АЛГЕБРАИЧЕСКИЙ АЛГОРИТМ ЭЦП С ДВУМЯ СКРЫТЫМИ ГРУППАМИ

Молдовян Н. А.[1], Петренко А. С.[2]

DOI: 10.21681/2311-3456-2024-6-98-107

Цель работы: *повышение производительности алгебраических алгоритмов ЭЦП с усиленной рандомизацией подписи.*

Метод исследования: *применение двух скрытых коммутативных групп для усиления рандомизации подписи в алгебраических алгоритмах ЭЦП на конечных некоммутативных ассоциативных алгебрах (КНАА). Известные результаты по изучению декомпозиции четырехмерных КНАА как конечных колец на множество коммутативных подколец используются для вычисления параметров алгоритма ЭЦП с двумя скрытыми коммутативными группами. Применение проверочного уравнения с многократным вхождением подгоночного элемента подписи, представляющего собой вектор S, вычисляемый по двум некоммутативным элементам из разных скрытых групп. Задание операции возведения в степень, вычисляемую как значение хеш-функции от S. В качестве алгебраического носителя алгоритма ЭЦП используются КНАА, заданные по прореженным таблицам умножения базисных векторов.*

Результаты исследования: *впервые механизм усиления рандомизации реализован в алгебраическом алгоритме ЭЦП без использования удвоения проверочного уравнения. Разработанный алгоритм ЭЦП отличается использованием двух скрытых групп для вычисления случайного вектора-фиксатора, по которому вычисляется рандомизирующий элемент генерируемой подписи. Последнее обеспечивает усиление рандомизации не только для значений подписи, но и для значений вектора фиксатора. Благодаря этому существенно повышается потенциально достижимый уровень стойкости. Достаточность выполнения проверки подлинности ЭЦП по одному проверочному уравнению обеспечивается использованием следующих двух приемов: 1) многократным вхождением подгоночного элемента подписи S в проверочное уравнение и 2) использованием значения хеш-функции, зависящего от вектора S, в качестве значения степени одной из операций экспоненциирования, выполняемой в ходе процедуры проверки подлинности подписи. Выполнен анализ стойкости к прямой атаке и к атаке на основе многих известных подписей.*

Научная и практическая значимость результатов статьи состоит в повышении производительности алгебраических алгоритмов ЭЦП с двумя скрытыми коммутативными группами, представляющими, благодаря малым размерам подписи и открытого ключа, интерес для разработки практичных постквантовых стандартов ЭЦП.

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

Введение

Разработка практичных постквантовых алгоритмов электронной цифровой подписи (ЭЦП) является одной из актуальных задач в области прикладной и криптографии [1, 2]. Постквантовые криптоалгоритмы должны быть основаны на вычислительно сложных задачах, которые отличны от задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), поскольку для решения ЗДЛ и ЗФ на квантовом вычислителе известны полиномиальные алгоритмы[3]. Разрабатываются постквантовые двухключевые криптосхемы на группах [3], алгебраических решетках [4], кодах [5], хеш-функциях [6], труднообратимых отображениях [7,8] и некоммутативных алгебрах [9,10].

Большое внимание со стороны криптографического сообщества уделяется разработке постквантовых алгоритмов с открытым ключом на нелинейных трудно обратимых отображениях с секретной лазейкой, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений в конечных полях [11,12]. Такой интерес связан с тем, что использование квантового компьютера для нахождения решений таких систем не является эффективным. Существенным недостатком алгоритмов указанного типа, включая алгоритмы ЭЦП, является чрезвычайно большой размер открытого ключа [13, 14]. При этом обеспечивается малый размер цифровой подписи. Для устранения данного недостатка недавно была предложена концепция задания трудно обратимого отображения как операции экспоненцирования в векторных конечных полях [15, 16]. Однако и в рамках данной концепции, позволяющей уменьшить размер открытого ключа

1 Молдовян Николай Андреевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: nmold@mail.ru

2 Петренко Алексей Сергеевич, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

3 Yan S. Y. Quantum Computational Number Theory. – Springer. 2015. – 252 p.

в десятки раз, его размер существенно превышает этот параметр для многих других известных постквантовых алгоритмов ЭЦП.

Новый подход к построению алгоритмов ЭЦП, стойкость которых базируется на вычислительной сложности решения больших систем степенных уравнений, предложен в работах [17–20] и позволяет обеспечить малые размеры подписи и открытого ключа. В этом подходе в качестве алгебраического носителя используются конечные некоммутативные ассоциативные алгебры (КНАА), а базовой операцией в процедурах генерации и верификации подписи является операция возведения в степень большого размера. При этом открытый ключ формируется как совокупность векторов, вычисляемых по некоторому набору элементов скрытой (секретной) коммутативной группы, содержащейся в КНАА. Фактически элементы открытого ключа представляют собой замаскированные элементы скрытой группы. Маскировка выполняется путем умножения слева и справа на секретные векторы.

Характерной особенностью алгебраических алгоритмов ЭЦП [17–20] является использование подгоночного элемента подписи в виде вектора $\mathbf{S}$, вычисляемого как замаскированный случайно выбираемый элемент скрытой группы и входящего в проверочное уравнение (уравнение верификации) в качестве множителя. Эта особенность обуславливает потенциальную возможность фальсификации подписи с использованием значения $\mathbf{S}$ в качестве подгоночного параметра атаки. Для устранения такой атаки используется уравнение верификации с двукратным или многократным вхождением множителя $\mathbf{S}$, при котором решение проверочного уравнения относительно неизвестного вектора $\mathbf{S}$ является вычислительно невыполнимым.

Однако в работах [21, 22] была показана неполнота рандомизации в алгебраических алгоритмах ЭЦП со скрытой группой, обусловливающая потенциальную возможность вычисления части секретного ключа по некоторой совокупности известных подлинных подписей. Это приводит к существенному снижению уровня стойкости. Для устранения этого недостатка в работах [21, 22] предложены способы усиления рандомизации подписи, которые потребовали использования удвоенного проверочного уравнения, что существенно увеличило вычислительную сложность процедур генерации и верификации ЭЦП, т.е. привело к значительному снижению производительности алгоритмов ЭЦП со скрытой группой.

