УДК 330.1
doi:10.18720/SPBPU/2/id24-509

Александрова Елена Борисовна [1],
профессор, д-р техн. наук, доцент;
Костин Сергей Олегович [2],
студент;
Тулинова Анастасия Викторовна [3],
доцент, канд. техн. наук

МАСКИРОВАНИЕ ПАРАМЕТРОВ КАК СПОСОБ ПОВЫШЕНИЯ СТОЙКОСТИ ПРОТОКОЛА МНОЖЕСТВЕННОЙ ПОДПИСИ

[1,2,3] Россия, Санкт-Петербург,
Санкт-Петербургский политехнический университет Петра Великого,
[1] aleksandrova_eb@spbstu.ru, [2] kostin.so@edu.spbstu.ru,
[3] yarmak.av@spbstu.ru

Аннотация. Одним из преимуществ постквантовых протоколов на изогениях суперсингулярных эллиптических кривых является размер открытых параметров. Однако большинство SIDH-подобных схем на сегодняшний день не применимы. Для решения этой проблемы в работе использован метод маскирования параметров и рассмотрены пути его эффективной реализации.

Ключевые слова: множественная подпись, изогении, постквантовая криптография.

Elena B. Aleksandrova [1],
Professor, Doctor of Technical Sciences;
Sergey O. Kostin [2],
Student;
Anastasia V. Tulinova [3],
Associate Professor, Candidate of Technical Sciences

PARAMETER MASKING AS A WAY TO INCREASE THE RESISTANCE OF GROUP SIGNATURE

[1,2,3] Peter the Great St.Petersburg Polytechnic University, St. Petersburg, Russia,
[1] aleksandrova_eb@spbstu.ru, [2] kostin.so@edu.spbstu.ru,
[3] yarmak.av@spbstu.ru

Abstract. One of the advantages of post-quantum protocols based on isogenies of supersingular elliptic curves is the size of the public parameters. However, most of SIDH-like schemes are currently not applicable. To deal with this problem, we use the parameter masking and show how it can be effectively implemented.

Keywords: group signature, isogeny, post-quantum cryptography.

Введение

В августе 2024 года Национальный институт стандартов и технологий США (NIST) представил основные стандарты новых постквантовых алгоритмов. В их числе механизм формирования общего ключевого значения [1], а также два способа выработки цифровой подписи [2, 3]. При этом протокол SIKE [4], основанный на изогениях эллиптических кривых, выбыл из конкурса после того, как была опубликована атака по восстановлению его закрытого ключа [6], реализация которой даже на обычном ноутбуке занимает около одного часа. Универсальность данной атаки позволяет распространить ее и на другие SIDH-подобные схемы. А значит, многие схемы на изогениях не могут быть использованы без доработки.

В настоящее время в российской постквантовой криптографии можно выделить такие алгоритмы как «Шиповник» [5], «Крыжовник» и «Гиперикум». Ни один из данных алгоритмов в качестве своей основы не использует аппарат изогений эллиптических кривых.

Тем не менее аппарат изогений все еще является привлекательным, поскольку обеспечивает наименьший размер открытых параметров. К тому же, атаку на протокол SIDH можно использовать и для эффективного вычисления изогении между двумя кривым, как это реализовано в работах [7–9].

1. Постановка задачи

1.1. Описание предметной области

Протоколы [2, 3] на сегодняшний день позволяют формировать только электронную подпись сообщения. Протоколы «Шиповник» и «Гиперикум» пока только претендуют быть стандартизованными, при этом также являются протоколами подписи.

На практике же часто требуется такая схема электронной подписи, которая позволяла бы подписывать сообщение не только одному участнику, но и определенному коллективу или группе. При этом группа участников в результате должна сформировать единую подпись для сообщения. Например, если необходимо удостовериться, что пакет в сети прошел через заранее определенные роутеры, или же что устройства определенной системы были инициализированы в заранее определенном порядке. Во всех этих случаях задачу можно решить с помощью формирования общей подписи для сообщения. На сегодня не существует квантово-устойчивых алгоритмов для ее решения, поэтому разрабатываемый протокол должен удовлетворять следующим требованиям:

1) для множества участников формируется одна единая подпись;

2) проверка подписи не должна осуществляться с использованием доверенной стороны;

3) размер формируемой подписи не должен зависеть от числа участников;

4) протокол должен быть устойчивым к атакам на квантовом компьютере.

