НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2026 Том 26 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2026 Vol. 26 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КРАТКИЕ СООБЩЕНИЯ

BRIEF PAPERS

doi: 10.17586/2226-1494-2026-26-2-442-445
УДК 004.056.2

Забывчивая подпись на основе теории изогений эллиптических кривых

Алтана Феликсовна Хуцаева✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

afkhutsaeva@itmo.ru✉, https://orcid.org/0000-0001-5494-7142

Аннотация
В работе представлена новая схема постквантовой забывчивой подписи типа 1-из-*n*, построенная на изогениях суперсингулярных эллиптических кривых. В качестве основы использована схема Commutative Supersingular Isogeny based Fiat-Shamir, стойкость которой опирается на предположение о сложности многоцелевой задачи обращения группового действия. Такой подход обеспечивает устойчивость к атакам с использованием алгоритма Шора. Формализованы алгоритм генерации ключей, протокол интерактивного формирования подписи и алгоритм верификации. Экспериментальная оценка в среде SageMath демонстрирует более чем трехкратное снижение объема передаваемых данных относительно аналога на решетках.

Ключевые слова
забывчивая подпись, постквантовая криптография, изогении эллиптических кривых, цифровая подпись, MT-GAIP, CSI-FiSh

Благодарности
Работа выполнена в рамках государственного задания (проект FSER-2025-0003).
Автор признателен С.В. Беззатееву за научное руководство и ценные консультации. Также автор выражает благодарность анонимному рецензенту и редактору за конструктивную критику, способствовавшую улучшению статьи.

Ссылка для цитирования: Хуцаева А.Ф. Забывчивая подпись на основе теории изогений эллиптических кривых // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 2. С.442–445. doi: 10.17586/2226-1494-2026-26-2-442-445

Oblivious signature based on the theory of elliptic curve isogeny

Altana F. Khutsaeva✉

ITMO University, Saint Petersburg, 197101, Russian Federation
Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation

afkhutsaeva@itmo.ru✉, https://orcid.org/0000-0001-5494-7142

Abstract
This paper presents a novel 1-out-of-*n* post-quantum oblivious signature scheme based on supersingular elliptic curve isogenies. The proposed scheme is built upon the Commutative Supersingular Isogeny based Fiat-Shamir scheme whose security relies on the hardness assumption of the multiple-target group action inverse problem. This approach ensures resistance against attacks using Shor's algorithm. The key generation algorithm, the interactive signing protocol, and the verification algorithm are formalized. Experimental evaluation in SageMath demonstrates more than a threefold reduction in communication overhead compared to a lattice-based counterpart.

Keywords
oblivious signature, post-quantum cryptography, isogenies of elliptic curves, digital signature, MT-GAIP, CSI-FiSh

Acknowledgements
This research was funded by the State Assignment grant number FSER-2025-0003.
The author is grateful to S.V. Bezzateev for scientific supervision and valuable advice. The author also wishes to thank the anonymous reviewer and the editor for their constructive criticism which helped improve this paper.

For citation: Khutsaeva A.F. Oblivious signature based on the theory of elliptic curve isogeny. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 2, pp. 442–445 (in Russian). doi: 10.17586/2226-1494-2026-26-2-442-445

Забывчивая подпись 1-из-n представляет собой криптографический протокол, позволяющий пользователю получить подпись только на одно сообщение из n возможных сообщений. При этом подписывающая сторона не может определить, какое именно сообщение из множества подписанных ею было выбрано пользователем. Ключевое свойство этого примитива состоит в том, что подписант остается неосведомленным о выборе пользователя, а пользователь может получить подпись лишь на одно из n сообщений, которые он отправлял подписывающей стороне для подписи. Таким образом, можно дать следующее определение.

Определение 1. Забывчивая подпись 1-из-n — интерактивная схема подписи, которая позволяет получателю подписи получить валидную подпись σ_i на одно и только одно сообщение m_i из открытого множества сообщений $\{m_1, \ldots, m_n\}$. При этом подписант по завершении протокола подписи не узнает, какое именно сообщение m_i с соответствующей ему подписью σ_i было выбрано из подписанных им сообщений $\{m_1, \ldots, m_n\}$.

