ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 1 2024

Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь–март 2024. Т. 31, № 1. С. 52–84

УДК 519.7 DOI: 10.33048/daio.2024.31.772

ПОСТКВАНТОВЫЕ КРИПТОСИСТЕМЫ: ОТКРЫТЫЕ ВОПРОСЫ И СУЩЕСТВУЮЩИЕ РЕШЕНИЯ. КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ И КОДАХ, ИСПРАВЛЯЮЩИХ ОШИБКИ

Е. С. Малыгина[1,2,a], *А. В. Куценко*[2,b], *С. А. Новосёлов*[1,c], *Н. С. Колесников*[1,d], *А. О. Бахарев*[2,e], *И. С. Хильчук*[2,f], *А. С. Шапоренко*[2,g], *Н. Н. Токарева*[2,1,h]

[1] Балтийский федеральный университет им. И. Канта,
ул. Александра Невского, 14, 236041 Калининград, Россия
[2] Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
E-mail: [a] emalygina@kantiana.ru, [b] alexandrkutsenko@bk.ru,
[c] novsem@gmail.com, [d] nikolesnikov100@gmail.com, [e] a.bakharev@g.nsu.ru,
[f] irina.khilchuk@gmail.com, [g] shaporenko.alexandr@gmail.com,
[h] crypto1127@mail.ru

Аннотация. Представлен обзор основных постквантовых криптографических схем на основе кодов, исправляющих ошибки, и изогений эллиптических кривых, а также вычислительно трудных задач, лежащих в их основе. Особое внимание уделено описанию атак на представленные схемы. В частности, для кодовых криптосистем описаны атаки на основе информационных совокупностей и расщепления носителя, для криптосистем на изогениях дано подробное описание атаки Кастрика — Декру на схему SIDH/SIKE. Табл. 2, библиогр. 43.

Ключевые слова: постквантовая криптография, код, исправляющий ошибки, эллиптическая кривая, изогения.

Введение

Настоящая статья является продолжением работы [1], в которой рассмотрены криптосистемы, основанные на теории решёток, и задачи, лежащие в основе их стойкости. Как отмечено в [1], помимо схем на основе решёток, выбранных в качестве нового стандарта постквантовой криптографии, существуют альтернативные кандидаты, а именно — криптосистемы на основе кодов, исправляющих ошибки, и изогений суперсингулярных эллиптических кривых. Данная работа посвящена описанию

таких криптосистем, а также вычислительно трудных задач, на которых базируется их стойкость.

В отличие от криптографии на решётках, в которой безопасность ряда протоколов основывается на сложности аппроксимации случайного вектора далёко за пределами ближайшего вектора решётки, в криптографии на кодах безопасность протоколов зависит от нахождения кодовых слов малого веса ниже границы Варшамова — Гилберта, поскольку алгоритм декодирования за пределами этой границы на данный момент не известен.

К основным преимуществам и недостаткам криптосистем на кодах (в частности, схем цифровой подписи) стоит отнести следующие:

- использование алгоритма Куртуа — Финьяза — Сондриера (CFS) [2] приводит к малому размеру самой подписи при сравнительно медленной скорости работы и большому размеру открытого ключа;
- использование эвристики Фиата — Шамира [3], наоборот, приводит к малому размеру открытого ключа (как правило, несколько сотен бит), обеспечивает достаточно высокую скорость работы, однако размер подписи сравнительно велик (составляет около 10^5 бит).

Криптография на изогениях существенно отличается от предыдущих двух типов, поскольку основана на естественно возникающей в теории чисел задаче вычисления изогений между эллиптическими кривыми. Таким образом, криптосистемы на изогениях составляют одно из немногих семейств, на данный момент устойчивых к атакам с использованием квантового компьютера и основанных на теоретико-числовых задачах (если рассматривать задачу решения нелинейных систем уравнений от многих переменных как теоретико-числовую). В некотором смысле задачу нахождения изогении можно рассматривать как аналог задачи дискретного логарифмирования, в рамках которого вместо абелевой группы точек кривой используют граф изогений. В то время как квантовый компьютер решает задачу дискретного логарифма в группе точек эллиптической кривой за полиномиальное время, для вычисления изогении существующими алгоритмами требуется субэкспоненциальное время при использовании обычных эллиптических кривых и экспоненциальное время при использовании суперсингулярных эллиптических кривых [4].

К основным преимуществам и недостаткам криптосистем на изогениях стоит отнести небольшие размеры ключей при относительно медленной скорости работы. Несмотря на то, что криптографические системы данного типа выглядят многообещающе, они нуждаются в более глубоком изучении. Это обусловлено появлением эффективных атак на некоторые варианты подобных криптосистем, например, атаки Кастрика — Декру (см. разд. 2.5), опубликованной в 2022 г.

1. Коды, исправляющие ошибки

1.1. Предварительные сведения. Коды, исправляющие ошибки, используются для передачи информации в каналах связи, в которых информация искажается. Определённая избыточность в передаваемых кодовых словах (блоках) позволяет обнаруживать ошибки в принятых словах (блоках) и исправлять их, выбирая ближайшие кодовые слова. Особое распространение получили линейные коды в силу более эффективных алгоритмов кодирования и декодирования.

Пусть $\mathbb{F}_q$ — конечное поле, состоящее из q элементов, $\mathbb{F}_q^n$ — векторное пространство над $\mathbb{F}_q$. *Линейным* $[n,k]$*-кодом* $\mathcal{C}$ называется k-мерное векторное подпространство в $\mathbb{F}_q^n$. При этом вектор $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$ называется *кодовым словом* $\mathcal{C}$.

Важным качеством кода является возможность исправления приобретённых ошибок в ходе передачи информации по зашумлённому каналу. Для определения кодового расстояния введём метрику на векторном пространстве $\mathbb{F}_q^n$.

Расстоянием Хэмминга между векторами $x, y \in \mathbb{F}_q^n$ называется число координат, в которых векторы различаются:

$$d_H(x,y) = |\{i \mid x_i \neq y_i\}|.$$

Весом Хэмминга вектора $x \in \mathbb{F}_q^n$ называется число его ненулевых координат:

$$wt_H(x) = |\{i \mid x_i \neq 0\}| = d_H(x,0).$$

Кодовым расстоянием кода $\mathcal{C}$ называется минимальное расстояние Хэмминга между его различными кодовыми словами:

$$d = \min\{d_H(x,y) \mid x,y \in \mathcal{C},\ x \neq y\}.$$

В случае линейных кодов имеем

$$d = \min\{d_H(x,y) \mid x,y \in \mathcal{C},\ x \neq y\} = \min\{wt_H(x) \mid x \in \mathcal{C},\ x \neq 0\}.$$

При этом число исправляемых кодом $\mathcal{C}$ ошибок равно $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Чтобы задать линейный код, можно либо задать его базис, либо задать систему линейных уравнений, решением которой являются координаты кодовых слов. Формально это можно сделать с помощью матриц.

Порождающей матрицей линейного $[n,k]$-кода $\mathcal{C}$ называется матрица G над $\mathbb{F}_q$ размера $k \times n$ такая, что

$$\mathcal{C} = \left\{xG \mid x \in \mathbb{F}_q^k\right\}.$$

Проверочной матрицей линейного $[n,k]$-кода $\mathcal{C}$ называется матрица H над $\mathbb{F}_q$ размера $(n-k) \times n$ такая, что

$$\mathcal{C} = \{y \in \mathbb{F}_q^n \mid Hy^\top = 0\}.$$

Одним из главных в теории кодирования является вопрос, как использовать коды для исправления ошибок. Ответ на него даёт процедура декодирования. *Декодированием* кода $\mathcal{C}$ называется отображение $D_{\mathcal{C}}\colon \mathbb{F}_q^n \to \mathcal{C}$. Код *исправляет* t *ошибок*, если $D_{\mathcal{C}}(c+e) = c$ для любых $c \in \mathcal{C}$ и $e \in \mathbb{F}_q^n$, $wt_H(e) \leqslant t$.

1.2. Базовые кодовые криптосистемы.

Схема Мак-Элиса. Первой криптосистемой на кодах была схема шифрования с открытым ключом, предложенная в 1978 г. Мак-Элисом [5]. Однако практически все асимметричные модификации на базе кодов, предложенные позже, имеют общий недостаток — большие требования к памяти.

Рассмотрим оригинальную криптосистему Мак-Элиса. Её секретным ключом является классический код Гоппы.

Пусть m и t — положительные целые числа. Определим *многочлен Гоппы*

$$g(X) = \sum_{i=0}^{t} g_i X^i \in \mathbb{F}_{2^m}[X]$$

и множество

$$\mathcal{L} = \{\alpha_0, \ldots, \alpha_{n-1}\} \in \mathbb{F}_{2^m}^n,$$

где $g(\alpha_j) \neq 0$, $j = 0, \ldots, n-1$. *Синдром* представляет собой многочлен вида

$$\mathcal{S}_c(X) = \left(-\sum_{i=0}^{n-1} \frac{c_i}{g(\alpha_i)} \cdot \frac{g(X) - g(\alpha_i)}{X - \alpha_i} \right) \bmod g(X),$$

где $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_{2^m}^n$. *Двоичным кодом Гоппы* над $\mathbb{F}_{2^m}$ называется линейный код

$$\mathcal{C}(\mathcal{L}, g(X)) = \left\{ c \in \mathbb{F}_{2^m}^n \mid \mathcal{S}_c(X) = \sum_{i=0}^{n-1} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)} \right\}.$$

При этом проверочная матрица кода Гоппы $\mathcal{C}(\mathcal{L}, g(X))$ имеет вид

$$H = \begin{pmatrix} \frac{g_s}{g(\alpha_0)} & \frac{g_s}{g(\alpha_1)} & \cdots & \frac{g_s}{g(\alpha_{n-1})} \\ \frac{g_{s-1}+g_s\alpha_0}{g(\alpha_0)} & \frac{g_{s-1}+g_s\alpha_0}{g(\alpha_1)} & \cdots & \frac{g_{s-1}+g_s\alpha_0}{g(\alpha_{n-1})} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{g_1+g_2\alpha_0+\cdots+g_s\alpha_0^{s-1}}{g(\alpha_0)} & \frac{g_1+g_2\alpha_0+\cdots+g_s\alpha_0^{s-1}}{g(\alpha_1)} & \cdots & \frac{g_1+g_2\alpha_0+\cdots+g_s\alpha_0^{s-1}}{g(\alpha_{n-1})} \end{pmatrix},$$

или

$$H = \begin{pmatrix} g_s & 0 & \dots & 0 \\ g_{s-1} & g_s & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ g_1 & g_2 & \dots & g_s \end{pmatrix} \times \begin{pmatrix} \frac{1}{g(\alpha_0)} & \frac{1}{g(\alpha_1)} & \dots & \frac{1}{g(\alpha_{n-1})} \\ \frac{\alpha_0}{g(\alpha_0)} & \frac{\alpha_1}{g(\alpha_1)} & \dots & \frac{\alpha_{n-1}}{g(\alpha_{n-1})} \\ \vdots & \vdots & \dots & \vdots \\ \frac{\alpha_0^{s-1}}{g(\alpha_0)} & \frac{\alpha_1^{s-1}}{g(\alpha_1)} & \dots & \frac{\alpha_{n-1}^{s-1}}{g(\alpha_{n-1})} \end{pmatrix},$$

где $g(X) = g_s X^s + g_{s-1} X^{s-1} + \dots + g_0$.

Генерация ключей. Алгоритм генерации ключей начинается с выбора двоичного кода Гоппы, исправляющего до t ошибок. Для этого случайным образом выбирается неприводимый многочлен Гоппы степени t. Затем вычисляется соответствующая порождающая матрица G. Поскольку злоумышленник, зная G, сможет определить структуру используемого кода и эффективно его декодировать, алгебраическая структура матрицы G должна быть скрыта. Для этой цели используются обратимая матрица S и перестановочная матрица P, которые генерируются случайным образом и умножаются на G слева и справа соответственно, чтобы сформировать $\widetilde{G} = SGP$. Таким образом, $\widetilde{G}$ является порождающей матрицей для кода, эквивалентного $\mathcal{C}$.

