DOI: 10.55648/1998-6920-2023-17-1-76-91 УДК 004.021

Усовершенствованная схема пороговой подписи CSI-FiSh со свойством быстрой сборки секрета*

В. В. Давыдов[1], А. Ф. Хуцаева[1], И. Д. Иогансон[1], Ж.-М. Н. Дакуо[1], С. В. Беззатеев[1,2]

[1]Университет ИТМО
[2] Санкт-Петербургский гос. унив. аэрокосмического приборостроения (ГУАП)

Аннотация: В работе приводится новый вариант построения пороговой подписи CSI-FiSh, опубликованной в 2020 году (L. De Feo, M. Meyer). В предложенной схеме дополнительно обновляются открытые и закрытые ключи, что позволяет избежать случая компрометации дилера. В усовершенствованной схеме предлагается исключить последовательную передачу информации между пользователями при подписи и заменить её на сборку с участием дилера. Также в работе представлены экспериментальные результаты, подтверждающие эффективность предложенного подхода, и оценка безопасности полученной схемы.

Ключевые слова: криптография на изогениях эллиптических кривых, постквантовая криптография, электронно-цифровая подпись, пороговая подпись, схемы разделения секрета.

Для цитирования: Давыдов В. В., Хуцаева А. Ф., Иогансон И. Д., Дакуо Ж.-М. Н., Беззатеев С. В. Усовершенствованная схема пороговой подписи CSI-FiSh со свойством быстрой сборки секрета // Вестник СибГУТИ. 2023. Т. 17, № 1. С. 76–91. https://doi.org/10.55648/1998-6920-2023-17-1-76-91.

Статья поступила в редакцию 05.12.2022;
переработанный вариант – 25.01.2023;
принята к публикации 04.02.2023.

1. Введение

В настоящее время одними из важнейших криптографических схем являются схемы пороговой подписи, которые нашли своё применение в большом количестве практических приложений [1, 2]. В связи с угрозой появления квантового компьютера большинство современных алгоритмов пороговой подписи, например подписи ECDSA [3], BLS [4], становятся уязвимыми к квантовым атакам с помощью алгоритма Шора [5]. Для решения данной проблемы предлагается использовать постквантовые алгоритмы, основанные на задачах, отличных от задач факторизации и дискретного логарифмирования.

Одна из таких задач – поиск изогений между эллиптическими кривыми. Данная область – самая молодая область постквантовой криптографии, которая бурно развивается в последнее время. Первая работа, посвящённая криптосистемам на изогениях и опубликованная в 2002 году, принадлежит Александру Ростовцеву и Елене Маховенко (Александровой) [6]. В дальнейшем данное направление получило широкое развитие: было опубликовано множество работ, в которых были представлены постквантовые криптосистемы, подписи и протоколы. Алгоритм выработки общего ключа SIKE [7] был представлен в конкурсе

* Работа выполнена при поддержке программы Приоритет-2030.

постквантовых алгоритмов на стандартизацию [8], однако недавно Castryck и Decru представили атаку, компрометирующую данный алгоритм [9]. Тем не менее, несмотря на это, многие алгоритмы, основанные на изогениях, остаются стойкими как к классическим, так и к квантовым атакам [10].

Отличительной особенностью алгоритмов, относящихся к данному разделу, являются относительно небольшие размеры ключей и подписей по сравнению с криптосистемами и протоколами, основанными на других задачах постквантовой криптографии. Однако время выполнения алгоритмов достаточно велико, поэтому их использование не всегда практически реализуемо в системах, в которых время играет ключевую роль. На сегодняшний день существует несколько алгоритмов подписи, основанных на задаче поиска изогений. Наиболее важными алгоритмами являются подписи SeaSign [11], CSI-FiSh [12] и SQISign [13].

Стоит отметить, что в силу специфики математического аппарата, на котором строится теория изогений, построение пороговой подписи – достаточно трудная задача. Сложность обуславливается некоммутативностью кольца эндоморфизмов суперсингулярных кривых над расширением поля. Следовательно, с математической точки зрения необходимо рассматривать суперсингулярные кривые над полем $\mathbb{F}_p$, где p – простое число. Так, подпись SeaSign, основанная на схеме CSIDH [14], использует групповое действие идеалов на множестве *j*-инвариантов над полем $\mathbb{F}_p$. Дальнейшим улучшением SeaSign является подпись CSI-FiSh, где предложено эффективное вычисление группового действия. Подпись SQISign, в свою очередь, строится над расширением поля $\mathbb{F}_{p^2}$, поэтому построение пороговой подписи затруднительно.

В 2020 году Luca de Feo и Michael Meyer предложили схему пороговой подписи CSI-FiSh [15]. Позже Daniel Cozzo и Nigel Smart представили вариант активно защищённой распределённой пороговой подписи CSI-FiSh [16]. Однако такие варианты имеют ключевой недостаток – сборка секрета и случайного значения в схеме осуществляется последовательно всеми пользователями, что сильно замедляет работу схемы. В нашей работе мы предлагаем усовершенствованный вариант схемы без последовательной передачи информации между пользователями при подписи, сильно сокращая время выполнения алгоритма.

2. Математический аппарат

Пусть K – конечное поле, E – эллиптическая кривая, заданная над K. Изогенией между двумя эллиптическими кривыми E и E_1 называется нетривиальный гомоморфизм:

$$\phi : E \to E_1;\ \phi(0_E) = 0_{E_1},$$

где 0 – точка на бесконечности на кривых E и E_1 соответственно.

Пусть $K = \mathbb{F}_p$, где p – некоторое простое число. Эллиптическая кривая называется суперсингулярной, тогда и только тогда, когда $E[p] = \{0_E\}$, где $E[p]$ – это множество точек кручения.

Множество точек на кривой $E(\bar{K})$ ($\bar{K}$ – алгебраическое замыкание поля K), отображающееся изогенией ϕ в точку 0_{E_1} на кривой E_1, называется ядром изогении и обозначается $\ker(\phi)$. Поскольку изогения ϕ определяет групповой гомоморфизм из E в E_1, ее ядро $\ker(\phi)$ – это подгруппа на кривой E. И, наоборот, любая подгруппа $X \subset E(\mathbb{F}_{p^k})$ определяет изогению $\phi : E \to E_1$ с $\ker(\phi) = X$, то есть $E_1 = E / X$. Уравнение для E_1 и изогения ϕ могут быть

вычислены с помощью алгоритма Велу [17]; обычно выбираются подгруппы X небольшого размера.

