НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2025 Том 25 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2025 Vol. 25 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2025-25-3-446-456
УДК 004.056.55

Анализ применимости существующих схем разделения секрета в условиях постквантовой эры

Елизар Филаретович Кустов[1]✉, Сергей Валентинович Беззатеев[2]

[1,2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[2] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

[1] elizarkustov@mail.ru✉, https://orcid.org/0000-0002-0191-1178
[2] sergey.bezzateev@gmail.com, https://orcid.org/0000-0002-0924-6221

Аннотация
Рассмотрены современные подходы к разделению секрета, включая как классические, так и постквантовые криптографические схемы. Исследованы методы распределения секретной информации между несколькими участниками с использованием математических примитивов, таких как многочлены Лагранжа и Ньютона, китайская теорема об остатках, коды исправляющие ошибки, теория решеток, изогении эллиптических кривых, многомерные уравнения и хэш-функции. Приведен сравнительный анализ различных схем с точки зрения их устойчивости к квантовым атакам, эффективности и соответствия критериям Шамира. Особое внимание уделено оценке устойчивости схем к атакам с использованием квантовых компьютеров, что особенно актуально в условиях развития квантовых технологий. Рассмотрены преимущества и недостатки каждой из схем, включая их вычислительную сложность, гибкость и возможность адаптации к различным условиям. Показано, что классические схемы, такие как схемы Шамира и Ньютона, остаются эффективными и простыми в реализации, но уязвимы к квантовым атакам. В то же время постквантовые схемы, основанные на теории решеток, демонстрируют высокий уровень безопасности, но требуют более сложных вычислений.

Ключевые слова
постквантовая криптография, схема распределение секрета, пороговая схема, криптография с открытым ключом, теория решеток, эллиптические кривые, многомерные уравнения, коды исправляющее ошибки, хэш-функции

Благодарности
Работа выполнена в рамках государственного задания (проект № FSER-2025-0003).

Ссылка для цитирования: Кустов Е.Ф., Беззатеев С.В. Анализ применимости существующих схем разделения секрета в условиях постквантовой эры // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 3. С. 446–456. doi: 10.17586/2226-1494-2025-25-3-446-456

Analysis of the applicability of existing secret separation schemes in the post-quaternary era

Elizar F. Kustov[1]✉, Sergey V. Bezzateev[2]

[1,2] ITMO University, Saint Petersburg, 197101, Russian Federation
[2] Saint-Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation

[1] elizarkustov@mail.ru✉, https://orcid.org/0000-0002-0191-1178
[2] sergey.bezzateev@gmail.com, https://orcid.org/0000-0002-0924-6221

Abstract
Modern approaches to secret sharing have been examined, encompassing both classical and post-quantum cryptographic schemes. The study explores methods for distributing secret information among multiple participants using various mathematical primitives, such as Lagrange and Newton polynomials, the Chinese remainder theorem, error-correcting

codes, lattice theory, elliptic curve isogenies, multivariate equations, and hash functions. A comparative analysis of different schemes is provided in terms of their resistance to quantum attacks, efficiency, and compliance with Shamir's criteria. Special attention is given to assessing the schemes resilience against attacks using quantum computers, which is particularly relevant given the advancement of quantum technologies. The advantages and disadvantages of each scheme are discussed, including their computational complexity, flexibility, and adaptability to various conditions. It is shown that classical schemes, such as those by Shamir and Newton, remain efficient and easy to implement but are vulnerable to quantum attacks. Meanwhile, post-quantum schemes based on lattice theory demonstrate a high level of security but require more complex computations.

Keywords
post-quantum cryptography, secret sharing scheme, threshold scheme, public-key cryptography, lattice theory, elliptic curves, multivariate equations, error-correcting codes, hash functions

Acknowledgments
The work was carried out within the framework of the State Assignment (project No. FSER-2025-0003).

For citation: Kustov E.F., Bezzateev S.V. Analysis of the applicability of existing secret separation schemes in the post-quaternary era. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 3, pp. 446–456 (in Russian). doi: 10.17586/2226-1494-2025-25-3-446-456

Введение

Первый метод разделения секрета был предложен еще в 1979 году Шамиром [1] и Блейкли [2] независимо друг от друга. Схемы разделения секрета применяются в случаях, когда существует значимая вероятность компрометации хранителей секрета, но вероятность недобросовестного сговора значительной части участников считается пренебрежимо малой.

Появление алгоритма Шора для квантового компьютера, поставило под угрозу классические криптосистемы, основанные на проблемах факторизации числа и дискретного логарифма. Возник вопрос о создании новых систем, устойчивых к атаке с использованием квантового компьютера.

Исследование в этой области дало толчок к развитию криптографии на новых постквантовых криптопримитивах, таких как коды исправляющие ошибки, теория решеток, изогении эллиптических кривых, многомерные уравнения и хэш-функции. Активное развитие этой области создало множество новых систем, в частности схемы разделения секрета. В связи с этим возник вопрос о возможной замене классических схем Шамира, Ньютона и Блейкли, которые сами по себе не обеспечивают безопасность от квантовых атак, на новые постквантовые схемы.

В настоящей работе выполнен анализ и сравнение между собой новых постквантовых и классических схем разделения секрета для поиска оптимальных схем. Сравнение происходит по критериям Шамира: размер доли меньше или равен самому секрету, возможность повторного использования секрета, невозможность проанализировать секрет, возможность добавления нового участника, возможность обновить секрет, возможность изменения веса долей.

В результате проведенного анализа различных схем представлена схема разделения секрета, отвечающая наибольшему числу критериев.

Схема разделения секрета по интерполяционному многочлену Лагранжа

Схема разделения секрета по интерполяционному многочлену Лагранжа, также известная как схема Шамира [1], является одной из самых популярных пороговых схем разделения секрета. Она основана на интерполяции многочленов [3] и позволяет разделить секрет между n участниками так, что для его восстановления требуется как минимум k долей ($k \le n$).

В этой схеме секретная информация, представленная целым числом S, распределяется между n участниками и может быть восстановлена при наличии как минимум k долей. Доверенный центр, называемый дилером, выбирает простое число $p > S$ и генерирует многочлен $q(x)$ степени $k-1$ над $GF(p)$:

$$q(x) = S + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1},$$

где $a_1, \ldots, a_{k-1}$ выбираются дилером случайным образом из равномерно распределенных элементов $GF(p)$. Участник P_i ($i = 1, \ldots, n$) получает только целое число $D_i = q(i)$ в качестве доли, где i — уникальный идентификатор участника P_i; $q(i)$ — значение многочлена в точке i. При наличии k долей можно восстановить $q(x)$ с использованием интерполяции Лагранжа и, следовательно, восстановить секрет $S = q(0)$.

В схеме по интерполяционному многочлену Лагранжа, при наличии $k-1$ долей для любого секрета S', невозможно восстановить соответствующий ему многочлен. Таким образом, $k-1$ долей не дают никакой информации о секрете.

Злоумышленник не сможет восстановить секрет S при условии, что он не имеет доступа к k или более долям, так как многочлен степени $k-1$ однозначно определяется k точками. Схема устойчива к атакам, основанным на переборе, благодаря использованию конечного поля $GF(p)$ при выборе большого значения p. Также благодаря использованию интерполяционного многочлена Лагранжа можно добавить нового участника.

