УДК 004.056
doi:10.18720/SPBPU/2/id24-508

Александрова Елена Борисовна [1],
профессор, д-р техн. наук, доцент;
Бугаев Вячеслав Александрович [2],
студент;
Терёшкина Елизавета Александровна [3],
студент

КВАНТОВО-УСТОЙЧИВАЯ УПОРЯДОЧЕННАЯ КОЛЛЕКТИВНАЯ ПОДПИСЬ НА ОСНОВЕ CSI-FISH

[1,2,3] Россия, Санкт-Петербург,
Санкт-Петербургский политехнический университет Петра Великого,
[1] helen@ibks.spbstu.ru, [2] bugaev.va@edu.spbstu.ru,
[3] tereshkina.ea@edu.spbstu.ru

Аннотация. В статье рассматривается проблема формирования квантово-устойчивой упорядоченной коллективной подписи для обеспечения безопасной маршрутизации. Проанализированы схемы упорядоченных электронных подписей (ЭП), выделены подходы к созданию схем упорядоченной коллективной подписи. Предложена модель предположительно квантово-устойчивой схемы упорядоченной коллективной ЭП, основанной на изогениях эллиптических кривых. Проведен анализ безопасности полученной модели и предложены способы ее применения на практике.

Ключевые слова: постквантовая криптография, криптография на изогениях эллиптических кривых, суперсингулярные эллиптические кривые, электронная цифровая подпись, коллективная подпись, упорядоченная цифровая подпись, групповая операция.

Elena B. Aleksandrova [1],
Professor, Doctor of Technical Sciences;
Vyachelsav A. Bugaev [2],
Student;
Elizaveta A. Tereshkina [3],
Student

POST-QUANTUM SAFE ORDERED MULTISIGNATURES BASED ON CSI-FISH

[1,2,3] Peter the Great St.Petersburg Polytechnic University, St. Petersburg, Russia,
[1] helen@ibks.spbstu.ru, [2] bugaev.va@edu.spbstu.ru,
[3] tereshkina.ea@edu.spbstu.ru

Abstract. The article contains research of the problem of creating a post-quantum safe ordered multisignature to ensure secure routing. Existing schemes of ordered multisignature are analyzed. Approaches to the creation of ordered multisignatures are formulated. A model of a supposedly post-quantum safe scheme of an isogeny-based ordered multisignature is proposed. The safety analysis of the model is proposed. The ways of applying the model in practice are proposed.

Keywords: post-quantum cryptography, isogeny-based cryptography, supersingular elliptic curves, digital signature, multisignature, ordered signature, group action.

Введение

В современном мире проблема информационной безопасности не теряет своей актуальности, количество процессов, выполняемых с помощью информационных технологий и систем, постоянно растет. Конфиденциальные данные участников этих процессов нуждаются в защите.

В последние годы некоторые компании предоставляют доступ к квантовым вычислительным ресурсам через облачные системы [1], что повышает актуальность алгоритмов, позволяющих за полиномиальное время решать вычислительно сложные задачи, лежащие в основе большинства схем электронной подписи (ЭП). Алгоритм Шора [2] обеспечивает экспоненциальную сложность задач разложения на множители и дискретного логарифмирования в циклической группе. Таким образом, создание схем подписей, предположительно стойких к атакам с применением квантовых компьютеров, является важным. В настоящей работе рассматриваются схемы упорядоченных (иерархических) коллективных ЭП.

1. Постановка задачи

1.1. Описание предметной области

Концепция упорядоченных подписей может применяться в протоколах безопасной маршрутизации [3]. Основной протокол динамической маршрутизации в сети Интернет, BGP (Border Gateway Protocol), предназначен для обмена информацией о достижимости подсетей между

автономными системами (autonomous system, AS). AS – набор маршрутизаторов под единым техническим и административным управлением. Для определения маршрута внутри AS используется протокол внутридоменной маршрутизации (OSPF, RIP). Примером AS может служить интернет-провайдер или сеть организации.