Кольцо эндоморфизмов $\mathrm{End}(E)$ состоит из всех изогений $\phi\colon E \to E$. Если кривая задана над конечным полем, то соответствующее кольцо эндоморфизмов обозначается $\mathrm{End}_{\mathbb{F}_p}(E)$. Для обычной (несуперсингулярной) кривой $E(\mathbb{F}_p)$: $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_p}(E)$, для суперсингулярной кривой над $\mathbb{F}_p$: $\mathrm{End}_{\mathbb{F}_p}(E) \subset \mathrm{End}(E)$.

По теореме Дойринга [18] для суперсингулярной кривой E над $\mathbb{F}_p$ полное кольцо эндоморфизмов $\mathrm{End}(E)$ изоморфно порядку $\mathcal{O}$ в алгебре кватернионов, тогда как $\mathrm{End}_{\mathbb{F}_p}(E)$ изоморфно порядку $\mathcal{O}'$ в мнимом квадратичном поле $\mathbb{Q}(\sqrt{-p})$.

Групповое действие (операция) [19] обычно представляет собой простое отображение:

$$\star : G \times X \to X,$$

где G – это группа, а X – это множество, такие что для любых $g_1, g_2 \in G$ и $x \in X$ выполняется:

$$g_1 \star (g_2 \star x) = (g_1 g_2) \star x.$$

В нашем случае $\mathrm{G} = \mathrm{Cl}(\mathcal{O})$, где Cl – группа классов идеалов, $X = \mathcal{A}$ – множество эллиптических кривых.

Множество $\mathcal{A}$ состоит из элементов A, таких что $E_A : y^2 = x^3 + Ax^2 + x$. Таким образом, E_0 соответствует $y^2 = x^3 + x$.

Пример выполнения группового действия [20].

Пусть задан идеал $\mathfrak{l} = (\ell, \pi - 1)$, и если $\mathrm{E}(\mathbb{F}_q)[\ell] = \langle P \rangle$ – это циклическая группа, тогда групповое действие l-изогении задается следующим образом:

$$[\mathfrak{l}] \star E = E / \langle P \rangle.$$

Следовательно, вычисление группового действия для идеала $\mathfrak{l} = (\ell, \pi - 1)$ происходит в два этапа:

1. Найти точку $P \in E(\mathbb{F}_q)$ порядка ℓ.
2. Вычислить l-изогению $E \to E / \langle P \rangle$, используя формулу Велу [17].

Также на данный момент существуют более эффективные алгоритмы, позволяющие вычислять идеалы вида $\mathfrak{g}^l = (g, \pi - 1)^l$ [14].

Далее предполагается, что группа классов идеалов $\mathrm{Cl}(\mathcal{O})$ является циклической порядка $N = \#\mathrm{Cl}(\mathcal{O})$, генерируется классом идеала $\mathfrak{g}$.

В [14] был предложен эффективный способ вычисления групповой операции $\star$ на суперсингулярных эллиптических кривых с большим количеством $\mathbb{F}_p$ рациональных подгрупп малой размерности. Важно отметить, что в современных криптографических алгоритмах, использующих в своей основе суперсингулярные эллиптические кривые, на начальном этапе алгоритма необходимо выбирать кривую с известным кольцом эндоморфизмов. Обычно в качестве начальной кривой выбирается кривая $E_0 : y^2 = x^3 + x$.

Безопасность, основанная на групповом действии, зиждется на допущении, что это действие трудно обратимо. Выделяют две основные проблемы: GAIP (Group Action Inverse Problem – проблема поиска обратного для группового действия) и MT-GAIP (Multi-Target

Group Action Inverse Problem – проблема поиска множественных обратных для группового действия).

Проблема GAIP описывается следующим образом. Пусть дана эллиптическая кривая E, $\mathrm{End}(E)=\mathcal{O}$, необходимо найти такой идеал $\mathfrak{a}\subset\mathcal{O}$, что $E=\mathfrak{a}\star E_0$.

Сложность решения GAIP строится на отсутствии методов на изогениях, подобных алгоритму быстрого возведения в степень, и проблемы, как и поиск обратного в группе [12].

Проблема MT-GAIP может быть описана следующим образом. Пусть дано k эллиптических кривых $E_1,\ldots,E_k$, где $\mathrm{End}(E_1)=\ldots=\mathrm{End}(E_k)=\mathcal{O}$, необходимо найти такой идеал $\mathfrak{a}\subset\mathcal{O}$, что $E_i=\mathfrak{a}\star E_j$, для некоторых $i,\ j\in\{1,2,\ldots,\ k\}$ и $i\neq j$. Схема подписи CSI-FiSh основана на сложности MT-GAIP.

3. Схема подписи CSI-FiSh

Кратко опишем схему подписи CSI-FiSh, приведённую в [14]. Схема основывается на преобразовании Фиата–Шамира, которое используется в схеме идентификации на основе изогений, предложенной Столбуновым [21] и Кувенем (Couveignes) [22]. Авторы предложили неинтерактивный протокол, на основе которого и строится подпись.

В данной подписи открытым ключом является набор кривых $E_1,\ldots,\ E_{S-1}$, полученный из набора идеалов $\mathfrak{a}_1,\mathfrak{a}_2,\ \ldots,\ \mathfrak{a}_{S-1}$, который, в свою очередь, получен как $\mathfrak{g}^{a_i}=\mathfrak{a}_i$, $i\in\{1,\ \ldots,\ S-1\}$, где множество a_i выступает в качестве закрытого ключа. Открытые ключи получаются как $E_i=\mathfrak{g}^{a_i}\star E_0=[a_i]E_0,\ \ i\in\{1,\ldots,S-1\}$, где E_0 – начальная кривая, $a_i\ \epsilon_R\ \mathbb{Z}_N$, где N – размерность заданной группы классов идеалов, то есть $N=\#\mathrm{Cl}(\mathcal{O})$.

Подписывающая сторона вычисляет набор кривых $E^{(i)}=\mathfrak{g}^{b_i}\star E_0=[b_i]E_0$, где $b_i\epsilon_R\mathbb{Z}_N$, $i\in\{1,\ldots,t\}$, $N=\#\mathrm{Cl}(\mathcal{O})$. Значение b_i выбирается случайно и не разглашается, данный параметр необходим для формирования и проверки подписи. Далее формируются компоненты подписи, вычисляется хэш от набора получившихся кривых и подписываемого сообщения с помощью дерева Меркла, то есть $(c_1,\ldots,\ c_t)=\mathcal{H}\left(E^{(1)}\|\ldots\|\ E^{(t)}\,\|\,m\right)$, где $c_i\in\{-S+1,\ldots,S-1\}$, $\mathcal{H}$ – криптографическая хэш-функция, такая что $\mathcal{H}:\{0,1\}^*\to\{-S+1,\ldots,S-1\}^t$.