В табл. 1 представлены значения размеров ключей и долей секрета для 128-битной и 256-битной безопасности для схемы Шамира. В качестве ключей были использованы RSA (Rivest, Shamir, Adleman) из рекомендации NIST [4]. 128-битная и 256-битная безопасность — уровни криптографической стойкости, которые показывают, насколько сложно взломать систему перебором или другими атаками и означают, что для

Таблица 1. Сравнение размера ключевых элементов схемы Шамира, бит

Table 1. Comparison of the key elements size of the Shamir scheme, bit

Параметр	128-битная безопасность	256-битная безопасность
Секрет S	3072	15 360
Доля D_i	3072	15 360
Коэффициенты	$3072 \times (k-1)$	$15\,360 \times (k-1)$

взлома потребуется в среднем 2^{128} и 2^{256} операций соответственно.

Как видно из табл. 1 размер секрета и его долей равны, что позволяет использовать доли секрета в качестве секрета в криптосхемах без дополнительных модификаций. Отметим, что наиболее затратным для хранения данных, является размер коэффициентов многочлена.

Подчеркнем, что рассматриваемая схема не обеспечивает безопасность самого секрета S и его долей D_i, для этого сегодня используются вариации схемы Шамира с криптосистемами RSA [5], ECDCA [6] и Эль-Гамаль [7]. В этом варианте реализации общая криптосистема становится уязвима к атаке с применением квантового компьютера, в отличии от криптосистем, основанных на постквантовых криптопримитивах. Также к недостаткам схемы можно отнести ненадежность дилера, так как предполагается, что все участники могут доверять выбранному центру, что не всегда верно.

Схема разделения секрета по интерполяционному многочлену Ньютона

Схема разделения секрета на основе интерполяционного многочлена Ньютона — метод разделения секрета, который использует интерполяцию многочлена Ньютона для восстановления секрета. Этот подход похож на схему Шамира, но вместо интерполяции Лагранжа применяется интерполяция Ньютона. Многочлен Ньютона степени $t-1$ имеет вид:

$$f(x) = a_0 + a_1(x - x_1) + a_2(x - x_1)(x - x_2) + \ldots$$
$$\ldots + a_{t-1}(x - x_1)(x - x_2) \ldots (x - x_{t-1}),$$

где $a_0, a_1, \ldots, a_{t-1}$ — коэффициенты; $x_1, x_2, \ldots, x_{t-1}$ — заранее выбранные точки.

В начале дилер выбирает $x_1, x_2, \ldots, x_n$, где n — количество участников. Для каждого участника P_i вычисляется значение многочлена в точке x_i, т. е. $f(x_i)$. Это значение является долей участника.

Для восстановления секрета необходимо собрать как минимум t долей. Используя интерполяцию Ньютона, строится многочлен $f(x)$ по t точкам $(x_i, f(x_i))$. Секрет S восстанавливается как значение многочлена в точке $x = 0$, т. е. $S = f(0)$.

Схема разделения секрета на основе многочлена Ньютона обладает теми же свойствами, что и схема разделения секрета по Лагранжу. Это значит, что она также уязвима к атаке с использованием квантового компьютера, если не добавить в схему постквантовые криптопримитивы. Размеры ключей схемы подобны значениям, что и в схеме разделения секрета по Лагранжу, представленные в табл. 1.

Схема разделения секрета на основе китайской теоремы об остатках

Схема распределения секрета на основе китайской теоремы об остатках [8] — метод разделения секрета, который использует свойства модульной арифметики, и китайскую теорему об остатках для распределения и восстановления секрета. Этот подход позволяет разделить секрет между несколькими участниками так, чтобы только определенное подмножество участников могло его восстановить.

Как и в схеме Шамира, в работе [8] присутствует доверенный дилер, который определяет общий секрет S и попарно взаимно простые числа $m_1, \ldots, m_n$, такие что:

$$m_{n-k+2} \times m_{n-k+3} \times \ldots m_n < S < m_1 \times m_2 \times \ldots m_k,$$
$$m_1 < m_2 < \ldots < m_n,$$

где k — пороговое значение.

Каждому участнику выдается значение $S_i = S \bmod m_i$. Для восстановления секрета требуется собрать хотя бы k значений S_i и решить систему сравнений с помощью китайской теоремы об остатках.

Размеры ключей схемы подобны значениям, что и в схеме разделения секрета по Лагранжу, представленные в табл. 1. Отметим, что наиболее затратным является хранение модулей $m_i > 2^{256}$ бит для 128-битной и 256-битной безопасности.

К преимуществам данной схемы можно отнести ее эффективность по сравнению со схемой на основе интерполяционной формулы Лагранжа, так как восстановление секрета требуется только решение системы линейных сравнений, что вычислительно проще, чем интерполяция многочлена в схеме Шамира. Также, выбирая новые модули, можно добавить новых участников.

Важно, что, как и в схеме Шамира, схема на основе китайской теоремы об остатках не обеспечивает безопасность секрета и его долей, что приводит к ее уязвимости к квантовым атакам при использовании классических криптопримитивов.

Схемы разделения секрета, основанные на кодах, исправляющих ошибки

В [9] доказано, что схема Шамира является частным случаем обмена секретами с использованием кодов Рида–Соломона. Позже Мэсси [10] обнаружил взаимосвязь между структурой доступа для совместного использования секретов и кодовыми словами двойственного кода. Построение схем совместного использования секретов с применением кодовых конструкций остается важной темой и в настоящее время. Некоторые исследователи продолжают разрабатывать новые схемы обмена секретами [11–13].

В работе [9] было замечено, что схема разделения секрета Шамира является частным слу-

чаем более общей схемы, основанной на кодах Рида–Соломона. В этой схеме принято, что $(\alpha_1, \ldots, \alpha_{r-1})$ — фиксированный список ненулевых элементов некоторого поля $\mathbf{F}$ ($|\mathbf{F}| = r$, $r > n$), информационное слово $a = (S, a_1, \ldots, a_{k-1}) \in \mathbf{F}_k$ кодируется в кодовое слово $D = (D_0, \ldots, D_{r-2})$ с использованием кода Рида–Соломона:

$$D_i = \sum_{j=0}^{k-1} a_j \alpha_i^j, \; a_0 = S,$$

где D_i — доля участника P_i. При наличии всех r долей, чтобы восстановить секрет необходимо вычислить:

$$S = -\sum_{i=0}^{r-1} D_i.$$

При наличии s долей ($r \geq s \geq k$), из которых t содержат ошибки $\left(t \leq \dfrac{s-k}{2}\right)$, можно восстановить кодовое слово D с использованием алгоритма исправления ошибок и, следовательно, информационное слово a и секрет S.

В табл. 2 представлены значения размеров ключей и долей секрета для 128-битной и 256-битной безопасности. В качестве секрета был использован секретный ключ RSA.

Как видно из табл. 2 для хранения всех значений требуется достаточно большой объем памяти.

Данная схема обладает всеми свойствами схемы Шамира, а также новым свойством устойчивости к искажениям или деградации хранилища.

В работе [10] Мэсси показал, что минимальные кодовые слова в дуальном коде полностью определяют структуру схемы разделения секрета, и наоборот. Мэсси также определил, что структура схемы разделения секрета, соответствующая линейному (n, k) коду $\mathbf{V}$, задается теми минимальными кодовыми словами в дуальном коде, у которых первый компонент равен 1.

