УДК 003.26
doi:10.31799/1684-8853-2026-4-17-27
EDN: GJXNHN

Научные статьи
Articles

# Постквантовый алгоритм цифровой подписи с новым механизмом задания вспомогательных скрытых групп

***Н. А. Молдовян***[a], *доктор техн. наук, профессор, главный научный сотрудник, orcid.org/0000-0002-4483-5048, moldovyan.na@talantiuspeh.ru*
***А. А. Молдовян***[б], *доктор техн. наук, профессор, главный научный сотрудник, orcid.org/0000-0001-5480-6016, maa1305@yandex.ru*
[a]*Научный центр информационных технологий и искусственного интеллекта Научно-технологического университета «Сириус», Олимпийский пр., 1, Краснодарский край, федеральная территория «Сириус», 354340, РФ*
[б]*Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ*

***Введение:*** *с точки зрения практического применения известные постквантовые алгоритмы электронной цифровой подписи имеют недостаток, состоящий в их сравнительно большом общем размере открытого ключа и подписи.* ***Цель:*** *разработать постквантовый алгоритм электронной цифровой подписи с малым общим размером подписи и открытого ключа при заданном уровне стойкости.* ***Метод:*** *применение скрытых коммутативных групп в конечной алгебре квадратных матриц, заданных над простым конечным полем GF(p), и формирование открытого ключа в виде набора матриц, которые связаны с секретными матрицами через степенные выражения.* ***Результаты:*** *разработан практичный постквантовый алгебраический алгоритм цифровой подписи со скрытыми коммутативными группами, стойкость которого основана на вычислительной трудности решения больших систем степенных уравнений. Применен новый способ задания вспомогательных скрытых групп и новый механизм верификации подписи по двум проверочным уравнениям с вхождением всех элементов подписи в каждое из них. В качестве алгебраического носителя использованы конечные алгебры матриц μ × μ при значениях μ = 3, 5 и 7, задающих три версии предложенного алгоритма. Для всех версий алгоритма получены оценки стойкости к прямой атаке, к атаке на основе известных подписей и к подделке подписи.* ***Практическая значимость:*** *разработанный алгоритм обладает малыми размерами открытого ключа и подписи и является кандидатом на практичную постквантовую схему подписи.*

***Ключевые слова*** *— постквантовая криптография, компьютерная безопасность, электронная цифровая подпись, система степенных уравнений, вычислительно трудная задача, конечная алгебра матриц.*

**Для цитирования:** Молдовян Н. А., Молдовян А. А. Постквантовый алгоритм цифровой подписи с новым механизмом задания вспомогательных скрытых групп. *Информационно-управляющие системы*, 2026, № 4, с. 17–27. doi:10.31799/1684-8853-2026-4-17–27, EDN: GJXNHN

**For citation:** Moldovyan N. A., Moldovyan A. A. Post-quantum digital signature algorithm with a new mechanism for specifying auxiliary hidden groups. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 4, pp. 17–27 (In Russian). doi:10.31799/1684-8853-2026-4-17-27, EDN: GJXNHN

## Введение

Значительное внимание мирового криптографического сообщества уделяется разработке постквантовых криптоалгоритмов с открытым ключом (ОК). Одним из перспективных направлений постквантовой криптографии является использование вычислительной трудности решения больших систем степенных уравнений (БССУ) [1, 2]. На протяжении более тридцати пяти лет в рамках этого направления алгоритмы открытого шифрования и электронной цифровой подписи (ЭЦП) строились на трудно обратимых отображениях с секретной лазейкой [3–5]. Алгоритмы ЭЦП такого типа обладают малым размером подписи, однако длина ОК является чрезвычайно большой (от десятков килобайт при уровне стойкости $2^{80}$ до нескольких мегабайт при стойкости $2^{256}$) [1], что с точки зрения практического применения является существенным недостатком.

Попыткой устранения этого недостатка явилась новая парадигма [6, 7] задания трудно обратимых отображений в виде набора многочленов, описывающих операции возведения в небольшую степень $n$ в векторном конечном поле с секретной модификацией, а потайной лазейки — в виде операции извлечения корня степени $n$. Этот подход позволяет уменьшить размер ОК до нескольких десятков раз, однако и в этом случае упомянутый недостаток не устраняется в полной мере.

Использование вычислительной трудности синдромного декодирования для построения постквантовых алгоритмов ЭЦП [8, 9] позволяет обеспечить достаточно малый размер ОК (около 200 байт), однако размер подписи составляет сотни килобайт. Разработка алгоритмов ЭЦП с использованием синдромного декодирования ограниченных ошибок [10] привела к сокращению размера ЭЦП до 17 Кбайт [11], ≈10 Кбайт [12, 13] и 7 Кбайт [14].

Представляет интерес сравнительно новая концепция построения алгебраических алгоритмов ЭЦП, стойкость которых основана на вычислительной сложности решения БССУ [15, 16]. В рамках этой концепции в качестве алгебраического носителя используются конечные некоммутативные ассоциативные алгебры, а цифровая подпись включает подгоночный элемент в виде многомерного вектора **S**, формируемого путем выбора случайного элемента **G** из секретной коммутативной группы и маскирования вектора **G** путем умножения его слева и справа на фиксированные секретные векторы **D** и **F** : **S** = **DGF**. В работах [17, 18] показана ограниченность рандомизации, задаваемой последней формулой, которая создает уязвимость к атакам на основе известных подписей. Для устранения этой уязвимости предложены механизмы усиления рандомизации подгоночного элемента подписи путем вычисления вектора **S** 1) по двум случайным векторам, выбираемым из скрытой коммутативной группы [19]; 2) по двум случайным взаимно некоммутативным векторам, выбираемым из двух скрытых коммутативных групп [20, 21], и 3) по трем случайным векторам, выбираемым из трех скрытых коммутативных групп [22].

Алгебраическая структура, в рамках которой выполняются вычисления, связанные с формированием секретного и открытого ключей и с генерацией и верификацией подписи, называется носителем алгоритма ЭЦП. В качестве алгебраического носителя алгебраических алгоритмов ЭЦП, использующих вычислительную трудность решения БССУ, перспективно применение конечных алгебр квадратных матриц $\mu \times \mu$, заданных над простым конечным полем $GF(p)$, размер порядка которого выбирается в зависимости от размерности матриц [19, 23]. В целом постквантовые алгебраические алгоритмы ЭЦП рассматриваемого типа имеют общий размер ОК и подписи менее 1 Кбайт, что обусловливает значительный практический интерес к ним. Однако их базовая концепция является сравнительно новой, и требуется расширение исследований по анализу их стойкости, включая рассмотрение специфических атак, использующих особенности их построения.

Проверочные уравнения известных алгебраических алгоритмов ЭЦП относятся к трем различным типам, отличающимся механизмом обеспечения стойкости к подделке подписи путем решения проверочного уравнения относительно подгоночного элемента подписи **S** как неизвестного алгебраического элемента [21]. Известны следующие типы упомянутого механизма:

1) двукратное вхождение элемента **S** в проверочное уравнение, включая возведение **S** в степень большого размера;

2) использование в проверочном уравнении операции возведения в степень, вычисляемую как значение однонаправленной функции, вычисляемое от **S**;

3) комбинирование первых двух механизмов.

В данной работе предлагается четвертый тип проверочных соотношений, отличающийся заданием двух проверочных уравнений первой степени относительно **S**, задающих при попытках подделки подписи переопределенную несовместную систему линейных уравнений. На основе нового механизма задания стойкости к подделке подписи разработан практичный постквантовый алгоритм ЭЦП с двумя базовыми и двумя вспомогательными скрытыми коммутативными группами.