Авторы статьи предложили увеличить количество значений c_i в два раза, поскольку кривая $E=[a]E_0$ изоморфна кривой $E'=[-a]E_0$, что позволяет в два раза расширить набор публичных ключей. Получается, что ранее набор представлял собой последовательность из $E_0,E_1,\ldots,\ E_{S-1}$, а сейчас из $E_{-S+1},\ \ldots,E_0,\ldots,E_{S-1}$.

Затем вычисляется $r_i=b_i-\mathrm{sign}(c_i)\,a_{|c_i|}\bmod N$, откуда получаем множество $(r_1,\ldots,\ r_t)$. Так как c_i может принимать отрицательные значения, то его значения берутся по модулю. Действительно, согласно с вычислением r_i знание b_i позволит узнать информацию о секретном ключе.

Другими словами, пользователь самостоятельно генерирует набор обязательств $(c_1,\ldots,\ c_t)$, а затем сразу же дает на него набор ответов $(r_1,\ldots,\ r_t)$ для проверки корректности обязательств. Таким образом, подпись формируется как $\sigma=(r_1,\ldots,\ r_t,c_1,\ldots,\ c_t)$. Необходимо

подчеркнуть, что увеличение отрезка c_i повышает свойство надежности протокола (soundness); вероятность «подлога» одного значения c_i составляет $1/(2S-1)$.

Проверка подписи осуществляется с помощью проверки равенства $(c_1,\ldots, c_t) == \left(c_1^{'},\ldots, c_t^{'}\right)$, где $c_i^{'}$ вычисляется как хэш от получившегося набора кривых и сообщения.

С помощью набора ответов $(r_1,\ldots, r_t)$ происходит вычисление $E^{(i)} = [r_i]E_{c_i}$, а затем $\left(c_1^{'},\ldots, c_t^{'}\right), = \mathcal{H}\left(E^{(1)} \| \ldots \| E^{(t)} \| m\right)$.

Выбор параметров S и t зависит от требуемого уровня безопасности, в статье проводится оценка зависимости размера подписи, времени генерации ключей, подписи и ее проверки от значений S, t.

В свою очередь, S и t соотносятся как вероятность «подлога» значений подписи (или обязательств) $1/(2S-1)^t$, то есть t раз отправляются значения $c_i \in \{-S+1,\ldots, S-1\}$.

4. Вариант пороговой подписи CSI-FiSh

Опишем построение пороговой подписи, показанное в работе [15]. Важной особенностью такой схемы является структура коммуникации между пользователями во время сборки секрета. Для разделения и сборки секрета используется схема разделения секрета Шамира [23].

Опишем последовательную сборку секрета d для групповой операции. Пусть участники $\mathcal{P}_1, \mathcal{P}_2, \ldots \mathcal{P}_n$ используют (k,n)-схему Шамира для полинома $f(x) = x^{k-1} + f_{k-2}x^{k-2} + \ldots f_1 x + d$ и получают свои тени секрета $d_1, d_2,\ldots, d_n$, где $d_i = f(x_i)$. Им необходимо собрать секрет d, не разглашая его, то есть получить $[d]E_0$, где E_0 – начальная кривая в изогенном графе. Для упрощения записи и без ущерба для общности будем считать, что в сборке секрета принимают участие $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_k$.

В таком случае базисные полиномы Лагранжа вычисляются как:

$$l_i(x) = \prod_{j=1,\, j\neq i}^{k} \frac{x - x_j}{x_i - x_j}.$$

Тогда, чтобы собрать секрет, кривая E_0 передаётся участнику $\mathcal{P}_1$, который вычисляет кривую E_1 следующим образом:

$$E_1 = \left[d_1 \cdot l_1(0)\right]E_0,$$

где $i = 1,\ldots,k$.

Затем кривая E_1 передается участнику $\mathcal{P}_2$, который вычисляет E_2:

$$E_2 = \left[d_2 \cdot l_2(0)\right]E_1 = \left[d_2 \cdot l_2(0) + d_1 \cdot l_1(0)\right]E_0.$$

Действие продолжается до участника k, который вычисляет:

$$E_k = \left[d_k \cdot l_k(0)\right]E_{k-1} = [d]E_0.$$

Заметим, что секрет d не получает никто из участников, его нахождение – сложная задача, равносильная задаче поиска пути в изогенном графе.

В пороговой схеме CSI-FiSh [15] происходит разделение между участниками двух параметров – секретных ключей $a_i, i \in \{1,\ldots, S-1\}$, которые раздаются участникам дилером, а

также случайных значений $b_i \epsilon_R \mathbb{Z}_N$, $i \in \{1, \ldots, t\}$, тени которых генерируются участниками самостоятельно на этапе подписи. Случайные значения b_i используются в протоколе доказательства без разглашения, основанном на схеме CSIDH, и участвуют в создании подписи. При этом самой «затратной» операцией с точки зрения времени выполнения является последовательное вычисление t значений b_i, полученных из теней b_{ij}, сгенерированных случайно каждым пользователем $\mathcal{P}_j$. Сборка таких значений осуществляется по алгоритму, показанному выше в данном разделе. При большом значении k такая схема работает неэффективно по времени, поэтому необходимо её оптимизировать.

5. Описание предлагаемого решения

Поскольку длительное время работы пороговой подписи обусловлено выполнением $t \cdot k$ операций группового действия при осуществлении подписи, целесообразно сократить количество таких операций. Для этого предлагается использовать дилера не только для генерации ключа, но и при вычислении подписи.

Важным условием является то, что в процессе генерации секрет не должен знать никто из участников, в том числе и сам дилер. В современных схемах данную проблему решают просто – дилер «забывает» секрет. Однако стоит учитывать факт компрометации дилера, в таком случае секрет становится известен третьим лицам. Таким образом, предлагается схема, основанная на [15], сохраняющая конфиденциальность секрета, то есть секрет (в собранном виде) никому не известен.

Генерация ключей

Согласно оригинальной схеме секретный ключ – это набор целых чисел $a_i \in \mathbb{Z}_N$, где $N = \#\mathrm{Cl}(\mathcal{O})$, $i \in \{1, \ldots, S-1\}$, где S – параметр безопасности. Будем «делить» каждое число между участниками с помощью схемы разделения секрета Шамира. Для того, чтобы дилер не знал собранный секрет, предлагается следующее усовершенствование схемы.

