cdot (y - x) \\ \dot{y} = r \cdot x - y - x \cdot z, \\ \dot{z} = -b \cdot z + x \cdot y \end{cases} \tag{1.98}$$

где $\sigma, b, r \in \mathbf{R}_+$ – такие параметры, что $r > 0$ и $\sigma > b+1$. Система (1.98) была исследована Э. Лоренцом в 1963г. при значениях параметров $\sigma = 10$, $b = \frac{8}{3}$ и $r = 28$.

Система *Лоренца* является математической моделью, применяемой при описании ряда физических явлений (конвекция в подогреваемом снизу слое жидкости, одномодовый лазер, водяное колесо, диссипативный осциллятор с инерционным возбудителем и т.д.). Отметим, что:

1) система *Лоренца* обладает симметрией

$$\begin{cases} x \to -x \\ y \to -y; \\ z \to z \end{cases}$$

2) если $0 < r \le 1$, то система *Лоренца* имеет единственную неподвижную точку – устойчивый узел

$$O = (0,0,0);$$

3) если $r > 1$, то система *Лоренца* имеет три неподвижные точки: неустойчивое положение равновесия

$$O = (0,0,0)$$

(эта точка характеризуется неустойчивым одномерным многообразием, а также устойчивым двумерным многообразием) и положения равновесия

$$O_1 = (\sqrt{r-1}, \sqrt{r-1}, r-1)$$

и

$$O_2 = (-\sqrt{r-1}, -\sqrt{r-1}, r-1),$$

которые являются либо устойчивыми узлами, либо устойчивыми фокусами, если

$$r \in (1; (\sigma - b - 1)^{-1} \cdot \sigma \cdot (\sigma + b + 3)),$$

и неустойчивыми узлами, если

$$r > (\sigma - b - 1)^{-1} \cdot \sigma \cdot (\sigma + b + 3);$$

4) существует такое значение

$$r_0 \in (1; (\sigma - b - 1)^{-1} \cdot \sigma \cdot (\sigma + b + 3))$$

числа r, что в фазовом пространстве системы *Лоренца* возникают два неустойчивых предельных цикла L_1 и L_2;

5) существует такое значение r_1 $(r_1 > r_0)$ числа r, что в фазовом пространстве системы *Лоренца* появляется *странный аттрактор Лоренца*, определяемый множеством траекторий, сходящихся к предельным циклам L_1 и L_2, и характеризующий хаотический режим колебаний значений переменных x, y и z.

2. Система *Рёсслера* имеет вид

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + a \cdot y \\ \dot{z} = b + (x - r) \cdot z \end{cases}, \qquad (1.99)$$

где $\sigma, b, r \in \mathbf{R}_+$ – параметры.

Система (1.99) была исследована О. Рёсслером в 1976г. при значениях параметров $a = b = 0.2$ и $r = 5.7$, причем им было установлено, что исследуемая система имеет странный аттрактор – *ленточный аттрактор Рёсслера*, существенно отличающийся от *странного аттрактора Лоренца*.

3. Системы *Спротта* представляют собой 19 динамических систем с хаотической динамикой и имеют следующий вид:

$$S_A^{Cn}: \begin{cases} \dot{x} = y \\ \dot{y} = -x + y \cdot z \\ \dot{z} = 1 - y^2 \end{cases}, \quad S_B^{Cn}: \begin{cases} \dot{x} = y \cdot z \\ \dot{y} = x - y \\ \dot{z} = 1 - x \cdot y \end{cases}, \quad S_C^{Cn}: \begin{cases} \dot{x} = y \cdot z \\ \dot{y} = x - y \\ \dot{z} = 1 - x^2 \end{cases},$$

$$S_D^{Cn}: \begin{cases} \dot{x} = -y \\ \dot{y} = x + z \\ \dot{z} = x \cdot z + 3 \cdot y^2 \end{cases}, \quad S_E^{Cn}: \begin{cases} \dot{x} = y \cdot z \\ \dot{y} = x^2 - y \\ \dot{z} = 1 - 4 \cdot x \end{cases}, \quad S_F^{Cn}: \begin{cases} \dot{x} = y + z \\ \dot{y} = -x + 0.5 \cdot y \\ \dot{z} = x^2 - z \end{cases},$$

$$S_G^{Cn}: \begin{cases} \dot{x} = 0.4 \cdot x + z \\ \dot{y} = x \cdot z - y \\ \dot{z} = -x + y \end{cases}, \quad S_H^{Cn}: \begin{cases} \dot{x} = -y + z^2 \\ \dot{y} = x + 0.5 \cdot y \\ \dot{z} = x - z \end{cases}, \quad S_I^{Cn}: \begin{cases} \dot{x} = -0.5 \cdot y \\ \dot{y} = x + z \\ \dot{z} = x + y^2 - z \end{cases},$$

$$S_J^{Cn}: \begin{cases} \dot{x} = 2 \cdot z \\ \dot{y} = -2 \cdot y + z \\ \dot{z} = -x + y + y^2 \end{cases}, \quad S_K^{Cn}: \begin{cases} \dot{x} = x \cdot y - z \\ \dot{y} = x - y \\ \dot{z} = x + 0.3 \cdot z \end{cases}, \quad S_L^{Cn}: \begin{cases} \dot{x} = y + 3.9 \cdot z \\ \dot{y} = 0.9 \cdot x^2 - y \\ \dot{z} = 1 - x \end{cases},$$

$$S_M^{Cn}:\begin{cases}\dot{x}=-z\\ \dot{y}=-x^2-y\\ \dot{z}=1.7\cdot(1+x)+y^2\end{cases},\qquad S_N^{Cn}:\begin{cases}\dot{x}=-2\cdot y\\ \dot{y}=x+z^2\\ \dot{z}=1+y-2\cdot x\end{cases},$$

$$S_O^{Cn}:\begin{cases}\dot{x}=y\\ \dot{y}=x-z\\ \dot{z}=x+x\cdot z+2.7\cdot y\end{cases},\qquad S_P^{Cn}:\begin{cases}\dot{x}=2.7\cdot y+z\\ \dot{y}=-x+y^2\\ \dot{z}=x+y\end{cases},$$

$$S_Q^{Cn}:\begin{cases}\dot{x}=-z\\ \dot{y}=x-y\\ \dot{z}=3.1+y^2+0.5\cdot z\end{cases},\qquad S_R^{Cn}:\begin{cases}\dot{x}=0.9-y\\ \dot{y}=0.4+z\\ \dot{z}=x\cdot y-z\end{cases},\qquad S_S^{Cn}:\begin{cases}\dot{x}=-x-4\cdot y\\ \dot{y}=x+z^2\\ \dot{z}=1+x\end{cases}.$$

Эти системы были построены, и исследованы Дж. Спроттом в 1994г.

Система S_A^{Cn} сохраняет фазовый объем, и демонстрирует хаотическую динамику, характерную для консервативных систем, а S_i^{Cn} $(i\in\{B,C,\ldots,S\})$ – диссипативные системы, в которых хаос ассоциируется с наличием в фазовом пространстве странного аттрактора. Этот аттрактор для систем S_B^{Cn} и S_C^{Cn} аналогичен *странному аттрактору Лоренца*, а для систем S_i^{Cn} $(i\in\{D,E,\ldots,S\})$ *– ленточному аттрактору Росслера*.

Отметим, что системы S_A^{Cn}, S_B^{Cn} и S_C^{Cn} обладают той же симметрией, что и система *Лоренца*.

Известно, что теория симметрий [36] представляет собой мощный аппарат анализа динамических систем. Поэтому особый интерес представляют хаотических динамические системы, обладающие нетривиальной группой симметрий.

Для таких систем симметрия в начальных условиях сохраняется вдоль траектории, а симметричный образ любого аттрактора также является аттрактором.

Рассмотрим следующие две такие системы с нетривиальной структурой множества аттракторов, исследованные в [239].

4. *Guckenheimer and Holmes cycle* представляет собой поток и имеет вид

$$\begin{cases}\dot{x}=x\cdot(l+a\cdot x^2+b\cdot y^2+c\cdot z^2)\\ \dot{y}=y\cdot(l+a\cdot y^2+b\cdot z^2+c\cdot x^2),\\ \dot{z}=z\cdot(l+a\cdot z^2+b\cdot x^2+c\cdot y^2)\end{cases}\qquad (1.100).$$

где $l,a,b,c\in\mathbf{R}$ – параметры.

Система (1.100), построенная Дж. Гюкенхеймером и П. Холмсом в 1988г., обладает симметрией относительно начала координат, координатных плоскостей, координатных осей, а также отображений

$$\begin{cases} x \to \Diamond_1 y \\ y \to \Diamond_2 z \\ z \to \Diamond_3 x \end{cases} \quad (\Diamond_1, \Diamond_2, \Diamond_3 \in \{+,-\})$$

и

$$\begin{cases} x \to \Diamond_1 z \\ y \to \Diamond_2 x \\ z \to \Diamond_3 y \end{cases} \quad (\Diamond_1, \Diamond_2, \Diamond_3 \in \{+,-\}).$$

Известно, что для системы (1.100) существует такое открытое множество значений параметров a, b и c, что существует аттрактор, который представляет собой предельный цикл.

Этот цикл образован тремя точками равновесия, расположенными на координатных осях и соединяющими эти точки равновесия траекториями, лежащими в координатных плоскостях.

5. *Free-running* система представляет собой отображение и имеет вид

$$\begin{cases} x_{n+1} = f(x_n) \cdot e^{-\gamma \cdot z_n} \\ y_{n+1} = f(y_n) \cdot e^{-\gamma \cdot x_n} \\ z_{n+1} = f(z_n) \cdot e^{-\gamma \cdot y_n} \end{cases} \quad (n \in \mathbf{Z}_+), \qquad (1.101)$$

где

$$f(x) = a \cdot x \cdot (1-x)$$

представляет собой *логистическое отображение* с параметром $a \in (0;4)$.

Эта система, построенная П. Ашвином, А. Руклиджем и Р. Штурманом в 2002г., обладает симметрией относительно поворотов

$$\begin{cases} x \to y \\ y \to z \\ z \to x \end{cases}$$

и

$$\begin{cases} x \to z \\ y \to x \\ z \to y \end{cases}.$$

Отметим, что система (1.101) сводится к *логистическому* отображению, если либо $x_0 = y_0 = 0$, либо $x_0 = z_0 = 0$, либо $y_0 = z_0 = 0$.

Одной из актуальных задач преобразования информации на основе хаотических динамических систем является разработка эффективных поточных шифров на основе этих систем [274,276,277].

Безусловным достоинством таких шифров являются их высокая скорость и вычислительная стойкость.

Рассмотрим динамическую систему

$$\dot{\mathbf{q}} = \mathbf{f}(\mathbf{q}, \mathbf{a}), \tag{1.102}$$

где вектор динамических переменных

$$\mathbf{q} = (q_1, \ldots, q_n)^T \in \mathbf{R}^n$$

определяет состояние системы (1.102) в момент $t \in \mathbf{R}_+$, а вектор

$$\mathbf{a} = (a_1, \ldots, a_n)^T \in \mathbf{R}^n$$

определяет значения параметров системы (1.102).

Построение поточного шифра на основе динамической системы (1.102) может быть сведено к ее дискретизации и аддитивном внесении информационной переменной x, т.е. за счет приведения системы (1.102) к дискретной динамической системе с внешним управлением, либо вида

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t + h \cdot B \cdot \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \cdot \mathbf{q}_t + D \cdot \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{1.103}$$

либо вида

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t + h \cdot B \cdot \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \cdot \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{1.104}$$

где h $(h > 0)$ – шаг дискретизации, A, B, C и D – $n \times n$-матрицы, $\mathbf{q}_0 \in \mathbf{R}^n$ – начальное состояние динамической системы, управляющий вектор

$$\mathbf{x}_{t+1} = (x_{t+1}^{(1)}, \ldots, x_{t+1}^{(n)})^T \in \mathbf{E}^n$$

определяет значение n-битового блока информации, шифруемого в момент $t+1$, а вектор $\mathbf{y}_{t+1}$ $(t \in \mathbf{Z}_+)$ (т.е. значение выхода динамической системы в момент $t+1$) представляет собой результат шифрования блока информации $\mathbf{x}_{t+1}$.

Утверждение 1.6. Динамическая система (1.103) представляет собой поточный шифр тогда и только тогда, когда D – невырожденная $n \times n$-матрица.

Доказательство. Система уравнений

$$D \cdot \mathbf{x}_{t+1} = \mathbf{y}_{t+1} - C \cdot \mathbf{q}_t \tag{1.105}$$

является совместной при любых фиксированных значениях $t \in \mathbf{Z}_+$ и $\mathbf{y}_{t+1}, \mathbf{q}_t \in \mathbf{R}^n$. Система уравнений (1.105) имеет единственное решение $\mathbf{x}_{t+1}$ тогда и только тогда, когда D – невырожденная $n \times n$-матрица.

Таким образом, при любом фиксированном начальном состоянии $\mathbf{q}_0 \in \mathbf{R}^n$ динамическая система (1.103) осуществляет биекцию множества $(\mathbf{E}^n)^+$ на множество $(\mathbf{E}^n)^+$ (т.е. является поточным шифром) тогда и только тогда, когда D – невырожденная $n \times n$-матрица.

Утверждение доказано.

Следствие 1.8. Для поточного шифра (1.103) расшифровку осуществляет динамическая система

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + (I - h \cdot B \cdot D^{-1} \cdot C) \cdot \mathbf{q}_t + h \cdot B \cdot D^{-1} \cdot \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = D^{-1} \cdot (\mathbf{x}_{t+1} - C \cdot \mathbf{q}_t) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (1.106)$$

Доказательство. Так как динамическая система (1.103) – поточный шифр, то D – невырожденная $n \times n$-матрица.

Из системы уравнений (1.105) находим, что

$$\mathbf{x}_{t+1} = D^{-1} \cdot (\mathbf{y}_{t+1} - C \cdot \mathbf{q}_t) \quad (t \in \mathbf{Z}_+). \quad (1.107)$$

Из (1.103) и (1.107) вытекает, что

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + (I - h \cdot B \cdot D^{-1} \cdot C) \cdot \mathbf{q}_t + h \cdot B \cdot D^{-1} \cdot \mathbf{y}_{t+1} \\ \mathbf{x}_{t+1} = D^{-1} \cdot (\mathbf{y}_{t+1} - C \cdot \mathbf{q}_t) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (1.108)$$

где I – единичная $n \times n$-матрица. Осуществив в (1.108) замену $\mathbf{x}_{t+1}$ на $\mathbf{y}_{t+1}$ и $\mathbf{y}_{t+1}$ на $\mathbf{x}_{t+1}$, получим (1.106).

Следствие доказано.

Утверждение 1.7. Динамическая система (1.104) представляет собой поточный шифр тогда и только тогда, когда B и C – невырожденные $n \times n$-матрицы.

Доказательство. Из (1.104) вытекает, что если, по крайней мере, одна из матриц B или C — вырожденная матрица, то при любом фиксированном начальном состоянии $\mathbf{q}_0 \in \mathbf{R}^n$ динамическая система (1.104) осуществляет отображение множества $(\mathbf{E}^n)^+$ в множество $(\mathbf{E}^n)^+$, не являющееся инъекцией.

Пусть B и C — невырожденные матрицы.

Подставив 1-е уравнение системы (1.104) во второе уравнение, находим, что

$$h \cdot C \cdot B \cdot \mathbf{x}_{t+1} = \mathbf{y}_{t+1} - h \cdot C \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) - C \cdot \mathbf{q}_t. \quad (1.109)$$

Система уравнений (1.109) является совместной при любых фиксированных значениях $t \in \mathbf{Z}_+$ и $\mathbf{y}_{t+1}, \mathbf{q}_t \in \mathbf{R}^n$.

Отсюда вытекает, что система уравнений (1.109) имеет единственное решение $\mathbf{x}_{t+1}$ тогда и только тогда, когда B и C – невырожденные $n \times n$-матрицы.

Таким образом, при любом фиксированном начальном состоянии $\mathbf{q}_0 \in \mathbf{R}^n$ динамическая система (1.104) осуществляет биекцию множества $(\mathbf{E}^n)^+$ на множество $(\mathbf{E}^n)^+$ (т.е. является поточным шифром) тогда и только тогда, когда B и C – невырожденные $n \times n$-матрицы.

Утверждение доказано.

Следствие 1.9. Для поточного шифра (1.104) расшифровку осуществляет динамическая система

$$\begin{cases} \mathbf{q}_{t+1} = C^{-1} \cdot \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = -h^{-1} \cdot B^{-1} \cdot (h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t) + h^{-1} \cdot B^{-1} \cdot C^{-1} \cdot \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (1.110)$$

Доказательство. Так как динамическая система (1.104) – поточный шифр, то B и C – невырожденные $n \times n$-матрицы.

Из системы уравнений (1.109) находим, что

$$\mathbf{x}_{t+1} = h^{-1} \cdot B^{-1} \cdot C^{-1} \cdot (\mathbf{y}_{t+1} - h \cdot C \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) - C \cdot \mathbf{q}_t). \quad (1.111)$$

Из (1.104) и (1.111) вытекает, что

$$\begin{cases} \mathbf{q}_{t+1} = C^{-1} \cdot \mathbf{y}_{t+1} \\ \mathbf{x}_{t+1} = -h^{-1} \cdot B^{-1} \cdot (h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t) + h^{-1} \cdot B^{-1} \cdot C^{-1} \cdot \mathbf{y}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (1.112)$$

Осуществив в (1.112) замену $\mathbf{x}_{t+1}$ на $\mathbf{y}_{t+1}$ и $\mathbf{y}_{t+1}$ на $\mathbf{x}_{t+1}$, получим (1.110).

Следствие доказано.

Каждый из шифров (1.103) и (1.104) представляет собой симметричный поточный шифр. При этом секретным ключом для шифра (1.103) являются параметры $h, \mathbf{a}, B, C, D$ и начальное состояние $\mathbf{q}_0$, а для шифра (1.104) – параметры $h, \mathbf{a}, B, C$ и начальное состояние $\mathbf{q}_0$.

Следует особо отметить, что в процессе *шифрование-расшифровка* динамические системы (1.103) и (1.106), а также динамические системы (1.104) и (1.110) движутся по одной и той же траектории в пространстве состояний.

Вычисления в поле действительных чисел $\mathbf{R}$ (или в поле рациональных чисел $\mathbf{Q}$ при компьютерном моделировании) наталкиваются на фактор «накопления ошибок округления», в результате проявления которого процесс *шифрование-расшифровка* теряет свою корректность. При этом обеспечение корректности вычислений за счет повышения точности вычислений связано с непростым анализом секретного ключа, зависящим от длины шифруемой двоичной последовательности. Такой подход заведомо неприемлем, так как он приводит к существенному замедлению, как процесса шифрования, так и процесса расшифровки.

Поэтому естественный путь нивелирования ошибок округления – это переход в (1.103) и в (1.104) к действиям в конечной алгебраической системе.

Отметим, что в течение последнего десятилетия тенденция перехода от чисто комбинаторных конструкций к конечным алгебраическим системам четко проявляется в криптографии, так как практически во всех современных стандартах шифрования присутствует фрагментарное применение теории конечных полей [218,229].

Известно, что поле – это специальный случай кольца. При этом в кольце (в отличие от поля) наличие делителей нуля дает возможность алгебраически охарактеризовать сложность поиска, а именно: как сложность решения алгебраических уравнений над кольцом.

Таким образом, в (1.103) и в (1.104) естественно перейти от действий в поле $\mathbf{R}$ (или в поле $\mathbf{Q}$) к действиям в конечном кольце Z_{p^k}.

В результате такого перехода естественно возникает новый класс динамических систем, а именно: класс динамических систем над кольцом Z_{p^k}.

Исследование таких систем актуально с позиции следующих точек зрения.

Во-первых, эти системы имеют нетривиальную область приложения – криптографию, так как при соответствующих ограничениях на параметры они определяют класс вычислительно стойких скоростных потоковых шифров, вычислительная стойкость которых может быть теоретически охарактеризована в терминах сложности решения уравнений над конечным кольцом.

Во-вторых, устанавливается внутренняя связь между теорией динамических систем [74,111] и криптологией, так как сложность атак криптоаналитика может быть охарактеризована в терминах сложности решения таких классических задач теории динамических систем, как управляемость, наблюдаемость, параметрическая идентификация.

В-третьих, выделяется новый класс конечных автоматов – класс автоматов над конечным кольцом, что дает возможность эффективно применить для их анализа весь арсенал как теории автоматов [30,31,98,208] и современной алгебры [16,97]. Тем самым устанавливается внутренняя связь между теорией динамических систем, теорией автоматов и современной алгеброй.

То, что эта связь – нетривиальная вытекает из того, что такие чисто комбинаторные задачи абстрактной теории автоматов, как контрольный эксперимент с автоматом [265] для исследуемых систем – это обычная задача параметрической идентификации.

Более того, в свете подхода, развитого в [49], исследование управляемости и наблюдаемости для рассматриваемых систем – это задачи построения установочного и диагностического экспериментов со слабоинициальным автоматом.

В-четвертых, решение для исследуемых систем классических задач теории динамических систем (таких, как параметрическая идентификация, управляемость и наблюдаемость) дает возможность выделить и осознать те особенности, которые возникают при переходе от поля характеристики нуль к конечным алгебраическим системам.

В-пятых, предыдущий опыт применения методов теории конечных полей дал возможность выделить узкие классы дискретных систем, для кото-

рых решения задач значительно проще, чем решение этих же задач для дискретных систем, определенных на абстрактных множествах. Яркими примерами являются исследование линейных последовательностных машин [30,220], задач теории кодов, контролирующих ошибки [21], а также многочисленные потенциальные приложения, указанные в [104].

1.8. Квантовые вычисления.

Одним из новых перспективных направлений современной криптологии является *квантовая криптология* (см., напр., [126,243-247,254,268,281]). Перспективность этого направления обусловлена следующими обстоятельствами.

Проблемы классической теории алгоритмов, связанные с исследованием *переборных задач* [50], т.е. комбинаторных задач, для которых в настоящее время единственным известным методом решения является *поиск* [89,141], стимулировали разработку новых парадигм, в рамках которых может быть реализована идея «неограниченного параллелизма» вычислений. *Квантовые вычисления* и являются одной из таких парадигм.

В 1980г. американский физик Р.Фейнман и советский математик Ю.И. Манин обратили внимание на то обстоятельство, что *некоторые квантово-механические процессы невозможно эффективно моделировать на классическом компьютере*.

Исследование этого обстоятельство привело к выводу о том, что для проведения вычислений квантовые процессы являются более эффективными, чем классические. В квантовых системах «пространство вычислений» растет экспоненциально при линейном росте «размера» квантовой системы, что и делает возможным реализацию экспоненциального параллелизма.

Такую возможность подтвердила разработка П. Шора в 1994г. квантового алгоритма разложения целых чисел на множители за *полиномиальное время* [302].

По-видимому, это обстоятельство должно послужить серьезным предостережением для криптографов, так как достаточно много современных шифров построено именно на предположении о том, что задача факторизации целых чисел – это трудная задача.

С 1994г. квантовые вычисления, как математическая теория, предназначенная для разработки принципиально новых информационных технологий, интенсивно развиваются (с соответствующим финансированием исследований) во всех ведущих странах мира. В этих исследованиях принимают участие как физики, так и математики.

Соответственно, выделяются два направления развития квантовых вычислений.

Первое направление исследований в области квантовых вычислений связано с синтезом квантового компьютера.

Исходя из современных представлений квантовый компьютер будет иметь вид, представленный на рис. 1.45.

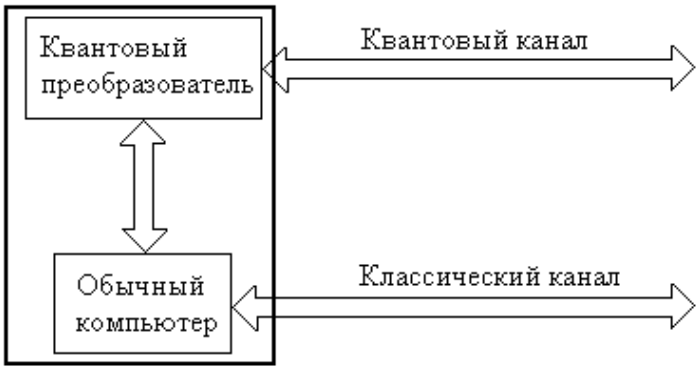


Рис. 1.45. Квантовый компьютер.

В настоящее время в этом направлении нет существенного прорыва, по-видимому, из-за высокой сложности управления квантовыми процессами. Тем не менее, примитивные действующие образцы квантовых преобразователей созданы в ряде ведущих стран мира (Россия, Китай, США).

Второе направление исследований в области квантовых вычислений связано с разработкой теории квантовых алгоритмов.

В этом направлении, несмотря на его высокую сложность и принципиальное отличие от классической теории алгоритмов, имеется существенный прорыв. Об этом свидетельствуют фундаментальные результаты, характеризующие современное состояние теории квантовых алгоритмов, представленные в многочисленных публикациях (см., напр., [129,248,262,296,302]).

Рассмотрим кратко основные понятия, лежащие в основе теории квантовых алгоритмов.

Квантовые вычисления основаны на выполнении последовательности *обратимых преобразований* состояния *квантовой системы*, за которой следует *измерение*, представляющее собой *доступ к результатам* квантовых вычислений. При этом, *процесс измерения возмущает состояние квантовой системы и искажает его*.

Такое обстоятельство является весьма привлекательным для криптографов. Действительно, появляется дополнительная возможность для защиты информации, так как некорректное измерение информации криптоаналитиком не даст ему возможность восстановить истинный результат.

Кроме того, появляется возможность обнаружения атаки криптоаналитика за счет сверки отправителем и адресатом по классическому каналу тех или иных характеристик отправленной и полученной информации.

Проиллюстрируем идею, лежащую в основе квантовых вычислений, на следующей простой модели.

Рассмотрим луч света, поляризованный случайным образом и направленный на отражающий экран (рис. 1.46.а).

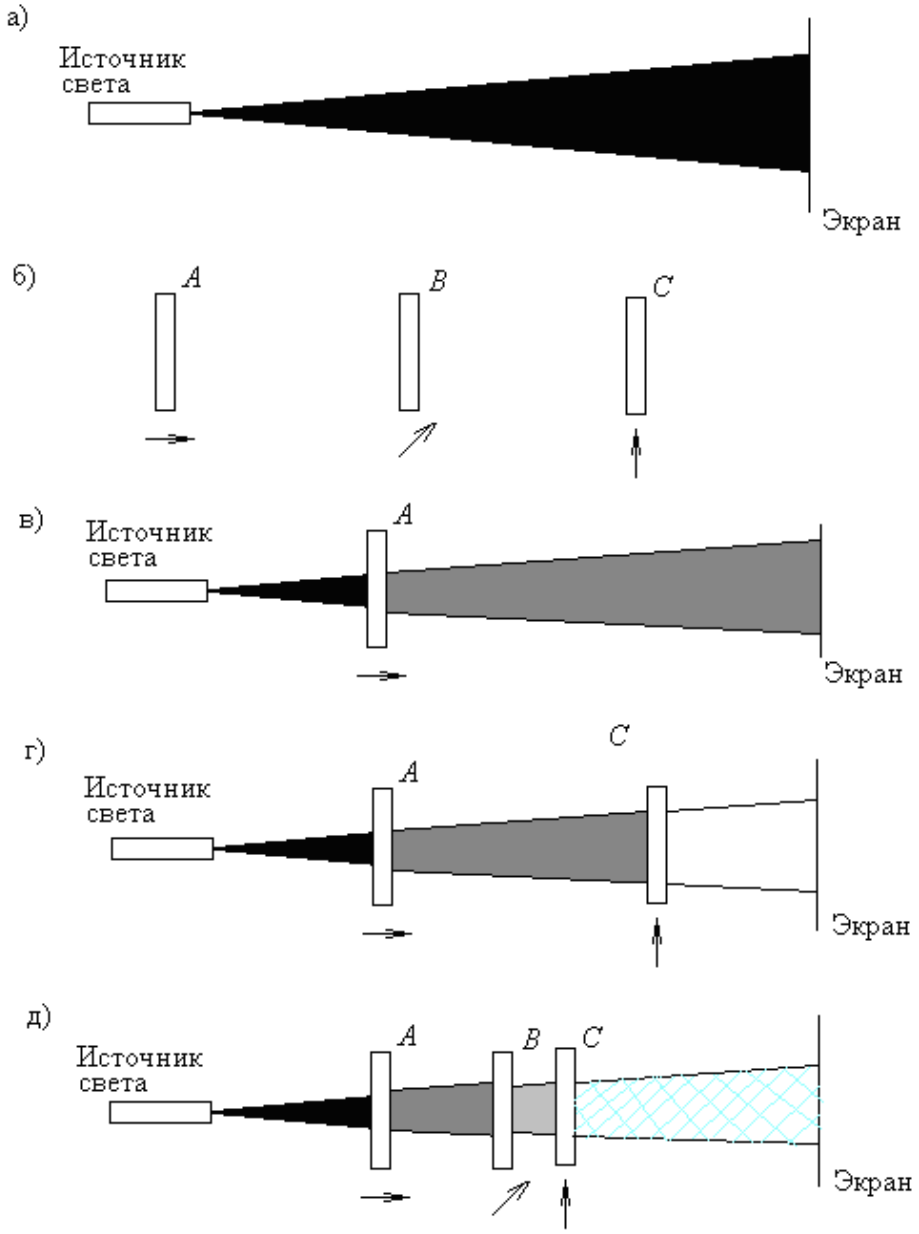


Рис. 1.46. Поляризация света при его прохождении через фильтры.

Пусть имеются следующие три фильтра (рис. 1.46.б):

1) фильтр A, поляризованный горизонтально;
2) фильтр B, поляризованный под углом 45°;
3) фильтр C, поляризованный вертикально.

Установим на пути света фильтр A (рис. 1.46.в). Интенсивность выходящего света равна половине интенсивности входящего света. При этом все фотоны, прошедшие через фильтр A, поляризованы горизонтально.

Установим теперь фильтр C за фильтром A (рис. 1.46.г). Интенсивность фотонов, выходящих из фильтра C, равна нулю.

Теперь установим фильтр B между фильтрами A и C (рис. 1.46.д). Интенсивность света на экране равна одной восьмой от первоначальной интенсивности света. При этом все фотоны, прошедшие через фильтр C, поляризованы вертикально.

Объясним рассмотренную выше ситуацию в терминах формальной модели. Пусть

$$B = \{\mathbf{e_0}, \mathbf{e_1}\}$$

суть ортонормированный базис в 2-х мерном комплексном векторном пространстве H_2.

Кубит (это сокращение от словосочетания «квантовый бит») представляет собой физическую систему, состояние которой представлено вектором

$$|\xi\rangle = \lambda_0 \cdot \mathbf{e}_0 + \lambda_1 \cdot \mathbf{e}_1,$$

где $\lambda_0, \lambda_1 \in \mathbf{C}$, причем

$$|\lambda_0|^2 + |\lambda_1|^2 = 1.$$

При измерении в базисе $B = \{\mathbf{e_0}, \mathbf{e_1}\}$ кубит переходит в базисное состояние $\mathbf{e}_i$ $(i = 0,1)$ с вероятностью $|\lambda_i|^2$.

Для случайно поляризованного света каждый фотон находится в состоянии

$$|\xi\rangle = 2^{-0.5} \cdot (|\uparrow\rangle + |\rightarrow\rangle),$$

где

$$B_1 = \{|\rightarrow\rangle, |\uparrow\rangle\}$$

представляет собой ортонормированный базис.

При установке фильтра A на пути такого света осуществляется измерение фотонов по базисному вектору $|\rightarrow\rangle$ ортонормированного базиса B_1. Вероятность того, что после такого измерения состояние кубита преобразуется в состояние $|\rightarrow\rangle$ (так как только такие фотоны проходят через фильтр A), равна

$$(2^{-0.5})^2 = 0.5.$$

Поэтому интенсивность потока света, прошедшего через фильтр A, равна половине интенсивности исходного потока света.

При установке фильтра C за фильтром A осуществляется измерение фотонов, прошедших через фильтр A (каждый из таких фотонов находится в состоянии $|\rightarrow\rangle$), по базисному вектору $|\uparrow\rangle$ ортонормированного базиса B_1.

Так как

$$|\rightarrow\rangle = 1 \cdot |\rightarrow\rangle + 0 \cdot |\uparrow\rangle,$$

то при измерении по базисному вектору $|\uparrow\rangle$ ортонормированного базиса B_1 ни один фотон, находящийся в состоянии $|\rightarrow\rangle$, не может перейти в состояние $|\uparrow\rangle$.

Поэтому, интенсивность потока света, прошедшего через фильтр C, равна нулю.

Рассмотрим, что происходит при установке фильтра B между фильтрами A и C.

При установке фильтра B за фильтром A осуществляется измерение фотонов, прошедших через фильтр A (каждый из таких фотонов находится в состоянии $|\rightarrow\rangle$), по вектору $|45^\circ\rangle$. Этот вектор является базисным вектором ортонормированного базиса

$$B_2 = \{|45^\circ\rangle, |135^\circ\rangle\}.$$

Каждый фотон, прошедший через фильтр B, находится в состоянии $|45^\circ\rangle$.

Так как

$$|\rightarrow\rangle = 2^{-0.5} \cdot (|45^\circ\rangle - |135^\circ\rangle),$$

то вероятность того, что после измерения по базисному вектору $|45^\circ\rangle$ ортонормированного базиса B_2 фотон, прошедший через фильтр A, пройдет также и через фильтр B, равна

$$(2^{-0.5})^2 = 0.5.$$

Поэтому, интенсивность света, последовательно прошедшего через фильтры A и B, равна одной четвертой интенсивности исходного потока света.

Фотоны, прошедшие через фильтр B, попадают в фильтр C. Таким образом, осуществляется измерение фотонов, прошедших через фильтр B (каждый из таких фотонов находится в состоянии $|45^\circ\rangle$), по базисному вектору $|\uparrow\rangle$ ортонормированного базиса B_1. Каждый фотон, прошедший через фильтр C, находится в состоянии $|\uparrow\rangle$. Так как

$$|45^\circ\rangle = 2^{-0.5} \cdot (|\uparrow\rangle + |\rightarrow\rangle)|,$$

то вероятность того, что после измерения по базисному вектору $|\uparrow\rangle$ ортонормированного базиса B_1, фотон, прошедший через фильтр B, пройдет также и через фильтр C, равна

$$(2^{-0.5})^2 = 0.5.$$

Поэтому интенсивность света, последовательно прошедшего через фильтры A, B и C, равна одной восьмой интенсивности исходного потока света.

Естественным обобщением *кубита* является *n-кубитовая система* ($n \in \mathbf{N}$), которая определяется следующим образом.

Зафиксируем в 2-х мерном комплексном векторном пространстве H_2 ортонормированный базис

$$B^{(2)} = \{|0\rangle, |1\rangle\}.$$

Построим тензорное произведение n экземпляров пространства H_2

$$\mathsf{H}_{2^n} = \underbrace{\mathsf{H}_2 \otimes \ldots \otimes \mathsf{H}_2}_{n \text{ раз}}.$$

Зафиксируем в пространстве H_{2^n} такой ортонормированный базис

$$B^{(2^n)} = \{\mathbf{e}_{\mathbf{x}} \mid \mathbf{x} \in \mathbf{E}^n\},$$

что для каждого $\mathbf{x} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n$

$$\mathbf{e}_{\mathbf{x}} = |\alpha_1\rangle \otimes \ldots \otimes |\alpha_n\rangle.$$

Отметим, что для базисного вектора $\mathbf{e}_{\mathbf{x}} \in B^{(2^n)}$, где $\mathbf{x} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{E}^n$, используется также обозначение $|\alpha_1 \ldots \alpha_n\rangle$.

n-кубитовая система ($n \in \mathbf{N}$) представляет собой физическую систему, состояние которой представлено вектором

$$|\xi\rangle = \sum_{\mathbf{x} \in \mathbf{E}^n} \lambda_{\mathbf{x}} \cdot \mathbf{e}_{\mathbf{x}},$$

где $\lambda_{\mathbf{x}} \in \mathbf{C}$ ($\mathbf{x} \in \mathbf{E}^n$), причем

$$\sum_{\mathbf{x} \in \mathbf{E}^n} \lambda_{\mathbf{x}}^2 = 1.$$

При измерении в базисе $B^{(2^n)}$ n-кубитовая система $|\xi\rangle$ переходит в базисное состояние $|\mathbf{x}\rangle$ ($\mathbf{x} \in \mathbf{E}^n$) с вероятностью $|\lambda_{\mathbf{x}}|^2$.

Состояние n-кубитовой системы ($n \in \mathbf{N}$)

$$|\xi\rangle = \sum_{\mathbf{x} \in \mathbf{E}^n} \lambda_{\mathbf{x}} \cdot \mathbf{e}_{\mathbf{x}}$$

называется *запутанным состоянием*, если его невозможно представить в виде тензорного произведения состояний отдельных кубитов, т.е. в виде

$$|\xi\rangle = (a_1 \cdot |0\rangle + b_1 \cdot |1\rangle) \otimes \ldots \otimes (a_n \cdot |0\rangle + b_n \cdot |1\rangle),$$

где $a_j \cdot |0\rangle + b_j \cdot |1\rangle$ ($j = 1, \ldots, n$) – состояние j-го кубита системы.

Запутанные состояния не имеют классического аналога. Именно наличие таких состояний обеспечивает экспоненциальный рост пространства квантовых состояний при увеличении числа кубитов.

Исходя из положений квантовой механики, допустимыми преобразованиями n-кубитовой системы ($n \in \mathbf{N}$) являются *унитарные преобразования* пространства H_{2^n}.

Таким образом, любое квантовое вычисление представляет собой последовательность унитарных преобразований пространства H_{2^n}, за которой следует измерение. Именно эволюция состояния n-кубитовой системы ($n \in \mathbf{N}$) под действием последовательности унитарных преобразований пространства H_{2^n} обеспечивает экспоненциальное ускорение квантовых вычислений по сравнению с классическими вычислениями.

Измерение финального состояния n-кубитовой системы ($n \in \mathbf{N}$) представляет собой последовательность измерений в базисе $B^{(2)}$ состояний отдельных кубитов. На этом этапе получение того или иного результата осуществляется с соответствующей вероятностью.

Это обстоятельство является весьма привлекательным с позиции криптографии, так как именно при измерении результата появляется возможность оценить вероятность вмешательства криптоаналитика в процесс передачи информации за счет сверки отправителем и адресатом по классическому каналу тех или иных характеристик отправленной и полученной информации.

Таким образом, теория квантовых алгоритмов представляет собой симбиоз, как минимум, классической теории алгоритмов, теории унитарных операторов в конечномерных комплексных пространствах и теории вероятностей.

Из всего сказанного выше вытекает, что для осуществления квантовых вычислений требуется разработка специальных методов − *квантового программирования.* Эти методы предназначены для такого управления состоянием квантовой системы, чтобы:

1) можно было «прочитать» некоторое общее свойство всех результирующих значений (симметричность, период функции и т.д.);

2) можно было увеличить вероятность интересующего нас результата вычислений.

Простейшие унитарные преобразования, применяемые в квантовых вычислениях, принято называть *квантовыми вентилями*.

Рассмотрим некоторые квантовые вентили. Отметим, что квантовый вентиль (как и любое линейное преобразование) может быть задан как матрицей, так и своим действием на базисных векторах.

В пространстве H_2 часто применяются следующие квантовые вентили:

1) *тождественное преобразование*, определенное матрицей

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

т.е.

$$I(|0\rangle) = |0\rangle,$$
$$I(|1\rangle) = |1\rangle;$$

2) *отрицание*, определенное матрицей

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

т.е.

$$I(|0\rangle) = |0\rangle,$$
$$I(|1\rangle) = |1\rangle;$$

3) *операция сдвига по фазе*, определенная матрицей

$$Z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

т.е.

$$I(|0\rangle) = |0\rangle,$$
$$I(|1\rangle) = -|1\rangle;$$

4) композиция

$$Y = Z \cdot X,$$

определенная матрицей

$$Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

т.е.

$$I(|0\rangle) = -|1\rangle,$$
$$I(|1\rangle) = |0\rangle;$$

5) *преобразование Адамара*, определенное матрицей

$$H = \begin{pmatrix} 2^{-0.5} & 2^{-0.5} \\ 2^{-0.5} & -2^{-0.5} \end{pmatrix},$$

т.е.

$$I(|0\rangle) = 2^{-0.5} \cdot (|0\rangle + |1\rangle),$$
$$I(|1\rangle) = 2^{-0.5} \cdot (|0\rangle - |1\rangle).$$

В пространстве H_{2^2} часто применяются следующие квантовые вентили:

1) *преобразование CONTROLLED-NOT*, определенное матрицей

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

т.е. для каждого базисного вектора $|\alpha_1\alpha_2\rangle \in B^{(2^2)}$ $(\alpha_1, \alpha_2 \in \mathbf{E})$

$$C_{not}(|\alpha_1\alpha_2\rangle) = |\alpha_1\beta\rangle,$$

где

$$\beta = \begin{cases} \alpha_2, \text{ если } \alpha_1 = 0 \\ \overline{\alpha}_2, \text{ если } \alpha_1 = 1 \end{cases};$$

2) *операция обмена*, определенная матрицей

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

т.е. для каждого базисного вектора $|\alpha_1\alpha_2\rangle \in B^{(2^2)}$ $(\alpha_1, \alpha_2 \in \mathbf{E})$

$$S(|\alpha_1\alpha_2\rangle) = |\alpha_2\alpha_1\rangle.$$

В пространстве H_{2^3} часто применяются следующие квантовые вентили:

1) *операция управляемого обмена* (или *вентиль Фредкина*), следующим образом определенная через ее действие на базисных векторах

$$F(|\alpha\beta\gamma\rangle) = \begin{cases} |\alpha\beta\gamma\rangle, \text{ если } \alpha = 0 \\ |\alpha\gamma\beta\rangle, \text{ если } \alpha = 1 \end{cases} \quad (\alpha, \beta, \gamma \in \mathbf{E});$$

2) *вентиль Тоффоли*, следующим образом определенный через его действие на базисных векторах

$$T(|\alpha\beta 0\rangle) = |\alpha\beta(\alpha \,\&\, \beta)\rangle \quad (\alpha, \beta \in \mathbf{E}),$$

$$T(|\alpha\beta 1\rangle) = |\alpha\beta\overline{\alpha \,\&\, \beta}\rangle \quad (\alpha, \beta \in \mathbf{E}).$$

Из определения вентиля Тоффоли вытекает, что

$$T(|11\alpha\rangle) = |11\overline{\alpha}\rangle \quad (\alpha \in \mathbf{E}),$$

т.е. вентиль Тоффоли дает возможность реализовать операции «конъюнкция» и «отрицание».

В пространстве H_{2^n} $(n \in \mathbf{N})$ часто применяются следующие квантовые вентили:

1) *преобразование Уолша-Адамара*, определенное равенством

$$W_n = \underbrace{H \otimes \ldots \otimes H}_{n \text{ раз}} \quad (n \in \mathbf{N});$$

2) *квантовый вентиль* $U_{\mathbf{f}}$ $(\mathbf{f} \in P_2(k,m);\ k, m \in \mathbf{N};\ k + m = n)$, следующим образом определенный через его действие на базисных векторах

$$U_{\mathbf{f}}(|\mathbf{x}, \mathbf{y}\rangle) = |\mathbf{x}, \mathbf{f}(\mathbf{y})\rangle \quad (\mathbf{x} \in \mathbf{E}^k, \mathbf{y} \in \mathbf{E}^m);$$

3) *квантовое преобразование Фурье* U_{QFT}, следующим образом определенное через его действие на базисных векторах

$$U_{QFT}(|\mathbf{x}\rangle) = \frac{1}{\sqrt{2^n}} \cdot \sum_{\mathbf{y} \in \mathbf{E}^n} e^{\frac{2 \cdot \pi \cdot \mathbf{y} \cdot \mathbf{x} \cdot i}{2^n}} \cdot |\mathbf{y}\rangle \quad (\mathbf{x} \in \mathbf{E}^n),$$

где запись $\mathbf{y} \cdot \mathbf{x}$ в показателе означает произведение двух чисел, двоичными записями которых являются $\mathbf{y}$ и $\mathbf{x}$.

Известно, что квантовое преобразование Фурье U_{QFT} пространства H_{2^n} $(n \in \mathbf{N})$ может быть реализовано последовательностью из $0.5 \cdot n \cdot (n+1)$ одно- и двух-кубитовых квантовых вентилей.

Именно возможность эффективной реализации квантового преобразование Фурье и лежит в основе построения ряда полиномиальных квантовых алгоритмов (включая алгоритм факторизации П. Шора).

Отметим, что из определения преобразования Уолша-Адамара вытекает, что

$$W_n(\mathbf{e}_{(\underbrace{0,\ldots,0}_{n\ раз})}) = 2^{-0.5 \cdot n} \cdot \sum_{\mathbf{x} \in \mathbf{E}^n} \mathbf{e}_{\mathbf{x}}.$$

Преобразования Уолша-Адамара W_k $(k \in \mathbf{N})$ и квантовый вентиль $U_{\mathbf{f}}$, где $\mathbf{f} \in P_2(k,m)$ $(m \in \mathbf{N})$, лежат в основе следующей схемы организации *квантового параллелизма*:

Шаг 1. К k-кубитовой системе $(k \in \mathbf{N})$, находящейся в состоянии $\left|\underbrace{0\ldots0}_{k\ раз}\right\rangle$, применяем преобразование Уолша-Адамара W_k. Получим k-кубитовую систему, находящуюся в состоянии

$$W_k(\left|\underbrace{0\ldots0}_{k\ раз}\right\rangle) = 2^{-0.5 \cdot k} \cdot \sum_{\mathbf{x} \in \mathbf{E}^k} |\mathbf{x}\rangle.$$

Шаг 2. Добавляем регистр $\left|\underbrace{0\ldots0}_{m\ раз}\right\rangle$ к «концу» k-кубитовой системы. Получим $(k+m)$-кубитовую систему, находящуюся в состоянии

$$|\xi\rangle = 2^{-0.5 \cdot k} \cdot \sum_{\mathbf{x} \in \mathbf{E}^k} \left|\mathbf{x}, \underbrace{0\ldots0}_{m\ раз}\right\rangle.$$

Шаг 3. Применяем к $(k+m)$-кубитовой системе квантовый вентиль $U_{\mathbf{f}}$. Получим $(k+m)$-кубитовую систему, находящуюся в состоянии

$$U_{\mathbf{f}}(|\xi\rangle) = 2^{-0.5 \cdot k} \cdot \sum_{\mathbf{x} \in \mathbf{E}^k} |\mathbf{x}, \mathbf{f}(\mathbf{x})\rangle.$$

Такая схема организации параллельных вычислений дает возможность эффективно осуществлять преобразования графика отображения $\mathbf{f} \in P_2(k,m)$ $(k,m \in \mathbf{N})$, как единого целого. Это обстоятельство, а также тот фактор, что квантовое преобразование Фурье дает возможность строить отображения, чьи значения «сконцентрированы» в определенных точках, должно послужить серьезным предостережением для криптографов.

Действительно, значительное число исследований, направленных на обоснование вычислительной стойкости современных шифров, основано на сложности анализа специальных нелинейных отображений $\mathbf{f} \in P_2(k,m)$ $(k,m \in \mathbf{N})$ методами классической теории алгоритмов, которая не дает возможности эффективно работать с графиком отображения $\mathbf{f} \in P_2(k,m)$, как с единым целым.

Для теории квантовых алгоритмов, как и для классической теории алгоритмов, фундаментальной является *проблема полноты*. Известно, что:

1) *полную систему* отображений для построения комбинационных схем образуют квантовые вентили T и F;

2) *полную систему* для построения любых унитарных преобразований пространства H_{2^n} $(n \in \mathbf{N})$ образует множество отображений, содержащее квантовый вентиль C_{not} (предполагается, что C_{not} может быть применен к любой паре кубитов n-кубитовой системы), квантовые вентили

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \quad (0 \le \alpha < 2 \cdot \pi)$$

и квантовые вентили

$$\begin{pmatrix} e^{i\cdot\alpha} & 0 \\ 0 & e^{-i\cdot\alpha} \end{pmatrix} \quad (0 \le \alpha < 2 \cdot \pi).$$

В заключение отметим ряд направлений исследований в области квантовых вычислений, которые интенсивно развиваются в настоящее время.

Во-первых, это построение квантовых алгоритмов и анализ их сложности в терминах квантовой машины Тьюринга с *оракулом*, который для отображения $\mathbf{f} \in P_2(k,m)$ $(k,m \in \mathbf{N})$ определяется равенством

$$Qu_{\mathbf{f}}(|\mathbf{a},\mathbf{b}\rangle) = |\mathbf{a},\mathbf{b} \oplus \mathbf{f}(\mathbf{a})\rangle.$$

Во-вторых, это разработка методов коррекции ошибок в квантовых вычислениях.

В-третьих, это исследования в области квантовой криптографии.

1.9. Выводы.

В настоящем разделе сделана попытка дать системный анализ проблемы защиты информации и изложить математические модели и методы, применяемые в современной криптологии.

Анализ современных шифров показывает, что при их построении фрагментарно применяются комбинаторные модели и методы дискретной математики, теоретико-числовые методы, методы современной алгебры, конечно-автоматные модели над конечным полем или кольцом, а также развитый в течение последних 15-и лет аппарат теории булевых функций, предназначенный для анализа и синтеза нелинейных отображений со специальными свойствами.

Слово «фрагментарно» выбрано не случайно, так как в настоящее время отсутствует цельная математическая теория криптологии, систематически проработанная методами дискретной математики, теории систем, теории автоматов и современной алгебры. Поэтому дальнейшая разработка математических основ криптологии является сложной и актуальной проблемой. Сложность этой проблемы обусловлена еще и тем, что в течение последних 15-и лет наблюдается тесное переплетение криптологии с новыми для нее математическими теориями: хаотической динамикой и квантовыми вычислениями.

Успешное применение хаотических динамических систем при решении задач преобразования информации делает весьма привлекательным их применение в процессе решении задач защиты информации. Как следствие, возникает необходимость в систематической проработке моделей и методов, предназначенных для построения скоростных вычислительно стойких шифров и основанных на хаотической динамике.

Квантовые вычисления представляют собой математическую теорию, предназначенную для создания принципиально новых информационных технологий. Успешное применение квантовых вычислений для решения задач преобразования информации, а также отсутствие проработанной математической модели квантового компьютера обосновывают необходимость теоретического исследования вычислительной стойкости квантовых алгоритмов преобразования информации.

Таким образом, для разработки математических основ современной криптологии актуальными являются следующие задачи:

1. Исследование сложности построения высокоскоростных вычислительно стойких нестационарных поточных шифров на основе комбинаторных моделей и методов дискретной математики. К таким задачам относятся следующие задачи:

1) исследование сложности построение высокоскоростного вычислительно стойкого нестационарного поточного шифра на основе *разрушения частот* посредством регулярных комбинаторных структур дискретной математики [58,222];

2) исследование сложности построение высокоскоростного вычислительно стойкого нестационарного поточного шифра на основе *диффузии информации* посредством перестановок, порождаемых графом с почти регулярной структурой [253];

3) исследование сложности построение высокоскоростного вычислительно стойкого нестационарного поточного шифра на основе семейства автоматных моделей;

4) исследование сложности построение высокоскоростного вычислительно стойкого нестационарного поточного шифра, основанного на задаче о рюкзаке;

5) исследование сложности построения на основе автоматных моделей *нестационарного секретного замка*, предназначенного для обеспечения конфиденциального доступа пользователя к информации, содержащейся в компьютере, т.е. исследование сложности построения эффективной вычислительно стойкой аппаратно-программной реализации парольного доступа пользователя к компьютеру. Решению этих задач посвящен раздел 2.

2. Исследование сложности решения модельных задач криптографии методами хаотической динамики. Решению этой задачи посвящен раздел 3.

3. Исследование сложности обнаружения и локализации неисправностей для основных типов блоков управляемых операций перестановки и подстановки. Решению этой задачи посвящен раздел 4.

4. Исследование новых разделов теории автоматов, а именно: *автоматов над конечными кольцами* методами *теории автоматов*, *теории систем* и *современной алгебры*. Такое исследование предполагает решение, по крайней мере, следующих задач:

1) перечисление автоматов, принадлежащих заданным классам;
2) анализ классов эквивалентных состояний автомата;
3) анализ сложности различения двух автоматов;
4) анализ сложности параметрической идентификации автомата;
5) анализ сложности идентификации начального состояния автомата;
6) анализ поведения автомата при вариации его начального состояния и/или параметров.

Ясно, что сложность решения этих задач различная для линейных и нелинейных автоматов над конечным кольцом. Поэтому исследование линейных автоматов над конечным кольцом сосредоточено в разделе 5, а исследование нелинейных автоматов над конечным кольцом – в разделе 6.

5. Разработка формальных моделей атак на квантовые системы передачи информации и исследование вычислительной стойкости квантовых алгоритмов преобразования информации. Решению этой задачи посвящен раздел 7.

6. Построение в терминах теории алгебраических систем и теории автоматов структурированной модели «шифр - внешняя среда», предназначенной для унифицированного моделирования поведения существующих шифрсистем при действии атак криптоаналитика. Решению этой задачи посвящен раздел 8.

2. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ РЕШЕНИЯ МОДЕЛЬНЫХ ЗАДАЧ КРИПТОГРАФИИ

В настоящем разделе рассмотрены модели и методы решения некоторых модельных задач криптографии, основанные на применении комбинаторных структур дискретной математики [58].

В п.2.1 построена общая модель нестационарного поточного шифра, в рамках которой проводятся исследования в пп. 2.2-2.5 настоящего раздела. В п.2.2 представлен аксиоматический подход, в рамках которого предложена общая модель, предназначенная для разрушения частот в исходном тексте на основе регулярных комбинаторных структур. Исследованы две детализации предложенной модели. Для 1-й детализации в качестве регулярной комбинаторной структуры выбраны шары в векторном пространстве над полем $\mathbf{GF}(2)$ [21], а для 2-й детализации — грани единичного куба [58]. В п.2.3 построена общая модель «диффузии информации» на основе использования подгрупп симметрической группы подстановок. Исследована детализации предложенной модели, в которой подгруппа порождается графом с почти регулярной структурой. В п.2.4 построен нестационарный поточный шифр, основанный на семействе автоматных моделей. Этот шифр заслуживает особого внимания, так как один из кандидатов на современный поточный шифр, представленных в рамках европейского проекта NESSIE (шифр LEVIATHAN), основан на использовании множества бинарных деревьев. В п.2.5 построен нестационарный поточный шифр, основанный на «задаче о рюкзаке». При построении этого шифра используются сверхрастущие векторы различной длины, что дает возможность ликвидировать лазейки, присущие классическому шифру, основанному на «задаче о рюкзаке».

В п.2.6 предложена схема организации электронной цифровой подписи, основанная на использовании эллиптических кривых над полем $\mathbf{Q}$. В этой схеме, в отличие от использования эллиптических кривых над полем $\mathbf{GF}(p)$, отсутствуют проблема выбора эллиптической кривой, а также проблема поиска точек на выбранной кривой.

В п.2.7 исследуется нестационарный секретный замок, в котором «ключ» построен с использованием счетчиков (т.е. конечных автоматов специального вида), а сам «замок» — с использованием алгоритмов вычисления значений общерекурсивных функций.

2.1. Модель нестационарного поточного шифра.

В [11,69,81,82,153,217] построен ряд шифров, которые укладываются в рамки следующей общей модели.

Пусть зафиксировано семейство алгоритмов шифрования

$$\mathbf{A} = \{\mathsf{A}_i\}_{i \in \mathbf{N}_n} \quad (n \in \mathbf{N})$$

и псевдослучайные генераторы $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$. Предназначение генераторов следующее.

1. Генератор Γ_1 — это псевдослучайный генератор чисел, принадлежащих множеству $\mathbf{N}_n$. Очередное число $i \in \mathbf{N}_n$, сгенерированное генератором Γ_1, определяет выбор текущего алгоритма шифрования $\mathsf{A}_i \in \mathbf{A}$.

2. Генераторы Γ_2 и Γ_3 — это псевдослучайные генераторы двоичных последовательностей. При этом:

1) двоичная последовательность, сгенерированная генератором Γ_2, определяет выбор параметров настройки текущего алгоритма шифрования $\mathsf{A}_i \in \mathbf{A}$ $(i \in \mathbf{N}_n)$;

2) двоичная последовательность, сгенерированная генератором Γ_3, определяет выбор ключа, используемого при текущем применении алгоритма шифрования $\mathsf{A}_i \in \mathbf{A}$ $(i \in \mathbf{N}_n)$.

3. Генератор Γ_4 — это псевдослучайный генератор чисел, принадлежащих множеству $\mathbf{N}_{n_1}$ $(n_1 \in \mathbf{N})$. Очередное число $j \in \mathbf{N}_{n_1}$, сгенерированное генератором Γ_4, определяет количество блоков информационной последовательности, шифруемых алгоритмом $\mathsf{A}_i \in \mathbf{A}$ $(i \in \mathbf{N}_n)$ при текущем его применении.

Обозначим через $\mathsf{S}(\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \mathbf{A})$ нестационарный поточный шифр, схема которого представлена на рис. 2.1.

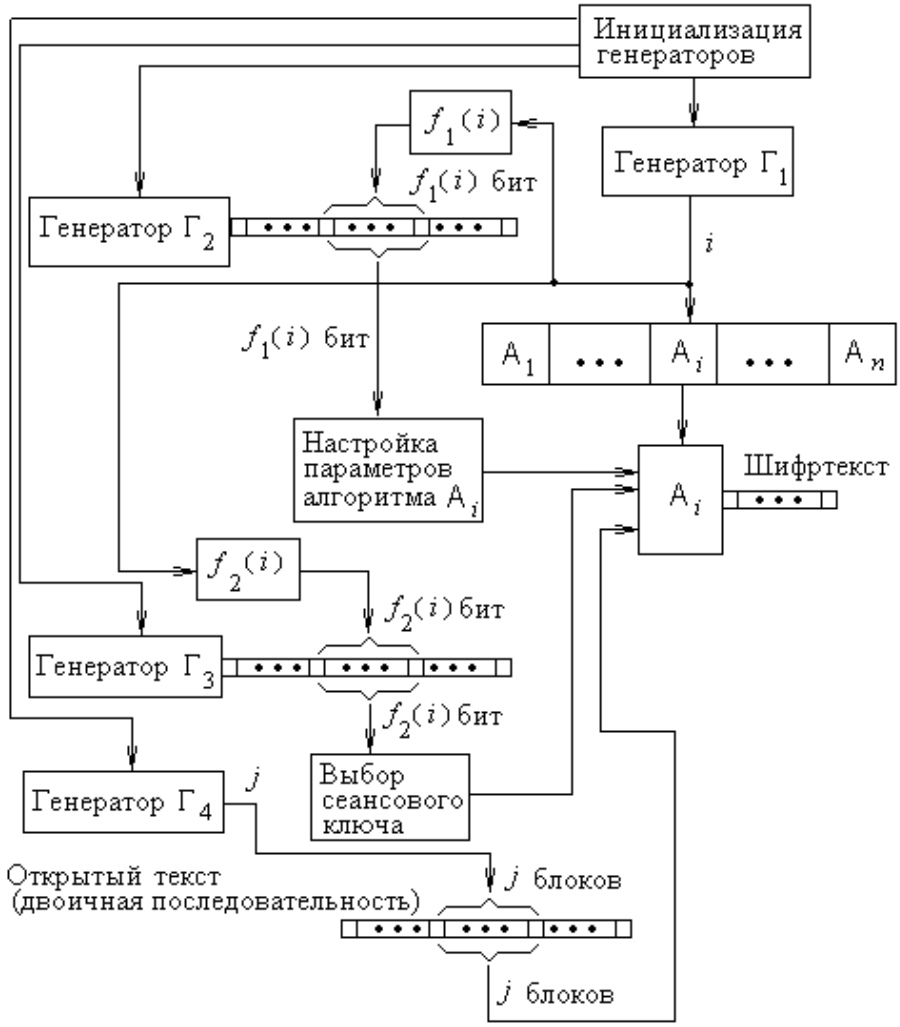


Рис. 2.1. Общая схема нестационарного поточного шифра.

Подчеркнем, что секретным ключом для шифра $\mathsf{S}(\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4,\mathbf{A})$ являются параметры, определяющие инициализацию псевдослучайных генераторов $\Gamma_1,\Gamma_2,\Gamma_3$ и Γ_4.

Для шифра $\mathsf{S}(\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4,\mathbf{A})$ отсутствуют внешние обмены между пользователями, связанные с информацией об используемых алгоритмах шифрования, о настройках этих алгоритмов, а также о сеансовых ключах. Поэтому при атаке, направленной на «взлом» секретного ключа алгоритма $\mathsf{S}(\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4,\mathbf{A})$, т.е. на идентификацию параметров, определяющих инициализацию псевдослучайных генераторов $\Gamma_1,\Gamma_2,\Gamma_3$ и Γ_4, даже при известном открытом тексте возникает следующая ситуация.

Пусть известна пара «открытый текст — шифртекст»

$$(\alpha_1\ldots\alpha_{l_1},\beta_1\ldots\beta_{l_2})\quad (l_1\le l_2). \tag{2.1}$$

Во-первых, возникает задача разбиения этих последовательностей на соответствующие блоки, т.е. представления пары (2.1) в виде

$$(\boldsymbol{\alpha}_1\ldots\boldsymbol{\alpha}_h,\boldsymbol{\beta}_1\ldots\boldsymbol{\beta}_h), \tag{2.2}$$

где $(\boldsymbol{\alpha}_r,\boldsymbol{\beta}_r)$ $(r=1,\ldots,h)$ — пара «блок открытого текста — блок шифртекста», полученная в результате работы алгоритма $\mathsf{A}_i\in\mathbf{A}$ $(i\in\mathbf{N}_n)$.

Отметим, что поиск представления (2.2) представляет собой вариант задачи тождества слов для заданных в неявном виде полугрупп.

Ясно, что этот вариант *задачи тождества слов* для полугрупп алгоритмически разрешим, так как

$$d(\boldsymbol{\alpha}_r)\le d(\boldsymbol{\beta}_r)$$

для всех $r=1,\ldots,h$.

Однако, множество допустимых решений может быть найдено только методом поиска.

По каждому представлению (2.2) методом поиска можно определить множество допустимых алгоритмов $\mathsf{A}_i\in\mathbf{A}$ $(i\in\mathbf{N}_n)$, множество допустимых параметров их настройки и множество допустимых значений сеансовых ключей.

Во-вторых, для каждого такого выбора значений методом поиска можно определить множество допустимых двоичных последовательностей, сгенерированных псевдослучайными генераторами Γ_2 и Γ_3.

В-третьих, для каждого возможного выбора последовательностей, сгенерированных псевдослучайными генераторами $\Gamma_1,\Gamma_2,\Gamma_3$ и Γ_4, возникает задача идентификации инициализации генератора по сгенерированной им последовательности.

Сложность решения последней задачи достаточно высока даже в классе псевдослучайных генераторов, построенных на основе регистров сдвига с линейной обратной связью, так как эта задача представляет собой задачу

идентификации начального состояния соответствующего автономного автомата с достаточно большим множеством состояний.

Задача идентификации параметров, определяющих инициализацию псевдослучайных генераторов $\Gamma_1, \Gamma_2, \Gamma_3$ и Γ_4, еще более усложняется, если неизвестен открытый текст.

В этом случае методом поиска можно найти множество всех возможных открытых текстов $\alpha_1 \ldots \alpha_{l_1}$, формирующих допустимые пары (2.1), а затем к каждому такому варианту применить рассмотренную выше схему идентификации параметров, определяющих инициализацию псевдослучайных генераторов $\Gamma_1, \Gamma_2, \Gamma_3$ и Γ_4.

2.2. Разрушение частот букв на основе регулярных комбинаторных структур.

Одной из типичных атак на шифр является *частотный анализ*, т.е. использование статистических свойств применяемого естественного языка и поиск слов с характерной для сообщения структурой [8,17,59,148,227,229]. Этот тип атак является основным при наличии у криптоаналитика только шифртекста, т.е. в наихудшей для криптоаналитика ситуации. Шифры неустойчивые к таким атакам принято считать *абсолютно неустойчивыми* шифрами [59].

Поэтому разработка методов, обеспечивающих стойкость шифра к частотному анализу, – актуальная задача при построении любых вычислительно стойких коммерческих шифров.

Решение этой задачи, предложенное в [153], сводится к тому, чтобы на этапе предвычислений снабдить схему шифрования дискретным преобразователем, осуществляющим разрушение частот в двоичной последовательности, представляющей исходный текст (рис. 2.2).

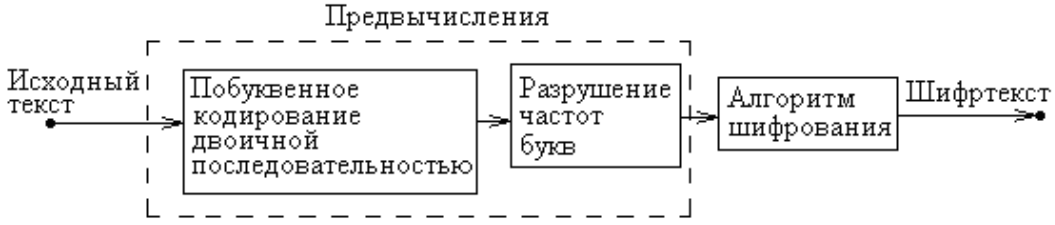


Рис. 2.2. Положение дискретного преобразователя, осуществляющего разрушение частот букв в схеме шифрования.

Побуквенное кодирование исходного текста двоичной последовательностью осуществляется обычным образом, и укладывается в рамки следующей модели.

Предположим, что зафиксирован конечный алфавит Σ, а исходные сообщения образуют бесконечный язык $L \subseteq \Sigma^+$, причем каждая буква алфавита Σ встречается, по крайней мере, в одном слове $u \in L$.

Положим

$$l_1 = \lceil \log |\Sigma| \rceil . \qquad (2.3)$$

Зафиксируем инъективное отображение $cdng : \Sigma \to \mathbf{E}^{l_1}$.

Расширим это отображение на множество Σ^+ в соответствии с равенством:

$$cdng(\sigma_1 \ldots \sigma_n) = cdng(\sigma_1) \ldots cdng(\sigma_n) . \qquad (2.4)$$

Из (2.4) вытекает, что язык

$$cdng(L) = \{cdng(u) \mid u \in L\}$$

является языком в алфавите

$$cdng(\Sigma) = \{cdng(\sigma) \mid \sigma \in \Sigma\},$$

причем в силу (2.3)

$$d(cdng(u)) = l_1 \cdot d(u) \quad (u \in \Sigma^+) \qquad (2.5)$$

и для любого слова $u \in \Sigma^+$

$$d_{cdng(\Sigma)}(cdng(u)) = d(u), \qquad (2.6)$$

где $d_{cdng(\Sigma)}(cdng(u))$ — это длина слова $cdng(u)$ в алфавите $cdng(\Sigma)$.

Таким образом, отображение $cdng$ определяет такое инъективное вложение языка L во множество $\bigcup_{u \in L} \mathbf{E}^{l_1 \cdot d(u)}$, что $cdng(u) \in \mathbf{E}^{l_1 \cdot d(u)}$ для всех $u \in L$.

Алгоритм побуквенного кодирования исходного текста двоичными последовательностями — это любой алгоритм, вычисляющий значение $cdng(\sigma)$ $(\sigma \in \Sigma)$ с временной и емкостной сложностью, соответственно, равной

$$T_{cdng} = O(\lceil \log |\Sigma| \rceil) \quad (|\Sigma| \to \infty)$$

и

$$V_{cdng} = O(|\Sigma| \cdot \lceil \log |\Sigma| \rceil) \quad (|\Sigma| \to \infty).$$

Эффективность представленной на рис. 2.2 системы шифрования для легальных пользователей и ее стойкость к криптоанализу существенно зависят от *комбинаторных структур*, применяемых в процессе разрушения частот букв.

Поэтому важными характеристиками являются возможность компактного представления используемой комбинаторной структуры в неявном виде и существование эффективного алгоритма порождения элементов этой структуры одного за другим в явном виде. Комбинаторные структуры, обладающие этими двумя свойствами, назовем *регулярными комбинаторными структурами*.

Формально «регулярная комбинаторная структура» может быть определена следующим образом.

Обозначим через $n(u,\sigma)$ $(u \in \Sigma^+, \sigma \in \Sigma)$ число вхождений буквы σ в слово u.

Ясно, что для любого слова $u \in \Sigma^+$

$$\sum_{\sigma \in \Sigma} n(u,\sigma) = d(u). \tag{2.7}$$

Кроме того,

$$n(cdng(u), cdng(\sigma)) = n(u,\sigma) \tag{2.8}$$

для любого слова $u \in \Sigma^+$ и для всех $\sigma \in \Sigma$.

Положим

$$L(k) = \{u \in L \mid d(u) \le k\} \ \ (k \in \mathbf{N})$$

и

$$\nu(L(k),\sigma) = \frac{\sum\limits_{u \in L(k)} n(u,\sigma)}{\sum\limits_{u \in L(k)} d(u)} \quad (k \in \mathbf{N}, \sigma \in \Sigma). \tag{2.9}$$

Из (2.7) и (2.9) вытекает, что

$$\sum_{\sigma \in \Sigma} \nu(L(k),\sigma) = 1.$$

Кроме того, из (2.6), (2.8) и (2.9) вытекает, что

$$\nu(cdng(L(k)), cdng(\sigma)) = \nu(L(k),\sigma) \quad (k \in \mathbf{N}, \sigma \in \Sigma). \tag{2.10}$$

Предположим, что для каждого $\sigma \in \Sigma$ существует предел

$$\lim_{k \to \infty} \nu(L(k),\sigma) = a(\sigma) > 0. \tag{2.11}$$

Из (2.11) вытекает, что для любого фиксированного числа $\varepsilon > 0$ для каждого $\sigma \in \Sigma$ существует такое число $k_0(\sigma,\varepsilon) \in \mathbf{N}$, что

$$|\nu(L(k),\sigma) - a(\sigma)| < \varepsilon \tag{2.12}$$

для всех $k \ge k_0(\sigma,\varepsilon)$ $(k \in \mathbf{N})$.

Зафиксируем такое достаточно малое число $\varepsilon > 0$, что

$$a(\sigma) - \varepsilon > 0 \quad (\sigma \in \Sigma). \tag{2.13}$$

Пусть

$$k_0(\varepsilon) = \max\{k_0(\sigma,\varepsilon) \mid \sigma \in \Sigma\}. \tag{2.14}$$

Положим

$$frqnc(L,\sigma) = \nu(L(k_0(\varepsilon)),\sigma). \tag{2.15}$$

Назовем число $frqnc(L,\sigma)$ $(\sigma \in \Sigma)$ *относительной частотой появления буквы* $\sigma \in \Sigma$ *в словах языка* L.

Из (2.12-2.15) вытекает, что

$$frqnc(L,\sigma) > 0 \quad (\sigma \in \Sigma). \tag{2.16}$$

В дальнейшем предполагается, что относительная частота $frqnc(L,\sigma)$ появления каждой буквы $\sigma \in \Sigma$ в словах языка L представлена двоичной дробью и вычислена с точностью до 2^{-r} $(r \in \mathbf{N})$, причем

$$\sum_{\sigma \in \Sigma} frqnc(L,\sigma) = 1. \tag{2.17}$$

Из (2.10) вытекает, что

$$frqnc(cdng(L), cdng(\sigma)) = frqnc(L,\sigma) \ (\sigma \in \Sigma),$$

т.е. относительные частоты букв в словах языков L и $cdng(L)$ совпадают.

Отсюда вытекает корректность построения комбинаторных структур в терминах языка $cdng(L)$ и относительных частот букв в словах языка L.

Для краткости записи относительную частоту $frqnc(L,\sigma)$ $(\sigma \in \Sigma)$ появления буквы σ в словах языка L будем обозначать $frqnc(\sigma)$.

Зафиксируем число $h \in \mathbf{N}$ $(h \geq r)$ и такое число $l_2 \in \mathbf{N}$, что

$$l_2 \geq l_1 + h. \tag{2.18}$$

Определение 2.1. Регулярной комбинаторной структурой для языка $L \subseteq \Sigma^+$ назовем бинарное отношение

$$\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2},$$

удовлетворяющее следующим пяти условиям:

Условие 2.1. Истинно равенство

$$pr_1 \Delta = cdng(\Sigma). \tag{2.19}$$

Условие 2.2. Для всех $\sigma \in \Sigma$ истинно равенство

$$|\Delta(cdng(\sigma))| = 2^r \cdot frqnc(\sigma). \tag{2.20}$$

Условие 2.3. Для всех $\sigma_1, \sigma_2 \in \Sigma$ $(\sigma_1 \neq \sigma_2)$ истинно равенство

$$\Delta(cdng(\sigma_1)) \cap \Delta(cdng(\sigma_2)) = \varnothing. \tag{2.21}$$

Условие 2.4. Емкостная сложность представления каждого множества $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ в неявном виде равна

$$V_{\Delta(cdng(\sigma))} = O(l_2) \quad (|\Sigma| \to \infty). \tag{2.22}$$

Условие 2.5. Существует алгоритм A, который при фиксированной начинающейся с нуля нумерации элементов любого множества $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ порождает 0-й элемент множества $\Delta(cdng(\sigma))$ и по j-му элементу $(j = 0,1,\ldots,|\Delta(cdng(\sigma)|-1)$ множества $\Delta(cdng(\sigma))$ порождает $(j+1)(\bmod |\Delta(cdng(\sigma))|)$-й элемент множества $\Delta(cdng(\sigma))$ с временной и емкостной сложностью, соответственно, равной

$$T_{\mathsf{A}} = O(l_2) \quad (l_2 \to \infty) \tag{2.23}$$

и

$$V_{\mathsf{A}} = O(l_2) \quad (l_2 \to \infty). \tag{2.24}$$

Бинарное отношение Δ схематически изображено на рис. 2.3.

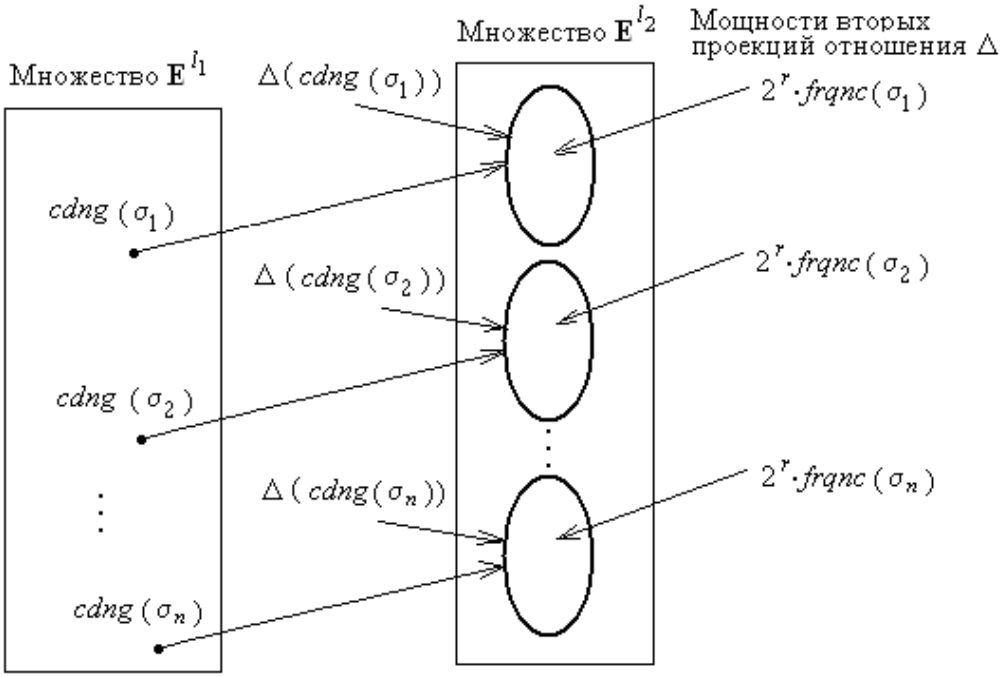


Рис. 2.3. Схематическое представление бинарного отношения Δ.

Теорема 2.1. Для языка $L \subseteq \Sigma^+$ множество регулярных комбинаторных структур — непустое множество.

Доказательство. Достаточно показать, что существует регулярная комбинаторная структура для языка $L \subseteq \Sigma^+$ в случае, когда

$$l_2 = l_1 + h. \tag{2.25}$$

Предположим, что равенство (2.25) истинно.

Пусть $S_{\sigma,h}$ $(\sigma \in \Sigma)$ — это множество всех таких последовательностей $\alpha_\sigma \uparrow\uparrow 0^{h-r} \in \mathbf{E}^h$ $(\alpha_\sigma \in \mathbf{E}^r)$, что α_σ — двоичное представление числа, принадлежащего множеству $\{0,1,\ldots,2^r \cdot frqnc(\sigma)-1\}$.

Определим бинарное отношение

$$\Delta_h \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$$

равенством

$$\Delta_h = \bigcup_{\sigma \in \Sigma} \{(cdng(\sigma), (cdng(\sigma) \uparrow\uparrow \alpha_\sigma \uparrow\uparrow 0^{h-r}) \mid \alpha_\sigma \uparrow\uparrow 0^{h-r} \in S_{\sigma,h}\}. \tag{2.26}$$

Из (2.26) вытекает, что для бинарного отношения Δ_h

$$pr_1 \Delta_h = cdng(\Sigma)$$

и

$$|\Delta_h(cdng(\sigma))| = 2^r \cdot frqnc(\sigma) \quad (\sigma \in \Sigma),$$

т.е. для бинарного отношения Δ_h выполнены условия 2.1 и 2.2.

А так как $cdng$ — инъективное отображение, то из (2.26) вытекает, что для всех $\sigma_1, \sigma_2 \in \Sigma$ $(\sigma_1 \neq \sigma_2)$

$$(cdng(\sigma_1), (cdng(\sigma_1) \uparrow\uparrow \alpha_{\sigma_1} \uparrow\uparrow 0^{h-r})) \neq$$
$$\neq (cdng(\sigma_2), (cdng(\sigma_2) \uparrow\uparrow \alpha_{\sigma_2} \uparrow\uparrow 0^{h-r}))$$

при всех $\alpha_{\sigma_1} \uparrow\uparrow 0^{h-r} \in S_{\sigma_1,h}$ и $\alpha_{\sigma_2} \uparrow\uparrow 0^{h-r} \in S_{\sigma_2,h}$, т.е.

$$\Delta_h(cdng(\sigma_1)) \cap \Delta_h(cdng(\sigma_2)) = \varnothing \quad (\sigma_1, \sigma_2 \in \Sigma; \sigma_1 \neq \sigma_2).$$

Таким образом, для бинарного отношения Δ_h выполнено условие 2.3.

Из (2.26) вытекает, что представлением каждого множества $\Delta_h(cdng(\sigma))$ $(\sigma \in \Sigma)$ в неявном виде является упорядоченная тройка $(cdng(\sigma), 2^r \cdot frqnc(\sigma), h-r)$. Следовательно, емкостная сложность представления каждого множества $\Delta_h(cdng(\sigma))$ $(\sigma \in \Sigma)$ в неявном виде равна

$$V_{\Delta_h(cdng(\sigma))} = O(l_2) \quad (|\Sigma| \to \infty),$$

т.е. для бинарного отношения Δ_h выполнено условие 2.4.

Зафиксируем такую нумерацию элементов множества $\Delta_h(cdng(\sigma))$ $(\sigma \in \Sigma)$, что номер любого элемента $cdng(\sigma) \uparrow\uparrow \alpha \uparrow\uparrow 0^{h-r} \in \Delta_h(cdng(\sigma))$ $(\alpha_\sigma \uparrow\uparrow 0^{h-r} \in S_{\sigma,h})$ совпадает с тем двоичным числом, которое представляет последовательность α. Из (2.26) вытекает, что выполнено условие 2.5.

Теорема доказана.

Отметим, что из (2.17) и (2.19)-(2.21) вытекает, что для любой регулярной комбинаторной структуры Δ $(\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2})$ истинно равенство

$$|\, pr_2 \Delta\,| = 2^r. \qquad (2.27)$$

Построим математическую модель дискретного преобразователя, осуществляющего разрушения частот букв в словах языка $cdng(L)$ и основанного на использовании регулярной комбинаторной структуры Δ $(\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2})$.

Обозначим через $\mathsf{A}(\sigma, j)$ $(\sigma \in \Sigma,\ j \in \mathbf{Z}_{|\Delta(cdng(\sigma))|})$ j-й элемент множества $\Delta(cdng(\sigma))$, порождаемый алгоритмом A, а через $CNTR$ – одномерный массив длины $|\Sigma|$, элементы которого занумерованы элементами множества $cdng(\Sigma)$. Положим

$$\mathrm{Q} = \{CNTR \mid 0 \le CNTR(cdng(\sigma)) \le |\,\Delta(cdng(\sigma))\,| \text{ для всех } \sigma \in \Sigma\}.$$

Отметим, что массив $CNTR \in \mathrm{Q}$ предназначен для подсчета (по $\mathrm{mod}\,|\,\Delta(cdng(\sigma))\,|$) числа вхождений каждой буквы $cdng(\sigma) \in cdng(\Sigma)$ $(\sigma \in \Sigma)$ в заданное слово

$$cdng(u) = cdng(\sigma_1) \ldots cdng(\sigma_n) \in cdng(L).$$

Обозначим через $GNRT(\mathrm{Q})$ псевдослучайный выбор элемента $CNTR \in \mathrm{Q}$, т.е. такое заполнение при помощи псевдослучайного генератора массива $CNTR$ неотрицательными целыми числами, что

$$0 \le CNTR(cdng(\sigma)) \le |\Delta(cdng(\sigma))|$$

для всех $\sigma \in \Sigma$.

Рассмотрим следующий алгоритм преобразования слова

$$cdng(u) = cdng(\sigma_1)\ldots cdng(\sigma_n) \in cdng(L)$$

в слово в алфавите $pr_2\Delta$.

Алгоритм 2.1.

Шаг 1. $result := \Lambda$, $CNTR := GNRT(\mathrm{Q})$, $i := 1$.

Шаг 2. $CNTR(cdng(\sigma_i)) := (CNTR(cdng(\sigma_i)) + 1) \pmod{|\Delta(cdng(\sigma_i))|}$.

Шаг 3. $b_i := \mathsf{A}(\sigma_i, CNTR(cdng(\sigma_i)))$.

Шаг 4. $result := result \uparrow\uparrow b_i$, $i := i + 1$.

Шаг 5. Если $i \le n$, то переход к шагу 2, иначе конец.

Обозначим через $\mathsf{B}(cdng(u))$ слово в алфавите $pr_2\Delta$, в которое алгоритм 2.1 переводит слово $cdng(u) \in cdng(L)$. Положим

$$\mathsf{L} = \{\mathsf{B}(cdng(u)) \mid u \in L\}.$$

Из (2.21) вытекает, что алгоритм 2.1 осуществляет инъекцию языка L в язык L. При этом, для любого слова $cdng(u) \in cdng(L)$

$$d_{pr_2\Delta}(\mathsf{B}(cdng(u))) = d(u), \tag{2.28}$$

где $d_{pr_2\Delta}(\mathsf{B}(cdng(u)))$ — длина слова $\mathsf{B}(cdng(u))$ в алфавите $pr_2\Delta$.

Теорема 2.2. Относительная частота появления каждой буквы $x \in pr_2\Delta$ в словах языка L равна 2^{-r}.

Доказательство. Из (2.28) вытекает, что

$$\nu(\mathsf{L}(k), x) = \frac{\sum\limits_{u \in L(k)} n(\mathsf{B}(cdng(u)), x)}{\sum\limits_{u \in L(k)} d(u)} \quad (k \in \mathbf{N},\ x \in pr_2\Delta).$$

При этом

$$\sum_{x \in pr_2\Delta} \nu(\mathsf{L}(k), x) = 1 \quad (k \in \mathbf{N}). \tag{2.29}$$

Следовательно,

$$\lim_{k \to \infty} \sum_{x \in pr_2\Delta} \nu(\mathsf{L}(k), x) = 1,$$

т.е.

$$\sum_{x \in pr_2\Delta} frqnc(\mathsf{L}, x) = 1. \tag{2.30}$$

Из шагов 2-4 алгоритма 2.1 вытекает, что алгоритм 2.1 построен таким образом, что для любого слова $cdng(u) \in cdng(L)$

$$n(\mathsf{B}(cdng(u)), x) \le \frac{n(u,\sigma)}{|\Delta(cdng(\sigma))|} + 1 \quad (x \in \Delta(cdng(\sigma))).$$

Следовательно, для всех $x \in \Delta(cdng(\sigma))$

$$\nu(\mathsf{L}(k), x) \le \frac{\sum\limits_{u \in L(k)} \left(\frac{n(u,\sigma)}{|\Delta(cdng(\sigma))|} + 1 \right)}{\sum\limits_{u \in L(k)} d(u)} =$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot \frac{\sum\limits_{u \in L(k)} n(u,\sigma)}{\sum\limits_{u \in L(k)} d(u)} + \frac{\sum\limits_{u \in L(k)} 1}{\sum\limits_{u \in L(k)} d(u)} =$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot \frac{\sum\limits_{u \in L(k)} n(u,\sigma)}{\sum\limits_{u \in L(k)} d(u)} + \frac{|\mathsf{L}(k)|}{\sum\limits_{u \in L(k)} d(u)}.$$

Отсюда вытекает, что для всех $x \in \Delta(cdng(\sigma))$

$$frqnc(\mathsf{L}, x) = \lim_{k \to \infty} \nu(\mathsf{L}(k), x) \le$$

$$= \lim_{k \to \infty} \left(\frac{1}{|\Delta(cdng(\sigma))|} \cdot \frac{\sum\limits_{u \in L(k)} n(u,\sigma)}{\sum\limits_{u \in L(k)} d(u)} + \frac{|\mathsf{L}(k)|}{\sum\limits_{u \in L(k)} d(u)} \right) =$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot \lim_{k \to \infty} \frac{\sum\limits_{u \in L(k)} n(u,\sigma)}{\sum\limits_{u \in L(k)} d(u)} + \lim_{k \to \infty} \frac{|\mathsf{L}(k)|}{\sum\limits_{u \in L(k)} d(u)} = \tag{2.31}$$

$$= \frac{1}{|\Delta(cdng(\sigma))|} \cdot frqnc(L,\sigma) + \lim_{k \to \infty} \frac{|\mathsf{L}(k)|}{\sum\limits_{u \in L(k)} d(u)}.$$

Так как L — бесконечный язык, то

$$\lim_{k \to \infty} \frac{|\mathsf{L}(k)|}{\sum\limits_{u \in L(k)} d(u)} = 0. \tag{2.32}$$

Из (2.20), (2.31) и (2.32) вытекает, что для всех $x \in \Delta(cdng(\sigma))$

$$frqnc(\mathsf{L}, x) \le \frac{1}{|\Delta(cdng(\sigma))|} \cdot frqnc(L,\sigma) =$$

$$= \frac{1}{2^r \cdot frqnc(L,\sigma)} \cdot frqnc(L,\sigma) = 2^{-r}.$$

Предположим, что существует такое $x \in \Delta(cdng(\sigma))$, что

$$frqnc(\mathsf{L}, x) < 2^{-r}. \tag{2.33}$$

Из (2.27), (2.30) и (2.33) вытекает, что

$$1 = \sum_{x \in pr_2\Delta} frqnc(\mathsf{L}, x) < \sum_{x \in pr_2\Delta} 2^{-r} = 2^r \cdot 2^{-r} = 1.$$

Получено противоречие. Следовательно, предположение — ложное.

Отсюда вытекает, что

$$frqnc(\mathsf{L}, x) = 2^{-r}$$

для всех $x \in \Delta(cdng(\sigma))$.

Теорема доказана.

Теорема 2.3. Временная и емкостная сложность преобразования посредством алгоритма 2.1 слова

$$cdng(u) = cdng(\sigma_1)\ldots cdng(\sigma_n) \in cdng(L)$$

в слово в алфавите $pr_2\Delta$ равна, соответственно,

$$T_{2.1}(n) = O(T_{GNRT}(|\Sigma|) + n \cdot l_2 \cdot 2^r) \quad (|\Sigma| \to \infty) \tag{2.34}$$

и

$$V_{2.1}(n) = O(V_{GNRT}(|\Sigma|) + l_2 \cdot |\Sigma| + n \cdot l_2) \quad (|\Sigma| \to \infty), \tag{2.35}$$

где $T_{GNRT}(|\Sigma|)$ и $V_{GNRT}(|\Sigma|)$ — соответственно, временная и емкостная сложность заполнения массива $CNTR$ при помощи псевдослучайного генератора такими числами, что $0 \le CNTR(\sigma) \le |\Delta(cdng(\sigma))|$ $(\sigma \in \Sigma)$.

Доказательство. Временная сложность шага 1 алгоритма 2.1 равна

$$T_1 = O(T_{GNRT}(|\Sigma|)) \ (|\Sigma| \to \infty). \tag{2.36}$$

Оценим временную сложность цикла, определяемого шагами 2-5 алгоритма 2.1.

Временная сложность выполнения как шага 2, так и шага 4 равна

$$T_2 = O(l_2) \quad (|\Sigma| \to \infty). \tag{2.37}$$

Из условия 2.5 вытекает, что временная сложность 1-го исполнения шага 3 равна

$$T_3' = O(l_2 \cdot 2^r) \quad (|\Sigma| \to \infty), \tag{2.38}$$

а для каждого последующего исполнения шага 2

$$T_3'' = O(l_2) \ (|\Sigma| \to \infty). \tag{2.39}$$

Временная сложность выполнения шага 5 равна

$$T_4 = O(1) \quad (|\Sigma| \to \infty). \tag{2.40}$$

Из (2.37)-(2.40) вытекает, что временная сложность цикла, определяемого шагами 2-5 алгоритма 2.1 равна

$$T_2 = O(l_2 \cdot 2^r) \quad (|\Sigma| \to \infty). \tag{2.41}$$

Из (2.36) и (2.41) вытекает, что

$$T_{2.1}(n) = O(T_{GNRT}(|\Sigma|) + n \cdot l_2 \cdot 2^r) \quad (|\Sigma| \to \infty),$$

т.е. что формула (2.34) истинна.

Емкостная сложность шага 1 алгоритма 2.1 равна

$$V_1 = O(V_{GNRT}(|\Sigma|)) \quad (|\Sigma| \to \infty). \tag{2.42}$$

Оценим объем памяти необходимой для реализации цикла, определяемого шагами 2-5 алгоритма 2.1.

Объем памяти, необходимой для хранения вычисленных в процессе работы алгоритма 2.1 текущих значений $\mathsf{A}(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ равен

$$V_2 = O(l_2 \cdot |\Sigma|) \quad (|\Sigma| \to \infty). \tag{2.43}$$

Объем памяти необходимой для реализации как шага 2, так и шага 3 равен

$$V_3 = O(l_2) \quad (|\Sigma| \to \infty). \tag{2.44}$$

Объем памяти, необходимой для реализации шага 4 равен

$$V_4 = O(n \cdot l_2) \quad (|\Sigma| \to \infty). \tag{2.45}$$

Объем памяти, необходимой для реализации шага 5 равен

$$V_5 = O(n) \quad (|\Sigma| \to \infty). \tag{2.46}$$

Из (2.42)-(2.46) вытекает, что

$$V_{2.1}(n) = O(V_{GNRT}(|\Sigma| + l_2 \cdot |\Sigma| + n \cdot l_2) \quad (|\Sigma| \to \infty),$$

т.е. что формула (2.35) истинна.

Теорема доказана.

Замечание 2.1. Секретным «сеансовым ключом» для алгоритма 2.1 являются параметры настройки псевдослучайного генератора $GNRT$.

Из (2.34), (2.36), (2.38) и (2.39) вытекает, что временная сложность алгоритма 2.1 во многом определяется именно исполнением шага 1 и первым исполнением шага 3.

Ни массив $GNRT(\mathrm{Q})$, ни исходные значения $\mathsf{A}(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ не зависят от слова $cdng(u) \in cdng(L)$, преобразуемого алгоритмом 2.1.

Следовательно, если «разворачивание ключа», т.е. вычисление массива $GNRT(\mathrm{Q})$ и массива исходных значений $\mathsf{A}(\sigma, CNTR(cdng(\sigma)))$ $(\sigma \in \Sigma)$ вынести за рамки алгоритма 2.1 (т.е. на этап предвычислений), то асимптотическая временная сложность преобразования посредством алгоритма 2.1 слова

$$cdng(u) = cdng(\sigma_1) \ldots cdng(\sigma_n) \in cdng(L)$$

в слово в алфавите $pr_2\Delta$ равна

$$T_{2.1}(n) = O(n \cdot l_2) \quad (|\Sigma| \to \infty). \tag{2.47}$$

Из (2.47) вытекает, что полное разрушение частот букв посредством использования регулярных комбинаторных структур осуществимо с «линейным замедлением».

Охарактеризуем вычислительную стойкость алгоритма 2.1, рассматриваемого как поточный шифр.

Предположим вначале, что криптоаналитик совершает атаку на основе заранее выбранного исходного текста.

Пусть $\Sigma = \{\sigma_1, \ldots, \sigma_{|\Sigma|}\}$. Подадим на вход алгоритма 2.1 слово $(cdng(\sigma_1))^{a_1} \ldots (cdng(\sigma_{|\Sigma|}\})^{a_{|\Sigma|}}$, где $a_1, \ldots, a_{|\Sigma|} \in \mathbf{N}$ — такие достаточно большие числа, что заведомо истинны неравенства $a_i > |\Delta(cdng(\sigma_i))|$ $(i = 1, \ldots, |\Sigma|)$. Ясно, что выход алгоритма 2.1 дает возможность вычислить как число l_2, так и каждое из множеств $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$.

Таким образом, алгоритм 2.1 не является вычислительно стойким относительно атаки на основе заранее подобранного исходного текста.

Предположим теперь, что криптоаналитик совершает атаку только на основе известного шифртекста.

Алгоритм 2.1 полностью разрушает частоты букв в словах языка $cdng(L)$ и использует в качестве секретного «сеансового ключа» параметры настройки псевдослучайного генератора *GNRT*. Поэтому даже при фиксированной нумерации элементов множеств $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ восстановление слова $cdng(u)$ по слову $\mathsf{B}(cdng(u))$ сводится, фактически, к полному перебору вариантов.

Это означает, что алгоритм 2.1 является вычислительно стойким относительно атаки только на основе известного шифртекста.

Ясно, что сложность восстановления слова $cdng(u)$ по слову $\mathsf{B}(cdng(u))$ возрастает, если в алгоритм 2.1 включить управление нумерацией элементов множеств $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ посредством псевдослучайного генератора.

Эта сложность становится еще выше, если криптоаналитику неизвестно число l_2.

Охарактеризуем *имитостойкость* алгоритма 2.1.

Изменение значений группы бит искажает ограниченный объем передаваемого сообщения. Такое вмешательство криптоаналитика часто обнаруживается за счет искажения смысла сообщения, либо за счет невозможности расшифровки измененного фрагмента последовательности. При этом подозрительные биты могут быть локализованы по окончанию процесса расшифровки.

В то же время, изменение криптоаналитиком длины последовательности может привести к разрушению финального отрезка сообщения.

Покажем, что в алгоритме 2.1 в качестве регулярных комбинаторных структур, предназначенных для детализации бинарного отношения $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$, могут быть выбраны как шары фиксированного радиуса [21], так и грани единичного куба [58].

Пример 2.1. Пусть ρ – *расстояние* (по Хеммингу) в множестве $\mathbf{E}^{l_2}$, т.е.

$$\rho(\mathbf{v}', \mathbf{v}'') = wt(\mathbf{v}' \oplus \mathbf{v}'') \quad (\mathbf{v}', \mathbf{v}'' \in \mathbf{E}^{l_2}),$$

где $wt(\mathbf{v}) = \sum_{i=1}^{l_2} v_i \quad (\mathbf{v} = (v_1, \ldots, v_l) \in \mathbf{E}^{l_2})$ – *вес* вектора $\mathbf{v}$.

Шаром радиуса R с центром в точке $\mathbf{v} \in \mathbf{E}^{l_2}$ называется множество

$$S_R(\mathbf{v}) = \{\mathbf{v}' \in \mathbf{E}^{l_2} \mid \rho(\mathbf{v}, \mathbf{v}') \le R\}.$$

Известно, что

$$|S_R(\mathbf{v})| = \sum_{j=0}^{R} \binom{l_2}{j} \quad (\mathbf{v} \in \mathbf{E}^{l_2}).$$

Ясно, что для того, чтобы представить в неявном виде шар $S_R(\mathbf{v}) \quad (\mathbf{v} \in \mathbf{E}^{l_2})$, достаточно хранить пару $(\mathbf{v}, R)$, что осуществимо с емкостной сложностью $O(l_2)$.

Пусть $l_2 = (m+n) \cdot k \quad (m, n, k \in \mathbf{N})$. Положим

$$\mathbf{v}_0 = (\underbrace{\mathbf{1}, \ldots, \mathbf{1}}_{m \text{ раз}}, \underbrace{\mathbf{0}, \ldots, \mathbf{0}}_{n \text{ раз}}) \in \mathbf{E}^{l_2},$$

где

$$\mathbf{1} = \underbrace{1, \ldots, 1}_{k \text{ раз}}$$

и

$$\mathbf{0} = \underbrace{0, \ldots, 0}_{k \text{ раз}}.$$

Определим операцию $prmt_{i,j} \quad (i = 1, \ldots, m;\ j = 1, \ldots, n)$ равенством

$$prmt_{i,j}(\mathbf{v}_0) = (\underbrace{\mathbf{1}, \ldots, \mathbf{1}}_{i-1 \text{ раз}}, \mathbf{0}, \underbrace{\mathbf{1}, \ldots, \mathbf{1}}_{m-i \text{ раз}}, \underbrace{\mathbf{0}, \ldots, \mathbf{0}}_{j-1 \text{ раз}}, \mathbf{1}, \underbrace{\mathbf{0}, \ldots, \mathbf{0}}_{n-j \text{ раз}}).$$

Ясно, что:

1) для любых $i = 1, \ldots, m$ и $j = 1, \ldots, n$

$$wt(prmt_{i,j}(\mathbf{v}_0)) = m \cdot k;$$

2) если либо $i_1 \ne i_2$ и $j_1 = j_2$, либо $i_1 = i_2$ и $j_1 \ne j_2$, то

$$\rho(prmt_{i_1,j_1}(\mathbf{v}_0), prmt_{i_2,j_2}(\mathbf{v}_0)) = 2 \cdot k;$$

3) если $i_1 \ne i_2$ и $j_1 \ne j_2$, то

$$\rho(prmt_{i_1,j_1}(\mathbf{v}_0), prmt_{i_2,j_2}(\mathbf{v}_0)) = 4 \cdot k;$$

4) если $i_1 \ne i_2$ или $j_1 \ne j_2$, то

$$S_{k-1}(prmt_{i_1,j_1}(\mathbf{v}_0)) \cap S_{k-1}(prmt_{i_2,j_2}(\mathbf{v}_0)) = \varnothing;$$

5) для любых $i = 1, \ldots, m$ и $j = 1, \ldots, n$

$$|S_{k-1}(prmt_{i,j}(\mathbf{v}_0))| = \sum_{u=0}^{k-1} \binom{l_2}{u}.$$

Пусть числа $m, n \in \mathbf{N}$ выбраны так, что:

1) истинно неравенство $m \cdot n \geq |\Sigma|$;
2) истинно неравенство

$$\sum_{u=0}^{k-1} \binom{l_2}{u} \geq \max\{2^r \cdot frqnc(\sigma) \mid \sigma \in \Sigma\}.$$

Зафиксируем любые $|\Sigma|$ элемента $\mathbf{v}(\sigma)$ $(\sigma \in \Sigma)$ множества

$$\{prmt_{i,j}(\mathbf{v}_0) \mid i = 1,\ldots,m;\ j = 1,\ldots,n\}.$$

Занумеруем элементы каждого шара $S_{k-1}(\mathbf{v}(\sigma))$ $(\sigma \in \Sigma)$.

В качестве множества $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ выберем первые $k \cdot frqnc(\sigma)$ элемента множества $S_{k-1}(\mathbf{v}(\sigma))$. Для построенного бинарного отношения Δ расшифровка каждого блока $\mathbf{v} \in \mathbf{E}^{l_2}$ сводится к выбору такого единственного элемента $\mathbf{v}(\sigma) \in \{\mathbf{v}(\sigma') \mid \sigma' \in \Sigma\}$, что $\rho(\mathbf{v}, \mathbf{v}(\sigma)) \leq k-1$.

Итак, построено бинарное отношение $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$ на основе выбора шаров радиуса $k-1$ с центрами веса $m \cdot k$.

Пример 2.2. Построим бинарное отношение $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$ на основе выбора граней единичного куба (отметим, что один из вариантов такого отношения построен при доказательстве теоремы 2.1).

Зафиксируем такие числа $i_1,\ldots,i_{l_1} \in \mathbf{N}$, что $1 \leq i_1 < \ldots < i_{l_1} \leq l_2$.

Вектор $cdng(\sigma) = (\alpha_1,\ldots,\alpha_{l_1}) \in \mathbf{E}^{l_1}$ $(\sigma \in \Sigma)$ определяет в кубе $\mathbf{E}^{l_2}$ такую $(l_2 - l_1)$-мерную грань

$$\mathbf{F}(\sigma) = \{\mathbf{v} = (v_1,\ldots,v_{l_2}) \in \mathbf{E}^{l_2} \mid v_{i_j} = \alpha_i\ (j = 1,\ldots,l_1)\}\ (\sigma \in \Sigma),$$

что

$$|\mathbf{F}(\sigma)| = 2^{l_2 - l_1}.$$

Для того, чтобы представить в неявном виде грань $\mathbf{F}(\sigma)$, достаточно хранить вектор $cdng(\sigma)$, что осуществимо с емкостной сложностью $O(l_2)$.

Предположим, что для всех $\sigma \in \Sigma$ истинно неравенство

$$|\mathbf{F}(\sigma)| \geq \{2^r \cdot frqnc(\sigma) \mid \sigma \in \Sigma\}.$$

Занумеруем элементы каждой грани $\mathbf{F}(\sigma)$ $(\sigma \in \Sigma)$. В качестве множества $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ выберем первые $k \cdot frqnc(\sigma)$ элемента множества $\mathbf{F}(\sigma)$. Для построенного бинарного отношения Δ расшифровка блока $\mathbf{v} = (v_1,\ldots,v_{l_2)} \in \mathbf{E}^{l_2}$ сводится к выбору такого единственного элемента $cdng(\sigma) = (\alpha_1,\ldots,\alpha_{l_1}) \in \mathbf{E}^{l_1}$, что $v_{i_j} = \alpha_i$ для всех $j = 1,\ldots,l_1$.

Итак, построено бинарное отношение $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$ на основе выбора $(l_2 - l_1)$-мерных граней единичного куба.

Рассмотренный выше подход к разрушению частот букв в словах языка $cdng(L)$ на основе регулярных комбинаторных структур допускает следующее обобщение.

Пусть в неявном виде задано семейство регулярных комбинаторных структур

$$\mathbf{\Delta} = \{\Delta_i \mid i = 1, \ldots, n\},$$

а в процессе реализации алгоритма 2.1 выбор бинарного отношения $\Delta_i \in \mathbf{\Delta}$ для разрушения частот букв в очередном фрагменте слова

$$cdng(u) = cdng(\sigma_1) \ldots cdng(\sigma_n) \in cdng(L)$$

осуществляется с помощью псевдослучайного генератора Γ чисел, принадлежащих множеству $\mathbf{N}_n$.

Будем считать, что инициализация генератора Γ является частью секретного сеансового ключа.

В результате мы приходим к нестационарному поточному шифру, схема которого представлена на рис. 2.4.

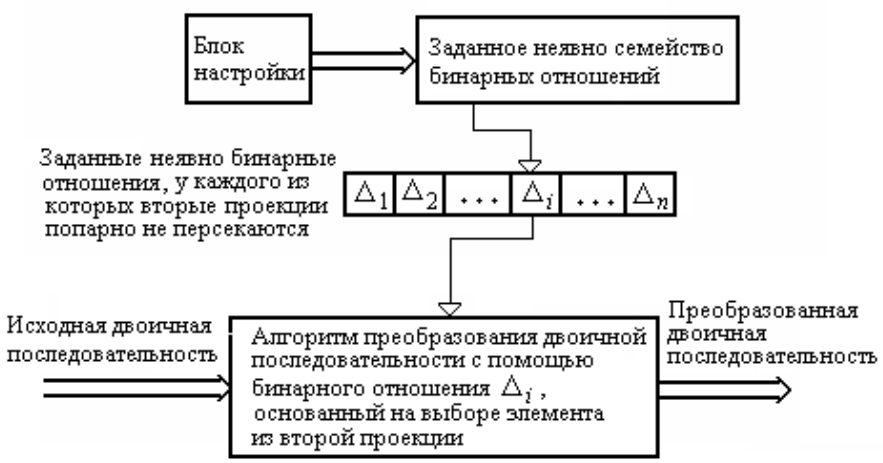


Рис. 2.4. Схема разрушения частот в двоичной последовательности на основе управляемого семейства регулярных комбинаторных структур.

Подчеркнем, что такой поточный шифр осуществляет полное разрушение частот букв в словах языка $cdng(L)$ с «линейным замедлением».

В заключение отметим, что неявно заданное семейство регулярных комбинаторных структур

$$\mathbf{\Delta} = \{\Delta_i \mid i = 1, \ldots, n\}$$

представляет собой естественное обобщение применяемой при анализе высокоскоростных блочных шифров парадигмы управляемой подстановочной операции [123], полученное за счет перехода от отображений к бинарным отношениям.

2.3. «Диффузия информации» посредством перестановок.

«Диффузия информации» посредством перестановок предназначена для разрушения «локальности» представления информации в (возможно, полученной в результате работы алгоритма 2.1) двоичной последовательности и укладывается в рамки схемы, представленной на рис. 2.5.

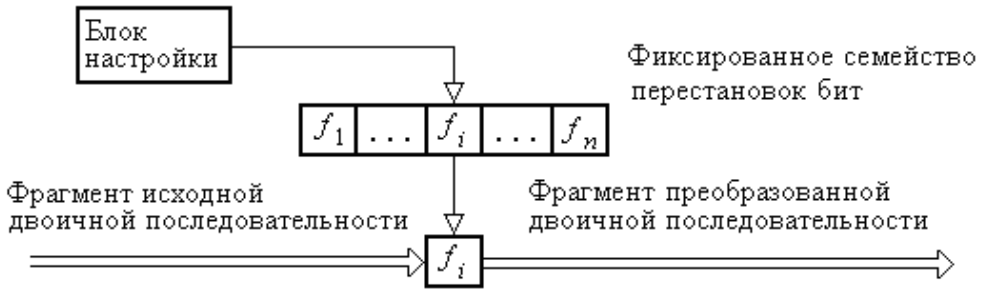


Рис. 2.5. Схема "диффузии информации" на основе перестановок.

