ТИПОВЫЕ УРАВНЕНИЯ ВЕРИФИКАЦИИ В АЛГЕБРАИЧЕСКИХ СХЕМАХ ЭЦП С ДВУМЯ СКРЫТЫМИ ГРУППАМИ

Молдовян Н. А.[1], Петренко А. С.[2]

DOI: 10.21681/2311-3456-2025-3-8-20

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

Метод исследования: *применение двух скрытых коммутативных групп, элементы одной из которых некоммутативны с элементами другой, для обеспечения достаточной полноты рандомизации подписи в алгебраических схемах ЭЦП, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений в простом конечном поле GF(p). Вычисление подгоночного элемента ЭЦП в виде вектора S в зависимости от взаимно некоммутативных нескалярных векторов, выбираемых из скрытых групп, и случайного скалярного вектора. Применение конечных некоммутативных ассоциативных алгебр (КНАА) с хорошо изученным строением в качестве алгебраического носителя алгоритмов ЭЦП с проверочным уравнением с многократным вхождением вектора S. Задание КНАА по прореженным таблицам умножения базисных векторов.*

Результаты исследования: *предложены три типа постквантовых алгебраических схем ЭЦП, отличающихся приемами обеспечения высокой стойкости к подделке подписи с использованием вектора S в качестве подгоночного параметра атаки. В первом типе используется прием экспоненцирования произведения, в которое входит вектор S, в большую степень, во втором типе – выполнение операции экспоненцирования в степень, равную значению хеш-функции, вычисляемой от S, и в третьем типе – комбинирование первых двух приемов. Осуществлены алгоритмические реализации схем ЭЦП каждого типа и показана корректность разработанных алгоритмов. Выполнены оценки стойкости к прямой атаке, атаке на основе известных подписей и к подделке подписи. Представлено сравнение предложенных алгоритмов ЭЦП с известными аналогами. В качестве приемов повышения производительности алгебраических алгоритмов ЭЦП использовано 1) задание КНАА по прореженным таблицам умножения базисных векторов и 2) умножение на скалярный вектор при вычислении вектора S.*

Научная и практическая значимость *результатов статьи состоит в апробации способа усиления рандомизации подписи, включающего вычисление подгоночного элемента подписи S в зависимости от произведения двух взаимно некоммутативных векторов и одного скалярного вектора, при разработке алгебраических алгоритмов трех различных типов, представляющих интерес в качестве прототипа практичного постквантового стандарта ЭЦП.*

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

Введение

В настоящее время исследования и разработки в области постквантовой криптографии с открытым ключом сохраняют достаточно высокую степень актуальности [1]. В основе стойкости постквантовых криптоалгоритмов с открытым ключом, в том числе алгоритмов электронной цифровой подписи (ЭЦП), лежат вычислительно трудные задачи, отличные от факторизации и дискретного логарифмирования. Это определяется тем, что для квантового компьютера известны полиномиальные по времени алгоритмы решения двух последних задач. В области постквантовой криптографии можно выделить следующие направления: разработка криптоалгоритмов на кодах [2–4], на группах [5], на алгебраических решетках [6], на трудно обратимых функциях [7,8], на однонаправленных отображениях с секретной лазейкой [9,10] и на некоммутативных алгебрах [11,12].

Использование нелинейных трудно обратимых отображений с секретной лазейкой в качестве постквантового криптографического примитива представляет значительный интерес, поскольку это приводит к построению двухключевых криптосхем, стойкость которых основана на вычислительной трудности решения систем многих степенных уравнений с многими неизвестными [13], т.е. на задаче, для решения которой квантовый компьютер не является эффективным. Существенным практическим недостатком постквантовых алгоритмов данного типа

1 Молдовян Николай Андреевич, доктор технических наук, профессор, главный научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: moldovan.NA@talantiuspeh.ru

2 Петренко Алексей Сергеевич, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, младший научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

является большая длина открытого ключа. Даже при применении способов реализации трудно обратимых отображений как операций экспоненцирования в векторном конечном поле [14,15], которые потенциально позволяют сократить размер открытого ключа в 10 и более раз, разрабатываемые постквантовые алгоритмы ЭЦП и открытого шифрования остаются ограниченно применимыми на практике.

Сравнительно недавно предложена новая парадигма построения постквантовых алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений (БССУ) [16–19]. В рамках этой парадигмы в качестве алгебраического носителя используется многомерная конечная некоммутативная ассоциативная алгебра (КНАА), в которой в качестве одного из элементов секретного ключа задается коммутативная скрытая группа. При этом цифровая подпись вычисляется в виде двух элементов (e, $\mathbf{S}$), первый из которых является рандомизирующим натуральным числом, а второй – подгоночным вектором, обеспечивающим выполнение проверочного уравнения. При этом вектор $\mathbf{S}$ входит в проверочное уравнение в качестве множителя, что создает предпосылки для атак по подделке ЭЦП с использованием $\mathbf{S}$ как подгоночного параметра атаки. Обеспечение стойкости реализуется заданием проверочных уравнений с многократным вхождением вектора $\mathbf{S}$. Эффективность такого приема обусловливается свойством некоммутативности операции умножения в КНАА.

Процедура генерации ЭЦП в алгоритмах [16–19] включает вычисление вектора $\mathbf{S}$ в зависимости от двух фиксированных секретных векторов $\mathbf{D}$ и $\mathbf{F}$ и случайного вектора $\mathbf{H}$, выбираемого из скрытой коммутативной группы, по формуле:

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

Выбор вектора $\mathbf{H}$ определяется значениями рандомизирующих параметров и подписываемым документом M, т.е. является уникальным для каждого значения M. Однако в работах [20,21] была показана недостаточная полнота рандомизации подписи, задаваемая по формуле (1), создающая уязвимость к атакам на основе известных подписей, и предложен способ усиления рандомизации за счет включения в формулу для вычисления вектора $\mathbf{S}$ случайного обратимого вектора $\mathbf{V}$, выбираемого из всей КНАА, используемой в качестве алгебраического носителя. Предложенные в [20,21] алгоритмы ЭЦП используют удвоенное проверочное уравнение с однократным вхождением подгоночного элемента подписи $\mathbf{S}$, что приводит к увеличению размера открытого ключа и снижению производительности алгоритма ЭЦП. Однако основным недостатком использования приема удвоения проверочного уравнения по сравнению с использованием одного уравнения верификации с многократным вхождением вектора $\mathbf{S}$ является необходимость использования дополнительного механизма обеспечения стойкости к подделке подписи (атака, включающая формирование подписи без знания секретного ключа).

