УДК 004.056 Научная статья

https://doi.org/10.32603/2071-8985-2026-19-5-38-46

Постквантовый протокол с нулевым разглашением и алгоритм цифровой подписи

Б. Я. Советов[1], **В. В. Цехановский**[1]✉, **Н. А. Молдовян**[1], **А. А. Костина**[2]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия

[2] СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПИИРАН СПб ФИЦ РАН), Санкт-Петербург, Россия

✉ vvcehanovsky@mail.ru

Аннотация. Рассматривается построение постквантового протокола аутентификации с нулевым разглашением и его преобразование в алгоритм цифровой подписи, стойкость которого основана на вычислительной трудности решения больших систем степенных уравнений. В качестве алгебраического носителя предлагается использовать конечные некоммутативные ассоциативные алгебры (КНАА), в частности конечные алгебры квадратных матриц различного размера. Показано, что по сравнению с известными аналогами предложенный алгоритм электронной цифровой подписи обладает существенно меньшим суммарным размером подписи и открытого ключа. В различных версиях разработанного алгоритма в качестве алгебраического носителя используются КНАА различных размерностей.

Ключевые слова: постквантовая криптография, протокол с нулевым разглашением, алгоритм цифровой подписи, конечная некоммутативная алгебра, конечная алгебра матриц, система степенных уравнений

Для цитирования: Постквантовый протокол с нулевым разглашением и алгоритм цифровой подписи / Б. Я. Советов, В. В. Цехановский, Н. А. Молдовян, А. А. Костина // Изв. СПбГЭТУ «ЛЭТИ». 2026. Т. 19, № 5. С. 38–46. doi: 10.32603/2071-8985-2026-19-5-38-46.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Original article

Zero-Knowledge Protocol and Digital Signature Algorithm

B. Ya. Sovetov[1], **V. V. Tsekhanovsky**[1]✉, **N. A. Moldovyan**[1], **A. A. Kostina**[2]

[1] Saint Petersburg Electrotechnical University, Saint Petersburg, Russia

[2] SPIIRAS of Saint Petersburg Federal Research Center of the Russian Academy of Sciences (SPIIRAS – SPC RAS), Saint Petersburg, Russia

✉ vvcehanovsky@mail.ru

Abstract. This paper discusses the construction of a post-quantum zero-knowledge authentication protocol and its trans-formation into a digital signature algorithm whose security is based on the computational difficulty of solving large systems of power equations. Finite non-commutative associative algebras (FNAA), specifically finite algebras of square matrices of varying sizes, are proposed as the algebraic support. It is shown that, compared to known analogues, the proposed digital signature algorithm has a significantly smaller total size of the signature and public key. In various versions of the developed algorithm, FNAA of various dimensions are used as an algebraic carrier.

Keywords: post-quantum cryptography, zero-knowledge protocol, digital signature algorithm, finite non-commutative algebra, finite matrix algebra, system of power equations

For citation: Zero-Knowledge Protocol and Digital Signature Algorithm / B. Ya. Sovetov, V. V. Tsekhanovsky, N. A. Moldovyan, A. A. Kostina // LETI Transactions on Electrical Engineering & Computer Science. 2026. Vol. 19, no. 5. P. 38–46. doi: 10.32603/2071-8985-2026-19-5-38-46.

Conflict of interests. The authors declare no conflicts of interests.

Введение. Для обеспечения информационной безопасности в компьютерных системах и сетях широко применяются двухключевые криптографические алгоритмы и протоколы, стойкость которых базируется на вычислительной трудности задачи факторизации (ЗФ) или задачи дискретного логарифмирования (ЗДЛ) [1]. Однако прогресс в технологии квантовых вычислений и существование полиномиальных алгоритмов решения ЗФ и ЗДЛ [2] на квантовом компьютере обусловил актуальность разработки практичных криптосхем с открытым ключом, основанных на вычислительно трудных задачах других типов, для решения которых квантовый компьютер неэффективен. Криптографические алгоритмы и протоколы, стойкие к квантовым атакам (атакам с использованием квантового компьютера), относятся к постквантовой криптографии – актуальной области прикладных и теоретических исследований [3], [4]. Для разработки постквантовых алгебраических алгоритмов электронной цифровой подписи (ЭЦП) со скрытой группой [5] недавно предложена новая вычислительно трудная задача (ВТЗ), задаваемая в конечных некоммутативных ассоциативных алгебрах (КНАА). Однако в предложенной на ее основе схеме подписи [5] не обеспечивается достаточной полноты рандомизации подписи, что не позволяет достигнуть высокого уровня стойкости (2^{128} и более). В связи с последним представляет интерес разработка других подходов к построению постквантовых алгоритмов ЭЦП, основанных на вычислительно трудной задаче [5].