Будем считать, что $q = 2^m$. Обобщая вышесказанное, заметим, что для генерации ключей необходимо следующее.

1. Выбрать двоичный $[n, k, d]$-код Гоппы $\mathcal{C}$, исправляющий $t = \lfloor \frac{d-1}{2} \rfloor$ ошибок.
2. Вычислить порождающую матрицу кода G над $\mathbb{F}_q$ размера $k \times n$.
3. Выбрать случайную обратимую матрицу $S \in GL_k(\mathbb{F}_q)$.
4. Выбрать случайную перестановочную матрицу $P \in S_n(\mathbb{F}_q)$.
5. Вычислить $\widetilde{G} = SGP$.

Секретным ключом является тройка $K_{\text{priv}} = \{G, S, P\}$, открытым — $K_{\text{pub}} = \widetilde{G}$.

Зашифрование представляет собой простое векторно-матричное умножение k-битного сообщения m на порождающую матрицу $\widetilde{G}$ и добавление случайного вектора ошибки e веса Хэмминга, не превосходящего t.

1. Представить исходное сообщение в виде двоичной строки m длины k.
2. Выбрать случайный вектор ошибки $e \in \mathbb{F}_q^n$ такой, что $wt_H(e) \leqslant t$.
3. Вычислить $c = m\widetilde{G} + e$.

Расшифрование представляет собой исправление ошибок в полученном сообщении с использованием известного алгоритма декодирования $D_{\mathcal{C}}$ для кода $\mathcal{C}$. Декодирование является наиболее трудоёмкой частью

процесса расшифрования, что делает его более медленным, чем шифрование.

1. Вычислить $\widetilde{c} = cP^{-1}$.
2. Применяя алгоритм декодирования $D_{\mathcal{C}}$ к $\widetilde{c}$, вычислить вектор $\widetilde{m}$ длины k.
3. Вычислить $m = (\widetilde{m}G^{-1})S^{-1}$.

Корректность расшифрования. Имеем

$$\widetilde{c} = cP^{-1} = (mSGP + e)P^{-1} = (mS)G + eP^{-1}.$$

Поскольку $wt_H(eP^{-1}) \leqslant t$, то $\widetilde{m} = D_{\mathcal{C}}(\widetilde{c}) = D_{\mathcal{C}}(cP^{-1}) = mSG$. Восстанавливаем исходное сообщение m:

$$(\widetilde{m}G^{-1})S^{-1} = ((mSG)G^{-1})S^{-1} = m.$$

Схема Нидеррайтера. В 1986 г. Нидеррайтер предложил ещё одну кодовую криптосистему [6]. В этой схеме сообщение полностью кодируется в вектор ошибок, что позволяет избежать утечки информации из битов открытого текста, в отличие от схемы Мак-Элиса. В качестве открытого ключа для вычисления синдрома используется проверочная матрица. Преимуществом этой схемы является меньший размер открытого ключа.

Генерация ключей. Как и ранее, $q = 2^m$. Чтобы сгенерировать ключи, необходимо следующее.

1. Выбрать двоичный $[n, k, d]$-код Гоппы $\mathcal{C}$, исправляющий $t = \lfloor \frac{d-1}{2} \rfloor$ ошибок.
2. Вычислить проверочную матрицу кода H над $\mathbb{F}_q$ размера $(n-k)\times n$.
3. Выбрать случайную обратимую матрицу $S \in GL_{n-k}(\mathbb{F}_q)$.
4. Выбрать случайную перестановочную матрицу $P \in S_n(\mathbb{F}_q)$.
5. Вычислить $\widetilde{H} = SHP$.

Секретным ключом является тройка $K_{\text{priv}} = \{H, S, P\}$, открытым — $K_{\text{pub}} = \widetilde{H}$.

Зашифрование осуществляется следующим образом.

1. Представить исходное сообщение в виде двоичной строки e длины n веса $wt_H(e) = t$.
2. Вычислить $c = \widetilde{H}e^{\top}$.

Расшифрование выполняется с применением алгоритма декодирования кода Гоппы, лежащего в основе криптосистемы.

1. Вычислить $\widetilde{c} = S^{-1}c$.
2. Применяя алгоритм декодирования $D_{\mathcal{C}}$ к $\widetilde{c}$, вычислить $\widetilde{e}$.
3. Вычислить вектор $e = P^{-1}\widetilde{e}$ длины n веса t.

Корректность расшифрования заключается в том, что исходное сообщение имеет вес t. Это значит, что к зашифрованному сообщению можно применить алгоритм декодирования.

Позже было показано, что схема Нидеррайтера имеет такой же уровень стойкости, что и схема Мак-Элиса [7].

1.3. Задачи, лежащие в основе безопасности. Согласно [8] два основных аспекта, на которых основывается безопасность схемы Мак-Элиса, следующие:

(1) сложность задачи декодирования общего неизвестного кода, которая NP-трудна [9];

(2) сложность атак, восстанавливающих структуру базового кода.

Ключевым действием, обеспечивающим безопасность кодовых криптосистем, является сокрытие структуры используемого кода. Как и ранее, пусть G — порождающая матрицей приватного кода $\mathcal{C}$, а $\widetilde{\mathcal{C}}$ — открытый код, полученный из $\mathcal{C}$ с помощью одного или нескольких секретных преобразований. Приведём наиболее распространённые преобразования.

• Умножение G справа на случайную обратимую матрицу S над $\mathbb{F}_q$ размера $k \times k$.

• Умножение G слева на случайную обратимую матрицу T над $\mathbb{F}_q$ размера $n \times n$.

• Умножение G справа на случайную матрицу полного ранга S над $\mathbb{F}_q$ размера $\ell \times k$, $\ell < k$. В этом случае имеем подкод $\mathcal{C}_{SG} \subseteq \mathcal{C}$ с порождающей матрицей SG, для которого всё так же можно использовать соответствующий алгоритм декодирования, исправляющий заданное число ошибок.

• Использование подполевых подкодов $\mathcal{C} \cap \mathbb{F}_p$ при условии, что исходный код $\mathcal{C}$ определён над расширением конечного поля $\mathbb{F}_p$.

• Использование кода $\mathcal{C}_{[G|SG]}$, чья порождающая матрица получена с помощью конкатенации $[\,G \mid SG\,]$, где S определена над $\mathbb{F}_q$, имеет размер $k \times k$ и обратима.

• Добавление ℓ случайных столбцов слева к матрице G.

• Укорачивание и прокалывание кода $\mathcal{C}$.

Под *прокалыванием* и *укорачиванием* кода будем понимать следующее. *Проколотый* (*единожды*) код $\mathcal{C}^*$ получается из $\mathcal{C}$ удалением одной и той же i-й координаты в каждом кодовом слове. Если G — порождающая матрица кода $\mathcal{C}$, то порождающая матрица G^* кода $\mathcal{C}^*$ получается удалением i-го столбца из G. Пусть T — множество индексов, $|T| = s$. *Проколотый* (*многократно*) код $\mathcal{C}^T$ получается из $\mathcal{C}$ удалением позиций с индексами из T в каждом кодовом слове $\mathcal{C}$. Отметим, что $\mathcal{C}^T$ — код с параметрами $[n - s, \geqslant k - s, \geqslant d - s]$. Пусть $\mathcal{C}(T) \subseteq \mathcal{C}$ — подкод с нулевыми координатами при индексах из T. *Укороченный* код $\mathcal{C}_T$ длины $n - s$ получается прокалыванием кода $\mathcal{C}(T)$ в позициях с индексами из T.

Рассмотрим некоторые известные задачи, сложность решения которых лежит в основе безопасности схем типа Мак-Элиса и Нидеррайтера.

Задача Мак-Элиса. *Для заданных открытого ключа* $\widetilde{G}$ *и шифртекста* c *найти единственное сообщение* m *такое, что* $wt_H(m\widetilde{G} - c) = t$.

Поскольку код $\widetilde{\mathcal{C}}$ с порождающей матрицей $\widetilde{G}$ эквивалентен исходному коду $\mathcal{C}$, нельзя предполагать, что задача Мак-Элиса NP-трудна в отличие от общей задачи декодирования. Однако решение данной задачи позволило бы найти решение общей задачи декодирования лишь для некоторых классов кодов, но не для всех.

В схеме Нидеррайтера процесс зашифрования можно записать иначе, а именно: $c = e\widetilde{H}$. Тогда задача декодирования сводится к нахождению кодового слова $x \in \mathcal{C}$, близкого к e относительно расстояния Хэмминга. На практике трудно проверить, действительно ли вектор ошибки, лежащий в смежном классе $e + \mathcal{C}$, имеет минимальный вес, поэтому рассматриваемая задача декодирования не NP-трудна. Рассмотрим задачу синдромного декодирования.

Синдромом вектора $y \in \mathbb{F}_q^n$ относительно проверочной матрицы H кода $\mathcal{C}$ называется вектор $S_H(y) = yH \in \mathbb{F}_q^{n-k}$. Отметим, что два вектора из $\mathbb{F}_q^n$ имеют один и тот же синдром тогда и только тогда, когда лежат в одном смежном классе по $\mathcal{C}$.

Задача синдромного декодирования. *Для матрицы* H *над* $\mathbb{F}_2$ *размера* $r \times n$, *вектора* $c \in \mathbb{F}_2^r$ *и целого* $t > 0$ *найти слово* x *в смежном классе* $S_H^{-1}(c) = e + \mathcal{C}$ *такое, что* $d(x) \leqslant t$.

Значение параметра t существенно влияет на сложность решения задачи синдромного декодирования. Задача имеет решение тогда и только тогда, когда t таково, что с высокой вероятностью обеспечивает существование единственного решения (т. е. t не больше границы Варшамова — Гилберта).

Задача нахождения ненулевых слов малого веса Хэмминга в заданном линейном коде схожа с задачей синдромного декодирования.

Задача нахождения кодового слова малого веса Хэмминга. *Для матрицы* H *над* $\mathbb{F}_2$ *размера* $r \times n$ *и целого* $t > 0$ *найти ненулевое слово* x *в* $S_H^{-1}(0)$ *такое, что* $d(x) \leqslant t$.

Отметим, что если $\mathcal{C}$ — линейный код с проверочной матрицей H, то любое решение задачи синдромного декодирования с входными параметрами H, t, $eH^\top$ также является решением задачи нахождения кодового слова малого веса Хэмминга с параметрами H', t, где H' — проверочная матрица кода $\mathcal{C}' = \mathcal{C} \cup (y + \mathcal{C})$. Обратное верно только в том случае, если $t < d$, где d — кодовое расстояние кода $\mathcal{C}$, которое обычно

неизвестно. Однако большинство двоичных линейных кодов длины n и коразмерности r (под коразмерностью имеем в виду число $r = n - \dim \mathcal{C}$ при условии, что $\mathcal{C} \subseteq \mathbb{F}_q^n$) имеют кодовое расстояние, очень близкое к расстоянию Варшамова — Гилберта $d_0(n, r)$, которое является максимально возможным значением, удовлетворяющим условию

$$\sum_{i=0}^{d_0(n,r)-1} \binom{n}{i} \leqslant 2^r.$$

В трёх рассматриваемых задачах вес t является входным значением. Особый интерес представляют те случаи, когда вес t будет зависеть от длины n и размерности k кода. Такие случаи имеют место в задачах полного и ограниченного декодирования. Расшифрование будет заключаться в нахождении слова минимального веса. Если синдром случайный, то зачастую решение будет иметь вес, равный расстоянию Варшамова — Гилберта.

Задача полного декодирования. *Для матрицы H над $\mathbb{F}_2$ размера $r \times n$ и $c \in \mathbb{F}_2^r$ найти слово x в классе $S_H^{-1}(c)$ такое, что $d(x) \leqslant d_0(n, r)$.*

В действительности задача полного декодирования является самой сложной вычислительной задачей для заданных параметров n и r. В кодовых криптосистемах типа Мак-Элиса или Нидеррайтера вес t равен числу ошибок, исправляемых кодом.

