УДК512.552.18+003.26 **DOI** 10.15622/ia.25.3.11

А.А. Молдовян, Н.А. Молдовян, Д.Н. Молдовян, А.А. Костина

ПОСТКВАНТОВЫЙ АЛГОРИТМ ЭЦП НА ОСНОВЕ ТРУДНОСТИ РЕШЕНИЯ СТЕПЕННЫХ УРАВНЕНИЙ

Молдовян А.А., Молдовян Н.А., Молдовян Д.Н., Костина А.А. **Постквантовый алгоритм ЭЦП на основе трудности решения степенных уравнений.**

Аннотация. Вычислительная сложность нахождения решений больших систем нелинейных уравнений (БСНУ) лежит в основе ряда постквантовых двухключевых криптосхем, включая алгебраические алгоритмы цифровой подписи с использованием матриц в качестве элементов секретного ключа. Такие алгоритмы относятся к вероятностным криптосхемам и характеризуются использованием некоторой матрицы **S** в качестве подгоночного элемента подписи. Последнее обусловливает актуальность рассмотрения стойкости к атакам, использующим известные подписи. При этом лобовой (прямой) атакой является атака на основе решения БСНУ. В известных алгебраических алгоритмах цифровой подписи в рамках лобовой атаки возникают недоопределенные БСНУ с большим числом решений, что создает предпосылки к атакам на основе эквивалентных ключей. В статье рассматривается построение постквантового алгоритма на конечных алгебрах квадратных матриц, при прямой атаке на который возникают близкие к сбалансированным (с равным числом уравнений и неизвестных) и переопределенные БСНУ (с числом уравнений, превышающим число неизвестных). Особенностью предложенного алгоритма является использование вспомогательных скрытых групп, вспомогательного параметра рандомизации ЭЦП, вычисляемого как значение сжимающей односторонней функции от значения **S**. Приводится оценка стойкости к лобовой атаке и нескольким вариантам атак на основе известных подписей.

Ключевые слова: постквантовая криптография, алгоритм ЭЦП, конечная алгебра матриц, система степенных уравнений, секретная группа.

1. Введение. Разработка практичных криптоалгоритмов с открытым ключом, обладающих достаточно высоким уровнем стойкости к атакам с использованием квантового вычислителя, является актуальной задачей постквантовой криптографии [1 – 3]. Существуют эффективные алгоритмы решения задачи дискретного логарифмирования и факторизации [4, 5], поэтому в качестве постквантовых примитивов используются другие вычислительно сложные задачи. Направления постквантовой криптографии задаются видом используемой вычислительно трудной задачи. Достаточно многочисленные исследования посвящены разработке двухключевых криптосхем на корректирующих кодах [6, 7], включая алгоритмы электронной цифровой подписи (ЭЦП) на основе трудности синдромного декодирования [8, 9], построенные путем преобразования протоколов с нулевым разглашением в схему ЭЦП. Однако такое построение приводит к большому размеру открытого ключа (более 600 Кбайт в [8] и более 150 Кбайт в [9] при уровне стойкости 2^{80}). С целью уменьшения длины открытого ключа предложены алгоритмы ЭЦП

на основе задачи синдромного декодирования ограниченных ошибок [10, 11], что позволило существенно уменьшить размер подписи (до 17 Кбайт в [12] и до 11 Кбайт в [13] при уровне стойкости 2^{128}).

В работе [14] рассматривается построение постквантовых алгоритмов ЭЦП на группах, в работе [15] – на булевых функциях. Перспективно использование алгебраических решеток [16, 17] и трудно обратимых функций [18] в качестве носителей постквантовых криптосхем.

Большое число работ посвящено разработке и анализу стойкости криптосхем с открытым ключом, включая алгоритмы ЭЦП, на трудно обратимых отображениях с потайной лазейкой [19 – 21]. Отображения данного типа служат открытым ключом, имеющим очень большой размер, и задаются в виде набора степенных многочленов над конечным полем сравнительно малого порядка. Для уменьшения размера открытого ключа многочлены описываются в виде упорядоченного набора коэффициентов и обычно используются многочлены второй степени. Для выполнения криптографических преобразований входные сообщения (в алгоритмах шифрования по открытому ключу) и значения хеш-функции от подписываемого сообщения (в алгоритмах ЭЦП) представляются в виде многомерных векторов. Прямой атакой на криптоалгоритмы данного типа является вычисление вектора-прообраза по известному выходному вектору, а именно, реализация обратного отображения без знания потайной лазейки, для чего требуется найти решение большой системы нелинейных уравнений (БСНУ), которая определяется набором многочленов, заданным как открытый ключ.

Для квантовых вычислителей неизвестны эффективные алгоритмы решения БСНУ, поэтому криптосхемы на отображениях, являющиеся стойкими в обычном смысле, являются постквантовыми. Однако криптосхемы данного вида обладают существенным с практической точки зрения недостатком – непрактично большим размером открытого ключа. Парадигма [22, 23] построения трудно обратимого отображения с потайной лазейкой как операции возведения в степень $n = 2, 3$ в векторном конечном поле с секретной модификацией и определению потайной лазейки, как операции извлечения корня степени n позволяет сократить длину открытого ключа в несколько десятков раз, но этот недостаток в полной мере не устраняется.

Парадигма разработки алгебраических схем подписи [24, 25], использующих вычислительную трудность решения БСНУ, обеспечивает малые длины открытого ключа и подписи с общей длиной менее 1 Кбайт при уровне стойкости 2^{256}. В качестве носителя

схем ЭЦП данного типа используются некоммутативные конечные алгебры с глобальной единицей, в которых определена ассоциативная операция умножения векторов.

В работе [25] подгоночный элемент ЭЦП в виде вектора **S** вычисляется по формуле:

$$\mathbf{S} = \mathbf{D}\mathbf{J}^{n}\mathbf{V}\mathbf{J}^{d}\mathbf{F}, \quad (1)$$

где **J** – генератор скрытой коммутативной группы <**J**>; $\mathbf{J}^{n}$ и $\mathbf{J}^{d}$ – векторы, выбираемые из группы <**J**> по случайным значениям многоразрядных неотрицательных целых чисел n и d; **D**, **V** и **F** – векторы, являющиеся элементами секретного ключа, которые некоммутативны с векторами из группы <**J**>.

В алгоритме из статьи [26] значение подгоночного вектора **S** задается выражением:

$$\mathbf{S} = \mathbf{D}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{J}^{d}\mathbf{F}, \quad (2)$$

где **G** и **J** – взаимно некоммутативные генераторы двух скрытых коммутативных групп <**G**> и <**J**>; $\mathbf{G}^{n}$ и $\mathbf{J}^{d}$ – векторы, выбираемые по случайным значениями случайных неотрицательных целых чисел n и d, имеющих большую разрядность (100 бит и более); **D** и **F** – элементы секретного ключа, используемые в качестве левого и правого маскирующих множителей, которые некоммутативны между собой и с каждым из векторов **G** и **J**; $\mathbf{L}^{u}$ – скалярный вектор, задаваемый как случайная степень u скалярного вектора **L**, являющегося элементом секретного ключа.

Другой важной особенностью алгоритмов ЭЦП с секретной группой является многократное вхождение вектора **S** в уравнение верификации. Этот прием позволяет обеспечить стойкость к подделке подписи путем решения проверочного уравнения относительно неизвестного значения **S**. Для обеспечения защищенности к такой атаке в некоторых алгоритмах [26] дополнительно используется операция возведения в степень $\rho = \Phi(\mathbf{S})$, где $\Phi(\mathbf{S})$ – некоторая сжимающая однонаправленная функция, например, коллизионно стойкая хэш-функция. В этом случае степень ρ играет роль дополнительного рандомизирующего параметра, который в явном виде не входит в набор значений, составляющих подпись. Поскольку значение ρ вычисляется после получения значения подгоночного элемента **S** и вносит дополнительную рандомизацию, то в проверочное

уравнение указанных алгоритмов ЭЦП требуется включить дополнительный подгоночный элемент подписи.

Формирование подгоночного элемента подписи **S** как по формуле (1), так и по формуле (2) позволяет задать достаточно высокий уровень стойкости к криптоанализу на основе известных подписей, однако прямая атака на алгоритмы из статей [24, 25] связана с решением недоопределенных БСНУ, в которых число степенных уравнений существенно меньше числа неизвестных. Последнее означает наличие большого числа решений, которые соответствуют различным секретным ключам, связанным с открытым ключом. Это означает наличие большого числа эквивалентных секретных ключей, а знание одного из них потенциально позволяет вычислить правильную подпись к произвольному электронному документу.

Несмотря на то, что вычисление даже одного эквивалентного ключа в случае алгоритмов [24, 25] является вычислительно невыполнимым, сам факт существования большого числа эквивалентных ключей создает предпосылки для потенциальных вычислительно эффективных атак с использованием эквивалентных ключей, например, подобных атаке [27], свободной от решения БСНУ. Кроме того, в случае недоопределенных БСНУ в рамках прямой атаки возникает возможность подбора и фиксирования значений части неизвестных, при которых потенциально снижается сложность решения БСНУ.

Потенциальные возможности использования указанных предпосылок в общем случае существенно нивелируются в алгоритмах, для которых БСНУ является сбалансированной (число уравнений равно числу неизвестных) или переопределенной (число неизвестных меньше числа уравнений). Говорить о полном устранении потенциальных атак на основе эквивалентных ключей будет некорректным, так как для этого надо было бы показать, что не существуют варианты представления связи заданного открытого ключа с некоторым секретным ключом с помощью альтернативных формул при обеспечении корректности работы модифицированной схемы подписи и сохранении заданного проверочного уравнения. Однако в случае алгебраических алгоритмов с секретной группой, в которых прямая атака связана с нахождением решения сбалансированных и переопределенных БСНУ, можно ожидать значительного повышения уровня стойкости к потенциальным атакам, использующих факт наличия эквивалентных ключей.