Замечание 2.2. «Навесим» схему, представленную на рис. 2.5, на кодер, осуществляющий кодирование, контролирующее ошибки [21].

Получим поточный шифр, обладающий свойством «быть шифром, контролирующим ошибки» (отметим, что представляется весьма привлекательным исследование таких поточных шифров, построенных с использованием кодов Рида-Маллера [100]).

Ясно, что такой шифр обладает достаточно высокой вычислительной стойкостью, если перестановки бит — циклические и принадлежат различным симметрическим группам, а мощность применяемого семейства перестановок бит достаточно велика.

В силу последнего обстоятельства для схемы, представленной на рис. 2.5, актуальным является построение семейств перестановок, допускающих компактное представление в неявном виде и эффективное восстановление в явном виде любого элемента семейства.

В [153] предложена следующая общая модель «диффузии информации», т.е. разрушения локальности представления информации в (возможно, полученной в результате работы алгоритма 2.1) двоичной последовательности $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_{m^l}$, основанная на использовании подгрупп симметрической группы подстановок.

Зафиксируем подгруппы

$$\mathsf{G}_i = (G_i, \circ) \quad (i = 1, \ldots, l)$$

симметрических групп $\mathsf{S}(m^i)$, удовлетворяющие следующим двум условиям:

Условие 2.6. Емкостная сложность представления группы G_i $(i = 1, \ldots, l)$ в неявном виде равна

$$V = o(|G_i|) \quad (m \to \infty).$$

Условие 2.7. Существует алгоритм C, который для всех $i = 1, \ldots, l$ при фиксированной. начинающейся с нуля нумерации элементов группы G_i,

порождает 0-й элемент группы G_i и по известному j-му элементу $(j = 0,1,\ldots,m^i - 1)$ группы G_i порождает $(j+1)\,(\mathrm{mod}\,|G_i|)$-й элемент группы G_i с временной и емкостной сложностью, соответственно, равной

$$T_{\mathsf{C}} = O(m^i) \quad (m \to \infty)$$

и

$$V_{\mathsf{C}} = O(m^i) \quad (m \to \infty)$$

Отметим, что:

1) любая циклическая подгруппа симметрической группы $\mathsf{S}(m^i)$ удовлетворяет условиям 2.6 и 2.7;

2) группы G_i $(i = 1,\ldots,l)$ (даже в классе циклических групп) могут быть выбраны так, что их порядки являются субэкспонентами от числа m^i.

Обозначим через $\mathsf{C}(i, j) \in G_i$ $(i = 1,\ldots,l;\ j \in \mathbf{Z}_{|G_i|})$ j-й элемент группы G_i, порождаемый алгоритмом C.

Предположим, что зафиксирован алгоритм *GNRT* генерации псевдослучайной последовательности неотрицательных целых чисел

$$a(0), a(1), \ldots.$$

Для каждого $i = 1,\ldots,l$ положим

$$GNRT[i] = a(\sum_{j=1}^{i-1} m^{l-j}), a(\sum_{j=1}^{i-1} m^{l-j} + 1), \ldots, a(\sum_{j=1}^{i} m^{l-j} - 1),$$

$$prtn(\boldsymbol{\alpha}, i) = \boldsymbol{\alpha}_0^{(i)} \boldsymbol{\alpha}_1^{\{i)} \ldots \boldsymbol{\alpha}_{m^{l-i}-1}^{(i)} \quad (i = 1,\ldots,l),$$

где

$$\boldsymbol{\alpha}_h = \alpha_{h \cdot m^i + 1} \ldots \alpha_{(h+1) \cdot m^i} \quad (h = 0,1,\ldots,m^{l-i} - 1),$$

и

$$\mathsf{C}(i, j)[\boldsymbol{\alpha}_h] = \beta_1 \ldots \beta_{m^i} \quad (j \in \mathbf{Z}_{|G_i|}),$$

где

$$\beta_r = \alpha_{h \cdot m^i + \mathsf{C}(i,j)(r)}$$

для всех $r = 1,\ldots,m^i$.

Рассмотрим следующий алгоритм «диффузии информации» в двоичной последовательности $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_{m^l}$.

Алгоритм 2.2.

Шаг 1. $i := 1$.

Шаг 2. $\gamma_0, \gamma_1, \ldots, \gamma_{m^{l-i}-1} := GNRT[i]$.

Шаг 3. $\boldsymbol{\alpha}_0^{(i)} \boldsymbol{\alpha}_1^{\{i)} \ldots \boldsymbol{\alpha}_{m^{l-i}-1}^{(i)} := prtn(\boldsymbol{\alpha}, i)$.

Шаг 4. $h := 0$.

Шаг 5. $\boldsymbol{\alpha}_h^{(i)} := \mathsf{C}(i, \gamma_h)[\boldsymbol{\alpha}_h^{(i)}]$, $h := h + 1$.

Шаг 6. Если $h \le m^{l-i} - 1$, то переход к шагу 5, иначе переход к шагу 7.

Шаг 7. $\boldsymbol{\alpha} := \boldsymbol{\alpha}_0^{(i)} \boldsymbol{\alpha}_1^{\{i\}} \ldots \boldsymbol{\alpha}_{m^{l-i}-1}^{(i)}$.

Шаг 8. $i := i + 1$.

Шаг 9. Если $i \le l$, то переход к шагу 2, иначе конец.

Так как перестановка бит – обратимая операция, то алгоритм 2.2 реализует биекцию множества $\mathbf{E}^{m^l}$ на себя.

Отсюда вытекает, что существует алгоритм, осуществляющий восстановление исходной последовательности

$$\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_{m^l}$$

по выходу алгоритма 2.1.

Ясно, что цикл, определяемый шагами 4-6 алгоритма 2.2, может быть реализован в виде параллельных вычислений на основе «треугольной» многопроцессорной структуры при соответствующей настройке каждого из процессоров (рис. 2.6).

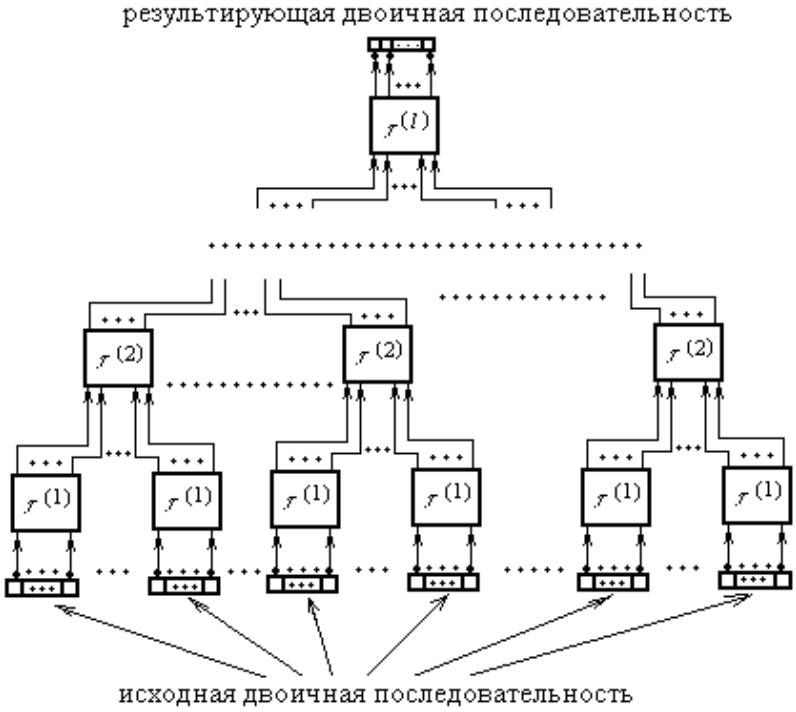


Рис. 2.6. Реализация алгоритма 2.2 на основе "треугольной" многопроцессорной структуры.

При такой организации вычислений временная и емкостная сложность реализации алгоритма 2.2, соответственно, равна

$$T = O(m^{l+1}) \quad (m \to \infty)$$

и

$$V = O(m^{l+1}) \quad (m \to \infty).$$

Отметим, что существуют следующие две возможности управления алгоритмом 2.2:

1) управление настройкой генератора *GNRT* ;

2) управление выбором нумерации элементов групп G_i $(i = 1,\ldots,l)$.

Ясно, что комбинация этих управлений приводит к достаточно широкому классу перестановок, осуществляющих «диффузию информации» в двоичной последовательности

$$\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_{m^l}.$$

Выше предполагалось, что подгруппы, удовлетворяющие условиям 2.6 и 2.7, фиксированы.

Очевидно, что если в алгоритм 2.2 внедрить возможность управления выбором указанных подгрупп, то:

1) существенно расширится класс перестановок, осуществляющих «диффузию информации» в двоичной последовательности

$$\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_{m^l};$$

2) существенно повысится вычислительная стойкость алгоритма 2.2, рассматриваемого как поточный шифр.

В связи с указанными обстоятельствами представляет интерес метод порождения семейства подгрупп симметрической группы, удовлетворяющих условиям 2.6 и 2.7, основанный на использовании графов [253].

Такой метод предложен в [153] и основан на том, что порождающий элемент циклической группы определяется *гамильтоновым путем* между двумя фиксированными вершинами связного графа.

При этом представляют интерес связные графы с n вершинами, удовлетворяющие следующим трем условиям.

Условие 2.8. Граф имеет почти регулярную структуру.

Условие 2.9. Число гамильтоновых путей между двумя фиксированными вершинами является субэкспонентой от числа ребер.

Условие 2.10. Существует такой алгоритм, порождающий субэкспоненциальное число гамильтоновых путей на графе между этими фиксированными вершинами, что каждый из этих путей порождается за время

$$T = O(n) \ \ (n \to \infty).$$

Отметим, что свойство «быть почти регулярным связным графом с числом ребер, линейным от числа вершин» является предпосылкой для возможности построения гамильтонового пути по графу, представленному в неявном виде.

В [168] построена такая последовательность почти регулярных графов

$$G_l = (V_l, E_l) \ \ (l \in \mathbf{N}),$$

что

$$V_l = \{1,\ldots,3 \cdot l + 2\}$$

и

$$E_l = \{\{1,2\},\{1,3\},\{1,4\},\{3\cdot l-1,3\cdot l+2\},\{3\cdot l,3\cdot l+2\},\{3\cdot l+1,3\cdot l+2\}\cup$$

$$\cup(\bigcup_{i=1}^{l-1}(\{3\cdot i-1,3\cdot i,3\cdot i+1\}\times\{3\cdot i+2,3\cdot i+3,3\cdot i+4\}))\cup$$

$$\cup(\bigcup_{i=1}^{l}\{\{3\cdot i-1,3\cdot i\},\{3\cdot i-1,3\cdot i+1\},\{3\cdot i,3\cdot i+1\}\}). \qquad (2.48)$$

Граф G_{13} изображен на рис. 2.7.

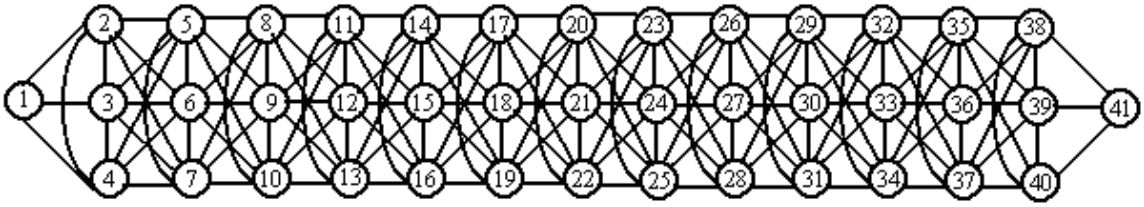


Рис. 2.7. Граф G_{13}.

Граф G_l $(l \in \mathbf{N})$ удовлетворяет условиям 2.8-2.10.

Действительно, из (2.48) вытекает, что граф G_l имеет почти регулярную структуру, а из гамильтонового пути

$$\pi = [1,2,\ldots,3\cdot l+2]$$

могут быть порождены 6^l гамильтоновых путей между вершиной 1 и вершиной $3\cdot l+2$ за счет независимого выполнения всех возможных перестановок троек вершин

$$(3\cdot i-1,3\cdot i,3\cdot i+1)\ \ (i=1,\ldots,l).$$

Построим алгоритм порождения указанных выше гамильтоновых путей в графе G_l $(l \in \mathbf{N})$.

Обозначим через f_i $(i \in \mathbf{Z}_5)$ элементы симметрической группы $\mathrm{S}(3)$, через M — одномерный массив длины $3\cdot l+2$, предназначенный для хранения очередного гамильтонового пути между вершиной 1 и вершиной $3\cdot l+2$ в графе G_l, а через M_1 — такой одномерный массив длины l, что $M_1[i] \in \mathbf{Z}_5$ $(i=1,\ldots,l)$ определяет индекс перестановки $f \in \mathrm{S}(3)$, которая применяется к тройке вершин $(3\cdot i-1,3\cdot i,3\cdot i+1)$, а через *flag* — булеву переменную, являющуюся признаком переноса при сложении по $\bmod 5$.

Алгоритм порождения указанных гамильтоновых путей в графе G_l $(l \in \mathbf{N})$ имеет следующий вид

Алгоритм 2.3.

/* инициализация значений вершин гамильтогового пути*/

Шаг 1. $i := 1$.

Шаг 2. $M[i] := i$, $i := i+1$.

Шаг 3. Если $i \le 3 \cdot l + 2$, то переход к шагу 2, иначе — к шагу 4.

/* порождение очередного гамильтонового пути */

Шаг 4. $i := 1$, $flag := 0$.

Шаг 5. $M_1[i] := M_1[i] + 1$.

Шаг 6. Если $M_1[i] > 5$, то переход к шагу 7, иначе — к шагу 8.

Шаг 7. $M_1[i] := 0$, $flag := 1$ и переход к шагу 9.

Шаг 8. $flag := 0$.

Шаг 9. $X := M[f_{M_1[i]}(1) + 3 \cdot i - 2]$.

Шаг 10. $Y := M[f_{M_1[i]}(2) + 3 \cdot i - 2]$.

Шаг 11. $Z := M[f_{M_1[i]}(3) + 3 \cdot i - 2]$.

Шаг 12. $M[3 \cdot i - 1] := X$.

Шаг 13. $M[3 \cdot i] := Y$.

Шаг 14. $M[3 \cdot i + 1] := Z$.

Шаг 15. Если $flag = 1$, то $i := i + 1$ и переход к шагу 16, иначе — шагу 17.

Шаг 16. Если $i \le l$, то переход к шагу 5, иначе — к шагу 19.

Шаг 17. Выдать массив M.

Шаг 18. Переход к шагу 4.

Шаг 19. Выдать массив M и конец.

Так как итерация цикла, определяемого шагами 4-18 алгоритма 2.3, выполняется за время

$$T = O(l) \ \ (l \to \infty),$$

то для последовательности графов G_l $(l \in \mathbf{N})$ условие 2.10 выполнено.

В заключение отметим, что использование графа G_l при построении схемы, представленной на рис. 2.5, дает возможность эффективно порождать семейства перестановок бит, содержащие субэкспоненциальное от длины фрагмента преобразуемой двоичной последовательности число элементов.

2.4. Нестационарный поточный шифр, основанный на семействе автоматных моделей.

С теоретической точки зрения необходимым условием для построения программных реализаций высокоскоростных вычислительно стойких шифров является применение стандартной техники построения эффективных алгоритмов к стандартным структурам данных [15].

Этот момент чаще всего остается «в тени» при построении современных шифров, что, по-видимому, обусловлено многообразием используемых комбинаторных и алгебраических моделей и большой сложностью методов их исследования.

Целью настоящего пункта является систематическое изложение подхода к построению нестационарного поточного шифра на основе представления инициальных БПИ-автоматов стандартными структурами данных, развитого в [79-82,146,147,176,217].

Такой подход заслуживает особого внимания, так как один из кандидатов на современный поточный шифр, представленных в рамках европейского проекта NESSIE, а именно, шифр LEVIATHAN, основан на использовании множества бинарных деревьев.

Пусть L — язык исходных сообщений, а язык $cdng(L)$ $(L \subseteq \Sigma^{+})$ построен (см. п.2.2) посредством инъективного отображения $cdng : \Sigma \to \mathbf{E}^{l_1}$, где

$$l_1 = \lceil \log |\Sigma| \rceil .$$

Основные характеристики нестационарного высокоскоростного вычислительно стойкого шифра состоят в том, что:

1) работа легального пользователя с исходным сообщением $u \in L$ длины n $(n \in \mathbf{N})$ осуществляется с временной сложностью равной

$$T = O(\lceil n \cdot \log |\Sigma| \rceil) \quad (n \to \infty);$$

2) перенастройка шифра осуществляется фиксацией значений конечного числа параметров;

3) атака криптоаналитика сводится либо к угадыванию результата, либо перебору всех возможных вариантов.

Покажем, что математической моделью, обеспечивающей перечисленные выше требования, является множество инициальных БПИ-автоматов, каждый из которых представлен полным бинарным деревом фиксированной высоты, т.е. с использованием стандартной структуры данных, применяемой при разработке эффективных алгоритмов [15].

Исследование о.-д. функции, реализуемой инициальным конечным автоматом (M, q_0) $(M = (Q, X, Y, \delta, \lambda), q_0 \in Q)$, сводится к анализу потенциально бесконечного ранжированного ориентированного $|X|$-арного дерева $T(M, Q_0)$, дуги которого отмечены соответствующими вход-выходными парами $(x, y) \in X \times Y$ (см., напр., [208]).

Будем считать, что уровни дерева $T(M, Q_0)$ занумерованы неотрицательными целыми числами, а вершины дерева $T(M, Q_0)$ — натуральными числами, причем нумерация вершин осуществляется последовательно, уровень за уровнем, а в пределах любого уровня — слева направо. Обозначим через $T_h(M, Q_0)$ $(h \in \mathbf{N})$ поддерево высоты h дерева $T(M, Q_0)$.

Число вершин поддерева $T_h(M, Q_0)$ равно

$$1 + |X| + |X|^2 + \ldots + |X|^h = \frac{|X|^{h+1} - 1}{|X| - 1}. \qquad (2.49)$$

Отождествим в поддереве $T_h(M,Q_0)$ вершины последнего h-го уровня с корнем дерева, т.е. отметим каждую вершину h-го уровня числом 1. Получим инициальный конечный автомат.

Такой автомат является БПИ-автоматом тогда и только тогда, когда выходные значения дуг, выходящих из любой вершины — попарно различные элементы множества Y. Последнее условие может быть выполнено тогда и только тогда, когда

$$|X| \le |Y|.$$

Пусть

$$X = Y = \mathbf{E}.$$

Тогда дерево $T_h(M,Q_0)$ представляет собой ранжированное ориентированное полное бинарное дерево высоты h, дуги которого отмечены элементами множества $\mathbf{E}^2$.

Условимся переход по входному символу 0 представлять левым поддеревом, а переход по входному символу 1 — правым поддеревом. Тогда в качестве отметок дуг полного бинарного дерева $T_h(M,Q_0)$ можно оставить только соответствующие выходные символы, являющиеся элементами множества $\mathbf{E}$.

Из (2.49) вытекает, что каждое полное бинарное дерево T_h $(h \in \mathbf{N})$ высоты h содержит $2^{h+1}-1$ вершину, и, следовательно, число дуг дерева T_h равно $2^{h+1}-2$.

Итак, исходным объектом является такое ранжированное ориентированное полное бинарное дерево T_h $(h \in \mathbf{N})$ высоты h, что выполнены следующие четыре условия.

Условие 2.11. Из каждой вершины i-го уровня $(i = 0,1,\ldots,h-1)$ дерева T_h выходит две дуги. Эти дуги ведут в вершины $(i+1)$-го уровня дерева T_h.

Условие 2.12. Дуги, выходящие из любой вершины дерева T_h, отмечены различными элементами множества $\mathbf{E}$.

Условие 2.13. Вершины дерева T_h, расположенные в уровнях с номерами $0,1,\ldots,h-1$, так отмечены натуральными числами, что нумерация вершин осуществляется последовательно, уровень за уровнем, а в пределах любого уровня — слева направо.

Условие 2.14. Каждая вершина дерева T_h, расположенная в последнем, h-м уровне, отмечена числом 1.

Обозначим через $\boldsymbol{T}_h$ $(h \in \mathbf{N})$ множество всех полных бинарных деревьев T_h высоты h, удовлетворяющих условиям 2.11-2.14.

Теорема 2.4. Истинны равенства

$$|\boldsymbol{T}_h| = 0.5 \cdot 2^{2^h} \quad (h \in \mathbf{N}). \tag{2.50}$$

Доказательство. Пусть $h = 1$.

Тогда существуют два различных дерева $T_1 \in \boldsymbol{T}_1$ (рис. 2.8).

Рис. 2.8. Деревья $T_1 \in \boldsymbol{T}_1$.

Таким образом, показано, что

$$|\boldsymbol{T}_1| = 0.5 \cdot 2^{2^1}, \tag{2.51}$$

т.е. формула (2.50) истинна, если $h = 1$.

Пусть $h \geq 2$.

Если в дереве $T_h \in \boldsymbol{T}_h$ удалить вершины последнего, h-го уровня, а отметку каждой вершины $(h-1)$-го уровня заменить числом 1, то получим дерево $T_{h-1} \in \boldsymbol{T}_{h-1}$. Ясно, что:

1) каждое дерево $T_{h-1} \in \boldsymbol{T}_{h-1}$ порождается указанным способом;

2) деревья $T_h', T_h'' \in \boldsymbol{T}_h$ порождают одно и то же дерево $T_{h-1} \in \boldsymbol{T}_{h-1}$ тогда и только тогда, когда деревья T_h' и T_h'' отличаются друг от друга только отметками дуг, заходящих в вершины h-го уровня.

Отсюда и из условия 2.11 вытекает, что

$$|\boldsymbol{T}_h| = 2^{2^{h-1}} \cdot |\boldsymbol{T}_{h-1}| \quad (h \geq 2). \tag{2.52}$$

Кроме того,

$$|\boldsymbol{T}_1| = 2^{2^0}. \tag{2.53}$$

Из (2.52) и (2.53) вытекает, что для всех $h \geq 2$ истинны равенства

$$\begin{cases} |\boldsymbol{T}_1| = 2^{2^0} \\ |\boldsymbol{T}_2| = 2^{2^1} \cdot |\boldsymbol{T}_1| \\ \quad\vdots \\ |\boldsymbol{T}_h| = 2^{2^{h-1}} \cdot |\boldsymbol{T}_{h-1}| \end{cases}. \tag{2.54}$$

Перемножив равенства (2.54), получим, что для всех $h \geq 2$

$$(|\boldsymbol{T}_1| \cdot \ldots \cdot |\boldsymbol{T}_{h-1}|) \cdot |\boldsymbol{T}_h| = (2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^{h-1}}) \cdot (|\boldsymbol{T}_1| \cdot \ldots \cdot |\boldsymbol{T}_{h-1}|) \Rightarrow$$

$$\Rightarrow |\boldsymbol{T}_h| = 2^{2^0 + 2^1 \ldots + 2^{h-1}} \Leftrightarrow |\boldsymbol{T}_h| = 2^{\frac{2^h - 1}{2-1}} \Leftrightarrow |\boldsymbol{T}_h| = 0.5 \cdot 2^{2^h}.$$

Таким образом, показано, что формула (2.50) истинна для всех $h \geq 2$.

Теорема доказана.

Известно (см., напр., [15]), что полное бинарное дерево может быть эффективно представлено одномерным массивом.

Построение одномерного массива M_h ($h \in \mathbf{N}$) длины $2^{h+1}-2$, представляющего дерево $T_h \in \boldsymbol{T}_h$, осуществляется в соответствии со следующим алгоритмом (через $T_h[i,0]$ и $T_h[i,1]$ обозначены выходные символы, являющиеся отметками дуг, выходящих из вершины с номером i дерева T_h, соответственно, к левому и правому поддеревьям, а через $\mathsf{M}_h[j]$ — j-й элемент массива M_h).

Алгоритм 2.4.

Шаг 1. $i := 1$.

Шаг 2. $\mathsf{M}_h[2 \cdot i - 1] := T_h[i,0]$,

Шаг 3. $\mathsf{M}_h[2 \cdot i] := T_h[i,1]$.

Шаг 4. $i := i + 1$.

Шаг 5. Если $i \le 2^h - 1$, то переход к шагу 2, иначе — конец.

Использование массива M_h ($h \in \mathbf{N}$) при шифровании двоичной последовательности $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_h$ осуществляется следующим образом.

Алгоритм 2.5.

Шаг 1. $i := 1,\ j := 1,\ \boldsymbol{\beta} := \Lambda$.

Шаг 2. Если $\alpha_i = 0$, то

$$\boldsymbol{\beta} := \boldsymbol{\beta} \uparrow\uparrow \mathsf{M}_h[2 \cdot j - 1],\quad j := 2 \cdot j + 1,$$

иначе

$$\boldsymbol{\beta} := \boldsymbol{\beta} \uparrow\uparrow \mathsf{M}_h[2 \cdot j],\quad j := 2 \cdot (j+1).$$

Шаг 3. $i := i + 1$.

Шаг 4. Если $i \le h$, то переход к шагу 2, иначе — конец.

Расшифровка последовательности $\boldsymbol{\beta} = \beta_1 \ldots \beta_h$, полученной в результате работы алгоритма 2.5, осуществляется в соответствии со следующим алгоритмом.

Алгоритм 2.6.

Шаг 1. $i := 1,\ j := 1,\ \boldsymbol{\alpha} := \Lambda$.

Шаг 2. Если $\beta_i = \mathsf{M}_h[j]$, то

$$\boldsymbol{\alpha} := \boldsymbol{\alpha} \uparrow\uparrow 0,\quad j := 2 \cdot j + 1,$$

иначе

$$\boldsymbol{\alpha} := \boldsymbol{\alpha} \uparrow\uparrow 1,\quad j := 2 \cdot (j+1).$$

Шаг 3. $i := i + 1$.

Шаг 4. Если $i \le h$, то переход к шагу 2, иначе — конец.

Ясно, что время работы как алгоритма 2.5, так и алгоритма 2.6 с двоичной последовательностью длины h равно

$$T = O(h) \quad (h \to \infty).$$

Обозначим через $E_{A.2.5}(\mathsf{M}_h, \boldsymbol{\alpha})$ $(\boldsymbol{\alpha} \in \mathbf{E}^h)$ результат шифрования двоичной последовательности $\boldsymbol{\alpha}$ посредством алгоритма 2.5 в случае, когда в качестве модели БПИ-автомата используется двоичный массив M_h, а через $D_{A.2.6}(\mathsf{M}_h, \boldsymbol{\beta})$ $(\boldsymbol{\beta} \in \mathbf{E}^h)$ — результат расшифровки двоичной последовательности $\boldsymbol{\beta}$ посредством алгоритма 2.6 в случае, когда в качестве модели БПИ-автомата используется двоичный массив M_h.

Рассмотрим структуру нестационарного поточного шифра, построенного на основе инициальных БПИ-автоматов, определяемых полными бинарными деревьями $T_h \in \boldsymbol{T}_h$ $(h \in \mathbf{N})$, представленными массивами M_h.

Зафиксируем число $h \in \mathbf{N}$, простое число p $(p < 0.5 \cdot 2^{2^h})$ и p-элементное подмножество полных бинарных деревьев

$$\boldsymbol{T}' = \bigcup_{i=1}^{h} \boldsymbol{T}_i ,$$

элементы которого занумерованы числами $0,1,\ldots, p-1$.

Обозначим через S такой двумерный массив, что для каждого $i = 1,\ldots, p$ одномерный массив $\mathsf{S}[i;*]$ имеет длину, не превосходящую $2^{h+1} - 2$ и представляет i-е дерево, принадлежащее множеству $\boldsymbol{T}'$, а через H — алгоритм псевдослучайного выбора одномерного массива $\mathsf{S}[i;*]$ $(i = 1,\ldots, p)$ в двухмерном массиве S.

Предположим, что алгоритм H реализован при помощи сдвигового регистра с линейной обратной связью, который генерирует линейную рекуррентную последовательность k-го порядка над полем Галуа $\mathbf{GF}(p)$

$$s_{n+k} = a_{k-1} \circ s_{n+k-1} \oplus \ldots \oplus a_0 \circ s_n \oplus a \quad (n \in \mathbf{Z}_+). \tag{2.55}$$

Будем считать, что вектор $\mathbf{s} = (s_{k-1}, \ldots, s_0)$ — секретный сеансовый ключ, а вектор $\mathbf{a} = (a_{k-1}, \ldots, a_0, a)$ — секретный ключ средней длительности.

Пару векторов $(\mathbf{s}, \mathbf{a})$ назовем допустимой настройкой, если последовательность

$$s_k, s_{k+1}, \ldots, s_{k+p-1}$$

содержит каждый элемент поля Галуа $\mathbf{GF}(p)$.

Обозначим через $\mathsf{H}[i]$ $(i \in \mathbf{N})$ i-й член последовательности

$$s_k, s_{k+1}, \ldots,$$

генерируемой сдвиговым регистром при фиксированной настройке $(\mathbf{s}, \mathbf{a})$, а через $l(\mathsf{H}[i])$ $(i \in \mathbf{N})$ — длину одномерного массива $\mathsf{S}[\mathsf{H}[i];*]$.

Пусть $\boldsymbol{\gamma}$ — двоичная последовательность.

Обозначим через $prfx(m,\boldsymbol{\gamma})$ $(m\in\mathbf{N})$ начальный отрезок длины m последовательности $\boldsymbol{\gamma}$, если $d(\boldsymbol{\gamma})\geq m$ и последовательность $\boldsymbol{\gamma}\uparrow\uparrow\boldsymbol{\mu}$, где $\boldsymbol{\mu}\in\mathbf{E}^{m-d(\gamma)}$ — фиксированная последовательность, если $d(\boldsymbol{\gamma})<m$.

Аналогичным образом, обозначим через $sffx(m,\boldsymbol{\gamma})$ $(m\in\mathbf{N})$ финальный отрезок длины $d(\boldsymbol{\gamma})-m$ последовательности $\boldsymbol{\gamma}$, если $d(\boldsymbol{\gamma})\geq m$ и последовательность $\boldsymbol{\gamma}\uparrow\uparrow\boldsymbol{\mu}$, где $\boldsymbol{\mu}\in\mathbf{E}^{m-d(\gamma)}$ — фиксированная последовательность, если $d(\boldsymbol{\gamma})<m$.

Шифрование двоичной последовательности $\boldsymbol{\alpha}\in\mathbf{E}^{+}$ осуществляется следующим образом.

Алгоритм 2.7.

Шаг 1. $i:=1,\ j:=d(\boldsymbol{\alpha}),\ \boldsymbol{\beta}:=\Lambda$.

Шаг 2. $\mathsf{M}_{l(\mathsf{H}[i])}:=\mathsf{S}[\mathsf{H}[i];*]$.

Шаг 3. $\boldsymbol{\gamma}:=prfx(l(\mathsf{H}[i]),\boldsymbol{\alpha})$.

Шаг 4. $\boldsymbol{\beta}:=\boldsymbol{\beta}\uparrow\uparrow E_{A.2.5}(\mathsf{M}_{l(\mathsf{H}[i])},\boldsymbol{\gamma})$.

Шаг 5. $j:=j-d(\boldsymbol{\gamma})$.

Шаг 6. Если $j>0$, то переход к шагу 7, иначе — конец.

Шаг 7. $\boldsymbol{\alpha}:=sffx(l(\mathsf{H}[i]),\boldsymbol{\alpha})$.

Шаг 8. $i:=i+1$ и переход к шагу 2.

Расшифровка последовательности $\boldsymbol{\beta}\in\mathbf{E}^{+}$, полученной в результате работы алгоритма 2.7, осуществляется в соответствии со следующим алгоритмом.

Алгоритм 2.8.

Шаг 1. $i:=1,\ j:=d(\boldsymbol{\beta}),\ \boldsymbol{\alpha}:=\Lambda$.

Шаг 2. $\mathsf{M}_{l(\mathsf{H}[i])}:=\mathsf{S}[\mathsf{H}[i];*]$.

Шаг 3. $\boldsymbol{\gamma}:=prfx(l(\mathsf{H}[i]),\boldsymbol{\beta})$.

Шаг 4. $\boldsymbol{\alpha}:=\boldsymbol{\alpha}\uparrow\uparrow D_{A.2.6}(\mathsf{M}_{l(\mathsf{H}[i])},\boldsymbol{\gamma})$.

Шаг 5. $j:=j-d(\boldsymbol{\gamma})$.

Шаг 6. Если $j>0$, то переход к шагу 7, иначе — конец.

Шаг 7. $\boldsymbol{\beta}:=sffx(l(\mathsf{H}[i]),\boldsymbol{\beta})$.

Шаг 8. $i:=i+1$ и переход к шагу 2.

Ясно, что время работы как алгоритма 2.7, так и алгоритма 2.8 с двоичной последовательностью длины n равно

$$T=O(n)\quad(n\to\infty).$$

Итак, построен нестационарный поточный шифр, допустимой настройкой которого является такая пара векторов $(\mathbf{s},\mathbf{a})$, что последовательность $s_k,s_{k+1},\ldots,s_{k+p-1}$ содержит каждый элемент поля Галуа $\mathbf{GF}(p)$.

Перенастройка шифра осуществляется фиксацией значений $2 \cdot k + 1$ параметров, каждый из которых является элементом поля Галуа $\mathbf{GF}(p)$.

При работе с языком $cdng(L)$ $(L \subseteq \Sigma^{+})$ вычислительная стойкость построенного нестационарного поточного шифра существенно зависит от выбора множества полных бинарных деревьев $\boldsymbol{T}'$.

Предпочтительным является выбор такого множества $\boldsymbol{T}'$, что осуществляется существенное разрушение частот букв алфавита $cdng(\Sigma)$ в словах языка $cdng(L)$ при любой допустимой настройке $(\mathbf{s}, \mathbf{a})$.

Ясно, что построение такого множества полных бинарных деревьев — весьма трудоемкий процесс.

Отметим, что проблема построения множества $\boldsymbol{T}'$ вообще не возникает, если построенный поточный шифр применять к языку L, построенному в п.2.2. В этом случае в качестве множества $\boldsymbol{T}'$ может быть выбрано любое p-элементное подмножество множества $\bigcup_{i=1}^{h} \boldsymbol{T}_i$, не содержащее деревья, реализующие тождественные словарные отображения.

Охарактеризуем *имитостойкость* построенного нестационарного поточного шифра.

При изменении значений группы бит в передаваемом сообщении, адресат получит локальные искажения переданной информации.

Такое вмешательство криптоаналитика часто может быть обнаружено за счет искажения смысла сообщения.

В то же время, изменение длины переданной последовательности за счет удаления из него или вставки в него двоичной последовательности приводит к невозможности расшифровки финального отрезка сообщения, что, в частности, обусловлено тем, что высоты деревьев, принадлежащих множеству $\boldsymbol{T}'$, могут быть различными.

2.5. Нестационарный поточный шифр, основанный на задаче о рюкзаке.

Одним из подходов, применяемых при разработке современных шифров, является использование комбинаторных конструкций, идентификация которых сводится к решению NP-полных задач [50].

Однако, то обстоятельство, что такие конструкции применяются именно при построении шифра, часто приводит к такому сужению множества исходных данных, что соответствующая задача дискретной математики теряет свойство «быть NP-полной задачей».

По-видимому, наиболее известным таким примером является блочный шифр, построенный на основе «задачи о рюкзаке» (см., напр., [234]). В [299,300] показано, что этот шифр может быть «взломан» с полиномиальной временной сложностью.

Классическая формулировка «задачи о рюкзаке» (которая, как известно, является NP-полной задачей) состоит в следующем.

Пусть задано натуральное число b и вектор $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$ $(n \in \mathbf{N})$ с попарно различными компонентами (такой вектор называется *рюкзачным вектором*).

Требуется определить, существует ли решение $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{Z}_+^n$ уравнения

$$b = \sum_{i=1}^{n} a_i \cdot x_i \,, \tag{2.55}$$

и в случае положительного ответа найти все такие решения.

Идея применения «задачи о рюкзаке» при построении симметричного блочного шифра основана на замене для фиксированного числа n $(n \in \mathbf{N})$ (предполагается, что $n \geq 2$) при фиксированном рюкзачном векторе $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$ (который является секретным сеансовым ключом) блока информации $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_n \in \mathbf{E}^n$ натуральным числом

$$b = \sum_{i=1}^{n} a_i \cdot \alpha_i \,. \tag{2.56}$$

При такой организации процесса шифрования необходимое и достаточное условие корректности процесса расшифровки блока шифртекста состоит в выборе такого секретного сеансового ключа $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$, что для любой двоичной последовательности $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_n \in \mathbf{E}^n$ натуральное число b, вычисленное в соответствии с формулой (2.56), обладает тем свойством, что уравнение (2.55) имеет единственное решение. Рюкзачный вектор $\mathbf{a} \in \mathbf{Z}_+^n$, удовлетворяющий указанному условию, назовем *инъективным* рюкзачным вектором.

Замечание 2.3. Для того чтобы обеспечить корректность процесса расшифровки для шифра, основанного на замене блока информации натуральным числом, необходимо и достаточно внедрить в процесс шифрования «механизм выделения блоков» в шифртексте.

С позиции теории алгоритмов универсальным таким механизмом является применение начальных и финальных маркеров блока шифртекста. Однако такой подход приводит к необоснованному увеличению длины блока шифртекста по сравнению с длиной блока исходного текста.

Чтобы избежать указанного выше недостатка, достаточно представлять блоки шифртекста двоичными последовательностями фиксированной длины, что, как правило, применяется на практике.

В дальнейшем предполагается, что для шифра, основанного на замене блока информации натуральным числом, применяется именно такой «механизм выделения блоков» в шифртексте.

Если на *инъективный* рюкзачный вектор не наложены никакие ограничения, то процесс расшифровки (т.е. поиск единственного решения урав-

нения (2.55) по заданному числу $b \in \mathbf{N}$ и заданному инъективному рюкзачному вектору $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$) сводится к решению «задачи о рюкзаке».

Для того чтобы процесс расшифровки осуществлялся с полиномиальной сложностью естественно сузить множество инъективных рюкзачных векторов, выбираемых в качестве секретного сеансового ключа.

Эта идея привела к выделению множества *сверхрастущих* рюкзачных векторов, т.е. таких рюкзачных векторов

$$\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n,$$

что

$$a_j > \sum_{i=1}^{j-1} a_i \quad (j = 2, \ldots, n).$$

Если секретный сеансовый ключ $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$ — сверхрастущий рюкзачный вектор, то процесс расшифровки блока шифртекста, т.е. вычисления двоичной последовательности $\boldsymbol{\alpha} = \alpha_1 \ldots \alpha_n \in \mathbf{E}^n$ по заданному натуральному числу b, вычисленному в соответствии с формулой (2.56), осуществляется следующим образом.

Алгоритм 2.9.

Шаг 1. $i := n$, $\boldsymbol{\alpha} := \Lambda$.

Шаг 2. Если $b < a_i$, то

$$\boldsymbol{\alpha} := 0 \uparrow\uparrow \boldsymbol{\alpha},$$

иначе

$$\boldsymbol{\alpha} := 1 \uparrow\uparrow \boldsymbol{\alpha}, \quad b := b - a_i.$$

Шаг 3. $i := i - 1$.

Шаг 4. Если $i \geq 1$, то переход к шагу 2, иначе — конец.

Таким образом, при использовании в качестве секретного сеансового ключа сверхрастущего рюкзачного вектора $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$ шифрование и расшифровка осуществляется при логарифмическом весе с временной сложностью, равной

$$T = O(n \cdot \lceil \log a_n \rceil) \quad (n \to \infty),$$

т.е. шифр, является высокоскоростным блочным шифром.

Этот шифр не является вычислительно стойким, так как секретный ключ

$$\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{Z}_+^n$$

идентифицируется двоичной последовательностью

$$\boldsymbol{\alpha}_1 \uparrow\uparrow \ldots \uparrow\uparrow \boldsymbol{\alpha}_n,$$

где

$$\boldsymbol{\alpha}_i = \underbrace{0 \ldots 0}_{i-1 \text{ раз}} 1 \underbrace{0 \ldots 0}_{n-i \text{ раз}} \quad (i = 1, \ldots, n).$$

Поэтому была предпринята следующая попытка преобразовать построенный выше симметричный блочный шифр в асимметричный блочный шифр.

Зафиксируем сверхрастущий рюкзачный вектор $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbf{Z}_+^n$ и такое число $m\in\mathbf{N}$, что

$$m>\sum_{i=1}^{n}a_i\,.$$

Обозначим через $\circ_m$ операцию умножения по $\bmod m$ чисел, принадлежащих множеству $\mathbf{Z}_+$.

Для любого числа $t\in\mathbf{N}$ положим

$$t\circ_m\mathbf{a}=(t\circ_m a_1,\ldots,t\circ_m a_n).$$

Известно, что для заданного числа $t\in\mathbf{N}$ сравнение

$$t\cdot u=1(\bmod m) \tag{2.57}$$

имеет (единственное) решение тогда и только тогда, когда

$$(t,m)=1. \tag{2.58}$$

Таким образом, если число $t\in\mathbf{N}$ удовлетворяет условию (2.58), то

$$\mathbf{c}=t\circ_m\mathbf{a}\Leftrightarrow a=u\circ_m\mathbf{c},$$

где u — единственное решение сравнения (2.57).

Пусть число $t\in\mathbf{N}$, удовлетворяющее условию (2.58) и сверхрастущий рюкзачный вектор $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbf{Z}_+^n$ являются секретным ключом, а вектор $\mathbf{c}=t\circ_m\mathbf{a}=(c_1,\ldots,c_n)$ и число $m\in\mathbf{N}$ являются открытым ключом.

Шифрование блока информации $\boldsymbol{\alpha}=\alpha_1\ldots\alpha_n\in\mathbf{E}^n$ сводится к вычислению числа

$$e=\sum_{i=1}^{n}c_i\cdot\alpha_i\,. \tag{2.59}$$

Расшифровка блока шифртекста, т.е. вычисления двоичной последовательности $\boldsymbol{\alpha}=\alpha_1\ldots\alpha_n\in\mathbf{E}^n$ по натуральному числу e, вычисленному в соответствии с формулой (2.59), сводится к вычислению числа $b=u\circ_m e$, где u — единственное решение сравнения (2.57), а затем к применению к числу b алгоритма 2.9.

В [299,300] показано, что построенный выше асимметричный блочный шифр может быть «взломан» с полиномиальной временной сложностью.

Причина того, что шифр не является вычислительно стойким, состоит именно в том, что он является блочным шифром, построенным на основе фиксированного сверхрастущего рюкзачного вектора $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbf{Z}_+^n$. Поэтому естественно преобразовать этот шифр в (симметричный) нестационарный поточный шифр.

Рассмотрим решение этой задачи, предложенное в [11].

Зафиксируем:

1) последовательность сверхрастущих рюкзачных векторов

$$\begin{aligned}&\mathbf{a}_1 = (a_1^{(1)},\ldots,a_{n_1}^{(1)}),\\ &\ldots\ldots\ldots\ldots\ldots\ldots\quad (l\in\mathbf{N}, l\geq 2);\\ &\mathbf{a}_l = (a_1^{(l)},\ldots,a_{n_l}^{(l)});\end{aligned}\tag{2.60}$$

2) такое число $m\in\mathbf{N}$, что

$$m > \max\{m_i \mid i=1,\ldots,l\},\tag{2.61}$$

где

$$m_i = \max\{a_1^{(i)},\ldots,a_{n_i}^{(i)}\}\quad (i=1,\ldots,l);$$

3) такие псевдослучайные генераторы Γ и Γ_i $(i=1,\ldots,l)$, что генератор Γ генерирует числа, принадлежащие множеству $\mathbf{N}_l$, а генератор Γ_i $(i=1,\ldots,l)$ генерирует числа, принадлежащие множеству $\mathbf{N}_{l_i-1}$;

4) алгоритм $SLCT(i,j)$ $(i=1,\ldots,l;\ j=1,\ldots,l_i-1)$, осуществляющий псевдослучайный выбор j-элементного подмножества множества $\mathbf{N}_{n_i}$.

Обозначим через $\Gamma[j]$ и $\Gamma_i[j]$ $(i=1,\ldots,l)$ j-е число, генерируемое, соответственно, генератором Γ и Γ_i, через $\mathbf{b}|_s$ $(\mathbf{b}=(b_1,\ldots,b_n), \varnothing\neq s\subset\mathbf{N}_n)$ — вектор, полученный из вектора $\mathbf{b}$ в результате вычеркивания компонент с номерами, не принадлежащими множеству s, а через M — одномерный массив длины l, первоначально заполненный нулями.

Для двоичной последовательности $\boldsymbol{\gamma}$ обозначим через $prfx(m,\boldsymbol{\gamma})$ $(m\in\mathbf{N})$ начальный отрезок длины m последовательности $\boldsymbol{\gamma}$, если $d(\boldsymbol{\gamma})\geq m$ и последовательность $\boldsymbol{\gamma}\uparrow\uparrow\boldsymbol{\mu}$, где $\boldsymbol{\mu}\in\mathbf{E}^{m-d(\gamma)}$ — фиксированная последовательность, если $d(\boldsymbol{\gamma})<m$, а через $sffx(m,\boldsymbol{\gamma})$ $(m\in\mathbf{N})$ — финальный отрезок длины $d(\boldsymbol{\gamma})-m$ последовательности $\boldsymbol{\gamma}$, если $d(\boldsymbol{\gamma})\geq m$ и последовательность $\boldsymbol{\gamma}\uparrow\uparrow\boldsymbol{\mu}$, где $\boldsymbol{\mu}\in\mathbf{E}^{m-d(\gamma)}$ — фиксированная последовательность, если $d(\boldsymbol{\gamma})<m$.

Пусть число $t\in\mathbf{N}$ удовлетворяет условию (2.58).

Рассмотрим следующий алгоритм шифрования двоичной последовательности $\boldsymbol{\alpha}\in\mathbf{E}^+$.

Алгоритм 2.10.

Шаг 1. $i:=1$.

Шаг 2. $\mathbf{c}_i = t\circ\mathbf{a}_i$, $i:=i+1$.

Шаг 3. Если $i\leq l$, то переход к шагу 1, иначе — к шагу 4.

Шаг 4. $i:=1$, $h=d(\boldsymbol{\alpha})$, $\boldsymbol{\beta}:=\Lambda$.

Шаг 5. $r:=\Gamma[i]$, $\mathsf{M}[r]:=\mathsf{M}[r]+1$, $s:=SLCT(r,\Gamma_r[\mathsf{M}[r]])$.

Шаг 6. $\mathbf{b} \coloneqq \mathbf{c}_r\,|_s\ (=(b_1,\ldots,b_{|s|}))$.

Шаг 7. $\boldsymbol{\eta} \coloneqq prfx(\boldsymbol{\alpha},|\,s\,|)\ (=\eta_1\ldots\eta_{|s|}))$.

Шаг 8. $e \coloneqq \sum_{j=1}^{|s|} b_j \cdot \eta_j$.

Шаг 9. $\boldsymbol{\beta} \coloneqq \boldsymbol{\beta} \uparrow\uparrow e$.

Шаг 10. $h \coloneqq h - d(\boldsymbol{\eta})$.

Шаг 11. Если $h > 0$, то переход к шагу 12, иначе — конец.

Шаг 12. $\boldsymbol{\alpha} \coloneqq sffx(|\,s\,|,\boldsymbol{\alpha})$.

Шаг 13. $i \coloneqq i+1$ и переход к шагу 5.

Расшифровка шифртекста $e_1\ldots e_k$, полученного в результате работы алгоритма 2.10, осуществляется в соответствии со следующим алгоритмом.

Алгоритм 2.11.

Шаг 1. $\boldsymbol{\alpha} \coloneqq \Lambda$, $u \coloneqq$ решение сравнения (2.57).

Шаг 2. $i \coloneqq 1$.

Шаг 3. $b \coloneqq u \circ_m e_i$.

Шаг 4. $r \coloneqq \Gamma[i]$, $\mathrm{M}[r] \coloneqq \mathrm{M}[r]+1$, $s \coloneqq SLCT(r,\Gamma_r[\mathrm{M}[r]])$.

Шаг 5. $\mathbf{c} \coloneqq \mathbf{a}_r\,|_s\ (=(c_1,\ldots,c_{|s|}))$.

Шаг 6. $j \coloneqq |\,s\,|$, $\boldsymbol{\beta} \coloneqq \Lambda$.

Шаг 7. Если $b < c_j$, то

$$\boldsymbol{\beta} \coloneqq 0 \uparrow\uparrow \boldsymbol{\beta},$$

иначе

$$\boldsymbol{\beta} \coloneqq 1 \uparrow\uparrow \boldsymbol{\beta},\ \ b \coloneqq b - c_j.$$

Шаг 8. $j \coloneqq j-1$.

Шаг 9. Если $j \geq 1$, то переход к шагу 7, иначе — к шагу 10.

Шаг 10. $\boldsymbol{\alpha} \coloneqq \boldsymbol{\alpha} \uparrow\uparrow \boldsymbol{\beta}$.

Шаг 11. $i \coloneqq i+1$.

Шаг 12. Если $i \leq k$, то переход к шагу 3, иначе — конец.

Ясно, что время работы как алгоритма 2.10, так и алгоритма 2.11 с двоичной последовательностью длины n равно $T = O(n)$ $(n \to \infty)$.

Итак, построен симметричный нестационарный поточный шифр, для которого секретный ключ средней длительности — последовательность сверхрастущих рюкзачных векторов (2.60) и модуль $m \in \mathbf{N}$, удовлетворяющий условию (2.61), а секретный сеансовый ключ — число $t \in \mathbf{N}$, удовлетворяющее условию (2.58), настройки генераторов Γ и Γ_i $(i=1,\ldots,l)$, а также настройка алгоритма $SLCT(i,j)$ $(i=1,\ldots,l;\ j=1,\ldots,l_i-1)$.

Обоснованием высокой вычислительной стойкости построенного шифра, как и шифра, построенного в п.2.4, является то, что оба эти шифра существенно опираются на метод вариации окна шифрования (рис. 2.9).

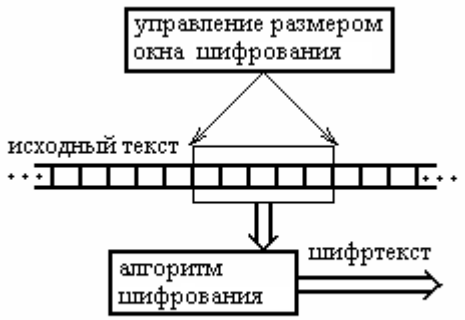


Рис. 2.9. Шифрование с варьируемым "размером окна".

Поэтому при любой атаке криптоаналитик сталкивается с теми проблемами поиска, которые перечислены в п.2.1.

Охарактеризуем *имитостойкость* построенного нестационарного поточного шифра.

При изменении значений группы бит в передаваемом сообщении, адресат получит локальные искажения переданной информации. Такое вмешательство криптоаналитика часто может быть обнаружено за счет искажения смысла сообщения.

В то же время, изменение длины переданной последовательности за счет удаления из него или вставки в него двоичной последовательности приводит к невозможности расшифровки финального отрезка сообщения, что, в частности, обусловлено вариацией окна шифрования.

2.6. Электронная цифровая подпись на основе эллиптических кривых над полем рациональных чисел.

Как известно, электронная цифровая подпись (ЭЦП) является необходимым элементом электронного документооборота.

На протяжении последнего десятилетия одним из перспективных направлений криптографии является реализация ЭЦП на основе эллиптических кривых (ЭК) над полем Галуа.

В настоящее время стандарты ЭЦП на основе ЭК над полем Галуа приняты во многих странах мира, а именно: *ECDSA* — в США и Западной Европе, *ГОСТ Р 34.10-2001* — в России, *ДСТУ 4145-2002* — в Украине. При этом, ЭЦП в стандартах *ECDSA* и *ГОСТ Р 34.10-2001* формируется на основе ЭК над полем Галуа $\mathbf{GF}(p)$, а в стандарте *ДСТУ 4145-2002* — на основе ЭК над полем Галуа $\mathbf{GF}(p^k)$ $(k \in \mathbf{N})$.

Применение ЭК дает возможность строить вычислительно стойкие системы ЭЦП с ключами значительно меньших размеров, по сравнению с аналогичными системами типа *RSA* или *DSA* (см., напр., [229]).

Отметим, что системы ЭЦП на основе ЭК менее требовательны к вычислительной мощности и объему памяти оборудования и, поэтому, они хорошо подходят для смарт-карт, портативных телефонов электронной торговли, банковских операций и т.д.

Однако существует ряд проблем, которые ограничивают широкое распространение на практике систем ЭЦП на основе ЭК над полями Галуа.

К таким проблемам относится то, что реальная безопасность таких систем ЭЦП недостаточно изучена, а также то, что существует ряд сложностей, связанных с генерацией подходящих ЭК и точек на них. В конечном итоге все это вызывает проблемы с лицензированием и патентированием протоколов ЭЦП на основе ЭК над полями Галуа.

Кроме этого, реализация на компьютере операций в поле Галуа $\mathbf{GF}(p)$ (или $\mathbf{GF}(p^k)$) значительно медленнее, чем реализация аналогичных операций над рациональными числами.

Поэтому естественно возникает вопрос о реализации систем ЭЦП на основе ЭК над полем рациональных чисел. Рассмотрим решение этой задачи, предложенное в [48].

Введем вначале необходимые понятия и определения.

Эллиптической кривой (ЭК) *над полем действительных чисел* называется гладкая кривая, определяемая уравнением

$$E:\ y^2 = a\cdot x^3 + b\cdot x^2 + c\cdot x + d \quad (a,b,c,d \in \mathbf{R}), \tag{2.62}$$

где $a\cdot x^3 + b\cdot x^2 + c\cdot x + d$ — полином с различными корнями.

Из (2.62) вытекает, что ЭК E симметрична относительно оси абсцисс, т.е.

$$P_1 = (x_1, y_1) \in E \Rightarrow P_2 = (x_1, -y_1) \in E.$$

Если к множеству точек ЭК E добавить бесконечно удаленную точку (обозначается буквой O), то получим абелеву группу

$$\mathsf{G}_E = (G_E, +_{\mathsf{G}_E}).$$

В этой абелевой группе:

1) точка O является нулем, т.е.

$$P +_{\mathsf{G}_E} O = O +_{\mathsf{G}_E} P = P$$

для всех $P \in G_E$;

2) для любой точки $P = (x, y) \in E$ противоположным элементом является точка

$$-P = (x, -y). \tag{2.63}$$

Из (2.63) вытекает, что

$$P = (x,0) \in E \Rightarrow -P = P,$$

т.е.

$$P = (x,0) \in E \Rightarrow -P = P +_{\mathsf{G}_E} (-P) = O.$$

Для любых точек $P_1, P_2 \in E$ $(P_1 \neq -P_2)$ если $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$, то

$$P_1 +_{G_E} P_2 = P_3,$$

где точка $P_3 = (x_3, y_3) \in E$ определяется следующим образом:

$$x_1 \neq x_2 \Rightarrow \begin{cases} \lambda = (y_2 - y_1) \cdot (x_2 - x_1)^{-1} \\ x_3 = a^{-1} \cdot \lambda^2 - x_1 - x_2 - b \cdot a^{-1} \\ y_3 = \lambda \cdot (x_1 - x_3) - y_1 \end{cases} \qquad (2.64)$$

и

$$x_1 = x_2 \Rightarrow \begin{cases} \lambda = (3 \cdot x_1^2 + 2 \cdot b \cdot x_1 + c) \cdot (2 \cdot y_1)^{-1} \\ x_3 = a^{-1} \cdot \lambda^2 - 2 \cdot x_1 - b \cdot a^{-1} \\ y_3 = \lambda \cdot (x_1 - x_3) - y_1 \end{cases} . \qquad (2.65)$$

Замечание 2.4. Вычисление координат точки $P_3 = P_1 +_{G_E} P_2$ $(P_1, P_2, P_3 \in E)$ в соответствии с формулой (2.64) допускает следующую геометрическую интерпретацию:

Шаг 1. Проведем прямую l_1 через точки P_1 и P_2.

Шаг 2. Найдем точку $A \in E$ пересечения прямой l_1 с ЭК E.

Шаг 3. Проведем через точку A вертикальную прямую l_2.

Шаг 4. Найдем вторую точку $B \in E$ пересечения прямой l_2 с ЭК E.

Шаг 5. $P_3 := B$ и конец.

Сказанное выше проиллюстрировано на рис. 2.10 для ЭК E, определенной уравнением $y^2 = x^3 - x$.

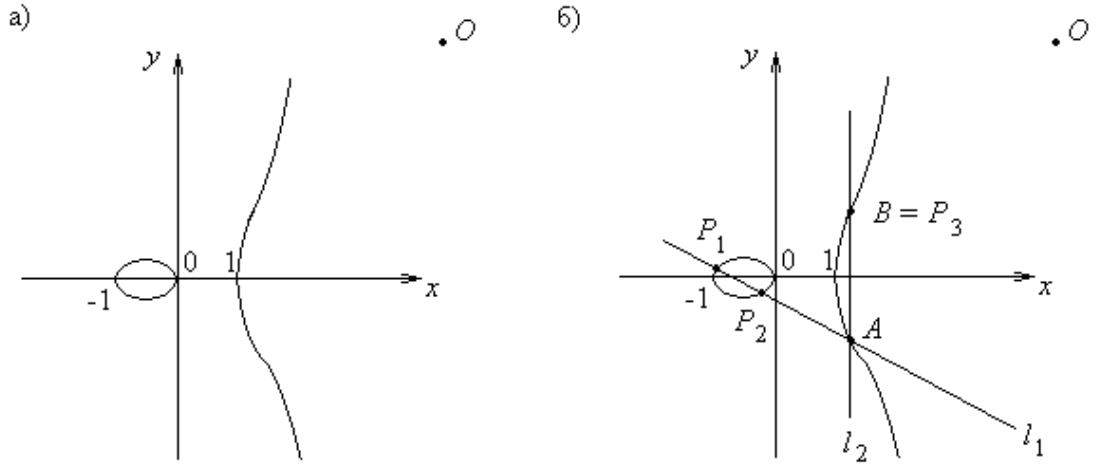


Рис. 2.10. Абелева группа для ЭК E: а) ЭК E, определенная уравнением $y^2 = x^3 - x$; б) сложение точек P_1 и P_2 ЭК E.

Для любого элемента $P \in G_E$ группы G_E, как и для элемента любой аддитивной группы, полагают

$$n \cdot P = \underbrace{P +_{\mathsf{G}_E} \ldots +_{\mathsf{G}_E} P}_{n \ раз} \quad (n \in \mathbf{N}).$$

Эллиптические кривые можно рассматривать над любым полем.

Если в (2.62) перейти к полю Галуа $\mathbf{GF}(p^k) = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (где p — простое число, а $k \in \mathbf{N}$), то получим уравнение

$$E: \ y^2 = a \circ x^3 \oplus b \circ x^2 \oplus c \circ x \oplus d \quad (a,b,c,d \in \mathbf{Z}_{p^k}). \tag{2.66}$$

Множество точек $(x, y) \in \mathbf{Z}_{p^k}^2$, являющихся решением уравнения (2.66), называется *эллиптической кривой* (ЭК) *над полем Галуа* $\mathbf{GF}(p^k)$.

Для ЭК E над полем Галуа $\mathbf{GF}(p^k)$, определенной уравнением (2.66), формулы (2.63)-(2.65) принимают следующий вид:

$$-P = (x, \Theta y), \tag{2.67}$$

$$x_1 \neq x_2 \Rightarrow \begin{cases} \lambda = (y_2 \Theta y_1) \circ \cdot (x_2 \Theta x_1)^{-1} \\ x_3 = a^{-1} \cdot \lambda^2 \Theta x_1 \Theta x_2 \Theta b \circ a^{-1} \\ y_3 = \lambda \circ (x_1 \Theta x_3) \Theta y_1 \end{cases} \tag{2.68}$$

и

$$x_1 = x_2 \Rightarrow \begin{cases} \lambda = (3 \circ x_1^2 \oplus 2 \circ b \circ x_1 \oplus c) \circ (2 \circ y_1)^{-1} \\ x_3 = a^{-1} \circ \lambda^2 \Theta 2 \circ x_1 \Theta b \circ a^{-1} \\ y_3 = \lambda \circ (x_1 \Theta x_3) \Theta y_1 \end{cases}. \tag{2.69}$$

Подчеркнем, что любая ЭК E над полем Галуа $\mathbf{GF}(p^k)$, в отличие от ЭК, определенных над полем действительных или рациональных чисел, представляет собой конечное множество точек.

Таким образом, каждая точка $P \in E$ является элементом конечного порядка в группе G_E.

Отметим, что порядком точки $P \in E$ является такое наименьшее число $n \in \mathbf{N}$, что

$$n \cdot P = O.$$

Для ЭК E над полем Галуа $\mathbf{GF}(p^k)$ поиск решения уравнения

$$x \cdot A = B \quad (A, B \in E)$$

является решением задачи дискретного логарифмирования на ЭК.

Именно этот фактор делает привлекательным построение систем ЭЦП на основе ЭК, определенных над конечными полями.

Практика показала, что решение задачи дискретного логарифмирования на ЭК сложнее решения задачи дискретного логарифмирования на мультипликативной группе $Z_p = (\mathbf{Z}_p, \circ)$ (p — простое число).

По-видимому, это объясняется тем, что сложение точек ЭК в соответствии с формулами (2.68) и заведомо (2.69) сложнее модульного умножения.

Известно, что если $p > 3$, то с помощью замены переменных от уравнения (2.66) можно перейти к уравнению вида

$$E:\ y^2 = x^3 \oplus a \circ x \oplus b \quad (a, b \in \mathbf{Z}_{p^k}). \tag{2.70}$$

Именно такие ЭК, определенные над полем Галуа $\mathbf{GF}(p^k)$, и используются в реальных системах ЭЦП на основе ЭК над конечными полями.

Для ЭК E над полем Галуа $\mathbf{GF}(p^k)$, определенной уравнением (2.70), формулы (2.68) и (2.69) упрощаются и принимают следующий вид

$$x_1 \neq x_2 \Rightarrow \begin{cases} \lambda = (y_2 \Theta y_1) \circ \cdot (x_2 \Theta x_1)^{-1} \\ x_3 = \lambda^2 \Theta x_1 \Theta x_2 \\ y_3 = \lambda \circ (x_1 \Theta x_3) \Theta y_1 \end{cases} \tag{2.71}$$

и

$$x_1 = x_2 \Rightarrow \begin{cases} \lambda = (3 \circ x_1^2 \oplus a) \circ (2 \circ y_1)^{-1} \\ x_3 = \lambda^2 \Theta 2 \circ x_1 \\ y_3 = \lambda \circ (x_1 \Theta x_3) \Theta y_1 \end{cases}. \tag{2.72}$$

Рассмотрим алгоритм *ECDSA* формирования ЭЦП на основе ЭК, определенных над полем Галуа.

Для организации такой ЭЦП вначале осуществляется генерация ключей на основе следующего алгоритма.

Алгоритм 2.12.

Шаг 1. Выбираем над полем Галуа $\mathbf{GF}(p)$ такую ЭК E, что число точек ЭК E делится на достаточно большое натуральное число n.

Шаг 2. Выбираем точку $P \in E$ порядка n.

Шаг 3. Выбираем случайное число $d \in \{1, \ldots, n-1\}$.

Шаг 4. $Q := d \cdot P$.

Шаг 5. Число d — секретный ключ, а (E, P, n, Q) — открытый ключ.

Обозначим через H хэш-функцию, отображающую последовательность $u \in \mathbf{E}^+$ в элемент поля Галуа $\mathbf{GF}(p)$.

Замечание 2.5. В стандартах *ANSI X9F1* и *IEEE P1363* в качестве хэш-функции H используется стандартная хэш-функция *SHA-1*.

Алгоритм *ECDSA* формирования ЭЦП под сообщением $u \in \mathbf{E}^+$ имеет следующий вид.

Алгоритм 2.13.

Шаг 1. Выбираем случайное число $k \in \{1,\ldots,n-1\}$.

Шаг 2. Вычисляем точку $k \cdot P$ $(=(x_1, y_1))$ ЭК E.

Шаг 3. $r := x_1 \pmod n$.

Шаг 4. Если $r = 0$, то переход к шагу 1, иначе — к шагу 5.

Шаг 5. Вычисляется элемент k^{-1} поля Галуа $\mathbf{GF}(p)$.

Шаг 6. Вычисляется элемент $H(u)$ поля Галуа $\mathbf{GF}(p)$.

Шаг 7. $s := k^{-1} \circ (H(u) \oplus d \circ r)$.

Шаг 8. Если $s = 0$, то переход к шагу 1, иначе — к шагу 9.

Шаг 9. Упорядоченная пара чисел (r, s) объявляется ЭЦП под сообщением u и конец.

Алгоритм проверки ЭЦП (r, s) имеет следующий вид

Алгоритм 2.14.

Шаг 1. Если $r, s \in \{1,\ldots,n-1\}$, то переход к шагу 2, иначе — к шагу 10.

Шаг 2. Вычисляется элемент s^{-1} поля Галуа $\mathbf{GF}(p)$.

Шаг 3. Вычисляется элемент $H(u)$ поля Галуа $\mathbf{GF}(p)$.

Шаг 4. $\alpha := H(u) \circ s^{-1}$.

Шаг 5. $\beta := r \circ s^{-1}$.

Шаг 6. $(x_0, y_0) := \alpha \cdot P +_{\mathsf{G}_E} \beta \cdot Q$.

Шаг 7. $v := x_0 \pmod n$.

Шаг 8. Если $v = r$, то переход к шагу 9, иначе — к шагу 10.

Шаг 9. ЭЦП (r, s) принимается и конец.

Шаг 10. ЭЦП (r, s) отвергается и конец.

Рассмотрим теперь организацию системы ЭЦП на основе ЭК, определенных над полем рациональных чисел, предложенную в [48].

Предполагается, что ЭК E задана уравнением (2.62), где $a, b, c, d \in \mathbf{Q}$. Таким образом, сложение в группе G_E осуществляется в соответствии с формулами (2.64) и (2.65).

По аналогии с тем, как это сделано для алгоритма *ECDSA*, секретный ключ — случайно выбранное натуральное число l, а открытый ключ — набор (E, P, Q), где $Q = l \cdot P$.

Обозначим через $gnrtr()$ псевдослучайный генератор натуральных чисел, а через H — такую хэш-функцию, что

$$H(u) \in \mathbf{E}^{256} \quad (u \in \mathbf{E}^+).$$

Для двоичной последовательности

$$\boldsymbol{\alpha} = \alpha_{255} \ldots \alpha_1 \alpha_0 \in \mathbf{E}^{256}$$

положим

$$a(\boldsymbol{\alpha}) = \sum_{i=0}^{255} \alpha_i \cdot 2^i .$$

Предложенный в [48] алгоритм формирования под сообщением $u \in \mathbf{E}^+$ ЭЦП на основе ЭК E, определенной над полем рациональных чисел, имеет следующий вид.

Алгоритм 2.15.

Шаг 1. $\boldsymbol{\alpha} := H(u)$, $v := a(\boldsymbol{\alpha})$.

Шаг 2. Если $v = 0$, то $v := 1$.

Шаг 3. $k := gnrtr()$.

Шаг 4. Вычисляем точку $k \cdot P$ $(= (x_1, y_1))$ ЭК E.

Шаг 5. $r := \lfloor x_1 \rfloor$.

Шаг 6. Если $r = 0$, то переход к шагу 3, иначе — к шагу 7.

Шаг 7. $s := r \cdot l + k \cdot v^{-1}$.

Шаг 8. Если $s = 0$, то переход к шагу 3, иначе — к шагу 9.

Шаг 9. Упорядоченная пара чисел (r, s) объявляется ЭЦП под сообщением u и конец.

Замечание 2.6. Отличия алгоритма 2.15 от алгоритма, используемого в *ГОСТ Р 34.10-2001*, состоят в следующем.

На шаге 5 алгоритма 2.15 число r определяется формулой

$$r := \lfloor x_1 \rfloor ,$$

а в алгоритме *ГОСТ Р 34.10-2001* — формулой

$$r := x_1 \ .$$

На шаге 6 алгоритма 2.15 число s определяется формулой

$$s := r \cdot l + k \cdot v^{-1},$$

а в алгоритме *ГОСТ Р 34.10-2001* — формулой

$$s := r \circ l \oplus k \cdot v .$$

Алгоритм проверки ЭЦП (r, s) состоит в следующем.

Алгоритм 2.16.

Шаг 1. $\boldsymbol{\alpha} := H(u)$, $v := a(\boldsymbol{\alpha})$.

Шаг 2. Если $v = 0$, то $v := 1$.

Шаг 3. $z_1 := s \cdot v$.

Шаг 4. $z_2 := (-r) \cdot v$.

Шаг 5. $(x_0, y_0) := z_1 \cdot P +_{\mathsf{G}_E} z_2 \cdot Q$.

Шаг 6. $w := \lfloor x_0 \rfloor$.

Шаг 7. Если $w = r$, то переход к шагу 9, иначе — к шагу 9.

Шаг 8. ЭЦП (r, s) принимается и конец.

Шаг 9. ЭЦП (r, s) отвергается и конец.

Замечание 2.7. Отличия алгоритма 2.16 от алгоритма, используемого в *ГОСТ Р 34.10-2001*, состоят в следующем.

На шаге 3 алгоритма 2.16 число z_1 определяется формулой

$$z_1 := s \cdot v,$$

а в алгоритме *ГОСТ Р 34.10-2001* — формулой

$$z_1 := s \circ v^{-1}.$$

На шаге 4 алгоритма 2.16 число z_2 определяется формулой

$$z_2 := (-r) \cdot v,$$

а в алгоритме *ГОСТ Р 34.10-2001* — формулой

$$z_2 := (-r) \circ v^{-1}.$$

Из корректности алгоритма *ГОСТ Р 34.10-2001* и из замечаний 2.6 и 2.7 вытекает

Теорема 2.5. Пара алгоритмов 2.15 и 2.16 является корректной системой ЭЦП на основе ЭК, определенных над полем рациональных чисел.

Предложенная система ЭЦП на основе ЭК, определенных над полем рациональных чисел, реализована на ЭВМ.

Реализация имеет модульную структуру.

В виде отдельных функций реализованы базовые алгоритмы вычисления:

1) координат точек $2 \cdot P$ $(P \in E)$ ЭК E;

2) координат суммы $P_1 +_{G_E} P_2$ $(P_1, P_2 \in E)$ двух точек ЭК E;

3) координат точек $n \cdot P$ $(P \in E)$ ЭК E (для увеличения скорости работы программы сложение реализовано по степеням числа 2, а для подсчета оставшихся членов данная функция вызывается рекурсивным образом).

Входными данными программы является хэш-образ подписываемого сообщения, коэффициенты, определяющие ЭК E над полем рациональных чисел, и базовая точка $P \in E$ ЭК E.

Хэш-образ вычислялся с помощью стандартного алгоритма *MD 5*.

Результаты контрольных просчетов приведены в таблице 2.1.

Таблица 2.1.

Размер сообщения, Мбайт	Время формирования ЭЦП, с.
Менее 1	Менее 1
Менее 2	Менее 1
Менее 10	Менее 4
Менее 20	Менее 10

Теоретически возможно, что в процессе применения программной реализации предложенной системы ЭЦП на основе ЭК, определенной над полем рациональных чисел могут возникнуть ошибки, связанные с процессом округления.

Для нивелирования таких ошибок достаточно применить подход, основанный на повышении точности вычислений, по аналогии с тем, как это сделано в [13,91-96] при решении обратных задач хаотической динамики.

2.7. Рекурсивный нестационарный секретный замок.

Известно, что одним из способов предотвращения несанкционированного доступа к информации является установка секретного замка. Простейшим вариантом секретного замка является парольный доступ к компьютеру.

Классическая математическая модель секретного замка — это сильно связный инициальный конечный автомат, построенный следующим образом (см., напр., [208]).

Зафиксируем входной алфавит X $(|X|\geq 2)$.

Обозначим через T_h $(h\in \mathbf{N})$ корневое ранжированное дерево высоты h, удовлетворяющее следующим пяти условиям.

Условие 2.15. Вершины дерева T_h расположены в уровнях с номерами $0,1,\ldots,h$ и так отмечены натуральными числами, что нумерация вершин осуществляется последовательно, уровень за уровнем, а в пределах любого уровня — слева направо.

Условие 2.16. Каждая вершина дерева T_h, расположенная в последнем, h-м уровне, отмечена числом 1.

Условие 2.17. Из каждой вершины, расположенной в i-м уровне $(i=0,1,\ldots,h-1)$ дерева T_h, выходит $|X|$ дуг, идущих в вершины $(i+1)$-го уровня.

Условие 2.18. Дуги дерева T_h так отмечены элементами множества $X\times\mathbf{E}$, что для отметок (x_1,α_1) и (x_2,α_2) любых двух дуг, выходящих из одной и той же вершины, $x_1\neq x_2$.

Условие 2.19. В дереве T_h существует единственная дуга с такой отметкой $(x,\alpha)\in X\times\mathbf{E}$, что $\alpha=1$. Эта дуга выходит из вершины расположенной в $(h-1)$-м уровне дерева T_h.

Дерево T_h определяет такой инициальный автомат, что:

1) существует единственное входное слово $x_1\ldots x_h\in X^h$, на которое реакцией автомата является выходное слово $\underbrace{0\ldots0}_{h-1\ раз}1$;

2) реакцией автомата на любое входное слово $u \neq x_1 \dots x_h$ является выходное слово $\underbrace{0 \dots 0}_{h \text{ раз}}$.

Инициальный автомат, определяемый деревом T_h, называется *секретным замком*, а входное слово $x_1 \dots x_h \in X^h$ — *секретным ключом*.

Так как дерево T_h (а, следовательно, и секретный ключ $x_1 \dots x_h \in X^h$) не изменяется во времени, то такой секретный замок естественно назвать *стационарным* секретным замком.

Стационарный секретный замок, определяемый деревом T_h, обладает следующими двумя недостатками.

Во-первых, представляется сомнительной возможность эффективной вычислительно стойкой компактной реализации стационарного секретного замка, если на структуру секретного ключа $x_1 \dots x_h \in X^h$ не наложены никакие ограничения. В то же время, ограничения, накладываемые на структуру секретного ключа, могут существенно сократить множество допустимых вариантов.

Во-вторых, постоянство ключа $x_1 \dots x_h \in X^h$ во времени приводит к тому, что часть этой последовательности может быть найдена из-за «утечки информации». В результате перебор вариантов, направленный на восстановление недостающей части ключа, может существенно сократиться и оказаться выполнимым для криптоаналитика.

В силу указанных выше недостатков представляется весьма перспективной разработка математических моделей и методов построения *нестационарного* секретного замка, т.е. такого секретного замка, что:

1) «отверстие», а, следовательно, и секретный ключ изменяются во времени;

2) «утечка информации» о текущем значении секретного ключа практически не дает криптоаналитику никакой информации о будущих значениях секретного ключа;

3) секретный замок допускает эффективную вычислительно стойкую компактную программно-аппаратную реализацию;

4) вычислительных ресурсов криптоаналитика недостаточно для осуществления полного перебора вариантов.

Рассмотрим подход к решению этой задачи, развитый в [165-167,305].

Пусть $f \in \mathsf{S}(\mathbf{Z}_n)$ и

$$f = D_{r_1} \dots D_{r_l} \quad (r_1, \dots, r_l \in \mathbf{N}; r_1 + \dots + r_l = n),$$

где D_{r_i} $(i = 1, \dots, l)$ — цикл длины r_i. Тогда

$$|f| = [r_1, \dots, r_l], \tag{2.73}$$

где $|f|$ — порядок подстановки f.

Из (2.73) вытекает, что циклическая группа, порожденная подстановкой $f \in \mathsf{S}(\mathbf{Z}_n)$, дает возможность строить достаточно широкий класс преобразований множества $\mathbf{Z}_n$.

А так как

$$f^h = D_{r_1}^h \ldots D_{r_l}^h \quad (h \in \mathbf{N}), \tag{2.74}$$

то каждую подстановку f^h $(h \in \mathbf{N})$ можно рассматривать как независимое «параллельное функционирование» циклов D_{r_i} $(i = 1, \ldots, l)$.

Равенство (2.74) обосновывает целесообразность использования при построении секретного замка следующей комбинаторной конструкции.

Определение 2.2. Назовем *счетчиком* такой автономный автомат без выхода $C(k) = (\mathbf{Z}_k, \{x\}, \delta_k)$ $(k \in \mathbf{N}; k \geq 2)$, что для всех $z \in \mathbf{Z}_k$

$$\delta_k(z, x) = (z + 1) \pmod{k}.$$

Сопоставим с каждой конечной последовательностью счетчиков

$$C(k_1), \ldots, C(k_n)$$

такой автономный автомат

$$\varsigma(C(k_1), \ldots, C(k_n)) = (\overset{n}{\underset{j=1}{\times}} \mathbf{Z}_{k_j}, \{x\}, \boldsymbol{\delta}),$$

что

$$\boldsymbol{\delta}((z_1, \ldots, z_n), x) = (\delta_{k_1}(z_1, x), \ldots, \delta_{k_n}(z_n, x)). \tag{2.75}$$

для всех $(z_1, \ldots, z_n) \in \overset{n}{\underset{j=1}{\times}} \mathbf{Z}_{k_j}$.

Отметим, что из (2.75) вытекает, что автомат $\varsigma(C(k_1), \ldots, C(k_n))$ представляет собой декартово произведение счетчиков $C(k_1), \ldots, C(k_n)$ с отождествлением их входов.

Так как

$$\prod_{j=1}^{n} k_j = (k_1, \ldots, k_n) \cdot [k_1, \ldots, k_n],$$

то из (2.73) и (2.74) вытекает, что:

1) автомат $\varsigma(C(k_1), \ldots, C(k_n))$ состоит из $(k_1, \ldots, k_n)$ компонент сильной связанности, каждая из которых содержит $[k_1, \ldots, k_n]$ состояний;

2) состояния $(z_1^{(1)}, \ldots, z_n^{(1)})$ и $(z_1^{(2)}, \ldots, z_n^{(2)})$ автомата $\varsigma(C(k_1), \ldots, C(k_n))$ принадлежат одной и той же компоненте сильной связанности тогда и только тогда, когда существует такое число $l \in \{0, 1, \ldots, [k_1, \ldots, k_n] - 1\}$, что совместна система сравнений

$$l \equiv (z_j^{(2)} - z_j^{(1)}) \pmod{k_j} \quad (j = 1, \ldots, n).$$

Построим теперь рекурсивный нестационарный секретный замок.

Зафиксируем последовательность счетчиков $C(k_1), \ldots, C(k_n)$ и автомат

$$\varsigma(C(k_1),\ldots,C(k_n)) = (\overset{n}{\underset{j=1}{\times}}\mathbf{Z}_{k_j},\{x\},\boldsymbol{\delta}).$$

Положим

$$Q = \overset{n}{\underset{j=1}{\times}}\mathbf{Z}_{k_j},$$

$$k = \prod_{j=1}^{n} k_j,$$

$$d = (k_1,\ldots,k_n)$$

и

$$m = [k_1,\ldots,k_n].$$

Упорядочим множество Q с помощью обычного отношения лексикографического порядка $<_Q$ и занумеруем элементы множества Q в порядке их возрастания, т.е. $Q = \{q_1,\ldots,q_k\}$, где $q_1 <_Q \ldots <_Q q_k$.

Обозначим через π разбиение множества Q, блоками которого являются множества состояний, принадлежащие одной и той же компоненте сильной связанности автомата $\varsigma(C(k_1),\ldots,C(k_n))$.

Занумеруем блоки разбиения π в порядке возрастания их минимальных элементов. Таким образом, $\pi = \{B_1,\ldots,B_m\}$, где $|B_i| = d$ $(i = 1,\ldots,m)$ и для всех $i, j \in \mathbf{N}_m$ $(i \neq j)$

$$i < j \Rightarrow \min B_i < \min B_j.$$

Определим функцию $g : \mathbf{N}_d \to Q$ равенством

$$g(i) = \min B_i \quad (i \in \mathbf{N}_d).$$

Зафиксируем такое число $L \in \mathbf{N}$, что $L >> m$ и положим

$$T_r = \{j + L\cdot(r-1) \mid j \in \mathbf{Z}_L\} \quad (r \in \mathbf{N}).$$

Пусть задана такая кусочно-постоянная общерекурсивная функция $\Psi : \mathbf{Z}_+ \to \mathbf{N}_k$, что для каждого значения $r \in \mathbf{N}$:

1) $\Psi(t) = const$ при всех значениях $t \in T_r$;

2) если $t_1 \in T_r$ и $t_2 \in T_{r+1}$, то $\Psi(t_1) \neq \Psi(t_2)$.

Обозначим через $P_\Psi : \mathbf{Z}_+ \times \mathbf{N}_d \times \mathbf{Z}_+ \to \mathbf{E}$ общерекурсивный предикат, значения $P_\Psi(t,i,h)$ $(t \in \mathbf{Z}_+, i \in \mathbf{N}_d, h \in \mathbf{Z}_+)$ которого вычисляются в соответствии со следующим алгоритмом.

Алгоритм 2.17.

Шаг 1. $u := g(i)$.

Шаг 2. $v := \boldsymbol{\delta}(u, x^h)$.

Шаг 3. $w := q_{\Psi(t)}$.

Шаг 4. Если $v = w$, то переход к шагу 5, иначе — к шагу 6.

Шаг 5. $P_\Psi(t,i,h) \coloneqq 1$ и конец.

Шаг 6. $P_\Psi(t,i,h) \coloneqq 0$ и конец.

Предикат P_Ψ и является *рекурсивным нестационарным секретным замком*.

Число $t \in \mathbf{Z}_+$ — это момент времени, в который начинается процедура открытия секретного замка.

Любая такая упорядоченная пара (i,h) $(i \in \mathbf{N}_d, h \in \mathbf{Z}_+)$, что $P_\Psi(t,i,h) = 1$ — *секретный ключ*, а общерекурсивная функция Ψ — средство управления «отверстием» замка.

Отметим, что в каждый момент времени $t \in \mathbf{Z}_+$ для каждого секретного ключа (i,h) существует единственное допустимое значение $i \in \{1,\ldots,d\}$ и бесконечное множество S $(S \subseteq \mathbf{Z}_+)$ таких допустимых значений числа h, что

$$h_1 - h_2 \equiv 0 \,(\mathrm{mod}(m-1))$$

для любых $h_1, h_2 \in S$.

Построенный рекурсивный нестационарный секретный замок допускает реализацию, представленную на рис. 2.11.

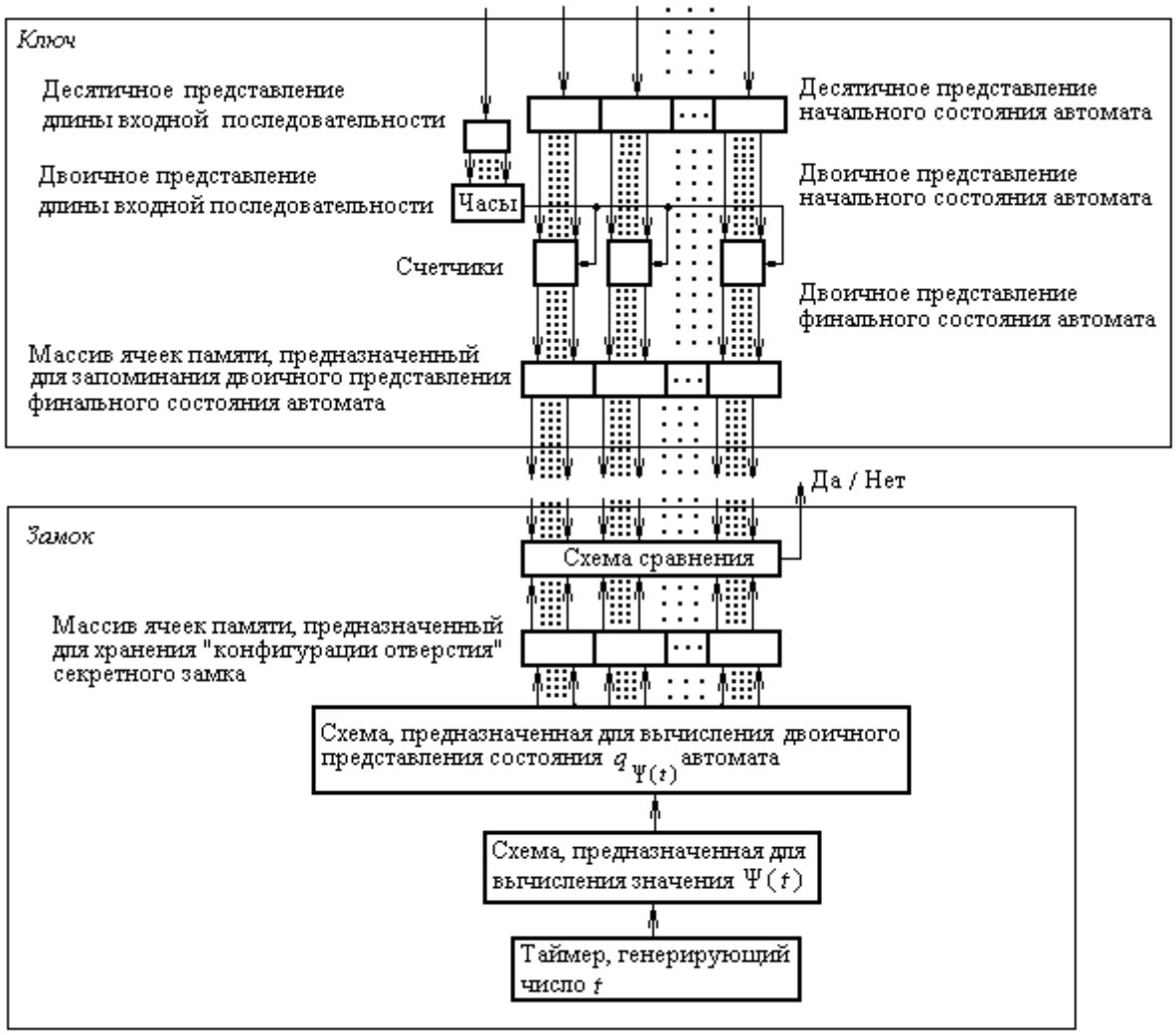


Рис. 2.11. Схематическое представление рекурсивного нестационарного секретного замка.

Предположим, что криптоаналитик не располагает никакой информацией об общерекурсивной функции Ψ, а вся информация, известная криптоаналитику о последовательности счетчиков представляет собой число n и либо число

$$k = \prod_{j=1}^{n} k_j ,$$

либо число

$$r = \sum_{j=1}^{n} k_j .$$

Тогда единственный метод «взлома» рекурсивного нестационарного секретного замка состоит в следующем. Вначале криптоаналитик решает, соответственно, задачу факторизации числа k на n сомножителей или задачу разбиения числа k на n положительных слагаемых. Затем для каждого решения осуществляется перебор по всем допустимым упорядоченным парам (i,h).

Если время апробации всех допустимых комбинаций (i,h) значительно превосходит длительность интервала постоянства общерекурсивной функции Ψ, то вероятность «взлома» предложенного рекурсивного нестационарного секретного замка, фактически эквивалентна вероятности «угадывания результата».

2.8. Выводы.

В настоящем разделе рассмотрены математические модели и методы решения модельных задач криптографии. Основные результаты состоят в следующем:

1. Предложена общая модель нестационарного поточного шифра, основанного на выборе и настройке с помощью псевдослучайных генераторов алгоритмов шифрования, принадлежащих заданному семейству. Для такого шифра секретный сеансовый ключ — это параметры, определяющие настройку псевдослучайных генераторов. Показано, что отсутствие внешних обменов, связанных с настройкой алгоритмов шифрования и с передачей сеансовых ключей для алгоритмов шифрования существенно усложняет «взлом» такого шифра.
2. Разработан аксиоматический подход к решению задачи полного разрушения частот букв в словах исходного текста, основанный на использовании регулярных комбинаторных структур. Исследованы детализации для случаев, когда в качестве регулярной комбинаторной структуры выбраны либо шары в векторном пространстве над полем $\mathbf{GF}(2)$, либо грани единичного куба.
3. Построена модель «диффузии информации», основанная на использовании подгрупп симметрической группы подстановок. Исследована детализация, когда подгруппа порождается графом с почти регулярной структурой.
4. Предложена, и исследована модель нестационарного поточного шифра, основанная на семействе автоматных моделей, представленных полными бинарными деревьями.
5. Предложена, и исследована модель нестационарного поточного шифра «рюкзачного типа», основанная на использовании множества сверхрастущих рюкзачных векторов различной длины.
6. Предложена схема организации электронной цифровой подписи, основанная на использовании эллиптических кривых над полем $\mathbf{Q}$. В этой схеме, в отличие от использования эллиптических кривых над полем $\mathbf{GF}(p)$, отсутствуют проблема выбора эллиптической кривой, а также проблема поиска точек на выбранной кривой.
7. Предложена, и исследована модель нестационарного секретного замка, в котором «секретный ключ» — комбинация счетчиков, т.е. конечных

автоматов специального вида, а сам «замок» основан на алгоритме вычисления значений общерекурсивной функции.

3. РЕШЕНИЕ МОДЕЛЬНЫХ ЗАДАЧ ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ КУСОЧНО-ЛИНЕЙНЫХ ОТОБРАЖЕНИЙ

При использовании хаотических отображений в процессе решения задач преобразования информации предполагается, что применяются сужения этих отображений на соответствующее конечное подмножество рациональных чисел. Отсюда сразу же вытекает, что существует глубокая внутренняя связь между эволюцией динамических систем, представленных хаотическими отображениями, и шифрами, основанными на перестановках.

Актуальность исследования этой внутренней связи обусловлена тем, что появляется возможность охарактеризовать в терминах хорошо изученных комбинаторных структур как сложность, так и вычислительную стойкость процессов, представленных в терминах динамики в фазовом пространстве.

Основная цель настоящего раздела состоит в том, чтобы исследовать в терминах симметрической группы особенности применения простейших одномерных кусочно-линейных отображений к решению модельных задач преобразования информации.

В п.3.1 построен нестационарный шифр, основанный на использовании ансамбля динамических систем, каждая из которых представлена хаотическим отображением «зуб пилы». В п.3.2 построена и исследована общая схема нестационарного шифра, основанного на записи информации на кодируемых впоследствии циклических аттракторах одномерных кусочно-линейных отображений. Детализирован механизм кодирования этих циклических аттракторов в терминах их представления элементами симметрической группы. В п.3.3 построена и исследована схема организации многопользовательского доступа к каналу связи, основанная на использовании циклических аттракторов ансамбля одномерных кусочно-линейных отображений. Предложенная схема представляет собой, по своей сути, нестационарный шифр, основанный на перестановках.

Материал, представленный в настоящем разделе, основан на результатах, полученных в [170,171,173].

3.1. Шифр на основе отображения «зуб пилы».

Рассмотрим хаотическое отображение «зуб пилы»

$$x_{n+1} = \{2 \cdot x_n\} \ (n \in \mathbf{Z}_+). \tag{3.1}$$

где $\{a\}$ $(a \in \mathbf{R})$ – дробная часть числа a, а начальное значение x_0 выбирается так, что

$$x_0 \in (0,1). \tag{3.2}$$

Динамическая система $S_2^{зп}$, эволюция которой описывается рекуррентным соотношением (3.1) при начальном состоянии x_0, удовлетворяющем условию (3.2), осуществляет движение по траектории в фазовом пространстве

$$X = [0,1).$$

Итерационная диаграмма, иллюстрирующая динамику этого движения на первых пяти шагах дискретного времени изображена на рис. 3.1.

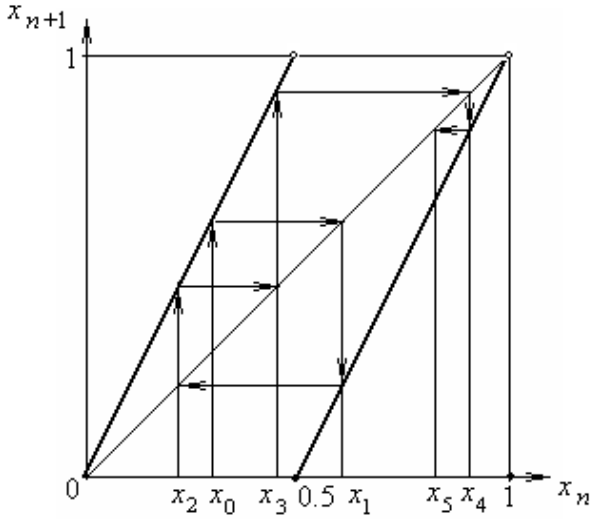


Рис. 3.1. Итерационная диаграмма.

Представим состояния

$$x_0, x_1, x_2, \ldots$$

динамической системы $\mathsf{S}_2^{зп}$ в двоичной системе счисления (это предположение не ограничивает общности рассуждения, и принято только для упрощения изложения). Тогда вычисление в соответствии с рекуррентным соотношением (3.1) состоит в том, что двоичная последовательность

$$x_n = 0.\alpha_1\alpha_2\alpha_3\ldots$$

сдвигается на один разряд влево, причем цифра, оказавшаяся слева от точки отбрасывается, т.е.

$$x_{n+1} = 0.\alpha_2\alpha_3\ldots.$$

Пусть x_0 – рациональное число, представимое бесконечной периодической двоичной дробью

$$x_0 = 0.\alpha_1\alpha_2\alpha_3\ldots\alpha_k(\beta_1\beta_2\ldots\beta_l) \quad (l \geq 2).$$

Тогда

$$x_n = x_{n+l}$$

для всех $n \geq k$, т.е. аттрактором является устойчивый предельный цикл, определяемый следующей последовательностью l точек

$$x_k = (\beta_1\beta_2\ldots\beta_l),\ x_{k+1} = (\beta_2\beta_3\ldots\beta_l\beta_1),\ \ldots, x_{k+l-1} = (\beta_l\beta_1\ldots\beta_{l-2}\beta_{l-1})$$

Этот предельный цикл определяется всеми правыми циклическими сдвигами двоичной последовательности $\beta_1\beta_2\ldots\beta_l$. Таким образом, установлено соответствие между динамикой системы $\mathsf{S}_2^{зп}$ и элементами симметрической группы $\mathsf{S}(l)$ $(l \in \mathbf{N})$.

Установленное выше соответствие между динамикой системы $\mathsf{S}_2^{зп}$ и элементами симметрической группы $\mathsf{S}(l)$ $(l \in \mathbf{N})$ дает возможность выде-

лить следующий нетривиальный подкласс класса нестационарных шифров, основанных на перестановках.

Пусть исходная двоичная последовательность распределена тем или иным образом по двоичным последовательностям меньшей длины, каждую из которых будем интерпретировать как период правильной дроби, представленной в двоичном виде. Применим одновременно к каждой полученной последовательности несколько правых циклических сдвигов. Такое действие эквивалентно начальному фрагменту динамики ансамбля динамических систем $S_2^{зп}$, стартующих из начальных состояний, определяемых полученными последовательностями.

Таким образом, мы приходим к шифру, представленному на рис. 3.2.

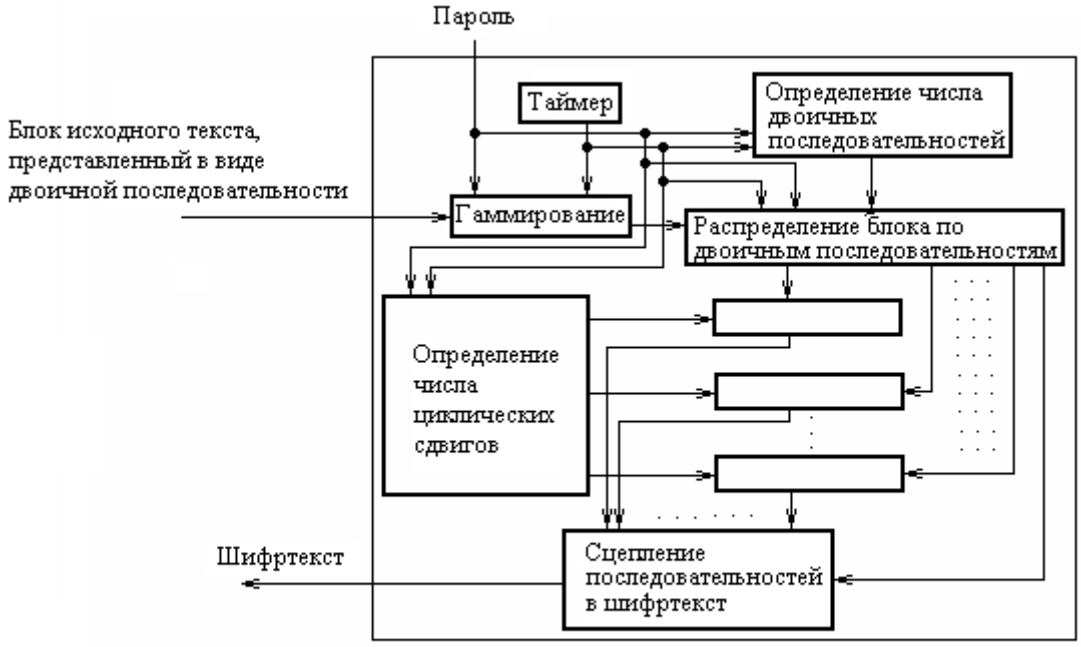


Рис. 3.2. Схема шифра, основанного на отображении "зуб пилы".

Внутренний таймер обеспечивает свойство «быть нестационарным шифром». Гаммирование в совокупности с распределением исходного текста по двоичным последовательностям определяет этап предвычислений, главная цель которого состоит в том, чтобы усложнить криптоанализ и осуществить диффузию информации. Основной этап шифрования осуществляется включением ансамбля динамических систем $S_2^{зп}$. Ясно, что в результате сцепления последовательностей, представляющих финальные состояния систем, входящих в ансамбль, произойдет разрушение частот, присущих исходному тексту, подвергнутому предвычислениям.

Отметим, что для построенного шифра секретный ключ представляет собой пароль, а также средства, предназначенные для синхронизации процессов шифрования и расшифровки. Именно этот пароль и дает возмож-

ность осуществить расшифровку шифртекста. Существование такой возможности вытекает из обратимости применяемых операций.

Демо-версия предложенного алгоритма была реализована с помощью интегрированной среды разработки Delphi. Построенная программная реализация дает возможность осуществлять «шифрование-расшифровку» текстов, а также изображений, представленных bmp-файлами, причем зашифрованные изображения являются стандартными bmp-файлами, и доступны для просмотра.

Для оценки последствий изменений в зашифрованных данных, полученных в результате внешнего вмешательства криптоаналитика, имеется возможность загрузки файлов в виде битовой последовательности и их побитового редактирования с последующим сохранением.

Главное окно программы (рис. 3.3) содержит поле для ввода исходного текста, а также две диаграммы. На первой диаграмме изображен в графическом виде набор битовых последовательностей, которые были получены в результате разбиения исходных данных по группам, а на второй диаграмме – набор битовых последовательностей, к каждой из которых были применены несколько правых циклических сдвигов. Каждая точка на диаграмме представляет собой периодическую дробь из интервала [0,1), которой соответствует некоторая битовая последовательность.

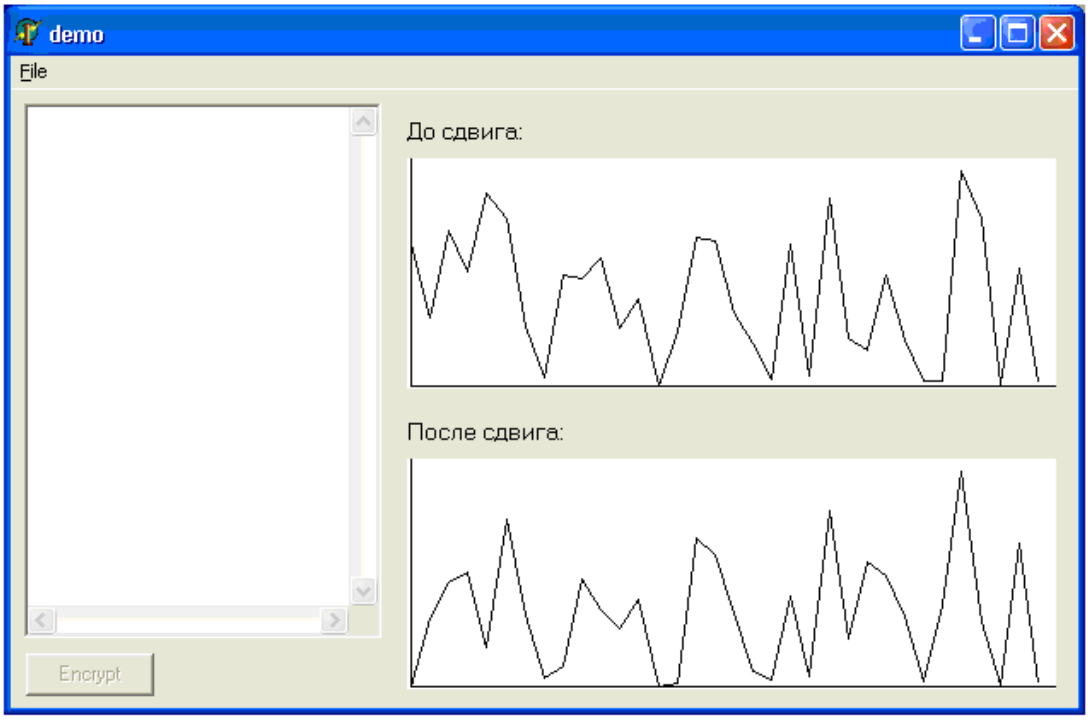


Рис. 3.3. Главное окно программы.

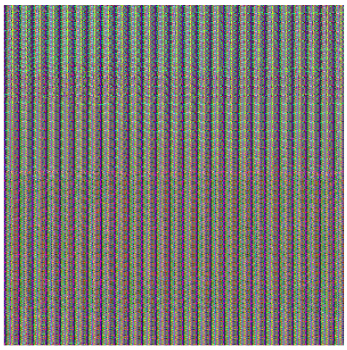
Все операции по «шифрованию-расшифровке» осуществляются из меню **File** главного окна программы.

Поскольку в процессе вычислений используются только простейшие арифметические операции, а также высокоскоростные функции ассемблера для осуществления циклического сдвига, данная программная реализация обладает высокой скоростью работы.

Пример 3.1. Ниже приведены две иллюстрации применения разработанной демо-версии к bmp-файлам.

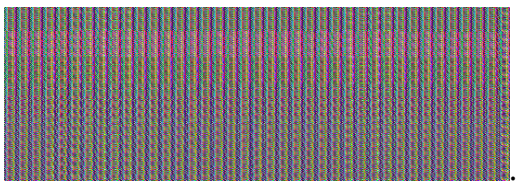
Графическому файлу

при фиксированном пароле соответствует графический файл



Графическому файлу

при фиксированном пароле соответствует графический файл



При вводе неправильного пароля, получаем неинформативное изображение

Предложенный шифр представляет собой, по своей сути, нестационарный шифр, основанный на перестановках, примененный к информации, предварительно подвергнутой диффузии. Это обстоятельство обосновывает высокую вычислительную стойкость предложенного шифра, которая подтверждается результатами экспериментов, как с текстовой, так и с графической информацией.

Полученные результаты естественным образом обобщаются на кусочно-линейные хаотические отображения вида

$$y = \{q \cdot x\} \quad (q \in \mathbf{N}, q > 2)$$

при условии, что точка $x \in [0,1)$ представлена в системе счисления с основанием q.

3.2. Шифры, основанные на циклических аттракторах кусочно-линейных отображений.

В [9,10] предложено решение задач записи и восстановления информации на основе методов хаотической динамики. Идея такого подхода состоит в том, что точка фазового пространства попадает в бассейн притяжения аттрактора хаотического отображения

$$\mathbf{u}_{n+1} = \mathbf{f}(\mathbf{u}_n, \mathbf{a}),$$

где $\mathbf{a}$ – вектор параметров, а $n \in \mathbf{N}$, с последующим ее падением на предельный цикл (рис.3.4).

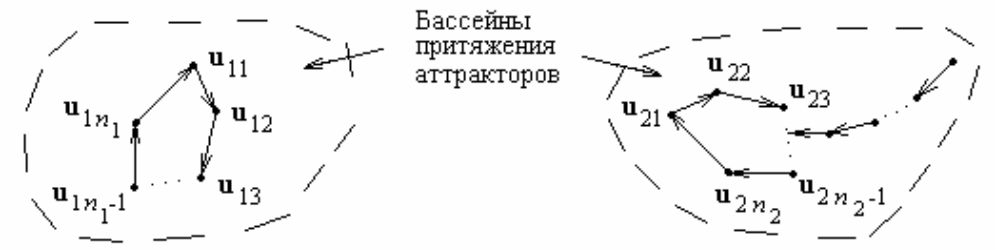


Рис. 3.4. Падение точки фазового пространства на предельный цикл.

Запись информации сводится к построению легко вычислимых отображений, реализующих указанные выше предельные циклы.

Покажем, что кусочно-линейные одномерные отображения

$$x_{n+1} = f(x_n) \quad (n \in \mathbf{N})$$

представляют собой эффективное средство для унифицированной реализации всех циклических перестановок

$$(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$$

букв алфавита

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Соответствие

$$a_j \leftrightarrow b_j = (j - 0.5) \cdot n^{-1} \in (0;1) \quad (j = 1, \ldots, n)$$

дает возможность осуществить переход от циклической перестановки

$$(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$$

букв, принадлежащих алфавиту A, к циклической перестановке

$$(b_{i_1}, b_{i_2}, \ldots, b_{i_n}),$$

чисел, принадлежащих алфавиту

$$\{(j-0.5)\cdot n^{-1} \mid j=1,\ldots,n\}.$$

Циклической перестановке чисел

$$(b_{i_1}, b_{i_2}, \ldots, b_{i_n})$$

поставим в соответствие последовательность точек плоскости

$$\mathbf{b}_j = (b_{i_j}, b_{i_{(j+1)(\mathrm{mod}\, n)}}) \quad (j=1,\ldots,n).$$

Определим кусочно-линейное одномерное отображение

$$x_{n+1} = f(x_n) \quad (n \in \mathbf{N})$$

на интервале

$$((j-1)\cdot n^{-1}; j\cdot n^{-1}) \quad (j=1,\ldots,n)$$

отрезком прямой линии с коэффициентом наклона s $(0<s<1)$, проходящей через точку $\mathbf{b}_j$.