Код Гоппы длины $n = 2m$, исправляющий t ошибок, имеет коразмерность $r = tm$. В этом случае сложность решения следующей вычислительной задачи напрямую зависит от стойкости схемы.

Задача ограниченного декодирования. *Для матрицы H над $\mathbb{F}_2$ размера $r \times n$ и вектора $c \in \mathbb{F}_2^r$ найти слово x в классе $S_H^{-1}(c)$ такое, что $d(x) \leqslant \frac{r}{\log_2 n}$.*

1.4. Атаки. В качестве основных атак можно выделить две:

1) дешифрование конкретного зашифрованного сообщения;

2) структурная атака, направленная на определение структуры кода, а значит, секретного ключа.

Подбор параметров, обеспечивающих безопасность схем типа Мак-Элиса, должен осуществляться с учётом известных атак. Несмотря на то, что в основе кодовых криптосистем лежит задача декодирования, структурная атака на схемы типа Мак-Элиса отличается от общей задачи декодирования.

Задача декодирования на основе информационных совокупностей лежит в основе первого типа атак. Представим обобщённый вариант такого декодирования, отмечая, что Ли и Брикелл были первыми, кто использовал его для анализа криптосистемы Мак-Элиса [10].

Алгоритм 1. Декодирование на основе информационных совокупностей для параметра α

Вход: Матрица G над $\mathbb{F}_q$ размера $k \times n$, $w \in \mathbb{Z}$.
Выход: Кодовое слово $x \neq 0$, $wt(x) \leqslant w$.

1: **repeat**
2: $x = 0 \in \mathbb{F}_q^n$
3: Выбрать перестановочную матрицу P над $\mathbb{F}_q$ размера $n \times n$.
4: Вычислить $G' = UGP = [\mathbb{I} \mid R]$, полагая, что первые k позиций информационные, U — обратимая матрица над $\mathbb{F}_q$ размера $k \times k$, $\mathbb{I}$ — единичная матрица размера $k \times k$.
5: Вычислить все суммы α строк матрицы G'.
6: **if** wt(одна из сумм) $\leqslant w$ **then** $x \leftarrow$ эта строка
7: **until** $x \neq 0$
8: **return** x

Перейдём к рассмотрению структурной атаки. Коды, исправляющие ошибки и имеющие эффективный алгоритм декодирования, как правило, либо обладают алгебраической структурой, либо строятся специальным образом. Зная порождающую матрицу кода, можно эффективно исправить приобретённые ошибки. Это справедливо для всех кодов, имеющих большую размерность, с целью рассмотрения их в криптографических приложениях.

Рассмотрим, как можно восстановить алгебраическую структуру кода при условии, что проверочная матрица не разреженная.

В кодовых криптосистемах, как было сказано ранее, секретный код $\mathcal{C}$ стараются скрыть. Один из способов — применить к коду изометрию f. Тогда открытым ключом будет порождающая или проверочная матрица эквивалентного кода $\mathcal{C}' = f(\mathcal{C})$. В двоичном случае изометрией является любая перестановка носителя. Если метрическое пространство образует векторное пространство, то рассматривают полулинейные изометрии

$$f\colon \mathbb{F}_q^n \to \mathbb{F}_q^n\colon (x_1, \ldots, x_n) \mapsto (v_1\pi(x_{\sigma^{-1}(1)}), \ldots, v_n\pi(x_{\sigma^{-1}(n)})).$$

Здесь $(v_1, \ldots, v_n) \in \mathbb{F}_q^n$ — вектор с ненулевыми компонентами, π — автоморфизм поля $\mathbb{F}_q$, σ — перестановка носителя исходного кода, т. е. множества $\{1, \ldots, n\}$.

Два линейных кода $\mathcal{C}$ и $\mathcal{C}'$ назовём *эквивалентными,* если $\mathcal{C}' = f(\mathcal{C})$ для некоторой полулинейной изометрии f. В случае произвольного поля $\mathbb{F}_q$ эквивалентность отличается от перестановочной эквивалентности: коды $\mathcal{C}$ и $\mathcal{C}'$ *перестановочно эквивалентны,* если для некоторой перестановки $\sigma \in S_n$ имеем $\mathcal{C}' = \{(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) \in \mathbb{F}_q^n \mid (x_1, \ldots, x_n) \in \mathcal{C}\}$. В двоичном случае эти понятия совпадают.

Алгоритм расщепления носителя решает задачу эквивалентности кодов, которая заключается в следующем. Необходимо определить, существуют ли перестановочно эквивалентные линейные коды $\mathcal{C}_1$ и $\mathcal{C}_2$ с порождающими матрицами G_1 и G_2, определёнными над некоторым конечным полем. Эта задача была предложена Петранком и Ротом [11], которые показали, что она достаточно сложная однако не NP-полна.

Прежде чем описать алгоритм расщепления носителя, приведём ряд необходимых определений. Более детально с терминологией, относящейся к алгоритму, можно ознакомиться в [12].

Для некоторого множества $J \subseteq I = \{1, \ldots, n\}$ через $\mathcal{C}_J$ обозначим множество векторов, которые получены из кодовых слов кода $\mathcal{C}$ путём зануления координат, имеющих номера из J. Через $\mathcal{L}_n$ обозначим множество всех линейных кодов длины n. Тогда множество $\mathcal{L} = \bigcup\limits_{n \geqslant 1} \mathcal{L}_n$ является множеством всех линейных кодов. Отображение $\nu\colon \mathcal{L} \to E$ называется *инвариантом* над некоторым множеством E, если для любых двух перестановочно эквивалентных кодов $\mathcal{C}$ и $\mathcal{C}'$ имеет место равенство $\nu(\mathcal{C}) = \nu(\mathcal{C}')$. Отображение $\Sigma\colon \mathcal{L}_n \times I \to E$ называется *сигнатурой* над E, если $\Sigma(\mathcal{C}, i) = \Sigma(\sigma(\mathcal{C}), \sigma(i))$ для любых $\mathcal{C} \in \mathcal{L}_n$, $i \in I$ и $\sigma \in S_n$. Далее будем рассматривать сигнатуры, удовлетворяющие условию $\Sigma(\mathcal{C}, i) = \nu(\mathcal{C}_{\{i\}})$. Здесь $\mathcal{C}_{\{i\}} = \mathcal{C}_J$ для $J = \{i\}$ в соответствии с обозначением, введённым выше.

Имея сигнатуру Σ, гораздо проще ответить на вопрос, являются ли коды $\mathcal{C}$ и $\mathcal{C}'$ перестановочно эквивалентными. Для этого следует вычислить $\Sigma(\mathcal{C}, I)$ и $\Sigma(\mathcal{C}', I)$. Если коды $\mathcal{C}$ и $\mathcal{C}'$ перестановочно эквивалентны, то $\Sigma(\mathcal{C}, I) = \Sigma(\mathcal{C}', I)$. Сигнатура Σ называется *дискриминантом* кода $\mathcal{C}$, если существуют $i, j \in I$ такие, что $\Sigma(\mathcal{C}, i) \neq \Sigma(\mathcal{C}, j)$. Сигнатура Σ называется *полным дискриминантом* кода $\mathcal{C}$, если для любых $i \neq j$ из I выполняется $\Sigma(\mathcal{C}, i) \neq \Sigma(\mathcal{C}, j)$.

Отметим, что если $\mathcal{C}' = \sigma(\mathcal{C})$ и Σ — полный дискриминант кода $\mathcal{C}$, то для любого $i \in I$ найдётся единственный элемент $j \in I$ такой, что $\Sigma(\mathcal{C}, i) = \Sigma(\mathcal{C}', j)$. Равенства $\sigma(i) = j$, $i \in I$, определяют перестановку σ.

Алгоритм 2. Алгоритм расщепления носителя

Вход: $G_1, G_2 \in \mathbb{F}_q^{k \times n}$.
Выход: Перестановка σ такая, что $\mathcal{C}' = \sigma(\mathcal{C})$.

1: Вычислить сигнатуру Σ, являющуюся полным дискриминантом.
2: **for** $i, j \in \{1, \ldots, n\}$ **do**
3: **if** $\Sigma(G_1, i) = \Sigma(G_2, j)$ **then** $\sigma(i) = j$
4: **return** σ

1.5. Схемы, актуальные на сегодняшний день.

Инкапсуляция ключа переключением битов. BIKE (bit flipping key encapsulation) — схема шифрования на основе двоичных линейных QC-MDPC-кодов [13].

Под QC-MDPC-кодом, ассоциированным с тройкой (n, r, w), будем понимать код, проверочная матрица H которого определена над $\mathbb{F}_2$, имеет размер $r \times n$ и строку веса w:

$$H = [H_0 \mid H_1 \mid \cdots \mid H_{n_0-1}],$$

где r простое, $n = n_0 r$ и H_i — циркулянтный блок над $\mathbb{F}_2$ размера $r \times r$.

Обозначим $\mathcal{R} = \mathbb{F}_2[X]/(X^r - 1)$. Секретным ключом схемы BIKE является проверочная матрица $H = (H_0 \mid H_1)$ над $\mathbb{F}_2$ размера 1×2 двоичного линейного $[n, k]$-QC-MDPC-кода $\mathcal{C}$, причём $|H_0| = |H_1| = \frac{w}{2}$. Благодаря изоморфизму между кольцом циркулянтных матриц размера $r \times r$ и кольцом многочленов $\mathcal{R}$ все матричные операции могут быть рассмотрены как операции над многочленами. Открытым ключом является секретный ключ в каноническом виде, а именно: $H_{\text{pub}} = \left(\mathbb{I} \mid H_0^{-1} H_1\right)$.

В основе процедуры шифрования лежит схема Нидеррайтера. Исходное сообщение представляет собой вектор e веса t, а соответствующим шифртекстом является $H_{\text{pub}} e^\top$. Расшифрование выполняется с помощью умножения шифртекста на блок H_0, чтобы получить синдром $He^\top$, а далее для восстановления e используется black-grey-flip-декодер с переключением битов [14].

Безопасность IND-CPA, лежащая в основе схемы BIKE, базируется на сложности решения следующих задач.

Задача квазициклического синдромного декодирования (QCSD)**.** *Для заданного $h \in \mathcal{R}$, вектора $y \in \mathcal{R}$ и параметра $t > 0$ определить, существует ли пара $(e_0, e_1) \in \mathcal{R}^2$ такая, что $wt_H(e_0) + wt_H(e_1) = t$ и $e_0 + e_1 h = y$.*

Задача поиска квазициклического кодового слова (QCCF)**.** *Для заданного $h \in \mathcal{R}$ и параметра $v > 0$ определить, существует ли пара $(c_0, c_1) \in \mathcal{R}^2$ такая, что $wt_H(c_0) + wt_H(c_1) = v$ и $c_0 + c_1 h = 0$.*

Считается, что вес $wt_H(h)$ нечётный, а $wt_H(y) = t$. Наиболее известными алгоритмами для решения этих задач являются декодирование на основе информационных совокупностей и его вариации. Чтобы обеспечить λ бит защиты в смысле IND-CPA, сложность обеих задач QCSD и QCCF должна превышать 2λ. В [15] показано, что параметры BIKE для каждого уровня стойкости выбираются согласно условию

$$\lambda \approx t - \frac{1}{2}\log_2 r \approx w - \log_2 r.$$

Безопасность IND-CCA обеспечивается с помощью использования преобразования Фуджисаки — Окомото [16]

Классическая схема Мак-Элиса. Эта схема на основе двоичных кодов Гоппы использует стандартные методы для достижения надёжности в смысле IND-CCA.

Использование классической схемы Мак-Элиса гарантирует доказательство безопасности IND-CCA2 в модели квантового оракула [17], основанной на предположении, что схема обеспечивает одностороннюю защиту при атаках на выбранный открытый текст. В качестве альтернативы стойкость схемы может быть обеспечена благодаря предположениям, что проверочная матрица двоичного кода Гоппы неотличима от проверочной матрицы случайного линейного кода такой же размерности, а задача синдромного декодирования сложна для случайных линейных кодов такой же размерности, что и используемый код.