Пусть дилер генерирует набор секретных чисел $\{a_1, a_2, \ldots, a_{S-1}\}$, считает тени для каждого из них с помощью схемы разделения секрета Шамира, а затем передаёт полученные тени s_{ij} каждому из участников соответственно. После этого системой выбирается случайный участник, который генерирует набор случайных значений соли $\{\mathrm{salt}_1, \mathrm{salt}_2, \ldots, \mathrm{salt}_{S-1}\} \in \mathbb{Z}_N$, «делит» каждый элемент набора с помощью схемы разделения секрета Шамира, обновляет набор публичных ключей и отправляет каждому другому участнику $\mathcal{P}_j$ доли salt_{ij}, $i \in \{1, \ldots, S-1\}$, $j \in \{1, \ldots, n\}$, где n – общее количество участников. Выбор случайного участника можно осуществлять с помощью специальных протоколов, например схемы электронной лотереи Пейе [24].

Затем каждый участник вычисляет сумму полученных теней соли и своих теней секрета $s_{ij} + \mathrm{salt}_{ij}$, таким образом обновляя итоговый секрет. В итоге имеем две групповые операции для каждого из чисел – подсчёт $E_i = [a_i]E_0, i \in \{1, \ldots, S-1\}$ дилером, где a – секретный ключ, а также подсчёт $PK_i = [\mathrm{salt}_i]E_i, i \in \{1, \ldots, S-1\}$ каждым участником. Всего групповых операций – $2 \cdot (S-1)$.

Подпись

Основной проблемой при формировании подписи является последовательное вычислительно затратное выполнение нескольких групповых операций для сборки случайных

значений $\{b_1, b_2, \ldots, b_t\}$. В схеме [15] реализована круговая система последовательного подсчёта $E_j^k \leftarrow \left[b_{ij}\right] E_j^{k-1}, i \in \{1,\ldots,t\}, j \in \{1,\ldots,n\}$.

Для значительного ускорения процесса сборки теней предлагается вариант с использованием дилера, аналогичный варианту, предложенному при генерации ключей. Дилер сгенерирует набор случайных значений $\{b_1, b_2, \ldots, b_t\}$ и раздаст их тени между всеми участниками с помощью схемы разделения секрета Шамира, после чего один случайный участник сгенерирует соль, которую разделит между пользователями, а затем каждый добавит соль к своей тени b_{ij}.

Ниже приведены протокол генерации ключей (Протокол 1) и протокол подписи сообщения (Протокол 2). Верификация подписи не изменяется и аналогична верификации, представленной в работе [14] (Алгоритм 3).

Протокол 1. Генерация ключей.
Входные данные: $E_0, N = \#\mathrm{Cl}(\mathcal{O})$, идентификаторы участников IDs.

Выходные данные: набор секретных ключей sk_i, открытый ключ pk.

1. Дилер получает запрос на генерацию случайных кривых.
2. Для $i \in \{1,\ldots,S-1\}$
   a. $a_i \leftarrow_R \mathbb{Z}_N$;
   b. $E_i = \left[a_i\right] E_0$.
3. Дилер делит каждое значение a_i для $i \in \{1,\ldots,S-1\}$ на тени a_{ij} по схеме Шамира для $x_j \in IDs$.
4. Дилер отправляет значения $\left\{\left\{a_{ij}\right\}, E_i\right\}_{i=1,\ldots,S-1}$ пользователю с идентификатором x_j.
5. Один из пользователей, выбранный случайным образом, продолжает генерацию ключа.
6. Для всех $i \in \{1,\ldots,S-1\}$
   a. $\mathrm{salt}_i \leftarrow_R \mathbb{Z}_N$;
   b. $PK_i = \left[\mathrm{salt}_i\right] E_i$.
7. Выбранный на шаге 5 пользователь делит каждое значение salt_i для $i \in \{1,\ldots,S-1\}$ на тени salt_{ij} по схеме Шамира для $x_j \in IDs$.
8. Выбранный на шаге 5 пользователь отправляет значения $\left\{\left\{\mathrm{salt}_{ij}\right\}, PK_i\right\}_{i=1,\ldots,S-1}$ пользователю с идентификатором x_j.
9. Каждый пользователь i получает $sk_i = \left\{a_{ji} + \mathrm{salt}_{ji}\right\}_{j=1,\ \ldots,\ S-1}$ и $PK = \left\{PK_j\right\}_{j=1,\ldots,S-1}$.

Протокол 2. Подпись.
Входные данные: сообщение m, идентификаторы участников IDs.
Выходные данные: подпись $\sigma = \left(z_1,\ldots,z_t; c_1,\ldots,c_t\right)$.

1. Дилер получает запрос на генерацию случайных кривых.
2. Для всех $i \in \{1,\ \ldots,\ t\}$

a. $b_i \leftarrow_R \mathbb{Z}_N$;
b. $E_i = [b_i] E_0$.

3. Дилер делит каждое значение b_i для $i \in \{1,\ldots,t\}$ на тени b_{ij} по схеме Шамира для $x_j \in IDs$.
4. Дилер отправляет значения $\left\{\{b_{ij}\}, E_i\right\}_{i=1,\ldots,t}$ пользователю с идентификатором x_j.
5. Один из пользователей продолжает вычисление подписи.
6. Для всех $i \in \{1,\ldots,t\}$
   a. $\text{salt}_i \leftarrow_R \mathbb{Z}_N$;
   b. $B_i = [\text{salt}_i] E_i$.
7. Выбранный на шаге 5 пользователь делит каждое значение salt_i для $i \in \{1,\ldots,t\}$ на тени salt_{ij} по схеме Шамира для $x_j \in IDs$.
8. Выбранный на шаге 5 пользователь отправляет значения $\left\{\{\text{salt}_{ij}\}, B_i\right\}_{i=1,\ldots,t}$ пользователю с идентификатором x_j.
9. Каждый пользователь вычисляет $(c_1,\ldots,c_t) = \mathcal{H}(B_1 \| B_2 \| \ldots \| B_t \| m)$.
10. Примем $sk_0 = 0$.
11. Каждый пользователь x_j вычисляет значение

$$z_{ij} = \left(b_{ij} + \text{salt}_{ij} - \text{sign}(c_i) \cdot sk_{j,|c_i|}\right) \cdot l_j(0) \text{ для } i \in \{1,\ldots,t\}.$$

12. Вычисляется $z_i = \sum_{j \in IDs} z_{ij}$ для $i \in \{1,\ldots,t\}$.
13. Собирается подпись $\sigma = (z_1,\ldots,z_t; c_1,\ldots,c_t)$.

Алгоритм 3. Верификация.

Входные данные: сообщение m, подпись $\sigma = (z_1,\ldots,z_t; c_1,\ldots,c_t)$, открытый ключ $PK = \{E_1,\ldots,E_{S-1}\}$.

Выходные данные: ver $= \{\text{True или False}\}$.