Представляет интерес способ усиления рандомизации, предложенный в [22] и заключающийся в вычислении элемента подписи $\mathbf{S}$ в зависимости от взаимно некоммутативных векторов $\mathbf{P}^b$ и $\mathbf{G}^n$, выбираемых их двух скрытых коммутативных групп по уникальным значениям степеней b и n, по следующей формуле

$$\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}, \qquad (2)$$

В способе [22] усиление рандомизации ЭЦП обеспечивается за счет того, что вектор, равный произведению $\mathbf{P}^b\mathbf{G}^n$ ($\mathbf{P}$ имеет порядок $p^2 - 1$, а $\mathbf{G}$ – простой порядок $(p - 1)/2$), пробегает $\approx p^3$ значений, принадлежащих различным циклическим группам, содержащимся в четырехмерной КНАА, заданной над полем $GF(p)$, где простое число $p = 2q + 1$ при простом q, и используемой в качестве алгебраического носителя. Предложенный в [22] механизм обеспечения стойкости к подделке подписи основан на взаимной некоммутативности генераторов $\mathbf{P}$ и $\mathbf{G}$ скрытых групп и включает вычисление вспомогательного параметра рандомизации в виде значения ρ хеш-функции $\mathbf{\Phi}$ от вектора $\mathbf{S}$ и использование вспомогательного подгоночного элемента подписи в виде натурального числа s, задающего степень одной из операций экспоненцирования, выполняемых в ходе процедуры верификации ЭЦП. В алгоритме [22] также используются два проверочных уравнения.

Впервые алгоритмическая реализация способа рандомизации подписи по формуле (2) и механизма защищенности от подделки ЭЦП из [22] с использованием одного проверочного уравнения выполнена в работе [23]. Представляет интерес рассмотрение дополнительных механизмов снижения вычислительной сложности процедур генерации и верификации ЭЦП. В частности, повышение производительности алгебраического алгоритма ЭЦП с двумя скрытыми группами может быть достигнуто путем двукратного уменьшения битового размера порядка вектора $\mathbf{P}$, а именно, путем выбора вектора $\mathbf{P}$, имеющего порядок, равный $p + 1$ или p.

Формализация цели исследования

Для построения алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения БССУ, в качестве алгебраического носителя будем использовать четырехмерные КНАА, заданные над конечным простым полем $GF(p)$ простого порядка $p = 2q + 1$, где q – простое 128-битное число. Такой

выбор связан с тем, что декомпозиция таких алгебр, как некоммутативных колец на коммутативные подкольца порядка p^2, хорошо изучена [12,24] и показана общность свойств их разбиения независимо от вида таблицы умножения базисных векторов (ТУБВ), по которой задается операция умножения. В частности показано, что имеются только три типа таких колец, характеризующихся строением и значением порядка ($p^2 - 1$; $(p-1)^2$ и $p(p-1)$) их мультипликативных групп. При этом эти подкольца пересекаются строго в множестве скалярных векторов. Краткая сводка общих свойств разбиения четырехмерных КНАА, важных для построения алгоритмов ЭЦП и оценивания стойкости, представлена в работе [23].

Для достижения цели повышения производительности алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения БССУ, зададим вычисление подгоночного элемента подписи по следующей формуле

$$\mathbf{S} = \mathbf{D}\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}, \qquad (3)$$

где взаимно некоммутативные векторы $\mathbf{P}$ и $\mathbf{G}$ являются генераторами циклических групп порядка $p+1$, p или q, таких, что все их элементы являются нескалярными векторами, кроме единичного элемента $\mathbf{E}$; $\mathbf{L}$ – скалярный вектор порядка $p-1$. Легко показать, что вектор, равный поизведению $\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u$, принимает $\approx p^3$ различных значений, принадлежащих $\approx p^2$ различным коммутативным подкольцам, содержащимся в четырехмерной КНАА, используемой в качестве алгебраического носителя. Обоснование достаточности рандомизации, задаваемой по формуле (3), выполняется аналогично обоснованию рандомизации подписи, задаваемой по формуле (2), которое представлено в [23].

Благодаря коммутативности векторов $\mathbf{L}^u$ со всеми элементами КНАА открытый ключ может быть сформирован таким образом, что в проверочном уравнении степени операции экспоненцирования имеющие битовый размер $|p^2|$ заменяются на степени размером $|p|$ ($|x|$ обозначает длину значения x в двоичном представлении). Задачей, решаемой в настоящей работе, является разработка алгебраических алгоритмов ЭЦП с двумя скрытыми коммутативными группами с использованием способа рандомизации, задаваемого формулой (3), и одного уравнения верификации подписи. При этом разрабатываются алгоритмы трех различных типов, отличающихся использованием 1) многократного вхождения вектора $\mathbf{S}$ в проверочное уравнение, 2) вычисления значения хеш-функции $\rho = \mathbf{\Phi}(\mathbf{S})$ как одной из степеней операции экспоненцирования, присутствующей в уравнении верификации ЭЦП, или 3) комбинирования первых двух приемов.

1. Варианты задания четырехмерных КНАА

Элементами конечной m-мерной алгебры являются векторы $\mathbf{V} = (v_0, v_1, v_2, \ldots v_{m-1})$, координатами которых являются элементы некоторого конечного поля. В нашем случае рассматривается задание векторов над простым конечным полем $GF(p)$ простого порядка $p = 2q + 1$, где q – простое 128-битное число. Операция сложения векторов описывается как сложение одноименных координат. Операция умножения векторов задается таким образом, что она является замкнутой и дистрибутивной слева и справа относительно операции сложения. Для использования конечных алгебр в качестве алгебраического носителя разрабатываемых алгоритмов требуется наличие следующих дополнительных свойств:

1) существование в алгебре глобальной двухсторонней единицы;
2) некоммутативность операции умножения;
3) ассоциативность операции умножения.

При упоминании о векторе, действующем как единичный элемент на каждый элемент алгебры при умножении слева и справа, мы используем термин двухсторонний, поскольку существуют КНАА с множеством глобальных односторонних (левосторонних или правосторонних) единиц [25]. Для формирования КНАА с глобальной двухсторонней единицей можно задать операцию умножения векторов

$$\mathbf{A} = \sum_{i=0}^{m-1} a_i e_i \text{ и } \mathbf{B} = \sum_{j=0}^{m-1} b_j e_j,$$

где e_i – базисные векторы, по формуле:

$$\mathbf{AB} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j (e_i e_j) \qquad (4)$$

где вместо произведения пары базисных векторов $\mathbf{e}_i$ и $\mathbf{e}_j$ подставляется значение некоторого однокомпонентного вектора в соответствии с некоторой ТУБВ, обеспечивающей наличие требуемых свойств. Известен способ [26] построения таких ТУБВ для произвольных четных размерностей $m > 4$. Для интересующего нас случая $m = 4$ известны различные ТУБВ, в том числе прореженные ТУБВ, в которых половина из всевозможных произведений пар базисных векторов заменяется на нулевой вектор (вектор со всеми нулевыми координатами), в результате чего операция умножения двух четырехмерных векторов выполняется всего за восемь операций умножения в поле $GF(p)$. Таблицы 1–4 представляют различные ТУБВ, задающие четырехмерные КНАА с глобальной двухсторонней единицей.