Одной из наиболее удобных математических структур для решения поставленной задачи являются изогении эллиптических кривых. Ввиду их особенностей, описанные выше требования легко переносятся на данную область. Более того, изогении позволяют получать подпись существенно меньших размеров.

1.2. Определение проблемы

Для получения результирующей подписи как можно меньшей длины, необходимо использовать SIDH-подобные схемы, так как на текущий момент именно они предлагают необходимый размер параметров. Главной проблемой при использовании SIDH-подобных схем является раскрытие как точек (P_A, Q_A) подгруппы группы кручения на стартовой кривой E_0, так и их образа $(\varphi(P_A), \varphi(Q_A))$ на результирующей кривой E, при этом $\varphi: E_0 \to E$ – изогения между кривыми E_0 и E. Вместе с информацией о степени $deg\,\varphi$ изогении данный набор может быть использован для реализации атаки [6].

Таким образом, для решения данной проблемы необходимо либо полностью отказаться от использования таких параметров, либо рассмотреть метод, в котором можно было бы скрыть один или несколько параметров, что не позволило бы получить исчерпывающий набор для проведения атаки.

2. Моделирование системы множественной подписи

2.1. Обоснование выбора языка моделирования

За основу модели взят подход, представленный в протоколе FESTA. На образ точек подгруппы группы кручения предлагается накладывать маску в виде матрицы A_{2x2}, которая имеет формат $\begin{pmatrix} a_1 & 0 \\ 0 & a_4 \end{pmatrix}$. Данный формат обусловлен необходимостью выполнения свойства коммутативности: $AB = BA$. Однако в нашем случае данное свойство является избыточным, поэтому можно использовать матрицу в «полном виде», а именно $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$. Образ точек на итоговый кривой принимает вид

$$\begin{pmatrix} P \\ Q \end{pmatrix} = A \begin{pmatrix} \varphi(P_0) \\ \varphi(Q_0) \end{pmatrix}.$$

Также особенностью протокола FESTA является наличие двух функций $f_{PK}(p) = c$ и $f_{SK}^{-1}(c) = p$. Для простоты будем считать, что первая функция формирует шифртекст по открытому ключу участника, а вторая функция является обратной, то есть по закрытому ключу первого участника формирует исходное значение. Вторая функция является трудно обратимой, поэтому только обладатель закрытого ключа может легко ее вычислить. Дополнительной особенностью обратной функции является метод вычисления: использование атаки [6] для эффективного восстановления изогении.

Используя данную особенность протокола FESTA, а также изначальное условие о том, что необходимо получить протокол инициализации системы, в котором сообщение последовательно передается от одного устройства к другому в заранее определенном порядке, можно дополнительно добавить в моделируемый протокол возможность аутентификации промежуточного участника.

2.2. Построение модели протокола множественной подписи

Для описания шагов протокола для простоты рассмотрим промежуточный k-й шаг:

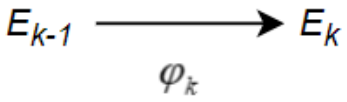

Рис. 1. Промежуточный шаг протокола

На данном шаге участник с номером k-1 передает сообщение участнику с номером k. Так как сообщение передается по известному маршруту, это позволяет участнику с номером k однозначно определить открытые параметры участника с номером k-1 и выполнить его аутентификацию по следующему алгоритму:

1) k-й участник, получив сообщение для формирования подписи, генерирует случайное значение по заранее известным параметрам (k-1)-го участника, используя функцию $f_{PK_{k-1}}(p) = c$, и передает выработанное значение;

2) (k-1)-й участник формирует значение $f^{-1}_{SK_{k-1}}(c) = p$, используя свой закрытый ключ, и отправляет его k-му участнику;

3) если данные совпадают, то k-й участник считает, что аутентификация выполнена успешно, и может выполнять дальнейшие шаги по формированию подписи.

В данном сценарии только обладатель закрытого ключа может однозначно выполнить обратную операцию; при этом злоумышленник, наблюдая сообщения p и c в открытом канале, не получает дополнительной информации ввиду того, что, зная общеизвестный открытый ключ, любой из участников может вычислить функцию $f_{PK_{k-1}}(p) = c$.

