АЛГОРИТМ ЭЦП НА АЛГЕБРЕ МАТРИЦ 3×3, ИСПОЛЬЗУЮЩИЙ ДВЕ СКРЫТЫЕ ГРУППЫ

Захаров Д. В.[1], Костина А. А.[2], Морозова Е. В.[3], Молдовян Д. Н.[4]

DOI: 10.21681/2311-3456-2025-3-45-54

Цель работы: *повышение производительности алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений.*

Метод исследования: *применение алгебры матриц размерности 3×3, заданных над конечным полем GF(p), в качестве алгебраического носителя. Выбор треугольных матриц как элементов простого порядка p. Применение автоморфного отображения некоммутативной конечной алгебры для генерации матриц требуемого порядка, имеющих общий вид.*

Результаты исследования: *впервые в качестве алгебраического носителя алгоритмов ЭЦП, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений, использована алгебра матриц размерности 3×3. Рандомизация подписи обеспечивается ее вычислением в зависимости от двух случайных элементов, выбираемых из двух скрытых коммутативных групп, элементы одной из которых является некоммутативными с элементами другой. Предложены алгоритмы вычисления генераторов скрытых групп порядков p, $p^2 - 1$ и $p^2 + p + 1$. Впервые при вычислении элементов открытого ключа по элементам секретного ключа в качестве маскирующего множителя использован алгебраический элемент порядка два и показано существование достаточно большого числа нескалярных матриц, обладающих порядком два. Дана оценка стойкости разработанного алгоритма.*

Научная и практическая значимость *результатов статьи состоит в повышении производительности постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений.*

Ключевые слова: *конечная некоммутативная алгебра; ассоциативная алгебра; алгебра матриц, вычислительно трудная задача; скрытая коммутативная группа; цифровая подпись; рандомизация подписи; постквантовая криптография.*

Введение

Разработка постквантовых криптографических алгоритмов с открытым ключом в настоящее время привлекает существенное внимание мирового криптографического сообщества [1, 2]. Криптоалгоритмы, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений, представляют существенный интерес в качестве постквантовых криптосхем. До последнего времени такие алгоритмы строились на трудно-обратимых нелинейных отображениях с секретной лазейкой [3–5]. Основным недостатком известных алгоритмов данного типа является большой размер открытого ключа (от сотни килобайт до нескольких мегабайт). Даже способ многократного уменьшения размера открытого ключа, предложенный в работах [6-8], не решает в полной мере этой проблемы. Сравнительно недавно [9–11] предложены алгебраические алгоритмы ЭЦП со скрытой группой, использующие вычислительную трудность решения больших систем степенных уравнений. Алгоритмы последнего типа обладают сравнительно малыми размерами подписи и открытого ключа, однако для обеспечения достаточной рандомизации подписи в них используется удвоенное проверочное уравнение, что приводит к снижению производительности процедуры верификации ЭЦП.

В настоящей статье разрабатывается способ усиления рандомизации подписи за счет использования двух скрытых коммутативных групп и вычисления ЭЦП в зависимости от двух случайных взаимно некоммутативных элементов, выбираемых из скрытых групп. На основе предложенного способа реализован алгебраический алгоритм ЭЦП с одним проверочным уравнением, за счет чего достигнуто повышение производительности процедуры верификации ЭЦП. Для повышения стойкости в качестве алгебраического носителя используется конечная алгебра матриц 3×3. Выбор такой размерности связан с сочетанием возможности получения достаточно низкой сложности операции матричного умножения

1 Захаров Дмитрий Викторович, кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. Санкт-Петербург, Россия. ORCID: https://orcid.org0009-0004-5731-3611. E-mail: zakharov.dmitriy@gmail.com

2 Костина Анна Александровна, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

3 Морозова Елена Владимировна, кандидат технических наук, доцент кафедры Комплексного обеспечения информационной безопасности. Государственный университет морского и речного флота имени адмирала С. О. Макарова. Санкт-Петербург, Россия. E-mail: lenmor@mail.ru

4 Молдовян Дмитрий Николаевич, кандидат технических наук, доцент кафедры Информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ». Санкт-Петербург, Россия. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

и достаточно высокого коэффициента увеличения числа уравнений при сведении системе векторных степенных уравнений к соответствующей системе скалярных уравнений. Впервые в качестве маскирующего секретного множителя при вычислении элементов открытого ключа используется случайная матрица порядка два, отличная от скалярной матрицы.

Формализация цели исследования

Вычисление подгоночного элемента $\mathbf{S}$ подписи $(e, \mathbf{S})$ в алгебраических алгоритмах ЭЦП со скрытой группой [9], использующих конечную некоммутативную ассоциативную алгебру (КНАА), выполняется по формуле, включающей уникальный элемент $\mathbf{G}$ скрытой группы, вычисляемый в зависимости от рандомизирующего элемента подписи e:

$$\mathbf{S} = \mathbf{DGF}, \quad (1)$$

где $\mathbf{D}$ и $\mathbf{F}$ – секретные маскирующие множители (элементы секретного ключа). Несмотря на уникальность значения $\mathbf{G}$ для каждой подписи $(e, \mathbf{S})$, атака на основе набора известных подписей, позволяющая вычислить секретный элемент $\mathbf{D}$ и некоторый представитель $\mathbf{G}'$ скрытой группы, имеет сравнительно низкую вычислительную сложность, что означает снижение уровня стойкости. Эта уязвимость связана с неполнотой рандомизации подписи, обусловленной ограниченностью выбора элемента $\mathbf{G}$ из скрытой группы, имеющей порядок, намного меньший порядка КНАА.