Формализация цели исследования

Рандомизация подписи в алгебраических алгоритмах ЭЦП, представленных в работах [17–20], обеспечивается выбором случайного вектора $\mathbf{H}$ из скрытой коммутативной группы и вычислением подгоночного элемента подписи $\mathbf{S}$ по формуле

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

где $\mathbf{D}$ и $\mathbf{F}$ секретные маскирующие множители (элементы секретного ключа). С каждой подписью связано уникальное значение $\mathbf{H}$, однако, как замечено в [21], последнее выбирается из существенно ограниченного подмножества векторов, входящих в КНАА. Поскольку векторы $\mathbf{D}$ и $\mathbf{F}$ являются фиксированными, вектор $\mathbf{S}$ принимает очень малую долю возможных значений в КНАА. Коммутативное кольцо, включающее скрытую группу, может быть описано математическими формулами с числом скалярных переменных μ, существенно меньшей размерности m алгебры, используемой в качестве алгебраического носителя алгоритма ЭЦП. Значения указанных скалярных переменных являются случайными и неизвестными для каждой подписи, вычисленной владельцем открытого ключа по значениям подписываемого документа и его личного секретного ключа.

Таким образом, одна известная подпись позволяет записать m скалярных степенных уравнений, выражающих координаты вектора $\mathbf{S}$ через $2m$ фиксированных (для всех известных подписей) скалярных неизвестных (которыми являются координаты секретных векторов $\mathbf{D}$ и $\mathbf{F}$) и μ уникальных скалярных неизвестных. Для числа z известных подписей может быть составлена система, включающая mz степенных уравнений с $2m$ фиксированными неизвестными и μz уникальными скалярными неизвестными. Поскольку $\mu < m$, с увеличением значения число неизвестных (равное $2m + \mu z$) растет медленнее числа уравнений и при некотором z система будет иметь ограниченное число решений, которые могут быть найдены. Очевидно, что построенная таким образом система будет совместной для произвольного значения z. Ввиду того, что имеем дело со степенными уравнениями в общем случае будем иметь различные решения системы для произвольных значений z. При малых значениях z имеем очень большое число решений. Принимая в качестве критерия получения достаточно ограниченного числа решений равенство числа уравнений и неизвестных в системе, можно оценить требуемое число z_0 известных подписей и вычислительную сложность нахождения элементов $\mathbf{D}$ и $\mathbf{F}$ секретного ключа.

В соответствии с этим критерием имеем $mz = 2m + \mu z$, откуда получаем $z_0 = 2m / (m - \mu)$. Для четырехмерных КНАА известно их разбиение (как конечного некоммутативного кольца) на множество конечных коммутативных подколец [23, 24], из которого имеем конкретные значения $\mu = 2$ и $z_0 = 4$. Для этого случая вычислительная сложность

атаки на основе z_0 известных подписей определяется сложностью решения системы из $4z_0 = 16$ степенных уравнений в конечном поле, над которым задана КНАА, используемая в качестве алгебраического носителя. Используя оценки [25] (см. табл. 1 в [25]) сложности решения систем степенных уравнений, получаем уровень стойкости к данной атаке менее 2^{80}, что существенно меньше стойкости алгоритмов [17–20] к прямой атаке при их реализации на четырехмерных КНАА. Хотя атака на основе известных подписей не приводит к нахождению всех элементов секретного ключа, следует принять во внимание существенное снижение стойкости за счет того, что секретные векторы D и F становятся известными.

В работах [21, 22] также показано, что для оценивания полноты рандомизации следует принимать во внимание и значение случайного вектора-фиксатора $\mathbf{R}$, вычисляемого в процессе генерации подписи по формуле

$$\mathbf{R} = \mathbf{A}\mathbf{H}'\mathbf{B}, \quad (2)$$

где $\mathbf{H}'$ – случайный вектор, принадлежащий скрытой группе, $\mathbf{A}$ и $\mathbf{B}$ – секретные векторы. Действительно, значение $\mathbf{R}$ вычисляется в ходе процедуры верификации ЭЦП, поэтому формула (2) дает дополнительные уравнения, связанные с известной подписью, а также дополнительные фиксированные (координаты векторов $\mathbf{A}$ и $\mathbf{B}$) и уникальные (связанные с вектором $\mathbf{H}'$) скалярные неизвестные. В зависимости от конкретного алгоритма ЭЦП со скрытой группой для построения системы степенных уравнений, решаемой в рамках атаки на основе известных подписей, для минимизации сложности атаки может быть использована формула (1) и/или (2).

В работах [21, 22] предложены способы усиления рандомизации, требующие использования приема удвоения проверочного уравнения (по аналогии с реализацией алгоритмов [26] со скрытой группой, основанных на вычислительной сложности скрытой задачи дискретного логарифмирования), за счет чего существенно снижается производительность процедур генерации и верификации ЭЦП. В способах [21,22] векторы $\mathbf{R}$ и $\mathbf{S}$ вычисляются по формулам с использованием случайного вектора $\mathbf{V}$, что устраняет возможность использования проверочного уравнения с многократным вхождением вектора $\mathbf{S}$.

В данной работе решается задача разработки способа усиления рандомизации подписи, сохраняющего возможность использования одного проверочного уравнения с многократным вхождением вектора $\mathbf{S}$. Благодаря последнему достигается повышение производительности алгебраических алгоритмов ЭЦП с усиленной рандомизацией подписи. В основу способа положена идея использования двух скрытых коммутативных групп в четырехмерной КНАА (с глобальной двухсторонней единицей), заданной над конечным простым полем $GF(p)$, таких, что элементы одной из них не коммутируют с элементами другой, и вычисления подгоночного элемента подписи $\mathbf{S}$ по формуле

$$\mathbf{S} = \mathbf{D}\mathbf{P}^b\mathbf{H}^n\mathbf{F}, \quad (3)$$

а вектора-фиксатора $\mathbf{R}$ – по формуле

$$\mathbf{R} = \mathbf{A}\mathbf{H}^k\mathbf{P}^t\mathbf{B}, \quad (4)$$

где $\mathbf{P}$ – генератор первой скрытой (циклической) группы порядка $p^2 - 1$; $\mathbf{H}$ – генератор второй скрытой (циклической) группы простого порядка q, содержащей единственный скалярный вектор в виде двухсторонней глобальной единицы $\mathbf{E}$, используемой КНАА; $b,t < p^2 - 1$ и $n,k < q$ – случайные натуральные числа. Использование КНАА размерности $m = 4$ связано с тем, что информация о разбиении КНАА как конечного кольца на коммутативные подкольца имеет существенное значение для обоснования выбора параметров алгоритма ЭЦП, реализующего разработанный способ усиления рандомизации, и обоснования достаточности достигаемого усиления рандомизации подписи.

