МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Нестеренко Алексей Юрьевич

Математические методы обеспечения защищенного взаимодействия средств защиты информации

специальность 2.3.6
«Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва — 2023 г.

Диссертация выполнена на кафедре компьютерной безопасности департамента прикладной математики Московского института электроники и математики им. А.Н. Тихонова федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики».

Научный консультант — *Чирский Владимир Григорьевич*
доктор физико-математических наук, профессор, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», кафедра математического анализа механико-математического факультета, профессор

Официальные оппоненты — *Алиев Физули Камилович*
доктор физико-математических наук, доцент, Министерство обороны Российской Федерации, Департамент информационных систем, консультант

— *Логачев Олег Алексеевич*
доктор физико-математических наук, доцент, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», кафедра информационной безопасности факультета вычислительной математики и кибернетики, доцент

— *Смышляев Станислав Витальевич*
доктор физико-математических наук, ООО «КРИПТО-ПРО», заместитель генерального директора

Защита диссертации состоится 18 октября 2023 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.012.3 ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27), а также на портале: `https://dissovet.msu.ru/dissertation/012.3/2604`

Автореферат разослан 28 июня 2023 г.

Ученый секретарь
диссертационного совета МГУ.012.3,
к.ф.-м.н. Галатенко
Алексей Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертация посвящена решению проблемы построения и математического обоснования безопасности криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи.

Решение данной проблемы является важным в теоретическом и практическом отношении для разработки отечественных средств, применяемых для защиты информационных систем, информационно-телекоммуникационных сетей связи, автоматизированных систем управления, а также, для защиты критической информационной инфраструктуры Российской Федерации.

В диссертационной работе разработан математический аппарат, позволяющий строить криптографические протоколы и их формализованные модели на основе предъявляемых требований по безопасности.

Использование формализованных моделей позволяет свести задачу оценки безопасности криптографического протокола к определению трудоемкости решения ряда сложных математических задач, в частности, задачи дискретного логарифмирования, задаче определения начального заполнения генератора псевдослучайных последовательностей, задаче построения коллизии для сжимающего отображения и т.п. В диссертационной работе рассматриваются способы решения указанных задач, а также методы выбора параметров криптографических протоколов при которых рассматриваемые задачи оказываются трудноразрешимыми.

Диссертация представляет результаты исследований в области математических проблем информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) по следующим областям исследований:

- теория и методология обеспечения информационной безопасности и защиты информации;
- методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида;
- модели и методы оценки защищенности информации и информационной безопасности объекта;
- технологии идентификации и аутентификации пользователей и субъектов информационных процессов;
- принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности;
- исследования в области безопасности криптографических алгоритмов, криптографических примитивов и криптографических протоколов.

Актуальность темы. Необходимость проведения научных исследований в целях создания перспективных средств обеспечения информационной безопасности определяется Доктриной информационной безопасности Российской Федерации. Области применения результатов таких исследований определяются Федеральным законом

«О безопасности критической информационной инфраструктуры Российской Федерации», постановлением Правительства РФ о реализации государственной программы «Информационное общество», а также рядом приказов отраслевых министерств и ведомств.

В подавляющем большинстве случаев использование средств обеспечения информационной безопасности возможно только после проведения процедуры их сертификации и проверки выполнения требований, предъявляемых ФСТЭК и ФСБ России. При проведении указанной процедуры важным фактором является получение обоснованных оценок показателей мер защиты, реализуемых средствами защиты информации и, в частности, входящими в их состав криптографическими протоколами. Высокий уровень защиты информации, обеспечиваемый криптографическими протоколами, является необходимым фактором для обоснования безопасности передаваемой информации.

При передаче информации ее безопасность обеспечивается, как правило, совокупностью нескольких криптографических протоколов:

- протоколом односторонней, взаимной или многосторонней аутентификации участников информационного взаимодействия,
- протоколом выработки общей для участников взаимодействия ключевой информации, действующей в рамках одной сессии информационного взаимодействия,
- транспортным протоколом, предназначенным для передачи защищенной информации по каналам связи,
- процедурами выработки производной ключевой информации, контроля за временем и объемом используемой ключевой информации,
- вспомогательными протоколами, предназначенными для передачи ошибок информационного взаимодействия, квитирования абонентов, инициализации процедуры выработки нового сессионного ключа и т.п.

Указанной совокупностью протоколов ограничивается область диссертационных исследований. Выбор конкретного криптографического протокола, применяемого в средстве защиты информации, проводится с учетом большого числа факторов, к которым могут быть отнесены — число участников информационного взаимодействия, объем передаваемой информации, срок действия информационной системы или телекоммуникационной сети связи, свойства открытого канала связи, по которому передается информация, тип используемой ключевой информации и т.д.

Различные эксплуатационные требования к применяемым криптографическим протоколам приводят к необходимости разработки как универсальных решений и включения таких решений в действующую в Российской Федерации систему стандартизации, так и разработки частных решений, специализированных для конкретных условий эксплуатации. Однако во всех случаях необходимо обеспечение одинокого высокого уровня защиты информации.

Цель диссертационной работы заключается в совершенствовании методов построения криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи, а также методов получения обоснованных оценок безопасности криптографических протоколов.

Для достижения поставленной цели были решены следующие актуальные и трудные математические задачи:

- уточнения трудоемкости нахождения дискретных логарифмов в группах точек эллиптических кривых и построения параметров эллиптических кривых, обладающих заданной трудоемкостью решения задачи дискретного логарифмирования;

- выработки псевдослучайных последовательностей, удовлетворяющих предъявляемым требованиям по безопасности;

- построения режима работы блочных шифров, реализующего аутентифицированное шифрование;

- оценки численных значений показателей эффективности мер защиты для криптографических протоколов, используемых в средствах защиты информации.

Степень разработанности темы. В диссертации решены актуальные и трудные математические задачи, представляющие исключительную важность для обеспечения защищенного взаимодействия средств защиты информации. В рамках вводных разделов диссертации к каждой главе диссертации представлен исчерпывающий обзор предшествующих результатов по теме исследования, наиболее важные из которых указаны далее в разделе «Краткое содержание работы».

Научная новизна. В диссертационной работе получены следующие новые результаты.

1. Получена верхняя оценка числа шагов алгоритма Госпера, используемого для поиска двух совпадающих элементов числовых последовательностей. Автором предложен метод дискретного логарифмирования в группе точек эллиптической кривой, в основе которого лежит алгоритм Госпера, и получена асимптотическая оценка трудоемкости предложенного метода. Соответствие асимптотической оценки получаемым на практике значениям подтверждено результатами практических экспериментов на ЭВМ.

2. Доказана теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного. Получены точные оценки трудоемкости такого алгоритма и объема используемой им памяти. Предложено два различных способа реализации рассматриваемого алгоритма, позволившие снизить объем используемой памяти и практически реализовать алгоритм на ЭВМ. Теоретические оценки трудоемкости алгоритма подтверждены результатами практических экспериментов на ЭВМ.

3. Введено понятие «слабого» ключа и определено значение средней трудоемкости алгоритма дискретного логарифмирования в группе точек эллиптической кривой. Получено точное количество «слабых» ключей для эллиптических кривых, параметры которых рекомендованы Р 1323565.1.024-2019 для использования в средствах защиты информации.

4. Предложен алгоритм вычисления явного представления эндоморфизмов эллиптических кривых. Предъявлены ранее не известные эндоморфизмы для всех эллиптических кривых, чье кольцо эндоморфизмов изоморфно порядку мнимого квадратичного поля с числом классов равным единице.

5. Построены формы эллиптических кривых, обеспечивающие минимальную трудоемкость вычисления предъявленных эндоморфизмов. Доказана теорема о представлении натуральных чисел значениями многочленов в точках мнимого квадратичного поля. Предложен способ применения доказанной теоремы для реализации нового алгоритма вычисления кратной точки на эллиптической кривой.

6. Предъявлены усиленные, по сравнению с ГОСТ Р 34.10-2012, требования к параметрам эллиптических кривых, рекомендуемых к применению в средствах защиты информации. Предложен алгоритм построения таких эллиптических кривых. Приведены явные значения параметров построенных эллиптических кривых, доказывающие возможность достижения предъявленных требований.

7. Доказана теорема об иррациональности значений действительных чисел, определяемых рядами специального вида. Предложены новые алгоритмы представления действительных чисел специального вида в виде систематической дроби по произвольному основанию и способ применения предложенных алгоритмов для выработки псевдослучайных последовательностей. Получены верхние оценки объема памяти, необходимого для реализации предложенных алгоритмов.

8. Доказана теорема об оценках неизвестных коэффициентов действительных чисел специального вида. Автором работы предложены алгоритмы восстановления неизвестных коэффициентов по известному рациональному приближению числа специального вида. Доказаны утверждения о невозможности применения предложенных алгоритмов для построения более точных рациональных приближений.

9. Предложен метод локальной аутентификации пользователей средств защиты информации, основанный на алгоритме представления действительных чисел специального вида в виде систематической дроби по произвольному основанию.

10. Определен новый класс ключевых функций хэширования, представляющих собой линейные формы от перестановок на множестве кодов аутентификации. Доказаны теоремы о том, что функции из данного класса являются равновероятными функциями относительно сжимаемых сообщений и строго равновероятными функциями относительно множества ключей.

11. Предложен режим аутентифицированного шифрования, в основе которого лежит построенный класс равновероятных ключевых функций хэширования. Доказана теорема о выполнении свойства равновероятности для сжимающего отображения предложенного режима при фиксированных ключах шифрования и аутентификации. Приведены результаты практической реализации предложенного режима, показывающие его преимущество в скорости при программной реализации над регламентированными в Российской Федерации алгоритмами аутентифицированного шифрования.

12. Построена гибридная схема и ряд ее модификаций, реализующих процесс шифрования с помощью полиномиального преобразования. Определена модель возможностей нарушителя и, в этой модели, доказана теорема о стойкости предложенной схемы шифрования относительно задач определения секретного ключа аутентификации, дешифрования и навязывания сообщений. Предложен протокол передачи ключевой информации, основанный на использовании рассматриваемой гибридной схемы шифрования.

13. Предложен новый протокол выработки общего ключа со взаимной аутентификацией субъектов взаимодействия. Доказана теорема о стойкости предложенного протокола относительно задач определения общего ключа, дешифрования и навязывания передаваемой в ходе выполнения протокола информации. Предложено семейство криптографических протоколов, предназначенное для обеспечения защищенного взаимодействия в сетях «Интернета вещей».

14. Автором предъявлена формальная модель, имитирующая криптографический протокол в виде дискретной динамической системы. В рамках данной модели формализован перечень свойств безопасности и определены показатели эффективности мер защиты, обеспечиваемых криптографическим протоколом. Для получения численных значений показателей эффективности мер защиты предложен метод, использующий оценки трудоемкости компрометации криптографических преобразований, изменяющих состояния дискретной динамической системы.

15. Предложена методика проведения исследования безопасности криптографических протоколов.

Теоретическая значимость работы. Результаты исследования развивают методы оценки безопасности средств защиты информации, использующих математический аппарат эллиптических кривых.

Автором найден нетривиальный алгоритм решения задачи дискретного логарифмирования в группе точек эллиптической кривой, трудоемкость которого зависит от разыскиваемого неизвестного значения. Это привело не только к корректировке методов выбора параметров эллиптических кривых, но и к необходимости выработки секретных ключей криптографических схем и протоколов из множества значений, на которых найденный алгоритм имеет максимальную трудоемкость.

Предложенный автором способ выработки псевдослучайных последовательностей удовлетворил требованиям, традиционно накладываемым на криптографические датчики случайных чисел, а также обеспечил ряд дополнительных эксплуатационных характеристик, например, существенно затруднил реализацию датчиков на программируемых логических интегральных схемах.

Разработанный в диссертации новый класс ключевых сжимающих отображений, а также свойства, которыми данный класс обладает, позволили не только разработать несколько новых режимов аутентификационного шифрования для блочных шифров, но и обеспечить возможность высокоэффективной реализации данных режимов на вычислительных средствах с различной архитектурой.

Разработанная в работе методика проведения исследований безопасности криптографических протоколов является на настоящий момент единственным математически обоснованным документом, позволяющим не только проводить комплексные исследования всех факторов, влияющих на безопасность криптографического протокола, но и получать численные значения показателей мер защиты информации.

Практическая значимость работы. Результаты диссертационных исследований автора были использованы при подготовке положительных заключений о возможности применения ряда государственных стандартов и рекомендаций по стандартизации в области криптографической защиты информации, в частности, ГОСТ Р 34.10-2012 «Процессы формирования и проверки электронной цифровой подписи», Р 1323565.1.004-2017 «Схемы выработки общего ключа с аутентификацией на основе

открытого ключа», Р 1323565.1.018-2018 «Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта», Р 1323565.1.024–2019 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов», Р 1323565.1.028–2019 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств».

Результаты выносимые на защиту.

- Доказательство теоремы 1.2 об оценке числа шагов алгоритма Госпера, используемого для поиска двух совпадающих элементов числовых последовательностей.
- Алгоритм решения задачи дискретного логарифмирования в группе точек эллиптической кривой, основанный на методе Госпера и асимптотическая оценка сложности данного алгоритма.
- Доказательство теоремы 1.3 об алгоритме дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного, а также точные оценки трудоемкости такого алгоритма и объема используемой им памяти.
- Два варианта (однопоточный и параллельный) алгоритма решения задачи дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного.
- Алгоритм вычисления явного представления эндоморфизмов эллиптических кривых, а также явный вид эндоморфизмов для всех эллиптических кривых, чье кольцо эндоморфизмов изоморфно порядку мнимого квадратичного поля с числом классов равным единице.
- Доказательство теоремы 1.6 о представлении натуральных чисел значениями многочленов в точках мнимого квадратичного поля, и алгоритм вычисления кратной точки эллиптической кривой, основанный на утверждении доказанной теоремы.
- Алгоритм построения эллиптических кривых, удовлетворяющих усиленным, по сравнению с ГОСТ Р 34.10-2012, требованиям к параметрам эллиптических кривых, а также явные значения построенных параметров.
- Доказательство теоремы 2.1 об иррациональности действительных чисел, определяемых рядом $\alpha = \sum_{k=0}^{\infty} \frac{x_k}{k!}$ для периодической последовательности рациональных чисел $(x_k)_{k=0}^{\infty}$.
- Доказательство теоремы 2.3 об оценке неизвестных натуральных значений $x_1, \ldots, x_m$, участвующих в определении действительного числа $\alpha = \sum_{n=0}^{\infty} \sum_{i=1}^{m} \frac{u_i b^{-n}}{dn+x_i}$, при известных значениях $b, d, u_1, \ldots, u_m$ и известном рациональном приближении к α.
- Алгоритм вычисления неизвестных элементов периодической последовательности $(x_k)_{k=0}^{\infty}$, определяющих действительное число $\alpha = \sum_{k=0}^{\infty} \frac{x_k}{k!}$, при известном рациональном приближении к α.
- Доказательство утверждений (см. теоремы 2.4 и 2.5) о совпадении разложений в систематическую дробь, а также доказательство критерия (см. теорему 2.6) нормальности действительных чисел из рассматриваемых классов.

- Алгоритм преобразования парольной информации, используемый для локальной аутентификации пользователей средств защиты информации.

- Новый класс ключевых функций хэширования, представляющих собой линейные формы от перестановок на множестве кодов аутентификации. Доказательство теорем 3.1, 3.2 и 3.3 о том, что функции из данного класса являются равновероятными функциями относительно сжимаемых сообщений и строго равновероятными функциями относительно множества ключей.

- Режим аутентифицированного шифрования и доказательство теоремы 3.4 о выполнении свойства равновероятности для сжимающего отображения предложенного режима при фиксированных ключах шифрования и аутентификации.

- Гибридная схема, реализующая процесс шифрования с помощью полиномиального преобразования, а также доказательство теоремы 4.1 о стойкости предложенной схемы шифрования относительно задач определения секретного ключа аутентификации, дешифрования и навязывания сообщений.

- Протокол выработки общего ключа со взаимной аутентификацией субъектов взаимодействия, а также доказательство теоремы 4.2 о стойкости предложенного протокола относительно задач определения общего ключа, дешифрования и навязывания передаваемой информации.