## Алгебраический носитель

В разработанном алгоритме ЭЦП в качестве алгебраического носителя используются конечные алгебры квадратных матриц, заданных над простым конечным полем $GF(p)$ с числом строк, равным простым числам $\mu = 3, 5$ и 7. Эти значения $\mu$ задают три версии разработанного алгоритма с общими формулами для 1) вычисления открытого ключа по секретному ключу, 2) вычисления элементов цифровой подписи и 3) выполнения процедуры проверки подлинности подписи. Свойства указанных матричных алгебр, используемых при разработке алгоритмов ЭЦП, стойкость которых базируется на вычислительной трудности решения БССУ, детально представлены в работах [19, 23].

В данной работе используются следующие известные факты [19–24].

1. Для простых значений $\mu$ конечная алгебра матриц $\mu \times \mu$, заданная над полем $GF(p)$ нечетного простого порядка $p$, содержит достаточно большое число ($\gg p^{\mu}$) коммутативных циклических групп порядка $p^{\mu} - 1$.

2. Достаточно легко могут быть сгенерированы простые значения $r$ такие, что числа $p = 2r - 1$ и

$$q = p^{\mu-1} + p^{\mu-2} + \ldots + p + 1 \qquad (1)$$

являются простыми. Легко видеть, что в этом случае $q$ является делителем числа $p^{\mu} - 1$,

и матрица **G** порядка $q$ генерирует циклическую группу <**G**> простого порядка $q$. Под термином «порядок матрицы» в данной статье понимается ее порядок как элемента мультипликативной группы конечной алгебры матриц.

В разработанном алгоритме ЭЦП используются простые значения $p$, для которых $r$ и $q$ также являются простыми в связи с тем, что при генерации подписи требуется вычислять обратные значения для случайных чисел по модулю $q$ и по модулю $rq$. При таком выборе практически устраняется проблема появления случаев, когда обратные значения не существуют. Разрядность чисел $r$, $p$ и $q$ для различных версий разработанного алгоритма представлена в табл. 1.

3. Если задана невырожденная нескалярная матрица **P**, содержащаяся в некоторой некоммутативной группе Γ, то элементы любой матрицы, содержащейся в Γ, могут быть представлены в виде линейных комбинаций некоторого уникального набора из μ скалярных значений $a_i \in GF(p)$, где $i = 0, 1, \ldots, \mu - 1$, в которых коэффициенты определяются значениями элементов матрицы **P**, которую будем называть представителем группы Γ. Заметим, что коммутативная группа Γ содержится в некотором коммутативном подкольце порядка $p^{\mu}$ конечного кольца всех возможных матриц размера $\mu \times \mu$. При фиксированной матрице-представителе **P** каждому уникальному набору из μ скалярных значений соответствует уникальная матрица из упомянутого подкольца. Очевидно, что каждой матрице из группы Γ соответствует уникальный набор указанных скалярных значений.

Последнее означает, что выбор η матриц из некоторой скрытой коммутативной циклической группы <**G**> задает $\mu^2$ скалярных неизвестных (элементы первой выбранной неизвестной матрицы **G**′), соответствующих выбору первой неизвестной матрицы, и $\mu(\eta - 1)$ скалярных неизвестных, соответствующих выбору остальных матриц, координаты каждой из которых могут быть описаны через уникальный набор из μ скалярных неизвестных при рассмотрении матрицы **G**′ в качестве представителя группы <**G**>.

## Генерация секретного и открытого ключей

Секретный ключ формируется по следующему алгоритму.

1. Генерируются четыре случайные попарно некоммутирующие обратимые матрицы **G**, **J**, **Q** и **U** такие, что порядок **G** и **J** равен $q$, а порядок **Q** и **U** равен $rq$.

2. Генерируются случайные невырожденные попарно некоммутирующие матрицы **A**, **B**, **D** и **F**, каждая из которых является некоммутирующей с матрицами **G**, **J**, **Q** и **U**, и случайные натуральные числа α, β, γ, ε, λ и τ, не превышающие значение $q$.

3. Генерируются четыре случайных натуральных числа $x$, $z$, $u$ и $v$ ($< q$) и вычисляются матрицы $\mathbf{K}_1 = \mathbf{Q}\mathbf{J}^{-z}\mathbf{G}^{-x}$ и $\mathbf{K}_2 = \mathbf{J}^{-v}\mathbf{G}^{-u}\mathbf{U}$.

В результате выполнения этого алгоритма получаем секретный ключ в виде набора из восьми матриц (**A**, **B**, **D**, **F**, **G**, **J**, **Q**, **U**) и набора из 10 чисел (α, β, γ, ε, λ, τ, $x$, $z$, $u$, $v$). Открытый ключ представляет собой набор из шести матриц (**Y**, **Z**, **W**, **N**, $\mathbf{T}_1$, $\mathbf{T}_2$), которые вычисляются в зависимости от секретного по следующим формулам:

$$\mathbf{Y} = \mathbf{A}\mathbf{Q}^{\alpha}\mathbf{A}^{-1},\ \mathbf{Z} = \mathbf{D}\mathbf{G}\mathbf{D}^{-1},$$

$$\mathbf{W} = \mathbf{F}^{-1}\mathbf{J}\mathbf{F},\ \mathbf{N} = \mathbf{B}\mathbf{U}^{\tau}\mathbf{B}^{-1}; \quad (2)$$

$$\mathbf{T}_1 = \mathbf{A}\mathbf{Q}^{\beta}\mathbf{K}_1\mathbf{G}^{\gamma}\mathbf{D}^{-1},$$

$$\mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{J}^{\varepsilon}\mathbf{K}_2\mathbf{U}^{\lambda}\mathbf{B}^{-1}. \quad (3)$$

Размеры открытого и секретного ключей представлены в табл. 2.

Формулы, используемые на шаге 3, определяют следующую связь базовых скрытых коммутативных групп <**G**> и <**J**> с вспомогательными скрытыми группами <**Q**> и <**U**>:

$$\mathbf{Q} = \mathbf{K}_1\mathbf{G}^{x}\mathbf{J}^{z}; \quad (4)$$

$$\mathbf{U} = \mathbf{G}^{u}\mathbf{J}^{v}\mathbf{K}_2. \quad (5)$$

■ ***Таблица 1.*** Размер используемых простых чисел
■ ***Table 1.*** The size of used primes

| Версия алгоритма | Разрядность, бит | | |
|---|---|---|---|
| | $r$ | $p$ | $q$ |
| μ = 3 | 63 | 64 | 128 |
| μ = 5 | 31 | 32 | 128 |
| μ = 7 | 23 | 24 | 144 |

■ ***Таблица 2.*** Размеры параметров предложенного алгоритма ЭЦП
■ ***Table 2.*** The size of used primes

| Версия алгоритма | Размер, байт | | |
|---|---|---|---|
| | открытого ключа | секретного ключа | ЭЦП |
| μ = 3 | 432 | 896 | 216 |
| μ = 5 | 600 | 1168 | 236 |
| μ = 7 | 882 | 1656 | 291 |

Формулы (4) и (5) отличаются от формул задания связи вспомогательных и базовых скрытых групп из работы [21] наличием множителей в виде невырожденных матриц $\mathbf{K}_1$ и $\mathbf{K}_2$. Это отличие упрощает процедуру генерации секретного ключа, что служит сопутствующим эффектом. Главным назначением этого модифицирования является предотвращение возможности использовать альтернативные формулы для вычисления ЭЦП, что обусловливало бы необходимость оценивания стойкости с учетом альтернативной процедуры генерации подписи.