Вычисление векторов $\mathbf{S}$ и $\mathbf{R}$ по формулам (2) и (3) обеспечивает высокий уровень стойкости к атакам на основе известных подписей благодаря следующим утверждениям:

1) порядок поля $GF(p)$ выбирается равным $p = 2q + 1$, где q – простое число, за счет чего как множество векторов $\mathbf{P}^i\mathbf{H}^j$ (обозначим его как $\{\mathbf{P}|\mathbf{H}\}$), так и множество векторов $\mathbf{H}^j\mathbf{P}^i$ (обозначим его как $\{\mathbf{H}|\mathbf{P}\}$) при всевозможных степенях i и j включает $\approx p^3$ различных значений КНАА, используемой в качестве алгебраического носителя алгоритма ЭЦП;
2) каждое из множеств $\{\mathbf{P}|\mathbf{H}\}$ и $\{\mathbf{H}|\mathbf{P}\}$ вычислительно невозможно описать формулой с тремя скалярными переменными, из-за чего в рамках атаки на основе известных подписей атакующий вынужден рассматривать векторы $\mathbf{P}^b\mathbf{H}^n$ и $\mathbf{H}^k\mathbf{P}^t$, фигурирующие в формулах (3) и (4), как псевдослучайные векторы, каждый из которых вносит четыре уникальных скалярных неизвестных.

1. Свойства используемого алгебраического носителя

Конечная алгебра размерности m представляет собой m-мерное векторное пространство, заданное над конечным полем, с дополнительно определенной операцией векторного умножения, обладающей свойствами замкнутости и дистрибутивности слева и справа относительно операции сложения векторов. Вектор $\mathbf{V} = (v_0, v_1, v_2, v_3)$ можно представить как сумму

однокомпонентных векторов $\mathbf{V} = v_0e_0 + v_1e_1 + v_2e_2 + +v_3e_3$. Операция умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$, где $\mathbf{e}_i$ – базисные векторы, может быть определена по следующей формуле:

$$\mathbf{AB} = \sum_{ji=0}^{m-1}\sum_{j=0}^{m-1} a_ib_j(\mathbf{e}_i\mathbf{e}_j), \quad (5)$$

где каждое из всевозможных произведений пар базисных векторов заменяется на однокомпонентный вектор по правилу, задаваемому некоторой таблицей умножения базисных векторов (ТУБВ). Для построения алгоритмов ЭЦП с операциями экспоненциирования в степень большого размера требуется использовать алгебры с ассоциативным умножением (это свойство позволяет применить способ быстрого возведения в степень, основанный на процессе последовательного возведения в квадрат).

В данной статье в качестве алгебраического носителя разрабатываемого алгоритма используется четырехмерная КНАА с глобальной двухсторонней единицей $\mathbf{E} = (1, 1, 0, 0)$, заданная над простым конечным полем $GF(p)$ с характеристикой в виде простого 128-битного числа вида $p = 2q + 1$, где q есть простое 127-битное число. Операция умножения четырехмерных векторов задается по прореженной ТУБВ (см. табл. 1), а именно по ТУБВ, в половине ячеек которой присутствует структурная константа с нулевым значением. Выбор КНАА размерности $m = 4$, заданной по прореженной табл. 1 связано с тем, что для выполнения одной операции векторного умножения требуется выполнить всего восемь операций умножения в поле $GF(p)$.

Таблица 1.

Прореженная ТУБВ для задания умножения четырехмерных векторов ($\lambda \neq 0$) [9]

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

Декомпозиция этой КНАА как конечного некоммутативного кольца на коммутативные подкольца детально изучена в работе [9] и описывается следующим образом:

1. Множество четырехмерных векторов, содержащихся в рассматриваемой КНАА, разбивается на $\eta = p^2 + p + 1$ коммутативных подколец порядка p^2.
2. Последние пересекаются строго в множестве векторов вида $\mathbf{L} = \alpha\mathbf{E}$, где $\mathbf{E}$ – единичный вектор (глобальная двухсторонняя единица) и $\alpha \in GF(p)$.
3. Имеются только три типа коммутативных подколец порядка p^2:
   3.1. Подкольца (их число $\approx p^2/2$), изоморфные полю $GF(p^2)$ и включающие циклическую мультипликативную группу порядка $\Omega_1 = p^2 - 1$ (группу типа Γ_1).
   3.2. Подкольца (их число $\approx p^2/2$), мультипликативная группа которых (группа типа Γ_2) порождается базисом, включающим два вектора одинакового порядка $p - 1$. Порядок групп типа Γ_2 равен $\Omega_2 = (p_2 - 1)^2$.
   3.3. Подкольца (их число равно $p + 1$), мультипликативная группа которых (группа типа Γ_3) имеет циклическое строение и порядок $\Omega_3 = p(p - 1)$.
4. Произвольный фиксированный представитель $\mathbf{C} = (c_0, c_1, c_2, c_3)$ некоторого подкольца, который отличен от скалярного вектора, позволяет описать все элементы подкольца $\mathbf{V}$ с помощью формулы, включающей две скалярные переменные $d,h \in GF(p)$ и координаты представителя $\mathbf{C}$. Для подколец с мультипликативной группой типа Γ_1 и Γ_2 указанная формула имеет вид (см. формулу (8) в работе [9]):

$$\mathbf{V} = (v_0,v_1,v_2,v_3) = (d,\ d + h(c_1 - c_0)c_2^{-1},\ h,\ hc_3c_2), \quad (6)$$

Векторы $\mathbf{A}$ и $\mathbf{B}$ называются коммутативными, если $\mathbf{AB} = \mathbf{BA}$, и некоммутативными, если $\mathbf{AB} \neq \mathbf{BA}$. Докажем следующее утверждение, обосновывающее выбор векторов $\mathbf{P}$ и $\mathbf{H}$, входящих в формулы (3) и (4) как генераторы двух скрытых коммутативных групп.

Утверждение 1. Пусть в четырехмерной КНАА умножение задано по табл. 1 над полем $GF(p)$ при простом $p = 2q + 1$, где q есть простое число, и вектор $\mathbf{H}$ является генератором циклической подгруппы группы типа Γ_2, имеет порядок равный q и отличен от скалярного вектора. Тогда векторы $\mathbf{H}^x$ при $0 < x < q$ являются нескалярными векторами.