Наиболее эффективной из известных атак на классическую схему Мак-Элиса является декодирование на основе информационных совокупностей. Попытки найти секретный ключ с помощью алгебраического криптоанализа или перебором являются более дорогостоящими.

Квазициклическая схема Хэмминга. HQC (Hamming quasi-cyclic) — схема на основе QC-MDPC-кодов без скрытой структуры [18].

Основная идея заключается в извлечении выгоды из квазициклической структуры наряду со снижением стойкости при декодировании случайного линейного кода. В частности, трудно свести обеспечение стойкости кодовой схемы к сложности решения общей задачи декодирования, если открытым ключом является замаскированный секретный ключ с применением скремблирования или перестановки.

Рассмотрим кольцо $\mathcal{R} = \mathbb{F}_2[X]/(X^p - 1)$, где p простое. Секретный ключ представляет собой случайно выбранную пару $(x, y) \in \mathcal{R}^2$, а открытый ключ — пару $(h, s = x + hy)$, где $h \in \mathcal{R}$ выбирается случайным образом и используется для построения порождающей матрицы $G \in \mathbb{F}_2^{k \times n}$ кода. Поскольку секретный ключ генерируется независимо от кода, в самом коде нет скрытой структуры. Проверочная матрица открыта, что позволяет редуцировать уровень безопасности независимо от алгоритма декодирования, используемого в расшифровании.

Чтобы зашифровать сообщение $m \in \mathbb{F}_2^k$, необходимо выбрать случайным образом три элемента $e, r_1, r_2 \in \mathcal{R}$ подходящего веса. Тогда зашифрованный текст представляет собой пару $(u, v) = (r_1 + hr_2, mG + sr_2 + e)$. Для расшифрования шифртекста необходимо применить алгоритм декодирования для вектора $v - uy$. Декодер, лежащий в основе схемы HQC, представляет собой конкатенацию кодов Рида — Соломона и Рида — Маллера [19].

Безопасность схемы HQC в смысле IND-CPA зависит от сложности решения задачи QCSD. Декодер, используемый в схеме HQC, имеет корректно определённое минимальное расстояние d и, следовательно, может исправить до $t = \lfloor \frac{d-1}{2} \rfloor$ ошибок. Вероятность того, что зашифрованный текст содержит вектор ошибки e и $wt_H(e) > t$, используется для получения верхней границы частоты сбоев процедуры расшифрования. Как и в случае с другими кодовыми схемами, наиболее известные атаки на HQC представляют собой декодирование на основе информационных совокупностей и его модификации. Безопасность IND-CCA обеспечивается с помощью использования преобразования Фуджисаки — Окомото.

В табл. 1 приведён сравнительный анализ актуальных криптосистем: классической схемы Мак-Элиса, BIKE и HQC; все представлены с уровнями стойкости 1, 3 и 5.

Таблица 1

Размеры ключа и зашифрованного текста для актуальных KEM схем (в байтах)

Схема	Уровень стойкости	Открытый ключ	Закрытый ключ	Шифр-текст
McEliece348864	1	261 120	6492	128
McEliece460896	3	524 160	13 608	188
McEliece6688128	5	104 992	13 932	240
McEliece6960119	5	1 047 319	13 948	226
McEliece8192128	5	1 357 824	14 120	240
BIKE	1	1540	280	1572
	3	3082	418	3114
	5	5122	580	5154
HQC-128	1	2249	40	4481
HQC-192	3	4522	40	9026
HQC-256	5	7245	40	14 469

2. Изогении

2.1. Предварительные сведения. *Эллиптической кривой* над полем $\mathbb{F}$ называется гладкая кривая E, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. Условие гладкости означает, что кривая не имеет сингулярных точек, т. е. точек, в которых обе частные производные функции $y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ равны нулю. Если характеристика поля $\mathbb{F}$ не равна 2 или 3, то кривую можно привести (изоморфным преобразованием) к *краткой форме Вейерштрасса*

$$y^2 = x^3 + a\ x + b.$$

Множество точек кривой E вместе с бесконечно удалённой точкой $\mathcal{O}$ обозначается через $E(\mathbb{F})$. Заметим, что кривая может быть задана над одним полем $\mathbb{F}$ (т. е. коэффициенты a_1, a_2, a_3, a_4, a_6 или a, b лежат в $\mathbb{F}$), но при этом точки кривой можно брать над некоторым его расширением, например, алгебраическим замыканием $\overline{\mathbb{F}}$. Такие точки получаются из решений уравнения кривой над алгебраическим замыканием поля или — в общем случае — над расширением поля. Множество точек кривой E (заданной над $\mathbb{F}$), которые имеют координаты из поля $\overline{\mathbb{F}}$, обозначается через $E(\overline{\mathbb{F}})$. На множестве $E(\mathbb{F})$ по известным формулам задаётся групповая операция, называемая сложением (см., например, [20, § 13.1] или [21, § 2.2.2]). При этом бесконечно удалённая точка является нейтральным элементом группы точек. Операцию сложения точки с самой собой ℓ раз будем обозначать через $[\ell]$, а результат её применения к точке $P \in E(\mathbb{F})$ — через $[\ell]P$.

Порядком точки $P \in E(\mathbb{F})$ называется наименьшее натуральное число $\operatorname{ord} P$, при котором $[\operatorname{ord} P]P = \mathcal{O}$. Множество точек

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}) \mid [\ell]P = \mathcal{O}\}$$

образует подгруппу $E[\ell] \subset E(\overline{\mathbb{F}})$, которая называется *подгруппой ℓ-кручения кривой*. Это множество всех точек кривой (с координатами из алгебраического замыкания поля), чей порядок делит ℓ.

Эллиптическая кривая E над конечным полем $\mathbb{F}_q$, где $q = p^n$ — степень простого p, называется *суперсингулярной*, если $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$.

Изогенией двух эллиптических кривых E_1, E_2 над одним и тем же полем $\mathbb{F}$ называется ненулевой гомоморфизм эллиптических кривых, задаваемый рациональными отображениями. Заметим, что в литературе также встречаются другие эквивалентные определения:

1) гомоморфизм кривых E_1 и E_2, который над замыканием поля $\mathbb{F}$ сюръективен и имеет конечное ядро;

2) сюръективный морфизм кривых, отображающий единицу группы точек E_1 в единицу группы точек E_2.

Данные определения получаются из соответствующих определений для более общих объектов — проективных кривых и абелевых многообразий, поэтому они сильно упрощаются в частном случае — случае эллиптических кривых.

Явно изогении задаются в виде рациональных функций:

$$\varphi\colon (x, y) \mapsto \left(\frac{f_1(x, y)}{f_2(x, y)}, \frac{g_1(x, y)}{g_2(x, y)}\right)$$

для некоторых $f_1, f_2, g_1, g_2 \in \mathbb{F}[x, y]$. Используя замену $y^2 \mapsto x^3 + a\,x + b$, изогению можно привести [22, лемма 4.26] к виду

$$\varphi\colon (x,y) \mapsto \left(\frac{u(x)}{v(x)}, \frac{s(x)y}{t(x)}\right),$$

где $u, v, s, t \in \mathbb{F}[x]$. Такая форма изогении называется стандартной. *Степень* изогении определяется как $\deg\varphi = \max(\deg u, \deg v)$. Изогения называется *сепарабельной*, если производная $\frac{u}{v}$ по x не равна 0, и *несепарабельной* в противном случае. Для сепарабельных изогений выполняется условие $\deg\varphi = |\ker\varphi|$, где $\ker\varphi = \{P \in E_1(\overline{\mathbb{F}}) \mid \varphi(P) = \mathcal{O}_{E_2}\}$.

Кривые, между которыми существует изогения степени ℓ, называются *ℓ-изогенными*. Имея подгруппу $G \subseteq E_1(\overline{\mathbb{F}}_q)$, можно построить изогению степени $\ell = |G|$ и уравнение соответствующей изогенной кривой E_2, используя формулы Велу [23]. Кривая E_2, построенная по подгруппе G группы точек кривой E_1, обозначается также через E_1/G и называется *фактор-кривой* E_1 по модулю G. Для каждой изогении $\varphi\colon E_1 \to E_2$ существует изогения $\widehat{\varphi}\colon E_2 \to E_1$ такая, что $\widehat{\varphi} \circ \varphi = [\deg\varphi]$, называемая *дуальной*.

Для описания атаки Кастрика и Декру на схему SIDH в последующих разделах нам потребуется выйти за пределы эллиптических кривых к более общим объектам — абелевым многообразиям.

Абелевым многообразием называется группа, образованная множеством решений системы уравнений, составленной из однородных многочленов от нескольких переменных, при выполнении условий:

1) групповой закон задаётся рациональными отображениями, определёнными во всех точках;

2) данное множество является неприводимым многообразием, т. е. оно не может быть представлено в виде объединения двух множеств, которые являются множествами решений систем уравнений, составленных из однородных многочленов.

Размерность абелева многообразия определяется как размерность соответствующей системы уравнений. Эллиптическая кривая представляет собой абелево многообразие размерности 1 (строго говоря, абелевым многообразием является множество $E(\mathbb{F})$, которое содержит в себе бесконечно удалённую точку; для её явного определения требуется переход к проективным координатам и задание кривой однородным многочленом). Абелево многообразие размерности 2 называется *абелевой поверхностью*. Есть два типа абелевых поверхностей — произведение двух эллиптических кривых и якобианы кривых рода 2 (определение якобиана кривой рода 2 и его свойства можно найти в [24]). Первый случай часто можно свести ко второму методом склейки двух эллиптических кривых в якобиан кривой рода 2. Случаи, когда склейку невозможно осуществить, относительно редки, их классификация приведена в работе [25]. Соответствующие теоремы лежат в основе атаки Кастрика — Декру. Так же, как и для случая эллиптических кривых, подгруппе G

абелева многообразия A можно поставить в соответствие некоторую изогению с ядром G в другое абелево многообразие A/G, которое называется *фактор-многообразием* по подгруппе G. Однако в общем случае формулы и алгоритмы для вычисления изогений и фактор-многообразий (аналоги формул Велу) достаточно громоздки, поэтому, как правило, на практике ограничиваются якобианами кривых, что накладывает дополнительные ограничения на выбор подгруппы G (необходимо выбирать максимальные изотропические подгруппы, подробнее см. в [26]). В случае якобианов задача построения фактор-многообразия и изогении сильно упрощается: например, в случае изогений степени 2 есть явные формулы Ришело [27, утверждение 1], которых достаточно для получения секретного ключа одного из участников в протоколе SIDH/SIKE.

2.2. Построение криптосистем на действиях групп. Пусть X — некоторое множество, а G — группа. Будем говорить, что G действует на множестве X, если задано отображение $* : G \times X \to X$ такое, что для любых $g_1, g_2 \in G$ и $x \in X$ выполняется $g_1 * (g_2 * x) = (g_1 g_2) * x$.

В терминах действия группы можно описать многие схемы шифрования с открытым ключом, протоколы распределения и инкапсуляции ключа (key encapsulation mechanism, KEM) [28]. При этом действие группы должно обладать некоторым криптографическим («трудновычислимым») свойством, как например, следующие:

• группа G действует как односторонняя функция, т. е. для любых $x_1, x_2 \in X$ нахождение элемента $g \in G$ такого, что $x_1 = g * x_2$, является трудной задачей (даже в предположении, что такой элемент существует);

• действие группы обладает свойством псевдослучайного генератора, т. е. для случайно выбранного элемента $g \in G$ злоумышленник не может отличить множество принятых векторов $\{(x_i, g * x_i)\}_{i \in I}$ от множества векторов вида $\{(x_i, u_i)\}_{i \in I}$, где u_i, $i \in I$, — равномерно распределённые на X случайные величины.

Например, опишем в терминах действия группы на множестве широко известный алгоритм обмена ключами (выработки общего секрета) Диффи — Хеллмана. В качестве пространства открытых ключей выберем некоторую группу большого простого порядка $X = \mathbb{Z}_p = \langle x \rangle$. На множестве X определим действие мультипликативной группы $G = \mathbb{Z}_p^*$ как отображение $*\colon G \times X \to X\colon z * h \mapsto h^z$. Генерация общего секретного ключа происходит следующим образом.