Забывчивые подписи решают проблему обеспечения приватности и анонимности в системах, требующих проверяемого приватного выбора. К таким системам относятся электронные платежи, схемы анонимных учетных данных и протоколы приватного доступа к базам данных [1].

С появлением угрозы квантовых компьютеров, способных нарушить стойкость классических криптографических алгоритмов (RSA [2], ГОСТ Р 34.10-2012[1]), разработка постквантовых аналогов становится критически важной задачей. Существующие схемы забывчивых подписей [3–5] уязвимы для квантового алгоритма Шора [6].

Разработка постквантовых забывчивых подписей является необходимым условием обеспечения долгосрочной безопасности и приватности различных систем. Постквантовые алгоритмы основываются на математических задачах, которые считаются трудными для решения даже при наличии квантовых вычислителей. Это гарантирует, что достигнутый сегодня уровень приватности пользователей не будет нарушен по мере развития квантовых технологий.

Существующие схемы постквантовых забывчивых подписей, основанные на теории решеток [7] и теории изогений эллиптических кривых [8], обладают недостатками. Так, схема [7] требует для хранения и передачи данных большого объема памяти по сравнению со схемой подписи на изогениях эллиптических кривых [8]. Однако схема подписи, предложенная в работе [8], требует доработок для повышения стойкости подписи.

Важным результатом настоящей работы является повышение криптографической стойкости подписи по сравнению со схемой подписи, предложенной в [8], где забывчивая подпись основана на задаче обращения группового действия (Group Action Inverse Problem, GAIP) и подходе Шнорра. Однако прямая адаптация схемы Шнорра для групповых действий может создавать уязвимости, связанные с компрометацией подписи без решения сложной задачи. Предлагаемая схема подписи основана на многоцелевой задаче обращения группового действия (Multi-Target GAIP, MT-GAIP) и использует идеи построения подписи Commutative Supersingular Isogeny based Fiat-Shamir (CSI-FiSh) [9]. CSI-FiSh является постквантовой схемой цифровой подписи с доказуемой стойкостью в модели случайного оракула. Предлагаемая схема подписи включает в себя алгоритмы генерации ключей и верификации, а также интерактивный протокол подписи.

Рассмотрим описание схемы постквантовой забывчивой подписи на изогениях эллиптических кривых. В протоколе, реализующем подпись, принимают участие: пользователь — получатель подписи, подписант — подписывающая сторона. Под H: $\{0, 1\}^* \rightarrow \rightarrow \{-S + 1, \ldots, S - 1\}^t$ понимается криптографическая хэш-функция, где S — параметр безопасности подписи.

Кратко опишем математический аппарат изогений эллиптических кривых. Пусть E — суперсингулярная эллиптическая кривая, заданная над конечным полем $\mathbb{F}_p$, p — простое число. Обозначим через $\mathcal{O} = End_{\mathbb{F}_p}(E)$ — кольцо эндоморфизмов кривой E, определенное над $\mathbb{F}_p$. Это кольцо коммутативно и изоморфно порядку в мнимом квадратичном поле $\mathbb{Q}(\sqrt{-p})$. Группу классов идеалов кольца $\mathcal{O}$ обозначим как $Cl(\mathcal{O})$, ее порядок (мощность) $N = |Cl(\mathcal{O})|$.

