

## **Выдержки из автореферата диссертации**

### **«МЕТОДОЛОГИЯ ПРОЕКТИРОВАНИЯ АЛГОРИТМОВ АУТЕНТИФИКАЦИИ ДЛЯ КРИТИЧЕСКИХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»**

**на соискание Ростовцевым А. Г. ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность**

#### **Общая характеристика работы**

**Актуальность проблемы.** Стремительное развитие средств защиты информации и методов их анализа в ряде случаев приводит к изменению взгляда на безопасность существующей аппаратуры защиты информации, пересмотру модели нарушителя и повышению нормативных требований. В наибольшей степени указанные изменения характерны для подсистем аутентификации, в которых возникает необходимость обеспечения информационной безопасности в условиях взаимного недоверия или сговора участников протокола, что позволяет говорить о критических подсистемах аутентификации. Важнейшим этапом создания таких подсистем является проектирование алгоритмов аутентификации.

Безопасность подсистем аутентификации не может быть проверена экспериментально в ходе испытаний на функционирование. Кроме того, из-за обилия криптографических алгоритмов и многообразия задач аутентификации эти системы зачастую проектируются «с нуля», что увеличивает трудоемкость разработки. Алгоритмизация процесса проектирования и обоснование принимаемых решений позволят избежать типовых ошибок, а также сравнивать различные варианты построения алгоритмов аутентификации и выбрать наилучший из них.

**Целью работы** является создание общей концепции и теоретических основ методологии проектирования алгоритмов аутентификации для критических информационно-телекоммуникационных систем.

Для достижения поставленной цели решались следующие **задачи**.

1. Формальная постановка задачи проектирования алгоритмов аутентификации; разработка общей схемы процесса проектирования.
2. Анализ сложности математических задач, положенных в основу безопасности; разработка новых и развитие существующих математических методов решения этих задач.
3. Разработка методики построения комплекса алгоритмов аутентификации; разработка обобщенных протоколов аутентификации и анализ их безопасности.
4. Экспериментальная проверка предложенной методики на примере разработки набора алгоритмов аутентификации на эллиптических кривых.

**Основные научные результаты, выносимые на защиту, и их новизна.**

1. Впервые проведена формализация задачи проектирования алгоритмов аутентификации путем минимизации набора защитных функций на основе сопоставления классов унифицированных математических задач с множеством криптографических примитивов.
2. Разработана общая схема проектирования алгоритмов аутентификации, позволяющая реализовать функционально полный набор защитных функций, в том числе с экспоненциальной и переборной стойкостью.
3. Проведены исследования сложности решения математических задач, положенных в основу безопасности, в том числе с использованием оригинальных математических методов:
  - предложен метод решения задачи о встрече на случайном лесе;
  - впервые предложен решеточный метод анализа итерированной хэш-функции;
  - улучшен метод логарифмирования на эллиптических кривых за счет использования разрешимых орбит автоморфизмов;
  - предложен подход к логарифмированию на эллиптической кривой, основанный на поднятии точки кривой в числовое поле.
4. Разработана методика построения функционально полного набора протоколов аутентификации на произвольной конечной абелевой группе, обладающих экспоненциальной и переборной стойкостью.

5. Впервые предложено использовать задачу вычисления изогении между эллиптическими кривыми для построения алгоритмов аутентификации.
6. Разработана методика выбора параметров подсистемы аутентификации на эллиптических кривых.
7. Разработаны быстрые алгоритмы арифметики эллиптических кривых над простыми полями на основе комплексного умножения.

**Практическая ценность работы.** Разработанные теоретические положения диссертации положены в основу создания ряда подсистем аутентификации, что позволило существенно улучшить функциональные возможности и защитные характеристики подсистем аутентификации.

Создан комплекс учебных программ по основным курсам специализации «Защита информации в компьютерных системах» и магистерской программы «Безопасность и защита информации». Значительная часть материалов диссертации вошла в издания «Алгебраические основы криптографии» и «Введение в криптографию с открытым ключом».

### Содержание работы

#### Глава 1. Формализация задачи проектирования алгоритмов аутентификации.

Для постановки задачи проектирования в работе вводится обобщенная схема аутентификации (рис. 1), включающая в себя двух легальных участников – претендента  $P$  и верификатора  $V$ , причем верификатор по определению не доверяет претенденту. Кроме того, предполагается существование нарушителя  $I$ , способного формировать информацию  $i$  и действовать автономно или в сговоре с верификатором. Для аутентификации сообщения  $m$  претендент предъявляет верификатору некоторую служебную информацию  $p$ , формируемую с помощью конфиденциального ключа  $k$ . Если аутентификация выполняется путем диалога, то  $p$  зависит от запросов  $v$  верификатора. Верификатор умеет проверять правильность текстов, формируемых претендентом, т. е. обладает некоторой информацией  $k'$  о ключе  $k$  (открытым ключом). Задача вычисления ключа  $k$  на основе передаваемых, а также других доступных нарушителю данных должна быть сложной. Генерация параметров подсистемы аутентификации и ключей  $k, k'$  осуществляется соответствующими службами.