Усиление рандомизации подписи в алгоритмах [11, 12] обеспечивается за счет того, что вычисление подгоночного элемента подписи $\mathbf{S}$ выполняется по формуле, включающей случайный обратимый элемент $\mathbf{V}$ конечной алгебры, используемой в качестве алгебраического носителя:

$$\mathbf{S} = \mathbf{DGV}. \quad (2)$$

Однако, использование случайного элемента $\mathbf{V}$ при вычислении подгоночного элемента подписи делает невозможным использование уравнения верификации ЭЦП с многократным вхождением значения $\mathbf{S}$, поэтому в алгоритмах [11, 12] используется процедура верификации ЭЦП по двум проверочным уравнениям. Использование такого приема создает предпосылки к подделке подписи с использованием элемента $\mathbf{S}$ в качестве подгоночного параметра атаки.

Для устранения такой потенциальной атаки используются вспомогательные приемы, требующие выполнения дополнительных операций, что приводит к дополнительному снижению производительности алгебраических алгоритмов ЭЦП со скрытой группой. Прием такого типа, предложенный в работе [13], связан с заданием двух скрытых коммутативных групп, элементы одной из которых являются некоммутативными с элементами другой, и использованием вспомогательного параметра рандомизации ρ, вычисляемого как хеш-значение от предварительно вычисленного значения $\mathbf{S}$, и вспомогательного подгоночного элемента подписи в виде натурального числа σ.

В работе [13] также показано, что включение в формулу (2) дополнительного случайного множителя в виде элемента $\mathbf{P}$ из второй скрытой группы вносит самостоятельное существенное усиление рандомизации подписи. При этом формула рандомизации подписи приобретает вид:

$$\mathbf{S} = \mathbf{DPGV} \quad (3)$$

с тремя уникальными (в каждой подписи) множителями $\mathbf{P}$, $\mathbf{G}$ и $\mathbf{V}$. В статье [13] показано, что выбор случайного обратимого элемента из всей КНАА, используемой в качестве алгебраического носителя, не обеспечивает безусловно полной рандомизации, так как следует учесть, что для обеспечения корректности работы алгоритма ЭЦП случайный вектор $\mathbf{V}$ также входит и в формулу для вычисления рандомизирующего вектора $\mathbf{R}$, значение которого восстанавливается в ходе процедуры верификации ЭЦП и позволяет составить по известным подписям систему степенных уравнений с числом неизвестных, меньшим числа уравнений.

В настоящей работе используется следующая формула усиленной (по сравнению с формулой (1)) рандомизации подписи:

$$\mathbf{S} = \mathbf{DPGF}. \quad (4)$$

При этом в процедуре верификации ЭЦП используется только одно проверочное уравнение, но с многократным вхождением подгоночного элемента подписи $\mathbf{S}$. Для обеспечения корректности работы алгоритма ЭЦП с двумя скрытыми коммутативными группами используется вспомогательный подгоночный элемент подписи в виде натурального числа σ.

1. Используемые свойства алгебры матриц 3×3

В качестве алгебраического носителя в разработанном алгоритме ЭЦП используется конечная алгебра матриц 3×3, заданная над простым конечным полем $GF(p)$. Такой носитель можно трактовать как девятимерная КНАА, заданная по таблице умножения базисных векторов (ТУБВ), представленной в виде табл. 1. В m-мерной КНАА векторы можно представить в виде упорядоченного набора координат $\mathbf{A} = (a_1, a_2, \ldots, a_m)$ и в виде суммы его компонент $\mathrm{A} = \sum_{i=1}^{m} a_i\, e_i$, где e_i – базисные векторы. Умножение двух векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=1}^{m} b_j\, e_j$ обычно определяется как перемножение каждой компоненты $\mathbf{A}$ с каждой компонентой $\mathbf{B}$, а именно, по следующей формуле:

$$\mathbf{AB} = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i\, b_j\, (e_i\, e_j), \quad (5)$$

в которой каждое из всех произведений пар базисных векторов вида $\mathbf{e}_i\mathbf{e}_j$ подлежит замене на некоторый однокомпонентный вектор вида $\lambda\mathbf{e}_k$ (в общем случае – на многокомпонентный вектор) в соответствии с некоторой ТУББ. Значение $\lambda \neq 1$ называется структурной константой. При этом левый множитель в произведении $\mathbf{e}_i\mathbf{e}_j$ указывает строку, а правый – столбец, пересечение которых выделяет ячейку, содержащую значение $\lambda\mathbf{e}_k$. При наличии многих ячеек, содержащих структурную константу, равную нулю, ТУББ называется прореженной. Далее матрицы будем обозначать жирными латинскими буквами.

Таблица 1 относится к прореженным ТУББ, обеспечивающим сравнительно низкую вычислительную сложность операции умножения векторов. Прореженные ТУББ известны для случая четырехмерных КНАА и используются в алгоритмах ЭЦП, предложенных в работах [12, 13]. Интерес к использованию четырехмерных КНАА, заданных над $GF(p)$, также обусловливается тем, что для них (в том числе для алгебры матриц 2×2) детально исследована декомпозиция на коммутативные подалгебры порядка p^2 [14, 15]. Знание строения КНАА имеет значение как для синтеза алгебраических алгоритмов ЭЦП, так и для анализа их стойкости к различным видам атак.