- Формальная модель, имитирующая криптографический протокол в виде дискретной динамической системы, а также метод получения численных значений показателей эффективности мер защиты, использующий оценки трудоемкости компрометации криптографических преобразований, изменяющих состояния дискретной динамической системы.

- Методика проведения исследования безопасности криптографических протоколов.

Методы исследования. В рамках диссертационного исследования применяются математические методы алгебры, теории чисел, алгебраической геометрии и теории функций комплексного переменного, теории вероятностей и математической статистики, а также теории автоматов.

Достоверность результатов. Достоверность полученных результатов обеспечивается строгими математическими выкладками и доказательствами, апробацией на конференциях и семинарах, а также публикациями в рецензируемых научных журналах. Результаты других авторов, упомянутые в тексте диссертации, отмечены ссылками на соответствующие публикации.

Апробация работы. Результаты, полученные в диссертации, докладывались на международных и всероссийских конференциях и научно-исследовательских семинарах.

- Семинар научного руководителя Московского института электроники и математики им. А.Н. Тихонова федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики», г. Москва, 2022 г.

- Междуднародный симпозиум XVII International Symposium Problems of Redundancy in Information and Control Systems, г. Москва, 2021 г.
- Научно-практическая конференция «РусКрипто», г. Солнечногорск, 2021 г., 2015 г., 2012 г.
- Международная конференция «Компьютерная безопасность и криптография SIBECRYPT-18», г. Абакан, 2018 г.
- Международный симпозиум «Современные тенденции в криптографии CTCrypt», г. Суздаль, 2018, г. Казань, 2015 г.
- Семинар «Математические методы криптографического анализа» кафедры информационной безопасности факультета вычислительной математики и кибернетики МГУ им. В.В. Ломоносова», г. Москва, 2023 г., 2018 г.
- Всероссийский симпозиум по прикладной и промышленной математике ВСППМ, г. Сочи, 2016 г.
- Международная конференция Indo-Russian conference on Algebra, Number Theory, Discrete Mathematics and their Applications, г. Москва, 2014 г.
- Международународный симпозиум «The 7th International Computer Science Symposium in Russia», г. Нижний Новгород, 2014 г.
- Международная конференция «Алгебра и теория чисел: современные проблемы и приложения», г. Саратов, 2013 г., 2012 г.
- XXXIII-я дальневосточная математическая школа-семинар им. академика Е.В. Золотова, г. Владивосток, 2008 г.
- Третья международная научная конференция по проблемам безопасности и противодействия терроризму, г. Москва, 2007 г.
- Седьмая международная научно-техническая конференция «Новые информационные технологии и системы», г. Пенза, 2006 г.

Публикации по теме исследования. Результаты работы изложены в 29 публикациях; в том числе, в 21 публикации в изданиях, индексируемых в Web of Science, Scopus, RSCI и входящих в списки ВАК Минобрнауки России; из них 15 – в изданиях, индексируемых в Web of Science, Scopus, RSCI. Также автором получены 4 свидетельства о государственной регистрации программ для ЭВМ.

Структура и объем работы. Диссертация состоит из введения (общей характеристики работы), четырех глав, заключения, списка литературы, включающего 395 источников, и приложения с программами для ЭВМ. Общий объем диссертации составляет 426 (без приложения — 397) страниц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В **первой** главе диссертационной работы развивается математический аппарат, необходимый для уточнения трудоемкости решения задачи дискретного логарифмирования в группе точек эллиптических кривых и построения параметров эллиптических кривых, обладающих заданной трудоемкостью решения задачи дискретного логарифмирования.

Основным преобразованием, используемым в средствах защиты информации, является операция вычисления «кратной» точки эллиптической кривой. Пусть $p > 3$ простое число и $P \in \mathcal{E}_{a,b}(\mathbb{F}_p)$ произвольная точка эллиптической кривой $\mathcal{E}_{a,b}(\mathbb{F}_p) : y^2 \equiv x^3 + ax + b \pmod p$, определенной над конечным простым полем $\mathbb{F}_p$. Точка $Q \in E_{a,b}(\mathbb{F}_p)$ называется точкой кратности $k \in \mathbb{N}$, если

$$Q = [k]P = \underbrace{P + \cdots + P}_{k \text{ раз}}.$$

Задача определения неизвестного значения k по известным точкам P, Q называется задачей дискретного логарифмирования в группе точек эллиптической кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$. Первый метод решения задачи дискретного логарифмирования, имеющий сложность, меньшую чем сложность тотального опробования, предложил в 1962 году А.О. Гельфонд[1]. Метод Гельфонда в отечественной литературе принято называть методом «согласования», в зарубежной – методом «больших и малых шагов» Д. Шенкса[2]. Данный метод применим к любой абелевой группе, а его трудоемкость оценивается величиной $O(\sqrt{q})$ групповых операций, где q порядок группы. Метод требует хранения $O(\sqrt{q})$ элементов группы, что делает его неприменимым при больших значениях q.

Большую роль в решении задачи дискретного логарифмирования сыграли методы поиска циклов в последовательностях. Самый известный метод решения этой задачи предложен в 1968 году Р. Флойдом[3]. Позднее появились методы Р. Брента, Б. Госпера[4], Р. Седжвика и Т. Сжимански[5], Г. Ниваша[6] и др.

Основываясь на методе Р. Флойда в 1975 году Дж. Поллард[7], предложил вероятностный алгоритм решения задачи дискретного логарифмирования (ρ-метод Полларда). Математическое ожидание трудоемкости его работы оценивается величиной $O(\sqrt{q})$, однако, в отличие от метода согласования, алгоритм Полларда-Флойда использует константный объем памяти. Также Поллард[8] предложил еще один вариант данного алгоритма, называемый λ-методом. В 2001 годе Э. Теске[9] предложила модификацию алгоритма Полларда-Флойда, позволившую незначительно снизить его сложность за счет использования памяти, хранящей $O(\log_2 q)$ элементов группы.

---

[1]см. гл.6, § 3 в книге Нечаев В.И. Элементы криптографии (Основы теории защиты информации). — М. : Высшая школа, 1999. — С. 109.

[2]Shanks D. Class number, a theory of factorization and genera // Proceedings Of Symposium Pure Mathematics. — Vol. 20. — Providence, R. I. : AMS, 1971. — P. 415–440.

[3]см. п.3.1, задача 6b, в книге Кнут Д.Э. Искусство программирования для ЭВМ. Получисленные алгоритмы. — 3 изд. — М. : Вильямс, 2000. — Т. 2. — С. 788.

[4]Beeler M., Gosper R.W., Schroeppel R. HACKMEM. — 1972.

[5]Sedgewick R., Szymansky T.G., Yao A.C. The Complexity of Finding Cycles In Pediodic Functions // Siam Journal Of Computing. — 1982. — Vol. 11, no. 2. — P. 376–390.

[6]Nivash G. Cycle Detecting Using a Stack // Journal Information Processing Letters. — 2004.

[7]Pollard J.M. A Monte Carlo Method for Factorisation // BIT. — 1975. — no. 15. — P. 331–334.

[8]Pollard J.M. Monte Carlo methods for index computation (mod p) // Mathematics Of Computation. — 1978. — Vol. 32, no. 143. — P. 918– 924.

[9]Teske E. On Random Walks For Pollard's Rho Method // Mathematics of Computation. — 2000. — Vol. 70. — P. 809–825.

В 1998 году П. ван Ооршотом и М. Винером[10] был предложен универсальный метод поиска коллизий. Математическое ожидание трудоемкости его работы также оценивается величиной $O(\sqrt{q})$, однако он допускает эффективную параллельную реализацию. Вопросы применения метода Ооршота-Винера к группе точек эллиптических кривых рассматривались в ряде работ[11,12], также известны[13,14] результаты практического применения данного метода для простых значений p порядка 2^{112} и 2^{114}.

Развивая указанные алгоритмы в 2010 году автор диссертации предложил алгоритм дискретного логарифмирования, основанный на идеях Б. Госпера.

Рассмотрим задачу поиска двух совпадающих элементов последовательности $(a_n)_{n=0}^{\infty}$, определяемой равенством $a_{n+1} = f(a_n)$ для некоторого фиксированного отображения f. Фиксируем значение $n > 0$ и поместим во множество $M(n)$ элементы $a_{n_0},\ a_{n_1},\ \ldots$ рассматриваемой последовательности, с условием

$$n_i = \max_{r<n}\{r|\nu_2(r+1) = i\},$$

для всех возможных значений $i = 0,\ 1,\ \ldots$, где функция $\nu_2(r+1)$ возвращает наибольшую степень двойки, делящую величину $r+1$. Из определения следует, что для фиксированного значения n множество $M(n)$ конечно, содержит не более $\lfloor \log_2 n \rfloor + 1$ чисел и отличается от множества $M(n+1)$ лишь одним элементом. В § 1.2.3 диссертационной работы доказана следующая теорема.

Теорема 1.2. *Пусть заданы параметры λ и τ, определяющие длину подхода к циклу и длину цикла последовательности $(a_n)_{n=0}^{\infty}$. Тогда найдутся натуральные индексы r и $n = r + \tau$ такие, что*

1. *элемент a_r принадлежит множеству $M(n)$ и выполнено равенство $a_n = a_r$,*
2. *$\lambda + \tau \leqslant n < \lambda + 2\tau$.*

Доказательство теоремы является конструктивным и позволяет предложить алгоритм явного определения величины τ. Сравнение такого алгоритма с известными ранее приводится в следующей таблице.

Из приведенных значений следует, что алгоритм Госпера имеет наименьшую трудоемкость среди рассматриваемых алгоритмов используя при этом несколько больший объем памяти.

Алгоритм поиска длины цикла может быть использован для решения задачи дискретного логарифмирования в группе точек эллиптической кривой, т.е. отыскания натуральной величины k по известным параметрам эллиптической кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$ и точкам $P, Q \in \mathcal{E}_{a,b}(\mathbb{F}_p)$ таким, что

$$Q = [k]P, \quad P, Q \in \mathcal{E}_{a,b}(\mathbb{F}_p), \quad k \in \mathbb{Z}_q^*, \quad q = \mathtt{ord}(P).$$

[10] Oorschot P.C., Wiener M.J. Parallel Collision Search with Cryptanalytic Applications // Journal of Cryptology. — 1999. — Vol. 12. — P. 1–28.

[11] Bos J.W., Costello C., Miele A. Elliptic and Hyperelliptic Curves: A Practical Security Analysis // Public-Key Cryptography (PKC 2014). — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — P. 203–220.

[12] Wiener M.J., Zuccherato R.J. Faster Attacks on Elliptic Curve Cryptosystems // Selected Areas in Cryptography (SAC-98). — Berlin, Heidelberg : Springer Berlin Heidelberg, 1999. — P. 190–200.

[13] Solving a 112-Bit Prime Elliptic Curve Discrete Logarithm Problem on Game Consoles Using Sloppy Reduction / J.W. Bos, M.E. Kaihara, T. Kleinjung et al. // Int. J. Appl. Cryptol. — 2012. — Feb. — Vol. 2, no. 3. — P. 212–228.

[14] Solving a 114-Bit ECDLP for a Barreto-Naehrig Curve / T. Kusaka, S. Joichi, K. Ikuta et al. // Information Security and Cryptology – ICISC 2017. — 2018. — P. 231–244.

Алгоритм	*Трудомкость*	*Объем памяти*
Флойд	$\tau\left(3\left\lceil\frac{\lambda}{\tau}\right\rceil+1\right)$	3
Брент	не менее $\tau+\frac{3}{2}\max\{\lambda+1,\tau\}$	4
Теорема 1.2 (Госпер)	не более $\lambda+2\tau$	$\lceil\log_2(\lambda+2\tau)\rceil+4$

Таблица 1.2: Оценки трудоемкости и объема памяти для алгоритмов поиска длин циклов в последовательностях

Определим в качестве множества $\mathcal{M}$ — подгруппу порядка q, порожденную точкой P, т.е.

$$\mathcal{M}=\{P,\ [2]P,\ [3]P,\ \ldots,\ [q]P=\mathcal{O}\},\quad \mathcal{M}\subseteq\mathcal{E}_{a,b}(\mathbb{F}_p)$$

где $\mathcal{O}$ – бесконечно удаленная точка кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$. Зафиксируем натуральное число $s=\lceil\log_2 q\rceil$ и разобьем множество $\mathcal{M}$ на s не пересекающихся подмножеств

$$\mathcal{M}=\bigcup_{l=0}^{s-1}J_l$$

следующим образом – будем относить к подмножеству J_l те точки множества $\mathcal{M}$, у которых x-координата сравнима с l по модулю s.

Построим случайное отображение f множества $\mathcal{M}$ в себя. Для этого выберем случайным образом вычеты

$$\gamma_i,\omega_i\in_R\mathbb{Z}_q^*,\quad i=1,\ldots,s,$$

и для произвольной точки $R\in\mathcal{M}$ такой, что $R=(x,y)$ и $x\equiv l\pmod s$, определим

$$f(R)\ =\ R+[\gamma_l]P+[\omega_l]Q,\quad \text{если}\quad R\in J_l.$$

Используем построенное отображение для выработки последовательности точек $\{R_n\}_{n=0}^{\infty}$ множества $\mathcal{M}$. Выберем в качестве начальной точки

$$R_0=[\alpha_0]P+[\beta_0]Q,\quad \alpha_0,\beta_0\in_R\mathbb{Z}_q^*,$$

где α_0,β_0 – случайные вычеты из $\mathbb{Z}_q^*$, и определим

$$R_{n+1}=f(R_n)=R_n+[\gamma_l]P+[\omega_l]Q,\quad \text{если}\quad R_n\in J_l.$$

Для каждой точки R_n найдется номер $l_n\in\mathbb{Z}_s$ такой, что $R_n\in J_{l_n}$. Тогда для любого индекса $n=0,1,\ldots$получаем равенство

$$\begin{aligned}R_{n+1}&=R_n+[\gamma_{l_n}]P+[\omega_{l_n}]Q=\\&=R_{n-1}+[\gamma_{l_{n-1}}]P+[\omega_{l_{n-1}}]Q+[\gamma_{l_n}]P+[\omega_{l_n}]Q=\ldots\end{aligned}$$

$$\begin{aligned}\cdots&=R_0+\left[\sum_{j=0}^{n}\gamma_{l_j}\pmod q\right]P+\left[\sum_{j=0}^{n}\omega_{l_j}\pmod q\right]Q=\\&=\left[\alpha_0+\sum_{j=0}^{n}\gamma_{l_j}\pmod q\right]P+\left[\beta_0+\sum_{j=0}^{n}\omega_{l_j}\pmod q\right]Q=\\&=[\alpha_{n+1}]P+[\beta_{n+1}]Q,\end{aligned}$$

где $\alpha_{n+1}, \beta_{n+1} \in \mathbb{Z}_q$. Используя утверждение теоремы 1.2 можно найти два элемента R_t и R_l такие, что $R_t = R_l$, тогда

$$[\alpha_t + \beta_t k \pmod q]P = \\ = [\alpha_t]P + [\beta_t k \pmod q]P = [\alpha_t]P + [\beta_t]Q = R_t = \\ = R_l = [\alpha_l]P + [\beta_l]Q = [\alpha_l]P + [\beta_l k \pmod q]P = \\ = [\alpha_l + \beta_l k \pmod q]P.$$

Последнее равенство позволяет выразить неизвестное k через значения величин $\alpha_t, \alpha_l, \beta_t, \beta_l \in \mathbb{Z}_q$

$$k \equiv \frac{\alpha_t - \alpha_l}{\beta_l - \beta_t} \pmod q .$$

Для практической реализации описанного алгоритма необходимо использование двух массивов. Первый массив – S, будет хранить точки

$$S[l] = [\gamma_l]P + [\omega_l]Q, \quad l = 0, 1, \ldots, s-1,$$

а также выбранные ранее случайным образом вычеты $\gamma_l, \omega_l \in \mathbb{Z}_q^*$.

Во втором массиве будут храниться элементы множества $M(n)$, определяемого при вычислении n-го элемента последовательности $\{R_n\}_{n=0}^{\infty}$. Каждый элемент массива должен хранить в себе точку R, находящуюся во множестве $M(n)$, а также коэффициенты α, β, выражающие точку R через исходные точки P и Q.