1. Пользователь A выбирает секретный ключ $a \in G$ и вычисляет его действие на образующем элементе $x \in X$. Полученное значение $a * x = x^a$ является открытым ключом и отправляется пользователю B.

2. Пользователь B выбирает секретный ключ $b \in G$, вычисляет с помощью действия группы открытый ключ $b * x = x^b$ и отправляет его пользователю A.

После этого каждый пользователь действует своим секретным ключом $a \in G$ или $b \in G$ на полученное значение $b*x$ или $a*x$ соответственно, получая общий секрет $a*(b*x) = b*(a*x) = x^{ab} \in X$.

В данном примере группа G действует как односторонняя функция. В самом деле, злоумышленник знает пары значений $(x, a*x)$, $(x, b*x) \in X \times X$, однако нахождение по ним элементов $a \in G$, $b \in G$ является трудной задачей, так как по сути это задача дискретного логарифмирования в $\mathbb{Z}_p^*$ (discrete logarithm problem, DLP).

2.3. Схема SIDH/SIKE. Схема SIDH (supersingular isogeny Diffie — Hellman), предложенная в 2011 г. де Фео, Яо и Плутом [29], представляет собой протокол обмена ключами, аналогичный протоколу Диффи — Хеллмана, где в качестве X используется множество суперсингулярных эллиптических кривых над конечным полем, а элементы $\varphi_A, \varphi_B \in G$ — изогении суперсингулярных кривых. Схема уязвима к атаке Кастрика — Декру, описанной в п. 2.5, и вследствие этого небезопасна. Кратко опишем саму схему обмена ключами SIDH.

Публичные параметры схемы:

• простое число $p = \ell_A^{e_A} \ell_B^{e_B} c \pm 1$, где ℓ_A, ℓ_B — малые простые, c — фиксированный дополнительный множитель, как правило, малый;

• E — суперсингулярная кривая над $\mathbb{F}_{p^2}$ с числом рациональных точек, равным $|E(\mathbb{F}_{p^2})| = \left(\ell_A^{e_A} \ell_B^{e_B} c\right)^2$.

Открытый ключ:

A: (P_A, Q_A) — базис подгруппы точек $E\left[\ell_A^{e_A}\right] \subseteq E(\mathbb{F}_{p^2})$;

B: (P_B, Q_B) — базис подгруппы $E\left[\ell_B^{e_B}\right] \subseteq E(\mathbb{F}_{p^2})$.

Секретный ключ:

A: $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$; изогения $\varphi_A \colon E \to E_A$, заданная своим ядром $\ker \varphi_A = \langle [m_A]P_A + [n_A]Q_A \rangle$.

B: $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$; изогения $\varphi_B \colon E \to E_B$, заданная своим ядром $\ker \varphi_B = \langle [m_B]P_B + [n_B]Q_B \rangle$.

Схема обмена ключами SIDH следующая.

1. Пользователь A выбирает случайным образом секретные параметры $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ (не должны делиться на ℓ_A одновременно), которые определяют изогению φ_A. Затем вычисляет образы базисных точек $\varphi_A(P_B), \varphi_A(Q_B)$ и отправляет их пользователю B вместе с кривой E_A.

2. Пользователь B выбирает случайным образом секретные параметры $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ (не должны делиться на ℓ_B одновременно), которые определяют изогению φ_B. Затем вычисляет образы базисных точек $\varphi_B(P_A), \varphi_B(Q_A)$ и отправляет их пользователю A вместе с кривой E_B.

3. Пользователь A вычисляет изогению $\varphi'_A \colon E_B \to E_{AB}$, которая определяется своим ядром $\ker \varphi'_A = \langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$.

4. Пользователь B вычисляет аналогично изогению $\varphi'_B\colon E_A \to E_{BA}$.

В итоге пользователи A и B имеют кривые E_{AB} и E_{BA} соответственно, связанные изогенией $E_{AB} = \varphi'_B(\varphi_A(E)) \cong \varphi'_A(\varphi_B(E)) = E_{BA}$. В качестве общего секретного ключа можно использовать j-инварианты [20, § 13.1] этих кривых, так как $j(E_{AB}) = j(E_{BA})$.

SIKE — протокол инкапсуляции ключа (KEM), предложенный к стандартизации в NIST в качестве алгоритма, устойчивого к квантовым атакам. Конструкция протокола вполне повторяет схему SIDH, дополняя её выбором конкретных «стандартных» параметров и рядом технических модификаций, позволяющих использовать SIDH для инкапсуляции ключа. После публикации атаки [30] протокол считается небезопасным.

2.4. Схема CSIDH. Схема CSIDH (commutative supersingular isogeny Diffie — Hellman) — ещё один протокол обмена ключами, безопасность которого основана на сложности нахождения изогении между двумя суперсингулярными кривыми. Конструкция схемы основана на криптосистеме Ростовцева — Столбунова, однако вместо обычных эллиптических кривых используются суперсингулярные эллиптические кривые. Кроме того, в отличие от схемы SIDH в CSIDH используется действие коммутативной группы. Впервые протокол CSIDH описан в 2018 г. Кастриком, Ланге и др. [31], впоследствии опубликовано множество его технических оптимизаций [32].

Теорема (форма Монтгомери [31, утверждение 8]). *Пусть $\mathbb{F}_p$ — конечное поле характеристики $p \equiv 3 \pmod 8$, E — суперсингулярная кривая над $\mathbb{F}_p$. Тогда кольцо эндоморфизмов кривой имеет вид* $\operatorname{End}(E) = \mathbb{Z}[\pi_p]$ *в том и только том случае, когда существует единственный элемент $A \in \mathbb{F}_p$ такой, что $E \simeq \widetilde{E}\colon y^2 = x^3 + Ax^2 + x$, где $\pi_p(x, y) = (x^p, y^p)$ — эндоморфизм Фробениуса.*

Кривая $\widetilde{E}$, удовлетворяющая условиям теоремы, называется *формой Монтгомери* эллиптической кривой, а элемент $A \in \mathbb{F}_p$ — *коэффициентом Монтгомери*. Обозначим через $\mathcal{E}\ell\ell_p(\mathbb{Z}[\pi_p])$ множество эллиптических кривых, удовлетворяющих вышеперечисленным условиям, т. е. допускающих представление в форме Монтгомери.

Конструкция схемы CSIDH основана на действии *группы классов идеалов* $G = \operatorname{Cl}(\mathbb{Z}[\pi_p])$ на множестве $X = \mathcal{E}\ell\ell_p(\mathbb{Z}[\pi_p])$ эллиптических кривых, определённых над полем $\mathbb{F}_p$ и имеющих кольцо эндоморфизмов, изоморфное $\mathbb{Z}[\pi_p]$. Определение и базовые свойства группы классов идеалов описаны в [33, разд. 4.9].

Действие класса идеалов $\bigl[\prod_i \mathfrak{l}_i^{e_i}\bigr] \in G$ на кривую $E \in X$ вычисляется следующим образом. Так как $\pi^2 = -p \equiv 1 \pmod{\ell_i}$, собственные

значения действия эндоморфизма Фробениуса на все подгруппы ℓ_i-кручения равны $\lambda_i = \pm 1$. Следовательно, для вычисления действия каждого из классов $[\mathfrak{l}_i]$ можно найти все $\mathbb{F}_p$-рациональные (или $\mathbb{F}_{p^2}$-рациональные в случае собственного значения $\lambda_i = -1$) точки порядка ℓ_i и применить к ним формулы Велу. Более подробно этот алгоритм описан в [31, § 3]. Кратко опишем схему обмена ключами CSIDH.

Публичные параметры схемы:

• простое число $p = 4\ell_1 \cdots \ell_n - 1$, где $\ell_1, \ldots, \ell_n$ — попарно различные малые нечётные простые;

• суперсингулярная эллиптическая кривая $E_0\colon y^2 = x^3 + x$ над $\mathbb{F}_p$.

Схема обмена ключами CSIDH следующая.

1. Пользователь A формирует целочисленный вектор $(e_1, \ldots, e_n) \in \{-m, \ldots, m\}^n$, после чего определяет класс идеалов $[\mathfrak{a}] = \left[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}\right] \in \mathrm{Cl}(\mathbb{Z}[\pi_p])$, где $m > 0$ — наименьшее целое число такое, что $2m + 1 \geqslant \sqrt[n]{|\mathrm{Cl}(\mathbb{Z}[\pi_p])|}$,

$$[\mathfrak{l}_i] = [(\ell_i, \pi_p - 1)], \quad [\mathfrak{l}_i]^{-1} = [(\ell_i, \pi_p + 1)].$$

Далее пользователь вычисляет действие $[\mathfrak{a}] * E_0$, приводит уравнение полученной кривой к форме Монтгомери $E_A\colon y^2 = x^3 + Ax^2 + x$. Полученный коэффициент Монтгомери $A \in \mathbb{F}_p$ является открытым ключом пользователя A, а исходный случайный вектор $(e_1, \ldots, e_n)$ — секретным ключом.

2. Пользователь B формирует целочисленный вектор $(e_1, \ldots, e_n) \in \{-m, \ldots, m\}^n$, затем определяет класс $[\mathfrak{b}] = \left[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}\right] \in \mathrm{Cl}(\mathbb{Z}[\pi_p])$. Пользователь вычисляет действие $[\mathfrak{b}] * E_0$, приводит уравнение полученной кривой к форме Монтгомери $E_B\colon y^2 = x^3 + Bx^2 + x$. Полученный коэффициент Монтгомери $B \in \mathbb{F}_p$ является открытым ключом пользователя B, а исходный случайный вектор $(e_1, \ldots, e_n)$ — секретным ключом.

В итоге пользователи A и B имеют ключевые пары $([\mathfrak{a}], A)$ и $([\mathfrak{b}], B)$ соответственно. Пользователь A действует своим секретным ключом $[\mathfrak{a}]$ на принятую кривую E_B и получает $[\mathfrak{a}] * E_B = [\mathfrak{a}][\mathfrak{b}]E_0$. Пользователь B действует симметрично. В качестве общего секретного ключа может выступать коэффициент Монтгомери общей кривой $[\mathfrak{a}][\mathfrak{b}]E_0$.

В отличие от схемы SIDH схема CSIDH не использует значения секретных изогений в точках, и поэтому атака Кастрика — Декру её не затрагивает.

2.5. Атака Кастрика — Декру. Протокол обмена ключами SIDH использует в своей работе образы $\varphi_B(P_A)$, $\varphi_B(Q_A)$, $\varphi_A(P_B)$, $\varphi_A(Q_B)$ открытых ключей участников протокола под действием секретных изогений Алисы φ_A и Боба φ_B. Открытые ключи (P_A, Q_A) и (P_B, Q_B) являются образующими групп $E\left[\ell_A^{e_A}\right] = \langle P_A, Q_A \rangle$ и $E\left[\ell_B^{e_B}\right] = \langle P_B, Q_B \rangle$.

Долгое время считалось, что эта дополнительная информация не позволяет взломать криптосистему. Однако в августе 2022 г. Кастрик и Декру опубликовали препринт [30], в котором описывается полиномиальная атака на криптосистему SIKE — версию SIDH-кандидата на стандартизацию NIST. Атака была рассчитана на использование начальной кривой из параметров SIKE. В [34] параллельно работающие в том же направлении Майно и Мартиндейл представили вариант атаки для любой начальной кривой. Изначально доказательство полиномиальности атаки в указанных работах основывалось на эвристиках. Этот недостаток был устранён Робером в [35], где было доказано, что атака занимает классическое детерминированное полиномиальное время. В этом пункте приведём описание атаки Кастрика — Декру и её последствий.

Пусть $B = \langle [m_B]P_A + [n_B]Q_A \rangle$ — секретное ядро изогении Боба, по которому с помощью формул Велу можно построить секретную изогению φ_B и получить открытые параметры Боба: уравнение кривой E/B и пару $(\varphi_B(P_A),\ \varphi_B(Q_A))$. Тогда в строгом виде задача восстановления ключа в SIDH формулируется следующим образом: по известной четвёрке $(E, E/B, \varphi_B(P_A),\ \varphi_B(Q_A))$ восстановить φ_B.