1. Примем $E_{-i} = E_i^t$, для всех $i \in \{1,\ldots,S-1\}$.
2. Для $i = 1,\ldots,t$
   a. $E^{(i)} = [z_i] E_{c_i}$.
3. $\left(c_1^{'},\ldots,c_t^{'}\right) = \mathcal{H}\left(E^{(1)} \| \ldots \| E^{(t)} \| m\right)$.
4. Если $\left(c_1^{'},\ldots,c_t^{'}\right) = (c_1,\ldots,c_t)$:
   a. ver $=$ True.
5. Иначе:
   a. ver $=$ False.

6. Безопасность

Главной уязвимостью предлагаемого алгоритма является атака сговора. Она заключается в том, что если некоторое количество участников сговорится с дилером, то существует вероятность P того, что злоумышленники смогут узнать секретный ключ:

$$P = \begin{cases} \frac{r}{t}, r < t \\ 1, r \geq t \end{cases},$$

где r – количество сговорившихся участников и t – это количество участвующих в подписи сообщения пользователей.

Уязвимость появляется вследствие генерации ключа в два этапа.

На первом этапе дилер самостоятельно выбирает случайные кривые $E_i = [a_i]E_0$ и рассылает пользователям кортеж данных $\left(\{a_{ij}\}, E_i\right)$.

На втором этапе случайный пользователь досчитывает секретный ключ, используя salt_i:

$$sk_i = a_i + \text{salt}_i.$$

Таким образом, если дилер, генерирующий a_i, и пользователь, генерирующий salt_i, сговорятся и сообщат друг другу значения своих секретных переменных, они узнают секретный ключ. Чем больше у дилера потенциальных союзников, тем выше вероятность успешной атаки сговором.

Еще одним вектором атаки для сговора участников с дилером является протокол вычисления подписи. В начале протокола дилер и случайно выбранный участник совместно генерируют случайные значения b_i и salt_i. Данные значения, как и секретный ключ, не должны быть скомпрометированы. Если кто-либо из участников узнает значения $\{b_i, \text{salt}_i\}$, то, зная z_i и c_i, он сможет узнать значение секретного ключа $sk_{c_i} = -\text{sign}(c_i)*(z_i - b_i - \text{salt}_i)$. Вероятность того, что один из участников, сговорившись с дилером, узнает эти значения, вычисляется аналогично вероятности P того, что злоумышленник узнает секретный ключ при генерации ключа.

Теперь рассмотрим безопасность данного протокола при Honest-but-Curious [25] модели злоумышленника. В данной модели злоумышленник – это легитимный пользователь, который не отклоняется от определенных протоколом действий, однако пытается собрать всю возможную информацию о системе.

Как было показано выше, безопасность системы основана на конфиденциальности случайно сгенерированных значений $\{a_i, \text{salt}_i\}$ – при генерации ключа и $\{b_i, \text{salt}_i\}$ – при вычислении подписи. Чтобы узнать секретный ключ злоумышленнику достаточно узнать $a_i + \text{salt}_i$ или $b_i + \text{salt}_i$. Рассмотрим множество значений, которые знает каждый пользователь: $\{E_0, N, S, t, IDs\}$, множество значений, полученных пользователем j в процессе генерации ключа: $\left\{\left\{a_{1j}, \ldots, a_{(S-1)j}\right\}, \left\{\text{salt}_{1j}, \ldots, \text{salt}_{(S-1)j}\right\}, PK = \{E_1, \ldots, E_{S-1}\}\right\}$ и множество значений, полученных пользователем в процессе вычисления подписи:

$$\left\{m, \sigma = (z_1, \ldots, z_t; c_1, \ldots, c_t), \left\{b_{1j}, \ldots, b_{tj}\right\}, \left\{\text{salt}_{1j}, \ldots, \text{salt}_{tj}\right\}, \{B_1, \ldots, B_t\}\right\}.$$

Из данных значений невозможно получить секретный ключ, так как $\left\{a_{1j}, \ldots, a_{(S-1)j}\right\}, \left\{\text{salt}_{1j}, \ldots, \text{salt}_{(S-1)j}\right\}$ являются частями секретного ключа, но так как схема разделения Шамира совершенна, то знание одной доли секрета не даст злоумышленнику

никакой информации о секрете. Также $E_i = [sk_i]E_0$, однако отсюда злоумышленник также не сможет получить секретный ключ за разумное время из-за свойств группового действия. И последнее, $z_i = b_i + \mathrm{salt}_i - \mathrm{sign}(c_i)\cdot sk_{|c_i|}$, однако, не зная $b_i + \mathrm{salt}_i$ злоумышленник также не сможет отсюда получить информацию о $sk_{|c_i|}$.

Дилер и выбранный пользователь имеют преимущество, так как один из них знает $\{a_i\}$, а другой знает $\{\mathrm{salt}_i\}$. Однако знание одного из этих значений не даст информации о значении $\{sk_i = a_i + \mathrm{salt}_i\}$. Таким образом, можно сказать, что при модели злоумышленника Honest-but-Curious предложенная схема безопасна.

В общем случае безопасность рассматриваемой схемы эквивалентна безопасности ее составляющих – алгоритма Шамира [23] и схемы подписи CSi-FiSh [14]. Корректность схемы обусловлена протоколами 1, 2 и алгоритмом 3, где показана валидность подписи. Нам необходимо лишь доказать, что $B_i = E^{(i)}$. Для вычисления данных кривых используется схема Шамира, она работает корректно, потому что все вычисления происходят в коммутативных группах. Рассмотрим подробнее каждую из вычисляемых кривых.

Кривая, получаемая при подписи сообщения:

$$B_i = [\mathrm{salt}_i]E_i = [\mathrm{salt}_i][b_i]E_0 = [\mathrm{salt}_i + b_i]E_0.$$

Кривая, получаемая при проверке:

$$E^{(i)} = [z_i]E_{c_i} = \left[b_i + \mathrm{salt}_i - \mathrm{sign}(c_i)\,sk_{i,|c_i|}\right]E_{c_i} =$$

$$\left[b_i + \mathrm{salt}_i - \mathrm{sign}(c_i)\,sk_{i,|c_i|}\right]\left[\mathrm{sign}(c_i)\,sk_{i,|c_i|}\right]E_0 =$$

$$\left[b_i + \mathrm{salt}_i - \mathrm{sign}(c_i)\,sk_{i,|c_i|} + \mathrm{sign}(c_i)\,sk_{i,|c_i|}\right]E_0 =$$

$$[b_i + \mathrm{salt}_i]E_0.$$

Откуда очевидно, что $B_i = E^{(i)}$. Следовательно, верно следующее:

$$\mathcal{H}\left(B_1 \| \ldots \| B_t \| m\right) = \mathcal{H}\left(E^{(1)} \| \ldots \| E^{(t)} \| m\right).$$

Очевидно, что выполняется и равенство $\left(c_1', \ldots, c_t'\right) = \left(c_1, \ldots, c_t\right)$.