В протоколе BGP и его расширениях выделяют понятия *control-plane* (информационные сообщения о маршрутах в BGP) и *data-plane* (трафик, содержащий полезные данные клиентов) [4] и рассматривают следующие задачи безопасности [5]:

– AS Number Authentication (control-plane);

– Prefix Origination Verification (control-plane);

– Path Validation (control-plane/data-plane);

– Data Integrity (control-plane/data-plane).

1.2. Определение проблемы

Анализ безопасных модификаций BGP (psBGP, S-BGP, soBGP, SPV, IRV) показал, что данные протоколы не выполняют проверку маршрута на уровне data-plane (см. табл. 1).

Таблица 1

Протоколы безопасной маршрутизации и решаемые в них задачи обеспечения безопасности

Задачи / Протоколы	AS Number Authentication		Prefix Origination verification		Path validation		Data Integrity	
	Control plane	Data plane	Control plane	Data plane	Control plane	Data plane	Control plane	Data plane
S-BGP	реш-ся	отсут.	реш-ся	отсут.	реш-ся	не реш-ся	реш-ся	реш-ся
psBGP	реш-ся	отсут.	реш-ся	отсут.	реш-ся	не реш-ся	реш-ся	реш-ся
soBGP	реш-ся	отсут.	реш-ся	отсут.	реш-ся	не реш-ся	реш-ся	реш-ся
SPV	реш-ся	отсут.	реш-ся	отсут.	реш-ся	не реш-ся	реш-ся	реш-ся
IRV	реш-ся	отсут.	реш-ся	отсут.	реш-ся	не реш-ся	реш-ся	реш-ся

Одним из решений этой задачи может быть применение схем упорядоченной коллективной подписи.

Под коллективной подписью (multisignature) будем подразумевать такую схему подписи, для которой справедливы следующие утверждения:

– выполняется агрегирование открытых ключей пользователей;

– выполняется агрегирование подписей пользователей;

– агрегирование выполняется последовательно (sequential);

– выполняется проверка агрегированным открытым ключом агрегированной подписи;

– размеры агрегированных ключа и подписи совпадают с размерами исходных ключей и подписей.

Для упорядоченной коллективной подписи справедливо следующее:

– выполняются все требования к коллективной подписи;

– в агрегированных открытом ключе и подписи заложены требуемый и фактический порядок подписывающих сторон соответственно.

В настоящей работе были исследованы схемы [3, 6, 8]. Каждая из них использует различный математический аппарат, однако все три схемы учитывают порядок подписантов, а также являются схемами коллективной подписи, проверка ЭП агрегированным ключом группы по трудоемкости аналогична проверке открытым ключом участника схемы.

В основу схемы [3] положена задача дискретного логарифмирования, поэтому схема не является стойкой к атакам с применением квантовых компьютеров. Отслеживание порядка подписантов вводится в схему с помощью дополнительных операций, то есть математический аппарат не поддерживает его по умолчанию.

Схема [6] использует изогении эллиптических кривых и основана на задаче CSSI, которая была решена позднее с помощью атаки [7] за полиномиальное время.

Схема упорядоченной подписи [8] на основе делегирования базиса решётки является предположительно стойкой к атакам с применением квантовых компьютеров. Однако формирование и проверка подписи выполняются медленнее, чем в схеме CSI-FiSh [9].

Таким образом, на данный момент не существует схемы упорядоченной ЭП, предположительно стойкой к атакам на квантовом компьютере и использующей аппарат изогений эллиптических кривых.

2. Моделирование схемы упорядоченной коллективной подписи

2.1. Обоснование выбора математического аппарата для моделирования

На основе анализа схем, приведённых выше, сформулированы подходы к созданию схем упорядоченной коллективной подписи.

1) *Использование свойств математического аппарата* [6, 8]. Результирующая изогения в подписи [6] зависит от порядка пользовательских изогений в их композиции.

2) *Искусственное добавление отслеживания порядка подписания в коллективную подпись* [3]. К схеме коллективной подписи добавлены дополнительные вычисления, результирующее значение которых зависит от того, в каком порядке участники подписывают сообщение.