## Процедура генерации и верификации ЭЦП. Доказательство корректности разработанного алгоритма ЭЦП

В разработанном алгоритме ЭЦП предполагается использование некоторой 512-битной хеш-функции $\Phi(\cdot)$, стойкой к коллизиям. Процесс генерации подписи требует использования секретного ключа и включает следующие шаги.

1. Сгенерировать четыре случайных натуральных числа $k < rq$, $t < q$, $b < q$, $g < rq$ и вычислить две рандомизирующие матрицы $\mathbf{R}_1$ и $\mathbf{R}_2$ по следующим формулам:

$$\mathbf{R}_1 = \mathbf{A}\mathbf{Q}^k\mathbf{J}^t\mathbf{F}; \tag{6}$$

$$\mathbf{R}_2 = \mathbf{D}\mathbf{G}^b\mathbf{U}^g\mathbf{B}^{-1}. \tag{7}$$

2. Вычислить четыре 128-битных рандомизирующих элемента ЭЦП $e_1, e_2, e_3, e_4$, конкатенация которых представляет собой значение 512-битной хеш-функции $\Phi(\cdot)$, вычисленной от документа $M$ с присоединенными к нему рандомизирующими матрицами: $e_1||e_2||e_3||e_4 = \Phi(M||\mathbf{R}_1||\mathbf{R}_2)$.

3. Вычислить элементы подписи $\xi$ и $\psi$:

$$\xi = (e_3\alpha)^{-1}(k - \beta - 1) \bmod rq; \tag{8}$$

$$\psi = (e_4\tau)^{-1}(g - \lambda - 1) \bmod rq. \tag{9}$$

4. Найти значения $s$ и $n$ путем решения следующей системы из двух уравнений первой степени:

$$\begin{cases} \gamma + e_1 s + n = x \bmod q, \\ e_3 s + n = u + b \bmod q, \end{cases} \tag{10}$$

что соответствует выполнению вычислений по формулам

$$s = (e_3 - e_1)^{-1}(u + b + \gamma - x) \bmod q;$$

$$n = x - \gamma - e_1 s \bmod q. \tag{11}$$

5. Найти значения $\sigma$ и $d$ путем решения следующей системы из двух уравнений первой степени:

$$\begin{cases} d + e_2\sigma = z + t \bmod q, \\ d + e_4\sigma + \varepsilon = v \bmod q, \end{cases} \tag{12}$$

что соответствует выполнению вычислений по формулам

$$\sigma = (e_4 - e_2)^{-1}(v - \varepsilon - z - t) \bmod q;$$

$$d = z + t - e_2\sigma \bmod q. \tag{13}$$

6. Вычислить значение подгоночной матрицы $\mathbf{S}$ по формуле

$$\mathbf{S} = \mathbf{D}\mathbf{G}^n\mathbf{J}^d\mathbf{F}. \tag{14}$$

Подпись представляет собой набор элементов ($e_1, e_2, e_3, e_4, s, \sigma, \xi, \psi, \mathbf{S}$). Размер подписи для различных версий разработанного алгоритма представлен в табл. 2. Вычислительная сложность процедуры генерации ЭЦП определяется, главным образом, шестью операциями возведения в степень (вычисление следующих матриц $\mathbf{Q}^k$, $\mathbf{J}^t$, $\mathbf{G}^b$, $\mathbf{U}^g$, $\mathbf{G}^n$ и $\mathbf{J}^d$) и равна примерно $2 \cdot 10^8$ (для версий алгоритма со значениями параметра $\mu = 3, 5$) и $3 \cdot 10^8$ битовые операции (для версии с параметром $\mu = 7$).

Алгоритм проверки подлинности ЭЦП ($e_1, e_2, e_3, e_4, s, \sigma, \xi, \psi, \mathbf{S}$) к электронному документу $M$ осуществляется по ОК ($\mathbf{Y}, \mathbf{Z}, \mathbf{W}, \mathbf{N}, \mathbf{T}_1, \mathbf{T}_2$) и описывается следующим образом.

1. Вычислить проверочные матрицы $\mathbf{R}'_1$ и $\mathbf{R}'_2$ по следующим формулам:

$$\mathbf{R}'_1 = \mathbf{Y}^{e_3\xi}\mathbf{T}_1\mathbf{Z}^{e_1 s}\mathbf{S}\mathbf{W}^{e_2\sigma}; \tag{15}$$

$$\mathbf{R}'_2 = \mathbf{Z}^{e_3 s}\mathbf{S}\mathbf{W}^{e_4\sigma}\mathbf{T}_2\mathbf{N}^{e_4\psi}. \tag{16}$$

2. Вычислить 512-битное хеш-значение, представленное в виде конкатенации четырех 128-битных чисел: $e'_1||e'_2||e'_3||e'_4 = \Phi(M||\mathbf{R}'_1||\mathbf{R}'_2)$.

3. Если $e'_1||e'_2||e'_3||e'_4 = e_1||e_2||e_3||e_4$, то подпись подлинная, иначе — ложная.

Вычислительная сложность процедуры верификации ЭЦП примерно равна сложности процедуры генерации подписи и определяется в основном шестью операциями экспоненцирования матриц в степень большой разрядности. При использовании алгоритма быстрого возведения в степень, основанного на процессе последовательного возведения в квадрат, сложность верификации ЭЦП составляет примерно $2 \cdot 10^8$ (для случаев $\mu = 3, 5$) и $3 \cdot 10^8$ битовые операции (для случая $\mu = 7$).

Для подписи ($e_1$, $e_2$, $e_3$, $e_4$, $s$, σ, ξ, ψ, **S**), вычисленной в соответствии с процедурой генерации ЭЦП, вычисление проверочных матриц $\mathbf{R}'_1$ и $\mathbf{R}'_2$ по формулам (15) и (16) дает следующее:

$$\mathbf{R}'_1 = \left(\mathbf{A}\mathbf{Q}^{\alpha}\mathbf{A}^{-1}\right)^{e_3\xi}\left(\mathbf{A}\mathbf{Q}^{\beta}\mathbf{K}_1\mathbf{G}^{\gamma}\mathbf{D}^{-1}\right)\left(\mathbf{D}\mathbf{G}\mathbf{D}^{-1}\right)^{e_1 s} \times$$

$$\times\left(\mathbf{D}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F}\right)\left(\mathbf{F}^{-1}\mathbf{J}\mathbf{F}\right)^{e_2\sigma} =$$

$$= \mathbf{A}\mathbf{Q}^{\alpha e_3\xi+\beta}\mathbf{K}_1\mathbf{G}^{\gamma+e_1 s+n}\mathbf{J}^{d+e_2\sigma}\mathbf{F} =$$

[учитывая формулы (11) и (13), далее имеем]

$$= \mathbf{A}\mathbf{Q}^{\alpha e_3\xi+\beta}\mathbf{K}_1\mathbf{G}^{x}\mathbf{J}^{z+t}\mathbf{F} = \mathbf{A}\mathbf{Q}^{\alpha e_3\xi+\beta}\left(\mathbf{K}_1\mathbf{G}^{x}\mathbf{J}^{z}\right)\mathbf{J}^{t}\mathbf{F} =$$