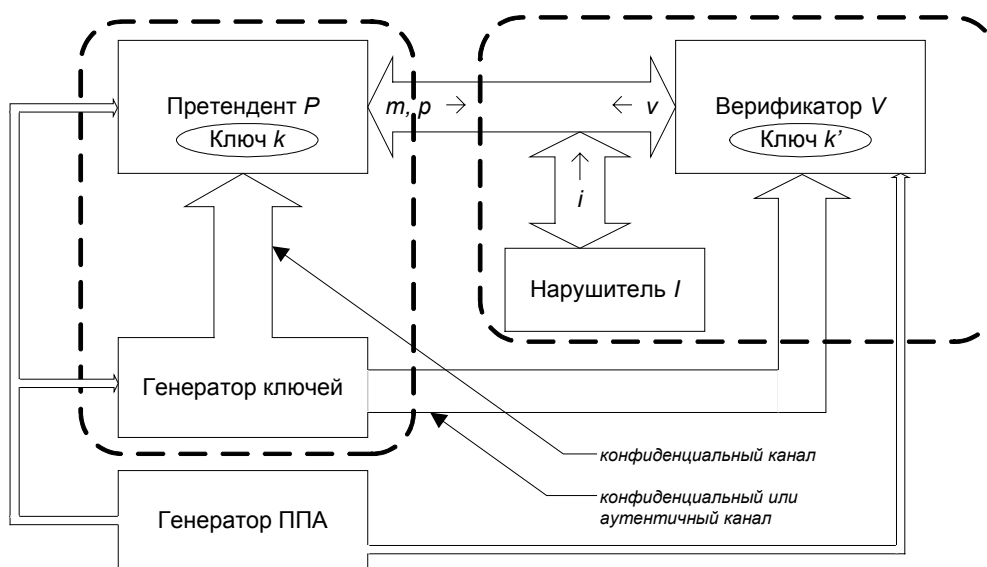


Рис. 1. Обобщенная схема аутентификации

В ходе аутентификации нарушитель по определению знает информацию  $\{v, m, p\}$ , которая может давать ему некоторые знания о ключе  $k$  как условную колмогоровскую энтропию  $H_K(k|\{v, m, p\})$ . Нарушитель может знать и ключ  $k'$ , если верификатор не является доверенной стороной. В зависимости от объема  $\delta H_K$  разглашаемых за один сеанс знаний о ключе  $k$ ,  $\delta H_K = 1 - H_K(k | (k', \{v, m, p\})) / H_K(k | k')$ , можно говорить об однократной, ограниченной

кратности и многократной аутентификации. Случаи полного и частичного, а также минимального и нулевого разглашения знаний различаются непринципиально, поэтому можно рассматривать схемы только однократной и многократной аутентификации.

Важнейшей частью подсистемы аутентификации является совокупность алгоритмов аутентификации, которые задают набор защитных функций, определяющих, что и при каких условиях может быть защищено. Доказано, что защитные функции образуют решетку, изоморфную подрешетке булевых функций.

### Упорядоченность защитных функций аутентификации

Координаты защитных функций	Упорядоченность
Тип аутентификации	аутентификация сообщения $\supseteq$ опознавание
Число сеансов на одном ключе	многократная аутентификация $\supseteq$ однократная аутентификация
Тип используемого канала связи (возможность диалога)	бездиалоговая аутентификация $\supseteq$ диалоговая аутентификация
Доверие к верификатору	недоверенный верификатор $\supseteq$ доверенный верификатор
Качество связи (при однократной аутентификации требуется надежное доведение информации)	некритичность надежного доведения информации $\supseteq$ необходимость надежного доведения информации
Наличие службы единого времени (необходимо для защиты от повторов или задержек информации при бездиалоговой аутентификации)	необязательность единого времени $\supseteq$ наличие единого времени
Относительный объем передаваемой служебной информации (отношение объема передаваемых данных к энтропии $H_K(k k')$ )	меньший относительный объем служебной информации $\supseteq$ больший относительный объем служебной информации

В работе в состав алгоритмов аутентификации включены:

- собственно протоколы аутентификации;
- быстрые алгоритмы, реализующие вычисления в соответствующих математических структурах;
- вспомогательные алгоритмы, влияющие на безопасность;
- алгоритмы выбора параметров подсистемы аутентификации;
- алгоритмы управления ключами, включая смену параметров подсистемы аутентификации.

Стандартные алгоритмы аутентификации не всегда удовлетворяют требованиям, предъявляемым к критическим информационно-телекоммуникационным системам, поэтому появляется необходимость проектирования оригинальных алгоритмов аутентификации. Безопасность этих алгоритмов традиционно основывается на сложности решения математической задачи, для выбора которой в ходе проектирования предлагается трехуровневая систематизация задач.

К первому уровню отнесены классы унифицированных математических задач (КУМЗ), в качестве которых предложено рассматривать следующие типы задач, ориентированных на построение алгоритмов аутентификации:

- 1) задача о выполнимости (к которой сводятся задачи вскрытия ключа, обращения и вычисления коллизий хэш-функции);
- 2) задача определения структуры и порядка конечной группы;
- 3) задача вычисления индекса элемента конечной абелевой группы;
- 4) задача об укладке ранца;
- 5) кроме того, впервые вводится задача вычисления морфизма между объектами категории.

Ко второму уровню отнесены массовые основные математические задачи выбора (ОМЗ), полученные в результате параметризации КУМЗ с помощью математических структур, определяющих область математики, к которой относится ОМЗ, а также классы связанных задач, к которым сводится ОМЗ. Кроме задач выбора при исследовании безопасности используются также дополнительные задачи распознавания и поиска.

К третьему уровню отнесены частные математические задачи, соответствующие массовой ОМЗ.

Проектирование алгоритмов аутентификации (рис. 2) предлагается формально определять как процесс построения цепочек отображений:

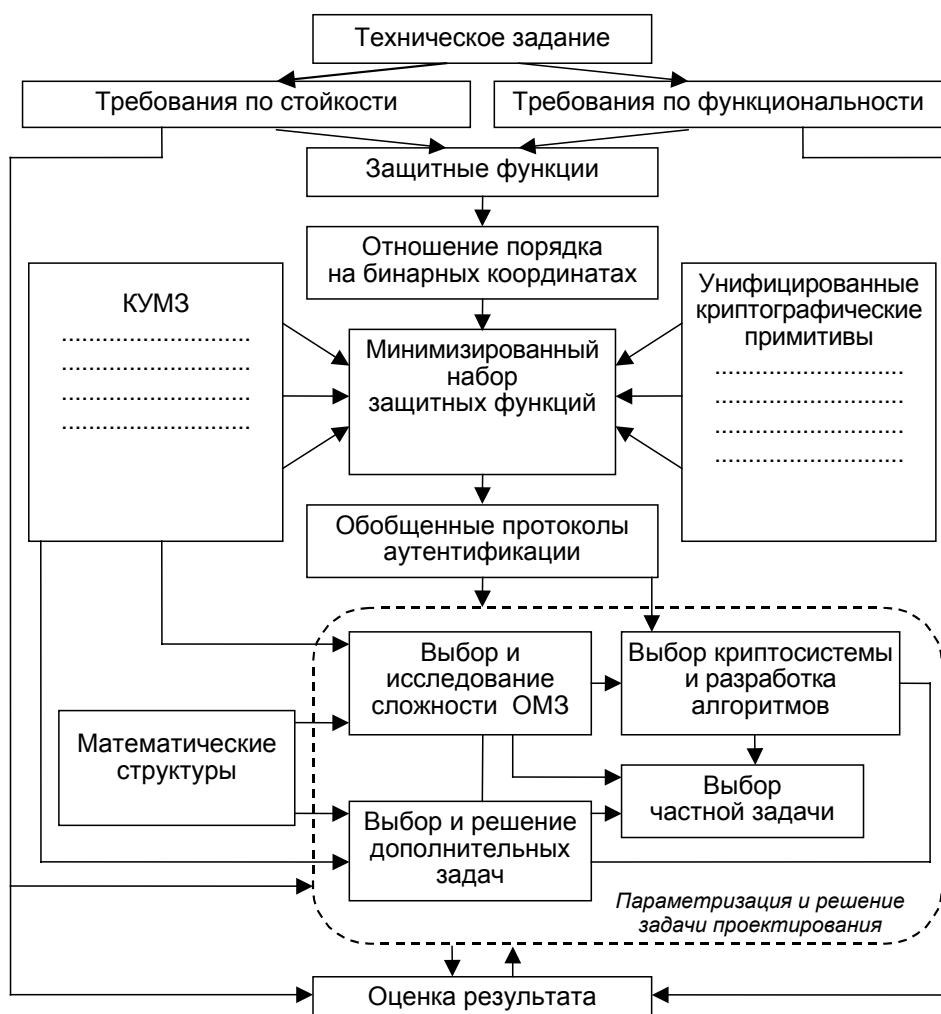
$$\begin{aligned} & \{КУМЗ\} \times \{\text{унифицированные криптографические примитивы}\} \rightarrow \\ & \rightarrow \{\text{минимизированный набор защитных функций}\} \rightarrow \\ & \rightarrow \{\text{обобщенные протоколы аутентификации}\}; \\ & \{КУМЗ\} \times \{\text{математические структуры}\} \rightarrow \{ОМЗ\} \cup \{\text{дополнительные задачи}\}; \\ & \{ОМЗ\} \times \{\text{обобщенные протоколы аутентификации}\} \rightarrow \\ & \rightarrow \{\text{алгоритмы аутентификации}\} \rightarrow \{\text{быстрые вычислительные алгоритмы}\}; \\ & \{ОМЗ\} \cup \{\text{дополнительные задачи}\} \rightarrow \{\text{алгоритмы генерации параметров подсистемы аутентификации}\} \rightarrow \{\text{частные математические задачи}\} \rightarrow \{\text{алгоритмы управления ключами}\}. \end{aligned}$$


Рис. 2. Схема процесса проектирования алгоритмов аутентификации

Унифицированные криптографические примитивы включают в себя: симметричное шифрование, шифрование с открытым ключом, бесключевую и ключевую хэш-функцию, цифровую подпись, диалоговые и бездиалоговые доказательства с нулевым разглашением знаний, секретные гомоморфизмы. Множества математических задач и криптографических примитивов следует рассматривать в их диалектическом развитии.

**Глава 2. Математические задачи и структуры и параметризация задачи проектирования.** При проектировании алгоритмов аутентификации нужно прогнозировать как снижение сложности математической задачи, так и рост производительности вычислитель-

ной техники, позволяющей решить эту задачу, а также развитие других (не связанных непосредственно с вычислениями) возможностей нарушителя, направленных на снижение безопасности.

Скорость  $s(t, T)$  падения стойкости  $S(t)$  на интервале времени  $(T, T + t)$  предложено определять по формуле  $s(t, T) = (\log S(T) - \log S(T + t)) / (t \log S(T))$ . Показано, что сложность задач падает примерно с постоянной скоростью. Полученные оценки позволяют прогнозировать снижение сложности и определять время жизни ключа.

Задачи, положенные в основу безопасности алгоритмов аутентификации, предлагается классифицировать по трем типам: выбор, распознавание, поиск. В ходе проектирования обычно требуется обосновать сложность задачи выбора и найти или оценить решение задач распознавания и поиска.