По полученным результатам можно заключить, что предложенный протокол работает корректно.

7. Экспериментальные результаты

Для проверки полученных результатов и оценки времени работы схем реализованы оригинальная пороговая схема CSI-FiSh [15] и предложенный в данной работе вариант. Реализация проведена на языке Python с использованием программного обеспечения SAGEMath на персональном компьютере со следующими характеристиками: процессор Intel Core i5-6300HQ 2.30 GHz, оперативная память 8 ГБ.

Для сравнения времени работы алгоритмов генерации ключей и подписи для оригинальной схемы и её улучшенной версии подсчитаны экспериментальные значения времени выполнения в зависимости от параметров безопасности S и t, а также от порога k. На рис. 1 показана зависимость времени подписи от порога схемы при фиксированных значениях $n = 10$, $S = 2$, $t = 6$.

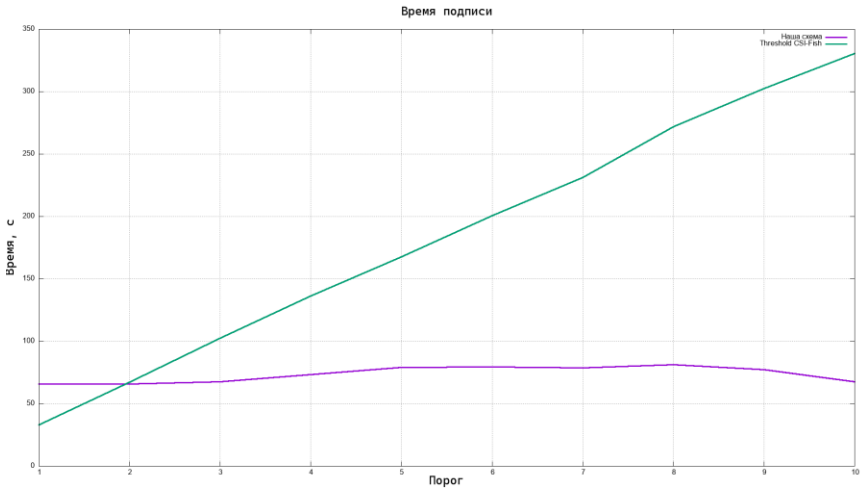

Рис. 1. Время подписи для оригинальной и предложенной схем в зависимости от порога при $n = 10$, $S = 2$, $t = 6$

Из графика видно, что время подписи для предложенной схемы практически не меняется при увеличении порога, в то время как для оригинального Threshold CSI-FiSh время сильно увеличивается. Это обусловлено тем, что с увеличением порога в оригинальной схеме увеличивается и количество выполняемых групповых операций; для нашей схемы это количество фиксировано и не зависит от значения порога.

На рис. 2 показана зависимость времени подписи от параметра безопасности t при фиксированных значениях $n = 10$, $S = 2$, $k = 3$.

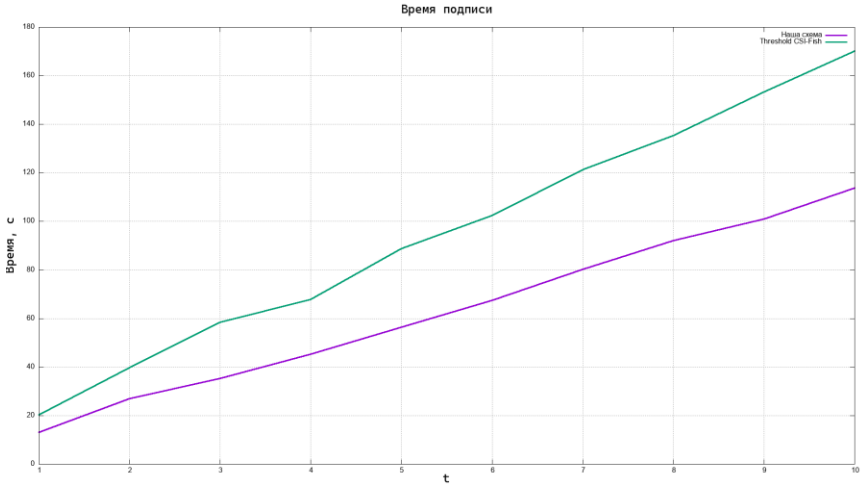

Рис. 2. Время подписи для оригинальной и предложенной схем в зависимости от параметра безопасности t при $n = 10$, $S = 2$, $k = 3$

Можно заметить, что предложенная схема работает быстрее оригинальной – это обусловлено тем, что в предложенной схеме время выполнения не зависит от порога, а количество выполняемых групповых операций – $2t$; для оригинальной схемы количество таких операций – $k \cdot t$, то есть в данном случае – $3t$.

На рис. 3 показана зависимость времени генерации ключа от параметра безопасности S при фиксированных значениях $n = 10$, $t = 6$, $k = 3$.

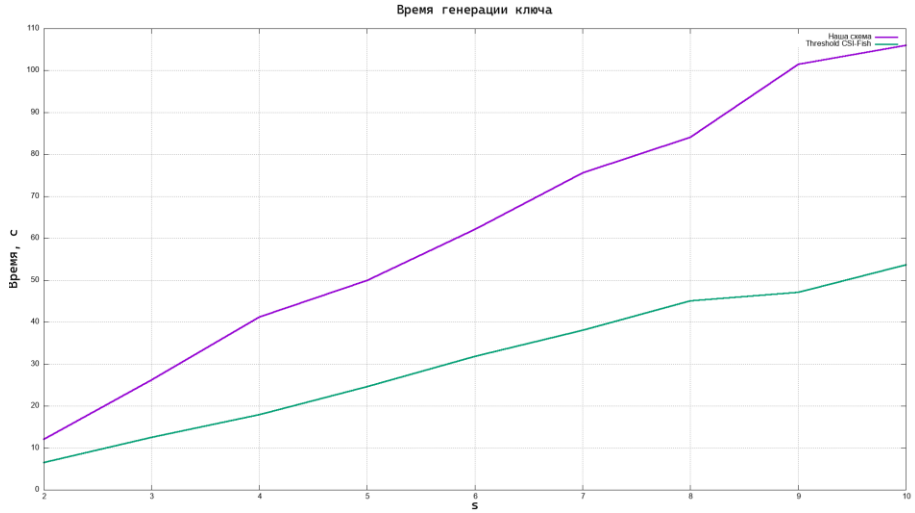

Рис. 3. Время генерации ключей для оригинальной и предложенной схем в зависимости от параметра безопасности S при $n = 10$, $t = 6$, $k = 3$

В данном случае предложенная схема работает дольше оригинальной, это обусловлено обновлением секрета случайным пользователем для обеспечения безопасности при недобросовестности дилера; в данном случае в предложенной схеме выполняется в два раза больше групповых операций, чем в оригинальной.