В [14] Мэсси расширил ранее полученные результаты, показав, что каждое кодовое слово q-ичного линейного кода может быть записано как линейная комбинация минимальных кодовых слов, которые его покрывают.

Таблица 2. Сравнение размера ключевых элементов схемы, основанной на кодах с исправлением ошибок, бит

Table 2. Comparison of the key elements size of a scheme based on error-correcting codes, bit

Параметр	128-битная безопасность	256-битная безопасность
Кодовое слово D	786 432	7 864 320
Информационное слово a	685 056	6 881 280
Проверочная матрица $\mathbf{H}$	25 067 520	503 316 480

Примечание. Все параметры зависят от размерности кода Рида–Соломона (n, k).

Схемы разделения секрета, основанные на теории решеток

Первая схема разделения секрета на основе решеток была предложена в [15], где использовалась задача нахождения ближайшего вектора (Closest Vector Problem, CVP). Современные схемы чаще опираются на задачи нахождения кратчайшего вектора (Shortest Vector Problem, SVP) [16] и обучения с ошибками (Learning With Error, LWE) [17], которые являются NP-трудными, что делает их пригодными для криптографических приложений.

В [18] была предложена пороговая схема разделения секрета, основанная на SVP. В этой схеме для восстановления секрета требуется не менее n_1 участников, где $n_1 = n_2$ (количество участников, получающих доли). Основная идея заключается в восстановлении базисной матрицы, которая необходима для вычисления секретного вектора.

Безопасность схемы основана на использовании криптографических хэш-функций. В работе [19] предложено использовать хэш-функции Айтаи [20], Любашевского и Миккианчио [21] а также Пейкерта и Розена [22], что делает схему устойчивой к атакам с применением квантового компьютера. Основным недостатком схемы является условие, что для восстановления секрета необходимо участие всех участников P_i со своими долями.

В [23] была предложена пороговая схема (n, n), основанная на LWE. Обозначим участников как P_i, $1 \leq i \leq n-1$, а секретный вектор как $\mathbf{s} \in \mathbf{Z}_q^m$. Дилер выбирает модуль q, простое число p, генератор g группы $GF(p)$ и распределение ошибок $\chi \in \mathbf{Z}^q$. Для каждого участника дилер выбирает случайный вектор $\mathbf{a}_i \in \mathbf{Z}_q^m$ и ошибку $e_i \in \mathbf{Z}_q$. Доля секрета $D_i = (\mathbf{a}_i, b_i)$, где b_i вычисляется как:

$$b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i, \; 1 \leq i \leq n-1,$$

где $\langle \mathbf{a}_i, \mathbf{s} \rangle$ — скалярное произведение. Дилер публикует $V_i = g^{S_i} = (g^{a_i}, g^{b_i})$. Для последнего участника P_i дилер вычисляет $e_n = -e_1 - e_2 - \cdots - e_{n-1}$ и соответственно

$$b_n = \langle \mathbf{a}_n, \mathbf{s} \rangle + e_n.$$

В фазе восстановления участники предоставляют агрегатору свои доли D_i. Если все доли валидные, для восстановления секрета $\mathbf{s}$ необходимо просуммировать доли:

$$D_1 + \cdots + D_n = \left(\sum_{i=1}^{n} \mathbf{a}_i \sum_{i=1}^{n} \langle \mathbf{a}_i, \mathbf{s} \rangle \right).$$

В работе [24] выполнена модификация фазы восстановления с помощью добавления порога t, тем самым превратив схему из (n, n) в (t, n). Используя $t \leq n$ долей, решена система линейных уравнений для нахождения секрета $\mathbf{s}$. Поскольку полученная система уравнений является недоопределенной, было предложено использовать метод наименьших квадратов (МНК) [25] для нахождения приближенного решения. Однако применение МНК не всегда возможно или эффективно, что накладывает на схему дополнительные ограничения.

Таблица 3. Сравнение размера ключевых элементов схемы на решетках, бит

Table 3. Comparison of the key elements size of a lattice-based scheme, bit

Параметр	128-битная безопасность	256-битная безопасность
Секрет **s**	20 224	38 912
Ошибка e_i	45	64
Доля D_i	20 224	38 912

В табл. 3 представлены значения размеров ключей и долей секрета для 128-битной и 256-битной безопасности. Данные взяты на основе рекомендации NIST.

Как видно из табл. 3 для хранения секрета и его долей, необходимо значительно больше ресурсов, чем в классических схемах. Это может ограничивать применение схемы в системах с ограниченными ресурсами.

Схемы разделения секрета, основанные на изогениях эллиптических кривых

Эллиптические кривые, традиционно использующиеся в классических подходах, основаны на задаче дискретного логарифма для эллиптических кривых, демонстрируют уязвимость к квантовым атакам с применением алгоритма Шора [26]. Это послужило стимулом для развития нового направления — криптографии на изогениях, где вместо работы с точками на кривых используются сами эллиптические кривые и морфизмы между ними (изогении) [27].

Криптография на изогениях базируется на вычислительной сложности задачи нахождения изогении между заданными изогенными кривыми над конечным полем $GF(p)$ [28, 29]. Этот подход породил множество научных работ в этой области [30, 31].

Одной из прорывных работ является разработка протоколов обмена ключами SIDH [32] и CSIDH [33]. Последний протокол предлагает более компактные размеры ключей за счет использования суперсингулярных кривых. Особого внимания заслуживает схема цифровых подписей CSI-FiSh [34], демонстрирующая практическую применимость подхода.

В контексте пороговых схем важными разработками стали модификации схем Кувеньес–Ростовцев–Столбунова [35], основанные на классической схеме Шамира и использующие концепцию Hard Homogeneous Spaces [36, 37]. Безопасность этих схем опирается на сложность решения Group Action Inverse Problem [38, 39].

Рассмотрим пороговую схему группового действия, предложенную в [36]. Пусть P_i — участник пороговой схемы и владеет частью секрета $s_i = f(i)$, где сам секрет — сумма всех долей:

$$S = \sum_{i \in S} s_i,\ S \in \mathbf{Z}_q.$$

Основная идея заключается в вычислении группового действия $[s]E_0$ без раскрытия своих долей. Пусть $S \subset \{1, \ldots, n\}$ — множество мощности не менее k. Тогда секрет может быть вычислен как:

$$S = \sum_{i \in S} s_i \times L_{0,i}^S,$$

где $L_{0,i}^S$ — коэффициенты Лагранжа P_i.

Пусть в схеме участвуют k участников. Сначала E_0 отправляется участнику P_1, который вычисляет:

$$E_1 = [s_1 \times L_{0,1}^S]E_0,$$
$$[a]E = g^a \times E,$$

где g — элемент порядка q группы $GF(q)$.

Результат E_1 отправляется следующему участнику $P_j, j \le k$, который вычисляет:

$$E_j = [s_j \times L_{0,j}^S]E_{j-1} = [\sum_{i \in S} s_i \times L_{0,i}^S]E_0 = [s]E_0.$$

Таким образом, общая структура коммуникации выглядит следующем образом:

$$\xrightarrow{E_0,\, s} P_1 \xrightarrow{E_1,\, s} P_2 \xrightarrow{E_2,\, s} \ldots \xrightarrow{E_{k-1},\, s} P_k \xrightarrow{[s]E_0}.$$

Особенность системы заключается в том, что только последний участник знает секрет, и он должен распределить его между другими участниками. В табл. 4 представлены размеры ключевых значений, основываясь на NIST Level 1 (минимальный уровень стойкости в постквантовых стандартах NIST [4]).