Если задан интервал, содержащий начальную точку $\mathbf{b}_1$, то отображение f однозначно восстанавливает перестановку $(b_{i_1}, b_{i_2}, \ldots, b_{i_n})$, так как осуществляется движение (рис.3.5) по устойчивому циклу, определяемому точками

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n.$$

Устойчивость этого цикла обеспечивает условие $0<s<1$.

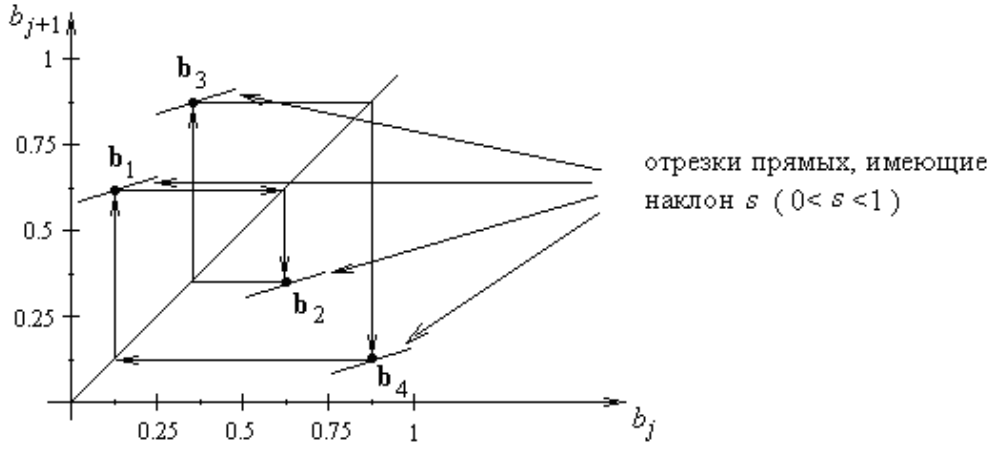


Рис. 3.5. Восстановление циклической перестановки в 4-х буквенном алфавите.

Подчеркнем, что восстановление блока информации $a_{i_1} a_{i_2} \ldots a_{i_n}$, состоящего из попарно различных букв алфавита A, обеспечивается взаимно-однозначным соответствием между этим блоком и упорядоченной парой

(*начальная точка*, *цикл*).

Рассмотренный выше метод записи блока информации, состоящего из попарно различных букв алфавита A, можно следующим образом распространить на запись любого блока информации

$$C = c_1 \ldots c_l \in A^l \quad (l \in \mathbf{N}),$$

т.е. на l-размещения с повторениями в алфавите A.

Положим

$$\mathbf{skltn}(C) = (\alpha_1, \ldots, \alpha_n),$$

где α_j $(j = 1, \ldots, n)$ – число вхождений буквы $a_j \in A$ в блок C. Таким образом, $\alpha_j \in \mathbf{Z}_+$ $(j = 1, \ldots, n)$ и $\sum\limits_{j=1}^{l} \alpha_j = l$. Обозначим через

$$a_{j_1}, \ldots, a_{j_h} \quad (1 \le j_1 < \ldots < j_h \le n)$$

те буквы алфавита A, которые соответствуют ненулевым компонентам вектора $\mathbf{skltn}(C)$. Зафиксируем такое h-блочное разбиение

$$\pi(C) = \{B_1, \ldots, B_h\}$$

множества $\mathbf{N}_l$, что

$$|B_r| = \alpha_{j_r}.$$

Рассмотрим следующую процедуру

Procedure $CDNG(C)$

begin
$code(C) := \Lambda$
do $i = 1, \ldots, l$
do $r = 1, \ldots, h$
if $c_i = a_{j_r}$
then
$code(C) := code(C) \uparrow\uparrow \min B_{j_r}$,
$B_{j_r} := B_{j_r} \setminus \min B_{j_r}$
end_if
end_do
end_do
end_begin

Ясно, что блок $code(C)$, полученный в результате применения процедуры $CDNG$ к блоку C, представляет собой циклическую перестановку букв алфавита $\mathbf{N}_l$. Поэтому рассмотренный выше метод записи информации непосредственно применим к блоку $code(C)$.

Любой цикл, определяемый последовательностью

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_l$$

точек плоскости

$$\mathbf{b}_j = (b_{i_j}, b_{i_{(j+1) \pmod l}}) \quad (j = 1, \ldots, l),$$

где

$$(b_{i_1}, b_{i_2}, \ldots, b_{i_n})$$

представляет собой циклическую перестановку чисел

$$b_j = (j - 0.5) \cdot l^{-1} \ (j = 1, \ldots, l),$$

т.е. характеризуется подстановкой

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_{l-1} & i_l \\ i_2 & i_3 & & i_l & i_1 \end{pmatrix} \in \mathsf{S}(l),$$

принадлежащей цикловому классу $\{1^0 2^0 \ldots l^1\}$.

Установленное взаимно-однозначное соответствие естественно приводит к задаче разработки шифров, основанных на представлении l-элементных блоков информации элементами симметрической группы $\mathsf{S}(l)$, принадлежащими цикловому классу $\{1^0 2^0 \ldots l^1\}$, кодируемыми впоследствии тем или иным образом. Общая схема такого шифра представлена на рис. 3.6.

Рис. 3.6. Общая схема шифра, основанного на циклических аттракторах.

Многообразие предложенных шифров определяется множеством механизмов управления нумерацией букв алфавита A, множеством механизмов выбора разбиения $\pi(C)$, а также множеством механизмов кодирования элементов циклового класса $\{1^0 2^0 \ldots l^1\}$.

Нумерацию букв алфавита A можно осуществить $n!$ способами, выбор разбиения $\pi(C) = \{B_1, \ldots, B_h\}$ можно осуществить $\dfrac{l!}{\alpha_{j_1}! \cdot \alpha_{j_2}! \cdot \ldots \cdot \alpha_{j_r}!}$ способами, а число способов кодирования элементов, принадлежащих цикловому классу $\{1^0 2^0 \ldots l^1\}$, заведомо не меньше, чем $(l-1)!$.

При этом ясно, что управление нумерацией букв алфавита A в комбинации с представлением информационного блока элементом циклового

класса $\{1^0 2^0 \ldots l^1\}$ и его последующим кодированием полностью разрушает возможность частотного анализа.

Следовательно, предложенная схема обеспечивает систематическое построение вычислительно стойких нестационарных поточных шифров за счет организации управления независимым выбором ключей в каждом из трех указанных субэкспоненциальных по мощности множеств.

Достаточно представительный класс механизмов управления ключами (т.е. управление нумерацией букв алфавита A, управление выбором разбиения $\pi(C)$ и управление кодированием элементов циклового класса $\{1^0 2^0 \ldots l^1\}$) основан на следующих двух операциях над элементами симметрической группы $\mathsf{S}(k)$ $(k \in \mathbf{N})$:

1) по заданной подстановке

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ v_1 & v_2 & & v_k \end{pmatrix} \in \mathsf{S}(k)$$

сгенерировать следующую за ней подстановку;

2) вычислить номер заданной подстановки

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ v_1 & v_2 & & v_k \end{pmatrix} \in \mathsf{S}(k).$$

Ясно, что достаточно рассмотреть эти операции при фиксированном упорядочении элементов симметрической группы $\mathsf{S}(k)$.

В качестве такого отношения порядка выберем лексикографический порядок, т.е.

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ v_1^{(1)} & v_2^{(1)} & \cdots & v_k^{(1)} \end{pmatrix} \prec \begin{pmatrix} 1 & 2 & \cdots & k \\ v_1^{(2)} & v_2^{(2)} & \cdots & v_k^{(2)} \end{pmatrix} \Leftrightarrow$$

$$\Leftrightarrow (\exists i \in \{0,1,\ldots,k-1\})(\forall j \in \{1,\ldots,i\})(v_j^{(1)} = v_j^{(2)} \ \& \ v_{i+1}^{(1)} < v_{i+1}^{(2)}).$$

При этом будем считать, что порядок – циклический, т.е. за последним элементом следует первый. Для упрощения обозначений будем представлять подстановку

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ v_1 & v_2 & & v_k \end{pmatrix} \in \mathsf{S}(k)$$

в виде $v_1 v_2 \ldots v_k$.

Рассмотрим вначале первую операцию.

Известно, что (см., напр., [168]) генерацию подстановки, следующей за подстановкой $v_1 v_2 \ldots v_k$, можно осуществить в соответствии со схемой, изображенной на рис. 3.7.

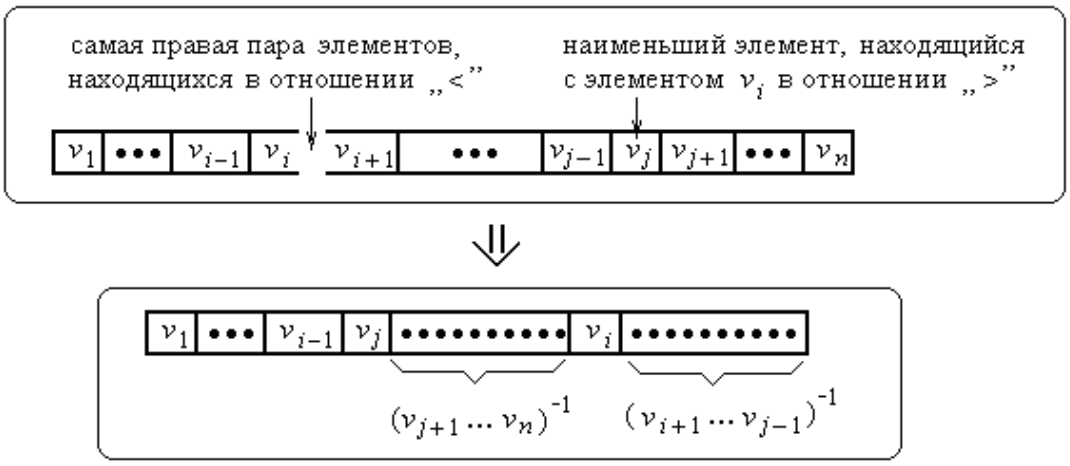


Рис. 3.7. Схема порождения следующего элемента множества $S(k)$.

Соответствующая процедура имеет следующий вид (через γ^{-1} обозначена записанная в обратном порядке последовательность γ).

Procedure $NEXT(v_1 v_2 \ldots v_k)$

begin

if $v_1 v_2 \ldots v_k = k(k-1)\ldots 21$

then $next(v_1 v_2 \ldots v_k) := 12\ldots(k-1)k$ **and** HALT

else $i := k-1$ **and go to** LABEL1

end_if

LABEL1: **if** $v_i > v_{i+1}$

then $i := i-1$ **and go to** LABEL1

else go to LABEL2

end_if

LABEL2: $\zeta := v_1 \ldots v_{i-1}$, $j := i+1$ **and go to** LABEL3

LABEL3: **if** $v_j > v_i$

then go to LABEL4

else $j := j-1$ **and go to** LABEL6

end_if

LABEL4: $j := j+1$

if $j \le k$

then go to LABEL3

else go to LABEL5

end_if

LABEL5: $\beta := v_{i+1} \ldots v_k$, $next(v_1 v_2 \ldots v_k) := \zeta \uparrow\uparrow \beta^{-1} \uparrow\uparrow v_i$ **and** HALT

LABEL6: $\xi := v_{i+1} \ldots v_{j-1}$, $\beta := v_{i+1} \ldots v_k$,

$next(v_1 v_2 \ldots v_k) := \zeta \uparrow\uparrow v_j \uparrow\uparrow \beta^{-1} \uparrow\uparrow v_i \uparrow\uparrow \xi^{-1}$ **and** HALT

end_begin

Ясно, что как временная, так и емкостная сложность процедуры *NEXT* равна $V = O(k)$ $(k \to \infty)$.

Для блока информации C процедура *NEXT* дает возможность организовать нестационарный выбор разбиения $\pi(C)$ с помощью итерационного процесса, имеющего временную сложность $O(l^2)$ $(l \to \infty)$ и емкостную сложность $O(l)$ $(l \to \infty)$.

Действительно, при первом появлении блока информации C выберем в качестве начального условия упорядоченную пару, состоящую из разбиения

$$\pi(C) = \{\overline{1,\ldots,\alpha_{j_1}}, \overline{\alpha_{j_1}+1,\ldots,\alpha_{j_1}+\alpha_{j_2}}, \ldots, \overline{\alpha_{j_1}+\alpha_{j_2}+\ldots+\alpha_{j_{h-1}}+1,\ldots,l}\}$$

и подстановки $12\ldots(l-1)l$. При r-м $(r \geq 2)$ появлении блока информации C применяем к разбиению $\pi(C)$, построенному на $(r-1)$-м шаге, элемент $next(\nu_1\nu_2\ldots\nu_k)$, полученный в результате применения процедуры *NEXT* к подстановке $\nu_1\nu_2\ldots\nu_k$, построенной на $(r-1)$-м шаге.

Рассмотрим теперь вторую операцию.

Номер подстановки $\nu_1\nu_2\ldots\nu_k$ может быть вычислен с емкостной сложностью

$$V = O(k) \quad (k \to \infty)$$

с помощью следующей процедуры.

Procedure $SBSTTN\_NMBR(\nu_1\nu_2\ldots\nu_k)$

begin
$nmbr := 0$, $h := k$
LABEL1: **if** $h = 1$
then $nmbr := nmbr + 1$ **and** HALT
else go to LABEL2
end_if
LABEL2: **do** $j = 1,\ldots,h-1$
if $\nu_{j+1} > \nu_1$
then $\mu_j := \nu_{j+1} - 1$
else $\mu_j := \nu_{j+1}$
end_if
end_do
$nmbr := (\nu_1 - 1)\cdot(h-1)!$, $h := h-1$
do $j = 1,\ldots,h$
$\nu_j := \mu_j$
end_do
go to LABEL1
end_begin

Ясно, что подстановка

$$v_1 v_2 \ldots v_k ,$$

номер которой равен $nmbr$, восстанавливается с емкостной сложностью

$$V = O(k) \quad (k \to \infty)$$

с помощью следующей процедуры

Procedure $PRMTTN(nmbr)$

begin

$prmttn \coloneqq 12\ldots(k-1)k$

do $j = 1,\ldots, mnbr - 1$

$prmttn \coloneqq NEXT(prmttn)$

end_do

end_begin

Однако следует отметить, что временная сложность процедуры $PRMTTN$ равна

$$T = O(k!) \quad (k \to \infty),$$

что существенно замедляет процесс расшифровки при росте длины l блока информации C.

Избежать такого замедления процесса расшифровки можно следующим образом.

Во-первых, фиксируется приемлемая длина блока информации C, что является стандартным приемом, применяемым при построении блочных шифров.

Во-вторых, строится таблица, в которой для фиксированного значения $h \in \mathbf{N}$ вычислены подстановки с номерами

$$i \cdot h^{-1} \cdot k! \quad (i = 1,2,\ldots, h-1).$$

Проведенный выше анализ механизма управления секретными сеансовыми ключами, основанного на операциях генерации следующей подстановки и вычислении номера заданной подстановки, показывает, что наиболее сложными (по затратам времени) являются фрагменты, связанные с применением именно второй операции.

Основная причина этого состоит во внутренней сложности связей между лексикографическим порядком и согласованной с ним нумерацией.

Отметим, что некоторое (хотя и незначительное) сокращение объема вычислений можно обеспечить за счет использования дополнительной информации (четность/нечетность перестановки, число инверсий и т.д.).

Предложенный шифр реализован программой на языке C++.

Интерфейс представляет собой диалоговое окно.

Пользователь выбирает один из двух режимов (шифрование или расшифровку) и задает пути к трем файлам, предназначенным для записи ис-

ходной информации, для записи ключа и для записи преобразованной информации.

С целью оценки времени работы программы был проведен вычислительный эксперимент с текстами объемом до 1Кб.

Результаты эксперимента представлены в таблице 3.1.

Таблица 3.1.

Число символов в исходном тексте	Время шифрования	Время расшифровки
1-9	до 1 сек.	2 сек.
10-18	до 1 сек.	3 сек.
19-27	до 1 сек.	4 сек.
28-36	до 1 сек.	5 сек.
82-90	1 сек.	12 сек.
892-900	2 сек.	120 сек.

Анализ результатов вычислительного эксперимента дает основания предположить, что время расшифровки растет экспоненциально с увеличением количества символов в исходном тексте.

Эту ситуацию можно устранить с помощью следующих двух подходов:

1) подстановки заранее табулируются в явном виде (а не генерируются программными средствами) и применяются быстрые алгоритмы поиска;

2) исходный текст разбивается на блоки не очень большой длины.

При реализации и тестировании 1-го подхода было установлено, что время расшифровки приблизительно равно времени шифрования. Однако в этом случае наблюдается резкий рост времени шифрования, если объем блока информации превосходит 3Кб.

Поэтому целесообразно использовать комбинацию 1-го и 2-го подходов, что дает возможность обеспечить не только необходимую стойкость шифра, но и высокую скорость процессов шифрования и расшифровки.

В заключение отметим, что предложенный класс шифров, основанных на методе записи информации на циклических аттракторах одномерных кусочно-линейных отображений, осуществляет разрушение частот присущих исходному языку сообщения, что дает возможность строить шифры, вычислительно стойкие к частотному анализу. Построенные механизмы управления секретными сеансовыми ключами основаны на операциях с элементами симметрической группы и дают возможность обеспечить свойство «быть нестационарным шифром».

В совокупности все это приводит к тому, что единственным методом анализа шифртекста является поиск с возвращением [141].

Таким образом, выделен нетривиальный класс вычислительно стойких нестационарных шифров, основанных на циклических аттракторах кусочно-линейных отображений.

3.3. Многопользовательский доступ к каналу связи, основанный на циклических аттракторах кусочно-линейных отображений.

Одной из классических задач теории телекоммуникационных сетей и сетей связи является задача организации эффективного многопользовательского доступа к каналу связи.

Усилия, направленные на решение этой задачи, привели к выработке следующих двух основных подходов.

Первый подход основан на распределении между пользователями времени доступа к каналу связи (стандарт типа TDMA).

Второй подход основан на распределении между пользователями частот в качестве внутреннего алфавита пользователя в канале связи (стандарт типа FDMA).

При этом ясно, что эффективное использование канала связи, ориентированное на пользователя, и обеспечивающее некоторый уровень защиты передаваемой информации от пассивных внешних атак (кроме применения методов непосредственного шифрования и обычного физического экранирования канала), может быть достигнуто только за счет решения многокритериальной задачи, формулируемой в терминах комбинации указанных выше подходов.

Переход к цифровой связи естественно трансформировал распределение частот в распределение кодов между пользователями (стандарт типа CDMA). Соответственно изменилась и задача управления доступом пользователей к каналу связи.

Более того, как формулировка, так и метод решения этой задачи существенно зависит от механизма генерации кодов и их распределения между пользователями.

В последнее время уделяется значительное внимание разработке методов организации многопользовательского доступа к каналу связи, основанных на использовании свойств детерминированного хаоса динамических систем (см., напр., [294]).

Схематически организация доступа абонентов к многопользовательскому каналу связи, основанная на использовании хаотического сигнала, изображена на рис. 3.8.

Можно выделить следующие два подхода к применению детерминированного хаоса динамических систем в процессе передачи информации по каналу связи.

Первый подход основан на том, что хаотические сигналы применяются только в роли эффективного гибкого средства формирования шума.

Существенной характеристикой такого подхода является то обстоятельство, что не уделяется никакого внимания вопросам, связанным с исследованием многообразия хаотических режимов, с гибким управлением их динамикой, самосинхронизацией и конфиденциальностью передаваемой информации.

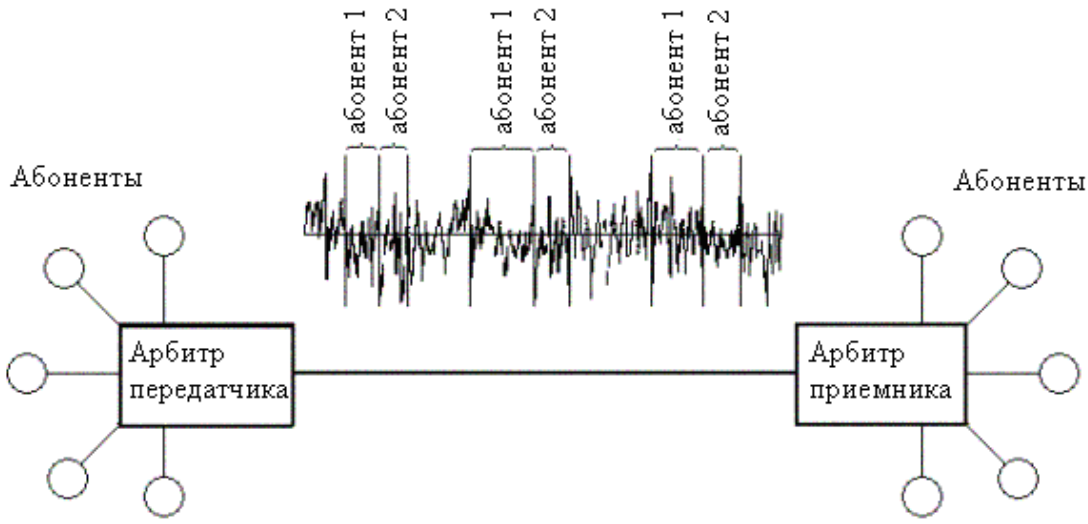


Рис. 3.8. Передача информации по многопользовательскому каналу связи, основанная на использовании хаотического сигнала.

Второй подход (см., напр., [294]), основанный на применении детерминированного хаоса динамических систем, предназначен именно для организации эффективного распределения доступа пользователей к каналу связи и состоит в следующем.

Вначале составляется каталог нестабильных периодических орбит различных периодов (иными словами, бифуркационная диаграмма) отображения Эно. Некоторые из таких орбит выбираются в качестве внутренних алфавитов пользователей каналом связи. В качестве критерия отбора орбит был выбран критерий минимизации общей корреляционной связи между орбитами.

Отметим, что обоснование целесообразности выбора именно такого критерия отбора орбит отсутствует.

Управление процессом передачи информации по каналу связи состоит в следующем.

Этап 1. Осуществляется переход системы от хаотического движения по фазовому пространству к выбранной нестабильной периодической орбите.

Этап 2. Осуществляется поддержка движения системы в течение некоторого времени в окрестности этой орбиты.

Этап 3. Осуществляется обратный переход системы к хаотическому состоянию.

Существенной характеристикой изложенного выше подхода является то обстоятельство, что арбитр приемника обеспечивает потенциальный доступ всей передаваемой информации каждому пользователю (рис.3.9).

Задача каждого из пользователей как раз и состоит в том, чтобы из потока передаваемых сигналов выделить те и только те сигналы, которые принадлежат его внутреннему алфавиту.

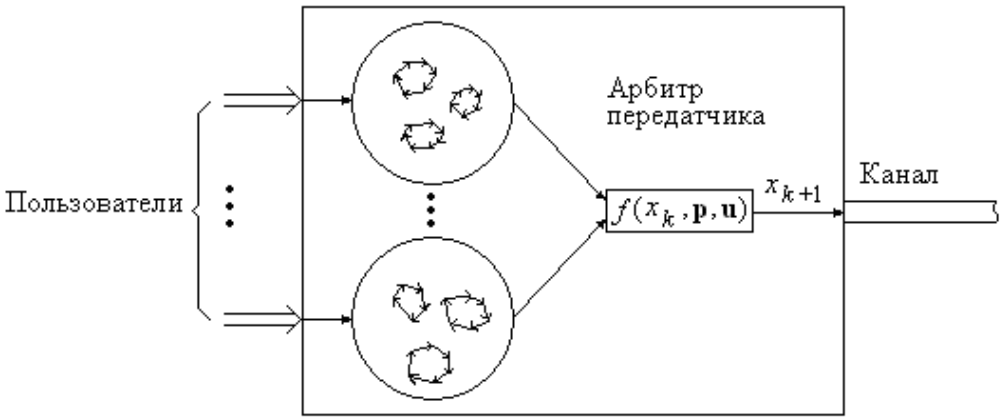


Рис. 3.9. Схема подключения арбитра передатчика.

Отметим, что решение этой задачи состоит, по своей сути, в выборе такой меры ρ и такого порога ε $(\varepsilon > 0)$, чтобы для любой пары (C_1, C_2) выделяемых пользователям алфавитов было выполнено следующее условие

$$(\forall c_1 \in C_1)(\forall c_2 \in C_2)(\rho(c_1, c_2) > \varepsilon). \qquad (3.3)$$

Рассмотренный выше подход дает возможность построить некоторое распределение кодов между потенциально неограниченным числом пользователей.

Однако остается открытым вопрос о методах оценки качества такого распределения кодов. Неясно также, каким образом можно сравнивать уровень защиты информации с уровнем защиты информации, обеспечиваемым методами классической криптографии.

Последняя задача приобретает особую актуальность в связи с концепцией хаотического процессора, развитой в [10].

Кроме того, при использовании нелинейных хаотических отображений возникают проблемы, связанные с точностью вычислений траекторий в процессе эволюции соответствующих динамических систем.

Именно фактор накопления погрешностей в процессе вычисления траектории нелинейной хаотической динамической системы может привести к ошибке в выборе нестабильной периодической орбиты.

Покажем, что распределение кодов, построенное на основе кусочно-линейных отображений, рассмотренных в п.3.2, дает возможность обеспечить уровень защиты информации, сопоставимый с уровнем защиты информации, обеспечиваемым вычислительно стойкими нестационарными шифрами, основанными на перестановках.

Обозначим через S_k $(k \in \mathbf{N})$ множество всех циклических перестановок чисел, принадлежащих множеству $\{(j - 0.5) \cdot k^{-1} \mid j = 1, \ldots, k\}$.

С каждой перестановкой

$$g = (b_{i_1}, \ldots, b_{i_k}) \in S_k$$

сопоставим динамическую систему S_g, эволюция которой осуществляется в соответствии с таким кусочно-линейным одномерным отображением

$$x_{n+1} = f_g(x_n) \quad (n \in \mathbf{N}),$$

что на интервале $((j-1)\cdot k^{-1}; j\cdot k^{-1})$ $(j = 1,\ldots,k)$ отображение f_g представлено отрезком прямой линии с коэффициентом наклона s $(0 < s < 1)$, проходящей через точку $\mathbf{b}_j = (b_{i_j}, b_{i_{(j+1)(\mathrm{mod}\, n)}})$.

Положим

$$\mathbf{S}_k = \{\mathsf{S}_g \mid g \in S_k\} \quad (k \in \mathbf{N}).$$

Покажем, что множество $\mathbf{S}_k$ $(k \in \mathbf{N})$ может быть наделено структурой метрического пространства с легко вычислимой при параллельных вычислениях метрикой.

Пусть

$$H_k = \{h_r^{(k)} : \mathbf{N}_k \to \mathbf{N}_k \mid r \in \mathbf{Z}_k\} \quad (k \in \mathbf{N}),$$

где для всех $r \in \mathbf{Z}_k$ и $x \in \mathbf{N}_k$

$$h_r^{(k)}(x) = (x + r) \,(\mathrm{mod}\, k).$$

Определим отображение

$$\rho_k : \mathbf{S}_k \times \mathbf{S}_k \to \mathbf{R}_+ \quad (k \in \mathbf{N})$$

следующим образом: для любых динамических систем $\mathsf{S}_{g_1}, \mathsf{S}_{g_2} \in \mathbf{S}_k$, если

$$g_j = (b_{i_1}^{(j)}, \ldots, b_{i_k}^{(j)}) \in S_k \quad (j = 1,2),$$

то

$$\rho_k(\mathsf{S}_{g_1}, \mathsf{S}_{g_2}) = \min_{r \in \mathbf{Z}_k} \sum_{l=1}^{k} | b_{i_l}^{(1)} - b_{i_{h_r(l)}}^{(2)} |. \tag{3.4}$$

Нетрудно убедиться в том, что отображение ρ_k $(k \in \mathbf{N})$ удовлетворяет аксиомам метрики.

Таким образом, $(\mathbf{S}_k, \rho_k)$ $(k \in \mathbf{N})$ представляет собой метрическое пространство.

Покажем, что при параллельных вычислениях метрика ρ_k $(k \in \mathbf{N})$ является легко-вычислимой функцией.

Рассмотрим такую двухуровневую систему $\subset (P_0, P_1, \ldots, P_{k-1}; P_k)$, содержащую $k+1$ процессор $P_0, P_1, \ldots, P_k$, что:

1) процессор P_r $(r = 0,1,\ldots,k-1)$ расположен в 1-м уровне, и вычисляет величину

$$x_r = \sum_{l=1}^{k} | b_{i_l}^{(1)} - b_{i_{h_r(l)}}^{(2)} |; \tag{3.5}$$

2) процессор P_k расположен во 2-м уровне, и вычисляет величину

$$y = \min\{x_0, x_1, \ldots, x_{k-1}\}. \tag{3.6}$$

Так как каждая из операций (3.5) и (3.6) может быть реализована с временной сложностью

$$T = O(k \cdot \log k) \quad (k \to \infty), \tag{3.7}$$

то двухуровневая система процессоров $\subset (P_0, P_1, \ldots, P_{k-1}; P_k)$ осуществляет вычисление в соответствии с формулой (3.4) с временной сложностью, определенной формулой (3.7).

Таким образом, показано, что при параллельных вычислениях метрика ρ_k $(k \in \mathbf{N})$ является легко-вычислимой функцией.

Отметим, что для метрики ρ_k $(k \in \mathbf{N})$, определенной равенством (3.4) не составляет особого труда обеспечить выполнение условия (3.3) в множестве динамических систем $\mathbf{S}_k$.

Использование множества динамических систем $\mathbf{S}_k$ $(k \in \mathbf{N})$, где параметр k определяется ожидаемым числом пользователей каналом связи, естественно приводит к схеме организации доступа к каналу связи, изображенной на рис. 3.10.

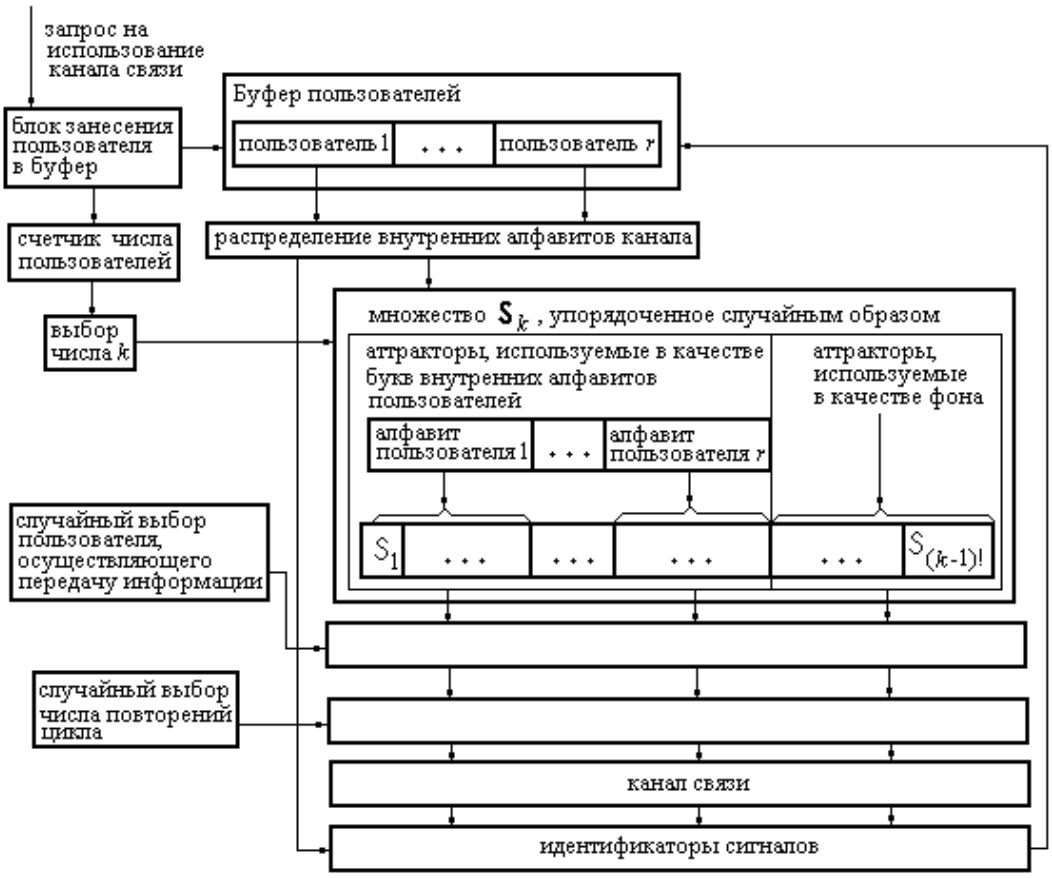


Рис. 3.10. Схема организации многопользовательского доступа к каналу связи, основанная на использовании циклических аттракторов кусочно-линейных отображений.

Подчеркнем, что именно под управлением блока занесения пользователей в буфер осуществляется связь между пользователями на уровне их внешних алфавитов.

При этом вся та часть системы управления каналом связи, которая осуществляет управление передачей информации во внутренних алфавитах канала, является для пользователей «черным ящиком».

Рассмотрим, кратко, основные проблемы, связанные с предложенной схемой организации многопользовательского доступа к каналу связи.

Сложность, связанная с определением ожидаемого числа пользователей в «час пик», может быть преодолена следующим образом.

Фиксируется некоторое число $k_1 \in \mathbf{N}$. Функционирование схемы осуществляется обычным образом на множестве динамических систем $\mathbf{S}_{k_1}$.

Как только доля аттракторов, используемых в качестве «фона», становится меньше допустимого порога, выбирается некоторое такое число $k_2 \in \mathbf{N}$, что $k_2 \neq k_1$. Вновь поступающие пользователи обслуживаются с помощью множества динамических систем $\mathbf{S}_{k_2}$ и т.д.

Так как

$$k_1 \neq k_2 \Rightarrow \mathbf{S}_{k_1} \cap \mathbf{S}_{k_2} = \varnothing,$$

то конфликты между пользователями, связанные с распределением алфавитов, невозможны в принципе.

Прием информации, передаваемой по каналу связи, осуществляется всеми пользователями одновременно. Отсюда вытекает, что величина задержки при приеме сигнала сводится к времени идентификации сигнала по принципу «свой – чужой».

Ясно, что такая идентификация сигнала осуществима за линейное время при использовании одноуровневой схемы процессоров $\subset (P_1,\ldots,P_l)$, где l – число символов алфавита, выделенных пользователю, а процессор P_i $(i=1,\ldots,l)$ предназначен для идентификации i-го символа, принадлежащего алфавиту, выделенному данному пользователю.

Сложность возникает при выборе пользователя, осуществляющего в данный промежуток времени передачу информации. Эта сложность обусловлена следующими обстоятельствами.

Во-первых, необходимо одновременно контролировать все таймеры, фиксирующие время ожидания доступа пользователей к процессу передачи информации, не допуская превышения порога ни на одном из них.

Во-вторых, необходимо варьировать длину промежутка, выделяемого для передачи информации одним пользователем.

В-третьих, необходимо контролировать объемы информации, подготовленной к передаче и помещенной в специальные буферы, чтобы не допустить их переполнения.

Таким образом, возникает необходимость многократного решения в реальном времени многопараметрической задачи теории расписаний.

Следует, однако, отметить, что именно эта особенность присуща любому последовательно организованному доступу пользователей к каналу.

Предложенная схема организации многопользовательского доступа к каналу связи с точки зрения классической криптографии эквивалентна применению циклических перестановок, возможно, различной длины.

Принципиально новые возможности, связанные с разрушением частот появления символов в сообщении, возникающие именно в процессе передачи циклических аттракторов, обеспечиваются следующими тремя типами действий:

1) вариацией числа повторений цикла;

2) сопоставлением различным пользователям попарно непересекающихся подмножеств множества $\mathbf{S}_k$ $(k \in \mathbf{N})$;

3) вариацией параметра k.

А так как число пользователей – случайная величина, то управление комбинацией перечисленных выше действий дает возможность организовать функционирование канала связи, вычислительно стойкое к любому частотному анализу.

Предложенная схема организации многопользовательского доступа к каналу связи предусматривает следующие три типа управления, связанные с переупорядочением элементов множеств.

Во-первых, это выбор упорядочения элементов множества $\mathbf{S}_k$ $(k \in \mathbf{N})$.

Число возможных вариантов такого упорядочения равно $|\mathbf{S}_k|!$.

Во-вторых, это выбор аттракторов, выделяемых конкретному пользователю при фиксированном упорядочении элементов множества $\mathbf{S}_k$ $(k \in \mathbf{N})$.

Пусть число пользователей каналом связи равно r и каждому из них выделяется l-элементный алфавит (это типичная ситуация при доступе к каналу связи). Тогда число способов распределения аттракторов между пользователями равно $(l \cdot r)!\cdot(l!)^{-r}$.

В-третьих, это выбор кодирования элементов внешнего алфавита выделенными пользователям аттракторами.

Пусть число пользователей каналом связи равно r и каждому из них выделяется l-элементный алфавит. Тогда число способов кодирования элементов внешнего алфавита при фиксации выделенных пользователям аттракторов равно $(l!)^r$.

Ясно, что независимое управление выбором перечисленных выше вариантов (например, с использованием псевдослучайных генераторов чисел) приводит к субэкспоненциальному числу ситуаций, возникающих в процессе функционирования канала связи.

Отсюда вытекает, что, фактически, выделен класс нестационарных блочных шифров, основанных на перестановках и предназначенных для организации многопользовательского доступа к каналу связи. Секретным сеансовым ключом для любого такого шифра является настройка указанных выше псевдослучайных генераторов.

3.4. Выводы.

В настоящем разделе исследована возможность применения кусочно-линейных отображений к решению модельных задач преобразования информации. Основные результаты состоят в следующем:

1. Исследована взаимосвязь между эволюцией динамических систем, представленных кусочно-линейными хаотическими отображениями, и шифрами, основанными на перестановках.

2. Построен нестационарный шифр, основанный на использовании ансамбля динамических систем, каждая из которых представлена хаотическим отображением «зуб пилы».

3. В терминах симметрической группы исследована общая схема нестационарного шифра, основанного на записи информации на кодируемых впоследствии циклических аттракторах одномерных кусочно-линейных отображений.

4. В терминах циклических аттракторов ансамбля одномерных кусочно-линейных отображений выделен класс нестационарных блочных шифров, основанных на перестановках, и предназначенных для организации многопользовательского доступа к каналу связи.

4. ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ НЕИСПРАВНОСТЕЙ В БЛОКАХ УПРАВЛЯЕМЫХ ПЕРЕСТАНОВОК И ПОДСТАНОВОК

Исследование проблемы построения скоростных блочных шифров, допускающих эффективную реализацию на программном, аппаратном или аппаратно/программном уровне, привело к математическим моделям, известным в настоящее время под именем «блок управляемых перестановок» (БУП) и «управляемая подстановочная операция» (УПО) [123]. Именно из-за возможности применения этих математических моделей при аппаратной реализации блочных шифров задача контроля (т.е. обнаружения или локализации) неисправностей в комбинационных схемах (КС), реализующих БУП или УПО, является актуальной. В настоящем разделе исследуется off-line контроль неисправностей БУП и УПО.

В п.4.1 вводятся необходимые понятия и определения. В пп.4.2-4.4 исследуется задача контроля неисправностей в базовых БУП, применяемых при построении современных скоростных блочных шифров, а именно: в матричных БУП (п.4.2), в послойных БУП (п.4.3) и в рекурсивных БУП (п.4.4). Получены оценки сложности тестов, предназначенных для обнаружения или локализации константных неисправностей, а также коротких замыканий. В п.4.5 рассматривается задача контроля неисправностей в УПО.

Материал, представленный в настоящем разделе, основан на результатах, полученных в [12,172,176,177,180,181].

4.1. Основные понятия и определения.

Стандартными операциями, используемыми при построении современных высокоскоростных блочных шифров, является перестановка бит блока информации и подстановка одних блоков вместо других, выполняемые под управлением ключевой последовательности. Анализ этих операций привел к математическим моделям, известным как, соответственно, БУП и УПО. Охарактеризуем эти математические модели. Представим вектор-функцию

$$\mathbf{f}:\mathbf{E}^n\times\mathbf{E}^m\to\mathbf{E}^l \quad (m,n,l\in\mathbf{N};\, l\geq n) \tag{4.1}$$

в виде $\mathbf{y}=\mathbf{f}(\mathbf{x},\mathbf{v})$ $(\mathbf{x}\in\mathbf{E}^n,\mathbf{v}\in\mathbf{E}^m)$. Вектор $\mathbf{x}=(x_1,\ldots,x_n)$ – информационный вектор, а вектор $\mathbf{v}=(v_1,\ldots,v_m)$ – управляющий вектор.

УПО представляет собой КС $S_{\mathbf{f}}$, реализующую вектор-функцию (4.1), удовлетворяющую следующему условию.

Условие 4.1. Для каждого $\mathbf{v}_0\in\mathbf{E}^m$ вектор-функция $\mathbf{g}_{\mathbf{v}_0}:\mathbf{E}^n\to\mathbf{E}^l$, где

$$\mathbf{g}_{\mathbf{v}_0}(\mathbf{x})=\mathbf{f}(\mathbf{x},\mathbf{v}_0) \quad (\mathbf{x}\in\mathbf{E}^n),$$

является инъекцией множества $\mathbf{E}^n$ в множество $\mathbf{E}^l$.

Так как число инъекций 2^n-элементного множества в 2^l-элементное множество, которые могут быть получены с помощью УПО $S_{\mathbf{f}}$, не превосходит 2^m, то при построении любого семейства УПО естественным является ограничение

$$2^m\leq\frac{(2^l)!}{(2^l-2^n)!}. \tag{4.2}$$

Положив $l = n$ в (4.1), получим

$$\mathbf{f} : \mathbf{E}^n \times \mathbf{E}^m \to \mathbf{E}^n \quad (m, n \in \mathbf{N}). \tag{4.3}$$

БУП представляет собой КС $S_{\mathbf{f}}$, реализующую вектор-функцию (4.3), удовлетворяющую следующим двум условиям.

Условие 4.2. Для любого фиксированного значения $\mathbf{v}_0 \in \mathbf{E}^m$ вектор-функция $\mathbf{g}_{\mathbf{v}_0} : \mathbf{E}^n \to \mathbf{E}^n$, где

$$\mathbf{g}_{\mathbf{v}_0}(\mathbf{x}) = \mathbf{f}(\mathbf{x}, \mathbf{v}_0) \quad (\mathbf{x} \in \mathbf{E}^n),$$

представляет собой перестановку компонент информационного вектора.

Условие 4.3. Если $\mathbf{v}_0 \neq \mathbf{v}_1$ $(\mathbf{v}_0, \mathbf{v}_1 \in \mathbf{E}^m)$, то $g_{\mathbf{v}_0}$ и $g_{\mathbf{v}_1}$ представляют собой различные перестановки компонент информационного вектора.

Число различных перестановок компонент информационного вектора, которые могут быть получены с помощью БУП $S_{\mathbf{f}}$, не превосходит 2^m. Поэтому при построении БУП естественно считать, что

$$2^m \leq n!, \tag{4.4}$$

т.е.

$$m \leq \lceil \log n! \rceil. \tag{4.5}$$

КС, реализующие БУП и УПО, схематически изображены на рис. 4.1.

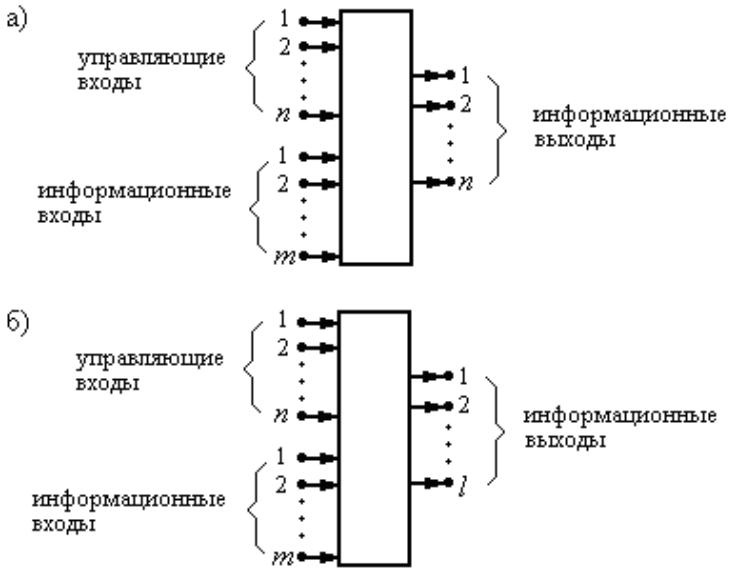


Рис. 4.1. КС $S_{\mathbf{f}}$, реализующая: а) БУП; б) УПО.

В [123] дан систематический анализ БУП и УПО. Однако задачи обнаружения или локализации неисправностей КС $S_{\mathbf{f}}$ (как и других схем, используемых в процессе построения высокоскоростных блочных шифров) остаются вне внимания криптографии. Хотя эти задачи могут быть решены на основе стандартных методов технической диагностики [131], при таком

подходе не учитываются существенные характеристики КС $S_{\mathbf{f}}$ как на функциональном уровне (такие, как инъективное преобразование посредством БУП и БУО информационных векторов при фиксированном управляющем векторе или равенство $wt(\mathbf{x}) = wt(\mathbf{y})$ для БУП), так и на структурном уровне. Как следствие, построенные таким образом тесты, оказываются намного сложнее, чем оптимальные тесты. Поэтому задача построения эффективных тестов для off-line контроля неисправностей для основных типов БУП и БУО является актуальной.

Введем соответствующие понятия и определения.

Под неисправностью КС S будем понимать одиночную константную неисправность любой ножки любого входящего в нее элемента, а также короткое замыкание (КЗ) между любыми двумя соседними ножками любого ее элемента. Для определенности считаем, что синтез КС S осуществляется в позитивной логике. Сложность $\mu(C)$ любого элемента C КС S определим как общее число ножек элемента C, а сложность КС S определим равенством

$$\mu(S) = \sum \mu(C),$$

где сумма берется по всем элементам C КС S.

Тест для КС S – это матрица, строки которой – вход-выходные пары эталона, т.е. исправной схемы. Пусть $\mathbf{A}_{dtct}$ и $\mathbf{A}_{lclz}$ – минимальные по длине (т.е. по числу строк) тесты, предназначенные для, соответственно, обнаружения и локализации неисправностей КС S. Сложность обнаружения или локализации неисправностей КС S определим равенством

$$\mu_a(S) = \alpha_a \cdot \beta_a \quad (a \in \{dtct, lclz\}),$$

где α_a и β_a есть число, соответственно, строк и столбцов матрицы $\mathbf{A}_a$.

4.2. Анализ матричных БУП.

Матричный БУП $\mathbf{M}_{n,m}$ содержит дешифратор D_m и $2^m - 2$ элемента P_n. Дешифратор D_m реализует такое отображение $\mathbf{g}: \mathbf{E}^m \to \mathbf{E}^{2^m}$, что

$$\mathbf{g}(v_1, \ldots, v_m) = (u_0, u_1, \ldots, u_{2^m-1}),$$

где

$$u_i = \begin{cases} 1, \ \textit{если} \ i = \sum_{j=1}^{m} 2^{j-1} \cdot v_j \\ 0, \ \textit{иначе} \end{cases} \quad (i = 0,1,\ldots,2^m - 1).$$

Дешифратор D_m предназначен для активации элементов P_n.

Каждый элемент P_n реализует такую вектор-функцию $\mathbf{h}_{P_n}: \mathbf{E}^n \times \mathbf{E} \to \mathbf{E}^n$, что $\mathbf{h}_{P_n}(\mathbf{x}, 1)$ – перестановка компонент информационного вектора $\mathbf{x}$, отличная от тождественной перестановки. При этом эти перестановки отличаются друг от друга для различных элементов P_n.

Пусть $P_n^{(1)}$ – такой элемент P_n, что $\mathbf{h}_{P_n}(\mathbf{x},0)=\mathbf{x}$ для всех $\mathbf{x}\in\mathbf{E}^n$, а $P_n^{(2)}$ – такой элемент P_n, что $\mathbf{h}_{P_n}(\mathbf{x},0)=\mathbf{0}$ для всех $\mathbf{x}\in\mathbf{E}^n$.

Обозначим через $\mathbf{M}_{n,m}^{(1)}$ матричный БУП $\mathbf{M}_{n,m}$, содержащий элемент D_m и 2^m-2 элемента $P_n^{(1)}$, а через $\mathbf{M}_{n,m}^{(2)}$ – матричный БУП $\mathbf{M}_{n,m}$, содержащий элемент D_m и 2^m-2 элемента $P_n^{(2)}$. Эти математические модели схематически представлены на рис. 4.2.

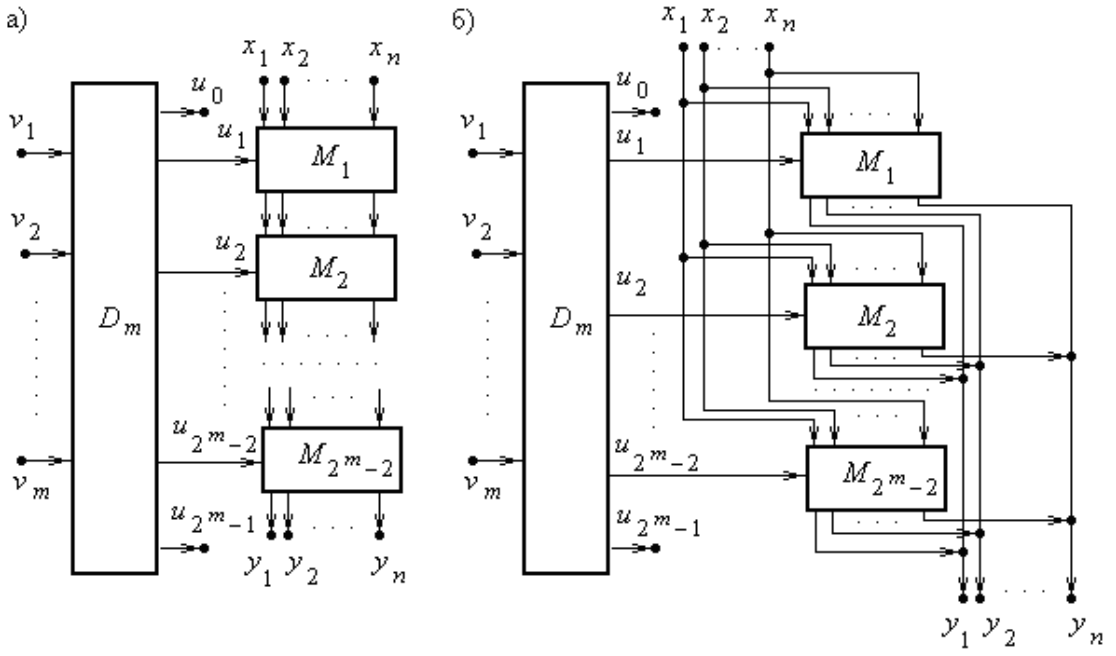


Рис. 4.2. Матричный БУП $\mathbf{M}_{n,m}$: а) модель $\mathbf{M}_{n,m}^{(1)}$ (M_i $(i=1,\ldots,2^m-2)$ – элементы $P_n^{(1)}$); б) модель $\mathbf{M}_{n,m}^{(2)}$ (M_i $(i=1,\ldots,2^m-2)$ – элементы $P_n^{(2)}$).

Отметим, что выходы u_0 и u_{2^m-1} дешифратора D_m – это контрольные точки, предназначенные для off-line контроля БУП $\mathbf{M}_{n,m}\in\{\mathbf{M}_{n,m}^{(1)},\mathbf{M}_{n,m}^{(2)}\}$.

Так как $\mu(D_m)=m+2^m$ и $\mu(P_n)=2\cdot n+1$, то

$$\mu(\mathbf{M}_{n,m})=m+2^m+(2\cdot n+1)\cdot(2^m-2)=$$

$$=m-2\cdot(2\cdot n+1)+(n+1)\cdot 2^{m+1}\quad(\mathbf{M}_{n,m}\in\{\mathbf{M}_{n,m}^{(1)},\mathbf{M}_{n,m}^{(2)}\}). \qquad (4.8)$$

Теорема 4.1. Для всех $m,n\in\mathbf{N}$ $(m\le\lceil\log n!\rceil)$ истинны неравенства

$$\mu_{dtct}(\mathbf{M}_{n,m}^{(1)})\le(m+2\cdot n+2)\cdot(2^m+\lceil 0.5\cdot m\rceil+1), \qquad (4.9)$$

$$\mu_{lclz}(\mathbf{M}_{n,m}^{(1)})\le(m+2\cdot n+2)\cdot(2^m\cdot(n+1)+\lceil 0.5\cdot m\rceil-2\cdot n+1), \qquad (4.10)$$

$$\mu_{a}(\mathbf{M}_{n,m}^{(2)})\le(m+2\cdot n+2)\cdot(2^m\cdot(n+1)+\lceil 0.5\cdot m\rceil-2\cdot n+1)\ , \qquad (4.11)$$

где $a\in\{dtct,lclz\}$.

Доказательство. Рассмотрим БУП $\mathbf{M}_{n,m}^{(1)}$.

Векторы $(\mathbf{x}_1,\mathbf{0})$ и $(\mathbf{x}_2,\mathbf{1})$, где

$$\mathbf{x}_1 = \begin{cases} (1,0,1,0,\ldots,1,0), \text{ если } n-\text{четное число} \\ (1,0,1,0,\ldots,1,0,1), \text{ если } n-\text{нечетное число} \end{cases}$$

и

$$\mathbf{x}_2 = \begin{cases} (0,1,0,1,\ldots,0,1), \text{ если } n-\text{четное число} \\ (0,1,0,1,\ldots,0,1,0), \text{ если } n-\text{нечетное число} \end{cases}$$

дают возможность:

1) обнаружить любую константную неисправность на входных ножках дешифратора D_m;

2) обнаружить (более того, локализировать) любую константную неисправность на выходных ножках u_0 и u_{2^m-1} дешифратора D_m;

3) обнаружить любую неисправность на информационных ножках любого элемента M_i $(i=1,\ldots,2^m-2)$.

Входные векторы $(\mathbf{x}_3,\tilde{\mathbf{e}}_i)$ $(i=1,\ldots,\lceil 0.5\cdot m\rceil)$, где $\mathbf{x}_3$ – произвольный информационный вектор, а $\tilde{\mathbf{e}}_i = (\underbrace{1,\ldots,1}_{2\cdot i-1 \text{ раз}},0,\underbrace{1,\ldots,1}_{m-2\cdot i \text{ раз}})$ $(i=1,\ldots,\lceil 0.5\cdot m\rceil)$ дают возможность:

1) обнаружить (более того, локализировать) КЗ между любыми соседними входными ножками дешифратора D_m;

2) локализировать любую константную неисправность на входных ножках дешифратора D_m.

Векторы $(\mathbf{x}_4,\mathbf{v}_1)$ и $(\mathbf{x}_4,\mathbf{v}_2)$, где $\mathbf{x}_4$ – произвольный информационный вектор, а $\mathbf{v}_1=(1,0,\ldots,0)$ и $\mathbf{v}_2=(0,1,\ldots,1)$ дают возможность:

1) обнаружить (более того, локализировать) КЗ между выходными ножками u_0 и u_1 дешифратора D_m;

2) обнаружить (более того, локализировать) КЗ между выходными ножками u_{2^m-2} и u_{2^m-1} дешифратора D_m.

Векторы $(\mathbf{x}_5^{(i)},\mathbf{v}_3^{(i)})$ $(i=1,\ldots,2^m-3)$, где $\mathbf{v}_3^{(i)}=(v_1^{(i)},\ldots,v_m^{(i)})$ $(i=1,\ldots,2^m-3)$ – такой вектор, что $\sum_{j=1}^{m} 2^{j-1}\cdot v_j^{(i)} = i$ $(i=1,\ldots,2^m-3)$, а $\mathbf{x}_5^{(i)}$ $(i=1,\ldots,2^m-3)$ – такой вектор, что $\mathbf{h}_{M_{i+1}}(\mathbf{h}_{M_i}(\mathbf{x}_5^{(i)},1),1) \neq \mathbf{h}_{M_i}(\mathbf{x}_5^{(i)},1)$ $(i=1,\ldots,2^m-3)$, дают возможность:

1) обнаружить (более того, локализировать) КЗ между любыми соседними выходными ножками u_i $(i=1,\ldots,2^m-3)$ и u_{i+1} дешифратора D_m;

2) обнаружить (более того, локализировать) любую константную неисправность на ножках дешифратора D_m.

Итак,

$$\mu_{dtct}(\mathbf{M}_{n,m}^{(1)}) \le (m + 2\cdot n + 2)\cdot(2 + \lceil 0.5\cdot m\rceil + 2 + 2^m - 3) =$$
$$= (m + 2\cdot n + 2)\cdot(2^m + \lceil 0.5\cdot m\rceil + 1),$$

что и требовалось показать.

Для локализации неисправностей БУП $\mathbf{M}_{n,m}^{(1)}$ достаточно к построенному выше тесту добавить входную последовательность

$$\mathbf{w} = \mathbf{z}_1 \ldots \mathbf{z}_{2^m-2}, \tag{4.12}$$

где $\mathbf{z}_i = (\mathbf{e}_1, \mathbf{v}_i)\ldots(\mathbf{e}_n, \mathbf{v}_i)$ $(i = 1,\ldots,2^m - 2)$, $\mathbf{e}_j = (\underbrace{0,\ldots,0}_{j-1\ раз},1,\underbrace{0,\ldots,0}_{n-j\ раз})$ $(j = 1,\ldots,n)$, а $\mathbf{v}_i = (v_1^{(i)},\ldots,v_m^{(i)})$ $(i = 1,\ldots,2^m - 2)$ – такой вектор, что $\sum_{j=1}^{m} 2^{j-1}\cdot v_j^{(i)} = i$.

Итак,

$$\mu_{lclz}(\mathbf{M}_{n,m}^{(1)}) \le \mu_{dtct}(\mathbf{M}_{n,m}^{(1)}) + (m + 2\cdot n + 2)\cdot n\cdot(2^m - 2) \le$$
$$\le (m + 2\cdot n + 2)\cdot(2^m + \lceil 0.5\cdot m\rceil + 1) + (m + 2\cdot n + 2)\cdot n\cdot(2^m - 2) =$$
$$= (m + 2\cdot n + 2)\cdot(2^m\cdot(n+1) + \lceil 0.5\cdot m\rceil - 2\cdot n + 1),$$

что и требовалось показать.

Рассмотрим БУП $\mathbf{M}_{n,m}^{(2)}$.

Входные векторы $(\mathbf{x}_6, \mathbf{0})$ и $(\mathbf{x}_7, \mathbf{1})$, где $\mathbf{x}_6$ и $\mathbf{x}_7$ – произвольные информационные векторы, дают возможность:

1) обнаружить любую константную неисправность на входных ножках дешифратора D_m;

2) обнаружить (и, следовательно, локализировать) любую константную неисправность на выходных ножках u_0 и u_{2^m-1} дешифратора D_m;

3) обнаружить любую константную неисправность $\equiv 1$ на выходных информационных ножках любого элемента M_i $(i = 1,\ldots,2^m - 2)$.

Построенные выше векторы $(\mathbf{x}_3, \tilde{\mathbf{e}}_i)$ $(i = 1,\ldots,\lceil 0.5\cdot m\rceil)$ дают возможность:

1) обнаружить (и, следовательно, локализировать) КЗ между любыми соседними входными ножками дешифратора D_m;

2) локализировать любую константную неисправность на входных ножках дешифратора D_m.

Построенные выше векторы $(\mathbf{x}_4, \mathbf{v}_1)$ и $(\mathbf{x}_4, \mathbf{v}_2)$ дают возможность:

1) обнаружить (и, следовательно, локализировать) КЗ между соседними выходными ножками u_0 и u_1 дешифратора D_m;

2) обнаружить (и, следовательно, локализировать) КЗ между соседними выходными ножками u_{2^m-2} и u_{2^m-1} дешифратора D_m.

Построенные входные векторы $(\mathbf{x}_5^{(i)}, \mathbf{v}_3^{(i)})$ $(i = 1,\ldots,2^m - 3)$ дают возможность:

1) обнаружить (и, следовательно, локализировать) КЗ между любыми соседними выходными ножками u_i $(i = 1,\ldots,2^m - 3)$ и u_{i+1} дешифратора D_m;

2) обнаружить (и, следовательно, локализировать) любую константную неисправность на ножках дешифратора D_m.

Для обнаружения (а, следовательно, локализации) любых неисправностей информационных ножек элементов M_i $(i = 1,\ldots,2^m - 2)$ достаточно теперь подать входную последовательность (4.12).

Таким образом, неравенства (4.11) истинны.

Теорема доказана.

Пусть

$$2^m = O(n!) \quad (n \to \infty), \tag{4.13}$$

т.е.

$$m = O(n \cdot \log n) \quad (n \to \infty). \tag{4.14}$$

Из (4.8) вытекает, что при выполнении условия (4.13)

$$\mu(\mathbf{M}_{n,m}) = O(n \cdot n!) \quad (n \to \infty) \quad (\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}), \tag{4.15}$$

асимптотическая оценка правой части неравенства (4.9) равна

$$O((n \cdot n!) \cdot \log n) \quad (n \to \infty), \tag{4.16}$$

а асимптотическая оценка правой части неравенств (4.10) и (4.11) равна

$$O((n \cdot n!) \cdot n \cdot \log n) \quad (n \to \infty). \tag{4.17}$$

Из (4.15)-(4.17) вытекает, что истинно

Утверждение 4.1. Если $2^m = O(n!)$ $(n \to \infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$ по отношению к асимптотической сложности самой БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$ не превосходит $O(\log n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$ по отношению к асимптотической сложности самой БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$ не превосходит $O(n \cdot \log n)$ $(n \to \infty)$.

Таким образом, асимптотическая сложность контроля неисправностей БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$ незначительно отличается от асимптотической сложности самой БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}_{n,m}^{(1)}, \mathbf{M}_{n,m}^{(2)}\}$.

Сложность контроля матричного БУП во многом определяется наличием дешифратора. Поэтому естественно перейти к БУП, который не содержит дешифратор. На рис. 4.3 изображен БУП $\mathbf{S}_{n,m}$, где ключевой поток подается непосредственно на управляющие входы $v_1,\ldots,v_m$ элементов $P_n^{(1)}$.

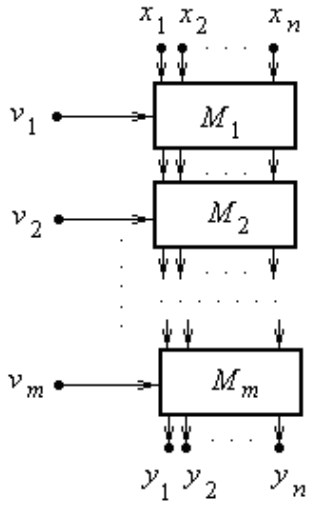


Рис.4.3. БУП $\mathbf{S}_{n,m}$ ($M_i\,(i=1,\ldots,m)$ – элементы $P_n^{(1)}$).

Так как $\mu(P_n)=2\cdot n+1$, то

$$\mu(\mathbf{S}_{n,m})=m\cdot(2\cdot n+1). \tag{4.18}$$

Отметим, что БУП $\mathbf{S}_{n,m}$ реализует всевозможные суперпозиции

$$\mathbf{h}_{M_m}^{v_m}\circ\ldots\circ\mathbf{h}_{M_1}^{v_1}, \tag{4.19}$$

где $\mathbf{h}_{M_i}^1$ $(i=1,\ldots,m)$ – перестановка бит информационного вектора, реализуемая элементом M_i $(i=1,\ldots,m)$ при значении 1 управляющего символа v_i, а $\mathbf{h}_{M_i}^0$ $(i=1,\ldots,m)$ – тождественная перестановка.

Пусть $n=k\cdot m$ $(k\geq 2, m\geq 2)$, а $\pi=\{B_1,\ldots,B_m\}$ – такое разбиение множества $\mathbf{N}_n$, что $B_i=\{i+j\cdot m \mid j=0,1,\ldots,k-1\}$ $(i=1,\ldots,m)$.

Если $\mathbf{h}_{M_i}^1$ $(i=1,\ldots,m)$ представляет собой циклическую перестановку тех бит информационного вектора, номера которых принадлежат множеству B_i, а все те биты, номера которых принадлежат множеству $\mathbf{N}_n\setminus B_i$, оставляет на месте, то все суперпозиции (4.19) являются попарно различными. Это означает, что построенный БУП $\mathbf{S}_{n,m}$ реализует $2^{n\cdot k^{-1}}$ различных перестановок бит информационно вектора.

Теорема 4.2. Для всех $m,n\in\mathbf{N}$ $(m\leq\lceil\log n!\rceil)$ истинны неравенства

$$\mu_{dtct}(\mathbf{S}_{n,m})\leq 2\cdot n\cdot(2\cdot n+m) \tag{4.20}$$

и

$$\mu_{dtct}(\mathbf{S}_{n,m})\leq(2\cdot n+m)\cdot(2\cdot n+m+n\cdot m). \tag{4.21}$$

Доказательство. Для обнаружения неисправностей на ножках любого элемента КС $\mathbf{S}_{n,m}$ достаточно подать входную последовательность

$$(\mathbf{e}_1,\mathbf{0})\ldots(\mathbf{e}_n,\mathbf{0})(\mathbf{e}_1,\mathbf{1})\ldots(\mathbf{e}_n,\mathbf{1}),$$

где $\mathbf{e}_i = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{n-i\ раз})$ $(i=1,\ldots,n)$, откуда и вытекает, что неравенство (4.20) истинно.

Векторы $(\mathbf{x}_3^{(i)},\mathbf{e}_i)$ $(i=1,\ldots,m)$, где $\mathbf{e}_i = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{m-i\ раз})$ $(i=1,\ldots,m)$, а $\mathbf{x}_3^{(i)}$ $(i=1,\ldots,m)$ – такие информационные векторы, что

$$\mathbf{h}_{M_1}(\mathbf{x}_3^{(1)},1) \neq \mathbf{x}_3^{(1)},$$

$$\mathbf{h}_{M_i}(\mathbf{h}_{M_{i-1}}(\mathbf{x}_3^{(i)},1),1) \neq \mathbf{h}_{M_{i-1}}(\mathbf{x}_3^{(i)},1) \quad (i=2,\ldots,m-1)$$

и

$$\mathbf{h}_{M_m}(\mathbf{x}_3^{(m)},1) \neq \mathbf{x}_3^{(m)}$$

дают возможность локализировать любую неисправность на управляющей ножке любого элемента M_i $(i=1,\ldots,m)$.

Для локализации неисправностей на информационных ножках БУП $\mathbf{S}_{n,m}$ достаточно к построенному выше тесту добавить такую входную последовательность $\mathbf{w} = \mathbf{z}_1\ldots\mathbf{z}_m$, что

$$\mathbf{z}_i = (\tilde{\mathbf{e}}_1,\mathbf{e}_i)\ldots(\tilde{\mathbf{e}}_n,\mathbf{e}_i) \quad (i=1,\ldots,m),$$

где $\mathbf{e}_i = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{m-i\ раз})$ $(i=1,\ldots,m)$ и $\tilde{\mathbf{e}}_j = (\underbrace{0,\ldots,0}_{j-1\ раз},1,\underbrace{0,\ldots,0}_{n-j\ раз})$ $(i=1,\ldots,n)$.

Следовательно,

$$\mu_{lclz}(\mathbf{S}_{n,m}) \leq \mu_{dtct}(\mathbf{S}_{n,m}) + (2\cdot n+m)\cdot(m+n\cdot m) \leq$$
$$\leq 2\cdot n\cdot(2\cdot n+m)+(2\cdot n+m)(m+n\cdot m) =$$
$$= (2\cdot n+m)\cdot(2\cdot n+m+n\cdot m),$$

т.е. неравенство (4.21) истинно.

Теорема доказана.

Пусть выполнено условие (4.14). Из (4.18) вытекает, что

$$\mu(\mathbf{S}_{n,m}) = O(n^2\cdot\log n) \quad (n\to\infty), \tag{4.22}$$

асимптотическая оценка правой части неравенства (4.20) равна

$$O((n^2\cdot\log n)\cdot\log n) \quad (n\to\infty), \tag{4.23}$$

а асимптотическая оценка правой части неравенства (4.21)

$$O((n^2\cdot\log n)\cdot n\cdot\log n) \quad (n\to\infty), \tag{4.24}$$

Из (4.22)-(4.24) вытекает, что истинно

Утверждение 4.2. Если $m = O(n\cdot\log n)$ $(n\to\infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{S}_{n,m}$ по отношению к асимптотической сложности самой БУП $\mathbf{S}_{n,m}$ не превосходит величины $O(\log n)$ $(n\to\infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{S}_{n,m}$ по отношению к асимптотической сложности самого БУП $\mathbf{S}_{n,m}$ не превосходит величины $O(n \cdot \log n)$ $(n \to \infty)$.

Итак, асимптотическая сложность контроля неисправностей БУП $\mathbf{S}_{n,m}$ не превосходит квадрат асимптотической сложности самого БУП $\mathbf{S}_{n,m}$.

4.3. Анализ послойных БУП.

Послойный БУП $\mathbf{P}_{n,m}$, где n – четное число, состоит из l элементов $\pi^{(1)},\ldots,\pi^{(l)}$ и m $(m = 0.5 \cdot n \cdot (l-1))$ элементов $\mathbf{P}_{2,1}$ (рис. 4.4).

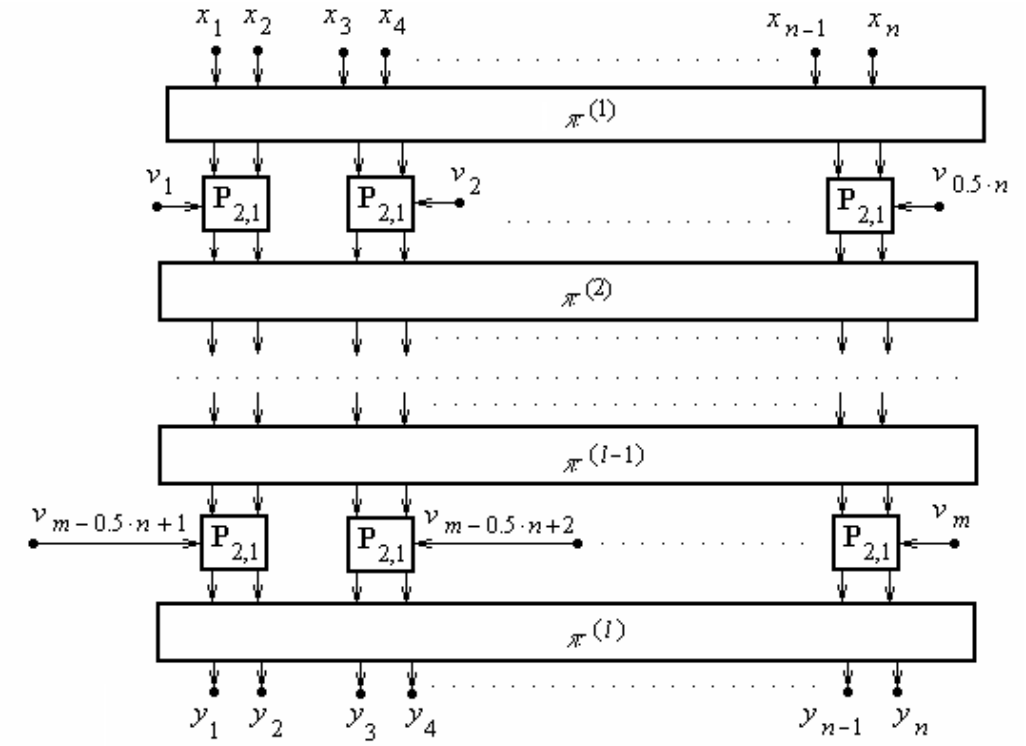


Рис. 4.4. Послойный БУП $\mathbf{P}_{n,m}$ (n – четное число).

Элемент π_i $(i = 1,\ldots,l)$ реализует перестановку $\mathbf{h}_i$ бит двоичного вектора, поступающего на его вход, а элемент $\mathbf{P}_{2,1}$ – такое отображение $\mathbf{g}: \mathbf{E}^2 \times \mathbf{E} \to \mathbf{E}^2$, что $\mathbf{g}(\mathbf{x},1) = (x_2, x_1)$ и $\mathbf{g}(\mathbf{x},0) = \mathbf{x}$ для любого $\mathbf{x} = (x_1, x_2) \in \mathbf{E}^2$.

Таким образом, в отличие от БУП $\mathbf{M}_{n,m} \in \{\mathbf{M}^{(1)}_{n,m}, \mathbf{M}^{(2)}_{n,m}\}$ и $\mathbf{S}_{n,m}$, рассмотренных в п.4.2, в БУП $\mathbf{P}_{n,m}$ управляющие символы сосредоточены на элементах $\mathbf{P}_{2,1}$, каждый из которых может переставить только пару бит.

Так как $\mu(\mathbf{P}_{2,1}) = 5$ и $\mu(\pi^{(i)}) = 2 \cdot n$ $(i = 1,\ldots,l)$, то

$$\mu(\mathbf{P}_{n,m}) = 5 \cdot m + 2 \cdot n \cdot l = 2.5 \cdot n \cdot (l-1) + 2 \cdot n \cdot l = \\ = 4.5 \cdot n \cdot l - 2.5 \cdot n. \qquad (4.25)$$

Теорема 4.3. Для всех $n,l \in \mathbf{N}$, где n – четное число, истинны неравенства

$$\mu_{dtct}(\mathbf{P}_{n,m}) \le n^2 \cdot (l+3) \tag{4.26}$$

и

$$\mu_{lclz}(\mathbf{P}_{n,m}) \le (l+3) \cdot (l-1) \cdot n^2 . \tag{4.27}$$

Доказательство. Для обнаружения любых неисправностей на ножках любого элемента КС $\mathbf{P}_{n,m}$ достаточно подать входную последовательность

$$(\mathbf{e}_1,\mathbf{0})\ldots(\mathbf{e}_n,\mathbf{0})(\mathbf{e}_1,\mathbf{1})\ldots(\mathbf{e}_n,\mathbf{1})$$

где $\mathbf{e}_i = (\underbrace{0,\ldots,0}_{i-1 \text{ раз}},1,\underbrace{0,\ldots,0}_{n-i \text{ раз}})$ $(i=1,\ldots,n)$, откуда и вытекает, что

$$\mu_{dtct}(\mathbf{P}_{n,m}) \le 2 \cdot n \cdot (2 \cdot n + m) =$$

$$= 2 \cdot n \cdot (2 \cdot n + 0.5 \cdot n \cdot (l-1)) = n^2 \cdot (l+3),$$

т.е. что неравенство (4.26) истинно.

Для локализации неисправностей на ножках любого элемента КС $\mathbf{P}_{n,m}$ достаточно подать такую последовательность $\mathbf{w} = \mathbf{z}_1 \ldots \mathbf{z}_{l-1}$, что $\mathbf{z}_i = \mathbf{z}_1^{(i)} \ldots \mathbf{z}_{0.5 \cdot n}^{(i)}$ $(i=1,\ldots,l-1)$ и $\mathbf{z}_j^{(i)} = (\mathbf{x}_{j1}^{(i)}, \mathbf{v}_j^{(i)})(\mathbf{x}_{j1}^{(i)},\mathbf{0})(\mathbf{x}_{j2}^{(i)}, \mathbf{v}_j^{(i)})(\mathbf{x}_{j2}^{(i)},\mathbf{0})$ $(i=1,\ldots,l-1)$ для всех $j=1,\ldots,0.5 \cdot n$, где:

1) $\mathbf{x}_{j1}^{(i)}$ – информационный вектор, обеспечивающий подачу на информационные входы элемента $\mathbf{P}_{2,1}$, управляемого символом $v_{j+(i-1)\cdot 0.5 \cdot n}$, вектора (0,1) и нулей на информационные входы всех остальных элементов $\mathbf{P}_{2,1}$, расположенных в том же уровне КС $\mathbf{P}_{n,m}$;

2) $\mathbf{x}_{j2}^{(i)}$ – информационный вектор, обеспечивающий подачу на информационные входы элемента $\mathbf{P}_{2,1}$, управляемого символом $v_{j+0.5 \cdot n \cdot (i-1)}$, вектора (1,0) и нулей на информационные входы всех остальных элементов $\mathbf{P}_{2,1}$, расположенных в том же уровне КС $\mathbf{P}_{n,m}$;

3) управляющий вектор $\mathbf{v}_j^{(i)}$ $(i=1,\ldots,l-1;\ j=1,\ldots,0.5 \cdot n)$ имеет вид

$$\mathbf{v}_j^{(i)} = (\underbrace{0,\ldots,0}_{j+0.5 \cdot n \cdot (i-1)-1 \text{ раз}},1,\underbrace{0,\ldots,0}_{0.5 \cdot n \cdot (l-i)-j \text{ раз}}).$$

Отсюда вытекает, что для $a \in \{dtct, lclz\}$

$$\mu_a(\mathbf{P}_{n,m}) \le (m + 2 \cdot n) \cdot (l-1) \cdot 4 \cdot 0.5 \cdot n =$$

$$= 2 \cdot (0.5 \cdot n \cdot (l-1) + 2 \cdot n) \cdot (l-1) \cdot n = (l+3) \cdot (l-1) \cdot n^2,$$

т.е. неравенства (4.26) истинны.

Теорема доказана.

Отметим, что из (4.25)-(4.27) вытекает

Утверждение 4.3. Если $n \to \infty$ и $l \to \infty$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{P}_{n,m}$ по отношению к асимптотической сложности самого БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(n) \quad (n \to \infty)$;

2) асимптотическая сложность локализации неисправностей БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(\mu^2(\mathbf{P}_{n,m})) \quad (n \to \infty, l \to \infty)$.

4.4. Анализ рекурсивных БУП.

Рекурсивный БУП основан на использовании 2-х или 3-х уровневой сети Клоса.

3-х уровневая сеть Клоса $\mathbf{C}_{(r,s,r),m} \quad (r \cdot s = n)$ изображена на рис. 4.5 (чтобы не загромождать рисунок, управляющие входы не изображаются).

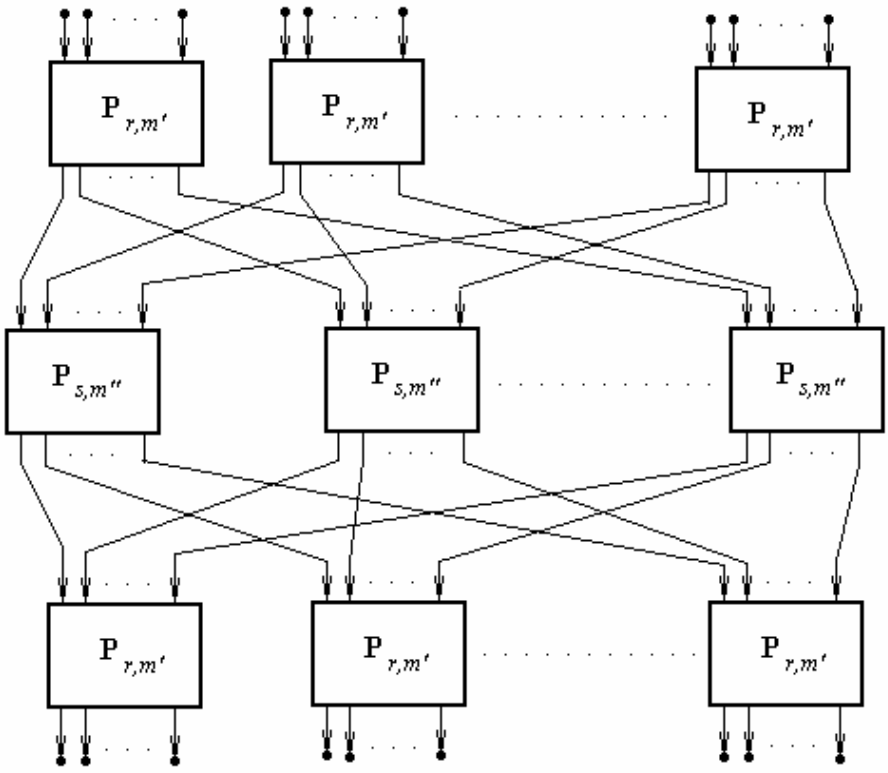


Рис. 4.5. 3-х уровневая сеть Клоса $\mathrm{C}_{(r,s,r),m} \quad (r \cdot s = n)$.

В 3-х уровневой сети Клоса $\mathbf{C}_{(r,s,r),m}$ 1-й уровень содержит s КС $\mathbf{P}_{r,m'}$, каждая из которых реализует одно и то же отображение $g : \mathbf{E}^r \times \mathbf{E}^{m'} \to \mathbf{E}^r$, 2-й уровень содержит r КС $\mathbf{P}_{s,m''}$, каждая из которых реализует одно и то же отображение $h : \mathbf{E}^s \times \mathbf{E}^{m''} \to \mathbf{E}^s$, а 3-й уровень идентичен 1-му уровню.

2-х уровневая сеть Клоса $\mathbf{C}_{(r,s),m}$ $(r \cdot s = n)$ получается, если в 3-х уровневой сети Клоса $\mathbf{C}_{(r,s,r),m}$ отсечь 3-й уровень.

Таким образом, $m = s \cdot (2 \cdot m' + m'')$ для 3-х уровневой сети Клоса $\mathbf{C}_{(r,s,r),m}$ и $m = s \cdot (m' + m'')$ для 2-х уровневой сети Клоса $\mathbf{C}_{(r,s),m}$.

Сложность сетей Клоса определяется равенствами

$$\mu(\mathbf{C}_{(r,s,r),m}) = 2 \cdot s \cdot \mu(\mathbf{P}_{r,m'}) + r \cdot \mu(\mathbf{P}_{s,m''}) \tag{4.28}$$

и

$$\mu(\mathbf{C}_{(r,s),m}) = s \cdot \mu(\mathbf{P}_{r,m'}) + r \cdot \mu(\mathbf{P}_{s,m''}). \tag{4.29}$$

Теорема 4.4. Для каждого значения $a \in \{dtct, lclz\}$ истинны следующие неравенства

$$\mu_a(\mathbf{C}_{(r,s,r),m}) = 2 \cdot s \cdot (2 \cdot r + 2 \cdot m' + m'') \cdot (2 \cdot s \cdot \mu_a(\mathbf{P}_{r,m'}) + r \cdot \mu_a(\mathbf{P}_{r,m''})) \tag{4.30}$$

и

$$\mu_a(\mathbf{C}_{(r,s),m}) = 2 \cdot s \cdot (2 \cdot r + m' + m'') \cdot (s \cdot \mu_a(\mathbf{P}_{r,m'}) + r \cdot \mu_a(\mathbf{P}_{r,m''})). \tag{4.31}$$

Доказательство. Рассмотрим следующий процесс off-line контроля сети Клоса $\mathbf{C} \in \{\mathbf{C}_{(r,s,r),m}, \mathbf{C}_{(r,s),m}\}$.

Уровни сети $\mathbf{C}$ анализируются последовательно, один за другим, в направлении возрастания номеров уровней. Анализируемый уровень сети $\mathbf{C}$ назовем выделенным уровнем. Предполагается, что фиксированы значения всех управляющих входов всех элементов, расположенных в уровнях, отличных от выделенного уровня сети $\mathbf{C}$ (для определенности можно считать, что эти значения управляющих входов равны нулю). Анализ выделенного уровня сети $\mathbf{C}$ состоит в том, что последовательно, один за другим, анализируются послойные БУПы, расположенные в выделенном уровне сети $\mathbf{C}$. Анализ послойного БУПа, расположенного в выделенном уровне сети $\mathbf{C}$, осуществляется следующим образом. Вначале на анализируемый послойный БУП подается соответствующий тест при условии, что на все информационные входы всех остальных послойных БУПов, расположенных в выделенном уровне сети $\mathbf{C}$, подаются нули. Затем на анализируемый послойный БУП подается этот же тест при условии, что на все информационные входы всех остальных послойных БУПов, расположенных в выделенном уровне сети $\mathbf{C}$, подаются единицы.

Таким образом, для каждого значения $a \in \{dtct, lclz\}$

$$\mu_a(\mathbf{C}_{(r,s,r),m}) \le (2 \cdot n + m) \cdot (4 \cdot s \cdot \mu_a(\mathbf{P}_{r,m'}) + 2 \cdot r \cdot \mu_a(\mathbf{P}_{r,m''})) =$$
$$= 2 \cdot s \cdot (2 \cdot r + 2 \cdot m' + m'') \cdot (2 \cdot s \cdot \mu_a(\mathbf{P}_{r,m'}) + r \cdot \mu_a(\mathbf{P}_{r,m''}))$$

и

$$\mu_a(\mathbf{C}_{(r,s),m}) \le (2 \cdot n + m) \cdot (2 \cdot s \cdot \mu_a(\mathbf{P}_{r,m'}) + 2 \cdot r \cdot \mu_a(\mathbf{P}_{r,m''})) =$$
$$= 2 \cdot s \cdot (2 \cdot r + m' + m'') \cdot (s \cdot \mu_a(\mathbf{P}_{r,m'}) + r \cdot \mu_a(\mathbf{P}_{r,m''})).$$

Теорема доказана.

Известно, что рекурсивный послойный БУП – это специальный случай 2-х уровневой сети Клоса $\mathbf{C}_{(r,s),m}$, а рекурсивные БУП Бенеша и Ваксмана – это специальные случаи 3-х уровневой сети Клоса $\mathbf{C}_{(r,s,r),m}$ [123]. Поэтому оценки (4.28)-(4.31) характеризуют сложность обнаружения и локализации неисправностей в этих рекурсивных БУП. Эти оценки могут быть улучшены для специальных случаев рекурсивных БУП, так как рекурсивная структура БУП может быть отображена в структуру теста, а анализ фрагмента, представленного на рис. 4.6, можно осуществить в соответствии со следующей схемой (которая была использована при анализе сетей Клоса):

Этап 1. Проверяется левый блок F_1 при условии, что правый блок F_1 является пассивным.

Этап 2. Проверяется правый блок F_1 при условии, что левый блок F_1 является пассивным.

Этап 3. Проверяется блок F_2.

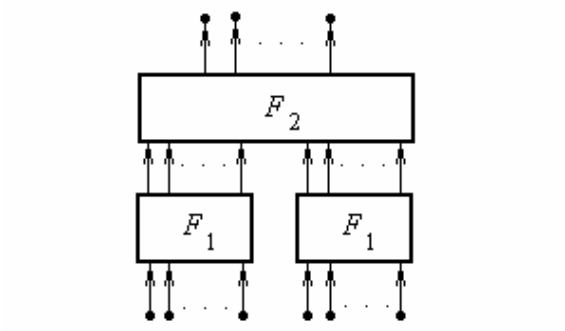


Рис. 4.6. Фрагмент рекурсивного БУП.

Действительно, так как F_1 и F_2 – КС, то соответствующие им тестовые наборы допускают любое переупорядочение. Следовательно, этапы 2 и 3 могут быть объединены за счет построения «тасованного» произведения тестов, предназначенных для левого и правого блоков F_1.

4.5. Анализ УПО.

Для УПО, в отличие от БУП, в настоящее время отсутствуют хорошо проработанные базовые типы КС, что, По всей видимости, это вызвано следующими причинами.

Во-первых, достаточно широкий класс совершенно различных по своей структуре вектор-функций (4.1) удовлетворяет условию 4.1.

Во-вторых, криптографические характеристики (показатели нелинейности, неравномерное движение, корреляционная иммунность и т.д.) определяются, по сути, в терминах графика соответствующей вектор-функции.

В-третьих, элементы ключевой последовательности, используемые в качестве управляющих векторов, могут быть подвержены рекурсивным преобразованиям.

Тем не менее, за счет вывода контрольных точек в КС, реализующей УПО, всегда можно выделить достаточно небольшой по числу внешних ножек элемент, представленный на рис. 4.1.б.

Рассмотрим контроль неисправностей такого элемента.

Из условия 4.1 вытекает, что последовательность векторов $(\mathbf{e}_i, \mathbf{v})$ $(i = 1,\ldots,n)$, где $\mathbf{v} \in \mathbf{E}^m$ – фиксированный вектор, а $\mathbf{e}_i = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{n-i\ раз})$ $(i = 1,\ldots,n)$ дает возможность обнаружить (более того, локализировать) любую неисправность на информационных входах КС, реализующей УПО.

Предположим, что УПО удовлетворяет следующему условию.

Условие 4.4. Для каждого $\mathbf{x}_0 \in \mathbf{E}^n$ вектор-функция $\mathbf{h}_{\mathbf{x}_0} : \mathbf{E}^m \to \mathbf{E}^l$, где

$$\mathbf{h}_{\mathbf{x}_0}(\mathbf{v}) = \mathbf{f}(\mathbf{x}_0, \mathbf{v}) \quad (\mathbf{v} \in \mathbf{E}^m),$$

является инъекцией множества $\mathbf{E}^m$ в множество $\mathbf{E}^l$.

Тогда для обнаружения (более того, для локализации) любой неисправности на управляющих входах КС, реализующей УПО, достаточно подать такую последовательность $\mathbf{z}_1 \ldots \mathbf{z}_m$, что

$$\mathbf{z}_i = (\mathbf{x}_1^{(i)}, \tilde{\mathbf{e}}_i)(\mathbf{x}_2^{(i)}, \tilde{\mathbf{e}}_i)(\mathbf{x}_3^{(i)}, \tilde{\mathbf{e}}_i),$$

где $\tilde{\mathbf{e}}_i = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{m-i\ раз})$ $(i = 1,\ldots,m)$, а $\mathbf{x}_1^{(i)}, \mathbf{x}_2^{(i)}, \mathbf{x}_3^{(i)} \in \mathbf{E}^n$ $(i = 1,\ldots,m)$ – такие информационные векторы, что

$$\mathbf{f}(\mathbf{x}_1^{(i)}, \tilde{\mathbf{e}}_i) \neq \mathbf{f}(\mathbf{x}_1^{(i)}, \mathbf{0}), \tag{4.32}$$

$$\mathbf{f}(\mathbf{x}_2^{(i)}, \tilde{\mathbf{e}}_i) \neq \mathbf{f}(\mathbf{x}_2^{(i)}, (\underbrace{0,\ldots,0}_{i-2\ раз},1,1,\underbrace{0,\ldots,0}_{m-i\ раз})) \tag{4.33}$$

и

$$\mathbf{f}(\mathbf{x}_3^{(i)}, \tilde{\mathbf{e}}_i) \neq \mathbf{f}(\mathbf{x}_3^{(i)}, (\underbrace{0,\ldots,0}_{i-1\ раз},1,1,\underbrace{0,\ldots,0}_{m-i-1\ раз})). \tag{4.34}$$

Будем говорить, что i-выход $(i = 1,\ldots,l)$ КС, реализующей УПО, активируем, если существуют такие векторы $(\tilde{\mathbf{x}}_1^{(i)}, \mathbf{v}_1^{(i)}), (\tilde{\mathbf{x}}_2^{(i)}, \mathbf{v}_2^{(i)}) \in \mathbf{E}^{n+m}$, что

$$pr_i\mathbf{f}(\tilde{\mathbf{x}}_1^{(i)}, \mathbf{v}_1^{(i)}) \neq pr_i\mathbf{f}(\tilde{\mathbf{x}}_2^{(i)}, \mathbf{v}_2^{(i)}). \tag{4.35}$$

Ясно, что если i-выход $(i = 1,\ldots,l)$ КС, реализующей УПО, активируем, то пара векторов $(\tilde{\mathbf{x}}_1^{(i)}, \mathbf{v}_1^{(i)}), (\tilde{\mathbf{x}}_2^{(i)}, \mathbf{v}_2^{(i)}) \in \mathbf{E}^{n+m}$ дает возможность обнаружить (более того, локализировать) константные неисправности на этом выходе.

Для обнаружения (более того, для локализации) КЗ на активируемом выходе КС, реализующей УПО, достаточно:

1) если $i = 1$, то найти такой вектор $(\tilde{\mathbf{x}}_3^{(1)}, \mathbf{v}_3^{(1)}) \in \mathbf{E}^{n+m}$, что

$$pr_1\mathbf{f}(\tilde{\mathbf{x}}_3^{(1)}, \mathbf{v}_3^{(1)}) \neq pr_2\mathbf{f}(\tilde{\mathbf{x}}_3^{(1)}, \mathbf{v}_3^{(1)}); \tag{4.36}$$

2) если $i = l$, то найти такой вектор $(\tilde{\mathbf{x}}_3^{(l)}, \mathbf{v}_3^{(l)}) \in \mathbf{E}^{n+m}$, что

$$pr_l \mathbf{f}(\tilde{\mathbf{x}}_3^{(l)}, \mathbf{v}_3^{(l)}) \neq pr_{l-1} \mathbf{f}(\tilde{\mathbf{x}}_3^{(l)}, \mathbf{v}_3^{(l)}); \quad (4.37)$$

3) если $i = 2,\ldots,l-1$, то найти такие векторы $(\tilde{\mathbf{x}}_3^{(i)}, \mathbf{v}_3^{(i)}), (\tilde{\mathbf{x}}_4^{(i)}, \mathbf{v}_4^{(i)}) \in \mathbf{E}^{n+m}$, что

$$pr_i \mathbf{f}(\tilde{\mathbf{x}}_3^{(i)}, \mathbf{v}_3^{(i)}) \neq pr_{i-1} \mathbf{f}(\tilde{\mathbf{x}}_3^{(i)}, \mathbf{v}_3^{(i)}); \quad (4.38)$$

и

$$pr_i \mathbf{f}(\tilde{\mathbf{x}}_4^{(i)}, \mathbf{v}_4^{(i)}) \neq pr_{i+1} \mathbf{f}(\tilde{\mathbf{x}}_4^{(i)}, \mathbf{v}_4^{(i)}). \quad (4.39)$$

Таким образом, асимптотическая сложность построенного теста не превосходит квадрат асимптотической сложности элемента, представленного на рис. 4.1.б.

Однако для того, чтобы обеспечить условия (4.32)-(4.39), необходимо вычислить булевы производные вектор-функции $\mathbf{f}$, а затем построить и решить соответствующие системы булевых уравнений. Именно в этом и состоит основная сложность обнаружения и локализации неисправностей на внешних входах и выходах КС, реализующей УПО.

4.6. Выводы.

В настоящем разделе исследована задача off-line контроля неисправностей БУП и УПО. Основные результаты состоят в следующем:

1. Выделены два типа матричных БУП. Доказано, что асимптотическая сложность контроля неисправностей этих БУП незначительно отличается от асимптотической сложности самих БУП.
2. Построен матричный БУП $\mathbf{S}_{n,m}$, у которого ключевой поток подается непосредственно на управляющие входы $v_1,\ldots,v_m$ элементов $P_n^{(1)}$. Доказано, что асимптотическая сложность локализации неисправностей этого БУП не превосходит квадрат асимптотической сложности самого БУП.
3. Доказано, что асимптотическая сложность локализации неисправностей послойного БУП не превосходит квадрат асимптотической сложности самого БУП.
4. Установлены оценки сложности обнаружения и локализации неисправностей 2-х уровневой и 3-х уровневой сети Клоса.
5. Показано, что сложность асимптотическая сложность локализации неисправностей УПО, рассматриваемой как элемент, не превосходит квадрат асимптотической сложности этого элемента.

5. ЛИНЕЙНЫЕ АВТОМАТЫ НАД КОНЕЧНЫМ КОЛЬЦОМ

В п.1.7 показано, что для современной криптологии актуальным является исследование динамических систем, представленных системами уравнений над конечным кольцом. Такие динамические системы естественно приводят к новым классам автоматов – автоматам над конечными кольцами, для анализа которых применим не только математический аппарат теории автоматов, но и математический аппарат современной алгебры и теории систем.

Целью настоящего раздела является систематическое исследование линейных автоматов над кольцом $\mathsf{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbf{N}$).

В п.5.1 изложен математический аппарат линейной алгебры над конечным кольцом, используемый в настоящем и следующем разделах. В п.5.2 представлены исследуемые модели – линейные автоматы Мили и Мура с лагом 1 над конечным кольцом. Выделены подмножества этих автоматов, представляющие собой поточные шифры. В п.5.3 охарактеризованы основные нетривиальные подмножества линейных автоматов над конечным кольцом. Оценены мощности этих подмножеств автоматов. В п.5.4 установлены критерии эквивалентности линейных автоматов над конечным кольцом, а также охарактеризованы классы эквивалентных состояний линейного автомата над конечным кольцом. В п.5.5. решены задачи параметрической идентификации и идентификации начального состояния для линейных автоматов над конечным кольцом. В п.5.6 охарактеризованы множества неподвижных точек словарных функций, реализуемых инициальными линейными автоматами над конечным кольцом. В п.5.7 построены канонические формы линейных автоматов над конечным кольцом. В п.5.8 исследуется вариация поведения линейных автоматов над конечным кольцом. В п.5.9 охарактеризованы линейные одномерные автоматы с лагом l над конечным кольцом.

Материал, представленный в настоящем разделе, представляет собой систематическое изложение результатов, полученных в [156-163].

5.1. Элементы линейной алгебры над конечным кольцом.

Известно, что если $k \geq 2$, то в кольце Z_{p^k} имеются делители нуля, т.е. из равенства

$$a \circ b = 0 \quad (a, b \in \mathbf{Z}_{p^k})$$

не следует, что $a \neq 0$ и $b \neq 0$.

Отсюда, в частности, вытекает, что условие $a \neq 0$ не является достаточным условием для существования решения линейного уравнения

$$a \circ x = b.$$

Кроме того, это уравнение может иметь неединственное решение.

Для любого элемента a кольца Z_{p^k} и для любой подстановки $f \in \mathsf{S}(n)$ $(n \in \mathbf{N})$ положим

$$sign_f(a) = \begin{cases} a, & \text{если } f \text{ определяет четную перестановку} \\ & \text{элементов множества } \mathbf{N}_n \\ \ominus a, & \text{если } f \text{ определяет нечетную перестановку} \\ & \text{элементов множества } \mathbf{N}_n. \end{cases}$$

Определитель квадратной матрицы

$$M = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

над кольцом Z_{p^k} определяется равенством

$$\det(M) = \sum_{f \in S(n)} sign_f (a_{1\,f(1)} \circ \dots \circ a_{n\,f(n)}).$$

Ясно, что для квадратной матрицы M над кольцом Z_{p^k} условие

$$\det(M) \neq 0$$

не является достаточным условием для существования обратной матрицы M^{-1}, так как $\det(M)$ может не быть обратимым элементом кольца Z_{p^k}.

Основная цель проводимых ниже исследований состоит в том, чтобы оценить число обратимых матриц над кольцом Z_{p^k}, а также исследовать решение систем линейных уравнений, состоящих из n уравнений от n переменных над кольцом Z_{p^k}.

Охарактеризуем вначале мультипликативную группу кольца Z_{p^k}

Лемма 5.1. Число $a \in \mathbf{Z}_{p^k}$ является обратимым элементом кольца Z_{p^k} тогда и только тогда, когда

$$a \not\equiv 0 \pmod{p}.$$

Доказательство. 1. Пусть $a \in \mathbf{Z}_{p^k}$ и $a \not\equiv 0 \pmod{p}$.

Так как $a \not\equiv 0 \pmod{p}$, а p – простое число, то $(a, p) = 1$. Следовательно, $(a, p^k) = 1$. Из теоремы Эйлера вытекает, что

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k}, \qquad (5.1)$$

где φ – функция Эйлера.

Так как $\varphi(p^k) = p^k - p^{k-1}$, то из (5.1) вытекает, что

$$a^{p^k - p^{k-1}} \equiv 1 \pmod{p^k} \Leftrightarrow a^{p^k - p^{k-1} - 1} \cdot a \equiv 1 \pmod{p^k} \Leftrightarrow a^{p^k - p^{k-1} - 1} \circ a = 1.$$

т.е. $a \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, что и требовалось показать.

2. Пусть $a \in \mathbf{Z}_{p^k}$ и $a \equiv 0 \pmod{p}$.

Известно, что необходимое условие, при котором истинно сравнение

$$u \equiv v \pmod{m}$$

имеет вид

$$d \mid u \;\&\; d \mid m \Rightarrow d \mid v. \qquad (5.2)$$

Так как $a \equiv 0 \pmod{p}$, то $p \mid a$. Следовательно, для сравнения

$$a \cdot x \equiv 1 \pmod{p^k}, \qquad (5.3)$$

где $x \in \mathbf{N}$, истинно условие

$$(\forall x \in \mathbf{N})(p \mid (a \cdot x) \;\&\; p \mid p^k \;\&\; p \nmid 1),$$

т.е. для сравнения (5.3) условие (5.2) не выполняется ни при каком $x \in \mathbf{N}$.

Следовательно, при всех $x \in \mathbf{N}$ сравнение (5.3) не имеет решений. Отсюда вытекает, что равенство

$$a \circ x = 1$$

является ложным для всех таких $a \in \mathbf{Z}_{p^k}$, что $a \equiv 0 \pmod{p}$. Последнее означает, что ни одно такое число $a \in \mathbf{Z}_{p^k}$, что $a \equiv 0 \pmod{p}$, не является обратимым элементом кольца Z_{p^k}.

Лемма доказана.

Из леммы 5.1 непосредственно вытекает

Утверждение 5.1. Квадратная матрица M над кольцом Z_{p^k} обратима тогда и только тогда, когда

$$\det(M) \not\equiv 0 \pmod{p}.$$

Представим элемент $a \in \mathbf{Z}_{p^k}$ в системе счисления с основанием p, т.е. в виде

$$a = \alpha_{k-1} \ldots \alpha_1 \alpha_0,$$

где $\alpha_i \in \mathbf{Z}_p \;\; (i = 0,1,\ldots,k-1)$.

Из леммы 5.1 вытекает, что a – обратимый элемент кольца Z_{p^k} тогда и только тогда, когда $\alpha_0 \neq 0$. Отсюда, в свою очередь, вытекает, что истинны следующие два утверждения.

Утверждение 5.2. В кольце Z_{p^k} существует в точности $(p-1) \cdot p^{k-1}$ обратимых элементов.

Утверждение 5.3. В кольце Z_{p^k} существует в точности p^{k-1} необратимых элементов.

Определим p-тип элемента $a \in \mathbf{Z}_{p^k}$ кольца Z_{p^k} следующим образом:

1) если $a = 0$, то p-тип элемента a равен k;

2) если $a \neq 0$, то p-тип элемента a равен такому наименьшему числу $r \in \mathbf{Z}_k$, что $a \equiv 0 \pmod{p^r}$ и $a \not\equiv 0 \pmod{p^{r+1}}$.

Таким образом, множеством p-типов элементов кольца Z_{p^k} является множество $\mathbf{Z}_{k+1}$, причем множество элементов p-типа 0 – это множество всех обратимых элементов кольца Z_{p^k}.

Будем говорить что над кольцом Z_{p^k} линейное уравнение

$$a \circ x = b \quad (a,b \in \mathbf{Z}_{p^k}). \tag{5.4}$$

имеет p-тип (h,r) $(h,r \in \mathbf{Z}_{k+1})$, если a – элемент p-типа h, а b – элемент p-типа r.

Ясно, что множество решений уравнения (5.4) следующим образом характеризуется его p-типом (h,r).

Утверждение 5.4. Если $h=0$, то уравнение (5.4) имеет единственное решение. Это решение имеет вид

$$x = a^{-1} \circ b.$$

Утверждение 5.5. Если $h > r$, то уравнение (5.4) не имеет решений.

Утверждение 5.6. Если $h \in \mathbf{Z}_k$ и $h \le r$, то уравнение (5.4) имеет p^h решений. Эти решения имеют вид

$$x = y \circ p^{k-h} \oplus x_0,$$

где x_0 – фиксированный элемент множества $\mathbf{Z}_{p^{k-h}}$, а y – произвольный элемент множества $\mathbf{Z}_{p^h}$.

Утверждение 5.7. Если $h = r = k$, то решением уравнения (5.4) является любой элемент кольца Z_{p^k}.

Отметим, что из утверждений 5.4, 5.6 и 5.7 вытекает

Утверждение 5.8. Если $h \le r$, то уравнение (5.4) имеет p^h решений.

Обозначим через M_n $(n \in \mathbf{N})$ множество всех $n \times n$-матриц над кольцом Z_{p^k}, а через M_n^{inv} – множество всех обратимых матриц $M \in M_n$.

Ясно, что

$$|M_n| = p^{k \cdot n^2} \quad (n \in \mathbf{N}). \tag{5.5}$$

Теорема 5.1. Истинны следующие верхняя и нижняя оценки для числа обратимых $n \times n$-матриц над кольцом Z_{p^k}

$$n!\cdot(p-1)^n \cdot p^{-n^2} \cdot |M_n| \le |M_n^{inv}| \le (1-p^{-n})^n \cdot |M_n| \quad (n \in \mathbf{N}). \tag{5.6}$$

Доказательство. 1. Покажем, что истинна нижняя оценка для числа обратимых $n \times n$-матриц над кольцом Z_{p^k}.

Зафиксируем подстановку $f \in S(n)$.

Обозначим через $M_n^{(f)}$ множество всех таких матриц

$$M = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in M_n,$$

что:

1) каждый элемент $a_{i\,f(i)}$ $(i=,1,\ldots,n)$ матрицы M является обратимым элементом кольца Z_{p^k};

2) для каждого $i\in \mathbf{N}_n$ при всех $j\neq f(i)$ элемент a_{ij} матрицы M является необратимым элементом кольца Z_{p^k}.

Для любой матрицы $M\in \mathsf{M}_n^{(f)}$

$$\det(M)=sign(f)\circ a_{1\,f(1)}\circ\ldots\circ a_{n\,f(n)}\oplus b,$$

где b – необратимый элемент кольца Z_{p^k}.

Следовательно, $\det(M)$ – обратимый элемент кольца Z_{p^k} для любой матрицы $M\in \mathsf{M}_n^{(f)}$, т.е.

$$\mathsf{M}_n^{(f)}\subset \mathsf{M}_n^{inv}.$$

Отсюда вытекает, что

$$\mathsf{M}_n^{inv}\supseteq \bigcup_{f\in \mathsf{S}(n)} \mathsf{M}_n^{(f)}. \qquad (5.7)$$

А так как множества $\mathsf{M}_n^{(f)}$ $(f\in \mathsf{S}(n))$ попарно не пересекаются, то из (5.6) вытекает, что

$$|\mathsf{M}_n^{inv}|\geq \sum_{f\in \mathsf{S}(n)} |\mathsf{M}_n^{(f)}|. \qquad (5.8)$$

Вычислим $|\mathsf{M}_n^{(f)}|$ $(f\in \mathsf{S}(n))$.