В качестве математического аппарата для моделирования схемы были выбраны изогении эллиптических кривых, так как с их использованием возможна реализация квантово-устойчивых схем, а в схеме [8] формирование и проверка подписи выполняются медленнее, чем в схеме CSI-FiSh [9].

2.2. Построение модели схемы упорядоченной коллективной подписи

В ходе исследования была модифицирована схема коллективной подписи [10] на основе CSI-FiSh [9] для достижения свойства

упорядоченности. В качестве вычислительно трудной задачи используется задача множественного обращения групповой операции (MT-GAIP). Смоделированная схема является предположительно стойкой к атакам с использованием квантового компьютера.

Схема 1

Генерация параметров. Выбрать стартовую суперсингулярную эллиптическую кривую E_0 (как в CSI-FiSh) и вычислить $N = \#E$. Положить $\mathbb{G} = \mathbb{Z}_N$. Выбрать параметр безопасности λ: $t = \frac{\lambda}{log_2(k)}$ и криптографические хэш-функции: $H_{agg}: \{0,1\}^* \longrightarrow \mathbb{G}$ и $H_{sign}: \{0,1\}^* \longrightarrow \{-k+1, k-1\}^t$. В протоколе фигурируют n участников: $P_1, \dots, P_n$.

Генерация ключей. Для каждого j-го пользователя: выбрать $k-1$ закрытых ключей $\left(x_1^{(j)}, \dots, x_{k-1}^{(j)}\right) \longleftarrow \mathbb{G}$ и соответствующие открытые ключи $\left(Y_1^{(j)}, \dots, Y_{k-1}^{(j)}\right)$, где $Y_i = [x_i]E_0$ для $i \in [1, k-1]$.

Агрегирование ключей. Каждый участник P_j для $i \in [1, k-1]$ вычисляет коэффициенты агрегирования $a_i^{(j)} = H_{agg}\left(Y_i^{(j)} || L_{pk}\right)$, где $L_{pk} = \left(Y_1^{(1)}, \dots, Y_{k-1}^{(1)}, \dots, Y_1^{(n)}, \dots, Y_{k-1}^{(n)}\right)$ – список открытых ключей всех пользователей. Кривые инициализируются как: $\left(\bar{Y}_1^{(0)}, \dots, \bar{Y}_{k-1}^{(0)}\right) \longleftarrow (E_0, \dots, E_0)$. Каждый участник P_j получает $\left(\bar{Y}_1^{(j-1)}, \dots, \bar{Y}_{k-1}^{(j-1)}\right)$ от участника P_{j-1} (P_1 работает с $\bar{Y}_i^{(0)}$) и вычисляет $\bar{Y}_i^{(j)} = \left[a_i^{(j)} \cdot x_i^{(j)} \cdot j\right] \bar{Y}_i^{(j-1)}$ для $i \in [1, k-1]$, используя свои секретные ключи $\left(x_1^{(j)}, \dots, x_{k-1}^{(j)}\right)$. В конце P_n вычисляет $\bar{Y}_i = \bar{Y}_i^{(n)} = \left[a_i^{(1)} \cdot x_i^{(1)} \cdot 1\right] \dots \left[a_i^{(j)} \cdot x_i^{(j)} \cdot j\right] \dots [a_i^{(n)} \cdot x_i^{(n)} \cdot n]E_0 = \left[a_i^{(1)} \cdot x_i^{(1)} \cdot 1 + \dots + a_i^{(j)} \cdot x_i^{(j)} \cdot j + \dots + a_i^{(n)} \cdot x_i^{(n)} \cdot n\right] E_0$ для $i \in [1, k-1]$ и отправляет агрегированный ключ $Agg = (\bar{Y}_1, \dots, \bar{Y}_{k-1})$ остальным участникам.