[учитывая (2), (6) и (8), далее имеем]

$$= \mathbf{A}\mathbf{Q}^{\alpha e_3\xi+\beta+1}\mathbf{J}^{t}\mathbf{F} = \mathbf{A}\mathbf{Q}^{k}\mathbf{J}^{t}\mathbf{F} = \mathbf{R}_1;$$

$$\mathbf{R}'_2 = \left(\mathbf{D}\mathbf{G}\mathbf{D}^{-1}\right)^{e_3 s}\left(\mathbf{D}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F}\right)\left(\mathbf{F}^{-1}\mathbf{J}\mathbf{F}\right)^{e_4\sigma} \times$$

$$\times\left(\mathbf{F}^{-1}\mathbf{J}^{\varepsilon}\mathbf{K}_2\mathbf{U}^{\lambda}\mathbf{B}^{-1}\right)\left(\mathbf{B}\mathbf{U}^{\tau}\mathbf{B}^{-1}\right)^{e_4\psi} =$$

$$= \mathbf{D}\mathbf{G}^{e_3 s+n}\mathbf{J}^{d+e_4\sigma+\varepsilon}\mathbf{K}_2\mathbf{U}^{\lambda+\tau e_4\psi}\mathbf{B}^{-1} =$$

[с учетом второго уравнения в (10) и второго уравнения в (12) далее имеем]

$$= \mathbf{D}\mathbf{G}^{u+b}\mathbf{J}^{v}\mathbf{K}_2\mathbf{U}^{\lambda+\tau e_4\psi}\mathbf{B}^{-1} =$$

$$= \mathbf{D}\mathbf{G}^{-b}\left(\mathbf{G}^{u}\mathbf{J}^{v}\mathbf{K}_2\right)\mathbf{U}^{\lambda+\tau e_4\psi}\mathbf{B}^{-1} =$$

[учитывая выражения (3), (7) и (9), далее имеем]

$$= \mathbf{D}\mathbf{G}^{b}\left(\mathbf{G}^{u}\mathbf{J}^{v}\mathbf{K}_2\right)\mathbf{U}^{\lambda+\tau e_4\psi}\mathbf{B}^{-1} = \mathbf{D}\mathbf{G}^{b}\mathbf{U}^{1+\lambda+\tau e_4\psi}\mathbf{B}^{-1} =$$

$$= \mathbf{D}\mathbf{G}^{b}\mathbf{U}^{g}\mathbf{B}^{-1} = \mathbf{R}_2.$$

Поскольку для подлинной подписи в ходе процесса верификации имеют место равенства $\mathbf{R}'_1 = \mathbf{R}_1$ и $\mathbf{R}'_2 = \mathbf{R}_2$, то выполняется и равенство $e'_1||e'_2||e'_3||e'_4 = \Phi(M||\mathbf{R}'_1||\mathbf{R}'_2) = \Phi(M||\mathbf{R}_1||\mathbf{R}_2) = e_1||e_2||e_3||e_4$. Последнее означает корректность работы разработанного алгоритма ЭЦП.

## Стойкость

Обоснованием использования множителей $\mathbf{K}_1$ и $\mathbf{K}_2$ в формулах (2) и (3), по которым задаются вспомогательные скрытые группы <**Q**> и <**U**>, является устранение возможности генерации ЭЦП с использованием модифицированной процедуры генерации ЭЦП, свободной от связи матриц **Q** и **U** с матрицами **G** и **J**. Действительно, в случае задания вычисления матриц **Q** и **U** порядка $rq$ по формулам $\mathbf{Q} = \mathbf{G}^{x}\mathbf{J}^{z}$ и $\mathbf{U} = \mathbf{G}^{u}\mathbf{J}^{v}$ описанный выше алгоритм генерации ЭЦП имеет силу, однако имеется возможность генерации ЭЦП по альтернативному алгоритму, отличающемуся шагами 3–5, которые имеют следующий модифицированный вид.

3. Вычислить элементы подписи ξ и ψ:

$$\xi = (e_3\alpha)^{-1}(k - \beta) \bmod rq;$$

$$\psi = (e_4\tau)^{-1}(g - \lambda) \bmod rq.$$

4. Найти значения $s$ и $n$ путем решения системы из следующих двух уравнений первой степени:

$$\gamma + e_1 s + n = 0 \bmod q;$$

$$e_3 s + n = b \bmod q,$$

что соответствует выполнению вычислений по формулам

$$s = (e_3 - e_1)^{-1}(b + \gamma) \bmod q;$$

$$n = b - e_3 s \bmod q.$$

5. Найти значения σ и $d$ путем решения системы из следующих двух уравнений первой степени:

$$d + e_2\sigma = t \bmod q;$$

$$d + e_4\sigma + \varepsilon = 0 \bmod q,$$

что соответствует вычислению σ и $d$ по следующим двум формулам:

$$\sigma = (e_2 - e_4)^{-1}(\varepsilon + t) \bmod q;$$

$$d = t - e_2\sigma \bmod q.$$

Подпись, сформированная по альтернативной процедуре генерации ЭЦП, проходит процедуру верификации с проверочными уравнениями (15) и (16) как подлинная подпись. Легко видеть, что в альтернативной процедуре генерации ЭЦП матрицы **Q** и **U** могут быть произвольными, т. е. формулы не накладывают на матрицы **Q** и **U** связь с матрицами **G** и **J**. Это означает, что альтернативная процедура генерации ЭЦП соответствует модифицированной схеме подписи, в которой сохраняются проверочные уравнения (15) и (16) и связь элементов открытого ключа с элементами секретного ключа, задаваемая только формулами (4) и (5), тогда как в исходной схеме ЭЦП уравнения $\mathbf{Q} = \mathbf{G}^{x}\mathbf{J}^{z}$ и $\mathbf{U} = \mathbf{G}^{u}\mathbf{J}^{v}$ также должны учитываться.

Уменьшение числа матричных уравнений с восьми до шести, которые должны быть совместно решены для вычисления секретного ключа, соответствует существенному снижению уровня стойкости (например, с уровня $2^{192}$ до $\approx 2^{128}$ для случая версии алгоритма ЭЦП, соответствующей значению $\mu = 3$). Таким образом, механизм задания вспомогательных скрытых групп по формулам (2) и (3), в которых $\mathbf{K}_1$ и $\mathbf{K}_2$ являются нескалярными невырожденными матрицами, имеет принципиальное значение для устранения атак, использующих модифицирование процедуры генерации ЭЦП в целях снижения уровня стойкости.

*Прямолинейная атака* на разработанный алгоритм состоит в вычислении секретного ключа по открытому, что предполагает решение системы из восьми матричных нелинейных уравнений с неизвестными матрицами **A**, **B**, **D**, **F**, **G**, **J**, **Q**, **U**, $\mathbf{K}_1$, $\mathbf{K}_2$ и неизвестными натуральными числами $\alpha$, $\beta$, $\gamma$, $\varepsilon$, $\lambda$, $\tau$, $x$, $z$, $u$, $v$, входящими в матричные уравнения в качестве неизвестных степеней. Указанные неизвестные степени имеют разрядность, равную или превышающую 128 бит, что делает практически невыполнимым прямолинейное сведение системы матричных уравнений к системе скалярных уравнений.