В настоящей статье предлагается построение постквантового алгоритма ЭЦП посредством разработки протокола с нулевым разглашением и преобразование его в схему ЭЦП в соответствии со способом [6]. Показано, что при заданном уровне стойкости разработанный алгоритм ЭЦП обладает существенно меньшим суммарным размером подписи и открытого ключа по сравнению с алгоритмами, основанными на трудности задачи синдромного декодирования [7], [8] и полученными преобразованием протоколов с нулевым разглашением.

Используемый алгебраический носитель. В предлагаемых криптосхемах в качестве их носителя используются КНАА, заданные над простым конечным полем $GF(p)$. Элементами КНАА служат m-мерные векторы. Некоторый m-мерный вектор $\mathbf{A}$ можно представить: 1) в виде упорядоченного набора его координат $a_i \in GF(p)$: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$ и 2) в виде суммы его компонент $a_i\mathbf{e}_i$: $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$, где $\mathbf{e}_i$ – базисные векторы. Сложение векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ задается как сложение одноименных координат, а умножение по правилу перемножения каждой компоненты вектора $\mathbf{A}$ с каждой компонентой вектора $\mathbf{B}$ – по следующей формуле:

$$\mathbf{AB} = \sum_{i,j=0}^{m-1} a_i b_j \left(\mathbf{e}_i\mathbf{e}_j\right),$$

в которой всевозможные произведения пар базисных векторов $\mathbf{e}_i\mathbf{e}_j$ заменяются на однокомпонентные векторы вида $\lambda\mathbf{e}_k$ (λ – структурная константа), указанные в ячейках на пересечении i-й строки и j-го столбца в так называемой таблице умножения базисных векторов (ТУБВ). Если $\lambda = 1$, то в ячейках ТУБВ указывается только базисный вектор $\mathbf{e}_k$. Если заданная операция векторного умножения обладает свойством ассоциативности, то алгебра называется ассоциативной. Для задания КНАА разрабатываются ТУБВ, которые определяют операцию умножения, обладающую свойствами ассоциативности и некоммутативности. Известен унифицированный способ задания КНАА произвольных четных размерностей, содержащих глобальную единицу [9]. Табл. 1 представляет собой ТУБВ, задающую шестимерную КНАА по способу [9].

Табл. 1. Задание шестимерной КНАА по способу [9]
Tab. 1. Setting six-dimensional non-commutative associative algebra by [9]

	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_5$	$\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$

Конечные алгебры матриц размером $\mu \times \mu$, заданные над полем $GF(p)$, могут рассматриваться как частный случай КНАА (с глобальной единицей) размером $m = \mu^2$, для которых ТУБВ составляются в соответствии с правилом матричного умножения. При этом получаются ТУБВ прореженного типа (с большим числом ячеек, содержащих нулевую структурную константу), которые задают операцию умножения, имеющую существенно более низкую вычислительную сложность по сравнению со случаем «плотных» ТУБВ. Табл. 2 представляет собой ТУБВ, задающую умножение матриц 2×2 как умножение четырехмерных векторов.

Табл. 2. Задание умножения матриц 2×2 как четырехмерных векторов
Tab. 2. Setting multiplication of the 2×2 matrices as four-dimensional vectors

	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_3$	$\mathbf{e}_2$

Используемая вычислительно трудная задача. Всевозможные степени некоторого обратимого элемента КНАА $\mathbf{A}$ образуют конечную циклическую группу порядка ω. Значение ω также называется порядком вектора $\mathbf{A}$. Множество всех обратимых векторов образуют мультипликативную группу КНАА, которая является некоммутативной и содержит множество коммутативных подгрупп различного типа, отличающихся числом векторов, входящих в минимальную систему образующих, и порядком этих векторов. В случае конечной алгебры матриц размером $\mu \times \mu$, заданных над полем $GF(p)$ порядок мультипликативной группы Ω равен:

$$\Omega = \prod_{i=0}^{\mu-1} p^i \left(p^{\mu-i} - 1 \right).$$

Для простых значений μ легко найти простые значения p, такие, что число

$$q = p^{m-1} + p^{m-2} + \ldots + p + 1$$

– простое. Известно, что для любого простого делителя d порядка Ω конечной некоммутативной группы существует элемент, имеющий порядок d (теорема Коши). Для таких значений p алгебра матриц содержит элемент $\mathbf{A}$, имеющий порядок, значительно превышающий значение p. При этом каждая невырожденная матрица $\mathbf{X}$, некоммутативная с $\mathbf{A}$, задает другую матрицу $\mathbf{B} = \mathbf{X}^{-1}\mathbf{A}\mathbf{X}$, которая также имеет порядок q и некоммутативна с $\mathbf{A}$: $\mathbf{BA} \neq \mathbf{AB}$. Таким образом, в рассматриваемом случае имеется множество попарно некоммутативных матриц простого порядка q. Матрица $\mathbf{C} = \alpha\mathbf{B}$, полученная умножением $\mathbf{B}$ на скаляр α, – примитивный элемент в поле $GF(p)$, имеет порядок $\omega = (p-1)q = p^{\mu} - 1$.