Определение размера второго массива тесно связано с трудоемкостью рассматриваемого алгоритма. Рассматривая отображение $f : \mathcal{M} \to \mathcal{M}$ как случайную величину на множестве всех возможных отображений множества $\mathcal{M}$ в себя, можно записать[15,16], что

$$\lim_{q\to\infty} \frac{E_q(\lambda, f)}{\sqrt{q}} = \lim_{q\to\infty} \frac{E_q(\tau, f)}{\sqrt{q}} = \sqrt{\frac{\pi}{8}}.$$

Теперь, делая предположение о независимости величин λ и τ, можно считать, что асимптотическая оценка числа шагов n в рассматриваемом алгоритме следует из равенства

$$\lim_{q\to\infty} \frac{E_q(\lambda, f) + 2E_q(\tau, f)}{\sqrt{q}} = 3\sqrt{\frac{\pi}{8}}.$$

Определим $h = 2 + \lfloor \log_2 \sqrt{q} \rfloor$. Поскольку множество $M(n)$ содержит не более $\lfloor \log_2 n \rfloor + 1$ элементов последовательности $\{R_n\}_{n=0}^{\infty}$, получим неравенство

$$\lfloor \log_2 n \rfloor + 1 < \left\lfloor \log_2 3\sqrt{\frac{\pi q}{8}} \right\rfloor + 1 = \\ = \left\lfloor \frac{1}{2}\Big(\log_2 9\pi + \log_2 q - 3 \Big) \right\rfloor + 1 < \left\lfloor \frac{\log_2 q}{2} \right\rfloor + 2 = h,$$

из которого следует, что ожидаемый размер множества $M(n)$ не превысит величины h. Алгоритм был реализован автором на ЭВМ. Получаемые на практике значения величины n хорошо согласуются с ожидаемым теоретическим значением $3\sqrt{\frac{\pi q}{8}}$.

[15] Flajolet P., Odlyzko A.M. Random mapping statistics // Advances in Cryptology: Proc. Eurocrypt'89. — Vol. 434. — NY. : Springer, 1990. — P. 329–354.

[16] Колчин В.Ф. Случайные графы. — 2 изд. — М. : Физматлит, 2004. — С. 206.

Рассмотренные выше методы являются универсальными и применимы к любой абелевой группе. Для решения задачи дискретного логарифмирования в мультипликативной группе $\mathbb{F}_p^*$ известны алгоритмы[17,18], имеющие трудоемкость, меньшую чем у перечисленных ранее методов. Однако для группы точек эллиптической кривой, определенной над конечным простым полем $\mathbb{F}_p$, вопрос о построении алгоритма, имеющего алгоритмическую сложность меньшую, чем $O(\sqrt{q})$, остается открытым.

Вопросы решения задачи дискретного логарифмирования для эллиптических кривых частного вида рассматривались в работах Т. Сато и К. Араки[19], И.А. Семаева[20], Н. Смарта[21], Р. Шипси и К. Суорт[22]. Методы сведения задачи дискретного логарифмирования в группе точек эллиптической кривой к другим трудноразрешимым математическим задачам рассматривались в работах А. Менезеса, С. Ванстоуна, Т. Окамото[23], а также К. Пети, М. Костерса и А. Мессенга[24]. Следует также отметить носящие теоретический характер работы Дж. Сильвермена[25] и И.А. Семаева[26].

Алгоритмы дискретного логарифмирования, рассматриваемые в § 1.3 диссертационной работы, также представляют собой методы решения задачи в частном случае.

Одним из важных вопросов при анализе средств защиты информации является вопрос о существовании так называемых «слабых» ключей, то есть секретных значений, использование которых приводит к снижению алгоритмической сложности решения задачи, обосновывающей стойкость средства защиты информации. Примеры «слабых» ключей, применительно к задачам анализа алгоритмов блочного шифрования, можно найти в работах Н. Фергюссона[27], Дж. Ким[28], а также рекомендациях к TDEA[29]. Для задачи дискретного логарифмирования вопрос о «слабых» ключах был решен автором диссертационной работы. В § 1.3 доказана следующая теорема.

Теорема 1.3. *Пусть $p > 3$ – простое число, $\mathcal{E}_{a,b}(\mathbb{F}_p)$ эллиптическая кривая и $P \in \mathcal{E}_{a,b}(\mathbb{F}_p)$ – точка кривой, порождающая циклическую подгруппу $\langle P \rangle \subseteq E_{a,b}(\mathbb{F}_p)$ простого порядка q.*

Пусть $Q = [k]P$, $k \in \mathbb{Z}_q$ и $\mathtt{ord}_q\, k = r$. Если $q > 6$ и $r \geqslant 6$, то алгоритмическая сложность нахождения величины k не превосходит $8\sqrt{r}\log_2 q$ групповых операций.

[17]Gordon D. Discrete Logarithms in Fp Using the Number Field Sieve // SIAM J. Discrete Math. — 1993. — Vol. 6. — P. 124–138.

[18]Joux A., Lercier R. Improvements to the general Number Field Sieve for Discrete Logarithms in Prime Fields // Mathematics Of Computation. — 2003. — Vol. 72, no. 242. — P. 953–967.

[19]Satoh T., Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous curves // Comm. Math. Univ. Sancti Pauli. — 1998. — Vol. 47. — P. 81–92.

[20]Semaev I. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p // Mathematics of Computation. — 1998. — Vol. 67, no. 221. — P. 353–356.

[21]Smart N. The discrete logarithm problem on elliptic curves of trace one // Journal of Cryptology. — 1999. — Vol. 12. — P. 193–196.

[22]Shipsey R., Swart C. Elliptic divisibility sequences and the elliptic curve discrete logarithm problem. — 2008.

[23]Menezes A., Vanstone S., Okamoto T. Reducing elliptic curve logarithms to logarithms in a finite field // Proc. 23rd ACM Symp. Theory of Computing. — 1991. — P. 80–89.

[24]Petit C., Kosters M., Messeng A. Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields // Public-Key Cryptography (PKC 2016). — Berlin Heidelberg : Springer, 2016. — P. 3–18.

[25]Silverman J.H. The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem // Designs, Codes and Cryptography. — 2000. — no. 20. — P. 5–40.

[26]Semaev I. Summation Polynomials and the Discrete Logarithm Problem on Elliptic Curves. — 2004. – preprint.

[27]Ferguson N. Authentication weaknesses in GCM. — 2005.

[28]Kim J. On the security of the block cipher GOST suitable for the protection in U-business services // Personal and Ubiquitous Computing volume. — 2013. — P. 1429–1435.

[29]Barker E., Mouha N. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. — 2012. — NIST Special Publication 800-67, Revision 2.

Доказательство теоремы конструктивно и позволяет предъявить алгоритм поиска неизвестной величины k, основанный принципах «согласования» А.О. Гельфонда. Поскольку при практически важных значениях параметров эллиптической кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$ такой метод не может быть реализован на практике, автором были разработаны две его модификации, основанные на упомянутом выше λ-методе Полларда.

Зафиксируем произвольный первообразный корень g по модулю q, определим $\alpha \equiv g^{\frac{q-1}{r}} \pmod q$ и будем искать неизвестное значение k в виде $k \equiv \alpha^x \pmod q$. Рассмотрим подмножество точек на эллиптической кривой $\mathcal{M}$, определяемое равенством

$$\mathcal{M} = \{[\alpha]P,\ [\alpha^2 \pmod q]P,\ \ldots,\ [\alpha^r \pmod p]P = P\}.$$

Точка Q принадлежит рассматриваемому подмножеству $\mathcal{M}$, поскольку $Q = [k]P = [\alpha^x]P \in \mathcal{M}$ для некоторого значения $x \in \mathbb{Z}_r$.

Определим случайное отображение $f : \mathcal{M} \to \mathcal{M}$. Для этого зафиксируем $s = \lceil \log_2 r \rceil$, выберем случайным образом вычеты

$$\xi_0,\ \ldots,\ \xi_{s-1} \in_R \mathbb{Z}_r^*.$$

и для любой точки $R \in \mathcal{M}$, заданной в аффинной форме координатами (x_R, y_R), определим

$$f(R) = [\alpha^{\xi_l} \pmod q]R, \quad \text{где} \quad l \equiv x_R \pmod s$$

для некоторого $l \in \mathbb{Z}_s$.

Первая модификация алгоритма поиска неизвестного значения k использует факт пересечения двух различных последовательностей, образуемых при помощи отображения f. Выберем случайные вычеты $\gamma_0, \omega_0 \in_R \mathbb{Z}_r^*$ и определим начальные точки

$$R_0 = [\alpha^{\gamma_0} \pmod q]P, \quad U_0 = [\alpha^{\omega_0} \pmod q]Q.$$

Остальные элементы последовательностей $\{R_n\}_{n=0}^{\infty}$ и $\{U_i\}_{i=0}^{\infty}$ определим равенствами

$$R_{n+1} = f(R_n), \quad U_{n+1} = f(U_n), \quad n = 0, 1, \ldots$$

Легко видеть, что выполнены равенства

$$\begin{aligned} R_{n+1} = [\alpha^{\xi_{l_n}} \pmod q]R_n = [\alpha^{\xi_{l_n}}\alpha^{\xi_{l_{n-1}}} \pmod q]R_{n-1} = \cdots \\ = [\alpha^{\gamma_0 + \sum_{i=0}^{n}\xi_{l_i}} \pmod q]P = [\alpha^{\gamma_n} \pmod q]P \in \mathcal{M}, \end{aligned}$$

для некоторого $\gamma_n \equiv \gamma_0 + \sum_{i=0}^{n}\xi_{l_i} \pmod r$, и

$$\begin{aligned} U_{i+1} = [\alpha^{\xi_{l_i}} \pmod q]U_n = [\alpha^{\xi_{l_i}}\alpha^{\xi_{l_{i-1}}} \pmod q]U_{i-1} = \cdots \\ = [\alpha^{\omega_0 + \sum_{j=0}^{n}\xi_{l_j}} \pmod q]Q = [\alpha^{\omega_i} \pmod q]Q = [k\alpha^{\omega_i} \pmod q]P \in \mathcal{M}, \end{aligned}$$

для некоторого $\omega_i \equiv \omega_0 + \sum_{j=0}^{n}\xi_{l_j} \pmod r$.

Выберем индекс n_0, удовлетворяющий неравенству

$$n_0 \geqslant \left\lfloor \sqrt{\frac{\pi r}{2}} \right\rfloor$$

и зафиксируем точку R_{n_0}. Поскольку n_0 достаточно велико, можно ожидать, что точка R_0 лежит на цикле последовательности $\{R_n\}_{n=0}^{\infty}$. Если найдется индекс i такой, что $R_{n_0} = U_i$, то выполнено равенство

$$[\alpha^{\gamma_{n_0}} \pmod q]P = [\alpha^{\omega_i} \pmod q]Q = [k\alpha^{\omega_i} \pmod q]P.$$

и неизвестное k удовлетворяет сравнению

$$k \equiv \alpha^{\gamma_{n_0} - \omega_i} \pmod{q}.$$

При случайном выборе точек R_0 и U_0 может случиться так, что последовательности $\{R_n\}_{n=0}^{\infty}$ и $\{U_i\}_{i=0}^{\infty}$ не будут иметь общих точек. Отображение f разбивает[30] множество $\mathcal{M}$ на m не пересекающихся областей. При этом, для математического ожидания $E_r(m, f)$ величины m выполнено равенство

$$\lim_{r \to \infty} \frac{E_r(m, f)}{\log_2 r} = 1.$$

Следовательно, можно ожидать, что для нахождения совпадающих точек $R_{n_0} = U_i$ и, как следствие, определения неизвестного k, потребуется выбрать $\log_2 r$ случайных пар R_0 и U_0.

Поскольку для каждой из последовательностей $\{R_n\}_{n=0}^{\infty}$ и $\{U_i\}_{i=0}^{\infty}$ вычисляется не более n_0 элементов с трудоемкостью не более, чем $2\lceil \log_2 q \rceil$ групповых операций, а общее количество вырабатываемых пар R_0 и U_0 не превышает $\lfloor \log_2 r \rfloor$, то алгоритмическая сложность первой модификации алгоритма поиска неизвестного значения k не превышает

$$4n_0 \lfloor \log_2 r \rfloor \lceil \log_2 q \rceil < 2\sqrt{2\pi r} \log_2 r (\log_2 q + 1).$$

операций в группе точек эллиптической кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$. Данная оценка несколько хуже, чем утверждение теоремы 1.3. Вместе с тем в алгоритме требуется хранение лишь трех точек эллиптической кривой, что делает возможной его реализацию на ЭВМ при любых значениях r.

Вторая модификация алгоритма поиска неизвестного значения k комбинирует идеи λ-метода Полларда и метода поиска коллизий Ооршота-Винера. Данная модификация описывается в § 1.3.2 диссертационной работы и предназначена для реализации на ЭВМ, допускающих распараллеливание вычислений.

Для того, чтобы исключить частные случаи из рассмотрения и обеспечить высокую трудоемкость решения задачи дискретного логарифмирования необходимо выбирать параметры эллиптических кривых специальным образом. Перечни требований к параметрам эллиптических кривых могут быть найдены в стандартах ГОСТ Р 34.10-2012, BSI TR-03111 и др., в работах Д.Бернштейна и Т.Ланге[31], П.Баррето, Г.Перейры и Дж.Рикардини[32], а также автора настоящей диссертационной работы.

Напомним, что нечетное простое число называют *безопасным*, если число $\frac{p-1}{2}$ также является простым. В этом случае простое число $\frac{p-1}{2}$ принято называть простым числом Софи Жермен[33].

Пусть $0 < \alpha < \beta$ натуральные числа, $p > 3$ простое число. Мы будем называть эллиптическую кривую $\mathcal{E}_{a,b}(\mathbb{F}_p)$, определенную сравнением

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

безопасной, если найдется точка $P \in \mathcal{E}_{a,b}(\mathbb{F}_p)$ такая, что $\mathtt{ord}\, P = q$ и выполняются следующие условия:

---

[30] Flajolet P., Odlyzko A.M. Random mapping statistics // Advances in Cryptology: Proc. Eurocrypt'89. — Vol. 434. — NY. : Springer, 1990. — P. 329–354.

[31] Bernstein D., Lange T. Faster addition and doubling on elliptic curves // Advances in Cryptology: ASIACRYPT 2007. — Vol. 4833. — NY. : Springer, 2007. — P. 29–50.

[32] Barreto P., Pereira G., Ricardini J. A note on high-security general-purpose elliptic curves // Cryptology ePrint Archive, Report 2013/647. — 2013.

[33] Shoup V. A Computational Introduction to Number Theory and Algebra. — 2nd edition. — Cambridge University Press, 2009. — P. 590.

1. $m = |\mathcal{E}_{a,b}(\mathbb{F}_p)|$ и $m \neq p$;
2. p безопасное простое, т.е. $\frac{p-1}{2}$ также простое число;
3. $j(\mathcal{E}_{a,b}) \not\equiv 0$ или $1728 \pmod p$, где величина $j(\mathcal{E}_{a,b})$ определена сравнением $j(\mathcal{E}_{a,b}) \equiv 1728 \cdot \frac{4a^3}{4a^3-27b^2} \pmod p$;
4. $2^\alpha < q < 2^\beta$;
5. q безопасное простое, т.е. $\frac{q-1}{2}$ также простое число;
6. для фиксированного значения B условие $p^t \not\equiv 1 \pmod q$ выполняется для всех $t = 1, 2, \ldots, B$.

Легко видеть, что безопасная эллиптическая кривая удовлетворяет требованиям из ГОСТ Р 34.10-2012 при $\alpha = 254$ и $\beta = 256$, дополненным требованиями простоты чисел $\frac{p-1}{2}$ и $\frac{q-1}{2}$.

Первое условие из данного выше определения делает нецелесообразным применение упомянутых ранее методов Т. Сато и К. Араки, И.А. Семаева и Н. Смарта. Условие безопасности простого числа p делает нецелесообразным применения метода К. Пети, М. Костерса и А. Мессенга. Условие безопасности простого числа q минимизирует мощность множества «слабых» ключей. Последнее, шестое условие делает нецелесообразным применение метода А. Менезеса, С. Ванстоуна, Т. Окамото.