В общем случае изучение декомпозиции (на коммутативные подалгебры) КНАА размерности шесть и более представляет собой нетривиальную задачу. В случае алгебр матриц 3×3 частные детали строения, важные для разработки алгебраических алгоритмов ЭЦП, могут быть установлены. Рассмотрим некоторые из таких деталей, поясняющих выбор матриц в качестве элементов секретного ключа. В случае конечных групп невырожденных матриц $\mathbf{M}$ размерности $m \times m$, заданных над полем $GF(p)$, их порядок $\boldsymbol{\Omega}$ описывается следующей формулой[5]:

$$\boldsymbol{\Omega} = \prod_{i=0}^{m-1} p^i (p^{m-i} - 1). \quad (6)$$

В соответствии с теоремой Силова наличие простого делителя q порядка конечной некоммутативной группы показывает наличие элементов порядка q, содержащихся в таких группах. Такие элементы генерируют коммутативные группы, содержащиеся в алгебре матриц. Для случая размерности $m = 3$ порядок мультипликативной группы алгебры матриц равен

$$\boldsymbol{\Omega}_{3\times 3} = p^3(p-1)^3(p^2+p+1)(p+1). \quad (7)$$

Из формулы (7) видим, что существуют матрицы простого порядка p, причем для заданного значения битовой длины простое значение p может быть выбрано таким, что число $q = p^2 + p + 1$ также является простым. Примеры таких случаев представлены в табл. 2. Матрица порядка q генерирует коммутативную группу, включающую $q - 1$ нескалярных матриц. Учитывая наличие в некоммутативных группах автоморфного отображения вида

$$\mathbf{Y} = \mathbf{AQA}^{-1}, \quad (8)$$

где $\mathbf{A}$ – обратимая (невырожденная) матрица и $\mathbf{Q}$ – матрица порядка q, можно сделать заключение о достаточном числе различных циклических групп порядка q.

Утверждение 1. Пусть дано разрешимое уравнение $\mathbf{A} = \mathbf{XBX}^{-1}$ с неизвестной матрицей $\mathbf{X}$ при фиксированных нескалярных невырожденных матрицах $\mathbf{A}$ и $\mathbf{B} \neq \mathbf{A}$. Тогда данное уравнение имеет количество

5 Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. – М.: Физматлит, 1996. – 287 с.

Таблица 1.

Таблица умножения базисных векторов при трактовке матриц $||a_{ij}||$ размерности 3×3 как девятимерных векторов $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33})$

.	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0	0	0	0
$\mathbf{e}_1$	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0
$\mathbf{e}_2$	0	0	0	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0	0	0	0
$\mathbf{e}_4$	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0
$\mathbf{e}_5$	0	0	0	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0	0	0	0
$\mathbf{e}_7$	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0
$\mathbf{e}_8$	0	0	0	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$

Таблица 2.

ТПростые значения $q = p^2 + p + 1$ при небольших простых p

p	3	5	37	59	71	89	101	131
q	13	31	1723	3541	5113	8011	10303	17293

решений, равное числу всех матриц коммутативных с матрицей $\mathbf{B}$, включая саму матрицу $\mathbf{B}$.

Доказательство. Разрешимость матричного уравнения $\mathbf{A} = \mathbf{XBX}^{-1}$ означает существование некоторого решения $\mathbf{X}_0$. Каждый обратимый вектор $\mathbf{V}$, коммутативный с $\mathbf{B}$, задает уникальное решение $\mathbf{X} = \mathbf{X}_0\mathbf{V}$. Действительно, имеем

$$(\mathbf{X}_0\mathbf{V})\mathbf{B}(\mathbf{X}_0\mathbf{V})^{-1} = \mathbf{X}_0\mathbf{VBV}^{-1}\mathbf{X}_0^{-1} = \\ = \mathbf{X}_0\mathbf{BVV}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{BX}_0^{-1} = \mathbf{A}.$$

Таким образом, имеем столько уникальных решений, сколько имеется невырожденных матриц, коммутативных с $\mathbf{B}$. Покажем, что других решений нет. Пусть имеется решение $\mathbf{X}_i$. Тогда имеем:

$$\{\mathbf{X}_i\mathbf{BX}_i^{-1} = \mathbf{X}_0\mathbf{BX}_0^{-1}\} \Rightarrow \{(\mathbf{X}_0^{-1}\mathbf{X}_i)\mathbf{B} = \mathbf{B}(\mathbf{X}_0^{-1}\mathbf{X}_i); \\ \mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)\}.$$

Последние два равенства показывают, что любое решение $\mathbf{X}_i$ представимо в виде произведения решения $\mathbf{X}_0$ на вектор $(\mathbf{X}_0^{-1}\mathbf{X}_i)$, который коммутативен с $\mathbf{B}$.

С учетом того, что матрица $\mathbf{Q}$, имеющая порядок q, является нескалярной матрицей, а значит базис <$\mathbf{Q}$, $\mathbf{L}$>, где $\mathbf{L}$ – скалярная матрица порядка $p - 1$, генерирует коммутативную группу порядка $(p^2 + p + 1)(p - 1)$, причем вне этой группы нет векторов, перестановочных с $\mathbf{Q}$, легко видеть, что имеется $(p^2 + p + 1)(p - 1)$ различных матриц $\mathbf{A}$, задающих один и тот же автоморфный образ циклической группы, генерируемой матрицей $\mathbf{Q}$. При подстановке всех невырожденных матриц 3×3 в формулу (8) в качестве матрицы $\mathbf{A}$ получаем η_q' различных матриц $\mathbf{Y}$. Для значения η_q имеем следующую формулу:

$$\eta_q' = p^3(p - 1)^2(p + 1). \qquad (9)$$

Доля матриц $\mathbf{Y}$ попадающих в одну и ту же коммутативную группу порядка $p^3 - 1$ является достаточно малой, поэтому количество различных коммутативных групп порядка $p^3 - 1$ (а значит и коммутативных групп порядка q) можно оценить значением $\eta_q' \approx \eta_q \approx p^6$. Рассмотрение числа η_p различных циклических групп порядка p также приводит к оценке $\eta_p \approx p^6$. При предполагаемом для использования 80-битном размере простого числа p доля матриц, входящих в циклические группы порядков p и q, достаточно велика, чтобы алгоритм генерации матриц простых порядков p и q, основанный на выборе случайных матриц, имел достаточную вычислительную эффективность.