Для построения криптосхем далее используется ВТЗ, представляющая собой модифицированный вариант ВТЗ, предложенной в [5], и задаваемая следующей системой из четырех векторных (матричных) уравнений вида ($i = 1, 2, 3, 4$)

$$\mathbf{Q}_i = \mathbf{G}^{x_i}\mathbf{K}\mathbf{J}^{z_i}, \qquad (1)$$

где заданные векторы $\mathbf{Q}_1$, $\mathbf{Q}_2$, $\mathbf{Q}_3$, $\mathbf{Q}_4$, $\mathbf{G}$ и $\mathbf{J}$ попарно некоммутативны и имеют достаточно большой порядок ω (размером 100 бит и более). Набор этих векторов будет использоваться как открытый ключ, которому соответствует секретный ключ, включающий неизвестный вектор $\mathbf{K}$ и набор из восьми неизвестных натуральных степеней x_i, z_i ($i = 1, 2, 3, 4$), меньших значения ω. Задача состоит в нахождении неизвестных значений, удовлетворяющих каждому из уравнений (1).

В [5] предложен способ решения систем вида (1) сведением к решению системы степенных скалярных уравнений, используя тот факт, что векторы $\mathbf{G}^{x_i}$ принадлежат циклической коммутативной группе, генерируемой вектором $\mathbf{G}$, а векторы $\mathbf{J}^{z_i}$ – группе, генерируемой вектором $\mathbf{J}$. При этом каждый из векторов $\mathbf{G}^{x_i}$ (и $\mathbf{J}^{z_i}$) описывается по координатам известного вектора $\mathbf{G}(\mathbf{J})$ как представителя коммутативной группы, которой они принадлежат, и $b < m$ скалярным неизвестным, причем формулы такого описания линейны относительно скалярных неизвестных. Такой способ описания коммутативных групп в алгебре матриц 2×2 и четырехмерных КНАА детально рассмотрен в [10], [11], где показано, что для этих случаев $b = 2$. Формулы, описывающие координаты векторов некоторой коммутативной группы по координатам ее представителя $\mathbf{P}$ и b скалярным неизвестным, могут быть сравнительно легко найдены из решения уравнения $\mathbf{PX} = \mathbf{XP}$, где $\mathbf{X}$ – неизвестный вектор (матрица), при этом также определяется значение b, которое в общем случае зависит от конкретной КНАА и конкретного представителя. Однако в типовых случаях

для конечных алгебр матриц имеем $b = \mu$, а для шестимерной КНАА, заданной по табл. 1, $b = 3$.

Большое значение имеет принципиальная возможность описания коммутативных групп по их представителю и b скалярным неизвестным. Трудоемкость вывода подобных формул и вычислений, связанных с таким описанием, пренебрежимо мала по сравнению с решением большой системы степенных уравнений (БССУ) в поле $GF(p)$, к которой сводится система векторных (матричных) уравнений (1). Вычислительная сложность W решения БССУ определяется главным образом числом уравнений (неизвестных), если оно меньше или равно числу неизвестных (уравнений). Значение W для заданного числа уравнений и неизвестных возрастает с ростом порядка поля, в котором задана БССУ, и с увеличением степени уравнений, входящих в БССУ. Оценка трудоемкости W решения БССУ при использовании лучших известных алгоритмов приведена в [12] для случая квадратных уравнений и полей малого порядка (256 и менее). Для оценки стойкости разрабатываемых криптосхем будем использовать оценки [12] в качестве нижней границы стойкости к прямым атакам, связанным с решением ВТЗ, положенной в основу криптосхем. При использовании в качестве алгебраического носителя шестимерных КНАА, заданных по ТУББ, представленной как табл. 1, имеем значение $W \approx 2^{80}$. Значения вычислительной сложности при задании рассматриваемой ВТЗ над алгебрами матриц различной размерности представлено в табл. 3.