Для построения безопасных кривых автором применялся следующий подход. В начале, с использованием поиска простых чисел в арифметических прогрессиях, определяются простое число p и порядок группы точек эллиптической кривой q, удовлетворяющие перечисленным выше требованиям, после чего, с использованием математического аппарата теории комплексного умножения[34], определяются коэффициенты безопасной эллиптической кривой (впервые такой подход к построению эллиптических кривых был реализован на практике Ф. Морейном[35,36]).

Детальное описание алгоритма построения эллиптической кривой и доказательство вспомогательных утверждений, позволяющих снизить трудоемкость поиска безопасных простых p и q, содержится в § 1.5.2. В приложении к диссертационной работе содержится более 60-ти эллиптических кривых, построенных с помощью разработанной автором программной реализации предложенного алгоритма, в частности, эллиптическая кривая

$$y^2 \equiv x^3 - 3x + \\ + 30248189431475512214188672690637910310234046139542618758265309564348112627199 \\ \pmod{2^{256} - 188069}.$$

Еще одной задачей, возникающей при применении эллиптических кривых в средствах защиты информации, является задача снижения трудоемкости реализации операции вычисления кратной точки для значений p в интервале $2^{160} < p < 2^{640}$. Для ее решения принято использовать комбинации из одного или нескольких подходов:

1) оптимизация элементарных операций сложения, умножения, а также взятия обратного элемента в поле $\mathbb{F}_p$;

[34]Семинар по комплексному умножению / Ж.-П. Серр, А. Борель, К. Ивасава, Чоула // Математика. — 1968. — Т. 12. — С. 55–95.

[35]Atkin A.O.L., Morain F. Elliptic curves and primality proving // Mathematics Of Computation. — 1993. — Vol. 61. — P. 29–68.

[36]Morain F. Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm. — 1988. — RR-0911, INRIA.

2) использование проективных координат для реализации операций в группе точек эллиптической кривой;

3) использование различных представлений (форм) эллиптических кривых, позволяющих минимизировать количество элементарных операций в поле $\mathbb{F}_p$, необходимых для реализации операций сложения и удвоения точек эллиптической кривой (среди таких форм следует отметить формы Вейерштрасса, Якоби, Гессе, Монтгомери, Эдвардса, и др.);

4) использование алгоритмов вычисления кратной точки, минимизирующих количество операций сложения и удвоения в группе точек эллиптической кривой (к таким алгоритмам относятся «оконные» методы, методы с несколькими основаниями и т.п.);

5) использование оптимизаторов программного кода, минимизирующих число используемых переменных и операций пересылки данных между регистрами вычислительного средства;

6) использование эндоморфизмов эллиптической кривой.

Остановимся на последнем подходе подробнее и предположим, что нам известен комплексный эндоморфизм $\phi : \mathcal{E}_{a,b}(\mathbb{F}_p) \to \mathcal{E}_{a,b}(\mathbb{F}_p)$. В 2001 году Р. Галант, Р. Ламберт и С. Ванстоун[37] предложили использовать для вычисления кратной точки равенство

$$Q = [k]P = [k_1]P + [k_2]\phi(P),$$

где k_1, k_2 целые, зависящие от числа k и эндоморфизма ϕ коэффициенты, удовлетворяющие неравенствам $0 \leqslant k_1, k_2 \leqslant c_0\sqrt{\mathtt{ord}(P)}$ для некоторой эффективно вычислимой[38] константы c_0. Независимо, этот подход рассматривался в работах А.Г. Ростовцева[39,40]. В дальнейшем подход развивался в работах зарубежных авторов[41,42,43].

До недавнего времени было известно только четыре эллиптических кривых с явно заданным эндоморфизмом и лишь две из них могли применяться в средствах защиты информации. В 2014 году автор диссертационной работы предложил эффективно реализуемый на практике алгоритм вычисления явного вида комплексного эндоморфизма эллиптической кривой, основанный на теории комплексного умножения. Это позволило разработать программное обеспечение и вычислить явный вид эндоморфизмов для большого числа эллиптических кривых.

Зафиксируем $\tau \in \mathbb{C}_+$ – мнимую квадратичную иррациональность такую, что $\mathrm{Im}(\tau) > 0$, тогда найдется эллиптическая кривая $\mathcal{E}_{a,b}(\mathbb{F}_p)$ такая, что решетка

$$\Lambda_\tau = \{n + m\tau,\ n, m \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-d}),$$

[37] Gallant R.P., Lambert R.J., Vanstone S.A. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms // Advances in Cryptology – CRYPTO 2001. — 2001. — P. 190–200.

[38] Sica F., Ciet M., Quisquater J.J. Analysis of the Gallant-Lambert- Vanstone Method Based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves // Selected Areas in Cryptography. SAC 2002. — 2003. — P. 21–36.

[39] Ростовцев А.Г. О выборе эллиптической кривой над простым полем для построения криптографических алгоритмов // Проблемы информационной безопасности. Компьютерные системы. — 1999. — Т. 3. — С. 37–40.

[40] Ростовцев А.Г. Арифметика эллиптических кривых над простыми полями без удвоения точек // Проблемы информационной безопасности. Компьютерные системы. — 2000. — Т. 4.

[41] An Alternate Decomposition of an Integer for Faster Point Multiplication on Certain Elliptic Curves / Y.-H. Park, S. Jeong, C. Kim, J. Lim // Public Key Cryptography. PKC 2002. — 2002. — P. 323–334.

[42] Galbraith S.D., Lin X., Scott M. Endomorphisms for faster elliptic curve cryptography on general curves // Journal Of Cryptology. — 2011. — Vol. 24. — P. 446–469.

[43] Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms / M. Ciet, T. Lange, F. Sica, J.J. Quisquater // Advances in Cryptology — EUROCRYPT 2003. — 2003. — P. 388–400.

определяемая для некоторого свободного от квадратов числа $d \in \mathbb{N}$, изоморфна кольцу эндоморфизмов кривой $\mathcal{E}_{a,b}(\mathbb{F}_p)$.

Пусть $\mathcal{E}(\Lambda_\tau)$ комплексная эллиптическая кривая с решеткой периодов $\{1, \tau\}$. Тогда, каждая точка на кривой $\mathcal{E}(\Lambda_\tau)$ может быть параметризована значениями эллиптической функции Вейерштрасса $\wp$, а эндоморфизм ϕ_α, соответствующий элементу $\alpha \in \Lambda_\tau$, задается[44] отображением

$$(\wp(z) : \wp'(z) : 1) \to (\wp(\alpha z) : \wp'(\alpha z) : 1).$$

Поскольку эллиптические функции образуют поле, а функция $\wp(z)$ – четна, то $\wp(\alpha z)$ и $\wp'(\alpha z)$ как функции переменной z могут быть рационально выражены[45,46] через $\wp(z)$ и $\wp'(z)$. Обозначим символом $j()$ модулярную функцию. Тогда найдется рациональная функция $R(x) = \dfrac{P(x)}{Q(x)}$, где $P(x), Q(x) \in \mathbb{H}[x]$ и $\mathbb{H} = \mathbb{Q}(\sqrt{-d}, j(\tau))$ такая, что

$$\wp(\alpha z) = R(\wp(z)), \quad \wp'(\alpha z) = \frac{R'(\wp(z))\wp'(z)}{\alpha}.$$

Степени многочленов $P(x), Q(x)$, как функции от величины α, определяются[47] равенствами $\deg P(x) = N(\alpha), \quad \deg Q(x) = N(\alpha) - 1$, где $N(\alpha)$ – норма алгебраического числа $\alpha \in \Lambda_\tau$. Таким образом, задача явного определения эндоморфизма ϕ_α сводится к построению рациональной функции $R(x)$.

В § 1.4.2 автором описывается следующий алгоритм. Для произвольного целого неотрицательного k рассмотрим четную эллиптическую функцию $f_k(z)$, имеющую в нуле полюс второго порядка и определяемую рядом

$$f_k(z) = \sum_{n=0}^{\infty} d_{k,n} z^{2n-2} = \frac{d_{k,0}}{z^2} + d_{k,1} + d_{k,2} z^2 + \cdots, \quad d_{k,n} \in \mathbb{H}.$$

Примером такой функции могут служить $\wp(z)$ или $\wp(\alpha z)$. Воспользовавшись формулой для разложения функции Вейерштрасса $\wp(z)$ в ряд Лорана запишем равенство

$$f_k(z) = d_{k,0} \underbrace{\left(\frac{1}{z^2} + \sum_{n=2}^{\infty} c_n z^{2n-2} \right)}_{\wp(z)} + d_{k,1} + \sum_{n=2}^{\infty} (d_{k,n} - d_{k,0} c_n) z^{2n-2} =$$

$$= l_k(\wp(z)) + f'_{k+1}(z),$$

где $l_k(x) = d_{k,0} x + d_{k,1} \in \mathbb{H}[x]$ и $\deg l_k(x) = 1$. Функция $f_{k+1}(z)$ также является четной эллиптической функцией и имеет в нуле полюс второго порядка, следовательно, полагая $f_0(z) = \wp(\alpha z)$, для любого m мы можем записать равенство

$$\wp(\alpha z) = l_0(\wp(z)) + \frac{1}{f_1(z)} = \cdots$$

$$\cdots = l_0(\wp(z)) + \cfrac{1}{l_1(\wp(z)) + \cfrac{1}{\cdots + \cfrac{1}{l_{m-1}(\wp(z)) + \cfrac{1}{f_m(z)}}}}.$$

[44] Husemöller D. Elliptic Curves. — 2 edition. — New-York : Springer- Verlag, 2004.

[45] Гурвиц А. Теория аналитических и эллиптических функций. — М. : ГТТИ, 1933. — С. 344.

[46] Cox D. Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication. – NY. : J.Wiles and Sons, 1989. – P. 363.

[47] Stark H. Class numbers of complex quadratic fields // Modular Functions of one variable I. — Vol. 320 of Lecture Notes in Math. — Springer-Verlag, 1973. — P. 153–174.

Поскольку представление $\wp(\alpha z)$ в виде рациональной функции от $\wp(z)$ единственно и $\deg l_k(x) = 1$ для всех $k \in \mathbb{N}_0$, то при $m = N(\alpha) - 1$ будет выполнено равенство $f_m(z) = l_m(\wp(z))$ и мы получим разложение функции $\wp(\alpha z)$ в непрерывную дробь. Приводя полученное представление к виду рациональной дроби мы получаем искомое равенство.

Для иллюстрации разработанного алгоритма автором диссертационной работы были построены эндоморфизмы для всех эллиптических кривых $\mathcal{E}(\Lambda_\tau)$ таких, что $j(\tau) \in \mathbb{Z}$. В частности были получены следующие новые эндоморфизмы:

- кривая $y^2 = 4x^3 - 15x - 11$, $\alpha = \sqrt{-3}$ и $N(\alpha) = 3$:

$$\phi_\alpha : (x, y) \to \left(-\frac{4x^3 + 12x^2 + 33x + 28}{3(2x+3)^2},\ \frac{-8x^3 - 36x^2 - 6x + 13}{3\alpha(2x+3)^3} y \right),$$

- кривая: $y^2 = 4x^3 - 264x - 847$, $\alpha = \frac{1}{2}(1 + \sqrt{-11})$ и $N(\alpha) = 3$:

$$\phi_\alpha : (x, y) \to \left(-\frac{(\alpha+2)x^3 + 6(\alpha+5)x^2 - 33(4\alpha - 13)x - 11(59\alpha - 134)}{9(x - \alpha + 6)^2}, \right.$$
$$\left. -\frac{(\alpha+2)x^3 + 9(\alpha+5)x^2 + 33(4\alpha - 1)x + 11(19\alpha - 70)}{9\alpha(x - \alpha + 6)^3} y \right).$$

Полный перечень построенных эндоморфизмов приводится в приложении к диссертационной работе. Для некоторых эллиптических кривых из рассматриваемого класса, с использованием соотношений Дж.Тейта, были найдены формы, минимизирующие количество элементарных операций, необходимых для вычисления построенных эндоморфизмов. Перечень таких кривых содержится в таблице 1.5.

№	τ	θ	γ	$\mathcal{H}(\mathbb{C})$
1	$2\sqrt{-1}$	-1	2	$v^2 = u^3 - 6u^2 + u$
2	$\sqrt{-2}$	-2	$\frac{2}{3}$	$v^2 = u^3 - 4u^2 + 2u$
3	$\sqrt{-3}$	-1	2	$v^2 = u^3 - 6u^2 - 3u$
4	$\frac{3}{2}\left(1 + \sqrt{-3}\right)$	-3	1	$v^2 = u^3 - 9u^2 - 3u - \frac{1}{4}$
5	$\frac{1}{2}\left(1 + \sqrt{-7}\right)$	$\frac{\alpha-4}{2}$	$-\frac{(\alpha+10)}{112}$	$v^2 = u^3 - \frac{3}{32}(\alpha - 6)u^2 - \frac{1}{64}(3\alpha - 2)u$
5	$\frac{1}{2}\left(1 + \sqrt{-7}\right)$	$-\frac{1}{2}$	$\frac{1}{2}$	$v^2 = u^3 - \frac{3}{4}u^2 - 2u - 1$

Таблица 1.5: Эллиптические кривые с целым j-инвариантом.

При этом некоторые из построенных эндоморфизмов принимают следующий вид:

1. кривая $v^2 = u^3 - 6u^2 + u$, $\alpha = 2\sqrt{-1}$ и $N(\alpha) = 4$,

$$\hat{\phi}_\alpha : (u, v) \to \left(-\frac{(u-1)^2 v^2}{4u^2(u+1)^2}, -\frac{\left(u^5 + 3u^4 - 30u^3 + 30u^2 - 3u - 1\right)}{4\alpha u^2(u+1)^3} v \right).$$

2. кривая $v^2 = u^3 - \frac{3}{32}(\alpha - 6)u^2 - \frac{1}{64}(3\alpha - 2)u$, $\alpha = \frac{1}{2}(1 + \sqrt{-7})$ и $N(\alpha) = 2$:

$$\hat{\phi}_\alpha : (u, v) \to \left(-\frac{(\alpha+1)u^2 + u - \mu}{4u},\ -\frac{(\alpha+1)u^2 + \mu}{4\alpha u^2} v, \right),$$

где $\mu = \frac{\alpha-2}{16} = \left(\frac{\alpha}{4}\right)^2 = \frac{1}{4(\alpha+1)}$.

Для применения построенных эндоморфизмов в средствах защиты информации автором был разработан способ вычисления кратной точки эллиптической кривой, описываемый в § 1.4.5 диссертационной работы. Автором доказана следующая теорема.

Теорема 1.6. *Пусть $d > 1$ – свободное от квадратов, целое число и задан элемент $\alpha \in \Lambda_\tau \subseteq \mathbb{Z}_\mathbb{K} \subset \mathbb{Q}(\sqrt{-d})$ такой, что $N(\alpha) \geqslant 2$. Определим натуральное число*

$$n_\alpha = \frac{N(\alpha) - \delta_\alpha}{2}, \quad \textit{где} \quad \delta_\alpha \equiv N(\alpha) \ (mod\, 2)\,,$$

и множество $\mathcal{N} = [-n_\alpha, -n_\alpha + 1, \ldots, n_\alpha - 1, n_\alpha]$. Тогда, если α удовлетворяет неравенству $|\operatorname{tr}(\alpha) - 1| \leqslant n_\alpha$, то для любого натурального k найдется многочлен $g(x) \in \mathcal{N}[x]$ такой, что

$$k = g(\alpha) = \sum_{i=0}^{w+c_1} g_i \alpha^i, \quad g_i \in \mathcal{N},$$

где $\deg g(x) \leqslant w_1 = c_1 + \left\lceil 2 \log_{N(\alpha)} k \right\rceil$, *где*

$$c_1 = \begin{cases} 4, & \textit{если} \quad \alpha = 1 \pm \sqrt{-2}, \\ 3, & \textit{иначе.} \end{cases}$$

Отметим, что вопросы представления целых чисел в системах счисления с произвольным действительным основанием α ведут начало от работ А. Реньи[48] и В. Перри[49]. Используемый в данной работе метод представления натурального числа k в системе счисления с комплексным основанием α базируется на результатах работ В. Мюллера[50] и Н. Смарта[51]. Также, в более слабой форме, доказанная теорема формулировалась в упомянутой ранее работе А.Г. Ростовцева.