В табл. 1 для наглядности показаны некоторые значения полученного времени при различных параметрах S, t, k, n.

Таблица 1. Сравнение времени выполнения алгоритмов генерации ключей и подписи для оригинальной и усовершенствованной схем для различных параметров безопасности и порога

S	t	(k, n)	Время генерации ключей, схема [15], с	Время генерации ключей, предложенная схема, с	Время подписи, схема [15], с	Время подписи, предложенная схема, с
2	1	(1,10)	6.04	11.83	5.99	12.42
4	3	(3,10)	17.71	37.57	54.97	34.75
6	5	(5,10)	29.46	61.62	147.98	60.48
8	7	(7,10)	41.04	85.24	289.58	85.03
10	9	(9,10)	54.65	108.20	477.80	109.22

Как видно из табл. 1, с ростом значений параметров безопасности и порога схемы предложенная схема работает в несколько раз быстрее оригинальной.

8. Заключение

В работе предложен усовершенствованный вариант пороговой подписи CSI-FiSh со свойством быстрой сборки секрета. Введено дополнительное обновление секрета на этапе генерации ключей для защиты от недобросовестного дилера, а также последовательная сборка секрета была заменена сборкой с участием дилера, что позволило сильно сократить время подписи. Были доказаны корректность и безопасность предлагаемого подхода. Предложенная схема может использоваться в реальных системах, где есть необходимость защиты от квантовых атак.

Литература

1. *Goldfeder S. et al.* Securing bitcoin wallets via threshold signatures. 2014.
2. *Stathakopoulou C., Cachin C.* Threshold signatures for blockchain systems //Swiss Federal Institute of Technology. 2017. V. 30. P. 1.
3. *Johnson D., Menezes A., Vanstone S.* The elliptic curve digital signature algorithm (ECDSA) // International journal of information security. 2001. V. 1, № 1. P. 36–63.
4. *Zhang F., Safavi-Naini R., Susilo W.* An efficient signature scheme from bilinear pairings and its applications // International workshop on public key cryptography. Springer, Berlin, Heidelberg, 2004. P. 277–290.
5. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM review. 1999. V. 41, № 2. P. 303–332.
6. *Ростовцев А. Г., Маховенко Е. Б.* Криптосистема на категории изогенных эллиптических кривых // Проблемы информационной безопасности. Компьютерные системы. 2002. № 3. С. 74.
7. *Jao D. et al.* SIKE: Supersingular isogeny key encapsulation // HAL. 2017.
8. Computer Security Division I. T. L. Post-Quantum Cryptography | CSRC | CSRC // CSRC | NIST [Электронный ресурс]. URL: `https://csrc.nist.gov/projects/post-quantum-cryptography` (accessed: 04.12.2022).
9. *Castryck W., Decru T.* An efficient key recovery attack on SIDH (preliminary version) // Cryptology ePrint Archive. 2022.
10. Is SIKE broken yet? // Is SIKE broken yet? [Электронный ресурс]. URL: `https://issikebrokenyet.github.io/` (accessed: 04.12.2022).
11. *De Feo L., Galbraith S. D.* SeaSign: compact isogeny signatures from class group actions // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2019. P. 759–789.
12. *Beullens W., Kleinjung T., Vercauteren F.* CSI-FiSh: efficient isogeny based signatures through class group computations // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2019. P. 227–247.
13. *De Feo L. et al.* SQISign: compact post-quantum signatures from quaternions and isogenies // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2020. P. 64–93
14. *Castryck W. et al.* CSIDH: an efficient post-quantum commutative group action // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018. P. 395–427.
15. *De Feo L., Meyer M.* Threshold schemes from isogeny assumptions // IACR International Conference on Public-Key Cryptography. Springer, Cham, 2020. P. 187–212.
16. *Cozzo D., Smart N. P.* Sashimi: cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol // International Conference on Post-Quantum Cryptography. Springer, Cham, 2020. P. 169–186.
17. *Vélu J.* Isogénies entre courbes elliptiques // CR Acad. Sci. Paris, Séries A. 1971. V. 273. P. 305–347.
18. *Silvermann J. H.* The arithmetic of elliptic curves // Graduate Texts in Mathematics. 1986. V. 106.
19. *Alamati N. et al.* Cryptographic group actions and applications // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2020. P. 411–439.
20. *Sotakova J.* Elliptic curves, isogenies, and endomorphism rings. P. 17.
21. *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, № 2. P. 215.
22. *Couveignes J. M.* Hard homogeneous spaces // Cryptology ePrint Archive. 2006.

23. *Shamir A.* How to share a secret // Communications of the ACM. 1979. V. 22, № 11. P. 612–613.
24. *Paillier P.* Public-key cryptosystems based on composite degree residuosity classes // International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 1999. P. 223–238.
25. *Paverd A., Martin A., Brown I.* Modelling and automatically analysing privacy properties for honest-but-curious adversaries // Tech. Rep. 2014.

Давыдов Вадим Валерьевич
аспирант 4 года обучения факультета безопасности информационных технологий, преподаватель, Университет ИТМО (НИУ ИТМО,197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А.), e-mail: vvdavydov@itmo.ru, ORCID ID: 0000-0002-5544-2434.

Хуцаева Алтана Феликсовна
инженер, магистрант 2 курса факультета безопасности информационных технологий, Университет ИТМО (НИУ ИТМО,197101, Санкт-Петербург, Кронверкский проспект, д. 49, лит. А.), e-mail: afkhutsaeva@itmo.ru, ORCID ID: 0000-0001-5494-7142.

Иогансон Иван Дмитриевич
инженер, аспирант факультета безопасности информационных технологий, Университет ИТМО (НИУ ИТМО, 197101, Санкт-Петербург, Кронверкский проспект, д.49, литер А.), e-mail: ivan.ioganson@itmo.ru, ORCID ID: 0000-0002-0856-2249.

Дакуо Жан-Мишель Никодэмович
инженер, аспирант факультета безопасности информационных технологий, Университет ИТМО (НИУ ИТМО, 197101, Санкт-Петербург, Кронверкский проспект, д.49, литер А.), e-mail: jeandakuo@mail.ru, ORCID ID: 0000-0002-4084-8829.