Из табл. 4 можно сделать вывод, что схемы на основе изогений обладают наименьшими размерами по сравнению с постквантовыми аналогами, представленными в данной работе. Основная проблема — выбор параметров для обеспечения безопасности системы. Используя параметры CSIDH, нельзя установить схему разделения секрета из-за недостатка квантовой безопасности. В итоге в [36] сделан вывод, что безопасность схемы соответствует уровню NIST Level 1, но сделать ее более безопасной проблематично [40]. Для обеспечения безопасности необходимо использовать суперсингулярные кривые с параметрами поля $p \ge 2^{254}$.

Схемы разделения секрета, основанные на хэш-функциях

Хэш-функции являются одним из основных элементов при проектировании схем разделения секрета. Их безопасность основывается на свойстве стойкости к прообразу, которое гарантирует, что вычислительно невозможно восстановить исходное сообщение по его хэш-значению [41]. Однако существенным недостатком схем, основанных на хэш-функциях, является то, что их безопасность напрямую зависит от стойкости используемой хэш-функции.

Table 4. Размер ключевых элементов схемы, бит

Table 4. Size of the key elements, bit

Параметр	128-битная безопасность
Секрет **s**	512
Кривая E_j	512
Доля s_i	512

Одна из первых схем распределения секрета, основанная на хэш-функциях, описана в работе [42], в которой была выдвинута идея использования хэш-функций для проектирования схем распределения секрета. Впоследствии данная схема получила развитие в работах [43–45]. В [43] хэш-функции использовались как дополнительный механизм для повышения безопасности и эффективности схем. Однако в [44, 45] хэш-функции стали основным вычислительным механизмом, что значительно улучшило производительность схем.

Среди последних работ стоит отметить схему Кета и Чжан [46]. При инициализации схемы случайным образом генерируются n долей $s_1, \ldots, s_n$ для n участников. Далее задаются авторизованные подмножества $A_i = \{p_{A_i,1}, \ldots, p_{A_i,t}\}$, которые определяют группы пользователей, которые могут восстановить секрет S.

Для каждого авторизованного подмножества A_i формируется приватное сообщение PM_i путем конкатенации долей участников подмножества:

$$PM_i = s_{A_i,1} \| s_{A_i,2} \| \ldots \| s_{A_i,t}.$$

Для каждого приватного сообщения PM_i вычисляется его хэш-значение:

$$h_i = H(PM_i),$$

где h_i имеет тот же размер, что и секрет s. Для каждого авторизованного подмножества генерируется контрольное значение:

$$c_i = h_i \oplus s,$$

где $\oplus$ — побитовое исключающее ИЛИ (XOR).

Чтобы восстановить общий секрет s для авторизованного подмножества A_i, участники объединяют свои доли:

$$PM_i = s_{A_i,1} \| s_{A_i,2} \| \ldots \| s_{A_i,t}.$$

Вычисляется хэш-значение восстановленного приватного сообщения

$$h_i = H(PM_i).$$

С использованием контрольного значения c_i секрет S восстанавливается следующим образом:

$$S = h_i \oplus c_i.$$

Размеры секрета и его долей могут быть любыми так как, они затем преобразуются в хэш-значения.

К преимуществам схемы можно отнести теоретико-информационную идеальность схемы, т. е. частичная информация о долях участников авторизованного подмножества не предоставляет никакой информации о секрете до тех пор, пока их количество не станет равным заданному порогу схемы.

Возможные атаки на схему совпадают с атаками на хэш-функцию. Использование современных хэш-функций таких как Keccak [47], делает схему устойчивой к атакам с применением квантового компьютера.

Однако вычисление хэш-значений для больших авторизованных подмножеств может быть вычислительно затратным. Схема имеет ограниченную гибкость, что делает ее сложной для адаптации в случае динамического изменения авторизованных подмножеств или количества участников.

Схемы разделения секрета на основе многомерных уравнений

Рассмотрим схемы разделения секрета, основанные на многомерных уравнениях. Такие схемы используют многочлены от нескольких переменных для разделения и восстановления секрета.

В работе [48] предложен вариант схемы Шамира, в котором вместо одномерного многочлена использован многомерный многочлен степени n:

$$f(x_1, x_2, \ldots, x_m) = \sum_{i=0}^{k-1} a_i x_1^{e_{i1}} x_2^{e_{i2}} \ldots x_m^{e_{im}},$$

где $a_i \in GF(p)$; $k = \binom{n+m}{m}$ — биномиальный коэффициент; $e_{i_m} \in \mathbf{N} \cup \{0\}$, причем $\sum_{j=1}^{m} e_{i_j} \le n$. Долями секрета являются наборы $x_i = (x_{i_1}, \ldots, x_{i_m}, f_i)$. Для секрета необходимо собрать k долей и использовать интерполяционную формулу Лагранжа.

В [49] предложена схема Карнина–Грина–Хеллмана, основанная на решении системы линейных уравнений. Секрет $S \in \mathbf{F}_q$ разделяется с использованием случайных векторов $\mathbf{u}, \mathbf{v}_0 \in \mathbf{F}_q^t$, таких что $\langle \mathbf{u}, \mathbf{v}_0 \rangle = S$. Для вычисления теней выбираются случайные векторы $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbf{F}^t$, такие что любые t из них линейно независимы. Тени вычисляются как $S = \langle \mathbf{u}, \mathbf{v}_i \rangle$, для $i \in \{1, \ldots, n\}$. Вектор $\mathbf{u}$ забывается, а $\mathbf{v}_1, \ldots, \mathbf{v}_n$ становятся публично доступными. Для восстановления секрета необходимо собрать t теней и решить систему линейных уравнений для нахождения $\mathbf{u}$.

В схеме [50], представляющей собой обобщенную схему Асмута–Блума [51], секретом является многочлен $s(\mathbf{x}) \in \mathbf{F}_q[\mathbf{x}]$ степени меньше d_0, где $\mathbf{x} = (x_1, \ldots, x_m)$. Для разделения секрета генерируется набор взаимно простых многочленов $m_i(\mathbf{x}) \in \mathbf{F}_q[\mathbf{x}]$, где $m_0(\mathbf{x}) = x^{d_0}$. Затем генерируется случайный многочлен $a(x)$, $\deg a(x) \le \sum_{i=1}^{t} d_i - d_0 - 1$ и вычисляется $f(x) = s(x) + a(x) \times m_0(x)$. Долями секрета будут являться $s_i(x) = f(x) \bmod m_i(x)$. В фазе комбинации секрета применена китайская теорема об остатках. В [52] предложено обобщение схемы на многомерные многочлены.

Схемы разделения секрета на основе многомерных уравнений обладают свойствами теоретико-информационной идеальности схемы, так как знание менее k долей не дает информации о секрете, где размеры секрета и долей одинаковы. Однако их применение требует учета ограничений, таких как необходимость раскрытия секрета для его использования и сложность добавления новых пользователей. Размеры ключей подобны значениям, что и в схеме разделения секрета по интерполяционным многочленам Лагранжа и представлены в табл. 1.