Доказательство. Предположение, что при некотором x, таком, что $0 < x < q$, $\mathbf{H}^x$ равно скалярному вектору $\mathbf{L}$, приводит к противоречию: существует натуральное число $x' = x^{-1} \bmod q$, для которого имеем $\{\mathbf{H}^x = \mathbf{L}\} \Rightarrow \{\mathbf{H} = \mathbf{L}^{x'} = \mathbf{L}'\}$, где $\mathbf{L}'$ скалярный вектор.

Утверждение 2. Пусть вектор $\mathbf{P}$ является генератором циклической группы типа Γ_1, а вектор $\mathbf{H}$ является генератором циклической подгруппы группы типа Γ_2, имеет порядок равный q, и отличен от скалярного вектора. Тогда векторы $\mathbf{P}$ и $\mathbf{H}$ некоммутативны и каждое из произведений $\mathbf{P}^i\mathbf{H}^j$ и $\mathbf{H}^j\mathbf{P}^i$ при $i = 1, 2, \ldots p^2 - 1$ и $j = 1, 2, \ldots q$ принимает $(p^2 - 1)q$ различных значений в КНАА, в которой умножение задано по табл. 1 над полем $GF(p)$ при простом $p = 2q + 1$, где q есть простое число.

Доказательство. Скалярный вектор имеет порядок, равный делителю числа $p - 1$, поэтому не может быть генератором циклической группы порядка $p^2 - 1$, т. е. P является нескалярным вектором. Поэтому векторы $\mathbf{P}$ и $\mathbf{H}$ некоммутативны как несклярные векторы, принадлежащие разным коммутативным подкольцам порядка p^2. Пусть при некоторых целых неотрицательных числах $i,k < p^2 - 1$ и $j,t < q$ имеем $\mathbf{P}^i\mathbf{H}^j = \mathbf{P}^k\mathbf{H}^t$. Тогда $\{\mathbf{P}^i\mathbf{H}^j = \mathbf{P}^k\mathbf{H}^t\} \Rightarrow \{\mathbf{P}^{i-k} = \mathbf{H}^{j-t}\}$. Поскольку $\mathbf{H}$ является несклярным вектором, то все его степени $\mathbf{H}^x$ при $0 < x < q$ являются нескалярными векторами (см. утверждение 1), а пересечение различных подколец рассматриваемой КНАА имеет место только в множестве скалярных векторов, равенство $\mathbf{P}^{i-k} = \mathbf{H}^{j-t}$ возможно только в случае $\mathbf{H}^{j-t} = \mathbf{E}$, из чего следует $\mathbf{P}^{i-k} = \mathbf{E}$. Из последних двух равенств имеем $\{j \equiv t \bmod q\} \Rightarrow \{j = t\}$ и $\{i \equiv k \bmod (p^2 - 1)\} \Rightarrow$ $\Rightarrow \{i = k\}$. Таким образом, каждая уникальная пара значений (i, j) задает уникальный вектор $\mathbf{P}^i\mathbf{H}^j$, т. е. число последних равно $(p^2 - 1)q$. Аналогично доказывается, что вектор $\mathbf{H}^j\mathbf{P}^i$ также принимает $(p^2 - 1)q$ разных значений.

2. Оценка стойкости к атакам на основе известных подписей

Формулы (3) и (4) описывают разработанный способ рандомизации подписи и определяют стойкость реализующих его конкретных алгебраических алгоритмов ЭЦП к атаке на основе известных подписей. Дадим общую оценку достигаемого уровня стойкости к указанной атаке в случае использования четырехмерных КНАА в качестве алгебраического носителя. Следует рассмотреть случаи использования формул (3) и/или (4) для составления системы уравнений, из которой вычисляются элементы секретного ключа.

Случай использования формулы (3). При наличии z известных подписей с подгоночными элементами $\mathbf{S}_i = \mathbf{D}\mathbf{P}_i\mathbf{H}_i\mathbf{F}$ (где $i = 1,2,\ldots z$; $\mathbf{P}_i$ и $\mathbf{H}_i$ – случайные некоммутативные векторы, выбираемые из двух разных скрытых групп) имеем систему из $4z$ скалярных степенных уравнений в поле $GF(p)$, составленных для координат векторов $\mathbf{S}_i$. Неизвестные секретные векторы $\mathbf{D}$ и $\mathbf{F}$ задают 8 фиксированных скалярных неизвестных (которыми являются координаты $\mathbf{D}$ и $\mathbf{F}$). Сделаем сильное предположение в пользу атакующего, состоящее в том, что он нашел способ описания множества векторов $\{\mathbf{P}|\mathbf{H}\}$ мощности $\approx p^3$ по фиксированным координатам некоторого представителя $\mathbf{C}$ этого множествами и тройку скалярных значений $t,v,u \in GF(p)$. Поскольку скрытые группы являются секретными, то координаты вектора $\mathbf{C}$ являются неизвестными, т. е. имеем еще четыре фиксированных неизвестных. При этом каждое уравнение в системе вносит $\mu = 3$ уникальных скалярных неизвестных. Таким образом, имеем 12 фиксированных неизвестных и $3z$ уникальных. По критерию равенства числа неизвестных и числа уравнений составляем выражение

$$4z = 12 + 3z, \qquad (7)$$

из которого получаем нужное для выполнения атаки число известных подписей $z_0 = 12$. Это значение z_0 соответствует 48 степенным уравнениям, входящим в решаемую в ходе атаки систему, и уровню стойкости к данной атаке $>2^{128}$ (см. табл. 1 в [25]).

Сделанное в пользу атакующего допущение является очень сильным. На самом деле описание выбора случайного вектора из множества $\{\mathbf{P}|\mathbf{H}\}$ через случайные три скалярные неизвестные t, v и u, видимо, является вычислительно нереализуемым, поскольку в общем случае произведение $\mathbf{P}^b\mathbf{H}^n$ со случайными степенями b и n в общем случае генерируют векторы, принадлежащие разным подкольцам порядка p^2, что потребует рассмотрения четырех уникальных скалярных неизвестных, связанных с каждой подписью. В этом случае число неизвестных в решаемой системе будет превосходить число уравнений, т.е., если будет возможным, приемлемо ограниченное число решений может быть получено для числа известных подписей $z_0 >> 12$. Последнее приводит к оценке уровня стойкости $> 2^{256}$.