Табл. 3. Сложность решения рассматриваемой вычислительно трудной задачи для различных значений μ
Tab. 3. The complexity of solving the considered computationally hard problem for different values of μ

μ	W
3	2^{100}
4	2^{128}
5	2^{160}
6	2^{192}
7	2^{256}

Протокол с нулевым разглашением. К протоколам данного вида относят протоколы аутентификации удаленного абонента по его открытому ключу, в ходе которых никакой утечки информации о секретном ключе не происходит, хотя проверяющий убеждается в том, что доказывающий (удаленный абонент) знает секретный ключ, связанный с открытым. На основе описанной ВТЗ разработан следующий протокол с нулевым разглашением, в котором открытым ключом доказывающего служит набор из шести векторов ($\mathbf{Q}_1$, $\mathbf{Q}_2$, $\mathbf{Q}_3$, $\mathbf{Q}_4$, $\mathbf{G}$, $\mathbf{J}$), связанных с секретным ключом в виде вектора $\mathbf{K}$ и восьми натуральных чисел x_i, z_i ($i = 1, 2, 3, 4$) соотношениями вида (1). В протоколе последовательно выполняются δ раундов, каждый из которых включает следующие три шага:

1. Доказывающий генерирует три случайных равновероятных натуральных числа k, t, w, меньших ω, и вычисляет фиксатор в виде вектора $\mathbf{R}$:

$$\mathbf{R} = \mathbf{G}^k \mathbf{Q}_1 \mathbf{T}^t \mathbf{Q}_2^{-1} \mathbf{G}^w.$$

Затем он направляет значение $\mathbf{R}$ проверяющему.

2. Проверяющий генерирует три случайных равновероятных бита $e_1 \in \{0,1\}$, $e_2 \in \{0,1\}$ и $e_3 \in \{0,1\}$ и направляет тройку (e_1, e_2, e_3) доказывающему в качестве своего запроса.

3. Доказывающий устанавливает значения индексов g и h в соответствии с табл. 4 и вычисляет тройку чисел (k', t', w') по следующим формулам:

$$\begin{aligned} k' &= k + x_1 - x_g \bmod \omega; \\ t' &= t + z_1 + z_h - z_2 - z_g \bmod \omega; \\ w' &= w + x_h - x_2 \bmod \omega. \end{aligned} \qquad (2)$$

Затем он направляет проверяющему тройку (k', t', w') в качестве своего ответа на запрос.

Проверяющий выполняет проверку правильности ответа следующим образом. Он устанавливает значения индексов g и h по табл. 4 и вычисляет вектор $\mathbf{R}'$ по формуле

$$\mathbf{R}' = \mathbf{G}^{k'} \mathbf{Q}_g \mathbf{J}^{t'} \mathbf{Q}_h^{-1} \mathbf{G}^{w'}. \qquad (3)$$

Затем он сравнивает значения $\mathbf{R}'$ и $\mathbf{R}$. Если $\mathbf{R}' = \mathbf{R}$, то проверяющий признает ответ правильным.

Такая проверка выполняется после каждого раунда. Подлинный доказывающий знает секретный ключ, поэтому он дает правильные ответы в каждом раунде с вероятностью 1. Потенциальный нарушитель может дать правильный ответ с вероятностью 2^{-3}, выбирая конкретную пару значений индексов g и h и вычисляя фиксатор по (3). Это позволяет ему иметь правильный ответ на один запрос из восьми возможных, а именно на тот, который задаст по табл. 4 выбор использованной нарушителем пары значений индексов g и h, остальные семь значений запроса выявляют

нарушителя. Вероятность обмана в ходе δ-раундового протокола равна $2^{-3\delta}$. Задавая достаточное число раундов, можно обеспечить достаточно низкую вероятность обмана.

Отсутствие утечки информации о секретном ключе (нулевое разглашение) в ходе протокола определяется тем, что на третьем шаге раунда передается ответ (k', t', w'), который сам по себе (т. е. вне доступа к значениям k, t и w) – равновероятная случайная тройка натуральных чисел, меньших значения ω.

Табл. 4. Правило установки значений индексов g и h
Tab. 4. Rule for setting values of the indices g and h

Запрос (e_1, e_2, e_3)	Индекс (g, h)
000	(1, 2)
001	(4, 1)
010	(3, 1)
011	(2, 3)
100	(2, 4)
101	(3, 2)
110	(3, 4)
111	(4, 3)

Корректность работы описанного протокола состоит в том, что ответ, сформированный по формуле (2) будет принят проверяющим в качестве правильного ответа. Действительно, по формулам (2) и (3) имеем:

$$\mathbf{R}' = \mathbf{G}^{k'}\mathbf{Q}_g\mathbf{J}^{t'}\mathbf{Q}_h^{-1}\mathbf{G}^{w'} = \mathbf{G}^{k+x_1-x_g}\mathbf{G}^{x_g} \times$$
$$\times \mathbf{K}\mathbf{J}^{z_g}\mathbf{J}^{t+z_1+z_h-z_2-z_g}\mathbf{J}^{-z_h}\mathbf{K}^{-1}\mathbf{G}^{-x_h} \times$$
$$\times \mathbf{G}^{w+x_h-x_2} = \mathbf{G}^{k}\mathbf{G}^{x_1}\mathbf{K}\mathbf{J}^{z_1}\mathbf{J}^{t}\mathbf{J}^{-z_2}\mathbf{K}^{-1}\mathbf{G}^{-x_2}\mathbf{G}^{w} =$$
$$= \mathbf{G}^{k}\mathbf{Q}_1\mathbf{J}^{t_2}\mathbf{G}^{w} = \mathbf{R}.$$