В настоящей работе рассматривается построение постквантового алгоритма ЭЦП на алгебре матриц с использованием вычислительной трудности решения сбалансированных или

переопределенных БСНУ (в зависимости от размерности используемых матриц).

2. Алгебраический носитель. Конечные алгебры матриц размера $\mu\times\mu$ могут быть рассмотрены как частные случаи конечных некоммутативных алгебр (размерности μ^2) с ассоциативной операцией умножения, задаваемой по специальным сильно прореженным таблицам умножения базисных векторов, которые легко записать по правилам матричного умножения. При задании матриц над конечным полем $GF(p)$ имеем конечную алгебру, представляющую собой некоммутативное конечное кольцо с единичным элементом. Совокупность всех невырожденных матриц образует мультипликативную группу этого кольца, порядок которой Ω, выражается следующей формулой:

$$\Omega = \prod_{i=0}^{\mu-1} p^i\,(p^{\mu-i}-1). \tag{3}$$

Если некоторое простое число q является делителем порядка Ω, то, согласно теореме Коши, множество невырожденных матриц содержит матрицу порядка q. В зависимости от значения простого числа p значение выражений в скобках формулы (3) содержит простые делители, разрядность которых может быть как меньше, так и значительно больше разрядности p. Максимальный размер делителя q, который задается специальным выбором простого числа p, имеет место для простых значений μ. При этом значение q выражается формулой:

$$q = p^{\mu-1} + p^{\mu-2} + p + 1. \tag{4}$$

При разрядности числа p, превышающей 15 бит, для случаев $\mu = 2, 3, 5, \ldots, 13$, используя формулу (2) путем многократного тестирования случайно выбираемых простых чисел r, имеющих разрядность $|r|$, легко найти простые числа $p = 2r + 1$ разрядности $|r| + 1$, для которых значение q, вычисленное по формуле (4), также является простым. Примеры нужных троек простых чисел (r, p, q) для значения $\mu = 3$ приведены в статье [25].

Существование матрицы **G** простого порядка q означает существование большого числа матриц **Y** такого порядка, которые могут быть найдены по формуле $\mathbf{Y} = \mathbf{X}^{-1}\mathbf{G}\mathbf{X}$ для каждой невырожденной матрицы **X**, некоммутативной с **G.** Матрица **Y** генерирует циклическую

группу <**Y**> порядка q. Легко показать, что матрица $\pi\mathbf{Y}$, где π является примитивным элементом в $GF(p)$, генерирует циклическую группу $<\pi\mathbf{Y}>$ порядка $p^{\mu-1}-1$. Таким образом, при упомянутом специальном выборе простого числа p в конечной алгебре матриц существуют множество попарно некоммутативных матриц достаточно больших простых порядков. Этот факт далее используется при построении постквантового алгоритма ЭЦП.

При рассмотрении вопроса стойкости разработанного алгоритма возникает задача сведения системы матричных уравнений к системе скалярных уравнений с минимизацией числа скалярных неизвестных. С неизвестной матрицей связаны μ^2 неизвестных элементов поля $GF(p)$, однако в случае выбора η случайных матриц из секретной коммутативной группы неопределенность в значительной степени снимается, благодаря заданию выбора из достаточно ограниченного подмножества матриц по сравнению с множеством всех невырожденных матриц, мощность которого равна Ω (см. формулу (3)). Указанные η матриц вносят всего $\mu^2 + (\eta - 1)\mu$ скалярных неизвестных. Действительно, генератор секретной группы является неизвестным, поэтому он задает μ^2 скалярных неизвестных. При этом, элементы каждой из остальных $\eta - 1$ неизвестных матриц могут быть описаны через значения элементов матрицы-генератора и μ скалярных переменных.

Последнее связано с тем, что множество матриц, входящих в коммутативную группу (в том числе группа, генерируемая матрицей, порядок которой равен многоразрядному натуральному числу), может быть описано по элементам некоторой фиксированной матрицы-представителя и μ скалярным переменным. В качестве такого представителя может быть взят, например, генератор **G** циклической группы <**G**>. На самом деле μ скалярные переменные, каждая из которых принимает значения $0, 1, \ldots, p-1$, описывают множество матриц, образующее коммутативное подкольцо порядка p^{μ}. При этом описывается и любое подмножество матриц, содержащихся в этом подкольце, включая и коммутативную группу <**G**>.

Действительно, рассмотрим матрицу $\mathbf{A} = \|a_{i,j}\|$, в которой задана нумерация строк и столбцов значениями $i,j = 0, 1, \ldots, \mu - 1$, следующего вида:

$$A = \|a_{i,j}\| = \begin{pmatrix} a & b & \ldots & z \\ z & a & b & \ldots \\ \ldots & z & a & b \\ b & \ldots & z & a \end{pmatrix}. \qquad (5)$$

Матрица такого вида задается следующим равенством, имеющим место для каждой фиксированной пары индексов i,j при всех значениях $k = 0, 1, \ldots, \mu - 1$:

$$a_{i,j} = a_{i+k,j+k}. \tag{6}$$

Утверждение. Для любого значения $\mu \geq 2$ и произвольных матриц $\mathbf{A} = \|a_{i,j}\|$ и $\mathbf{A}' = \|a'_{i,j}\|$ вида (5) имеет место равенство $\mathbf{AA}' = \mathbf{A}'\mathbf{A}$ и матрица $\mathbf{B} = \mathbf{AA}' = \|b_{i,j}\|$ также имеет вид (5).

Доказательство. Обозначим нулевую строку матрицы $\mathbf{A}$ ($\mathbf{A}'$) как последовательность $\alpha_0, \alpha_1, \ldots, \alpha_{\mu-1}$ ($\alpha'_0, \alpha'_1, \ldots, \alpha'_{\mu-1}$). Тогда можно записать $a_{i,j} = \alpha_{j-i}$ и $a'_{i,j} = \alpha'_{j-i}$ (где вычитание выполняется по модулю μ). В соответствии с правилами матричного умножения имеем для элементов матриц $\mathbf{B} = \mathbf{AA}' = \|b_{i,j}\|$ и $\mathbf{B}' = \mathbf{A}'\mathbf{A} = \|b'_{i,j}\|$ следующее:

$$b_{i,j} = \sum_{d=0}^{\mu-1} \alpha_{i,d}\alpha'_{d,j} = \sum_{d=0}^{\mu-1} \alpha_{d-i}\alpha'_{j-d}, \tag{7}$$

$$b'_{i,j} = \sum_{d=0}^{\mu-1} \alpha'_{i,d}\alpha_{d,j} = \sum_{d=0}^{\mu-1} \alpha'_{d-i}\alpha_{j-d}. \tag{8}$$

Подставляя в (8) вместо d индекс $d' = (i + j - d) \bmod \mu$, получаем:

$$b'_{i,j} = \sum_{d=0}^{\mu-1} \alpha'_{d-i}\alpha_{j-d} = \sum_{d'=i+j}^{i+j-\mu+1} \alpha'_{j-d'}\alpha_{d'-i}. \tag{9}$$

Легко видеть, что правые части в равенствах (7) и (9) отличаются только порядком слагаемых, поэтому $b'_{i,j} = b_{i,j}$. Поскольку последнее равенство имеет место для всевозможных пар индексов (i,j), то $\mathbf{AA}' = \mathbf{A}'\mathbf{A}$.

В соответствии с формулой (8) для элемента $b_{i+k,j+k}$ (где сложение выполняется по модулю μ) матрицы $\mathbf{B} = \mathbf{AA}'$ можно записать:

$$b_{i+k,j+k} = \sum_{d=0}^{\mu-1} \alpha_{d-i-k}\alpha'_{j+k-d} = \sum_{d=0}^{\mu-1} \alpha_{(d-k)-i}\alpha'_{j-(d-k)}. \tag{10}$$

Сделав замену переменных по формуле $d' = d - k \bmod \mu$, легко видеть, что правые части в равенствах (7) и (10) отличаются только порядком слагаемых, поэтому $b_{i+k,j+k} = b_{i,j}$, т. е. матрица $\mathbf{B}$ относится к матрицам типа (5).

Всевозможные матрицы вида (5) образуют коммутативное подкольцо порядка p^{μ}. Каждая матрица $\mathbf{W} = \|w_{i,j}\|$ этого подкольца может служить его представителем, через который могут быть выражены все матрицы $\mathbf{W}' = \|w'_{i,j}\|$, содержащиеся в подкольце, с помощью μ скалярных переменных $\pi_0, \pi_1, \ldots, \pi_{\mu-1}$, каждая из которых принимает значения $0, 1, \ldots, p-1$. Такое описание задается, например, следующей формулой:

$$w'_{i,j} = w_{i,j} + \pi_{j-i}. \tag{11}$$

Если рассмотреть матрицу $\mathbf{\Pi} = \|\pi_{i,j}\|$ типа (5) с нулевой строкой $\pi_0, \pi_1, \ldots, \pi_{\mu-1}$, то формулу (11) можно записать в виде $\mathbf{W}' = \mathbf{W} + \mathbf{\Pi}$. Из последней формулы для фиксированной невырожденной матрицы $\mathbf{X}$, некоммутативной с матрицей $\mathbf{W}$, имеем:

$$\mathbf{Y}' = \mathbf{X}^{-1}\mathbf{W}'\mathbf{X} = \mathbf{X}^{-1}\mathbf{W}\mathbf{X} + \mathbf{X}^{-1}\mathbf{\Pi}\mathbf{X}, \tag{12}$$

где матрицы $\mathbf{Y}'$ пробегают все значения в некотором коммутативном подкольце порядка p^{μ}, матрицы в котором имеют общий вид, а матрица $\mathbf{Y} = \mathbf{X}^{-1}\mathbf{W}\mathbf{X}$ является представителем этого подкольца, по которому можно описать все значения последнего с помощью скалярных переменных $\pi_0, \pi_1, \ldots, \pi_{\mu-1}$. Действительно, каждый элемент матрицы $\mathbf{X}^{-1}\mathbf{\Pi}\mathbf{X}$ в (12) выражается через элементы матрицы $\mathbf{X}$ и некоторую линейную комбинацию переменных $\pi_0, \pi_1, \ldots, \pi_{\mu-1}$. Для предполагаемого криптоаналитика вывод таких формул не составит значительной трудности в сравнении с вычислительной сложностью решения БСНУ.