Доказательство теоремы 1.6 конструктивно и позволяет предъявить алгоритм построения коэффициентов многочлена $g(x)$ по заданным значениям k и α. После чего, вычисление кратной точки сводится к вычислению равенства

$$[k]P = [g_0]P + [g_1]\phi_\alpha(P) + [g_2]\phi_\alpha^2(P) + \cdots + [g_{w_1}]\phi_\alpha^{w_1}(P) = \\ = [g_0]P + \phi_\alpha\Big([g_1]P + \cdots \phi_\alpha\big([g_{w_1-1}]P + \phi_\alpha([g_{w_1}]P)\big)\Big).$$

Отметим, что для фиксированной точки P можно заранее вычислить точки $[g_0]P, \ldots, [g_{w_1}]P$, понизив тем самым трудоемкость вычисления кратной точки до w_1 операций вычисления эндоморфизма ϕ_α и w_1 операций сложения точек на эллиптической кривой.

Во **второй** главе диссертационной работы приводятся результаты исследований, позволяющие обосновать целесообразность применения в средствах защиты информации генераторов псевдослучайных чисел, основанных на представлении действительных иррациональных чисел в виде систематических дробей по заданному основанию.

---

[48] Rényi A. Representations for real numbers and their ergodic properties // Acta Mathematica Academiae Scientiarum Hungaricae. — 1957. — Vol. 8. — P. 477–493.

[49] Parry W. On the β-expansions of real numbers // Acta Mathematica Academiae Scientiarum Hungaricae. — 1960. — Vol. 11. — P. 401–416.

[50] Müller V. Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two // Journal of Cryptology. — 1998. — Vol. 11. — P. 219–234.

[51] Smart N. Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic // Journal of Cryptology. — 1999. — Vol. 12. — P. 141– 151.

В § 2.2 диссертационной работы рассматриваются два класса действительных чисел. Пусть $b > 1$, $d > 1$ – целые числа, m – натуральное и $x_1, \ldots, x_m \in \mathbb{N}$ попарно различные числа, удовлетворяющие неравенствам $0 < x_k \leqslant d$ для всех $k = 1, \ldots, m$. Пусть $u_1, \ldots, u_m \in \mathbb{Q}$ — не все одновременно равные нулю рациональные числа. К первому классу относятся действительные числа вида

$$\alpha = \sum_{n=0}^{\infty} \left(\frac{u_1}{dn + x_1} + \cdots + \frac{u_m}{dn + x_m} \right) b^{-n} = \sum_{n=0}^{\infty} \sum_{k=1}^{m} \frac{u_k}{dn + x_k} b^{-n}.$$

Из работ Р. Тайдемана и его соавторов[52,53] следует, что число α – иррационально. Ко втором классу чисел относятся числа вида

$$\alpha = \sum_{n=0}^{\infty} \frac{x_n}{n!}.$$

где $(x_n)_{n=0}^{\infty}$ — чисто периодическая последовательность рациональных чисел с периодом длины m. Иррациональность таких чисел следует из доказанной автором, совместно с В.Г. Чирским, теоремы, см. § 2.2.2.

Теорема 2.1. *Пусть m – натуральное число и $(x_n)_{n=0}^{\infty}$ — чисто периодическая последовательность рациональных чисел с периодом длины m такая, что существует индекс $k \geqslant 0$ для которого $x_k \neq 0$. Пусть α число из второго класса и $\alpha \neq 0$, тогда α — иррационально.*

Отметим, что иррациональность чисел из второго класса для случая непериодической последовательности коэффициентов $(x_n)_{n=0}^{\infty}$ изучалась в работе Дж. Ханцля и Р. Тайдемана[54].

Напомним, что любое действительное число α может быть представлено в виде систематической дроби

$$\alpha = \sum_{k=0}^{\infty} a_k b^{-k}, \quad a_k \in \mathbb{Z}, \quad \text{и} \quad 0 \leqslant a_k < b \quad \text{при} \quad k > 0.$$

для произвольного натурального $b > 1$. Разработанные автором алгоритмы, позволяющие представить действительные числа из рассматриваемых классов в виде систематической дроби рассматриваются автором в § 2.3 диссертационной работы.

Наличие таких алгоритмов позволяет рассмотреть вопрос о целесообразности применения в средствах защиты информации генераторов псевдослучайных последовательностей, образованных коэффициентами представления числа α из рассматриваемых классов в виде систематической дроби. Хорошо известно[55,56], что такие последовательности не являются периодическими.

К генераторам, применяемым в средствах защиты информации, предъявляется ряд требований, среди которых отметим следующие.

---

[52]Transcendental infinite sums / S.D. Adhikari, N. Saradha, T.N. Shorey, R. Tijdeman // Indag. Math. — 2001. — Vol. 12. — P. 1–14.

[53]Tijdeman R. On irrationality and transcendency of infinite sums of rational numbers // Diophantine Equations / Ed. by N. Saradha. — New Delhi, India : Narosa Publisher, 2008. — P. 279–296.

[54]Hancl J., Tijdeman R. On the irrationality of factorial series II // Journal of Number Theory. — 2010. — Vol. 130. — P. 595– 607.

[55]Remmert R., Ullrich P. Elementare Zahlentheorie. — Berlin : Birkhäuser, 1995. — P. 276.

[56]Нестеренко Ю.В. Теория чисел. — М. : Академия, 2008. — С. 272.

1. Необходимо[57,58], чтобы для любых значений входных параметров n, $x_1, \ldots, x_m$ вырабатываемая генератором последовательность $(a_k)_{k=1}^n$ представляла собой реализацию случайной величины, равномерно распределенной на интервале $[0, b-1]$. Для некоторых из используемых в средствах защиты информации генераторов псевдослучайных последовательностей сформулированное требование доказать не удается. Поэтому, на практике, оно заменяется на более слабое – требование статистической неотличимости выработанной последовательности от равномерно распределенной.

2. Необходимо, чтобы задача определения любого подмножества элементов последовательности $(a_k)_{k=1}^n$ по известному другому подмножеству элементов той же последовательности имела высокую алгоритмическую сложность. Частными случаями данного свойства являются высокая трудоемкость определения начальных значений генератора $x_1, \ldots, x_m$ по элементам последовательности $(a_k)_{k=1}^n$ и отсутствие у последовательности $(a_k)_{k=1}^n$ периода длиной τ при $\tau < n$.

Впервые вопрос о нормальности произвольных действительных иррациональных чисел, т.е. о равномерном распределении коэффициентов систематических дробей в произвольной системе счисления, по-видимому, был поставлен Э. Борелем[59]. Отдельно стоит выделить случай числа π, для которого исследования начались существенно ранее. Исторический обзор указанных вычислений можно найти в монографии А.В. Жукова[60], а также в статье Д. Борвейна и соавторов[61]. Один из последних результатов о вычислении мантиссы числа π можно найти в работе А. Йи[62].

Гипотеза о нормальности числа π формулировалась в работе Д. Бейли и Р. Кренделла[63] и экспериментально проверялась в ряде работ[64,65,66]. В настоящее время доказана нормальность только нескольких иррациональных чисел специального вида[67,68], однако для произвольного иррационального числа α, не известен критерий, позволяющий определить, является ли число α нормальным или нет.

В начале 20-го века Г. Вейль, Г.Харди и Дж.Литллвуд доказали[69], что для почти всех иррациональных чисел α последовательность действительных чисел $\{\alpha b^n\}$, где $b > 1$ натуральное число, равномерно распределена на отрезке $[0, 1)$. Позднее

[57]Бабаш А.В., Шанкин Г.П. Криптография / Под ред. В.П. Шерстюка, Э.А. Применко. — М. : Солон-Пресс, 2007. — С. 512.

[58]Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 2 изд. — М. : Гелиос АРВ, 2002. — С. 480.

[59]Borel E. Lesons sur la theorie des functions. — Paris, 1914.

[60]Жуков А.В. Вездесущее число π. — 5-е изд. — М. : Либроком, 2012. — С. 240.

[61]The Quest for π / D.H. Bailey, J.M. Borwein, P.B. Borwein, S. Plouffe // Mathematical Intelligencer. — 1997. — Vol. 19, no. 1. — P. 50–57.

[62]Yee A.J. World π record for both desktop and supercomputer. — 2012.

[63]Bailey D.H., Crandall R.E. On the random character of fundamental constant expansions // Experimental Mathematics. — 2001. — Vol. 10, no. 2. — P. 175–190.

[64]Lagarias J.C. On the normality of arithmetical constants // Experimental Mathematics. — 2001. — Vol. 10, no. 3. — P. 355– 368.

[65]Tu S.J., Fischbach E. A study on the randomness of the digits of π // International Journal of Modern Physics C. — 2005. — Vol. 16, no. 2. — P. 281–294.

[66]Нестеренко А.Ю. О статистических свойствах некоторых трансцендентных чисел // Ученые записки Орловского государственного университета. — 2012. — № 6 (часть 2). — С. 170–176.

[67]Champernowne D.G. The Construction of the Decimals Normal in the Scale of Ten // Journal Of London Mathematical Society. — 1933. — Vol. 8. — P. 254–260.

[68]Copeland A.H., Erdos P. Note on Normal Numbers // Bulletin Of American Mathematical Society. — 1946. — Vol. 52. — P. 857–860.

[69]Кейперс Л., Нидеррайтер Г. Равномерно распределенные последовательности. — М. : Наука, 1985. — С. 408.

Н.М. Коробов показал[70], что из равномерного распределения элементов указанной последовательности следует равномерное распределение коэффициентов разложения числа α в системе счисления по основанию b. В § 1.2.3 автором доказана теорема, являющаяся прямым следствием результатов Н.М. Коробова.

Представим число α в виде быстро сходящегося ряда

$$\alpha = \sum_{n=0}^{\infty} \omega_n$$

где $\omega_n \in \mathbb{Q}$ и найдется индекс $n_0 \in \mathbb{N}$ такой, что для любого индекса $n \geqslant n_0$ будет выполнено неравенство

$$0 < |\omega_n| < f(n)b^{-n}, \quad 0 < f(n) < 1, \quad \lim_{n\to\infty} f(n) = 0,$$

для некоторой функции $f(n)$ натурального аргумента n.

Определим начальные значения $\alpha_0 = \alpha$, $\delta_{-1} = 0$ и последовательность рациональных величин

$$\alpha_n = b\delta_{n-1} + \omega_n b^n, \quad a_n = \lfloor \alpha_n \rfloor, \quad \delta_n = \alpha_n - a_n, \quad n = 0,\ 1,\ \ldots,$$

где $\delta_n, \omega_n, \alpha_n \in \mathbb{Q}$, $\delta_{-1}, a_n \in \mathbb{Z}$.

Теорема 2.6. *Пусть $\alpha > 0$ иррациональное число из рассматриваемых классов чисел. Тогда коэффициенты систематической дроби числа α по основанию b равномерно распределены на интервале $[0, b-1]$, если последовательность величин $(\delta_k)_{k=0}^{\infty}$ является реализацией равновероятно распределенной на интервале $[0, 1)$ случайной величины.*

Утверждение доказанной теоремы позволяет свести проверку гипотезы о нормальности числа α к проверке статистической гипотезы о равномерном распределении на интервале $[0, 1)$ последовательности значений $(\delta_k)_{k=1}^{\infty}$, вырабатываемых в ходе представления числа α в виде систематической дроби.

Задача о восстановлении начального состояния генератора псевдослучайных чисел является хорошо известной[71,72]. Вместе с тем, применительно к систематическим дробям действительных иррациональных чисел данная задача, по видимому, впервые рассматривалась автором[73]. Для восстановления неизвестных параметров чисел из первого класса может быть использована доказанная в § 2.4.1 теорема.

Теорема 2.3. *Определим последовательность действительных чисел α_k*

$$\alpha_1 = s_r(\alpha) = \sum_{n=0}^{r} a_n b^{-n}, \quad \alpha_k = \alpha_{k-1} - u_{k-1}\xi_{k-1} \quad \textit{для} \quad k = 2, \ldots, m,$$

где величины $\xi_1, \ldots, \xi_{m-1}$ удовлетворяют равенствам

$$\alpha = \sum_{i=1}^{m} u_i \xi_i, \quad \xi_i = \sum_{n=0}^{\infty} \frac{b^{-n}}{(dn + x_i)^s}, \quad i = 1, \ldots, m.$$

Если для r выполнены условия:

[70]Коробов Н.М. О некоторых вопросах равномерного распределения // Известия Академии наук СССР. Серия математическая. — 1950. — Т. 14. — С. 215–231.

[71]Иванов М.А., Чугунков И.В. Теория, практика и оценка качества генераторов псевдослучайных последовательностей. — М. : Кудиц-Образ, 2003. — С. 240.

[72]Поточные шифры. Результаты зарубежной открытой криптологии. — 1997.

[73]Нестеренко А.Ю. Алгоритм восстановления параметров одного класса иррациональных чисел // Известия Саратовского университета. Серия: Математика. Механика. Информатика. — 2013. — Т. 13, № 4 (часть 2). — С. 89–93.

1. *величина* $s_r(\alpha)$ *отлична от нуля,*

2. *выполнено неравенство* $u_m > \frac{2(b-1)(dr+x_m)^s}{b^r(1-b^{-r})}$,

3. *выполнено неравенство* $\sum_{i=1}^{m} u_i < (b-1)(dr)^s b^r$,

то для всех индексов $k = 1, \ldots, m$ *выполнены неравенства*

$$\left(\frac{u_k}{\alpha_k}\right)^{\frac{1}{s}} < x_k < \left(\frac{b}{\alpha_k(b-1)}\sum_{i=k}^{m} u_i\right)^{\frac{1}{s}}.$$

Утверждение теоремы 2.3 определяет верхние и нижние оценки неизвестных $x_1, \ldots, x_m$ Это позволяет предъявить алгоритм, перебирающий неизвестные значения в интервалах, зависящих от величины r, определяющей точность приближения $s_r(\alpha)$ к числу α. Практическая работоспособность данного алгоритма, при небольших значениях m, была подтверждена автором диссертации экспериментально.

Еще один алгоритм восстановления неизвестных параметров чисел из рассматриваемых классов приводится автором в § 2.4.2. Числа из первого класса могут быть записаны в виде

$$\alpha = \sum_{n=0}^{\infty}\sum_{l=1}^{d}\frac{w_l}{dn+l}b^{-n},$$

где $w_l = u_i$ если найдется индекс $i \in \{1, \ldots, m\}$ такой, что $x_i = l$. В противном случае, $w_l = 0$. Для чисел из второго класса выполнено, полученное в ходе доказательства теоремы 2.1, равенство

$$\alpha = \sum_{i=1}^{m} x_i\xi_i, \quad \text{и} \quad \sum_{i=1}^{m}\xi_i = e,$$

где e основание натурального логарифма. В обоих случаях исходное число α образует целочисленное соотношение

$$c_1\xi_1 + \cdots + c_m\xi_m + c_{m+1}\alpha = 0, \quad c_1, \ldots, c_{m+1} \in \mathbb{Z},$$

в котором величины $\xi_1, \ldots, \xi_m$ и приближение $s_r(\alpha)$ к числу α известны нарушителю.

Задача поиска неизвестных значений $c_1, \ldots, c_{m+1}$ в указанном целочисленном соотношении ведет отсчет от расширенного алгоритма Эвклида. Случай произвольного натурального значения m исследовался большим числом авторов, включая Якоби, Пуанкаре, Минковского, Перрона и т.д. Первым алгоритмом, для которого получена оценка трудоемкости, полиномиальная от нормы разыскиваемого соотношения, является алгоритм Фергюссона и Фуркада[74]. Далее, появился целый ряд алгоритмов – LLL[75], HJLS[76] и PSLQ[77]. Последний из них наиболее пригоден для поиска неизвестных значений $c_1, \ldots, c_{m+1}$, а количество итераций алгоритма PSLQ может быть

[74]Ferguson H.R.P., Forcade R.W. Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two // Bulletin (New Series) of the American Mathematical Society. — 1979. — no. 1. — P. 912–914.

[75]Lenstra A.K., H.W. Lenstra H. W., Lovasz L. Factoring polynomials with rational coefficients // Mathematische Annalen. — 1981. — Vol. 4, no. 261. — P. 515–534.