Параллельная форма протокола. Для реальных применений предпочтительно параллельное выполнение всех δ раундов. Это может быть осуществлено следующими тремя шагами:

1. Доказывающий генерирует δ различных случайных равновероятных троек натуральных чисел (k_i, t_i, w_i), $i = 1, 2, \ldots, \delta$, меньших значения ω, и вычисляет «комплексный фиксатор» в виде δ векторов-фиксаторов по следующей формуле:

$$\mathbf{R}_i = \mathbf{G}^{k_i}\mathbf{Q}_1\mathbf{J}^{t_i}\mathbf{Q}_2^{-1}\mathbf{G}^{w_i}, \qquad (4)$$

и направляет проверяющему упорядоченный набор векторов $(\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_\delta)$.

2. Проверяющий генерирует случайную равновероятную 3δ-битную строку $E = (e_1, e_2, \ldots, e_{3\delta})$ в качестве своего запроса, причем эта последовательность трактуется как последовательность битовых троек $(e_{3i-2}, e_{3i-1}, e_{3i})$ при $i = 1, 2, \ldots, \delta$: $E = ((e_1, e_2, e_3), (e_4, e_5, e_6), \ldots, (e_{3\delta-2}, e_{3\delta-1}, e_{3\delta}))$.

3. Доказывающий направляет в качестве ответа последовательность троек $((k'_1, t'_1, w'_1), (k'_2, t'_2, w'_2), \ldots, (k'_\delta, t'_\delta, w'_\delta))$, вычисляемых для каждого значения $i = 1, 2, \ldots, \delta$ следующим образом:

3.1. Используя табл. 4, по значению $(e_{3i-2}, e_{3i-1}, e_{3i})$ установить значения индексов g и h.

3.2. Вычислить значения

$$k'_i = k_i + x_1 - x_g \bmod \omega;$$
$$t'_i = t_i + z_1 + z_h - z_2 - z_g \bmod \omega; \qquad (5)$$
$$w'_i = w_i + x_h - x_2 \bmod \omega.$$

Для каждого значения $i = 1, 2, \ldots, \delta$ проверяющий по табл. 4 (и соответствующей тройке битов запроса) устанавливает значения индексов g и h и вычисляет вектор $\mathbf{R}'_i$ по следующей формуле:

$$\mathbf{R}'_i = \mathbf{G}^{k'_i}\mathbf{Q}_g\mathbf{J}^{t'_i}\mathbf{Q}_h^{-1}\mathbf{G}^{w'_i}. \qquad (6)$$

Если для каждого значения $i = 1,2, \ldots, \delta$ выполняется равенство $\mathbf{R}'_i = \mathbf{R}_i$, ответ признается правильным, а доказывающий – подлинным. Также, как и в случае последовательного выполнения δ раундов с трехбитными запросами, вероятность не обнаружения нарушителя равна $2^{-3\delta}$.

Постквантовый алгоритм ЭЦП. Параллельная форма протокола с нулевым разглашением секрета может быть преобразована в алгоритм ЭЦП по способу [6], в основе которого лежит идея формирования запроса в виде значения λ-битной хеш-функции $f(M, \mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_\delta) = E$, вычисляемого от подписываемого документа M с присоединенным к нему набором векторов $(\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_\delta)$, генерируемых на первом шаге протокола. Для обеспечения возможности проверки подлинности ЭЦП значение $E = (e_1, e_2, \ldots, e_{3\delta}, \ldots, e_\lambda)$, где $\lambda \geq 3\delta$, используется в качестве первого элемента ЭЦП, а в качестве второго – последовательность троек $((k'_1, t'_1, w'_1), (k'_2, t'_2, w'_2), \ldots, (k'_\delta, t'_\delta, w'_\delta))$, вычисляемых на третьем шаге протокола. Легко установить, что стойкость к подделке подписи с попыткой угадать значение запроса равна $2^{3\delta}$. Стойкость к атаке на основе парадокса о днях рождения равна $2^{\lambda/2}$. Для получения уровня стойкости к последней атаке следует использовать значение разрядности хеш-функции $\lambda = 6\delta$.

С учетом сделанных замечаний приходим к такой процедуре генерации ЭЦП:

1. Для каждого из значений $i = 1, 2, \ldots, \delta$ сгенерировать случайную равновероятную тройку натуральных чисел (k_i, t_i, w_i) и вектор $\mathbf{R}_i$ по формуле (4).