Сравнительный анализ схем разделения секрета

Для сравнения различных схем разделения секрета использованы критерии Шамира, которые включают: размер доли меньше или равен самому секрету, возможность повторного использования секрета, невозможность проанализировать секрет, возможность добавления нового участника, возможность обновить секрет, возможность изменения веса долей. Результаты представлены в табл. 5.

Как видно из табл. 5 классические схемы (Шамира, Ньютона, на основе китайской теоремы об остатках) остаются актуальными благодаря своей простоте и эффективности, однако они уязвимы к атакам с применением квантовых компьютеров. Схемы на основе теории решеток и кодах, исправляющих ошибки, являются наиболее перспективными для использования в постквантовой криптографии, так как они обеспечивают высокий уровень безопасности и соответствуют большинству критериев Шамира.

В табл. 6 представлены данные по сложности взлома представленных схем, с использованием квантового компьютера и классических способов. Под защитными мерами понимается условия, при которых, указанная атака не может быть реализована за полиномиальное время.

Одной из возможных атак на схему Шамира и схему на основе интерполяции Ньютона, является перебор многочленов, при которой злоумышленник пытается восстановить секретный многочлен $q(x)$ степени $k-1$, имея менее k долей. Для этого необходимо решить систему уравнений с $k-1$ неизвестными коэффициентами. Если p будет меньше указанного значения, то злоумышленник сможет перебрать все возможные варианты многочленов и тем самым восстановить секрет S.

Специфичной атакой на схему на китайской теореме об остатках является перебор модулей, при которой злоумышленник пытается восстановить секрет S, подбирая взаимно простые модули $m_1, \ldots, m_k$ при наличии $k-1$ долей. Если $m_i < 2^{256}$, то злоумышленник сможет восстановить все m_i, и тем самым решить систему уравнений и найти S.

Одной из самых распространенных атак на криптопримитивы на основе кодов, исправляющих ошибки, является атака по информационным совокупностям. Атака представляет собой семейство алгоритмов для решения задачи синдромного декодирования, заключающейся в нахождении вектора ошибок **e** веса t. При $n < 6960$ злоумышленник сможет построить таблицу синдромов и тем самым восстановить кодовое слово D.

В качестве специальной атаки на схему на решетках, была рассмотрена атака поиска секретного вектора в решетке (SVP, CVP). При $n < 1024$ у злоумышленника появляется возможность перебрать все возможные вектора решетки и тем самым найти кратчайший вектор.

В криптографии на изогениях для нахождения секрета злоумышленнику необходимо найти все возможные пути изогений между кривыми, где p — размер поля. При малом значении $p < 2^{254}$, злоумышленник сможет перебрать все пути в графе изогений кривых, а значит восстановить все кривые E_j и тем самым найти секрет s.

Специфичными атаками на многомерные уравнения являются линеаризация и атаки, использующие базис Грёбнера. Цель данных атак преобразовать нелинейную систему в линейную для решения стандартными мето-

Таблица 5. Сравнение схем разделения секрета по критериям Шамира

Table 5. Comparison of the secret separation schemes according to Shamir's criteria

Критерии Шамира	Схема Лагранжа	Схема разделения секрета по интерполяционному многочлену Ньютона	Схема на китайской теореме об остатках	Схемы на кодах, исправляющих ошибки	Схемы на решетках	Схемы на эллиптических кривых	Схемы на хэш-функциях	Схемы на многомерных уравнениях
Размер доли не больше секрета	+	+	–	+	+	+	+	+
Возможность повторного использования секрета	–	–	–	–	–	–	–	–
Невозможность проанализировать секрет	+	+	+	+	+	+	+	+
Возможность добавления нового участника	+	+	–	+	+	–	–	–
Возможность обновить секрет	+	+	–	+	+	–	+	–
Возможность изменения веса долей	–	–	–	–	–	–	–	–

Таблица 6. Сравнение схем разделения секрета по сложности взлома
Table 6. Comparison of the secret sharing schemes by hacking complexity

Схема	Квантовый метод	Классический метод	Возможные атаки	Защитные меры
Схема Шамира (RSA)	$O((\log_2 N)^3)$	$O(p^{k-1})$	Квантовый компьютер (алгоритм Шора), перебор многочленов	Замена классической криптографии на постквантовую, $p \geq 2^{256}$
Схема на основе интерполяции Ньютона (RSA)				
Схема на китайской теореме об остатках (RSA)	$O((\log_2 N)^3)$	$O(N)$	Квантовый компьютер (алгоритм Шора), перебор модулей	Замена классической криптографии на постквантовую, $m_i > 2^{256}$
Схемы на кодах, исправляющих ошибки (RSA)	$O((\log_2 N)^3)/O(2^{0,1n})$	$O(n^3)$	Квантовый компьютер (алгоритм Шора, атака на секрет, кодовое слово), атака по информационным совокупностям	Замена классической криптографии на постквантовую, $n \geq 6960$, использовать коды Гоппы
Схемы на решетках	$O(2^{0,1N})$	$O(2^N)$	Поиск секретного вектора в решетке	$n \geq 1024$
Схемы на эллиптических кривых	$O(p^{1/4})$	$O(p^{1/4})$	Перебор всех возможных путей изогений между кривыми	суперсингулярные эллиптические кривые над полем $GF(p)$, $p \geq 2^{254}$
Схемы на хэш-функциях	$O(2^N)$	$O(2^N)$	Коллизии, атаки на прообраз	Использование Keccak (SHA-3), $n \geq 256$
Схемы на многомерных уравнениях	$O(p^m)$	$O(k^x)$	Линеаризация, Грёбнеровы базисы	$x \geq 64$, $k \geq 5$

Примечание. N — параметр безопасности; n — размер кодового слова; p — размер поля; x — число переменных; k — степень многочленов.

дами. При $x < 64$, $k < 5$ полученная система уравнений будет слишком простой, что дает злоумышленнику возможность решить ее.

Из табл. 6 видно, что классические схемы разделения секрета уязвимы к квантовым атакам, так как сложность их взлома с использованием квантового компьютера оценивается как $O((\log_2 N)^3)$, что делает их непригодными для долгосрочного применения. В то же время постквантовые схемы, основанные на теории решеток, демонстрируют высокую устойчивость к квантовым атакам.

Схемы на изогениях эллиптических кривых также устойчивы к квантовым атакам, но требуют тщательного выбора параметров. Схемы на хэш-функциях зависят от криптостойкости самой функции, а схемы на многомерных уравнениях сложны в реализации и вычислениях.

Сложность квантовой атаки на схемы, основанные на постквантовых криптопримитивах является теоретической, так как в настоящий момент не существует эффективного квантового алгоритма их решения.

Заключение

В работе проведен анализ современных схем разделения секрета, как классических, так и постквантовых. Рассмотрены схемы, основанные на различных математических примитивах, включая многочлены Лагранжа и Ньютона, китайскую теорему об остатках, коды исправляющие ошибки, теорию решеток, изогении эллиптических кривых, многомерные уравнения и хэш-функции. Выполнен сравнительный анализ по критериям Шамира, который позволил выделить наиболее перспективные схемы для использования в условиях постквантовой эры.