Действие группы классов идеалов $Cl(\mathcal{O})$ на множестве эллиптических кривых $Ell_{\mathbb{F}_p}(\mathcal{O}, \pi)$, где под π понимается эндоморфизм Фробениуса, определим как отображение $Cl(\mathcal{O}) \times Ell_{\mathbb{F}_p}(\mathcal{O}, \pi) \rightarrow Ell_{\mathbb{F}_p}(\mathcal{O}, \pi)$ или, в случае циклической группы как в работе [9], $\mathbb{Z}_N \times Ell_{\mathbb{F}_p}(\mathcal{O}, \pi) \rightarrow \rightarrow Ell_{\mathbb{F}_p}(\mathcal{O}, \pi)$, где $\mathbb{Z}_N$ — кольцо классов вычетов по модулю N. Получим, что применение конкретного класса идеалов $[a] \in Cl(\mathcal{O})$ к конкретной эллиптической кривой $E_0 \in Ell_{\mathbb{F}_p}(\mathcal{O}, \pi)$ порождает изогенную кривую E_1, обозначим это действие как $[a]E_0 = E_1$.

Определим задачу MT-GAIP. Пусть заданы кривые $E_0, E_1, \ldots, E_k \in Ell_{\mathbb{F}_p}(\mathcal{O}, \pi)$. Задача состоит в том, чтобы найти идеал $a \subset \mathcal{O}$ (или эквивалентный ему элемент группы классов $[a] \in Cl(\mathcal{O})$) такой, что $[a]E_i = E_j$ для $i, j \in \{0, \ldots, k\}$, $i \neq j$. Данная задача считается вычислительно трудной [9].

[1] ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введ. 01.01.2013. М.: Стандартинформ, 2013. 24 с.

Алгоритм 1. Генерация ключей. Входные данные: параметр безопасности подписи S, стартовая эллиптическая кривая E_0, мощность N группы классов идеалов $Cl(\mathcal{O})$.

Выходные данные: секретный ключ sk, открытый ключ PK.

1. Для $i \in \{1, \ldots, S-1\}$:
1.1. $a_i \in_R \mathbb{Z}_N$;
1.2. $E_i = [a_i]E_0$.
2. $sk = \{a_i\}_{i\in\{1,\ldots,S-1\}}$ и $PK = \{E_i\}_{i\in\{1,\ldots,S-1\}}$.

Протокол. Подпись. Входные данные: множество сообщений M, мощность множества сообщений n, стартовая эллиптическая кривая E_0, секретный ключ sk, открытый ключ PK, параметры безопасности подписи t и S, мощность N группы классов идеалов $Cl(\mathcal{O})$.

Выходные данные: подпись σ.

1. Для всех $j \in \{1, \ldots, n\}$, $i \in \{1, \ldots, t\}$:
1.1. подписант выбирает значение $b_i^{(j)} \in_R \mathbb{Z}_N$;
1.2. подписант вычисляет кривую $E_i^{(j)} = [b_i^{(j)}]E_0$.
2. Подписант отправляет полученный набор кривых $\{E_i^{(j)}\}_{i\in\{1,\ldots,t\};\, j\in\{1,\ldots,n\}}$ пользователю.
3. Для $i \in \{1, \ldots, t\}$:
3.1. пользователь выбирает $s_i \in_R \mathbb{Z}_N$;
3.2. пользователь вычисляет кривую $E_{s_i} = [s_i]E_i^{(l)}$, где l — индекс сообщения, на которое пользователь хочет получить подпись.
4. Пользователь формирует множество сообщений $M = \{m_1, \ldots, m_n\}$ и набор кривых $\{E_{s_i}\}_{i\in\{1,\ldots,t\}}$ и отправляет эти данные подписанту.
5. Для $j \in \{1, \ldots, n\}$ подписант вычисляет:
5.1. $(c_1^{(j)}, \ldots, c_t^{(j)}) = H(E_{s_1}\|\ldots\|E_{s_t}\|m_j)$;
5.2. для $i \in \{1, \ldots, t\}$:
5.2.1. $r_i^{(j)} = b_i^{(j)} - sign(c_i^{(j)})a_{|c_i^{(j)}|} mod\ N$, где $sign(c_i^{(j)})$ возвращает знак числа $c_i^{(j)}$, $a_{|c_i^{(j)}|} \in sk$.
6. Подписант формирует промежуточный набор подписей $\{(c_1^{(j)}, \ldots, c_t^{(j)}, r_1^{(j)}, \ldots, r_t^{(j)})\}_{j\in\{1,\ldots,n\}}$ и отправляет пользователю.
7. Для каждого $i \in \{1, \ldots, t\}$ пользователь вычисляет:
7.1. $r_i = r_i^{(l)} + s_i$;
7.2. $E_{r_i} = [r_i]E_{c_i^{(l)}}$, где $E_{c_i^{(l)}} \in PK$.
8. Пользователь проверяет равенство $H(E_{r_1}\|\ldots\|E_{r_t}\|m_l) = (c_1^{(l)}, \ldots, c_t^{(l)})$.
9. Если равенство на шаге 8 выполняется, то пользователь устанавливает подпись $\sigma = (r_1, \ldots, r_t, c_1, \ldots, c_t)$, где $(c_1, \ldots, c_t) = (c_1^{(l)}, \ldots, c_t^{(l)})$. В противном случае пользователь устанавливает подпись $\sigma = \perp$.