Выполненные исследования декомпозиции четырехмерных КНАА с глобальной двухсторонней единицей, заданных по многим различным ТУБВ, в том числе прореженным, на множество коммутативных подколец порядка p^2 показали идентичность строения таких КНАА [12,24,28,29]. В связи с этим

Таблица 1.

Задание операции умножения в четырехмерной КНАА ($\lambda\mu \neq 1$) [11,27]

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

Таблица 2.

Прореженная ТУБВ ($\lambda \neq 0$) для задания КНАА с глобальной двухсторонней единицей (1, 1, 0, 0) [12]

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

Таблица 3.

Задание (при $\lambda = 1$) операции умножения матриц 2×2 как умножения в четырехмерной КНАА ($\lambda \neq 0$)

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

Таблица 4.

Задание ($\lambda \neq 0$) четырехмерной КНАА с глобальной двухсторонней единицей (0, 0, 1, 1) [29]

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

для получения более высокой производительности в данной работе предполагается реализация алгоритмов ЭЦП на четырехмерных КНАА, заданных по прореженным ТУБВ, например, представленных в табл. 2–4. Существуют и другие варианты прореженных ТУБВ. Заметим, что табл. 1 при $\lambda = \mu = 0$ задает четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (0, 1, 1, 0)$, при $\lambda = 0$ и $\mu \neq 0$ – четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (-\mu, 1, 1, 0)$, а при $\lambda \neq 0$ и $\mu = 0$ – четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (0, 1, 1, -\lambda)$.

2. Алгоритм ЭЦП первого типа

В алгоритмах первого типа стойкость к подделке подписи обеспечивается двукратным или многократным вхождением подгоночного элемента подписи $\mathbf{S}$ в проверочное уравнение. При таком построении алгоритма ЭЦП подделка подписи связана с решением проверочного уравнения относительно $\mathbf{S}$ как неизвестного вектора. Важным моментом является то, что хотя бы один раз вектор $\mathbf{S}$ входит в проверочное уравнение в некоторую группу сомножителей, возводимую в степень достаточно большого размера (больше 100 бит в нашем случае). Действительно, легко видеть, что в четырехмерной КНАА при известных векторах $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ и $\mathbf{R}$ решение векторного уравнения вида

$$\mathbf{R} = \mathbf{A}\mathbf{S}^d\mathbf{B}\mathbf{S}^h\mathbf{C}. \qquad (5)$$

Сводится к решению системы из четырех скалярных уравнений степени $d + h$ в поле $GF(p)$. Естественным способом сделать такое сведение вычислительно невыполнимым является задание хотя бы одной из степеней d и h настолько большой, что степенные скалярные уравнения будут включать число слагаемых не менее 2^{80}. Это может быть обеспечено при $|d| > 100$ и/или $|h| > 100$ бит.

В приводимом ниже алгоритме ЭЦП в проверочное уравнение входит множитель $\mathbf{S}^{-1}$, для вычисления которого по известному вектору $\mathbf{S}$ из векторного уравнения $\mathbf{SX} = \mathbf{E}$ требуется выполнить не более 100 умножений в поле $GF(p)$, что вносит несущественный вклад в вычислительную сложность процедуры верификации ЭЦП. Включение множителя $\mathbf{S}^{-1}$ вместо $\mathbf{S}$ так же несущественно увеличивает вычислительную сложность подделки подписи.

Формирование секретного ключа выполняется как генерация 1) случайного примитивного элемента α по модулю p, 2) случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$ и 3) случайных обратимых, нескалярных и попарно некоммутативных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что векторы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $p + 1$ и q соответственно (общий размер секретного ключа равен ≈512 байт). Для формирования открытого ключа вычисляется вспомогательный вектор $\mathbf{L} = \alpha^2\mathbf{E}$ порядка q. Открытый ключ вычисляется в виде совокупности следующих десяти четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$ и $\mathbf{T}_5$ (с общим размером ≈640 байт) по формулам:

$$\mathbf{Y}_1 = \mathbf{AGA}^{-1};\ \mathbf{Z}_1 = \mathbf{KG}^x\mathbf{LK}^{-1};\ \mathbf{Y}_2 = \mathbf{BP}^x\mathbf{B}^{-1};$$
$$\mathbf{Z}_2 = \mathbf{BGL}^x\mathbf{B}^{-1};\ \mathbf{U} = \mathbf{DPD}^{-1}; \quad (6)$$

$$\mathbf{T}_1 = \mathbf{AG}^w\mathbf{K}^{-1};\ \mathbf{T}_2 = \mathbf{KG}^y\mathbf{F};\ \mathbf{T}_3 = \mathbf{DP}^w\mathbf{B}^{-1};$$
$$\mathbf{T}_4 = \mathbf{BP}^y\mathbf{D}^{-1};\ \mathbf{T}_5 = \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}. \quad (7)$$

Предполагается, что при генерации и верификации подписи используется некоторая коллизионно стойкая 512-битная хеш-функция $\mathbf{\Phi}$, которая является частью рассматриваемой постквантовой схемы ЭЦП.

Алгоритм генерации ЭЦП

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить значение рандомизирующего вектора-фиксатора $\mathbf{R}$ по формуле: $\mathbf{R} = \mathbf{AG}^k\mathbf{P}^t\mathbf{L}^v\mathbf{B}^{-1}$.
2. Вычислить хеш-значение от документа M с присоединенным к нему вектором $\mathbf{R}$: $e = e_1||e_2||e_3||e_4 = \mathbf{\Phi}(M, \mathbf{R})$, где 512-битное хеш-значение e представлено в виде конкатенации четырех 128-битных натуральных чисел e_1, e_2, e_3 и e_4.
3. Вычислить натуральное число

$$n: n = -z - e_4 \bmod (p + 1).$$

4. Вычислить натуральное число

$$b: b = (e_1 - 1)^{-1}(t - e_2 - w - e_1e_3x - e_1y) \bmod q.$$

5. Вычислить натуральное число

$$u: u = (e_1 - 1)^{-1}(v - e_1 - e_1e_4x) \bmod q.$$

6. По формуле (3) вычислить подгоночный элемент ЭЦП в виде вектора $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}$.
7. Вычислить вспомогательный подгоночный элемент подписи в виде числа

$$s: s = (k - w - e_1x - y + n) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой тройку значений $(e, s, \mathbf{S})$ с общим размером ≈144 байт. Вычислительная сложность процедуры генерации ЭЦП главным образом определяется четырьмя операциями возведения в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$) и двумя операциями возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^v$ и $\mathbf{L}^u$), что составляет ≈6600 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \mathbf{S})$ к документу M осуществляется с использованием 640-байтного открытого ключа $(\mathbf{Y}_1, \mathbf{Z}_1, \mathbf{Y}_2, \mathbf{Z}_2, \mathbf{U}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4, \mathbf{T}_5)$ по следующему алгоритму:

1. Вычислить вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = \mathbf{Y}_1^s\mathbf{T}_1\mathbf{Z}_1^{e_1}\mathbf{T}_2\mathbf{S}^{-1}\mathbf{U}^{e_2}\mathbf{T}_3(\mathbf{Y}_2^{e_3}\mathbf{T}_4\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{e_4})^{e_1}. \quad (8)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_1||\varepsilon_1||\varepsilon_1 = \mathbf{\Phi}(M, \mathbf{R}'),$$

где 512-битное хеш-значение представлено в виде конкатенации четырех 128-битных чисел ε_1, ε_2, ε_3 и ε_4.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$, $\varepsilon_2 = e_2$, $\varepsilon_3 = e_3$ и $\varepsilon_4 = e_4$, то подпись принимается как подлинная, иначе она отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как шесть операций возведения четырехмерных векторов в 128-битную степень, что составляет ≈9200 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (8) элементов открытого ключа, выраженных через элементы секретного ключа, следующим образом.

Доказательство корректности алгоритма ЭЦП первого типа

Подставляя в проверочное уравнение (8) элементы открытого ключа, выраженные через элементы секретного ключа по формулам (6) и (7), для корректно сгенерированной подписи получаем:

$$\mathbf{R}' = \mathbf{Y}_1^s\mathbf{T}_1\mathbf{Z}_1^{e_1}\mathbf{T}_2\,\mathbf{S}^{-1}\mathbf{U}^{e_2}\mathbf{T}_3(\mathbf{Y}_2^{e_3}\mathbf{T}_4\mathbf{S}\,\mathbf{T}_5\mathbf{Z}_2^{e_4})^{e_1} =$$
$$= (\mathbf{AG}\,\mathbf{A}^{-1})^s\mathbf{A}\,\mathbf{G}^w\,\mathbf{K}^{-1}(\mathbf{K}\,\mathbf{G}^x\mathbf{L}\,\mathbf{K}^{-1})^{e_1}\mathbf{K}\,\mathbf{G}^y\mathbf{F}\times$$
$$\times(\mathbf{F}^{-1}\mathbf{L}^{-u}\mathbf{G}^{-n}\mathbf{P}^{-b}\mathbf{D}^{-1})\,(\mathbf{DP}\,\mathbf{D}^{-1})^{e_2}\,\mathbf{D}\,\mathbf{P}^w\mathbf{B}^{-1})\times$$
$$\times[(\mathbf{B}\,\mathbf{P}^x\mathbf{B}^{-1})^{e_3}\mathbf{B}\,\mathbf{P}^y\mathbf{D}^{-1}\,(\mathbf{D}\,\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F})\,\mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}\times$$
$$\times(\mathbf{BG}\,\mathbf{L}^x\mathbf{B}^{-1})^{e_4}]^{e_1} = \mathbf{A}\,\mathbf{G}^s\mathbf{G}^w\mathbf{G}^{xe_1}\mathbf{L}^{e_1}\mathbf{G}^y\mathbf{L}^{-u}\mathbf{G}^{-n})\times$$
$$\times\,\mathbf{P}^{-b}\mathbf{P}^{e_2}\mathbf{P}^w\mathbf{B}^{-1}(\mathbf{B}\,\mathbf{P}^{xe_3}\mathbf{P}^y\mathbf{P}^b\mathbf{L}^u\mathbf{G}^n\mathbf{G}^z\mathbf{G}^{e_4}\mathbf{L}^{xe_4}\mathbf{B}^{-1})^{e_1} =$$
$$= \mathbf{A}\,\mathbf{G}^{s+w+xe_1+y-n}\mathbf{L}^{e_1-u}\mathbf{P}^{-b+e_2+w}\mathbf{B}^{-1}\times$$
$$(\mathbf{B}\,\mathbf{P}^{xe_3+y+b}\mathbf{G}^{n+z+e_4}\mathbf{L}^{u+xe_4}\mathbf{B}^{-1})^{e_1} = \mathbf{A}\,\mathbf{G}^{(k-w-xe_1-y+n)+w+xe_1+y-n}\times$$
$$\times\,\mathbf{L}^{e_1-u}\mathbf{P}^{-b\,+\,e_2\,+\,w}\,\mathbf{B}^{-1}(\mathbf{B}\,\mathbf{P}^{xe_3+y+b}\mathbf{G}^0\,\mathbf{L}^{u+xe_4}\mathbf{B}^{-1})^{e_1} =$$
$$= \mathbf{A}\,\mathbf{G}^k\mathbf{P}^{-b+e_2+w+e_1(xe_3+y+b)}\mathbf{L}^{e_1-u+e_1u+xe_4e_1}\mathbf{B}^{-1} =$$
$$= \mathbf{A}\,\mathbf{G}^k\mathbf{P}^t\mathbf{L}^v\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем $\varepsilon_1||\varepsilon_2||\varepsilon_3||\varepsilon_4 = \mathbf{\Phi}(M, \mathbf{R}') = \mathbf{\Phi}(M, \mathbf{R}) = e_1||e_2||e_3||e_4$, т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

3. Алгоритмы ЭЦП второго типа

Второй тип алгебраических алгоритмов ЭЦП с двумя скрытыми группами характеризуется тем, что стойкость к атакам типа подделка подписи обеспечивается наличием в проверочном уравнении операций экспоненцирования, степень которых вычисляется как значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S})$, вычисляемое от подгоночного элемента подписи $\mathbf{S}$. Формирование секретного ключа выполняется как генерация 1) случайного примитивного элемента