Из утверждений 5.2 и 5.3 вытекает, что для матрицы $M\in \mathsf{M}_n^{(f)}$ число способов выбора элементов $a_{i\,f(i)}$ $(i=1,\ldots,n)$ равно $((p-1)\cdot p^{k-1})^n$, а число способов выбора элементов a_{ij} $(i,j\in \mathbf{N}_n;\ j\neq f(i))$ равно $(p^{k-1})^{n^2-n}$.

Следовательно,

$$|\mathsf{M}_n^{(f)}|=((p-1)\cdot p^{k-1})^n\cdot (p^{k-1})^{n^2-n}=(p-1)^n\cdot p^{-n^2}\cdot|\mathsf{M}_n|. \qquad (5.9)$$

Подставив (5.9) в (5.8), получим

$$|\mathsf{M}_n^{inv}|\geq \sum_{f\in \mathsf{S}(n)} (p-1)^n\cdot p^{-n^2}\cdot|\mathsf{M}_n|=n!\cdot(p-1)^n\cdot p^{-n^2}\cdot|\mathsf{M}_n|,$$

что и требовалось показать.

2. Покажем, что истинна верхняя оценка для числа обратимых $n\times n$-матриц над кольцом Z_{p^k}.

Обозначим через $\mathsf{M}_n^{non\_inv}$ множество всех необратимых матриц $M\in \mathsf{M}_n$. Тогда

$$\mathsf{M}_n^{inv}=\mathsf{M}_n\setminus \mathsf{M}_n^{non\_inv}.$$

Следовательно,

$$|\mathsf{M}_n^{inv}| = |\mathsf{M}_n| - |\mathsf{M}_n^{non\_inv}|. \qquad (5.10)$$

Обозначим через $\mathsf{M}_n(i)$ $(i = 1,\ldots,n)$ множество всех таких матриц $M \in \mathsf{M}_n$, что:

1) в каждом столбце с номером $j \in \{1,\ldots,i-1\}$ расположен, по крайней мере, один обратимый элемент кольца Z_{p^k};

2) каждый элемент i-го столбца – необратимым элементом кольца Z_{p^k}.

Из равенства

$$\det(M) = \sum_{f \in \mathsf{S}(n)} sign_f (a_{1\,f(1)} \circ \ldots \circ a_{n\,f(n)})$$

вытекает, что $\det(M)$ – необратимый элемент кольца Z_{p^k} для любой матрицы $M \in \mathsf{M}_n(i)$ $(i = 1,\ldots,n)$, т.е.

$$\mathsf{M}_n^{non\_inv} \supseteq \bigcup_{i=1}^{n} \mathsf{M}_n(i). \qquad (5.11)$$

Так как множества $\mathsf{M}_n(i)$ $(i = 1,\ldots,n)$ попарно не пересекаются, то из (5.11) вытекает, что

$$|\mathsf{M}_n^{non\_inv}| \geq \sum_{i=1}^{n} |\mathsf{M}_n(i)|. \qquad (5.12)$$

Вычислим $|\mathsf{M}_n(i)|$ $(i = 1,\ldots,n)$.

Общее число n-мерных векторов, компоненты которых – элементы кольца Z_{p^k}, равно $p^{k \cdot n}$.

Из утверждения 5.3 вытекает, что число n-мерных векторов, компоненты которых – необратимые элементы кольца Z_{p^k}, равно $p^{(k-1) \cdot n}$.

Следовательно, число n-мерных векторов, компоненты которых – элементы кольца Z_{p^k}, причем хотя бы одна компонента – обратимый элемент кольца Z_{p^k}, равно

$$p^{k \cdot n} - p^{(k-1) \cdot n} = p^{k \cdot n} \cdot (1 - p^{-n}).$$

Таким образом, для матрицы $M \in \mathsf{M}_n(i)$ $(i = 1,\ldots,n)$ число способов выбора столбцов с номерами $1,\ldots,i-1$, равно $(p^{k \cdot n} \cdot (1 - p^{-n}))^{i-1}$, число способов выбора i-го столбца равно $p^{(k-1) \cdot n}$, а число способов выбора столбцов с номерами $i+1,\ldots,n$ равно $(p^{k \cdot n})^{n-i}$.

Отсюда вытекает, что

$$|\mathsf{M}_n(i)| = (p^{k \cdot n} \cdot (1 - p^{-n}))^{i-1} \cdot p^{(k-1) \cdot n} \cdot (p^{k \cdot n})^{n-i} =$$

$$= (1 - p^{-n})^{i-1} \cdot p^{-n} \cdot |\mathsf{M}_n|. \qquad (5.13)$$

Подставив (5.13) в (5.12), получим

$$|\mathsf{M}_n^{non\_inv}| \geq \sum_{i=1}^{n} (1-p^{-n})^{i-1} \cdot p^{-n} \cdot |\mathsf{M}_n| = p^{-n} \cdot |\mathsf{M}_n| \cdot \sum_{i=1}^{n} (1-p^{-n})^{i-1} =$$

$$= p^{-n} \cdot |\mathsf{M}_n| \cdot \frac{1-(1-p^{-n})^n}{1-(1-p^{-n})} = (1-(1-p^{-n})^n) \cdot |\mathsf{M}_n|. \qquad (5.14)$$

Подставив (5.14) в (5.10), получим

$$|\mathsf{M}_n^{inv}| \leq |\mathsf{M}_n| - (1-(1-p^{-n})^n) \cdot |\mathsf{M}_n| = (1-p^{-n})^n \cdot |\mathsf{M}_n|.$$

Теорема доказана.

Рассмотрим теперь систему, состоящую из n линейных уравнений от n переменных над кольцом Z_{p^k}

$$A \circ \mathbf{x} = \mathbf{b} \quad (A \in \mathsf{M}_n, \mathbf{b} \in \mathbf{Z}_{p^k}^n) \qquad (5.15)$$

Число l_n $(n \in \mathbf{N})$ различных систем (5.15) над кольцом Z_{p^k} равно

$$l_n = |\mathsf{M}_n| \cdot p^{k \cdot n} \quad (n \in \mathbf{N}).$$

Для системы (5.15) возможны следующие два случая.

Случай 1. Пусть $A \in \mathsf{M}_n^{inv}$.

Тогда система (5.15) имеет единственное решение

$$\mathbf{x} = A^{-1} \circ \mathbf{b}.$$

Из теоремы 5.1 вытекает

Утверждение 5.9. Доля ν_n $(n \in \mathbf{N})$ систем (5.15), которые имеют единственное решение, удовлетворяет неравенствам

$$n!\cdot(p-1)^n \cdot p^{-n^2} \leq \nu_n \leq (1-p^{-n})^n \quad (n \in \mathbf{N}).$$

Случай 2. Пусть $A \in \mathsf{M}_n^{non\_inv}$.

Посредством элементарных преобразований и, возможно, изменив нумерацию переменных, приведем систему (5.15) к эквивалентной системе уравнений

$$C \circ \mathbf{y} = \mathbf{d}, \qquad (5.16)$$

где $C \in \mathsf{M}_n^{non\_inv}$ – такая диагональная матрица

$$C = \begin{pmatrix} c_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & c_n \end{pmatrix},$$

что $c_1, \dots, c_l$ $(0 \leq l \leq n-1)$ – обратимые, а $c_{l+1}, \dots, c_n$ – необратимые элементы кольца Z_{p^k}.

Запишем систему (5.16) в явном виде

$$\begin{cases} c_1 \circ y_1 = d_1 \\ \quad \vdots \\ c_n \circ y_n = d_n \end{cases}. \qquad (5.17)$$

Назовем p-типом системы (5.17) упорядоченный набор

$$\mathbf{s} = ((h_1, r_1), \ldots, (h_n, r_n)),$$

где (h_i, r_i) $(i = 1, \ldots, n)$ – p-тип уравнения $c_i \circ y_i = d_i$.

Из утверждений 5.4-5.8 вытекают

Утверждение 5.10. Если существует такая упорядоченная пара

$$(h_j, r_j) \in \mathbf{s} \quad (j = l+1, \ldots, n),$$

что $h_j > r_j$, то система (5.17) не имеет решений.

Утверждение 5.11. Если каждая упорядоченная пара

$$(h_j, r_j) \in \mathbf{s} \quad (j = l+1, \ldots, n),$$

удовлетворяет условию $h_j \le r_j$, то система (5.17) имеет в точности

$$p^{\sum_{j=l+1}^{n} r_j}$$

решений.

Таким образом, p-тип системы линейных уравнений (5.17) дает возможность выяснить, имеет ли эта система решения (т.е. является ли эта система совместной), и в случае положительного ответа вычислить число решений этой системы.

5.2. Исследуемые модели.

Объектами исследования настоящего раздела являются инициальные автоматы Мили и Мура над кольцом $\mathbf{Z}_{p^k}$, соответственно,

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+) \qquad (5.18)$$

и

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (5.19)$$

где

$$A, B, C, D \in \mathsf{M}_n \quad (n \in \mathbf{N}),$$

а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathbf{Z}_{p^k}^n$ – вектор-столбцы, представляющие, соответственно, состояние автомата, входной и выходной символ в момент t.

Обозначим через $\mathsf{A}_{n,1}$ множество всех автоматов M_1, определяемых формулой (5.18), а через $\mathsf{A}_{n,2}$ – множество всех автоматов M_2, определяемых формулой (5.19).

Из (5.5) вытекает, что

$$|\mathsf{A}_{n,1}| = p^{4\cdot k\cdot n^2}$$

и

$$|\mathsf{A}_{n,2}| = p^{3\cdot k\cdot n^2}.$$

Истинны следующие два утверждения.

Утверждение 5.12. Автомат $M_1 \in \mathsf{A}_{n,1}$ является обратимым автоматом тогда и только тогда, когда $D \in \mathsf{M}_n^{inv}$.

Утверждение 5.13. Автомат $M_2 \in \mathsf{A}_{n,2}$ является обратимым автоматом тогда и только тогда, когда $B, C \in \mathsf{M}_n^{inv}$.

Доказательство этих утверждений аналогично доказательству утверждений 1.6 и 1.7.

При этом соответствующие обратные автоматы имеют, соответственно, вид:

$$(M_1^{-1}, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A_1 \circ \mathbf{q}_t \oplus B_1 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1} \end{cases} (t \in \mathbf{Z}_+),$$

где $A_1 = A \Theta B \circ D^{-1} \circ C$, $B_1 = B \circ D^{-1}$, $C_1 = \Theta D^{-1} \circ C$, $D_1 = D^{-1}$ и

$$(M_2^{-1}, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = B_1 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1} \end{cases} (t \in \mathbf{Z}_+),$$

где $B_1 = C^{-1}$, $C_1 = \Theta A$, $D_1 = B^{-1} \circ C^{-1}$.

Обозначим через $\mathsf{A}_{n,i}^{inv}$ $(i = 1,2)$ множество всех обратимых автоматов $M_i \in \mathsf{A}_{n,i}$.

Ясно, что пара

$$((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0)) \quad (M \in \mathsf{A}_{n,1}^{inv} \cup \mathsf{A}_{n,2}^{inv})$$

представляет собой симметричный поточный шифр, для которого начальное состояние $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ представляет собой секретный сеансовый ключ.

Отметим, что число секретных сеансовых ключей для симметричного поточного шифра $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ $(M \in \mathsf{A}_{n,1}^{inv} \cup \mathsf{A}_{n,2}^{inv})$ равно $p^{k\cdot n}$.

Процесс шифрования на основе автомата $(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1}^{inv} \cup \mathsf{A}_{n,2}^{inv})$ схематически представлен на рис. 5.1.

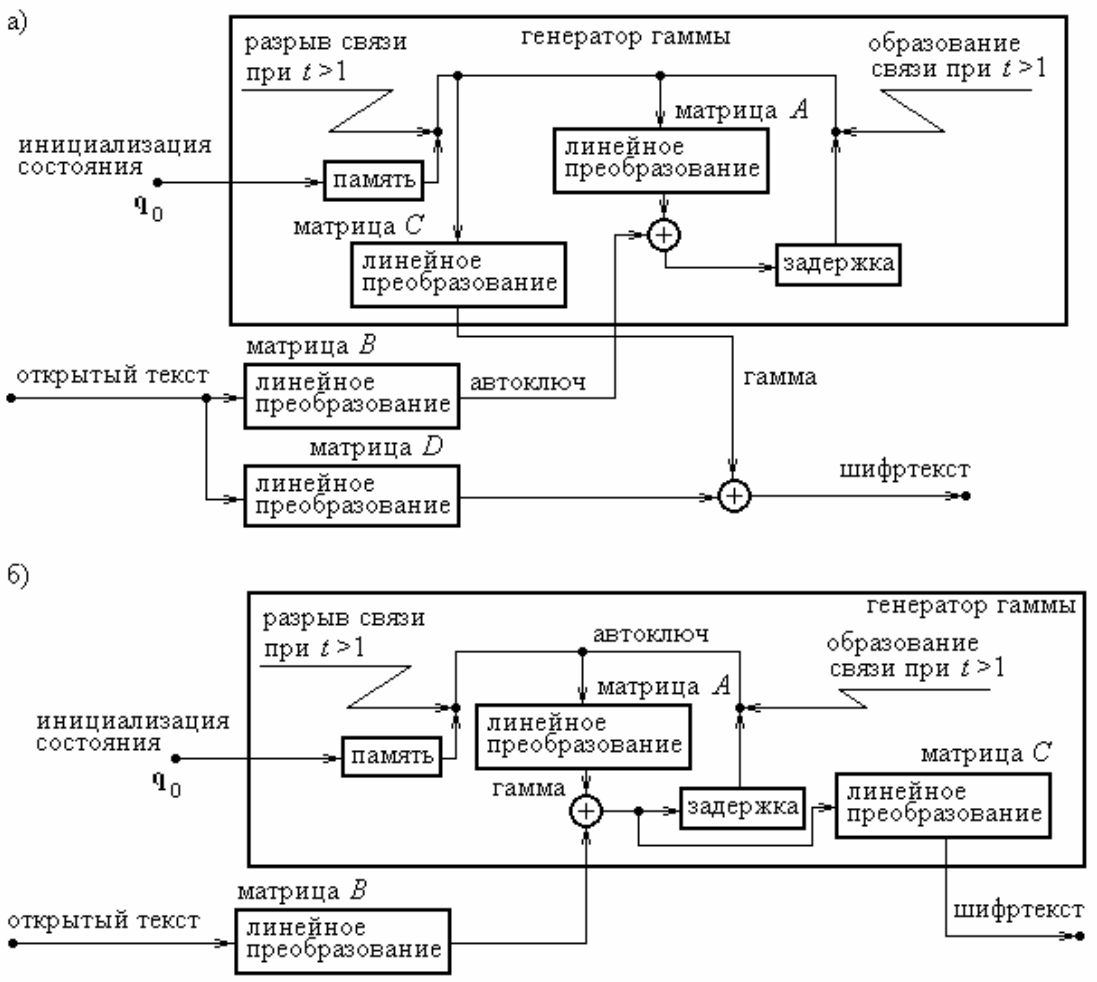


Рис. 5.1. Процесс шифрования на основе БПИ-автомата $(M, \mathbf{q}_0)$: а) $M = M_1$; б) $M = M_2$.

Отметим следующие три отличия предложенной схемы от классической схемы шифра гаммирования, предложенной К. Шенноном [59,227].

Во-первых, открытый текст подвергается линейным преобразованиям над кольцом Z_{p^k}.

Во-вторых, генератор гаммы существенно использует автоключ, конструируемый на основе открытого текста, подвергнутого линейным преобразованиям над кольцом Z_{p^k}.

В-третьих, генератор гаммы при шифровании построен на основе прямого автомата, а генератор гаммы при расшифровке – на основе обратного ему автомата.

Из последнего обстоятельства вытекает, что в процессе шифрования осуществляется движение по некоторой траектории в пространстве состояний, а в процессе расшифровки – движение в том же пространстве состояний по той же траектории в том же самом направлении.

Поэтому, если симметричный поточный шифр

$$((M, \mathbf{q_0}), (M^{-1}, \mathbf{q_0}))\ \ (M \in \mathsf{A}_{n,1}^{inv} \cup \mathsf{A}_{n,2}^{inv})$$

функционирует в предположении, что

$$x_1 = \ldots = x_n,$$

т.е. в процессе передачи информации осуществляется n-кратное дублирование (на уровне элементов кольца Z_{p^k}), то появляется возможность несложного контроля (т.е. обнаружения или исправления) ошибок, возникающих в процессе передачи информации.

Действительно, применение мажоритарной схемы в процессе расшифровки информации дает возможность обнаруживать $n-1$ ошибку. Если же дополнительно снабдить адресат также и схемой коррекции состояния, то появляется возможность исправления $\lfloor 0.5 \cdot (n-1) \rfloor$ ошибок.

Теорема 5.2. Для всех $n \in \mathbf{N}$

$$(n! \cdot (p-1)^n \cdot p^{-n^2})^i \cdot |\mathsf{A}_{n,i}| \le |\mathsf{A}_{n,i}^{inv}| \le (1-p^{-n})^{n \cdot i} \cdot |\mathsf{A}_{n,i}| \quad (i = 1,2). \quad (5.20)$$

Доказательство. Так как для автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ выбор матриц из множества M_n осуществляется независимо, то

$$|\mathsf{A}_{n,1}| = |\mathsf{M}_n|^4 \quad (5.21)$$

и

$$|\mathsf{A}_{n,2}| = |\mathsf{M}_n|^3. \quad (5.22)$$

Для автомата $M_1 \in \mathsf{A}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, B, C \in \mathsf{M}_n$ и $D \in \mathsf{M}_n^{inv}$, а для автомата $M_2 \in \mathsf{A}_{n,2}^{inv}$ – независимый выбор матриц $A \in \mathsf{M}_n$ и $B, C \in \mathsf{M}_n^{inv}$.

Следовательно,

$$|\mathsf{A}_{n,1}^{inv}| = |\mathsf{M}_n|^3 \cdot |\mathsf{M}_n^{inv}| \quad (5.23)$$

и

$$|\mathsf{A}_{n,2}^{inv}| = |\mathsf{M}_n| \cdot |\mathsf{M}_n^{inv}|^2. \quad (5.24)$$

Подставив (5.6) в (5.23) и (5.24) и воспользовавшись равенствами (5.21) и (5.22), получим (5.20).

Теорема доказана.

Положим

$$\nu_{n,i}^{inv} = |\mathsf{A}_{n,i}^{inv}| \cdot |\mathsf{A}_{n,i}|^{-1} \quad (i = 1,2).$$

Из теоремы 1 вытекает

Следствие 5.1. Для всех $n \in \mathbf{N}$

$$(n! \cdot (p-1)^n \cdot p^{-n^2})^i \le |\nu_{n,i}^{inv}| \le (1-p^{-n})^{n \cdot i} \quad (i = 1,2).$$

5.3. Конечно-автоматные характеристики исследуемых моделей.

Охарактеризуем основные нетривиальные подмножества множества автоматов $\mathsf{A}_{n,1}^{inv} \cup \mathsf{A}_{n,2}^{inv}$.

Обозначим через $\mathsf{D}_n^{(1)}$ множество всех диагональных матриц $X \in \mathsf{M}_n$, на главной диагонали которых расположены обратимые элементы кольца Z_{p^k}. Ясно, что

$$\mathsf{D}_n^{(1)} \subseteq \mathsf{M}_n^{inv}.$$

Положим

$$\mathsf{B}_{n,1}^{inv} = \{M_1 \in \mathsf{A}_{n,1}^{inv} \mid D \in \mathsf{D}_n^{(1)}\}$$

и

$$\mathsf{B}_{n,2}^{inv} = \{M_2 \in \mathsf{A}_{n,2}^{inv} \mid B, C \in \mathsf{D}_n^{(1)}\}.$$

Теорема 5.3. Для всех $n \in \mathbf{N}$

$$|\mathsf{B}_{n,i}^{inv}| = ((p-1)^n \cdot p^{(k-1-k\cdot n)\cdot n})^i \cdot |\mathsf{A}_{n,i}^{inv}| \quad (i = 1,2). \tag{5.25}$$

Доказательство. Для автомата $M_1 \in \mathsf{B}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, B, C \in \mathsf{M}_n$ и $D \in \mathsf{D}_n^{(1)}$, а для автомата $M_2 \in \mathsf{B}_{n,2}^{inv}$ – независимый выбор матриц $A \in \mathsf{M}_n$ и $B, C \in \mathsf{D}_n^{(1)}$. Следовательно,

$$|\mathsf{B}_{n,1}^{inv}| = |\mathsf{M}_n|^3 \cdot |\mathsf{D}_n^{(1)}| \tag{5.26}$$

и

$$|\mathsf{B}_{n,2}^{inv}| = |\mathsf{M}_n| \cdot |\mathsf{D}_n^{(1)}|^2. \tag{5.27}$$

Так как число обратимых элементов кольца Z_{p^k} равно $(p-1)\cdot p^{k-1}$, а для матрицы $X \in \mathsf{D}_n^{(1)}$ выбор диагональных элементов осуществляется независимо, то

$$|\mathsf{D}_n^{(1)}| = (p-1)^n \cdot p^{(k-1)\cdot n} = (p-1)^n \cdot p^{(k-1)\cdot n - k\cdot n^2} \cdot |\mathsf{M}_n|. \tag{5.28}$$

Подставив (5.28) в (5.26) и (5.27) и воспользовавшись равенствами (5.21) и (5.22), получим (5.25).

Теорема доказана.

Охарактеризуем теперь автоматы $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ в терминах теории автоматов [208].

Обозначим через $\mathsf{G}_{n,i}$ $(i = 1,2)$ множество всех автоматов $M_i \in \mathsf{A}_{n,i}$, у которых граф переходов – полный граф с петлями.

Положим

$$\mathsf{G}_{n,i}^{inv} = \mathsf{G}_{n,i} \cap \mathsf{A}_{n,i}^{inv} \quad (i = 1,2).$$

Теорема 5.4. Для всех $n \in \mathbf{N}$

$$\mathsf{G}_{n,2}^{inv} = \mathsf{A}_{n,2}^{inv} \tag{5.29}$$

и

$$((n!)\cdot(p-1)^n \cdot p^{-n^2})^2 \cdot |\mathsf{A}_{n,1}| \le |\mathsf{G}_{n,1}^{inv}| \le (1-p^{-n})^{2\cdot n} \cdot |\mathsf{A}_{n,1}|. \tag{5.30}$$

Доказательство. Для доказательства теоремы нам понадобится следующая лемма.

Лемма 5.2. Пусть $n \in \mathbf{N}$. Граф переходов автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ – полный граф с петлями тогда и только тогда, когда $B \in \mathsf{M}_n^{inv}$.

Доказательство. Пусть $B \in \mathsf{M}_n^{inv}$. Тогда для любых фиксированных состояний $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ и для любого входного символа $\mathbf{x} \in \mathbf{Z}_{p^k}^n$

$$\mathbf{q}' = A \circ \mathbf{q} \oplus B \circ \mathbf{x} \Leftrightarrow B \circ \mathbf{x} = \mathbf{q}' \ominus A \circ \mathbf{q} \Leftrightarrow \mathbf{x} = B^{-1} \circ (\mathbf{q}' \ominus A \circ \mathbf{q}).$$

Следовательно, в автомате $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ переход из любого состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ в любое состояние $\mathbf{q}' \in \mathbf{Z}_{p^k}^n$ осуществляется за один такт. Отсюда вытекает, что граф переходов автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ – полный граф с петлями.

Пусть $B \in \mathsf{M}_n^{non\_inv}$. Предположим, что граф переходов автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ – полный граф с петлями. Тогда для любого состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ и любых входных символов $\mathbf{x}_1, \mathbf{x}_2 \in \mathbf{Z}_{p^k}^n$ $(\mathbf{x}_1 \ne \mathbf{x}_2)$

$$B \circ \mathbf{x}_1 \oplus A \circ \mathbf{q} \ne B \circ \mathbf{x}_2 \oplus A \circ \mathbf{q} \Leftrightarrow B \circ (\mathbf{x}_1 \ominus \mathbf{x}_2) \ne \mathbf{0}.$$

Так как $B \in \mathsf{M}_n^{non\_inv}$, то система уравнений $B \circ \mathbf{u} = \mathbf{0}$ является совместной системой уравнений. Следовательно, она имеет решение $\mathbf{u}_0 \ne \mathbf{0}$.

Положим

$$\mathbf{x}_2 = \mathbf{x}_1 \oplus \mathbf{u}_0.$$

Тогда $\mathbf{x}_1 \ne \mathbf{x}_2$, но

$$B \circ (\mathbf{x}_1 \ominus \mathbf{x}_2) = \mathbf{0}.$$

Получено противоречие. Следовательно, предположение – ложное. Отсюда вытекает, что если $B \in \mathsf{M}_n^{non\_inv}$, то граф переходов автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ не является полным графом с петлями.

Лемма доказана.

Так как $B \in \mathsf{M}_n^{inv}$ для любого автомата $M_2 \in \mathsf{A}_{n,2}^{inv}$ (см. утверждение 5.13), то

$$\mathsf{G}_{n,2}^{inv} = \mathsf{A}_{n,2}^{inv},$$

что и требовалось показать.

Для автомата $M_1 \in \mathsf{G}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A,\ C \in \mathsf{M}_n$ и $B, D \in \mathsf{M}_n^{inv}$. Следовательно,

$$|\mathsf{G}_{n,1}^{inv}| = |\mathsf{M}_n|^2 \cdot |\mathsf{M}_n^{inv}|^2. \qquad (5.31)$$

Подставив (5.6) в (5.31) и воспользовавшись равенством (5.21), получим неравенства (5.30).

Теорема доказана.

Обозначим через $\mathsf{C}_{n,i}$ $(i = 1,2)$ множество всех перестановочных автоматов $M_i \in \mathsf{A}_{n,i}$.

Положим

$$\mathsf{C}_{n,i}^{inv} = \mathsf{C}_{n,i} \cap \mathsf{A}_{n,i}^{inv} \ \ (i = 1,2).$$

Теорема 5.5. Для всех $n \geq 2$

$$|\mathsf{C}_{n,i}^{inv}| \geq (n!\cdot(p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathsf{A}_{n,i}| \ \ (i = 1,2). \qquad (5.32)$$

Доказательство. Для доказательства теоремы нам понадобится следующая лемма.

Лемма 5.3. Если $A \in \mathsf{M}_n^{inv}$, то автомат $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ – перестановочный автомат.

Доказательство. Пусть $A \in \mathsf{M}_n^{inv}$. Предположим противное, т.е. что автомат $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ не является перестановочным автоматом.

Тогда существуют такие состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$ и входной символ $\mathbf{x} \in \mathbf{Z}_{p^k}^n$, что

$$A \circ \mathbf{q} \oplus B \circ \mathbf{x} = A \circ \mathbf{q}' \oplus B \circ \mathbf{x} \Leftrightarrow A \circ \mathbf{q}' = A \circ \mathbf{q} \Leftrightarrow A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0}.$$

Так как $A \in \mathsf{M}_n^{inv}$, то

$$A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \Leftrightarrow \mathbf{q}' \ominus \mathbf{q} = \mathbf{0} \Leftrightarrow \mathbf{q}' = \mathbf{q}.$$

Получено противоречие.

Следовательно, предположение – ложное. Отсюда вытекает, что если $A \in \mathsf{M}_n^{inv}$, то $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ – перестановочный автомат.

Лемма доказана.

Для автомата $M_1 \in \mathsf{C}_{n,1}^{inv}$ осуществляется независимый выбор матриц $B, C \in \mathsf{M}_n$ и $A, D \in \mathsf{M}_n^{inv}$, а для автомата $M_2 \in \mathsf{C}_{n,2}^{inv}$ – независимый выбор матриц $A, B, C \in \mathsf{M}_n^{inv}$.

Следовательно,

$$|\mathsf{C}_{n,1}^{inv}| \geq |\mathsf{M}_n|^2 \cdot |\mathsf{M}_n^{inv}|^2 \qquad (5.33)$$

и

$$|\mathsf{C}_{n,2}^{inv}| \geq |\mathsf{M}_n^{inv}|^3. \qquad (5.34)$$

Подставив (5.6) в (5.33) и (5.34) и воспользовавшись равенствами (5.21) и (5.22), получим (5.32).

Теорема доказана.

Обозначим через $\mathsf{D}_{n,i}$ $(i=1,2)$ – множество всех приведенных автоматов $M_i \in \mathsf{A}_{n,i}$.

Положим

$$\mathsf{D}_{n,i}^{inv} = \mathsf{D}_{n,i} \cap \mathsf{A}_{n,i}^{inv} \ (i=1,2).$$

Теорема 5.6. Для всех $n \geq 2$

$$|\mathsf{D}_{n,i}^{inv}| \geq (n!\cdot(p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathsf{A}_{n,i}| \ (i=1,2). \qquad (5.35)$$

Доказательство. Для доказательства теоремы нам понадобится следующие две леммы.

Лемма 5.4. Если $C \in \mathsf{M}_n^{inv}$, то автомат $M_1 \in \mathsf{A}_{n,1}$ – приведенный автомат, степень различимости которого равна 1.

Доказательство. Пусть $C \in \mathsf{M}_n^{inv}$. Предположим противное, т.е. что автомат $M_1 \in \mathsf{A}_{n,1}$ не является приведенным автоматом или степень его различимости не равна 1. Тогда существуют такие состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$, что для всех $\mathbf{x} \in \mathbf{Z}_{p^k}^n$

$$C \circ \mathbf{q} \oplus D \circ \mathbf{x} = C \circ \mathbf{q}' \oplus D \circ \mathbf{x} \Leftrightarrow C \circ \mathbf{q}' = C \circ \mathbf{q} \Leftrightarrow C \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0}.$$

Так как $C \in \mathsf{M}_n^{inv}$, то

$$C \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \Leftrightarrow \mathbf{q}' \ominus \mathbf{q} = \mathbf{0} \Leftrightarrow \mathbf{q}' = \mathbf{q}.$$

Получено противоречие.

Следовательно, предположение – ложное. Отсюда вытекает, что если $C \in \mathsf{M}_n^{inv}$, то $M_1 \in \mathsf{A}_{n,1}$ – приведенный автомат, степень различимости которого равна 1.

Лемма доказана.

Лемма 5.5. Если $A, C \in \mathsf{M}_n^{inv}$, то автомат $M_2 \in \mathsf{A}_{n,2}$ – приведенный автомат, степень различимости которого равна 1.

Доказательство. Пусть $A, C \in \mathsf{M}_n^{inv}$. Предположим противное, т.е. что автомат $M_2 \in \mathsf{A}_{n,2}$ не является приведенным автоматом или степень его различимости не равна 1. Тогда существуют такие состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$, что для всех $\mathbf{x} \in \mathbf{Z}_{p^k}^n$

$$C \circ (A \circ \mathbf{q}' \oplus B \circ \mathbf{x}) = C \circ (A \circ \mathbf{q} \oplus B \circ \mathbf{x}) \Leftrightarrow C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0}.$$

Так как $A, C \in \mathsf{M}_n^{inv}$, то $C \circ A \in \mathsf{M}_n^{inv}$. Следовательно,

$$C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \Leftrightarrow \mathbf{q}' \ominus \mathbf{q} = \mathbf{0} \Leftrightarrow \mathbf{q}' = \mathbf{q}.$$

Получено противоречие. Следовательно, предположение – ложное. Отсюда вытекает, что автомат $M_2 \in A_{n,2}$ – приведенный автомат, степень различимости которого равна 1.

Лемма доказана.

Для автомата $M_1 \in \mathsf{D}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, B \in \mathsf{M}_n$ и $C, D \in \mathsf{M}_n^{inv}$, а для автомата $M_2 \in \mathsf{D}_{n,2}^{inv}$ – независимый выбор матриц $A, B, C \in \mathsf{M}_n^{inv}$. Следовательно,

$$|\mathsf{D}_{n,1}^{inv}| \geq |\mathsf{M}_n|^2 \cdot |\mathsf{M}_n^{inv}|^2 \tag{5.36}$$

и

$$|\mathsf{D}_{n,2}^{inv}| \geq |\mathsf{M}_n^{inv}|^3. \tag{5.37}$$

Подставив (5.6) в (5.36) и (5.37) и воспользовавшись равенствами (5.21) и (5.22), получим (5.35).

Теорема доказана.

Обозначим через $\mathsf{E}_{n,i}$ $(i = 1,2)$ множество всех автоматов $M_i \in \mathsf{A}_{n,i}$, имеющих состояния-близнецы.

Положим

$$\mathsf{E}_{n,i}^{inv} = \mathsf{E}_{n,i} \cap \mathsf{A}_{n,i}^{inv} \quad (i = 1,2).$$

Теорема 5.7. Для всех $n \geq 2$

$$|\mathsf{E}_{n,1}^{inv}| \geq n! \cdot (p-1)^n \cdot p^{-n^2} \cdot (1-(1-p^{-n})^n)^2 \cdot |\mathsf{A}_{n,1}| \tag{5.38}$$

и

$$|\mathsf{E}_{n,2}^{inv}| \geq (1-(1-p^{-n})^n) \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathsf{A}_{n,2}|. \tag{5.39}$$

Доказательство. Для доказательства теоремы нам понадобятся следующие две утверждения.

Лемма 5.6. Если $A, C \in \mathsf{M}_n^{non\_inv}$ и система уравнений

$$\begin{cases} A \circ \mathbf{u} = \mathbf{0} \\ C \circ \mathbf{u} = \mathbf{0} \end{cases} \tag{5.40}$$

имеет ненулевое решение, то в автомате $M_1 \in \mathsf{A}_{n,1}$ существуют состояния-близнецы.

Доказательство. Пусть $A, C \in \mathsf{M}_n^{non\_inv}$. Состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$ автомата $M_1 \in \mathsf{A}_{n,1}$ являются близнецами тогда и только тогда, когда для любого входного символа $\mathbf{x} \in \mathbf{Z}_{p^k}^n$

$$\begin{cases} A \circ \mathbf{q}' \oplus B \circ \mathbf{x} = A \circ \mathbf{q} \oplus B \circ \mathbf{x} \\ C \circ \mathbf{q}' \oplus D \circ \mathbf{x} = C \circ \mathbf{q} \oplus D \circ \mathbf{x} \end{cases} \Leftrightarrow \begin{cases} A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \\ C \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \end{cases}. \tag{5.41}$$

Пусть $\mathbf{u}_0$ – ненулевое решение системы (5.40).

Положим

$$\mathbf{q}' = \mathbf{q} \oplus \mathbf{u}_0 .$$

Тогда $\mathbf{q}' \neq \mathbf{q}$ и состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ удовлетворяют условию (5.41). Следовательно, $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ – состояния-близнецы.

Лемма доказана.

Лемма 5.7. Если $A \in \mathsf{M}_n^{non\_inv}$, то в автомате $M_2 \in \mathsf{A}_{n,2}$ существуют состояния-близнецы.

Доказательство. Пусть $A \in \mathsf{M}_n^{non\_inv}$. Состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$ автомата $M_2 \in \mathsf{A}_{n,2}$ являются близнецами тогда и только тогда, когда для любого входного символа $\mathbf{x} \in \mathbf{Z}_{p^k}^n$

$$\begin{cases} A \circ \mathbf{q}' \oplus B \circ \mathbf{x} = A \circ \mathbf{q} \oplus B \circ \mathbf{x} \\ C \circ (A \circ \mathbf{q}' \oplus B \circ \mathbf{x}) = C \circ (A \circ \mathbf{q} \oplus B \circ \mathbf{x}) \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \\ C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0} \end{cases} \Leftrightarrow A \circ (\mathbf{q}' \ominus \mathbf{q}) = \mathbf{0}. \qquad (5.42)$$

Так как $A \in \mathsf{M}_n^{non\_inv}$, то уравнение

$$A \circ \mathbf{u} = \mathbf{0}$$

имеет ненулевое решение $\mathbf{u}_0$. Положим

$$\mathbf{q}' = \mathbf{q} \oplus \mathbf{u}_0 .$$

Тогда $\mathbf{q}' \neq \mathbf{q}$ и состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ удовлетворяют условию (5.42). Следовательно, $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ состояния-близнецы.

Лемма доказана.

Из (5.6) вытекает, что

$$(1-(1-p^{-n})^n)\cdot|\mathsf{M}_n| \le |\mathsf{M}_n^{non\_inv}| \le (1-n!\cdot(p-1)^n \cdot p^{-n^2})\cdot|\mathsf{M}_n|. \qquad (5.43)$$

Для автомата $M_1 \in \mathsf{E}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, C \in \mathsf{M}_n^{non\_inv}$, $B \in \mathsf{M}_n$ и $D \in \mathsf{M}_n^{inv}$, а для автомата $M_2 \in \mathsf{E}_{n,2}^{inv}$ – независимый выбор матриц $A \in \mathsf{M}_n^{non\_inv}$ и $B, C \in \mathsf{M}_n^{inv}$. Следовательно,

$$|\mathsf{E}_{n,1}^{inv}| \ge |\mathsf{M}_n^{non\_inv}|^2 \cdot |\mathsf{M}_n| \cdot |\mathsf{M}_n^{inv}| \qquad (5.44)$$

и

$$|\mathsf{E}_{n,2}^{inv}| \ge |\mathsf{M}_n^{non\_inv}| \cdot |\mathsf{M}_n^{inv}|^2. \qquad (5.45)$$

Подставив (5.6) и (5.43) в (5.44) и (5.45) и воспользовавшись равенствами (5.21) и (5.22), получим (5.38) и (5.39).

Теорема доказана.

Обозначим через $\mathsf{D}_n^{(2)}$ множество всех диагональных матриц $X \in \mathsf{M}_n$, на главной диагонали которых расположены необратимые элементы кольца Z_{p^k}. Ясно, что

$$\mathsf{D}_n^{(2)} \subseteq \mathsf{M}_n^{non\_inv}.$$

Положим

$$\mathsf{F}_{n,1}^{inv} = \{M_1 \in \mathsf{E}_{n,1}^{inv} \mid A, C \in \mathsf{D}_n^{(2)}\}$$

и

$$\mathsf{F}_{n,2}^{inv} = \{M_2 \in \mathsf{E}_{n,2}^{inv} \mid A \in \mathsf{D}_n^{(2)}\}.$$

Теорема 5.8. Для всех $n \in \mathbf{N}$

$$|\mathsf{F}_{n,1}^{inv}| \geq n! \cdot (p-1)^n \cdot p^{-n^2} \cdot p^{2 \cdot n \cdot (k-1-k \cdot n)} \cdot |\mathsf{A}_{n,1}| \tag{5.46}$$

и

$$|\mathsf{F}_{n,2}^{inv}| \geq p^{n \cdot (k-1-k \cdot n)} \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathsf{A}_{n,2}|. \tag{5.47}$$

Доказательство. Для автомата $M_1 \in \mathsf{F}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, C \in \mathsf{D}_n^{(2)}$, $B \in \mathsf{M}_n$ и $D \in \mathsf{M}_n^{inv}$, а для автомата $M_2 \in \mathsf{F}_{n,2}^{inv}$ – независимый выбор матриц $A \in \mathsf{D}_n^{(2)}$ и $B, C \in \mathsf{M}_n^{inv}$. Следовательно,

$$|\mathsf{F}_{n,1}^{inv}| \geq |\mathsf{D}_n^{(2)}|^2 \cdot |\mathsf{M}_n| \cdot |\mathsf{M}_n^{inv}| \tag{5.48}$$

и

$$|\mathsf{F}_{n,2}^{inv}| \geq |\mathsf{D}_n^{(2)}| \cdot |\mathsf{M}_n^{inv}|^2. \tag{5.49}$$

Число необратимых элементов кольца Z_{p^k} равно

$$p^k - (p-1) \cdot p^{k-1} = p^{k-1}.$$

Для матрицы $X \in \mathsf{D}_n^{(2)}$ выбор диагональных элементов осуществляется независимо. Следовательно,

$$|\mathsf{D}_n^{(2)}| = p^{(k-1) \cdot n} = p^{(k-1) \cdot n - k \cdot n^2} \cdot |\mathsf{M}_n|. \tag{5.50}$$

Подставив (5.6) и (5.50) в (5.48) и (5.49) и воспользовавшись равенствами (5.21) и (5.22), получим (5.46) и (5.47).

Теорема доказана.

5.4. Эквивалентность линейных автоматов и их состояний.

Исследуем эквивалентность автоматов $M_i, M_i' \in \mathsf{A}_{n,i}$ $(i = 1,2)$, где

$$(M_1', \mathbf{q}_0): \begin{cases} \mathbf{q}'_{t+1} = A' \circ \mathbf{q}'_t \oplus B' \circ \mathbf{x}_{t+1} \\ \mathbf{y}'_{t+1} = C' \circ \mathbf{q}'_t \oplus D' \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+) \tag{5.51}$$

и

$$(M_2', \mathbf{q}_0): \begin{cases} \mathbf{q}'_{t+1} = A' \circ \mathbf{q}'_t \oplus B' \circ \mathbf{x}_{t+1} \\ \mathbf{y}'_{t+1} = C' \circ \mathbf{q}'_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{5.52}$$

Пусть $O \in \mathsf{M}_n$ – нулевая матрица.

Индукцией по t несложно показать, что для автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ истинны равенства

$$\mathbf{q}_{t+1} = A^{t+1} \circ \mathbf{q}_0 \oplus \overset{t}{\underset{i=1}{\oplus}} A^{t+1-i} \circ B \circ \mathbf{x}_i \oplus B \circ \mathbf{x}_{t+1} \ (t \in \mathbf{Z}_+). \qquad (5.53)$$

Теорема 5.9. Инициальные автоматы $(M_1, \mathbf{q}_0)$ и $(M_1', \mathbf{q}_0')$ $(M_1, M_1' \in \mathsf{A}_{n,1})$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

а) $D = D'$;

б) $C' \circ \mathbf{q}_0' \Theta C \circ \mathbf{q}_0 = \mathbf{0}$;

в) для любого состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ существует такое состояние $\mathbf{q}_0' \in \mathbf{Z}_{p^k}^n$ и, наоборот, для любого состояния $\mathbf{q}_0' \in \mathbf{Z}_{p^k}^n$ существует такое состояние $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, что

$$C' \circ (A')^t \circ \mathbf{q}_0' \Theta C \circ A^t \circ \mathbf{q}_0 = \mathbf{0} \ \ (t = 1,\ldots,2 \cdot p^{kn} - 2);$$

г) $C' \circ (A')^j \circ B' \Theta C \circ A^j \circ B = O$ $(j = 1,\ldots,2 \cdot p^{k \cdot n} - 3)$;

д) $C' \circ B' \Theta C \circ B = O$.

Доказательство. Операторы, реализуемые инициальными автоматами $(M_1, \mathbf{q}_0)$ и $(M_1', \mathbf{q}_0')$ равны тогда и только тогда, когда равенства

$$\mathbf{y}_t = \mathbf{y}_t' \ \ (t = 1,\ldots,2 \cdot p^{k \cdot n} - 1)$$

истинны для любой входной последовательности $\mathbf{x}_1 \ldots \mathbf{x}_t \in (\mathbf{Z}_{p^k}^n)^+$.

Пусть $t = 1$.

Из 2-го уравнения систем (5.18) и (5.51) вытекает, что

$$\mathbf{y}_1' = \mathbf{y}_1 \Leftrightarrow C' \circ \mathbf{q}_0' \oplus D' \circ \mathbf{x}_1 = C \circ \mathbf{q}_0 \oplus D \circ \mathbf{x}_1 \Leftrightarrow$$

$$\Leftrightarrow (D' \Theta D) \circ \mathbf{x}_1 = C' \circ \mathbf{q}_0' \Theta C \circ \mathbf{q}_0. \qquad (5.54)$$

для любого входного символа $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$.

Так как для фиксированных значений матриц $D', D, C', C \in \mathsf{M}_n$ и начальных состояний $\mathbf{q}_0', \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ равенство (5.54) истинно для всех значений входного символа $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$, то

$$D' \Theta D = O,$$

т.е.

$$D' = D.$$

Следовательно, условие а) выполнено.

Отсюда вытекает, что равенство (5.54) имеет вид

$$C' \circ \mathbf{q}'_0 \Theta C \circ \mathbf{q}_0 = \mathbf{0},$$

т.е. условие б) выполнено.

Пусть $t = 2,\ldots,2 \cdot p^{k \cdot n} - 1$.

Из 2-го уравнения систем (5.18) и (5.51) и равенства

$$D' = D$$

вытекает, что

$$\mathbf{y}'_t = \mathbf{y}_t \Leftrightarrow C' \circ \mathbf{q}'_{t-1} \oplus D \circ \mathbf{x}_t = C \circ \mathbf{q}_{t-1} \oplus D \circ \mathbf{x}_t \Leftrightarrow$$

$$\Leftrightarrow C' \circ \mathbf{q}'_{t-1} = C \circ \mathbf{q}_{t-1} \qquad (5.55)$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbf{Z}_{p^k}^{n \cdot t}$.

Воспользуемся в (5.55) равенством (5.53). Получим, что

$$\mathbf{y}'_t = \mathbf{y}_t \Leftrightarrow C' \circ ((A')^{t-1} \circ \mathbf{q}'_0 \oplus \bigoplus_{i=1}^{t-2} (A')^{t-1-i} \circ B' \circ \mathbf{x}_i \oplus B' \circ \mathbf{x}_{t-1}) =$$

$$= C \circ (A^{t-1} \circ \mathbf{q}_0 \oplus \bigoplus_{i=1}^{t-2} A^{t-1-i} \circ B \circ \mathbf{x}_i \oplus B \circ \mathbf{x}_{t-1}) \Leftrightarrow$$

$$\Leftrightarrow (C' \circ (A')^{t-1} \circ \mathbf{q}'_0 \Theta C \circ A^{t-1} \circ \mathbf{q}_0) \oplus$$

$$\oplus \bigoplus_{i=1}^{t-2} (C' \circ (A')^{t-1-i} \circ B' \Theta C \circ A^{t-1-i} \circ B) \circ \mathbf{x}_i \oplus$$

$$\oplus (C' \circ B' \Theta C \circ B) \circ \mathbf{x}_{t-1} = \mathbf{0} \qquad (5.56)$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbf{Z}_{p^k}^{n \cdot t}$.

Положив в (5.56)

$$\mathbf{x}_1 \ldots \mathbf{x}_{t-1} = \underbrace{\mathbf{0} \ldots \mathbf{0}}_{t-1},$$

получим

$$C' \circ (A')^t \circ \mathbf{q}'_0 \Theta C \circ A^t \circ \mathbf{q}_0 = \mathbf{0} \quad (t = 1,\ldots,2 \cdot p^{kn} - 2),$$

т.е. условие в) выполнено.

Следовательно, равенство (5.56) принимает вид

$$\bigoplus_{i=1}^{t-2} (C' \circ (A')^{t-1-i} \circ B' \Theta C \circ A^{t-1-i} \circ B) \circ \mathbf{x}_i \oplus$$

$$\oplus (C' \circ B' \Theta C \circ B) \circ \mathbf{x}_{t-1} = \mathbf{0}. \qquad (5.57)$$

Для $i=1,\ldots,t-2$ последовательно положим в (5.57)

$$\mathbf{x}_1\ldots\mathbf{x}_{t-1}=\underbrace{\mathbf{0}\ldots\mathbf{0}}_{i-1}\mathbf{x}_i\underbrace{\mathbf{0}\ldots\mathbf{0}}_{t-i-2}\mathbf{0}\mathbf{0}.$$

Получим, что для всех $i=1,\ldots,t-2$ равенство

$$(C'\circ(A')^{t-1-i}\circ B'\Theta C\circ A^{t-1-i}\circ B)\circ\mathbf{x}_i=\mathbf{0}$$

истинно при всех $\mathbf{x}_i\in\mathbf{Z}^n_{p^k}$.

Следовательно,

$$C'\circ(A')^j\circ B'\Theta C\circ A^j\circ B=O\ \ (j=1,\ldots,2\cdot p^{k\cdot n}-3), \qquad (5.58)$$

т.е. условие г) выполнено.

Подставим (5.58) в (5.57). Получим что равенство

$$(C'\circ B'\Theta C\circ B)\circ\mathbf{x}_{t-1}=\mathbf{0}$$

истинно при всех $\mathbf{x}_{t-1}\in\mathbf{Z}^n_{p^k}$.

Следовательно,

$$C'\circ B'\Theta C\circ B=\mathbf{0},$$

т.е. условие д) выполнено.

Теорема доказана.

Теорема 5.10. Инициальные автоматы $(M_2,\mathbf{q}_0)$ и $(M'_2,\mathbf{q}'_0)$ $(M_2,M'_2\in\mathsf{A}_{n,2})$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

а) $C'\circ B'\Theta C\circ B=O$;

б) для любого состояния $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$ существует такое состояние $\mathbf{q}'_0\in\mathbf{Z}^n_{p^k}$ и, наоборот, для любого состояния $\mathbf{q}'_0\in\mathbf{Z}^n_{p^k}$ существует такое состояние $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$, что

$$C'\circ(A')^t\circ\mathbf{q}'_0\Theta C\circ A^t\circ\mathbf{q}_0=\mathbf{0}\ \ (t=1,\ldots,2\cdot p^{kn}-1);$$

в) $C'\circ(A')^j\circ B'\Theta C\circ A^j\circ B=O\ \ (j=1,\ldots,2\cdot p^{k\cdot n}-2)$.

Доказательство. Операторы, реализуемые инициальными автоматами $(M_2,\mathbf{q}_0)$ и $(M'_2,\mathbf{q}'_0)$, равны тогда и только тогда, когда равенства

$$\mathbf{y}_t=\mathbf{y}'_t\ \ (t=1,\ldots,2\cdot p^{k\cdot n}-1)$$

истинны для любой входной последовательности $\mathbf{x}_1\ldots\mathbf{x}_t\in(\mathbf{Z}^n_{p^k})^+$.

Пусть $t=1$.

Из 2-го уравнения систем (5.19) и (5.52) вытекает, что

$$\mathbf{y}'_1 = \mathbf{y}_1 \Leftrightarrow C' \circ \mathbf{q}'_1 = C \circ \mathbf{q}_1 \Leftrightarrow$$

$$\Leftrightarrow C' \circ (A' \circ \mathbf{q}'_0 \oplus B' \circ \mathbf{x}_1) = C \circ (A \circ \mathbf{q}_0 \oplus B \circ \mathbf{x}_1) \Leftrightarrow$$

$$\Leftrightarrow (C' \circ B' \Theta C \circ B) \circ \mathbf{x}_1 = C \circ A \circ \mathbf{q}_0 \Theta C' \circ A' \circ \mathbf{q}'_0 \qquad (5.59)$$

для любого входного символа $\mathbf{x}_1 \in \mathbf{Z}^n_{p^k}$.

Так как для фиксированных значений матриц $A, A', B, B', C, C' \in \mathsf{M}_n$ и начальных состояний $\mathbf{q}_0, \mathbf{q}'_0 \in \mathbf{Z}^n_{p^k}$ равенство (5.59) истинно для всех $\mathbf{x}_1 \in \mathbf{Z}^n_{p^k}$, то

$$\begin{cases} C' \circ B' \Theta C \circ B = O \\ C \circ A \circ \mathbf{q}_0 \Theta C' \circ A' \circ \mathbf{q}'_0 = \mathbf{0} \end{cases},$$

т.е. при $t = 1$ выполнено и условие а), и условие б).

Пусть $t = 2, \ldots, 2 \cdot p^{k \cdot n} - 1$.

Из 2-го уравнения систем (5.19) и (5.52) вытекает, что

$$\mathbf{y}'_t = \mathbf{y}_t \Leftrightarrow C' \circ \mathbf{q}'_t = C \circ \mathbf{q}_t \qquad (5.60)$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbf{Z}^{n \cdot t}_{p^k}$.

Воспользуемся в (5.60) равенством (5.53). Получим, что

$$\mathbf{y}'_t = \mathbf{y}_t \Leftrightarrow C' \circ ((A')^t \circ \mathbf{q}'_0 \oplus \mathop{\oplus}_{i=1}^{t-1} (A')^{t-i} \circ B' \circ \mathbf{x}_i \oplus B' \circ \mathbf{x}_t) =$$

$$= C \circ (A^t \circ \mathbf{q}_0 \oplus \mathop{\oplus}_{i=1}^{t-1} A^{t-i} \circ B \circ \mathbf{x}_i \oplus B \circ \mathbf{x}_t) \Leftrightarrow$$

$$\Leftrightarrow (C' \circ (A')^t \circ \mathbf{q}'_0 \Theta C \circ A^t \circ \mathbf{q}_0) \oplus$$

$$\oplus \mathop{\oplus}_{i=1}^{t-1} (C' \circ (A')^{t-i} \circ B' \Theta C \circ A^{t-i} \circ B) \circ \mathbf{x}_i = \mathbf{0} \qquad (5.61)$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbf{Z}^{n \cdot t}_{p^k}$.

Положив в (5.61)

$$\mathbf{x}_1 \ldots \mathbf{x}_{t-1} = \underbrace{\mathbf{0} \ldots \mathbf{0}}_{t-1},$$

получим

$$C' \circ (A')^t \circ \mathbf{q}'_0 \Theta C \circ A^t \circ \mathbf{q}_0 = \mathbf{0},$$

т.е. при $t = 2, \ldots, 2 \cdot p^{kn} - 1$ условие в) выполнено.

Для $i=1,\ldots,t-1$ последовательно положим в (5.61)

$$\mathbf{x}_1\ldots\mathbf{x}_{t-1}=\underbrace{\mathbf{0}\ldots\mathbf{0}}_{i-1}\mathbf{x}_i\underbrace{\mathbf{0}\ldots\mathbf{0}}_{t-i-1}\mathbf{0}.$$

Получим, что для всех $i=1,\ldots,t-1$ равенство

$$(C'\circ(A')^{t-i}\circ B'\Theta C\circ A^{t-i}\circ B)\circ\mathbf{x}_i=\mathbf{0}$$

истинно при всех $\mathbf{x}_i\in\mathbf{Z}^n_{p^k}$.

Следовательно,

$$C'\circ(A')^j\circ B'\Theta C\circ A^j\circ B=O\ \ (j=1,\ldots,2\cdot p^{k\cdot n}-2),$$

т.е. условие в) выполнено.

Теорема доказана.

Выделим специальный случай теорем 5.9 и 5.10, когда

$$M_i=M_i'\ \ (i=1,2).$$

В этом случае теоремы 5.9 и 5.10 устанавливают критерии эквивалентности состояний $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$ и $\mathbf{q}_0'\in\mathbf{Z}^n_{p^k}$ автомата $M_i\ \ (i=1,2)$.

При этом операторы, реализуемые инициальными автоматами $(M_i,\mathbf{q}_0)$ и $(M_i,\mathbf{q}_0')$ равны тогда и только тогда, когда равенства

$$\mathbf{y}_t=\mathbf{y}_t'\ \ (t=1,\ldots,p^{k\cdot n}-1)$$

истинны для любой входной последовательности $\mathbf{x}_1\ldots\mathbf{x}_t\in(\mathbf{Z}^n_{p^k})^+$.

Поэтому критерии эквивалентности состояний $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$ и $\mathbf{q}_0'\in\mathbf{Z}^n_{p^k}$ автомата $M_i\ \ (i=1,2)$ имеют следующий вид.

Следствие 5.2. Состояния $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$ и $\mathbf{q}_0'\in\mathbf{Z}^n_{p^k}$ автомата $M_1\in\mathsf{A}_{n,1}$ эквивалентны друг другу тогда и только тогда, когда выполнены следующие два условия:

а) $C\circ(\mathbf{q}_0'\Theta\mathbf{q}_0)=\mathbf{0}$;

б) для всех значений $t=1,\ldots,p^{kn}-2$

$$C\circ(A)^t\circ(\mathbf{q}_0'\Theta\mathbf{q}_0)=\mathbf{0}.$$

Следствие 5.3. Состояния $\mathbf{q}_0\in\mathbf{Z}^n_{p^k}$ и $\mathbf{q}_0'\in\mathbf{Z}^n_{p^k}$ автомата $M_2\in\mathsf{A}_{n,2}$ эквивалентны друг другу тогда и только тогда, когда

$$C\circ(A)^t\circ(\mathbf{q}_0'\Theta\mathbf{q}_0)=\mathbf{0}.$$

для всех значений $t=1,\ldots,p^{kn}-2$.

Отметим, что из следствий 5.2 и 5.3 непосредственно вытекает, что истинны следующие два утверждение, представляющее собой часть, соответственно, леммы 5.4 и леммы 5.5.

Следствие 5.4. Если $C \in \mathsf{M}_n^{inv}$, то автомат $M_1 \in \mathsf{A}_{n,1}$ – приведенный автомат.

Следствие 5.5. Если $A, C \in \mathsf{M}_n^{inv}$, то автомат $M_2 \in \mathsf{A}_{n,2}$ – приведенный автомат.

5.5. Задачи идентификации для автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$.

Рассмотрим решение задач идентификации для автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$ в предположении, что экспериментатор полностью управляет входом, а также полностью наблюдает выход автомата M_i.

Выбор таких предположений обоснован тем, что они характеризуют внутреннюю сложность задач идентификации. Ясно, что если эти предположения заменить более слабыми, то сложность решения задач идентификации существенно возрастет.

Рассмотрим вначале задачу параметрической идентификации для автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$, в предположении, что экспериментатор имеет возможность также управлять инициализацией автомата M_i, т.е. проводить с автоматом M_i кратный эксперимент требуемой кратности.

Теорема 5.11. Пусть $M_1 \in \mathsf{A}_{n,1}$ и экспериментатор полностью управляет входом и инициализацией автомата M_1, а также полностью наблюдает выход автомата M_1. Тогда:

1) каждая из матриц C и D идентифицируется единственным образом посредством n-кратного эксперимента высоты 1;

2) если $C \in \mathsf{M}_n^{inv}$, то идентификация каждой из матриц A и B сводится к решению n систем линейных уравнений n-го порядка над кольцом Z_{p^k}, построенных в результате n-кратного эксперимента высоты 2.

Доказательство. Пусть $M_1 \in \mathsf{A}_{n,1}$ и экспериментатор полностью управляет входом и инициализацией автомата M_1, а также полностью наблюдает его выход.

Положим

$$\mathbf{q}_0 = \mathbf{0}$$

и

$$\mathbf{x}_1 = \mathbf{e}_i \quad (i = 1, \ldots, n),$$

где

$$\mathbf{e}_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})^T \quad (i = 1, \ldots, n).$$

Из 2-го уравнения системы (5.18) находим, что

$$\mathbf{y}_1 = D \circ \mathbf{e}_i .$$

Так как $D \circ \mathbf{e}_i \ \ (i = 1, \ldots, n)$ – это i-й столбец матрицы D, то матрица D идентифицируется в результате следующего n-кратного эксперимента высоты 1

$$\{(\mathbf{q}_0 = \mathbf{0}, \mathbf{x}_1 = \mathbf{e}_i) \mid i = 1, \ldots, n\},$$

что и требовалось показать.

Положим

$$\mathbf{q}_0 = \mathbf{e}_i \quad (i = 1, \ldots, n)$$

и

$$\mathbf{x}_1 = \mathbf{0} .$$

Из 2-го уравнения системы (5.18) находим, что

$$\mathbf{y}_1 = C \circ \mathbf{e}_i .$$

Так как $C \circ \mathbf{e}_i \ (i = 1, \ldots, n)$ – это i-й столбец матрицы C, то матрица C идентифицируется в результате следующего n-кратного эксперимента высоты 1

$$\{(\mathbf{q}_0 = \mathbf{e}_i, \mathbf{x}_1 = \mathbf{0}) \mid i = 1, \ldots, n\},$$

что и требовалось показать.

Пусть $C \in M_n^{inv}$. Положим

$$\mathbf{q}_0 = \mathbf{e}_i \quad (i = 1, \ldots, n)$$

и

$$\mathbf{x}_1 = \mathbf{0} .$$

Из 1-го уравнения системы (5.18) находим, что

$$\mathbf{q}_1 = A \circ \mathbf{e}_i .$$

Положив теперь

$$\mathbf{x}_2 = \mathbf{0},$$

получим

$$\mathbf{y}_2 = C \circ (A \circ \mathbf{e}_i) \Leftrightarrow C^{-1} \circ \mathbf{y}_2 = A \circ \mathbf{e}_i .$$

Так как $A \circ \mathbf{e}_i \ \ (i = 1, \ldots, n)$ – это i-й столбец матрицы A, то идентификация матрицы A сводится к решению n систем линейных уравнений n-го порядка над кольцом Z_{p^k}, построенных в результате следующего n-кратного эксперимента высоты 2

$$\{(\mathbf{q}_0 = \mathbf{e}_i, \mathbf{x}_1 \mathbf{x}_2 = \mathbf{00}) \mid i = 1, \ldots, n\},$$

что и требовалось показать.

Положим

$$\mathbf{q}_0 = \mathbf{0}$$

и

$$\mathbf{x}_1 = \mathbf{e}_i \quad (i = 1, \ldots, n).$$

Из 1-го уравнения системы (5.18) находим, что

$$\mathbf{q}_1 = B \circ \mathbf{e}_i.$$

Положив теперь

$$\mathbf{x}_2 = \mathbf{0},$$

получим

$$\mathbf{y}_2 = C \circ (B \circ \mathbf{e}_i) \Leftrightarrow C^{-1} \circ \mathbf{y}_2 = B \circ \mathbf{e}_i.$$

Так как $B \circ \mathbf{e}_i \ \ (i = 1, \ldots, n)$ – это i-й столбец матрицы B, то идентификация матрицы B сводится к решению n систем линейных уравнений n-го порядка над кольцом Z_{p^k}, построенных в результате следующего n-кратного эксперимента высоты 2

$$\{(\mathbf{q}_0 = \mathbf{0}, \mathbf{x}_1\mathbf{x}_2 = \mathbf{e}_i\,\mathbf{0}) \mid i = 1, \ldots, n\},$$

что и требовалось показать.

Теорема доказана.

Рассмотрим теперь, как изменяется сложность идентификации матриц A и B автомата $M_1 \in \mathsf{A}_{n,1}$ в случае, когда $C \in \mathsf{M}_n^{non\_inv}$.

Поиск возможных кандидатов на матрицу A сводится к решению n систем линейных уравнений

$$\mathbf{y}_2 = C \circ (A \circ \mathbf{e}_i) \ \ (i = 1, \ldots, n), \tag{5.62}$$

построенных в результате n-кратного эксперимента высоты 2

$$\{(\mathbf{q}_0 = \mathbf{e}_i, \mathbf{x}_1\mathbf{x}_2 = \mathbf{00}) \mid i = 1, \ldots, n\},$$

а поиск возможных кандидатов на матрицу B сводится к решению n систем линейных уравнений

$$\mathbf{y}_2 = C \circ (B \circ \mathbf{e}_i) \quad (i = 1, \ldots, n), \tag{5.63}$$

построенных в результате n-кратного эксперимента высоты 2

$$\{(\mathbf{q}_0 = \mathbf{0}, \mathbf{x}_1\mathbf{x}_2 = \mathbf{e}_i\,\mathbf{0}) \mid i = 1, \ldots, n\}.$$

Каждая из систем (5.62) и (5.63) является совместной системой линейных уравнений, число решений которой может быть достаточно большим (см. утверждение 5.11).

Поэтому естественно возникает задача выделения истинных значений матриц A и B.

С помощью равенства (5.53) представим 2-е уравнение системы (5.18) в виде

$$\mathbf{y}_{i+1} = C \circ (A^i \circ \mathbf{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i) \oplus D \circ \mathbf{x}_{i+1} \ (i \in \mathbf{N}). \qquad (5.64)$$

Из (5.64) вытекает, что идентификация матриц A и B сводится к решению при известных матрицах C и D систем нелинейных уравнений

$$C \circ (A^i \circ \mathbf{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i) = \mathbf{y}_{i+1} \Theta D \circ \mathbf{x}_{i+1} \qquad (5.65)$$

для всех $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Следовательно, выделение истинных значений матриц A и B сводится к выделению тех решений систем (5.62) и (5.63), которые являются решениями систем нелинейных уравнений (5.65) .

Рассмотрим теперь решение задачи параметрической идентификации для автомата $M_2 \in \mathsf{A}_{n,2}$.

С помощью равенства (5.53) представим 2-е уравнение системы (5.19) в виде

$$\mathbf{y}_{i+1} = C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \bigoplus_{j=0}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_{j+1} \oplus B \circ \mathbf{x}_{i+1}) \ \ (i \in \mathbf{Z}_+). \qquad (5.66)$$

Из (5.66) вытекает, что решение задачи параметрической идентификации для автомата $M_2 \in \mathsf{A}_{n,2}$ сводится к решению относительно матриц A, B и C системы нелинейных уравнений

$$C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \bigoplus_{j=0}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_{j+1} \oplus B \circ \mathbf{x}_{i+1}) = \mathbf{y}_{i+1} \ \ (i = 1, \ldots, p^{n \cdot k} - 1) \qquad (5.67)$$

для всех $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Таким образом, задача параметрической идентификации для автомата $M_2 \in \mathsf{A}_{n,2}$ значительно сложнее чем задача параметрической идентификации для автомата $M_1 \in \mathsf{A}_{n,1}$.

Рассмотрим теперь решение задачи идентификации начального состояния автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1, 2)$.

Предположим, что экспериментатору известны параметры модели (т.е. матрицы A, B, C и D для автомата $M_1 \in \mathsf{A}_{n,1}$ и матрицы A, B и C для автомата $M_2 \in \mathsf{A}_{n,2}$), однако экспериментатор не может управлять этими параметрами.

Выбор таких предположений обоснован тем, что они характеризуют внутреннюю сложность задачи идентификации начального состояния автомата, поскольку при их ослаблении сложность решения задачи иденти-

фикации начального состояния существенно возрастает, так как при этом возникает тот или иной вариант задачи построения контрольного эксперимента с автоматом.

Пусть $M_1 \in \mathsf{A}_{n,1}$.

Положив $t = 0$ во 2-м уравнении системы (5.18), получим

$$C \circ \mathbf{q}_0 = \mathbf{y}_1 \Theta D \circ \mathbf{x}_1. \qquad (5.68)$$

Предположим, что $C \in \mathsf{M}_n^{inv}$.

Из (5.68) вытекает, что

$$\mathbf{q}_0 = C^{-1} \circ (\mathbf{y}_1 \Theta D \circ \mathbf{x}_1).$$

Таким образом, если $C \in \mathsf{M}_n^{inv}$, то идентификация начального состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_1 \in \mathsf{A}_{n,1}$ осуществляется однозначно (так как M_1 – приведенный автомат, что вытекает из леммы 5.4) и сводится к решению системы линейных уравнений (5.68), полученной в результате простого эксперимента длины 1.

Предположим, что $C \in \mathsf{M}_n^{non\_inv}$.

Тогда решение системы (5.68) дает возможность найти только множество допустимых кандидатов на начальное состояние $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_1 \in \mathsf{A}_{n,1}$, которое может быть значительно шире класса эквивалентных состояний.

Ясно, что идентификация начального состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_1 \in \mathsf{A}_{n,1}$ с точностью до класса эквивалентных состояний в случае, когда $C \in \mathsf{M}_n^{non\_inv}$ сводится к решению при известных матрицах A, B, C и D систем линейных уравнений (5.65) для всех $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Пусть $M_2 \in \mathsf{A}_{n,2}$.

Положив $t = 0$ во 2-м уравнении системы (5.19), получим

$$C \circ A \circ \mathbf{q}_0 = \mathbf{y}_1 \Theta C \circ B \circ \mathbf{x}_1. \qquad (5.69)$$

Предположим, что $A, C \in \mathsf{M}_n^{inv}$.

Из (5.69) вытекает, что

$$\mathbf{q}_0 = A^{-1} \circ C^{-1} \circ (\mathbf{y}_1 \Theta C \circ B \circ \mathbf{x}_1).$$

Таким образом, если $A, C \in \mathsf{M}_n^{inv}$, то идентификация начального состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_2 \in \mathsf{A}_{n,2}$ осуществляется однозначно (так как M_2 – приведенный автомат, что вытекает из леммы 5.5) и сводится к решению системы линейных уравнений, полученной в результате простого эксперимента длины 1.

Предположим, что $A \in \mathsf{M}_n^{non\_inv}$ или $C \in \mathsf{M}_n^{non\_inv}$.

Тогда решение системы (5.69) дает возможность найти только множество допустимых кандидатов на начальное состояние $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_2 \in \mathsf{A}_{n,2}$, которое может быть значительно шире класса эквивалентных состояний.

Ясно, что идентификация начального состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M_2 \in \mathsf{A}_{n,2}$ с точностью до класса эквивалентных состояний в случае когда $A \in \mathsf{M}_n^{non\_inv}$ или $C \in \mathsf{M}_n^{non\_inv}$ сводится к решению при известных матрицах A, B и C систем линейных уравнений (5.67) для всех $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

5.6. Неподвижные точки автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$.

Неподвижной точкой словарной функции $f : X^+ \to X^+$ называется такое слово $u \in X^+$, что

$$f(u) = u.$$

Обозначим через $S_{fxd}(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ множество всех неподвижных точек словарной функции

$$f_{(M,\mathbf{q}_0)} : (\mathbf{Z}_{p^k}^n)^+ \to (\mathbf{Z}_{p^k}^n)^+,$$

реализуемой инициальным автоматом $(M, \mathbf{q}_0)$.

Положим

$$S_{fxd}^{(t+1)}(M, \mathbf{q}_0) = S_{fxd}(M, \mathbf{q}_0) \cap (\mathbf{Z}_{p^k}^n)^{t+1} \quad (t \in \mathbf{Z}_+).$$

Ясно, что для любого инициального автомата $(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$, $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ истинно равенство

$$S_{fxd}(M, \mathbf{q}_0) = \bigcup_{t=0}^{\infty} S_{fxd}^{(t+1)}(M, \mathbf{q}_0), \tag{5.70}$$

причем если $t_1 \neq t_2$, то

$$S_{fxd}^{(t_1+1)}(M, \mathbf{q}_0) \cap S_{fxd}^{(t_2+1)}(M, \mathbf{q}_0) = \varnothing.$$

Отсюда вытекает, что для исследования структуры множества $S_{fxd}(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ достаточно охарактеризовать общий элемент последовательности множеств $\{S_{fxd}^{(t+1)}(M, \mathbf{q}_0)\}_{t \in \mathbf{Z}_+}$.

Отметим, что из включения

$$S_{fxd}^{(t+2)}(M, \mathbf{q}_0) \subseteq \{\mathbf{ux} \mid \mathbf{u} \in S_{fxd}^{(t+2)}(M, \mathbf{q}_0), \mathbf{x} \in \mathbf{Z}_{p^k}^n\}$$

вытекает

Утверждение 5.14. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ при любом начальном состоянии $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, если существует такое значение $t_0 \in \mathbf{Z}_+$, что

$$S_{fxd}^{(t_0+1)}(M, \mathbf{q}_0) = \varnothing,$$

то для всех $t > t_0$

$$S_{fxd}^{(t+1)}(M, \mathbf{q}_0) = \varnothing$$

Из утверждения 5.14 и равенства (5.70), в свою очередь, вытекает

Утверждение 5.15. Множество $S_{fxd}(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ – конечное множество тогда и только тогда, когда существует такое значение $t_0 \in \mathbf{Z}_+$, что

$$S_{fxd}^{(t_0+1)}(M, \mathbf{q}_0) = \varnothing.$$

Обозначим через $I \in \mathsf{M}_n$ единичную матрицу.

Теорема 5.12. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ при любом начальном состоянии $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ для всех $t \in \mathbf{Z}_+$ множество $S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$ состоит из всех таких входных слов $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in \mathbf{Z}_{p^k}^{n\cdot(t+1)}$, что:

1) если $M \in \mathsf{A}_{n,1}$, то $(\mathbf{x}_1, \ldots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I \Theta D) \circ \mathbf{x}_1 = C \circ \mathbf{q}_0 \\ (I \Theta D) \circ \mathbf{x}_{i+1} = C \circ (A^i \circ \mathbf{q}_0 \oplus \\ \oplus \bigoplus\limits_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i) \ (i = 1, \ldots, t); \end{cases} \tag{5.71}$$

2) если $M \in \mathsf{A}_{n,2}$, то $(\mathbf{x}_1, \ldots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I \Theta C \circ B) \circ \mathbf{x}_1 = C \circ A \circ \mathbf{q}_0 \\ (I \Theta C \circ B) \circ \mathbf{x}_{i+1} = C \circ A \circ (A^i \circ \mathbf{q}_0 \oplus \\ \bigoplus\limits_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i) \ (i = 1, \ldots, t). \end{cases} \tag{5.72}$$

Доказательство. Пусть $M \in \mathsf{A}_{n,1}$.

Предположим, что $t = 0$ и $\mathbf{x}_1 \in S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$. Из 2-го уравнения системы (5.18) находим

$$\mathbf{x}_1 = C \circ \mathbf{q}_0 \oplus D \circ \mathbf{x}_1 \Leftrightarrow (I \Theta D) \circ \mathbf{x}_1 = C \circ \mathbf{q}_0, \tag{5.73}$$

что и требовалось показать.

Предположим, что $t \in \mathbf{N}$ и $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$. Полагая в (5.64)

$$\mathbf{y}_{i+1} = \mathbf{x}_{i+1} \quad (i \in \mathbf{N})$$

и принимая во внимание равенство (5.73), получим (5.71), что и требовалось показать.

Пусть $M \in \mathsf{A}_{n,2}$.

Предположим, что $t = 0$ и $\mathbf{x}_1 \in S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$. Из системы (5.19) находим

$$\mathbf{x}_1 = C \circ A \circ \mathbf{q}_0 \oplus C \circ B \circ \mathbf{x}_1 \Leftrightarrow (I \Theta C \circ B) \circ \mathbf{x}_1 = C \circ A \circ \mathbf{q}_0. \qquad (5.74)$$

Предположим, что $t \in \mathbf{N}$ и $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$. Полагая в (5.66)

$$\mathbf{y}_{i+1} = \mathbf{x}_{i+1} \quad (i \in \mathbf{N})$$

и принимая во внимание равенство (5.74), получим (5.72), что и требовалось показать.

Теорема доказана.

Рассмотрим ряд следствий из теоремы 5.12.

Из (5.71) непосредственно вытекает

Следствие 5.6. Для любого автомата $M \in \mathsf{A}_{n,1}$, если $I \Theta D \in \mathsf{M}_n^{inv}$, то при любом начальном состоянии $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ множество $S_{fxd}(M, \mathbf{q}_0)$ – бесконечное множество, причем для каждого $t \in \mathbf{Z}_+$ множество $S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$ – одноэлементное множество и содержит единственное такое входное слово $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in \mathbf{Z}_{p^k}^{n \cdot (t+1)}$, что

$$\begin{cases} \mathbf{x}_1 = (I \Theta D)^{-1} \circ C \circ \mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I \Theta D)^{-1} \circ (C \circ (A^i \circ \mathbf{q}_0 \oplus \\ \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i)) \quad (i = 1, \ldots, t). \end{cases} \qquad (5.75)$$

Из (5.72) непосредственно вытекает

Следствие 5.7. Для любого автомата $M \in \mathsf{A}_{n,2}$, если $I \Theta C \circ B \in \mathsf{M}_n^{inv}$, то при любом начальном состоянии $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ множество $S_{fxd}(M, \mathbf{q}_0)$ – бесконечное множество, причем для каждого $t \in \mathbf{Z}_+$ множество $S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$ – одноэлементное множество и содержит единственное такое входное слово $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in \mathbf{Z}_{p^k}^{n \cdot (t+1)}$, что

$$\begin{cases} \mathbf{x}_1 = (I \Theta C \circ B)^{-1} \circ C \circ A \circ \mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I \Theta C \circ B)^{-1} \circ (C \circ A \circ (A^i \circ \mathbf{q}_0 \oplus \\ \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i)) \quad (i = 1, \ldots, t). \end{cases} \qquad (5.76)$$

Из 1-го уравнения систем (5.71) и (5.72) вытекает, что существует следующий локальный критерий проверки пустоты множества $S_{fxd}(M,\mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}^n_{p^k})$.

Следствие 5.8. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ множество $S_{fxd}(M,\mathbf{q}_0)$ – непустое множество для таких и только таких начальных состояний $\mathbf{q}_0 \in \mathbf{Z}^n_{p^k}$, для которых имеет решения уравнение

$$(I \Theta D) \circ \mathbf{x} = C \circ \mathbf{q}_0 \quad (\mathbf{x} \in \mathbf{Z}^n_{p^k}), \tag{5.77}$$

если $M \in \mathsf{A}_{n,1}$ и уравнение

$$(I \Theta C \circ B) \circ \mathbf{x} = C \circ A \circ \mathbf{q}_0 \quad (\mathbf{x} \in \mathbf{Z}^n_{p^k}), \tag{5.78}$$

если $M \in \mathsf{A}_{n,2}$.

Если $\mathbf{q}_0 = \mathbf{0}$, то уравнения (5.77) и (5.78) имеют решение $\mathbf{x} = \mathbf{0}$. Отсюда вытекает

Следствие 5.9. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$

$$S_{fxd}(M,\mathbf{0}) \neq \varnothing.$$

Особенность следствия 5.8 состоит в том, что оно представляет собой «локальный критерий», т.е. характеристику структуры всего множества $S_{fxd}(M,\mathbf{q}_0)$, являющегося подмножеством свободной полугруппы $(\mathbf{Z}^n_{p^k})^+$, в терминах образующих элементов $\mathbf{x} \in \mathbf{Z}^n_{p^k}$ этой полугруппы, выраженных через структуру множества $S^{(1)}_{fxd}(M,\mathbf{q}_0)$.

Отсюда вытекает целесообразность исследования структуры множества $S^{(1)}_{fxd}(M,\mathbf{q})$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2})$ при любом текущем состоянии $\mathbf{q} \in \mathbf{Z}^n_{p^k}$.

Рассмотрим некоторые такие характеристики.

Из следствия 5.8 вытекает

Следствие 5.10. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ проверка пустоты множества $S_{fxd}(M,\mathbf{q})$ при любом текущем состоянии $\mathbf{q} \in \mathbf{Z}^n_{p^k}$ сводится к проверке пустоты множества решений уравнение

$$(I \Theta D) \circ \mathbf{x} = C \circ \mathbf{q} \quad (\mathbf{x} \in \mathbf{Z}^n_{p^k}), \tag{5.79}$$

если $M \in \mathsf{A}_{n,1}$ и уравнения

$$(I \Theta C \circ B) \circ \mathbf{x} = C \circ A \circ \mathbf{q} \quad (\mathbf{x} \in \mathbf{Z}^n_{p^k}), \tag{5.80}$$

если $M \in \mathsf{A}_{n,2}$.

Из (5.79) и (5.80) вытекает

Следствие 5.11. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ и для любых состояний $\mathbf{q}', \mathbf{q}'' \in \mathbf{Z}_{p^k}^n$, если $\mathbf{x}' \in S_{fxd}^{(1)}(M, \mathbf{q}')$ и $\mathbf{x}'' \in S_{fxd}^{(1)}(M, \mathbf{q}'')$, то $\mathbf{x}' \ominus \mathbf{x}'' \in S_{fxd}^{(1)}(M, \mathbf{q}' \ominus \mathbf{q}'')$.

Из следствия 5.11 непосредственно вытекает

Следствие 5.12. Для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ при каждом текущем состоянии $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ для любого входного символа $\mathbf{x}' \in S_{fxd}^{(1)}(M, \mathbf{q})$ истинно равенство

$$S_{fxd}^{(1)}(M, \mathbf{q}) = \{\mathbf{x}' \oplus \mathbf{x}'' \mid \mathbf{x}'' \in S_{fxd}^{(1)}(M, \mathbf{0})\}. \qquad (5.81)$$

Из следствия 5.12 вытекает, что для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ в явном виде достаточно построить только множество $S_{fxd}^{(1)}(M, \mathbf{0})$. Для любого текущего состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ множество $S_{fxd}^{(1)}(M, \mathbf{q})$ всегда может быть вычислено в соответствии с равенством (5.81).

Рассмотрим теперь автоматы $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ специального вида.

Пусть $M \in \mathsf{A}_{n,1}$ и

$$D = I.$$

Из (5.79) вытекает, что

$$S_{fxd}^{(1)}(M, \mathbf{q}) = \mathbf{Z}_{p^k}^n$$

для любого такого текущего состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$, что

$$C \circ \mathbf{q} = \mathbf{0}.$$

Пусть $M \in \mathsf{A}_{n,2}$ и

$$C \circ B = I.$$

Из (5.80) вытекает, что

$$S_{fxd}^{(1)}(M, \mathbf{q}) = \mathbf{Z}_{p^k}^n$$

для любого такого текущего состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$, что

$$C \circ A \circ \mathbf{q} = \mathbf{0}.$$

Пусть $M \in \mathsf{A}_{n,1}$ и существует такой элемент $a \in \mathbf{Z}_{p^k}$, что

$$I \ominus D = a \circ C.$$

Из (5.79) вытекает, что

$$S_{fxd}(M, \mathbf{q}) \neq \varnothing.$$

для любого такого текущего состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$, что уравнение

$$a \circ \mathbf{x} = \mathbf{q}$$

имеет решения.

Пусть $M \in \mathsf{A}_{n,2}$ и существует такой элемент $a \in \mathbf{Z}_{p^k}$, что

$$I \Theta C \circ B = a \circ C \circ A.$$

Из (5.80) вытекает, что

$$S_{fxd}(M, \mathbf{q}) \neq \varnothing.$$

для любого такого текущего состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$, что уравнение

$$a \circ \mathbf{x} = \mathbf{q}$$

имеет решения.

5.7. Каноническая форма автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1,2)$.

Известно, что множество $\mathbf{Z}_{p^k}^n$ представляет собой $\mathbf{Z}_{p^k}^n$-модуль линейных форм [16]. Следовательно, каждое линейное преобразование пространства $\mathbf{Z}_{p^k}^n$ в себя, иными словами, каждая матрица $H \in \mathsf{M}_n$, с помощью элементарных операций (т. е. умножения слева и справа на соответствующие матрицы $G, F \in \mathsf{M}_n^{inv}$) может быть представлено в виде

$$G \circ H \circ F = \begin{pmatrix} U & O_{r,h} \\ O_{h,r} & V \end{pmatrix}, \tag{5.82}$$

где $U \in \mathsf{D}_r^{(1)}$, $V \in \mathsf{D}_h^{(2)}$ $(r + h = n)$, а $O_{l,m}$ – нулевая $l \times m$-матрица.

Обозначим через $\mathsf{D}_n^{(1),(2)}$ множество всех матриц вида (5.82).

Отметим, что любая матрица $X \in \mathsf{D}_n^{(1),(2)}$ осуществляет умножение компонент вектора $\mathbf{z} \in \mathbf{Z}_{p^k}^n$ на соответствующие элементы кольца Z_{p^k}, а множество матриц M_n^{inv} – группа (по умножению), изоморфная подгруппе симметрической группы $\mathsf{S}(p^{k \cdot n})$.

Будем говорить, что автомат $(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ представлен в канонической форме, если все выполняемые в его представлении линейные преобразования – элементы множеств $\mathsf{D}_n^{(1),(2)}$ и M_n^{inv}.

Из (5.18) и (5.19) вытекает, что канонические формы автоматов $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathsf{A}_{n,1}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ и $(M_2, \mathbf{q}_0)$ $(M_2 \in \mathsf{A}_{n,2}, \mathbf{q}_0 \in \mathbf{Z}_{p^k}^n)$ имеют, соответственно, следующий вид

$$(M_1, \mathbf{q}_0): \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus \\ \qquad \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ \mathbf{x}_{t+1}) \\ G_3 \circ \mathbf{y}_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus \\ \qquad \oplus R_4 \circ X_4 \circ (F_4^{-1} \circ \mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+)$$

и

$$(M_2,\mathbf{q}_0):\begin{cases} F_1^{-1}\circ\mathbf{q}_{t+1}=R_1\circ X_1\circ(F_1^{-1}\circ\mathbf{q}_t)\oplus \\ \qquad\qquad \oplus R_2\circ X_2\circ(F_2^{-1}\circ\mathbf{x}_{t+1}) \\ G_3\circ\mathbf{y}_{t+1}=X_3\circ R_3\circ(F_1^{-1}\circ\mathbf{q}_{t+1}) \end{cases} (t\in\mathbf{Z}_+),$$

где $X_i\in\mathsf{D}_n^{(1),(2)}$ $(i=1,\ldots,4)$ и $G_i,R_i\in\mathsf{M}_n^{inv}$ $(i=1,\ldots,4)$, причем

$$X_1=G_1\circ A\circ F_1,\ \ X_2=G_2\circ B\circ F_2,\ \ X_3=G_3\circ C\circ F_3,\ \ X_4=G_2\circ D\circ F_2,$$

$$R_1=F_1^{-1}\circ G_1^{-1},\ \ R_2=F_1^{-1}\circ G_2^{-1},\ \ R_3=F_3^{-1}\circ F_1,\ \ R_4=G_3\circ G_4^{-1}.$$

Если $M_i\in\mathsf{A}_{n,i}^{inv}$ $(i=1,2)$, то канонические формы имеют более простой вид, а именно:

$$(M_1,\mathbf{q}_0):\begin{cases} F_1^{-1}\circ\mathbf{q}_{t+1}=R_1\circ X_1\circ(F_1^{-1}\circ\mathbf{q}_t)\oplus \\ \qquad\qquad \oplus R_2\circ X_2\circ(F_2^{-1}\circ\mathbf{x}_{t+1}) \\ G_3\circ\mathbf{y}_{t+1}=X_3\circ R_3\circ(F_1^{-1}\circ\mathbf{q}_t)\oplus \\ \qquad\qquad \oplus Y_1\circ\mathbf{x}_{t+1} \end{cases} (t\in\mathbf{Z}_+)$$

и

$$(M_2,\mathbf{q}_0):\begin{cases} F_1^{-1}\circ\mathbf{q}_{t+1}=R_1\circ X_1\circ(F_1^{-1}\circ\mathbf{q}_t)\oplus \\ \qquad\qquad \oplus Y_2\circ\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1}=Y_3\circ(F_1^{-1}\circ\mathbf{q}_{t+1}) \end{cases} (t\in\mathbf{Z}_+),$$

где $Y_1=G_3\circ D\in\mathsf{M}_n^{inv}$, $Y_2=F_1^{-1}\circ B\in\mathsf{M}_n^{inv}$, $Y_3=C\circ F_1\in\mathsf{M}_n^{inv}$.

5.8. Вариация поведения автомата $M_i\in\mathsf{A}_{n,i}$ $(i=1,2)$.

В п.1.3 отмечено, что к стандартным методам анализа вычислительной стойкости современных блочных шифров относится их дифференциальный и интегральный анализ.

Суть этих методов состоит в исследовании вариации значений применяемой булевой вектор-функции при вариации аргументов, т.е. открытых текстов и/или секретных сеансовых ключей.

Для инициального автомата $(M,\mathbf{q}_0)$ $(M\in\mathsf{A}_{n,1}^{inv}\cup\mathsf{A}_{n,2}^{inv},\mathbf{q}_0\in\mathbf{Z}_{p^k}^n)$, используемого в качестве поточного шифра, аналогом такого анализа является исследование вариации соответствующей словарной функции при вариации определяющих ее матриц, вариации начального состояния и вариации входной последовательности.

При этом переход от булевой функции к словарной функции, реализуемой инициальным конечным автоматом (т.е. к о.-д. функции) является

принципиально новым моментом дифференциального и интегрального анализа.

В свете сказанного выше актуальной с позиции современной криптологии и интересной с позиции теории автоматов является задача исследования вариации о.-д. функции, реализуемой инициальным автоматом $(M, \mathbf{q}_0)$ $M_i \in \mathsf{A}_{n,i}$ $(i=1,2)$ (отметим, что некоторые аспекты решения этой задачи охарактеризованы в пп.5.4-5.6).

Рассмотрим решение этой задачи.

Пусть

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1} \end{cases} (t \in \mathbf{Z}_+) \tag{5.83}$$

и

$$(\tilde{M}_1, \tilde{\mathbf{q}}_0): \begin{cases} \tilde{\mathbf{q}}_{t+1} = \tilde{A} \circ \tilde{\mathbf{q}}_t \oplus \tilde{B} \circ \tilde{\mathbf{x}}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = \tilde{C} \circ \tilde{\mathbf{q}}_t \oplus \tilde{D} \circ \tilde{\mathbf{x}}_{t+1} \end{cases} (t \in \mathbf{Z}_+). \tag{5.84}$$

Положим

$$\tilde{A} = A \oplus \Delta A, \quad \tilde{B} = B \oplus \Delta B, \quad \tilde{C} = C \oplus \Delta C, \quad \tilde{D} = D \oplus \Delta D,$$

$$\tilde{\mathbf{q}}_{t+1} = \mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1}, \quad \tilde{\mathbf{q}}_t = \mathbf{q}_t \oplus \Delta\mathbf{q}_t, \quad \tilde{\mathbf{x}}_{t+1} = \mathbf{x}_{t+1} \oplus \Delta\mathbf{x}_{t+1}, \quad \tilde{\mathbf{y}}_{t+1} = \mathbf{y}_{t+1} \oplus \Delta\mathbf{y}_{t+1}.$$

Тогда уравнения системы (5.84) примут, соответственно, вид

$$\begin{aligned} \mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1} &= (A \oplus \Delta A) \circ (\mathbf{q}_t \oplus \Delta\mathbf{q}_t) \oplus (B \oplus \Delta B) \circ (\mathbf{x}_{t+1} \oplus \Delta\mathbf{x}_{t+1}) = \\ &= (A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1}) \oplus (A \circ \Delta\mathbf{q}_t \oplus B \circ \Delta\mathbf{x}_{t+1}) \oplus \\ &\oplus (\Delta A \circ \mathbf{q}_t \oplus \Delta B \circ \mathbf{x}_{t+1}) \oplus (\Delta A \circ \Delta\mathbf{q}_t \oplus \Delta B \circ \Delta\mathbf{x}_{t+1}) \quad (t \in \mathbf{Z}_+) \end{aligned} \tag{5.85}$$

и

$$\begin{aligned} \mathbf{y}_{t+1} \oplus \Delta\mathbf{y}_{t+1} &= (C \oplus \Delta C) \circ (\mathbf{q}_t \oplus \Delta\mathbf{q}_t) \oplus (D \oplus \Delta D) \circ (\mathbf{x}_{t+1} \oplus \Delta\mathbf{x}_{t+1}) = \\ &= (C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1}) \oplus (C \circ \Delta\mathbf{q}_t \oplus D \circ \Delta\mathbf{x}_{t+1}) \oplus \\ &\oplus (\Delta C \circ \mathbf{q}_t \oplus \Delta D \circ \mathbf{x}_{t+1}) \oplus (\Delta C \circ \Delta\mathbf{q}_t \oplus \Delta D \circ \Delta\mathbf{x}_{t+1}) \quad (t \in \mathbf{Z}_+). \end{aligned} \tag{5.86}$$

Вычтем из уравнений (5.85) и (5.86), соответственно, 1-е и 2-е уравнения системы (5.83). Получим

$$\begin{aligned} \Delta\mathbf{q}_{t+1} &= (A \circ \Delta\mathbf{q}_t \oplus B \circ \Delta\mathbf{x}_{t+1}) \oplus \\ &\oplus (\Delta A \circ \mathbf{q}_t \oplus \Delta B \circ \mathbf{x}_{t+1}) \oplus (\Delta A \circ \Delta\mathbf{q}_t \oplus \Delta B \circ \Delta\mathbf{x}_{t+1}) \quad (t \in \mathbf{Z}_+) \end{aligned} \tag{5.87}$$

и

$$\begin{aligned} \Delta\mathbf{y}_{t+1} &= (C \circ \Delta\mathbf{q}_t \oplus D \circ \Delta\mathbf{x}_{t+1}) \oplus \\ &\oplus (\Delta C \circ \mathbf{q}_t \oplus \Delta D \circ \mathbf{x}_{t+1}) \oplus (\Delta C \circ \Delta\mathbf{q}_t \oplus \Delta D \circ \Delta\mathbf{x}_{t+1}) \quad (t \in \mathbf{Z}_+). \end{aligned} \tag{5.88}$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом (5.84), по отношению к о.-д. функции, реализуемой инициальным автоматом (5.83), характеризуется о.-д. функцией, представленной рекуррентными соотношениями (5.87) и (5.88).

Отметим, что из (5.87) и (5.88) вытекает, что:

1) если

$$\Delta\mathbf{x}_{t+1} \equiv \mathbf{0} \quad (t \in \mathbf{Z}_+),$$

то

$$\Delta\mathbf{q}_{t+1} = A \circ \Delta\mathbf{q}_t \oplus \Delta A \circ \mathbf{q}_t \oplus \Delta A \circ \Delta\mathbf{q}_t \quad (t \in \mathbf{Z}_+)$$

и

$$\Delta\mathbf{y}_{t+1} = C \circ \Delta\mathbf{q}_t \oplus \Delta C \circ \mathbf{q}_t \oplus \Delta C \circ \Delta\mathbf{q}_t \quad (t \in \mathbf{Z}_+);$$

2) если

$$\Delta A = \Delta B = \Delta C = \Delta D = O,$$

то

$$\Delta\mathbf{q}_{t+1} = A \circ \Delta\mathbf{q}_t \oplus B \circ \Delta\mathbf{x}_{t+1} \quad (t \in \mathbf{Z}_+)$$

и

$$\Delta\mathbf{y}_{t+1} = C \circ \Delta\mathbf{q}_t \oplus D \circ \Delta\mathbf{x}_{t+1} \quad (t \in \mathbf{Z}_+).$$

Пусть

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.89}$$

и

$$(\tilde{M}_2, \tilde{\mathbf{q}}_0): \begin{cases} \tilde{\mathbf{q}}_{t+1} = \tilde{A} \circ \tilde{\mathbf{q}}_t \oplus \tilde{B} \circ \tilde{\mathbf{x}}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = \tilde{C} \circ \tilde{\mathbf{q}}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.90}$$

Положим

$$\tilde{A} = A \oplus \Delta A, \quad \tilde{B} = B \oplus \Delta B, \quad \tilde{C} = C \oplus \Delta C,$$

$$\tilde{\mathbf{q}}_{t+1} = \mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1}, \quad \tilde{\mathbf{q}}_t = \mathbf{q}_t \oplus \Delta\mathbf{q}_t, \quad \tilde{\mathbf{x}}_{t+1} = \mathbf{x}_{t+1} \oplus \Delta\mathbf{x}_{t+1}, \quad \tilde{\mathbf{y}}_{t+1} = \mathbf{y}_{t+1} \oplus \Delta\mathbf{y}_{t+1}.$$

Тогда 1-е уравнение системы (5.90) примет вид (5.85), а 2-е уравнение системы (5.90) – вид

$$\mathbf{y}_{t+1} \oplus \Delta\mathbf{y}_{t+1} = (C \oplus \Delta C) \circ (\mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1}) =$$

$$= C \circ \mathbf{q}_{t+1} \oplus (C \circ \Delta\mathbf{q}_{t+1} \oplus \Delta C \circ (\mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1})) \quad (t \in \mathbf{Z}_+). \tag{5.91}$$

Вычтем из уравнений (5.85) и (5.91), соответственно, 1-е и 2-е уравнения системы (5.90).

Получим (5.87) и

$$\Delta \mathbf{y}_{t+1} = C \circ \Delta \mathbf{q}_{t+1} \oplus \Delta C \circ (\mathbf{q}_{t+1} \oplus \Delta \mathbf{q}_{t+1}) \quad (t \in \mathbf{Z}_+). \tag{5.92}$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом (5.90), по отношению к о.-д. функции, реализуемой инициальным автоматом (5.89), характеризуется о.-д. функцией, представленной рекуррентными соотношениями (5.87) и (5.92).

5.9. Линейные одномерные автоматы с лагом l.

Инициальные линейные одномерные автоматы Мили и Мура с лагом l ($l \in \mathbf{N}$) над кольцом Z_{p^k} определяются, соответственно, рекуррентными соотношениями

$$(M_1, \mathbf{q}_0): \begin{cases} q_{t+l} = \bigoplus\limits_{i=1}^{l} a_i \circ q_{t+l-i} \oplus b \circ x_{t+1} \\ y_{t+1} = \bigoplus\limits_{i=1}^{l} c_i \circ q_{t+l-i} \oplus d \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.93}$$

и

$$(M_2, \mathbf{q}_0): \begin{cases} q_{t+l} = \bigoplus\limits_{i=1}^{l} a_i \circ q_{t+l-i} \oplus b \circ x_{t+1} \\ y_{t+1} = \bigoplus\limits_{i=1}^{l} c_i \circ q_{t+l+1-i} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.94}$$

где $a_i, c_i, d, d \in \mathbf{Z}_{p^k}$ $(i = 1, \ldots, l)$ – параметры, $x \in \mathbf{Z}_{p^k}$ и $y \in \mathbf{Z}_{p^k}$ – соответственно, входная и выходная переменная, $q \in \mathbf{Z}_{p^k}$ – переменная состояния, а $\mathbf{q}_0 = (q_{l-1}, \ldots, q_1, q_0)^T \in \mathbf{Z}_{p^k}^l$ – начальное состояние автомата M_i $(i = 1,2)$.

Перепишем (5.93) и (5.94) в следующем матричном виде

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+)$$

и

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где

$$\mathbf{q}_t = (q_{t+l-1}, \ldots, q_{t+1}, q_t)^T \in \mathbf{Z}_{p^k}^l \quad (t \in \mathbf{Z}_+),$$

$$\mathbf{x}_{t+1} = (x_{t+1}, \underbrace{0, \ldots, 0}_{l-1 \text{ раз}})^T \in \mathbf{Z}_{p^k}^l \quad (t \in \mathbf{Z}_+)$$

и

$$\mathbf{y}_{t+1} = (y_{t+1}, \underbrace{0, \ldots, 0}_{l-1 \text{ раз}})^T \in \mathbf{Z}_{p^k}^l \quad (t \in \mathbf{Z}_+),$$

а $A,B,C,D\in \mathsf{M}_l$ – такие диагональные матрицы, что

$$A=\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_l \end{pmatrix}, \quad B=\begin{pmatrix} b & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix},$$

$$C=\begin{pmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & c_l \end{pmatrix}, \quad D=\begin{pmatrix} d & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Таким образом, для автоматов (5.93) и (5.94) заведомо истинны все результаты, полученные в пп.5.2-5.8 для линейных автоматов при замене числа n числом l, с учетом сужения входной и выходной полугрупп автоматов с множества $(\mathbf{Z}^{l}_{p^k})^{+}$ до множества $\mathbf{Z}^{+}_{p^k}$.

Рассмотрим некоторые из таких результатов.

Обозначим через $\widetilde{\mathsf{A}}_{l,1}$ множество всех автоматов M_1, определенных формулой (5.93), а через $\widetilde{\mathsf{A}}_{l,2}$ – множество всех автоматов M_2, определенных формулой (5.94). Ясно, что

$$|\widetilde{\mathsf{A}}_{l,j}|=p^{k\cdot(2\cdot l+3-j)} \quad (j=1,2). \tag{5.95}$$

Из (5.93) и (5.94) вытекают

Утверждение 5.16. Автомат $M_1\in\widetilde{\mathsf{A}}_{l,1}$ является обратимым автоматом тогда и только тогда, когда d – обратимый элемент кольца Z_{p^k}.

Утверждение 5.17. Автомат $M_2\in\widetilde{\mathsf{A}}_{l,2}$ является обратимым автоматом тогда и только тогда, когда c_1 и b – обратимые элементы кольца Z_{p^k}.

При этом, автомат обратный автомату $M_1\in\widetilde{\mathsf{A}}_{l,1}$ имеет вид

$$(M_1^{-1},\mathbf{q}_0):\begin{cases} q_{t+l}=\bigoplus\limits_{i=1}^{l}\alpha_i\circ q_{t+l-i}\oplus\beta\circ x_{t+1} \\ y_{t+1}=\bigoplus\limits_{i=1}^{l}\gamma_i\circ q_{t+l-i}\oplus\delta\circ x_{t+1} \end{cases} \quad (t\in\mathbf{Z}_+),$$

где $\beta=b\circ d^{-1}$, $\delta=d^{-1}$ и для всех $i=1,\dots,l$

$$\alpha_i=a_i\Theta b\circ d^{-1}\circ c_i$$

и

$$\gamma_i=\Theta d^{-1}\circ c_i,$$

а автомат, обратный автомату $M_2 \in \tilde{\mathsf{A}}_{l,2}$ имеет вид

$$(M_2^{-1}, \mathbf{q}_0): \begin{cases} q_{t+l} = \bigoplus\limits_{i=2}^{l} \alpha_i \circ q_{t+l-i} \oplus \beta \circ x_{t+1} \\ y_{t+1} = \bigoplus\limits_{i=1}^{l} \gamma_i \circ q_{t+l-i} \oplus \delta \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\beta = c_1^{-1}$, $\delta = b^{-1} \circ c_1^{-1}$, $\alpha_i = c_1^{-1} \circ c_i$ $(i = 2,\ldots,l)$ и

$$\gamma_i = \begin{cases} \Theta b^{-1} \circ (c_1^{-1} \circ c_{i+1} \oplus a_i), \ \textit{если} \ i = 1,\ldots,l-1 \\ \Theta b^{-1} \circ a_l, \ \textit{если} \ i = l. \end{cases}$$

Пусть $\tilde{\mathsf{A}}_{l,j}^{inv}$ $(j = 1,2)$ – множество всех обратимых автоматов $M_j \in \tilde{\mathsf{A}}_{l,j}$. Из утверждений 5.16, 5.17 и формулы (5.95) вытекает

Следствие 5.13. Для всех $l \in \mathbf{N}$

$$|\tilde{\mathsf{A}}_{l,j}^{inv}| = p^{-j} \cdot (p-1)^j \cdot |\tilde{\mathsf{A}}_{l,j}| \quad (j = 1,2). \tag{5.96}$$

Из (5.96) вытекает, что

$$\frac{|\tilde{\mathsf{A}}_{l,j}^{inv}|}{|\tilde{\mathsf{A}}_{l,j}|} = p^{-j} \cdot (p-1)^j \quad (j = 1,2),$$

т.е. в множестве $\tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ доля обратимых автоматов не зависит ни от значения числа $k \in \mathbf{N}$, ни от значения числа $l \in \mathbf{N}$.

Охарактеризуем некоторые подмножества множеств $\tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ и $\tilde{\mathsf{A}}_{l,j}^{inv}$ $(j = 1,2)$, естественно определяемых в терминах теории автоматов.

Теорема 5.13. Для всех $l \in \mathbf{N}$ автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ является сильно связным автоматом тогда и только тогда, когда b – обратимый элемент кольца Z_{p^k}.

Доказательство. 1. Пусть $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ – сильно связный автомат.

Тогда для любых двух его состояний

$$\mathbf{q}_0 = (q_{l-1},\ldots,q_1,q_0)^T \in \mathbf{Z}_{p^k}^l$$

и

$$\mathbf{q}_0' = (q_{l-1}',\ldots,q_1',q_0')^T \in \mathbf{Z}_{p^k}^l$$

существует входное слово $x_1 \ldots x_n \in \mathbf{Z}_{p^k}^n$ $(n \in \mathbf{N})$, переводящее состояние $\mathbf{q}_0$ в состояние $\mathbf{q}_0'$.

Предположим противное, т.е. что b – необратимый элемент кольца Z_{p^k}.

Рассмотрим любое такое состояние

$$\mathbf{q}_0 = (q_{l-1},\ldots,q_1,q_0)^T \in \mathbf{Z}_{p^k}^l,$$

что

$$q_i \equiv 0 \,(\mathrm{mod}\ p)$$

для всех $i = 0,1,\ldots l-1$.

Из 1-го уравнения, определяющего автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$, вытекает, что

$$q_l \equiv 0 \,(\mathrm{mod}\ p)$$

для любого входного символа $x \in \mathbf{Z}_{p^k}$.

Таким образом, состояние $\mathbf{q}_0$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в такое состояние

$$\mathbf{q}_1 = (q_l,\ldots,q_2,q_1)^T \in \mathbf{Z}_{p^k}^l,$$

что

$$q_i \equiv 0 \,(\mathrm{mod}\ p)$$

для всех $i = 1,\ldots l$.

Отсюда вытекает (доказывается индукцией по длине входного слова), что состояние $\mathbf{q}_0$ под действием любого входного слова $x_1 \ldots x_n \in \mathbf{Z}_{p^k}^n$ $(n \in \mathbf{N})$ переходит в такое состояние

$$\mathbf{q}_n = (q_{n+l-1},\ldots,q_{n+1},q_n)^T \in \mathbf{Z}_{p^k}^l,$$

что

$$q_i \equiv 0 \,(\mathrm{mod}\ p)$$

для всех $i = n, n+1,\ldots n+l-1$.

Поэтому из состояния $\mathbf{q}_0$ недостижимо ни одно состояние

$$\mathbf{q}_0' = (q_{l-1}',\ldots,q_1',q_0')^T \in \mathbf{Z}_{p^k}^l,$$

удовлетворяющее следующему условию: существует такое $i \in \{0,1,\ldots l-1\}$, что

$$q_i \equiv m \,(\mathrm{mod}\ p),$$

где $m \in \{1,\ldots, p-1\}$. Это означает, что автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ не является сильно связным автоматом.

Получено противоречие.

Следовательно, предположение – ложное.

Таким образом, если $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j = 1,2)$ – сильно связный автомат, то b – обратимый элемент кольца Z_{p^k}, что и требовалось показать.

2. Пусть b – обратимый элемент кольца Z_{p^k}. Покажем, что из любого состояния

$$\mathbf{q}_0 = (q_{l-1}, \ldots, q_1, q_0)^T \in \mathbf{Z}^l_{p^k}$$

автомата $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$ достижимо любое его состояние

$$\mathbf{q}'_0 = (q'_{l-1}, \ldots, q'_1, q'_0)^T \in \mathbf{Z}^l_{p^k}.$$

Выберем такое входное слово $x_1 \ldots x_l \in \mathbf{Z}^l_{p^k}$, что

$$b \circ x_{i+1} = q'_i \Theta \overset{i}{\underset{m=1}{\oplus}} a_m \circ q'_{i-m} \Theta \overset{l-1}{\underset{m=i}{\oplus}} a_m \circ q_m \quad (i = 0,1,\ldots l-1). \tag{5.97}$$

Так как b – обратимый элемент кольца Z_{p^k}, то система уравнений (5.97) имеет единственное решение

$$x_{i+1} = b^{-1} \circ (q'_i \Theta \overset{i}{\underset{m=1}{\oplus}} a_m \circ q'_{i-m} \Theta \overset{l-1}{\underset{m=i}{\oplus}} a_m \circ q_m) \quad (i = 0,1,\ldots l-1). \tag{5.98}$$

Из 1-го уравнения, определяющего автомат $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$, вытекает, что входное слово $x_1 \ldots x_l \in \mathbf{Z}^l_{p^k}$, где x_{i+1} $(i = 0,1,\ldots l-1)$ определяется равенством (5.98), порождает следующую последовательность переходов состояний автомат $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$

$$\mathbf{q}_0 \to \mathbf{q}_1 \to \ldots \to \mathbf{q}_{l-1} \to \mathbf{q}_l = \mathbf{q}'_0, \tag{5.99}$$

где

$$\mathbf{q}_i = (q_i, \ldots, q_{l-1}, q'_0, q'_1, \ldots, q'_{i-1}) \quad (i = 1, \ldots l). \tag{5.100}$$

Из (5.99) и (5.100) вытекает, что если b – обратимый элемент кольца Z_{p^k}, то из любого состояния $\mathbf{q}_0 \in \mathbf{Z}^l_{p^k}$ автомата $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$ достижимо любое его состояние $\mathbf{q}'_0 \in \mathbf{Z}^l_{p^k}$.