3. Разработанный алгоритм ЭЦП. Основными вариантами используемого алгебраического носителя являются конечные алгебры матриц размера $\mu \times \mu$ при простых значениях $\mu = 2, 3, 5, 7$ и 11. При этом алгебра матриц задается над полем $GF(p)$, размер порядка которого составляет $|p| = 64$ бит (при $\mu = 3$), $|p| = 32$ бит ($\mu = 5$) и $|p| = 24$ бит ($\mu = 7$). Конкретное значение p берется таким, что $p = 2r + 1$ при некотором простом значении r, а значение q, вычисленное по формуле (4) также является простым. Выбор таких значений простого числа p позволяет существенно снизить

вычислительную сложность процедуры генерации секретного и открытого ключей. Также рассматриваются параметры реализации разработанной схемы ЭЦП на алгебрах матриц 4×4 и 6×6, однако эти две версии предложенного алгоритма требуют внесения некоторых изменений в процедуру формирования секретного и открытого ключа, которые связаны с тем, что для этих двух случаев формула (4) для получения максимального простого делителя мультипликативной группы алгебры матриц не имеет силы.

Практический интерес представляет также задание матриц над полями характеристики два $GF(2^g)$ при специально выбранных значениях степени расширения g двоичного поля. В настоящей работе рассматривается случай задания алгебры матриц над полем $GF(p)$. Секретный ключ формируется следующим образом:

1. Генерируются случайные невырожденные матрицы **G** и **J** порядка q, которые некоммутативны между собой.

2. Генерируются случайные попарно некоммутативные невырожденные матрицы **A**, **B**, **D** и **F**, которые также некоммутативны с матрицами **G** и **J**.

3. Выбираются два случайных неотрицательных целых числа $x < q$ и $z < q$, таких, что матрица:

$$\mathbf{Q} = \mathbf{G}^x\mathbf{J}^z, \tag{13}$$

имеет порядок $\omega = rq$ и некоммутативна с **A**, **B**, **D**, **F**, **G** и **J**.

4. Генерируются случайные целые числа $u < q$ *и* $v < q$, такие, что матрица:

$$\mathbf{U} = \mathbf{G}^u\mathbf{J}^v, \tag{14}$$

некоммутативна с матрицами **A**, **B**, **D**, **F**, **G**, **J**, **Q** и имеет порядок $\omega = rq$.

5. Выбираются случайные натуральные числа λ, β, α, γ, τ и ε, удовлетворяющие условиям $\lambda < \omega$, $\beta < \omega$, $\alpha < q$, $\gamma < q$, $\tau < q$ и $\varepsilon < q$.

Множество матриц (**A**, **B**, **D**, **F**, **G**, **J**, **Q**, **U**) и набор чисел (x, z, u, v, λ, β, α, γ, τ, ε) составляют секретный ключ, который используется для вычисления набора из девяти матриц (**Y**, **Z**, **K**, **N**, **V**, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$) по следующим формулам формирования открытого ключа:

$$\mathbf{Y} = \mathbf{A}\mathbf{G}^{\alpha}\mathbf{A}^{-1}; \qquad \mathbf{Z} = \mathbf{B}\mathbf{J}^{\alpha}\mathbf{B}^{-1}; \qquad \mathbf{K} = \mathbf{A}\mathbf{Q}^{\lambda}\mathbf{A}^{-1}; \tag{15}$$

$$\mathbf{N} = \mathbf{B}\mathbf{U}^{\lambda}\mathbf{B}^{-1}; \qquad \mathbf{V} = \mathbf{D}\mathbf{G}\mathbf{D}^{-1}; \qquad \mathbf{W} = \mathbf{F}^{-1}\mathbf{J}\mathbf{F}; \tag{16}$$

$$\mathbf{T}_1 = \mathbf{A}\mathbf{Q}^{\beta}\mathbf{G}^{\gamma}\mathbf{B}^{-1}; \quad \mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{J}^{\varepsilon}\mathbf{B}^{-1}; \quad \mathbf{T}_3 = \mathbf{B}\mathbf{U}^{\beta}\mathbf{G}^{\tau}\mathbf{D}^{-1}. \tag{17}$$

Основной вклад в вычислительную трудоемкость процедуры формирования секретного ключа вносят шаги 3 и 4, на каждом из которых осуществляются многочисленные проверки различных пар целочисленных степеней (x, z) и (u, v), соответственно. Размеры открытого и секретного ключей представлены в таблице 1 (следует отметить, что для случаев $\mu = 4$ и $\mu = 6$ простое значение q вычисляется по формуле, отличной от (4)).

Таблица 1. Разрядность параметров p, q, ω и длина открытого и секретного ключей

μ	$\lvert p\rvert$, бит	$\lvert q\rvert$, бит	$\lvert\omega\rvert$, бит	Длина ключа, байт	
				Секретного	Открытого
2	128	128	255	672	576
3	64	128	191	754	648
4	64	128	254	1216	1152
5	32	128	159	968	900
6	32	128	190	1232	1296
7	24	144	167	1362	1323
11	16	160	175	2140	2178

Генерация цифровой подписи к электронному документу M выполняется по секретному ключу и следующему алгоритму (Рис. 1):

1. Выбрать случайные неотрицательные целочисленные значения k, t, w (меньшие, чем q) и y (меньшие, чем ω) и вычислить матрицы:

$$\mathbf{R}_1 = \mathbf{A}\mathbf{G}^{k}\mathbf{Q}^{y}\mathbf{J}^{t}\mathbf{B}^{-1}. \tag{18}$$

$$\mathbf{R}_2 = \mathbf{B}\mathbf{J}^{k}\mathbf{U}^{y}\mathbf{J}^{w}\mathbf{B}^{-1}. \tag{19}$$

2. Вычислить рандомизирующий элемент ЭЦП в виде 512-битного хеш-значения $e = e_1||e_2||e_3||e_4 = \Phi(M||\mathbf{R_1}||\mathbf{R_2})$, где Φ – некоторая специфицированная коллизионно стойкая хеш-функция, а значение e представлено в виде конкатенации четырех 128-битных чисел e_1, e_2, e_3 и e_4.

3. Вычислить подгоночные элементы подписи ξ и ψ:

$$\xi = k(e_1\alpha)^{-1} \bmod q. \tag{20}$$

$$\psi = (y - \beta - 1)(e_2\lambda)^{-1} \bmod \omega. \quad (21)$$

4. Найти значения третьего подгоночного элемента ЭЦП s и подгоночной степени n путем решения следующей системы из двух уравнений первой степени:

$$\begin{cases} \gamma + e_3 s + n = x \bmod q, \\ \tau + e_4 s + n = u \bmod q. \end{cases} \quad (22)$$

Требуемые значения устанавливаются по следующим двум формулам:

$$s = (u - \tau - x + \gamma)(e_4 - e_3)^{-1} \bmod q, \quad (23)$$

$$n = x - \gamma - e_3 s \bmod q. \quad (24)$$

5. Найти подгоночную степень d по формуле:

$$d = z + t - \varepsilon - \alpha e_2 \bmod q. \quad (25)$$

6. Вычислить значение подгоночной матрицы **S** по формуле:

$$\mathbf{S} = \mathbf{D}\mathbf{G}^n\mathbf{J}^d\mathbf{F}. \quad (26)$$

7. Вычислить значение $\rho = \Phi(S) \bmod q$, вносящее дополнительную рандомизацию в процесс формирования ЭЦП.

8. Найти значение вспомогательного подгоночного элемента ЭЦП в виде неотрицательного целого числа σ:

$$\sigma = w - d + v - \varepsilon - \alpha\rho \bmod q. \quad (27)$$

9. Вывести набор значений $(e, \xi, \psi, s, \sigma, \mathbf{S})$ в качестве сформированной цифровой подписи.