Алгоритм генерации матрицы $\mathbf{Q}$ простого порядка $q = p^2 + p + 1$, например, может включать следующие шаги:

1. Сгенерировать случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить значение $z = \Omega_{3\times3}(p^2 + p + 1)^{-1} = p^3(p - 1)^3(p + 1)$.
3. Вычислить матрицу $\mathbf{Q} = \mathbf{M}^z$ и проверить выполнимость неравенства $\mathbf{Q} \neq \mathbf{E}$. Если $\mathbf{Q} = \mathbf{E}$, то перейти к шагу 1.
4. Вывести матрицу $\mathbf{Q}$ как матрицу простого порядка $q = p^2 + p + 1$.

Для генерации матриц порядка p можно предложить алгоритм с более высокой вычислительной эффективностью, который основан на следующем утверждении.

Утверждение 2[6]. Невырожденные треугольные матрицы размерности 3×3 над конечным полем $GF(p)$ имеют простое значение порядка, равное p.

Доказательство. Возведение верхне-треугольной матрицы в квадрат дает следующее:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}. \qquad (10)$$

Допустим, что для произвольного целого $k \geq 2$ имеет место формула

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}. \qquad (11)$$

Тогда возведение рассматриваемой матрицы в степень $k + 1$ дает

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} =$$

6 Горячев А.А., Молдовян Д.Н., Куприянов И.А. Выбор параметров задачи скрытого дискретного логарифмирования для синтеза криптосхем // Вопросы защиты информации. 2011. 1. С. 19–23.

$$= \begin{pmatrix} 1 & a+ka & b+kac+kb+\frac{k(k-1)}{2}ac \\ 0 & 1 & c+kc \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & (1+k)a & (1+k)b+\frac{k(k+1)}{2}ac \\ 0 & 1 & (1+k)c \\ 0 & 0 & 1 \end{pmatrix}. \quad (12)$$

Формула (10) получается из (11) при подстановке значения степени $k = 2$. В соответствии с методом математической индукции делаем вывод, что формула (11) верна при произвольных натуральных степенях k. При $k = p$ получаем единичную матрицу, т.е. порядок рассматриваемой треугольной матрицы равен p. Аналогичным путем получаем следующую формулу для произвольной нижне-треугольной матрицы:

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 & 0 \\ ka & 1 & 0 \\ kb+\frac{k(k-1)}{2}ac & kc & 1 \end{pmatrix}. \quad (13)$$

При $k = p$ правая часть формул (11) и (13) равна единичной матрице, что требовалось доказать.

Алгоритм генерации матрицы $\mathbf{P}$ порядка p включает следующие шаги:

1. Сгенерировать случайную треугольную матрицу $\mathbf{T}$ и случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить матрицу $\mathbf{P}$ по формуле $\mathbf{P} = \mathbf{MTM}^{-1}$.

Для разработки алгоритмов ЭЦП со скрытой группой также представляет интерес использование матриц порядка $p - 1$. Для оценки доли таких матриц, содержащихся в мультипликативной группе алгебры матриц 3×3, интерес представляет следующее утверждение.

Утверждение 3. Множество невырожденных диагональных матриц размерности 3×3, заданных над конечным полем $GF(p)$, образуют коммутативную группу порядка $(p - 1)^3$.

Доказательство. Умножение двух произвольных матриц $(a_{11}, 0, 0, 0, a_{22}, 0, 0, 0, a_{33})$ и $(b_{11}, 0, 0, 0, b_{22}, 0, 0, 0, b_{33})$, где $0 < a_{11}, a_{22}, a_{33}, b_{11}, b_{22}, b_{33} < p$, по правилам матричного умножения дает в качестве результата матрицу $(a_{11}b_{11}, 0, 0, 0, a_{22}b_{22}, 0, 0, 0, a_{33}b_{33})$, т.е. все рассматриваемые матрицы коммутативны между собой и имеет место следующее тождество:

$$(a,0,0,0,b,0,0,0,c)^{p-1} = (a^{p-1},0,0,0,b^{p-1},0,0,0,c^{p-1}) = (1, 0, 0, 0, 1, 0, 0, 0, 1). \quad (14)$$

Из формулы (14) следует, что все матрицы диагонального вида имеют порядок, равный делителю числа $p - 1$, включая само это число. Легко видеть, что число таких матриц (порядок группы, который они образуют) равно $(p - 1)^3$. Естественным базисом коммутативной группы таких матриц является $<\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3>$, где $\mathbf{B}_1 = (\alpha, 0, 0, 0, 1, 0, 0, 0, 1)$; $\mathbf{B}_2 = (1, 0, 0, 0, \beta, 0, 0, 0, 1)$; $\mathbf{B}_3 = (1, 0, 0, 0, 1, 0, 0, 0, \delta)$; α, β и δ – примитивные элементы по модулю p. Будем обозначать коммутативные группы, порождаемые базисом из трех матриц порядка $p - 1$ как Γ_3. Учитывая автоморфизм, задаваемый формулой (8), легко видеть, что наличие группы диагональных матриц, относящихся к типу Γ_3, означает существование большого числа изоморфных Γ_3-групп, содержащих матрицы произвольно вида.

В соответствии с утверждением 1 разрешимое матричное уравнение

$$\mathbf{A} = \mathbf{XBX}^{-1}, \quad (15)$$

записанное для нескалярной матрицы $\mathbf{B}$, входящей в Γ_3-группу диагональных матриц имеет число различных решений, равное числу матриц, коммутативных с диагональной матицей $\mathbf{B}$. Число последних равно числу различных решений матричного уравнения

$$\mathbf{ZB} = \mathbf{BZ}. \quad (16)$$

Рассматривая систему из девяти линейных уравнений с девятью неизвестными координатами вектора $\mathbf{Z}$, к которой сводится последнее векторное уравнение, легко установить, что ранг главного определителя этой системы линейных уравнений равен шести, а значит, она имеет p^3 различных решений. Каждое из решений задает некоторую матрицу, вырожденную или невырожденную.