2. Вычислить первую часть ЭЦП в виде хеш-значения $E = f(M, \mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_\delta)$ и представить его в виде $E = (e_1, e_2, \ldots, e_{3\delta}, \ldots, e_\lambda)$. Представить первые 3δ битов значения E в виде последовательности, включающей δ битовых троек $(e_{3i-2}, e_{3i-1}, e_{3i})$ при $i = 1, 2, \ldots, \delta$.

3. Для каждого из значений $i = 1, 2, \ldots, \delta$ по табл. 4 и тройки битов $(e_{3i-2}, e_{3i-1}, e_{3i})$ установить значения индексов g и h и вычислить тройку натуральных чисел (k'_i, t'_i, w'_i) по формулам (5). Взять последовательность троек (k'_1, t'_1, w'_1), (k'_2, t'_2, w'_2), ..., $(k'_\delta, t'_\delta, w'_\delta)$ в качестве второй части подписи.

Алгоритм верификации ЭЦП описывается следующими шагами:

1. По первой части подписи выделить последовательность битовых троек $(e_{3i-2}, e_{3i-1}, e_{3i})$, где $i = 1, 2, \ldots, \delta$. Затем для каждого значения i по табл. 4 установить значения индексов g и h и по второй части ЭЦП и формуле (6) вычислить вектор $\mathbf{R}'_i$.

2. Вычислить значение λ-битной хеш-функции $E = f(M, \mathbf{R}'_1, \mathbf{R}'_2, ..., \mathbf{R}'_\delta)$.

3. Проверить выполнимость равенства $E' = E$. Если это равенство верно, то подпись к документу M признается подлинной, в противном случае – ложной.

Размеры открытого ключа (ОК), подписи и секретного ключа (СК) зависят от используемого алгебраического носителя, разрядности $|p|$ порядка поля $GF(p)$ и значения δ. Эти данные и оценка уровня стойкости U для различных вариантов реализации разработанного алгоритма ЭЦП представлены в табл. 5 для различных размеров m КНАА, заданных по унифицированному способу [9] и различных значений размеров $\mu \times \mu$ матричных алгебр.

Сравнение с алгоритмами ЭЦП, стойкость которых основана на вычислительной трудности синдромного декодирования [7], [8], включая случаи синдромного декодирования с ограниченными ошибками [13], [14], представлено в табл. 6. Из данных последней видно, что разработанный постквантовый алгоритм ЭЦП представляется более практичным по сравнению с известными аналогами. Производительность процедуры генерации ЭЦП для предложенного алгоритма зависит от его конкретной модификации. Например, для модификации, использующей в качестве алгебраического носителя алгебру матриц 5×5, вычислительная сложность генерации (и верификации) ЭЦП составляет $\approx 4.7 \cdot 10^6$ операций умножения по 32-битному модулю.

Для сравнения отметим – при использовании широко известного алгоритма ЭЦП RSA для обеспечения стойкости 2^{109} требуется использовать модуль размером 2048 бит, что задает сложность генерации (верификации) подписи, равную $\approx 6 \cdot 10^6$ ($\approx 10^5$) умножений по 32-битному модулю. Указанная версия разработанного алгоритма ЭЦП значительно уступает по производительно-

Табл. 5. Сравнение нескольких версий разработанного алгоритма
Tab. 5. Comparison of several version of the developed signature algorithm

$m/\mu \times \mu$	$\|p\|$, бит	δ	ОК, байт	ЭЦП, байт	СК, байт	U
4	128	19	348	920	192	2^{56}
6	96	27	432	990	170	2^{80}
3×3	64	34	432	1650	200	2^{100}
4×4	48	43	576	2320	240	2^{128}
5×5	32	66	600	3170	228	2^{192}
7×7	24	86	890	4700	270	2^{256}

Табл. 6. Сравнение разработанного алгоритма с аналогами
Tab. 6. Comparison of the developed signature algorithm with analogues

Алгоритм	δ	ОК + ЭЦП, байт	ЭЦП, байт	U
Предложенный ($m = 6$)	27	1422	990	2^{80}
Предложенный ($\mu = 5$)	66	3770	3170	2^{192}
[7]	137	≈655 000	655 000	2^{70}
[8]	137	≈174 000	174 000	2^{80}
[13]	–	>17 400	17 400	2^{128}
[14]	–	>11 260	11 260	2^{128}

сти процедуры верификации подписи, однако она обеспечивает существенно более высокий уровень стойкости и стойкость к квантовым атакам. В дальнейших разработках алгоритмов ЭЦП, основанных на различных модификациях ВТЗ из [9], следует рассмотреть возможные варианты уменьшения вычислительной сложности генерации и верификации ЭЦП. В частности, для этого можно рассмотреть варианты реализации предложенного алгоритма на КНАА и алгебрах матриц, заданных над конечными полями четной характеристики, т. е. над полями $GF(2^s)$.