Классические схемы сохраняют свою актуальность благодаря простоте реализации и высокой эффективности. Однако их уязвимость к атакам с использованием квантовых компьютеров делает их непригодными для долгосрочного применения в условиях постквантовой эры.

Постквантовые схемы, включая схемы на основе теории решеток, изогений эллиптических кривых, многомерных уравнений и хэш-функций, демонстрируют повышенную устойчивость к квантовым атакам. Несмотря на это, они требуют более сложных вычислений, что может ограничивать их применение в системах с ограниченными вычислительными ресурсами, таких как устройства интернета вещей.

Схемы, основанные на теории решеток, выделяются как наиболее перспективные направления в постквантовой криптографии. Они не только обеспечивают высокий уровень безопасности, но и соответствуют большинству критериев Шамира, что делает их пригодными для широкого использования в современных криптографических системах.

Для дальнейшего развития рекомендуется исследовать совместное использование классических схем и новых постквантовых криптопримитивов, особенно на основе теории решеток. Объединение двух подходов сможет сохранить преимущества классических схем и защиту от квантовых атак.

Литература

1. Blakley G.R. Safeguarding cryptographic keys // Proc. of the International Workshop on Managing Requirements Knowledge (MARK). 1979. P. 313–313. https://doi.org/10.1109/mark.1979.8817296
2. Shamir A. How to share a secret // Communications of the ACM. 1979. V. 22. N 11. P. 612–613. https://doi.org/10.1145/359168.35917
3. Ильин В.А., Позняк Э.Г. Основы математического анализа. М.: Физматлит, 2005. 646 с.
4. Barker E., Barker W., Burr W., Polk W., Smid M. NIST special publication 800-57 // NIST Special publication. 2007. V. 800. N 57. P. 1–142.
5. Desmedt Y., Frankel Y. Threshold cryptosystems // Lecture Notes in Computer Science. 1990. V. 435. P. 307–315. https://doi.org/10.1007/0-387-34805-0_28
6. Gennaro R., Jarecki S., Krawczyk H., Rabin T. Secure distributed key generation for discrete-log based cryptosystems // Lecture Notes in Computer Science. 1999. V. 1592. P. 295–310. https://doi.org/10.1007/3-540-48910-X_21
7. Menezes A.J. Handbook of Applied Cryptography. Taylor & Francis, 1997. 810 p.
8. Feldman P. A practical scheme for non-interactive verifiable secret sharing // Proc. of the 28th Annual Symposium on Foundations of Computer Science (sfcs 1987). 1987. P. 427–438. https://doi.org/10.1109/SFCS.1987.4
9. McEliece R.J., Sarwate D.V. On sharing secrets and Reed-Solomon codes // Communications of the ACM. 1981. V. 24. N 9. P. 583–584. https://doi.org/10.1145/358746.358762
10. Massey J.L. Minimal codewords and secret sharing // Proc. of the 6th joint Swedish-Russian international workshop on information theory. 1993. P. 276–279.
11. Martínez-Peñas U. Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes // IEEE Transactions on Information Theory. 2018. V. 64. N 6. P. 4191–4206. https://doi.org/10.1109/tit.2018.2823326
12. Sole P., Çalkavur S., Bonnecaze A., Dela Cruz R. Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory. World Scientific Pub Co Inc., 2022. 212 p.
13. Kurihara J., Uyematsu T., Matsumoto R. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2012. V. E95.A. N 11. P. 2067–2075. https://doi.org/10.1587/transfun.e95.a.2067
14. Massey J.L. Some applications of coding theory in cryptography // Codes and Ciphers: Cryptography and Coding IV. 1995. P. 33–47.
15. Steinfeld R., Wang H., Pieprzyk J. Lattice-based threshold-changeability for standard Shamir secret-sharing schemes // Lecture Notes in Computer Science. 2004. V. 3329. P. 170–186. https://doi.org/10.1007/978-3-540-30539-2_13
16. Ajtai M. Generating hard instances of lattice problems (extended abstract) // Proc. of the 28th Annual ACM Symposium on Theory of Computing (STOC '96). 1996. P. 99–108. https://doi.org/10.1145/237814.237838
17. Regev O. On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM (JACM). 2009. V. 56. N 6. P. 1–40. https://doi.org/10.1145/1568318.1568324
18. Bansarkhani R.E., Meziani M. An efficient lattice-based secret sharing construction // Lecture Notes in Computer Science. 2012. V. 7322. P. 160–168. https://doi.org/10.1007/978-3-642-30955-7_14
19. Khorasgani H.A. Asaad S., Eghlidos T., Aref M. A lattice-based threshold secret sharing scheme // Proc. of the 11th International ISC Conference on Information Security and Cryptology. 2014. P. 173–179. https://doi.org/10.1109/ISCISC.2014.6994043
20. Ajtai M., Dwork C. A public-key cryptosystem with worst-case/average-case equivalence // Proc. of the 29th Annual ACM Symposium on Theory of Computing (STOC '97). 1997. P. 284–293. https://doi.org/10.1145/258533.258604
21. Lyubashevsky V., Micciancio D. Generalized compact knapsacks are collision resistant // Lecture Notes in Computer Science. 2006. V. 4052. P. 144–155. https://doi.org/10.1007/11787006_13
22. Peikert C., Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices // Lecture Notes in Computer Science. 2006. V. 3876. P. 145–166. https://doi.org/10.1007/11681878_8