[76]Polynomial Time Algorithms for Finding Integer Relations Among Real Numbers / J. Hastad, B. Just, J.C. Lagarias, C.P. Schnorr // SIAM Journal of Computing. — 1989. — Vol. 18. — P. 859–881.

[77]Ferguson H.R.P., Bailey D.H. A Polynomial Time, Numerically Stable Integer Relation Algorithm. — 1992.

оценено[78] величиной $\frac{m(m+1)\ln(2^m N(c))}{2\ln\sqrt{2}}$, где $N(c) = \sqrt{\sum_{i=1}^{m+1} c_i^2}$ – норма неизвестного целочисленного соотношения.

Алгоритм поиска неизвестных значений был реализован автором на ЭВМ. Согласно экспериментальным исследованиям, алгоритм PSLQ успешно завершает свою работу в случае, когда задано рациональное приближение $s_r(\alpha)$ к числу α с точностью $r \geqslant \lceil (m+1)\log_r(N(c))\rceil$. Конкретные результаты вычислений приведены в § 2.4.2.

Естественной защитой генератора псевдослучайных последовательностей от приведенной атаки является отбрасывание первых $\lceil (m+1)\log_r(N(c))\rceil$ элементов последовательности коэффициентов $(a_n)_{n=1}^{\infty}$. В этом случае, нарушитель не может получить точное приближение к числу α и, воспользовавшись описанным выше методом, восстановить неизвестные параметры числа α.

С другой стороны, нарушитель может перехватить произвольный фрагмент последовательности коэффициентов $(a_n)_{n=k+1}^{k+r}$ и, рассматривая его как приближение к некоторому числу β, предпринять попытку найти неизвестные параметры числа β. Безуспешность такой попытки следует из доказанных автором в § 2.4.3 утверждений.

Теорема 2.4. *Разложение в систематическую дробь действительного иррационального числа* $\alpha = \sum_{n=0}^{\infty}\sum_{i=1}^{m}\frac{w_l}{dn+x_i}b^{-n}$ *совпадает с разложением в систематическую дробь действительного иррационального числа* β *того же вида тогда и только тогда, когда* $\beta = \alpha b^s$ *для некоторого целого числа* s.

Теорема 2.5 содержит аналогичное утверждение относительно действительных чисел вида $\alpha = \sum_{n=0}^{\infty}\frac{x_n}{n!}$. Таким образом, по известному фрагменту последовательности коэффициентов $(a_n)_{n=k+1}^{k+r}$ действительного числа α из рассматриваемых классов нарушитель не может восстановить неизвестные параметры другого числа β и, тем самым, выработать другие фрагменты последовательности коэффициентов $(a_n)_{n=k+r}^{\infty}$. Вопрос о возможности восстановления параметров некоторого числа β из других классов действительных чисел, в настоящее время является открытым.

В качестве примера практического применения рассмотренного метода генерации псевдослучайных последовательностей в § 2.6 описывается метод локальной аутентификации пользователей средства защиты информации, удовлетворяющий предъявляемым требованиям к эксплуатационным характеристикам и безопасности[79].

В **третьей** главе диссертационной работы приводятся результаты исследований, позволившие обосновать целесообразность применения в средствах защиты информации равновероятных сжимающих отображений, представляющих собой линейные формы от значений взаимно-однозначных функций.

Введем в рассмотрение следующий класс сжимающих отображений. Пусть множество кодов аутентичности $\mathbb{A}$ есть конечная аддитивная абелева группа. Зафиксируем натуральные числа l, s, u и рассмотрим конечное множество $\mathbb{B}$ такое, что $|\mathbb{A}| = |\mathbb{B}|^u$. Рассмотрим множество отображений

$$\pi_n : \mathbb{V}_u(\mathbb{B}) \to \mathbb{A},\ n = 1, \ldots, l,$$

задающее взаимно-однозначное соответствие между векторным пространством $\mathbb{V}_u(\mathbb{B})$ и конечным множеством $\mathbb{A}$.

Определим множество сообщений $\mathbb{S}$ и множество ключей $\mathbb{K}$ равенствами

$$\mathbb{S} = \mathbb{V}_{lu}(\mathbb{B}) = \{(x_1, \ldots, x_{lu})\}, \quad \mathbb{K} = \mathbb{V}_{slu}(\mathbb{B}) = \{(k_1, \ldots, k_{slu})\},$$

[78] Ferguson H.R.P., Bailey D.H., Arno S. Analysis of PSLQ, an integer relation finding algorithm // Mathematics Of Computation. — 1999. — Vol. 68, no. 225. — P. 351–369.

[79] Password Hashing Competition. — 2015.

где координаты $x_1, \ldots, x_{lu},\ k_1, \ldots, k_{slu} \in \mathbb{B}$, а также рассмотрим сжимающее отображение

$$g(k_1, \ldots, k_s, x) : \mathbb{V}_{s+1}(\mathbb{B}) \to \mathbb{B},$$

удовлетворяющее следующим свойствам.

1. При фиксированном наборе значений $k_1, \ldots, k_s \in \mathbb{B}$ отображение

   $$g(k_1, \ldots, k_s, x) = g(x) : \mathbb{B} \to \mathbb{B},$$

   является взаимно-однозначным отображением множества $\mathbb{B}$ в себя.

2. При фиксированном значении $x \in \mathbb{B}$ и любом значении $z \in \mathbb{B}$ уравнение $g(k_1, \ldots, k_s, x) = z$ имеет ровно $|\mathbb{B}|^{(s-1)}$ различных решений, относительно неизвестных $k_1, \ldots, k_s$.

3. Зафиксируем произвольные элементы $x, y \in \mathbb{B}$ и будем считать, что вычеты $z, t \in \mathbb{B}$ пробегают множество всех возможных значений. Тогда суммарное число решений системы уравнений

   $$\begin{cases} g(k_1, \ldots, k_s, x) = z, \\ g(k_1, \ldots, k_s, y) = t, \end{cases}$$

   относительно неизвестных $k_1, \ldots, k_s$, в точности равно $|\mathbb{B}|^s$.

Пусть $x = (x_1, \ldots, x_{lu}) \in \mathbb{S}$, $k = (k_1, \ldots, k_{slu}) \in \mathbb{K}$. Определим сжимающее отображение $h(x, k) : \mathbb{S} \times \mathbb{K} \to \mathbb{A}$

$$h(x, k) = \sum_{n=1}^{l} \pi_n(z_{(n-1)u+1}, \ldots, z_{nu-1}, z_{nu}),$$

где

$$z_i = g(k_{s(i-1)+1}, \ldots, k_{si}, x_i),$$

для всех $i = 1, \ldots, lu$. Определенное отображение $h(x, k)$ представляет собой класс ключевых функций хэширования, параметризованный отображениями $\pi_1, \ldots, \pi_l$ и функцией g. В § 3.2.1 диссертационной работы доказаны следующие утверждения, описывающие свойства введенного отображения $h(k, x)$.

Теорема 3.1. *Для любого $a \in \mathbb{A}$ и любого $k = (k_1, \ldots, k_{slu}) \in \mathbb{K}$ найдется ровно $|\mathbb{A}|^{(l-1)}$ элементов $x = (x_1, \ldots, x_{lu}) \in \mathbb{S}$ таких, что $h(x, k) = a$.*

Из утверждения теоремы 3.1 следует, что отображение $h(x, k)$ является равновероятной ключевой функцией хэширования относительно сжимаемых сообщений, поскольку

$$|\mathbb{A}|^{(l-1)} = \frac{|\mathbb{A}|^l}{|\mathbb{A}|} = \frac{|\mathbb{S}|}{|\mathbb{A}|},$$

и вероятность выбора случайного сообщения $x \in \mathbb{S}$ с заданным значением функции $h(x, k) = a$ не зависит от выбора ключа $k \in \mathbb{K}$, значения кода аутентичности $a \in \mathbb{A}$ и равна $|\mathbb{A}|^{-1}$.

Теорема 3.2. *Для любого $a \in \mathbb{A}$ и любого $x = (x_1, \ldots, x_{lu}) \in \mathbb{S}$ найдется ровно $|\mathbb{B}|^{u(sl-1)}$ элементов $k = (k_1, \ldots, k_{slu}) \in \mathbb{K}$ таких, что $h(x, k) = a$.*

Из теоремы 3.2 следует, что число ключей $k \in \mathbb{K}$ таких, что выполнено равенство $h(x,k) = a$ в точности равно

$$|\mathbb{B}|^{u(sl-1)} = \frac{|\mathbb{B}|^{slu}}{|\mathbb{B}|^u} = \frac{|\mathbb{K}|}{|\mathbb{A}|}$$

и вероятность выбора случайного ключа $k \in \mathbb{K}$ такого, что $h(x,k) = a$, не зависит от выбора сообщения $x \in \mathbb{S}$, значения кода аутентичности $a \in \mathbb{A}$ и равна $|\mathbb{A}|^{-1}$.

Теорема 3.3. *Для любых элементов $a, b \in \mathbb{A}$ и любых $x = (x_1, \ldots, k_{lu})$, $y = (y_1, \ldots, y_{lu})$ из множества $\mathbb{S}$ найдется не более $|\mathbb{B}|^{u(sl-1)}$ элементов $k = (k_1, \ldots, k_{slu})$ таких, что*

$$\begin{cases} h(x,k) = a, \\ h(y,k) = b. \end{cases}$$

Утверждение теоремы 3.3 позволяет получить оценку условной вероятности выбора ключа k такого, что $h(x,k) = a$ при условии, что $h(y,k) = b$. Приведенный в § 3.2 пример показывает, что полученная оценка является достижимой.

Для построения равновероятного отображения $h(x,k)$ использовался подход, ведущий свое начало от работ Дж. Картера и М. Вегмана[80,81], а также Д. Стинсона[82]. Позднее подход развивался при построении ключевых функций хэширования в ряде работ[83,84,85,86]. Существенным развитием указанных работ является предъявленная автором диссертационной работы возможность применения построенного отображения для реализации аутентифицированного шифрования, т.е. режима работы произвольного блочного шифра, реализующего одновременный процесс шифрования и имитозащиты данных[87].

Формально, такой режим может быть определен следующим образом. Пусть $v \in \mathbb{N}$, $x, y, c \in \mathbb{S}$, $k_1, k_2 \in \mathbb{K}$ и $a \in \mathbb{A}$. Определим отображения

$$\texttt{authenc}(k_1, k_2, iv, y, x) = \{c, a\} : \quad \mathbb{K} \times \mathbb{K} \times \mathbb{V}_v \times \mathbb{S} \times \mathbb{S} \to \mathbb{S} \times \mathbb{A},$$

$$\texttt{authdec}(k_1, k_2, iv, y, c, a) = \{x, b\} : \quad \mathbb{K} \times \mathbb{K} \times \mathbb{V}_v \times \mathbb{S} \times \mathbb{S} \times \mathbb{A} \to \mathbb{S} \times \mathbb{V}_1$$

такие, что для любых $k_1, k_2 \in \mathbb{K}$, $iv \in \mathbb{V}_v$ и $y \in \mathbb{S}$ выполнено равенство

$$\texttt{authdec}(k_1, k_2, iv, y, \texttt{authenc}(k_1, k_2, iv, y, x)) = \{x, \texttt{true}\}.$$

Будем говорить, что отображение **authenc** зашифровывает сообщение x и вычисляет код аутентичности (имитовставку) сообщений x, y, а отображение **authdec**

[80] Carter J.L., Wegman M.N. Universal Classes of Hash Functions // Journal Of Computer and System Sciences. — 1979. — Vol. 18. — P. 143–154.

[81] Wegman M.N., Carter J.L. New Hash Functions and their Use in Authentication and Set Equality // Journal of Computer and System Sciences. — 1981. — Vol. 22, no. 3. — P. 265–279.

[82] Stinson D.R. Universal hashing and message authentication codes // Designs, Codes, and Cryptography. — 1994. — Vol. 4, no. 4. — P. 369– 380.

[83] Etzel M., Patel S., Ramzan Z. Square Hash: Fast Message Authentication via Optimized Universal Hash Functions // Advances in Cryptology – Crypto 99. — Springer, 1999. — P. 234–251.

[84] Halevi S., Krawczyk H. MMH: Software Message Authentication in the Gbit/second Rates // Proceedings Of Fast Software Encryption. — Springer, 1997. — P. 172–189.

[85] Nandi M. On the Minimum Number of Multiplications Necessary for Universal Hash Constructions. — 2013.

[86] UMAC: Fast and Secure Message Authentication / J. Black, Halevi S., H. Krawczyk et al. // Advances in Cryptology – Crypto 99. — Springer, 1999. — P. 216–233.

[87] Bellare M., Namprempre C. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm // Advances in Cryptology — ASIACRYPT 2000 / Ed. by T. Okamoto. — Berlin : Springer, 2000. — P. 531–545.

расшифровывает шифртекст c и проверяет код аутентичности (имитовставку) сообщений x, y.

Примером режима аутентифицированного шифрования служит режим, регламентируемый Р 1323565.1.026-2019. Другой пример предложен автором в § 3.3.1. Для его описания необходимо определить следующие элементарные преобразования.

1. Алгоритм блочного шифрования $E_k(x) : \mathbb{V}_{256} \times \mathbb{V}_w \to \mathbb{V}_w$, где w это длина блока алгоритма шифрования, $w \in \{64, 128\}$.

2. Отображение $\phi : \mathbb{V}_8 \to \mathbb{V}_8$, представляющее собой нелинейную перестановку на двоичных векторах длины 8, определяемую в стандарте ГОСТ Р 34.11-2012.

3. Отображение $S : \mathbb{V}_w \to \mathbb{V}_w$, определяемое равенством

$$S(x) = (\phi(x_0)|| \dots ||\phi(x_{(w/8)-1})).$$

4. Линейный оператор $L(x) : \mathbb{V}_w \to \mathbb{V}_w$, который представляет собой умножение двоичного вектора $x \in \mathbb{V}_w$ на фиксированную, обратимую матрицу $L \in GL_w(\mathbb{F}_2)$.

5. Отображение $\pi : \mathbb{V}_w \times \mathbb{V}_w \to \mathbb{V}_{2w}$, зависящее от четырех констант $\zeta_0, \dots, \zeta_3 \in \mathbb{V}_w$ и представляющее собой 4-х раундовую сеть Фейстеля с раундовой функцией $L(S(x \oplus \zeta))$. Аналитически, отображение π может быть записано следующим образом.

$$\pi(x_0||x_1) = (\underbrace{x_2 \oplus L(S(x_3 \oplus \zeta_2))}_{x_4} || \underbrace{x_3 \oplus L(S(x_4 \oplus \zeta_3))}_{x_5}) = (x_4||x_5),$$

где $x_2 = x_0 \oplus L(S(x_1 \oplus \zeta_0), \quad x_3 = x_1 \oplus L(S(x_2 \oplus \zeta_1)$.

6. Отображение $G_{\gamma_{-1},\alpha}(n) = \gamma_{-1}\alpha^{n+1}$, в котором α является примитивным элементом конечного поля $\mathbb{F}_{2^{2w}}$, порожденного следующим примитивным многочленом

$2w$	$p(x)$
128	$x^{128} + x^7 + x^2 + x + 1$
256	$x^{256} + x^{10} + x^5 + x^2 + 1$

а также произвольным элементом $\gamma_{-1} \in \mathbb{F}_{2^{2w}}$. В дальнейшем мы будем использовать обозначение $\gamma_n = (\gamma_{n,0}||\gamma_{n,1}) = G_{\gamma_{-1},\alpha}(n)$, $n = 0, 1, \dots$.

Мы будем представлять открытые данные, подлежащие зашифрованию, а также ассоциированные данные, как конкатенацию фрагментов фиксированной длины

$$x = x_0|| \dots ||x_{l-1}||x_l, \quad y = y_0|| \dots ||y_{r-1}||y_r,$$

где $\mathrm{len}_2(x_0) = \dots = \mathrm{len}_2(x_{l-1}) = \mathrm{len}_2(y_0) = \dots = \mathrm{len}_2(y_{r-1}) = w$, а также $\mathrm{len}_2 x_l \leqslant w$, $\mathrm{len}_2 y_r \leqslant w$ и $l, r \in \mathbb{N}_0$. Кроме того, введем ограничение на общую длину открытых данных и будем считать, что $\mathrm{len}_2 x \geqslant 2w$.