Это означает, что $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$ – сильно связный автомат.

Теорема доказана.

Обозначим через $\tilde{A}^{sc}_{l,j}$ $(j = 1,2)$ множество всех сильно связных автоматов $M_j \in \tilde{A}_{l,j}$ $(j = 1,2)$.

Из теоремы 5.13 вытекает

Следствие 5.14. Для всех $l \in \mathbf{N}$

$$|\tilde{A}^{sc}_{l,j}| = p^{-1} \cdot (p-1) \cdot |\tilde{A}_{l,j}| \ (j = 1,2).$$

Кроме того, степень достижимости [208] автомата $M_j \in \tilde{\mathsf{A}}^{sc}_{l,j}$ $(j=1,2)$ характеризуется следующим образом.

Следствие 5.15. Для всех $l \in \mathbf{N}$ диаметр графа переходов любого автомата $M_j \in \tilde{\mathsf{A}}^{sc}_{l,j}$ $(j=1,2)$ равен l.

Доказательство. Выберем такие состояния

$$\mathbf{q}_0 = (q_{l-1},\ldots,q_1,q_0)^T \in \mathbf{Z}^l_{p^k}$$

и

$$\mathbf{q}'_0 = (q'_{l-1},\ldots,q'_1,q'_0)^T \in \mathbf{Z}^l_{p^k}$$

автомата $M_j \in \tilde{\mathsf{A}}^{sc}_{l,j}$ $(j=1,2)$, что

$$q_i \neq q'_i$$

для всех $i = 0,1,\ldots l-1$.

Из (5.97)-(5.100) вытекает, что $x_1 \ldots x_l \in \mathbf{Z}^l_{p^k}$ – кратчайшее входное слово, переводящее состояние $\mathbf{q}_0 \in \mathbf{Z}^l_{p^k}$ в состояние $\mathbf{q}'_0 \in \mathbf{Z}^l_{p^k}$.

Следовательно, диаметр графа переходов любого автомата $M_j \in \tilde{\mathsf{A}}^{sc}_{l,j}$ $(j=1,2)$ равен l.

Следствие доказано.

Положим

$$\tilde{\mathsf{A}}^{sc-inv}_{l,j} = \tilde{\mathsf{A}}^{sc}_{l,j} \cap \tilde{\mathsf{A}}^{inv}_{l,j} \quad (j=1,2). \tag{5.101}$$

Следствие 5.16. Для всех $l \in \mathbf{N}$

$$\tilde{\mathsf{A}}^{sc-inv}_{l,2} = \tilde{\mathsf{A}}^{inv}_{l,2}. \tag{5.102}$$

Доказательство. Из (5.101) вытекает, что

$$\tilde{\mathsf{A}}^{sc-inv}_{l,2} \subseteq \tilde{\mathsf{A}}^{inv}_{l,2}. \tag{5.103}$$

Из утверждения 5.17 вытекает, что

$$\tilde{\mathsf{A}}^{inv}_{l,2} \subseteq \tilde{\mathsf{A}}^{sc-inv}_{l,2}. \tag{5.104}$$

Из включений (5.103) и (5.104) вытекает равенство (5.102).

Следствие доказано.

Из формулы (5.95), утверждений 5.16 и 5.17, а также теоремы 5.13 вытекает

Следствие 5.17. Для всех $l \in \mathbf{N}$

$$|\tilde{\mathsf{A}}^{sc-inv}_{l,j}| = (1-p^{-1})^2 \cdot |\tilde{\mathsf{A}}_{l,j}| \quad (j=1,2).$$

Теорема 5.14. Для всех $l \in \mathbf{N}$ автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$ является перестановочным автоматом тогда и только тогда, когда a_l – обратимый элемент кольца Z_{p^k}.

Доказательство. Автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$ не является перестановочным автоматом тогда и только тогда, когда существуют два такие его состояния

$$\mathbf{q}_0 = (q_{l-1},\ldots,q_1,q_0)^T \in \mathbf{Z}_{p^k}^l$$

и

$$\mathbf{q}_0' = (q_{l-1}',\ldots,q_1',q_0')^T \in \mathbf{Z}_{p^k}^l,$$

а также такой входной символ $x \in \mathbf{Z}_{p^k}$, что

$$\mathbf{q}_1 = \mathbf{q}_1', \tag{5.105}$$

где

$$\mathbf{q}_1 = (q_l,\ldots,q_1)^T \in \mathbf{Z}_{p^k}^l \tag{5.106}$$

и

$$\mathbf{q}_1' = (q_l',\ldots,q_1')^T \in \mathbf{Z}_{p^k}^l, \tag{5.107}$$

а значения q_l и q_l' вычисляются из 1-го уравнения, определяющего автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$.

Из (5.105)-(5.107) вытекает, что

$$q_i = q_i' \quad (i=1,\ldots l). \tag{5.108}$$

Так как $\mathbf{q}_0 \neq \mathbf{q}_0'$, то из (5.105)-(5.108) вытекает, что

$$\mathbf{q}_0 = (q_{l-1},\ldots,q_1,q_0)^T \in \mathbf{Z}_{p^k}^l$$

и

$$\mathbf{q}_0' = (q_{l-1},\ldots,q_1,q_0')^T \in \mathbf{Z}_{p^k}^l,$$

причем

$$q_0 \neq q_0'.$$

Так как $q_0 \neq q_0'$ и $q_l = q_l'$, то из 1-го уравнения, определяющего автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$, вытекает, что $q_0' \ominus q_0$ – ненулевое решение уравнения

$$a_l \circ u = 0. \tag{5.109}$$

Уравнение (5.109) имеет ненулевое решение тогда и только тогда, когда элемент $a_l \in \mathbf{Z}_{p^k}$ – необратимый элемент кольца Z_{p^k}.

Итак, показано, что автомат $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$ не является перестановочным автоматом тогда и только тогда, когда элемент $a_l \in \mathbf{Z}_{p^k}$ не является обратимым элементом кольца Z_{p^k}.

Теорема доказана.

Обозначим через $\tilde{\mathsf{A}}^{p}_{l,j}$ $(j=1,2)$ множество всех перестановочных автоматов $M_j \in \tilde{\mathsf{A}}_{l,j}$ $(j=1,2)$.

Из формулы (5.95) и теоремы 5.14 вытекает

Следствие 5.18. Для всех $l \in \mathbf{N}$

$$|\tilde{\mathsf{A}}^{p}_{l,j}| = (1-p^{-1})\cdot|\tilde{\mathsf{A}}_{l,j}| \quad (j=1,2).$$

Положим

$$\tilde{\mathsf{A}}^{p-inv}_{l,j} = \tilde{\mathsf{A}}^{p}_{l,j} \cap \tilde{\mathsf{A}}^{inv}_{l,j} \quad (j=1,2).$$

Из формулы (5.95), утверждений 5.16 и 5.17, а также теоремы 5.14 вытекает

Следствие 5.19. Для всех $l \in \mathbf{N}$

$$|\tilde{\mathsf{A}}^{p-inv}_{l,j}| = (1-p^{-1})^{j+1}\cdot|\tilde{\mathsf{A}}_{l,j}| \quad (j=1,2).$$

5.10. Выводы.

В настоящем разделе исследован класс линейных автоматов Мили и Мура над кольцом Z_{p^k} (где p – простое число, а $k \in \mathbf{N}$). Эти исследования проведены как с позиции теории автоматов, теории систем, а также с учетом возможного применения этих автоматов в качестве математических моделей при решении задач современной криптологии. Именно в силу последнего обстоятельства значительное внимание уделено исследованию обратимых линейных автоматов Мили и Мура над кольцом Z_{p^k}.

Основные результаты состоят в следующем:

1. Проработан аппарат линейной алгебры над кольцом Z_{p^k}. Оценено число обратимых матриц фиксированного порядка над кольцом Z_{p^k}. Исследованы решения линейных уравнений и систем линейных уравнений над кольцом Z_{p^k}.

2. Охарактеризованы основные нетривиальные подмножества линейных автоматов над кольцом Z_{p^k}, а именно: автоматов, в уравнения которых входят только диагональные матрицы, автоматов, у которых граф переходов – полный граф с петлями, перестановочных автоматов, приведенных автоматов, автоматов, имеющих состояния-близнецы.

Оценены мощности этих подмножеств автоматов.

3. Установлены критерии эквивалентности линейных автоматов над кольцом Z_{p^k}, а также охарактеризованы классы эквивалентных состояний линейного автомата над кольцом Z_{p^k}.

4. Решены задачи параметрической идентификации и идентификации начального состояния для линейных автоматов над кольцом Z_{p^k}.

5. Охарактеризована структура множества неподвижных точек словарных функций, реализуемых инициальными линейными автоматами над кольцом Z_{p^k}.

6. Построены канонические формы линейных автоматов над кольцом Z_{p^k}, характеризующиеся тем, что все выполняемые в его представлении линейные преобразования либо обратимые линейные преобразования, либо представлены диагональными матрицами.

7. Охарактеризована вариация о.-д. функции, реализуемой инициальным линейным автоматом над кольцом Z_{p^k}, при вариации определяющих ее матриц, вариации начального состояния, а также вариации входной последовательности.

8. Охарактеризованы линейные одномерные автоматы с лагом l над кольцом Z_{p^k}.

6. НЕЛИНЕЙНЫЕ АВТОМАТЫ НАД КОНЕЧНЫМ КОЛЬЦОМ

Целью настоящего раздела является систематическое исследование нелинейных автоматов над кольцом $Z_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbf{N}$). Таким образом, настоящий раздел представляет собой логическое продолжение исследований, представленных в предыдущем разделе.

Пп.6.1-6.4 посвящены исследованию нелинейных автоматов Мили и Мура с лагом 1 над конечным кольцом, в предположении, что «нелинейность» характеризуется следующим образом: изменение значений переменных состояний и выходных переменных представлено алгебраической суммой квадратичной и линейной форм от переменных состояний с линейной формой от входных переменных. Выбор объекта исследования обусловлен тем, что аналоги над конечным кольцом для большинства хаотических динамических систем укладываются в рамки именно таких моделей. В п.6.1 представлены исследуемые модели – нелинейные автоматы Мили и Мура с лагом 1 над конечным кольцом. Выделены, а также охарактеризованы подмножества нелинейных автоматов, представляющих собой поточные шифры, которые исследуются в пп.6.2-6.4. В п.6.2 охарактеризованы классы эквивалентных состояний исследуемых автоматов. В п.6.3 решены задачи параметрической идентификации и идентификации начального состояния для исследуемых автоматов. В п.6.4 исследуется вариация поведения автоматов при вариации его параметров либо при вариации его начального состояния.

В п.6.5 исследуется задача построения поточного шифра на основе псевдофракталов. Охарактеризован класс семейств легко вычислимых перестановок, применяемых при построении таких шифров.

В п.6.6 исследуются два типа нелинейных автоматов над конечным кольцом, являющихся аналогами симметричных хаотических динамических систем, а именно: Guckenheimer and Holmes cycle и free-running system [239]. Эти автоматы характеризуются тем, что, во-первых, они не укладываются в рамки моделей, исследованных в пп.6.1-6.4, а, во-вторых, они обладают нетривиальной группой симметрий. С позиции теории автоматов охарактеризованы структуры исследуемых автоматов. Решены задачи параметрической идентификации и идентификации начального состояния. Исследована структура множества неподвижных точек словарных функций, реализуемых инициальными автоматами.

В настоящем разделе систематически изложены результаты, полученные в работах [69,84,146,147,154,155,175,178,179,182,183,185-187,189,294,205,306,307].

6.1. Исследуемые модели.

Рассмотрим инициальные автоматы Мили и Мура над кольцом Z_{p^k}, определяемые, соответственно, рекуррентными соотношениями

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G \circ \mathbf{q}_t \oplus F \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (6.1)$$

и

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G \circ \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (6.2)$$

где $\mathbf{q}_t = (q_t^{(1)},\ldots,q_t^{(n)})^T$, $\mathbf{x}_t = (x_t^{(1)},\ldots,x_t^{(n)})^T$ и $\mathbf{y}_t = (y_t^{(1)},\ldots,y_t^{(n)})^T$ – соответственно, состояние автомата, входной и выходной символ в момент t, $\mathbf{b} = (b^{(1)},\ldots,b^{(n)})^T \in \mathbf{Z}_{p^k}^n$ и $\mathbf{d} = (d^{(1)},\ldots,d^{(n)})^T \in \mathbf{Z}_{p^k}^n$ – фиксированные векторы, а $A,C,E,G,F \in \mathsf{M}_n$ – фиксированные матрицы.

С позиции теории автоматов выделение класса автоматов, представимых в виде (6.1) или (6.2), заслуживает внимания из-за возможности применения для их исследования аппарата современной алгебры, а также в связи со следующим обстоятельством.

При логарифмическом весе [15] емкостная сложность представления автомата M соотношениями (6.1) или (6.2) равна

$$V = O(n^2 \cdot k \cdot \lceil \log p \rceil) \quad (p,k,n \to \infty).$$

В тоже время емкостная сложность представления каждого из автоматов M_1 и M_2 автоматной таблицей равна

$$V = O(p^{2 \cdot k \cdot n} \cdot k \cdot \lceil \log p \rceil) \quad (p,k,n \to \infty).$$

Обозначим через $\mathrm{A}_{n,1}$ множество всех автоматов M_1, определяемых формулой (6.1), а через $\mathrm{A}_{n,2}$ – множество всех автоматов M_2, определяемых формулой (6.2).

Из (5.5) вытекает, что

$$|\mathrm{A}_{n,1}| = p^{5 \cdot k \cdot n^2 + 2 \cdot k \cdot n} \tag{6.3}$$

и

$$|\mathrm{A}_{n,2}| = p^{4 \cdot k \cdot n^2 + 2 \cdot k \cdot n}. \tag{6.4}$$

Истинны следующие два утверждения.

Утверждение 6.1. Автомат $M_1 \in \mathrm{A}_{n,1}$ является обратимым автоматом тогда и только тогда, когда $F \in \mathsf{M}_n^{inv}$.

Утверждение 6.2. Автомат $M_2 \in \mathrm{A}_{n,2}$ является обратимым автоматом тогда и только тогда, когда $E,G \in \mathsf{M}_n^{inv}$.

Доказательство этих утверждений аналогично доказательству утверждений 1.6 и 1.7.

В случае, когда автоматы $M_1 \in \mathrm{A}_{n,1}$ и $M_2 \in \mathrm{A}_{n,2}$ являются обратимыми автоматами, соответствующие им обратные автоматы имеют, соответственно, вид:

$$(M_1^{-1},\mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C_1 \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E_1 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = F^{-1} \circ (\mathbf{x}_{t+1} \Theta G \circ \mathbf{q}_t) \end{cases} \quad (t \in \mathbf{Z}_+)$$

где $C_1 = C \Theta E \circ F^{-1} \circ G$, $E_1 = E \circ F^{-1}$ и

$$(M_2^{-1},\mathbf{q}_0):\begin{cases}\mathbf{q}_{t+1}=G^{-1}\circ\mathbf{y}_{t+1}\\ \mathbf{y}_{t+1}=E^{-1}\circ(G^{-1}\circ\mathbf{x}_{t+1}\Theta(A\circ\mathbf{q}_t\circ\mathbf{q}_t^T\circ\mathbf{b}\oplus C\circ\mathbf{q}_t\oplus\mathbf{d}))\end{cases}\quad(t\in\mathbf{Z}_+).$$

Обозначим через $\mathrm{A}_{n,i}^{inv}$ $(i=1,2)$ множество всех обратимых автоматов $M_i\in\mathrm{A}_{n,i}$.

Теорема 6.1. Для всех $n\in\mathbf{N}$

$$(n!\cdot(p-1)\cdot p^{-n^2})^i\cdot p^{3\cdot k\cdot n}\cdot|\mathrm{M}_n|^{6-i}\le|\mathrm{A}_{n,i}^{inv}|\le(1\text{-}p^{-n})^{i\cdot n}\cdot p^{3\cdot k\cdot n}\cdot|\mathrm{M}_n|^{6-i}\quad(i=1,2).$$

Доказательство теоремы 6.1 аналогично доказательству теоремы 5.2.

Ясно, что $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M\in\mathrm{A}_{n,1}^{inv}\cup\mathrm{A}_{n,2}^{inv})$ представляет собой симметричный поточный шифр с гаммированием, построенный на основе нелинейного автоключа (рис. 6.1).

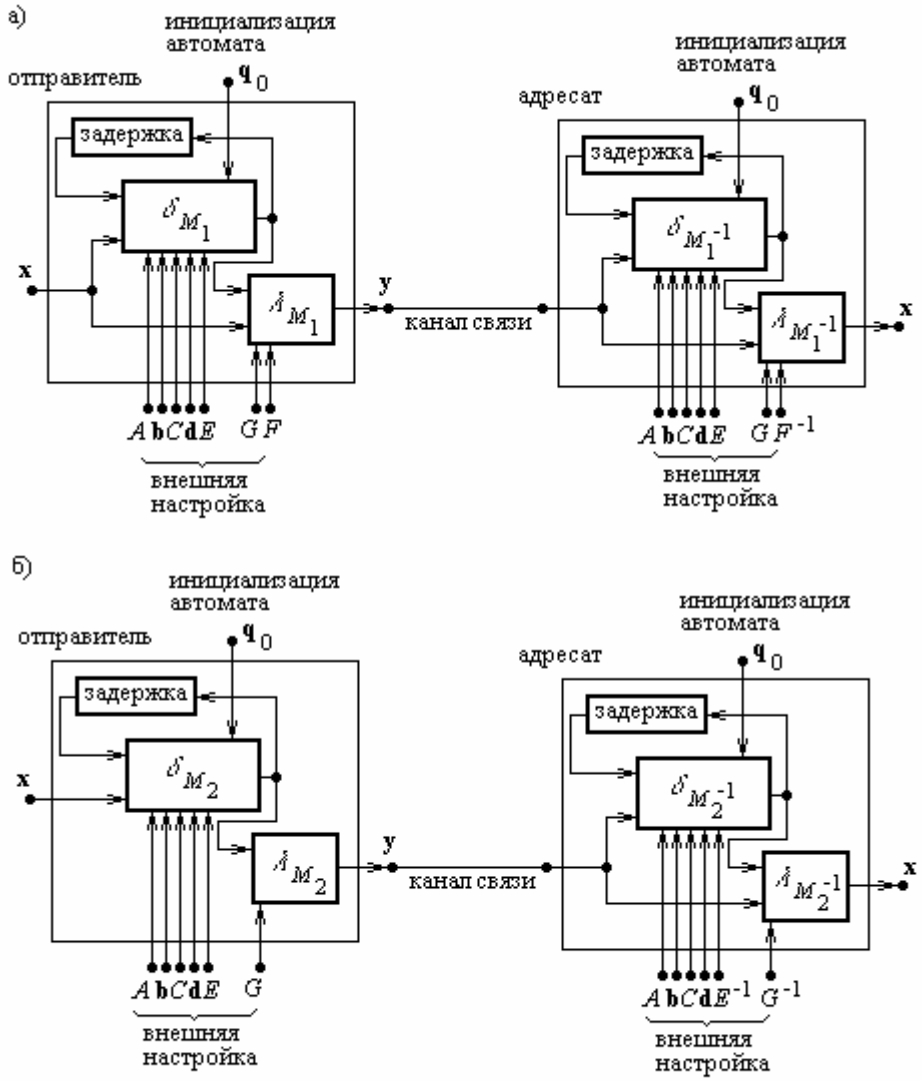


Рис. 6.1. Шифр $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$: а) $M=M_1$; б) $M=M_2$.

Отметим, что шифр $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ характеризуется тем, что в процессе шифрования осуществляется движение по некоторой траектории в пространстве состояний, а в процессе расшифровки – движение в том же пространстве состояний по той же траектории в том же самом направлении.

Секретным ключом для шифра $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ являются параметры и начальное состояние автомата.

Из (6.3) и (6.4) вытекает

Утверждение 6.3. Длина L (в битах) секретного ключа шифра $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ равна

$$L = k \cdot n \cdot \lceil \log p \rceil \cdot (5 \cdot n + 3),$$

если $M \in \mathrm{A}_{n,1}^{inv}$ и

$$L = k \cdot n \cdot \lceil \log p \rceil \cdot (4 \cdot n + 3),$$

если $M \in \mathrm{A}_{n,2}^{inv}$.

Убедиться в том, что $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ представляет собой шифр с гаммированием на основе нелинейного автоключа можно следующим образом.

Ассоциируем с автоматами $(M_1,\mathbf{q}_0)$ и $(M_2,\mathbf{q}_0)$ следующий автомат без выхода

$$\mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1} \quad (t \in \mathbf{Z}_+).$$

Будем рассматривать этот автомат как генератор гаммы с автоключом.

Шифр, построенный на основе автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$, имеет вид, представленный на рис. 6.2.а, а шифр, построенный на основе автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$, имеет вид, представленный на рис. 6.2.б.

Отличие этих схем от классической схемы К. Шеннона, представленной на рис. 6.2.в, состоит не только в том, что вычисление осуществляется в кольце Z_{p^k} (а не в поле $\mathbf{GF}(2)$), но и в наличии линейных преобразований (т.е. перестановок), определенных на множестве $\mathbf{Z}_{p^k}$.

Отметим, что шифр $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ осуществляет шифрование без увеличения длины исходного текста, если $p = 2$, а если $p \neq 2$, то длина шифртекста превышает длину исходного текста на величину

$$\Delta = k \cdot l \cdot (\lceil \log p \rceil - \lfloor \log p \rfloor),$$

где l – длина исходного текста (в битах).

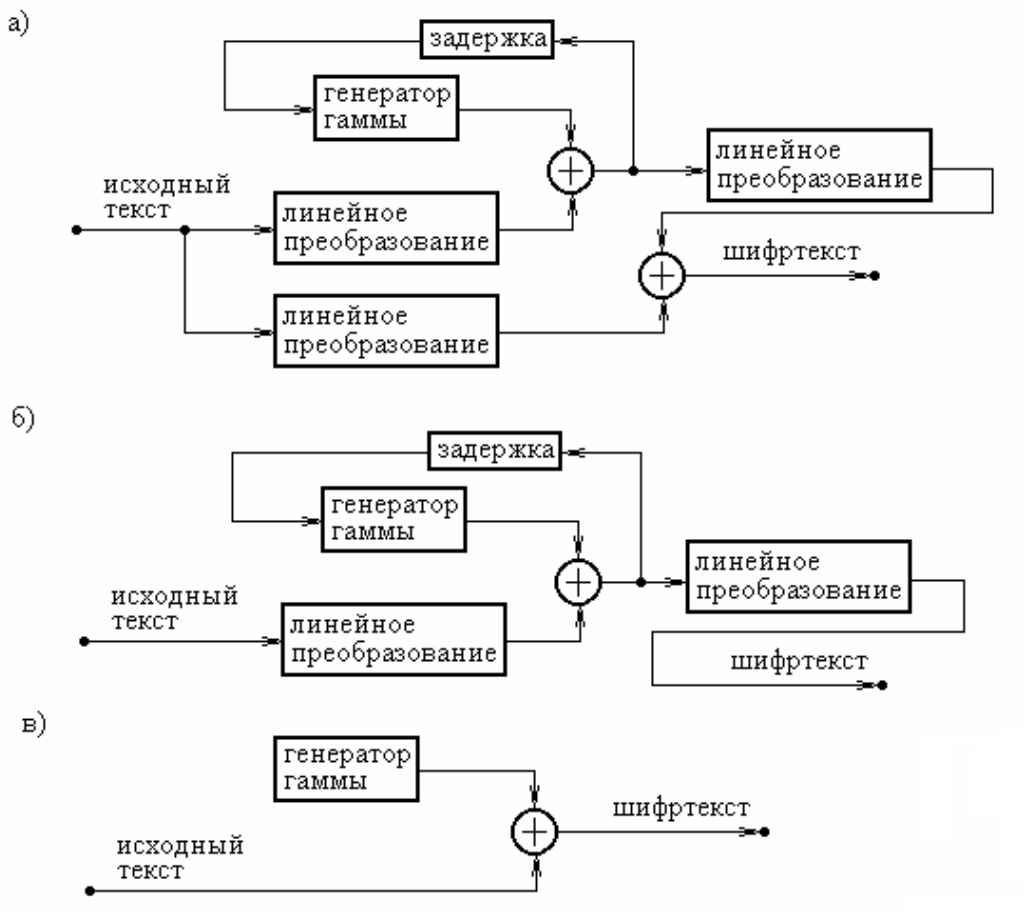


Рис. 6.2. Шифры с гаммированием: а) $M = M_1$; б) $M = M_2$; в) классическая схема К. Шеннона.

Охарактеризуем пару взаимно обратных инициальных автоматов $(M, \mathbf{q_0})$ и $(M^{-1}, \mathbf{q_0})$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ с позиции преобразователей информации при передаче информации по каналу связи (рис. 6.3).

Поместим в источнике информации автомат $(M, \mathbf{q_0})$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$, а у адресата – автомат $(M^{-1}, \mathbf{q_0})$, снабженный схемой коррекции состояния, и схему, осуществляющую вычисление функции переходов δ_M.

Предположим, что информация представлена словами в алфавите $\mathbf{Z}_{p^k}$, а входной символ автомата M имеет вид

$$\mathbf{x}^T = (\underbrace{x, \ldots, x}_{n \ раз}),$$

т.е. в процессе преобразования информации осуществляется ее n-кратное (посимвольное) дублирование. Мажоритарная схема на выходе автомата $(M^{-1}, \mathbf{q_0})$ дает возможность обнаружить $n-1$, а также исправить $\lfloor 0.5 \cdot (n-1) \rfloor$ ошибок, возникших именно в процессе передачи информации по каналу связи (но не при вычислениях, осуществляемых автоматами

$(M, \mathbf{q_0})$ и $(M^{-1}, \mathbf{q_0})$). При этом схема, осуществляющую вычисление функции переходов δ_M, дает возможность вычислить корректное состояние автомата M^{-1}.

Для контроля ошибок, возникающих именно при вычислениях, осуществляемых автоматами $(M, \mathbf{q_0})$ и $(M^{-1}, \mathbf{q_0})$ (но не в процессе передачи информации по каналу связи), достаточно в их представлениях добавить проверочные символы для величин $\mathbf{x}, \mathbf{y}$ и $\mathbf{q}$ в соответствии со стандартными методами построения блоковых кодов, контролирующих ошибки (см., напр. [21]).

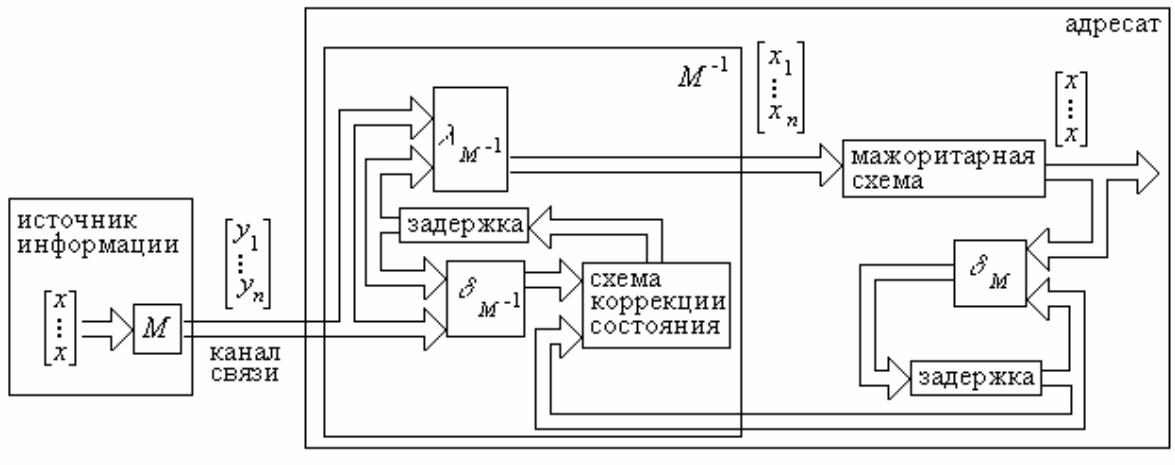


Рис. 6.3. Схема контроля ошибок в процессе передачи информации по каналу связи.

В дальнейшем предполагается, что $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv}$.

Рассмотрим основные характеристики автомата $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv}$ с позиции теории автоматов.

Пусть $E \in \mathsf{M}_n^{inv}$. Определим семейство отображений

$$\mathbf{f_u} : \mathbf{Z}_{p^k}^n \to \mathbf{Z}_{p^k}^n \quad (\mathbf{u} \in \mathbf{Z}_{p^k}^n),$$

равенством

$$\mathbf{f_u}(\mathbf{x}) = A \circ \mathbf{u} \circ \mathbf{u}^T \circ \mathbf{b} \oplus C \circ \mathbf{u} \oplus \mathbf{d} \oplus E \circ \mathbf{x} \quad (\mathbf{x} \in \mathbf{Z}_{p^k}^n).$$

Ясно, что при каждом фиксированном значении $\mathbf{u} \in \mathbf{Z}_{p^k}^n$ отображение $\mathbf{f_u}$ является перестановкой множества $\mathbf{Z}_{p^k}^n$.

Отсюда вытекает, что для любых фиксированных значений $\mathbf{v}, \mathbf{u} \in \mathbf{Z}_{p^k}^n$ уравнение

$$\mathbf{v} = A \circ \mathbf{u} \circ \mathbf{u}^T \circ \mathbf{b} \oplus C \circ \mathbf{u} \oplus \mathbf{d} \oplus E \circ \mathbf{x} \qquad (6.5)$$

имеет единственное решение $\mathbf{x} \in \mathbf{Z}_{p^k}^n$.

Таким образом:

1) если $E \in \mathsf{M}_n^{inv}$, то автомат $M \in \mathrm{A}_{n,1}^{inv}$ – сильно связный перестановочный автомат, причем диаметр его графа переходов равен 1;

2) автомат $M \in \mathrm{A}_{n,2}^{inv}$ является сильно связным перестановочным автомат, причем диаметр его графа переходов равен 1 (так как $E \in \mathsf{M}_n^{inv}$ для любого автомата $M \in \mathrm{A}_{n,2}^{inv}$).

Утверждение 6.4. Если $E \in \mathsf{M}_n^{non\_inv}$, то или автомат $M \in \mathrm{A}_{n,1}^{inv}$ несвязен, или диаметр его графа переходов больше, чем 1.

Доказательство. Зафиксируем произвольный элемент $\mathbf{u} \in \ker A \cap \ker C$ (это всегда возможно сделать, так как $\ker A \cap \ker C \neq \varnothing$ для любых линейных операторов, определенных на M_n-модуле $(\mathbf{Z}_{p^k}^n, \oplus)$). Подставив выбранное значение $\mathbf{u}$ в (6.5), получим

$$\mathbf{v} = \mathbf{d} \oplus E \circ \mathbf{x}. \qquad (6.6)$$

Так как $E \in \mathsf{M}_n^{non\_inv}$, то

$$Val\ E \subset \mathbf{Z}_{p^k}^n .$$

Следовательно, существует такой элемент $\mathbf{v} \in \mathbf{Z}_{p^k}^n$, что

$$\mathbf{v} \ominus \mathbf{d} \notin Val\ E .$$

Подставим это значение $\mathbf{v}$ в (6.6). Тогда уравнение (6.6) не имеет решений.

Следовательно, если $\mathbf{q}'$ и $\mathbf{q}''$ – такие состояния автомата $M \in \mathrm{A}_{n,1}^{inv}$, что

$$\mathbf{q}' \in \ker A \cap \ker C$$

и

$$\mathbf{q}'' \ominus \mathbf{d} \notin Val\ E,$$

то для всех $\mathbf{x} \in \mathbf{Z}_{p^k}^n$.

$$\mathbf{q}'' \neq A \circ \mathbf{q}' \circ (\mathbf{q}')^T \circ \mathbf{b} \oplus C \circ \mathbf{q}' \oplus \mathbf{d} \oplus E \circ \mathbf{x}$$

Отсюда вытекает, что, или состояния $\mathbf{q}'$ и $\mathbf{q}''$ принадлежат разным компонентам связности автомата $M \in \mathrm{A}_{n,1}^{inv}$, или в графе переходов автомата $M \in \mathrm{A}_{n,1}^{inv}$ расстояние между вершинами, соответствующими состояниям $\mathbf{q}'$ и $\mathbf{q}''$, больше, чем 1.

Утверждение доказано.

При построении шифров на основе аналогов над кольцом Z_{p^k} хаотических динамических систем вместо автомата $(M, \mathbf{q_0})$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$ часто более удобно использовать инициальные автоматы Мили $(M_3, \mathbf{q}_0)$ и

инициальные автоматы Мура $(M_4, \mathbf{q}_0)$, определяемые следующими четырьмя условиями.

Условие 6.1. Инициальные автоматы $(M_3, \mathbf{q}_0)$ и $(M_4, \mathbf{q}_0)$определяются, соответственно, соотношениями (6.1) и (6.2).

Условие 6.2. Зафиксировано r $(1 \le r \le n)$ таких упорядоченных пар чисел (i_h, j_h) $(h = 1, \ldots, r)$, что:

1) $i_h, j_h \in \mathbf{N}_n$ для всех $h = 1, \ldots, r$;

2) если $h_1 \ne h_2$ $(h_1, h_2 = 1, \ldots, r)$, то $i_{h_1} \ne i_{h_2}$ и $j_{h_1} \ne j_{h_2}$.

Условие 6.3. В каждой из матриц E, G, F в клетках (i_h, j_h) $(h = 1, \ldots, r)$ расположены обратимые элементы кольца Z_{p^k}, а во всех остальных клетках – нули.

Условие 6.4. Входной алфавит каждого из автоматов M_3 и M_4 – это множество всех таких векторов $\mathbf{x} = (x^{(1)}, \ldots, x^{(n)})^T \in \mathbf{Z}_{p^k}^n$, что $x^{(j)} = 0$ для всех $j \in \mathbf{N}_n \setminus \{j_1, \ldots, j_r\}$.

За счет изменения нумерации компонент векторов $\mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{b}, \mathbf{d}$ представления (6.1) и (6.2) автоматов $(M_3, \mathbf{q}_0)$ и $(M_4, \mathbf{q}_0)$ могут быть приведены, соответственно, к виду

$$(M_3, \mathbf{q}_0): \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \\ q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \ \ (i = r+1, \ldots, n) \\ y_{t+1}^{(i)} = g_i \circ q_t^{(i)} \oplus f_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+) \qquad (6.7)$$

где $A_i \in \mathsf{M}_n$ $(i = 1, \ldots, n)$ – фиксированные матрицы, f_i $(i = 1, \ldots, r)$ – фиксированные обратимые элементы кольца Z_{p^k}, а $\mathbf{c}_i = (c_i^{(1)}, \ldots, c_i^{(n)}) \in \mathbf{Z}_{p^k}^n$ $(i = 1, \ldots, n)$ – фиксированный вектор и

$$(M_4, \mathbf{q}_0): \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \\ q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \ \ (i = r+1, \ldots, n) \\ y_{t+1}^{(i)} = g_i \circ q_{t+1}^{(i)} \quad (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (6.8)$$

где $A_i \in \mathsf{M}_n$ $(i = 1, \ldots, n)$ – фиксированные матрицы, e_i, g_i $(i = 1, \ldots, r)$ – фиксированные обратимые элементы кольца Z_{p^k}, а $\mathbf{c}_i = (c_i^{(1)}, \ldots, c_i^{(n)}) \in \mathbf{Z}_{p^k}^n$ $(i = 1, \ldots, n)$ – фиксированный вектор.

Отметим, что если $p \neq 2$, то в качестве $A_i \in \mathsf{M}_n$ $(i = 1, \ldots, n)$ всегда могут быть выбраны симметрические матрицы.

Обозначим через $\mathrm{A}_{n,3}$ множество всех автоматов M_3, определяемых формулой (6.7), а через $\mathrm{A}_{n,4}$ – множество всех автоматов M_4, определяемых формулой (6.8). Отметим, что любой автомат $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ является обратимым автоматом. При этом

$$\mathrm{A}_{n,3} \subsetneq \mathrm{A}_{n,1}^{inv}$$

и

$$\mathrm{A}_{n,4} \subsetneq \mathrm{A}_{n,2}^{inv}.$$

Более того, утверждения

$$M_3 \in \mathrm{A}_{n,3} \Rightarrow M_3 \in \mathrm{A}_{n,1}^{inv}$$

и

$$M_4 \in \mathrm{A}_{n,4} \Rightarrow M_4 \in \mathrm{A}_{n,2}^{inv}$$

истинны тогда и только тогда, когда $r = n$.

Ясно, что $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ $(M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4})$ – симметричный поточный шифр с гаммированием, построенный на основе нелинейного автоключа, который (как и шифр $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv})$) характеризуется тем, что в процессе шифрования осуществляется движение по некоторой траектории в пространстве состояний, а в процессе расшифровки – движение в том же пространстве состояний по той же траектории в том же самом направлении.

Кроме того, в соответствии со схемой, представленной на рис. 6.3, для шифра $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ $(M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4})$ можно организовать обнаружение $r-1$ и исправление $\lfloor 0.5 \cdot (r-1) \rfloor$ ошибок, возникших именно в процессе передачи информации по каналу связи (но не при вычислениях, осуществляемых автоматами $(M, \mathbf{q_0})$ и $(M^{-1}, \mathbf{q_0})$).

Утверждение 6.5. Пусть $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$. Тогда:

1) если $r = n$, то M – сильно связный перестановочный автомат, причем диаметр его графа переходов равен 1;

2) если $r < n$, то или M автомат несвязен, или диаметр его графа переходов больше, чем 1.

Доказательство. 1. Пусть $r = n$. Для каждого обратимого элемента $e \in \mathbf{Z}_{p^k}$ кольца Z_{p^k} определим семейство отображений

$$\mathbf{f}_{\mathbf{u}} : \mathbf{Z}_{p^k} \to \mathbf{Z}_{p^k} \quad (\mathbf{u} \in \mathbf{Z}_{p^k}^n)$$

равенством

$$\mathbf{f}_{\mathbf{u}}(x) = \mathbf{u}^T \circ A \circ \mathbf{u} \oplus \mathbf{c} \circ \mathbf{u} \oplus d \oplus e \circ x \quad (x \in \mathbf{Z}_{p^k}).$$

Ясно, что при каждом фиксированном значении $\mathbf{u} \in \mathbf{Z}_{p^k}^n$ отображение $\mathbf{f}_\mathbf{u}$ является перестановкой множества $\mathbf{Z}_{p^k}$.

Отсюда вытекает, что для любых состояний

$$\mathbf{q} = (q^{(1)}, \ldots, q^{(n)})^T$$

и

$$\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \ldots, \tilde{q}^{(n)})^T$$

автомата $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ система уравнений

$$\begin{cases} \tilde{q}^{(1)} = \mathbf{q}^T \circ A_1 \circ \mathbf{q} \oplus \mathbf{c}_1 \circ \mathbf{q} \oplus d_1 \oplus e_1 \circ x^{(1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{q}^{(n)} = \mathbf{q}^T \circ A_n \circ \mathbf{q} \oplus \mathbf{c}_n \circ \mathbf{q} \oplus d_n \oplus e_n \circ x^{(n)} \end{cases}$$

имеет единственное решение $\mathbf{x} = (x^{(1)}, \ldots, x^{(n)})^T \in \mathbf{Z}_{p^k}^n$ (так как $e_1, \ldots, e_n$ – обратимые элементы кольца Z_{p^k}).

Отсюда, в свою очередь, вытекает, что если $r = n$, то $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ – сильно связный перестановочный автомат, причем диаметр его графа переходов равен 1, что и требовалось доказать.

2. Пусть $r < n$. Выберем такие состояния $\mathbf{q} = (q^{(1)}, \ldots, q^{(n)})^T$ и $\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \ldots, \tilde{q}^{(n)})^T$ автомата $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$, что $\tilde{q}^{(i)}$ $(i = r+1, \ldots, n)$ – обратимый элемент кольца Z_{p^k}, если элемент $\mathbf{q}^T \circ A_i \circ \mathbf{q} \oplus \mathbf{c}_i \circ \mathbf{q} \oplus d_i$ не является обратимым в кольце Z_{p^k}, и элемент $\tilde{q}^{(i)}$ $(i = r+1, \ldots, n)$ не является обратимым в кольце Z_{p^k}, если $\mathbf{q}^T \circ A_i \circ \mathbf{q} \oplus \mathbf{c}_i \circ \mathbf{q} \oplus d_i$ – обратимый элемент кольца Z_{p^k}.

Тогда система уравнений

$$\begin{cases} \tilde{q}_1 = \mathbf{q}^T \circ A_1 \circ \mathbf{q} \oplus \mathbf{c}_1 \circ \mathbf{q} \oplus d_1 \oplus e_1 \circ x_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{q}_r = \mathbf{q}^T \circ A_r \circ \mathbf{q} \oplus \mathbf{c}_r \circ \mathbf{q} \oplus d_r \oplus e_r \circ x_r \\ \tilde{q}_{r+1} = \mathbf{q}^T \circ A_{r+1} \circ \mathbf{q} \oplus \mathbf{c}_{r+1} \circ \mathbf{q} \oplus d_{r+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{q}_n = \mathbf{q}^T \circ A_n \circ \mathbf{q} \oplus \mathbf{c}_n \circ \mathbf{q} \oplus d_n \end{cases}$$

является несовместной.

Отсюда вытекает, что если $r < n$, то или автомат $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ несвязен, или диаметр его графа переходов больше, чем 1.

Утверждение доказано.

Утверждение 6.6. Из каждого состояния $\mathbf{q}=(q^{(1)},\ldots,q^{(n)})^T$ автомата $M\in \mathrm{A}_{n,4}$ 1-достижимыми являются в точности $p^{k\cdot r}$ различных состояния автомата $M\in \mathrm{A}_{n,4}$

Доказательство. Из (6.8) вытекает, что значения компонент $q_{t+1}^{(i)}$ $(i=r+1,\ldots,n)$ состояния, в которое автомат $M\in \mathrm{A}_{n,4}$ переходит под действием любого входного символа $(x_{t+1}^{(1)},\ldots,x_{t+1}^{(r)},\underbrace{0,\ldots,0}_{n-r\ раз})^T\in \mathbf{Z}_{p^k}^n$, не зависят от значения этого входного символа.

Так как e_i $(i=1,\ldots,r)$ – обратимые элементы кольца Z_{p^k}, то при каждом фиксированном значении вектора $\mathbf{u}\in \mathbf{Z}_{p^k}^n$ для любых $q_1,\ldots,q_r\in \mathbf{Z}_{p^k}$ система уравнений

$$\begin{cases} q_1=\mathbf{q}^T\circ A_1\circ\mathbf{q}\oplus\mathbf{c}_1\circ\mathbf{q}\oplus d_1\oplus e_1\circ x_1 \\ \quad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ q_r=\mathbf{q}^T\circ A_r\circ\mathbf{q}\oplus\mathbf{c}_r\circ\mathbf{q}\oplus d_r\oplus e_r\circ x_r \end{cases}$$

имеет (единственное) решение.

Число различных векторов $\tilde{\mathbf{q}}=(\tilde{q}^{(1)},\ldots,\tilde{q}^{(n)})^T$, у которых фиксированы последние $n-r$ компонент, а первые r компонент – произвольные элементы кольца Z_{p^k} равно $p^{k\cdot r}$.

Утверждение доказано.

Пример 6.1. Построим автомат $(M,\mathbf{q}_0)$ $(M\in \mathrm{A}_{n,4})$ для некоторых модельных динамических систем, рассмотренных в п.1.7.

1. Рассмотрим систему Рёсслера

$$\begin{cases} \dot{x}=-y-z \\ \dot{y}=x+a\cdot y \\ \dot{z}=b+(x-r)\cdot z \end{cases}.$$

Внесем информационную переменную в 1-ое уравнение.

Перейдя к вычислениям в кольце Z_{p^k}, получим автомат

$$(M_R,\mathbf{q}_0):\begin{cases} q_{t+1}^{(1)}=q_t^{(1)}\Theta h\circ q_t^{(2)}\Theta h\circ q_t^{(3)}\Theta h\circ d\circ x_{t+1} \\ q_{t+1}^{(2)}=h\circ q_t^{(1)}\oplus(a\circ h\oplus 1)\circ q_t^{(2)} \\ q_{t+1}^{(3)}=h\circ b\oplus(1\Theta h\circ r)\circ q_t^{(3)}\oplus h\circ q_t^{(1)}\circ q_t^{(3)} \\ y_{t+1}=q_{t+1}^{(1)} \end{cases}\quad (t\in \mathbf{Z}_+),\qquad (6.9)$$

где $a,b,d,h,r\in \mathbf{Z}_{p^k}$, причем d и h – обратимые элементы кольца Z_{p^k}.

2. Рассмотрим 1-ю систему Спротта

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + y \cdot z \\ \dot{z} = 1 - y^2 \end{cases}.$$

Внесем информационную переменную в 1-ое уравнение. Перейдя к вычислениям в кольце Z_{p^k}, получим автомат

$$(M_{S_1}, \mathbf{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \Theta h \circ a \circ x_{t+1} \\ q_{t+1}^{(2)} = q_t^{(2)} \Theta h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)} \\ q_{t+1}^{(3)} = h \oplus q_t^{(3)} \Theta h \circ (q_t^{(2)})^2 \\ y_{t+1} = q_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (6.10)$$

где $a, h \in \mathbf{Z}_{p^k}$ – обратимые элементы кольца Z_{p^k}.

3. Рассмотрим систему Лоренца

$$\begin{cases} \dot{x} = a_1 \cdot (y - x) \\ \dot{y} = x \cdot (a_2 - z) - y \\ \dot{z} = x \cdot y - a_3 \cdot z \end{cases}$$

Внесем информационную переменную во 2-ое уравнение. Перейдя к вычислениям в кольце Z_{p^k}, получим автомат

$$(M_L, \mathbf{q}_0) \begin{cases} q_{t+1}^{(1)} = (1 \Theta h \circ a_1) \circ q_t^{(1)} \oplus h \circ a_1 \circ q_t^{(2)} \\ q_{t+1}^{(2)} = (1 \Theta h) \circ q_t^{(2)} \oplus h \circ q_t^{(1)} \circ (a_2 \Theta q_t^{(3)}) \Theta h \circ a \circ x_{t+1} \\ q_{t+1}^{(3)} = (1 \Theta h \circ a_3) \circ q_t^{(3)} \oplus h \circ q_t^{(1)} \circ q_t^{(2)} \\ y_{t+1} = q_{t+1}^{(2)} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.11)$$

где $a_1, a_2, a_3, a, h \in \mathbf{Z}_{p^k}$, причем a и h – обратимые элементы кольца $\mathbf{z}_{p^k}$.

4. Перейдем от отображения Эно

$$\begin{cases} x_{n+1} = 1 - a \cdot x_n^2 - b \cdot y_n \\ y_{n+1} = x_n \end{cases} \quad (n \in \mathbf{Z}_+)$$

к отображению

$$x_{t+2} = 1 - a \cdot x_{t+1}^2 - b \cdot x_t \quad (t \in \mathbf{Z}_+).$$

Добавим информационную переменную. Перейдя к вычислениям в кольце Z_{p^k}, получим автомат

$$(M_H, \mathbf{q}_0): \begin{cases} q_{t+2} = 1\Theta a \circ q_{t+1}^2 \Theta b \circ q_t \oplus c \circ x_{t+1} \\ y_{t+1} = q_{t+2} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.12)$$

где $c \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}.

6.2. Эквивалентность состояний исследуемых автоматов.

Исследуем вначале автомат $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv}$.

Теорема 6.2. Если $G \in \mathsf{M}_n^{inv}$, то автомат $M_1 \in \mathrm{A}_{n,1}^{inv}$ является приведенным автоматом.

Доказательство. Предположим противное, т.е. что $G \in \mathsf{M}_n^{inv}$, а автомат $M_1 \in \mathrm{A}_{n,1}^{inv}$ не является приведенным автоматом.

Тогда существуют эквивалентные состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$.

Подставив $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ во 2-е уравнение системы (6.1), получим, что для любого входного символа $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$

$$\mathbf{y}_1^{(2)} = G \circ \mathbf{q}_0^{(2)} \oplus F \circ \mathbf{x}_1$$

и

$$\mathbf{y}_1^{(1)} = G \circ \mathbf{q}_0^{(1)} \oplus F \circ \mathbf{x}_1.$$

Так как $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ – эквивалентные состояния автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$, то

$$\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)}$$

для всех $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$. Следовательно,

$$G \circ (\mathbf{q}_0^{(2)} \Theta \mathbf{q}_0^{(1)}) = \mathbf{0}.$$

А так как $G \in \mathsf{M}_n^{inv}$, то из последнего равенства получим

$$\mathbf{q}_0^{(2)} \Theta \mathbf{q}_0^{(1)} = \mathbf{0},$$

т.е.

$$\mathbf{q}_0^{(1)} = \mathbf{q}_0^{(2)}.$$

Полученное противоречие показывает, что предположение – ложное, т.е. $M_1 \in \mathrm{A}_{n,1}^{inv}$ – приведенный автомат.

Теорема доказана.

Следствие 6.1. Если $G \in \mathsf{M}_n^{inv}$, то любые два состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$ различаются любым входным символом $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$.

Доказательство. Из доказательства теоремы 6.2 вытекает, что равенство

$$\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)}$$

эквивалентно равенству

$$\mathbf{q}_0^{(1)} = \mathbf{q}_0^{(2)}.$$

Следствие доказано.

Теорема 6.3. Если $G \in \mathsf{M}_n^{non\_inv}$, то состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$ являются эквивалентными состояниями тогда и только тогда, когда

$$G \circ (\mathbf{q}_0^{(2)} \Theta \mathbf{q}_0^{(1)}) = \mathbf{0} \tag{6.13}$$

и

$$G \circ (\mathbf{q}_t^{(2)} \Theta \mathbf{q}_t^{(1)}) = \mathbf{0} \quad (t = 1, \ldots, p^{kn} - 2) \tag{6.14}$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbf{Z}_{p^k}^{n \cdot t}$.

Доказательство. Известно (см., напр., [30]), что два неэквивалентных состояния автомата $M = (Q, X, Y, \delta, \lambda)$ являются $(|Q| - 1)$-различимыми состояниями.

Число состояний автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$ равно p^{kn}.

Следовательно, состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\mathbf{y}_1^{(2)} \ldots \mathbf{y}_{p^{kn}-1}^{(2)} = \mathbf{y}_1^{(1)} \ldots \mathbf{y}_{p^{kn}-1}^{(1)} \tag{6.15}$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_{p^{kn}-1} \in (\mathbf{Z}_{p^k}^{n})^{p^{kn}-1}$.

Из 2-го уравнения системы (6.1) вытекает, что равенство (6.15) истинно тогда и только тогда, когда

$$\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)} \Leftrightarrow G \circ (\mathbf{q}_0^{(2)} \Theta \mathbf{q}_0^{(1)}) = \mathbf{0}$$

и

$$(\forall i = 2, \ldots, p^{k \cdot n} - 1)(\mathbf{y}_i^{(2)} = \mathbf{y}_i^{(1)}) \Leftrightarrow$$
$$\Leftrightarrow (\forall i = 2, \ldots, p^{k \cdot n} - 1)(G \circ (\mathbf{q}_{i-1}^{(2)} \Theta \mathbf{q}_{i-1}^{(1)}) = \mathbf{0})^{,}$$

т.е. когда истинны равенства (6.13) и (6.14).

Теорема доказана.

Теорема 6.4. Состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ являются эквивалентными состояниями тогда и только тогда, когда они являются близнецами.

Доказательство. 1. Пусть состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ являются близнецами. Тогда $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ – эквивалентные состояния автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$.

2. Пусть состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ являются эквивалентными состояниями автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$. Подставив $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ во 2-е уравнение системы (6.2), получим, что для всех $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$

$$\mathbf{y}_1^{(2)} = G \circ \mathbf{q}_1^{(2)}$$

и

$$\mathbf{y}_1^{(1)} = G \circ \mathbf{q}_1^{(1)}.$$

Так как $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ – эквивалентные состояния автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$, то

$$\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)}$$

для всех $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$.

Следовательно,

$$G \circ (\mathbf{q}_1^{(2)} \Theta \mathbf{q}_1^{(1)}) = \mathbf{0}.$$

А так как $G \in \mathsf{M}_n^{inv}$, то из последнего равенства получим

$$\mathbf{q}_1^{(2)} \Theta \mathbf{q}_1^{(1)} = \mathbf{0},$$

т.е.

$$\mathbf{q}_1^{(1)} = \mathbf{q}_1^{(2)},$$

откуда и вытекает, что состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ являются состояниями близнецами.

Теорема доказана.

Следствие 6.2. Для любого состояния $\mathbf{q}_0$ автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ класс всех состояний $\tilde{\mathbf{q}}$ автомата M_2 эквивалентных состоянию $\mathbf{q}_0$ совпадает с множеством всех решений нелинейного уравнения

$$A \circ (\tilde{\mathbf{q}} \circ \tilde{\mathbf{q}}^T \Theta \mathbf{q}_0 \circ \mathbf{q}_0^T) \circ \mathbf{b} \oplus C \circ (\tilde{\mathbf{q}} \Theta \mathbf{q}_0) = \mathbf{0}. \qquad (6.16)$$

Доказательство. Зафиксируем состояние $\mathbf{q}_0$ автомата $M \in \mathrm{A}_{n,2}^{inv}$.

Из теоремы 6.4 вытекает, что состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}$ автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ являются эквивалентными состояниями тогда и только тогда, когда они являются близнецами, т.е. совпадают их преемники по любому входному символу $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$.

Следовательно, подставив состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}$ в 1-е уравнение системы (6.2), получим, что для всех $\mathbf{x}_1 \in \mathbf{Z}_{p^k}^n$

$$A \circ \tilde{\mathbf{q}} \circ \tilde{\mathbf{q}}^T \circ \mathbf{b} \oplus C \circ \tilde{\mathbf{q}} \oplus \mathbf{d} \oplus E \circ \mathbf{x}_1 = A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_0 \oplus \mathbf{d} \oplus E \circ \mathbf{x}_1,$$

или

$$A \circ \tilde{\mathbf{q}} \circ \tilde{\mathbf{q}}^T \circ \mathbf{b} \oplus C \circ \tilde{\mathbf{q}} = A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_0.$$

Последнее уравнение эквивалентно уравнению (6.16).
Следствие доказано.

Исследуем теперь автомат $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$.

Теорема 6.5. Состояния $\mathbf{q}_0 = (q_0^{(1)}, \ldots, q_0^{(n)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \ldots, \tilde{q}_0^{(n)})^T$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ автомата $M_3 \in \mathrm{A}_{n,3}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} \tilde{q}_0^{(1)} \Theta q_0^{(1)} = 0 \\ \ldots\ldots\ldots\ldots\ldots \\ \tilde{q}_0^{(r)} \Theta q_0^{(r)} = 0 \end{cases} \tag{6.17}$$

и

$$\begin{cases} \tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \\ \ldots\ldots\ldots\ldots\ldots \quad (t = 1, \ldots, p^{kn} - 2) \\ \tilde{q}_t^{(r)} \Theta q_t^{(r)} = 0 \end{cases} \tag{6.18}$$

для всех входных слов

$$(x_1^{(1)}, \ldots, x_1^{(r)}, \underbrace{0, \ldots, 0}_{n-r \ раз})^T \ldots (x_{p^{kn}-1}^{(1)}, \ldots, x_{p^{kn}-1}^{(r)}, \underbrace{0, \ldots, 0}_{n-r \ раз})^T \in \mathbf{Z}_{p^k}^{n \cdot t}.$$

Доказательство. Число состояний автомата $M_3 \in \mathrm{A}_{n,3}$ равно p^{kn}.

Следовательно, состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ автомата $M_3 \in \mathrm{A}_{n,3}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\mathbf{y}_1 \ldots \mathbf{y}_{p^{kn}-1} = \tilde{\mathbf{y}}_1 \ldots \tilde{\mathbf{y}}_{p^{kn}-1} \tag{6.19}$$

для любого входного слова

$$(x_1^{(1)}, \ldots, x_1^{(r)}, \underbrace{0, \ldots, 0}_{n-r \ раз})^T \ldots (x_{p^{kn}-1}^{(1)}, \ldots, x_{p^{kn}-1}^{(r)}, \underbrace{0, \ldots, 0}_{n-r \ раз})^T \in \mathbf{Z}_{p^k}^{n \cdot t}.$$

Так как g_i $(i = 1, \ldots, r)$ – обратимые элементы кольца Z_{p^k}, то из последних r уравнений системы (6.7) вытекает, что равенство (6.19) истинно тогда и только тогда, когда

$$\tilde{\mathbf{y}}_1 = \mathbf{y}_1 \Leftrightarrow \begin{cases} g_1 \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) = 0 \\ \ldots\ldots\ldots\ldots\ldots \\ g_r \circ (\tilde{q}_0^{(r)} \Theta q_0^{(r)}) = 0 \end{cases} \Leftrightarrow \begin{cases} \tilde{q}_0^{(1)} \Theta q_0^{(1)} = 0 \\ \ldots\ldots\ldots\ldots\ldots \\ \tilde{q}_0^{(r)} \Theta q_0^{(r)} = 0 \end{cases}$$

и

$$(\forall i = 2,\ldots, p^{k\cdot n} - 1)(\tilde{\mathbf{y}}_i = \mathbf{y}_i) \Leftrightarrow$$

$$\Leftrightarrow (\forall i = 2,\ldots, p^{k\cdot n} - 1)\begin{cases} g_1 \circ (\tilde{q}_{i-1}^{(1)} \Theta q_{i-1}^{(1)}) = 0 \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ g_r \circ (\tilde{q}_{i-1}^{(r)} \Theta q_{i-1}^{(r)}) = 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow (\forall i = 2,\ldots, p^{k\cdot n} - 1)\begin{cases} \tilde{q}_{i-1}^{(1)} \Theta q_{i-1}^{(1)} = 0 \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{q}_{i-1}^{(r)} \Theta q_{i-1}^{(r)} = 0 \end{cases},$$

т.е. когда истинны равенства (6.17) и (6.18).

Теорема доказана.

Следствие 6.3. Если $r = n$, то автомат $M_3 \in \mathrm{A}_{n,3}$ является приведенным автоматом.

Доказательство. Предположим противное, т.е. что $r = n$, а автомат $M_3 \in \mathrm{A}_{n,3}$ не является приведенным автоматом.

Пусть состояния $\mathbf{q}_0 = (q_0^{(1)},\ldots, q_0^{(n)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)},\ldots, \tilde{q}_0^{(n)})^T$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ автомата $M_3 \in \mathrm{A}_{n,3}$ являются эквивалентными состояниями.

При $r = n$ и $t = 0$ из (6.17) вытекает, что $\mathbf{q}_0 = \tilde{\mathbf{q}}_0$.

Полученное противоречие показывает, что предположение – ложное, т.е. $M_3 \in \mathrm{A}_{n,3}$ – приведенный автомат.

Следствие доказано.

Теорема 6.6. Состояния $\mathbf{q}_0 = (q_0^{(1)},\ldots, q_0^{(n)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)},\ldots, \tilde{q}_0^{(n)})^T$ автомата $M_4 \in \mathrm{A}_{n,4}$ являются эквивалентными состояниями тогда и только тогда, когда истинны равенства

$$\begin{cases} \tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (t = 1,\ldots, p^{kn} - 1) \\ \tilde{q}_t^{(r)} \Theta q_t^{(r)} = 0 \end{cases} \tag{6.20}$$

для всех входных слов

$$(x_1^{(1)},\ldots, x_1^{(r)}, \underbrace{0,\ldots,0}_{n-r\ раз})^T \ldots (x_{p^{kn}-1}^{(1)},\ldots, x_{p^{kn}-1}^{(r)}, \underbrace{0,\ldots,0}_{n-r\ раз})^T \in \mathbf{Z}_{p^k}^{n\cdot t}.$$

Доказательство. Число состояний автомата $M_4 \in \mathrm{A}_{n,4}$ равно p^{kn}.

Следовательно, состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ автомата $M_4 \in \mathrm{A}_{n,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\mathbf{y}_1 \dots \mathbf{y}_{p^{kn}-1} = \tilde{\mathbf{y}}_1 \dots \tilde{\mathbf{y}}_{p^{kn}-1} \tag{6.21}$$

для любого входного слова

$$(x_1^{(1)},\dots,x_1^{(r)},\underbrace{0,\dots,0}_{n-r\ раз})^T \dots (x_{p^{kn}-1}^{(1)},\dots,x_{p^{kn}-1}^{(r)},\underbrace{0,\dots,0}_{n-r\ раз})^T \in \mathbf{Z}_{p^k}^{n\cdot t}.$$

Так как g_i $(i=1,\dots,r)$ – обратимые элементы кольца Z_{p^k}, то из последних r уравнений системы (6.8) вытекает, что равенство (6.21) истинно тогда и только тогда, когда

$$(\forall i=1,\dots,p^{k\cdot n}-1)\begin{cases} g_1 \circ (\tilde{q}_i^{(1)} \Theta q_i^{(1)}) = 0 \\ \quad \dots\dots\dots\dots\dots \\ g_r \circ (\tilde{q}_i^{(r)} \Theta q_i^{(r)}) = 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow (\forall i=1,\dots,p^{k\cdot n}-1)\begin{cases} \tilde{q}_i^{(1)} \Theta q_i^{(1)} = 0 \\ \quad \dots\dots\dots\dots\dots \\ \tilde{q}_i^{(r)} \Theta q_i^{(r)} = 0 \end{cases},$$

т.е. когда истинны равенства (6.20).

Теорема доказана.

Следствие 6.4. Если $r=n$, то состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ автомата $M_4 \in \mathrm{A}_{n,4}$ являются эквивалентными состояниями тогда и только тогда, когда они являются близнецами.

Доказательство. 1. Пусть состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_4 \in \mathrm{A}_{n,4}$ являются близнецами. Тогда $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ – эквивалентные состояния автомата $M_4 \in \mathrm{A}_{n,4}$.

2. Пусть состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ $(\mathbf{q}_0 \neq \tilde{\mathbf{q}}_0)$ являются эквивалентными состояниями автомата $M_4 \in \mathrm{A}_{n,4}$. При $r=n$ и $t=0$ из системы (6.20) вытекает, что $\mathbf{q}_1 = \tilde{\mathbf{q}}_1$ для любого входного символа $\mathbf{x} \in \mathbf{Z}_{p^k}^n$. Следовательно, состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ автомата $M_4 \in \mathrm{A}_{n,4}$ являются близнецами.

Следствие доказано.

Из теорем 6.5 и 6.6 вытекает

Утверждение 6.7. Если $r<n$, то при логарифмическом весе временная сложность проверки для автомата $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ свойства «быть приведенным автоматом», а также временная сложность построения множеств эквивалентных состояний автомата $M \in \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ в явном виде равна

$$T = O(\eta \cdot \log \eta) \quad (p \to \infty, \text{ или } k \to \infty, \text{ или } n \to \infty),$$

где

$$\eta = p^{k\cdot(2\cdot n+r)} \cdot k \cdot (n+r) \cdot \log p.$$

Пример 6.2. Охарактеризуем классы состояний, эквивалентных состоянию $\mathbf{q}_0$ для автоматов, рассмотренных в примере 6.1.

1. Рассмотрим автомат $M_R \in \mathrm{A}_{3,4}$.

Теорема 6.7. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_R \in \mathrm{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} \tilde{q}_0^{(1)} = q_0^{(1)} \Theta (a \oplus h^{-1}) \circ \Delta \\ \tilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta \\ \tilde{q}_0^{(3)} = q_0^{(3)} \Theta (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta \end{cases}, \tag{6.22}$$

где Δ – решение уравнения

$$(a \circ h \oplus 1) \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta^2 \Theta$$
$$\Theta (q_0^{(3)} \circ (a \circ h \oplus 1) \oplus q_0^{(1)} \circ (a \oplus h^{-1} \oplus h) \oplus$$
$$\oplus (1 \Theta h \circ r) \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1)) \circ \Delta = 0. \tag{6.23}$$

Доказательство. Пусть состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ являются эквивалентными состояниями автомата $M_R \in \mathrm{A}_{3,4}$.

Условие (6.20) имеет вид

$$\tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 1) \tag{6.24}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.24) вытекает, что

$$\tilde{q}_1^{(1)} \Theta q_1^{(1)} = 0 \tag{6.25}$$

и

$$\tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \quad (t = 2, \ldots, p^{3 \cdot k} - 1) \tag{6.26}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$. Воспользовавшись 1-м уравнением системы (6.9), получим, что (6.25) и (6.26) принимают, соответственно, вид

$$(\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \Theta h \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta h \circ (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) = 0 \tag{6.27}$$

и

$$(\tilde{q}_t^{(1)} \Theta q_t^{(1)}) \Theta h \circ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) \Theta h \circ (\tilde{q}_t^{(3)} \Theta q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 2) \tag{6.28}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.24) вытекает, что (6.28) принимает вид

$$(\tilde{q}_t^{(2)} \Theta q_t^{(2)}) \oplus (\tilde{q}_t^{(3)} \Theta q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 2). \tag{6.29}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из 2-го и 3-го уравнения системы (6.9) находим, что

$$\tilde{q}_t^{(2)} \Theta q_t^{(2)} = h \circ (\tilde{q}_{t-1}^{(1)} \Theta q_{t-1}^{(1)}) \oplus$$
$$\oplus (a \circ h \oplus 1) \circ (\tilde{q}_{t-1}^{(2)} \Theta q_{t-1}^{(2)}) \quad (t = 1, \ldots, p^{3 \cdot k} - 2) \tag{6.30}$$

и

$$\tilde{q}_t^{(3)} \Theta q_t^{(3)} = (1 \Theta h \circ r) \circ (\tilde{q}_{t-1}^{(3)} \Theta q_{t-1}^{(3)}) \oplus$$
$$\oplus\, h \circ (\tilde{q}_{t-1}^{(1)} \circ \tilde{q}_{t-1}^{(3)} \Theta q_{t-1}^{(1)} \circ q_{t-1}^{(3)}) \quad (t = 1, \ldots, p^{3 \cdot k} - 2). \qquad (6.31)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$

Подставив (6.30) и (6.31) в (6.29), и учитывая равенства (6.24), получим

$$h \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus (a \circ h \oplus 1) \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \oplus$$
$$\oplus\, (1 \Theta h \circ r) \circ (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) \oplus h \circ (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)}) = 0 \qquad (6.32)$$

и

$$(a \circ h \oplus 1) \circ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) \oplus$$
$$\oplus\, (1 \Theta h \circ r \oplus h \circ q_t^{(1)}) \circ (\tilde{q}_t^{(3)} \Theta q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 3) \qquad (6.33)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Так как h – обратимый элемент кольца Z_{p^k}, то из утверждения 6.6. вытекает, что если x_t пробегает множество $\mathbf{Z}_{p^k}$, то $1 \Theta h \circ r \oplus h \circ q_t^{(1)}$ $(t = 1, \ldots, p^{3 \cdot k} - 3)$ также пробегает множество $\mathbf{Z}_{p^k}$. При этом $\tilde{q}_t^{(2)}$ и $q_t^{(2)}$ не зависят от значения x_t.

Следовательно, равенства (6.33) истинны тогда и только тогда, когда

$$\tilde{q}_t^{(3)} \Theta q_t^{(3)} = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 3). \qquad (6.34)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.31) вытекает, что при выполнении условий (6.24) система равенств (6.34) эквивалентна равенству

$$\tilde{q}_1^{(3)} \Theta q_1^{(3)} = 0.$$

Воспользовавшись равенством (6.31) при $t = 1$, получим

$$(1 \Theta h \circ r) \circ (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) \oplus h \circ (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)}) = 0 \qquad (6.35)$$

При выполнении равенств (6.34) равенства (6.33) принимают вид

$$(a \circ h \oplus 1) \circ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 3). \qquad (6.36)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.30), учитывая равенства (6.24), получим, что

$$\begin{cases} (\tilde{q}_1^{(2)} \Theta q_1^{(2)}) = h \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus (a \circ h \oplus 1) \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \\ (\tilde{q}_2^{(2)} \Theta q_2^{(2)}) = (a \circ h \oplus 1) \circ (\tilde{q}_1^{(2)} \Theta q_1^{(2)}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\tilde{q}_{t-1}^{(2)} \Theta q_{t-1}^{(2)}) = (a \circ h \oplus 1) \circ (\tilde{q}_{t-2}^{(2)} \Theta q_{t-2}^{(2)}) \\ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) = (a \circ h \oplus 1) \circ (\tilde{q}_{t-1}^{(2)} \Theta q_{t-1}^{(2)}) \end{cases} \qquad (6.37)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$ $(t = 2, \ldots, p^{3 \cdot k} - 3)$.

Умножая i-е уравнение $(i=1,\ldots,t-1)$ системы (6.37) на $(a\circ h\oplus 1)^{t-i}$ и складывая после этого все уравнения системы (6.37), получим, что

$$(\tilde{q}_t^{(2)}\Theta q_t^{(2)})=(a\circ h\oplus 1)^{t-1}\circ(h\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\oplus$$

$$\oplus(a\circ h\oplus 1)\circ(\tilde{q}_0^{(2)}\Theta q_0^{(2)}))\quad (t=2,\ldots,p^{3\cdot k}-3).$$

Следовательно, (6.36) принимает вид

$$(a\circ h\oplus 1)^{t}\circ(h\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\oplus$$

$$\oplus(a\circ h\oplus 1)\circ(\tilde{q}_0^{(2)}\Theta q_0^{(2)}))=0\quad (t=1,\ldots,p^{3\cdot k}-3). \tag{6.38}$$

Подставив (6.35) в (6.32), получим

$$h\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\oplus(a\circ h\oplus 1)\circ(\tilde{q}_0^{(2)}\Theta q_0^{(2)})=0 \tag{6.39}$$

Отсюда вытекает, что равенства (6.38) истинны.

Таким образом, состояния $\mathbf{q}_0=(q_0^{(1)},q_0^{(2)},q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0=(\tilde{q}_0^{(1)},\tilde{q}_0^{(2)},\tilde{q}_0^{(3)})^T$ являются эквивалентными состояниями автомата $M_R\in \mathrm{A}_{3,4}$ тогда и только тогда, когда истинны равенства (6.27), (6.35) и (6.38), т.е. когда

$$\begin{cases}(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\Theta h\circ(\tilde{q}_0^{(2)}\Theta q_0^{(2)})\Theta h\circ(\tilde{q}_0^{(3)}\Theta q_0^{(3)})=0\\ h\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\oplus(a\circ h\oplus 1)\circ(\tilde{q}_0^{(2)}\Theta q_0^{(2)})=0\\ (1\Theta h\circ r)\circ(\tilde{q}_0^{(3)}\Theta q_0^{(3)})\oplus h\circ(\tilde{q}_0^{(1)}\circ\tilde{q}_0^{(3)}\Theta q_0^{(1)}\circ q_0^{(3)})=0.\end{cases} \tag{6.40}$$

Положим

$$\tilde{q}_0^{(2)}=q_0^{(2)}\oplus\Delta, \tag{6.41}$$

т.е.

$$\tilde{q}_0^{(2)}\Theta q_0^{(2)}=\Delta. \tag{6.42}$$

Подставив (6.42) в 1-е и 2-е уравнения системы (6.40), получим

$$(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\Theta h\circ\Delta\Theta h\circ(\tilde{q}_0^{(3)}\Theta q_0^{(3)})=0 \tag{6.43}$$

и

$$h\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\oplus(a\circ h\oplus 1)\circ\Delta=0. \tag{6.44}$$

Учитывая, что h – обратимый элемент кольца Z_{p^k}, из (6.44) и (6.43) получим

$$\tilde{q}_0^{(1)}\Theta q_0^{(1)}=\Theta(a\oplus h^{-1})\circ\Delta \tag{6.45}$$

и

$$\tilde{q}_0^{(3)}\Theta q_0^{(3)}=h^{-1}\circ(\tilde{q}_0^{(1)}\Theta q_0^{(1)})\Theta\Delta. \tag{6.46}$$

Подставив (6.45) в (6.46), получим

$$\tilde{q}_0^{(3)}\Theta q_0^{(3)}=\Theta(a\circ h^{-1}\oplus h^{-2}\oplus 1)\circ\Delta. \tag{6.47}$$

Из (6.45) и (6.47) получим, что

$$\tilde{q}_0^{(1)} = q_0^{(1)} \Theta (a \oplus h^{-1}) \circ \Delta \tag{6.48}$$

и

$$\tilde{q}_0^{(3)} = q_0^{(3)} \Theta (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta . \tag{6.49}$$

Применяя равенства (6.48) и (6.49) получим

$$\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)} = (a \oplus h^{-1}) \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta^2 \Theta$$

$$\Theta (q_0^{(3)} \circ (a \oplus h^{-1}) \oplus q_0^{(1)} \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1)) \circ \Delta . \tag{6.50}$$

Подставив (6.46) и (6.50) в 3-е уравнение системы (6.40), получим, что Δ является решением уравнения (6.23).

Теорема доказана.

Следствие 6.5. Если у двух различных состояний $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_R \in \mathrm{A}_{3,4}$ совпадают вторые компоненты, то состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ являются неэквивалентными состояниями автомата $M_R \in \mathrm{A}_{3,4}$.

Доказательство. Пусть у двух различных состояний $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_R \in \mathrm{A}_{3,4}$ совпадают вторые компоненты.

Предположим противное, т.е. что состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ являются эквивалентными состояниями автомата $M_R \in \mathrm{A}_{3,4}$.

Из равенства

$$\tilde{q}_0^{(2)} = q_0^{(2)}$$

вытекает, что $\Delta = 0$.

Так как $\Delta = 0$ является решением уравнения (6.23), то из (6.22) вытекает, что

$$\tilde{q}_0^{(i)} = q_0^{(i)} \quad (i = 1,2,3),$$

т.е. что

$$\tilde{\mathbf{q}}_0 = \mathbf{q}_0 .$$

Получено противоречие.

Следовательно, предположение – ложное, т.е. состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ являются неэквивалентными состояниями автомата $M_R \in \mathrm{A}_{3,4}$.

Следствие доказано.

Следствие 6.6. Любые эквивалентные состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_R \in \mathrm{A}_{3,4}$ являются близнецами.

Доказательство. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_R \in \mathrm{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\tilde{q}_1^{(i)} \Theta q_1^{(i)} = 0 \quad (i = 1,2,3) \tag{6.52}$$

для всех $x_1 \in \mathbf{Z}_{p^k}$.

Воспользовавшись первыми тремя уравнениями системы (6.9), получим что равенства (6.52) эквивалентны системе (6.40).

Следствие доказано.

2. Рассмотрим автомат $M_{S_1} \in \mathrm{A}_{3,4}$.

Теорема 6.8. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_{S_1} \in \mathrm{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) = 0 \\ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta h \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(2)} \circ q_0^{(3)}) = 0 \\ \tilde{q}_t^{(2)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(2)} \circ q_t^{(3)} = 0 \ \ (t = 1, \ldots, p^{3k} - 3) \end{cases} \qquad (6.53)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Доказательство. Пусть состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ являются эквивалентными состояниями автомата $M_{S_1} \in \mathrm{A}_{3,4}$.

Условие (6.20) имеет вид

$$\tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \quad (t = 1, \ldots, p^{3k} - 1) \qquad (6.54)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.54) вытекает, что

$$\tilde{q}_1^{(1)} \Theta q_1^{(1)} = 0 \qquad (6.55)$$

и

$$\tilde{q}_t^{(1)} \Theta q_t^{(1)} = 0 \quad (t = 2, \ldots, p^{3k} - 1) \qquad (6.56)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Воспользовавшись 1-м уравнением системы (6.10), получим, что (6.55) и (6.56) принимают, соответственно, вид

$$(\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) = 0 \qquad (6.57)$$

и

$$(\tilde{q}_t^{(1)} \Theta q_t^{(1)}) \oplus h \circ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) = 0 \quad (t = 1, \ldots, p^{3k} - 2) \qquad (6.58)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.54), с учетом того, что $h \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, вытекает, что (6.58) принимает вид

$$\tilde{q}_t^{(2)} \Theta q_t^{(2)} = 0 \quad (t = 1, \ldots, p^{3k} - 2). \qquad (6.59)$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из 2-го уравнения системы (6.10) находим, что

$$\tilde{q}_t^{(2)} \Theta q_t^{(2)} = (\tilde{q}_{t-1}^{(2)} \Theta q_{t-1}^{(2)}) \Theta h \circ (\tilde{q}_{t-1}^{(1)} \Theta q_{t-1}^{(1)}) \oplus$$

$$\oplus h \circ (\tilde{q}_{t-1}^{(2)} \circ \tilde{q}_{t-1}^{(3)} \Theta q_{t-1}^{(2)} \circ q_{t-1}^{(3)}) \quad (t = 1, \ldots, p^{3 \cdot k} - 2) \tag{6.60}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Подставив (6.59) в (6.60), и учитывая равенства (6.54), получим

$$(\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta h \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(2)} \circ q_0^{(3)}) = 0. \tag{6.61}$$

и

$$(\tilde{q}_t^{(2)} \Theta q_t^{(2)}) \oplus h \circ (\tilde{q}_t^{(2)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(2)} \circ q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 3). \tag{6.62}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

С учетом равенств (6.59) и того, что $h \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, получим, что (6.62) принимает вид

$$\tilde{q}_t^{(2)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(2)} \circ q_t^{(3)} = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 3). \tag{6.63}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Равенства (6.57), (6.61) и (6.63) и составляют систему равенств (6.53).

Теорема доказана.

Следствие 6.7. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_{S_1} \in \mathrm{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\begin{cases} \tilde{q}_0^{(1)} = q_0^{(1)} \Theta h \circ \Delta \\ \tilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta \\ \tilde{q}_0^{(3)} = q_0^{(3)} \oplus 2 \circ h \circ q_0^{(2)} \circ \Delta \oplus h \circ \Delta^2 \end{cases}, \tag{6.64}$$

где Δ – решение уравнения

$$\Delta^3 \oplus 3 \circ q_0^{(2)} \circ \Delta^2 \oplus$$

$$\oplus (2 \circ (q_0^{(2)})^2 \oplus h^{-1} \circ q_0^{(3)} \oplus 1 \oplus h^{-2}) \circ \Delta = 0. \tag{6.65}$$

Доказательство. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_{S_1} \in \mathrm{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\tilde{q}_1^{(i)} \Theta q_1^{(i)} = 0 \quad (i = 1,2,3). \tag{6.66}$$

Первые два равенства системы (6.66) имеют, соответственно, вид (6.57) и (6.61). Кроме того, из 3-го уравнения системы (6.10) вытекает, что

$$\tilde{q}_1^{(3)} \Theta q_1^{(3)} = 0 \Leftrightarrow (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) \Theta h \circ ((\tilde{q}_0^{(2)})^2 \Theta (q_0^{(2)})^2) = 0.$$

Следовательно, равенства (6.66) имеют вид

$$\begin{cases} (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) = 0 \\ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta h \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ (\tilde{q}_0^{(2)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(2)} \circ q_0^{(3)}) = 0. \\ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \Theta h \circ ((\tilde{q}_0^{(2)})^2 \Theta (\tilde{q}_0^{(2)})^2) = 0 \end{cases} \tag{6.67}$$

Пусть

$$\begin{cases} \tilde{q}_0^{(1)} = q_0^{(1)} \oplus \Delta_1 \\ \tilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta \\ \tilde{q}_0^{(3)} = q_0^{(3)} \oplus \Delta_3 \end{cases}. \tag{6.68}$$

Подставив (6.68) в (6.67), получим

$$\begin{cases} \Delta_1 \oplus h \circ \Delta = 0 \\ \Delta \Theta h \circ \Delta_1 \oplus h \circ (q_0^{(3)} \circ \Delta \oplus q_0^{(2)} \circ \Delta_3 \oplus \Delta \circ \Delta_3) = 0 \\ \Delta_3 \Theta h \circ \Delta \circ (2 \circ q_0^{(2)} \oplus \Delta) = 0 \end{cases}. \tag{6.69}$$

Из 1-го и 3-го равенств системы (6.69) находим, что

$$\Delta_1 = \Theta h \circ \Delta \tag{6.70}$$

и

$$\Delta_3 = 2 \circ h \circ q_0^{(2)} \circ \Delta \oplus h \circ \Delta^2. \tag{6.71}$$

Подставив (6.70) и (6.71) во 2-е равенство системы (6.69), получим, что Δ – решение уравнения

$$h^2 \circ \Delta^3 \oplus 3 \circ h^2 \circ q_0^{(2)} \circ \Delta^2 \oplus$$

$$\oplus (2 \circ h^2 \circ (q_0^{(2)})^2 \oplus h \circ q_0^{(3)} \oplus h^2 \oplus 1) \circ \Delta = 0 \tag{6.72}$$

Так как $h \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, то уравнение (6.72) эквивалентно уравнению (6.65).

Следствие доказано.

3. Рассмотрим автомат $M_L \in \mathrm{A}_{3,4}$.

Теорема 6.9. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_L \in \mathrm{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} a_2 \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus (h^{-1} \Theta 1) \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)}) = 0 \\ a_2 \circ (\tilde{q}_t^{(1)} \Theta q_t^{(1)}) \Theta (\tilde{q}_t^{(1)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(1)} \circ q_t^{(3)}) = 0 \ \ (t = 1, \ldots, p^{3 \cdot k} - 2) \end{cases} \tag{6.73}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Доказательство. Пусть состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ являются эквивалентными состояниями автомата $M_L \in \mathrm{A}_{3,4}$.

Условие (6.20) имеет вид

$$\tilde{q}_t^{(2)} \Theta q_t^{(2)} = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 1). \tag{6.74}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.74) вытекает, что

$$\tilde{q}_1^{(2)} \Theta q_1^{(2)} = 0 \tag{6.75}$$

и

$$\tilde{q}_t^{(2)} \Theta q_t^{(2)} = 0 \quad (t = 2, \ldots, p^{3 \cdot k} - 1) \tag{6.76}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Воспользовавшись 2-м уравнением системы (6.11), получим, что (6.75) и (6.76) принимают, соответственно, вид

$$h \circ a_2 \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus (1 \Theta h) \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta$$

$$\Theta h \circ (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)}) = 0 \tag{6.77}$$

и

$$h \circ a_2 \circ (\tilde{q}_t^{(1)} \Theta q_t^{(1)}) \oplus (1 \Theta h) \circ (\tilde{q}_t^{(2)} \Theta q_t^{(2)}) \Theta$$

$$\Theta h \circ (\tilde{q}_t^{(1)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(1)} \circ q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 2) \tag{6.78}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Из (6.73), с учетом того, что $h \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, вытекает что (6.77) и (6.78) принимают, соответственно, вид

$$a_2 \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus (h^{-1} \Theta 1) \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)}) \Theta (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(3)} \Theta q_0^{(1)} \circ q_0^{(3)}) = 0 \tag{6.79}$$

и

$$a_2 \circ (\tilde{q}_t^{(1)} \Theta q_t^{(1)}) \Theta (\tilde{q}_t^{(1)} \circ \tilde{q}_t^{(3)} \Theta q_t^{(1)} \circ q_t^{(3)}) = 0 \quad (t = 1, \ldots, p^{3 \cdot k} - 2) \tag{6.80}$$

для всех $x_1 \ldots x_t \in \mathbf{Z}_{p^k}^t$.

Равенства (6.79) и (6.80) составляют систему равенств (6.73).

Теорема доказана.

Следствие 6.8. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_L \in \mathrm{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\begin{cases} \tilde{q}_0^{(1)} = q_0^{(1)} \oplus \Delta_1 \\ \tilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta_2 \\ \tilde{q}_0^{(3)} = q_0^{(3)} \oplus \Delta_3 \end{cases}, \tag{6.81}$$

где $(\Delta_1, \Delta_2, \Delta_3)$ – решение нелинейной системы уравнений

$$\begin{cases} (h^{-1} \Theta a_1) \circ \Delta_1 \oplus a_1 \circ \Delta_2 = 0 \\ (a_2 \Theta q_0^{(3)}) \circ \Delta_1 \oplus (h^{-1} \Theta 1) \circ \Delta_2 \Theta q_0^{(1)} \circ \Delta_3 \Theta \Delta_1 \circ \Delta_3 = 0 \\ q_0^{(2)} \circ \Delta_1 \oplus q_0^{(1)} \circ \Delta_2 \oplus (h^{-1} \Theta a_3) \circ \Delta_3 \oplus \Delta_1 \circ \Delta_2 = 0 \end{cases}. \tag{6.82}$$

Доказательство. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$ автомата $M_L \in \mathrm{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\tilde{q}_1^{(i)} \Theta q_1^{(i)} = 0 \quad (i = 1,2,3). \tag{6.83}$$

Второе равенство системы (6.83) – это равенство (6.79).

Кроме того, из 1-го и 3-го уравнений системы (6.11), с учетом того, что $h \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, получим

$$\tilde{q}_1^{(1)} \Theta q_1^{(1)} = 0 \Leftrightarrow (1 \Theta h \circ a_1) \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus h \circ a_1 \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)^2}) = 0 \Leftrightarrow .$$

$$\Leftrightarrow (h^{-1} \Theta a_1) \circ (\tilde{q}_0^{(1)} \Theta q_0^{(1)}) \oplus a_1 \circ (\tilde{q}_0^{(2)} \Theta q_0^{(2)^2}) = 0 \qquad (6.84)$$

и

$$\tilde{q}_1^{(3)} \Theta q_1^{(3)} = 0 \Leftrightarrow (1 \Theta h \circ a_3) \circ (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) \oplus h \circ (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(2)} \Theta q_0^{(1)} \circ q_0^{(2)}) = 0 \Leftrightarrow .$$

$$\Leftrightarrow (h^{-1} \Theta a_3) \circ (\tilde{q}_0^{(3)} \Theta q_0^{(3)}) \oplus (\tilde{q}_0^{(1)} \circ \tilde{q}_0^{(2)} \Theta q_0^{(1)} \circ q_0^{(2)}) = 0 . \qquad (6.85)$$

Подставив (6.81) в (6.79), (6.84) и (6.85), получим систему (6.82).

Следствие доказано.

4. Рассмотрим автомат $M_H \in \mathrm{A}_{2,4}$.

Из (6.12) вытекает, что:

1) если $a = b = 0$, то автомат $M_H \in \mathrm{A}_{2,4}$ представляет собой комбинационную схему, реализующую перестановку $f : \mathbf{Z}_{p^k} \to \mathbf{Z}_{p^k}$.

2) если $a = 0$ и $b \neq 0$, то автомат $M_H \in \mathrm{A}_{2,4}$ – это линейный одномерный автомат с лагом 2 (такие автоматы были рассмотрены в п.5.9).

Поэтому будем считать, что $a \neq 0$ и $b \neq 0$, либо $a \neq 0$ и $b = 0$.

Отметим, что из (6.12) вытекает

Утверждение 6.8. Выходной последовательностью, генерируемой автоматом $M_H \in \mathrm{A}_{2,4}$ на любую входную последовательность $x_1 \dots x_t \in \mathbf{Z}_{p^k}^t$ $(t \in \mathbf{N})$ является последовательность $q_2 \dots q_{t+1} \in \mathbf{Z}_{p^k}^t$.

Теорема 6.10. Состояния $\mathbf{q}_0 = (q_1, q_0)$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_1, \tilde{q}_0)$ автомата $M_H \in \mathrm{A}_{2,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} a \circ (\tilde{q}_1^2 \Theta q_1^2) \Theta b \circ (\tilde{q}_0 \Theta q_0) = 0 \\ b \circ (\tilde{q}_1 \Theta q_1) = 0 \end{cases} . \qquad (6.86)$$

Доказательство. Из утверждения 6.8 и 1-го уравнения системы (6.12) вытекает, что состояния $\mathbf{q}_0 = (q_1, q_0)$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_1, \tilde{q}_0)$ автомата $M_H \in \mathrm{A}_{2,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\tilde{q}_2 \Theta q_2 = 0 \qquad (6.87)$$

и

$$\tilde{q}_3 \Theta q_3 = 0 . \qquad (6.88)$$

Воспользовавшись в (6.87) и (6.88) 1-м уравнением системы (6.12), получим (6.86).

Теорема доказана.

Следствие 6.9. Если $b \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}, то $M_H \in \mathrm{A}_{2,4}$ – приведенный автомат.

Доказательство. Пусть $b \in \mathbf{Z}_{p^k}$ – обратимый элемент кольца Z_{p^k}.

Предположим, что состояния $\mathbf{q}_0 = (q_1, q_0)$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_1, \tilde{q}_0)$ автомата $M_H \in \mathrm{A}_{2,4}$ являются эквивалентными состояниями.

Из 2-го уравнения системы (6.86) получим, что

$$b \circ (\tilde{q}_1 \Theta q_1) = 0 \Leftrightarrow \tilde{q}_1 \Theta q_1 = 0 \Leftrightarrow \tilde{q}_1 = q_1 . \qquad (6.89)$$

Подставив (6.89) в 1-е уравнение системы (6.86), получим

$$b \circ (\tilde{q}_0 \Theta q_0) = 0 \Leftrightarrow \tilde{q}_0 \Theta q_0 = 0 \Leftrightarrow \tilde{q}_0 = q_0 . \qquad (6.90)$$

Из (6.89) и (6.90) вытекает, что

$$\tilde{\mathbf{q}}_0 = \mathbf{q}_0 .$$

Следствие доказано.

Следствие 6.10. Состояния $\mathbf{q}_0 = (q_1, q_0)$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_1, \tilde{q}_0)$ автомата $M_H \in \mathrm{A}_{2,4}$ являются близнецами тогда и только тогда, когда $\tilde{q}_1 = q_1$ для всех $x_1 \in \mathbf{Z}_{p^k}$ и

$$b \circ (\tilde{q}_0 \Theta q_0) = 0 . \qquad (6.91)$$

Доказательство. Пусть $\mathbf{q}_0 = (q_1, q_0)$ и $\tilde{\mathbf{q}}_0 = (\tilde{q}_1, \tilde{q}_0)$ – состояния автомата $M_H \in \mathrm{A}_{2,4}$. Тогда $\mathbf{q}_1 = (q_2, q_1)$ и $\tilde{\mathbf{q}}_1 = (\tilde{q}_2, \tilde{q}_1)$ для любого $x_1 \in \mathbf{Z}_{p^k}$, где q_2 и $\tilde{q}_2$ вычисляются в соответствии с 1-м уравнением системы (6.12).

Следовательно, состояния $\mathbf{q}_0$ и $\tilde{\mathbf{q}}_0$ автомата $M_H \in \mathrm{A}_{2,4}$ являются близнецами тогда и только тогда, когда

$$\tilde{q}_1 = q_1$$

и

$$\tilde{q}_2 = q_2 .$$

Положив $\tilde{q}_1 = q_1$ в 1-м равенстве системы (6.86) получим, что равенство (6.91) истинно.

Следствие доказано.

6.3. Задачи идентификации исследуемых автоматов.

Рассмотрим вначале задачу идентификации начального состояния автомата $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ посредством простого диагностического эксперимента с автоматом M.

В этом случае задача состоит в построении такого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_l \in \mathbf{Z}_{p^k}^{l \cdot n}$ заранее неизвестной длины, что:

1) входной символ $\mathbf{x}_1$ определяет множество допустимых начальных состояний $Q_{\mathbf{q}_0}$, т.е. осуществляет слабую инициализацию автомата M;

2) входное слово $\mathbf{x}_2 \ldots \mathbf{x}_l$ осуществляет идентификацию элемента, принадлежащего множеству $Q_{\mathbf{q}_0}$, с точностью до множества эквивалентных друг другу состояний автомата M.

Из (6.1), (6.2), (6.7) и (6.8) вытекает, что решение задачи слабой инициализации для автомата M сводится:

1) к решению системы линейных уравнений

$$G \circ \mathbf{q}_0 = \mathbf{y}_1 \Theta F \circ \mathbf{x}_1,$$

если $M = M_1$;

2) к решению системы нелинейных уравнений

$$A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_0 = G^{-1} \circ \mathbf{y}_1 \Theta \mathbf{d} \Theta E \circ \mathbf{x}_1,$$

если $M = M_2$;

3) к решению системы линейных уравнений

$$g_i \circ q_0^{(i)} = y_1^{(i)} \Theta f_i \circ x_1^{(i)} \quad (i = 1, \ldots, r),$$

если $M = M_3$;

4) к решению системы нелинейных уравнений

$$\mathbf{q}_0^T \circ A_i \circ \mathbf{q_0} \oplus \mathbf{q_0} = g_i^{-1} \circ y_1^{(i)} \Theta d_i \Theta e_i \circ x_1^{(i)} \quad (i = 1, \ldots, r),$$

если $M = M_4$.

Отсюда вытекает, что решение задачи слабой инициализации для автомата $M \in \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,4}$ заведомо сложнее, чем решение задачи слабой инициализации для автомата $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,3}$.

Из (6.1), (6.2), (6.7) и (6.8) вытекает, что решение задачи идентификации элемента, принадлежащего множеству $Q_{\mathbf{q}_0}$, с точностью до множества эквивалентных другу состояний автомата M, сводится:

1) к решению систем нелинейных уравнений

$$G \circ (A \circ \mathbf{q}_{t-1} \circ \mathbf{q}_{t-1}^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_{t-1}) =$$

$$= \mathbf{y}_{t+1} \Theta F \circ \mathbf{x}_{t+1} \Theta G \circ (\mathbf{d} \Theta E \circ \mathbf{x}_t) \quad (t = 1, \ldots, l-1),$$

если $M = M_1$ (в этих системах уравнений необходимо представить каждый вектор $\mathbf{q}_{t-1}$ $(t = 2, \ldots, l-1)$ через значения $A, \mathbf{b}, C, \mathbf{d}, E, \mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$);

2) к решению систем нелинейных уравнений

$$A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t =$$

$$= G^{-1} \circ \mathbf{y}_{t+1} \Theta \mathbf{d} \Theta E \circ \mathbf{x}_t \quad (t = 1, \ldots, l-1).$$

если $M = M_2$ (в этой системе уравнений необходимо представить каждый вектор $\mathbf{q}_t$ $(t = 1, \ldots, l-1)$ через значения $A, \mathbf{b}, C, \mathbf{d}, E, \mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$);

3) к решению систем нелинейных уравнений

$$g_i \circ (\mathbf{q}_{t-1}^T \circ A_i \circ \mathbf{q}_{t-1} \oplus \mathbf{c}_i \circ \mathbf{q}_{t-1}) =$$

$$= y_{t+1}^{(i)} \Theta f_i \circ x_{t+1}^{(i)} \Theta g_i \circ (d_i \oplus e_i \circ x_t^{(i)}) \quad (i = 1, \ldots, r;\ t = 1, \ldots l-1),$$

если $M = M_3$ (в этой системе уравнений необходимо представить каждый вектор $\mathbf{q}_{t-1}$ $(t = 2, \ldots, l-1)$ через значения $\mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$ и параметры системы);

4) к решению систем нелинейных уравнений

$$\mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t =$$

$$= g_i^{-1} \circ y_{t+1}^{(i)} \Theta d_i \Theta e_i \circ x_{t+1}^{(i)} \quad (i = 1, \ldots, r;\ t = 1, \ldots l-1),$$

если $M = M_4$ (в этой системе уравнений каждый необходимо представить вектор $\mathbf{q}_t$ $(t = 1, \ldots, l-1)$ через значения $\mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$ и параметры системы).

Таким образом, показано, что задача идентификация начального состояния автомата $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$ представляет собой трудную задачу, состоящую в поиске и решении систем нелинейных уравнений над кольцом Z_{p^k}.

Рассмотрим теперь задачу параметрической идентификации автомата $M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4}$.

Предположим, что экспериментатор может управлять входом, а также осуществлять инициализацию автомата M требуемое число раз, т.е. проводить кратный эксперимент любой кратности.

Такие предположения соответствуют наиболее сильной атаке на шифр $((M, \mathbf{q_0}), (M, \mathbf{q_0}))$. Ясно, что при ослаблении этих предположений сложность атаки на шифр $((M, \mathbf{q_0}), (M, \mathbf{q_0}))$ существенно возрастает.

Отметим, что этот рост сложности атаки заведомо не меньше, чем рост сложности решения задач теории экспериментов с автоматами при ограничении на кратность эксперимента или при переходе к простому эксперименту.

Рассмотрим автомат $M_1 \in \mathrm{A}_{n,1}^{inv}$.

Подача на автомат $(M_1, \mathbf{q_0})$, где

$$\mathbf{q}_0 = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, 1, \underbrace{0, \ldots, 0}_{n-i \text{ раз}})^T \quad (i = 1, \ldots, n),$$

входного символа

$$\mathbf{x}_1 = \mathbf{0}$$

идентифицирует i-й столбец матрицы G.

Следовательно, n-кратный эксперимент высоты 1 идентифицирует матрицу G.

Подача на автомат $(M_1,\mathbf{0})$ входного символа

$$\mathbf{x}_1 = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{n-i\ раз})^T \quad (i=1,\ldots,n)$$

идентифицирует i-й столбец матрицы F.

Следовательно, n-кратный эксперимент высоты 1 идентифицирует матрицу F.

Подав на автомат $(M_1,\mathbf{0})$ входной символ

$$\mathbf{x}_1 = \mathbf{0},$$

получим

$$\mathbf{q}_1 = \mathbf{d}.$$

Подав теперь на автомат M_1 любой входной символ $\mathbf{x}_2$, получим систему уравнений

$$G \circ \mathbf{d} = \mathbf{y}_2 \Theta F \circ \mathbf{x}_2. \qquad (6.92)$$

Если $G \in \mathsf{M}_n^{inv}$, то вектор $\mathbf{d}$ идентифицируется единственным образом.

Если же $G \in \mathsf{M}_n^{non\_inv}$, то система уравнений (6.92) определяет множество допустимых значений вектора $\mathbf{d}$.

Все дальнейшие действия необходимо производить по отдельности с каждым решением $\mathbf{d}$ системы уравнений (6.92).

Итак, идентификация вектора $\mathbf{d}$ с точностью, определяемой матрицей G, осуществляется простым экспериментом длины 2.

Подав на автомат $(M_1,\mathbf{0})$ входной символ

$$\mathbf{x}_1 = (\underbrace{0,\ldots,0}_{i-1\ раз},1,\underbrace{0,\ldots,0}_{n-i\ раз})^T \quad (i=1,\ldots,n),$$

получим

$$\mathbf{q}_1 = \mathbf{d} \oplus \mathbf{e}_i,$$

где $\mathbf{e}_i$ – i-й столбец матрицы E.

Подав теперь на автомат M_1 любой входной символ $\mathbf{x}_2$, получим систему уравнений

$$G \circ (\mathbf{d} \oplus \mathbf{e}_i) = \mathbf{y}_2 \Theta F \circ \mathbf{x}_2,$$

т.е. идентификация вектора $\mathbf{e}_i$ с точностью, определяемой матрицей G, осуществляется простым экспериментом длины 2.

Следовательно, идентификация матрицы E с точностью, определяемой матрицей G, осуществляется n-кратным экспериментом высоты 2.

Идентификация матриц A, C и вектора $\mathbf{b}$ сводится теперь к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_l$ заранее неизвестной длины l и начального состояния $\mathbf{q}_0$ с целью сформировать систему уравнений

$$G \circ (A \circ \mathbf{q}_{t-1} \circ \mathbf{q}_{t-1}^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_{t-1} \oplus \mathbf{d} \oplus E \circ \mathbf{x}_t) = \\ = \mathbf{y}_{t+1} \Theta F \circ \mathbf{x}_{t+1} \quad (t = 1, \ldots, l-1). \tag{6.93}$$

В системе уравнений (6.93) каждый вектор $\mathbf{q}_{t-1}$ $(t = 2, \ldots, l-1)$ с помощью 1-го уравнения системы (6.1) выражается через значения $A, \mathbf{b}, C, \mathbf{d}, E, \mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$. После этого полученная система нелинейных уравнений решается относительно A, C и $\mathbf{b}$.

Итак, параметрическая идентификация автомата $M_1 \in \mathrm{A}_{n,1}^{inv}$ – трудная задача, состоящая в поиске и последующего решения нелинейных систем уравнений над кольцом Z_{p^k}.

Рассмотрим автомат $M_2 \in \mathrm{A}_{n,2}^{inv}$.

Подав на автомат $(M_2, \mathbf{0})$ входной символ

$$\mathbf{x}_1 = \mathbf{0},$$

получим систему нелинейных уравнений

$$G \circ \mathbf{d} = \mathbf{y}_1. \tag{6.94}$$

Решив систему (6.94), найдем множество допустимых значений матрицы G и вектора $\mathbf{d}$.

Все дальнейшие действия необходимо производить по отдельности с каждым решением $(G, \mathbf{d})$ системы уравнений (6.94).

Подав на автомат $(M_2, \mathbf{0})$ входной символ

$$\mathbf{x}_1 = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, 1, \underbrace{0, \ldots, 0}_{n-i \text{ раз}})^T \quad (i = 1, \ldots, n),$$

получим

$$\mathbf{e}_i = G^{-1} \circ \mathbf{y}_1 \Theta \mathbf{d},$$

где $\mathbf{e}_i$ – i-й столбец матрицы E.

Таким образом, для каждого решения $(G, \mathbf{d})$ системы уравнений (6.94) идентификация матрицы E осуществляется n-кратным экспериментом высоты 1.

Идентификация матриц A, C и вектора $\mathbf{b}$ сводится теперь к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_l$ заранее неизвестной длины l и начального состояния $\mathbf{q}_0$ с целью сформировать систему уравнений

$$G \circ (A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1}) = \mathbf{y}_{t+1} \quad (t = 0, 1, \ldots, l-1). \tag{6.95}$$

В системе (6.95) каждый вектор $\mathbf{q}_t$ $(t=1,\ldots,l-1)$ с помощью 1-го уравнения системы (6.2) выражается через значения $A,\mathbf{b},C,\mathbf{d},E,\mathbf{q}_0,\mathbf{x}_1,\ldots,\mathbf{x}_t$. После этого полученная система нелинейных уравнений решается относительно A, C и $\mathbf{b}$.

Итак, параметрическая идентификация автомата $M_2 \in \mathrm{A}_{n,2}^{inv}$ – трудная задача, состоящая в поиске и последующего решения нелинейных систем уравнений над кольцом Z_{p^k}.

Рассмотрим автомат $M_3 \in \mathrm{A}_{n,3}$.

Подав на автомат $(M_3,\mathbf{q_0})$, где

$$\mathbf{q}_0 = (\underbrace{1,\ldots,1}_{i\ раз},\underbrace{0,\ldots,0}_{n-i\ раз})^T,$$

входной символ

$$\mathbf{x}_1 = \mathbf{0},$$

получим

$$g_i = y_1^{(i)} \quad (i=1,\ldots,r).$$

Следовательно, простой эксперимент длины 1 идентифицирует параметры g_i $(i=1,\ldots,r)$.

Подав на автомат $(M_3,\mathbf{0})$ входной символ

$$\mathbf{x}_1 = (\underbrace{1,\ldots,1}_{i\ раз},\underbrace{0,\ldots,0}_{n-i\ раз})^T,$$

получим

$$f_i = y_1^{(i)} \quad (i=1,\ldots,r).$$

Следовательно, простой эксперимент длины 1 идентифицирует параметры f_i $(i=1,\ldots,r)$.

Подав на автомат $(M_3,\mathbf{0})$ входной символ

$$\mathbf{x}_1 = \mathbf{0},$$

получим

$$q_1^{(i)} = d_i \quad (i=1,\ldots,r).$$

Подав теперь на автомат M_3 любой входной символ

$$\mathbf{x}_i = (x_2^{(1)},\ldots,x_2^{(r)},\underbrace{0,\ldots,0}_{n-r\ раз})^T,$$

получим

$$d_i = g_i^{-1} \circ (y_2^{(i)} \Theta x_2^{(i)}) \quad (i=1,\ldots,r).$$

Следовательно, простой эксперимент длины 2 идентифицирует параметры d_i $(i=1,\ldots,r)$.

Подав на автомат $(M_3, \mathbf{0})$ входной символ

$$\mathbf{x}_1 = (\underbrace{1,\ldots,1}_{i\ раз}, \underbrace{0,\ldots,0}_{n-i\ раз})^T,$$

получим

$$q_1^{(i)} = d_i \oplus e_i \quad (i = 1,\ldots,r).$$

Подав теперь на автомат M_3 любой входной символ

$$\mathbf{x}_i = (x_2^{(1)},\ldots,x_2^{(r)}, \underbrace{0,\ldots,0}_{n-r\ раз})^T,$$

получим

$$e_i = g_i^{-1} \circ (y_2^{(i)} \Theta f_i \circ x_2^{(i)}) \Theta d_i \quad (i = 1,\ldots,r).$$

Следовательно, простой эксперимент длины 2 идентифицирует параметры e_i $(i = 1,\ldots,r)$.

Идентификация параметров $A_i, \mathbf{c}_i$ $(i = 1,\ldots,n)$ и d_i $(i = r+1,\ldots,n)$ сводится к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_l$ заранее неизвестной длины l и начального состояния $\mathbf{q}_0$ с целью сформировать систему уравнений

$$g_i \circ (\mathbf{q}_{t-1}^T \circ A_i \circ \mathbf{q}_{t-1} \oplus \mathbf{c}_i \circ \mathbf{q}_{t-1}) =$$

$$= y_{t+1}^{(i)} \Theta f_i \circ x_{t+1}^{(i)} \Theta g_i \circ (d_i \oplus e_i \circ x_t^{(i)}) \quad (i = 1,\ldots,r;\ t = 1,\ldots l-1),$$

причем $\mathbf{q}_{t-1}$ $(t = 2,\ldots,l-1)$ выражаются через $\mathbf{q}_0, \mathbf{x}_1,\ldots,\mathbf{x}_{t-1}$ и параметры системы.