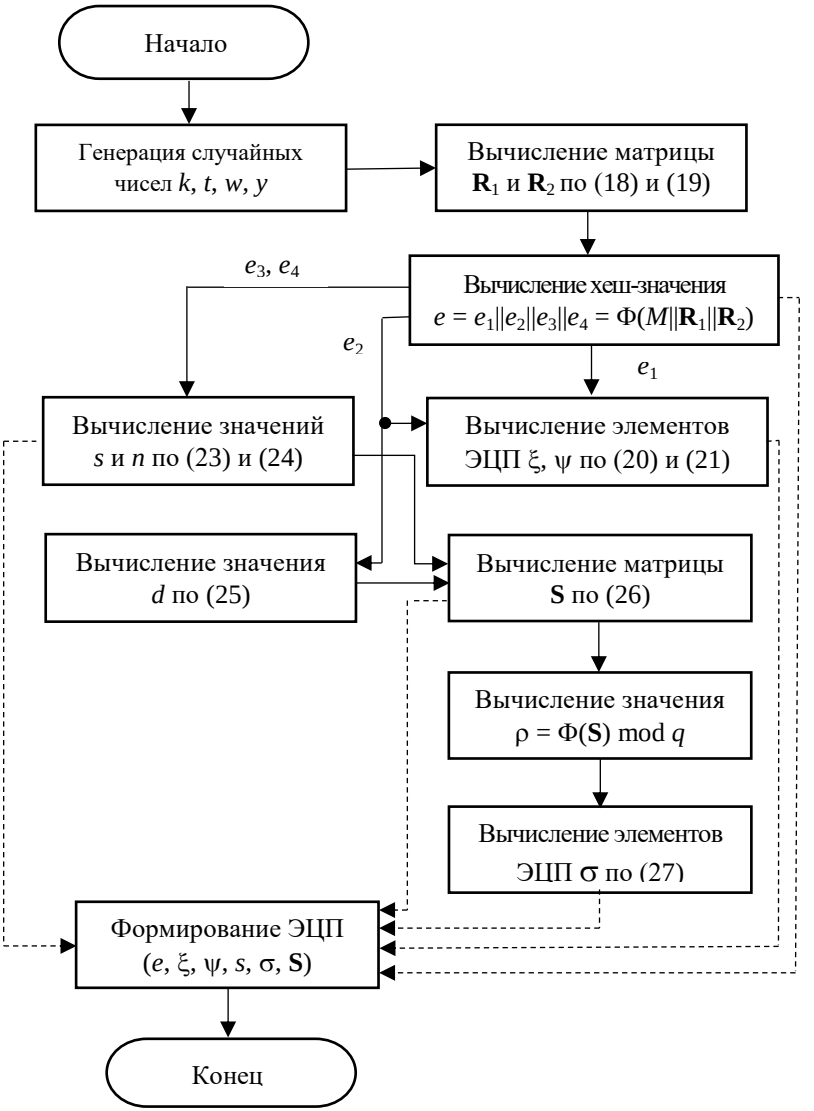

Рис. 1. Генерация ЭЦП

Размеры ЭЦП и отдельных ее элементов показаны в таблице 2 для различных версий разработанного алгоритма, отличающихся различными значениями параметров μ и p. Вычислительная сложность алгоритма генерации подписи в основном определяется восемью операциями возведения в целочисленную степень большого размера, выполняемыми в конечной алгебре матриц. Приближенные оценки вычислительной сложности представлены в таблице 3 с учетом зависимости сложности операций экспоненцирования от разрядности степени и параметров μ и $|p|$.

Таблица 2. Длина ЭЦП и ее отдельных элементов в байтах

μ	e	ξ	ψ	s	σ	**S**	ЭЦП
2	64	16	32	16	16	64	204
3	64	16	24	16	16	72	208
4	64	16	32	16	16	128	268
5	64	16	20	16	16	100	232
6	64	16	24	16	16	144	280
7	64	18	21	18	18	147	286
11	64	20	22	20	20	242	388

Процедура проверки подлинности ЭЦП (e, ξ, ψ, s, σ, **S**) к документу M выполняется с использованием открытого ключа (**Y**, **Z**, **K**, **N**, **V**, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$) по следующему алгоритму (Рис. 2):

1. Вычислить первую проверочную матрицу $\mathbf{R}_1'$ по формуле:

$$R_1^{'} = Y^{e_1\xi} K^{e_2\psi} T_1 V^{e_3 s} \mathrm{ST}_2 Z^{e_2}. \quad (28)$$

2. Вычислить значение $\rho = \Phi(\mathbf{S}) \bmod q$ и вторую проверочную матрицу $\mathbf{R}_2'$:

$$R_2^{'} = Z^{e_1\xi} N^{e_2\psi} T_3 V^{e_4 s} \mathrm{SW}^{\sigma} T_2 Z^{\rho}. \quad (29)$$

3. Вычислить $e' = e'_1||e'_2||e'_3||e'_4 = \Phi(M||\mathbf{R}_1'||\mathbf{R}_2')$.

4. Если $e' = e$, то подпись подлинная, иначе – ложная.

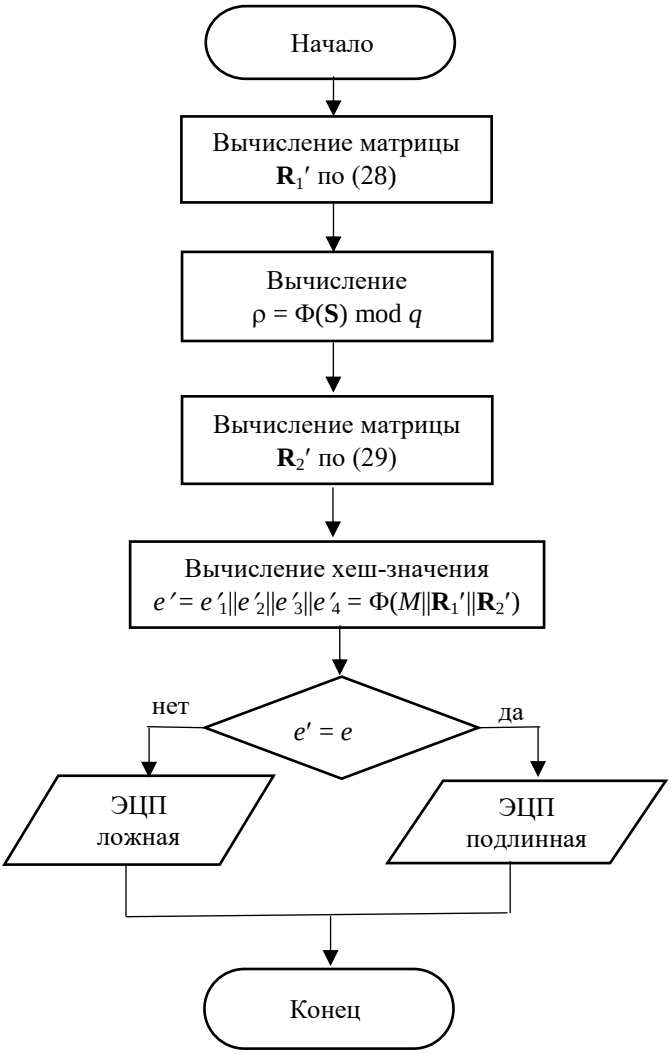

Рис. 2. Верификация ЭЦП

Вычислительная сложность процедуры верификации подписи задается в основном девятью операциями экспоненциирования, осуществляемыми в конечной алгебре квадратных матриц, играющей роль алгебраического носителя алгоритма ЭЦП. Грубые оценки вычислительной сложности процедуры верификации показаны в таблице 3 в приведенных единицах, а именно, в умножения по 16-битному модулю. Последнее позволяет учесть квадратичный рост сложности одной операции возведения в степень с ростом разрядности модуля.

Данные, приведенные в таблицах 2 и 3, показывают, что различные версии разработанного алгоритма вполне применимы на практике. В сопоставлении с известными в литературе постквантовыми алгоритмами-аналогами они представляют больший интерес для приложений, требующих фиксацию открытого ключа и/или цифровой подписи на бумажном носителе. По сравнению с известными постквантовыми алгоритмами ЭЦП разработанный алгоритм имеет минимальный суммарный размер подписи и открытого ключа, тогда как среди первых имеются алгоритмы с меньшим размером подписи при многократно большем размере открытого ключа [20, 21] и алгоритмы с меньшим размером открытого ключа при многократно большем размере подписи [8, 9].

Таблица 3. Вычислительная трудоемкость алгоритмов генерации и верификации ЭЦП для различных версий разработанного алгоритма

μ	Вычислительная сложность, умножений по 16-битному модулю	
	Генерация подписи	Верификация подписи
2	491500	540700
3	276500	304000
5	163200	182400
7	198500	222300
11	237300	266400

Для доказательства корректности работы предложенного постквантового алгоритма ЭЦП покажем, что проверочные матрицы $\mathbf{R}_1'$ и $\mathbf{R}_2'$, вычисляемые на первом и втором шагах процедуры верификации, равны рандомизирующим матрицам $\mathbf{R}_1$ и $\mathbf{R}_2$. Действительно, для подписи (e, ξ, ψ, s, σ, $\mathbf{S}$), вычисленной корректно и в полном соответствии с процедурой генерации ЭЦП, с учетом формул (13)-(18) имеем следующее значение матрицы $\mathbf{R}_1'$:

$$\mathbf{R}_1' = \mathbf{Y}^{e_1\xi}\mathbf{K}^{e_2\psi}\mathbf{T}_1\mathbf{V}^{e_3 s}\mathbf{S}\mathbf{T}_2\mathbf{Z}^{e_2} = (\mathbf{A}\mathbf{G}^{\alpha}A^{-1})^{e_1\xi}\left(\mathbf{A}\mathbf{Q}^{\lambda}\mathbf{A}^{-1}\right)^{e_2\psi}\mathbf{A}\mathbf{Q}^{\beta}\mathbf{G}^{\gamma}\mathbf{D}^{-1} \times$$
$$\times (\mathbf{D}\mathbf{G}\mathbf{D}^{-1})^{e_3 s}(\mathbf{D}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F})\mathbf{F}^{-1}\mathbf{J}^{\varepsilon}\mathbf{B}^{-1}(\mathbf{B}\mathbf{J}^{\alpha}\mathbf{B}^{-1})^{e_2} =$$
$$= \mathbf{A}\mathbf{G}^{\alpha e_1\xi}\boldsymbol{Q}^{\lambda e_2\psi+\beta}\mathbf{G}^{\gamma+e_3 s+n}\mathbf{J}^{d+\varepsilon+\alpha e_2}\mathbf{B}^{-1} =$$