Разобьем входные данные на пары и определим число пар равенствами

$$l_0 = l \pmod 2 + \left\lfloor \frac{l}{2} \right\rfloor, \quad r_0 = r \pmod 2 + \left\lfloor \frac{r}{2} \right\rfloor.$$

Вместе с каждой парой блоков будет преобразовываться элемент последовательности γ_n, при этом, элементы $\gamma_0, \dots, \gamma_{r_0-1}$ будут соответствовать парам ассоциированных данных, а элементы $\gamma_{r_0}, \dots, \gamma_{r_0+l_0-1}$ – парам открытого текста.

Определим процедуру зашифрования пары блоков открытых данных равенствами

$$\begin{aligned} c_{2n} &= E_{k_1}(x_{2n} \oplus \gamma_{n+r_0,0}) \oplus \gamma_{n+r_0,0}, \\ c_{2n+1} &= E_{k_1}(x_{2n+1} \oplus \gamma_{n+r_0,1}) \oplus \gamma_{n+r_0,1}, \end{aligned}$$

для $n = 0, 1, \ldots, l_0 - 1$ и $\gamma_n \in \mathbb{F}_{2^{2w}}$ определенного выше. Тогда, зашифрованный текст определяется равенством

$$c = (c_0 || \ \ldots \ || c_{l-1} || \operatorname{lsb}_{\operatorname{len}_2(x_l)}(c_l)).$$

Данный способ зашифрования иногда называют «гамма-коммутатор-гамма» или, в англоязычной литературе, «xor-encryption-xor»[88].

Теперь рассмотрим натуральное число m, удовлетворяющее неравенствам $1 \leqslant m \leqslant 2w$, и определим код аутентификации длины m следующими равенствами

$$s = (s_0||s_1) = \sum_{n=0}^{r_0-1} \pi\big(E_{k_1}(y_{2n} \oplus \gamma_{n,0})||E_{k_1}(y_{2n+1} \oplus \gamma_{n,1})\big) \oplus$$
$$\sum_{n=r_0}^{r_0+l_0-1} \pi\big(E_{k_1}(x_{2(n-r_0)} \oplus \gamma_{n,0})||E_{k_1}(x_{2(n-r_0)+1} \oplus \gamma_{n,1})\big) \oplus$$
$$\pi\big(E_{k_1}(\operatorname{len}_2(y) \oplus \gamma_{r_0+l_0,0})||E_{k_1}(\operatorname{len}_2(x) \oplus \gamma_{r_0+l_0,1})\big),$$

и $a = \operatorname{msb}_m\Big(E_{k_2}(s_0)||E_{k_2}(s_1 \oplus E_{k_2}(s_0))\Big)$.

Как видно из приведенных равенств, значение суммы s зашифровывается на ключе k_2 в режиме простой замены с зацеплением и с использованием нулевого инициализационного вектора. Окончательным кодом аутентификации служат старшие m бит вектора, полученного в результате шифрования.

Для построенного отображения автором доказана следующая теорема.

Теорема 3.4. *Пусть блочный шифр $E_k(x) : \mathbb{V}_w \to \mathbb{V}_w$ является перестановкой множества $\mathbb{V}_w$ для любого фиксированного значения ключа $k \in \mathbb{K}$. Тогда, для любых ключей шифрования и имитозащиты $k_1, k_2 \in \mathbb{K}$, а также инициализационного вектора $iv \in \mathbb{V}_{6w}$ определенное выше сжимающее отображение* $\texttt{authenc}(k_1, k_2, iv, x, y)$, *вычисляющее пару значений $\{c, a\}$, обладает свойством равновероятности, т.е. для любого $a \in \mathbb{V}_{2w}$ найдется в точности*

$$2^{\operatorname{len}_2(x)+\operatorname{len}_2(y)-2w}$$

пар x, y, для которых код аутентичности, вырабатываемый отображением $\texttt{authenc}(k_1, k_2, iv, x, y)$, *совпадает с a.*

Свойство равновероятности позволяет обеспечить защиту предложенного режима аутентифицированного шифрования от атак, направленных на подделку и навязывание передаваемой информации. Детальное рассмотрение подходов к построению коллизий для построенного отображения содержится в § 3.3.4.

В рамках разработанного автором программного СКЗИ с открытыми исходными текстами[89], были получены следующие показатели скорости работы различных алгоритмов аутентифицированного шифрования для блочного шифра «Магма» (вычисления производились на персональной ЭВМ с процессором Intel (i5-8250U) и тактовой частотой 1.60GHz), см. таблицу 1.5.

[88] Lyskov M., Rivest R., Wagner D. Tweakable Block Ciphers // Journal Of Cryptology. — 2011. — Vol. 24. — P. 588–613.

[89] Libakrypt: software crypto module for user space. – 2022. – (in accordance with R 1323565.1.012-2017) – https://git.miem.hse.ru/axelkenzo/libakrypt-0.x.

Режим	Скорость, МБс	%
ecb-magma	49,411111	100
mgm-magma	23,424500	47
ctr-cmac-magma	24,101876	48
ctr-hmac-magma-streebog256	35,713519	72
ctr-hmac-magma-streebog512	35,713049	72
xtsmac-magma	45,877878	92

Таблица 1.5: Режимы аутентифицированного шифрования для шифра «Магма».

Аналогичные результаты были получены и для блочного шифра «Кузнечик»[90]. Из приведенных значений следует, что предложенный автором алгоритм аутентифицированного шифрования позволяет достичь наибольшей скорости при программной реализации на универсальных процессорах.

В последней, **четвертой**, главе диссертационной работы рассматриваются вопросы разработки и обоснования безопасности криптографических протоколов защищенного взаимодействия. К таким протоколам относятся транспортные протоколы такие, как MACSec[91], L2TP[92], DTLS[93] и т.п., а также криптографические схемы асимметричного и гибридного шифрования, не предполагающие интерактивного обмена в процессе зашифрования сообщения. Примерами таких схем служат применяемые на практике варианты классических схем RSA[94], NTRU[95] или МакЭлиса[96], стандартизированные[97,98] или предлагаемые к стандартизации решения[99]. Вторым классом рассматриваемых протоколов являются протоколы аутентификации и выработки общего ключа. Примерами таких протоколов служат TLS[100,101], семейство протоколов SIGMA[102], протоколы IKEv2[103,104], а также схемы выработки общего ключа с аутен-

[90]Блочные шифры «Магма» и «Кузнечик» регламентируются стандартом Российской Федерации ГОСТ Р 34.12-2015.

[91]IEEE 802.1AE-2018 – IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security. — 2018.

[92]Layer Two Tunneling Protocol «L2TP» / W. Townsley, A. Valencia, A. Rubens et al. — 1999. — RFC 2661.

[93]Rescorla E., Tschofenig H., Modadugu N. The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. — 2022. — RFC 9147.

[94]PKCS #1: RSA Cryptography Specifications Version 2.2 / K. Moriarty, B. Kaliski, J. Jonsson, A. Rush. — 2016. — RFC 8017.

[95]Chen C., Danba O., Hoffstein J. et al. NTRU: Algorithm Specifications And Supporting Documentation. — 2019.

[96]Albrecht M., Bernstein D., Chou T. et al. Classic McEliece: conservative code-based cryptography. — 2020.

[97]ISO/IEC 18033-2:2006. Information technology. Security techniques. Encryption algorithms — Part 2: Asymmetric ciphers. — 2006.

[98]Р 1323565.1.025.–2019 Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами. — М. : Стандартинформ, 2019.

[99]Aragon N., Barreto P., Bettaieb S. et al. BIKE: Bit Flipping Key Encapsulation. — 2021.

[100]Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. — 2018. — RFC 8446.

[101]Р 1323565.1.030.–2020 Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3). — М. : Стандартинформ, 2020.

[102]Krawczyk H. SIGMA: The «SIGn-and-MAc» Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols // Advances in Cryptology - CRYPTO 2003. — 2003. — P. 400–425.

[103]Internet Key Exchange Protocol Version 2 (IKEv2) / C. Kaufman, P. Hoffman, Y. Nir et al. — 2014. — RFC 7296.

[104]МР 26.2.001.–2022 Информационная технология. Криптографическая защита информации. Ис-

тификацией[105] и протоколы промышленного «Интернета вещей»[106,107].

В § 4.1 уточняются общие модели угроз и нарушителя, используемые далее при оценке безопасности криптографических протоколов. Целью такой оценки является определение численных значений одного или нескольких показателей эффективности мер защиты, реализуемых криптографическим протоколом. При этом, система считается защищенной (безопасной), если полученные в ходе исследования значения показателей попадают в заданную область, установленную нормативными, правовыми документами или требованиями по безопасности.

В § 4.2 рассматривается предложенная автором, совместно с А.В. Пугачевым[108], базовая гибридная схема шифрования ECISPE[109], использующая в качестве шифрующего преобразования полином малой степени. Данная схема использует как асимметричные, так и предварительно распределенные ключи. Доказывается теорема 4.1 о сведении стойкости предложенной гибридной схемы к решению задач дискретного логарифмирования и Диффи-Хеллмана в группе точек эллиптической кривой, задаче определения элементов двоичных последовательностей, вырабатываемых ДСЧ, а также задачи построения коллизии для функции выработки имитовставки. Результаты, полученные в предыдущих главах диссертации, позволяют обеспечить высокую трудоемкость решения указанных задач.

Также рассматриваются несколько модификаций базовой схемы ECISPE, позволяющих изменить её эксплуатационные особенности без изменения стойкости, в частности, предлагается протокол передачи ключевой информации. Данный протокол представляет собой вариант гибридной схемы, обеспечивающий возможность зашифровывать информацию на ключах выработанных заранее, после чего передавать данные ключи вместе с зашифрованной информацией. Также, необходимость передачи ключевой информации от одного субъекта к другому возникает в автоматизированных системах с централизованным изготовлением ключевой информации.

В § 4.3 рассматривается предложенный автором протокол «Крокус». Целью выполнения данного протокола является взаимная аутентификация двух субъектов взаимодействия и последующее однократное выполнение операции типа «запрос-ответ». Данная операция востребована при обеспечении криптографической защиты запросов в удаленные базы данных, а также Интернет-протоколов HTTP и Gemini.

Протокол «Крокус» представляет собой модификацию схемы Диффи-Хеллмана выработки общего ключа, реализуемую в группе точек эллиптической кривой, и состоит из четырех последовательно выполняемых фаз: фазы взаимной аутентификации, фазы выработки общего ключа, фазы подтверждения выработанного общего ключа и фазы обмена зашифрованными сообщениями типа «запрос-ответ». Все перечисленные фазы реализуются в ходе обмена шестью сообщениями.

пользование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2). — М.:ТК26, 2022.

[105]Р 1323565.1.004.–2017 Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. — М. : Стандартинформ, 2017.

[106]Р 1323565.1.028.–2019 Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств. — М. : Стандартинформ, 2019.

[107]Р 1323565.1.032.–2020 Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS. — М.:Стандартинформ, 2020.

[108]Нестеренко А.Ю., Пугачев А.В. Об одной схеме гибридного шифрования // Прикладная дискретная математика. — 2015. — № 4. — С. 56–71.

[109]англ. Elliptic Curve based Integrated Scheme with Polynomial Encryption.

Автором доказывается теорема 4.2 о сведении стойкости протокола «Крокус» к решению следующих задач: задач дискретного логарифмирования и Диффи-Хеллмана в группе точек эллиптической кривой, задаче подделки электронной подписи, задаче определения элементов двоичных последовательностей, вырабатываемых ДСЧ, а также задачи построения прообраза для функции выработки производного ключа.

Также приводится разработанная автором, совместно с А.М. Семеновым и П.А. Лебедевым, модификация протокола «Крокус», направленная на снижение числа передаваемых в ходе выполнения протокола сообщений и сохранение уровня стойкости протокола. Данная модификация была успешно применена для защиты каналов управления контрольными и измерительными устройствами, и стандартизирована к качестве рекомендаций Р 1323565.1.028.–2019 (протокол SP FIOT).

В § 4.4 обосновывается общая методика оценки безопасности криптографических протоколов, частные случаи применения которой иллюстрируются результатами § 4.2 и § 4.3. При разработке методики рассматривалось несколько зарубежных подходов к моделированию криптографических протоколов: базовая модель Белларе-Рогавея[110] и ее модификации[111,112], модель Конетти-Кравчука[113] и ее модификации[114,115], а также ряд подходов, предназначенных для верификации протоколов. Рассматривался отечественный подход, основанный на классическом криптографическом анализе для получения оценок стойкости используемых базовых преобразований[116], а также возможность применения теории «доказуемой стойкости», позволяющей исследовать безопасность протоколов в заданных вероятностных моделях поведения нарушителя с ограниченными вычислительными ресурсами[117,118].

При разработке методики учитывались следующие факторы: необходимость проведения анализа по формальным моделям используемых на практике протоколов; необходимость формализации предъявляемых к протоколу требований (свойств безопасности); вывод численных значений показателей эффективности мер защиты, должен осуществляться с учетом результатов, полученных при оценке стойкости базовых криптографических преобразований, например, алгоритмов блочного шифрования, функций хеширования и выработки имитовставки, алгоритмов выработки электронной подписи и т.п. (в качестве таких показателей, традиционно, выступают вероятность π и трудоемкость Q успешной реализации алгоритмов компрометации крип-

[110]Bellare M., Rogaway P. Entity authentication and key distribution // Advances in Cryptology – Crypto '93. — Vol. 773 Of Lecture Notes Of Computer Science. — Springer, 1993. — P. 232–249.

[111]Blake-Wilson S., Johnson D., Menezes A. Key agreement protocols and their security analysis // Crypography and Coding – 6th IMA Conference. — Springer, 1997. — P. 20–45.

[112]364 Bellare M., Rogaway P., Pointcheval D. Authenticated key exchange secure against dictionary attacks // Advances in Cryptology – EUROCRYPT 2000. — Springer, 2000. — P. 139–155.

[113]Canetti R., Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels // Advances in Cryptology – EUROCRYPT 2001. — P. 453–474.

[114]LaMacchia B.A., Lauter K., Mityagin A. Stronger security of authenticated key exchange // Provable Security, First International Conference, ProvSec 2007 — P. 1–16.

[115]Menezes A., Ustaoglu B. On the importance of public-key validation in the MQV and HMQV key agreement protocols // Progress in Cryptology - INDOCRYPT 2006. — P. 133–147.

[116]Об основных концепциях криптографической стойкости / И.Ф. Качалин, А.С. Кузьмин, Е.А. Суслов и др. // Тезисы XII Всероссийской школы-коллоквиума по стохастическим методам и VI Всероссийского симпозиума по прикладной и промышленной математике. — 2005. — С. 982–983. — Сочи-Дагомыс, 1-7 октября 2005 г.

[117]Обзор уязвимостей некоторых протоколов выработки общего ключа с аутентификацией на основе пароля и принципы построения протокола SESPAKE / Е. К. Алексеев, Л. Р. Ахметзянова, И. Б. Ошкин, С. В. Смышляев // Математические вопросы криптографии. — 2016. — Vol. 7, no. 4. — P. 7–28.

[118]Akhmetzyanova L., Alekseev A., Sedov G., Smyshlyaev S. On Security of TLS 1.2 Record Layer with Russian Ciphersuites // Proceedings of 8-th Workshop on Current Trends in Cryptology (CTCrypt 2019). – 2019. – pp. 253-292.

тографических преобразований), необходимость учета атак на криптографические протоколы, успешность применения которых не зависит от свойств используемых криптографических преобразований.

В результате исследований была выработана модель, представляющая криптографический протокол в виде дискретной динамической системы, множество внутренних состояний которой образует информация, приводящая к компрометации предъявляемых к протоколу свойств. В рамках данной модели были описаны основные свойства безопасности, а также метод подсчета численных оценок указанных выше показателей эффективности мер защиты. Разработанная методика была успешно применена при анализе ряда отечественных криптографических протоколов, что привело к утверждению их в качестве национальных рекомендаций по стандартизации.

ЗАКЛЮЧЕНИЕ

В диссертационной работе предлагается решение актуальной проблемы в области информационной безопасности – проблемы синтеза безопасных криптографических схем и протоколов, применяемых для обмена информацией по открытым каналам связи.