Случай использования формулы (4). Полностью аналогичен случаю составления решаемой системы степенных уравнений по формуле (3), включая приведенные значения уровня стойкости.

Случай использования формул (3) *и* (4). С известными подписями связаны векторы $\mathbf{S}_i = \mathbf{D}\mathbf{P}_i\mathbf{H}_i\mathbf{F}$ и вычисляемые по проверочному уравнению векторы $\mathbf{R}_i = \mathbf{A}\mathbf{H}'_i\mathbf{P}'_i\mathbf{B}$ (где $i = 1,2,\ldots z$; $\mathbf{P}_i\mathbf{H}_i$ – случайные векторы, выбираемые множества $\{\mathbf{P}|\mathbf{H}\}$; $\mathbf{H}'_i\mathbf{P}'_i$ – случайные векторы, выбираемые множества $\{\mathbf{H}|\mathbf{P}\}$), по которым составляется система из $8z$ скалярных степенных уравнений, составленных для координат векторов $\mathbf{S}_i$ и $\mathbf{R}_i$. Неизвестные секретные векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$ и $\mathbf{F}$ задают 16 фиксированных неизвестных (координаты этих векторов). Расширяя указанное выше предположение в пользу атакующего на выбор случайного вектора из множества $\{\mathbf{H}|\mathbf{P}\}$ мощности $\approx p^3$ по фиксированным координатам некоторого представителя $\mathbf{C}'$ этого множества и тройку скалярных значений t', v', $u' \in GF(p)$, получаем восемь дополнительных фиксированных неизвестных (координаты векторов $\mathbf{C}$ и $\mathbf{C}'$) и $\mu = 6$ уникальных скалярных неизвестных. Таким образом, имеем 24 фиксированных неизвестных и $6z$ уникальных. В соответствии с критерием равенства числа неизвестных и числа уравнений имеем соотношение $8z = 24 + 6z$, из которого вычисляем $z_0 = 12$, что прямолинейно соответствует 96 степенным уравнениям, входящим в систему, и уровню стойкости к рассматриваемой атаке $>2^{256}$ (см. табл. 1 в [25]).

Однако, легко заметить, что «по построению» полученная система распадается на две независимые системы по 48 уравнений в каждой, причем последние полностью идентичны системам, возникающим в случаях проведения атаки с использованием только формулы (3) или (4).

Таким образом, рассмотренные варианты атаки на основе известных подписей имеют вычислительную сложность не менее 2^{128} в модели атаки с сильным допущением в пользу атакующего. В случае атаки без такого допущения ожидаемый уровень стойкости к данной атаке составляет не менее 2^{256}.

3. Постквантовый алгоритм ЭЦП

При генерации элементов секретного ключа в разработанном алгебраическом алгоритме ЭЦП используется следующее условие обратимости четырехмерного вектора $\mathbf{V} = (v_0, v_1, v_2, v_3)$ как элемента используемой в качестве алгебраического носителя КНАА, задаваемое используемой ТУБВ [9]:

$$v_0, v_1 \neq \lambda v_2 v_3 \qquad (8)$$

Формирование секретного ключа выполняется как генерация случайных натуральных чисел $x < p - 1$, $u < p - 1$ и $w < p - 1$ и случайных обратимых векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{H}$ и $\mathbf{P}$, которые попарно некоммутативны (с учетом строения используемой КНАА вероятность того, что пять случайных векторов будут обратимы и попарно некоммутативны, близка к единице). При этом вектор $\mathbf{H}$ является нескалярным, имеет порядок, равный 127-битному простому числу q, и принадлежит подкольцу, содержащему мультипликативную группу типа Γ_2, а вектор $\mathbf{P}$ имеет порядок $p^2 - 1$. Легко показать, что случайный вектор $\mathbf{H}$ (вектор $\mathbf{P}$) удовлетворяет указанным условиям с вероятностью ≈0,25 (≈0,1), а размер секретного ключа составляет ≈370 байт порядка.

Открытый ключ вычисляется по секретному в виде набора из восьми векторов $\mathbf{Y}$, $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{T}$, $\mathbf{V}$, $\mathbf{X}$, $\mathbf{K}$ и $\mathbf{U}$ (с общим размером 512 байт) по следующим формулам:

$$\mathbf{Y} = \mathbf{AHA}^{-1};\ \mathbf{N} = \mathbf{AH}^{u}\mathbf{P}^{wx}\mathbf{D}^{-1};$$
$$\mathbf{Z} = \mathbf{DPD}^{-1};\ \mathbf{T} = \mathbf{F}^{-1}\mathbf{H}^{x}\mathbf{A}^{-1}; \qquad (9)$$

$$\mathbf{V} = \mathbf{AH}^{w}\mathbf{P}^{x}\mathbf{D};\ \mathbf{X} = \mathbf{F}^{-1}\mathbf{H}^{u}\mathbf{F};\ \mathbf{K} = \mathbf{FH}^{x}\mathbf{P}^{u}\mathbf{B};\ \mathbf{U} = \mathbf{B}^{-1}\mathbf{PB}. \qquad (10)$$

Предполагается, что при генерации и верификации подписи используется некоторая коллизионно стойкая 256-битная хеш-функция Φ, которая является частью рассматриваемой постквантовой схемы ЭЦП.

Алгоритм генерации ЭЦП.

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < q$ и $t < p^2 - 1$ и вычислить значение вектора-фиксатора $\mathbf{R}$ по формуле (4): $\mathbf{R} = \mathbf{AH}^{k}\mathbf{P}^{t}\mathbf{B}$.
2. Вычислить хеш-значение от документа M с присоединенными к нему рандомизирующим вектором $\mathbf{R}$: $e = e_1 || e_2 = \Phi(M, \mathbf{R})$, где 256-битное хеш-значение e представлено в виде конкатенации двух 128-битных натуральных чисел e^1 и e^2.
3. Вычислить натуральную степень b: $b = -(wx + e) \bmod (p^2 - 1)$.
4. Вычислить натуральную степень n: $n = -(ue_2 + x) \bmod q$.
5. По формуле (3) вычислить вектор $\mathbf{S}$ (подгоночный элемент генерируемой подписи): $\mathbf{S} = \mathbf{DP}^{b}\mathbf{H}^{n}\mathbf{F}$.
6. Вычислить вспомогательный рандомизирующий элемент ЭЦП ρ по формуле $\rho = \Phi(\mathbf{S})$.
7. Вычислить первый вспомогательный подгоночный элемент ЭЦП в виде натурального 127-битного числа s по формуле $s = e_1^{-1}k - u - n - x - e_1^{-1}w \bmod q$.
8. Вычислить второй вспомогательный подгоночный элемент ЭЦП в виде натурального 256-битного числа σ по формуле $\sigma = t - x - \rho - b - u \bmod (p^2 - 1)$.