Изогения φ_B имеет степень $\ell_B^{e_B}$ и представляет собой композицию изогений степени ℓ_B, т. е. $\varphi_B = \varphi_{e_B} \circ \cdots \circ \varphi_1$, тем самым имеется цепочка изогений

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \ldots \xrightarrow{\varphi_{e_B}} E/B.$$

Изогении φ_i имеют степень ℓ_B, причём для криптосистем это число ℓ_B выбирается малым ($\ell_B = 3$ в SIKE), поэтому и количество возможных вариантов для φ_i мало. Точнее, так как $\ker \varphi_i$ — подгруппа $E_{i-1}[\ell_{e_B}] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, всего имеется ℓ_B^2 вариантов для выбора φ_i. Имея эффективно (за полиномиальное время) вычисляемый критерий для определения правильного варианта, можно последовательно перебирать все варианты для определения φ_1, затем, найдя φ_1, перейти к перебору вариантов для изогении φ_2 и т. д., пока не получим φ_{e_B}. До работы Кастрика и Декру такого эффективного критерия известно не было. Кастрик и Декру предложили использовать в качестве такого критерия теорему Кани [25, теорема 2.8] и изогении абелевых поверхностей для проверки её выполнения. Для формулировки теоремы и её применения в качестве критерия нам потребуется ввести несколько дополнительных определений.

Определение 1. *Алмазной изогенной конфигурацией степени N* называется тройка (φ, G_1, G_2) такая, что

(1) $\varphi\colon E' \to E''$ — изогения;
(2) $G_1, G_2 \subseteq \ker \varphi$;
(3) $\deg \varphi = |G_1| \cdot |G_2|$;
(4) $N = |G_1| + |G_2|$ и $G_1 \cap G_2 = \{0\}$.

Подгруппа $\langle R_1, R_2\rangle$ группы $E' \times E''$ такая, что $|R_1| = |R_2| = N$ (другими словами, (N, N)-подгруппа), называется *разложимой*, если фактор-поверхность $(E' \times E'')/\langle R_1, R_2\rangle$ изоморфна декартову произведению двух эллиптических кривых. В противном случае подгруппа называется *неразложимой*, и фактор-поверхность $(E' \times E'')/\langle R_1, R_2\rangle$ в этом случае изоморфна якобиану кривой рода 2. Атака Кастрика — Декру основана на том факте, что первый случай очень редко встречается по сравнению со вторым. Теорема Кани описывает данный редкий случай, она утверждает (в упрощённом виде), что (N, N)-подгруппа разложима тогда и только тогда, когда она получается из некоторой алмазной изогенной конфигурации степени N. Точнее,

$$\langle R_1, R_2\rangle = \langle (P, [x]\varphi(P)), (Q, [x]\varphi(Q))\rangle$$

для некоторого целого x и некоторых P, Q таких, что $E'[N] = \langle P, Q\rangle$.

Теорема Кани может быть применена для нахождения φ_1 методом «вписывания» изогении $\varphi'_B = \varphi_{e_B} \circ \cdots \circ \varphi_2$ в некоторую алмазную конфигурацию степени ℓ^{e_A} (напомним, что общий секретный ключ в SIDH получается из композиции секретных изогений степени $\ell_A^{e_A}$ и $\ell_B^{e_B}$), чтобы гарантировать, что при правильном выборе изогении φ_1 теорема Кани выполняется, т. е. соответствующая фактор-группа разложима, а при всех остальных выборах φ_1 получаются (в подавляющем большинстве случаев) неразложимые группы.

Предположим, что φ'_1 — один из возможных вариантов для φ_1 и $E'_1 = E/\ker\varphi_1$ (если $\varphi'_1 = \varphi_1$, то $E_1 = E'_1$). Для построения алмазной изогенной конфигурации подбирается вспомогательная изогения γ степени $\ell^{e_A} - \ell^{e_B - 1}$ (подойдёт любая изогения такой степени) из кривой E'_1 в некоторую эллиптическую кривую C (в качестве γ можно взять подходящий эндоморфизм, тогда $C \simeq E'_1$). При правильном выборе φ'_1, т. е. когда $\varphi'_1 = \varphi_1$, тройка $(\varphi'_B \circ \widehat{\gamma}, \ker\widehat{\gamma}, \gamma(B))$, где $\varphi'_B = \varphi_{e_B} \circ \cdots \circ \varphi_2$ — алмазная конфигурация степени $\ell_A^{e_A}$ и подгруппа

$$G = \langle (\gamma(\varphi'_1(P_A)), \varphi_B(P_A)), (\gamma(\varphi'_1(Q_A)), \varphi_B(Q_A))\rangle \subseteq C \times E/B$$

разложима по теореме Кани. Тем самым при неправильном выборе φ'_1 подгруппа неразложима и соответствующая фактор-поверхность является якобианом кривой рода 2.

Отсюда получается следующий метод для определения φ_1.

1. Выбрать φ'_1.

2. Построить для некоторой эллиптической кривой C вспомогательную изогению $\gamma\colon E'_1 \to C$ степени $\ell_A^{e_A} - \ell_B^{e_B - 1}$.

3. Шаг склейки. Построить фактор-поверхность A произведения $C \times E/B$ по подгруппе

$$G = \langle (\gamma(\varphi'_1(P_A)), \varphi_B(P_A)), (\gamma(\varphi'_1(Q_A)), \varphi_B(Q_A))\rangle.$$

4. Шаг разложения. Определить, изоморфна фактор-поверхность произведению двух эллиптических кривых или нет. Если изоморфна, то $\varphi_1' = \varphi_1$, в противном случае перейти к шагу 1.

После нахождения φ_1 данный метод можно применить и для нахождения φ_2, выбрав в качестве γ изогению степени $\ell_A^{e_A} - \ell_B^{e_B - 2}$, а затем аналогичным образом — для нахождения всех остальных φ_i, и получить на выходе секретную изогению φ_B. Рассмотрим подробнее шаги метода.

Выбор φ_1'. Выбирается подгруппа $E[\ell_B]$, затем по формулам Велу строятся изогения φ_1' и уравнение для кривой $E/\ker\varphi_1'$. Всего возможных выборов ℓ_B^2, так как $E[\ell_B] \simeq (\mathbb{Z}/\ell_B\mathbb{Z})^2$.

Построение вспомогательной изогении γ. Предположим, что надо найти φ_i. Тогда на этом шаге необходимо построить произвольную изогению γ степени $c = \ell_A^{e_A} - \ell_B^{e_B - i}$. В случае, если c гладкое, т. е. раскладывается на малые простые числа размера $(\log p)^{O(1)}$, это можно сделать с помощью формул Велу. В случае наличия у кривой эндоморфизма η малой нормы можно также использовать факторизацию c в $\mathbb{Z}[\eta]$.

Например, кривая $y^2 = x^3 + x$ имеет автоморфизм $\eta\colon (x, y) \mapsto (-x, iy)$. В этом случае можем найти с помощью алгоритма Корначчи [33, алгоритм 1.5.2] целые числа u, v такие, что $c = u^2 + v^2$ и $c = (u + iv)(u - iv)$. Тогда в качестве γ можно взять $u + iv\colon P \mapsto [u]P + [v]\eta(P)$. Аналогично можно построить γ для кривой $y^2 = x^3 + 6x^2 + x$ из SIKE, найдя представление $c = u^2 + 4v^2 = (u + 2iv)(u - 2iv)$.

Шаг склейки. Подгруппа G изоморфна $(\mathbb{Z}/\ell^{e_A}\mathbb{Z})^2$, поэтому построение фактор-поверхности $(C \times E/B)/G$ можно свести к построению цепочки изогений степени ℓ_A с ядрами, изоморфными $(\mathbb{Z}/\ell^{e_A}\mathbb{Z})^2$ (т. е. (ℓ_A, ℓ_A)-изогений), которая ведёт в целевую фактор-поверхность $(C \times E/B)/G$. Чтобы построить такую цепочку, кривые C и E/B сначала «склеиваются» в якобиан J_H кривой H рода 2. Другими словами, строится такая кривая H, что $J_H \sim C \times E/B$. Для $\ell_A = 2$, как в SIKE, это можно сделать с помощью формул Хау — Лепревоста — Пунена [36]. Затем после нахождения J_H итоговая фактор-поверхность A строится по цепочке изогений якобианов кривых рода 2 степени ℓ_A^2. Для случая $\ell_A = 2$ такие изогении и соответствующие им уравнения кривых рода 2 можно построить с помощью формул Ришело. Для $\ell_A = 3$ можно использовать формулы [37]. Для общего случая можно использовать алгоритмы из работ [38, 39].

Шаг разложения. Данный шаг можно объединить с шагом склейки, так как определение, является ли итоговая абелева поверхность произведением эллиптических кривых, осуществляется при попытке построения якобиана кривой на последнем шаге цепочки изогений степени ℓ_A.

В случае произведения эллиптических кривых кривой с таким якобианом не существует и будет получена ошибка. Например, для $\ell_A = 2$ появится деление на нуль при вычислении формул Ришело.

2.6. Перспективы. В атаке Кастрика — Декру используется информация о действии секретной изогении на базисы групп кручения, и применить её напрямую к общей задаче вычисления изогении между двумя заданными эллиптическими кривыми не получится, поэтому схемы из [31, 40], не использующие данную информацию, остаются стойкими к атаке.

В табл. 2 представлены параметры для актуальных схем на изогениях. Для схемы CRS (Кувейна — Ростовцева — Столбунова) указаны размеры параметров, предложенные в [41, § 4, табл. 3]. Для схемы OSIDH указаны размеры ключей, предложенные в недавней статье [42, § 5.2] по криптоанализу данной схемы.

Таблица 2

Размеры ключей для актуальных схем обмена ключами на изогениях (в байтах)

Схема	Уровень стойкости	Открытый ключ	Закрытый ключ	Общий ключ
CRS [41]	128/56	64	8	64
OSIDH [43]	128/128	36	31	36
CSIDH-512	128/62	64	32	64

Заметим, что указанные схемы на изогениях, несмотря на небольшие размеры ключей, достаточно медленные и для использования на практике требуют оптимизации.

Переход к кривым рода 2. Для обхода атаки Кастрика — Декру можно было бы рассмотреть кривые рода 2. Например, в [26] предложен соответствующий вариант схемы SIDH. Однако в этом случае используются суперсингулярные кривые рода 2, которые изогенны декартовому произведению суперсингулярных эллиптических кривых, значит, можно ожидать адаптации атаки Кастрика — Декру и к этому случаю. Использование же несупресингулярных кривых ведёт к субэкспоненциальным квантовым атакам из-за коммутативности кольца эндоморфизмов якобиана кривой.

Заключение

Постквантовая криптография на изогениях и кодах представляет собой перспективную область исследований с большим числом открытых проблем. В представленной статье приведён обзор основных подходов к построению постквантовых криптосистем на основе кодов и изогений,

а также вычислительно трудных задач, лежащих в основе их стойкости. В случае кодов с учётом размеров открытого и закрытого ключей классическая схема Мак-Элиса существенно проигрывает и схеме BIKE, и схеме HQC. Несмотря на то, что схема HQC обеспечивает надёжные гарантии безопасности, а также разумную частоту отказов при расшифровании, она проигрывает BIKE относительно размеров открытого ключа и зашифрованного текста. Тем самым схема BIKE показала себя вполне конкурентно способной. В случае изогений, несмотря на малый размер ключа, главной проблемой остаётся медленная скорость работы схем. Атака Кастрика — Декру вывела из рассмотрения наиболее перспективную с точки зрения практики схему SIDH/SIKE и все схемы, для оптимизации которых использовались значения изогении в точках кручения. Таким образом, наиболее важным направлением исследований в области изогений является исследование вопросов оптимизации имеющихся схем.