Формирование подписи. Обязательство. P_j выбирает $\left(b_1^{(j)}, \dots, b_t^{(j)}\right) \longleftarrow \mathbb{G}$. Стартовые кривые инициализируются как $(E_1^0, \dots, E_t^0) \longleftarrow (E_0, \dots, E_0)$. Участник P_j получает $\left(E_1^{(j-1)}, \dots, E_t^{(j-1)}\right)$ от P_{j-1} и вычисляет $E_i^{(j)} = \left[b_i^{(j)} \cdot j\right] E_i^{(j-1)}$ для $i \in [1, t]$. В конце P_n вычисляет $E_i^{(n)} = \left[b_i^{(n)} \cdot n\right] E_i^{(n-1)} = \left[b_i^{(1)} \cdot 1\right] \dots \left[b_i^{(j)} \cdot j\right] \dots \left[b_i^{(n)} \cdot n\right] E_0$ для $i \in [1, t]$ и рассылает $(E_1, \dots, E_t) = \left(E_1^{(n)}, \dots, E_t^{(n)}\right)$ остальным. Запрос. Каждый участник P_j вычисляет $(c_1, \dots, c_t) = H_{sign}(E_1 \dots E_t \,||\, m)$. Ответ. Каждый участник P_j вычисляет $r_i^{(j)} = b_i^{(j)} \cdot j - sign(c_i) a_{|c_i|}^{(j)} x_{|c_i|}^{(j)} j (mod\, N)$ для $i \in [1, t]$,

где $sign(\cdot)$ – знак. Формирование подписи. Каждый участник P_j формирует свою подпись $\sigma^{(j)} = \left(r_1^{(j)}, \dots, r_t^{(j)}, c_1, \dots, c_t\right)$.

Агрегирование подписей. Участник P_n вычисляет для $i \in [1, t]$ значение $r_i = \Sigma_{j=1}^{n} r_i^{(j)}$. Коллективная подпись $\Sigma = (r_1, \dots, r_t, c_1, \dots, c_t)$.

Проверка подписи. Выполняется проверка коллективной подписи на соответствие агрегированному открытому ключу. Для $i \in [1, t]$ вычисляется $E_i^* = [r_i]\bar{Y}_{c_i}$, $(c_1^*, \dots, c_t^*) = H_{sign}(E_1^*, \dots, E_t^* || m)$ и проверяется равенство $(c_1^*, \dots, c_t^*) = (c_1, \dots, c_t)$. Если оно выполнено, то подпись подлинная, иначе недействительна.

Корректность. $(c_1, \dots, c_t) = H_{sign}(E_1 \dots E_t \,||\, m)$. Для проверки $(c_1^*, \dots, c_t^*) = (c_1, \dots, c_t)$ имеем: $E_i^* = [r_i]\bar{Y}_{c_i} = \left[\sum_{j=1}^{n} b_i^{(j)} \cdot j - sign(c_i) a_{|c_i|}^{(j)} x_{|c_i|}^{(j)} j (mod\ N)\right]\left[sign(c_i) \sum_{j=1}^{n} a_{|c_i|}^{(j)} x_{|c_i|}^{(j)} j\right] E_0 = \left[\sum_{j=1}^{n} b_i^{(j)} \cdot j\right] E_0 = E_i^{(n)}$. То есть $\left([r_1]\bar{Y}_{c_1}^{(n)}, \dots, [r_t]\bar{Y}_{c_t}^{(n)}\right) = \left(E_1^{(n)}, \dots, E_t^{(n)}\right)$, $(c_1^*, \dots, c_t^*) = H_{sign}(E_1^*, \dots, E_t^* || m) = H_{sign}(E_1^{(n)}, \dots, E_t^{(n)} || m) = (c_1, \dots, c_t)$.

Предлагаемая схема наследует от схемы CSI-FiSh стойкость к следующим сценариям атаки:

1) *вскрытие личного ключа пользователя*: сводится к задаче обращения групповой операции (MT-GAIP);

2) *подделка сообщения*: сводится к поиску коллизии хэш-функции для генерации запросов.