Сгенерированная ЭП к документу M представляет собой четверку значений

$(e, s, \sigma, \mathbf{S})$ с общим размером ≈144 байт. Вычислительную сложность процедуры вычисления ЭЦП можно оценить как две операции возведения четырехмерных векторов в 256-битную степень ($\mathbf{P}^t$ и $\mathbf{P}^b$) и две операции возведения в 128-битную степень ($\mathbf{H}^k$ и $\mathbf{H}^n$), т. е. как ≈9200 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП.

Проверка подлинности подписи $(e, s, \sigma, \mathbf{S})$ к документу M осуществляется с использованием 512-байтного открытого ключа $(\mathbf{Y}, \mathbf{N}, \mathbf{Z}, \mathbf{T}, \mathbf{V}, \mathbf{X}, \mathbf{K}, \mathbf{U})$ по следующему алгоритму:

1. Вычислить 256-битное натуральное число ρ:$\rho = \Phi(\mathbf{S})$.
2. Вычислить вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = (\mathbf{Y}^{s}\mathbf{NZ}^{e}\mathbf{ST})^{e_1}\mathbf{VZ}^{\rho}\mathbf{SX}^{e_2}\mathbf{KU}^{\sigma}. \qquad (11)$$

3. Вычислить хеш-функцию от документа M с присоединенным к нему вектором $\mathbf{R}'$: $\varepsilon_1 || \varepsilon_2 = \Phi(M, \mathbf{R}')$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.
4. Если одновременно выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то подпись принимается как подлинная, иначе она отвергается как ложная.

Вычислительную сложность алгоритма верификации подписи можно оценить как три операции возведения четырехмерных векторов в 256-битную степень ($\mathbf{Z}^{e}$, $\mathbf{Z}^{\rho}$ и $\mathbf{U}^{\sigma}$) и три операции возведения четырехмерных векторов в 128-битную степень ($\mathbf{Y}^{s}$, $(\mathbf{Y}^{s}\mathbf{NZ}^{e}\mathbf{ST})^{e_1}$ и $\mathbf{X}^{e_2}$), для чего надо осуществить

≈13800 операций умножения в поле $GF(p)$. Подставляя в проверочное уравнение (11) элементы открытого ключа, выраженные через элементы секретного ключа, легко доказать корректность работы предложенного алгоритма ЭЦП.

Доказательство корректности схемы ЭЦП.

Подставляя в проверочное уравнение (11) элементы открытого ключа, выраженные через элементы секретного ключа по формулам (9) и (10), для корректно сгенерированной подписи получаем:

$$\mathbf{R}' = \left[\left(\mathbf{AHA}^{-1}\right)^{y}\left(\mathbf{AH}^{u}\mathbf{P}^{wx}\mathbf{D}^{-1}\right)^{x}\left(\mathbf{DPD}^{-1}\right)^{w}\left(\mathbf{DP}^{b}\mathbf{H}^{n}\mathbf{F}^{-1}\right)^{e}\left(\mathbf{FH}^{x}\mathbf{A}^{-1}\right)^{s}\right]^{e_1}\mathbf{AH}^{w}\mathbf{P}^{x}\mathbf{D}^{-1}\left(\mathbf{DPD}^{-1}\right)^{\rho}\times$$
$$\times\left(\mathbf{DP}^{b}\mathbf{H}^{n}\mathbf{F}^{-1}\right)\left(\mathbf{F}^{-1}\mathbf{H}^{x}\mathbf{P}^{u}\mathbf{B}\right)\left(\mathbf{B}^{-1}\mathbf{PB}\right)^{\sigma} =$$
$$= \left(\mathbf{AH}^{s+u}\mathbf{P}^{wx+e+b}\mathbf{H}^{n+x}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AH}^{w}\mathbf{P}^{x+\rho+b}\mathbf{H}^{n+we_2+x}\mathbf{P}^{u+\sigma}\mathbf{B} =$$
$$= \left(\mathbf{AH}^{s+u}\mathbf{P}^{0}\mathbf{H}^{n+x}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AH}^{w}\mathbf{P}^{x+\rho+b}\mathbf{H}^{0}\mathbf{P}^{u+\sigma}\mathbf{B} = \left(\mathbf{AH}^{s+u+n+x}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AH}^{w}\mathbf{P}^{x+\rho+b+u+\sigma}\mathbf{B} =$$
$$= \mathbf{AH}^{(s+u+n+x)e_1+w}\mathbf{P}^{x+\rho+b+we_2+t-x-\rho-b-we_2}\mathbf{B} = \mathbf{AH}^{\left(e_1^{-1}k-u-n-x-se_1^{-1}w+u+n+x\right)e_1^{-1}+w}\mathbf{P}'\mathbf{B} =$$
$$= \mathbf{AH}^{k}\mathbf{P}'\mathbf{B} = \mathbf{R}.$$

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

4. Обсуждение

В основе стойкости разработанного алгоритма ЭЦП является вычислительная сложность нахождения решений большой системы степенных уравнений, определяемых формулами (9) и (10) для вычисления элементов открытого ключа по элементам секретного ключа (являющихся неизвестными). Соответствующую систему векторных уравнений можно представить в виде следующего набора уравнений второй, третьей и четвертой степеней, решаемых совместно:

$$\mathbf{YA} = \mathbf{AH};\ \mathbf{N} = \mathbf{AH}^{u}\mathbf{P}^{wx}\mathbf{D}^{-1};\ \mathbf{ZD} = \mathbf{DP};\ \mathbf{FTA} = \mathbf{H}^{x}; \quad (12)$$

$$\mathbf{V} = \mathbf{AH}^{w}\mathbf{P}^{x}\mathbf{D};\ \mathbf{FX} = \mathbf{H}^{u}\mathbf{F};\ \mathbf{K} = \mathbf{FH}^{x}\mathbf{P}^{u}\mathbf{B};\ \mathbf{BU} = \mathbf{PB}. \quad (13)$$