Финансирование работы

Работа первого, третьего и четвёртого авторов выполнена при поддержке Северо-западного центра математических исследований им. С. Ковалевской (Балтийский федеральный университет им. И. Канта) в рамках соглашения с Министерством науки и высшего образования Российской Федерации (соглашение № 075–02–2023–934). Работа второго, пятого, шестого, седьмого и восьмого авторов выполнена при поддержке Математического центра в Академгородке в рамках соглашения с Министерством науки и высшего образования Российской Федерации (соглашение № 075–15–2022–282).

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Малыгина Е. С., Токарева Н. Н., Куценко А. В.** [и др.]. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решётках // Дискрет. анализ и исслед. операций. 2023. Т. 30, № 4. С. 46–90.
2. **Courtois N. T., Finiasz M., Sendrier N.** How to achieve a McEliece-based digital signature scheme // Advances in cryptology — ASIACRYPT'01. Proc. Int. Conf. Theory and Application of Cryptology (Gold Coast, Australia, Dec. 9–13, 2001). Heidelberg: Springer, 2001. P. 157–174. (Lect. Notes Comput. Sci.; V. 2248).
3. **Stern J.** A new paradigm for public key identification // IEEE Trans. Inf. Theory. 1996. V. 42, No. 6. P. 1757–1768.
4. **Childs A., Jao D., Soukharev V.** Constructing elliptic curve isogenies in quantum subexponential time // J. Math. Cryptology. 2014. V. 8, No. 1. P. 1–29. DOI: 10.1515/jmc-2012-0016.

5. **McEliece R. J.** A public-key cryptosystem based on algebraic coding theory // The deep space network. Progress report 42-44. Pasadena, CA: California Inst. Technol., 1978. P. 114–116.
6. **Niederreiter H.** Knapsack-type cryptosystems and algebraic coding theory // J. Prob. Contr. Inform. Theory. 1986. V. 15, No. 2. P. 159–166.
7. **Niederreiter H., Xing C.** Algebraic geometry in coding theory and cryptography. Princeton, NJ: Princeton Univ. Press, 2009. 272 p.
8. **Minder L., Shokrollahi A.** Cryptanalysis of the Sidelnikov cryptosystem // Advances in cryptology — EUROCRYPT'07. Proc. Int. Conf. Theory and Applications of Cryptographic Techniques (Barcelona, Spain, May 20–24, 2007). Heidelberg: Springer, 2007. P. 347–360. (Lect. Notes Comput. Sci.; V. 4515). DOI: 10.1007/978-3-540-72540-4_20.
9. **Berlekamp E., McEliece R. J., van Tilborg H.** On the inherent intractability of certain coding problems // IEEE Trans. Inf. Theory. 1978. V. 24, No. 3. P. 384–386.
10. **Lee P. J., Brickell E. F.** An observation on the security of McEliece's public-key cryptosystem // Advances in cryptology — EUROCRYPT'88. Proc. Workshop Theory and Application of Cryptographic Techniques (Davos, Switzerland, May 25–27, 1988). Heidelberg: Springer, 1988. P. 275–280. (Lect. Notes Comput. Sci.; V. 330).
11. **Petrank E., Roth R.** Is code equivalence easy to decide? // IEEE Trans. Inf. Theory. 1997. V. 43, No. 5. P. 1602–1604.
12. **Sendrier N.** Finding the permutation between equivalent linear codes: The support splitting algorithm // IEEE Trans. Inf. Theory. 2000. V. 46, No. 4. P. 1193–1203. DOI: 10.1109/18.850662.
13. **Misoczki R., Tillich J.-P., Sendrier N., Barreto P.** MDPC-McEliece: New McEliece variants from moderate density parity-check codes // Proc. IEEE Int. Symp. Information Theory (Istanbul, Turkey, Jul. 7–12, 2013). Los Alamitos, CA: IEEE Comput. Soc., 2013. P. 2069–2073. DOI: 10.1109/ISIT.2013.6620590.
14. **Drucker N., Gueron S., Kostic D.** QC-MDPC decoders with several shades of gray // Post-quantum cryptography. Proc. Int. Conf. (Paris, France, Apr. 15–17, 2020). Cham: Springer, 2020. P. 35–50. (Lect. Notes Comput. Sci.; V. 12100).
15. **Torres R. C., Sendrier N.** Analysis of information set decoding for a sublinear error weight // Post-quantum cryptography. Proc. Int. Conf. (Fukuoka, Japan, Feb. 24–26, 2016). Cham: Springer, 2016. P. 144–161. (Lect. Notes Comput. Sci.; V. 9606).
16. **Fujisaki E., Okamoto T.** Secure integration of asymmetric and symmetric encryption schemes // J. Cryptology. 2013. V. 26. P. 80–101.
17. **Bindel N., Hamburg M., Hövelmanns K., Hülsing A., Persichetti E.** Tighter proofs of CCA security in the quantum random oracle model // Theory of cryptography. Proc. Int. Conf. (Nuremberg, Germany, Dec. 1–5, 2019). Cham: Springer, 2019. P. 61–90. (Lect. Notes Comput. Sci.; V. 11892). DOI: 10.1007/978-3-030-36033-7_3.

18. **Aguilar-Melchor C., Blazy O., Deneuville J.-C., Gaborit P., Zémor G.** Efficient encryption from random quasi-cyclic codes // IEEE Trans. Inf. Theory. 2018. V. 64, No. 5. P. 3927–3943.
19. **Aragon N., Gaborit P., Zémor G.** HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code. Ithaca, NY: Cornell Univ., 2005. (Cornell Univ. Libr. e-Print Archive; arXiv:2005.10741)
20. **Doche C., Lange T.** Arithmetic of elliptic curves // Handbook of elliptic and hyperelliptic curve cryptography. Boca Raton, FL: Chapman & Hall/CRC Press, 2006. P. 267–302.
21. **Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.** Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006.
22. **Sutherland A.** Ellipic curves. Isogenies. Lecture notes. Cambridge, MA: MIT, 2022. Available at `math.mit.edu/classes/18.783/2022/LectureNotes4.pdf` (accessed Dec. 22, 2023).
23. **Vélu J.** Isogénies entre courbes elliptiques // C. R. Acad. Sci. Paris. Sér. A. 1971. V. 273. P. 238-241.
24. **Duquesne S., Lange T.** Arithmetic of hyperelliptic curves //Handbook of elliptic and hyperelliptic curve cryptography. Boca Raton, FL: Chapman & Hall/CRC Press, 2006. P. 303–353.
25. **Kani E.** The number of curves of genus two with elliptic differentials // J. Reine Angew. Math. 1997. V. 485. P. 93-122.
26. **Flynn E. V., Ti Y. B.** Genus two isogeny cryptography // Post-quantum cryptography. Proc. Int. Conf. (Chongquin, China, May 10–12, 2019). Cham: Springer, 2019. P. 286–306. (Lect. Notes Comput. Sci.; V. 11505).
27. **Castryck W., Decru T., Smith B.** Hash functions from superspecial genus-2 curves using Richelot isogenies // J. Math. Cryptology. 2020. V. 14, No. 1. P. 268–292.
28. **Alamati N., de Feo L., Montgomery H., Patranabis S.** Cryptographic group actions and applications. San Diego: Univ. California, 2020. (Cryptology ePrint Archive, Paper ID 2020/1188). Available at `eprint.iacr.org/2020/1188.pdf` (accessed Dec. 22, 2023).
29. **De Feo L., Jao D., Plût J.** Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. San Diego: Univ. California, 2011. (Cryptology ePrint Archive, Paper ID 2011/506). Available at `eprint.iacr.org/2011/506.pdf` (accessed Dec. 22, 2023).
30. **Castryck W., Decru T.** An efficient key recovery attack on SIDH. San Diego: Univ. California, 2022. (Cryptology ePrint Archive, Paper ID 2022/975). Available at `eprint.iacr.org/2022/975.pdf` (accessed Dec. 22, 2023).
31. **Castryck W., Lange T., Martindale C., Panny L., Renes J.** CSIDH: An efficient post-quantum commutative group action. San Diego: Univ. California, 2018. (Cryptology ePrint Archive, Paper ID 2018/383). Available at `eprint.iacr.org/2018/383.pdf` (accessed Dec. 22, 2023).

32. Chi-Domínguez J.-J., Rodríguez-Henríquez F. Optimal strategies for CSIDH // J. Adv. Math. Commun. 2022. V. 16, No. 2. P. 383–411.
33. Cohen H. A course in computational algebraic number theory. Berlin: Springer, 1993. 536 p.
34. Maino L., Martindale C. An attack on SIDH with arbitrary starting curve. San Diego: Univ. California, 2022. (Cryptology ePrint Archive, Paper ID 2022/1026). Available at `eprint.iacr.org/2022/1026.pdf` (accessed Dec. 22, 2023).
35. Robert D. Breaking SIDH in polynomial time. San Diego: Univ. California, 2022. (Cryptology ePrint Archive, Paper ID 2022/1038). Available at `eprint.iacr.org/2022/1038.pdf` (accessed Dec. 22, 2023).
36. Howe E. W., Leprevost F., Poonen B. Large torsion subgroups of split Jacobians of curves of genus two or three // J. Forum Math. 2000. V. 12, No. 3. P. 315–364.
37. Bruin N., Flynn E. V., Testa D. Descent via $(3, 3)$-isogeny on Jacobians of genus 2 curves // J. Acta Arithmetica. 2014. V. 165, No. 3. P. 201–223.
38. Cosset R., Robert D. Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves // Math. Comput. 2015. V. 84, No. 294. P. 1953–1975.
39. Milio E. Computing isogenies between Jacobians of curves of genus 2 and 3 // Math. Comput. 2020. V. 89, No. 323. P. 1331–1364.
40. De Feo L., Dobson S., Galbraith S. D., Zobernig L. SIDH proof of knowledge. San Diego: Univ. California, 2021. (Cryptology ePrint Archive, Paper ID 2021/1023). Available at `eprint.iacr.org/2021/1023.pdf` (accessed Dec. 22, 2023).
41. De Feo L., Kieffer J., Smith B. Towards practical key exchange from ordinary isogeny graphs // Advances in cryptology — ASIACRYPT'18. Proc. Int. Conf. Theory and Application of Cryptology (Brisbane, Australia, Dec. 2–6, 2018). Cham: Springer, 2018. P. 365–394. (Lect. Notes Comput. Sci.; V. 11274).
42. Dartois P., de Feo L. On the security of OSIDH // Public-key cryptography — PKC 2022. Proc. 25th IACR Int. Conf. Practice and Theory of Public-Key Cryptography (Yokohama, Japan, Mar. 8–11, 2022). Pt. I. Cham: Springer, 2022. P. 52–81. (Lect. Notes Comput. Sci.; V. 13177).
43. Colò L., Kohel D. Orienting supersingular isogeny graphs // J. Math. Cryptology. 2020. V. 14, No. 1. P. 414–437.

Малыгина Екатерина Сергеевна
Куценко Александр Владимирович
Новосёлов Семён Александрович
Колесников Никита Сергеевич
Бахарев Александр Олегович
Хильчук Ирина Сергеевна
Шапоренко Александр Сергеевич
Токарева Наталья Николаевна

Статья поступила
11 мая 2023 г.
После доработки —
7 августа 2023 г.
Принята к публикации
22 сентября 2023 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
January–March 2024. Vol. 31, No. 1. P. 52–84

UDC 519.7 DOI: 10.33048/daio.2024.31.772

POST-QUANTUM CRYPTOSYSTEMS: OPEN PROBLEMS AND CURRENT SOLUTIONS. ISOGENY-BASED AND CODE-BASED CRYPTOSYSTEMS

E. S. Malygina[1, 2, a], *A. V. Kutsenko*[2, b], *S. A. Novoselov*[1, c], *N. S. Kolesnikov*[1, d], *A. O. Bakharev*[2, e], *I. S. Khilchuk*[2, f], *A. S. Shaporenko*[2, g], and *N. N. Tokareva*[2, 1, h]

[1] Immanuel Kant Baltic Federal University,
14 Aleksandr Nevskii Street, 236041 Kaliningrad, Russia

[2] Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia

E-mail: [a] emalygina@kantiana.ru, [b] alexandrkutsenko@bk.ru, [c] novsem@gmail.com, [d] nikolesnikov100@gmail.com, [e] a.bakharev@g.nsu.ru, [f] irina.khilchuk@gmail.com, [g] shaporenko.alexandr@gmail.com, [h] crypto1127@mail.ru

Abstract. This paper is a survey of modern post-quantum cryptographic schemes based on codes and isogenies. Special attention is paid to cryptanalysis of these schemes. In particular, for code-based cryptosystems we describe the information set decoding and the support splitting algorithm as main attacks, and for cryptosystems based on isogenies we describe in detail the Castryck — Decru attack on SIDH/SIKE. Tab. 2, bibliogr. 43.