(далее с учетом формул (20)-(25) и (13) имеем следующее):

$$= \mathbf{A}\mathbf{G}^{\alpha e_1\frac{k}{\alpha e_1}}\mathbf{Q}^{\lambda e_2\frac{y-\beta-1}{\lambda e_2}+\beta}\mathbf{G}^{x}\mathbf{J}^{z+t}\mathbf{B}^{-1} = \mathbf{A}\mathbf{G}^{k}\boldsymbol{Q}^{y-1}(\mathbf{G}^{x}\mathbf{J}^{z})\mathbf{J}^{t}\mathbf{B}^{-1} =$$
$$= \mathbf{A}\mathbf{G}^{k}Q^{y-1}\mathbf{Q}\mathbf{J}^{t}\mathbf{B}^{-1} = \mathbf{A}\mathbf{G}^{k}\mathbf{Q}^{y}\mathbf{J}^{t}\mathbf{B}^{-1} = \mathbf{R}_1.$$

С учетом выражения (18) для матрицы $\mathbf{R}_2'$ имеем следующее:

$$\mathbf{R}_2' = \mathbf{Z}^{e_1\xi}\mathbf{N}^{e_2\psi}T_3V^{e_4 s}\mathrm{SW}^{\sigma}T_2Z^{\rho} = (\mathbf{B}\mathbf{J}^{\alpha}\mathbf{B}^{-1})^{e_1\xi}\left(\mathbf{B}\mathbf{U}^{\lambda}\mathbf{B}^{-1}\right)^{e_2\psi}\mathbf{B}\mathbf{U}^{\beta}\mathbf{G}^{\tau}\mathbf{D}^{-1} \times$$
$$\times (\mathbf{D}\mathbf{G}\mathbf{D}^{-1})^{e_4 s}(\mathbf{D}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F})(\mathbf{F}^{-1}\mathbf{J}\mathbf{F})^{\sigma}\mathbf{F}^{-1}\mathbf{J}^{\varepsilon}\mathbf{B}^{-1}(\mathbf{B}\mathbf{J}^{\alpha}\mathbf{B}^{-1})^{\rho} =$$
$$= \mathbf{B}\mathbf{J}^{\alpha e_1\xi}\mathbf{U}^{\lambda e_2\psi+\beta}\mathbf{G}^{\tau+e_4 s+n}\mathbf{J}^{d+\sigma+\varepsilon+\alpha\rho}\mathbf{B}^{-1} =$$

(далее с учетом формул (20)-(25), (14) и (27) имеем следующее):

$$= \mathbf{B}\mathbf{J}^{k}\mathbf{U}^{y-1}\mathbf{G}^{u}\mathbf{J}^{v+w}\mathbf{B}^{-1} = \mathbf{B}\mathbf{J}^{k}\mathbf{U}^{y-1}(\mathbf{G}^{u}\mathbf{J}^{v})\mathbf{J}^{w}\mathbf{B}^{-1} =$$
$$= \mathbf{B}\mathbf{J}^{k}\mathbf{U}^{y-1}\mathbf{U}\mathbf{J}^{w}\mathbf{B}^{-1} = \mathbf{A}\mathbf{J}^{k}\mathbf{U}^{y}\mathbf{J}^{w}\mathbf{B}^{-1} = \mathbf{R}_2.$$

С учетом полученных равенств $\mathbf{R}_1 = \mathbf{R}_1'$ и $\mathbf{R}_2 = \mathbf{R}_2'$ имеем $e' = \Phi(M\|\mathbf{R}_1'\|\mathbf{R}_2') = \Phi(M\|\mathbf{R}_1\|\mathbf{R}_2) = e$, что в соответствии с шагом 4 процедуры верификации ЭЦП означает то, что корректно вычисленная подпись принимается за подлинную подпись. Последний факт доказывает корректность предложенного в данной статье постквантового алгоритма ЭЦП.

4. Оценка стойкости. Предложенный в данной статье алгоритм относится к недетерминированным криптосхемам. При этом используемый механизм рандомизации подписи создает предпосылки для вычисления некоторых элементов секретного ключа по известным подписям. Атака данного типа состоит в вычислении элементов секретного ключа, которые могут быть вычислены непосредственно по подгоночному элементу подписи $\mathbf{S}$ с использованием выражения (26) и/или по матрицам $\mathbf{R}_1'$ и $\mathbf{R}_2'$, вычисляемым по формулам (28) и (29) с использованием всех элементов ЭЦП и следующих равенств $\mathbf{R}_1' = \mathbf{R}_1 = \mathbf{A}\mathbf{G}^{k}\mathbf{Q}^{y}\mathbf{J}^{t}\mathbf{B}^{-1}$ и $\mathbf{R}_2' = \mathbf{R}_2 = \mathbf{B}\mathbf{J}^{k}\mathbf{U}^{y}\mathbf{J}^{w}\mathbf{B}^{-1}$.

Можно выделить несколько основных вариантов атаки на основе известных подписей в зависимости от того, какие из параметров $\mathbf{S}$, $\mathbf{R}_1$ и $\mathbf{R}_2$ и формулы для их вычисления используются для выполнения такой атаки. Указанные параметры могут использоваться отдельно или

в различных сочетаниях, обусловливая существование семи различных вариантов атаки на основе известных подписей.

Вариант 1. Пусть известна совокупность из η подписей, в которых содержатся подгоночные матрицы $\mathbf{S}_1$, $\mathbf{S}_2$, …, $\mathbf{S}_\eta$. Из формулы (26) видно, что секретные матрицы **D** и **F** используются при вычислении каждой подгоночной матрицы $\mathbf{S}_i$ ($i = 1, 2, \ldots, \eta$), т.е. являются фиксированными неизвестными, а матрицы $(\mathbf{G}^{n_i})$ и $(\mathbf{J}^{d_i})$ – при вычислении только одной матрицы $\mathbf{S}_i$, т.е. являются уникальными неизвестными. Матрицы $(\mathbf{G}^{n_i})$ принадлежат коммутативной группе $\langle\mathbf{G}\rangle$, в качестве представителя которой можно взять матрицу $(\mathbf{G}^{n_1})$. Тогда матрицу $(\mathbf{G}^{n_1})$ можно считать фиксированной неизвестной, вносящей в скалярную БСНУ μ^2 скалярных неизвестных, и выражать каждую из остальных матриц $(\mathbf{G}^{n_i})$ для $i = 2, 3, \ldots, \eta$ через μ уникальных скалярных неизвестных. Аналогичным образом примем матрицу $(\mathbf{J}^{n_1})$ за представителя уникальных матриц $(\mathbf{J}^{d_i})$. Тогда в наборе известных подписей будем иметь четыре фиксированные матричные неизвестные **D**, **F**, $(\mathbf{G}^{n_1})$ и $(\mathbf{J}^{d_i})$, которые совместно задают $4\mu^2$ скалярных неизвестных, и $2(\eta - 1)$ уникальных матричных неизвестных, принадлежащих группам $\langle\mathbf{G}\rangle$ и $\langle\mathbf{J}\rangle$. Каждая из уникальных матричных неизвестных вносит μ скалярных неизвестных, а совокупность уникальных матриц – $2\mu(\eta - 1)$ уникальных скалярных неизвестных. Число скалярных неизвестных обоих типов равно $4\mu^2 + 2\mu(\eta - 1)$. Число уравнений в поле $GF(p)$, задаваемых известными подписями, равно $\eta\mu^2$. Эти уравнения образуют скалярную БСНУ, из которой потенциально можно вычислить секретные матрицы **D**, **F**. Из условия равенства числа уравнений и неизвестных имеем следующее уравнение для вычисления требуемого числа подписей η_0:

$$\eta_0\mu^2 = 4\mu^2 + 2\mu(\eta_0 - 1). \qquad (30)$$

Из уравнения (30) имеем $\eta_0 = (4\mu - 2)/(\mu - 2)$. При $\mu = 2$ имеем бесконечное значение, которое показывает, что для этого случая при любом количестве известных ЭЦП число неизвестных в скалярной БСНУ, возникающей в рамках рассматриваемой атаки, существенно превышает число уравнений. Это означает, что в этом случае решение БСНУ не может существенно снять неопределенность значений элементов секретного ключа **D**, **F**. Оценки значения η_0, числа

уравнений и неизвестных в БСНУ и вычислительной сложности атаки для других значений μ приведены в таблице 4.

Вариант 2. Для каждой i-й ($i = 1, 2, \ldots, \eta$) известной подписи по формуле (29) можно вычислить значение рандомизирующей матрицы $\mathbf{R}_{2(i)}$, которое по формуле (19) задает μ^2 уравнений в $GF(p)$. Рассмотрим матрицы $(\mathbf{J}^{k_1})$ и $(\mathbf{U}^{y_1})$ в качестве представителей групп $<\mathbf{J}>$ и $<\mathbf{U}>$. Это устанавливает три фиксированные матричные неизвестные $\mathbf{B}$, $(\mathbf{J}^{k_1})$, $(\mathbf{U}^{y_1})$, которые совместно задают $3\mu^2$ скалярных неизвестных. Матрица $\mathbf{B}^{-1}$ не вносит новых скалярных неизвестных, ввиду того, что она выражается через элементы матрицы $\mathbf{B}$. Каждая из матриц $(\mathbf{J}^{w_1})$, $(\mathbf{J}^{k_i})$, $(\mathbf{J}^{w_i})$, $(\mathbf{U}^{y_i})$, где $i = 2, 3, \ldots, \eta$, задает μ уникальных скалярных неизвестных, т.е. в целом имеется $\mu + 3\mu(\eta - 1)$ неизвестных такого типа. Для вычисления нужного числа известных подписей имеем такое уравнение:

$$\eta_0\mu^2 = 3\mu^2 + \mu + 3\mu(\eta_0 - 1). \tag{31}$$

Из уравнения (31) имеем $\eta_0 = (3\mu - 2)/(\mu - 3)$. При $\mu = 3$ ($\mu = 2$) имеем бесконечное (отрицательное) значение, которое показывает, что для этих случаев рассматриваемый вариант атаки не может дать ограниченного числа решений ни при каком числе известных подписей. Оценки значения η_0 для второго варианта атаки на основе известных подписей приведены в таблице 4.