При решении такой системы векторных степенных уравнений следует определиться с неизвестными 128-битными значениями x, u и w. Если считать их неизвестными, то наша система уже будет системой экспоненциальных уравнений, сложность решения которой представляется существенно большей, чем сложность системы степенных векторных уравнений, в которых векторы $\mathbf{H}_u = \mathbf{H}^u$, $\mathbf{H}_x = \mathbf{H}^x$ и $\mathbf{H}_w = \mathbf{H}^w$ рассматриваются как неизвестные значения, коммутативные с неизвестной $\mathbf{H}$, а векторы $\mathbf{P}_{wx} = \mathbf{P}^{wx}$, $\mathbf{P}_x = \mathbf{P}^x$ и $\mathbf{P}_u = \mathbf{P}^u$ – как неизвестные значения, коммутативные с неизвестной $\mathbf{P}$. Учет условия коммутативности приводит к добавлению в систему следующих 6 уравнений, описывающих коммутативность неизвестных векторов, выбираемых из одной и той же скрытой коммутативной группы (уравнения проверки коммутативности):

$$\mathbf{HH}_u = \mathbf{H}_u\mathbf{H};\ \mathbf{HH}_x = \mathbf{H}_x\mathbf{H};\ \mathbf{HH}_w = \mathbf{H}_w\mathbf{H}; \quad (14)$$

$$\mathbf{PP}_{wx} = \mathbf{P}_{wx}\mathbf{P};\ \mathbf{PP}_x = \mathbf{P}_x\mathbf{P};\ \mathbf{PP}_u = \mathbf{P}_u\mathbf{P}. \quad (15)$$

С учетом возможности представления каждого из неизвестных векторов $\mathbf{H}_u$, $\mathbf{H}_x$ и $\mathbf{H}_w$ через координаты вектора $\mathbf{H}$ и пару скалярных неизвестных (d_u, h_u), (d_x, h_x) и (d_w, h_w) соответственно, а неизвестных $\mathbf{P}_{wx}$, $\mathbf{P}_x$ и $\mathbf{P}_u$ через координаты вектора $\mathbf{P}$ и пару скалярных неизвестных (d'_w, h'_w), (d'_x, h'_x) и (d'_u, h'_u) соответственно (см. формулу (6)) при сведении решения рассматриваемой системы векторных уравнений к решению системы степенных скалярных уравнений уравнения (14) и (15) автоматически учитываются при использовании указанного представления. В результате получим 32 скалярных степенных уравнения с 36 скалярными неизвестными. При этом степень некоторых уравнений увеличивается, но это несущественно изменяет вычислительную сложность решения больших систем степенных уравнений, которая наиболее сильно зависит от числа уравнений (по сравнению со степенью уравнений и порядком поля, в котором задается система) [11, 25].

С учетом 128-битного порядка поля $GF(p)$, в котором задаются степенные уравнения, сложность решения системы из 32 уравнений, т.е. стойкость разработанного алгоритма ЭЦП к прямой атаке, можно оценить как $>2^{100}$ (см. табл. 1 в [25]). Поскольку сложность атаки на основе известных подписей существенно превышает последнее значение, можно сделать вывод о достаточности рандомизации подписи в описанном алгоритме.

Для повышения стойкости разработанного алгоритма ЭЦП в качестве его алгебраического носителя следует использовать КНАА размерности $m > 4$. Для выполнения оценки стойкости реализаций описанного алгоритма ЭЦП на КНАА с размерностями $m = 6, 8, 10, 12$ к атакам на основе известных подписей требуется предварительно изучить их декомпозицию как некоммутативных конечных колец на коммутативные подкольца. Оценка стойкости к прямым атакам может быть дана в предположении, что для всех указанных значений размерности при прямой атаке можно устранить уравнения проверки коммутативности (14) и (15) из решаемой системы степенных уравнений, число которых в этом случае становится равным $8m$. Обоснование этого предположения связано с тем, что элементы коммутативных подколец вычисляются из векторного уравнения вида $\mathbf{AX} = \mathbf{XA}$ при фиксированном векторе $\mathbf{A}$, решение которого сводится к решению системы из m линейных уравнений. Ранг γ главного определителя последней меньше значения m и коммутативное подкольцо, включающее вектор $\mathbf{A}$, описывается как линейное пространство решений размерности $m - \gamma$, а выбор неизвестного вектора из заданной скрытой коммутативной группы может быть описан через $m - \gamma$ скалярные неизвестные. В табл. 2

Таблица 2.

Ожидаемый уровень стойкости к прямой атаке для различных значений размерности

Размерность	4	6	8	10	12
Число степенных уравнений в системе	32	48	64	80	96
Уровень стойкости к прямой атаке	$\approx 2^{100}$	$>2^{128}$	$\approx 2^{192}$	$>2^{192}$	$\approx 2^{256}$

приведены ожидаемые оценки стойкости к прямой атаке для случая использования в качестве алгебраического носителя КНАА различных размерностей m (получение оценок стойкости к атаке на основе известных подписей требует знания конкретных значений ранга γ).

Другим аспектом, связанным с использованием КНАА с размерностями $m = 6, 8, 10, 12$, является существенное увеличение числа операций умножения в поле $GF(p)$, выполняемых в ходе процедур генерации и верификации ЭЦП. Снижение производительности алгоритма можно уменьшить, выбирая меньшие размеры порядка поля $GF(p)$ при переходе к большим значениям размерности m. Однако, такой способ также должен учитывать строение используемых КНАА (с точки зрения декомпозиции на коммутативные подкольца).

Выводы

Предложен способ усиления рандомизации подписи в алгебраических алгоритмах ЭЦП, отличающийся от известных аналогов вычислением вектора-фиксатора в зависимости от взаимно некоммутативных генераторов двух скрытых коммутативных групп и обеспечивающий возможность построения алгоритмов с одним уравнением верификации. Благодаря последнему обеспечивается повышение производительности алгоритма. Разработанный на основе способа алгоритм использует в качестве алгебраического носителя четырехмерную КНАА, заданную по прореженной ТУБВ, и обладает уровнем стойкости $>2^{100}$.