Итак, параметрическая идентификация автомата $M_3 \in \mathrm{A}_{n,3}$ – трудная задача, состоящая в поиске и последующего решения нелинейных систем уравнений над кольцом Z_{p^k}.

Рассмотрим автомат $M_4 \in \mathrm{A}_{n,4}$.

Подадим на автомат $(M_4, \mathbf{0})$ входной символ

$$\mathbf{x}_1 = \mathbf{0}.$$

Получим систему нелинейных уравнений

$$g_i \circ d_i = y_1^{(i)} \quad (i = 1,\ldots,r). \tag{6.96}$$

Решив систему уравнений (6.96), найдем множество допустимых значений параметров g_i и d_i.

Все дальнейшие действия необходимо производить по отдельности с каждым решением $\{(g_i, d_i) \mid i = 1,\ldots,r\}$ системы уравнений (6.96).

Подав на автомат $(M_4, \mathbf{0})$ входной символ

$$\mathbf{x}_1 = (\underbrace{1,\ldots,1}_{i\ раз}, \underbrace{0,\ldots,0}_{n-i\ раз})^T,$$

получим

$$e_i = g_i^{-1} \circ y_1^{(i)} \Theta d_i \ \ (i = 1, \ldots, r).$$

Следовательно, для каждого решения $\{(g_i, d_i) \mid i = 1, \ldots, r\}$ системы уравнений (6.96) простой эксперимент длины 1 идентифицирует параметры $e_i \ \ (i = 1, \ldots, r)$.

Идентификация параметров $A_i, \mathbf{c}_i \ \ (i = 1, \ldots, n)$ и $d_i \ \ (i = r+1, \ldots, n)$ сводится к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_l$ заранее неизвестной длины l и начального состояния $\mathbf{q}_0$ с целью сформировать систему уравнений

$$\mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t =$$

$$= g_i^{-1} \circ y_{t+1}^{(i)} \Theta d_i \Theta e_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r; \ t = 1, \ldots l-1),$$

причем $\mathbf{q}_t \ \ (t = 1, \ldots, l-1)$ выражаются через $\mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1}$ и параметры системы.

Итак, параметрическая идентификация автомата $M_4 \in \mathrm{A}_{n,4}$ – трудная задача, состоящая в поиске и последующего решения нелинейных систем уравнений над кольцом Z_{p^k}.

Пример 6.3. Решим задачи параметрической идентификации для автоматов, построенных в примере 6.1, в предположении, что экспериментатор может управлять входом, а также осуществлять инициализацию автомата требуемое число раз.

1. Рассмотрим, автомат $M_R \in \mathrm{A}_{3,4}$.

Подав на автомат $(M_R, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,1,0)^T,$$

входной символ

$$x_1 = 0,$$

получим

$$h = \Theta y_1.$$

Подав на автомат $(M_R, \mathbf{0})$ входной символ

$$x_1 = 1,$$

получим

$$d = \Theta h^{-1} \circ y_1.$$

Подав на автомат $(M_R, \mathbf{0})$ входное слово

$$x_1 x_2 = 00,$$

получим

$$b = \Theta h^{-2} \circ y_2.$$

Подав на автомат $(M_R, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,0,1)^T,$$

входное слово

$$x_1 x_2 = 00,$$

получим

$$r = h^{-2} \circ y_2 \oplus 2h^{-1} \Theta b.$$

Подав на автомат $(M_R, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,1,0)^T$$

входное слово

$$x_1 x_2 = 00,$$

получим

$$a = \Theta 2h^{-1} \Theta b \Theta h^{-2} \circ y_2.$$

2. Рассмотрим, автомат $M_{S_1} \in \mathrm{A}_{3,4}$.

Подав на автомат $(M_{S_1}, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,1,0)^T$$

входной символ

$$x_1 = 0,$$

получим

$$h = y_1.$$

Подав на автомат $(M_{S_1}, \mathbf{0})$ входной символ

$$x_1 = 1,$$

получим

$$a = \Theta h^{-1} \circ y_1.$$

3. Рассмотрим, автомат $M_L \in \mathrm{A}_{3,4}$.

Подав на автомат $(M_L, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,1,0)^T,$$

входной символ

$$x_1 = 0,$$

получим

$$h = 1 \Theta y_1.$$

Подав на автомат $(M_L, \mathbf{0})$ входной символ

$$x_1 = 1,$$

получим

$$a = \Theta h^{-1} \circ y_1.$$

Подав на автомат $(M_L, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (1,0,0)^T,$$

входное слово

$$x_1 x_2 = 00,$$

получим

$$a_2 = h^{-1} \circ y_1$$

и

$$y_2 = (1 \Theta h) \circ h \circ a_2 \oplus h \circ a_2 \circ (1 \Theta h \circ a_1). \qquad (6.97)$$

Из уравнения (6.97) находим множество допустимых значений параметра a_1.

Подав на автомат $(M_L, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (1,0,1)^T,$$

входное слово

$$x_1 x_2 = 00,$$

получим

$$y_2 = (1 \Theta h) \circ h \circ (a_2 \Theta 1) \oplus h \circ (1 \Theta h \circ a_1) \circ (a_2 \oplus h \circ a_3 \Theta 1). \qquad (6.98)$$

Из уравнения (6.98) находим множество допустимых значений параметра a_3.

4. Рассмотрим, автомат $M_H \in \mathrm{A}_{2,4}$.

Подав на автомат $(M_H, \mathbf{0})$ входной символ

$$x_1 = 1,$$

получим

$$c = y_1 \Theta 1.$$

Подав на автомат $(M_L, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (0,1),$$

входной символ

$$x_1 = 0,$$

получим

$$a = y_1 \Theta 1.$$

Подав на автомат $(M_L, \mathbf{q}_0)$, где

$$\mathbf{q}_0 = (1,0),$$

входной символ

$$x_1 = 0,$$

получим

$$a = y_1 \Theta 1.$$

6.4. Вариация поведения исследуемых автоматов.

В п.5.8 отмечено, что анализ вариации о.-д. функции, реализуемой инициальным автоматом над конечным кольцом, при вариации его параметров или начального состояния является для поточных шифров аналогом дифференциального и интегрального криптоанализа, разработанного для *DES*-подобных алгоритмов, осуществляющих блочное шифрование.

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M, \mathbf{q}_0)$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4})$.

Рассмотрим автомат $M_1 \in \mathrm{A}_{n,1}^{inv}$.

Охарактеризуем вариацию поведения о.-д. функции, реализуемой инициальным автоматом $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathrm{A}_{n,1}^{inv})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.1), получим

$$\begin{cases} \tilde{\mathbf{q}}_{t+1} = A \circ \tilde{\mathbf{q}}_t \circ \tilde{\mathbf{q}}_t^T \circ \mathbf{b} \oplus C \circ \tilde{\mathbf{q}}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = G \circ \tilde{\mathbf{q}}_t \oplus F \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.99)$$

Вычитая из уравнений системы (6.99) соответствующие уравнения системы (6.1), получим

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A \circ (\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \oplus \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \oplus \\ \qquad \oplus \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T)) \circ \mathbf{b} \oplus C \circ \Delta\mathbf{q}_t \quad (t \in \mathbf{Z}_+), \\ \Delta\mathbf{y}_{t+1} = G \circ \Delta\mathbf{q}_t \end{cases} \qquad (6.100)$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \ominus \mathbf{q}_t$$

и

$$\Delta\mathbf{y}_{t+1} = \tilde{\mathbf{y}}_{t+1} \ominus \mathbf{y}_{t+1}$$

для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация поведения о.-д. функции, реализуемой инициальным автоматом $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathrm{A}_{n,1}^{inv})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.100).

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathrm{A}_{n,1}^{inv})$, при переходе от параметров A, $\mathbf{b}$, C, $\mathbf{d}$, E, F, G к параметрам $\tilde{A}$, $\tilde{\mathbf{b}}$, $\tilde{C}$, $\tilde{\mathbf{d}}$, $\tilde{E}$, $\tilde{F}$, $\tilde{G}$.

Подставим эти значения параметров в систему (6.1), получим

$$\begin{cases} \tilde{\mathbf{q}}_1 = \tilde{A} \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \tilde{\mathbf{b}} \oplus \tilde{C} \circ \mathbf{q}_0 \oplus \tilde{\mathbf{d}} \oplus \tilde{E} \circ \mathbf{x}_1 \\ \tilde{\mathbf{y}}_1 = \tilde{G} \circ \mathbf{q}_0 \oplus \tilde{F} \circ \mathbf{x}_1 \end{cases} \qquad (6.101)$$

и

$$\begin{cases} \tilde{\mathbf{q}}_{t+1} = \tilde{A} \circ \tilde{\mathbf{q}}_t \circ \tilde{\mathbf{q}}_t^T \circ \tilde{\mathbf{b}} \oplus \tilde{C} \circ \tilde{\mathbf{q}}_t \oplus \tilde{\mathbf{d}} \oplus \tilde{E} \circ \mathbf{x}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = \tilde{G} \circ \tilde{\mathbf{q}}_t \oplus \tilde{F} \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{N}). \qquad (6.102)$$

Вычитая из уравнений систем (6.101) и (6.102) соответствующие уравнения системы (6.1), получим

$$\begin{cases} \Delta\mathbf{q}_1 = \Delta A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \mathbf{b} \oplus A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \mathbf{q}_0 \circ \mathbf{q}_0^T \circ \Delta\mathbf{b} \oplus \\ \qquad \oplus \Delta C \circ \mathbf{q}_0 \oplus \Delta\mathbf{d} \oplus \Delta E \circ \mathbf{x}_1 \\ \Delta\mathbf{y}_1 = \Delta G \circ \mathbf{q}_0 \oplus \Delta F \circ \mathbf{x}_1 \end{cases} \tag{6.103}$$

и

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus C \circ \Delta\mathbf{q}_t \oplus \\ \quad \oplus \Delta C \circ \mathbf{q}_t \oplus \Delta C \circ \Delta\mathbf{q}_t \oplus \Delta\mathbf{d} \oplus \Delta E \circ \mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = G \circ \Delta\mathbf{q}_t \oplus \Delta G \circ \mathbf{q}_t \oplus \Delta G \circ \Delta\mathbf{q}_t \oplus \Delta F \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{N}), \tag{6.104}$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \Theta \mathbf{q}_t \quad (t \in \mathbf{N})$$

и

$$\Delta u = \tilde{u} \Theta u \quad (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, F, G\}).$$

Таким образом, вариация поведения о.-д. функции, реализуемой инициальным автоматом $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathrm{A}_{n,1}^{inv})$, при вариации его параметров характеризуется системами равенств (6.103) и (6.104).

Рассмотрим автомат $M_2 \in \mathrm{A}_{n,2}^{inv}$.

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_2, \mathbf{q}_0)$ $(M_2 \in \mathrm{A}_{n,2}^{inv})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.2), получим

$$\begin{cases} \tilde{\mathbf{q}}_{t+1} = A \circ \tilde{\mathbf{q}}_t \circ \tilde{\mathbf{q}}_t^T \circ \mathbf{b} \oplus C \circ \tilde{\mathbf{q}}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = G \circ \tilde{\mathbf{q}}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+) \tag{6.105}$$

Вычитая из уравнений системы (6.105) соответствующие уравнения системы (6.2), получим

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A \circ (\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \oplus \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \oplus \\ \qquad \oplus \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T)) \circ \mathbf{b} \oplus C \circ \Delta\mathbf{q}_t \quad (t \in \mathbf{Z}_+), \\ \Delta\mathbf{y}_{t+1} = G \circ \Delta\mathbf{q}_{t+1} \end{cases} \tag{6.106}$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \Theta \mathbf{q}_t$$

и

$$\Delta\mathbf{y}_{t+1} = \tilde{\mathbf{y}}_{t+1} \Theta \mathbf{y}_{t+1}$$

для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_2, \mathbf{q}_0)$ $(M_2 \in \mathrm{A}_{n,2}^{inv})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.106).

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_2, \mathbf{q}_0)$ $(M_2 \in \mathrm{A}_{n,2}^{inv})$, при переходе от параметров A, $\mathbf{b}$, C, $\mathbf{d}$, E, G к параметрам $\tilde{A}$, $\tilde{\mathbf{b}}$, $\tilde{C}$, $\tilde{\mathbf{d}}$, $\tilde{E}$, $\tilde{G}$.

Подставив эти значения параметров в систему (6.2), получим

$$\begin{cases} \tilde{\mathbf{q}}_{t+1} = \tilde{A} \circ \tilde{\mathbf{q}}_t \circ \tilde{\mathbf{q}}_t^T \circ \tilde{\mathbf{b}} \oplus \tilde{C} \circ \tilde{\mathbf{q}}_t \oplus \tilde{\mathbf{d}} \oplus \tilde{E} \circ \mathbf{x}_{t+1} \\ \tilde{\mathbf{y}}_{t+1} = \tilde{G} \circ \tilde{\mathbf{q}}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.107)$$

Вычитая из уравнений системы (6.107) соответствующие уравнения системы (6.2), получим

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \Delta\mathbf{q}_t \circ \mathbf{q}_t^T \circ \Delta\mathbf{b} \oplus \Delta A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \mathbf{b} \oplus \\ \quad \oplus \Delta A \circ \Delta\mathbf{q}_t \circ (\Delta\mathbf{q}_t)^T \circ \Delta\mathbf{b} \oplus C \circ \Delta\mathbf{q}_t \oplus \\ \quad \oplus \Delta C \circ \mathbf{q}_t \oplus \Delta C \circ \Delta\mathbf{q}_t \oplus \Delta\mathbf{d} \oplus \Delta E \circ \mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = G \circ \Delta\mathbf{q}_{t+1} \oplus \Delta G \circ \mathbf{q}_{t+1} \oplus \Delta G \circ \Delta\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.108)$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \Theta \mathbf{q}_t \quad (t \in \mathbf{Z}_+)$$

и

$$\Delta u = \tilde{u} \Theta u \quad (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, F, G\}).$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_2, \mathbf{q}_0)$ $(M_2 \in \mathrm{A}_{n,2}^{inv})$, при вариации его параметров характеризуется системой равенств (6.108).

Рассмотрим автомат $M_3 \in \mathrm{A}_{n,3}$.

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_3, \mathbf{q}_0)$ $(M_3 \in \mathrm{A}_{n,3})$ при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.7), получим

$$\begin{cases} q_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ A_i \circ \tilde{\mathbf{q}}_t \oplus \mathbf{c}_i \circ \tilde{\mathbf{q}}_t \oplus \\ \qquad \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \\ q_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ A_i \circ \tilde{\mathbf{q}}_t \oplus \mathbf{c}_i \circ \tilde{\mathbf{q}}_t \oplus d_i \ \ (i = r+1, \ldots, n) \\ y_{t+1}^{(i)} = g_i \circ \tilde{q}_t^{(i)} \oplus f_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.109)$$

Вычитая из уравнений системы (6.109) соответствующие уравнения системы (6.7), получим

$$\begin{cases} \Delta q_{t+1}^{(i)} = (\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \ \ (i = 1, \ldots, r) \\ \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \ \ (i = r+1, \ldots, n) \\ \Delta y_{t+1}^{(i)} = g_i \circ \Delta q_t^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.110)$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \Theta \mathbf{q}_t,$$

$$\Delta q_t^{(i)} = \tilde{q}_t^{(i)} \Theta q_t^{(i)} \ \ (i = 1, \ldots, n)$$

и

$$\Delta y_{t+1}^{(i)} = \tilde{y}_{t+1}^{(i)} \Theta y_{t+1}^{(i)} \ \ (i = 1, \ldots, r)$$

для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_3, \mathbf{q}_0)$ $(M_3 \in \mathrm{A}_{n,3})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.110).

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_3, \mathbf{q}_0)$ $(M_3 \in \mathrm{A}_{n,3})$ при переходе от параметров A_{ii}, $\mathbf{c}_i$, d_i, e_i $(i = 1, \ldots, n)$ и g_i, f_i $(i = 1, \ldots, r)$ к параметрам $\tilde{A}_i$, $\tilde{\mathbf{c}}_i$, $\tilde{d}_i$, $\tilde{e}_i$ $(i = 1, \ldots, n)$ и $\tilde{g}_i$, $\tilde{f}_i$ $(i = 1, \ldots, r)$.

Подставив эти значения параметров в систему (6.7), получим

$$\begin{cases} q_1^{(i)} = \mathbf{q}_0^T \circ \tilde{A}_i \circ \mathbf{q}_0 \oplus \tilde{\mathbf{c}}_i \circ \mathbf{q}_0 \oplus \\ \qquad \oplus \tilde{d}_i \oplus \tilde{e}_i \circ x_1^{(i)} \ \ (i = 1, \ldots, r) \\ \tilde{q}_1^{(i)} = \mathbf{q}_0^T \circ \tilde{A}_i \circ \mathbf{q}_0 \oplus \tilde{\mathbf{c}}_i \circ \mathbf{q}_0 \oplus \tilde{d}_i \ \ (i = r+1, \ldots, n) \\ \tilde{y}_1^{(i)} = \tilde{g}_i \circ q_0^{(i)} \oplus \tilde{f}_i \circ x_1^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (6.111)$$

и

$$\begin{cases} \widetilde{q}_{t+1}^{(i)} = \widetilde{\mathbf{q}}_t^T \circ \widetilde{A}_i \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{\mathbf{c}}_i \circ \widetilde{\mathbf{q}}_t \oplus \\ \qquad \oplus \widetilde{d}_i \oplus \widetilde{e}_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \\ \widetilde{q}_{t+1}^{(i)} = \widetilde{\mathbf{q}}_t^T \circ \widetilde{A}_i \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{\mathbf{c}}_i \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{d}_i \ \ (i=r+1,\ldots,n) \\ \widetilde{y}_{t+1}^{(i)} = \widetilde{g}_i \circ \widetilde{q}_t^{(i)} \oplus \widetilde{f}_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \end{cases} \quad (t \in \mathbf{N}). \qquad (6.112)$$

Вычитая из уравнений систем (6.111) и (6.112) соответствующие уравнения системы (6.7), получим

$$\begin{cases} \Delta q_1^{(i)} = \mathbf{q}_0^T \circ \Delta A_i \circ \mathbf{q}_0 \oplus \Delta \mathbf{c}_i \circ \mathbf{q}_0 \oplus \\ \qquad \Delta d_i \oplus \Delta e_i \circ x_1^{(i)} \ \ (i=1,\ldots,r) \\ \Delta q_1^{(i)} = \mathbf{q}_0^T \circ \Delta A_i \circ \mathbf{q}_0 \oplus \Delta \mathbf{c}_i \circ \mathbf{q}_0 \oplus \Delta d_i \ \ (i=r+1,\ldots,n) \\ \Delta y_1^{(i)} = \Delta g_i \circ q_0^{(i)} \oplus \Delta f_i \circ x_1^{(i)} \ \ (i=1,\ldots,r) \end{cases} \qquad (6.113)$$

и

$$\begin{cases} \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta \mathbf{q}_t \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \Delta \mathbf{q}_t \oplus (\Delta \mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta \mathbf{q}_t)^T \circ A_i \circ \Delta \mathbf{q}_t \oplus (\Delta \mathbf{q}_t)^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta \mathbf{q}_t)^T \circ \Delta A_i \circ \Delta \mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta \mathbf{q}_t \oplus \Delta \mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \Delta \mathbf{c}_i \circ \Delta \mathbf{q}_t \oplus \Delta d_i \oplus \Delta e_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \\ \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta \mathbf{q}_t \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \Delta \mathbf{q}_t \oplus (\Delta \mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta \mathbf{q}_t)^T \circ A_i \circ \Delta \mathbf{q}_t \oplus (\Delta \mathbf{q}_t)^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta \mathbf{q}_t)^T \circ \Delta A_i \circ \Delta \mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta \mathbf{q}_t \oplus \Delta \mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \Delta \mathbf{c}_i \circ \Delta \mathbf{q}_t \oplus \Delta d_i \ \ (i=r+1,\ldots,n) \\ \Delta y_{t+1}^{(i)} = g_i \circ \Delta q_t^{(i)} \oplus \Delta g_i \circ q_t^{(i)} \oplus \\ \qquad \oplus \Delta g_i \circ \Delta q_t^{(i)} \oplus \Delta f_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \end{cases} \quad (t \in \mathbf{N}), \quad (6.114)$$

где

$$\Delta u = \widetilde{u} \Theta u \ \ (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, F, G\}).$$

для $u \in \{\widetilde{A}_i, \widetilde{\mathbf{c}}_i, \widetilde{d}_i, \widetilde{e}_i \mid i=1,\ldots,n\} \cup \{\widetilde{g}_i, \widetilde{f}_i \mid i=1,\ldots,r\}$ и

$$\Delta \mathbf{q}_t = \widetilde{\mathbf{q}}_t \Theta \mathbf{q}_t,$$

$$\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} \Theta q_t^{(i)} \ \ (i=1,\ldots,n)$$

и

$$\Delta y_{t+1}^{(i)} = \widetilde{y}_{t+1}^{(i)} \Theta y_{t+1}^{(i)} \ \ (i=1,\ldots,r)$$

для всех $t \in \mathbf{N}$.

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_3, \mathbf{q}_0)$ $(M_3 \in \mathrm{A}_{n,3})$, при вариации его параметров характеризуется системами равенств (6.113) и (6.114).

Рассмотрим автомат $M_4 \in \mathrm{A}_{n,4}$.

Охарактеризуем вариацию о.-д. функции, реализуемой инициальным автоматом $(M_4, \mathbf{q}_0)$ $(M_4 \in \mathrm{A}_{n,4})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.8), получим

$$\begin{cases} q_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ A_i \circ \tilde{\mathbf{q}}_t \oplus \mathbf{c}_i \circ \tilde{\mathbf{q}}_t \oplus \\ \qquad \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \\ q_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ A_i \circ \tilde{\mathbf{q}}_t \oplus \mathbf{c}_i \circ \tilde{\mathbf{q}}_t \oplus d_i \ \ (i = r+1, \ldots, n) \\ y_{t+1}^{(i)} = g_i \circ \tilde{q}_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.115)$$

Вычитая из уравнений системы (6.115) соответствующие уравнения системы (6.8), получим

$$\begin{cases} \Delta q_{t+1}^{(i)} = (\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \ \ (i = 1, \ldots, r) \\ \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \ \ (i = r+1, \ldots, n) \\ \Delta y_{t+1}^{(i)} = g_i \circ \Delta q_{t+1}^{(i)} \ \ (i = 1, \ldots, r) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.116)$$

где

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \ominus \mathbf{q}_t,$$

$$\Delta q_t^{(i)} = \tilde{q}_t^{(i)} \ominus q_t^{(i)} \ \ (i = 1, \ldots, n)$$

и

$$\Delta y_{t+1}^{(i)} = \tilde{y}_{t+1}^{(i)} \ominus y_{t+1}^{(i)} \ \ (i = 1, \ldots, r)$$

для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_4, \mathbf{q}_0)$ $(M_4 \in \mathrm{A}_{n,4})$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.116).

Охарактеризуем теперь вариацию о.-д. функции, реализуемой инициальным автоматом $(M_4, \mathbf{q}_0)$ $(M_4 \in \mathrm{A}_{n,4})$ при переходе от параметров $A_i, \mathbf{c}_i, d_i, e_i$ $(i = 1, \ldots, n)$ и g_i $(i = 1, \ldots, r)$ к параметрам $\tilde{A}_i, \tilde{\mathbf{c}}_i, \tilde{d}_i, \tilde{e}_i$ $(i = 1, \ldots, n)$ и $\tilde{g}_i$ $(i = 1, \ldots, r)$.

Подставив эти значения параметров в систему (6.8), получим

$$\begin{cases} \tilde{q}_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ \tilde{A}_i \circ \tilde{\mathbf{q}}_t \oplus \tilde{\mathbf{c}}_i \circ \tilde{\mathbf{q}}_t \oplus \\ \qquad \oplus \tilde{d}_i \oplus \tilde{e}_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \\ \tilde{q}_{t+1}^{(i)} = \tilde{\mathbf{q}}_t^T \circ \tilde{A}_i \circ \tilde{\mathbf{q}}_t \oplus \tilde{\mathbf{c}}_i \circ \tilde{\mathbf{q}}_t \oplus \tilde{d}_i \ \ (i=r+1,\ldots,n) \\ \tilde{y}_{t+1}^{(i)} = \tilde{g}_i \circ \tilde{q}_{t+1}^{(i)} \ \ (i=1,\ldots,r) \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.117)$$

Вычитая из уравнений системы (6.117) соответствующие уравнения системы (6.8), получим

$$\begin{cases} \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ \Delta A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \oplus \Delta\mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \Delta\mathbf{c}_i \circ \Delta\mathbf{q}_t \oplus \Delta d_i \oplus \Delta e_i \circ x_{t+1}^{(i)} \ \ (i=1,\ldots,r) \\ \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \mathbf{q}_t^T \circ \Delta A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ A_i \circ \Delta\mathbf{q}_t \oplus (\Delta\mathbf{q}_t)^T \circ \Delta A_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus (\Delta\mathbf{q}_t)^T \circ \Delta A_i \circ \Delta\mathbf{q}_t \oplus \mathbf{c}_i \circ \Delta\mathbf{q}_t \oplus \Delta\mathbf{c}_i \circ \mathbf{q}_t \oplus \\ \qquad \oplus \Delta\mathbf{c}_i \circ \Delta\mathbf{q}_t \oplus \Delta d_i \ \ (i=r+1,\ldots,n) \\ \Delta y_{t+1}^{(i)} = g_i \circ \Delta q_{t+1}^{(i)} \oplus \Delta g_i \circ q_{t+1}^{(i)} \oplus \Delta g_i \circ \Delta q_{t+1}^{(i)} \ \ (i=1,\ldots,r) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.118)$$

где

$$\Delta u = \tilde{u} \Theta u \quad (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, F, G\}).$$

для $u \in \{\tilde{A}_i, \tilde{\mathbf{c}}_i, \tilde{d}_i, \tilde{e}_i \mid i=1,\ldots,n\} \cup \{\tilde{g}_i, \tilde{f}_i \mid i=1,\ldots,r\}$ и

$$\Delta\mathbf{q}_t = \tilde{\mathbf{q}}_t \Theta \mathbf{q}_t,$$

$$\Delta q_t^{(i)} = \tilde{q}_t^{(i)} \Theta q_t^{(i)} \quad (i=1,\ldots,n)$$

и

$$\Delta y_{t+1}^{(i)} = \tilde{y}_{t+1}^{(i)} \Theta y_{t+1}^{(i)} \quad (i=1,\ldots,r)$$

для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_4, \mathbf{q}_0)$ $(M_4 \in \mathrm{A}_{n,4})$, при вариации его параметров характеризуется системой равенств (6.118).

Отметим, что установленные выше соотношения, характеризующие вариацию о.-д. функции, реализуемой инициальным автоматом $(M, \mathbf{q}_0)$ $(M \in \mathrm{A}_{n,1}^{inv} \cup \mathrm{A}_{n,2}^{inv} \cup \mathrm{A}_{n,3} \cup \mathrm{A}_{n,4})$, упрощаются, если на входящие в них величины наложены те или иные дополнительные ограничения.

Пример 6.4. Рассмотрим автоматы, построенные в примере 6.1.

1. Охарактеризуем вариацию о.-д. функций, реализуемых автоматами M_R, M_{S_1} и M_L при переходе от начального состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ к начальному состоянию $\tilde{\mathbf{q}}_0 = (\tilde{q}_0^{(1)}, \tilde{q}_0^{(2)}, \tilde{q}_0^{(3)})^T$.

Рассмотрим автомат M_R.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.9), получим

$$\begin{cases} \tilde{q}_{t+1}^{(1)} = \tilde{q}_t^{(1)} \Theta h \circ \tilde{q}_t^{(2)} \Theta h \circ \tilde{q}_t^{(3)} \Theta h \circ d \circ x_{t+1} \\ \tilde{q}_{t+1}^{(2)} = h \circ \tilde{q}_t^{(1)} \oplus (a \circ h \oplus 1) \circ \tilde{q}_t^{(2)} \\ \tilde{q}_{t+1}^{(3)} = h \circ b \oplus (1 \Theta h \circ r) \circ \tilde{q}_t^{(3)} \oplus h \circ \tilde{q}_t^{(1)} \circ \tilde{q}_t^{(3)} \\ \tilde{y}_{t+1} = \tilde{q}_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.119)$$

Вычитая из уравнений системы (6.119) соответствующие уравнения системы (6.9), получим

$$\begin{cases} \Delta q_{t+1}^{(1)} = \Delta q_t^{(1)} \Theta h \circ \Delta q_t^{(2)} \Theta h \circ \Delta q_t^{(3)} \\ \Delta q_{t+1}^{(2)} = h \circ \Delta q_t^{(1)} \oplus (a \circ h \oplus 1) \circ \Delta q_t^{(2)} \\ \Delta q_{t+1}^{(3)} = (1 \Theta h \circ r) \circ \Delta q_t^{(3)} \oplus h \circ (q_t^{(1)} \circ \Delta q_t^{(3)} \oplus \\ \qquad \oplus \Delta q_t^{(1)} \circ q_t^{(3)} \oplus \Delta q_t^{(1)} \circ \Delta q_t^{(3)}) \\ \Delta y_{t+1} = \Delta q_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.120)$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_R, \mathbf{q}_0)$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.120).

Рассмотрим автомат M_{S_1}.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.10), получим

$$\begin{cases} \tilde{q}_{t+1}^{(1)} = \tilde{q}_t^{(1)} \oplus h \circ \tilde{q}_t^{(2)} \Theta h \circ a \circ x_{t+1} \\ \tilde{q}_{t+1}^{(2)} = \tilde{q}_t^{(2)} \Theta h \circ \tilde{q}_t^{(1)} \oplus h \circ \tilde{q}_t^{(2)} \circ \tilde{q}_t^{(3)} \\ \tilde{q}_{t+1}^{(3)} = h \oplus \tilde{q}_t^{(3)} \Theta h \circ (\tilde{q}_t^{(2)})^2 \\ \tilde{y}_{t+1} = \tilde{q}_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.121)$$

Вычитая из уравнений системы (6.121) соответствующие уравнения системы (6.10), получим

$$\begin{cases} \Delta q_{t+1}^{(1)} = \Delta q_t^{(1)} \oplus h \circ \Delta q_t^{(2)} \\ \Delta q_{t+1}^{(2)} = \Delta q_t^{(2)} \Theta h \circ \Delta q_t^{(1)} \oplus h \circ (q_t^{(2)} \circ \Delta q_t^{(3)} \oplus \\ \qquad \oplus \Delta q_t^{(2)} \circ q_t^{(3)} \oplus \Delta q_t^{(2)} \circ \Delta q_t^{(3)}) \\ \Delta q_{t+1}^{(3)} = \Delta q_t^{(3)} \Theta h \circ (2 \circ \Delta q_t^{(2)} \oplus (\Delta q_t^{(2)})^2) \\ \Delta y_{t+1} = \Delta q_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+). \qquad (6.122)$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_{S_1}, \mathbf{q}_0)$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.122).

Рассмотрим автомат M_L.

Подставив $\tilde{\mathbf{q}}_0$ в систему (6.11), получим

$$\begin{cases} \tilde{q}_{t+1}^{(1)} = (1 \Theta h \circ a_1) \circ \tilde{q}_t^{(1)} \oplus h \circ a_1 \circ \tilde{q}_t^{(2)} \\ \tilde{q}_{t+1}^{(2)} = (1 \Theta h) \circ \tilde{q}_t^{(2)} \oplus h \circ \tilde{q}_t^{(1)} \circ (a_2 \Theta \tilde{q}_t^{(3)}) \Theta h \circ a \circ x_{t+1} \\ \tilde{q}_{t+1}^{(3)} = (1 \Theta h \circ a_3) \circ \tilde{q}_t^{(3)} \oplus h \circ \tilde{q}_t^{(1)} \circ \tilde{q}_t^{(2)} \\ \tilde{y}_{t+1} = \tilde{q}_{t+1}^{(2)} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (6.123)$$

Вычитая из уравнений системы (6.123) соответствующие уравнения системы (6.11), получим

$$\begin{cases} \Delta q_{t+1}^{(1)} = (1 \Theta h \circ a_1) \circ \Delta q_t^{(1)} \oplus h \circ a_1 \circ \Delta q_t^{(2)} \\ \Delta q_{t+1}^{(2)} = (1 \Theta h) \circ \Delta q_t^{(2)} \oplus h \circ a_2 \circ \Delta q_t^{(1)} \Theta \\ \qquad \Theta h \circ (q_t^{(1)} \circ \Delta q_t^{(3)} \oplus \Delta q_t^{(1)} \circ q_t^{(3)} \oplus \Delta q_t^{(1)} \circ \Delta q_t^{(3)}) \\ \Delta q_{t+1}^{(3)} = (1 \Theta h \circ a_3) \circ \Delta q_t^{(3)} \oplus \\ \qquad \oplus h \circ (q_t^{(1)} \circ \Delta q_t^{(2)} \oplus \Delta q_t^{(1)} \circ q_t^{(2)} \oplus \Delta q_t^{(1)} \circ \Delta q_t^{(2)}) \\ \Delta y_{t+1} = \Delta q_{t+1}^{(2)} \end{cases} \quad (t \in \mathbf{Z}_+). \quad (6.124)$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_L, \mathbf{q}_0)$, при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\tilde{\mathbf{q}}_0$ характеризуется системой равенств (6.124).

2. Охарактеризуем вариацию о.-д. функции, реализуемой автоматом M_H, при переходе от параметров a, b, c к параметрам $\tilde{a}$, $\tilde{b}$, $\tilde{c}$.

Подставив эти значения параметров в систему (6.12), получим

$$\begin{cases} \tilde{q}_{t+2} = 1 \Theta \tilde{a} \circ \tilde{q}_{t+1}^2 \Theta \tilde{b} \circ \tilde{q}_t \oplus \tilde{c} \circ x_{t+1} \\ \tilde{y}_{t+1} = \tilde{q}_{t+2} \end{cases} \quad (t \in \mathbf{Z}_+). \quad (6.125)$$

Вычитая из уравнений системы (6.125) соответствующие уравнения системы (6.12), получим

$$\begin{cases} \Delta q_{t+2} = \Theta a \circ (2 \circ q_{t+1} \circ \Delta q_{t+1} \oplus (\Delta q_{t+1})^2) \Theta \\ \qquad \Theta \Delta a \circ (q_{t+1}^2 \oplus 2 \circ q_{t+1} \circ \Delta q_{t+1} \oplus (\Delta q_{t+1})^2) \oplus \\ \qquad \oplus b \circ \Delta q_t \oplus \Delta b \circ q_t \oplus \Delta b \circ \Delta q_t \oplus \Delta c \circ x_{t+1} \\ \Delta y_{t+1} = \Delta q_{t+2} \end{cases} \quad (t \in \mathbf{Z}_+). \quad (6.126)$$

Таким образом, вариация о.-д. функции, реализуемой инициальным автоматом $(M_H, \mathbf{q}_0)$, при вариации его параметров характеризуется системой равенств (6.126).

6.5. Шифры на основе псевдофракталов.

Основная идея построения шифров на основе псевдофракталов состоит в следующем.

Очередной фрагмент исходной двоичной последовательности представляется 24-разрядным bmp-файлом [76], т.е. растровым массивом, элементы которого – RGB-компоненты (r,g,b) $(r,g,b\in \mathbf{Z}_{256})$, определяющие цвет соответствующего пикселя.

При обработке очередного пикселя реализуется итерационный процесс, состоящий в проверке выполнения (либо нарушения) некоторого условия, определяемого черно-белым представлением псевдофрактала в области дисплея (см. п.1.7).

Номер итерации, на котором заданное условие нарушается (соответственно, выполняется), определяет номер перестановки, определенной на множестве цветов пикселя и принадлежащей заданному семейству легко-вычислимых перестановок. Эта перестановка цветов применяется к обрабатываемому пикселю.

Обработанный таким образом bmp-файл (возможно, после преобразования его в двоичную последовательность) представляет собой соответствующий фрагмент шифртекста. Корректность предложенного подхода вытекает из обратимости перестановок.

Отметим, что предложенная схема шифрования применима к шифрованию не только двоичных последовательностей, но также и к шифрованию изображений, представленных bmp-файлами.

Таким образом, предложенная схема шифрования характеризуется тем, что черно-белое представление псевдофрактала в области дисплея применяется для управления семейством легко-вычислимых перестановок, каждая из которых определена на множестве цветов пикселя.

Более того, предложенная схема дает возможность строить достаточно широкий класс нестационарных поточных шифров.

Действительно, в п.2.1 предложена общая схема нестационарного поточного шифра, состоящая в том, что задан генератор чисел, принадлежащих множеству $\mathbf{N}_m$, а также семейство алгоритмов $\boldsymbol{A}=\{A_i\}_{i\in \mathbf{N}_m}$, представленных в неявном виде (рис. 6.4). При генерации числа $i\in \mathbf{N}_m$ шифрование очередного фрагмента исходного текста осуществляется алгоритмом A_i.

В предложенной выше схеме шифрования роль семейства алгоритмов $\boldsymbol{A}=\{A_i\}_{i\in \mathbf{N}_m}$ играет заданное семейство легко-вычислимых перестановок, определенных на множестве цветов пикселя.

Инициализация процесса шифрования очередного фрагмента исходной двоичной последовательности определяется выбором черно-белого представления псевдофрактала в области дисплея, а также семейства легко-вычислимых перестановок, определенных на множестве цветов пикселя.

Ясно, что свойство «быть поточным шифром» обеспечивается сквозной нумерацией выбираемых легко-вычислимых перестановок, определенных на множестве цветов пикселя.

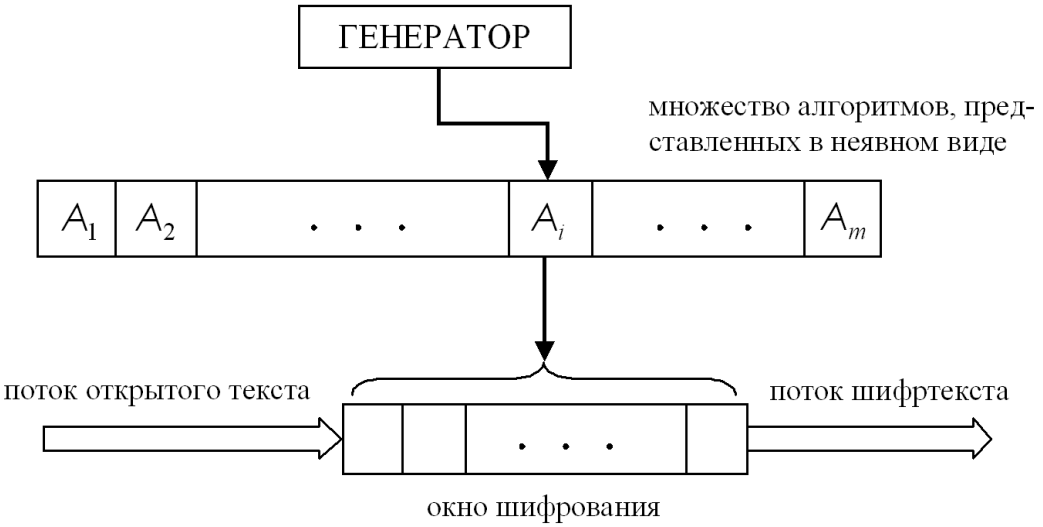


Рис. 6.4. Общая схема нестационарного поточного шифра.

В [69] предложенная выше схема реализована для одного из наиболее изученных фрактальных отображений – отображения Мандельброта [130], т.е. отображения $f : \mathbf{C} \to \mathbf{C}$, определяемого равенством

$$f(z) = z^2 + c,$$

где c – константа (рис. 6.5).

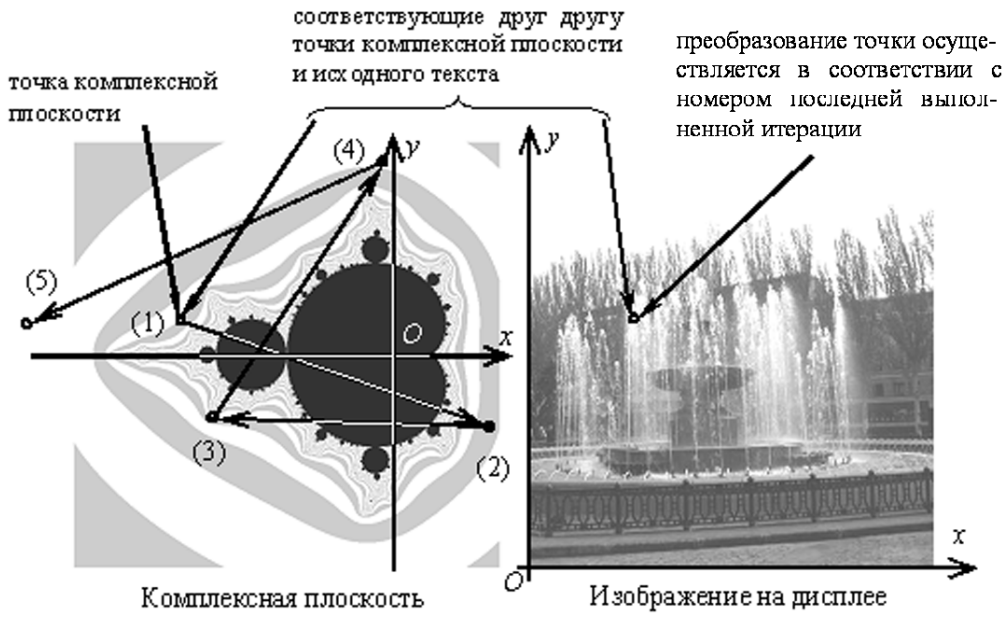


Рис. 6.5. Схема процесса шифрования на основе отображения Мандельброта.

Параметры шифра, определяющие число итераций – это радиус M круга (R,M) и верхняя граница числа K для числа итераций, применяемых к точке комплексной плоскости $\mathbf{C}$.

Условие, определяемое псевдофракталом Мандельброта, состоит в выходе образа за круг (R,O) в течение K итераций.

Класс используемых семейств легко-вычислимых перестановок определен равенствами

$$\mathbf{f}_n:\begin{cases} r_n = (r_0 + \\ \quad + n\cdot|\alpha_1^n\cdot a_1 - \alpha_2^n\cdot a_2 - \alpha_3^n\cdot a_3|) \pmod{256} \\ g_n = (g_0 + \\ \quad + n\cdot|\alpha_2^n\cdot a_2 - \alpha_1^n\cdot a_1 - \alpha_3^n\cdot a_3|) \pmod{256} \\ b_n = (b_0 + \\ \quad + n\cdot|\alpha_3^n\cdot a_3 - \alpha_1^n\cdot a_1 - \alpha_2^n\cdot a_2|) \pmod{256} \end{cases} \quad (n=1,\ldots,2^8-1), \quad (6.127)$$

где r_0, g_0, b_0 и r_n, g_n, b_n, соответственно, исходные и преобразованные компоненты цвета пикселя, а $\alpha_i, a_i \in \mathbf{Z}$ $(i=1,2,3)$ – параметры, играющие роль секретного сеансового ключа.

Показано, что любая перестановка $\mathbf{f}_n$ $(n=1,\ldots,2^8-1)$, определенная формулой (6.127), не имеет неподвижных точек тогда и только тогда, когда

$$\alpha_1\cdot a_1 + \alpha_2\cdot a_2 + \alpha_3\cdot a_3 \equiv 1 \pmod 2. \quad (6.128)$$

При этом длина секретного сеансового ключа

$$(\alpha_1,\alpha_2,\alpha_3,a_1,a_2,a_3) \in \mathbf{Z}_{2^8-1}^6 \quad (6.129)$$

составляет 48 бит, а число N секретных сеансовых ключей, удовлетворяющих условиям (6.128) и (6.129) равно

$$N \approx 27.4415\cdot 2^{42}. \quad (6.130)$$

Отметим, что из (6.130) вытекает, что вероятность того, что случайная двоичная последовательность длины 48 является допустимым секретным сеансовым ключом, равна

$$p \approx 0.4288.$$

Итак, алгоритм шифрования на основе псевдофрактала Мандельброта имеет следующий вид (через w и h обозначена, соответственно, ширина и высота изображения в пикселях, а параметрами, задаваемыми пользователем, являются такие положительные числа p_j, q_j $(j\in\{\min,\max\})$, что $u_{\max} > u_{\min}$ $(u\in\{p,q\})$, число $K\in\mathbf{N}$ – верхняя граница числа итераций при обработке пикселя, число $M\in\mathbf{N}$ – радиус круга и секретный сеансовый ключ $(\alpha_1,\alpha_2,\alpha_3,a_1,a_2,a_3)\in\mathbf{Z}_{2^8-1}^6$).

Алгоритм 6.1.

Шаг 1. $\Delta p := (p_{\max} - p_{\min}) \cdot w^{-1}$.

Шаг 2. $\Delta q := (q_{\max} - q_{\min}) \cdot h^{-1}$.

Шаг 3. $i := 1$.

Шаг 4. $j := 1$.

Шаг 5. $p_0 := p_{\min} + (i-1) \cdot \Delta p$.

Шаг 6. $q_0 := q_{\min} + (j-1) \cdot \Delta q$.

Шаг 7. $k := 0$.

Шаг 8. $x_0 := 0$.

Шаг 9. $y_0 := 0$.

Шаг 10. $x_{k+1} := x_k^2 - y_k^2 + p_0$,

Шаг 11. $y_{k+1} := 2 \cdot x_k \cdot y_k + q_0$.

Шаг 12. $k := k + 1$.

Шаг 13. $R := x_k^2 + y_k^2$.

Шаг 14. Если

$$R > M$$

или

$$k = K,$$

то

$$(r,g,b)_{(i-1)\cdot h+j} := \mathbf{f}_k((r,g,b)_{(i-1)\cdot h+j}, \alpha_1, \alpha_2, \alpha_3, a_1, a_2, a_3)$$

и переход к шагу 15, иначе – к шагу 10.

Шаг 15. $j := j + 1$.

Шаг 16. Если

$$j \le h,$$

то переход к шагу 5, иначе – к шагу 17.

Шаг 17. $i := i + 1$.

Шаг 18. Если

$$i \le w,$$

то переход к шагу 4, иначе – конец.

Алгоритм 6.1 был реализован Э.Е. Зайцевой в среде Microsoft Visual C++ с использованием MFC App Wizard.

Пример 6.5. В качестве примеров работы программы, реализующей алгоритм 6.1, приведем результаты шифрования текста, а также изображения, представленного bmp-файлом.

1. Текстовый файл объемом 64 Кб, преобразованный в 24-разрядный bmp-файл, изображен на рис. 6.6.а.

Результат шифрования этого файла, представленный в виде 24-разрядного bmp-файла, представлен на рис. 6.6.б.

После преобразования результата шифрования в текстовый файл был осуществлен анализ частот вхождения символов в исходный текст и шифртекст.

Гистограммы распределения частот символов в исходном тексте и шифртексте представлены на рис. 6.7.

2. На рис. 6.8 приведены результаты шифрования изображения.

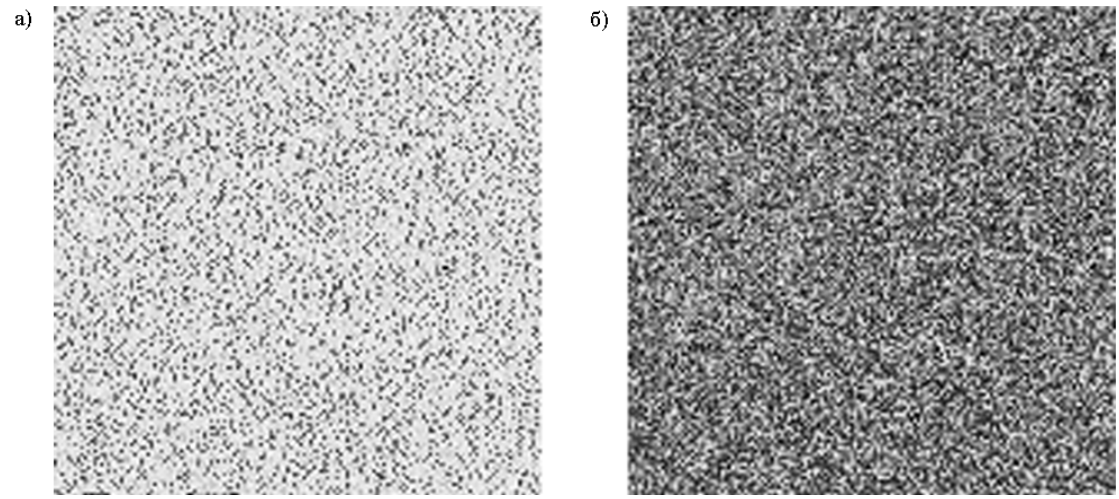


Рис. 6.6. Изображения текстовых файлов: а) исходного; б) зашифрованного.

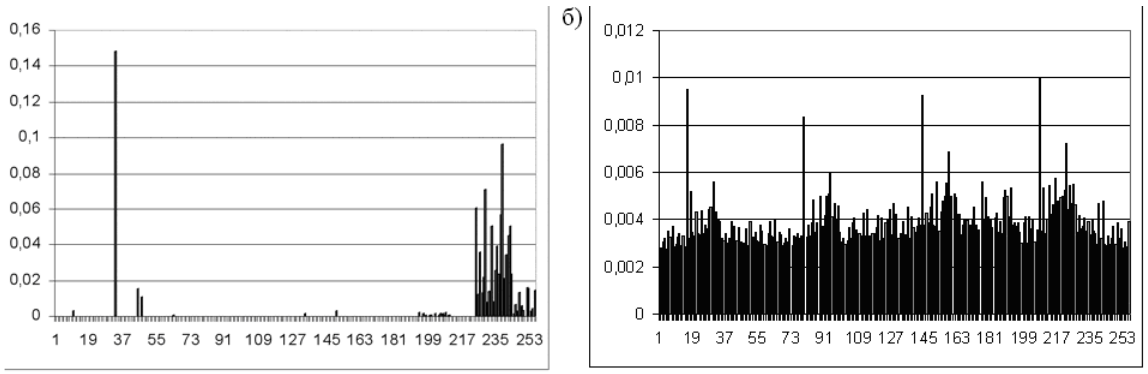


Рис. 6.7. Частоты букв в: а) исходном файле; б) зашифрованном файле.

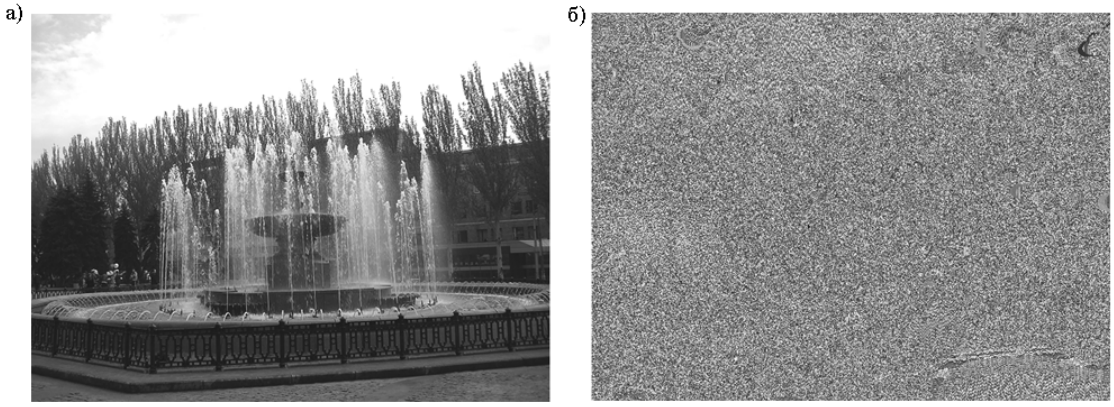


Рис. 6.8. Изображение, представленное 24-разрядным bmp-файлом: а) исходное изображение; б) зашифрованное изображение.

Естественным обобщением класса семейств перестановок (6.127) является определенный в терминах кольца Z_{p^k} класс семейств перестановок

$$\begin{cases} x_n^{(1)} = x_0^{(1)} \Theta n \circ (\overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \; \Theta 2 \circ \alpha_1^n \circ a_1) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (n = 1, \ldots, p^k - 1), \\ x_n^{(l)} = x_0^{(l)} \Theta n \circ (\overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \; \Theta 2 \circ \alpha_l^n \circ a_l) \end{cases} \qquad (6.131)$$

где $l \in \mathbf{N}$ и $\alpha_j, a_j \in \mathbf{Z}_{p^k}$ $(j = 1, \ldots, l)$.

Ясно, что класс семейств перестановок (6.131) дает возможность строить поточные шифры на основе черно-белого представления l-мерного $(l \in \mathbf{N})$ псевдофрактала в области l-мерного дисплея.

Так как класс семейств перестановок (6.131) представляет собой класс линейных автоматов с переменной структурой над кольцом Z_{p^k}, то предложенная схема шифрования на основе псевдофракталов представляет собой схему шифрования, построенную на основе класса линейных автоматов над конечным кольцом, что подчеркивает актуальность исследований, представленных в разделе 5.

Исследуем класс семейств легко вычислимых перестановок, являющийся естественным обобщением класса (6.131).

Введем вначале соответствующие понятия и определения.

Пусть S – конечное множество, а P_S – множество всех перестановок множества S.

Перестановку $f \in P_S$ назовем легко-вычислимой, если для любого элемента $s \in S$ асимптотическая емкостная и временная сложность алгоритма A_f, реализующего перестановку f, соответственно, равна

$$V_f = O(\log |S|) \;\; (|S| \to \infty)$$

и

$$T_f = O(\log^2 |S|) \;\; (|S| \to \infty).$$

Для любого конечного множества S обозначим через P_S^{ec} множество всех легко-вычислимых перестановок $f \in P_S$.

Если $S = \overset{l}{\underset{i=1}{\times}} S_i$ $(l > 1)$, где $|S_i| > 1$ $(i \in \mathbf{N}_l)$ и $\mathbf{f} = (f_1, \ldots, f_l)$, где $f_i \in P_{S_i}$ $(i \in \mathbf{N}_l)$, причем

$$\mathbf{f}(\mathbf{s}) = (f_1(s_1), \ldots, f_l(s_l))$$

для всех $\mathbf{s} = (s_1, \ldots, s_l) \in S$, то перестановку $\mathbf{f} \in P_S$ назовем l-разложимой.

Обозначим через $P_S^{l\text{-}s}$ множество всех l-разложимых перестановок множества S.

Целесообразность выделения подмножества $P_S^{l\text{-}s}$ множества P_S обосновывает следующее

Утверждение 6.9. Пусть $S=\underset{i=1}{\overset{l}{\times}} S_i$ $(l>1)$, где $|S_i|>1$ $(i\in \mathbf{N}_l)$ и $f_i\in P_{S_i}^{ec}$ $(i\in \mathbf{N}_l)$. Тогда $\mathbf{f}=(f_1,\ldots,f_l)\in P_S^{ec}$.

Доказательство. Предположим, что $f_i\in P_{S_i}^{ec}$ для всех $i\in \mathbf{N}_l$.

Асимптотическая временная и емкостная сложность вычисления образа любого элемента $s_i\in S_i$ $(i\in \mathbf{N}_l)$ равна, соответственно,

$$T_{f_i}=O(\log^2|S_i|)\quad (|S_i|\to\infty)$$

и

$$V_{f_i}=O(\log|S_i|)\quad (|S_i|\to\infty).$$

Так как вычисление значения $\mathbf{f}(\mathbf{s})$ $(\mathbf{s}=(s_1,\ldots,s_l)\in S)$ можно свести к независимым вычислениям значений $f_i(s_i)$ $(i\in \mathbf{N}_l)$, то

$$T_{\mathbf{f}}\le\sum_{i=1}^{l}T_{f_i}=O(\sum_{i=1}^{l}\log^2|S_i|)=O((\log\prod_{i=1}^{l}|S_i|)^2)=$$

$$=O(\log^2|S|)\quad (|S|\to\infty),$$

что и требовалось показать.

Так как $\mathbf{s}=(s_1,\ldots,s_l)$ и $V_{f_i}=O(\log|S_i|)$ $(i\in \mathbf{N}_l)$, то

$$V_f=O(\sum_{i=1}^{l}V_{f_i})=O(\sum_{i=1}^{l}\log|S_i|)=O(\log|S|)\quad (|S|\to\infty).$$

Утверждение доказано.

Семейство легко-вычислимых перестановок

$$\mathcal{S}=\{f_j\}_{j\in\mathbf{N}},$$

конечного множества S назовем легко-вычислимым семейством перестановок, если существует такой алгоритм последовательной генерации элементов семейства $\mathcal{S}$, что:

1) генерация алгоритма A_{f_1} осуществляется за время

$$T=O(\log|S|)\ (|S|\to\infty);$$

2) преобразование алгоритма A_{f_j} $(j\in\mathbf{N})$ в алгоритм $A_{f_{j+1}}$ осуществляется за время

$$T_1=O(\log^2|S|)\ (|S|\to\infty).$$

Обозначим через $\mathbf{Z}_{p^k}^{inv}$ множество всех обратимых элементов кольца Z_{p^k}, т.е. $(\mathbf{Z}_{p^k}^{inv},\circ)$ – мультипликативная группа кольца Z_{p^k}.

Пусть l $(2 < l \le k)$ – такое фиксированное число, что

$$(l-2) \pmod{p^k} \in \mathbf{Z}_{p^k}^{inv}.$$

Зафиксируем элементы $\alpha_i, \beta_i, a_i \in \mathbf{Z}_{p^k}^{inv}$ $(i \in \mathbf{N}_l)$ кольца Z_{p^k}. Положим

$$A_i(n) = \bigoplus_{j=1}^{l} a_j \circ \alpha_j^n \Theta 2 \circ a_i \circ \alpha_i^n \quad (i \in \mathbf{N}_l, n \in \mathbf{N}).$$

Определим однопараметрические семейства аффинных отображений

$$S^{(i)} = \{ f_n^{(i)} : \mathbf{Z}_{p^k} \to \mathbf{Z}_{p^k} \mid n \in \mathbf{N} \} \quad (i \in \mathbf{N}_l)$$

с помощью равенства

$$f_n^{(i)}(x) = \beta_i^n \circ x \oplus n \pmod{p^k} \circ A_i(n) \quad (x \in \mathbf{Z}_{p^k}, n \in \mathbf{N}). \qquad (6.132)$$

Так как $\beta_i \in \mathbf{Z}_{p^k}^{inv}$ $(i \in \mathbf{N}_l)$, то $f_n^{(i)} \in P_{\mathbf{Z}_{p^k}}$ $(i \in \mathbf{N}_l, n \in \mathbf{N})$.

При этом генерация алгоритма $A_{f_1^{(i)}}$ $(i \in \mathbf{N}_l)$ осуществляется за время

$$T_{f_1^{(i)}} = O(k \cdot \lceil \log p \rceil) \quad (k \to \infty \ \textit{или} \ p \to \infty),$$

а временная и емкостная сложность алгоритма $A_{f_1^{(i)}}$ $(i \in \mathbf{N}_l)$ равна, соответственно,

$$T_{f_1^{(i)}} = O((k \cdot \lceil \log p \rceil)^2) \quad (k \to \infty \ \textit{или} \ p \to \infty)$$

и

$$V_{f_1^{(i)}} = O(k \cdot \lceil \log p \rceil) \quad (k \to \infty \ \textit{или} \ p \to \infty).$$

Кроме того, при вычисленных значениях α_i^n, β_i^n $(i \in \mathbf{N}_l)$ преобразование алгоритма $A_{f_n^{(i)}}$ в алгоритм $A_{f_{n+1}^{(i)}}$ $(n \in \mathbf{N})$ осуществляется за время

$$T_{f_{n+1}^{(i)}} = O((k \cdot \lceil \log p \rceil)^2) \quad (k \to \infty \ \textit{или} \ p \to \infty),$$

а временная и емкостная сложность алгоритма $A_{f_{n+1}^{(i)}}$ $(i \in \mathbf{N}_l)$ равна, соответственно,

$$T_{f_{n+1}^{(i)}} = O((k \cdot \lceil \log p \rceil)^2) \quad (k \to \infty \ \textit{или} \ p \to \infty)$$

и

$$V_{f_{n+1}^{(i)}} = O(k \cdot \lceil \log p \rceil) \quad (k \to \infty \ \textit{или} \ p \to \infty).$$

Следовательно, каждое семейство перестановок $S^{(i)}$ $(i \in \mathbf{N}_l)$ представляет собой легко-вычислимое семейство перестановок на множестве $\mathbf{Z}_{p^k}$.

Охарактеризуем перестановки $f_n^{(i)} \in P_{\mathbf{Z}_{p^k}}^{ec}$ $(i \in \mathbf{N}_l, n \in \mathbf{N})$, определенные равенством (6.132).

Утверждение 6.10. Если

$$\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}_{p^k}^{inv}$$

и

$$a_1 = \ldots = a_l = a \in \mathbf{Z}_{p^k}^{inv},$$

то:

1) $f_n^{(i)} = f_n^{(j)}$ $(i, j \in \mathbf{N}_l, i \neq j)$ тогда и только тогда, когда $\beta_i^n = \beta_j^n$;

2) для каждого значения $n \in \mathbf{N}$ множество неподвижных точек перестановки $f_n^{(i)}$ $(i \in \mathbf{N}_l)$ совпадает с множеством решений уравнения

$$(1 \Theta \beta_i^n) \circ x = n \pmod{p^k} \circ (l-2) \circ a \circ \alpha^n. \qquad (6.133)$$

Доказательство. Пусть $\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}_{p^k}^{inv}$ и $a_1 = \ldots = a_l = a \in \mathbf{Z}_{p^k}^{inv}$. Тогда равенства (6.132) принимают вид

$$f_n^{(i)}(x) = \beta_i^n \circ x \oplus n \pmod{p^k} \circ (l-2) \circ a \circ \alpha^n \quad (i \in \mathbf{N}_l). \qquad (6.134)$$

Следовательно,

$$f_n^{(i)} = f_n^{(j)} \Leftrightarrow (\forall x \in \mathbf{Z}_{p^k})(f_n^{(i)}(x) = f_n^{(j)}(x)) \Leftrightarrow,$$

$$\Leftrightarrow (\forall x \in \mathbf{Z}_{p^k})((\beta_i^n \Theta \beta_j^n) \circ x = 0) \Leftrightarrow \beta_i^n = \beta_j^n,$$

что и требовалось показать.

Пусть $x \in \mathbf{Z}_{p^k}$ – неподвижная точка перестановки $f_n^{(i)}$ $(i \in \mathbf{N}_l)$. Положив $f_n^{(i)}(x) = x$ в равенстве (6.134), получим (6.133), что и требовалось показать.

Утверждение доказано.

Следствие 6.11. Пусть

$$\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}_{p^k}^{inv},$$

$$a_1 = \ldots = a_l = a \in \mathbf{Z}_{p^k}^{inv},$$

$$1 \Theta \beta_i^n \neq 0,$$

$$n \pmod{p^k} \neq 0$$

и r_1, r_2 – такие максимальные натуральные числа, что

$$1 \Theta \beta_i^n \equiv 0 \pmod{p^{r_1}}$$

и

$$(n \pmod{p^k}) \circ (l-2) \equiv 0 \pmod{p^{r_2}}.$$

Если $r_1 > r_2$, то перестановка $f_n^{(i)}$ не имеет неподвижных точек.

Доказательство. При сделанных предположениях уравнение (6.133) не имеет решений.

Следствие доказано.

Пусть φ – функция Эйлера. Так как

$$\varphi(p^k) = p^k - p^{k-1},$$

то показателями (по модулю p^k) элементов множества $\mathbf{Z}_{p^k}^{inv}$ могут быть только числа $p-1$, p^i и $(p-1)\cdot p^i$ $(i \in \mathbf{N}_{k-1})$.

Утверждение 6.11. Если

$$a_1 = \ldots = a_l = a \in \mathbf{Z}_{p^k}^{inv},$$

то перестановка $f_{\varphi(p^k)}^{(i)}$ $(i \in \mathbf{N}_l)$ имеет неподвижные точки тогда и только тогда, когда

$$l - 2 \equiv 0 \,(\mathrm{mod}\ p).$$

Доказательство. Положив $a_1 = \ldots = a_l = a \in \mathbf{Z}_{p^k}^{inv}$ и $n = \varphi(p^k)$ в (6.132), получим

$$f_{\varphi(p^k)}^{(i)}(x) = x \ominus p^{k-1} \circ (l-2) \circ a. \qquad (6.135)$$

Положив в (6.135)

$$f_{\varphi(p^k)}^{(i)}(x) = x,$$

получим

$$p^{k-1} \circ (l-2) \circ a = 0.$$

Последнее равенство истинно тогда и только тогда, когда

$$l - 2 \equiv 0 \,(\mathrm{mod}\ p).$$

Утверждение доказано.

Обозначим через ξ_i и ς_i $(i \in \mathbf{N}_l)$ показатели (по модулю p^k), соответственно, элементов β_i и α_i. Положим

$$[\xi_1, \ldots, \xi_l] = \delta,$$

$$[\varsigma_1, \ldots, \varsigma_l] = \lambda$$

и

$$[\delta, \lambda] = \gamma.$$

Из (6.132) вытекает, что для всех $i \in \mathbf{N}_l$

$$f_{m\cdot\delta}^{(i)}(x) = x \oplus ((m\cdot\delta)\,(\mathrm{mod}\ p^k)) \circ A_i(m\cdot\delta) \ \ (m \in \mathbf{N}), \qquad (6.136)$$

$$f_{m\cdot\lambda}^{(i)}(x) = \beta_i^{m\cdot\lambda} \circ x \oplus ((m\cdot\lambda)\,(\mathrm{mod}\ p^k)) \circ (\bigoplus_{j=1}^{l} a_j \ominus 2 \circ a_i) \ \ (m \in \mathbf{N}) \qquad (6.137)$$

и

$$f^{(i)}_{m\cdot\gamma}(x) = x \oplus ((m\cdot\gamma)\,(\mathrm{mod}\ p^k)) \circ (\overset{l}{\underset{j=1}{\oplus}} a_j \ominus 2 \circ a_i)\ \ (m \in \mathbf{N}). \qquad (6.138)$$

Из (6.136)-(6.138) вытекает, что:

1) перестановка $f^{(i)}_{m\cdot\delta}$ $(i \in \mathbf{N}_l)$ не имеет неподвижных точек тогда и только тогда, когда

$$((m\cdot\delta)\,(\mathrm{mod}\ p^k)) \circ A_i(m\cdot\delta) \neq 0;$$

2) перестановка $f^{(i)}_{m\cdot\delta}$ $(i \in \mathbf{N}_l)$ является тождественной перестановкой на множестве $\mathbf{Z}_{p^k}$ тогда и только тогда, когда

$$((m\cdot\delta)\,(\mathrm{mod}\ p^k)) \circ A_i(m\cdot\delta) = 0;$$

3) если

$$\overset{l}{\underset{j=1}{\oplus}} a_j \ominus 2 \circ a_i = 0 \quad (i \in \mathbf{N}_l),$$

то множество неподвижных точек перестановки $f^{(i)}_{m\cdot\lambda}$ совпадает с множеством решений уравнения

$$(\beta_i^{m\cdot\lambda} \ominus 1) \circ x = 0;$$

4) если

$$\overset{l}{\underset{j=1}{\oplus}} a_j \ominus 2 \circ a_i = 0,$$

то перестановка $f^{(i)}_{m\cdot\gamma}$ $(i \in \mathbf{N}_l)$ является тождественной перестановкой на множестве $\mathbf{Z}_{p^k}$.

Зафиксируем перестановку $h \in P_{\mathbf{N}_l}$. Определим семейство $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ отображений

$$\mathbf{f}_n : \mathbf{Z}^l_{p^k} \to \mathbf{Z}^l_{p^k} \quad (n \in \mathbf{N})$$

равенством

$$\mathbf{f}_n(\mathbf{x}) = (f^{(1)}_n(x_{h^n(1)}), \ldots, f^{(l)}_n(x_{h^n(l)}))^T \quad (\mathbf{x} = (x_1, \ldots, x_l)^T \in \mathbf{Z}^l_{p^k}),$$

где $f^{(i)}_n \in S^{(i)}$ $(n \in \mathbf{N}, i \in \mathbf{N}_l)$.

Ясно, что

$$\mathbf{f}_n \in P^{l\text{-}s}_{\mathbf{Z}^l_{p^k}} \cap P^{ec}_{\mathbf{Z}^l_{p^k}} \quad (n \in \mathbf{N}).$$

Исследуем класс $\boldsymbol{K}$ таких $(3\cdot l + 1)$-параметрических семейств перестановок $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$, что $h \in P_{\mathbf{N}_l}$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_l) \in (\mathbf{Z}^{inv}_{p^k})^l$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_l) \in (\mathbf{Z}^{inv}_{p^k})^l$ и $\mathbf{a} = (a_1, \ldots, a_l) \in (\mathbf{Z}^{inv}_{p^k})^l$.

Отметим, что так как l $(2 < l \leq k)$ – фиксированное число, то $\boldsymbol{K}$ – легковычислимый класс семейств перестановок множества $\mathbf{Z}^l_{p^k}$.

Схемная реализация легко-вычислимого класса семейств перестановок K представлена на рис. 6.9.

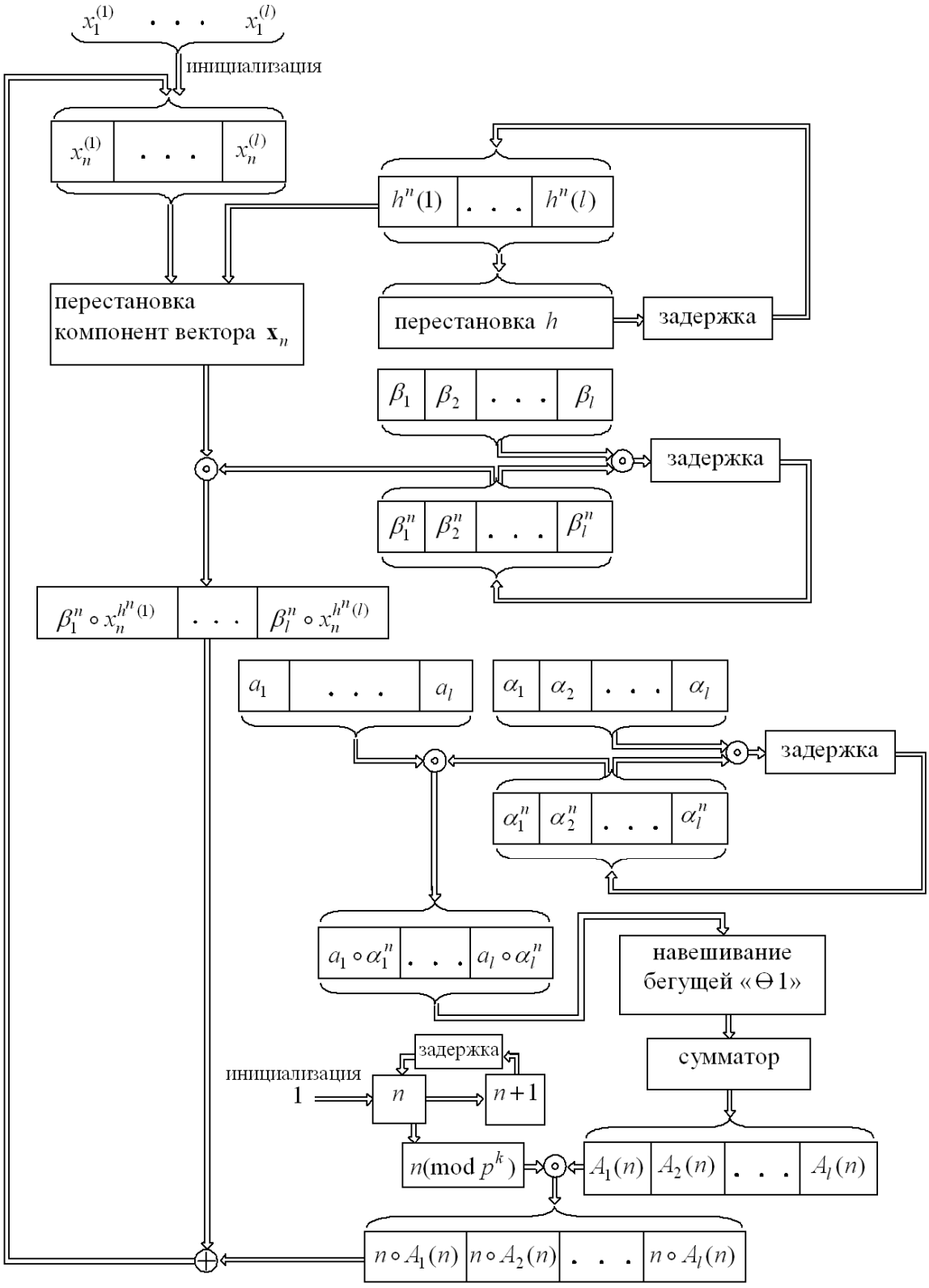


Рис. 6.9. Схемная реализация алгоритма A_K.

Представим семейство перестановок $\boldsymbol{S}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)\in\boldsymbol{K}$ в явном виде

$$\begin{cases} x_{n+1}^{(1)} = \beta_1^n \circ x_n^{h^n(1)} \oplus (n \,(\mathrm{mod}\ p^k)) \circ A_1(n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n+1}^{(l)} = \beta_l^n \circ x_n^{h^n(l)} \oplus (n \,(\mathrm{mod}\ p^k)) \circ A_l(n) \end{cases}, \qquad (6.139)$$

где

$$A_i(n) = \bigoplus_{j=1}^{l} a_j \circ \alpha_j^n \ominus 2 \circ a_i \circ \alpha_i^n \ \ (i\in\mathbf{N}_l, n\in\mathbf{N}),$$

причем $\beta_i, a_i, \alpha_i \in \mathbf{Z}_{p^k}^{inv}$ $(i\in\mathbf{N}_l)$ и $h\in P_{\mathbf{N}_l}$.

Для любых фиксированных чисел $n_0, n_1 \in \mathbf{N}$ $(n_1 \ge n_0)$ положим

$$\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h) = \{\mathbf{f}_n\}_{n\in\mathbf{N}_{n_1}\setminus\mathbf{N}_{n_0-1}}.$$

Образом элемента $\mathbf{x}_0 = (x_0^{(1)},\ldots,x_0^{(l)})^T \in \mathbf{Z}_{p^k}^l$ при действии семейства перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ назовем последовательность

$$\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)(\mathbf{x}) = \mathbf{x}_1 \ldots \mathbf{x}_{n_1-n_0+1},$$

где

$$\mathbf{x}_i = (x_i^{(1)},\ldots,x_i^{(l)})^T = \mathbf{f}_{n_0+i-1}(\mathbf{x}_{i-1}) \ \ (i\in\mathbf{N}_{n_1-n_0+1}).$$

Будем говорить, что $\mathbf{x}_0 \in \mathbf{Z}_{p^k}^l$ – неподвижная точка для семейства перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ тогда и только тогда, когда

$$\mathbf{x}_i = \mathbf{x}_0$$

для всех $i\in\mathbf{N}_{n_1-n_0+1}$.

Теорема 6.11. Пусть p – нечетное простое число. Тогда для всех $\boldsymbol{S}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)\in\boldsymbol{K}$ поиск семейства $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ $(n_0\le n_1)$, обладающего заданной неподвижной точкой $\mathbf{x}_0\in\mathbf{Z}_{p^k}^l$, при условии, что $n_0, n_1 \in \mathbf{N}$ не являются показателями (по модулю p^k) ни одного из чисел $\alpha_i, \beta_i \in \mathbf{N}_{p^k}^{inv}$ $(i\in\mathbf{N}_l)$, сводится к решению системы многостепенных диофантовых уравнений с $2\cdot l$ неизвестными с последующей проверкой для каждого ее решения разрешимости $2\cdot l$ задач дискретного логарифмирования.

Доказательство. Пусть $\mathbf{x}_0\in\mathbf{Z}_{p^k}^l$ – неподвижная точка для семейства перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$. Тогда

$$\mathbf{f}_{n_0+i-1}(\mathbf{x}_{i-1}) = \mathbf{x}_0$$

для всех $i\in\mathbf{N}_{n_1-n_0+1}$. Из (6.139) получим, что для всех $i\in\mathbf{N}_{n_1-n_0+1}$

$$((n_0+i-1)\,(\mathrm{mod}\ p^k)) \circ A_j(n_0+i-1) \oplus$$

$$\oplus\, \beta_j^{n_0+i-1} \circ x_0^{h^{n_0+i-1}(j)} = x_0^{(j)} \ \ (j\in\mathbf{N}_l). \qquad (6.140)$$

Положив в (6.140)

$$u_j = \alpha_j^{n_0} \quad (j \in \mathbf{N}_l) \tag{6.141}$$

и

$$v_j = \beta_j^{n_0} \quad (j \in \mathbf{N}_l), \tag{6.142}$$

получим систему многостепенных диофантовых уравнений с $2 \cdot l$ неизвестными u_j, v_j $(j \in \mathbf{N}_l)$.

Каждое решение этой системы диофантовых уравнений приводит к $2 \cdot l$ задачам дискретного логарифмирования, определяемым формулами (6.141) и (6.142).

Решение этой системы задач дискретного логарифмирования и определяет искомое семейство перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$.

Теорема доказана.

Отметим, что включение перестановки $h \in P_{\mathbf{N}_l}$ в число параметров, определяющих семейство перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$, целесообразно по следующим причинам.

Во-первых, применение конструкции, предложенной в [166], дает возможность систематически строить перестановки $h \in P_{\mathbf{N}_l}$ порядка $e^{O(\sqrt{l})}$ $(l \to \infty)$, что приводит к существенному росту порядка перестановок $\mathbf{f}_n$ $(n \in \mathbf{N})$, формирующих семейство перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$.

Во-вторых, существенно усложняется система многостепенных диофантовых уравнений, конструируемых при доказательстве теоремы 6.11.

В-третьих, разрушается регулярность для представления множества неподвижных точек семейства перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ $(n_0 \le n_1)$.

Следующая теорема показывает, что для кольца Z_{2^k} можно выделить достаточно широкий класс семейств перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$, не имеющих неподвижных точек.

Теорема 6.12. Пусть $p = 2$, $\beta_i = 1$ $(i \in \mathbf{N}_l)$, l – нечетное число и $k \ge 3$. Тогда для любого семейства перестановок $\boldsymbol{S}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},e) \in \boldsymbol{K}$ (где $e \in P_{\mathbf{N}_l}$ – тождественная перестановка) ни одно семейство перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},e)$ $(n_0 \le n_1 < 2^k)$ не имеет неподвижных точек.

Доказательство. Пусть $p = 2$, $\beta_i = 1$ $(i \in \mathbf{N}_l)$, l – нечетное число, $k \ge 3$ и $e \in P_{\mathbf{N}_l}$ – тождественная перестановка.

Предположим противное, т.е. что существует неподвижная точка $\mathbf{x}_0 \in \mathbf{Z}_{2^k}^l$ для семейства перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},e)$ $(n_0 \le n_1 < 2^k)$.

Из (6.139) получим, что для всех $i \in \mathbf{N}_{n_1-n_0+1}$

$$(n_0 + i - 1)(\mathrm{mod}\, 2^k) \circ A_j(n_0 + i - 1) = 0 \quad (j \in \mathbf{N}_l).$$

Так как $a_i, \alpha_i \in \mathbf{Z}_{2^k}^{inv}$ $(i \in \mathbf{N}_l)$, то a_i, α_i $(i \in \mathbf{N}_l)$ – нечетные числа.

А так как l – нечетное число, то

$$A_i(n) \neq 0 \ \ (i \in \mathbf{N}_l)$$

для всех $n \in \mathbf{N}$.

Следовательно,

$$n \circ A_i(n) \neq 0 \ \ (i \in \mathbf{N}_l)$$

для всех $n \in \mathbf{N}_{n_1}$.

Полученное противоречие означает, что предположение ложное.

Отсюда вытекает, что ни одно семейство перестановок $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, e)$ $(n_0 \leq n_1 < 2^k)$ не имеет неподвижных точек.

Теорема доказана.

Рассмотрим решение задач идентификации семейства перестановок $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ при условии, что экспериментатору доступны некоторые точки съема информации и/или управления алгоритмом, реализующим перестановки $\mathbf{f}_n$ $(n \in \mathbf{N})$.

Теорема 6.13. Пусть известны значения векторов параметров $\mathbf{a}$ и $\boldsymbol{\alpha}$. Если в момент $n_0 \in \mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим перестановку $\mathbf{f}_{n_0}$, и наблюдать соответствующий выход, то идентификация вектора параметров $\boldsymbol{\beta}$ сводится к независимому решению l задач дискретного логарифмирования.

Доказательство. Предположим, что известны значения векторов параметров $\mathbf{a}, \boldsymbol{\alpha}$ и в момент $n_0 \in \mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим перестановку $\mathbf{f}_{n_0}$, и наблюдать соответствующий выход.

Выберем в качестве входа алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$, вектор

$$\mathbf{x}_{n_0} = (\underbrace{1,\ldots,1}_{l \ раз})^T.$$

Из (6.139) получим следующую систему уравнений относительно неизвестных $\beta_1, \ldots, \beta_l \in \mathbf{Z}_{p^k}^{inv}$

$$\begin{cases} \beta_1^{n_0} = x_{n_0+1}^{(1)} \Theta n_0 \,(\mathrm{mod}\, p^k) \circ A_1(n_0) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_l^{n_0} = x_{n_0+1}^{(l)} \Theta n_0 \,(\mathrm{mod}\, p^k) \circ A_l(n_0) \end{cases}. \qquad (6.143).$$

Решение системы уравнений (6.143) сводится к независимому решению l задач дискретного логарифмирования.

Теорема доказана.

Теорема 6.14. Пусть p – нечетное простое число и известны значения векторов параметров $\mathbf{a}$ и $\boldsymbol{\beta}$. Если в момент $n_0 \in \mathbf{N}$, где $n_0 \,(\mathrm{mod}\, p^k) \in \mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров $\boldsymbol{\alpha}$ сводится к независимому решению l задач дискретного логарифмирования.

Доказательство. Предположим, что p – нечетное простое число, известны значения векторов параметров $\mathbf{a}$ и $\boldsymbol{\beta}$, а также в момент $n_0 \in \mathbf{N}$ $(n_0 \,(\mathrm{mod}\, p^k) \in \mathbf{Z}_{p^k}^{inv})$ экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$.

Из системы (6.139) получим следующую систему уравнений относительно неизвестных $\alpha_1, \ldots, \alpha_l \in \mathbf{Z}_{p^k}^{inv}$

$$\begin{cases} \bigoplus\limits_{j=1}^{l} a_j \circ \alpha_j^{n_0} \Theta 2 \circ a_1 \circ \alpha_1^{n_0} = \gamma_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \bigoplus\limits_{j=1}^{l} a_j \circ \alpha_j^{n_0} \Theta 2 \circ a_l \circ \alpha_l^{n_0} = \gamma_l \end{cases} \tag{6.144}$$

где

$$\gamma_i = (n_0 (\mathrm{mod}\, p^k))^{-1} \circ (x_{n_0+1}^{(i)} \Theta \beta_i^{n_0} \circ x_{n_0}^{h^{n_0}(i)}) \;\; (i \in \mathbf{N}_l).$$

Так как

$$\Delta = \begin{vmatrix} \Theta a_1 & a_2 & \ldots & a_l \\ a_1 & \Theta a_2 & \ldots & a_l \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & \Theta a_l \end{vmatrix} = a_1 \circ \ldots \circ a_l \circ 2^{l-1} \circ (p^k - l + 2) \in \mathbf{Z}_{p^k}^{inv},$$

то система уравнений (6.144) эквивалентна системе уравнений

$$\begin{cases} \alpha_1^{n_0} = c_1 \\ \quad \ldots \quad . \\ \alpha_l^{n_0} = c_l \end{cases} \tag{6.145}$$

Решение системы (6.145) сводится к независимому решению l задач дискретного логарифмирования.

Теорема доказана.

Следствие 6.12. Пусть p – нечетное простое число и известны значения векторов параметров $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$. Если в момент $n_0 \in \mathbf{N}$, где $n_0 \,(\mathrm{mod}\, p^k) \in \mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алго-

ритма, реализующего перестановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров $\mathbf{a}$ сводится к решению линейной системы уравнений.

Доказательство. Идентификация вектора параметров $\mathbf{a}$ сводится к решению линейной системы уравнений (6.144) относительно неизвестных $a_1,\ldots,a_l \in \mathbf{Z}_{p^k}^{inv}$.

Следствие доказано.

Следующая теорема показывает, что сложность задач идентификации существенно возрастает даже для семейства перестановок (6.131) в случае кольца Z_{2^k}, если это семейство перестановок встроено в поточный шифр, построенный на основе псевдофрактала, а экспериментатор имеет возможность анализировать исходный текст и шифртекст, и требуется идентифицировать два из трех векторов $\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a}$ параметров.

Теорема 6.15. Пусть в шифр, построенный на основе псевдофрактала, встроено семейство перестановок (6.131) над кольцом Z_{2^k} $(k \geq 3)$, где l $(3 \leq l \leq k)$ – нечетное число. Тогда идентификация вектора параметров $(\mathbf{a},\boldsymbol{\alpha})$ семейства перестановок (6.131) сводится к решению экспоненциального числа задач дискретного логарифмирования.

Доказательство. Предположим, что известны соответствующие пары $(\mathbf{x}_0,\mathbf{x}_n)$, $(n \in \mathbf{N}_{2^k-1})$ исходного текста и шифртекста.

Из (6.131) вытекает, что

$$\begin{cases} n \circ (2 \circ \alpha_1^n \circ a_1 \,\Theta \mathop{\oplus}\limits_{j=1}^{l} \alpha_j^n \circ a_j) = c_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ n \circ (2 \circ \alpha_l^n \circ a_l \,\Theta \mathop{\oplus}\limits_{j=1}^{l} \alpha_j^n \circ a_j) = c_l \end{cases}, \qquad (6.146)$$

где

$$c_i = x_n^{(i)} \Theta\, x_0^{(i)} \;\; (i \in \mathbf{N}_l).$$

Перейдем от системы уравнений (6.146) к эквивалентной системе уравнений. Для этого 1-е уравнение оставим без изменений, а i-е уравнение $(i = 2,\ldots,l)$, умноженное на элемент $\Theta(l-2) \in \mathbf{Z}_{2^k}^{inv}$, сложим с суммой всех уравнений системы (6.146). Получим систему уравнений

$$\begin{cases} n \circ (\alpha_1^n \circ a_1 \,\Theta\, \alpha_2^n \circ a_2 \,\Theta \ldots \Theta\, \alpha_l^n \circ a_l) = c_1 \\ \Theta 2 \circ n \circ (l-2) \circ \alpha_2^n \circ a_2 = \mathop{\oplus}\limits_{j=1}^{l} c_j \,\Theta\, (l-2) \circ c_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \Theta 2 \circ n \circ (l-2) \circ \alpha_l^n \circ a_l = \mathop{\oplus}\limits_{j=1}^{l} c_j \,\Theta\, (l-2) \circ c_l \end{cases}. \qquad (6.147)$$

Решим 2-е уравнение системы (6.147) относительно $n \circ \alpha_2^n \circ a_2$.

Так как $2 \in \mathbf{Z}_{2^k} \setminus \mathbf{Z}_{2^k}^{inv}$ и $(2, 2^k) = 2$, то для разрешимости этого уравнения достаточно, чтобы было выполнено условие

$$2 \mid (\overset{l}{\underset{j=1}{\oplus}} c_j \ominus (l-2) \circ c_2).$$

Положим

$$\overset{l}{\underset{j=1}{\oplus}} c_j \ominus (l-2) \circ c_2 = 2 \circ c_2'.$$

Сравнение

$$\ominus (l-2) \circ n \circ \alpha_2^n \circ a_2 \equiv c_2' \pmod{2^{k-1}}$$

имеет одно решение по модулю 2^{k-1} и два решения

$$\left[\begin{array}{l} n \circ \alpha_2^n \circ a_2 = v_2 \\ n \circ \alpha_2^n \circ a_2 = v_2 \oplus 2^{k-1} \end{array}\right.$$

по модулю 2^k, где

$$v_2 = \ominus c_2' \circ (l-2)^{-1}.$$

Аналогичным образом, i-е уравнение $(i = 3, \ldots, l)$ системы уравнений (6.147) имеет два решения

$$\left[\begin{array}{l} n \circ \alpha_i^n \circ a_i = v_i \\ n \circ \alpha_i^n \circ a_i = v_i \oplus 2^{k-1} \end{array}\right.$$

по модулю 2^k, если выполнено условие

$$2 \mid (\overset{l}{\underset{j=1}{\oplus}} c_j \ominus (l-2) \circ c_i).$$

Из 1-го уравнения системы уравнений (6.147) вытекает, что

$$n \circ \alpha_1^n \circ a_1 = c_1 \oplus n \circ \alpha_2^n \circ a_2 \oplus \ldots \oplus n \circ \alpha_l^n \circ a_l,$$

т.е.

$$\left[\begin{array}{l} n \circ \alpha_1^n \circ a_1 = c_1 \oplus \overset{l}{\underset{i=2}{\oplus}} v_i \\ n \circ \alpha_1^n \circ a_1 = c_1 \oplus \overset{l}{\underset{i=2}{\oplus}} v_i \oplus 2^{k-1} \end{array}\right. .$$

Таким образом, система уравнений (6.146) имеет 2^{l-1} решений, т.е. построено 2^{l-1} систем уравнений вида

$$\left\{\begin{array}{l} n \circ \alpha_1^n \circ a_1 = z_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ n \circ \alpha_l^n \circ a_l = z_l \end{array}\right. , \qquad (6.148)$$

где $z_1 \in \{c_1 \oplus \overset{l}{\underset{i=2}{\oplus}} v_i, c_1 \oplus \overset{l}{\underset{i=2}{\oplus}} v_i \oplus 2^{k-1}\}$ и $z_i \in \{v_i, v_i \oplus 2^{k-1}\}$ $(i = 2, \ldots, l)$.

Для решения системы уравнений (6.148) рассмотрим вход-выходную пару $(\mathbf{x}'_n, \mathbf{x}'_{n'})$ $(n' \in \mathbf{N}_{p^k-1})$.

Система уравнений (6.146) принимает следующий вид

$$\begin{cases} n' \circ (2 \circ \alpha_1^{n+n'} \circ a_1 \ominus \bigoplus_{j=1}^{l} \alpha_j^{n+n'} \circ a_j) = c'_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ n' \circ (2 \circ \alpha_l^{n+n'} \circ a_l \ominus \bigoplus_{j=1}^{l} \alpha_j^{n+n'} \circ a_j) = c'_l \end{cases} \qquad (6.149)$$

причем значения n и n' известны, исходя из алгоритма шифрования.

Решим систему уравнений (6.149) относительно $n' \circ \alpha_i^{n+n'} \circ a_i$ $(i \in \mathbf{N}_l)$ по аналогии с тем, как было описано выше.

В результате получим 2^{l-1} систем уравнений вида

$$\begin{cases} n' \circ \alpha_1^{n+n'} \circ a_1 = z'_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ n' \circ \alpha_l^{n+n'} \circ a_l = z'_l \end{cases},$$

т.е. полученная система уравнений имеет ту же структуру, что и система уравнений (6.148).

Решим систему уравнений (6.148) относительно $\alpha_i^n \circ a_i$ $(i \in \mathbf{N}_l)$.

Каждое уравнение системы уравнений (6.148) порождает

$$(n, 2^k) = 2^w$$

уравнений вида

$$\alpha_i^n \cdot a_i = u_i,$$

где

$$u_i \in \{\hat{z}_i \circ n_1^{-1}, \hat{z}_i \circ n_1^{-1} \oplus 2^{k-w}, \ldots, \hat{z}_i \circ n_1^{-1} \oplus 2^{k-1}\},$$

$$n = 2^w \circ n_1,$$

$$n_1 \in \mathbf{Z}_{2^k}^{inv}$$

и

$$z_i = 2^w \circ \hat{z}_i \quad (i \in \mathbf{N}_l).$$

Следовательно, количество решений систем уравнений (6.148) и (6.146) равно, соответственно, $l \cdot 2^w$ и

$$2^{l-1} \cdot l \cdot 2^w = l \cdot 2^{w+l-1}.$$

Аналогичным образом получаем, что система уравнений (6.149) имеет $l \cdot 2^{w'+l-1}$ решений, где

$$(n', 2^k) = 2^{w'}.$$

Поиск значений α_i и a_i $(i \in \mathbf{N}_l)$ сводится к решению $l^3 \cdot 2^{w+w'+2\cdot(l-1)}$ систем уравнений вида

$$\begin{cases} u^{\beta} \circ u^{\gamma} \circ v = h_1 \\ u^{\beta} \circ v = h_2 \end{cases}. \qquad (6.150)$$

Возможны следующие четыре случая.

Случай 1. Пусть u и v – обратимые элементы кольца Z_{2^k}. Тогда h_1 и h_2 – обратимые элементы.

Из 1-го уравнения системы уравнений (6.150) находим

$$u^{\beta} \circ v = h_1 \circ u^{-\gamma}.$$

Отсюда следует, что

$$h_1 \circ u^{-\gamma} = h_2,$$

т.е.

$$u^{\gamma} = h_1 \circ h_2^{-1}. \qquad (6.151)$$

Из уравнения (6.151) находим u, а из 2-го уравнения системы уравнений (6.150) находим v, т.е.

$$v = h_2 \circ u^{-\beta}. \qquad (6.152)$$

Случай 2. Пусть u – обратимый, а v – необратимый элемент кольца Z_{2^k}. Тогда h_1 и h_2 – необратимые элементы.

Из 1-го уравнения системы уравнений (6.150) находим

$$u^{\beta} \circ v = h_1 \circ u^{-\gamma}.$$

Отсюда следует, что

$$h_1 \circ u^{-\gamma} = h_2,$$

т.е.

$$h_2 \circ u^{\gamma} = h_1. \qquad (6.153)$$

Пусть

$$(h_2, 2^k) = q \geq 2.$$

Уравнение (6.153) разрешимо, если $q \mid h_1$. При этом число решений уравнения (6.153) равно q.

Значения v находим из уравнения (6.152).

Следовательно, система уравнений (6.151) имеет q решений.

Случай 3. Пусть u – необратимый, а v – обратимый элемент кольца Z_{2^k}. Тогда h_1 и h_2 – необратимые элементы. Пусть

$$u = 2^{\delta} \circ u_1,$$

где u_1 – обратимый элемент.

Тогда

$$\begin{cases} 2^{k_1} \circ u_1^{\beta} \circ u_1^{\gamma} \circ v = h_1 \\ 2^{k_2} \circ u_1^{\beta} \circ v = h_2 \end{cases}, \qquad (6.154)$$

где

$$k_1 = \delta \cdot (\beta + \gamma)$$

и

$$k_2 = \delta \cdot \beta .$$

Система уравнений (6.154) разрешима, если $2^{k_1} \mid h_1$ и $2^{k_2} \mid h_2$. При этом порождается $2^{k_1+k_2}$ систем сравнений вида

$$\begin{cases} u_1^{\beta} \circ u_1^{\gamma} \circ v \equiv h_1' \pmod{2^{k-k_1}} \\ u_1^{\beta} \circ v \equiv h_2' \pmod{2^{k-k_2}} \end{cases}, \qquad (6.155)$$

где

$$h_1 = h_1' \circ 2^{k_1}$$

и

$$h_2 = h_2' \circ 2^{k_2} .$$

Каждая из систем уравнений (6.155) имеет одно решение, а система уравнений (6.154) – $2^{k_1+k_2}$ решений.

Случай 4. Пусть u и v – необратимые элементы кольца Z_{2^k}. Тогда h_1 и h_2 – необратимые элементы.

Пусть

$$u = 2^{\delta} \circ u_1 ,$$

где u_1 – обратимый элемент и

$$v = 2^{\eta} \circ v_1 ,$$

где v_1 – обратимый элемент.

Тогда

$$\begin{cases} 2^{k_1} \circ u_1^{\beta} \circ u_1^{\gamma} \circ v_1 = h_1 \\ 2^{k_2} \circ u_1^{\beta} \circ v_1 = h_2 \end{cases}, \qquad (6.156)$$

где

$$k_1 = \delta \cdot (\beta + \gamma) + \eta$$

и

$$k_2 = \delta \cdot \beta + \eta .$$

Система уравнений (6.156) разрешима, если $2^{k_1} \mid h_1$ и $2^{k_2} \mid h_2$. При этом порождается $2^{k_1+k_2}$ систем сравнений вида

$$\begin{cases} u_1^{\beta} \circ u_1^{\gamma} \circ v_1 \equiv h_1' \pmod{2^{k-k_1}} \\ u_1^{\beta} \circ v_1 \equiv h_2' \pmod{2^{k-k_2}} \end{cases}, \qquad (6.157)$$

где

$$h_1 = h_1' \circ 2^{k_1}$$

и

$$h_2 = h_2' \circ 2^{k_2}.$$

Каждая из систем уравнений (6.157) имеет одно решение, а система уравнений (6.156) – $2^{k_1+k_2}$ решений.

Итак, для идентификации вектора $(\mathbf{a}, \boldsymbol{\alpha})$ необходимо решить экспоненциальное число задач дискретного логарифмирования, что и требовалось доказать.

Теорема доказана.

Итак, показано, что задачи идентификации параметров для класса семейств перестановок $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ сводятся к решению систем многостепенных диофантовых уравнений и систем задач дискретного логарифмирования. Следовательно, эти задачи являются трудными, что обосновывает вычислительную стойкость поточного шифра, построенного на основе управления этим классом перестановок посредством псевдофрактала.

6.6. Симметричные нелинейные автоматы.

В настоящее время построен ряд хаотических динамических систем, которые не укладываются в рамки автоматных моделей, исследованных в пп.6.1-6.4. К ним, в частности, относятся Guckenheimer and Holmes cycle и free-running система (см. п.1.7), исследованные в [239]. Эти две динамические системы имеют следующие особенности.

Во-первых, обе системы имеют нетривиальные группы симметрий, а, как известно, теория симметрий [36] представляет собой мощный аппарат анализа динамических систем.

Во-вторых, изменение динамических переменных Guckenheimer and Holmes cycle представлено многочленами третьей степени.

В-третьих, изменение динамических переменных free-running системы осуществляется с помощью показательной функции, а, как известно, дискретное логарифмирование (т.е. операция обратная показательной функции) – базовая конструкция современной криптографии.

Исследуем с позиции криптологии Guckenheimer and Holmes cycle автомат и free-running автомат, которые являются аналогами над кольцом Z_{p^k} указанных выше систем.

Динамическая система Guckenheimer and Holmes cycle имеет следующий вид

$$\begin{cases} \dot{x} = x \cdot (l + a \cdot x^2 + b \cdot y^2 + c \cdot z^2) \\ \dot{y} = y \cdot (l + a \cdot y^2 + b \cdot z^2 + c \cdot x^2) \\ \dot{z} = z \cdot (l + a \cdot z^2 + b \cdot x^2 + c \cdot y^2) \end{cases}. \qquad (6.158)$$

Выполним дискретизацию системы (6.158) и аддитивно внесем информационную переменную u в каждое уравнение системы. Получим систему

$$\begin{cases} x_{n+1} = x_n \cdot (d + a \cdot x_n^2 + b \cdot y_n^2 + c \cdot z_n^2) + \alpha_1 \cdot u_{n+1} \\ y_{n+1} = y_n \cdot (d + a \cdot y_n^2 + b \cdot z_n^2 + c \cdot x_n^2) + \alpha_2 \cdot u_{n+1} \\ z_{n+1} = z_n \cdot (d + a \cdot z_n^2 + b \cdot x_n^2 + c \cdot y_n^2) + \alpha_3 \cdot u_{n+1} \end{cases} \quad (n \in \mathbf{Z}_+). \qquad (6.159)$$

Free-running система имеет вид

$$\begin{cases} x_{n+1} = f(x_n) \cdot e^{-\gamma \cdot z_n} \\ y_{n+1} = f(y_n) \cdot e^{-\gamma \cdot x_n} \\ z_{n+1} = f(z_n) \cdot e^{-\gamma \cdot y_n} \end{cases} \quad (n \in \mathbf{Z}_+) \qquad (6.160)$$

где

$$f(x) = a \cdot x \cdot (1 - x)$$

представляет собой логистическое отображение с параметром $a \in (0;4)$.

Добавим аддитивно информационную переменную u в каждое уравнение системы (6.160). Получим систему

$$\begin{cases} x_{n+1} = f(x_n) \cdot e^{-\gamma \cdot z_n} + \alpha_1 \cdot u_{n+1} \\ y_{n+1} = f(y_n) \cdot e^{-\gamma \cdot x_n} + \alpha_2 \cdot u_{n+1} \\ z_{n+1} = f(z_n) \cdot e^{-\gamma \cdot y_n} + \alpha_3 \cdot u_{n+1} \end{cases} \quad (n \in \mathbf{Z}_+). \qquad (6.161)$$

Перейдем в (6.159) и (6.161) к действиям в кольце Z_{p^k} и к стандартным обозначениям теории автоматов. При этом примем во внимание, что нас интересуют именно обратимые автоматы.

В результате этих действий система (6.159) преобразуется в следующий Guckenheimer and Holmes cycle автомат Мура над кольцом Z_{p^k}

$$M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) =$$

$$= \begin{cases} q_{n+1}^{(1)} = q_n^{(1)} \circ (d \oplus a \circ (q_n^{(1)})^2 \oplus b \circ (q_n^{(2)})^2 \oplus c \circ (q_n^{(3)})^2) \oplus \\ \qquad \oplus \alpha_1 \circ x_{n+1} \\ q_{n+1}^{(2)} = q_n^{(2)} \circ (d \oplus c \circ (q_n^{(1)})^2 \oplus a \circ (q_n^{(2)})^2 \oplus b \circ (q_n^{(3)})^2) \oplus \\ \qquad \oplus \alpha_2 \circ x_{n+1} \\ q_{n+1}^{(3)} = q_n^{(3)} \circ (d \oplus b \circ (q_n^{(1)})^2 \oplus c \circ (q_n^{(2)})^2 \oplus a \circ (q_n^{(3)})^2) \oplus \\ \qquad \oplus \alpha_3 \circ x_{n+1} \\ y_{n+1}^{(i)} = q_{n+1}^{(i)} \quad (i = 1,2,3) \end{cases} \quad (n \in \mathbf{Z}_+), \quad (6.162)$$

где $\alpha_1,\alpha_2,\alpha_3$ – фиксированные обратимые элементы кольца Z_{p^k}, $a,b,c,d\in\mathbf{Z}_{p^k}\setminus\{0\}$ – фиксированные элементы кольца Z_{p^k}, x – входная переменная, $q^{(i)}$ $(i=1,2,3)$ – переменные состояния автомата, а $y^{(i)}$ $(i=1,2,3)$ – выходные переменные.

Аналогичным образом система (6.161) преобразуется в следующий free-running автомат Мура над кольцом Z_{p^k}

$$M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)=\begin{cases} q_{n+1}^{(1)}=f(q_n^{(1)})\circ\zeta^{q_n^{(3)}}\oplus\alpha_1\circ x_{n+1}\\ q_{n+1}^{(2)}=f(q_n^{(2)})\circ\zeta^{q_n^{(1)}}\oplus\alpha_2\circ x_{n+1}\\ q_{n+1}^{(3)}=f(q_n^{(3)})\circ\zeta^{q_n^{(2)}}\oplus\alpha_3\circ x_{n+1}\\ y_{n+1}^{(i)}=q_{n+1}^{(i)}\ (i=1,2,3)\end{cases}\quad (n\in\mathbf{Z}_+),\quad (6.163)$$

где

$$f(x)=a\circ x\circ(1\ominus x),$$

причем $\alpha_1,\alpha_2,\alpha_3$, ζ – фиксированные обратимые элементы кольца Z_{p^k}, $a\in\mathbf{Z}_{p^k}\setminus\{0\}$ – фиксированный элемент кольца Z_{p^k}, x – входная переменная, $q^{(i)}$ $(i=1,2,3)$ – переменные состояния автомата, а $y^{(i)}$ $(i=1,2,3)$ – выходные переменные.

Обозначим через $\mathsf{A}_{GH}(p,k)$ и $\mathsf{A}_{FR}(p,k)$ множество всех автоматов, соответственно, (6.162) и (6.163) над кольцом Z_{p^k}.

В [154] автоматы (6.162) и (6.163) исследованы при условии, что $x_{n+1}\equiv 0$ $(n\in\mathbf{Z}_+)$. Исследуем автоматы (6.162) и (6.163) в предположении, что $x_{n+1}\in\mathbf{Z}_{p^k}$ $(n\in\mathbf{Z}_+)$.

Применение автоматов (6.162) и (6.163) в качестве поточного шифра состоит в следующем: параметры автомата представляют собой ключ средней длительности, а начальное состояние $\mathbf{q}_0=(q_0^{(1)},q_0^{(2)},q_0^{(3)})$ – сеансовый ключ.

Для того чтобы процесс

исходная информация $\rightarrow$ *шифрование* $\rightarrow$ *расшифровка*

всегда был корректным необходимо и достаточно, чтобы эти автоматы являлись обратимыми автоматами (т.е. БПИ-автоматами).

Утверждение 6.12. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ любой автомат $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in\mathsf{A}_{GH}(p,k)$, а также любой автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in\mathsf{A}_{FR}(p,k)$ являются обратимыми автоматами.