Keywords: post-quantum cryptography, error-correcting code, elliptic curve, isogeny.

References

1. **E. S. Malygina, N. N. Tokareva, A. V. Kutsenko** [et al.]. Post-quantum cryptosystems: Open questions and solutions. Lattice-based cryptosystems, *Diskretn. Anal. Issled. Oper.* **30** (4), 46–90 (2023) [Russian] [*J. Appl. Ind. Math.* **17** (4), 767–790 (2023)].

English transl.: *Journal of Applied and Industrial Mathematics* **18** (1), 103–121 (2024), DOI: 10.1134/S1990478924010101.

2. **N. T. Courtois, M. Finiasz,** and **N. Sendrier,** How to achieve a McEliece-based digital signature scheme, in *Advances in Cryptology — ASIACRYPT'01,* Proc. Int. Conf. Theory and Application of Cryptology (Gold Coast, Australia, Dec. 9–13, 2001) (Springer, Heidelberg, 2001), pp. 157–174 (Lect. Notes Comput. Sci., Vol. 2248).
3. **J. Stern,** A new paradigm for public key identification, *IEEE Trans. Inf. Theory* **42** (6), 1757–1768 (1996).
4. **A. Childs, D. Jao,** and **V. Soukharev,** Constructing elliptic curve isogenies in quantum subexponential time, *J. Math. Cryptology* **8** (1), 1–29 (2014), DOI: 10.1515/jmc-2012-0016.
5. **R. J. McEliece,** A public-key cryptosystem based on algebraic coding theory, in *The Deep Space Network, Prog. Rep. 42-44* (California Inst. Tech., Pasadena, CA, 1978), pp. 114–116.
6. **H. Niederreiter,** Knapsack-type cryptosystems and algebraic coding theory, *J. Prob. Contr. Inform. Theory* **15** (2), 159–166 (1986).
7. **H. Niederreiter** and **C. Xing,** *Algebraic Geometry in Coding Theory and Cryptography* (Princeton Univ. Press, Princeton, NJ, 2009).
8. **L. Minder** and **A. Shokrollahi,** Cryptanalysis of the Sidelnikov cryptosystem, in *Advances in Cryptology — EUROCRYPT'07,* Proc. Int. Conf. Theory and Applications of Cryptographic Techniques (Barcelona, Spain, May 20–24, 2007) (Springer, Heidelberg, 2007), pp. 347–360 (Lect. Notes Comput. Sci., Vol. 4515), DOI: 10.1007/978-3-540-72540-4_20.
9. **E. Berlekamp, R. J. McEliece,** and **H. van Tilborg,** On the inherent intractability of certain coding problems, *IEEE Trans. Inf. Theory* **24** (3), 384–386 (1978).
10. **P. J. Lee** and **E. F. Brickell,** An observation on the security of McEliece's public-key cryptosystem, in *Advances in Cryptology — EUROCRYPT'88,* Proc. Workshop Theory and Application of Cryptographic Techniques (Davos, Switzerland, May 25–27, 1988) (Springer, Heidelberg, 1988), pp. 275–280 (Lect. Notes Comput. Sci., Vol. 330).
11. **E. Petrank** and **R. Roth,** Is code equivalence easy to decide?, *IEEE Trans. Inf. Theory* **43** (5), 1602–1604 (1997).
12. **N. Sendrier,** Finding the permutation between equivalent linear codes: The support splitting algorithm, *IEEE Trans. Inf. Theory* **46** (4), 1193–1203 (2000), DOI: 10.1109/18.850662.
13. **R. Misoczki, J.-P. Tillich, N. Sendrier,** and **P. Barreto,** MDPC-McEliece: New McEliece variants from moderate density parity-check codes, in *Proc. IEEE Int. Symp. Information Theory (Istanbul, Turkey, Jul. 7–12, 2013)* (IEEE Comput. Soc., Los Alamitos, CA, 2013), pp. 2069–2073, DOI: 10.1109/ISIT.2013.6620590.
14. **N. Drucker, S. Gueron,** and **D. Kostic,** QC-MDPC decoders with several shades of gray, in *Post-Quantum Cryptography,* Proc. Int. Conf. (Paris, France, Apr. 15–17, 2020) (Springer, Cham, 2020), pp. 35–50 (Lect. Notes Comput. Sci., Vol. 12100).

15. **R. C. Torres** and **N. Sendrier,** Analysis of information set decoding for a sublinear error weight, in *Post-Quantum Cryptography,* Proc. Int. Conf. (Fukuoka, Japan, Feb. 24–26, 2016) (Springer, Cham, 2016), pp. 144–161 (Lect. Notes Comput. Sci., Vol. 9606).
16. **E. Fujisaki** and **T. Okamoto,** Secure integration of asymmetric and symmetric encryption schemes, *J. Cryptology* **26**, 80–101 (2013).
17. **N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing,** and **E. Persichetti,** Tighter proofs of CCA security in the quantum random oracle model, in *Theory of Cryptography,* Proc. Int. Conf. (Nuremberg, Germany, Dec. 1–5, 2019) (Springer, Cham, 2019), pp. 61–90 (Lect. Notes Comput. Sci., Vol. 11892), DOI: 10.1007/978-3-030-36033-7_3.
18. **C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit,** and **G. Zémor,** Efficient encryption from random quasi-cyclic codes, *IEEE Trans. Inf. Theory* **64** (5), 3927–3943 (2018).
19. **N. Aragon, P. Gaborit,** and **G. Zémor,** HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code (Cornell Univ., Ithaca, NY, 2005) (Cornell Univ. Libr. e-Print Archive; arXiv:2005.10741)
20. **C. Doche** and **T. Lange,** Arithmetic of elliptic curves, in *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (Chapman & Hall/CRC Press, Boca Raton, FL, 2006), pp. 267–302.
21. **A. A. Bolotov, S. B. Gashkov, A. B. Frolov,** and **A. A. Chasovskikh,** *An Elementary Introduction to Ellipic Cryptography: Algebraic and Algorithmic Basics* (KomKniga, Moscow, 2006) [Russian].
22. **A. Sutherland,** Ellipic Curves. Isogenies, *Lecture Notes* (MIT, Cambridge, MA, 2022). Available at `math.mit.edu/classes/18.783/2022/LectureNotes4.pdf` (accessed Dec. 22, 2023).
23. **J. Vélu,** Isogénies entre courbes elliptiques, *C. R. Acad. Sci., Paris, Sér. A,* **273**, 238–241 (1971).
24. **S. Duquesne** and **T. Lange,** Arithmetic of hyperelliptic curves, in *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (Chapman & Hall/CRC Press, Boca Raton, FL, 2006), pp. 303–353.
25. **E. Kani,** The number of curves of genus two with elliptic differentials, *J. Reine Angew. Math.* **485**, 93-122 (1997).
26. **E. V. Flynn** and **Y. B. Ti,** Genus two isogeny cryptography, in *Post-Quantum Cryptography,* Proc. Int. Conf. (Chongquin, China, May 10–12, 2019) (Springer, Cham, 2019), pp. 286–306 (Lect. Notes Comput. Sci., Vol. 11505).
27. **W. Castryck, T. Decru,** and **B. Smith,** Hash functions from superspecial genus-2 curves using Richelot isogenies, *J. Math. Cryptology* **14** (1), 268–292 (2020).
28. **N. Alamati, L. de Feo, H. Montgomery,** and **S. Patranabis,** Cryptographic group actions and applications (Univ. California, San Diego, 2020) (Cryptology ePrint Archive, ID 2020/1188). Available at `eprint.iacr.org/2020/1188.pdf` (accessed Dec. 22, 2023).

29. L. De Feo, D. Jao, PlĴ. ut, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (Univ. California, San Diego, 2011) (Cryptology ePrint Archive, ID 2011/506). Available at `eprint.iacr.org/2011/506.pdf` (accessed Dec. 22, 2023).

30. W. Castryck and **T. Decru,** An efficient key recovery attack on SIDH (Univ. California, San Diego, 2022) (Cryptology ePrint Archive, ID 2022/975). Available at `eprint.iacr.org/2022/975.pdf` (accessed Dec. 22, 2023).

31. W. Castryck, T. Lange, C. Martindale, L. Panny, and **J. Renes,** CSIDH: An efficient post-quantum commutative group action (Univ. California, San Diego, 2018) (Cryptology ePrint Archive, ID 2018/383). Available at `eprint.iacr.org/2018/383.pdf` (accessed Dec. 22, 2023).

32. J.-J. Chi-Domínguez and **F. Rodríguez-Henríquez,** Optimal strategies for CSIDH, *J. Adv. Math. Commun.* **16** (2), 383–411 (2022).

33. H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, Berlin, 1993).

34. L. Maino and **C. Martindale,** An attack on SIDH with arbitrary starting curve (Univ. California, San Diego, 2022) (Cryptology ePrint Archive, ID 2022/1026). Available at `eprint.iacr.org/2022/1026.pdf` (accessed Dec. 22, 2023).

35. D. Robert, Breaking SIDH in polynomial time (Univ. California, San Diego, 2022) (Cryptology ePrint Archive, ID 2022/1038). Available at `eprint.iacr.org/2022/1038.pdf` (accessed Dec. 22, 2023).

36. E. W. Howe, F. Leprevost, and **B. Poonen,** Large torsion subgroups of split Jacobians of curves of genus two or three, *J. Forum Math.* **12** (3), 315–364 (2000).

37. N. Bruin, E. V. Flynn, and **D. Testa,** Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves, *J. Acta Arithmetica* **165** (3), 201–223 (2014).

38. R. Cosset and **D. Robert,** Computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves, *Math. Comput.* **84** (294), 1953–1975 (2015).

39. E. Milio, Computing isogenies between Jacobians of curves of genus 2 and 3, *Math. Comput.* **89** (323), 1331–1364 (2020).

40. L. De Feo, S. Dobson, S. D. Galbraith, and **L. Zobernig,** SIDH proof of knowledge (Univ. California, San Diego, 2021) (Cryptology ePrint Archive, ID 2021/1023). Available at `eprint.iacr.org/2021/1023.pdf` (accessed Dec. 22, 2023).

41. L. De Feo, J. Kieffer, and **B. Smith,** Towards practical key exchange from ordinary isogeny graphs, in *Advances in Cryptology — ASIACRYPT'18,* Proc. Int. Conf. Theory and Application of Cryptology (Brisbane, Australia, Dec. 2–6, 2018) (Springer, Cham, 2018), pp. 365–394 (Lect. Notes Comput. Sci., Vol. 11274).

42. P. Dartois and **L. de Feo,** On the security of OSIDH, in *Public-Key Cryptography — PKC 2022,* Proc. 25th IACR Int. Conf. Practice and Theory of Public-Key Cryptography (Yokohama, Japan, Mar. 8–11, 2022), Pt. I (Springer, Cham, 2022), pp. 52–81 (Lect. Notes Comput. Sci., Vol. 13177).

43. L. Colò and **D. Kohel,** Orienting supersingular isogeny graphs, *J. Math. Cryptology* **14** (1), 414–437 (2020).

Ekaterina S. Malygina
Aleksandr V. Kutsenko
Semyon A. Novoselov
Nikita S. Kolesnikov
Aleksandr O. Bakharev
Irina S. Khilchuk
Aleksandr S. Shaporenko
Natalia N. Tokareva

Received May 11, 2023
Revised August 7, 2023
Accepted September 22, 2023