Вариант 3. Для каждой i-й ($i = 1, 2, \ldots, \eta$) известной ЭЦП, используя выражение (28), устанавливается значение матрицы $\mathbf{R}_{1(i)}$, которое задает μ^2 уникальных скалярных уравнений, записываемых по формуле (18). Каждая из неизвестных матриц $\mathbf{A}$, $\mathbf{B}^{-1}$, $(\mathbf{G}^{k_1})$, $(\mathbf{Q}^{y_1})$, $(\mathbf{J}^{t_1})$, где $(\mathbf{G}^{k_1})$, $(\mathbf{Q}^{y_1})$ и $(\mathbf{J}^{t_1})$ принимаются за представителей секретных коммутативных групп $<\mathbf{G}>$, $<\mathbf{Q}>$ и $<\mathbf{J}>$ соответственно, задает μ^2 фиксированных скалярных неизвестных, т. е. имеем $5\mu^2$ неизвестных такого типа. Каждая из матриц $(\mathbf{G}^{k_i})$, $(\mathbf{Q}^{y_i})$, $(\mathbf{J}^{t_i})$, где $i = 2, 3, \ldots, \eta$, является уникальной матричной неизвестной, поскольку связана только с одной подгоночной матрицей, а именно, с матрицей $\mathbf{S}_i$. Все уникальные матричные неизвестные вносят $3\mu(\eta - 1)$ уникальных скалярных неизвестных. Для вычисления значения η_0 имеем уравнение:

$$\eta_0\mu^2 = 5\mu^2 + 3\mu(\eta_0 - 1). \tag{32}$$

Из (32) имеем формулу $\eta_0 = (5\mu - 3)/(\mu - 3)$. Число уравнений (T) в БСНУ для различных значений μ представлено в таблице 4,

где Λ – значение стойкости к атаке по вариантам 1–3, оцененное для случая $\eta = \eta_0$ с использованием оценок [28] сложности решения БСНУ по числу неизвестных.

Таблица 4. Значение параметров η_0, T и уровня стойкости Λ к атакам на основе известных подписей

μ	Вариант 1			Вариант 2			Вариант 3		
	η_0	T	Λ	η_0	T	Λ	η_0	T	Λ
2	∞	∞	$>2^{256}$	∞	∞	$>2^{256}$	∞	∞	$>2^{256}$
3	10	90	$>2^{192}$	∞	∞	$>2^{256}$	∞	∞	$>2^{256}$
4	7	112	$>2^{256}$	10	160	$>2^{256}$	17	272	$>2^{256}$
5	6	150	$>2^{256}$	6,5	162	$>2^{256}$	11	275	$>2^{256}$
6	5,5	$\approx$200	$>2^{256}$	5,3	191	$>2^{256}$	9	324	$>2^{256}$
7	5,2	$\approx$255	$>2^{256}$	4,8	235	$>2^{256}$	8	392	$>2^{256}$

Дробные значения для параметра η_0 соответствуют случаям, которые следует трактовать как использование только части скалярных уравнений, задаваемых одной из известных подписей при числе последних, равном наименьшему натуральному значению $\eta \geq \eta_0$. В целом все версии разработанного алгоритма обладают высокой стойкостью к рассмотренным вариантам атаки на основе известных подписей. Заметим, что знак ∞ для числа уравнений и неизвестных в БСНУ соответствует случаям, когда ни при каком значении числа известных подписей нельзя добиться ситуации, в которой число уравнений превышает или равно числу неизвестных.

Можно предложить и другие варианты атаки на основе известных ЭЦП, использующие формирование БСНУ:

- по параметрам **S** и $\mathbf{R}_1$;
- по параметрам **S** и $\mathbf{R}_2$;
- по параметрам $\mathbf{R}_1$ и $\mathbf{R}_2$;
- по параметрам **S**, $\mathbf{R}_1$ и $\mathbf{R}_2$.

Детальное рассмотрение этих вариантов показывает, что для каждого из них версии разработанного алгоритма, соответствующие значениям $\mu = 2, 3, \ldots, 7$, обладают стойкостью $>2^{256}$.

В рамках лобовой атаки на разработанный алгоритм требуется решить БСНУ, задаваемую выражениями (13)-(17). Решение системы степенных уравнений в алгебре матриц связано с переходом к скалярной БСНУ, в которой степенные уравнения заданы в конечном поле $GF(p)$. При таком переходе число уравнений возрастает в μ^2 раз.

В системе матричных уравнений неизвестными являются элементы секретного ключа, т.е. девять неизвестных матриц

(**A**, **B**, **D**, **F**, **G**, **J**, **Q**, **U**) и десять неизвестных натуральных значений (x, z, u, v, λ, β, α, γ, τ, ε), входящих в матричные уравнения в качестве степеней, причем разрядность каждого из них равна или превышает 128 бит. Большая разрядность указанных степеней обусловливает практическую невозможность прямолинейного сведения системы матричных уравнений к скалярной БСНУ. Это сведение можно осуществить, вводя следующие дополнительные матричные неизвестные:

− $(\mathbf{G}^x)$, $(\mathbf{G}^u)$, $(\mathbf{G}^\alpha)$, $(\mathbf{G}^\gamma)$ и $(\mathbf{G}^\tau)$, каждая из которых при сведении к скалярной БСНУ задаст μ скалярных неизвестных при их представлении через элементы представителя **G** коммутативной секретной группы <**G**>, т. е. в целом перечисленные матрицы вносят 5μ неизвестных;

− $(\mathbf{J}^z)$, $(\mathbf{J}^v)$, $(\mathbf{J}^\alpha)$ и $(\mathbf{J}^\varepsilon)$, которые зададут 4μ неизвестных в скалярной БСНУ при их представлении через элементы представителя **J** коммутативной секретной группы <**J**>;

− $(\mathbf{Q}^\lambda)$ и $(\mathbf{Q}^\beta)$, которые зададут 2μ неизвестных в скалярной БСНУ при их представлении через элементы представителя **Q** коммутативной секретной группы <**Q**>;

− $(\mathbf{U}^\lambda)$ и $(\mathbf{U}^\beta)$, которые зададут еще 2μ неизвестных в скалярной БСНУ при их представлении через элементы представителя **U** коммутативной секретной группы <**U**>.

Каждая из матриц (**A**, **B**, **D**, **F**, **G**, **J**, **Q**, **U**) вносит μ^2 уникальных скалярных неизвестных, а все вместе задают $8\mu^2$ неизвестных в скалярной БСНУ. С учетом того, что каждая из 13 дополнительных матричных неизвестных определяет μ скалярных неизвестных, имеем следующую формулу для полного числа η_1 скалярных неизвестных:

$$\eta_1 = 8\mu^2 + 13\mu. \tag{33}$$

Выражения (13)-(17) задают 11 матричных уравнений, которые сводятся к $\eta_2 = 11\mu^2$ уравнениям в поле $GF(p)$. В таблице 5 представлены значения числа неизвестных η_1 и уравнений η_2 в скалярной БСНУ, трудность решения которой определяет уровень стойкости Λ' различных версий разработанного алгоритма к прямой атаке.

При $\mu = 2$ и $\mu = 3$ мы имеем недоопределенные БСНУ, при $\mu = 4$ и $\mu = 5$ – примерно сбалансированные, а при $\mu \geq 6$ – переопределенные. Критерием отнесения БСНУ к типу примерно сбалансированных может служить условие $2|\eta_1 - \eta_2| < \mu^2$, использованное при заполнении второй колонки таблице 5. В целом

версии разработанного алгоритма, соответствующие значениям $\mu \geq 4$ обладают более высоким уровнем защищенности к атакам на основе использования эквивалентных секретных ключей по сравнении с алгоритмами [24, 25], для которых имеет место неравенство $\eta_1 - \eta_2 > \mu^2$ и большое число различных решений, соответствующих большому числу эквивалентных секретных ключей. Нахождение конкретных значений последних не проще, чем решение БСНУ с числом уравнений η_2. Однако в общем случае следует сделать предположение о существовании атак, использующих сам факт существования эквивалентных ключей без конкретного их вычисления, которые аналогичны атаке, описанной в работе [27].

Таблица 5. Число неизвестных η_1 и уравнений η_2 в БСНУ, сложность решения которой определяет уровень стойкости Λ' к прямой атаке

μ	Тип БСНУ	η_1	η_2	Λ'
2	недоопределенная	58	44	$>2^{128}$
3	недоопределенная	111	99	$>2^{256}$
4	≈ сбалансированная	180	176	$>2^{256}$
5	≈ сбалансированная	265	275	$>2^{256}$
6	переопределенная	366	396	$>2^{256}$
7	переопределенная	483	539	$>2^{256}$

Для алгоритмов, стойкость которых определяется трудностью решения сбалансированных или переопределенных БСНУ, указанное предположение теряет актуальность, что в данной статье трактуется как повышение защищенности к потенциальным атакам на основе эквивалентных ключей. Вопрос полного устранения атак последнего типа связан с выполнением формального доказательства вычислительной невозможности модифицировать формулы (13)-(17) таким образом, что будет получена модифицированная схема ЭЦП, сохраняющая проверочные уравнения (28) и (29). Выполнение такого доказательства является самостоятельной задачей и связано с принципиальными трудностями, аналогичными тем, которые возникают при попытках доказательства того факта, что некоторый найденный алгоритм взлома криптоалгоритма является наилучшим (обладающий минимальной вычислительной сложностью) из всех потенциально возможных.