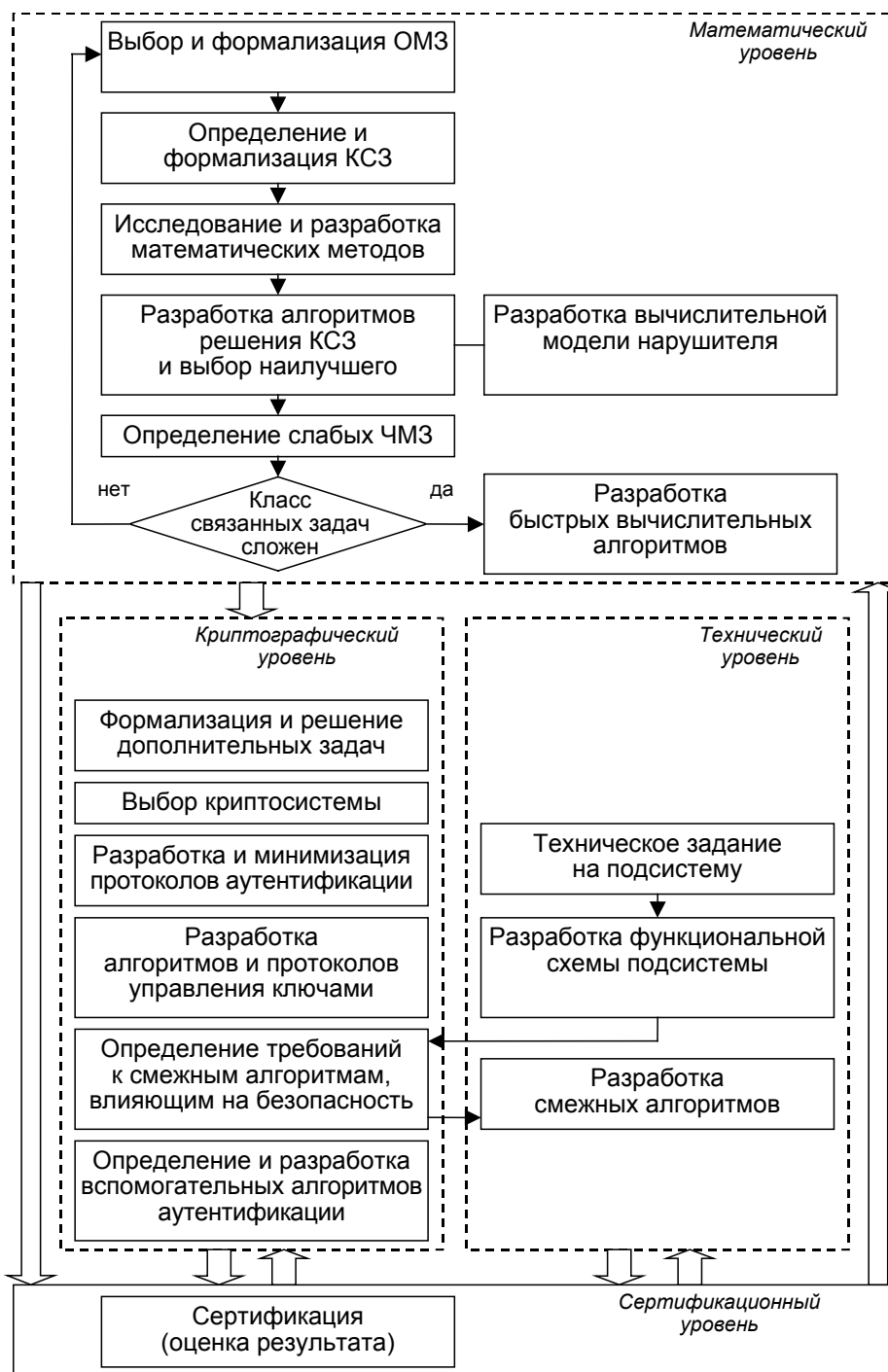


Рис. 3. Схема параметризации и решения задачи проектирования

Математические структуры, используемые при проектировании алгоритмов аутентификации в условиях доверенного верификатора, как правило, не обладают эффективно разрешимыми алгебраическими свойствами и вычислимыми статистическими характеристиками. Это вызывает необходимость введения дополнительных задач и обуславливает их сложность.

Для аутентификации в условиях недоверенного верификатора используются математические структуры с распознаваемыми алгебраическими свойствами (группы, кольца, категории) и соответствующие ОМЗ. Единственная известная сложная задача определения структуры и порядка группы, допускающая построение алгоритмов аутентификации, использует группу  $(\mathbb{Z}/n\mathbb{Z})^*$ , где  $n$  – число с секретным разложением. В работе доказана сводимость задачи определения структуры группы  $(\mathbb{Z}/n\mathbb{Z})^*$  или ее порядка к 3Р числа  $n$ , задачи логарифмирования в конечном поле к ЗДЛ на эллиптической кривой.

На основании анализа особенностей применения ОМЗ сформулированы требования к ОМЗ и соответствующим классам связанных задач (КСЗ), к которым полиномиально сводится задача нарушения безопасности.

Для параметризации и решения задачи проектирования алгоритмов аутентификации предлагается четырехуровневая схема (рис. 3), которая характеризуется, помимо традиционного технического уровня, наличием математического, криптографического и сертификационного уровней.

Математический уровень является наиболее специфическим, в значительной степени определяет трудоемкость проектирования, требует высокой научной квалификации исполнителей и по этой причине не может быть эффективно распараллелен.

**Глава 3. Исследование и разработка методов решения основных математических и дополнительных задач.** Как показано в гл. 1, одной из координат защитной функции является доверие или недоверие к верификатору. В работе анализируются ОМЗ для обоих значений этой координаты.

В случае доверенного верификатора в качестве ОМЗ обычно используется вариант NP-полной задачи о выполнимости. Соответствующий протокол аутентификации реализуется на основе примитива ключевой хэш-функции или симметричного шифрования.

Для исследования безопасности указанной ключевой хэш-функции в работе предложен решеточный метод решения задачи о выполнимости, основанный на вложении решетки булевых функций в дистрибутивную решетку над конечным множеством рациональных чисел  $\{a \mid 0 \leq a \leq 1\}$  и требующий для однозначного определения ключа в среднем  $1,36 \cdot \log_2(\#Z)$  бит аргументов и соответствующих значений хэш-функции, где  $Z$  – множество ключей. Продолжение функционального базиса  $\{\wedge, \vee, \bar{\phantom{a}}\}$  имеет вид  $a \wedge b = ab = \min(a, b)$ ;  $a \vee b = \max(a, b)$ ;  $\bar{\bar{a}} = 1 - a$ . При переходе к дизъюнктивной нормальной форме целевая функция представляется в виде

$$H = \tilde{z}_1 \dots \tilde{z}_N \bigvee_{i=1}^N (g_i z_i \bar{z}_i),$$
 где  $\tilde{z}_i$  означает вхождение переменной  $z_i$  с инверсией или без инверсии,  $\tilde{z}_1 \dots \tilde{z}_N$  – целевая конъюнкция,  $N$  – разрядность ключа,  $g_i$  – решеточные продолжения булевых функций. Функция  $H$  эффективно вычислима для произвольного набора аргументов.

Для вскрытия ключа переменным  $z_i$  придаются произвольные рациональные значения из интервала  $[0, 1]$  с попарно различными удалениями rem (числом переменных, расположенных к 0,5 ближе, чем значение функции) и вычисляется функция  $H$ . Если  $\text{rem}(H) > 0$ , то метод позволяет отбраковать  $2^{\text{rem}(H)}$  ключей за одно опробование и сократить объем перебора.