References

1. Blakley G.R. Safeguarding cryptographic keys. *Proc. of the International Workshop on Managing Requirements Knowledge (MARK)*, 1979, pp. 313–313. https://doi.org/10.1109/mark.1979.8817296
2. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, no. 11, pp. 612–613. https://doi.org/10.1145/359168.35917
3. Ilin V.A., Pozniak E.G. Fundamentals of Mathematical Analysis. Moscow, Fizmatlit Publ., 2005. 656 p. (in Russian)
4. Barker E., Barker W., Burr W., Polk W., Smid M. NIST special publication 800-57. *NIST Special publication*, 2007, vol. 800, no. 57, pp. 1–142.
5. Desmedt Y., Frankel Y. Threshold cryptosystems. *Lecture Notes in Computer Science*, 1990, vol. 435, pp. 307–315. https://doi.org/10.1007/0-387-34805-0_28
6. Gennaro R., Jarecki S., Krawczyk H., Rabin T. Secure distributed key generation for discrete-log based cryptosystems. *Lecture Notes in Computer Science*, 1999, vol. 1592, pp. 295–310. https://doi.org/10.1007/3-540-48910-X_21
7. Menezes A.J. *Handbook of Applied Cryptography*. Taylor & Francis, 1997, 810 p.
8. Feldman P. A practical scheme for non-interactive verifiable secret sharing. *Proc. of the 28th Annual Symposium on Foundations of Computer Science (sfcs 1987)*, 1987, pp. 427–438. https://doi.org/10.1109/SFCS.1987.4
9. McEliece R.J., Sarwate D.V. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 1981, vol. 24, no. 9, pp. 583–584. https://doi.org/10.1145/358746.358762
10. Massey J.L. Minimal codewords and secret sharing. *Proc. of the 6th joint Swedish-Russian international workshop on information theory*, 1993, pp. 276–279.
11. Martínez-Peñas U. Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes. *IEEE Transactions on Information Theory*, 2018, vol. 64, no. 6, pp. 4191–4206. https://doi.org/10.1109/tit.2018.2823326
12. Sole P., Çalkavur S., Bonnecaze A., Dela Cruz R. *Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory*. World Scientific Pub Co Inc., 2022. 212 p.
13. Kurihara J., Uyematsu T., Matsumoto R. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2012, vol. E95.A, no. 11, pp. 2067–2075. https://doi.org/10.1587/transfun.e95.a.2067
14. Massey J.L. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, 1995, pp. 33–47.
15. Steinfeld R., Wang H., Pieprzyk J. Lattice-based threshold-changeability for standard Shamir secret-sharing schemes. *Lecture Notes in Computer Science*. 2004, vol. 3329, pp. 170–186. https://doi.org/10.1007/978-3-540-30539-2_13
16. Ajtai M. Generating hard instances of lattice problems (extended abstract). *Proc. of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, 1996, pp. 99–108. https://doi.org/10.1145/237814.237838
17. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 2009, vol. 56, no. 6, pp. 1–40. https://doi.org/10.1145/1568318.1568324
18. Bansarkhani R.E., Meziani M. An efficient lattice-based secret sharing construction. *Lecture Notes in Computer Science*, 2012, vol. 7322, pp. 160–168. https://doi.org/10.1007/978-3-642-30955-7_14
19. Khorasgani H.A. Asaad S., Eghlidos T., Aref M. A lattice-based threshold secret sharing scheme. *Proc. of the 11th International ISC Conference on Information Security and Cryptology*. 2014, pp. 173–179. https://doi.org/10.1109/ISCISC.2014.6994043
20. Ajtai M., Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. *Proc. of the 29th Annual ACM Symposium on Theory of Computing (STOC '97)*, 1997, pp. 284–293. https://doi.org/10.1145/258533.258604
21. Lyubashevsky V., Micciancio D. Generalized compact knapsacks are collision resistant. *Lecture Notes in Computer Science*, 2006, vol. 4052, pp. 144–155. https://doi.org/10.1007/11787006_13
22. Peikert C., Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. *Lecture Notes in Computer Science*, 2006, vol. 3876, pp. 145–166. https://doi.org/10.1007/11681878_8

23. Georgescu A. A LWE-based secret sharing scheme // IJCA Special Issue on Network Security and Cryptography, NSC. 2011. V. 3. P. 27–29.
24. Dehkordi M.H., Farahi S.T., Mashhadi S. LWE-based verifiable essential secret image sharing scheme ((t, s, k, n) (t,s,k,n)-VESIS) // IET Image Processing. 2024. V. 18. N 4. P. 1053–1072. https://doi.org/10.1049/ipr2.13006
25. Golub G.H., Van Loan C.F. Matrix Computations. JHU press, 2013. 784 p.
26. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proc. of the 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700
27. Smith B. Pre-and post-quantum Diffie–Hellman from groups, actions, and isogenies // Lecture Notes in Computer Science. 2018. V. 11321. P. 3–40. https://doi.org/10.1007/978-3-030-05153-2_1
28. Couveignes J.M. Hard homogeneous spaces: Preprint // HAL science ouverte. 2006. hal-04538731
29. Rostovtsev A., Stolbunov A. Public-key cryptosystem based on isogenies // IACR Cryptology ePrint Archive. 2006.
30. Teske E. An elliptic curve trapdoor system // Journal of Cryptology. 2006. V. 19. P. 115–133. https://doi.org/10.1007/s00145-004-0328-3
31. Charles D.X., Lauter K.E., Goren E.Z. Cryptographic hash functions from expander graphs // Journal of Cryptology. 2009. V. 22. N 1. P. 93–113. https://doi.org/10.1007/s00145-007-9002-x
32. Jao D., De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Lecture Notes in Computer Science. 2011. V. 7071. P. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2
33. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an efficient post-quantum commutative group action // Lecture Notes in Computer Science. 2018. V. 11274. P. 395–427. https://doi.org/10.1007/978-3-030-03332-3_15
34. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations // Lecture Notes in Computer Science. 2019. V. 11921. P. 227–247. https://doi.org/10.1007/978-3-030-34578-5_9
35. Stolbunov A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves // Advances in Mathematics of Communications. 2010. V. 4. N 2. P. 215–235. https://doi.org/10.3934/amc.2010.4.215
36. De Feo L., Meyer M. Threshold schemes from isogeny assumptions // Lecture Notes in Computer Science. 2020. V. 12111. P. 187–212. https://doi.org/10.1007/978-3-030-45388-6_7
37. Cozzo D., Smart N.P. Sashimi: cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol // Lecture Notes in Computer Science. 2020. V. 12100. P. 169–186. https://doi.org/10.1007/978-3-030-44223-1_10
38. Sotáková J. Elliptic curves, isogenies, and endomorphism rings: Preprint. 2020.
39. Kim T. Security analysis of group action inverse problem with auxiliary inputs with application to CSIDH Parameters // Lecture Notes in Computer Science. 2020. V. 11975. P. 165–174. https://doi.org/10.1007/978-3-030-40921-0_10
40. Meyer M. Practical isogeny-based cryptography: dissertation. Universität Würzburg, 2021. 167 p.
41. Rogaway P., Shrimpton T. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance // Lecture Notes in Computer Science. 2004. V. 3017. P. 371–388. https://doi.org/10.1007/978-3-540-25937-4_24
42. Zheng Y., Hardjono T., Seberry J. Reusing shares in secret sharing schemes // The Computer Journal. 1994. V. 37. N 3. P. 199–205. https://doi.org/10.1093/comjnl/37.3.199
43. Liaojun P., Huixian L., Yumin W. An efficient and secure multi-secret sharing scheme with general access structures // Wuhan University Journal of Natural Sciences. 2006. V. 11. N 6. P. 1649–1652. https://doi.org/10.1007/BF02831842
44. Lin H.Y., Yeh Y.S. Dynamic multi-secret sharing scheme // International Journal of Contemporary Mathematical Sciences. 2008. V. 3. N 1. P. 37–42.
45. Das A., Adhikari A. An efficient multi-use multi-secret sharing scheme based on hash function // Applied Mathematics Letters. 2010. V. 23. N 9. P. 993–996. https://doi.org/10.1016/j.aml.2010.04.024