α по модулю p, 2) случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$ и 3) случайных обратимых, нескалярных и попарно некоммутативных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что векторы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $p + 1$ и q соответственно (общий размер секретного ключа равен ≈512 байт). Для формирования открытого ключа вычисляется вспомогательный вектор $\mathbf{L} = \alpha^z\mathbf{E}$. Открытый ключ вычисляется в виде совокупности следующих восьми четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, и $\mathbf{T}_4$ (с общим размером ≈512 байт) по формулам:

$$\mathbf{Y}_1 = \mathbf{APA}^{-1};\ \mathbf{Z}_1 = \mathbf{FGF}^{-1};$$
$$\mathbf{Y}_2 = \mathbf{KG}^x\mathbf{K}^{-1};\ \mathbf{Z}_2 = \mathbf{BG}^y\mathbf{B}^{-1}; \quad (9)$$

$$\mathbf{T}_1 = \mathbf{AP}^x\mathbf{D}^{-1};\ \mathbf{T}_2 = \mathbf{FG}^w\mathbf{K}^{-1};$$
$$\mathbf{T}_3 = \mathbf{KP}^w\mathbf{D}^{-1};\ \mathbf{T}_4 = \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}. \quad (10)$$

Алгоритм генерации ЭЦП

При генерации подписи к документу M выполняются следующие шаги:

1. Выбрать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить вектор $\mathbf{R} = \mathbf{AP}^t\mathbf{G}^k\mathbf{L}^v\mathbf{B}^{-1}$.
2. Используя некоторую специфицированную 256-битную хеш-функцию $\mathbf{\Phi}'$, вычислить хеш-значение $e = e_1||e_2 = \mathbf{\Phi}'(M, \mathbf{R})$, представленное в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.
3. Вычислить натуральную степень

$$n\colon n = k - z - ye_2 \bmod (p + 1).$$

4. Вычислить натуральное число

$$b\colon b = 2^{-1}(t - e_1 - x - w) \bmod q.$$

5. Вычислить натуральное число u: $u = 2^{-1}\ v \bmod q$.
6. По формуле (3) вычислить подгоночный элемент ЭЦП $\mathbf{S}$: $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}$.
7. Вычислить вспомогательное рандомизирующее значение $\rho = \mathbf{\Phi}''(\mathbf{S})$.
8. Вычислить вспомогательный подгоночный элемент ЭЦП в виде числа

$$s\colon s = -(n + w + x\rho) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой тройку значений $(e, s, \mathbf{S})$ с общим размером ≈112 байт. Вычислительная сложность процедуры генерации ЭЦП может быть оценена как четыре экспоненциирования в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$) и две операции возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^v$ и $\mathbf{L}^u$), что составляет ≈6600 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \mathbf{S})$ к документу M осуществляется с использованием 512-байтного открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$) по следующему алгоритму:

1. Вычислить значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S}) = \rho$ и вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = \mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{Z}_1^s\mathbf{T}_2\mathbf{Y}_2^{\mathbf{\Phi}''(\mathbf{S})}\mathbf{T}_3\mathbf{S}\mathbf{T}_4\mathbf{Z}_2^{e_2}. \quad (11)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(\mathrm{M}, \mathbf{R}'),$$

где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.

3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то подпись принимается как подлинная, иначе она отклоняется.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как четыре операции возведения четырехмерных векторов в 128-битную степень, что составляет ≈6150 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (11) элементов открытого ключа, выраженных через элементы секретного ключа по формулам (9) и (10).

Доказательство корректности алгоритма ЭЦП второго типа

Из проверочного уравнения (11) с учетом формул (9) и (10) для корректно вычисленной подписи $(e, s, \mathbf{S})$ получаем:

$$\mathbf{R}' = \mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{Z}_1^s\mathbf{T}_2\mathbf{Y}_2^{\mathbf{\Phi}''(\mathbf{S})}\mathbf{T}_3\mathbf{S}\mathbf{T}_4\mathbf{Z}_2^{e_2} =$$
$$= (\mathbf{APA}^{-1})^{e_1}\mathbf{AP}^x\mathbf{D}^{-1}(\mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F})\ (\mathbf{FGF}^{-1})^s \times$$
$$\times\ \mathbf{FG}^w\mathbf{K}^{-1}(\mathbf{KG}^x\mathbf{K}^{-1})^\rho\mathbf{KP}^w\mathbf{D}^{-1}(\mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}) \times$$
$$\times\ \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}\ (\mathbf{BG}^y\mathbf{B}^{-1})^{e_2} = \mathbf{AP}^{e_1+x+u}\mathbf{G}^{n+s+w+x\rho}\mathbf{P}^{w+b} \times$$
$$\times\ \mathbf{G}^{n+z+ye_2}\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+b}\mathbf{G}^{n+(-n-w-x\rho)+w+x\rho}\mathbf{P}^{w+b} \times$$
$$\mathbf{G}^{(k-z-ye_2)+z+ye_2}\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+b}\mathbf{G}^0\mathbf{P}^{w+b}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{e_1+x+2b+w}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+(t-e_1-x-w)+w}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^t\mathbf{G}^k\mathbf{L}^v\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем

$$\varepsilon_1||\varepsilon_2 = \mathbf{\Phi}(M, \mathbf{R}') = \mathbf{\Phi}(M, \mathbf{R}) = e_1||e_2,$$

т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

4. Алгоритмы ЭЦП третьего типа

В третьем типе алгебраических алгоритмов ЭЦП, основанных на вычислительной сложности решения БССУ, объединяются приемы обеспечения стойкости к подделке подписи, используемые по отдельности в алгоритмах первого и второго типов. Секретный ключ и вспомогательный скалярный вектор $\mathbf{L}$ формируются в точности, как и в алгоритме первого типа

(см. раздел 2). Элементы открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$) вычисляются по следующим формулам:

$$\mathbf{Y}_1 = \mathbf{APA}^{-1};\ \mathbf{Z}_1 = \mathbf{KG}^{y}\mathbf{K}^{-1};\ \mathbf{Y}_2 = \mathbf{BG}^{z}\mathbf{B}^{-1};$$

$$\mathbf{Z}_2 = \mathbf{BGB}^{-1};\ \mathbf{U} = \mathbf{DP}^{x}\mathbf{D}^{-1};\ \mathbf{T}_0 = \mathbf{AP}^{y}\mathbf{L}^{x}\mathbf{B}^{-1}; \quad (12)$$

$$\mathbf{T}_1 = \mathbf{AP}^{w}\mathbf{D}^{-1};\ \mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{G}^{x}\mathbf{K}^{-1};\ \mathbf{T}_3 = \mathbf{KG}^{w}\mathbf{A}^{-1};$$
$$\mathbf{T}_4 = \mathbf{BG}^{y}\mathbf{P}^{z}\mathbf{D}^{-1};\ \mathbf{T}_5 = \mathbf{F}^{-1}\mathbf{G}^{z}\mathbf{L}^{w}\mathbf{B}^{-1}. \quad (13)$$

Размер открытого ключа равен ≈704 байт.