Легко подсчитать число вырожденных диагональных матриц (коммутативных с матрицей $\mathbf{B}$), которое оказывается равным $3p^2 - 3p + 1$. Суммируя вырожденные и невырожденные диагональные матрицы, получаем все p^3 решений матричного уравнения (16). Таким образом, все невырожденные решения уравнений (16) входят в рассматриваемую Γ_3-группу диагональных матриц. Последнее означает, что матричное уравнение (15) имеет $(p - 1)^3$ различных решений. Если в уравнении (15) при фиксированном значении матрицы $\mathbf{B}$ переменная $\mathbf{X}$ пробегает значения всех невырожденных матриц в мультипликативной группе алгебры матриц 3×3, то получим число различных матриц A, равное

$$\eta_3 = \Omega_{3\times3}(p - 1)^3 = p^3(p^2 + p + 1)(p + 1). \quad (17)$$

В общем случае некоторые пары различных матриц могут принадлежать одной и той же Γ_3-группе, поэтому число различных Γ_3-групп, содержащихся в мультипликативной группе рассматриваемой алгебры матриц, меньше значения η_3. Вывод формулы для числа различных Γ_3-групп представляется интересной и важной самостоятельной задачей, однако

в настоящем исследовании достаточен вывод что это число достаточно велико.

Легко показать, что каждая из изоморфных Γ_3-групп разбивается на большое число различных коммутативных циклических подгрупп порядка $p-1$ (число таких подгрупп равно примерно p^2), пересекающихся в единичной матрице $\mathbf{E}$ и семи различных матрицах $\mathbf{W}$ порядка два. Матрицы $\mathbf{W}$ порядка два могут трактоваться как квадратные корни из единичной матрицы $\mathbf{E} = (1, 0, 0, 0, 1, 0, 0, 0, 1)$. Все Γ_3-группы попарно пересекаются в циклической группе скалярных матриц, содержащей матрицу $\mathbf{W} = -\mathbf{E}$. В заданной Γ_3-группе число уникальных (по всей алгебре матриц 3×3) матриц $\mathbf{W}$ равно всего лишь шести, однако число Γ_3-групп велико, порядка p^6, т.е. число уникальных матриц $\mathbf{W}$ достаточно велико для того, чтобы они могли быть эффективно использованы как элемент секретного ключа. Следует заметить, что в рассматриваемой алгебре матриц содержатся и другие уникальные корни из $\mathbf{E}$, например, содержащиеся в циклических группах, генерируемых матрицами порядка $p+1$. Если известна нескалярная матрица $\mathbf{V}$ порядка $p-1$, то некоторую уникальную матрицу $\mathbf{W}$ порядка два можно вычислить по следующей формуле:

$$\mathbf{W} = \mathbf{V}^{(p-1)/2}. \quad (18)$$

В алгоритме ЭЦП, описываемом в следующем разделе, используются случайные нескалярные матрицы порядка p^2-1 и случайные матрицы $\mathbf{W} \neq -\mathbf{E}$. Для генерации таких матриц могут быть использованы следующие вычислительно эффективные алгоритмы.

Алгоритм генерации нескалярной матрицы $\mathbf{V}$ *порядка* $p-1$:

1. Сгенерировать случайные натуральные числа $b < p$ и $c < p$ и случайный примитивный элемент α по модулю p.
2. Сформировать диагональную матрицу $\mathbf{M} = (\alpha, 0, 0, 0, b, 0, 0, 0, c)$. порядка $p-1$.
3. Сгенерировать случайную невырожденную матрицу $\mathbf{X}$ и вычислить матрицу $\mathbf{V}$: $\mathbf{V} = \mathbf{X}\mathbf{M}\mathbf{X}^{-1}$.

Алгоритм генерации случайной матрицы $\mathbf{W}$ *порядка 2*:

1. Сгенерировать случайную нескалярную матрицу $\mathbf{V}$ порядка $p-1$.
2. Вычислить матрицу $\mathbf{W} = \mathbf{V}^{(p-1)/2}$.

Алгоритм генерации нескалярной матрицы $\mathbf{G}$ *порядка* p^2-1:

1. Сгенерировать случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить значение $h = \Omega_{3\times3}(p^2-1)^{-1} = p^3(p-1)^2(p^2+p+1)$ и матрицу $\mathbf{X} = \mathbf{M}^h$.
3. Если $\mathbf{X} = \mathbf{E}$, то перейти к шагу 1.
4. Если для всех простых делителей δ числа p^2-1 выполняется неравенство $\mathbf{X}^{(p^2-1)/\delta} \neq \mathbf{E}$, то перейти к шагу 5, иначе перейти к шагу 1.
5. Взять матрицу $\mathbf{X}$ в качестве матрицы $\mathbf{G}$ порядка p^2-1.

Из последних трех алгоритмов существенно более высокую вычислительную сложность имеет последний алгоритм, поскольку в нем среднее число возвратов к шагу 1 составляет несколько десятков. Однако, для применения в процедуре формирования секретного и открытого ключа его производительность вполне достаточна.

3. Постквантовый алгебраический алгоритм на алгебре матриц 3×3

В разработанном алгоритме ЭЦП в качестве алгебраического носителя используется алгебра матриц 3×3, заданная над полем $GF(p)$ простого 80-битного порядка p, такого, что число $q = p^2+p+1$ является простым. Секретный ключ формируется путем генерации случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$, случайной матрицы $\mathbf{W}$, такой, что $\mathbf{W}^2 = \mathbf{E}$, и случайных невырожденных нескалярных и попарно некоммутативных матриц $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что матрицы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $q = p^2+p+1$ и p^2-1 соответственно (общий размер секретного ключа равен ≈710 байт). Формирование открытого ключа выполняется в соответствии со следующими формулами:

$$\mathbf{Y} = \mathbf{WGW}; \mathbf{Z} = \mathbf{KP}^z\mathbf{K}^{-1}; \mathbf{U} = \mathbf{BPB}^{-1}; \mathbf{T}_1 = \mathbf{WG}^x\mathbf{D}^{-1}; \quad (19)$$

$$\mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{P}^w\mathbf{K}^{-1}; \mathbf{T}_3 = \mathbf{KP}^y\mathbf{G}^w\mathbf{W}; \mathbf{T}_4 = \mathbf{F}^{-1}\mathbf{P}^x\mathbf{B}^{-1}. \quad (20)$$

Общий размер открытого ключа равен ≈630 байт. В процедурах генерации и верификации ЭЦП предполагается использование некоторой специфицированной коллизионно стойкой 480-битной хеш-функции Φ, которая является частью рассматриваемого алгоритма ЭЦП.