Заключение. Предложена новая реализация постквантового алгоритма ЭЦП, представляющего практический интерес благодаря сравнительно малым размерам открытого ключа и подписи. Выполненное исследование показывает, что использованная новая ВТЗ может быть задана в различных модификациях, и служит вкладом в развитие нового направления разработки постквантовых алгоритмов ЭЦП, связанных с предварительным построением протоколов с нулевым разглашением секрета.

Список литературы

1. Menezes A. J., Van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

2. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. of Comp. 1997. Vol. 26, no. 5. P. 1484–1509. doi: 10.1137/S0097539795293172.

3. Reducing signature size of matrix-code-based signature schemes / T. Chou, R. Niederhagen, L. Ran, S. Samardjiska // Post-Quantum Cryptography (PQCrypto 2024) Lecture Notes in Comp. Sci. (LNCS, vol. 14771). Cham, Switzerland: Springer, 2024. P. 107–134.

4. Kirshanova E., May A., Nowakowski Ju. New NTRU records with improved lattice bases // Post-Quantum Cryptography (PQCrypto 2023) Lecture Notes in Comp. Sci. (LNCS, vol. 14154). Cham, Switzerland: Springer, 2023. P. 167–195.

5. Молдовян А. А., Молдовян Д. Н. Новый тип постквантовых алгебраических алгоритмов цифровой подписи // Вопр. защиты информации. 2025. № 4. С. 51–56. doi: 10.52190/2073-2600_2025_4_51.

6. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in Cryptology – CRYPTO'86. Lecture Notes in Comp. Sci. (LNCS, vol. 263). Berlin, Heidelberg: Springer, 1987. P. 186–194. doi: 10.1007/3-540-47721-7_12.

7. Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Appl. Discrete Math. 2022. No. 57. P. 67–90. doi: 10.17223/20710410/57/5.

8. Ниткин И. С. Применение метода компактного описания подстановки для модификации схемы цифровой подписи на основе протокола аутентификации Штерна // Информационно-управляющие системы. 2025. № 6. С. 51–63. doi: 10.31799/1684-8853-2025-6-51-63.

9. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions // Quasi-groups and Related Syst. 2018. Vol. 26, no. 2. P. 263–270.

10. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2 × 2 matrix algebra // Vest. of Saint Petersburg University. Appl. Math. Comp. Sci. Control Proc. 2021. Vol. 17, no. 3. P. 254–261.

11. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Syst. 2022. Vol. 30, no. 1. P. 133–140. doi: 10.56415/qrs.v30.11.

12. Ding J., Petzoldt A. Current state of multivariate cryptography // IEEE Security & Privacy. 2017. Vol. 15, no. 4. P. 28–36. doi: 10.1109/MSP.2017.3151328.

13. Feneuil T., Joux A., Rivain M. Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature // Designs, Codes and Cryptography. 2023. Vol. 91. P. 563–608. doi: 10.1007/s10623-022-01116-1.

14. Feneuil Th., Joux A., Rivain M. Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs // Advances in Cryptology – CRYPTO 2022. Lecture Notes in Comp. Sci. (LNCS, vol. 13508). Cham, Switzerland: Springer, 2022. P. 541–572. doi: 10.1007/978-3-031-15979-4_19.

Информация об авторах

Советов Борис Яковлевич – д-р техн. наук, профессор кафедры информационных систем СПбГЭТУ «ЛЭТИ».
E-mail: bisovetov@etu.ru
https://orcid.org/0009-0000-2074-5438

Цехановский Владислав Владимирович – канд. техн. наук, профессор, зам. зав. кафедрой информационных систем СПбГЭТУ «ЛЭТИ».
E-mail: vvtcekhanovskii@etu.ru

Молдовян Николай Андреевич – д-р техн. наук, профессор кафедры информационных систем СПбГЭТУ «ЛЭТИ».
E-mail: nmold@mail.ru
https://orcid.org/0000-0002-4483-5048

Костина Анна Александровна – научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН – СПб ФИЦ РАН. 14-я линия В.О., 39, Санкт-Петербург, 199178, Россия.
E-mail: maa1305@yandex.ru
https://orcid.org/0009-0004-5784-7242

Вклад авторов:

Советов Б. Я. – предложил формулы для вычисления открытого ключа и фиксатора; построение протокола с нулевым разглашением.

Цехановский В. В. – предложил способ преобразования протокола с нулевым разглашением в алгоритм цифровой подписи.