Актуальным для разработанного алгоритма является вопрос об оценке сложности подделки подписи путем использования элемента подписи **S** в качестве подгоночного параметра атаки. Действительно, в отличие от известных алгоритмов ЭЦП такого типа, например, [24, 25]

в предложенном алгоритме используются два проверочных уравнения, в которые матрица **S** входит как множитель первой степени, поэтому совместное решение указанных матричных уравнений при прочих фиксированных параметрах сводится к решению системы из $2\mu^2$ скалярных уравнений первой степени, что имеет полиномиальную по времени вычислительную сложность. Способы подделки подписи на основе решения системы линейных уравнений практически устраняются тем, что имеют место следующие два момента.

Во-первых, в разработанном алгоритме одним из параметров второго проверочного уравнения является 128-битная степень ρ, которая вычисляется по значению матрицы **S**, т. е. нет реализуемой возможности зафиксировать значение ρ, что позволило бы прийти к линейной системе скалярных уравнений. Рассмотрение степени ρ в качестве неизвестной обусловливает практическую невыполнимость сведения матричных уравнений к системе скалярных уравнений (линейных или нелинейных).

Во-вторых, фиксирование элементов подписи ξ, ψ, s, σ и значений матриц $\mathbf{R}_1$ и $\mathbf{R}_2$, с последующим вычислением хеш-значения $e = e_1||e_2||e_3||e_4 = \Phi(M||\mathbf{R}_1||\mathbf{R}_2)$ и фиксированием значения ρ, позволяет свести задачу решения системы из двух матричных уравнений (28) и (29), относительно неизвестной матрицы **S,** к решению системы скалярных линейных уравнений, однако вероятность того, что последняя система совместной, т.е. будет иметь решения, является пренебрежимо малой.

Представленные варианты атак на разработанный алгоритм имеют высокую вычислительную сложность, однако в дальнейшем следует уделить внимание разработке других атак и оценкам стойкости к ним. На настоящий момент представляется, что предложенный алгоритм имеет перспективы как кандидат на практичную постквантовую схему подписи, а полученные результаты дают основание для привлечения более широкого круга исследователей к анализу стойкости предложенного алгоритма ЭЦП.

Разработанный в данной работе постквантовый ЭЦП алгоритм представляет существенный практический интерес, однако на данный момент этот алгоритм и общий подход к построению алгебраических алгоритмов на основе трудности решения БСНУ не прошли достаточно длительной апробации с участием широкого круга криптографов. Авторы предполагают, что данная статья послужит побудительным мотивом для вовлечения читателя в процесс указанной апробации.

5. Заключение. Предложен новый постквантовый алгоритм ЭЦП на конечных алгебрах матриц размера $\mu\times\mu$. Все версии разработанного

алгоритма, соответствующие значениям параметра $\mu = 2, 3, 4, 5, 6, 7$ и 11, обладают высоким уровнем стойкости к лобовой атаке и к атаке на основе известных подписей. За счет обеспечения сбалансированности или переопределенности БСНУ для версий алгоритма, соответствующих значениям $\mu = 4, 5, 6, 7, 11$, повышается уровень защищенности к потенциальным атакам на основе эквивалентных ключей. Благодаря сравнительно малой длине подписи и открытого ключа предложенный алгоритм представляет интерес как прототип постквантового стандарта ЭЦП, ориентированного на широкое практическое применение.

Важной задачей дальнейшего исследования предложенного постквантового алгоритма ЭЦП является разработка специальных атак, учитывающих особенности его построения, и оценивание его стойкости к таким атакам.

С целью увеличения производительности и уменьшения схемотехнической сложности аппаратной реализации представляет практический интерес рассмотрение модификации разработанной схемы ЭЦП, использующей в качестве своего носителя конечные алгебры квадратных матриц, заданных над конечными полями характеристики два.

Литература

1. Post-Quantum Cryptography. 16-th International Conference, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025. Proceedings, Part I // Lecture Notes in Computer Science. Springer. 2023. vol. 15577. DOI: 10.1007/978-3-031-86599-2.
2. Post-Quantum Cryptography. 16-th International Conference, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025. Proceedings, Part II // Lecture Notes in Computer Science. Springer. 2023. vol. 15578. DOI: 10.1007/978-3-031-86602-9.
3. Post-Quantum Cryptography. 15-th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. Springer. 2024. vol. 14771–14772. DOI: 10.1007/978-3-031-62743-9.
4. Yan S.Y. Quantum Computational Number Theory // Cham: Springer, 2015. 252 p. DOI: 10.1007/978-3-319-25823-2.
5. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems // New York: Springer, 2013. 207 p. DOI: 10.1007/978-1-4419-7722-9.
6. Codes, Cryptology and Information Security. 4th International Conference, C2SI 2023, Rabat, Morocco, May 29–31, 2023 // Lecture Notes in Computer Science. Springer. 2023. vol. 13874. 265 p. DOI: 10.1007/978-3-031-33017-9.
7. Baldi M., Battaglioni M., Chiaraluce F., et al. A new path to code-based signatures via identification schemes with restricted errors // Advances in Mathematics of Communications. 2025. vol. 19. no. 5. pp. 1360□1381. DOI: 10.3934/amc.2024058.
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.
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.
10. Bidoux L., Gaborit P., Kulkarni M., et al. Code-based signatures from new proofs of knowledge for the syndrome decoding problem // Designs, Codes and Cryptography. 2023. vol. 91. pp. 497–544. DOI: 10.1007/s10623-022-01114-3.
11. 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: Tang, Q., Teague, V. (eds) / Public-Key Cryptography – PKC 2024. PKC 2024 // Lecture Notes in Computer Science. Springer. 2024. vol. 14602. pp. 243–274. DOI: 0.1007/978-3-031-57722-2_8.
12. 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.
13. Feneuil T., Joux A., Rivain M. Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs // Lecture Notes in Computer Science. Springer. 2022. vol. 13508. pp. 541–572. DOI: 10.1007/978-3-031-15979-4_19.
14. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures / In: Johansson T., Smith-Tone D. (eds) / Post-Quantum Cryptography. PQCrypto 2023 // Lecture Notes in Computer Science. Springer. 2023. vol. 14154. pp. 113–138. DOI: 10.1007/978-3-031-40003-2_5.
15. Agibalov G.P. ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. №42. С. 57–65. DOI: 10.17223/20710410/42/4.
16. Gartner J. NTWE: A Natural Combination of NTRU and LWE / In: Johansson T., Smith-Tone D. (eds) / Post-Quantum Cryptography. PQCrypto 2023 // Lecture Notes in Computer Science. Springer. 2023. vol. 14154. pp. 321–353. DOI: 10.1007/978-3-031-40003-2_12.
17. Lysakov I.V. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method // Математические вопросы криптографии. 2023. Т. 14. №2. С. 111–122. DOI: 10.4213/mvk441.
18. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing / In: Ding, J., Steinwandt, R. (eds) / Post-Quantum Cryptography. PQCrypto 2019 // Lecture Notes in Computer Science. Springer. 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
19. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. vol. 17. no. 2. pp. 210–226. DOI: 10.1049/ise2.12092.
20. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography / In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer. 2020. vol. 80. pp. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
21. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar / In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer. 2020. vol. 80. pp. 89–150. DOI: 10.1007/978-1-0716-0987-3_5.
22. Moldovyan N.A. Parameterized method for specifying vector finite fields of arbitrary dimensions // Quasigroups and related systems. 2024. vol. 32. no. 2. pp. 299–312. DOI: 10.56415/qrs.v32.21.
23. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. no. 3(103). pp. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
24. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Постквантовые двухключевые криптосхемы на конечных алгебрах // Информатика и автоматизация. 2024. Т. 23. №4. С. 1246–1276. DOI: 10.15622/ia.23.4.12.

25. Молдовян А.А., Молдовян Д.Н., Костина А.А. Рандомизация в постквантовых алгоритмах ЭЦП с секретной группой // Информатика и автоматизация. 2025. Т. 24. №6. С. 1810–1835. DOI: 10.15622/ia.24.6.9.
26. Dinh K.L., Do T.B., Moldovyan N.A., Petrenko A.S. Typical Algebraic Signature Schemes with Two Hidden Groups / In: Dang, T.K., Kung, J., Chung, T.M. (eds) / Future Data and Security Engineering. FDSE 2025 // Communications in Computer and Information Science. Springer. 2026. vol 2709. pp. 83–99. DOI: 10.1007/978-981-95-4724-1_7.
27. Ma Y. Cryptanalysis of the cryptosystems based on the generalized hidden discrete logarithm problem // Computer Science Journal of Moldova. 2024. vol. 32. no. 2(95). pp. 289–3070. DOI: 10.56415/csjm.v.32.15.
28. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. vol. 15. no. 4. pp. 28–36. DOI: 10.1109/MSP.2017.3151328.

Молдовян Александр Андреевич — д-р тех. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, СПб ФИЦ РАН. Область научных интересов: криптография, постквантовые криптоалгоритмы с открытым ключом, электронная цифровая подпись, криптографические протоколы, компьютерная безопасность. Число научных публикаций — 230. maa1305@yandex.ru; 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-7181, fax +7(812)328-4450.

Молдовян Николай Андреевич — д-р тех. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, СПб ФИЦ РАН. Область научных интересов: криптография, постквантовые алгоритмы цифровой подписи, псевдовероятностные шифры, компьютерная безопасность. Число научных публикаций — 250. nmold@mail.ru; 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-7181, fax +7(812)328-4450.