Показана потенциальная возможность повышения стойкости до уровня 2^{256} при реализации разработанного алгоритма на КНАА размерности $m = 6, 8, 10, 12$. Однако конкретная реализация таких вариантов алгоритма связана с задачей детального изучения строения КНАА указанных размерностей, что составляет задачу дальнейших исследований, направленных на разработку алгебраического алгоритма, представляющего интерес в качестве основы практичного постквантового стандарта ЭЦП.

Исследование выполнено 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. *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, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *Gärtner 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, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12*
5. *Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. N. 1–2. P. 469–493.*
6. *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. 2019. V. 11505. P. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18*
7. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
8. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 25–60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
9. *Moldovyan D. N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. N.2(86). P. 206–226.*
10. *Moldovyan D. N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. No. 2 (93). P. 3–10.*

11. *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*
12. *Ding J., Petzoldt A., Schmidt D. S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. V. 80. P. 185–248. https://doi.org/10.1007/978-1-0716-0987-3_8*
13. *Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow // In: Cheon, J. H., Johansson, T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. V. 13512. P. 170–184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
14. *Ding, J., Petzoldt, A., Schmidt, D. S. Oil and Vinegar // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 89–151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
15. *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*
16. *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*
17. *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), pp. 56–65. DOI: https://doi.org/10.56415/basm.y2022.i1.p56.*
18. *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.*
19. *Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.*
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.*
21. *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.*
22. *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.*
23. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2022. Т. 18. Вып. 2. С. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
24. *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. https://doi.org/10.56415/qrs.v30.11*
25. *J. Ding, A. Petzoldt Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28–36.*
26. *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation // Информационно-управляющие системы. 2023. № 3. С. 59–69. doi:10.31799/1684-8853-2023-3-59-69.*

ALGEBRAIC SIGNATURE ALGORITHMS WITH TWO HIDDEN GROUPS

Moldovyan N. A.[4], Petrenko A. S.[5]

Purpose of work *is increasing the performance of algebraic digital signature algorithms with enhanced signature randomization.*

Research methods: *application of two hidden commutative groups to enhance signature randomization in algebraic digital signature algorithms on finite non-commutative associative algebras (FNAA). Known results on the study of the decomposition of four-dimensional FNAA as finite rings into a set of commutative subrings are used to calculate the parameters of the digital signature algorithm with two hidden commutative groups. Application of a verification equation with two entries of the tuning signature element, which is a vector* S*, calculated by two commutative elements from different hidden groups. The presence of the exponentiation operation to a power, calculated as the value of the hash function of* S*. FNAAs specified by sparse multiplication tables of basis vectors are used as an algebraic support of the digital signature algorithm.*

Results of the study: *for the first time, the randomization enhancement mechanism is implemented in the algebraic digital signature algorithm without using the doubling of the verification equation. The developed digital signature algorithm is distinguished by the use of two hidden groups for calculating a random latch vector, by which the randomizing element of the generated signature is calculated. The latter ensures increased randomization not only for the signature values, but also for the value of the fixator vector. Due to this, the potentially achievable level of security is significantly increased. The sufficiency of performing the signature verification using only one verification equation is ensured by the following two techniques: 1) multiple entries of the tuning signature element* S *in the products that exponentiated to a large power, which appear in the right-hand side of the verification equation and 2) using the value of the hash function, depending on the vector* S*, as the value of the degree of one of the exponentiation operations performed during the signature authenticity verification*

4 Nikolay A. Moldovyan, Ph.D. (in Tech.) chief 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/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: mdn.spectr@mail.ru

5 Alexey S. Petrenko, junior research fellow of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

procedure. An analysis of security to a direct attack and to signature forgery on the on base of many known signatures is performed.

Practical relevance: *The scientific and practical significance of the results of the article consists in increasing the performance of algebraic digital signature algorithms with two hidden commutative groups, which, due to the small sizes of the signature and public key, are of interest for the development of practical post-quantum signature standards.*

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

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. *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, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *Gärtner 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, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12*
5. *Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. Designs, Codes and Cryptography. 2017. V. 82. N. 1–2. P. 469–493.*
7. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
8. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 25–60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
9. *Moldovyan D. N. A practical digital signature scheme based on the hidden logarithm problem. Computer Science Journal of Moldova. 2021. Vol. 29. N.2(86). P. 206–226.*
10. *Moldovyan D. N. New Form of the Hidden Logarithm Problem and Its Algebraic Support. Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. No. 2 (93). P. 3–10.*
11. *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*
12. *Ding J., Petzoldt A., Schmidt D. S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. V. 80. P. 185–248. https://doi.org/10.1007/978-1-0716-0987-3_8*
13. *Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. In: Cheon, J.H., Johansson, T. (eds) Post-Quantum Cryptography. Lecture Notes in Computer Science. 2022. V. 13512. P. 170–184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
14. *Ding, J., Petzoldt, A., Schmidt, D. S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 89–151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
15. *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*
16. *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*
17. *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), pp. 56–65. DOI: https://doi.org/10.56415/basm.y2022.i1.p56.*
18. *Moldovyan D. N. Moldovyan A. A. Algebraic signature algorithms based on difficulty of solving systems of equations. Voprosy kiberbezopasnosti [Cibersecurity questtions]. 2022. N. 2(48). P. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.*
19. *Moldovyan A. A., Moldovyan N. A. Signature algorithms on finite non-commutative algebras over fields of characteristic two. Voprosy kiberbezopasnosti [Cibersecurity questtions]. 2022. № 3(49). C. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.*
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.*
21. *Moldovyan A. A., Moldovyan D. N., Kostina A. A. Algebraic signature algorithms with complete signature randomization. Voprosy kiberbezopasnosti [Cibersecurity questtions]. 2024. № 2(60). C. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.*
22. *Moldovyan D. N., Kostina A. A. A method for strengthening signature randomization in algebraic signature algorithms on non-commutative algebras. Voprosy kiberbezopasnosti [Cibersecurity questtions]. 2024. № 4(62). C. 71-81. DOI: 10.21681/2311-3456-2024-4-71-81.*
23. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2022. T. 18. Вып. 2. C. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
24. *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. https://doi.org/10.56415/qrs.v30.11*
25. *J. Ding, A. Petzoldt. Current State of Multivariate Cryptography. IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28–36.*
26. *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 3, pp. 59–69. doi:10.31799/1684-8853-2023-3-59-69.*