Алгоритм генерации ЭЦП

При генерации подписи к документу M выполняются следующие шаги:

1. Сгенерировать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить вектор $\mathbf{R} = \mathbf{AP}^{t}\mathbf{G}^{k}\mathbf{L}^{v}\mathbf{B}^{-1}$.
2. Используя некоторую специфицированную 256-битную хеш-функцию $\mathbf{\Phi}'$, вычислить хеш-значение $e = e_1||e_2 = \mathbf{\Phi}'(M, \mathbf{R})$, представленное в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.
3. Вычислить натуральную степень

$$n: n = -x - ye_2 - w \bmod (p + 1).$$

4. Вычислить натуральную степень

$$b: b = -z - e_1 x \bmod q.$$

5. Вычислить первый вспомогательный подгоночный элемент подписи

$$s: s = (t - y)(e_1 + w + b)^{-1} \bmod q.$$

6. Вычислить натуральную степень

$$u: u = (v - x - w)(s + 1)^{-1} \bmod q.$$

7. По формуле (3) вычислить основной подгоночный элемент ЭЦП $\mathbf{S}$: $\mathbf{S} = \mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}$.
8. Вычислить вспомогательное рандомизирующее значение $\rho = \mathbf{\Phi}''(\mathbf{S})$.
9. Вычислить вспомогательный подгоночный элемент ЭЦП в виде числа

$$\sigma: \sigma = (k - z\rho - y - n - z) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой четверку значений (e, s, σ, $\mathbf{S}$) с общим размером ≈128 байт. Вычислительная сложность процедуры генерации ЭЦП может быть оценена как четыре операции возведения в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^{t}$, $\mathbf{G}^{k}$, $\mathbf{P}^{b}$ и $\mathbf{G}^{n}$) и две операции возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^{v}$ и $\mathbf{L}^{u}$), что составляет ≈6530 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \sigma, \mathbf{S})$ к документу M осуществляется с использованием 704-байтного открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$) по следующему алгоритму:

1. Вычислить значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S}) = \rho$ и вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = (\mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}_1^{e_2}\mathbf{T}_3)^{s}\mathbf{T}_0\mathbf{Y}_2^{\Phi''(\mathbf{S})}\mathbf{T}_4\mathbf{U}^{e_1}\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{\sigma}. \quad (14)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(M, \mathbf{R}'),$$

где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то подпись принимается как подлинная, иначе она отклоняется.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как шесть операций возведения четырехмерных векторов в 128-битную степень, что составляет ≈9200 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (14) элементов открытого ключа, выраженных через элементы секретного ключа по формулам (12) и (13).

Доказательство корректности алгоритма ЭЦП третьего типа

Из проверочного уравнения (14) с учетом формул (12) и (13) для корректно вычисленной подписи (e, s, σ, $\mathbf{S}$) получаем:

$$\mathbf{R}\text{^}' = (\mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}_1^{e_2}\mathbf{T}_3)^{s}\mathbf{T}_0\mathbf{Y}_2^{\Phi''(\mathbf{S})}\mathbf{T}_4\mathbf{U}^{e_1}\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{\sigma} =$$
$$= [(\mathbf{APA}^{-1})^{e_1}\mathbf{AP}^{w}\mathbf{D}^{-1}(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}) \times$$
$$\times \mathbf{F}^{-1}\mathbf{G}^{x}\mathbf{K}^{-1}(\mathbf{KG}^{y}\mathbf{K}^{-1})^{e_2}\mathbf{KG}^{w}\mathbf{A}^{-1}]^{s}\mathbf{AP}^{y}\mathbf{L}^{x}\mathbf{B}^{-1} \times$$
$$(\mathbf{BG}^{z}\mathbf{B}^{-1})^{\rho}\mathbf{BG}^{y}\mathbf{P}^{z}\mathbf{D}^{-1}(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1}(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}) \times$$
$$\mathbf{F}^{-1}\mathbf{G}^{z}\mathbf{L}^{w}\mathbf{B}^{-1}(\mathbf{BGB}^{-1})^{\sigma} =$$
$$= (\mathbf{AP}^{e_1+w+b}\mathbf{G}^{n+x+ye_2+w}\mathbf{L}^{u}\mathbf{A}^{-1})^{s}\mathbf{AP}^{y}\mathbf{L}^{x} \times$$
$$\times \mathbf{G}^{\rho z+y}\mathbf{P}^{z+xe_1+b}\mathbf{G}^{n+z+\sigma}\mathbf{L}^{u+w}\mathbf{B}^{-1} =$$
$$= (\mathbf{AP}^{e_1+w+b}\mathbf{G}^{0}\mathbf{L}^{u}\mathbf{A}^{-1})^{s}\mathbf{AP}^{y}\mathbf{G}^{\rho z+y}\mathbf{P}^{0}\mathbf{G}^{n+z+\sigma}\mathbf{L}^{u+w+x}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{s(e_1+w+b)}\mathbf{L}^{su}\mathbf{P}^{y}\mathbf{G}^{\rho z+y+n+z+\sigma}\mathbf{L}^{u+w+x}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{s(e_1+w+b)+y}\mathbf{G}^{k}\mathbf{L}^{u(s+1)+w+x}\mathbf{B}^{-1} = \mathbf{AP}^{t}\mathbf{G}^{k}\mathbf{L}^{v}\mathbf{B}^{-1} =$$
$$= \mathbf{R} \Rightarrow \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(M,\mathbf{R}') = \mathbf{\Phi}'(M,\mathbf{R}) = e_1||e_2.$$

5. Обсуждение

Стойкость представленных типовых алгебраических алгоритмов ЭЦП основана на вычислительной трудности решения БССУ. Данная вычислительная задача достаточно хорошо изучена. Интерес к ней

возник с появлением криптоалгоритмов с открытым ключом, основанных на трудно обратимых отображениях с секретной лазейкой в 1988 году. К настоящему времени появились многочисленные алгоритмы открытого шифрования и ЭЦП, относящиеся к этому классу криптоалгоритмов, которые рассматриваются как постквантовые криптосхемы, поскольку применение квантового компьютера для решения БССУ не является эффективным. Предложенные в настоящей работе алгоритмы ЭЦП могут быть рассмотрены как кандидаты на прототипы практичных постквантовых стандартов ЭЦП. Их практичность связана с тем, что они обладают достаточно малыми размерами открытого ключа и подписи по сравнению с многочисленными известными постквантовыми алгоритмами. В рамках класса двухключевых криптосхем, использующих вычислительную трудность решения БССУ, алгебраические алгоритмы на КНАА свободны от существенного недостатка, чрезвычайно большого размера открытого ключа, который характерен криптоалгоритмам на трудно обратимых отображениях с секретной лазейкой.