Для осуществления такого сведения следует рассмотреть матрицы $\mathbf{Q}^{\alpha}$, $\mathbf{Q}^{\beta}$, $\mathbf{U}^{\tau}$, $\mathbf{U}^{\lambda}$, $\mathbf{G}^{x}$, $\mathbf{G}^{u}$, $\mathbf{U}^{\lambda}$, $\mathbf{U}^{\lambda}$, $\mathbf{J}^{z}$, $\mathbf{J}^{v}$ как матрицы, выбираемые из соответствующих скрытых коммутативных групп <**Q**>, <**U**>, <**G**> и <**J**> и описываемые по элементам матриц-представителей **Q**, **U**, **G** и **J** и уникальным наборам из $\mu$ скалярных неизвестных. Элементы матриц **Q**, **U**, **G** и **J** являются скалярными неизвестными, причем каждая из этих неизвестных матриц задает $\mu^2$ независимых скалярных неизвестных. Каждая матрица, задаваемая как некоторая степень одной из матриц-представителей, вносит только $\mu$ независимых скалярных неизвестных (см. раздел «Алгебраический носитель»). С учетом этих замечаний получаем некоторую исходную скалярную БССУ, в которой число скалярных неизвестных $\eta_1 = 10\mu^2 + 10\mu$, а число скалярных уравнений $\eta_2 = 8\mu^2$. Предположим, что нам удается зафиксировать значения $2\mu^2 + 10\mu$ скалярных неизвестных таким образом, что получаемая после этого БССУ имеет решения. Тогда вычислительная трудоемкость ее решения, т. е. стойкость $W$ разработанного алгоритма к прямолинейной атаке, может быть оценена по данным работы [4], показывающим зависимость трудоемкости от числа уравнений в случае равенства числа уравнений и неизвестных (см. табл. 1 в работе [4]). С учетом того, что при заданном числе уравнений с ростом порядка поля, в котором задана БССУ, сложность ее решения возрастает, получены оценки стойкости трех версий разработанного алгоритма к прямолинейной атаке (табл. 3).

■ ***Таблица 3.*** Оценка стойкости $W$ к прямолинейной атаке

■ ***Table 3.*** Security evaluation $W$ to the direct attack

| Версия алгоритма | $\eta_1$ | $\eta_2$ | $W$ |
|---|---|---|---|
| $\mu = 3$ | 120 | 72 | $2^{192}$ |
| $\mu = 5$ | 300 | 200 | $> 2^{256}$ |
| $\mu = 7$ | 560 | 392 | $> 2^{256}$ |

*Подделка подписи* представляет собой атаку, состоящую в вычислении подписи к некоторому документу $M$. Например, попытку подделки подписи можно осуществить по следующему алгоритму.

1. Сгенерировать произвольные невырожденные матрицы $\mathbf{R}'_1$ и $\mathbf{R}'_2$.

2. Вычислить хеш-значение $(e_1, e_2, e_3, e_4) = \Phi(M||\mathbf{R}'_1||\mathbf{R}'_2)$ и сгенерировать случайные натуральные числа $s < q$, $\sigma < q$, $\xi < rq$ и $\psi < rq$.

3. Систему из двух матричных уравнений, задаваемых формулами (15) и (16), представить в виде системы из $2\mu^2$ линейных скалярных уравнений, в которых неизвестными являются $\mu^2$ элементов матрицы **S**.

4. Найти решение системы уравнений, составленной на шаге 3.

Легко видеть, что система линейных уравнений, формируемая на шаге 3, с пренебрежимо малой вероятностью ($\ll 2^{256}$) является совместной. Действительно, каждая из систем, включающих $\mu^2$ линейных скалярных уравнений, составленных по матричным уравнениям (15) и (16), может быть легко решена. Однако каждое из двух получаемых решений включает $V = \mu^2$ скалярных значений и является случайным ввиду того, что коэффициенты в этих двух системах линейных уравнений являются случайными. Вероятность совпадения рассматриваемых двух решений может быть оценена значением $p^{-V} \approx 2^{-V|p|}$, где $|p|$ — разрядность числа $p$ в битах. Последнее значение определяет значение трудоемкости $\Lambda$ описанной процедуры подделки подписи: $\Lambda \approx 2^{V|p|} \gg 2^{256}$. Таким образом, по сравнению с алгоритмами ЭЦП, описанными в работах [19, 21, 23], в разработанном алгоритме защищенность от подделки подписи обеспечивается заданием несовместности системы линейных скалярных уравнений, к которым сводятся матричные проверочные уравнения с неизвестной матрицей **S**.

Более эффективным способом подделки подписи является модифицирование известной подписи $(e_1, e_2, e_3, e_4, s, \sigma, \xi, \psi, \mathbf{S})$ таким образом, что модифицированная подпись окажется подлинной для заданного документа $M$. Это может быть осуществлено по следующему алгоритму.

1. В соответствии с формулами (15) и (16) по известной подписи вычислить матрицы $\mathbf{R}'_1$ и $\mathbf{R}'_2$.

2. По заданному документу и вычисленным матрицам $\mathbf{R}'_1$ и $\mathbf{R}'_2$ вычислить хеш-значение $(e'_1, e'_2, e'_3, e'_4) = \Phi(M||\mathbf{R}'_1||\mathbf{R}'_2)$.

3. Вычислить элементы $\xi'$ и $\psi'$ модифицированной подписи: $\xi' = e_3\xi/e'_3 \bmod rq$ и $\psi' = e_4\psi/e'_4 \bmod rq$.

4. Вычислить элементы $s'$ и $\sigma'$ модифицированной подписи: $s' = e_1 s/e'_1 \bmod q$ и $\sigma' = e_2\sigma/e'_2 \bmod q$.

5. Если $e'_4 = e_4\sigma/\sigma' \bmod q$ и $e'_3 = e_3 s/s' \bmod q$, то выдать набор значений $(e'_1, e'_2, e'_3, e'_4, s', \sigma', \xi', \psi', \mathbf{S})$ как подлинную подпись к документу $M$.

В противном случае взять другую известную подпись и перейти к шагу 1 или модифицировать документ $M$ и перейти к шагу 2.

Вероятность выполнения на шаге 5 каждого из двух равенств может быть оценена как $\text{Prob}(e'_4 = e_4\sigma/\sigma' \bmod q) \approx \text{Prob}(e'_3 = e_3 s/s' \bmod q) \approx \approx 2^{-|q|}$. Вероятность одновременного выполнения обоих равенств равна $\approx 2^{-2|q|} \le 2^{256}$. Последнее значение определяет трудоемкость последнего способа подделки подписи, равную $\approx 2^{256}$.

Заметим, что на шаге 4 последнего алгоритма можно вычислить элементы $s'$ и $\sigma'$ модифицированной подписи по формулам $s' = e_3 s/e'_3 \bmod q$ и $\sigma' = e_4\sigma/e'_4 \bmod q$. Тогда успешная подделка имеет вероятность, равную произведению $\text{Prob}(e'_2 = e_2\sigma/\sigma' \bmod q) \times \text{Prob}(e'_1 = e_1 s/s' \bmod q) \approx 2^{-2|q|}$.

*Атака на основе известных подписей.* Для разработанного в настоящей статье алгоритма и известных алгоритмов [21–24], в которых матрицы используются в качестве секретных элементов, актуальным является рассмотрение атаки на основе известных подписей. Такую атаку можно отнести к структурным атакам, которые используют особенности построения алгоритма. Данная структурная атака ориентирована на вычисление только части секретного ключа. После того, как часть секретного ключа становится известной, вычислительная трудоемкость решения БССУ, рассматриваемой в рамках прямой атаки, существенно снижается. Для того чтобы атака на основе известных подписей не снижала оценку стойкости к прямой атаке, при разработке алгоритма следует обеспечить стойкость к упомянутой структурной атаке, равную или более высокую по сравнению со стойкостью к прямой атаке.

При практическом применении алгоритмов ЭЦП потенциальный нарушитель имеет доступ к многим различным известным подписям. В структурной атаке может использоваться одна из следующих случайных матриц, связанных с ЭЦП: $\mathbf{S}$, $\mathbf{R}_1$ и $\mathbf{R}_2$. Также можно рассмотреть версии атаки с использованием двух и трех матриц из указанной тройки. Однако рассмотрение всех версий такой структурной атаки приводит к одинаковым оценкам стойкости. Матрица $\mathbf{S}$ является элементом подписи, а матрицы $\mathbf{R}_1$ и $\mathbf{R}_2$ могут быть вычислены с использованием всех элементов подписи по формулам (15) и (16) соответственно. Рассмотрим вариант с использованием матрицы $\mathbf{S}$.