Молдовян Н. А. – выполнил оценку стойкости и размеров открытого ключа и подписи.

Костина А. А. – предложила способ сокращения размера подписи за счет увеличения размера открытого ключа.

References

1. Menezes A. J., Van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

2. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. of Comp. 1997. Vol. 26, no. 5. P. 1484–1509. doi: 10.1137/S0097539795293172.

3. Reducing signature size of matrix-code-based signature schemes / T. Chou, R. Niederhagen, L. Ran, S. Samardjiska // Post-Quantum Cryptography (PQCrypto 2024) Lecture Notes in Comp. Sci. (LNCS, vol. 14771). Cham, Switzerland: Springer, 2024. P. 107–134.

4. Kirshanova E., May A., Nowakowski Ju. New NTRU records with improved lattice bases // Post-Quantum Cryptography (PQCrypto 2023) Lecture Notes in Comp. Sci. (LNCS, vol. 14154). Cham, Switzerland: Springer, 2023. P. 167–195.

5. Moldovjan A. A., Moldovjan D. N. Novyj tip postkvantovyh algebraicheskih algoritmov cifrovoj podpisi // Vopr. zashhity informacii. 2025. № 4. S. 51–56. doi: 10.52190/2073-2600_2025_4_51. (In Russ.).

6. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in Cryptology – CRYPTO'86. Lecture Notes in Comp. Sci. (LNCS, vol. 263). Berlin, Heidelberg: Springer, 1987. P. 186–194. doi: 10.1007/3-540-47721-7_12.

7. Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Appl. Discrete Math. 2022. No. 57. P. 67–90. doi: 10.17223/20710410/57/5.

8. Nitkin I. S. Primenenie metoda kompaktnogo opisanija podstanovki dlja modifikacii shemy cifrovoj podpisi na osnove protokola autentifikacii Shterna // Informacionno-upravljajushhie sistemy. 2025. № 6. S. 51–63. doi: 10.31799/1684-8853-2025-6-51-63. (In Russ.).

9. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions // Quasi-groups and Related Syst. 2018. Vol. 26, no. 2. P. 263–270.

10. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2 × 2 matrix algebra // Vestn. of Saint Petersburg University. Appl. Math. Comp. Sci. Control Proc. 2021. Vol. 17, no. 3. P. 254–261.

11. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Syst. 2022. Vol. 30, no. 1. P. 133–140. doi: 10.56415/qrs.v30.11.

12. Ding J., Petzoldt A. Current state of multivariate cryptography // IEEE Security & Privacy. 2017. Vol. 15, no. 4. P. 28–36. doi: 10.1109/MSP.2017.3151328.

13. Feneuil T., Joux A., Rivain M. Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature // Designs, Codes and Cryptography. 2023. Vol. 91. P. 563–608. doi: 10.1007/s10623-022-01116-1.

14. Feneuil Th., Joux A., Rivain M. Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs // Advances in Cryptology – CRYPTO 2022. Lecture Notes in Comp. Sci. (LNCS, vol. 13508). Cham, Switzerland: Springer, 2022. P. 541–572. doi: 10.1007/978-3-031-15979-4_19.

Information about the authors

Boris Ya. Sovetov – Dr Sci. (Eng.), Professor of the Department of Information Systems, Saint Petersburg Electrotechnical University.
E-mail: bisovetov@etu.ru
https://orcid.org/0009-0000-2074-5438

Vladislav V. Tsekhanovsky – Cand. Sci. (Eng.), Professor, Deputy Head of the Department of Information Systems, Saint Petersburg Electrotechnical University.
E-mail: vvtcekhanovskii@etu.ru

Nikolay A. Moldovyan – Dr Sci. (Eng.), Professor of the Department of Information Systems, Saint Petersburg Electrotechnical University.
E-mail: nmold@mail.ru
https://orcid.org/0000-0002-4483-5048

Anna A. Kostina – Researcher at the Computer Security Laboratory of SPIIRAS – SPC RAS., 14th line, 39, Vasilievsky Island, St. Petersburg, 199178, Russia.
E-mail: maa1305@yandex.ru
https://orcid.org/0009-0004-5784-7242

Author contribution statement:
Sovetov B. Ya. – proposed formulas for calculating the public key and fixator; design of the zero-knowledge protocol.
Tsekhanovsky V. V. – proposed a method for transforming the zero-knowledge protocol into a digital signature algorithm.
Moldovyan N. A. – assessed the security and sizes of the public key and signature.
Kostina A. A. – proposed a method for reducing the signature size by increasing the size of the public key.

Статья поступила в редакцию 25.02.2026; принята к публикации после рецензирования 29.03.2026; опубликована онлайн 25.05.2026.

Submitted 25.02.2026; accepted 29.03.2026; published online 25.05.2026.