Формула (3) обеспечивает принятие вектором $\mathbf{S}$ примерно p^3 различных обратимых значений в КНАА, используемой в качестве алгебраического носителя, что легко доказывается с использованием утверждений, доказанных в работе [23]. При этом эти значения распределяются по $\approx p^2$ различным коммутативным подалгебрам, на которые разбивается КНАА. Обоснование достаточности рандомизации, обеспечиваемое формулой (3) выполняется аналогично тому, как это сделано в [23]. Действительно, легко показать, что (3) сводится к формуле рандомизации подписи, использованной в [23], если учесть, что вектор, равный произведению $\mathbf{G}^k\mathbf{L}^u$, принимает значения в коммутативной группе порядка $p^2 - 1$. Достаточная полнота рандомизации подписи, обеспечиваемая формулой (3) показывает, что все три предложенных типовых алгоритма ЭЦП с двумя скрытыми группами являются стойкими к атакам на основе известных подписей, т.е. по совокупности известных подписей вычислительно невыполнимо нахождение секретных векторов $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{P}$ и $\mathbf{L}$.

Следует отметить, что выполнение трех операций возведения в степень в формуле (3) практически не приводит к увеличению вычислительной сложности шага вычисления подгоночного элемента подписи $\mathbf{S}$ по сравнению с аналогичным шагом в алгоритме из [23], поскольку каждый из векторов $\mathbf{G}$, $\mathbf{P}$ и $\mathbf{L}$ возводится в 128-битную степень, тогда как в [23] выполняются две операции экспоненциирования – в 128-битную и в 256-битную степень. Введение скалярного множителя в формулы для вычисления рандомизирующего вектора-фиксатора и элементов открытого ключа позволило использовать проверочное уравнение с операциями возведения только в 128-битную степень, тогда как в алгоритме-прототипе используются также и операции возведения в 256-битую степень. В целом достигается существенное повышение производительности процедуры верификации подписи.

В использованном механизме рандомизации принципиальным моментом является использование двух скрытых коммутативных групп, которые взаимно некоммутативны. Выбор вектора $\mathbf{P}'$, принадлежащего одной из скрытых групп задается выбором некоторых степеней t и v' $(0 < t < q$ и $0 < v' < q)$ и вычислением вектора $\mathbf{P}' = \mathbf{P}^t\mathbf{L}^{v'}$, а элемента $\mathbf{G}'$ из второй – выбором некоторых степеней k и v'' $(0 < k < p + 1$ и $0 < v'' < q)$ и вычислением вектора $\mathbf{G}' = \mathbf{G}^k\mathbf{L}^{v''}$. Элементы открытого ключа вычисляются как замаскированные элементы скрытых групп при использовании умножения слева и справа на секретные векторы (маскирующие множители), причем при вычислении элементов открытого ключа, над которыми выполняется операция экспоненциирования в проверочном уравнении, левый и правый маскирующие множители являются взаимно обратными. Выбор маскирующих множителей осуществляется таким образом, что при записи элементов открытого ключа в проверочном уравнении, выраженных как произведения наборов секретных векторов, все пары соседних маскирующих множителей сокращаются и образуется длинная цепочка множителей, с некоторой очередностью выбираемых их двух взаимно некоммутативных скрытых групп. Это легко заметить при рассмотрении доказательства корректности каждого из трех предложенных типовых алгоритмов ЭЦП с двумя скрытыми группами. При этом наличие чередования множителей, принадлежащих взаимно некоммутативным скрытым группам, представляется имеющим принципиальное значение для обеспечения стойкости к гипотетическим атакам на основе потенциально возможных эквивалентных ключей. Наличие указанного чередования обусловливает необходимость задания в схеме ЭЦП дополнительного подгоночного элемента подписи s, за счет которого обеспечивается возможность вычисления значений ЭЦП, удовлетворяющих проверочному уравнению. (В алгоритмах ЭЦП, сочетающих в себе два различных механизма обеспечения стойкости к подделке подписи, возникает необходимость задания второго дополнительного подгоночного элемента подписи σ). В алгебраических алгоритмах ЭЦП

Таблица 5.

Сравнение предложенных алгоритмов ЭЦП с известными аналогами на четырехмерных КНАА

Алгоритм	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
Первого типа	640	144	6600	9200	$>2^{100}$
Второго типа	512	112	6600	9200	$\approx 2^{100}$
Третьего типа	704	128	6530	7680	$\approx 2^{128}$
[17]	256	113	12300	9220	$<2^{80}$
[19]	768	160	49200	13800	$\approx 2^{80}$
[23]	512	144	9200	13800	$\approx 2^{100}$

с одной скрытой группой такой необходимости нет [17–19].

Прямой атакой на каждый из трех типовых разработанных алгебраических алгоритмов ЭЦП является решение системы векторных степенных уравнений, связывающих элементы открытого ключа с секретными векторами (элементами секретного ключа). Решение системы векторных степенных уравнений сводится к решению систем скалярных степенных уравнений. При этом знание декомпозиции четырехмерных КНАА с глобальной двухсторонней единицей на коммутативные подалгебры позволяет существенно уменьшить число скалярных степенных уравнений в решаемой БССУ, как это показано, например, в [23]. Применяя методику [23] оценивания стойкости к прямой атаке, были получены данные, представленные в табл. 5.

Наиболее близким аналогом для предложенных алгоритмов ЭЦП является описанный в работе [23]. В алгоритмах из работ [17] и [19], которые также уступают по производительности предложенным в настоящей статье, используется только одна скрытая коммутативная группа и рандомизация подписи является ограниченной, из-за чего имеет место уязвимость к атаке на основе известных подписей [20]. Эти сравнения показывают, что использованный прием выделения скалярного множителя $\mathbf{L}^u$ в формуле (3) и скалярного множителя $\mathbf{L}^v$ в формуле для вычисления рандомизирующего вектора-фиксатора $\mathbf{R}$ (см. п. 1 в процедурах генерации ЭЦП каждого из трех описанных типовых алгоритмов) позволяет существенно снизить вычислительную сложность процедур генерации и верификации ЭЦП и тем самым повысить производительность.