В наборе из $m$ известных подписей выделим подгоночные матрицы $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_\eta$, каждая из которых вычислена по формуле (14) при фиксированных значениях секретных матриц $\mathbf{D}$ и $\mathbf{F}$ и уникальных неизвестных значениях матриц $(\mathbf{G}_i^n)$ и $(\mathbf{J}_i^d)$, где $i = 1, 2, \ldots, \eta$, выбираемых из коммутативных скрытых групп $<\mathbf{G}>$ и $<\mathbf{J}>$.

Матрицу $(\mathbf{G}_1^n)$ можно взять в качестве матрицы-представителя группы $<\mathbf{G}>$, а матрицу $(\mathbf{J}_1^d)$ – в качестве представителя группы $<\mathbf{J}>$. Тогда выбор каждой из случайных матриц $(\mathbf{G}_i^n)$ и $(\mathbf{J}_i^d)$ для $i = 2, 3, \ldots, \eta$ можно описать как выбор набора из $\mu$ случайных скалярных значений. Система степенных уравнений, записанных по формуле (14), может быть сведена к скалярной БССУ, включающей $\eta\mu^2$ уравнений, $4\mu^2$ фиксированных неизвестных (элементы матриц $\mathbf{D}$, $\mathbf{F}$, $(\mathbf{G}_1^n)$ и $(\mathbf{J}_i^n)$) и $2\mu(\eta - 1)$ уникальных скалярных неизвестных. Для получения БССУ с равным числом уравнений и неизвестных требуется некоторое число известных подписей $\eta_0$, которое может быть получено как решение следующего уравнения относительно $\eta$:

$$\eta\mu^2 = 4\mu^2 + 2\mu(\eta - 1). \qquad (17)$$

Из (17) получаем $\eta_0 = (\mu - 2)^{-1}(4\mu - 2)$. Последнее значение задает скалярную БССУ, содержащую $\mu^2(\mu - 2)^{-1}(4\mu - 2)$ скалярных уравнений. Сложность решения этой БССУ определяет значение стойкости $\Lambda$ к атаке на основе известных подписей. Для значения $\mu = 3$ число степенных уравнений в БССУ равно $\eta_2 = 90$, а для значений $\mu = 5$ и 7 $\eta_2 = 150$, что с учетом данных [4] дает оценки стойкости $\Lambda > 2^{192}$ (для случая $\mu = 3$) и $\Lambda > 2^{256}$ (для случаев $\mu = 5$ и 7), которые не меняют оценки стойкости $W$, полученные из рассмотрения прямолинейной атаки и приведенные в табл. 3.

При использовании значений матриц $\mathbf{R}_1$ и $\mathbf{S}$ в рамках атаки на основе известных подписей она реализуется по следующему алгоритму.

1. Для каждой $i$-й известной подписи ($i = 1, 2, \ldots, \eta$) по проверочному уравнению (15) вычисляется матрица $(\mathbf{R}'_1)_i$, которая в соответствии с формулой (6) равна рандомизирующей матрице $(\mathbf{R}_1)_i$. Индекс $i$ указывает принадлежность соответствующей матрицы $i$-й известной подписи.

2. С использованием формул (6) и (14) составляется система из $2\eta$ матричных уравнений с фиксированными матричными неизвестными $\mathbf{A}$, $\mathbf{D}$, $\mathbf{F}$, $(\mathbf{G}')_1$ и $(\mathbf{J}')_1$ и уникальными матричными неизвестными $\mathbf{G}_1$, $\mathbf{J}_1$, $\mathbf{G}_i$, $\mathbf{J}_i$, $(\mathbf{G}')_i$ и $(\mathbf{J}')_i$, где $i = 2, 3, \ldots, \eta$ и штрихом выделены неизвестные матрицы, относящиеся к рандомизирующей матрице $(\mathbf{R}_1)_i$, т. е. $(\mathbf{R}_1)_i = \mathbf{A}(\mathbf{G}')^k(\mathbf{J}')^t\mathbf{F}$.

3. По системе матричных уравнений, составленной на шаге 2, записывается скалярная БССУ, включающая $2\mu^2\eta$ уравнений в поле $GF(p)$ и $5\mu^2 + 2\mu\eta + 2\mu(\eta - 1)$ скалярных неизвестных, где последние два слагаемых относятся к уникальным матричным неизвестным, каждая из которых выбирается из скрытых циклических групп $<\mathbf{G}>$ и $<\mathbf{J}>$ и описываемых через координаты представителей $(\mathbf{G}')_1$ и $(\mathbf{J}')_1$ этих групп и $\mu$ уникальных скалярных неизвестных.

■ ***Таблица 4.*** Сравнение с постквантовыми стандартами
■ ***Table 4.*** Comparison with post-quantum standards

| Алгоритм | Уровень стойкости, бит (номер стандарта) | Размер, байт | | |
|---|---|---|---|---|
| | | ЭЦП | открытого ключа | секретного ключа |
| Версия $\mu = 3$ | 192 (–) | 216 | 432 | 896 |
| Версия $\mu = 5$ | 256 (–) | 236 | 600 | 1168 |
| Версия $\mu = 7$ | 256 (–) | 291 | 882 | 1656 |
| ML-DSA-65 | 192 (FIPS 204) | 3293 | 1952 | 4032 |
| ML-DSA-87 | 256 (FIPS 204) | 4627 | 2592 | 4896 |
| SLH-DSA-192f | 192 (FIPS 205) | 35 664 | 48 | – |
| SLH-DSA-256f | 256 (FIPS 205) | 49 856 | 64 | – |

4. Решается БССУ, составленная на шаге 4.

Легко установить, что в решаемой БССУ равенство числа уравнений и неизвестных достигается при числе известных подписей, равном $\eta_0 = (2\mu - 4)^{-1}(5\mu - 2)$. При $\mu = 3$ имеем число степенных уравнений $\eta_2 > 100$, а при $\mu = 5$ и 7 $\eta_2 > 150$, т. е. имеем вычислительную сложность последнего варианта атаки на основе известных подписей не меньше, чем для первого варианта.

Сравнение размеров подписи и открытого ключа в разработанном алгоритме и в постквантовых стандартах НИСТ FIPS 204 и FIPS 205 [25] при уровнях 192-битной и 256-битной стойкости представлено в табл. 4, из которой видно, что первый имеет существенно меньший суммарный размер ЭЦП и открытого ключа.

## Заключение

Предложен новый механизм задания вспомогательных скрытых групп в алгебраических схемах ЭЦП, основанных на вычислительной трудности решения БССУ, на основе которого разработан практичный постквантовый алгоритм ЭЦП с использованием алгебр матриц $\mu \times \mu$ в качестве алгебраического носителя. При обеспечении высокого уровня стойкости три версии разработанного алгоритма, соответствующие значениям $\mu = 3, 5, 7$, обладают малыми размерами подписи и открытого ключа, существенно меньшими по сравнению с известными постквантовыми алгоритмами ЭЦП. Предложенный алгоритм может быть использован в качестве прототипа для разработки практичного постквантового стандарта ЭЦП.

## Финансовая поддержка

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках Государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (соглашение № 23-03 от 27.09.2024 г.).

## Благодарность

Авторы признательны анонимному рецензенту за замечания и рекомендации, которые позволили существенно улучшить представление полученных результатов.