Доказательство. Так как $\alpha_1,\alpha_2,\alpha_3$ − обратимые элементы кольца Z_{p^k}, то из первых трех уравнений систем (6.162) и (6.163) находим, что, соответственно,

$$\begin{cases} x_{n+1}=\alpha_1^{-1}\circ(q_{n+1}^{(1)}\Theta \\ \qquad \Theta q_n^{(1)}\circ(d\oplus a\circ(q_n^{(1)})^2\oplus b\circ(q_n^{(2)})^2\oplus c\circ(q_n^{(3)})^2)) \\ x_{n+1}=\alpha_2^{-1}\circ(q_{n+1}^{(2)}\Theta \\ \qquad \Theta q_n^{(2)}\circ(d\oplus c\circ(q_n^{(1)})^2\oplus a\circ(q_n^{(2)})^2\oplus b\circ(q_n^{(3)})^2)) \\ x_{n+1}=\alpha_3^{-1}\circ(q_{n+1}^{(3)}\Theta \\ \qquad \Theta q_n^{(3)}\circ(d\oplus b\circ(q_n^{(1)})^2\oplus c\circ(q_n^{(2)})^2\oplus a\circ(q_n^{(3)})^2)) \end{cases} \quad (n\in\mathbf{Z}_+) \quad (6.164)$$

и

$$\begin{cases} x_{n+1}=\alpha_1^{-1}\circ(q_{n+1}^{(1)}\Theta f(q_n^{(1)})\circ\zeta^{q_n^{(3)}}) \\ x_{n+1}=\alpha_2^{-1}\circ(q_{n+1}^{(2)}\Theta f(q_n^{(2)})\circ\zeta^{q_n^{(1)}}) \\ x_{n+1}=\alpha_3^{-1}\circ(q_{n+1}^{(3)}\Theta f(q_n^{(3)})\circ\zeta^{q_n^{(2)}}) \end{cases} \quad (n\in\mathbf{Z}_+). \quad (6.165)$$

Из последних трех уравнений систем (6.162) и (6.163) находим, что

$$q_n^{(i)}=y_n^{(i)} \quad (i=1,2,3), \quad (6.166)$$

для всех $n\in\mathbf{Z}_+$, причем

$$\mathbf{y}_0=\mathbf{q}_0.$$

Подставив (6.166) в (6.164) и (6.165), а, также, заменив переменную x переменной y, а переменную y переменной x, получим

$$M_{GH}^{-1}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)=$$

$$=\begin{cases} y_{n+1}=\alpha_1^{-1}\circ(x_{n+1}^{(1)}\Theta \\ \qquad \Theta x_n^{(1)}\circ(d\oplus a\circ(x_n^{(1)})^2\oplus b\circ(x_n^{(2)})^2\oplus c\circ(x_n^{(3)})^2)) \\ y_{n+1}=\alpha_2^{-1}\circ(x_{n+1}^{(2)}\Theta \\ \qquad \Theta x_n^{(2)}\circ(d\oplus c\circ(x_n^{(1)})^2\oplus a\circ(x_n^{(2)})^2\oplus b\circ(x_n^{(3)})^2)) \\ y_{n+1}=\alpha_3^{-1}\circ(x_{n+1}^{(3)}\Theta \\ \qquad \Theta x_n^{(3)}\circ(d\oplus b\circ(x_n^{(1)})^2\oplus c\circ(x_n^{(2)})^2\oplus a\circ(x_n^{(3)})^2)) \end{cases} \quad (n\in\mathbf{Z}_+) \quad (6.167)$$

и

$$M_{FR}^{-1}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)=\begin{cases} y_{n+1}=\alpha_1^{-1}\circ(x_{n+1}^{(1)}\Theta f(x_n^{(1)})\circ\zeta^{x_n^{(3)}}) \\ y_{n+1}=\alpha_2^{-1}\circ(x_{n+1}^{(2)}\Theta f(x_n^{(2)})\circ\zeta^{x_n^{(1)}}) \\ y_{n+1}=\alpha_3^{-1}\circ(x_{n+1}^{(3)}\Theta f(x_n^{(3)})\circ\zeta^{x_n^{(2)}}) \end{cases} \quad (n\in\mathbf{Z}_+). \quad (6.168)$$

Утверждение доказано.

Отметим, что в процессе «шифрование-расшифровка» как автоматы $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ и $M_{GH}^{-1}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)$, так и автоматы $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ и $M_{FR}^{-1}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Представим элементы кольца Z_{p^k} двоичными последовательностями длины

$$l=\lceil k\cdot\log p\rceil.$$

Рассмотрим очередную выходную последовательность

$$\gamma_1\cdots\gamma_{3\cdot l},$$

генерируемую автоматом $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ (соответственно, автоматом $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$).

Предположим, что выходы автомата $M_{GH}^{-1}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)$ (соответственно, автомата $M_{FR}^{-1}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$) подсоединены к входам мажоритарной схемы. Из (6.167) и (6.168) вытекает, что в процессе расшифровки будут обнаружены все ошибки, возникшие в процессе передачи информации по каналу связи, состоящие в инвертировании значений битов и определяемые равенством

$$\gamma_{3\cdot i+1}\oplus\gamma_{3\cdot i+2}\oplus\gamma_{3\cdot i+3}\neq 0\quad (i\in\mathbf{Z}_l).$$

При этом будут исправлены все такие ошибки, возникшие в процессе передачи информации по каналу связи, что в каждой тройке бит

$$\gamma_{3\cdot i},\gamma_{3\cdot i+2},\gamma_{3\cdot i+3}$$

ошибка произошла не более чем в одном бите.

Охарактеризуем структуру автоматов, принадлежащих множествам $\mathsf{A}_{GH}(p,k)$ и $\mathsf{A}_{FR}(p,k)$.

Утверждение 6.13. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ истинны равенства

$$|\mathsf{A}_{GH}(p,k)|=(p^k-1)^4\cdot p^{3\cdot k}\cdot(p^{-1}\cdot(p-1))^3 \qquad (6.169)$$

и

$$|\mathsf{A}_{FR}(p,k)|=(p^k-1)\cdot p^{4\cdot k}\cdot(p^{-1}\cdot(p-1))^4. \qquad (6.170)$$

Доказательство. В автомате $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ параметры $\alpha_1,\alpha_2,\alpha_3$ – обратимые элементы кольца Z_{p^k}, а $a,b,c,d\in\mathbf{Z}_{p^k}\setminus\{0\}$.

Число обратимых элементов кольца Z_{p^k} равно $p^{k-1}\cdot(p-1)$, а выбор параметров $\alpha_1,\alpha_2,\alpha_3,a,b,c,d$ осуществляется независимо. Отсюда вытекает справедливость равенства (6.169).

В автомате $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ параметры $\alpha_1,\alpha_2,\alpha_3$ и ς – обратимые элементы кольца Z_{p^k}, а $a\in \mathbf{Z}_{p^k}\setminus\{0\}$.

Выбор параметров $\alpha_1,\alpha_2,\alpha_3,\zeta,a$ осуществляется независимо. Отсюда вытекает справедливость равенства (6.170).

Утверждение доказано.

Утверждение 6.14. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ любой автомат $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$, а также любой автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ не является сильно связным автоматом.

Доказательство. Пусть

$$\mathbf{q}_0=(q_0,q_0,q_0)\in \mathbf{Z}^3_{p^k}.$$

Из (6.162) (соответственно, из (6.163)) вытекает, что

$$\mathbf{q}_1=(q_1,q_1,q_1)$$

для любого входного символа $x_1\in \mathbf{Z}_{p^k}$.

Индукцией по длине слова можно показать, что

$$\mathbf{q}_n=(q_n,q_n,q_n)$$

для любого входного слова $x_1\ldots x_n\in \mathbf{Z}^n_{p^k}$.

Так как α − обратимый элемент кольца Z_{p^k}, то из (6.162) (соответственно, из (6.163)) вытекает, что для любых фиксированных состояний

$$\mathbf{q}=(q,q,q)\in \mathbf{Z}^3_{p^k}$$

и

$$\tilde{\mathbf{q}}=(\tilde{q},\tilde{q},\tilde{q})\in \mathbf{Z}^3_{p^k}$$

автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ (соответственно, автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$) существует единственный входной символ $x\in \mathbf{Z}_{p^k}$, переводящий состояние $\mathbf{q}$ в состояние $\tilde{\mathbf{q}}$.

Следовательно, собственное подмножество

$$S_1=\{\mathbf{q}=(q,q,q)\mid q\in \mathbf{Z}_{p^k}\}$$

состояний автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ (соответственно, автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$) определяет компоненту сильной связанности.

Отсюда вытекает, что автомат $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ (соответственно, автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$) не является сильно связным.

Утверждение доказано.

Из доказательства утверждения 6.14 вытекает

Следствие 6.13. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ как подавтомат автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d) \in \mathsf{A}_{GH}(p,k)$, так и подавтомат автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathsf{A}_{FR}(p,k)$, определяемый множеством состояний $S_1 = \{\mathbf{q} = (q,q,q) \mid q \in \mathbf{Z}_{p^k}\}$, является приведенным перестановочным автоматом, диаметр графа переходов которого равен 1.

Следующее утверждение показывает, что структура автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d) \in \mathsf{A}_{GH}(p,k)$ может существенно отличаться от структуры его подавтомата, определяемого множеством состояний S_1.

Утверждение 6.15. Пусть

$$d \equiv 0 \,(\mathrm{mod}\ p^{\lceil 0.5 \cdot k \rceil}). \tag{6.171}$$

Тогда для простого числа p при всех значениях числа $k \in \mathbf{N}$ множество состояний

$$S_2 = \{\mathbf{q} = (q^{(1)},q^{(2)},q^{(3)}) \mid q^{(i)} \equiv 0 \,(\mathrm{mod}\ p^{\lceil 0.5 \cdot k \rceil})\ \ (i = 1,2,3)\} \tag{6.172}$$

автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d) \in \mathsf{A}_{GH}(p,k)$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в одно и то же состояние

$$\mathbf{q}_1 = (\alpha_1 \circ x, \alpha_2 \circ x, \alpha_3 \circ x). \tag{6.173}$$

Доказательство. Пусть выполнено условие (6.171) и

$$\mathbf{q}_0 = (q^{(1)},q^{(2)},q^{(3)}) \in S_2,$$

где множество S_2 определяется равенством (6.172).

Так как

$$q^{(i)} \equiv 0 \,(\mathrm{mod}\ p^{\lceil 0.5 \cdot k \rceil})\ \ (i = 1,2,3),$$

то

$$(q^{(i)})^2 = 0 \quad (i = 1,2,3). \tag{6.174}$$

А так как

$$q^{(i)} \equiv 0 \,(\mathrm{mod}\ p^{\lceil 0.5 \cdot k \rceil})\ \ (i = 1,2,3)$$

и

$$d \equiv 0 \,(\mathrm{mod}\ p^{\lceil 0.5 \cdot k \rceil}),$$

то

$$q^{(i)} \circ d = 0\ \ (i = 1,2,3). \tag{6.175}$$

Из (6.162), (6.174) и (6.175) вытекает, что под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ состояние $\mathbf{q}_0$ переходит в состояние $\mathbf{q}_1$, определяемое равенством (6.173).

Утверждение доказано.

Из утверждения 6.15 вытекает

Следствие 6.14. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если

$$d \equiv 0 \,(\mathrm{mod}\, p^{\lceil 0.5 \cdot k \rceil}),$$

то любой автомат $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d) \in \mathsf{A}_{GH}(p,k)$ не является перестановочным автоматом.

Из (6.163) вытекает, что для автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathsf{A}_{FR}(p,k)$ имеет место

Утверждение 6.16. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ множество состояний

$$S_3 = \{\mathbf{q} = (q^{(1)},q^{(2)},q^{(3)}) \mid q^{(i)} \in \{0,1\} \ \ (i = 1,2,3)\}$$

любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathsf{A}_{FR}(p,k)$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в одно и то же состояние

$$\mathbf{q}_1 = (\alpha_1 \circ x, \alpha_2 \circ x, \alpha_3 \circ x).$$

Из утверждения 6.16 вытекает

Следствие 6.15. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ любой автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathsf{A}_{FR}(p,k)$ не является перестановочным автоматом.

Обозначим через $K(\mathbf{q}, M_u)$ $(u \in \{GH, FR\})$ множество всех состояний автомата $M_u \in \mathsf{A}_u(p,k)$ эквивалентных состоянию $\mathbf{q} \in \mathbf{Z}_{p^k}^3$.

Теорема 6.16. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ для любого автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d) \in \mathsf{A}_{GH}(p,k)$ и любого состояния $\mathbf{q} = (q^{(1)},q^{(2)},q^{(3)}) \in \mathbf{Z}_{p^k}^3$ множество $K(\mathbf{q}, M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d))$ состоит из всех таких состояний $\tilde{\mathbf{q}} = (\tilde{q}^{(1)},\tilde{q}^{(2)},\tilde{q}^{(3)}) \in \mathbf{Z}_{p^k}^3$, что истинны равенства

$$\begin{cases} \tilde{q}^{(1)} \circ (d \oplus a \circ (\tilde{q}^{(1)})^2 \oplus b \circ (\tilde{q}^{(2)})^2 \oplus c \circ (\tilde{q}^{(3)})^2) = \\ \quad = q^{(1)} \circ (d \oplus a \circ (q^{(1)})^2 \oplus b \circ (q^{(2)})^2 \oplus c \circ (q^{(3)})^2) \\ \tilde{q}^{(2)} \circ (d \oplus c \circ (\tilde{q}^{(1)})^2 \oplus a \circ (\tilde{q}^{(2)})^2 \oplus b \circ (\tilde{q}^{(3)})^2) = \\ \quad = q^{(2)} \circ (d \oplus c \circ (q^{(1)})^2 \oplus a \circ (q^{(2)})^2 \oplus b \circ (q^{(3)})^2) \\ \tilde{q}^{(3)} \circ (d \oplus b \circ (\tilde{q}^{(1)})^2 \oplus c \circ (\tilde{q}^{(2)})^2 \oplus a \circ (\tilde{q}^{(3)})^2) = \\ \quad = q^{(3)} \circ (d \oplus b \circ (q^{(1)})^2 \oplus c \circ (q^{(2)})^2 \oplus a \circ (q^{(3)})^2) \end{cases}. \qquad (6.176)$$

Доказательство. Зафиксируем состояние

$$\mathbf{q}=(q^{(1)},q^{(2)},q^{(3)})\in \mathbf{Z}_{p^k}^3$$

автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$.

Пусть

$$\tilde{\mathbf{q}}=(\tilde{q}^{(1)},\tilde{q}^{(2)},\tilde{q}^{(3)})\in K(\mathbf{q},M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)).$$

Из первых трех уравнений системы (6.162) находим, что для любого входного символа $x\in \mathbf{Z}_{p^k}$

$$\begin{cases} q_1^{(1)}=q^{(1)}\circ(d\oplus a\circ(q^{(1)})^2\oplus b\circ(q^{(2)})^2\oplus c\circ(q^{(3)})^2)\oplus\alpha_1\circ x \\ q_1^{(2)}=q^{(2)}\circ(d\oplus c\circ(q^{(1)})^2\oplus a\circ(q^{(2)})^2\oplus b\circ(q^{(3)})^2)\oplus\alpha_2\circ x \\ q_1^{(3)}=q^{(3)}\circ(d\oplus b\circ(q^{(1)})^2\oplus c\circ(q^{(2)})^2\oplus a\circ(q^{(3)})^2)\oplus\alpha_3\circ x \end{cases} \qquad (6.177)$$

и

$$\begin{cases} \tilde{q}_1^{(1)}=\tilde{q}^{(1)}\circ(d\oplus a\circ(\tilde{q}^{(1)})^2\oplus b\circ(\tilde{q}^{(2)})^2\oplus c\circ(\tilde{q}^{(3)})^2)\oplus\alpha_1\circ x \\ \tilde{q}_1^{(2)}=\tilde{q}^{(2)}\circ(d\oplus c\circ(\tilde{q}^{(1)})^2\oplus a\circ(\tilde{q}^{(2)})^2\oplus b\circ(\tilde{q}^{(3)})^2)\oplus\alpha_2\circ x. \\ \tilde{q}_1^{(3)}=\tilde{q}^{(3)}\circ(d\oplus b\circ(\tilde{q}^{(1)})^2\oplus c\circ(\tilde{q}^{(2)})^2\oplus a\circ(\tilde{q}^{(3)})^2)\oplus\alpha_3\circ x \end{cases} \qquad (6.178)$$

Так как состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ являются эквивалентными состояниями автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$, то из последних трех уравнений системы (6.162) вытекает, что

$$q_1^{(i)}=\tilde{q}_1^{(i)}\quad (i=1,2,3). \qquad (6.179)$$

Из (6.177)-(6.179) вытекает (6.176).

Теорема доказана.

Из доказательства теоремы 6.16 вытекает

Следствие 6.16. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ любые эквивалентные друг другу состояния любого автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ являются близнецами.

Теорема 6.17. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ для любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ и любого состояния $\mathbf{q}=(q^{(1)},q^{(2)},q^{(3)})\in \mathbf{Z}_{p^k}^3$ множество $K(\mathbf{q},M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ состоит из всех таких состояний $\tilde{\mathbf{q}}=(\tilde{q}^{(1)},\tilde{q}^{(2)},\tilde{q}^{(3)})\in \mathbf{Z}_{p^k}^3$, что истинны равенства

$$\begin{cases} f(\tilde{q}^{(1)})\circ\zeta^{\tilde{q}^{(3)}-q^{(3)}}=f(q^{(1)}) \\ f(\tilde{q}^{(2)})\circ\zeta^{\tilde{q}^{(1)}-q^{(1)}}=f(q^{(2)}). \\ f(\tilde{q}^{(3)})\circ\zeta^{\tilde{q}^{(2)}-q^{(2)}}=f(q^{(3)}) \end{cases} \qquad (6.180)$$

Доказательство. Зафиксируем состояние

$$\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in \mathbf{Z}_{p^k}^3$$

автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathsf{A}_{FR}(p,k)$.

Пусть

$$\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in K(\mathbf{q}, M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a)).$$

Из первых трех уравнений системы (6.163) находим, что для любого входного символа $x \in \mathbf{Z}_{p^k}$

$$\begin{cases} q_1^{(1)} = f(q^{(1)}) \circ \zeta^{q^{(3)}} \oplus \alpha_1 \circ x_{n+1} \\ q_1^{(2)} = f(q^{(2)}) \circ \zeta^{q^{(1)}} \oplus \alpha_2 \circ x_{n+1} \\ q_1^{(3)} = f(q^{(3)}) \circ \zeta^{q^{(2)}} \oplus \alpha_3 \circ x_{n+1} \end{cases} \tag{6.181}$$

и

$$\begin{cases} \tilde{q}_1^{(1)} = f(\tilde{q}^{(1)}) \circ \zeta^{\tilde{q}^{(3)}} \oplus \alpha_1 \circ x_{n+1} \\ \tilde{q}_1^{(2)} = f(\tilde{q}^{(2)}) \circ \zeta^{\tilde{q}^{(1)}} \oplus \alpha_2 \circ x_{n+1} \\ \tilde{q}_1^{(3)} = f(\tilde{q}^{(3)}) \circ \zeta^{\tilde{q}^{(2)}} \oplus \alpha_3 \circ x_{n+1} \end{cases}. \tag{6.182}$$

Так как состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ являются эквивалентными состояниями автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a)$, то из последних трех уравнений системы (6.163) вытекает, что

$$q_1^{(i)} = \tilde{q}_1^{(i)} \quad (i = 1,2,3). \tag{6.183}$$

Из (6.181)-(6.183) вытекает, что

$$\begin{cases} f(q^{(1)}) \circ \zeta^{q^{(3)}} \oplus \alpha_1 \circ x_{n+1} = f(\tilde{q}^{(1)}) \circ \zeta^{\tilde{q}^{(3)}} \oplus \alpha_1 \circ x_{n+1} \\ f(q^{(2)}) \circ \zeta^{q^{(1)}} \oplus \alpha_2 \circ x_{n+1} = f(\tilde{q}^{(2)}) \circ \zeta^{\tilde{q}^{(1)}} \oplus \alpha_2 \circ x_{n+1} \\ f(q^{(3)}) \circ \zeta^{q^{(2)}} \oplus \alpha_3 \circ x_{n+1} = f(\tilde{q}^{(3)}) \circ \zeta^{\tilde{q}^{(2)}} \oplus \alpha_3 \circ x_{n+1} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} f(q^{(1)}) \circ \zeta^{q^{(3)}} = f(\tilde{q}^{(1)}) \circ \zeta^{\tilde{q}^{(3)}} \\ f(q^{(2)}) \circ \zeta^{q^{(1)}} = f(\tilde{q}^{(2)}) \circ \zeta^{\tilde{q}^{(1)}} \\ f(q^{(3)}) \circ \zeta^{q^{(2)}} = f(\tilde{q}^{(3)}) \circ \zeta^{\tilde{q}^{(2)}} \end{cases}. \tag{6.184}$$

Так как ζ – обратимый элемент кольца Z_{p^k}, то из (6.184) вытекают равенства (6.180).

Теорема доказана.

Из доказательства теоремы 6.16 вытекает

Следствие 6.17. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ любые эквивалентные друг другу состояния любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathsf{A}_{FR}(p,k)$ являются близнецами.

Множество $K(\mathbf{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ может быть вычислено следующим образом.

Пусть число ζ принадлежит показателю δ, т.е. δ − такое наименьшее натуральное число, что

$$\zeta^{\delta} \equiv 1 (\mathrm{mod}\ p^k).$$

Представим компоненты состояния $\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in \mathbf{Z}^3_{p^k}$ в виде

$$q^{(i)} = \zeta^{h_i} \circ b_i \ \ (i = 1,2,3),$$

где

$$(b_i, \zeta) = 1 \ \ (i = 1,2,3).$$

Из (6.180) вытекает, что компоненты любого состояния

$$\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in K(\mathbf{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$$

удовлетворяют равенствам

$$\begin{cases} f(\tilde{q}^{(1)}) = \zeta^{l_3} \circ b_1 \\ f(\tilde{q}^{(2)}) = \zeta^{l_1} \circ b_2 \\ f(\tilde{q}^{(3)}) = \zeta^{l_2} \circ b_3 \end{cases}. \qquad (6.185)$$

Из (6.180) и (6.185) вытекает, что

$$\begin{cases} \tilde{q}^{(1)} \equiv h_1 \oplus q^{(1)} \Theta l_1 \ (\mathrm{mod}\,\delta) \\ \tilde{q}^{(2)} \equiv h_2 \oplus q^{(2)} \Theta l_2 \ (\mathrm{mod}\,\delta) \\ \tilde{q}^{(3)} \equiv h_3 \oplus q^{(3)} \Theta l_3 \ (\mathrm{mod}\,\delta) \end{cases}. \qquad (6.186)$$

Итак, для построения множества $K(\mathbf{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ достаточно найти все решения $(\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)})$ систем сравнений (6.186) при всех значениях $l_1, l_2, l_3 \in \{0,1,\ldots,\delta-1\}$.

При этом $(\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in K(\mathbf{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ тогда и только тогда, когда истинны равенства (6.185).

Рассмотрим задачу параметрической идентификации автомата $M_u \in \mathsf{A}_u(p,k)$ $(u \in \{GH, FR\})$ в предположении, что экспериментатор может управлять входом и инициализацией автомата.

Утверждение 6.17. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ идентификация параметров $\alpha_1, \alpha_2, \alpha_3$ любого автомата $M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) \in \mathsf{A}_{GH}(p,k)$ и $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathsf{A}_{FR}(p,k)$ осуществляется простым экспериментом длины 1.

Доказательство. Положим

$$q_0^{(1)} = q_0^{(2)} = q_0^{(3)} = 0$$

и

$$x = 1.$$

Как из равенств (6.162), так и из равенств (6.163) вытекает, что

$$\alpha_i = y_1^{(i)} \ (i = 1,2,3).$$

Утверждение доказано.

Теорема 6.18. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ идентификация параметров b и c любого автомата $M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) \in \mathsf{A}_{GH}(p,k)$ осуществляется кратным экспериментом кратности 2 и высоты 1.

Доказательство. Положив

$$\mathbf{q}_0 = (1,0,0)$$

и

$$x_1 = 0,$$

из (6.162) находим, что

$$d \oplus a = y_1^{(1)}. \tag{6.187}$$

Положив

$$\tilde{\mathbf{q}}_0 = (1,1,0)$$

и

$$x_1' = 0,$$

из (6.162) находим, что

$$\begin{cases} d \oplus a \oplus b = \tilde{y}_1^{(1)} \\ d \oplus a \oplus c = \tilde{y}_1^{(2)} \end{cases}. \tag{6.188}$$

Из (6.187) и (6.188) находим, что

$$\begin{cases} b = \tilde{y}_1^{(1)} \Theta y_1^{(1)} \\ c = \tilde{y}_1^{(2)} \Theta y_1^{(1)} \end{cases}.$$

Теорема доказана.

Теорема 6.19. Для любого простого числа $p>3$ при всех значениях числа $k\in\mathbf{N}$ идентификация параметров a и d любого автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$ сводится к решению системы двух линейных уравнений, сформированной в результате простого эксперимента длины 1.

Доказательство. Положив

$$\mathbf{q}_0=(1,2,0)$$

и

$$x_1=0,$$

из (6.162) находим, что

$$\begin{cases} d\oplus a\oplus 4\circ b=y_1^{(1)} \\ 2\circ d\oplus(8\,(\mathrm{mod}\,p))\circ a\oplus 2\circ c=y_1^{(2)} \end{cases}\Leftrightarrow$$

$$\Leftrightarrow\begin{cases} d\oplus a=y_1^{(1)}\Theta 4\circ b \\ 2\circ d\oplus(8\,(\mathrm{mod}\,p))\circ a=y_1^{(2)}\Theta 2\circ c \end{cases}\Leftrightarrow$$

$$\Leftrightarrow\begin{cases} (8\,(\mathrm{mod}\,p)\Theta 2)\circ a=y_1^{(2)}\Theta 2\circ y_1^{(1)}\Theta 2\circ c\oplus(8\,(\mathrm{mod}\,p))\circ b \\ d=y_1^{(1)}\Theta 4\circ b\Theta a \end{cases}. \quad (6.189)$$

Так как p – простое число и $p>3$, то элемент $8\,(\mathrm{mod}\,p)\Theta 2$ является обратимым элементом кольца Z_{p^k}.

Следовательно, из (6.189) вытекает, что

$$\begin{cases} a=(8\,(\mathrm{mod}\,p)\Theta 2)^{-1}\circ(y_1^{(2)}\Theta 2\circ y_1^{(1)}\Theta 2\circ c\oplus(8\,(\mathrm{mod}\,p))\circ b) \\ d=y_1^{(1)}\Theta 4\circ b\Theta \\ \qquad \Theta(8\,(\mathrm{mod}\,p)\Theta 2)^{-1}\circ(y_1^{(2)}\Theta 2\circ y_1^{(1)}\Theta 2\circ c\oplus(8\,(\mathrm{mod}\,p))\circ b) \end{cases}.$$

Теорема доказана.

Теорема 6.20. Для любого простого числа $p>3$ при всех значениях числа $k\in\mathbf{N}$, если известно, что a – обратимый элемент кольца Z_{p^k}, то идентификация параметров a и ζ автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ сводится к решению системы двух уравнений, полученной в результате простого эксперимента длины 1.

Доказательство. Пусть a – обратимый элемент кольца Z_{p^k}.

Положив

$$\mathbf{q}_0=(2,3,1)$$

и

$$x_1 = 0,$$

из (6.163) находим, что

$$\begin{cases} \zeta \circ a \circ 2 \circ (p^k - 1) = y_1^{(1)} \\ \zeta^2 \circ a \circ 3 \circ (p^k - 2) = y_1^{(2)} \end{cases}. \qquad (6.190)$$

Так как p − простое число и $p > 3$, то элементы 2, 3, $p^k - 1$ и $p^k - 2$ являются обратимыми элементами кольца Z_{p^k}.

А так как a − обратимый элемент кольца Z_{p^k} и система уравнений (6.190) − совместная, то $y_1^{(i)}$ $(i = 1,2)$ − обратимые элементы кольца Z_{p^k}.

Следовательно, из (6.190) вытекает, что

$$\begin{cases} \zeta = (y_1^{(1)})^{-1} \circ y_1^{(2)} \circ 2 \circ 3^{-1} \circ (p^k - 1) \circ (p^k - 2)^{-1} \\ a = (y_1^{(1)})^2 \circ (y_1^{(2)})^{-1} \circ 4^{-1} \circ 3 \circ (p^k - 1)^{-2} \circ (p^k - 2) \end{cases}.$$

Теорема доказана.

Отметим, что для автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathsf{A}_{FR}(p,k)$ идентификация параметров a и ζ существенно усложняется, если a − необратимый элемент кольца Z_{p^k}. В этом случае вначале необходимо найти все решения a и ζ системы уравнений (6.190), а затем обычными методами теории автоматов с помощью простого (или кратного) эксперимента решить задачу идентификации автомата в классе всех допустимых автоматов $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathsf{A}_{FR}(p,k)$.

Рассмотрим задачу идентификации начального состояния автомата $M_u \in \mathsf{A}_u(p,k)$ $(u \in \{GH, FR\})$ в предположении, что экспериментатору известны параметры автомата, и экспериментатор может управлять входом автомата.

Отметим, что сложность решения этой задачи существенно зависит от возможности экспериментатора управлять параметрами автомата.

Рассмотрим автомат $M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) \in \mathsf{A}_{GH}(p,k)$.

Предположим вначале, что экспериментатор может управлять параметрами автомата $M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) \in \mathsf{A}_{GH}(p,k)$.

Положим

$$(a, b, c, d) = (0,0,0,1)$$

и

$$x_1 = 0,$$

из (6.162) находим, что

$$q_0^{(i)} = y_1^{(i)} \ (i = 1,2,3).$$

Предположим теперь, что экспериментатор не может управлять параметрами автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$.

Из (6.162) вытекает, что для любого входного символа $x\in \mathbf{Z}_{p^k}$ мы получим систему трех нелинейных уравнений

$$\begin{cases} q_0^{(1)}\circ(d\oplus a\circ(q_0^{(1)})^2\oplus b\circ(q_0^{(2)})^2\oplus c\circ(q_0^{(3)})^2)=y_1^{(1)}\Theta\alpha_1\circ x \\ q_0^{(2)}\circ(d\oplus c\circ(q_0^{(1)})^2\oplus a\circ(q_0^{(2)})^2\oplus b\circ(q_0^{(3)})^2)=y_1^{(2)}\Theta\alpha_2\circ x. \\ q_0^{(3)}\circ(d\oplus b\circ(q_0^{(1)})^2\oplus c\circ(q_0^{(2)})^2\oplus a\circ(q_0^{(3)})^2)=y_1^{(3)}\Theta\alpha_3\circ x \end{cases} \quad (6.191)$$

Множество S решений $(q_0^{(1)},q_0^{(2)},q_0^{(3)})$ системы (6.191) уравнений третьей степени над кольцом Z_{p^k} определяет множество всех допустимых кандидатов на начальное состояние исследуемого автомата. Неэквивалентные состояния автомата $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in \mathsf{A}_{GH}(p,k)$, принадлежащие множеству S (если такие имеются), необходимо теперь различить обычными методами теории автоматов, т.е. с помощью диагностического эксперимента.

Рассмотрим автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$.

Предположим вначале, что экспериментатор имеет возможность управлять параметрами автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$.

Пусть

$$p^k>4.$$

Положим

$$a=4$$

и

$$\zeta=1.$$

Из (6.163) вытекает, что для любого входного символа $x\in \mathbf{Z}_{p^k}$ мы получим следующую систему трех уравнений над кольцом Z_{p^k}

$$\begin{cases} (2\circ q_0^{(1)}\Theta 1)^2=\alpha_1\circ x\Theta y_1^{(1)}\oplus 1 \\ (2\circ q_0^{(2)}\Theta 1)^2=\alpha_2\circ x\Theta y_1^{(2)}\oplus 1. \\ (2\circ q_0^{(3)}\Theta 1)^2=\alpha_3\circ x\Theta y_1^{(3)}\oplus 1 \end{cases} \quad (6.192)$$

Множество S решений $(q_0^{(1)},q_0^{(2)},q_0^{(3)})$ системы уравнений (6.192) определяет множество всех допустимых кандидатов на начальное состояние исследуемого автомата.

При этом

$$|S|=o(p^k),$$

если $p\to\infty$ или $k\to\infty$.

Неэквивалентные состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, принадлежащие множеству S (если такие имеются), необходимо теперь различить обычными методами теории автоматов, т.е. с помощью диагностического эксперимента.

Предположим теперь, что экспериментатор не может управлять параметрами автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$.

Из (6.163) вытекает, что для любого входного символа $x\in \mathbf{Z}_{p^k}$

$$\begin{cases} f(q_0^{(1)})\circ\zeta^{q_0^{(3)}} = y_1^{(1)}\Theta\alpha_1\circ x_1 \\ f(q_0^{(2)})\circ\zeta^{q_0^{(1)}} = y_1^{(2)}\Theta\alpha_2\circ x_1 \\ f(q_0^{(3)})\circ\zeta^{q_0^{(2)}} = y_1^{(3)}\Theta\alpha_3\circ x_1 \end{cases}. \qquad (6.193)$$

Так как система уравнений (6.193) − совместная, то

$$\begin{cases} y_1^{(1)}\Theta\alpha_1\circ x_1 = b_1\circ\zeta^{h_3} \\ y_1^{(2)}\Theta\alpha_1\circ x_1 = b_2\circ\zeta^{h_1} \\ y_1^{(3)}\Theta\alpha_1\circ x_1 = b_3\circ\zeta^{h_2} \end{cases}, \qquad (6.194)$$

где

$$(b_i,\zeta)=1 \quad (i=1,2,3).$$

Из (6.193) и (6.194) вытекает, что

$$\begin{cases} f(q_0^{(1)}) = \zeta^{l_3}\circ b_1 \\ f(q_0^{(2)}) = \zeta^{l_1}\circ b_2 \\ f(q_0^{(3)}) = \zeta^{l_2}\circ b_3 \end{cases}. \qquad (6.195)$$

Пусть число ζ принадлежит показателю δ.

Подставив (6.194) и (6.195) в (6.193), получим

$$\begin{cases} q_0^{(1)} \equiv h_1\Theta l_1 \pmod\delta \\ q_0^{(2)} \equiv h_2\Theta l_2 \pmod\delta \\ q_0^{(3)} \equiv h_3\Theta l_3 \pmod\delta \end{cases}. \qquad (6.196)$$

Таким образом, для идентификации начального состояния любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathsf{A}_{FR}(p,k)$ достаточно найти множество S всех решений $(q_0^{(1)},q_0^{(2)},q_0^{(3)})$ систем сравнений (6.196) при всех значениях чисел $l_1,l_2,l_3\in\{0,1,\ldots,\delta-1\}$, вычислить подмножество $\tilde{S}$, состоящее из всех элементов $(q_0^{(1)},q_0^{(2)},q_0^{(3)})\in S$, удовлетворяющих системе уравнений (6.195) и различить неэквивалентные состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, при-

надлежащие множеству $\tilde{S}$ (если такие имеются) обычными методами теории автоматов, т.е. с помощью диагностического эксперимента.

Охарактеризуем множества неподвижных точек о.-д. функций, реализуемых инициальными автоматами $(M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d),\mathbf{q}_0)$ и $(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\mathbf{q}_0)$.

Обозначим через $X(M_u,\mathbf{q})$ $(u\in\{GH,FR\})$ множество всех неподвижных точек о.-д. функции, реализуемой инициальным автоматом $(M_u,\mathbf{q})$. Положим

$$X^{(1)}(M_u,\mathbf{q})=X(M_u,\mathbf{q},)\cap\mathbf{Z}_{p^k}.$$

Рассмотрим автомат $M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d)\in\mathsf{A}_{GH}(p,k)$.

Из (6.162) вытекает, что $x_1\in X^{(1)}(M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d),\mathbf{q}_0)$ тогда и только тогда, когда x_1 является решением системы уравнений

$$\begin{cases}(1\Theta\alpha_1)\circ x_1=q_0^{(1)}\circ(d\oplus a\circ(q_0^{(1)})^2\oplus b\circ(q_0^{(2)})^2\oplus c\circ(q_0^{(3)})^2)\\(1\Theta\alpha_2)\circ x_1=q_0^{(2)}\circ(d\oplus c\circ(q_0^{(1)})^2\oplus a\circ(q_0^{(2)})^2\oplus b\circ(q_0^{(3)})^2).\\(1\Theta\alpha_3)\circ x_1=q_0^{(3)}\circ(d\oplus b\circ(q_0^{(1)})^2\oplus c\circ(q_0^{(2)})^2\oplus a\circ(q_0^{(3)})^2)\end{cases}\quad(6.197)$$

Из (6.197) вытекают

Утверждение 6.18. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$, если каждый элемент $1\Theta\alpha_i$ $(i=1,2,3)$ является обратимым элементом кольца Z_{p^k}, то:

1) равенство

$$X^{(1)}(M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d),\mathbf{q}_0)=\varnothing$$

истинно тогда и только тогда, когда выполнено, по крайней мере, одно из условий:

$$(1\Theta\alpha_1)^{-1}\circ q_0^{(1)}\circ(d\oplus a\circ(q_0^{(1)})^2\oplus b\circ(q_0^{(2)})^2\oplus c\circ(q_0^{(3)})^2)\neq$$
$$\neq(1\Theta\alpha_2)^{-1}\circ q_0^{(2)}\circ(d\oplus c\circ(q_0^{(1)})^2\oplus a\circ(q_0^{(2)})^2\oplus b\circ(q_0^{(3)})^2),\quad(6.198)$$

$$(1\Theta\alpha_1)^{-1}\circ q_0^{(1)}\circ(d\oplus a\circ(q_0^{(1)})^2\oplus b\circ(q_0^{(2)})^2\oplus c\circ(q_0^{(3)})^2)\neq$$
$$\neq(1\Theta\alpha_3)^{-1}\circ q_0^{(3)}\circ(d\oplus b\circ(q_0^{(1)})^2\oplus c\circ(q_0^{(2)})^2\oplus a\circ(q_0^{(3)})^2)\quad(6.199)$$

или

$$(1\Theta\alpha_2)^{-1}\circ q_0^{(2)}\circ(d\oplus c\circ(q_0^{(1)})^2\oplus a\circ(q_0^{(2)})^2\oplus b\circ(q_0^{(3)})^2)\neq$$
$$\neq(1\Theta\alpha_3)^{-1}\circ q_0^{(3)}\circ(d\oplus b\circ(q_0^{(1)})^2\oplus c\circ(q_0^{(2)})^2\oplus a\circ(q_0^{(3)})^2);\quad(6.200)$$

2) равенство

$$|X^{(1)}(M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d),\mathbf{q}_0)|=1$$

истинно тогда и только тогда, когда ни одно из условий (6.198)-(6.200) не выполнено.

Утверждение 6.19. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$, если, по крайней мере, один из элементов $1\Theta\alpha_i$ $(i=1,2,3)$ является необратимым элементом кольца Z_{p^k}, то

$$X^{(1)}(M_{GH}(\alpha_1,\alpha_2,\alpha_3,a,b,c,d),\mathbf{q}_0)=\varnothing,$$

если выполнено, по крайней мере, одно из условий:

1) $q_0^{(1)}\circ(d\oplus a\circ(q_0^{(1)})^2\oplus b\circ(q_0^{(2)})^2\oplus c\circ(q_0^{(3)})^2)$ − обратимый элемент кольца Z_{p^k}, а $1\Theta\alpha_1$ − необратимый элемент кольца Z_{p^k};

2) $q_0^{(2)}\circ(d\oplus c\circ(q_0^{(1)})^2\oplus a\circ(q_0^{(2)})^2\oplus b\circ(q_0^{(3)})^2)$ − обратимый элемент кольца Z_{p^k}, а $1\Theta\alpha_2$ − необратимый элемент кольца Z_{p^k},

3) $q_0^{(3)}\circ(d\oplus b\circ(q_0^{(1)})^2\oplus c\circ(q_0^{(2)})^2\oplus a\circ(q_0^{(3)})^2)$ − обратимый элемент кольца Z_{p^k}, а $1\Theta\alpha_3$ − необратимый элемент кольца Z_{p^k}.

Рассмотрим автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in\mathsf{A}_{FR}(p,k)$.

Из (6.163) вытекает, что $x_1\in X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\mathbf{q}_0)$ тогда и только тогда, когда x_1 является решением системы уравнений

$$\begin{cases}(1\Theta\alpha_1)\circ x_1=f(q_0^{(1)})\circ\zeta^{q_0^{(3)}}\\(1\Theta\alpha_2)\circ x_1=f(q_0^{(2)})\circ\zeta^{q_0^{(1)}}\\(1\Theta\alpha_3)\circ x_1=f(q_0^{(3)})\circ\zeta^{q_0^{(2)}}\end{cases}. \qquad (6.201)$$

Из (6.201) вытекают

Утверждение 6.20. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$, если каждый элемент $1\Theta\alpha_i$ $(i=1,2,3)$ является обратимым элементом кольца Z_{p^k}, то:

1) равенство

$$X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\mathbf{q}_0)=\varnothing$$

истинно тогда и только тогда, когда выполнено, по крайней мере, одно из условий:

$$(1\Theta\alpha_1)^{-1}\circ f(q_0^{(1)})\circ\zeta^{q_0^{(3)}}\neq(1\Theta\alpha_2)^{-1}\circ f(q_0^{(2)})\circ\zeta^{q_0^{(1`)}}, \qquad (6.202)$$

$$(1\Theta\alpha_1)^{-1}\circ f(q_0^{(1)})\circ\zeta^{q_0^{(3)}}\neq(1\Theta\alpha_3)^{-1}\circ f(q_0^{(3)})\circ\zeta^{q_0^{(2)}} \qquad (6.203)$$

или

$$(1\Theta\alpha_2)^{-1} \circ f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}} \neq (1\Theta\alpha_3)^{-1} \circ f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}}; \qquad (6.204)$$

2) равенство

$$|X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\mathbf{q}_0)|=1$$

истинно тогда и только тогда, когда ни одно из условий (6.202)-(6.204) не выполнено.

Утверждение 6.21. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если существует такое значение $i \in \{1,2,3\}$, что $1\Theta\alpha_i$ и $f(q_0^{(i)})$, соответственно, необратимый и обратимый элементы кольца Z_{p^k}, то

$$X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\mathbf{q}_0)=\varnothing.$$

6.7. Выводы.

Настоящий раздел является логическим продолжением исследований, представленных в разделе 5. Объектом исследования являются нелинейные автоматы Мили и Мура над кольцом $Z_{p^k}=(\mathbf{Z}_{p^k},\oplus,\circ)$ (где p – простое число, а $k \in \mathbf{N}$).

В настоящем разделе исследования проведены с позиции теории автоматов, теории систем, а также с учетом возможного применения этих автоматов в качестве математических моделей при решении задач современной криптологии. Именно в силу последнего обстоятельства основное внимание уделено исследованию обратимых нелинейных автоматов Мили и Мура над кольцом Z_{p^k}.

Целесообразность исследования таких автоматов обусловлена тем, что фрагментарное применение операций над кольцом Z_{2^k} используется в значительном числе кандидатов на современные схемы шифрования, представленные в рамках проектов, разрабатываемых в настоящее время.

Основные результаты, представленные в настоящем разделе, состоят в следующем:

1. Выделены, и охарактеризованы с позиции теории автоматов, классы нелинейных автоматов Мили и Мура с лагом 1 над конечным кольцом, в предположении, что «нелинейность» характеризуется тем, что изменение значений переменных состояний и выходных переменных представлено алгебраической суммой квадратичной и линейной форм от переменных состояний с линейной формой от входных переменных.

2. Охарактеризованы симметричные схемы шифрования, построенные на основе исследуемых автоматов. Для таких схем шифрования секретным сеансовым ключом является начальное состояние автомата, а секретным

ключом средней длительности – параметры, определяющие конкретный автомат, принадлежащий заданному классу.

3. В рамках построенной модели развиты средства контроля ошибок, возникающих в процессе передачи шифртекста по каналу связи.

4. Показано, что аналоги над кольцом Z_{p^k} таких модельных хаотических динамических систем, как системы Рёсслера, Спротта, Лоренца и Эно, укладываются в рамки исследуемых нелинейных автоматов.

Эти модельные нелинейные автоматы характеризуются тем, что в силу малой размерности пространства их состояний, на их основе могут быть построены высокоскоростные поточные шифры.

5. Охарактеризованы классы эквивалентных состояний исследуемых нелинейных автоматов.

6. Показано, что даже для модельных нелинейных автоматов Рёсслера, Спротта, Лоренца и Эно классы эквивалентных состояний имеют сложную структуру, характеризуемую нелинейными рекуррентными соотношениями.

Таким образом, установлено, что минимизация нелинейного автомата заведомо приведет к существенному усложнению модели, представляющей автомат. Следовательно, криптоаналитик при любой атаке, направленной на идентификацию секретного ключа, вынужден будет решать сложную задачу идентификации состояний автомата с точностью до класса эквивалентных состояний.

7. Решены задачи параметрической идентификации и идентификации начального состояния для исследуемых нелинейных автоматов.

8. Показано, что для исследуемого нелинейного автомата как задача идентификация начального состояния, так и задача параметрической идентификации представляют собой трудные задачи, состоящие в поиске и решении систем нелинейных уравнений над кольцом Z_{p^k}.

9. Детализированы решения задач параметрической идентификации и идентификации начального состояния для модельных нелинейных автоматов Рёсслера, Спротта, Лоренца и Эно.

10. Охарактеризована вариация о.-д. функции, реализуемой исследуемым инициальным нелинейным автоматом, при вариации его параметров или начального состояния, что является для поточных шифров аналогом дифференциального и интегрального криптоанализа, разработанного для *DES*-подобных алгоритмов, осуществляющих блочное шифрование.

11. Построены соотношения, характеризующие вариацию о.-д. функций, реализуемых инициальными нелинейными автоматами Рёсслера, Спротта, Лоренца и Эно

12. Предложена, и исследована схема поточного шифрования, основанная на представлении исходной двоичной последовательности в виде 24-разрядного bmp-файла и использовании черно-белого представления псев-

дофрактала Мандельброта в области дисплея для управления легко-вычислимым семейством перестановок.

13. Предложенная схема шифрования на основе псевдофракталов обобщена на случай перехода к действиям в кольце Z_{p^k} под управлением черно-белого изображения псевдофрактала любой размерности.

14. Исследован класс семейств легко-вычислимых семейств перестановок, определенных в терминах кольца Z_{p^k} и используемых в общей схеме шифрования, основанной на использовании псевдофракталов.

15. Показано, что задачи идентификации параметров, определяющих конкретное легко-вычислимое семейство перестановок, принадлежащее заданному классу, сводится к решению системы задач дискретного логарифмирования.

16. Охарактеризованы с позиции теории автоматов Guckenheimer and Holmes cycle автомат и free-running автомат над кольцом Z_{p^k}.

Эти автоматы являются аналогами над кольцом Z_{p^k} модельных хаотических динамических систем, обладающих нетривиальными группами симметрий и характеризующихся тем, что изменение динамических переменных в динамической системе Guckenheimer and Holmes cycle представлено многочленами третьей степени, а изменение динамических переменных в динамической системе free-running system осуществляется с помощью показательной функции.

17. Решены задачи параметрической идентификации и идентификации начального состояния для Guckenheimer and Holmes cycle автомата и free-running автомата над кольцом Z_{p^k}.

18. Охарактеризованы множества неподвижных точек о.-д. функций, реализуемых инициальным Guckenheimer and Holmes cycle автоматом и инициальным free-running автоматом над кольцом Z_{p^k}.

7. ЭЛЕМЕНТЫ КВАНТОВОЙ КРИПТОГРАФИИ

Интенсивная разработка теории квантовых алгоритмов (см. п.1.7), а также приложения этой теории к решению задач современной криптологии обосновывают актуальность исследования не только эффективности квантовых алгоритмов, но также исследование вычислительной стойкости квантовых алгоритмов, предназначенных для преобразования информации. Решение некоторых из таких задач представлено в настоящем разделе.

В п.7.1 исследуется квантовый алгоритм с оракулом, предназначенный для решения задачи идентификации булевой вектор-функции, являющейся модельной задачей современного криптоанализа. В п.7.2 исследуется вычислительная стойкость квантового протокола передачи ключа в предположении, что криптоаналитик может управлять как вероятностями выбора базисных векторов, предназначенных для измерения кубита, так и одновременным изменением базисов отправителя и адресата. В п.7.3 построен квантовый шифр, основанный на классическом квантовом алгоритме плотного кодирования. Показано, что этот шифр является вычислительно стойким, если секретный сеансовый ключ − последовательность, близкая к случайной последовательности.

Материал, представленный в настоящем разделе, основан на результатах, полученных в [28,167,174], а также на результатах, полученных в следующих трех работах, вышедших в последнее время и по этой причине не включенных в общий список литературы:

1. *Скобелев В.Г.* Введение в криптологию. – Донецк: Юго-Восток, 2008. – 176 с.
2. *Скобелев В.Г.* Анализ атак на квантовый протокол передачи ключа // Прикладная дискретная математика. – 2008. – № 2 (2). – С. 62-66.
3. *Скобелев В.Г.* Вычислительная стойкость квантовых алгоритмов преобразования информации. – Труды на CD IV Международной конференции «Параллельные вычисления и задачи управления (РФ, Москва, ИПУ РАН, 27-29 октября 2008 г.)» (PACO 2008). – М.: ИПУ РАН, 2008. – С. 1446-1461.

7.1. Идентификация булевой вектор-функции методами квантовых вычислений.

В п.1.6 (пример 1.8) задача идентификации булевой вектор-функции решена методами теории полей Галуа. Основная идея такого решения состоит в переходе от исследуемой булевой вектор-функции к булевой вектор-функции $\mathbf{f} \in (P_2^{(0)}(n))^m$, для которой множество

$$graph\,\mathbf{f} = \{(\alpha_1,\ldots,\alpha_{m+n}) \in \mathbf{E}^{n+m} \mid \mathbf{f}(\alpha_1,\ldots,\alpha_n) = (\alpha_{n+1},\ldots,\alpha_{n+m})\}$$

представляется в виде

$$graph\,\mathbf{f} = \bigcup_{\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})} \mathbf{V},$$

где $\mathbf{Lin}(graph\,\mathbf{f})$ $(\mathbf{f} \in P_2(n,m))$ множество всех максимальных по включению подпространств линейного пространства $\mathbf{E}^{n+m}$, содержащихся во множестве $graph\,\mathbf{f}$.

Таким образом, для любого множества $\mathbf{\Omega}$ $(\mathbf{\Omega} \subseteq \mathbf{E}^{n+m})$ проверка истинности включения

$$\mathbf{\Omega} \subseteq graph\,\mathbf{f} \tag{7.1}$$

сводится к проверке для каждого вектора $\mathbf{z} \in \mathbf{\Omega}$ следующего условия: «существует ли такое подпространство $\mathbf{V} \in \mathbf{Lin}(graph\,\mathbf{f})$, что $\mathbf{z} \in \mathbf{V}$?».

Такой подход к решению задачи идентификации булевой вектор-функции допускает следующую интерпретацию в терминах вычисления значений предикатов.

Пусть

$$\mathbf{Lin}(graph\,\mathbf{f}) = \{\mathbf{V}_1, \ldots, \mathbf{V}_s\},$$

а $\{\mathbf{k}_{i1}, \ldots, \mathbf{k}_{ir_i}\}$ $(i = 1, \ldots, s)$ – базис пространства $V_i^{\perp}$. Тогда предикат

$$h_1(\mathbf{z}) = \bigwedge_{i=1}^{s} \bigvee_{j=1}^{r_i} (\mathbf{k}_{ij} \circ \mathbf{z}) \quad (\mathbf{z} \in \mathbf{E}^{n+m})$$

обладает тем свойством, что

$$(\forall \mathbf{z} \in \mathbf{E}^{n+m})(h_1(\mathbf{z}) = 0 \Leftrightarrow \mathbf{z} \in graph\,\mathbf{f}).$$

Следовательно, предикат

$$h_2(\mathbf{z}) = \overline{h_1(\mathbf{z})} = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{r_i} \overline{\mathbf{k}_{ij} \circ \mathbf{z}} \quad (\mathbf{z} \in \mathbf{E}^{n+m}) \tag{7.2}$$

обладает тем свойством, что

$$(\forall \mathbf{z} \in \mathbf{E}^{n+m})(h_2(\mathbf{z}) = 1 \Leftrightarrow \mathbf{z} \in graph\,\mathbf{f}).$$

Положим

$$u_{ij} = \overline{\mathbf{k}_{ij} \circ \mathbf{z}} \quad (i = 1, \ldots, s;\ j = 1, \ldots, r_i)$$

и представим предикат (7.1) в виде

$$g(\mathbf{u}) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{r_i} u_{ij}, \tag{7.3}$$

где $\mathbf{u}$ – набор переменных $u_{ij} = \overline{\mathbf{k}_{ij} \circ \mathbf{z}}$ $(i = 1, \ldots, s;\ j = 1, \ldots, r_i)$.

Таким образом, задача определения принадлежности вектора $\mathbf{z} \in \mathbf{E}^{n+m}$ графику вектор-функции $\mathbf{f} \in (P_2^{(0)}(n))^m$ сводится к вычислению значения предиката (7.3), а именно:

$$(\forall \mathbf{z} \in \mathbf{E}^{n+m})(\mathbf{z} \in graph\,\mathbf{f} \Leftrightarrow g(\mathbf{u}) = 1).$$

Ясно, что метод проверки истинности включения (7.1) на основе такого подхода осуществляется с временной сложностью

$$T = O(|\mathbf{\Omega}| \cdot s \cdot r_{\max} \cdot (n+m)) \quad (n+m \to \infty). \tag{7.4}$$

где

$$r_{\max} = \max_{i \in \mathbf{N}_s} r_i.$$

Теперь рассмотрим решение задачи идентификации булевой вектор-функции методами квантовых вычислений.

Представим состояние системы из n кубитов в виде

$$|\psi\rangle = \sum_{k=0}^{2^n-1} a_k \cdot |k\rangle,$$

где $\{|0\rangle,|1\rangle,\ldots,|2^n-1\rangle\}$ – фиксированный базис пространства H_{2^n}, а a_k $(k=0,1,\ldots,2^n-1)$ – такие комплексные числа, что

$$\sum_{k=0}^{2^n-1} |a_k|^2 = 1.$$

Стандартный процесс вычисления значения булевой функции $f(x_1,\ldots,x_n)\in P_2(n)$ в терминах квантовой машины Тьюринга с оракулом состоит в применении к системе из n кубитов (первоначально находящейся в состоянии $|0\rangle\in\mathsf{H}_{2^n}$) последовательности унитарных преобразований

$$\Phi_0 \to Q \to \Phi_1 \to Q \to \ldots \to \Phi_{m-1} \to Q \to \Phi_m, \qquad (7.5)$$

и измерений, где оракул Q – это унитарное преобразование, определенное равенством

$$Q(|i\rangle \otimes |\alpha\rangle) = |i\rangle \otimes |\alpha \oplus x_i\rangle \quad (\alpha\in\mathbf{E}).$$

Значение, полученное при последнем измерении, представляет собой результат вычислений.

Известно, что для любых чисел $w\in\mathbf{N}$ и $v\in\mathbf{Z}_+$ $(v\le w)$, если

$$s = 2^{w-v}$$

и

$$r_i = 2^v \quad (i=1,\ldots,s),$$

а оракул Q представляет собой унитарное преобразование, определенное равенством

$$Q(|i\rangle \otimes |j\rangle \otimes |\alpha\rangle) = |i\rangle \otimes |j\rangle \otimes |\alpha \oplus u_{ij}\rangle \quad (\alpha\in\mathbf{E}), \qquad (7.6)$$

где $i=1,\ldots,2^{w-v}$ и $j=1,\ldots,2^v$, то квантовая машина Тьюринга с оракулом может вычислить значение предиката (7.3) с вероятностью ошибки ε посредством

$$\mathsf{T} = O(w\cdot\sqrt{2^w}) \quad (n+m\to\infty) \qquad (7.7)$$

вызовов оракула Q.

Такой метод вычисления значения предиката (7.3) основан на использовании алгоритма поиска Гровера [126,129,296] и состоит в следующем.

Вначале алгоритм Гровера применяется для построения оракула Q, который посредством

$$\mathsf{T} = O(w \cdot \sqrt{2^v}) \quad (n+m \to \infty)$$

вызовов оракула Q вычисляет значение любой конъюнкции

$$\bigwedge_{j=1}^{r_i} u_{ij} \quad (i = 1,\ldots,s)$$

с вероятностью ошибки $\varepsilon \cdot \sqrt{2^{-w+v}}$.

Затем алгоритм Гровера применяется для вычисления дизъюнкции s таких конъюнкций посредством

$$\mathsf{T} = O(\sqrt{2^{w-v}}) \quad (n+m \to \infty)$$

вызовов оракула Q.

Следующая теорема показывает, что этот метод применим для любых натуральных чисел s и r_i $(i = 1,\ldots,s)$.

Теорема 7.1. Существует квантовый алгоритм с оракулом A_g для вычисления значения предиката

$$g(\mathbf{u}) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{r_i} u_{ij}$$

с вероятностью ошибки ε посредством

$$\mathsf{T} = O(\sqrt{s \cdot r_{\max}} \cdot \log(s \cdot r_{\max})) \quad (n+m \to \infty) \tag{7.8}$$

вызовов оракула Q.

Доказательство. Дополним набор булевых переменных $\mathbf{u}$ до такого набора переменных $\mathbf{u}'$, что индексы пробегают значения до степеней двойки, а значение предиката g остается неизменным. С этой целью положим

$$v = \lceil \log r_{\max} \rceil, \tag{7.9}$$

$$w = \lceil \log s \rceil + \lceil \log r_{\max} \rceil \tag{7.10}$$

и

$$\tilde{u}_{ij} = \begin{cases} u_{ij}, & \textit{если } i \le s \ \textit{ и } \ j \le r_i \\ 1, & \textit{если } i \le s \ \textit{ и } \ j > r_i \\ 0, & \textit{если } i > s \end{cases}.$$

Ясно, что

$$g(\mathbf{u}) = g(\mathbf{u}').$$

Определим оракул $\tilde{Q}$ равенством

$$\tilde{Q}(|i\rangle \otimes |j\rangle \otimes |\alpha\rangle) = |i\rangle \otimes |j\rangle \otimes |\alpha \oplus \tilde{u}_{ij}\rangle \quad (\alpha \in \mathbf{E}),$$

где $i = 1,\ldots,2^{w-v}$ и $j = 1,\ldots,2^{v}$.

Модифицируем рассмотренный выше алгоритм вычисления значения предиката $g(\mathbf{u}')$ в соответствии со следующим правилом: если перед вызовом оракула $\tilde{Q}$:

1) истинно неравенство

$$i > s,$$

то вызов оракула $\tilde{Q}$ отменяется (т.е. применяется унитарный оператор, осуществляющий тождественное преобразование);

2) выполнено условие

$$(i \le s)\ \&\ (j > r_i),$$

то применяется преобразование

$$|i\rangle \otimes |j\rangle \otimes |\alpha\rangle \to |i\rangle \otimes |j\rangle \otimes |\alpha \oplus 1\rangle \quad (\alpha \in \mathbf{E});$$

3) выполнено условие

$$(i \le s)\ \&\ (j \le r_i),$$

то осуществляется вызов оракула $\tilde{Q}$ (т.е., по сути, вызов оракула Q).

Итак, построен квантовый алгоритм с оракулом A_g, который осуществляет вычисление значения предиката $g(\mathbf{u})$ с вероятностью ошибки ε, обращается только к оракулу Q, причем число вызовов оракула Q не превосходит величины, определенной формулой (7.7).

Подставив в (7.9) и (7.10) в (7.7), получим

$$\mathsf{T} = O((\lceil \log s \rceil + \lceil \log r_{\max} \rceil) \cdot \sqrt{2^{\lceil \log s \rceil + \lceil \log r_{\max} \rceil}}) \quad (n+m \to \infty),$$

т.е.

$$\mathsf{T} = O((\log s + \log r_{\max}) \cdot \sqrt{2^{\log s + \log r_{\max}}}) \quad (n+m \to \infty),$$

откуда и вытекает, что оценка (7.8) – истинная.

Теорема доказана.

Теорема 7.2. Емкостная и временная сложность квантового алгоритма с оракулом A_g равна, соответственно

$$V = O(\sum_{i=1}^{s} r_i \cdot (n+m)) = O(s \cdot r_{\max} \cdot (n+m)) \quad (n+m \to \infty). \qquad (7.11)$$

и

$$T = O(\sqrt{s \cdot r_{\max}} \cdot (n+m) \cdot \log^2 (s \cdot r_{\max})) \quad (n+m \to \infty). \qquad (7.12)$$

Доказательство. Емкостная сложность алгоритма A_g определяется объемом памяти, необходимой для хранения базисных векторов $\mathbf{k}_{ij}$ $(i=1,\ldots,s;\ j=1,\ldots,r_i)$, т.е.

$$V = O(\sum_{i=1}^{s} r_i \cdot (n+m)) \quad (n+m \to \infty). \tag{7.13}$$

Из (7.13) вытекает, что оценка (7.11) – истинная.

Оценим временную сложность алгоритма A_g.

Кроме количества обращений к оракулу необходимо учесть время вызова оракула Q (т.е. временную сложность преобразования (7.6)) и время выполнения унитарных операторов, не связанных с вызовом оракула.

Так как временная сложность доступа к базисному вектору $\mathbf{k}_{ij}$ $(i=1,\ldots,s;\ j=1,\ldots,r_i)$ по его индексам равна

$$T_1 = O(\log(s \cdot r_{\max})) \quad (n+m \to \infty),$$

а временная сложность вычисление скалярного произведения $\mathbf{k}_{ij} \circ \mathbf{z}$ равна

$$T_2 = O(n+m) \quad (n+m \to \infty),$$

то временная сложность вызова оракула Q равна

$$T_Q = O((n+m) \cdot \log(s \cdot r_{\max})) \quad (n+m \to \infty).$$

Анализ алгоритма Гровера показывает, что при поиске среди 2^w неупорядоченных элементов временная сложность шага, предваряющего вызов оракула (т.е. выполнения унитарного преобразования Φ_i $(i=0,1,\ldots m-1)$ в последовательности преобразований (7.5)) равна

$$T_3 = O(w) \quad (n+m \to \infty).$$

Для алгоритма A_g эта временная сложность увеличивается на время сравнения индексов i и s, а также на время сравнения индексов j и $r_{\max}$, т.е. на величину

$$T_4 = O(\lceil \log s \rceil + \lceil \log r_{\max} \rceil) \quad (n+m \to \infty). \tag{7.14}$$

Из (7.10) вытекает, что для алгоритма A_g временная сложность шага, предваряющего вызов оракула, определяется формулой (7.14), т.е. равна

$$T_5 = O(\log(s \cdot r_{\max})) \quad (n+m \to \infty).$$

Итак, алгоритм A_g осуществляет вычисление значения предиката $g(\mathbf{u})$ с вероятностью ошибки ε с временной сложностью

$$T = \mathsf{T} \cdot T_5 + (\mathsf{T}+1) \cdot T_Q \quad (n+m \to \infty),$$

т.е.

$$T = O(\sqrt{s \cdot r_{\max}} \cdot \log^2(s \cdot r_{\max}) +$$

$$+ (\sqrt{s \cdot r_{\max}} \cdot \log(s \cdot r_{\max}) + 1) \cdot (n+m) \cdot \log(s \cdot r_{\max})) \ \ (n+m \to \infty) \qquad (7.15)$$

Из (7.15) вытекает, что оценка (7.12) – истинная.

Теорема доказана.

Из теоремы 7.2 вытекает, что проверка истинности включения (7.1) с помощью квантового алгоритма с оракулом A_g осуществляется с временной сложностью

$$T = O(|\mathbf{\Omega}| \cdot \sqrt{s \cdot r_{\max}} \cdot (n+m) \cdot \log^2(s \cdot r_{\max})) \ \ (n+m \to \infty). \qquad (7.16)$$

Из (7.4) и (7.16) вытекает

Утверждение 7.1. Ускорение проверки истинности включения (7.1) с помощью квантового алгоритма с оракулом A_g по сравнению с проверкой истинности включения (7.1) с помощью обычного алгоритма, основанного на теории полей Галуа определяется величиной

$$O(\sqrt{s \cdot r_{\max}} \cdot \log^{-2}(s \cdot r_{\max})) \ \ (n+m \to \infty).$$

Теорема 7.3. Нижняя граница для числа запросов к оракулу, необходимых для вычисления предиката $g(\mathbf{u})$, равна

$$\mathsf{T}_l = \Omega(\sqrt{s \cdot r_{\min}}) \ \ (n+m \to \infty), \qquad (7.17)$$

где

$$r_{\min} = \min_{i \in \mathbf{N}_s} r_i.$$

Доказательство. Пусть $\mathbf{f} \in P_2(n,m)$, а $\mathbf{X}$ и $\mathbf{Y}$ – такие непустые подмножества множества $\mathbf{E}^n$, что

$$(\mathbf{x} \in \mathbf{X}) \,\&\, (\mathbf{y} \in \mathbf{Y}) \Rightarrow \mathbf{f}(\mathbf{x}) \neq \mathbf{f}(\mathbf{y}).$$

Предположим, что непустым является такое бинарное отношение

$$\omega \subseteq \mathbf{X} \times \mathbf{Y},$$

что:

1) для каждого $\mathbf{x} \in \mathbf{X}$ существует не менее m_1 таких элементов $\mathbf{y} \in \mathbf{Y}$, что $(\mathbf{x},\mathbf{y}) \in \omega$;

2) для каждого $\mathbf{y} \in \mathbf{Y}$ существует не менее m_2 таких элементов $\mathbf{x} \in \mathbf{X}$, что $(\mathbf{x},\mathbf{y}) \in \omega$;

3) для любых $\mathbf{x} \in \mathbf{X}$ и $i \in \mathbf{N}_n$ существует не более l_1 таких элементов $\mathbf{y} \in \mathbf{Y}$, что $(\mathbf{x},\mathbf{y}) \in \omega$ и $x_i \neq y_i$;

4) для любых $\mathbf{y} \in \mathbf{Y}$ и $i \in \mathbf{N}_n$ существует не более l_2 таких элементов $\mathbf{x} \in \mathbf{X}$, что $(\mathbf{x},\mathbf{y}) \in \omega$ и $x_i \neq y_i$.

Известно, что в этом случае любой квантовый алгоритм с оракулом, предназначенный для вычисления значений отображения $\mathbf{f}$, использует

$$\tilde{\mathsf{T}} = \Omega(\sqrt{m_1 \cdot m_2 \cdot l_1^{-1} \cdot l_2^{-1}}) \quad (n+m \to \infty) \tag{7.18}$$

запросов к оракулу.

Пусть $\mathbf{X}$ – непустое множество всех таких наборов $\mathbf{u}$, что для каждого $i \in \mathbf{N}_s$ существует такое единственное значение $j \in \mathbf{N}_{r_i}$, что $u_{ij} = 0$, а $\mathbf{Y}$ – непустое множество всех таких наборов $\mathbf{u}$, что существует такое единственное значение $i_0 \in \mathbf{N}_s$, что $u_{i_0 j} = 1$ для всех $j \in \mathbf{N}_{r_i}$, а для каждого $i \in \mathbf{N}_s \setminus \{ i_0 \}$ существует такое единственное значение $j \in \mathbf{N}_{r_i}$, что $u_{ij} = 0$.

Тогда

$$g(\mathbf{u}) = 0 \quad (\mathbf{u} \in \mathbf{X}),$$

так как если $\mathbf{u} \in \mathbf{X}$, то каждая конъюнкция в (7.3) равна нулю, и

$$g(\mathbf{u}) = 1 \quad (\mathbf{u} \in \mathbf{Y}),$$

так как i_0-я конъюнкция в (7.3) равна единице.

В качестве бинарного отношения ω выберем множество всех таких упорядоченных пар $(\mathbf{u}, \tilde{\mathbf{u}})$ $(\mathbf{u} \in \mathbf{X}, \tilde{\mathbf{u}} \in \mathbf{Y})$, что существует единственная такая пара индексов i и j, что

$$u_{ij} \neq \tilde{u}_{ij}.$$

Из построения множества $\mathbf{X}$ вытекает, что для каждого вектора $\mathbf{u} \in \mathbf{X}$ существует в точности s элементов u_{ij} равных нулю. Поочередно заменяя каждый из таких элементов u_{ij} единицей, получим s таких векторов $\tilde{\mathbf{u}} \in \mathbf{Y}$, что $(\mathbf{u}, \tilde{\mathbf{u}}) \in \omega$. Следовательно,

$$m_1 = s.$$

Из построения множества $\mathbf{Y}$ вытекает, что если в векторе $\tilde{\mathbf{u}} \in \mathbf{Y}$ поочередно заменять каждый из элементов $\tilde{u}_{i_0 j}$ нулем, то получим r_{i_0} таких векторов $\mathbf{u} \in \mathbf{X}$, что $(\mathbf{u}, \tilde{\mathbf{u}}) \in \omega$. Следовательно,

$$m_2 \geq r_{i_0} \geq r_{\min}.$$

Из построения бинарного отношения ω вытекает, что

$$l_1 = l_2 = 1.$$

Подставив найденные значения m_1, m_2, l_1 и l_2 в (7.18), получим (7.17).

Теорема доказана.

Таким образом, вопрос об оптимальности квантового алгоритма с оракулом A_g сводится к вопросу о возможности понижения оценки (7.8) до оценки (7.17).

7.2. Анализ атак на квантовый протокол передачи ключа.

Ранее было отмечено, что применение квантовых вычислений к решению задач криптологии обосновывает актуальность исследования вычислительной стойкости квантовых алгоритмов. При этом естественно возникает вопрос:

Что и как подвергается атаке?

Сложность ответа на этот вопрос состоит в том, что в настоящее время недостаточно проработана формальная модель квантового компьютера, а искажение передаваемой информации за счет ее измерения приводит к новым типам атак, представляющим собой симбиоз пассивных и активных атак [8].

Поэтому естественно исследовать вычислительную стойкость квантовых алгоритмов решения конкретных модельных задач криптологии.

Рассмотрим в качестве такой задачи классический квантовый протокол передачи ключа, предложенный и исследованный в [244,245].

Предполагается, что отправитель и адресат располагают квантовым и классическим каналами: квантовый канал применяется для передачи ключа последовательностью кубитов, а классический канал − для контроля вычислений (рис. 7.1).

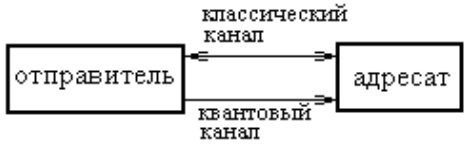


Рис. 7.1. Квантовая схема передачи ключа.

Обозначим через

$$B_j = \{\mathbf{e}_0^{(j)}, \mathbf{e}_1^{(j)}\} \quad (j = 0,1)$$

такие ортонормированные базисы пространства H_2, что

$$\mathbf{e}_i^{(1)} = 2^{-0.5} \cdot (\mathbf{e}_0^{(0)} + (-1)^{1+i} \mathbf{e}_1^{(0)}) \quad (i = 0,1).$$

Для того чтобы передать значение очередного бита, отправитель случайным образом выбирает базис B_j $(j = 0,1)$, измеряет кубит (представляющий собой случайным образом поляризованный фотон) в этом базисе и передает измеренный кубит адресату по квантовому каналу.

Для того чтобы принять значение очередного бита, адресат случайным образом выбирает базис B_j $(j = 0,1)$, а затем измеряет принятый кубит в этом базисе.

По завершению процесса передачи последовательности бит отправитель и адресат по классическому каналу сообщают друг другу, какие базисы были выбраны для кодирования и измерения каждого бита.

Те биты, при обработке которых отправитель и адресат использовали один и тот же базис, принимаются в качестве ключа, а остальные биты отбрасываются.

Доказано, что в среднем длина ключа составляет 50% длины переданной последовательности.

Классическая атака на этот протокол состоит в следующем.

Криптоаналитик перехватывает, измеряет передаваемые кубиты, а затем пересылает измеренные кубиты адресату. Кроме того, криптоаналитик имеет возможность прослушивать классический канал (рис. 7.2).

Рис. 7.2. Классическая атака на квантовый протокол передачи ключа.

Доказано, что в этом случае адресат в среднем верно измерит только 50% от длины ключа. Поэтому, сравнив по открытому каналу некоторое число бит ключа, отправитель и адресат с соответствующей вероятностью обнаружат наличие атаки.

Отметим, что (хотя об этом нигде явно не сказано) рассмотренный выше анализ атаки на квантовый протокол передачи ключа основан на предположении о том, что криптоаналитик и адресат при измерении кубита в базисе B_j $(j = 0,1)$ вычисляют его проекцию на один и тот же фиксированный базисный вектор.

Ослабим это предположение, а именно: будем считать, что только отправитель в процессе передачи значения i $(i = 0,1)$ бита, выбрав базис B_j $(j = 0,1)$, всегда конструирует проекцию передаваемого кубита на базисный вектор $\mathbf{e}_i^{(j)}$.

Рассмотренная выше атака на квантовый протокол передачи ключа предполагает, что в распоряжении криптоаналитика имеется минимум средств. Усилим эту атаку за счет следующих предположений:

Предположение 7.1. Для измерения перехваченного кубита в базисе B_j $(j = 0,1)$ криптоаналитик выбирает базисный вектор $\mathbf{e}_i^{(j)}$ $(i = 0,1)$ с вероятностью $p_1^{(j)}(i)$.

Предположение 7.2. Криптоаналитик определяет вероятность $p_2^{(j)}(i)$ $(i, j \in \{0,1\})$ выбора адресатом базисного вектора $\mathbf{e}_i^{(j)}$ при измерении кубита в базисе B_j, причем адресат не располагает информацией о том, что у него произошло изменение базисного вектора.

Предположение 7.3. Криптоаналитик может одновременно изменять у отправителя и адресата базис B_j $(j=0,1)$ на базис B_{1-j} с вероятностью $p_0(j)$, причем ни отправитель, ни адресат не располагают информацией о том, что у них произошло изменение базиса.

Таким образом, мы приходим к атаке на квантовый протокол передачи ключа, которая схематически представлена на рис. 7.3.

Рис. 7.3. Исследуемая атака на квантовый протокол передачи ключа.

Отметим, что из предположений 7.1 и 7.2 вытекает, что равенства

$$p_k^{(j)}(1-i)=1-p_k^{(j)}(i) \tag{7.19}$$

истинны для всех $i, j\in\{0,1\}$ и $k\in\{1,2\}$.

Исследуем вначале атаку на квантовый протокол передачи ключа, определяемую предположениями 7.1 и 7.2.

Обозначим через $P_{jhj}^{(i)}$ $(i,h,j\in\{0,1\})$ вероятность правильного считывания адресатом значения i бита при условии, что для данного кубита отправитель и адресат используют базис B_j, а криптоаналитик − базис B_h.

Теорема 7.4. Истинны равенства

$$P_{jjj}^{(i)}=1-p_2^{(j)}(i)+p_1^{(j)}(i)\cdot p_2^{(j)}(i)\ \ (j=0,1) \tag{7.20}$$

и

$$P_{j,1-j,j}^{(i)}=0.75-0.5\cdot p_2^{(j)}(i)\ \ (j=0,1). \tag{7.21}$$

Доказательство. Предположим, что при обработке очередного кубита отправитель, криптоаналитик и адресат используют один и тот же базис B_j $(j=0,1)$.

С использованием равенства (7.19) вычислим вероятности возможных элементарных событий, определяемых выбором криптоаналитиком и адресатом базисного вектора в базисе B_j $(j=0,1)$ (рис. 7.4).

Следовательно, если $j=0,1$, то

$$P_{jjj}^{(i)}=p_1^{(j)}(i)\cdot p_2^{(j)}(i)+p_1^{(j)}(i)-$$

$$- p_1^{(j)}(i) \cdot p_2^{(j)}(i) + (1 - p_1^{(j)}(i)) \cdot (1 - p_2^{(j)}(i)) =$$

$$= 1 - p_2^{(j)}(i) + p_1^{(j)}(i) \cdot p_2^{(j)}(i),$$

что и требовалось доказать.

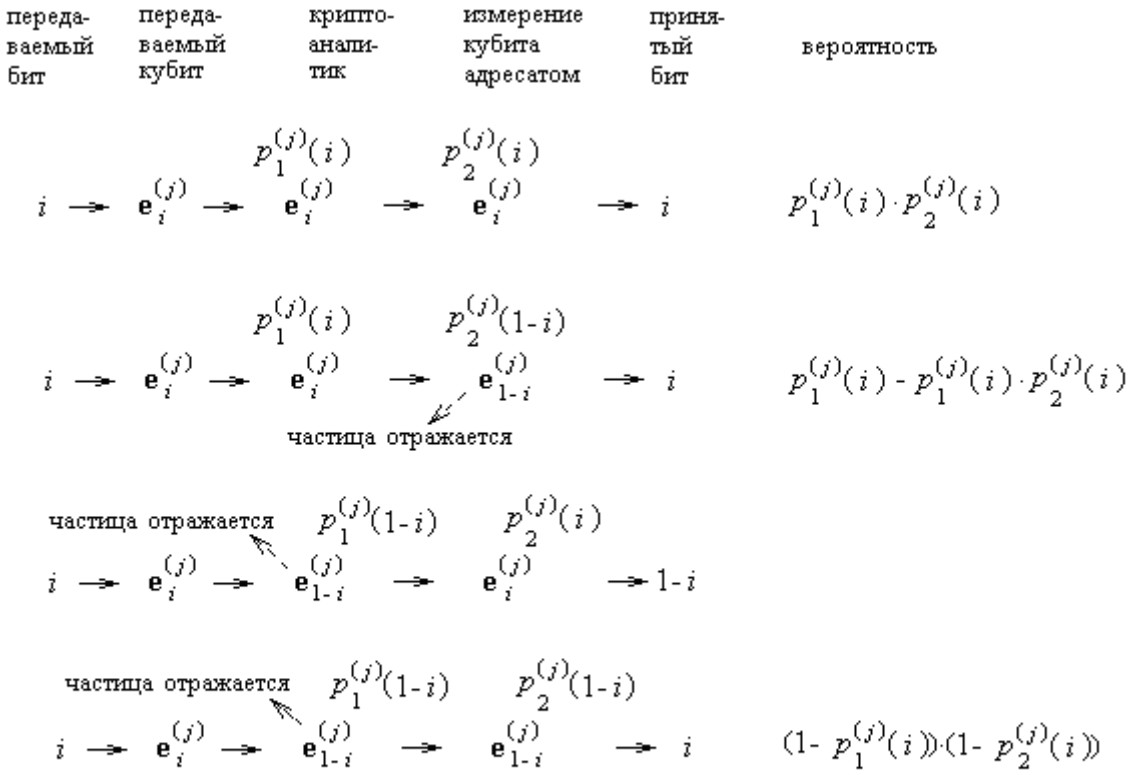


Рис. 7.4. Процесс передачи значения i $(i = 0, 1)$ бита при условии, что для кубита отправитель, криптоаналитик и адресат используют базис B_j $(j = 0, 1)$.

Предположим, что при обработке очередного кубита отправитель и адресат используют базис B_j $(j = 0,1)$, а криптоаналитик – базис B_{1-j}.

С использованием равенства (7.19) вычислим вероятности возможных элементарных событий, определяемых выбором адресатом базисного вектора в базисе B_j $(j = 0,1)$, а криптоаналитиком – базисного вектора в базисе B_{1-j} (рис. 7.5).

Следовательно, если $j = 0,1$, то

$$P_{j,1-j,j}^{(i)} = 0.25 \cdot p_1^{(1-j)}(i) \cdot p_2^{(j)}(i) + 0.75 \cdot p_1^{(1-j)}(i) \cdot (1 - p_2^{(j)}(i)) +$$

$$+ 0.25 \cdot (1 - p_1^{(1-j)}(i)) \cdot p_2^{(j)}(i) + 0.75 \cdot (1 - p_1^{(1-j)}(i)) \cdot (1 - p_2^{(j)}(i)) =$$

$$= 0.75 - 0.5 \cdot p_2^{(j)}(i).$$

Теорема доказана.

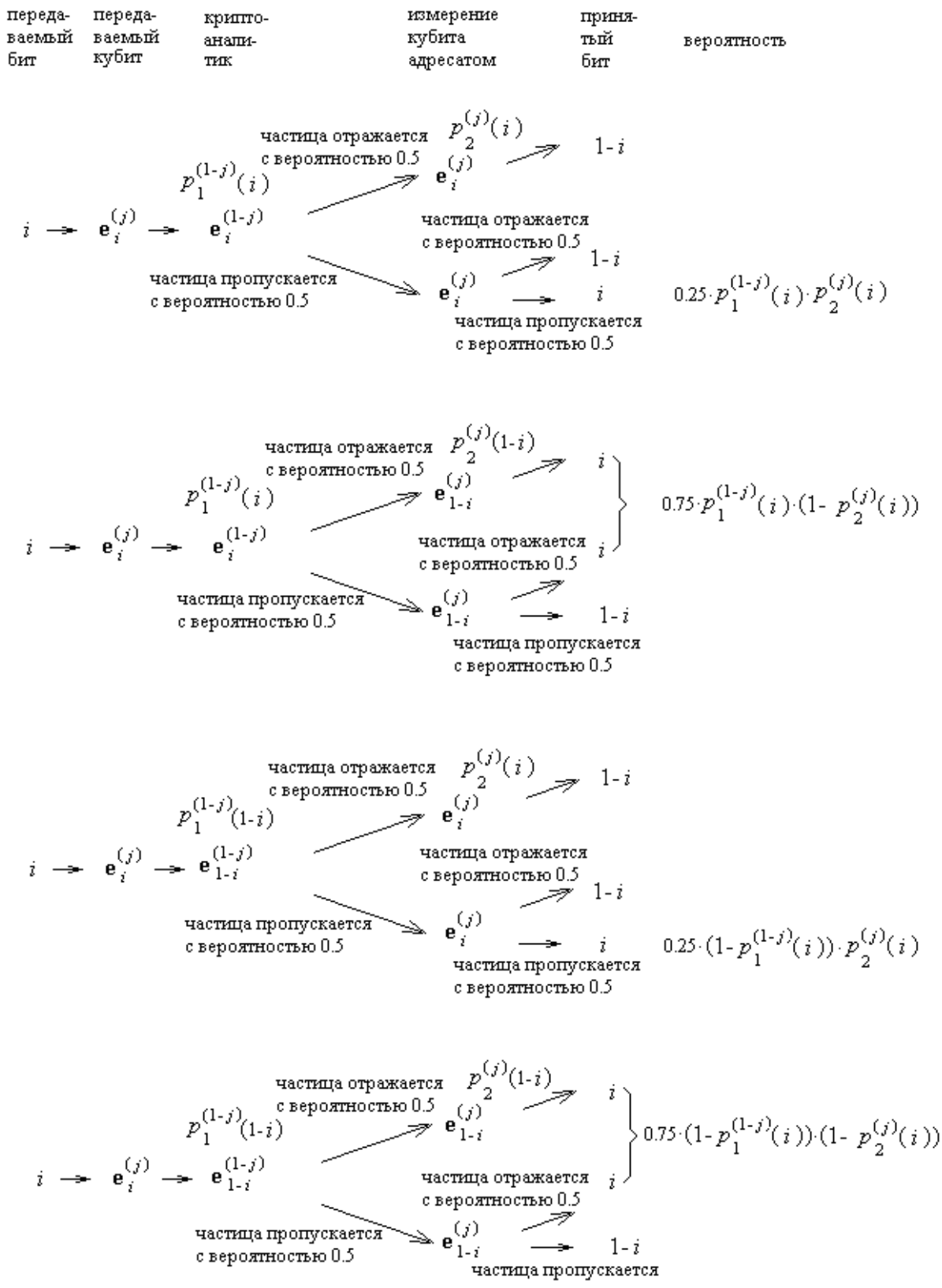


Рис. 7.5. Процесс передачи значения i ($i = 0,1$) при условии, что для данного кубита отправитель и адресат используют базис B_j ($j = 0,1$), а криптоаналитик – базис B_{1-j}.

Обозначим через $P_{jhj}(\alpha)$ $(j,h\in\{0,1\};\alpha\in[0;1])$ вероятность правильного считывания адресатом значения бита при условии, что для данного кубита отправитель и адресат используют базис B_j, криптоаналитик − базис B_{1-j}, а вероятность пересылки символа 0 отправителем равна α.

Теорема 7.5. Для всех $\alpha\in[0;1]$ истинны равенства

$$P_{jjj}(\alpha)=1-p_1^{(j)}(0)+p_1^{(j)}(0)\cdot p_2^{(j)}(0)+\alpha\cdot(p_1^{(j)}(0)-p_2^{(j)}(0))\ \ (j=0,1),\quad (7.22)$$

и

$$P_{j,1-j,j}(\alpha)=0.25+0.5\cdot\alpha+(0.5-\alpha)\cdot p_2^{(j)}(0)\ \ (j=0,1).\qquad (7.23)$$

Доказательство. Так как

$$P_{jjj}(\alpha)=\alpha\cdot P_{jjj}^{(0)}+(1-\alpha)\cdot P_{jjj}^{(1)}\ \ (j=0,1),$$

то, воспользовавшись равенствами (7.19) и (7.20), получим

$$P_{jjj}(\alpha)=\alpha\cdot(1-p_2^{(j)}(0)+p_1^{(j)}(0)\cdot p_2^{(j)}(0))+$$

$$+(1-\alpha)\cdot(p_2^{(j)}(0)+(1-p_1^{(j)}(0))\cdot(1-p_2^{(j)}(0)))=$$

$$=1-p_1^{(j)}(0)+p_1^{(j)}(0)\cdot p_2^{(j)}(0)+\alpha\cdot(p_1^{(j)}(0)-p_2^{(j)}(0))\ \ (j=0,1),$$

что и требовалось доказать.

Так как

$$P_{j,1-j,j}(\alpha)=\alpha\cdot P_{j,1-j,j}^{(0)}+(1-\alpha)\cdot P_{j,1-j,j}^{(1)}\ \ (j=0,1),$$

то, воспользовавшись равенствами (7.19) и (7.21), получим

$$P_{j,1-j,j}(\alpha)=\alpha\cdot(0.75-0.5\cdot p_2^{(j)}(0))+$$

$$+(1-\alpha)\cdot(0.75-0.5\cdot(1-p_2^{(j)}(0)))=$$

$$=\alpha\cdot(0.75-0.5\cdot p_2^{(j)}(0))+(1-\alpha)\cdot(0.25+0.5\cdot p_2^{(j)}(0))=$$

$$=0.25+0.5\cdot\alpha+(0.5-\alpha)\cdot p_2^{(j)}(0)\ \ (j=0,1).$$

Теорема доказана.

Отметим ряд следствий из равенства (7.22).

I. Пусть

$$p_2^{(j)}(0)=0.5\ \ (j=0,1).$$

Тогда

$$P_{jjj}(\alpha)=1-(0.5-\alpha)\cdot p_1^{(j)}(0)-0.5\cdot\alpha\ \ (j=0,1).\qquad (7.24)$$

При этом из (7.24) вытекает, что для всех $\alpha \in [0;1]$

$$P_{jjj}(\alpha) = \begin{cases} 1 - 0.5 \cdot \alpha, \ \textit{если} \ \ p_1^{(j)}(0) = 0 \\ 0.5 \cdot (1 + \alpha), \ \textit{если} \ \ p_1^{(j)}(0) = 1 \end{cases} \quad (j = 0,1).$$

II. Пусть

$$p_1^{(j)}(0) = p_2^{(j)}(0) = p^{(j)}(0) \quad (j = 0,1).$$

Тогда

$$P_{jjj}(\alpha) = 1 - p^{(j)}(0) + (p^{(j)}(0))^2 \quad (j = 0,1), \qquad (7.25)$$

т.е. вероятность $P_{jjj}(\alpha)$ не зависит от вероятности α.

Из (7.25) вытекает, что

$$P_{jjj}(\alpha) \in [0.75;1] \quad (j = 0,1)$$

для всех $p^{(j)}(0) \in [0;1]$, причем

$$P_{jjj}(\alpha) = \begin{cases} 0.75, \ \textit{если} \ \ p^{(j)}(0) = 0.5 \\ 1, \quad \textit{если} \ \ p^{(j)}(0) \in \{0;1\} \end{cases} \quad (j = 0,1).$$

III. Пусть

$$p_1^{(j)}(0) \neq p_2^{(j)}(0) \quad (j = 0,1).$$

Тогда:

1) для области значений вероятности $P_{jjj}(\alpha)$ $(j \in \{0,1\})$, как функции от вероятности α, истинно равенство

$$Val\ P_{jjj}(\alpha) = [l_1; L_1] \quad (j = 0,1),$$

где для всех значений $j = 0,1$

$$l_1 = \min\{1 - p_1^{(j)}(0) + p_1^{(j)}(0) \cdot p_2^{(j)}(0); 1 - p_2^{(j)}(0) + p_1^{(j)}(0) \cdot p_2^{(j)}(0)\} \qquad (7.26)$$

и

$$L_1 = \max\{1 - p_1^{(j)}(0) + p_1^{(j)}(0) \cdot p_2^{(j)}(0); 1 - p_2^{(j)}(0) + p_1^{(j)}(0) \cdot p_2^{(j)}(0)\}; \quad (7.27)$$

2) из (7.26) и (7.27) вытекает, что для всех значений $\alpha \in [0;1]$ если либо

$$\begin{cases} p_1^{(j)}(0) \to 0 \\ p_2^{(j)}(0) \to 0 \end{cases} \quad (j = 0,1),$$

либо

$$\begin{cases} p_1^{(j)}(0) \to 1 \\ p_2^{(j)}(0) \to 1 \end{cases} \quad (j = 0,1),$$

то

$$\begin{cases} l_1 \to 1 \\ L_1 \to 1 \end{cases},$$

т.е. для всех значений $\alpha \in [0;1]$

$$P_{jjj}(\alpha) \to 1 \quad (j = 0,1);$$

3) вероятность $P_{jjj}(\alpha)$ $(j = 0,1)$ − монотонная функция от вероятности α, причем $P_{jjj}(\alpha)$ монотонно возрастает, если

$$p_1^{(j)}(0) > p_2^{(j)}(0)$$

и монотонно убывает, если

$$p_1^{(j)}(0) < p_2^{(j)}(0);$$

4) если

$$\begin{cases} p_1^{(j)}(0) \to 1 \\ p_2^{(j)}(0) \to 0 \end{cases} \quad (j = 0,1),$$

то для всех значений $\alpha \in [0;1]$

$$P_{jjj}(\alpha) \to \alpha \quad (j = 0,1);$$

5) если

$$\begin{cases} p_1^{(j)}(0) \to 0 \\ p_2^{(j)}(0) \to 1 \end{cases} \quad (j = 0,1),$$

то для всех значений $\alpha \in [0;1]$

$$P_{jjj}(\alpha) \to 1 - \alpha \quad (j = 0,1).$$

Отметим ряд следствий из равенства (7.23).

I. Вероятность $P_{j,1-j,j}(\alpha)$ $(j = 0,1)$ не зависит от вероятности выбора криптоаналитиком базисного вектора в базисе B_{1-j} для измерения перехваченного кубита.

II. Для всех $\alpha \in [0;1]$

$$P_{j,1-j,j}(\alpha) = \begin{cases} 0.25 + 0.5 \cdot \alpha, \ \textit{если} \ \ p_2^{(j)}(0) = 0 \\ 0.75 - 0.5 \cdot \alpha, \ \textit{если} \ \ p_2^{(j)}(0) = 1 \end{cases} \quad (j = 0,1).$$

III. Пусть

$$p_2^{(j)}(0) = 0.5.$$

Тогда

$$P_{j,1-j,j}(\alpha) = 0.5 \quad (j = 0,1),$$

т.е. вероятность $P_{j,1-j,j}(\alpha)$ не зависит от вероятности α.

IV.Пусть

$$p_2^{(j)}(0) \neq 0.5.$$

Тогда:

1) для области значений вероятности $P_{j,1-j,j}(\alpha)$ $(j = 0,1)$, как функции от вероятности α, истинно равенство

$$Val\ P_{j,1-j,j}(\alpha) = [l_2; L_2] \quad (j = 0,1),$$

где для всех значений $j = 0,1$

$$l_2 = \min\{0.25 + 0.5 \cdot p_2^{(j)}(0); 0.75 - 0.5 \cdot p_2^{(j)}(0)\}, \tag{7.28}$$

и

$$L_2 = \max\{0.25 + 0.5 \cdot p_2^{(j)}(0); 0.75 - 0.5 \cdot p_2^{(j)}(0)\}; \tag{7.29}$$

2) вероятность $P_{j,1-j,j}(\alpha)$ $(j = 0,1)$ − монотонная функция от вероятности α, причем $P_{j,1-j,j}(\alpha)$ монотонно возрастает, если

$$p_2^{(j)}(0) < 0.5$$

и монотонно убывает, если

$$p_2^{(j)}(0) > 0.5;$$

3) из (7.28) и (7.29) вытекает, что для всех значений $\alpha \in [0;1]$, если

$$p_2^{(j)}(0) \to 0.5,$$

то

$$\begin{cases} l_2 \to 0.5 \\ L_2 \to 0.5 \end{cases},$$

т.е.

$$P_{j,1-j,j}(\alpha) \to 0.5 \quad (j = 0,1).$$

Обозначим через $P_1(\alpha)$ $(\alpha \in [0;1])$ вероятность правильного считывания адресатом значения бита при условии, что для обработки данного кубита отправитель и адресат используют один и тот же базис, а вероятность пересылки символа 0 отправителем равна α.

Теорема 7.6. Для всех $\alpha \in [0;1]$ истинно равенство

$$P_1(\alpha) = 0.25 \cdot (2.5 + \alpha - (1-\alpha) \cdot (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ (0.5 - 2 \cdot \alpha) \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0)). \tag{7.30}$$

Доказательство. Так как

$$P_1(\alpha) = 0.25 \cdot (P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha)),$$

то, воспользовавшись равенствами (7.22) и (7.23), получим

$$P_1(\alpha) = 0.25 \cdot (1 - p_1^{(0)}(0) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + \alpha \cdot (p_1^{(0)}(0) - p_2^{(0)}(0)) +$$

$$+ 1 - p_1^{(1)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0) + \alpha \cdot (p_1^{(1)}(0) - p_2^{(1)}(0)) +$$

$$+ 0.25 + 0.5 \cdot \alpha + (0.5 - \alpha) \cdot p_2^{(0)}(0) +$$

$$+ 0.25 + 0.5 \cdot \alpha + (0.5 - \alpha) \cdot p_2^{(1)}(0)) =$$

$$= 0.25 \cdot (2.5 + \alpha - (1 - \alpha) \cdot (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ (0.5 - 2 \cdot \alpha) \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0)).$$

Теорема доказана.

Отметим ряд следствий из равенства (7.30).

I. Вероятность $P_1(\alpha)$, как функция от вероятности α:

1) является монотонно возрастающей функцией, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) < 0.5 \cdot (1 + p_1^{(0)}(0) + p_1^{(1)}(0)),$$

причем

$$Val\ P_1(\alpha) = [l_3; L_3],$$

где

$$l_3 = 0.25 \cdot (2.5 - (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ 0.5 \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0))$$

и

$$L_3 = 0.25 \cdot (3.5 - 1.5 \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0));$$

2) является монотонно убывающей функцией, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) > 0.5 \cdot (1 + p_1^{(0)}(0) + p_1^{(1)}(0)),$$

причем

$$Val\ P_1(\alpha) = [l_4; L_4],$$

где

$$l_4 = 0.25 \cdot (3.5 - 1.5 \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0))$$

и

$$L_4 = 0.25 \cdot (2.5 - (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ 0.5 \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0));$$

3) не зависит от значения α, если

$$p_2^{(0)}(0) + p_2^{(1)}(0) = 0.5 \cdot (1 + p_1^{(0)}(0) + p_1^{(1)}(0)), \qquad (7.31)$$

причем

$$P_1(\alpha) = 0.25 \cdot (2.75 - 0.75 \cdot (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0)) \qquad (7.32)$$

для всех $\alpha \in [0;1]$.

II. Если для всех значений $j = 0,1$

$$\begin{cases} p_1^{(j)}(0) \to 0 \\ p_2^{(j)}(0) \to 0 \end{cases},$$

то

$$P_1(\alpha) \to 0.625 + 0.250 \cdot \alpha,$$

причем:

1) если $\alpha \to 0$, то

$$P_1(\alpha) \to 0.625;$$

2) если $\alpha \to 0.5$, то

$$P_1(\alpha) \to 0.750;$$

3) если $\alpha \to 1$, то

$$P_1(\alpha) \to 0.875.$$

III. Если для всех значений $j = 0,1$

$$\begin{cases} p_1^{(j)}(0) \to 1 \\ p_2^{(j)}(0) \to 0 \end{cases},$$

то

$$P_1(\alpha) \to 0.125 + 0.750 \cdot \alpha,$$

причем:

1) если $\alpha \to 0$, то

$$P_1(\alpha) \to 0.125;$$

2) если $\alpha \to 0.5$, то

$$P_1(\alpha) \to 0.500;$$

3) если $\alpha \to 1$, то

$$P_1(\alpha) \to 0.875.$$

IV. Если для всех значений $j = 0,1$

$$\begin{cases} p_1^{(j)}(0) \to 1 \\ p_2^{(j)}(0) \to 1 \end{cases},$$

то

$$P_1(\alpha) \to 0.875 - 0.250 \cdot \alpha,$$

причем:

1) если $\alpha \to 0$, то

$$P_1(\alpha) \to 0.875;$$

2) если $\alpha \to 0.5$, то

$$P_1(\alpha) \to 0.750;$$

3) если $\alpha \to 1$, то

$$P_1(\alpha) \to 0.625.$$

V. Если для всех значений $j = 0,1$

$$\begin{cases} p_1^{(j)}(0) \to 0.5 \\ p_2^{(j)}(0) \to 0.5 \end{cases},$$

то

$$P_1(\alpha) = 0.625.$$

Проведенный анализ показывает, что из теоремы 7.6 вытекает

Следствие 7.1. При атаке, определяемой предположениями 7.1 и 7.2, если криптоаналитик располагает информацией о том, какое из утверждений «$\alpha \in (0\,;0.5)$» или «$\alpha \in (0.5\,;1)$» истинно, то он всегда может выбрать свою стратегию так, что:

1) в среднем приблизительно 75% ключа будет передано адресату верно, если генератор последовательностей, используемый отправителем, близок к псевдослучайному генератору;

2) в среднем приблизительно 87.5% ключа может быть передано адресату верно, если генератор последовательностей, используемый отправителем, далек от псевдослучайного генератора.

Теорема 7.7. При атаке, определяемой предположениями 7.1 и 7.2, существует по крайней мере два связных континуальных множеств таких стратегий криптоаналитика, что при любом значении $\alpha \in [0;1]$ в среднем 68.75% ключа будет передано адресату верно.

Доказательство. Положив в (7.31)

$$p_1^{(0)}(0) = p_1^{(1)}(0) = 1,$$

получим

$$p_2^{(0)}(0) + p_2^{(1)}(0) = 1.5.$$

Следовательно, любая такая стратегия криптоаналитика, что

$$\begin{cases} p_1^{(0)}(0) = p_1^{(1)}(0) = 1 \\ p_2^{(0)}(0) + p_2^{(1)}(0) = 1.5 \end{cases} \tag{7.33}$$

удовлетворяет равенству (7.31).

Подставив (7.33) в (7.32), получим

$$P_1(\alpha) = 0.25 \cdot (2.75 - 0.75 \cdot 2 + 1.5) = 0.6875$$

для всех $\alpha \in [0;1]$.

Положив в (7.31)

$$p_1^{(0)}(0) = p_1^{(1)}(0) = 0,$$

получим

$$p_2^{(0)}(0) + p_2^{(1)}(0) = 0.5.$$

Следовательно, любая такая стратегия криптоаналитика, что

$$\begin{cases} p_1^{(0)}(0) = p_1^{(1)}(0) = 0 \\ p_2^{(0)}(0) + p_2^{(1)}(0) = 0.5 \end{cases} \tag{7.34}$$

удовлетворяет равенству (7.31).

Подставив (7.34) в (7.32), получим

$$P_1(\alpha) = 0.25 \cdot 2.75 = 0.6875$$

для всех $\alpha \in [0;1]$.

Множества (7.33) и (7.34) представляют собой два таких связные континуальных множества стратегий криптоаналитика, что при любом значении $\alpha \in [0;1]$ в среднем $68.75\,\%$ ключа будет передано адресату верно.

Теорема доказана.

Рассмотрим теперь атаку на квантовый протокол передачи ключа, определяемую предположениями 7.1-7.3.

Обозначим через $P_2(\alpha)$ $(\alpha \in [0;1])$ вероятность правильного считывания адресатом значения бита при условии, что при обработке данного кубита отправитель и адресат используют один и тот же базис B_j $(j = 0,1)$, вероятность пересылки символа 0 отправителем равна α, а вероятность одновременного изменения криптоаналитиком как у отправителя, так и у адресата базиса B_j $(j = 0,1)$ на базис B_{1-j} равна $p_0(j)$.

Теорема 7.8. Для всех $\alpha \in [0;1]$ истинно равенство

$$P_2(\alpha) = 0.25 \cdot (P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha) +$$

$$+ (p_0(1) - p_0(0)) \cdot (P_{000}(\alpha) + P_{010}(\alpha) - P_{101}(\alpha) - P_{111}(\alpha))). \qquad (7.35)$$

Доказательство. Если при обработке очередного кубита отправитель и адресат считают, что они используют один и тот же базис B_j $(j = 0,1)$, а криптоаналитик использует базис B_h $(h = 0,1)$, то при атаке, определяемой предположениями 7.1-7.3, вероятность правильного считывания адресатом значения бита равна

$$(1 - p_0(j)) \cdot P_{jhj}(\alpha) + p_0(j) \cdot P_{1-j,h,1-j}(\alpha)$$

для всех $\alpha \in [0;1]$.

Следовательно, для всех $\alpha \in [0;1]$

$$P_2(\alpha) = 0.25 \cdot (\sum_{j=0}^{1}\sum_{h=0}^{1}(1 - p_0(j)) \cdot P_{jhj}(\alpha) + p_0(j) \cdot P_{1-j,h,1-j}(\alpha)) =$$

$$= 0.25 \cdot ((1 - p_0(0)) \cdot P_{000}(\alpha) + p_0(0) \cdot P_{101}(\alpha) +$$

$$+ (1 - p_0(0)) \cdot P_{010}(\alpha) + p_0(0) \cdot P_{111}(\alpha) +$$

$$+ (1 - p_0(1)) \cdot P_{101}(\alpha) + p_0(1) \cdot P_{000}(\alpha) +$$

$$+ (1 - p_0(1)) \cdot P_{111}(\alpha) + p_0(1) \cdot P_{010}(\alpha)) =$$

$$= 0.25 \cdot (P_{000}(\alpha) + P_{111}(\alpha) + P_{010}(\alpha) + P_{101}(\alpha) +$$

$$+ (p_0(1) - p_0(0)) \cdot (P_{000}(\alpha) + P_{010}(\alpha) - P_{101}(\alpha) - P_{111}(\alpha))).$$

Теорема доказана.

Из (7.35) вытекают

Следствие 7.2. Неравенство

$$P_2(\alpha) > P_1(\alpha) \quad (\alpha \in [0;1])$$

истинно тогда и только тогда, когда либо

$$\begin{cases} P_{000}(\alpha) + P_{010}(\alpha) - P_{101}(\alpha) - P_{111}(\alpha) < 0 \\ p_0(1) - p_0(0) < 0 \end{cases},$$

либо

$$\begin{cases} P_{000}(\alpha) + P_{010}(\alpha) - P_{101}(\alpha) - P_{111}(\alpha) > 0 \\ p_0(1) - p_0(0) > 0 \end{cases}.$$

Следствие 7.3. Равенство

$$P_2(\alpha) = P_1(\alpha) \ \ (\alpha \in [0;1])$$

истинно тогда и только тогда, когда

$$p_0(1) = p_0(0)$$

или, когда

$$P_{000}(\alpha) + P_{010}(\alpha) - P_{111}(\alpha) - P_{101}(\alpha) = 0.$$

Итак, показано, что дополнительная возможность криптоаналитика управлять одновременным изменением базисов отправителя и адресата может усилить его атаку на квантовый протокол передачи ключа.

Подставив (7.22) и (7.23) в (7.35), получим, что для всех $\alpha \in [0;1]$

$$P_2(\alpha) = 0.25 \cdot (2.5 + \alpha - (1-\alpha) \cdot (p_1^{(0)}(0) + p_1^{(1)}(0)) +$$

$$+ (0.5 - 2 \cdot \alpha) \cdot (p_2^{(0)}(0) + p_2^{(1)}(0)) + p_1^{(0)}(0) \cdot p_2^{(0)}(0) + p_1^{(1)}(0) \cdot p_2^{(1)}(0) +$$

$$+ (p_0(1) - p_0(0)) \cdot (p_1^{(0)}(0) \cdot p_2^{(0)}(0) - p_1^{(1)}(0) \cdot p_2^{(1)}(0) +$$

$$+ (\alpha - 1) \cdot (p_1^{(0)}(0) - p_1^{(1)}(0)) + (0.5 - 2 \cdot \alpha) \cdot (p_2^{(0)}(0) - p_2^{(1)}(0)))) \qquad (7.36)$$

Из (7.36) вытекает, что вероятность $P_2(\alpha)$ $(\alpha \in [0;1])$, как функция от вероятности α:

1) монотонно возрастает, если

$$1 + (1 + p_0(1) - p_0(0)) \cdot (p_1^{(0)}(0) - 2 \cdot p_2^{(0)}(0)) +$$

$$+ (1 - p_0(1) + p_0(0)) \cdot (p_1^{(1)}(0) - 2 \cdot p_2^{(1)}(0)) > 0;$$

2) монотонно убывает, если

$$1 + (1 + p_0(1) - p_0(0)) \cdot (p_1^{(0)}(0) - 2 \cdot p_2^{(0)}(0)) +$$

$$+ (1 - p_0(1) + p_0(0)) \cdot (p_1^{(1)}(0) - 2 \cdot p_2^{(1)}(0)) < 0.$$

Таким образом, если в процессе передачи ключа отправитель управляет вероятностью α пересылки символа 0, а криптоаналитику известен этот

закон управления, то криптоаналитик располагает возможностью подобрать адаптивную стратегию атаки на квантовый протокол передачи ключа, определяемой предположениями 7.1-7.3, направленную либо на максимизацию, либо на минимизацию количества правильно прочитанных адресатом символов.

Подводя итог всему сказанному выше, заключаем, что атака на квантовый протокол передачи ключа, определяемая предположениями 7.1-7.3, может существенно усложнить работу легальных пользователей.

7.3. Шифр на основе квантового алгоритма плотного кодирования.

Задача плотного кодирования [296] состоит в том, что отправитель должен переслать адресату 2-х битовую последовательность

$$\alpha_1\alpha_2$$

используя систему из двух кубитов

$$|\psi\rangle = 2^{-0.5}\cdot(|00\rangle + |11\rangle).$$

При этом первый кубит находится у отправителя, а второй кубит − у адресата.

Алгоритм плотного кодирования состоит в следующем.

В зависимости от значения передаваемой последовательности

$$\alpha_1\alpha_2 \quad (\alpha_1,\alpha_2 \in \mathbf{E})$$

отправитель выполняет над своим кубитом унитарное преобразование

$$U_{\alpha_1\alpha_2} \quad (\alpha_1,\alpha_2 \in \mathbf{E})$$

а, следовательно, над системой $|\psi\rangle$ выполняется такое унитарное преобразование

$$U_{\alpha_1\alpha_2} \otimes I \quad (\alpha_1,\alpha_2 \in \mathbf{E}),$$

где через $\otimes$ обозначено тензорное произведение, а через I − тождественное преобразование, что

$$U_{00} = I,$$

$$U_{01} = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$U_{10} = Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$U_{11} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

После этого отправитель пересылает по квантовому каналу свой кубит адресату.