Алгоритм генерации ЭЦП.

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < q$ и $t < p+1$ и вычислить значение матрицы $\mathbf{R}$ по формуле: $\mathbf{R} = \mathbf{WG}^k\mathbf{P}^t\mathbf{B}^{-1}$.
2. Вычислить хеш-значение от документа M с присоединенной к нему матрицей $\mathbf{R}$: $e = e_1||e_2||e_3 = \Phi(M, \mathbf{R})$, где 480-битное хеш-значение e представлено в виде конкатенации трех 160-битных натуральных чисел e_1, e_2 и e_3.
3. Вычислить натуральное число b: $b = -(w + ze_2 + y) \bmod (p^2-1)$.
4. Вычислить натуральное число n: $n = (k - x - e_2e_3 - we_3 - xe_3 - e_1e_3)(e_3+1)^{-1} \bmod q$.
5. Вычислить подгоночный элемент ЭЦП в виде матрицы $\mathbf{S}$ по формуле: $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}$.

6. Вычислить вспомогательный подгоночный элемент подписи в виде числа σ: $\sigma = (t - b - x) \bmod (p^2 - 1)$.

Сгенерированная цифровая подпись представляет собой тройку значений $(e, \sigma, \mathbf{S})$ с общим размером ≈170 байт. Вычислительная сложность процедуры генерации ЭЦП главным образом определяется четырьмя операциями возведения в 160-битную степень в алгебре матриц (вычисление матриц $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$), что составляет ≈26000 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП.

Проверка подлинности 170-байтной подписи $(e, \sigma, \mathbf{S})$ к документу M осуществляется с использованием 630-байтного открытого ключа $(\mathbf{Y}, \mathbf{Z}, \mathbf{U}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4)$ по следующему алгоритму:

1. Вычислить матрицу $\mathbf{R}'$ по следующей формуле (проверочное уравнение):
$$\mathbf{R}' = (\mathbf{Y}^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}^{e_2}\mathbf{T}_3\mathbf{Y}^{e_2})^{e_3}\mathbf{T}_1\mathbf{S}\mathbf{T}_4\mathbf{U}^{\sigma}. \quad (21)$$
2. Вычислить значение хеш-функции Φ от документа M с присоединенной к нему матрицей $\mathbf{R}'$: $\varepsilon = \varepsilon_1||\varepsilon_2||\varepsilon_3 = \Phi(M, \mathbf{R}')$, где 480-битное хеш-значение представлено в виде конкатенации трех 160-битных чисел ε_1, ε_2 и ε_3.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$, $\varepsilon_2 = e_2$ и $\varepsilon_3 = e_3$, то ЭЦП принимается как подлинная, в противном случае она отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как пять операций возведения матриц в 160-битную степень, что составляет ≈33000 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (21) элементов открытого ключа, выраженных через элементы секретного ключа, указанным ниже образом.

Доказательство корректности алгоритма ЭЦП.

Подставляя в проверочное уравнение (21) элементы открытого ключа, выраженные через элементы секретного ключа по формулам (19) и (20), для корректно сгенерированной подписи получаем:

$$\mathbf{R}' = (\mathbf{Y}^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\,\mathbf{Z}^{e_2}\mathbf{T}\mathbf{Y}^{e_2})^{e_3}\mathbf{T}_1\mathbf{S}\mathbf{T}_4\mathbf{U}^{\sigma} =$$
$$= [(\mathbf{WGW})^{e_1}\mathbf{WG}^x\mathbf{D}^{-1}(\mathbf{DG}^n\mathbf{P}^b\mathbf{F})\mathbf{F}^{-1}\mathbf{P}^w\mathbf{K}^{-1} \times$$
$$\times (\mathbf{KP}^z\mathbf{K}^{-1})^{e_2}\mathbf{K}\,\mathbf{P}^y\mathbf{G}^w\mathbf{W}(\mathbf{WGW})^{e_2}]^{e_3}\mathbf{WG}^x\mathbf{D}^{-1} \times$$
$$\times (\mathbf{DG}^n\mathbf{P}^b\mathbf{F})\mathbf{F}^{-1}\mathbf{P}^x\,\mathbf{B}^{-1}(\mathbf{BPB}^{-1})^{\sigma} =$$
$$= (\mathbf{WG}^{e_1+x+n}\mathbf{P}^{b+w+ze_2+y}\mathbf{G}^{w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{b+x+\sigma}\mathbf{B}^{-1} =$$
$$= (\mathbf{WG}^{e_1+x+n}\mathbf{P}^{0}\mathbf{G}^{w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{b+x+(t-b-x)}\mathbf{B}^{-1} =$$
$$= (\mathbf{WG}^{e_1+x+n+w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{t}\mathbf{B}^{-1} =$$
$$= \mathbf{WG}^{e_1e_3+xe_3+ne_3+we_3+e_2e_3+x+n}\mathbf{P}^{t}\mathbf{B}^{-1} =$$
$$= \mathbf{WG}^{n(e_3+1)+e_1e_3+xe_3+we_3+e_2e_3+x}\mathbf{P}^{t}\mathbf{B}^{-1} = \mathbf{WG}^{k}\mathbf{P}^{t}\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем $\varepsilon_1||\varepsilon_2||\varepsilon_3 = \Phi(M, \mathbf{R}') = \Phi(M, \mathbf{R}) = e_1||e_2||e_3$, т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