Решение этой проблемы позволило разработать ряд математически обоснованных криптографических схем и протоколов, в частности, схему электронной подписи ГОСТ Р 34.10-2012, схемы выработки общего ключа с аутентификацией на основе открытого ключа Р 1323565.1.004-2017, криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков Р 1323565.1.019-2018, криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств Р 1323565.1.028-2019, протокол обмена ключами в сети Интернет МР 26.2.001- 2022, а также привело к стандартизации указанных схем и протоколов в рамках отечественной системы стандартизации.

В диссертационной работе получены следующие основные результаты:

- Получена верхняя оценка числа шагов алгоритма Госпера и предложен способ применения данного алгоритма для решения задачи дискретного логарифмирования в группе точек эллиптической кривой, что позволило уточнить оценки эффективности мер защиты, реализуемых криптографическими протоколами.

- Доказана теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного. Получены точные оценки трудоемкости такого алгоритма и объема используемой им памяти. Описано множество «слабых» ключей, для которых предложенный алгоритм находит решение с трудоемкостью, меньшей, чем у известных ранее алгоритмов дискретного логарифмирования. Получено точное количество «слабых» ключей для эллиптических кривых, параметры которых рекомендованы Р 1323565.1.024-2019 для использования в средствах защиты информации.

- Доказана теорема о представлении натуральных чисел значениями многочленов в точках мнимого квадратичного поля, а также предложен способ вычисления кратной точки эллиптической кривой, использующий утверждение доказанной теоремы. Предложен алгоритм вычисления явного представления эндоморфизмов эллиптических кривых. Практическая реализация данного алгоритма на

ЭВМ позволила получить представление эндоморфизмов для всех эллиптических кривых, чье кольцо эндоморфизмов изоморфно порядку мнимого квадратичного поля с числом классов равным единице.

- Предъявлены усиленные, по сравнению с ГОСТ Р 34.10-2012, требования к параметрам эллиптических кривых, рекомендуемых к применению в средствах защиты информации. Предложен алгоритм построения таких эллиптических кривых и приведены явные значения параметров, доказывающие возможность достижения предъявленных требований.

- Предложен подход к выработке псевдослучайных последовательностей, основанный на представлении действительных иррациональных чисел в виде систематической дроби по произвольному основанию. Предложены специализированные алгоритмы для представления действительных чисел специального вида, а также получены верхние оценки объема памяти, необходимого для реализации предложенных алгоритмов.

- Предложены алгоритмы восстановлении неизвестных параметров действительных иррациональных чисел специального вида. Доказаны утверждения о невозможности применения предложенных алгоритмов для построения более точных рациональных приближений, что позволяет говорить о невозможности восстановления всех элементов псевдослучайной последовательности по известному фрагменту.

- Предложен метод локальной аутентификации пользователей средств защиты информации, основанный на алгоритме представления действительных чисел в виде систематической дроби по заданному основанию. Данный метод удовлетворяет ряду специальных требований, накладываемых на подобные алгоритмы, в частности, существенно затрудняет процедуру опробования паролей с использованием специальных вычислительных средств.

- Предложен новый класс ключевых функций хэширования и доказан ряд утверждений о том, что функции из данного класса являются равновероятными сжимающими отображениями. Данный класс использован для построения нового режима аутентифицированного шифрования. Результаты практической реализации предложенного режима показывают его преимущество в скорости при программной реализации над регламентированными в Российской Федерации алгоритмами аутентифицированного шифрования.

- Предложена гибридная схема и ряд ее модификаций, реализующих процесс шифрования с помощью полиномиального преобразования. Определена модель возможностей нарушителя и, в этой модели, доказана теорема о стойкости предложенной схемы шифрования относительно задач определения секретного ключа аутентификации, дешифрования и навязывания сообщений. Полученные результаты позволили предложить протокол передачи ключевой информации, основанный на использовании рассматриваемой гибридной схемы шифрования.

- С целью обеспечения защищенного взаимодействия в сетях «Интернета вещей» предложен новый протокол выработки общего ключа со взаимной аутентификацией субъектов взаимодействия. Доказана теорема о стойкости предложенного протокола относительно задач определения общего ключа, дешифрования и навязывания передаваемой в ходе выполнения протокола информации. Модификация данного протокола, направленная на снижение числа передаваемых

в ходе выполнения протокола сообщений, успешно применена для защиты каналов управления контрольными и измерительными устройствами, и стандартизирована к качестве рекомендаций Р 1323565.1.028.–2019.

- Предложена формальная модель, имитирующая криптографический протокол в виде дискретной динамической системы. В рамках данной модели формализован перечень свойств безопасности и определены показатели эффективности мер защиты, обеспечиваемые криптографическим протоколом. Разработан метод получения численных значений показателей эффективности мер защиты, использующий оценки трудоемкости компрометации криптографических преобразований, изменяющих состояния дискретной динамической системы. Предложена методика проведения исследования безопасности криптографических протоколов.

Результаты диссертации могут применяться при исследовании специальных свойств средств криптографической защиты информации.

Благодарности. Автор диссертации выражает благодарность своему научному консультанту доктору физико-математических наук, профессору Чирскому Владимиру Григорьевичу, за постоянное внимание к работе и стимулирование научной деятельности, заведующему кафедрой компьютерной безопасности МИЭМ НИУ ВШЭ, кандидату технических наук Лосю Алексею Борисовичу за многолетнюю поддержку, а также всему коллективу департамента прикладной математики МИЭМ НИУ ВШЭ за внимание к работе.

Выражаю благодарность своему отцу Нестеренко Юрию Валентиновичу за постоянную поддержку и возможность заниматься научными исследованиями.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI:

[57] Chirskii V., Nesterenko A.Yu. An approach to the transformation of periodic sequences. Discrethe Mathematics and Applications. – 2017. – Vol. 27. – № 1.– P.1 – 7. // На русском яз.: [392] Чирский В.Г., Нестеренко А.Ю. Об одном подходе к преобразованию периодических последовательностей. Дискретная математика. – 2015. – Т. 27, № 4. – С. 150 – 157. (doi: 10.4213/dm1354, импакт-фактор: 0,297) / Постановка задачи выполнена Чирским В.Г., остальные результаты получены Нестеренко А.Ю. /

[173] Nesterenko A.Yu. Cycle detection algorithms and their applications. Journal of Mathematical Sciences. – 2012. Vol. 182, № 4. – P. 518 – 526. // На русском яз.: [325] Нестеренко А.Ю. Алгоритмы поиска длин циклов в последовательностях и их приложения. Фундаментальная и прикладная математика. – 2010. – Т. 16, № 6. – С. 109 – 122. (doi: 10.1007/s10958-012-0755-x, импакт-фактор: 0,157).

[175] Nesterenko A.Yu. Constructions of elliptic curves endomorphisms. Математические вопросы криптографии. – 2014. – Т. 5, № 2. – С. 99 – 102. (doi: 10.4213/mvk121, импакт-фактор: 0,36).

[176] Nesterenko A.Yu. Some remarks on the elliptic curve discrete logarithm problem. Математические вопросы криптографии. – 2016. – Т. 7, № 2. – P. 115–120. (doi: 10.4213/mvk189, импакт-фактор: 0,36).

[178] Nesterenko A.Yu. A new authenticated encryption mode for arbitrary block cipher based on universal hash function. Математические вопросы криптографии. – 2017. – Vol. 8, № 2. – P. 117–130. (doi: 10.4213/mvk228, импакт-фактор: 0,36).

[179] Nesterenko A.Yu. Construction of strong elliptic curves suitable for cryptographic applications. Математические вопросы криптографии. – 2019. – Vol. 10, № 2. – P. 135–144. (doi: 10.4213/mvk291, импакт-фактор: 0,36).

[181] Nesterenko A.Yu., Semenov A.M. On the practical implementation of Russian protocols for low-resource cryptographic modules. Journal of Computer Virology and Hacking Techniques. – 2020. – Vol. 16, № 4. – P. 305 – 312. (doi: 10.1007/s11416-020-00362-y). / Нестеренко А.Ю. принадлежат результаты о свойствах ключевой системы рассматриваемого семейства протоколов./

[311] Лебедев П.А., Нестеренко А.Ю. Арифметика эллиптических кривых с использованием графических вычислителей. Чебышевский сборник. – 2012. – Т. 13, № 2. – С. 91 – 105. (импакт-фактор: 0,419) /Нестеренко А.Ю. принадлежат теоретические результаты, Лебедеву П.А. – результаты практических экспериментов./

[326] Нестеренко А.Ю. О некоторых свойствах эллиптической кривой в форме Якоби. Чебышевский сборник. –2010.–Т.11,№ 1. – С.202 – 208. (импакт-фактор: 0,419)

[332] Нестеренко А.Ю. Алгоритм восстановления параметров одного класса иррациональных чисел. Известия Саратовского университета. Серия: Математика. Механика. Информатика. – 2013. – Т. 13, № 4 (часть 2). – С. 89 – 93. (doi: 10.18500/1816-9791-2013-13-4-89-93, импакт-фактор: 0.20)

[334] Нестеренко А.Ю. Об одном подходе к построению защищенных соединений. Математические вопросы криптографии. – 2013. – Т. 4, № 2. – С. 101 – 111. (doi: 10.4213/mvk86, импакт-фактор: 0,36).

[336] Нестеренко А.Ю. Об одном семействе универсальных функций хеширования. Математические вопросы криптографии. – 2015. – Т. 6, № 3. – С. 135 – 151. (doi: 10.4213/mvk164, импакт-фактор: 0,36).

[338] Нестеренко А.Ю. Об одном подходе к разложению иррациональных чисел. Математические вопросы криптографии. – 2018. – Т. 9, № 1. – С. 89 – 106. (doi: 10.4213/mvk189, импакт-фактор: 0,36).

[341] Нестеренко А.Ю., Пугачев А.В. Об одной схеме гибридного шифрования. Прикладная дискретная математика. – 2015. – № 4. – С. 56 – 71. (doi: 10.17223/20710410/30/5, импакт-фактор: 0.22) / Нестеренко А.Ю. принадлежат результаты оценки стойкости, а Пугачеву А.В. – оценки скорости работы рассматриваемой схемы шифрования./

[343] Нестеренко А.Ю., Семенов А.М. Методика оценки безопасности криптографических протоколов. Прикладная дискретная математика. – 2022. – № 56. – С. 33 – 82. (doi: 10.17223/20710410/56/4, импакт-фактор: 0.22) /Семенову А.М. принадлежат формализация и анализ свойств безопасности криптографических протоколов, Нестеренко А.Ю. – формулировка модели и метод оценки показателей мер защиты./

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

[272] Билык Т.А., Нестеренко А.Ю. Код аутентификации сообщений на основе универсального хэширующего преобразования. Безопасность информационных технологий. – 2012. – № 2. – С. 38 – 42. /Нестеренко А.Ю. принадлежит постановка задачи и результат о необходимости шифрования результата сжимающего отображения./

[312] Лебедев П.А., Нестеренко А.Ю. Режим шифрования с возможностью аутентификации. Системы высокой доступности. – 2013. – Т. 9, № 3. – С. 6 – 13. /Нестеренко А.Ю. принадлежат теоретические результаты, Лебедеву П.А. – результаты практических экспериментов. /

[327] Нестеренко А.Ю. Новый протокол выработки общего ключа. Системы высокой доступности. – 2012. – № 2. – С. 81 – 90.

[328] Нестеренко А.Ю. О криптографических протоколах удаленного управления. Проблемы информационной безопасности. Компьютерные системы. — 2012. — № 2. – С. 76 – 82.

[330] Нестеренко А.Ю. О статистических свойствах некоторых трансцендентных чисел. Ученые записки Орловского государственного университета. – 2012. – № 6 (часть 2). – С. 170 – 176.

[342] Нестеренко А.Ю., Семенов А.М. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств. Безопасность информационных технологий, 2020. – Т. 27, № 4, С. 7–16. /Нестеренко А.Ю. принадлежат результаты о ключевой системе рассматриваемого семейства протоколов, остальные результаты принадлежат Семенову А.М./

Другие публикации:

[180] Nesterenko A.Yu. Differential properties of authenticated encryption mode based on universal hash function (XTSMAC). XVII International Symposium «Problems of Redundancy in Information and Control Systems (REDUNDANCY)». — 2021.

[269] Аносов В.Д., Нестеренко А.Ю. Схема асимметричного шифрования, основанная на отечественных криптографических примитивах. Материалы IX международной конференции «Интеллектуальные системы и компьютерные науки» в МГУ, Москва, 2006.

[316] Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. Учебник для академического бакалавриата. Серия: Бакалавр. Академический курс. – 2 изд. – М.: Изд-во «Юрайт», 2016.

[322] Нестеренко А.Ю. Схема асимметричного шифрования с возможностью аутентификации. Труды VII Международной научно-технической конференции «Новые информационные технологии и системы», Пенза, 2006.

[323] Нестеренко А.Ю. Об одном варианте метода Ленстры факторизации целых чисел. Материалы третьей международной конференции по проблемам безопасности и противодействия терроризму в МГУ им. М.В. Ломоносова, Москва, 2008.

[331] Нестеренко А.Ю. Об одном протоколе выработки общего ключа. Материалы конференции «РусКрипто-2012», 2012.

[335] Нестеренко А.Ю. Об одном алгоритме развертки ключа из пароля. Материалы конференции «РусКрипто-2015», 2015.

[340] Нестеренко А.Ю., Лебедев П.А., Семенов А.М. Краткий анализ криптографических механизмов защищенного взаимодействия контрольных и измерительных устройств, Технический комитет по стандартизации «Криптографическая защита информации». Серия б/н «Криптографические исследования». — 2019.

Разработанные и исследованные в диссертации методы защиты информации и основанные на них криптографические механизмы стандартизированы в следующих стандартах, российских стандартах и рекомендациях по стандартизации.

[280] ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва, Стандартинформ, 2012.

[373] Р 50.1.115.–2016. Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля. Москва, Стандартинформ, 2016.

[352] Р 1323565.1.004-2017. Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. Москва, Стандартинформ, 2017.

[357] Р 1323565.1.018-2018. Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта. Москва, Стандартинформ, 2018.

[358] Р 1323565.1.019-2018. Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных. Москва, Стандартинформ, 2018.

[359] Р 1323565.1.020-2018. Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2). Москва, Стандартинформ, 2018.

[362] Р 1323565.1.024–2019. Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов. Москва, Стандартинформ, 2018.

[364] Р 1323565.1.026–2019. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование. Москва, Стандартинформ, 2019.

[365] Р 1323565.1.028–2019. Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств. Москва, Стандартинформ, 2019.

[366] Р 1323565.1.029–2019. Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем Москва, Стандартинформ, 2019.

[367] Р 1323565.1.030-2020. Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3). Москва, Стандартинформ, 2020.

[368] Р 1323565.1.032-2020. Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS. Москва, Стандартинформ, 2020.

[370] Р 1323565.1.035–2021. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP. Москва, Стандартинформ, 2021.

[317] МР 26.2.001- 2022. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2). Москва, Стандартинформ, 2022.

Результаты диссертации внедрены в программные средства защиты информации, имеющие следующие свидетельства о государственной регистрации программы для ЭВМ.

[376] Свидетельство о государственной регистрации программы для ЭВМ № 2018666094 «Библиотека криптографических механизмов защиты контрольных цифровых устройств». Правообладатель: ООО «НМП». Авторы: Жуков И.Ю., Мурашов О.Н., Нестеренко А.Ю., Решетник В.В.

[377] Свидетельство о государственной регистрации программы для ЭВМ № 2018666095 «Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта». Правообладатель: ООО «НМП». Авторы: Жуков И.Ю., Мурашов О.Н., Нестеренко А.Ю., Решетник В.В.

[378] Свидетельство о государственной регистрации программы для ЭВМ № 2018666420 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств». Правообладатель: ООО «НМП». Авторы: Жуков И.Ю., Мурашов О.Н., Нестеренко А.Ю., Решетник В.В.

[379] Свидетельство о государственной регистрации программы для ЭВМ № 2018666512 «Криптографические механизмы аутентификации и выработки ключа фискального признака». Правообладатель: ООО «НМП». Авторы: Жуков И.Ю., Мурашов О.Н., Нестеренко А.Ю., Решетник В.В.

В программах для ЭВМ, на которые выданы перечисленные выше свидетельства, внедрены методы защиты информации, разработанные в § 3.2, § 3.3 и § 4.3.2 диссертационной работы.