23. Georgescu A. A LWE-based secret sharing scheme. *IJCA Special Issue on Network Security and Cryptography*, NSC, 2011, vol. 3, pp. 27–29.
24. Dehkordi M.H., Farahi S.T., Mashhadi S. LWE-based verifiable essential secret image sharing scheme ((t, s, k, n) (t,s,k,n)-VESIS). *IET Image Processing*, 2024, vol. 18, no. 4, pp. 1053–1072. https://doi.org/10.1049/ipr2.13006
25. Golub G.H., Van Loan C.F. *Matrix Computations*. JHU press, 2013, 784 p.
26. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700
27. Smith B. Pre-and post-quantum Diffie–Hellman from groups, actions, and isogenies. *Lecture Notes in Computer Science*, 2018, vol. 11321, pp. 3–40. https://doi.org/10.1007/978-3-030-05153-2_1
28. Couveignes J.M. Hard homogeneous spaces: Preprint. *HAL science ouverte*. 2006. hal-04538731
29. Rostovtsev A., Stolbunov A. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006.
30. Teske E. An elliptic curve trapdoor system. *Journal of Cryptology*, 2006, vol. 19, pp. 115–133. https://doi.org/10.1007/s00145-004-0328-3
31. Charles D.X., Lauter K.E., Goren E.Z. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 2009, vol. 22, no. 1, pp. 93–113. https://doi.org/10.1007/s00145-007-9002-x
32. Jao D., De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Lecture Notes in Computer Science*, 2011, vol. 7071, pp. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2
33. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an efficient post-quantum commutative group action. *Lecture Notes in Computer Science*, 2018, vol. 11274, pp. 395–427. https://doi.org/10.1007/978-3-030-03332-3_15
34. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations. *Lecture Notes in Computer Science*, 2019, vol. 11921, pp. 227–247. https://doi.org/10.1007/978-3-030-34578-5_9
35. Stolbunov A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 2010, vol. 4, no. 2, pp. 215–235. https://doi.org/10.3934/amc.2010.4.215
36. De Feo L., Meyer M. Threshold schemes from isogeny assumptions. *Lecture Notes in Computer Science*, 2020, vol. 12111, pp. 187–212. https://doi.org/10.1007/978-3-030-45388-6_7
37. Cozzo D., Smart N.P. Sashimi: cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol. *Lecture Notes in Computer Science*, 2020, vol. 12100, pp. 169–186. https://doi.org/10.1007/978-3-030-44223-1_10
38. Sotáková J. *Elliptic curves, isogenies, and endomorphism rings*: Preprint. 2020.
39. Kim T. Security analysis of group action inverse problem with auxiliary inputs with application to CSIDH Parameters. *Lecture Notes in Computer Science*, 2020, vol. 11975, pp. 165–174. https://doi.org/10.1007/978-3-030-40921-0_10
40. Meyer M. *Practical isogeny-based cryptography*: dissertation. Universität Würzburg, 2021. 167 p.
41. Rogaway P., Shrimpton T. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. *Lecture Notes in Computer Science*, 2004, vol. 3017, pp. 371–388. https://doi.org/10.1007/978-3-540-25937-4_24
42. Zheng Y., Hardjono T., Seberry J. Reusing shares in secret sharing schemes. *The Computer Journal*, 1994, vol. 37, no. 3, pp. 199–205. https://doi.org/10.1093/comjnl/37.3.199
43. Liaojun P., Huixian L., Yumin W. An efficient and secure multi-secret sharing scheme with general access structures. *Wuhan University Journal of Natural Sciences*, 2006, vol. 11, no. 6, pp. 1649–1652. https://doi.org/10.1007/BF02831842
44. Lin H.Y., Yeh Y.S. Dynamic multi-secret sharing scheme. *International Journal of Contemporary Mathematical Sciences*, 2008, vol. 3, no. 1, pp. 37–42.
45. Das A., Adhikari A. An efficient multi-use multi-secret sharing scheme based on hash function. *Applied Mathematics Letters*, 2010, vol. 23, no. 9, pp. 993–996. https://doi.org/10.1016/j.aml.2010.04.024

46. Chum C.S., Zhang X. Hash function-based secret sharing scheme designs // Security and Communication Networks. 2013. V. 6. N 5. P. 584–592. https://doi.org/10.1002/sec.576
47. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak // Lecture Notes in Computer Science. 2013. V. 7881. P. 313–314. https://doi.org/10.1007/978-3-642-38348-9_19
48. Putra R.A., Effendie A.R., Aisah S.N., Christy J.R., Marpaung E.C.F., Syarkowi M.Z.H., Devi P.K. Analyzing the relationship between capital and risk in Indonesian life insurance companies using the 2SLS and GMM methods // Jurnal Riset dan Aplikasi Matematika. 2024. V. 8. N 2. P. 142–157.
49. Karnin E., Greene J., Hellman M. On secret sharing systems // IEEE Transactions on Information Theory. 1983. V. 29. N 1. P. 35–41. https://doi.org/10.1109/TIT.1983.1056621
50. Ning Y., Miao F., Huang W., Meng K., Xiong Y., Wang X. Constructing ideal secret sharing schemes based on Chinese remainder theorem // Lecture Notes in Computer Science. 2018. V. 11274. P. 310–331. https://doi.org/10.1007/978-3-030-03332-3_12
51. Asmuth C., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. 1983. V. 29. N 2. P. 208–210. https://doi.org/10.1109/tit.1983.1056651
52. Galibus T., Matveev G. Finite fields, Gröbner bases and modular secret sharing // Journal of Discrete Mathematical Sciences and Cryptography. 2012. V. 15. N 6. P. 339–348. https://doi.org/10.1080/09720529.2012.10698386

46. Chum C.S., Zhang X. Hash function-based secret sharing scheme designs. *Security and Communication Networks*, 2013, vol. 6, no. 5, pp. 584–592. https://doi.org/10.1002/sec.576
47. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak. *Lecture Notes in Computer Science*, 2013, vol. 7881, pp. 313–314. https://doi.org/10.1007/978-3-642-38348-9_19
48. Putra R.A., Effendie A.R., Aisah S.N., Christy J.R., Marpaung E.C.F., Syarkowi M.Z.H., Devi P.K. Analyzing the relationship between capital and risk in Indonesian life insurance companies using the 2SLS and GMM methods. *Jurnal Riset dan Aplikasi Matematika*, 2024, vol. 8, no. 2, pp. 142–157.
49. Karnin E., Greene J., Hellman M. On secret sharing systems. *IEEE Transactions on Information Theory*, 1983, vol. 29, no. 1, pp. 35–41. https://doi.org/10.1109/TIT.1983.1056621
50. Ning Y., Miao F., Huang W., Meng K., Xiong Y., Wang X. Constructing ideal secret sharing schemes based on Chinese remainder theorem. *Lecture Notes in Computer Science*, 2018, vol. 11274, pp. 310–331. https://doi.org/10.1007/978-3-030-03332-3_12
51. Asmuth C., Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 1983, vol. 29, no. 2, pp. 208–210. https://doi.org/10.1109/tit.1983.1056651
52. Galibus T., Matveev G. Finite fields, Gröbner bases and modular secret sharing. *Journal of Discrete Mathematical Sciences and Cryptography*, 2012, vol. 15, no. 6, pp. 339–348. https://doi.org/10.1080/09720529.2012.10698386

Авторы

Кустов Елизар Филаретович — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57672934000, https://orcid.org/0000-0002-0191-1178, elizarkustov@mail.ru
Беззатеев Сергей Валентинович — доктор технических наук, доцент, заведующий кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация; профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 6602425996, https://orcid.org/0000-0002-0924-6221, sergey.bezzateev@gmail.com

Authors

Elizar F. Kustov — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57672934000, https://orcid.org/0000-0002-0191-1178, elizarkustov@mail.ru
Sergey V. Bezzateev — D.Sc., Associate Professor, Head of Department, Saint-Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation; Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 6602425996, https://orcid.org/0000-0002-0924-6221, sergey.bezzateev@gmail.com

Статья поступила в редакцию 26.02.2025
Одобрена после рецензирования 18.04.2025
Принята к печати 28.05.2025

Received 26.02.2025
Approved after reviewing 18.04.2025
Accepted 28.05.2025