На основе данных свойств построим протокол по следующей модели:

1) на стартовой кривой E_0 случайным образом генерируются точки P_M, Q;

2) формируется хэш-значение $h = H(M)$ для подписываемого сообщения M, а также пара точек $(P_M, Q_M = hQ)$;

3) первый участник генерирует маску $A_{2x2}: det\, A \neq 0$;

4) на основе своего закрытого ключа участник вычисляет значения $(\varphi_1(P_M), \varphi_1(Q_M))$, после чего накладывает на них сгенерированную маску, получая новые точки:

$$\begin{pmatrix} R_{1,A} \\ S_{1,A} \end{pmatrix} = A_1 \begin{pmatrix} \varphi_1(P_M) \\ \varphi_1(Q_M) \end{pmatrix};$$

5) вместе с полученным точками первый участник отправляет следующему значения $deg\,\varphi_1\,(a_{1,1}a_{1,4} - a_{1,2}a_{1,3})$ и исходные точки (P_M, Q_M);

6) второй участник выполняет аутентификацию первого по рассмотренным ранее шагам; в случае успешной аутентификации проверяется промежуточная подпись с использованием свойств спаривания Вейля: $e(R_{1,A}, S_{1,A}) = e(P_M, Q_M)^{deg(\varphi)(a_1a_4 - a_2a_3)}$;

7) при успешной проверке в качестве начальных точек (P_M, Q_M) используются точки $R_{1,A}$ и $S_{1,A}$; шаги повторяются, начиная с третьего.

На финальном этапе присутствует набор значений:

$$\begin{pmatrix} R_{n,A} \\ S_{n,A} \end{pmatrix} = A_n \begin{pmatrix} \psi(P_M) \\ \psi(Q_M) \end{pmatrix}, \begin{pmatrix} P_M \\ Q_M \end{pmatrix}, r = deg\,\varphi_1\,(a_{1,1}a_{1,4} - a_{1,2}a_{1,3}) \cdot$$
$$deg\,\varphi_2\,(a_{2,1}a_{2,4} - a_{2,2}a_{2,3}) \cdot \ldots \cdot deg\,\varphi_n\,(a_{n,1}a_{n,4} - a_{n,2}a_{n,3}).$$

Это позволяет проверить итоговую сформированную подпись по следующему равенству

$$e(R_{n,A}, S_{n,A}) = e(P_M, Q_M)^r =$$
$$= e(P_M, Q_M)^{deg\,\varphi_1(a_{1,1}a_{1,4} - a_{1,2}a_{1,3}) \cdot deg\,\varphi_2(a_{2,1}a_{2,4} - a_{2,2}a_{2,3}) \cdot \ldots \cdot deg\,\varphi_n(a_{n,1}a_{n,4} - a_{n,2}a_{n,3})}.$$

Раскрытие этих значений не позволяет провести атаку [6], поскольку степень, и образ исходных точек скрыты под маской. Применив подобную модификацию, мы не сильно проигрываем и в размере открытых параметров.

Сравнение размеров открытого ключа приведено в таблице 1. Протокол FESTA, хотя и используется для формирования общего ключевого значения, приведен только потому, что он является базовым при моделировании схемы. Увеличение размера открытого ключа очевидно связано с передачей не только исходных точек, но и значения степени под маской. Из сравнения также видно, что протокол уже в текущей модели выигрывает у постквантовых протоколов формирования подписи Crystal-Dilithium и Falcon. Сравнительно малый размер открытого ключа протокола SPHINCS+ обусловлен большим размером подписи, что отражено в таблице 2.