Беззатеев Сергей Валентинович
заведующий кафедрой информационной безопасности, Санкт-Петербургский государственный университет аэрокосмического приборостроения (190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А);
директор лаборатории криптографических методов защиты информации, Университет ИТМО (НИУ ИТМО, 197101, Санкт-Петербург, Кронверкский проспект, д.49, литер А.), e-mail: bsv@aanet.ru, ORCID ID: 0000-0002-0924-6221.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Improved Threshold Signature Scheme CSI-FiSh with Fast Secret Recovery

Vadim V. Davydov[1], Altana F. Khutsaeva[1], Ivan D. Ioganson[1], Zhan-Mishel N. Dakuo[1], Sergey V. Bezzateev[1,2]

[1] ITMO University (ITMO)
[2] Saint Petersburg State University of Aerospace Instrumentation (SUAI)

Abstract: The paper presents an improved version of the CSI-FiSh threshold signature offered by L. De Feo and M. Meyer in 2020. In the proposed scheme, public and private keys are additionally updated avoiding the case of compromising a dealer. It is also proposed to eliminate the sequential information transfer between participants when signing and replace it with an assembly with the participation of the dealer. Experimental results showing the effectiveness of the proposed approach and the assessment of the resulting scheme safety are presented.

Keywords: isogeny-based cryptography, post-quantum cryptography, digital signature, threshold signature, secret sharing schemes.

For citation: Davydov V. V., Khutsaeva A. F., Ioganson I. D., Dakuo Z.-M. N., Bezzateev S. V. Improved threshold signature scheme CSI-FiSh with fast secret recovery (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 1. pp. 76-91. https://doi.org/10.55648/1998-6920-2023-17-1-76-91.

The article was submitted: 05.12.2022;
revised version: 25.01.2023;
accepted for publication 04.02.2023.

References

1. Goldfeder S. et al. *Securing bitcoin wallets via threshold signatures*. 2014.
2. Stathakopoulou C., Cachin C. Threshold signatures for blockchain systems. *Swiss Federal Institute of Technology*, 2017, vol. 30, pp. 1.
3. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*, 2001, vol. 1, no. 1, pp. 36-63.
4. Zhang F., Safavi-Naini R., Susilo W. An efficient signature scheme from bilinear pairings and its applications. *International workshop on public key cryptography*, Springer, Berlin, Heidelberg, 2004, pp. 277-290.
5. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 1999, vol. 41, no. 2, pp. 303-332.
6. Rostovcev A. G., Mahovenko E. B. Kriptosistema na kategorii izogennyh ellipticheskih krivyh [Cryptosystem on the category of isogenic elliptic curves] *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy*, Saint-Petersburg, 2002, no. 3, p. 74.
7. Jao D. et al. SIKE: Supersingular isogeny key encapsulation. *HAL*, 2017, vol. 2017.
8. Computer Security Division I. T. L. Post-Quantum Cryptography | CSRC | CSRC. *CSRC | NIST*, [Research and analysis of computer network monitoring tools and methods], available at: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed: 04.12.2022).
9. Castryck W., Decru T. An efficient key recovery attack on SIDH (preliminary version). *Cryptology ePrint Archive*, 2022.
10. Is SIKE broken yet? *Is SIKE broken yet?* [Research and analysis of computer network monitoring tools and methods], available at: https://issikebrokenyet.github.io/ (accessed: 04.12.2022).
11. De Feo L., Galbraith S. D. SeaSign: compact isogeny signatures from class group actions. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Cham, 2019, pp. 759-789.

12. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Cham, 2019, pp. 227-247.
13. De Feo L. et al. SQISign: compact post-quantum signatures from quaternions and isogenies. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Cham, 2020, pp. 64-93
14. Castryck W. et al. CSIDH: an efficient post-quantum commutative group action. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Cham, 2018, pp. 395-427.
15. De Feo L., Meyer M. Threshold schemes from isogeny assumptions. *IACR International Conference on Public-Key Cryptography*, Springer, Cham, 2020, pp. 187-212.
16. Cozzo D., Smart N. P. Sashimi: cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol. *International Conference on Post-Quantum Cryptography*, Springer, Cham, 2020, pp. 169-186.
17. Vélu J. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 1971, vol. 273, pp. 305-347.
18. Silvermann J. H. The arithmetic of elliptic curves. *Graduate Texts in Mathematics*, 1986, vol. 106.
19. Alamati N. et al. Cryptographic group actions and applications. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Cham, 2020, pp. 411-439.
20. Sotakova J. *Elliptic curves, isogenies, and endomorphism rings*. p. 17.
21. 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, p. 215.
22. Couveignes J. M. Hard homogeneous spaces. *Cryptology ePrint Archive*, 2006.
23. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, no. 11, pp. 612-613.
24. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. *International conference on the theory and applications of cryptographic techniques*, Springer, Berlin, Heidelberg, 1999, pp. 223-238.
25. Paverd A., Martin A., Brown I. Modelling and automatically analysing privacy properties for honest-but-curious adversaries. *Tech*. Rep., 2014.

Vadim V. Davydov

4th year PhD student of the Department of Information Security, lecturer, ITMO University (ITMO, Kronverksky Pr. 49, bldg. A, St. Petersburg, 197101, Russia), e-mail: vvdavydov@itmo.ru, ORCID ID: 0000-0002-5544-243.

Altana F. Khutsaeva

Engineer, 2nd year master's degree student of the Department of Information Security, ITMO University (ITMO, Kronverksky Pr. 49, bldg. A, St. Petersburg, 197101, Russia), e-mail: afkhutsaeva@itmo.ru, ORCID ID: 0000-0001-5494-7142.

Ivan D. Ioganson

Engineer, PhD student of the Department of Information Security, ITMO University (ITMO, Kronverksky Pr. 49, bldg. A, St. Petersburg, 197101, Russia), e-mail: ivan.ioganson@itmo.ru, ORCID ID: 0000-0002-0856-2249.

Zhan-Mishel N. Dakuo

Engineer, PhD student of the Department of Information Security, ITMO University (ITMO, Kronverksky Pr. 49, bldg. A, St. Petersburg, 197101, Russia), e-mail: jeandakuo@mail.ru, ORCID ID: 0000-0002-4084-8829.

Sergey V. Bezzateev

Head of Information Security Department, Saint-Petersburg State University of Aerospace Instrumentation (190000, Saint-Petersburg, Bolshaya Morskaya str. 67, lit. A); Director of Cryptographic Methods of Information Security Laboratory, ITMO University (197101, Saint-Petersburg, Kronverksky prospekt 49, lit. A), e-mail: bsv@aanet.ru, ORCID ID: 0000-0002-0924-6221.