## Литература

1. **Ding J., Petzoldt A., Schmidt D. S.** *Multivariate Cryptography*. In: *Multivariate Public Key Cryptosystems*. Ser.: *Advances in Information Security*, 2020, vol. 80, pp. 7–23. Springer, New York, NY. doi:10.1007/978-1-0716-0987-3_2
2. **Ikematsu Y., Nakamura S., Takagi T.** Recent progress in the security evaluation of multivariate public-key cryptography. *IET Information Security*, 2022, vol. 17, pp. 1–17. doi:10.1049/ise2.12092
3. **Shuaiting Q., Wenbao H., Yifa L., Luyao J.** Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.
4. **Ding J., Petzoldt A.** Current state of multivariate cryptography. *IEEE Security and Privacy Magazine*, 2017, vol. 15, no. 4, pp. 28–36.
5. **Sumit Debnath, Dheerendra Mishra.** Post-quantum digital signature scheme based on multivariate cubic problem. *Journal of Information Security and Applications*, 2020, vol. 53, no. 1, pp. 1–8. doi:10.1016/j.jisa.2020.102512

6. **Молдовян Д. Н.** Альтернативный способ построения алгоритмов многомерной криптографии. *Вопросы защиты информации*, 2022, № 3, с. 13–21. doi:10.52190/2073-2600_2022_3_13, EDN: VKCAOV
7. **Костина А. А., Морозова Е. В., Молдовян Д. Н.** Параметризуемые способы задания векторных конечных полей для криптоалгоритмов на нелинейных отображениях. *Вопросы защиты информации*, 2024, № 1, с. 3–10. doi:10.52190/2073-2600_2024_1_3, EDN: QAYIUE
8. **Vysotskaya V. V., Chizhov I. V.** The security of the code-based signature scheme based on the Stern identification protocol. *Прикладная дискретная математика*, 2022, № 57, с. 67–90. doi:10.17223/20710410/57/5, EDN: FFRFUH
9. **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, EDN: AEXSDC
10. **Baldi M., Battaglioni M., Chiaraluce F., Horlemann A.-L., Persichetti E., Santini P., Weger V.** A new path to code-based signatures via identification schemes with restricted errors. *Advances in Mathematics of Communications*, 2025, no. 19(5), pp. 1360–1381. doi:10.3934/amc.2024058
11. **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, pp. 563–608. doi:10.1007/s10623-022-01116-1
12. **Feneuil T., Joux A., Rivain M.** Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs. *Lecture Notes in Computer Science*, 2022, vol. 13508, pp. 541–572. Springer, Cham. doi:10.1007/978-3-031-15979-4_19
13. **Carozza E., Couteau G., Joux A**. Short Signatures from Regular Syndrome Decoding in the Head. *Lecture Notes in Computer Science*, 2023, vol. 14008. Springer, Cham. doi:10.1007/978-3-031-30589-4_19
14. **Baldi M., Bitzer S., Pavoni A., Santini P., Wachter-Zeh A., Weger V.** Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem. *Lecture Notes in Computer Science*, 2024, vol. 14602, pp. 243–274. Springer, Cham. doi:0.1007/978-3-031-57722-2_8
15. **May D. T., Bac D. T., Minh N. H., Kurysheva A. A., Kostina A. A., Moldovyan D. N.** Signature algorithms on non-commutative algebras over finite fields of characteristic two. *Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications (FDSE 2022)*, T. K. Dang, J. Küng, T. M. Chung (eds). *Communications in Computer and Information Science*, 2022, vol. 1688, pp. 273–284. Springer, Singapore. doi:10.1007/978-981-19-8069-5_18
16. **Moldovyan D. N.** A new type of digital signature algorithms with a hidden group. *Computer Science Journal of Moldova*, 2023, vol. 31, no. 1(91), pp. 111–124. doi:10.56415/csjm.v31.06
17. **Курышева А. А.** Способ задания полной рандомизации подписи и алгебраический алгоритм на его основе. *Вопросы защиты информации*, 2024, № 1, с. 38–46. doi:10.52190/2073-2600_2024_1_38, EDN: RPLELR
18. **Молдовян Д. Н., Костина А. А.** Способ усиления рандомизации подписи в алгоритмах ЭЦП на некоммутативных алгебрах. *Вопросы кибербезопасности*, 2024, № 4(62), с. 71–81. doi:10.21681/2311-3456-2024-4-71-81, EDN: RPQEUZ
19. **Молдовян А. А., Молдовян Д. Н., Костина А. А.** Способ усиления рандомизации в постквантовых алгоритмах ЭЦП со скрытой группой. *Информатика и автоматизация*, 2025, т. 24, № 6, с. 1810–1835. doi:10.15622/ia.24.6.9, EDN: WESESL
20. **Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T.** Structure of quaternion-type algebras and a post-quantum signature algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*, 2025, vol. 15, no. 3, pp. 2965–2976. doi:10.11591//ijece.v15i3.pp2965-2976
21. **Dinh K. L., Do T. B., Moldovyan N. A., Petrenko A. S.** Typical algebraic signature schemes with two hidden groups. *Future Data and Security Engineering (FDSE 2025)*, T. K. Dang, J. Küng, T. M. Chung (eds). *Communications in Computer and Information Science*, 2026, vol. 2709, pp. 83–99. Springer, Singapore. doi:10.1007/978-981-95-4724-1_7
22. **Dinh K.-L., Nguyen L.-G., Nguyen H.-M., Do T.-B., Moldovyan A. A., Moldovyan D. N., Kostina A. A.** Post-quantum signature algorithm on finite matrix algebras, using three hidden groups. *2025 2nd International Conference on Cryptography and Information Security (VCRIS) Proceedings*, Hanoi, Vietnam, October 30–31, 2025, pp. 1–8. doi:10.1109/VCRIS68011.2025.11250573
23. **Захаров Д. В., Костина А. А., Морозова Е. В., Молдовян Д. Н.** Алгоритм ЭЦП на алгебре матриц 3×3, использующий две скрытые группы. *Вопросы кибербезопасности*, 2025, № 3(67), с. 45–54. doi:10.21681/2311-3456-2025-3-45-54, EDN:QRNBDD
24. **Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Костина А. А.** Постквантовый алгоритм ЭЦП на основе трудности решения степенных уравнений. *Информатика и автоматизация*, 2026, т. 25, № 3, с. 958–985. doi:10.15622/ia.25.3.11
25. *ML-DSA vs SLH-DSA: Which to Choose*. https://dev.to/quantumsequrity/ml-dsa-vs-slh-dsa-which-to-choose-1c8c?ysclid=mqrutxllbb16437002 (дата обращения: 24.06.2024).

UDC 003.26
doi:10.31799/1684-8853-2026-4-17-27
EDN: GJXNHN

# Post-quantum digital signature algorithm with a new mechanism for specifying auxiliary hidden groups

N. A. Moldovyan[a], Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0002-4483-5048, moldovyan.na@talantiuspeh.ru
A. A. Moldovyan[b], Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0001-5480-6016, maa1305@yandex.ru
[a]Scientific Center of Information Technologies and Artificial Intelligence of Sirius University, 1, Olimpiyskiy Av., 354340, Krasnodar region, federal territory «Sirius», Russian Federation
[b]St. Petersburg Federal Research Center of the RAS, 39, 14th Line, 199178, Saint-Petersburg, Russian Federation

**Introduction:** From the point of view of practical application, the known post-quantum digital signature algorithms have a disadvantage of having a relatively large total size of the public key and signature. **Purpose:** To develop a post-quantum signature algorithm with a small total size of the signature and public key at a given level of security. **Method:** The application of hidden commutative groups in the finite-type algebra of square matrices that are defined over a ground finite field GF(p), and the formation of a public key as a set of matrices that are related to secret matrices through power expressions. **Results:** We develop a practical post-quantum algebraic digital signature algorithm with hidden commutative groups. The security of the algorithm is based on the computational difficulty of solving large systems of power equations. We employ a new method for defining auxiliary hidden groups and a new signature verification mechanism using two verification equations, each involving all signature elements. The finite algebras of $\mu \times \mu$ matrices with $\mu = 3$, 5, and 7 are used as the algebraic support, defining three versions of the proposed algorithm. Security estimates against direct attacks, attacks based on known signatures, and signature forgery have been obtained for all versions of the algorithm. **Practical relevance:** The developed algorithm has small public key size and signature size and is a candidate for a practical post-quantum signature scheme.