Таблица 1

Сравнение размеров открытого ключа

Протокол	Размер открытого ключа (байт), в соответствии с уровнем безопасности по NIST		
	128	192	256
Предлагаемый протокол	630	991	1419
FESTA [7]	561	864	1246
Crystal-Dilithium [2]	1312	1952	2592
Falcon [10]	897	~1017	1280
SPHINCS+ [3]	32	48	64

Таблица 2

Сравнение размеров подписи

Протокол	Размер подписи (байт), в соответствии с уровнем безопасности по NIST		
	128	192	256
Предлагаемый протокол	2579	3928	5540
Crystal-Dilithium [2]	2420	3293	4595
Falcon [10]	666	~989	1280
SPHINCS+ [3]	7856 (17088)	16224 (35664)	29792 (49856)

Модель предлагаемого протокола существенно выигрывает по размеру подписи у протокола SPHINCS+, но при этом незначительно проигрывает новым стандартам. Тем не менее для выполнения свойств множественной подписи новые стандарты требуют модификаций, что может дополнительно увеличить как размер открытого ключа, так и подписи.

Заключение

Метод маскирования параметров показывает, как, используя тривиальную операцию, можно полностью защититься от достаточно производительной атаки на криптосистемы, не потеряв при этом в изначальной производительности. Построенная на базе протокола FESTA модель дополнительно подчеркивает эту особенность. Также разработанная модель показывает, что SIDH-подобные протоколы все еще могут применяться на практике. Сделаны выводы о размерах открытых параметров. Даже в текущей модели протоколы на изогениях в своей неоптимизированной версии могут быть предпочтительнее чем новые стандарты, размер параметров которых уже приведен к допустимому минимуму. Тем не менее область изогений эллиптических кривых все еще является сравнимо молодой и перед реальным внедрением в системы требует детального изучения и анализа.

Список литературы

1. FIPS 203 (Draft). Module-lattice-based key-encapsulation mechanism standard [Electronic resource]. – Federal Information Processing Standards Publication. August 24, 2023. – URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf (access date: 31.05.2024).

2. FIPS 204 (Draft). Module-lattice-based digital signature standard [Electronic resource]. – Federal Information Processing Standards Publication. August 24, 2023. – URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf (access date: 31.05.2024).

3. FIPS 205 (Draft). Stateless hash-based digital signature standard [Electronic resource]. – Federal Information Processing Standards Publication. August 24, 2023. – URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf (access date: 31.05.2024).

4. Jao D., Azarderakhsh R., Campagna M., Costello C., De Feo L., Hess B., Jalali A., Koziel B., LaMacchia B., Longa P., Naehrig M., Renes J., Soukharev V., Urbanik D. SIKE: Supersingular Isogeny Key Encapsulation // sike.org. – 2017.

5. Высоцкая В. В., Чижов И. В. О стойкости кодовой электронной подписи на основе протокола идентификации Штерна // Прикладная дискретная математика. – Изд. 57. – 2022. – С. 67–90. – DOI:https://doi.org/10.17223/20710410/57/5.

6. Castryck W., Decru T. An efficient key recovery attack on SIDH // In: C. Hazay, M. Stam (eds.) Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part V. – Lecture Notes in Computer Science. – Vol. 14008. – Berlin, Heidelberg: Springer-Verlag, 2023. – Pp. 423–447. – DOI: doi.org/10.1007/978-3-031-30589-4_15.

7. Basso A., Maino L., Pope G. FESTA: Fast Encryption from a Supersingular Torsion Attacks // In: J. Guo, R. Steinfeld (eds.) Advances in Cryptology – ASIACRYPT 2023. – Singapore: Springer Nature Singapore, 2023. – Pp. 98–126.

8. Nakagawa K., Onuki H. QFESTA: efficient algorithms and parameters for FESTA using quaternion algebras [Electronic resource] // IACR Cryptol. ePrint Arch. – 2023. – Paper 2023/1468. – URL: https://eprint.iacr.org/2023/1468 (access date: 31.05.2024).

9. Moriya T. IS-CUBE: an isogeny-based compact KEM using a boxed SIDH diagram [Electronic resource] // IACR Cryptol. ePrint Arch. – 2023. – Paper 2023/1506. – URL: https://eprint.iacr.org/2023/1506 (access date: 31.05.2024).

10. Fouque P., Hoffstein J., Kirchner P., Lyubashevsky V., Pornin T., Prest T., Ricosset T., Seiler G., Whyte W., Zhang Z. Falcon: fast-fourier lattice-based compact signatures over NTRU [Electronic resource]. – Specifications v1.0. – 2019. – URL: https://www.di.ens.fr/~prest/Publications/falcon.pdf (access date: 31.05.2024).