Молдовян Дмитрий Николаевич — канд. тех. наук, доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ». Область научных интересов: криптография, постквантовые двухключевые криптоалгоритмы на алгебрах и нелинейных отображениях, цифровая подпись, информационная безопасность. Число научных публикаций — 120. mdn.spectr@mail.ru; ул. Профессора Попова, д. 5, г. Санкт-Петербург, 197022, РФ; р.т. +7(812)234-2772.

Костина Анна Александровна — научный сотрудник, лаборатория проблем компьютерной безопасности, СПб ФИЦ РАН. Область научных интересов: криптосхемы с открытым ключом, электронная цифровая подпись, криптографические протоколы, информационная безопасность. Число научных публикаций — 40. to.ann@inbox.ru; 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-7181, fax +7(812)328-4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РНФ: проект № 24-41-04006.

DOI 10.15622/ia.25.3.11

A. MOLDOVYAN, N. MOLDOVYAN, D. MOLDOVYAN, A. KOSTINA

POST-QUANTUM DIGITAL SIGNATURE ALGORITHM BASED ON THE DIFFICULTY OF SOLVING POWER EQUATIONS

Moldovyan A., Moldovyan N., Moldovyan D., Kostina A. **Post-Quantum Digital Signature Algorithm Based on the Difficulty of Solving Power Equations.**

Abstract. The computational complexity of finding solutions to large systems of nonlinear equations (LSNE) underlies a number of post-quantum public-key cryptosystems, including algebraic digital signature algorithms using matrices as secret key elements. Such algorithms belong to probabilistic cryptosystems and are characterized by the use of a certain matrix S as a fitting element of the signature. The latter makes it relevant to consider resistance to attacks using known signatures. In this case, a direct attack is based on the LSNE solution. In well-known algebraic digital signature algorithms, underdetermined LSNE with a large number of solutions arise in the framework of a direct attack, which creates the preconditions for attacks based on equivalent keys. The article considers the construction of a post-quantum algorithm on finite algebras of square matrices, which, when directly attacked, leads to close-to-balanced (with an equal number of equations and unknowns) and overdetermined LSNE (with a number of equations exceeding the number of unknowns). A special feature of the proposed algorithm is the use of auxiliary hidden groups, an auxiliary parameter for the randomization of the digital signature, which is calculated as the value of a compressive one-way function from the value of S. The article provides an assessment of the resistance to direct attacks and several variants of attacks based on known signatures.

Keywords: post-quantum cryptography, digital signature algorithm, finite matrix algebra, system of power equations, secret group.

References

1. Post-Quantum Cryptography. 16-th International Conference, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025. Proceedings, Part I. Lecture Notes in Computer Science. Springer. 2023. vol. 15577. DOI: 10.1007/978-3-031-86599-2.
2. Post-Quantum Cryptography. 16-th International Conference, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025. Proceedings, Part II. Lecture Notes in Computer Science. Springer. 2023. vol. 15578. DOI: 10.1007/978-3-031-86602-9.
3. Post-Quantum Cryptography. 15-th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings. Lecture Notes in Computer Science. Springer. 2024. vol. 14771–14772. DOI: 10.1007/978-3-031-62743-9.
4. Yan S.Y. Quantum Computational Number Theory. Cham: Springer, 2015. 252 p. DOI: 10.1007/978-3-319-25823-2.
5. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems. New York: Springer, 2013. 207 p. DOI: 10.1007/978-1-4419-7722-9.
6. Codes, Cryptology and Information Security. 4th International Conference, C2SI 2023, Rabat, Morocco, May 29–31, 2023. Lecture Notes in Computer Science. Springer. 2023. vol. 13874. 265 p. DOI: 10.1007/978-3-031-33017-9.
7. Baldi M., Battaglioni M., Chiaraluce F., et al. A new path to code-based signatures via identification schemes with restricted errors. Advances in Mathematics of Communications. 2025. vol. 19. no. 5. pp. 1360□1381. DOI: 10.3934/amc.2024058.
8. Vysotskaya V.V., Chizhov I.V. [The security of the code-based signature scheme based on the Stern identification protocol]. Prikladnaya diskretnaya matematika –

Applied discrete Mathematics. 2022. no. 57. pp. 67–90. DOI: 10.17223/20710410/57/5. (In Russ.).
9. Nitkin I.S. [Application of the method of compact substitution description for modifying the digital signature scheme based on the Stern authentication protocol]. Informatsionno-upravlyayushchiye sistemy – Information and Control Systems. 2025. no. 6. pp. 51–63. DOI: 10.31799/1684-8853-2025-6-51-63. (In Russ.).
10. Bidoux L., Gaborit P., Kulkarni M., et al. Code-based signatures from new proofs of knowledge for the syndrome decoding problem. Designs, Codes and Cryptography. 2023. vol. 91. pp. 497–544. DOI: 10.1007/s10623-022-01114-3.
11. 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: Tang, Q., Teague, V. (eds). Public-Key Cryptography – PKC 2024. PKC 2024. Lecture Notes in Computer Science. Springer. 2024. vol. 14602. pp. 243–274. DOI: 0.1007/978-3-031-57722-2_8.
12. 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.
13. Feneuil T., Joux A., Rivain M. Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs. Lecture Notes in Computer Science. Springer. 2022. vol. 13508. pp. 541–572. DOI: 10.1007/978-3-031-15979-4_19.
14. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures. In: Johansson T., Smith-Tone D. (eds). Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. Springer. 2023. vol. 14154. pp. 113–138. DOI: 10.1007/978-3-031-40003-2_5.
15. Agibalov G.P. [ElGamal cryptosystems on Boolean functions]. Prikladnaya diskretnaya matematika – Applied discrete Mathematics. 2018. no. 42. pp. 57–65. DOI: 10.17223/20710410/42/4. (In Russ.).
16. Gartner J. NTWE: A Natural Combination of NTRU and LWE. In: Johansson T., Smith-Tone D. (eds). Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. Springer. 2023. vol. 14154. pp. 321–353. DOI: 10.1007/978-3-031-40003-2_12.
17. Lysakov I.V. [Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method]. Matematicheskiye voprosy kriptografii – Mathematical issues of Cryptography. 2023. vol. 14. no. 2. pp. 111–122. DOI: 10.4213/mvk441. (In Russ.).
18. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing. In: Ding, J., Steinwandt, R. (eds). Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science. Springer. 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
19. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography. IET Information Security. 2022. vol. 17. no. 2. pp. 210–226. DOI: 10.1049/ise2.12092.
20. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. 2020. vol. 80. pp. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
21. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. 2020. vol. 80. pp. 89–150. DOI: 10.1007/978-1-0716-0987-3_5.
22. Moldovyan N.A. Parameterized method for specifying vector finite fields of arbitrary dimensions. Quasigroups and related systems. 2024. vol. 32. no. 2. pp. 299–312. DOI: 10.56415/qrs.v32.21.

23. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms. Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. no. 3(103). pp. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
24. Moldovyany A.A., Moldovyany D.N., Moldovyany N.A. [Post-Quantum Public-Key Cryptoschemes on Finite Algebras]. Informatika i avtomatizatsiya – Informatics and Automation. 2024. vol. 23. no.4. pp. 1246–1276. DOI: 10.15622/ia.23.4.12. (In Russ.).
25. Moldovyany A.A., Moldovyany D.N., Kostina A.A. [Randomization in Post-Quantum Digital Signature Algorithms with a Secret Group]. Informatika i avtomatizatsiya – Informatics and Automation. 2025. vol. 24. no. 6. pp. 1810–1835. DOI: 10.15622/ia.24.6.9. (In Russ.).
26. Dinh K.L., Do T.B., Moldovyan N.A., Petrenko A.S. Typical Algebraic Signature Schemes with Two Hidden Groups. In: Dang, T.K., Kung, J., Chung, T.M. (eds). Future Data and Security Engineering. FDSE 2025. Communications in Computer and Information Science. Springer. 2026. vol 2709. pp. 83–99. DOI: 10.1007/978-981-95-4724-1_7.
27. Ma Y. Cryptanalysis of the cryptosystems based on the generalized hidden discrete logarithm problem. Computer Science Journal of Moldova. 2024. vol. 32. no. 2(95). pp. 289–3070. DOI: 10.56415/csjm.v.32.15.
28. Ding J., Petzoldt A. Current State of Multivariate Cryptography. IEEE Security and Privacy Magazine. 2017. vol. 15. no. 4. pp. 28–36. DOI: 10.1109/MSP.2017.3151328.

Moldovyan Alexandr — Ph.D., Dr. Sci., Professor, Chief researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: cryptography, post-quantum public key cryptography, electronic digital signature, cryptographic protocols, computer security. The number of publications — 230. maa1305@yandex.ru; 39, 14th Line V. O., 199178, Saint-Petersburg, Russia; office phone: +7(921)953-0373.

Moldovyan Nikolay — Chief researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: cryptography, post-quantum digital signature algorithms, pseudo-probabilistic ciphers, computer security. The number of publications — 250. nmold@mail.ru; 39, 14th Line V. O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181.

Moldovyan Dmitry — Ph.D., Associate professor, Department of Information Systems, Federal State Autonomous Educational Institution of Higher Education St. Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin) (SPbGETU "LETI"). Research interests: cryptography, post-quantum two-key cryptographic algorithms on algebras and nonlinear mappings, digital signature, information security. The number of publications — 120. mdn.spectr@mail.ru; 5, Professora Popova St., 197022, Saint-Petersburg, Russia; office phone: +7(812)234-2772.

Kostina Anna — Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: public key cryptosystems, electronic digital signatures, cryptographic protocols, and information security. The number of publications — 40. to.ann@inbox.ru; 39, 14th Line V. O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181.

Acknowledgements. This research is supported by RSF (project #24-41-04006).