**Keywords** — post-quantum cryptography, computer security, digital signature, system of power equations, computationally difficult problem, finite matrix algebra.

**For citation:** Moldovyan N. A., Moldovyan A. A. Post-quantum digital signature algorithm with a new mechanism for specifying auxiliary hidden groups. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 4, pp. 17–27 (In Russian). doi:10.31799/1684-8853-2026-4-17-27, EDN: GJXNHN

## References

1. Ding J., Petzoldt A., Schmidt D. S. *Multivariate Cryptography*. In: *Multivariate Public Key Cryptosystems*. Ser.: *Advances in Information Security*, 2020, vol. 80, pp. 7–23. Springer, New York, NY. doi:10.1007/978-1-0716-0987-3_2
2. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography. *IET Information Security*, 2022, vol. 17, pp. 1–17. doi:10.1049/ise2.12092
3. Shuaiting Q., Wenbao H., Yifa L., Luyao J. Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.
4. Ding J., Petzoldt A. Current state of multivariate cryptography. *IEEE Security and Privacy Magazine*, 2017, vol. 15, no. 4, pp. 28–36.
5. Sumit Debnath, Dheerendra Mishra. Post-quantum digital signature scheme based on multivariate cubic problem. *Journal of Information Security and Applications*, 2020, vol. 53, no. 1, pp. 1–8. doi:10.1016/j.jisa.2020.102512
6. Moldovyan D. N. Alternative method for developing algorithms of multivariate cryptography. *Information Security Questions*, 2022, no. 3, pp. 13–21 (In Russian). doi:10.52190/2073-2600_2022_3_13, EDN: VKCAOV
7. Kostina A. A., Morozova E. V., Moldovyan D. N. Parameterizable methods for specifying vector finite fields for cryptoalgorithms on nonlinear mappings. *Information Security Questions*, 2024, no. 1, pp. 3–10 (In Russian). doi:10.52190/2073-2600_2024_1_3, EDN: QAYIUE
8. Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol. *Applied Discrete Mathematics*, 2022, no. 57, pp. 67–90. doi:10.17223/20710410/57/5, EDN: FFRFUH
9. Nitkin I. S. Permutation compact description method and its application for Stern-based digital signature modification. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 6, pp. 51–63 (In Russian). doi:10.31799/1684-8853-2025-6-51-63, EDN: AEXSDC
10. Baldi M., Battaglioni M., Chiaraluce F., Horlemann A.-L., Persichetti E., Santini P., Weger V. A new path to code-based signatures via identification schemes with restricted errors. *Advances in Mathematics of Communications*, 2025, no. 19(5), pp. 1360–1381. doi:10.3934/amc.2024058
11. 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, pp. 563–608. doi:10.1007/s10623-022-01116-1
12. Feneuil T., Joux A., Rivain M. *Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs*. In: *Lecture Notes in Computer Science*, 2022, vol. 13508, pp. 541–572. Springer, Cham. doi:10.1007/978-3-031-15979-4_19
13. Carozza E., Couteau G., Joux A. *Short Signatures from Regular Syndrome Decoding in the Head*. In: *Lecture Notes in Computer Science*, 2023, vol. 14008. Springer, Cham. doi: 10.1007/978-3-031-30589-4_19
14. Baldi M., Bitzer S., Pavoni A., Santini P., Wachter-Zeh A., Weger V. Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem. In: *Lecture Notes in Computer Science*, 2024, vol. 14602, pp. 243–274. Springer, Cham. doi:0.1007/978-3-031-57722-2_8
15. May D. T., Bac D. T., Minh N. H., Kurysheva A. A., Kostina A. A., Moldovyan D. N. Signature algorithms on non-commutative algebras over finite fields of characteristic two. *Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications (FDSE 2022)*, T. K. Dang, J. Küng, T. M. Chung (eds). *Communications in Computer and Information Science*, 2022, vol. 1688, pp. 273–284. Springer, Singapore. doi:10.1007/978-981-19-8069-5_18
16. Moldovyan D. N. A new type of digital signature algorithms with a hidden group. *Computer Science Journal of Moldova*, 2023, vol. 31, no. 1(91), pp. 111–124. doi:10.56415/csjm.v31.06
17. Kurysheva A. A. A method for specifying complete randomization of a signature and an algebraic algorithm based on it. *Information Security Questions*, 2024, no. 1, pp. 38–46 (In Russian). doi:10.52190/2073-2600_2024_1_38, EDN: RPLELR
18. Moldovyan D. N., Kostina A. A. A method for strengthening signature randomization in signature algorithms on non-commutative algebras. *Voprosy kiberbezopasnosti*, 2024, no. 4(62), pp. 71–81 (In Russian). doi:10.21681/2311-3456-2024-4-71-81, EDN: RPQEUZ
19. Moldovyan A. A., Moldovyan D. N., Kostina A. A. Randomization in post-quantum digital signature algorithms with a secret group. *Informatics and Automation*, 2025, vol. 24, no. 6, pp. 1810–1835 (In Russian). doi:10.15622/ia.24.6.9, EDN: WESESL

20. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T. Structure of quaternion-type algebras and a post-quantum signature algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*, 2025, vol. 15, no. 3, pp. 2965–2976. doi:10.11591//ijece.v15i3.pp2965-2976
21. Dinh K. L., Do T. B., Moldovyan N. A., Petrenko A. S. Typical algebraic signature schemes with two hidden groups. *Future Data and Security Engineering (FDSE 2025)*, T. K. Dang, J. Küng, T. M. Chung (eds). *Communications in Computer and Information Science*, 2026, vol. 2709, pp. 83–99. Springer, Singapore. doi:10.1007/978-981-95-4724-1_7
22. Dinh K.-L., Nguyen L.-G., Nguyen H.-M., Do T.-B., Moldovyan A. A., Moldovyan D. N., Kostina A. A. Post-quantum signature algorithm on finite matrix algebras, using three hidden groups. *2025 2nd International Conference on Cryptography and Information Security (VCRIS) Proceedings*, Hanoi, Vietnam, October 30–31, 2025, pp. 1–8. doi:10.1109/VCRIS68011.2025.11250573
23. Zakharov D. V., Moldovyan D. N., Kostina A. A., Morozova E. V. A digital signature algorithm on the algebra of 3×3 matrices, which uses two hidden groups. *Voprosy kiberbezopasnosti*, 2025, no. 3(67), pp. 45–54 (In Russian). doi:10.21681/2311-3456-2025-3-45-54, EDN: QRNBDD
24. Moldovyan A. A., Moldovyan N. A., Moldovyan D. N., Kostina A. A. Post-quantum digital signature algorithm based on the difficulty of solving power equations. *Informatics and Automation*, 2026, vol. 25, no. 3, pp. 958–983 (In Russian). doi:10.15622/ia.25.3.11
25. *ML-DSA vs SLH-DSA: Which to Choose*. Available at: https://dev.to/quantumsequrity/ml-dsa-vs-slh-dsa-which-to-choose-1c8c?ysclid=mqrutxllbb16437002 (accesed 24 June 2024).

## УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая Scopus и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12 языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org