**Теорема 1.** Задача вскрытия ключа сводится к задаче решеточного продолжения подстановок, которое сохраняет целевую конъюнкцию и при котором удаления выходных разрядов подстановок попарно различны.

**Теорема 2.** Задача вскрытия ключа сводится к задаче минимизации булевой функции, представленной в виде композиций дизъюнктивных нормальных форм.

Противодействие решеточному методу достигается увеличением числа итераций. Каждый разряд ключа должен использоваться не менее чем на двух итерациях, число итераций между первым и последним обращениями к данному разряду ключа должно быть не менее удвоенного числа итераций, необходимых для того, чтобы данный разряд ключа вошел во все булевы уравнения, описывающие разряды промежуточного текста.

В случае недоверенного верификатора аутентификация осуществляется методами криптографии с открытым ключом, а в качестве ОМЗ используются теоретико-числовые и алгебраические задачи в силу их хорошей изученности и удобства реализации. В работе дана классификация наиболее популярных криптосистем, выбираемых на криптографическом уровне, по КУМЗ.

Для решения ЗДЛ предложен и исследован метод встречи на случайном лесе, использующий сжимающие свойства случайного отображения.

**Теорема 3.** Алгоритм встречи на ориентированном лесе, индуцированном действием случайного отображения на элементах группы порядка  $r$ , имеет сложность  $O(\sqrt{r \log r})$ .

Отсюда вытекает невозможность улучшения алгоритма Полларда для решения ЗДЛ в циклической группе общего вида.

В качестве ОМЗ, соответствующей задаче вычисления морфизма между объектами категории, предложено использовать задачу вычисления изогении между эллиптическими кривыми (ЗВИК). В случае, когда морфизмы образованы несколькими изогениями простых степеней, ЗВИК сводится к вычислению пути на связанном неориентированном графе с ограниченной кратностью вершины и имеет сложность  $O(\sqrt[4]{p})$ .

Сравнительный анализ ОМЗ, используемых для многократной аутентификации при недоверенном верификаторе, показал, что наилучшими для критических информационно-телекоммуникационных систем являются ЗДЛ в группе точек эллиптической кривой и ЗВИК.

Для обеспечения высокой стойкости алгоритмов аутентификации на эллиптических кривых  $E(\mathbb{F}_p)$  параметры подсистемы аутентификации должны удовлетворять следующим требованиям: порядок  $r$  циклической группы – большое простое число;  $p^d \not\equiv 1 \pmod{r}$  для  $1 \leq d < 50$ ;  $r \neq p$ ; число классов  $h_{\mathbb{Q}(\sqrt{4p - \text{Tr}(\varphi)^2})} > 50$ , где  $\text{Tr}(\varphi) = p + 1 - \#E(\mathbb{F}_p)$  – след эндоморфизма Фробениуса. Если эти требования выполнены, то наилучшими известными методами решения задачи являются метод Полларда со сложностью  $O(\sqrt{r})$ , не допускающий распараллеливания, и метод встречи на случайном лесе, допускающий распараллеливание.

Предложен способ снижения сложности логарифмирования на эллиптических кривых: сначала применить алгоритм Полларда к эффективно разрешимым орбитам относительно группы автоморфизмов, затем уточнить логарифм внутри орбиты. Показано, что такими автоморфизмами могут служить только автоморфизмы, определяемые комплексным умножением. Снижение сложности пропорционально корню из порядка группы автоморфизмов. Предложен способ противодействия указанной атаке.

Предложен метод логарифмирования на эллиптической кривой, основанный на поднятии точки кривой из конечного поля в числовое поле. Соответствующий класс связанных задач включает в себя ЗДЛ в группе точек кривой и задачу поднятия точки в числовое поле и определяется следующей теоремой.

**Теорема 4.** ЗДЛ на эллиптической кривой  $E(\mathbb{F}_p)$  полиномиально сводится к задаче такого поднятия точки кривой из конечного поля  $\mathbb{F}_p$  в числовое поле  $K$ , что вес поднятой точки (сумма абсолютных значений координат векторного индекса) минимален, и к нахождению множества образующих кривой  $E(K)$ .

Для решения ЗДЛ, то есть для вычисления логарифма  $l$  такого, что  $P = lQ$ , где  $P, Q \in E(\mathbb{F}_p)$ , предлагается использовать следующий алгоритм.

1. Выбрать числовое поле  $K$  и кривую  $E(K)$  такие, что кривые  $E(K) \pmod{p}$  и  $E(\mathbb{F}_p)$  изогенны; при этом ранг  $\rho$  кривой  $E(K)$ , вычисленный на основании гипотезы Берча и Свиннертона-Дайера, должен быть достаточно велик (не менее 20).
2. Найти множество образующих группы Морделла – Вейля кривой  $E(K)$ .
3. Поднять  $O(\rho)$  точек вида  $aP + bQ$  кривой  $E(\mathbb{F}_p)$  для известных  $a, b$  в поле  $K$ .
4. Найти индексы поднятых точек кривой  $E(K)$  в группе Морделла – Вейля последовательной минимизацией их канонической высоты.
5. Методом гауссова исключения найти логарифм  $l$  в группе  $\mathbb{F}_r$ .

Поскольку оценки сложности поднятия не известны, теорема 4 определяет новое направление исследований ЗДЛ на эллиптической кривой. Принятой оценкой сложности ЗДЛ является сложность алгоритмов Полларда и встречи на случайном дереве.

Исследована сложность ЗДЛ на эллиптической кривой по отношению к молекулярному компьютеру. Показано, что при ограничении объема молекулярного компьютера значением  $10^{10}$  л эта вычислительная модель не имеет преимуществ по сравнению с традиционной. Квантовый компьютер большой разрядности теоретически позволяет решать за полиномиальное время ЗДЛ и ЗР, но не ЗВИК, однако возможность его создания проблематична.

Показано, что решение дополнительных задач распознавания и поиска может быть найдено известными методами.

**Глава 4. Методика построения алгоритмов аутентификации и управления ключами.** Разработанная методика построения алгоритмов аутентификации позволяет реализовать полный набор защитных функций аутентификации с учетом их упорядочения. Составлен набор обобщенных протоколов аутентификации, соответствующих полному минимизированному набору защитных функций, и исследована их безопасность.