4. Обсуждение

Представляет интерес реализация предложенного алгоритма с использованием в качестве секретной матрицы $\mathbf{G}$, имеющей порядок $p(p - 1)$. В такой версии алгоритма процедура верификации ЭЦП остается без изменения, а в процедуре генерации ЭЦП вычисление на шагах 3 и 6 будет выполняться по тем же формулам, но по модулю $p(p - 1)$ (вместо модуля $p^2 - 1$). Такое модифицирование алгоритма не влияет на его стойкость, однако несколько снижает вычислительную сложность процедуры формирования секретного ключа за счет возможности использования существенно более производительного алгоритма генерации матриц порядка $p(p - 1)$ по сравнению с алгоритмом генерации матриц порядка $p^2 - 1$.

Оценка стойкости разработанного алгоритма к атакам на основе известных подписей по способу, использованному в работах [13, 16], показала, что такие атаки связаны с решением системы матричных степенных уравнений, записанных по формуле формирования подгоночного элемента для десяти известных подписей. Это соответствует решению системы из 90 степенных скалярных уравнений в поле $GF(p)$.

Прямая атака на разработанный алгоритм связана с решением системы степенных матричных уравнений, связывающих элементы секретного ключа с элементами открытого ключа в соответствии с формулами (19) и (20). В такой системе матричных уравнений матрицы $\mathbf{G}^w$, $\mathbf{G}^x$, $\mathbf{P}^w$, $\mathbf{P}^x$, $\mathbf{P}^y$ и $\mathbf{P}^z$ рассматриваются как независимые неизвестные (в противном случае пришлось бы иметь дело с экспоненциальными матричными уравнениями), принадлежащие соответствующим скрытым группам. При этом матричные уравнения, выражающие условие коммутативности неизвестных, принадлежащих одной и той же скрытой группе, могут быть устранены при сведении решения системы матричных уравнений к соответствующей системе скалярных уравнений при наличии формул, выражающих все координаты векторов скрытой группы через координаты фиксированного представителя скрытой группы и три скалярных неизвестных.

Потенциально такие формулы могут быть выведены из рассмотрения декомпозиции алгебры матриц 3×3 на коммутативные подалгебры по аналогии с декомпозицией алгебры матриц 2×2 [15]. Вывод таких

Таблица 3.

Сравнение предложенного постквантового алгоритма ЭЦП с известными аналогами

Алгоритм и размер порядка поля *GF(p)*	Размер открытого ключа, байт	Размер подписи, байт	Сложность генерации подписи, умножений в *GF(p)*	Сложность верификации подписи, умножений в *GF(p)*	Уровень стойкости к прямой атаке
Предложенный, 80 бит	630	170	26000	33000	$\approx 2^{192}$
[16], 128 бит	512	144	9200	13800	$\approx 2^{100}$
[18] , 128 бит	387	97	12300	6100	$\approx 2^{100}$
[19] , 128 бит	256	113	12300	9220	$\approx 2^{80}$
[20], 128 бит	768	160	49200	13800	$\approx 2^{80}$

формул составляет самостоятельную задачу, однако такую потенциальную возможность следует учитывать при оценке стойкости к прямой атаке. С учетом такой возможности прямая атака оказывается связанной с решением системы из 63 степенных уравнений в поле $GF(p)$ 80-битного порядка p. При этом в систему входят 69 скалярных неизвестных. Оценка сложности решения такой системы в зависимости от числа степенных уравнений в системе, приводимая в работе [4], задает для разработанного алгоритма ЭЦП уровень стойкости $\approx 2^{192}$ к прямой атаке и $\approx 2^{256}$ к атаке на основе известных подписей. Заметим, что разработанный алгоритм ЭЦП с проверочным уравнением (21) может быть реализован на конечных некоммутативных ассоциативных алгебрах различных размерностей, например, заданных по методу [17].

Сравнение некоторых параметров разработанного алгебраического алгоритма ЭЦП с аналогами из статей [16, 18–20], использующими четырехмерные некоммутативные алгебры в качестве алгебраического носителя, приведено в табл. 3.

Выводы

Используя конечную алгебру матриц размерности 3×3, заданных над простым полем $GF(p)$, в качестве алгебраического носителя, разработан алгоритм ЭЦП с двумя скрытыми группами, стойкость которого основана на вычислительной трудности решения больших систем степенных уравнений. Алгоритм представляет интерес как потенциальный прототип для разработки практичного постквантового стандарта ЭЦП

Представляет интерес применение описанного построения схемы ЭЦП для реализации аналогичного алгоритма на алгебре матриц, заданных над конечным полем характеристики два. Важной задачей будущих исследований в затронутом направлении является исследование декомпозиции алгебры матриц 3×3 на коммутативные подалгебры. Также представляет интерес рассмотрение реализации аналога разработанного алгоритма с использованием в качестве алгебраического носителя алгебры матриц 5×5, заданных над конечным полем 32-битного порядка p.

Исследование выполнено частично за счет гранта Российского научного фонда № 24-41-04006, https://rscf.ru/project/24-41-04006/

Литература

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.
3. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092.
4. Ding J.,Petzoldt A.. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. Vol. 15. No. 4. P. 28–36.
5. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
6. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.

7. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
8. Moldovyan A.A. , Moldovyan N.A. Parameterized unified method for setting vector finite fields for multivariate cryptography // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2024. Т. 20. Вып. 4. С. 479–486. DOI: 10.21638/spbu10.2024.404.
9. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98). P. 56–65. DOI: 10.56415/basm.y2022.i1.p56.
10. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022, vol. 30, no. 2(48), pp. 287–298. DOI: 10.56415/qrs.v30.24.
11. Moldovyan A.A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1. P. 95–108. DOI: 10.56415/qrs.v32.08.
12. Молдовян А.А., Молдовян Д.Н., Костина А.А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.
13. 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.
14. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. DOI: 10.56415/qrs.v30.11.
15. Moldovyan N.A., Moldovyan A.A. Digital signature scheme on the 2x2 matrix algebra algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т., 17 Вып. 3. С. 254–261. DOI: 10.21638/11701/spbu10.2021.303.
16. Молдовян Н.А, Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
17. Dinh K.L., Nguyen L.G, Do T.B., Moldovyan A.A., Moldovyan D.N., Kostina A.A. Defining High-Dimensional Non-Commutative Algebras as Carriers for Post-Quantum Digital Signature Algorithms // Proceedings of the 1st International Conference On Cryptography and Information Security (VCRIS), Hanoi, Vietnam, 2024. P. 1–5. DOI: 10.1109/VCRIS63677.2024.10813386.
18. Duong M.T., Moldovyan D.N., Do B.V., Minh Hieu Nguyen M.H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740. ISSN 0920-5489.
19. Молдовян Д.Н., Молдовян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
20. 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.

A DIGITAL SIGNATURE ALGORITHM ON THE ALGEBRA OF 3×3 MATRICES, WHICH USES TWO HIDDEN GROUPS

Zakharov D. V.[7], Kostina A. A.[8], Morozova E. V.[9], Moldovyan D. N.[10]

Keywords: *finite non-commutative algebra; associative algebra; matrix algebra; computationally difficult problem; hidden group; digital signature; signature randomization; post-quantum cryptography.*

Purpose of work *is increasing the performance of algebraic digital signature algorithms based on the computational difficulty of solving large systems of power equations.*

Research methods: *application of the algebra of matrices of dimension 3×3 defined over a finite field GF(p) as an algebraic support. Selection of triangular matrices as the algebra elements of prime order p. Application of an automorphic mapping of a non-commutative finite algebra to generate the required-order matrices having a general form.*

Results of the study: *for the first time, the algebra of matrices of dimension 3×3 was used as an algebraic carrier of diital sinature algorithms, the security of which is based on the computational complexity of solving large systems of power equations. The randomization of the signature is provided by calculating it depending on two random elements selected from two hidden commutative groups, the elements of one of which are non-commutative with the elements of the other. Algorithms for calculating generators of hidden groups of orders p, $p^2 - 1$ and $p^2 + p + 1$ are proposed. For the first time, when calculating the elements of a public key from the elements of a secret key, an algebraic element of order two was used as a masking factor and the existence of a sufficiently large number of non-scalar matrices with order two was shown. An assessment of the security of the developed algorithm is given.*

7 Dmitriy V. Zakharov, Ph.D. (in Tech.), researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org0009-0004-5731-3611. E-mail: zakharov.dmitriy@gmail.com

8 Anna A. Kostina, researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

9 Elena V. Morozova, Ph.D. (in Tech.), associate professor of Department of Integrated Information Security, Admiral Makarov State University of Maritime and Inland Shipping. E-mail: lenmor@mail.ru

10 Dmitriy N. Moldovyan, Ph.D. (in Tech.), associate professor of St. Petersburg State Electrotechnical University «LETI», St. Petersburg, Russia. ORCID: https://orcid.org/0000-0001-5039-7198. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

Practical relevance: *the scientific and practical significance of the results of the article consists in increasing the performance of post-quantum algebraic signature algorithms exploiting computational complexity of solving large systems of power equations.*

References

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.
3. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092
4. Ding J.,Petzoldt A.. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. Vol. 15. No. 4. P. 28–36.
5. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
6. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.
7. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
8. Moldovyan A.A. , Moldovyan N.A. Parameterized unified method for setting vector finite fields for multivariate cryptography // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2024. T. 20. Vyp. 4. S. 479–486. DOI: 10.21638/spbu10.2024.404
9. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98). P. 56–65. DOI: 10.56415/basm.y2022.i1.p56.
10. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022, vol. 30, no. 2(48), pp. 287–298. DOI: 10.56415/qrs.v30.24.
11. Moldovyan A.A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1. P. 95–108. DOI: 10.56415/qrs.v32.08.
12. Moldovjan A.A., Moldovjan D.N., Kostina A.A. Algebraicheskie algoritmy JeCP s polnoj randomizaciej podpisi // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.
13. Moldovjan D.N., Kostina A.A. Sposob usilenija randomizacii podpisi v algoritmah JeCP na nekommutativnyh algebrah // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
14. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. DOI: 10.56415/qrs.v30.11.
15. Moldovyan N.A., Moldovyan A.A. Digital signature scheme on the 2x2 matrix algebra algebra // Vestnik Sankt_peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2021. T. 17 Vyp. 3. S. 254–261. DOI: 10.21638/11701/spbu10.2021.303
16. Moldovjan N.A, Petrenko A.S. Algebraicheskij algoritm JeCP s dvumja skrytymi gruppami // Voprosy kiberbezopasnosti. 2024. № 6(64). S. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
17. Dinh K.L., Nguyen L.G, Do T.B., Moldovyan A.A., Moldovyan D.N., Kostina A.A. Defining High-Dimensional Non-Commutative Algebras as Carriers for Post-Quantum Digital Signature Algorithms // Proceedings of the 1st International Conference On Cryptography and Information Security (VCRIS), Hanoi, Vietnam, 2024. P. 1–5, DOI: 10.1109/VCRIS63677.2024.10813386.
18. Duong M.T., Moldovyan D.N., Do B.V., Minh Hieu Nguyen M.H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740. ISSN 0920-5489.
19. Moldovjan D.N., Moldovjan A.A. Algebraicheskie algoritmy JeCP, osnovannye na trudnosti reshenija sistem uravnenij // Voprosy kiberbezopasnosti. 2022. № 2(48). S. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
20. 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.