При анализе безопасности предлагаемой схемы относительно нарушения свойства упорядоченности были рассмотрены также следующие сценарии:

1) *внедрение в цепочку подписи нарушителя*: если в агрегированном открытом ключе отсутствует ключ нарушителя, то при встраивании подписи нарушителя в цепочку проверка с помощью исходного агрегированного открытого ключа завершится неудачей;

2) *комбинирование подписи*: если нарушитель наблюдает подписи от (A, B) и (C, D) по отдельности, то он не сможет сгенерировать корректную подпись для (A, B, C, D), так как для этого необходимо будет поменять коэффициенты j в подписи, задача сводится к задаче вскрытия личных ключей;

3) *изменение порядка подписи сообщения*: в случае сговора пользователей группы не выполнится проверка корректности, так как надо изменить не только коэффициенты j при формировании подписи, но и использовать закрытые ключи другого участника.

Заключение

В работе изучена проблема моделирования квантово-устойчивой схемы упорядоченной коллективной подписи. Построена модель такой схемы. На данный момент предлагаемая схема является единственной

предположительно квантово-устойчивой схемой упорядоченной коллективной подписи, основанной на изогениях эллиптических кривых. Сделаны выводы об устойчивости предложенной модели к ряду сценариев атак на схему подписи, в том числе к атакам, направленным на нарушение свойства упорядоченности. Предлагаемая схема может быть применена на практике в информационных системах при проверке маршрутов сетевых пакетов, а также в системах электронного документооборота для построения иерархических систем.

Список литературы

1. Rodgers J. Quantum computers: available for free from your own home [Electronic resource] // The Tufts Daily – 2023. – URL: https://www.tuftsdaily.com/article/2023/10/quantum-computers-available-for-free-from-your-own-home (access date: 31.05.2024).

2. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th annual symposium on foundations of computer science. – IEEE, 1994. – Pp. 124–134.

3. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing / A. Boldyreva [et al.] // Proceedings of the 14th ACM conference on Computer and communications security. – 2007. – Pp. 276–285.

4. Feamster N., Balakrishnan H., Rexford J. Some foundational problems in interdomain routing // Proceedings of Third Workshop on Hot Topics in Networks (HotNets-III). – 2004. – Pp. 41–46.

5. Wan T., Kranakis E., van Oorschot P. C. Pretty secure BGP, psBGP [Electronic resource] // Proceedings of the Network and Distributed System Security Symposium, NDSS 2005, San Diego, CA, USA, January 2005. – URL: https://www.ndss-symposium.org/ndss2005/pretty-secure-bgp-psbgp/ (access date: 31.05.2024).

6. Ярмак А. В. Схема иерархической аутентификации на основе изогений эллиптических кривых: дипломная работа: 10.05.01 [Электронный ресурс] / Санкт-Петербургский политехнический университет Петра Великого, Институт компьютерных наук и технологий; науч. рук. Е. Б. Александрова. – СПб., 2018. – URL: https://elib.spbstu.ru/dl/2/v18-170.pdf/info (дата обращения: 31.05.2024).

7. Castryck W., Decru T. An efficient key recovery attack on SIDH (preliminary version) // IACR Cryptol. ePrint Arch. – 2022. – Vol. 2022. – P. 975.

8. Федичев А. В. Упорядоченная подпись на основе делегирования базиса решетки: выпускная квалификационная работа специалиста: направление 10.05.01 «Компьютерная безопасность»; образовательная программа 10.05. 01_02 «Математические методы защиты информации» / Санкт-Петербургский политехнический университет Петра Великого, Институт кибербезопасности и защиты информации; научный руководитель Е. Б. Александрова. – СПб., 2022. – URL: http://elib.spbstu.ru/dl/3/2022/vr/vr22-91.pdf (дата обращения: 31.05.2024).

9. 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. – Cham: Springer International Publishing, 2019. – Pp. 227–247.

10. de Goyon M., Miyaji A. Isogeny-Based Multi-signature Scheme // International Conference on Information Security Practice and Experience. – Singapore: Springer Nature Singapore, 2023. – Pp. 477–491.