В случае аутентификации в условиях доверенного верификатора весь набор защитных функций может быть реализован на основе стандартных примитивов, например, симметричного шифрования или ключевой хэш-функции по ГОСТ 28147–89. При бездиалоговой аутентификации в состав служебной информации  $p$  (см. рис. 1) вводится код текущего времени.

Однократная аутентификация сообщения в условиях недоверенного верификатора может осуществляться протоколами Меркля и Рабина с использованием симметричного шифрования по ГОСТ 28147–89.

В основу однократного бездиалогового опознавания (требующего надежного доведения информации) в условиях недоверенного верификатора положена задача обращения вычислимой в одну сторону бесключевой хэш-функции. Хэш-функция по ГОСТ Р 34.11–94 может использоваться, если в схеме аутентификации допустимы коллизии. Предлагается обобщенный способ построения хэш-функций без коллизий, допускающий использование произвольного циклического модуля и основанный на следующей теореме.

**Теорема 5.** Пусть  $G$  – циклический модуль простого порядка  $r$  с образующей  $a$  и  $f: \mathbf{F}_r \times G \rightarrow \mathbf{F}_r$  – вычислимая инъективная функция. Тогда хэш-функции  $h_i(u)$  вида  $h_1(u) = f(u, a)a$ ,  $h_2(u) = f(u, h_1)a$ , ...,  $h_n(u) = f(u, h_{n-1})a$  вычислимы в одну сторону и не имеют коллизий.

Предлагается способ построения функции  $f(u, x)$ . Размер аргумента  $u$  не превышает  $0,5 \cdot \log_2 r$ . В качестве значения функции берется конкатенация  $u||$ (отдельные разряды  $x$ ) такая, что это значение как целое число не превышает  $r$ . С ростом числа  $n$  возрастает сложность как вычисления хэш-функции  $h_n$ , так и ее обращения. При  $n \geq 2$  наилучшим известным алгоритмом обращения хэш-функции является перебор. Стойкость алгоритма однократного опознавания обосновывается следующей теоремой.

**Теорема 6.** Задача обращения хэш-функции  $h_n$  эквивалентна задаче дискретного логарифмирования в группе  $G$ .

Предложенная хэш-функция не имеет коллизий, обладает переборной сложностью обращения и в этом смысле не может быть улучшена.

Протоколы многократной аутентификации в условиях недоверия к верификатору могут базироваться на задачах вычисления индекса и категорного морфизма.

Предлагается следующий обобщенный протокол многократного диалогового опознавания на основе шифрования с открытым ключом и задачи вычисления индекса элемента произвольной абелевой группы. Параметрами протокола являются: группа  $G$ , элемент  $a \in G$ , функция  $f: \{m\} \times G \rightarrow G$ , обратимая по первому аргументу ( $\{m\}$  – множество открытых текстов), абелева группа вычислимых в одну сторону автоморфизмов  $\varphi_i$  группы  $G$ . Открытым ключом является элемент  $b \in G$ , секретным ключом – автоморфизм  $\varphi_x$  такой, что  $b = \varphi_x(a)$ . Верификатор вырабатывает (случайный) запрос  $m$  и зашифровывает его на ключе  $b$ : генерирует случайный автоморфизм  $\varphi_y$ , вычисляет значения  $\varphi_y(a)$ ,  $\varphi_y(b)$ ,  $c = f(m, \varphi_y(b))$  и от-

правляет шифрограмму  $(\varphi_y(a), c)$  претенденту. Претендент проверяет условие  $\varphi_y(a) \in G$  (невыполнение этого условия означает, что проводится атака на ключ претендента; в этом случае протокол останавливается), вычисляет  $\varphi_x(\varphi_y(a))$ , получая  $\varphi_x\varphi_y(a) = \varphi_y(b)$ , находит сообщение  $m' = f^{-1}(c, \varphi_y(b))$  и отправляет его верификатору. Верификатор проверяет, что  $m = m'$ . При выполнении равенства опознавание считается успешным.

Для многократного диалогового опознавания на основе ЗВИК (криптографическим примитивом для этой задачи является секретный гомоморфизм) предложен следующий протокол. Открытый ключ содержит пару изогенных кривых  $E_1, E_2$  и точки  $Q_1 \in E_1, Q_2 \in E_2$ , причем  $Q_2 = \psi(Q_1)$  для изогении  $\psi$ . Верификатор генерирует случайный логарифм  $z$ , вычисляет точку  $P_1 = zQ_1$  и посылает претенденту. Претендент проверяет, что  $P_1 \in E_1$  и что  $P_1$  имеет заданный порядок, вычисляет  $P_2 = \psi(P_1)$  и отправляет  $P_2$  верификатору. Верификатор проверяет, что  $P_2 = zQ_2$ . При выполнении равенства опознавание считается успешным. Показано, что для нарушения безопасности этого протокола нужно вычислить изогению в течение времени жизни ключа или вычислить логарифм на эллиптической кривой в реальном масштабе времени. Поскольку эффективная тактовая частота квантовых компьютеров мала, вычислить логарифм в реальном масштабе времени невозможно.

Для обобщенных протоколов диалогового опознавания на основе примитивов шифрования с открытым ключом, цифровой подписи, доказательств с нулевым разглашением знаний и секретных гомоморфизмов составлены уточненные перечни задач, положенных в основу безопасности. Сложность и номенклатура этих задач индуцируют отношение порядка на обобщенных протоколах диалогового опознавания. Показано, что шифрование с открытым ключом является наилучшим применительно к обычной вычислительной модели, а секретный гомоморфизм – применительно к квантовому компьютеру.