Алгоритм 2. Верификация. Входные данные: сообщение m, подпись $\sigma = (r_1, \ldots, r_t, c_1, \ldots, c_t)$, открытый ключ PK.

Выходные данные: ver = True или False.

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

Таким образом, предлагается схема постквантовой забывчивой подписи 1-из-n, где пользователь может получить подпись только на одно сообщение из n возможных. Использование подписи CSI-FiSh [9] в качестве базового примитива позволяет достичь компактности, недоступной для аналогов на решетках [7], при этом обеспечивая стойкость на основе сложности задачи MT-GAIP.

Программная реализация на языке программирования Python, подтверждающая работоспособность предлагаемого решения, была выполнена в среде SageMath 9.3 для параметров CSIDH-512 [10], $S = 2^{10}$, $t = 11$, соответствующих уровню стойкости 128 бит [9]. В качестве вычислительной платформы использовался персональный компьютер со следующими характеристиками: процессор AMD Ryzen 7 4800U (1,8 ГГц), оперативная память 16 ГБ.

На рисунке показана зависимость объема передаваемых данных от параметра n для предлагаемой схемы и схемы работы [7]. По сравнению со схемой [7], предлагаемое решение характеризуется не только меньшим начальным объемом данных, но и существенно более низкой скоростью роста относительно параметра n. Полученные результаты обосновывают преимущество предлагаемого решения над аналогом на решетках [7] в системах, критичных к объему передаваемой информации.

В настоящей работе предложена схема постквантовой забывчивой подписи 1-из-n, использующая математический аппарат изогений эллиптических кривых. Предложенное решение обеспечивает анонимность выбора сообщения для пользователя.