Адресат применяет к системе кубитов унитарное преобразование

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

измеряет второй кубит, применяет к первому кубиту преобразование Адамара

$$H = \begin{pmatrix} 2^{-0.5} & 2^{-0.5} \\ 2^{-0.5} & -2^{-0.5} \end{pmatrix},$$

а затем измеряет первый кубит.

Декодирование адресатом переданной 2-х битовой последовательности осуществляется в соответствии со следующей схемой

$$\begin{cases} |00\rangle \to 00 \\ |01\rangle \to 01 \\ |10\rangle \to 11 \\ |11\rangle \to 10 \end{cases}. \qquad (7.37)$$

Теорема 7.9. Алгоритм плотного кодирования остается корректным, если исходная система из двух кубитов имеет вид

$$|\xi\rangle = 2^{-0.5} \cdot (|01\rangle + |10\rangle).$$

При этом схема декодирования адресатом переданной 2-х битовой последовательности имеет вид

$$\begin{cases} |00\rangle \to 01 \\ |01\rangle \to 00 \\ |10\rangle \to 10 \\ |11\rangle \to 11 \end{cases}. \qquad (7.38)$$

Доказательство. В соответствии с алгоритмом плотного кодирования после применения отправителем унитарного преобразования к первому кубиту, получим

$$(U_{00} \otimes I)(|\xi\rangle) = (I \otimes I)(|\xi\rangle) = 2^{-0.5} \cdot (|01\rangle + |10\rangle),$$

$$(U_{01} \otimes I)(|\xi\rangle) = (X \otimes I)(|\xi\rangle) =$$

$$= 2^{-0.5} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 2^{-0.5} \cdot (|00\rangle + |11\rangle),$$

$$(U_{10} \otimes I)(|\xi\rangle) = (Y \otimes I)(|\xi\rangle) =$$

$$= 2^{-0.5} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = 2^{-0.5} \cdot (|00\rangle - |11\rangle),$$

$$(U_{11} \otimes I)(|\xi\rangle) = (Z \otimes I)(|\xi\rangle) =$$

$$= 2^{-0.5} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot (|01\rangle - |10\rangle).$$

После того, как отправитель перешлет по квантовому каналу свой кубит адресату, а адресат применит к системе кубитов унитарное преобразование C_{not}, получим

$$C_{not}(2^{-0.5} \cdot (|01\rangle + |10\rangle)) =$$

$$= 2^{-0.5} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 2^{-0.5} \cdot (|01\rangle + |11\rangle),$$

$$C_{not}(2^{-0.5} \cdot (|00\rangle + |11\rangle)) =$$

$$= 2^{-0.5} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 2^{-0.5} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 2^{-0.5} \cdot (|00\rangle + |10\rangle),$$

$$C_{not}(2^{-0.5}\cdot(|00\rangle+|11\rangle))=$$

$$=2^{-0.5}\cdot\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}=2^{-0.5}\cdot\begin{pmatrix}1\\0\\-1\\0\end{pmatrix}=2^{-0.5}\cdot(|00\rangle-|10\rangle),$$

$$C_{not}(2^{-0.5}\cdot(|00\rangle+|11\rangle))=$$

$$=2^{-0.5}\cdot\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\cdot\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}=2^{-0.5}\cdot\begin{pmatrix}0\\1\\0\\-1\end{pmatrix}=2^{-0.5}\cdot(|01\rangle-|11\rangle).$$

После измерения второго кубита адресат получит:

1) если результат измерения равен $|1\rangle$, то переданная последовательность 00 или 11;

2) если результат измерения равен $|0\rangle$, то переданная последовательность 01 или 10.

Таким образом, различимость исходных двоичных последовательностей после измерения второго кубита определяется разбиением

$$\pi_1=\{\overline{00,11};\overline{01,10}\}.$$

После применения к первому кубиту преобразование Адамара, получим

$$H(2^{-0.5}\cdot(|0\rangle+|1\rangle))=2^{-1}\cdot\begin{pmatrix}1&1\\1&-1\end{pmatrix}\cdot\begin{pmatrix}1\\1\end{pmatrix}=2^{-1}\cdot\begin{pmatrix}2\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0\rangle$$

и

$$H(2^{-0.5}\cdot(|0\rangle-|1\rangle))=2^{-1}\cdot\begin{pmatrix}1&1\\1&-1\end{pmatrix}\cdot\begin{pmatrix}1\\-1\end{pmatrix}=2^{-1}\cdot\begin{pmatrix}0\\2\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1\rangle.$$

После измерения первого кубита адресат получит:

1) если результат измерения равен $|0\rangle$, то переданная последовательность 00 или 01;

2) если результат измерения равен $|1\rangle$, то переданная последовательность 10 или 11.

Таким образом, различимость исходных двоичных последовательностей после измерения первого кубита определяется разбиением

$$\pi_2=\{\overline{00,01};\overline{10,11}\}.$$

Так как

$$\pi_1 \cdot \pi_2 = \{\overline{00}; \overline{01}; \overline{10}; \overline{11}\},$$

то в результате измерения адресатом кубитов переданная исходная двоичная последовательность идентифицируется единственным образом.

При этом схема декодирования результатов измерения адресатом кубитов определяется равенством (7.38).

Теорема доказана.

Из теоремы 7.9 вытекает корректность следующего алгоритма $C_{кв}$ шифрования $2 \cdot n$-битовой последовательности

$$\alpha_1 \alpha_2 \alpha_3 \alpha_4 \ldots \alpha_{2n-1} \alpha_{2n}$$

посредством системы из $2 \cdot n$ кубитов.

Пусть n-битовая последовательность

$$\beta_1 \ldots \beta_n$$

представляет собой секретный сеансовый ключ, имеющийся и у отправителя, и у адресата.

Отправитель подготавливает исходную систему из $2 \cdot n$ кубитов, имеющую вид

$$\chi_{2n} = \zeta_1 \otimes \ldots \otimes \zeta_n,$$

где

$$\zeta_i = \begin{cases} \psi, \ если \ \beta_i = 0 \\ \xi, \ если \ \beta_i = 1 \end{cases} \quad (i = 1, \ldots, n).$$

По квантовому каналу отправитель пересылает адресату кубиты с четными номерами.

После этого отправитель преобразует каждый кубит с нечетным номером в соответствии с алгоритмом плотного кодирования, а затем пересылает преобразованные кубиты адресату.

Адресат, получив кубиты от отправителя, компонует пары соответствующих кубитов, а затем обрабатывает каждую пару в соответствии с алгоритмом плотного кодирования.

Исследуем вычислительную стойкость шифра $C_{кв}$ при атаке на квантовый канал, состоящей в том, что криптоаналитик, представившись адресатом, перехватывает кубиты, пересылаемые отправителем.

Из (7.37) и (7.38) вытекает, что если криптоаналитик выбрал не ту схему декодирования, то он правильно расшифровывает бит с нечетным номером и неправильно расшифровывает бит с четным номером.

Обозначим через $p_i \in [0,1]$ $(i = 1,\ldots,n)$ вероятность того, что в процессе передачи $2 \cdot n$-битовой последовательности

$$\alpha_1\alpha_2\alpha_3\alpha_4 \ldots \alpha_{2n-1}\alpha_{2n},$$

зашифрованной с помощью шифра $C_{кв}$, криптоаналитик правильно определяет i-й бит секретного сеансового ключа

$$\beta_1 \ldots \beta_n.$$

Теорема 7.10. Вероятность $P_{2\cdot n,k}(p_1,\ldots,p_n)$ $(k = 0,1,\ldots,n)$ того, что в процессе расшифровки $2 \cdot n$-битовой последовательности, зашифрованной посредством шифра $C_{кв}$, криптоаналитик получит последовательность, отстоящую от исходной последовательности на расстоянии k $(0 \le k \le n)$ по Хеммингу, равна

$$P_{2\cdot n,k}(p_1,\ldots,p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} r_1 \cdot \ldots \cdot r_n \quad (k = 0,1,\ldots,n), \tag{7.39}$$

где

$$r_i = \begin{cases} 1 - p_i, \ \textit{если} \ i \in \{i_1,\ldots,i_k\} \\ p_i, \ \textit{если} \ i \notin \{i_1,\ldots,i_k\} \end{cases}. \tag{7.40}$$

Доказательство. Результат расшифровки криптоаналитиком $2 \cdot n$-битовой последовательности, зашифрованной посредством шифра $C_{кв}$, отстоит от исходной последовательности на расстоянии k $(0 \le k \le n)$ по Хеммингу тогда и только тогда, когда криптоаналитик неправильно определяет в точности k бит секретного сеансового ключа

$$\beta_1 \ldots \beta_n.$$

Вероятность того, что криптоаналитик неправильно определяет биты секретного ключа, имеющие номера $i_1,\ldots,i_k$ $(1 \le i_1 < \ldots < i_k \le n)$, и правильно определяет биты секретного ключа, имеющие номера, принадлежащие множеству $\mathbf{N}_n \setminus \{i_1,\ldots,i_k\}$ равна

$$r_1 \cdot \ldots \cdot r_n,$$

где r_i $(i = 1,\ldots,n)$ определяется в соответствии с (7.40).

Следовательно,

$$P_{2\cdot n,k}(p_1,\ldots,p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} r_1 \cdot \ldots \cdot r_n \quad (k = 0,1,\ldots,n).$$

Теорема доказана.

Для всех $p \in [0,1]$ положим

$$\mathrm{P}_{2\cdot n,k}(p) = P_{2\cdot n,k}(\underbrace{p,\ldots,p}_{n \ раз}) \quad (0 \le k \le n). \tag{7.41}$$

Следствие 7.4. Для всех $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ истинны равенства

$$\mathrm{P}_{2\cdot n,k}(p) = \binom{n}{k} \cdot (1-p)^k \cdot p^{n-k} \quad (0 \le k \le n). \tag{7.42}$$

Доказательство. Подставив

$$p_1 = \ldots = p_n = p$$

в (7.40), получим

$$r_i = \begin{cases} 1-p, \ \textit{если} \ i \in \{i_1,\ldots,i_k\} \\ p, \ \textit{если} \ i \notin \{i_1,\ldots,i_k\} \end{cases}. \tag{7.43}$$

Подставив (7.43) в (7.39), получим

$$P_{2\cdot n,k}(p_1,\ldots,p_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} (1-p)^k \cdot p^{n-k} =$$

$$= (1-p)^k \cdot p^{n-k} \cdot \sum_{1 \le i_1 < \ldots < i_k \le n} 1 = \binom{n}{k} \cdot (1-p)^k \cdot p^{n-k}. \tag{7.44}$$

Из (7.41) и (7.44) вытекает (7.42).

Следствие доказано.

Обозначим через $k^{cp}_{2\cdot n,k}(p)$, среднее число ошибок, допущенных криптоаналитиком в процессе расшифровки $2\cdot n$-битовой последовательности, зашифрованной посредством шифра $C_{кв}$, при условии, что $p_1 = \ldots = p_n = p$.

Следствие 7.5. Для всех $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ истинно равенство

$$k^{cp}_{2n,k}(p) = n \cdot (1-p). \tag{7.45}$$

Доказательство. При фиксированных значениях чисел $p \in [0,1]$, $n \in \mathbf{N}$ и $k \in \mathbf{Z}_+$ $(0 \le k \le n)$ правая часть формулы (7.42) представляет собой схему Бернулли с вероятностью события в каждом испытании, равной $1-p$.

Подставив, в формулу для математического ожидания биномиального распределения вместо вероятности значение $1-p$, получим (7.45).

Следствие доказано.

Случай, когда

$$p = 0.5$$

соответствует ситуации, когда секретный сеансовый ключ

$$\beta_1 \ldots \beta_n$$

представляет собой случайную последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом.

Из (7.42) и (7.45) вытекает, что

$$\mathrm{P}_{2\cdot n,k}(0.5)=\binom{n}{k}\cdot(0.5)^n \quad (0\le k\le n)$$

и

$$k_{2n,k}^{cp}(0.5)=0.5\cdot n. \qquad (7.46)$$

Из (7.46), в свою очередь, вытекает

Следствие 7.6. Если секретный сеансовый ключ $\beta_1\ldots\beta_n$ представляет собой случайную последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом, то в процессе расшифровки $2\cdot n$-битовой последовательности, зашифрованной посредством шифра $C_{кв}$, в среднем 25% переданной последовательности расшифровывается криптоаналитиком неправильно.

Отсюда вытекает

Следствие 7.7. Если секретный сеансовый ключ $\beta_1\ldots\beta_n$ – случайная последовательность, а криптоаналитик определяет значение каждого бита ключа случайным образом, то в процессе расшифровки $2\cdot n$-битовой последовательности, зашифрованной посредством шифра $C_{кв}$, для коррекции расшифрованного шифртекста криптоаналитик вынужден, в среднем, осуществлять полный перебор вариантов по четверти длины шифртекста.

Полученные результаты показывают, что построенный квантовый шифр $C_{кв}$ обладает достаточно высокой вычислительной стойкостью, если секретный сеансовый ключ $\beta_1\ldots\beta_n$ – последовательность, близкая к случайной последовательности.

7.4. Выводы.

В настоящем разделе исследован ряд модельных задач квантовой криптографии. Основные результаты состоят в следующем:

1. Построен квантовый алгоритм решения задачи идентификации булевой вектор-функции.

Исследована временная и емкостная сложность предложенного алгоритма.

Показано, что предложенный квантовый алгоритм решения задачи идентификации булевой вектор-функции обеспечивает примерно квадратичное ускорение по сравнению с классическим алгоритмом, основанном на теории полей Галуа.

2. Построены и исследованы формальные модели атак на квантовый протокол передачи ключа в предположении, что криптоаналитик управляет вероятностями выбора базисных векторов для измерения кубита, а также может управлять одновременным изменением базисов отправителя и адресата, причем ни отправитель, ни адресат не располагают информацией о том, что у них произошло изменение базиса.

Показано, что предложенная модель атаки на квантовый протокол передачи ключа является более эффективной, чем классическая атака и может существенно усложнить взаимодействие легальных пользователей.

3. Построена и исследована модель квантового шифра, основанная на квантовом алгоритме плотного кодирования.

Показано, что если секретный сеансовый ключ представляет собой последовательность, близкую к случайной последовательности, то для коррекции результатов расшифровки криптоаналитик, в среднем, вынужден осуществлять полный перебор вариантов примерно по четверти длины шифртекста.

8. ПРЕДСТАВЛЕНИЕ ШИФРСИСТЕМ МНОГООСНООЙ АЛГЕБРАИЧЕСКОЙ СИСТЕМОЙ

Большая сложность решения задач анализа и синтеза систем защиты информации обусловлена сложностью самих этих систем, сложностью внешней среды, содержащей интеллектуальные компоненты, а также многообразием и сложностью процессов взаимодействия этих систем с внешней средой. По этим причинам основным средством комплексного решения задач анализа и синтеза систем защиты информации является компьютерное моделирование с использованием систем автоматизированного вывода заключений.

Для разработки систем моделирования систем защиты информации, предназначенных для комплексного решения задач анализа и синтеза, актуально построение и исследование математических моделей, композиция которых характеризует функционирование шифрсистемы, подверженной атакам криптоаналитика, с позиции основных задач криптологии. При этом математическая модель шифрсистемы играет фундаментальную роль. Построение такой математической модели – основная цель настоящего раздела.

В п.8.1 построена и охарактеризована базовая многоосновная алгебраическая система. В п.8.2 в рамках этой модели охарактеризованы основные типы шифрсистем.

Материал, представленный в настоящем разделе, основан на результатах, полученных в [188], а также на результатах, полученных в следующей работе, вышедшей в последнее время и по этой причине не включенной в общий список литературы:

Иващенко Е.А., Скобелев В.Г. Представление криптосистем многоосновной алгебраической системой // Прикладная дискретная математика. – 2008. – № 2 (2). – С. 33-38.

8.1. Базовая многоосновная алгебраическая система.

Известны подходы к построению математических моделей шифрсистем с позиции теории систем [118], а также с позиции современной теории алгебраических систем [112].

В основе первого подхода [8] лежит система вход-выходного типа

$$\mathsf{S} = (E, D, \mathsf{M}, \mathsf{C}, \mathsf{K}_1, \mathsf{K}_2), \tag{8.1}$$

где M, C, K_1 и K_2 – множество, соответственно, открытых текстов, шифртекстов, ключей шифрования и ключей расшифровки, а $E : \mathsf{M} \times \mathsf{K}_1 \to \mathsf{C}$ и $D : \mathsf{C} \times \mathsf{K}_2 \to \mathsf{M}$ – алгоритмы шифрования и расшифровки.

Достоинством модели (8.1) является возможность представление согласованности процессов шифрования и расшифровки биекцией $\kappa : \mathsf{K}_1 \to \mathsf{K}_2$, возможность выделения блочных и поточных шифрсистем, а также возможность выделения ряда портов, через которые осуществляются пассивные атаки криптоаналитика.

Второй подход [282] основан на алгебраической системе

$$S = (T, F, domain, range, F_e, F_c), \tag{8.2}$$

где $domain : F \to T^*$ и $range : F \to T$ – заданные отображения, а T, F, F_e ($F_e \subseteq F$) и $F_c = \{f \in F \mid domain(f) = \lambda\}$ (где λ – пустое слово) – множества имен, соответственно, типов данных, типов функций, типов легковычислимых функций и типов констант.

Достоинством модели (8.2) является возможность построения нетривиальной системы конгруэнций на множестве термов, с помощью которой могут быть сформированы основные определяющие соотношения для конкретной шифрсистемы, а так же возможность выделения ряда портов, через которые осуществляются пассивные атаки криптоаналитика.

Однако обе модели (8.1) и (8.2) имеют существенные недостатки.

Во-первых, в рамки этих моделей укладываются системы с предвосхищением и системы, содержащие невычислимые функции.

Во-вторых, необходима дополнительная проработка и детализация этих моделей для выделения основных классов шифрсистем (симметричных, асимметричных, блочных, поточных и т.д.), а также для представления основных типов (пассивных и активных) атак криптоаналитика.

В-третьих, обе эти модели не дают возможность эффективно представлять параметрические и нестационарные шифрсистемы, а также шифрсистемы с вариацией окна шифрования.

Естественным способом устранения указанных выше недостатков является выбор в качестве базовой модели варианта системы алгоритмических алгебр [32], предназначенного именно для решения задач криптологии. Для этого необходимо построить соответствующую многоосновную алгебраическую систему.

В качестве такой системы выберем многоосновную алгебраическую систему

$$\mathsf{S} = (\mathsf{T}, \mathsf{F}),$$

где семейство T основных множеств и сигнатура F имеют, соответственно, вид

$$\mathsf{T} = \{T_{ij} = \{t_{ij}^{(r)} \mid r \in \mathbf{N}\} \mid i = 1,\ldots,8;\ j = 1,2\}$$

и

$$\mathsf{F} = U \cup F \cup \mathbf{K} \cup \Phi.$$

Предполагается, что множества T_{ij} $(i = 1,\ldots,8;\ j = 1,2)$ попарно не пересекаются, причем множества T_{i2} $(i = 1,\ldots,8)$ являются такими линейно упорядоченными множествами, что

$$t_{i2}^{(1)} < t_{i2}^{(2)} < \ldots < t_{i2}^{(n)} < \ldots.$$

Множества $T_{11},\ldots,T_{81}$ представляют собой множества имен, соответственно, открытых текстов, ключей шифрования, параметров шифрования, состояний шифрования, шифртекстов, ключей расшифровки, параметров расшифровки и состояний расшифровки.

Аналогичным образом, множества $T_{12},\ldots,T_{82}$ представляют собой множества размеров, соответственно, открытых текстов, ключей шифрования, параметров шифрования, состояний шифрования, шифртекстов, ключей расшифровки, параметров расшифровки и состояний расшифровки.

Охарактеризуем теперь сигнатуру F, состоящую из имен легко вычислимых функций.

I. Множество U имеет вид

$$U=\{u_i^{(1)}:\mathbf{N}\to\mathbf{N},\ u_i^{(2)}:\mathbf{N}^3\to\mathbf{N},\ u_i^{(3)}:\mathbf{N}^3\to\mathbf{N}\,|\,i=1,\ldots,8\},$$

где:

1) Каждый терм $u_i^{(1)}$ $(i=1,\ldots,8)$ является именем монотонно возрастающей функции;

2) при любых фиксированных значениях $y,z\in\mathbf{N}$ $(z<y)$ каждый терм

$$v_i(x)=u_i^{(2)}(x,y,z)\quad(i=1,\ldots,8)$$

является именем кусочно-постоянной функцией;

3) при любых фиксированных значениях $y,z\in\mathbf{N}$ $(z<y)$ каждая терм

$$w_i(x)=u_i^{(3)}(x,y,z)\quad(i=1,\ldots,8)$$

является именем периодической функцией на множестве $\{1,\ldots,u_i^{(1)}(y)\}$;

4) каждый терм v_i $(i=1,\ldots,8)$ и w_i $(i=1,\ldots,8)$ при любых фиксированных значениях $y,z\in\mathbf{N}$ $(z<y)$ является именем функции, отображающей множество $\{1,\ldots,u_i^{(1)}(y)\}$ на множество $\{1,\ldots,u_i^{(1)}(z)\}$.

Множество U предназначено для построения на каждом множестве $T_{i1}T_{i2}$ $(i=1,\ldots,8)$ системы определяющих соотношений вида

$$\begin{cases} t_{i1}^{(h)}t_{i2}^{(r)}=t_{i1}^{(h-u_i^{(1)}(r))}t_{i2}^{(r)},\ \textit{если}\ \ h>u_i^{(1)}(r) \\ t_{i1}^{(h)}t_{i2}^{(r)}=t_{i1}^{(h_1)}t_{i2}^{(r_1)}t_{i1}^{(h_2)}t_{i2}^{(r_2)} \end{cases}, \tag{8.3}$$

где

$$r=r_1+r_2\quad(r_1,r_2\in\mathbf{N}),$$
$$h_1=u_i^{(2)}(h,r,r_1),$$
$$h_2=u_i^{(3)}(h,r,r_2).$$

Ясно, что первое из соотношений (8.3) дает возможность перейти от множества $T_{i1}T_{i2}$ $(i=1,\ldots,8)$ к множеству

$$T_{i,12}=\{t_{i1}^{(h)}t_{i2}^{(r)}\,|\,r\in\mathbf{N},h\in\mathbf{N}_{u_i^{(1)}(r)}\}\subset T_{i1}T_{i2}\quad(i=1,\ldots,8).$$

Положим

$$T_{i,12}(n)=\{t_{i1}^{(h)}t_{i2}^{(n)}\,|\,h\in\mathbf{N}_{u_i^{(1)}(r)}\}\quad(i=1,\ldots,8;n\in\mathbf{N}).$$

Тогда

$$T_{i,12}=\bigcup_{n=1}^{\infty}T_{i,12}(n)\quad(i=1,\ldots,8),$$

где $T_{i,12}(n)$ $(n\in\mathbf{N})$ – попарно непересекающиеся конечные множества.

Систему определяющих соотношений (8.3) назовем полугрупповой системой определяющих соотношений, если каждый терм $t_{i1}^{(h)}t_{i2}^{(r)} \in T_{i,12}$ $(i=1,\ldots,8)$ единственным образом может быть представлен в виде

$$t_{i1}^{(h)}t_{i2}^{(r)} = t_{i1}^{(h_1)}t_{i2}^{(1)}\ldots t_{i1}^{(h_r)}t_{i2}^{(1)}.$$

Теорема 8.1. Полугрупповая система определяющих соотношений (8.3) непротиворечива.

Доказательство. Покажем, что существует интерпретация множества U, для которой система определяющих соотношений (8.3) является полугрупповой системой определяющих соотношений.

Зафиксируем конечное множество

$$X = \{x_1,\ldots,x_m\} \ (m \in \mathbf{N}).$$

Положим

$$t_{i2}^{(r)} = r \quad (r \in \mathbf{N})$$

и

$$u_i^{(1)}(r) = m^r.$$

Определим биекцию

$$\varphi : T_{i,12} \to X^+$$

равенствами

$$\varphi(t_{i1}^{(h)}t_{i2}^{(r)}) = x_{j_1}\ldots x_{j_r} \quad (h=1,\ldots,u_i^{(1)}(r); r \in \mathbf{N}),$$

где

$$h = j_r + (j_{r-1}-1)\cdot m + (j_{r-2}-1)\cdot m^2 + \ldots + (j_1-1)\cdot m^{r-1}.$$

В этом случае определяющие соотношения (8.3) согласуются с отношением лексикографического порядка на множестве $T_{i,12}(r)$ $(r \in \mathbf{N})$.

Теорема доказана.

Ясно, что полугрупповая система определяющих соотношений (8.3) дает возможность в любой интерпретации эффективно вычислять значение терма $t_{i1}^{(h)}t_{i2}^{(r)}$ $(h=1,\ldots,u_i^{(1)}(r); r \in \mathbf{N})$ через значения образующих элементов соответствующей полугруппы. Проиллюстрируем сказанное на следующем примере.

Пример 8.1. 1. Пусть

$$X = \mathbf{E}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Первое соотношение (8.3) дает возможность следующим образом вычислить значение терма $t_{11}^{(20)}t_{12}^{(1)}$

$$t_{11}^{(20)}t_{12}^{(1)} = t_{11}^{(12)}t_{12}^{(1)} = t_{11}^{(4)}t_{12}^{(1)} = 011.$$

2. Пусть

$$X = \mathbf{Z}_4 = \{000, 001, 010, 011\}.$$

Второе соотношение (8.3) дает возможность следующим образом вычислить значение терма $t_{11}^{(21)}t_{12}^{(2)}$

$$t_{11}^{(21)}t_{12}^{(2)} = t_{11}^{(5)}t_{12}^{(2)} = t_{11}^{(2)}t_{12}^{(1)}t_{11}^{(1)}t_{12}^{(1)} = 001000.$$

В дальнейшем считаем, что система определяющих соотношений (8.3) является такой полугрупповой системой определяющих соотношений, что истинны равенства

$$u_i^{(1)} = u_{i+4}^{(1)} \quad (i = 1,2,3,4).$$

II. Множество F имеет вид

$$F = F_1 \cup F_2,$$

где F_1 и F_2 – равномощные непересекающиеся множества имен функций, удовлетворяющие следующим трем условиям.

Условие 8.1. Для каждого терма $f_j \in F_j$ $(j = 1,2)$ существуют такие числа $n_{f_j}^{(1)}, n_{f_j}^{(2)} \in \mathbf{N}$, что

$$Dom\ f_j = (\bigcup_{n=1}^{\infty}(T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n))) \times T_{f_j},$$

где

$$\varnothing \neq T_{f_j} \subseteq T_{4\cdot j-1,12}(n_{f_j}^{(1)}) \times T_{4\cdot j,12}(n_{f_j}^{(2)})$$

и

$$Val\ f_j = \bigcup_{n=1}^{\infty} T_{9-4\cdot j,12}(n).$$

Условие 8.2. Для каждого терма $f_j \in F_j$ $(j = 1,2)$ соотношение

$$f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) \in T_{9-4\cdot j,12}(n)$$

истинно для всех термов $(t_{4\cdot j-1}, t_{4\cdot j}) \in T_{f_j}$ и $(t_{4\cdot j-3}, t_{4\cdot j-2}) \in T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n)$ при всех значениях числа $n \in \mathbf{N}$.

Условие 8.3. Для каждого терма $f_j \in F_j$ $(j = 1,2)$ терм

$$g_{f_j, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}}(t_{4\cdot j-3}) = f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j})$$

является именем биекции множества $T_{4\cdot j-3,12}(n)$ $(n \in \mathbf{N})$ на множество $T_{9-4\cdot j,12}(n)$ для любого терма $(t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) \in T_{4\cdot j-2,12}(n) \times T_{f_j}$.

Назовем множество F_1 множеством схем шифрования, а множество F_2 − множеством схем расшифровки.

III. Множество

$$\mathrm{K} = \{\kappa_1, \kappa_2\}$$

состоит из имен таких биекций

$$\kappa_j : F_j \to F_{3-j} \quad (j = 1,2)$$

что для каждого терма $f_j \in F_j$ $(j = 1,2)$ истинны равенства

$$|\, pr_1\, T_{f_j}\,| = |\, pr_1\, T_{\kappa_j(f_j)}\,|,$$

$$|\, pr_2\, T_{f_j}\,| = |\, pr_2\, T_{\kappa_j(f_j)}\,|,$$

и

$$|\, T_{f_j}\,| = |\, T_{\kappa_j(f_j)}\,|.$$

IV. Множество

$$\Phi = \bigcup_{j=1}^{2} \bigcup_{f_j \in F_j} \{\alpha_{f_j,n}, \beta_{f_j}, \gamma_{f_j} \mid n \in \mathbf{N}\}$$

состоит из имен таких биекций

$$\alpha_{f_j,n} : T_{4\cdot j-2,12}(n) \to T_{(4\cdot j+2)\,(\mathrm{mod}\,8),12}(n) \quad (n \in \mathbf{N}),$$

$$\beta_{f_j} : pr_1\, T_{f_j} \to pr_1\, T_{\kappa_j(f_j)}$$

и

$$\gamma_{f_j} : pr_2\, T_{f_j} \to pr_2\, T_{\kappa_j(f_j)},$$

что для каждого терма $f_j \in F_j$ $(j = 1,2)$ равенства

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3} \qquad (8.4)$$

истинны для любого терма $(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) \in T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n) \times T_{f_j}$ при всех значениях числа $n \in \mathbf{N}$.

Ясно, что равенства (8.4) обеспечивают взаимно-однозначное соответствие между результатами процессов шифрования и расшифровки.

Охарактеризуем теперь построенную многоосновную алгебраическую систему $\mathrm{S} = (\mathrm{T}, \mathrm{F})$.

Для каждого терма $f_j \in F_j$ $(j = 1,2)$ определим отношения эквивалентности

$$\varepsilon_1(f_j, n) \subseteq T_{4\cdot j-2,12}(n) \times T_{4\cdot j-2,12}(n) \quad (n \in \mathbf{N}),$$

$$\varepsilon_2(f_j) \subseteq pr_1\, T_{f_j} \times pr_1\, T_{f_j}$$

и

$$\varepsilon_3(f_j) \subseteq pr_2\, T_{f_j} \times pr_2\, T_{f_j}$$

следующим образом:

$$(t_{4\cdot j-2}, t'_{4\cdot j-2}) \in \varepsilon_1(f_j, n) \Leftrightarrow$$

$$\Leftrightarrow f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t'_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) \qquad (8.5)$$

для каждого терма $(t_{4\cdot j-3}, t_{4\cdot j-1}, t_{4\cdot j}) \in T_{4\cdot j-3,12}(n) \times T_{f_j}$,

$$(t_{4\cdot j-1}, t'_{4\cdot j-1}) \in \varepsilon_2(f_j) \Leftrightarrow$$

$$\Leftrightarrow f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t'_{4\cdot j-1}, t_{4\cdot j}) \qquad (8.6)$$

для каждого терма $(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j}) \in T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n) \times pr_2\, T_{f_j}$ при всех значениях числа $n \in \mathbf{N}$,

$$(t_{4\cdot j}, t'_{4\cdot j}) \in \varepsilon_3(f_j) \Leftrightarrow$$

$$\Leftrightarrow f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t'_{4\cdot j}) \qquad (8.7)$$

для каждого терма $(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}) \in T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n) \times pr_1\, T_{f_j}$ при всех значениях числа $n \in \mathbf{N}$.

Теорема 8.2. Для каждого терма $f_j \in F_j$ $(j = 1,2)$:

1) если $(t_{4\cdot j-2}, t'_{4\cdot j-2}) \in \varepsilon_1(f_j, n)$ $(n \in \mathbf{N})$, то

$$(\alpha_{f_j,n}(t_{4\cdot j-2}), \alpha_{f_j,n}(t'_{4\cdot j-2})) \in \varepsilon_1(\kappa_j(f_j), n); \qquad (8.8)$$

2) если $(t_{4\cdot j-1}, t'_{4\cdot j-1}) \in \varepsilon_2(f_j)$, то

$$(\beta_{f_j}(t_{4\cdot j-1}), \beta_{f_j}(t'_{4\cdot j-1})) \in \varepsilon_2(\kappa_j(f_j)); \qquad (8.9)$$

3) если $(t_{4\cdot j}, t'_{4\cdot j}) \in \varepsilon_3(f_j)$, то

$$(\gamma_{f_j}(t_{4\cdot j}), \gamma_{f_j}(t'_{4\cdot j})) \in \varepsilon_3(\kappa_j(f_j)). \qquad (8.10)$$

Доказательство. Пусть $(t_{4\cdot j-2}, t'_{4\cdot j-2}) \in \varepsilon_1(f_j, n)$ $(n \in \mathbf{N})$. Из (8.5) вытекает, что

$$f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t'_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}).$$

Следовательно, истинны равенства

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3} \qquad (8.11)$$

и

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t'_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t'_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3}. \qquad (8.12)$$

Из (8.5), (8.11) и (8.12) вытекает (8.8), что и требовалось показать.

Пусть $(t_{4\cdot j-1}, t'_{4\cdot j-1}) \in \varepsilon_2(f_j)$. Из (8.6) вытекает, что

$$f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t'_{4\cdot j-1}, t_{4\cdot j}).$$

Следовательно, истинны равенства

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3} \quad (8.13)$$

и

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t'_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t'_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3} \quad (8.14)$$

Из (8.6), (8.13) и (8.14) вытекает (8.9), что и требовалось показать.
Пусть $(t_{4\cdot j}, t'_{4\cdot j}) \in \varepsilon_3(f_j)$. Из (8.7) вытекает, что

$$f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}) = f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t'_{4\cdot j}).$$

Следовательно, истинны равенства

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t_{4\cdot j})) = t_{4\cdot j-3} \quad (8.15)$$

и

$$\kappa_j(f_j)(f_j(t_{4\cdot j-3}, t_{4\cdot j-2}, t_{4\cdot j-1}, t'_{4\cdot j}), \alpha_{f_j,n}(t_{4\cdot j-2}), \beta_{f_j}(t_{4\cdot j-1}), \gamma_{f_j}(t'_{4\cdot j})) = t_{4\cdot j-3} \quad (8.16)$$

Из (8.7), (8.15) и (8.16) вытекает (8.10).
Теорема доказана.

Рассмотренные выше понятия дают возможность выделить следующие классы многоосновных алгебраических систем $\mathsf{S} = (\mathsf{T}, \mathsf{F})$:

1) класс слабо F-минимальных многоосновных алгебраических систем $\mathsf{S} = (\mathsf{T}, \mathsf{F})$ характеризуется тем, что для любых двух термов $f_j, f'_j \in F_j$ $(j = 1,2)$ и для любого терма $(t_{4\cdot j-1}, t_{4\cdot j}) \in T_{f_j} \cap T_{f'_j}$ существует такое число $n \in \mathbf{N}$ и такой терм $t_{4\cdot j-2} \in T_{4\cdot j-2,12}(n)$, что

$$g_{f_j, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}} \neq g_{f'_j, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}};$$

2) класс слабо F-минимальных многоосновных алгебраических систем $\mathsf{S} = (\mathsf{T}, \mathsf{F})$ характеризуется тем, что для любых двух термов $f_j, f'_j \in F_j$ $(j = 1,2)$

$$g_{f_j, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}} \neq g_{f'_j, t_{4\cdot j-2}, t_{4\cdot j-1}, t_{4\cdot j}}$$

для любого терма $(t_{4\cdot j-1}, t_{4\cdot j}) \in T_{f_j} \cap T_{f'_j}$ и для всех термов $t_{4\cdot j-2} \in T_{4\cdot j-2,12}(n)$ при любом числе $n \in \mathbf{N}$;

3) класс K-минимальных многоосновных алгебраических систем $\mathsf{S}=(\mathsf{T},\mathsf{F})$ характеризуется тем, что

$$\kappa_1^{-1}=\kappa_2;$$

4) класс ε_1-минимальных многоосновных алгебраических систем $\mathsf{S}=(\mathsf{T},\mathsf{F})$ характеризуется тем, что для любого терма $f_j\in F_j$ $(j=1,2)$ каждое отношение эквивалентности $\varepsilon_1(f_j,n)$ $(n\in\mathbf{N})$ представляет собой отношение равенства на множестве $T_{4\cdot j-2,12}(n)$.

8.2. Типы шифрсистем.

Для каждого терма $f_j\in F_j$ $(j=1,2)$ и для любого терма $(t_{4\cdot j-1},t_{4\cdot j})\in T_{f_j}$ определим отображение

$$A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}:\bigcup_{n=1}^{\infty}(T_{4\cdot j-3,12}(n)\times T_{4\cdot j-2,12}(n))\to\bigcup_{n=1}^{\infty}T_{9-4\cdot j,12}(n)\quad(j=1,2)$$

равенством

$$A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t_{4\cdot j-3},t_{4\cdot j-2})=f_j(t_{4\cdot j-3},t_{4\cdot j-2},t_{4\cdot j-1},t_{4\cdot j}).$$

Отображение A_{f_1,t_3,t_4} $(f_1\in F_1;(t_3,t_4)\in T_{f_1})$ назовем алгоритмом (f_1,t_3,t_4)-шифрования, а отображение A_{f_2,t_7,t_8} $(f_2\in F_2;(t_7,t_8)\in T_{f_2})$ – алгоритмом (f_2,t_7,t_8)-расшифровки.

Такое определение алгоритмов шифрования и расшифровки дает возможность в терминах многоосновной алгебраической системы $\mathsf{S}=(\mathsf{T},\mathsf{F})$ выделить следующие три уровня понятия «ключ»:

1) элемент множества $T_{4\cdot j-2,12}$ $(j=1,2)$ интерпретируется как сеансовый или, иными словами, как кратковременный ключ;

2) элемент множества $pr_2\,T_{f_j}$ $(j=1,2)$ интерпретируется как ключ средней длительности, т.е. как ключ, применяемый для определенного числа сеансов;

3) элемент множества $pr_1\,T_{f_j}$ $(j=1,2)$ интерпретируется как долговременный ключ.

Определим стационарную (f_1,t_3,t_4)-шифрсистему $(f_1\in F_1;(t_3,t_4)\in T_{f_1})$ как упорядоченную пару

$$C_{f_1,t_3,t_4}=(A_{f_1,t_3,t_4},A_{\kappa_1(f_1),\beta_{f_1}(t_3),\gamma_{f_1}(t_4)}),\qquad(8.17)$$

а стационарную (f_2,t_7,t_8)-шифрсистему $(f_2\in F_2;(t_7,t_8)\in T_{f_2})$ – как упорядоченную пару

$$C_{f_2,t_7,t_8}=(A_{\kappa_2(f_2),\beta_{f_2}(t_7),\gamma_{f_2}(t_8)},A_{f_2,t_7,t_8}).\qquad(8.18)$$

Отметим, что определение шифрсистемы в виде упорядоченной пары дает возможность выделить, если такая необходимость возникает, что является приоритетным, а именно: процесс шифрования (для системы (8.17)) или процесс расшифровки (для системы (8.18)).

Покажем, что в терминах многоосновной алгебраической системы $S=(T,F)$ могут быть представлены основные классы шифрсистем.

Назовем стационарную $(f_j,t_{4\cdot j-1},t_{4\cdot j})$-шифрсистему $(j=1,2)$ $C_{f_j,t_{4\cdot j-1},t_{4\cdot j}}$ $(f_j\in F_j;(t_{4\cdot j-1},t_{4\cdot j})\in T_{f_j})$:

1) симметричной шифрсистемой, если для каждого терма $f_j\in F_j$ $(j=1,2)$ и для каждого числа $n\in\mathbf{N}$ терм $\alpha_{f_j,n}^{-1}$ является именем легковычислимой биекции;

2) асимметричной шифрсистемой, если для каждого терма $f_j\in F_j$ $(j=1,2)$ и для каждого числа $n\in\mathbf{N}$ терм $\alpha_{f_j,n}^{-1}$ является именем такой биекции, что в настоящее время не известен быстрый алгоритм вычисления биекции $\alpha_{f_j,n}^{-1}$, либо доказано, что такой алгоритм не существует;

3) шифрсистемой с автоключом, если каждый терм $t_{4\cdot j-2}\in T_{4\cdot j-2,12}$ является именем фиктивной переменной;

4) шифрсистемой с внешним сеансовым ключом, если каждый терм $t_{4\cdot j-2}\in T_{4\cdot j-2,12}$ является именем существенной переменной;

5) параметрической шифрсистемой, если для каждого терма $f_j\in F_j$ $(j=1,2)$ терм $t_{4\cdot j-1}\in pr_1T_{f_j}$ является именем существенного параметра для шифрсистемы $C_{f_j,t_{4\cdot j-1},t_{4\cdot j}}$, т.е. существуют два таких терма $t_{4\cdot j-1},t'_{4\cdot j-1}\in pr_1T_{f_j}$, что

$$C_{f_j,t_{4\cdot j-1},t_{4\cdot j}}\neq C_{f_j,t'_{4\cdot j-1},t_{4\cdot j}};$$

6) блочной шифрсистемой, если

$$A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t_{4\cdot j-3}t'_{4\cdot j-3},t_{4\cdot j-2}t'_{4\cdot j-2})=A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t_{4\cdot j-3},t_{4\cdot j-2})A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t'_{4\cdot j-3},t'_{4\cdot j-2})$$

для всех термов $(t_{4\cdot j-3},t_{4\cdot j-2}),(t'_{4\cdot j-3},t'_{4\cdot j-2})\in\bigcup_{n=1}^{\infty}(T_{4\cdot j-3,12}(n)\times T_{4\cdot j-2,12}(n))$;

7) шифрсистемой с предысторией, если существует хотя бы одна такая пара термов $(t_{4\cdot j-3},t_{4\cdot j-2}),(t'_{4\cdot j-3},t'_{4\cdot j-2})\in\bigcup_{n=1}^{\infty}(T_{4\cdot j-3,12}(n)\times T_{4\cdot j-2,12}(n))$, что

$$A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t_{4\cdot j-3}t'_{4\cdot j-3},t_{4\cdot j-2}t'_{4\cdot j-2})\neq A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t_{4\cdot j-3},t_{4\cdot j-2})A_{f_j,t_{4\cdot j-1},t_{4\cdot j}}(t'_{4\cdot j-3},t'_{4\cdot j-2}).$$

Выделим следующий подкласс класса шифрсистем с предысторией, являющийся предметом исследования классической криптографии.

Стационарную $(f_j, t_{4\cdot j-1}, t_{4\cdot j})$-шифрсистему $(j=1,2)$ с предысторией $C_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}$ $(f_j \in F_j; (t_{4\cdot j-1}, t_{4\cdot j}) \in T_{f_j})$ назовем стационарной поточной шифрсистемой, если терм

$$\delta_{f_j, t_{4\cdot j-1}, t_{4\cdot j}} : T_{f_j} \times \bigcup_{n=1}^{\infty} (T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n)) \to T_{f_j},$$

при условии, что для всех $(t_{4\cdot j-3}, t_{4\cdot j-2}), (t'_{4\cdot j-3}, t'_{4\cdot j-2}) \in \bigcup_{n=1}^{\infty} (T_{4\cdot j-3,12}(n) \times T_{4\cdot j-2,12}(n))$

$$A_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}(t_{4\cdot j-3} t'_{4\cdot j-3}, t_{4\cdot j-2} t'_{4\cdot j-2}) = A_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}(t_{4\cdot j-3}, t_{4\cdot j-2}) A_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}(t'_{4\cdot j-3}, t'_{4\cdot j-2}),$$

где

$$t'_{4\cdot j} = \delta_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}(t_{4\cdot j}, (t_{4\cdot j-3}, t_{4\cdot j-2}))$$

является именем легко-вычислимой биекции.

Ясно, что истинно

Утверждение 8.1. Для любой стационарной поточной $(f_j, t_{4\cdot j-1}, t_{4\cdot j})$-шифрсистемы $(j=1,2)$ $C_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}$ $(f_j \in F_j; (t_{4\cdot j-1}, t_{4\cdot j}) \in T_{f_j})$ при наличии терма

$$|T_{f_j}| < \infty$$

терм $A_{f_j, t_{4\cdot j-1}, t_{4\cdot j}}$ является именем о.-д. функции.

Следующий пример показывает, что современные шифрсистемы естественно укладываются в рамки построенной выше классификации шифрсистем.

Пример 8.2. 1. Шифр Вернама представляет собой стационарную непараметрическую блочную шифрсистему с внешним сеансовым ключом.

2. Шифры Виженера представляют собой стационарные параметрические шифрсистемы с предысторией и автоключом, причем роль параметра играет пароль.

3. Шифры DES, AES и ГОСТ 28147-89 представляют собой стационарные блочные параметрические шифрсистемы с внешним сеансовым ключом. Для DES и ГОСТ 28147-89 параметром является набор S-блоков, а для AES – набор коэффициентов многочленов.

4. Шифр RSA представляет собой стационарную блочную параметрическую криптосистему с автоключом, причем роль параметра играет набор натуральных чисел.

5. Шифр RC4 представляет собой стационарную поточную параметрическую шифрсистему с внешним сеансовым ключом, причем параметр – перестановка чисел 0,1,…,255.

6. Нелинейный БПИ-автомат над конечным кольцом представляет собой стационарную поточную параметрическую шифрсистему с автоключом, причем параметр – это набор коэффициентов многочленов.

7. Любой квантовый шифр представляет собой шифрсистему с предысторией.

8.3. Выводы.

В настоящем разделе построена многоосновная алгебраическая система $S=(T,F)$, предназначенная для исследования с единых позиций современных шифрсистем. Основные результаты состоят в следующем:

1. На множестве термов построены отношения эквивалентности, в терминах которых охарактеризовано свойство многоосновной алгебраической системы $S=(T,F)$ «быть минимальной алгебраической системой».

2. В терминах многоосновной алгебраической системы $S=(T,F)$ построены математические модели шифрсистемы, для которых, если такая необходимость возникает, естественно выделяется приоритет процесса шифрования или процесса расшифровки.

3. В терминах построенных математических моделей шифрсистемы выделены основные типы шифрсистем.

ЗАКЛЮЧЕНИЕ

В настоящей монографии сделана попытка изложить с единых позиций полученные авторами результаты, связанные с разработкой комбинаторно-алгебраических моделей и методов, предназначенных для решения задач современной криптологии.

Представленные в монографии результаты условно можно разделить по следующим направлениям.

Первое направление исследований – это анализ комбинаторно-алгебраических моделей, предназначенных для решения модельных задач криптографии в рамках схемы нестационарного поточного шифра, построенной в п.2.1.

Среди результатов, полученных в этом направлении, следует отметить аксиоматический подход к построению регулярных комбинаторных структур, которые представляют собой управляемое бинарное отношение, являются обобщением понятия управляемой подстановочной операции и предназначены для решения задачи разрушения частот букв в исходном тексте (п.2.2).

Тот фактор, что к регулярным комбинаторным структурам относятся шары и грани n-мерного куба является обоснованием того, что разработка указанной аксиоматики – нетривиальная задача.

Естественным развитием этих результатов является выделение и сравнительный анализ базовых регулярных комбинаторных структур по аналогии с тем, как это сделано в [123] для БУП.

Кроме того, нестационарные поточные шифры, основанные на семействе автоматных моделей (п.2.4) и на задаче о рюкзаке (п.2.5), обосновывают целесообразность обобщения регулярной комбинаторной структуры, предназначенного для представления семейств размеченных бинарных деревьев, семейства сверхрастущих векторов с варьируемой длиной и т.д.

В схеме нестационарного поточного шифра (п.2.1) отсутствуют внешние обмены между пользователями, связанные с информацией об используемых алгоритмах шифрования, о настройке этих алгоритмов, а также о сеансовых ключах. Передается только информация о настройке соответствующих псевдослучайных генераторов. Такой информацией, передаваемой с использованием асимметричного шифра, может быть указание на выбор решения параметрического диофантового уравнения или решения системы функциональных уравнений. Пример 1.4 показывает, что даже в простейших случаях структура множества решений параметрического диофантового уравнения может быть весьма нетривиальной, а пример 1.5 показывает, что поиск решения системы функциональных уравнений может быть достаточно сложным.

Поэтому представляет особый интерес выделение классов параметрических диофантовых уравнений и систем функциональных уравнений, реше-

ния которых могут быть эффективно использованы как для настройки указанных псевдослучайных генераторов, так и для генерации ключевых последовательностей.

Второе направление исследований – это применение хаотических отображений для решения модельных задач преобразования информации.

В разделе 3 в терминах симметрической группы охарактеризованы особенности применения простейших одномерных кусочно-линейных отображений при построении нестационарного шифра (п.3.1 и 3.2), а также для организации многопользовательского доступа к каналу связи (п.3.3).

Естественным развитием этих результатов является исследование особенностей применения аттракторов нелинейных хаотических отображений для решения модельных задач преобразования информации.

Ясно, что в этом случае возникает необходимость решения задачи определения точности вычислений, обеспечивающих корректность процесса расшифровки. Для простейших одномерных нелинейных хаотических отображений, которые эффективно могут быть сведены к кусочно-линейному отображению, для определения точности вычислений может быть применен подход, развитый в [13,91-96]. В остальных случаях задача определения точности вычислений является весьма нетривиальной. Отметим, что эта задача не решена и для алгоритма ЭЦП на основе эллиптических кривых над полем рациональных чисел, разработанного в п.2.6.

Третье направление исследований – это анализ сложности обнаружения и локализации неисправностей для аппаратных реализаций алгоритмов шифрования.

В разделе 4 охарактеризована сложность обнаружения и локализации неисправностей в схемах, реализующих матричные БУП (п.4.1), послойные БУП (п.4.2) и рекурсивные БУП (п.4.3), а также в схеме, реализующей УПО (п.4.4).

Естественным развитием этих результатов является функциональный анализ схем, реализующих бент-функции, частично максимально-нелинейные и корреляционно-иммунные булевы функции при наличии неисправностей на входе схемы, а также схем, реализующих булевы вектор-функции, являющиеся линейными разветвлениями с заданным разветвляющим пространством и с заданным разветвляющим отображением при наличии неисправностей на входе или выходе схемы.

Четвертое направление исследований – это систематический анализ нового класса конечных автоматов, а именно: конечных автоматов над кольцом Z_{p^k} (где p – простое число, а $k \in \mathbf{N}$).

Это направление исследований изложено в разделах 5, 6 и является центральным для данной монографии, так как такие автоматы представляют собой математические модели достаточно широкого класса вычислительно

стойких поточных шифров. Представленные в разделах 5 и 6 результаты получены методами теории автоматов, теории колец и теории систем.

Основным объектом исследования являются линейные автоматы (раздел 5) и нелинейные автоматы (пп.6.1-6.4), для которых «нелинейность» характеризуется тем, что изменение значений переменных состояний и выходных переменных представлено алгебраической суммой квадратичной и линейной форм от переменных состояний с линейной формой от входных переменных. Выбор такого типа «нелинейности» обусловлен тем, что аналоги над кольцом Z_{p^k} для большого числа модельных хаотических динамических систем укладываются именно в рамки такой модели.

Кроме того, в п.6.6. исследованы два типа симметричных нелинейных автоматов, которые не укладываются в рамки указанной нелинейной модели, а именно: Guckenheimer and Holmes cycle автомат, для которого изменение переменных состояния представлено многочленами третьей степени и free running автомат, для которого изменение переменных состояния осуществляется с помощью показательной функции.

Основные результаты исследования автоматов над кольцом Z_{p^k} состоят в следующем. Охарактеризованы основные нетривиальные подмножества автоматов. Оценены мощности этих подмножеств. Установлены критерии эквивалентности линейных автоматов. Охарактеризованы классы эквивалентных состояний автоматов. Решены задачи параметрической идентификации автомата и идентификации начального состояния автомата. Охарактеризованы множества неподвижных точек словарных функций, реализуемых инициальными линейными автоматами. Построены канонические формы линейных автоматов. Охарактеризованы линейные одномерные автоматы с лагом l. Найдены соотношения, характеризующие вариацию поведения автоматов, представляющие собой основу для разработки дифференциального и интегрального анализа поточных шифров.

Полученные результаты детализированы для автоматов, являющихся аналогом над кольцом Z_{p^k} модельных хаотических динамических систем Рёсслера, Спротта, Лоренца и Эно.

Естественным развитием этих результатов является более тонкая классификация нетривиальных подмножеств автоматов с оценкой их мощности.

Уже после завершения работы над монографией В.В. Скобелевым получена точная, хотя и менее обозримая, оценка в виде произведения для числа обратимых матриц над кольцом Z_{p^k}, которая, после ее приведения к компактному виду, может существенно усилить некоторые из приведенных в монографии оценок, а также получить ряд новых оценок мощности подклассов автоматов.

Большое значение имеет классификация автоматов над кольцом Z_{p^k} по сложности решения задач идентификации автомата, по сложности идентификации начального состояния автомата, по сложности исследования вариации поведения автомата.

Представляет также интерес дальнейшее детальное исследование различных типов автоматов над кольцом Z_{p^k}, являющихся аналогами модельных хаотических динамических систем.

Пятое направление исследований тесно связано со вторым и четвертым направлениями исследований и представляет собой систематический анализ шифров, построенных на основе управления семейством легковычислимых перестановок посредством псевдофрактала.

В п.6.5 построена схема такого шифра для псевдофрактала Мандельброта, а также охарактеризован один из классов семейств легко вычислимых перестановок, применяемых при построении таких шифров

Естественным развитием этих результатов является сравнительный анализ шифров, основанных на управлении семейством легко вычислимых перестановок посредством конструктивных псевдофракталов, а также поиск и анализ новых классов семейств легко вычислимых перестановок с целью разработки унифицированной процедуры построения поточного шифра, удовлетворяющего заданным требованиям.

Шестое направление исследований – это систематические исследования квантовых алгоритмов, предназначенных для решения задач преобразования информации.

В п.7.1 построен и исследован квантовый алгоритм с оракулом, предназначенный для решения задачи идентификации булевой вектор-функции.

Естественным развитием этих результатов является построение и систематический анализ квантовых алгоритмов, предназначенных для решения задач теории булевых функций и теории автоматов, являющихся модельными задачами современного криптоанализа.

В п.7.2 исследована вычислительная стойкость квантового протокола передачи ключа в предположении, что криптоаналитик может управлять вероятностями выбора базисных векторов, предназначенных для измерения кубита, а также одновременным изменением базисов отправителя и адресата.

Естественным развитием этих результатов является построение, анализ и классификация формальных моделей типов атак на квантовые алгоритмы преобразования информации.

В п.7.3 построен вычислительно стойкий квантовый шифр, основанный на классическом квантовом алгоритме плотного кодирования.

Естественным развитием этих результатов является разработка и системный анализ общей модели шифра, основанной на симбиозе алгоритмов квантовой и классической криптографии.

Седьмое направление исследований – это детальная проработка формальной модели, предназначенной для комплексного решения задач анализа и синтеза современных шифрсистем.

В п.8.1 построена и охарактеризована многоосновная алгебраическая система, предназначенная для унифицированного представления современных шифрсистем. В п.8.2 в рамках этой модели охарактеризованы основные типы шифрсистем.

Естественным развитием этих результатов является построение и анализ в терминах разработанной алгебраической системы формальных моделей атак на шифрсистему.

Таким образом, представленные в монографии результаты, в своей совокупности, представляют собой основу для дальнейшего системного анализа математических моделей и методов, предназначенных для решения задач современной криптологии с позиции дискретной математики, теории булевых функций, теории автоматов, теории систем и современной алгебры.

СПИСОК ЛИТЕРАТУРЫ

1. *Агибалов Г.П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Известия АН СССР. Техническая кибернетика. – 1970. – № 3. – С. 99-108.

2. *Агибалов Г.П., Юфит Я.Г.* О простых экспериментах для линейных инициальных автоматов // Автоматика и вычислительная техника. – 1972. – № 2. – С. 17-19.

3. *Агибалов Г.П.* Вероятностные схемы симметричного поточного щифрования над конечным полем // Вестник Томского государственного университета. Приложение. – 2005. – № 14. − С. 39-42.

4. *Агибалов Г.П.* Избранные теоремы начального курса криптографии. − Томск: Изд-во НТЛ, 2005. − 116 с.

5. *Агибалов Г.П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. – 2006. – № 17. − С. 4-9.

6. *Агибалов Г.П., Сунгурова О.Г.* Криптоанализ конечно-автоматного генератора ключевого потока с функцией выходов в качестве ключа // Вестник Томского государственного университета. Приложение. – 2006. – № 17. − С. 104-112.

7. *Алексейчук А.*Н., *Проскуровский Р.В., Шевцов А.С.* Аналитические оценки и достаточные условия стойкости блочных шифров и комбинирующих генераторов гаммы с неравномерным движением относительно статистических методов криптоанализа // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 264-273.

8. *Алферов А.П. и др*. Основы криптографии. − М.: Гелиос АРВ, 2002. − 480 с.

9. *Андреев Ю.В., Бельский Ю.Л., Дмитриев А.С*. Запись и восстановление информации с использованием устойчивых циклов двумерных и многомерных отображений // Радиотехника и электроника. − 1994. − **Т.39.** − С. 114-123.

10. *Андреев Ю.В. и др*. Хаотические процессоры // Радиотехника и электроника. − 1997. − **Т.42.** − Вып. 10. − С. 50-79.

11. *Анисимова Е.Н.* Построение стойкой криптосистемы, основанной на задаче о рюкзаке // Искусственный интеллект. − 2004. − № 1. − С. 4-12.

12. *Анисимова Е.Н., Скобелев В.Г.* Анализ послойных блоков управляемых перестановок // Искусственный интеллект. − 2005. − № 1. − С. 146-152.

13. *Антонов А.В*. Оценка вычислительных затрат на функционирование криптосистемы, использующей методы хаотической динамики, при решении задач защиты информации в информационно-коммуникационных системах и сетях // Прикладная радиоэлектроника. − **Т.5.** – 2007. – № 2. − С. 105-109.

14. *Асосков А.В. и др*. Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. – 326 с.

15. *Ахо А., Хопкрофт Дж., Ульман Дж*. Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979. – 536 с.

16. *Б. А. ван дер Варден*. Алгебра. – М.: Наука, 1979. – 634 с.

17. *Баричев С.Г., Гончаров В.В., Серов Р.Е*. Основы современной криптографии: Учебный курс. – М.: Горячая линия–Телеком, 2002. – 175 с.

18. Безопасность бизнеса / Под ред. *В.А. Динеса*. – Саратов: Регион. Приволж. Изд-во «Детская книга», 2002. – 304 с.

19. *Бернштейн А.С., Попков Ю.С., Фараджев Р.Г*. Аналитическое описание нелинейных последовательностных машин // Автоматика и телемеханика. – 1971. – № 12. – С. 69-77.

20. *Бессалов А.В., Телижненко А.Б.* Криптосистемы на эллиптических кривых. – Киев: Политехника, 2004. – 223 с.

21. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.

22. *Богомолов А.С., Сперанский Д.В.* Оптимальные синхронизирующие эксперименты с автоматами // Автоматика и телемеханика. – 2001. – № 10. – С. 203-208.

23. *Болотов и др.* Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.

24. *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз захищеності існуючих ЦП від атак на зв'язаних ключах // Прикладная радиоэлектроника. − **Т.5.** – 2007. – № 2. − С. 52-58.

25. *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз захищеності існуючих ЦП від атак на реалізацію // Прикладная радиоэлектроника. − **Т.5.** – 2007. – № 2. − С. 59-61.

26. *Брикcл Э.Ф., Одлижко Э.М.* Криптоанализ. Обзор новейших результатов // ТИИЭР (малый тематический выпуск: Защита информации). – 1988. – **76.** − № 5. – С. 75-94.

27. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. − 326 с.

28. *Волков О.Г., Скобелев В.Г.* Идентификация булевых вектор-функций методами квантовых вычислений // Труды ИПММ НАНУ. − **Т.15.** − 2007. − С. 15-20.

29. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 298 с.

30. *Гилл А.* Введение в теорию конечных автоматов. − М.: Наука, 1966. − 272 с.

31. *Глушков В.М.* Синтез цифровых автоматов. – М.: Физматлит, 1962. – 476 с.

32. *Глушков В.М., Цейтлин Г.Е., Ющенко Е.Л.* Алгебра, языки, программирование. – Киев: Наукова думка, 1978. – 320 с.

33. *Головашич С.А.* Безопасность режимов блочного шифрования // Радиотехника. – 2001. – Вып. 119. – С. 135-145.

34. *Головашич С.А.* Метод построения управляемых S-блоков с предельными показателями нелинейности // Радиотехника. – 2001. – Вып. 123. – С. 215-221.

35. *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 230-240.

36. *Голод П.И., Климык А.У.* Математические основы теории симметрий. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 528 с.

37. *Горбачев В.А., Иванисенко И.Н.* Классификация и формальные модели аппаратных закладных устройств // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 306-309.

38. *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных подстановок для алгоритма шифрования ГОСТ 28147-89 // Радиотехника. – 1997.

39. *Горбенко И.Д., Лепеха А.Н.* Сравнительный анализ блочных симметричных шифров, представленных в проекте NESSI // Радиотехника. − 2003. − Вып. 136. − С. 25-38.

40. *Горбенко І.Д., Гриненко Т.О.* Захист інформації в інформаційно-телекомунікаційних системах: Навчальний посібник. Ч.1. Криптографічний захист інормації – Харків: ХНУРЕ, 2004. – 368 с.

41. *Горбенко І.Д. та ін.* Порівняльний аналіз алгоритмів блокового симетричного шифрування (за результатами виконання проекту NESSI) // Радиотехника.− 2004. − Вып. 138. − С. 25-38.

42. *Горбенко І.Д. та ін*. Стан та проблемні питання створення та розвитку національної інфраструктури відкритих ключів // Прикладная радиоэлектроника. − **Т.5.** – 2006. – № 1. − С. 41-51.

43. *Горбенко І.Д. та ін*. Принципи побудування та властивості блокових симетричних IDEA шифрів // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 158-203.

44. *Горбенко И.Д. и др.* Анализ безопасности международного стандарта ISO/IEC 9797-1 // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 250-256.

45. *Горицкий В.М*. Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. – 1998. – Вып. 5. – С. 140-145.

46. ГОСТ 28147-89. Системы обработки информации. Защита информации. Алгоритм криптографического преобразования. − М.: Госстандарт СССР.

47. *Грибунин В.Г., Оков И.Н., Туринцев И.В*. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.

48. *Григор А.А., Скобелев В.Г*. Анализ ЭЦП, основанной на эллиптических кривых над полем Q // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 104-107.

49. *Горяшко А.П*. Проектирование легко тестируемых дискретных устройств: идеи, методы, реализация // Автоматика и телемеханика. – 1984. – № 7. – С.5-35.

50. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. − М.: Мир, 1982. − 416 с.

51. *Девянин П.Н. и др*. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192 с.

52. *Девянин П.Н*. Подходы к обеспечению безопасности информационных потоков в системах мандатного разграничения доступа // Вестник Томского государственного университета. Приложение. − 2004. − № 9(I) − С. 100-105.

53. *Девянин П.Н*. Модели безопасности компьютерных систем. Учебное пособие. – М.: Издательский центр «Академия», 2005. – 144 с.

54. *Девянин П.Н*. Моделирование условий передачи прав доступа и реализации информационных потоков в компьютерных системах с дискреционным управляемым доступом // Вестник Томского государственного университета. Приложение. − 2005. − № 14 − С. 105-110.

55. *Девянин П.Н*. Анализ безопасности информационных потоков по памяти на функционально ассоциированные с субъектами сущности // Вестник Томского государственного университета. Приложение. − 2006. − № 17 − С. 151-156.

56. *Девянин П.Н*. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. – 176 с.

57. *Девянин П.Н*. Опыт преподавания безопасности компьютерных систем с мандатным управляемым доступом // Вестник Томского государственного университета. Приложение. − 2007. − № 23 − С. 169-173.

58. Дискретная математика и математические вопросы кибернетики. **Т.1** / Под ред. *С.В. Яблонского* и *О.Б. Лупанова*. – М.: Наука, 1974. – 312 с.

59. *Диффи У., Хеллмен М.Е*. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. – 1979. – **Т.67.** – № 3. – С. 71-109.

60. *Дмитриев А.С*. Запись и восстановление информации в одномерных динамических системах // Радиотехника и электроника. − 1991. – **Т.36.** – № 1. – С. 101-108.

61. *Дмитриев А.С*. Хаос и обработка информации в нелинейных динамических системах // Радиотехника и электроника. − 1993. – **Т.38.** – № 1. – С. 1-24.

62. *Дмитриев А.С., Старков С.О.* Передача сообщений с использованием хаоса и классическая теория информации // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – 1998. – № 11. – С. 4-32.

63. *Долгов В.И., Неласая А.В.* Стойкость криптографических алгоритмов на гиперэллиптических кривых // Прикладная радиоэлектроника. − **Т.5.** – 2006. – № 1. − С. 30-34.

64. *Долгов В.И. и др.* Критерии случайности таблиц подстановок алгоритма шифрования ГОСТ 28147-89 // Прикладная радиоэлектроника. − **Т.5.** – 2006. – № 1. − С. 127-133.

65. *Долгов В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 257-263.

66. *Духов Н.Е.* Экономическая разведка и безопасность бизнеса. – Киев: ИМСо МО Украины, НВФ «Студцентр», 1997. – 175 с.

67. *Жуков А.Е., Чистяков В.П.* Матричный подход к исследованию прообразов выходной последовательности конечного автомата // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – № 1. – С. 108-117.

68. *Заде Л., Дезоер И.* Теория линейных систем. – М.: Наука, 1970. – 704 с.

69. *Зайцева Э.Е., Скобелев В.Г.* Шифр на основе отображения Мандельброта // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 107-113.

70. *Зачесов Ю.Л., Салихов Н.П.* Алгоритм решения полиномиального сравнения $P(x) \equiv 0 (\mathrm{mod}\, N)$ и его экспериментальное подтверждение // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 95-98.

71. *Зиммерман Ф.Р.* PGP: концепция безопасности и уязвимые места // Компьютера. – 1997. – № 48. – С. 36-40, 42-51.

72. *Зубов А.Ю.* Совершенные шифры. − М.: Гелиос АРВ, 2003. − 160 с.

73. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

74. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. − М.: Мир, 1971. − 400 с.

75. *Карр Н. Дж.* Блеск и нищета информационных технологий. – М.: Секрет фирмы, 2005. – 176 с.

76. *Климов А.С.* Форматы графических файлов. – Киев: НИПФ «ДиаСофт Лтд», 1995. – 480 с.

77. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы. – М.: Мир, 1988. – 316 с.

78. *Коблиц Н.* Курс теории чисел и криптография. М.: Научное изд-во «ТВП», 2001. – 262 с.

79. *Ковалев А.М., Скобелев В.В.* Шифры: от алгебры к быстрому поиску. − Сборник научных трудов 10-й международной конференции “Математические модели физических процессов (Таганрог, Россия, 29-30 июня, 2004г.)”, Таганрог: ТГПИ, 2004. − С. 175-177.

80. *Ковалев А.М., Скобелев В.Г.* Нестационарные стойкие шифры: модели и методы. − Материалы VI Международной научно-практической конференции «Информационная безопасность». – Таганрог, ТРТУ, 2004. – С. 250-252.

81. *Ковалев А.М., Скобелев В.Г.* Два подхода к защите информации: комбинаторика и хаос // Искусственный интеллект. − 2004. − № 3. − С. 806-815.

82. *Ковалев А.М., Скобелев В.Г.* Модели и методы защиты информации на основе комбинаторики и хаоса // Известия Таганрогского радиотехнического университета. − 2004. − № 9. − С. 135-142.

83. *Ковалев А.М., Скобелев В.Г.* Построение поточных шифров над конечными кольцами. − Материалы Международной научно-технической конференции «Интеллектуальные и многопроцессорные системы-2005». − **Т.1.** – Таганрог, ТРТУ, 2005. − С. 94-101.

84. *Ковалев А.М., Скобелев В.Г.* Шифр на основе хаоса: система Лоренца // Вестник Томского государственного университета. Приложение. − 2005. − № 14. − С. 54-57.

85. *Колбин С.Л.* О некоторых свойствах взаимно обратных систем функций p-значной логики // Дискретная математика. – 1994. – **Т.6.** – Вып. 2. – С. 145-149.

86. *Колегов Д.Н.* Общая схема вероятностной поточной шифрсистемы // Вестник Томского государственного университета. Приложение. – 2006. – № 17. − С. 112-114.

87. *Колесов Н.В.* Построение проверяющего теста для линейного конечного автомата // Автоматика и телемеханика. – 1982. – № 2. – С. 61-66.

88. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.

89. *Кормен Т., Лейзерсон Ч., Ривест Р.* Алгоритмы: построение и анализ. – М. МЦНМО, 2000. – 960 с.

90. *Коршунов А.Д.* О перечислении конечных автоматов. – В кн.: Проблемы кибернетики. Вып. 34. – М.: Наука, 1978. – С. 5-82.

91. *Костенко П.Ю., Антонов А.В., Сиващенко С.И.* Решение обратной задачи хаотической динамики как наиболее эффективный метод анализа криптографической системы с открытым ключом // Реєстрація, зберігання і обробка даних. – 2006. − № 1. – С. 103-113.

92. *Костенко П.Ю и др.* Применение методов хаотической динамики для обеспечения информационной скрытности в коммуникационных сетях // Известия Вузов. Радиоэлектроника. – 2006. − **49.** − № 3. – С. 63-70.

93. *Костенко П.Ю., Антонов А.В., Костенко Т.П.* Анализ эффективности обеспечения информационной скрытности в коммуникационных системах и сетях методами хаотической динамики // Известия Вузов. Радиоэлектроника. – 2006. − **49.** − № 4. – С. 27-38.

94. *Костенко П.Ю., Антонов А.В., Костенко Т.П.* Обратные задачи хаотической динамики и статистический анализ при обеспечении информационной скрытности в коммуникационных системах и сетях // Кибернетика и системный анализ. − 2006. − № 5. − С. 96-106.

95. *Костенко П.Ю., Антонов А.В., Костенко Т.П.* Анализ однозначности решения обратных задач хаотической динамики для обеспечения информационной скрытности в коммуникационных системах и сетях // Известия Вузов. Радиоэлектроника. – 2006. − **49.** − № 8. – С. 3-11.

96. *Костенко П.Ю., Антонов А.В., Костенко Т.П.* Развитие концепции односторонних функций для систем криптографической защиты информации с использованием достижений хаотической динамики // Кибернетика и системный анализ. − 2006. − № 6. − С. 136-146.

97. *Кострикин А.И.* Введение в алгебру. − **Т.1-3.** − М.: Наука, 1999-2000.

98. *Кудрявцев В.Б. и др.* Введение в теорию конечных автоматов. – М.: Наука, 1985. – 320 с.

99. *Кузнецов С.П.* Динамический хаос. − М.: Физматлит, 2001. − 296 с.

100. *Кузнецов Ю.В., Шкарин С.А.* Коды Рида-Маллера (обзор публикаций) // Математические вопросы кибернетики. – М.: Наука. – 1996. – № 6. – С. 5-50.

101. *Курмит А.А.* Автоматы без потери информации конечного порядка. – Рига: Зинатне, 1972. – 266 с.

102. *Ленг С.* Эллиптические функции. – М.: Наука, 1984. – 312 с.

103. *Лепеха и др*. Принципы функционирования протокола IPSec // Радиотехника. − 2001. − Вып. 119. − С. 101-107.

104. *Лидл Р.*, *Нидеррайтер Г*. Конечные поля. − **Т.1,2.** − М.: Мир, 1988.

105. *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В*. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 479 с.

106. *Логачев О.А*. Об одном рекурсивном алгоритме декодирования некоторых подмножеств кода Рида-Маллера первого порядка // Дискретная математика. – 1992. – **Т.4.** – Вып. 2. – С. 130-135.

107. *Лисовик Л. П*. Применение конечных преобразователей для задания фрактальных кривых // Кибернетика. – 1994. – № 3. – С. 11-22.

108. *Лисовик Л. П*. Фрактальные множества, определяемые конечными преобразователями // Кибернетика и системный анализ. – 1996. – № 4. – С. 13-27.

109. *Лисовик Л. П*. Применение макропреобразователей для задания частичных непрерывных операторов в метрических пространствах // Кибернетика и системный анализ. – 1996. – № 5. – С. 18-41.

110. *Личаргин Д.В*. Принципы автоматической генерации семантических шифров в форме осмысленного текста постороннего содержания // Вестник Томского государственного университета. Приложение. – 2006. – № 17. − С. 115-118.

111. *Льюнг Л*. Идентификация систем. Теория для пользователя. − М.: Наука, 1991. − 432 с.

112. *Мальцев А.И*. Алгебраические системы. – М.: Наука, 1970. – 329 с.

113. *Малютин А.А*. Быстрое корреляционное декодирование некоторых подмножеств кода Рида-Маллера первого порядка // Дискретная математика. 1990. − **Т.2.** – Вып. 2. – С. 155-158.

114. *Масленников М.Е*. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.

115. *Маховенко Е.Б*. Теоретико-числовые методы в криптографии. – М.: Гелиос АРВ, 2006. – 320 с.

116. *Медведев И.Л.*, *Фараджев Р.Г.*, *Чуйко А.С*. Применение модулярных линейных уравнений для описания линейных последовательностных машин // Автоматика и телемеханика. – 1971. – № 8. – С. 63-71.

117. *Мелецький О.П*. Властивості безпеки відносно протоколів узгодження ключів на базі білінійного відображення // Прикладная радиоэлектроника. − **Т.5.** – 2006. – № 1. − С. 35-40.

118. *Месарович М.*, *Такахара Я*. Общая теория систем: математические основы. – М: Мир, 1978. – 311 с.

119. *Михайлов В.Г*. О числе прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – № 1. – С. 118-121.

120. *Михайлов В.Г*. Обобщение теоремы о числе прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – №1. – С. 122-125.

121. *Михайлов В.Г*. Асимптотическая нормальность числа прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – №1. – С. 126-135.

122. *Михайлов В.Г.*, *Чистяков В.П*. О задачах теории конечных автоматов, связанных с числом прообразов выходной последовательности // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – №1. – С. 7-31.

123. *Молдовян А.А. и др*. Криптография. Скоростные шифры. – СПб: БХВ-Петербург, 2002. − 496 с.

124. *Морозов А.Д.* Введение в теорию фракталов. – Москва-Ижевск: Ин-т компьютерных исследований, 2002. – 160 с.

125. НД ТЗІ 2.5-004-99. Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

126. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. − М.: Мир, 2006. ─ 824 с.

127. *Норткат С. и др.* Анализ типовых нарушений в сетях. – М.: Вильямс, 2001. – 464 с.

128. *Носов В.А.* Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. ─ М.: МГУ им М.В. Ломоносова. – 1998. – **Т.3.** – Вып.3-4. – С. 307-320.

129. *Ожигов Ю.И.* Квантовые вычисления. − М.: МГУ, 2003. − 104 с.

130. *Пайтген Х.-О., Рихтер П.Н.* Красота фракталов. Образы комплексных динамических систем. – М.: Мир, 1993. – 176 с.

131. *Пархоменко П.П. и др.* Основы технической диагностики. – М.: Энергия, 1981. − 320 с.

132. *Петраков А.В.* Основы практической защиты информации. – М.: Радио и связь, 2000. − 368 с.

133. *Поздеев А.Г.* Защита программного обеспечения от нелегального использования: проблемы и решения // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 197-200.

134. Положення про проведення відкритого конкурсу криптографічних алгоритмів. http://dstszi.gov.ua/dstszi/control/uk/publish.

135. *Пономаренко П.В.* Метод шифрования сообщений, основанный на стеганографии // Искусственный интеллект. − 2004. − № 1. − С. 73-78.

136. *Потий А.В., Пестерев А.К.* Принципы системного подхода к сертификации генераторов псевдослучайных чисел в системах защиты информации // Радиотехника. – 1997. – Вып. 104. – С. 163-172.

137. *Прахар К.* Распределение простых чисел. – М.: Мир, 1967. – 511 с.

138. *Працьовитий М.В.* Фрактальний підхід у дослідженнях сингулярних розподілів. – Київ: НПУ ім. Драгоманова, 1998. – 296 с.

139. *Птицын Н.И.* Приложение теории детерминированного хаоса в криптографии. – М.: МГТУ, 2002. – 79 с.

140. *Пудовкина М.*А. Математические методы, использующиеся при синтезе и анализе поточных шифров (обзор по материалам конкурса ENCRYPT) // Вестник Томского государственного университета. Приложение. – 2006. – № 17. − С. 118-126.

141. *Рейнгольд Э., Нивергельт Ю., Део Н.* Комбинаторные алгоритмы. Теория и практика. – М.: Мир, 1980. – 476 с.

142. *Романцев С.А.* Анализ эффективности одного из алгоритмов стеганографического скрытия информации в статистические изображения // Прикладная радиоэлектроника. − **Т.5.** – № 1.– 2006. − С. 148-151.

143. *Ростовцев А.Г.* Логарифмирование через понятие // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 2. – С. 49-54.

144. *Рысцов И.К.* Оценка длины кратчайшего диагностического слова для конечного автомата // Кибернетика. – 1978. – № 6. – С. 40-45.

145. *Рысцов И.К.* Асимптотическая оценка длины кратчайшего диагностического слова для конечного автомата // Доклады АН СССР. – 1978. – **241**. – № 2. – С. 294-296.

146. *Савченко А.Я., Ковалев А.М., Скобелев В.Г.* Модели и методы защиты информации на основе комбинаторики и обратных задач хаотической динамики. − Труды на CD II-го Международного радиоэлектронного форума «Прикладная радиоэлектро-

ника. Состояние и перспективы развития» (МРФ 2005), (19-23 сентября 2005 г., г. Харьков). − 9 с.

147. *Савченко А.Я., Ковалев А.М., Скобелев В.Г.* О двух подходах к построению шифров на основе хаоса дискретных динамических систем. − Сборник научных трудов 11-й международной конференции “Математические модели физических процессов (Таганрог, Россия, 29-30 июня, 2005г.)”. − **Т.1.** − Таганрог: ТГПИ, 2005. − С. 247-254.

148. *Саломаа А*. Криптография с открытым ключом. – М.: Мир, 1996. – 318 с.

149. *Севостьянов Б.А., Чистяков В.П.* О числе входных последовательностей, соответствующих выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: ТВП. – 1994. – **Т.1.** – № 1. – С. 96-107.

150. *Симонович С.В., Евсеев Г.А., Мураховский В.И.* INTERNET: Лаборатория мастера. Работа в сети без проблем. – М.: АСТ-ПРЕСС КНИГА, 2003. – 720 с.

151. *Скембрей Дж., Шема М.* Безопасность Web-приложений − готовые решения. – М.: Издательский дом «Вильямс», 2003. – 384 с.

152. *Скобелев В.В*. Об одном типе диофантовых уравнений // Труды ИПММ НАНУ. − **Т.5.** − 2000. − С. 127-131.

153. *Скобелев В.В*. Построение стойких к частотному анализу криптосистем на основе регулярных комбинаторных структур // Искусственный интеллект. − 2004. − №1. − С. 88-96.

154. *Скобелев В.В*. Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Труды ИПММ НАНУ. − **Т.10.** − 2005. − С. 184-189.

155. *Скобелев В.В*. Free-running system над конечным кольцом. − Сборник научных трудов 11-й международной конференции “Математические модели физических процессов (Таганрог, Россия, 29-30 июня, 2005г.)”. − **Т.1.** − Таганрог: ТГПИ, 2005. − С. 190-192.

156. *Скобелев В.В*. Об обратимых матрицах над кольцом $\mathbf{Z}_{p^k}$. // Труды ИПММ НАНУ. − **Т.13.** − 2006. − С. 185-192.

157. *Скобелев В.В*. Анализ линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Труды ИПММ НАНУ. − **Т.14.** − 2007. − С. 162-173.

158. *Скобелев В.В*. Перечисление линейных автоматов над конечным кольцом. − Материалы IX Международного семинара «Дискретная математика и ее приложения» (РФ, Москва, МГУ, 18-23 июня 2007 г.), ─ Москва: Изд-во мех.-мат. факультета МГУ, 2007. − С. 178-181.

159. *Скобелев В.В*. Шифры на основе линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 118-122.

160. *Скобелев В.В*. Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Доповіді НАНУ. − 2007. − № 10. − С. 44-49.

161. *Скобелев В.В*. Анализ структуры класса линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Кибернетика и системный анализ. − 2008. − № 3. − С. 60-74.

162. *Скобелев В.В*. Задача идентификации линейных автоматов над кольцом $\mathbf{Z}_{p^k}$. − Труды на CD VII Международной конференции «Идентификация систем и задачи управления» (SICPRO 08) (Москва, Россия, 28-31 января, 2008) – Москва: ИПУ РАН, 2008. − С. 1154-1185.

163. *Скобелев В.В.* Характеристики линейных одномерных автоматов с лагом l над конечным кольцом // Труды ИПММ НАНУ. − **Т.16.** − 2008. − С. 190-196.

164. *Скобелев В.Г.* Об оценках длин диагностических и возвратных слов для автоматов // Кибернетика. – 1987. – № 4. – С. 114-116.

165. *Скобелев В.Г.* Общерекурсивная модель секретного замка // Доповіді НАНУ. − 1995. − № 6. − С. 73-75.

166. *Скобелев В.Г.* Построение нижних экспоненциальных оценок // Доповіді НАНУ. − 1997. − № 3. − С. 115-117.

167. *Скобелев В.Г.* Анализ дискретных систем. − Донецк: ИПММ НАНУ, 2002. − 172 с.

168. *Скобелев В.Г.* Локальные алгоритмы на графах. − Донецк: ИПММ НАНУ, 2003. − 217 с.

169. *Скобелев В.Г.* Схемы генерации управляемых подстановок на основе поиска // Вестник Томского государственного университета. Приложение. − 2004. − № 9 (I). − С. 77-82.

170. *Скобелев В.Г., Приходько О.В.* Шифры, основанные на циклических аттракторах // Искусственный интеллект. − 2004. − № 3. − С. 826-835.

171. *Скобелев В.Г., Ткаченко А.В.* Многопользовательский доступ к каналу связи на основе циклических аттракторов // Искусственный интеллект. − 2004. − № 3. − С. 836-843.

172. *Скобелев В.Г., Анисимова Е.Н.* Сложность локализации неисправностей блока управляемых перестановок // Искусственный интеллект. − 2004. − № 4. − С. 794-803.

173. *Скобелев В.Г., Сухинин В.А.* Шифр на основе отображения “зуб пилы” // Искусственный интеллект. − 2004. − № 4. − С. 804-810.

174. *Скобелев В.Г.* Анализ комбинационных схем: ДНФ и конечные поля. − Труды VI-ой международной конференции «Дискретные модели в теории управляющих систем». – Москва, МГУ, 2004. − С. 80-83.

175. *Скобелев В.Г., Тубольцева О.В.* Шифр на основе отображения Эно // Вестник Томского государственного университета. Приложение. − 2004. − № 9 (1). − С. 77-82.

176. *Скобелев В.Г.* Схемы генерации управляемых подстановок на основе поиска // Вестник Томского государственного университета. Приложение. − № 14. − 2005. − С. 74-78.

177. *Скобелев В.Г., Анисимова Е.Н.* Сложность тестирования матричных и послойных БУП // Вестник Томского государственного университета. Приложение. − 2005. − № 14. − С. 139-143.

178. *Скобелев В.Г., Зайцева Э.Е.* Шифры на основе фракталов // Труды ИПММ НАНУ. − **Т.12.** − 2006. − С. 63-68.

179. *Скобелев В.Г.* Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. − 2006. − № 6. − С. 29-42.

180. *Скобелев В.Г.* Контроль неисправностей блоков управляемых перестановок // Надежность. − 2006. − № 4. − С. 41-45.

181. *Скобелев В.Г., Анисимова Е.Н.* Сложность идентификации неисправностей блока управляемых перестановок. − Труды на CD V Международной конференции «Идентификация систем и задачи управления» (SICPRO 06) (Москва, Россия, 30 января – 2 февраля, 2006). − Москва: ИПУ РАН, 2006.− 18 с.

182. *Скобелев В.Г.* Потоковые шифры над конечным кольцом // Известия ТРТУ. − 2006. − № 7. − С. 167-173.

183. *Скобелев В.Г.* Анализ системы Лоренца над кольцом $\mathbf{Z}_{q^k}$ // Вестник Томского государственного университета. Приложение. − 2006. − № 17. − С. 134-139.

184. *Скобелев В.Г.* Алгоритмы и сложность экспериментов с автоматами над конечными кольцами. − Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, Россия, 4-6 марта, 2006г.) – Москва: МАКС Пресс, 2006. − С.339-345.

185. *Скобелев В.Г.* О некоторых свойствах нелинейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 288-299.

186. *Скобелев В.Г.* Задачи идентификации нелинейных динамических систем над кольцом $\mathbf{Z}_{q^k}$. − Труды на CD VI Международной конференции «Идентификация систем и задачи управления». (SICPRO 07) (Москва, Россия, 29-31 января, 2007). − Москва: ИПУ РАН, 2007. − С. 391-411.

187. *Скобелев В.Г.*, *Сухинин В.А*. Шифры на основе систем Спротта // Вестник Томского государственного университета. Приложение. – 2007. – № 23. − С. 122-126.

188. *Скобелев В.Г.*, *Иващенко Е.А*. Моделирование криптосистем многоосновной алгебраической системой. − Сборник трудов конференции “Моделирование-2008” (14-16 мая 2008, Киев). − **Т.2.** – Киев: ИПМЭ, 2008. − С. 504-509.

189. *Скобелев В.Г., Зайцева Э.Е.* Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. − 2008. − № 5. − С. 12-24.

190. *Соколовский М.Н.* Оценка длины диагностического слова для конечного автомата // Кибернетика. – 1976. – № 2. – С. 16-21.

191. *Сперанский Д.В*. Обобщенные автоматы без потери информации. I. // Кибернетика и системный анализ. – 1994. – № 3. – С. 63-69.

192. *Сперанский Д.В*. Обобщенные автоматы без потери информации конечного порядка. II. // Кибернетика и системный анализ. – 1994. – № 4. – С. 63-69.

193. *Сперанский Д.В*. Синхронизация линейных последовательностных машин // Автоматика и телемеханика. – 1996. – № 5. – С. 141-149.

194. *Сперанский Д.В*. Установочные и диагностические эксперименты для линейных последовательностных машин // Автоматика и телемеханика. – 1997. – № 5. – С. 133-141.

195. *Сперанский Д.В*. Обобщенная синхронизация линейных последовательностных машин // Кибернетика и системный анализ. – 1998. – № 3. – С. 174-178.

196. *Сперанский Д.В., Сперанский И.В*. Об одной задаче для сети из линейных автоматов без потери информации // Автоматика и телемеханика. – 1999. – № 1. – С. 140-147.

197. *Сперанский Д.В., Сперанский И.В*. Эксперименты с линейными дискретными системами // Электронное моделирование. – 1999. – № 4. – С. 64-73.

198. *Сперанский Д.В., Сперанский И.В*. Эксперименты с билинейными системами // Автоматика и телемеханика. – 2000. – № 6. – С. 176-189.

199. *Сперанский Д.В*. Распознавание состояний нестационарных линейных автоматов // Известия РАН. Теория и системы управления. – 2000. – № 6. – С. 82-89.

200. *Сперанский Д.В*. Связь между устойчивостью и синхронизируемостью нестационарных линейных автоматов над различными полями // Электронное моделирование. – 2001. – № 5. – С. 22-32.

201. *Сперанский Д.В*. Синтез тестов с минимальным числом перепадов сигналов для линейных автоматов // Автоматика и вычислительная техника. – 2002. – № 4. – С. 70-78.

202. *Сперанский Д.В*. Эксперименты с линейными и билинейными конечными автоматами. − Саратов: СГУ, 2004. −144 с.

203. *Столлингс В*. Криптография и защита сетей: принципы и практика. – М.: Вильямс, 2001. – 672 с.

204. *Сухинин В.А., Скобелев В.Г.* Эквивалентность состояний систем Спротта // Труды ИПММ НАНУ. − **Т.14.** − 2007. − С. 174-186.

205. *Сухинин В.А., Скобелев В.Г.* Алгоритмы и сложность идентификации автоматов Спротта над кольцом $\mathbf{Z}_{p^k}$. − Труды на CD VII Международной конференции «Идентификация систем и задачи управления» (SICPRO 08) (Москва, Россия, 28-31 января, 2008) – Москва: ИПУ РАН, 2008. − С. 1107-1153.

206. *Сухинин В.А., Скобелев В.Г.* Автоматизированная система анализа автоматов над конечными кольцами. − Сборник трудов конференции "Моделирование-2008" (14-16 мая 2008, Киев). − **Т.1.** – Киев: ИПМЭ, 2008. − С. 156-160.

207. *Торба А.А., Бобух В.А., Торба А.А.* Математические модели датчиков шума // Прикладная радиоэлектроника. − **Т.6.** – 2007. – № 2. − С. 277-281.

208. *Трахтенброт А.А., Барздинь Я.М.* Конечные автоматы (поведение и синтез). – М.: Наука, 1970. – 400 с.

209. *Тренькаев В.Н., Колесников Р.Г.* Автоматный подход к атакам на симметричные шифры // Вестник Томского государственного университета. Приложение. − 2007. − № 23. − С. 130-135.

210. *Трубачев А.П. и др.* Оценка безопасности информационных технологий. – М.: СИП РИА, 2001. – 356 с.

211. Труды по дискретной математике. − **Т.1** / Под общей редакцией *В.Я. Козлова*. − М.: ТВП, 1997. − 280 с.

212. Труды по дискретной математике. − **Т.2** / Под общей редакцией *В.Я. Козлова*. М.: ТВП, 1998. ─ 314 с.

213. *Тужилин М.Э.* Стандарт США шифрования данных АЭС и криптографические методы его анализа //Вестник Томского государственного университета. Приложение.− 2004. − № 9(I). − С. 89- 94.

214. *Тужилин М.Э.* Криптографические принципы создания блочных шифров // Вестник Томского государственного университета. Приложение. − 2007. − № 23. − С. 135-139.

215. *Турбин А.Ф.* Мультифрактальные методы сверхглубокой защиты информации // Фрактальний аналіз та суміжні питання. – Київ: ІМ НАН України − НПУ ім. Драгоманова. – 1998. – № 1. – С. 27-33.

216. *Турбин А.Ф., Працевитый Н.В.* Фрактальные множества, функции, распределения. – Киев: Наук. думка, 1992. – 208 с.

217. *Тыкулов Е.В.* Построение нестационарных поточных криптосистем на основе автоматных моделей // Искусственный интеллект. − 2004. − № 1. − С. 120-128.

218. *Харин Ю.С. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.

219. *Хилл Ф.* OpenGl. Программирование компьютерной графики. Для профессионалов. – СПб.: Питер, 2002. – 1088 с.

220. *Фараджев Р.Г.* Линейные последовательностные машины. − М.: Советское Радио. − 1975. − 248 с.

221. Федеральный стандарт обработки информации FIPS PUB 186 // NIST USA. − 1996.

222. *Фомичев В.М.* Дискретная математика и криптология. Курс лекций. – М.: Диалог-МИФИ, 2003. – 400 с.

223. *Черемисинов Д.И.* Формальные методы, используемые при защите программ // Вестник Томского государственного университета. Приложение. – 2005. – № 14. − С. 126-132.

224. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.

225. *Черемушкин А.В*. Проблемы автоматизации анализа безопасности протоколов // Вестник Томского государственного университета. Приложение. – 2005. – № 14. − С. 133-138.

226. *Чмора А.Л*. Современная прикладная криптография. – М.: Гелиос АРВ, 2002. – 256 с.

227. *Шеннон К.Э*. Теория связи в секретных системах // *Шеннон К.Э*. Работы по теории информации и кибернетики. – М.: ИЛ, 1963. – С. 333-402.

228. *Шнайер Б*. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368 с.

229. *Шнайер Б*. Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2003. – 816 с.

230. *Шустер Г*. Детерминированный хаос. – М.: Мир, 1985. – 255 с.

231. *Щеглов А.Ю*. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004. – 384 с.

232. *Щербаков А.Ю*. Введение в теорию и практику компьютерной безопасности. – М.: Издатель Молгачева С.В., 2001. – 352 с.

233. *Элспас Б*. Теория автономных линейных последовательных сетей // Кибернетический сборник, 1963. – Вып. 7. – С. 90-128.

234. *Ященко В.В*. Введение в криптографию. – М.: МЦНМО-ЧеРО, 1999. – 272 с.

235. *Adams C.M., Tavares S.E*. The structured design of cryptographically good S-boxes // Journal of Cryptology. – 1990. – Vol. 3. – № 1. – P. 27-41.

236. *Adams C.M., Tavares S.E*. Good S-boxes are easy to find // Proceedings of Advances in Cryptology (CRYPTO'89). Lecture Notes in Computer Science. – Springer-Verlag. – 1990. – Vol.435. – P. 612-615.

237. *Aldeman L*. A sub-exponential algorithm for the discrete logarithm problem with applications to cryptography // IEEE 18th Annual Symposium on Foundations of Computer Science. – 1979. – P. 55-60.

238. *Alia M.A., Samsydin A.B.* New key exchange protocol based on Mandelbrot and Julia fractal sets // International Journal of Computer Science and Network Security. – 2007. – Vol. 7. – № 2. – P.302-307.

239. *Ashwin P., Rucklidge A.M., Sturman R.* Cyclic attractors of coupled cell systems and dynamics with symmetry // Syncronization: Theory and Application. NATO Science Series. II. Mathematics, Physics and Chemistry.Vol. 109. − 2003. – Kluver Academic Publishers. – P. 5-23.

240. *Ben-Aroya I., Biham E*. Differential analysis of Lucifer // Proceedings of Advances in Cryptology − CRYPTO'93. – Springer-Verlag. – 1993. – P. 187-199.

241. *Bell D.E., LaPadula L.J*. Secure computer systems: unified expositional multics interpretation. – Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev. 1.

242. *Bender W. et. al*. Techniques for data hiding // IBM Systems Journal. – Vol. 35.− N 3,4. – 1996.

243. *Bennett C.H. et. al.* Quantum cryptography, or unfirable subway tokens // Proceedings of Crypto'82. – N.Y.: Plenum Press. – 1982. – P. 267-275.

244. *Bennett C.H., Brassard G.* Quantum public key distribution system // IBM Techn. Disclosure Bulletin. − Vol. 28. − 1985. − P. 3153-3164.

245. *Bennett C.H., Brassard G.* Quantum public key distribution reinvented. − SIGACT News. − 1987. − 18. – № 4. – P. 51-53.

246. *Bennett C.H., Brassard G., Ekert A.K.* Quantum cryptography // Scientific American. – 1992. – P. 50-57.

247. *Bennett C.H. et. al.* Experimental quantum cryptography // Journal of Cryptology. – 1992. – № 1. − P. 3-28.

248. *Bennett C.H. et. al.* Strength and weakness of quantum computer. – SIAM Journal on Computing. – 1997. – **26.** − № 5. – P. 1510-1523.

249. *Beth T., Ding C.* On almost perfect nonlinear permutations // Proceedings of Advances in Cryptology − EUROCRYPT'93. Lecture Notes in Computer Science. – NY: Springer-Verlag. – 1993. − Vol 765.– P. 65-76.

250. *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – № 1. − P. 3-72.

251. *Birykov A.* Block ciphers and stream ciphers: the state of the art // http://eprint.iarc.org/2004/094.

252. *Bishop M.* Computer security: art and science. − ISBN 0-201-44099-7, 2002. ─ 1084 p.

253. *Bollobás B.* Modern graph theory. – Springer-Verlag, 1998. – 394 p.

254. *Brassard G.* Resent developments in quantum cryptography // PRAGOCRYPT'96. – Prague. – 1996.

255. *Burrows M., Abadi M., Needham R.A.* A logic of authentication // ACM Transactions On Computer Systems – 1990. – Vol. 8. – № 1. – P. 18-36.

256. *Canteaut A., Trabbia M.* Ciphertext only reconstructing of stream ciphersbased on combination generators // Fast Software Encryption'2000. Lecture Notes in Computer Science. – NY: Springer-Verlag. – 2001. − Vol. 1978. – P. 165-180.

257. *Chepyzhov V., Smeets B.* A simple algorithm for fast correlation attack on stream ciphers // Fast Software Encryption'2000. Lecture Notes in Computer Science. – NY: Springer-Verlag. – 2001. − Vol. 1978. – P. 181-195.

258. *Courtois N. et. al.* Efficient algorithms for solving overdefined systems of multivariate polynomial equations // EUROCRYPT 2000: Lecture Notes in Computer Science. – 2000. – Vol. 1807. – P.392-407.

259. *Courtois N. et. al.* Solving underdefined systems of multivariate quadratic equations // PKC 2002: Lecture Notes in Computer Science. – 2002. — Vol. 2274. – P. 211-227.

260. *Courtois N., Pieprzyk J.* Cryptanalysis of block ciphers with overdefined systems of equations // ASIACRYPT 2002: Lecture Notes in Computer Science. – 2002. – Vol. 2501. – P. 267-287.

261. *Courtois N., Meier W.* Algebraic attack on stream ciphers with linear feedback // EUROCRYPT 2003: Lecture Notes in Computer Science. – 2003. – Vol. 2656. – P. 345-349.

262. *Deutsch D.* Quantum theory, the Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London. Ser A. A439. − P. 553-558.

263. *Dmitriev A.S. et. al.* Basic principles of direct chaotic communications // Syncronization: Theory and Application. NATO Science Series. II. Mathematics, Physics and Chemistry.Vol. 109. − 2003. – Kluver Academic Publishers. – P. 41-63.

264. *Even S.* On information-lossless automata of finite order // IEEE Transactions on Electronic Computers – 1965. – Vol. C-14. – № 4. – P. 561-569.

265. *Hennie F.C.* Finite state models for logical machines. NY: John Wiley&Sons Inc., 1962. − 466 p.

266. *Hibbard T.N.* Least upper bounds on minimal terminal state experiments for two classes of sequential machines // Journal of Association of Computer Mathematics – 1961. – № 8. – P. 601-612.

267. *Huffman D.A.* Canonical forms for information-lossless finite state logical machines // IRE Transactions Circuit Theory. Special Supplement. – 1959. – Vol. CT-6. – P. 41-59.

268. *Huges R.J. et. al*. Secure communications using quantum cryptography. – Photonic Quantum Computing. – 1997. – Vol. 3076. – P. 2-11.

269. *Izotov B.V., Moldovyan A.A., Moldovyan A.A.* Controlled operations as a cryptographic primitive // Methods, Models and Architectures for Networking Security: Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 2052. – P. 230-241.

270. *Kiny J*. Algorithm for complete automated cryptanalysis of periodic polyalphabetic substitution ciphers // Cryptologia. – 1994. – Vol. 18. − № 4. – P. 332-355.

271. *Koblitz N*. Hyperelliptic cryptosystems // Journal of Cryptology. – 1989.– № 1.– P. 139- 150.

272. Kohavi Z. Switching and finite automata theory. – McGrow-Hill Book Company: NY, 1970. – 592 p.

273. *Kohda T*. Information sources using chaotic dynamics // Proceedings of IEEE. – 2002. – **90.** – № 5. – P. 641-661.

274. *Kosarev L*. Chaos-based cryptography: a brief overview // IEEE Circuits and Systems Magazine. ─ 2001. ─ **1.** ─ P. 6-21.

275. *Kosarev L., Tasev Z.* Public-key encryption based on Chebushev maps // Proceedings of the IEEE Symposium on Circuits and Systems (ISCAS 2003). – 2003. – № 3. – P. 28-31.

276. *Kotulski Z. at. al*. Application of discrete chaotic dynamical systems in cryptography − DCC method // International Journal of Bifurcation and Chaos. – 1999. – № 9. – P. 1121-1135.

277. *Kotulski Z. at. al*. On constructive approach to chaotic pseudorandom number generator // RCMCIS. – 2002.

278. *Kurakin V.L. et. al*. A linear recurring sequences over rings and modules // Inst. of Math. Science. Contemporary Mathematics and its Applications. Thematic Surveys. – Vol. 10. – 1994.

279. *Kuzmin A.S. et. al*. A linear recurring sequences over rings and modules // Journal of Mathematical Sciences. – 1995. – Vol. 76. – № 6. – P. 2793-2915.

280. *Lanawehrm E. at. al*. A security model for military message system // ACM. Transactions on Computer Systems. – 1984. – Vol. 9. – № 3.

281. *Lo H.-K., Chau H.F*. Unconditional security in quantum cryptography // Science. – 1999. – **283.** – P. 2050-2056.

282. *Lynch N*. I/O automaton models and proofs for shared-key communication systems // Proceedings of the 12th IEEE Computer Security Foundations Workshop (CSFW'99), Mordana, Italy, June, 28-30, 1999. – 16 p.

283. *Masuda N., Aihara K*. Cryposystem with discretized chaotic maps // IEEE Transactions on Circuits and Systems 1: Fundamental Theory and Applications. – 2002. – **49.** – № 1. – P. 28-39.

284. *Matsui M*. Linear cryptanalysis methods for DES cipher // Advances in Cryptology (EUROCRYPT'93), Proceedings. − Springer-Verlag. − 1994. − P. 386-397.

285. *Maurer U., Wolf S*. Information-theoretic key agreement: from weak to strong secrecy for free // Advances in Cryptology (EUROCRYPT'00), Lecture Notes in Computer Science. – 2000. – P.351-368.

286. *Meier W., Staffelbach O*. Fast correlation attacks on certain stream ciphers // Journal of Cryptology. – 1989. – Vol. 1. − P. 159-176.

287. *Menezis A., van Oorschot P., Vanstone S*. Handbook of applied cryptography. − CRC Press, 1997. − 780 p.

288. *Maurer U*. Information-theoretically secure secret-key agreement by not authenticated public discussion // Advances in Cryptology (EUROCRYPT'97), Lecture Notes in Computer Science. – 1997. – P. 209-225.

289. *Nicolis J.S.* Chaotic dynamics as applied to information processing. – Rep. Prog. Phys. − 1986. – Vol. 49. – P.1109-1187.

290. *Nuborg K.* On the construction of highly nonlinear permutations // Advances in Cryptography − EUROCRYPT'92, Lecture Notes in Computer Science. – Springer-Verlag. – 1993. – Vol. 658. – P. 92-98.

291. *Odlyzko A.M.* The future of integer factorization // CryptoBites. – 1995. – **1.** – № 2. – P. 5-12.

292. *Odlyzko A.M.* Dictere algorithms: the past and the future // Designs, Codes and Cryptography. – 2000. – **19.** – P. 129-145.

293. *Poovendran R., Baras J.S.* An information theoretic analysis of rooted-tree based secure multicast key distribution schemes // Advances in Cryptology (CRYPTO'99). − 1999. – P. 624-628.

294. Proceedings of the 7th International Specialist Workshop on Nonlinear Dynamics of Electronic Systems (NDES'99) (Rønne, Island of Bornholm, Denmark, July 15-17, 1999). Technical University of Denmark, Technical University of Dresden, 1999. − 294 p.

295. Proceedings of the NATO Advanced Study Institute on Synchronization: Theory and Application (Yalta, Crimea, Ukraine, May 19 – June 1, 2002). Kluver Academic Publishers, 2002. Series II: Mathematics, Physics and Chemistry. − 258 p.

296. *Rieffel E., Pollak W.* Backgrounds of quantum computing // ACM Computing Surveys, 2000. Vol. 3 / Перевод с англ. А.Ю. Романюк, Л.Е. Федичкин. 57 с.

297. *Rivest R., Shamir A., Adleman I.* A method for obtaining digital signatures and public key cryptosystem // ACM Communications. – 1978. – **21.** – № 2. – P. 120-126.

298. *Schmeiher P., Diakonos F.K.* A general approach to the localization of unstable periodic orbits in chaotic dynamical systems // Physical Review. – 1998. − **E. 57.** − P. 2739-2751.

299. *Shamir A.* A polynomial time algorithm for breaking. The basic Merkle-Hellman cryptosystem // Proceedings of the 23rd FOCS Symposium. – 1982. – P. 145-152.

300. *Shamir A.* Embedding cryptographic trapdoors in arbitrary knapsack system // MIT Laboratory for Computer Science Technical Report 230. − 1982.

301. *Shary S.P.* Algebraic approach to the linear static identification. Tolerance and control problem, or one more application of Caucher arithmetic // Reliable Computing. − 1996. − Vol. 2. − № 1. − P. 3-33.

302. *Shor P.W.* Polynomial-time algorithms on a quantum computer // Society for Industrial and Applied Mathematics Journal on Computing. – 1997. – **26.** − № 5. – P.1484-1509.

303. *Sigentaler T.* Decrypting a class of stream ciphers using ciphertext only // IEEE Transactions on Computers. – 1985. – Vol.34. − №1. – P. 81-85.

304. *Skobelev V.V.* Solving of nonlinear functional equations by substitution method // Octogon. – 2002. – Vol. 10. – № 2. – P. 765-776.

305. *Skobelev V.G.* Non-stationary secret lock: model and checking. − Proceedings of IEEE East-West Design&Test Workshop (EWDTW'04). – Kharkov: KNURE, 2004. − P. 117-122.

306. *Skobelev V.G.* On Complexity of Checking of Cryptosystems. − Proceedings of IEEE East-West Design&Test Workshop (EWDTW'06). – Sochi, Russia, September 15-19, 2006. − P.82-88.

307. *Skobelev V.G.* Fault-tolerant discrete dynamical systems over finite ring. − Proceedings of the IXth International Conference CADSM 2007 (Lviv-Polyana, Ukraine, 20-24 February 2007). − P. 357-361.

308. *Skobelev V.G.* Automata-based anticipatory systems // International Journal of Computing Anticipatory Systems. − Vol. 15. − 2004. − P. 109-124.

309. *Starke P*. Uber experimente an automaten // Zetschr. f. Math. Logic und Grundl. d. Math. – 1967. – **13**. – P.67-80.

310. *Vaudeney S*. Decorrelation: a theory for block cipher security // Journal of Cryptology. – 2003. – № 4. − P. 249-286.

311. *Wiener M*. Cryptanalysis of short RSA secret exponents // IEEE Transactions on Information Theory. – 1990. – Vol. IT-36.

312. *Yannakakis M., Lee D*. Testing finite state machines: fault detection // Journal of Computer and Systems Science. – 1995. – Vol. 50. – P. 209-277.

313. *Zierler N., Mills W.H*. Products of linear recurring sequences // Journal of Algebra. – 1973. – Vol. 27. – № 1. – P. 147-157.

Подписано к печати 11.02.2009 г. Формат 60x84 1/16.
Усл. печ. л. 29,94. Печать лазерная. Заказ № 8129. Тираж 300 экз.

Отпечатано в ООО «Цифровая типография».
г.Донецк, ул. Челюскинцев, 291а. Тел.: (062) 388-07-31, 388-07-30