Предложены протоколы диалоговой и бездиалоговой аутентификации сообщения. Параметры протокола многократной бездиалоговой аутентификации сообщения на основе цифровой подписи и задачи вычисления индекса элемента произвольной абелевой группы те же, что и в протоколе на основе шифрования с открытым ключом. Кроме того, здесь используется вычисляемая в одну сторону хэш-функция  $h: \{m\} \times G \rightarrow \text{End}(G)$  и отображение  $g_{\text{End}}: \text{End}(G) \oplus \text{End}(G) \rightarrow \text{End}(G)$  прямой суммы кольца эндоморфизмов группы  $G$  в себя, обратимое по первому аргументу и индуцирующее отображение  $g: G \oplus G \rightarrow G$ . Претендент подписывает сообщение  $m$ , для чего генерирует случайный автоморфизм  $\varphi_y$ , вычисляет значение  $\varphi_y(a)$ , хэш-функцию  $\varphi_e = h(m, \varphi_y(a))$  и элемент  $\varphi_s = g_{\text{End}}(\varphi_y, \varphi_e\varphi_x) \in \text{End}(G)$ , проверяет, что  $\varphi_s\varphi_e \neq 0$ , и отправляет подписанное сообщение  $(m, \varphi_e, \varphi_s)$  верификатору. Верификатор проверяет, что  $\varphi_e \neq h(m, 0)$  и  $\varphi_s\varphi_e$  – обратимый элемент кольца  $\text{End}(G)$  (если хотя бы одно из условий не выполняется, то подпись неверна), вычисляет значение  $c = g^{-1}(\varphi_s(a), \varphi_e(b))$  и хэш-функцию  $\varphi_e' = h(m, c)$ . Если  $\varphi_e' = \varphi_e$ , то аутентификация считается успешной.

Этот протокол, как и протокол на основе шифрования с открытым ключом, обеспечивает экспоненциальную стойкость. Вскрытие ключа в обоих протоколах сводится к вычислению автоморфизма  $\varphi_x$  по значению  $\varphi_x(a)$ . В протоколе на основе подписи предъявляются более жесткие требования к генератору случайных чисел.

Предложен протокол диалоговой аутентификации сообщения на основе ЗВИК. Параметры и ключи аутентификации те же, что и в соответствующем протоколе опознавания. Кроме того, претендент и верификатор умеют вычислять бесключевую хэш-функцию  $h$ . Для аутентификации сообщения  $m$  верификатор генерирует случайное число  $z$ , вычисляет точку  $P_1 = zQ_1 \in E_1$  и направляет претенденту. Претендент вычисляет точки  $R_1 = h(m)P_1, R_2 = \psi(R_1) \in E_2$  и направляет пару  $(m, R_2)$  верификатору. Верификатор проверяет условие  $R_2 = h(m)zQ_2$ . При выполнении равенства аутентификация считается успешной. Безопасность этого протокола аналогична безопасности соответствующего протокола опознавания.

В работе предложены варианты централизованного и децентрализованного управления ключами аутентификации. Смена персональных ключей производится по окончании времени их жизни, а в случае однократной аутентификации – после ее выполнения. Показано, что криптографическая составляющая времени жизни ключа аутентификации определяется исходной сложностью и скоростью падения сложности ОМЗ, исходной производительностью вычислительной модели нарушителя и скоростью ее роста, а также сроком эксплуатации

подсистемы аутентификации. Приведено уравнение, позволяющее оценить время жизни ключа, параметров алгоритмического генератора случайных чисел и хэш-функции.

При смене персональных ключей параметры подсистемы аутентификации могут меняться или сохраняться в зависимости от ОМЗ. Стойкость замененного ключа определяется следующими утверждениями.

**Теорема 7.** Если алгоритм аутентификации основан на ЗДЛ в  $\mathbb{F}_p^*$  и длительность вычисления логарифма составляет  $S$  машинных тактов, то смена персональных открытых и секретных ключей после окончания их времени жизни при сохранении характеристики поля  $p$  позволяет продлить срок безопасной эксплуатации на  $O(\sqrt{S})$  машинных тактов.

**Следствие 8.** В подсистеме аутентификации, обладающей субэкспоненциальной стойкостью, время жизни персонального ключа аутентификации следует отсчитывать с момента выбора параметров подсистемы аутентификации.

Показано, что для ЗДЛ в циклической группе простого порядка  $r$  при ограничении  $V < O(\sqrt{r/\log r})$  на объем памяти  $V$  вычислительной модели асимптотическая оценка сложности не меняется. Поэтому периодической сменой персональных ключей при сохранении параметров подсистемы аутентификации можно обеспечить сколь угодно длительный срок безопасной эксплуатации алгоритмов аутентификации.

**Глава 5. Алгоритмизация выбора параметров и разработка быстрых вычислительных алгоритмов на эллиптических кривых.** Если в подсистеме аутентификации в качестве математической структуры используется группа точек эллиптической кривой над простым полем, то параметрами подсистемы являются конечное поле, уравнение кривой и порядок группы, для определения которого достаточно найти число точек кривой.

Для ускорения генерации параметров предлагается использовать эллиптические кривые  $E(\mathbb{F}_p)$  с комплексным умножением над  $\mathbb{C}$ . Приведена таблица с 13 типами таких кривых, которые в случае редукции по модулю  $p$  обладают эффективно вычислимым числом точек. Предложен алгоритм генерации эллиптической кривой, удовлетворяющей требованиям гл. 3, со сложностью  $O(\log^5 p)$ .

Показано, что число неизоморфных эллиптических кривых  $E(\mathbb{F}_p)$  с фиксированным простым числом точек  $r$ , где  $|r - p| < 2\sqrt{p}$ , асимптотически равно  $O(\sqrt{p})$ ; число неизоморфных эллиптических кривых  $E(\mathbb{F}_p)$  с произвольным простым числом точек равно  $O(p/\ln p)$ . Поэтому требование по мощности множества параметров подсистемы аутентификации, указанное в гл. 2, выполняется автоматически.

Установлено, что орбиты относительно группы автоморфизмов эффективно разрешимы только для кривых с  $j = 0$  и  $j = 12^3$ . Все другие кривые являются стойкими по отношению к методу логарифмирования на орбитах автоморфизмов и могут быть использованы для целей аутентификации в критических информационно-телекоммуникационных системах.