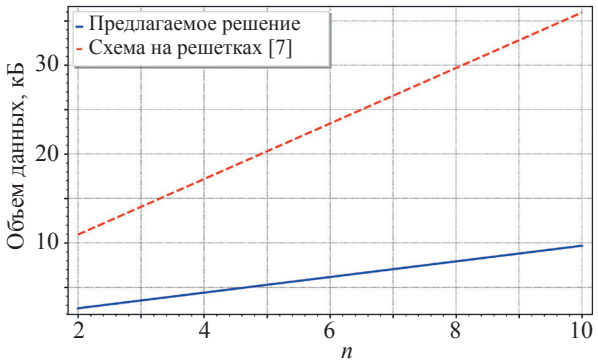

Рисунок. Зависимость объема передаваемых данных от параметра n

Figure. Dependence of communication size on parameter n

Литература

1. Khutsaeva A., Leevik A., Bezzateev S. A Survey of post-quantum oblivious protocols // Cryptography. 2025. V. 9. N 4. P. 62. https://doi.org/10.3390/cryptography9040062
2. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. V. 21. N 2. P. 120–126. https://doi.org/10.1145/359340.359342
3. Chen L. Oblivious signatures // Lecture Notes in Computer Science. 1994. V. 875. P. 161–172. https://doi.org/10.1007/3-540-58618-0_62
4. Tso R., Okamoto T., Okamoto E. 1-out-of-n oblivious signatures // Lecture Notes in Computer Science. 2008. V. 4991. P. 45–55. https://doi.org/10.1007/978-3-540-79104-1_4
5. Tso R. Two-in-one oblivious signatures // Future Generation Computer Systems. 2019. V. 101. P. 467–475. https://doi.org/10.1016/j.future.2019.06.014
6. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Review. 1999. V. 41. N 2. P. 303–332. https://doi.org/10.1137/s0036144598347011
7. You J.-S., Liu Z.-Y., Tso R., Tseng Y.-F., Mambo M. Quantum-resistant 1-out-of-n oblivious signatures from lattices // Lecture Notes in Computer Science. 2022. V. 13504. P. 166–186. https://doi.org/10.1007/978-3-031-15255-9_9
8. Хуцаева А.Ф., Давыдов В.В., Беззатеев С.В. Схема забывчивой подписи, построенная на изогениях суперсингулярных эллиптических кривых // Проблемы информационной безопасности. Компьютерные системы. 2023. № 4 (57). С. 116–121. https://doi.org/10.48612/jisp/2m49-vg37-99pt
9. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations // Lecture Notes in Computer Science. 2019. V. 11921. P. 227–247. https://doi.org/10.1007/978-3-030-34578-5_9
10. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an efficient post-quantum commutative group action // Lecture Notes in Computer Science. 2018. V. 11274. P. 395–427. https://doi.org/10.1007/978-3-030-03332-3_15

References

1. Khutsaeva A., Leevik A., Bezzateev S. A Survey of post-quantum oblivious protocols. *Cryptography*, 2025, vol. 9, no. 4, pp. 62. https://doi.org/10.3390/cryptography9040062
2. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120–126. https://doi.org/10.1145/359340.359342
3. Chen L. Oblivious signatures. *Lecture Notes in Computer Science*, 1994, vol. 875, pp. 161–172. https://doi.org/10.1007/3-540-58618-0_62
4. Tso R., Okamoto T., Okamoto E. 1-out-of-n oblivious signatures. *Lecture Notes in Computer Science*, 2008, vol. 4991, pp. 45–55. https://doi.org/10.1007/978-3-540-79104-1_4
5. Tso R. Two-in-one oblivious signatures. *Future Generation Computer Systems*, 2019, vol. 101, pp. 467–475. https://doi.org/10.1016/j.future.2019.06.014
6. 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. https://doi.org/10.1137/s0036144598347011
7. You J.-S., Liu Z.-Y., Tso R., Tseng Y.-F., Mambo M. Quantum-resistant 1-out-of-n oblivious signatures from lattices. *Lecture Notes in Computer Science*, 2022, vol. 13504, pp. 166–186. https://doi.org/10.1007/978-3-031-15255-9_9
8. Khutsaeva A.F., Davydov V.V., Bezzateev S.V. Oblivious signature scheme based on isogenies of supersingular elliptic curves. Information Security Problems. *Computer Systems*, 2023, no. 4 (57), pp. 116–121. (in Russian). https://doi.org/10.48612/jisp/2m49-vg37-99pt
9. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations. *Lecture Notes in Computer Science*, 2019, vol. 11921, pp. 227–247. https://doi.org/10.1007/978-3-030-34578-5_9
10. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an efficient post-quantum commutative group action. *Lecture Notes in Computer Science*, 2018, vol. 11274, pp. 395–427. https://doi.org/10.1007/978-3-030-03332-3_15

Автор

Хуцаева Алтана Феликсовна — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; ассистент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, SC 57884754300, https://orcid.org/0000-0001-5494-7142, afkhutsaeva@itmo.ru

Author

Altana F. Khutsaeva — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation; Assistant, Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation, SC 57884754300, https://orcid.org/0000-0001-5494-7142, afkhutsaeva@itmo.ru

Статья поступила в редакцию 20.01.2026
Одобрена после рецензирования 06.02.2026
Принята к печати 15.03.2026

Received 20.01.2026
Approved after reviewing 06.02.2026
Accepted 15.03.2026