Предложен алгоритм генерации параметров подсистемы аутентификации на основе ЗВИК. Для генерации пары кривых, между которыми существует цепочка изогений степени  $l_1$  и  $l_2$ , выбирается поле  $\mathbb{F}_p$  и кривая согласно таблице. Число точек кривой должно иметь вид  $(l_1 l_2)^2 r$ , где  $r$  – большое простое число. Для этой кривой вычисляется случайная цепочка изогений. На каждом шаге решаются два модулярных уравнения  $\Phi_{l_1}(u, j) = 0$ ,  $\Phi_{l_2}(u, j) = 0$ . В качестве очередного  $j$ -инварианта выбирается случайным образом корень любого из уравнений, и вычисляются параметры изогении. После  $O(\log p)$  шагов процесс останавливается. Приведены явные формулы для изогений, позволяющие генерировать параметры подсистемы аутентификации, при  $l_1 = 2$ ,  $l_2 = 3$ .

Для построения быстрых вычислительных алгоритмов на эллиптических кривых можно использовать комплексное умножение. Показано, что комплексное умножение для эллиптических кривых с  $j = 20^3$ ,  $j = -15^3$  и уравнением  $y^2 = x^3 + c_2 t x^2 + c_1 t^2 x \pmod{p}$  задается через изогению степени 2 выражением  $\psi(x, y) = (\alpha x + A + \beta/y, \gamma y(1 + \delta/x^2))$ ; соответствующие па-

параметры приведены в следующей таблице (знак коэффициента  $\gamma$  взаимно однозначно определяется знаком числа  $\theta$ ).

**Параметры комплексного умножения для изогении степени 2**

	$c_1$	$\alpha$	$A$	$\beta$	$\gamma^2$	$\delta$	$\theta$
Вариант 1	$\frac{1}{8}c_2^2$	$-\frac{1}{2}$	$-\frac{1}{2}c_2$	$-\frac{1}{16}c_2^2$	$-\frac{1}{8}$	$-\frac{1}{8}c_2^2$	$\sqrt{-2}$
Вариант 2	$\frac{9+5\sqrt{-7}}{72}c_2^2$	$\frac{-3+\sqrt{-7}}{8}$	$\frac{-11+\sqrt{-7}}{24}c_2$	$\frac{-31-3\sqrt{-7}}{288}c_2^2$	$\frac{9+5\sqrt{-7}}{128}$	$\frac{-9-5\sqrt{-7}}{72}c_2^2$	$\frac{1+\sqrt{-7}}{2}$
Вариант 3	$\frac{9-5\sqrt{-7}}{72}c_2^2$	$\frac{-3-\sqrt{-7}}{8}$	$\frac{-11-\sqrt{-7}}{24}c_2$	$\frac{-31+3\sqrt{-7}}{288}c_2^2$	$\frac{9-5\sqrt{-7}}{128}$	$\frac{-9+5\sqrt{-7}}{72}c_2^2$	$\frac{-1+\sqrt{-7}}{2}$

Случай  $j = 20^3$  соответствует комплексному умножению на  $\sqrt{-2}$ . При этом проективная кривая может быть задана уравнением  $Y^2Z = X^3 - 4tX^2Z + 2t^2XZ^2$ . Комплексное умножение имеет вид  $\psi(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$ , где  $X_2 = -Y_1^2Z_1$ ,  $Y_2 = Y_1(\sqrt{-2})^{-1}(X_1^2 - 2t^2Z_1^2)$ ,  $Z_2 = 2X_1^2Z_1$ . Эта операция почти в 2 раза быстрее, чем удвоение.

В случае  $j = -15^3$  определено комплексное умножение на  $(\pm 1 + \sqrt{-7})/2$ , которое при  $c_2 = -3/(1 + 2\alpha)$  имеет вид  $X_2 = Z_1(\alpha Y_1^2 + X_1^2)$ ,  $Y_2 = \gamma Y_1(X_1^2 + \delta Z_1^2)$ ,  $Z_2 = X_1^2Z_1$ , что в 1,7 раза быстрее, чем удвоение.

Предложены два алгоритма умножения точки на число  $k$  для кривых, обладающих комплексным умножением на число  $\theta$ . Первый алгоритм универсален, повышает скорость на 30% и основан на представлении показателя  $k$  в виде:  $k = k_0 + \theta k_1$ , где  $|k_0|, |k_1| < \sqrt{r}$ .

**Теорема 9.** Существует разложение  $r = \pi\bar{\pi}$  в кольце  $\mathbf{Z}[\theta]$ . Отображение  $\mathbf{Z}/(r) \rightarrow \mathbf{Z}[\theta]/(\pi)$ ,  $k \pmod{r} \rightarrow (k + 0\cdot\theta) \pmod{\pi}$  является изоморфизмом полей.

Второй алгоритм, использующий комплексное умножение вместо удвоения, применим при  $\theta = \sqrt{-2}$  и  $\theta = (1 + \sqrt{-7})/2$ , позволяет ускорить вычисления соответственно 72% и 59% и основан на следующих утверждениях.

**Теорема 10.** Для эллиптической кривой с комплексным умножением на  $\theta = \sqrt{-2}$  показатель  $k \in \mathbf{F}_r$  можно представить в виде многочлена от  $\theta$  степени не более  $\log_2 r$  с коэффициентами 0, 1 и  $-1$ .

**Теорема 11.** Для эллиптической кривой с комплексным умножением на  $\theta = (1 + \sqrt{-7})/2$  показатель  $k \in \mathbf{F}_r$  можно представить в виде многочлена от  $\theta^\varepsilon(1 - \theta)$ , где  $\varepsilon \in \{0, 1\}$ , степени не более  $\log_2 r$  с коэффициентами 0, 1 и  $-1$ .

Второй алгоритм является наиболее быстрым для эллиптических кривых над простыми полями, а также обеспечивает защиту от атаки типа «timing attack».

В работе приведены параметризованные для случая эллиптических кривых примитивы шифрования с открытым ключом и цифровой подписи, позволяющие реализовать различные протоколы аутентификации.

**Основные публикации.** Содержание диссертационной работы отражено в 45 печатных трудах.