Естественным способом повышения уровня стойкости предложенных алгоритмов является их реализация на КНАА с размерностью $m > 4$, что приводит к существенному увеличению размера БССУ, сложность решения которых лежит в основе стойкости. Для случая $m = 6$ ($m = 8$) число совместно решаемых скалярных степенных уравнений возрастает в полтора (два) раза, что для алгоритма третьего типа соответствует уровню стойкости 2^{192} (2^{256}) к прямой атаке. Однако утверждение о решении проблемы разработки способов построения практичных постквантовых алгоритмов ЭЦП было бы преждевременным, поскольку, как показывает история многих известных криптосхем, требуются годы всесторонних исследований стойкости к различным возможным атакам до того, как криптосхемы нового типа признаются апробированными. Выполненные в данной работе разработки трех типовых алгебраических алгоритмов с двумя скрытыми группами являются шагом в направлении развития способа построения постквантовых схем ЭЦП, использующих в качестве алгебраического носителя КНАА. Достоинства алгебраических алгоритмов ЭЦП с двумя скрытыми группами представляются достаточным обоснованием для ожидания того, что в связи с актуальностью проблемы разработки практичного постквантового стандарта ЭЦП, они обусловят интерес к их анализу и использованию в качестве прототипов при разработке новых постквантовых схем ЭЦП со стороны независимых исследователей.

Выводы

Предложены три типа алгебраических алгоритмов ЭЦП с двумя скрытыми группами, отличающиеся различными механизмами обеспечения стойкости

к подделке подписи, в которых в качестве алгебраического носителя используются четырехмерные КНАА с операцией умножения, заданной по прореженным ТУБВ. Последнее является одним из использованных приемов повышения производительности алгоритмов. Второй использованный прием состоит в выделении скалярного множителя в формулах для вычисления подгоночного элемента ЭЦП, вектора-фиксатора и элементов открытого ключа, за счет чего обеспечивается возможность уменьшения (по сравнению с прототипом [23]) в два раза размера степеней операций экспоненциирования, выполняемых в процедурах генерации и верификации ЭЦП.

В качестве одного из дальнейших направлений развития постквантовых схем ЭЦП с двумя скрытыми группами является изучение особенностей их реализации на КНАА, обладающих размерностью размерности $m = 6$ и более.

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

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. 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.
3. Vedenev K.. Kosolapov Yu. Code-based cryptography // Lecture Notes in Computer Science. 2023. Vol. 14311. P. 35–55. DOI: 10.1007/978-3-031-46495-9_3.
4. D'Alconzo G. On two modifications of the McEliece PKE and the CFS signature scheme // International Journal of Foundations of Computer Science. 2024. Vol. 35. N. 5. P. 501–512. DOI: 10.1142/S0129054123500132.
5. 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.
6. 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.
7. Li L., Lu X., Wang K. Hash-based signature revisited // Cybersecurity. 2022. V. 5. No. 13. https://doi.org/10.1186/s42400-022-00117-w.
8. 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.
9. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. Vol. 80. P. 7–23. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2.
10. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, 2021. Vol. 33. P. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
11. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. Vol. 93. No. 2. P. 3–10.
12. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.

18. 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.
19. 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.
20. Молдовян А. А., Молдовян Д. Н., Костина А. А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.
21. 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.
22. Moldovyan A. A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1, pp. 95–108. https://doi.org/10.56415/qrs.v32.08.
23. 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.
24. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T. (2024). Decomposition of Quaternion-Like Algebras into a Set of Commutative Subalgebras. In: Dang, T. K., Küng, J., Chung, T. M. (eds) Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2024. Communications in Computer and Information Science, vol 2310, p. 119–131. Springer, Singapore. https://doi.org/10.1007/978-981-96-0437-1_9.
25. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. Vol. 27. No. 2, pp. 293–308.
26. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018. vol. 26, no. 2. P. 263–270.
27. Duong M. T., Moldovyan D. N., Do B. V., 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.
28. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix 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.
29. 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.

ALGEBRAIC SIGNATURE ALGORITHMS WITH TWO HIDDEN GROUPS

Moldovyan N. A.[3], Petrenko A. S.[4]

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

Purpose of work *is improving the performance of post-quantum algebraic signature algorithms based on the computational difficulty of solving large systems of power equations.*

Research methods: *the use of two hidden commutative groups, the elements of one of which are non-commutative with the other, to ensure sufficient completeness of signature randomization in algebraic signature schemes, the security of which is based on the computational difficulty of solving large systems of power equations in the ground finite field* $GF(p)$*. Calculation of the fitting signature in the form of a vector* $\mathbf{S}$ *depending on mutually non-commutative non-scalar vectors selected from hidden groups and a random scalar vector. The use of finite non-commutative associative algebras (FNAA) with a well-studied structure as an algebraic carrier of signature algorithms with a verification equation with multiple occurrences of the vector* $\mathbf{S}$*. Defining the FNAAs by the sparse basic vector multiplication tables.*

Results of the study: *three types of post-quantum algebraic signature schemes are proposed, differing in techniques for ensuring high security to the forging signature attacks using vector* $\mathbf{S}$ *as a fitting parameter of the attacks. The first type uses the technique of exponentiating the product, which includes vector* $\mathbf{S}$*, to a large degree, the second type uses the exponentiation operation to a power equal to the value of the hash function calculated from* $\mathbf{S}$*, and the third type uses the combination of the first two techniques. Algorithmic implementations of signature schemes of each type are carried out*

3 Nikolay A. Moldovyan, Doctor of technical sciences, professor, Chief researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: moldovan.NA@talantiuspeh.ru

4 Alexei S. Petrenko, PhD student of Saint Petersburg State Electrotechnical University «LETI», St. Petersburg, Russia, junior researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

and the correctness of the developed algorithms is shown. Security to direct attack, to attack based on known signatures, and to signature forgery was assessed. A comparison of the proposed signature algorithms with known analogues is presented. The multiplication by a scalar vector when calculating vector $\mathbf{S}$ *and setting the FNAAs by the sparse basis vector multiplication tables are used as techniques for improving the performance of algebraic signature algorithms.*

Practical relevance: *the significance of the results of the article consists in testing a method for enhancing signature randomization, including calculating the signature fitting element* $\mathbf{S}$ *depending on the product of two non-commutative vectors, while developing algebraic algorithms of three different types, which are of interest as a prototype of a practical post-quantum signature standard.*

The results were obtained *with the financial support of the project «Technologies for countering previously unknown quantum cyber threats», implemented within the framework of the state program of the «Sirius» Federal Territory «Scientific and technological development of the «Sirius» Federal Territory (Agreement No. 23-03 dated September 27, 2024).*

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. 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.
3. Vedenev K.. Kosolapov Yu. Code-based cryptography // Lecture Notes in Computer Science. 2023. Vol. 14311. P. 35–55. DOI: 10.1007/978-3-031-46495-9_3.
4. D'Alconzo G. On two modifications of the McEliece PKE and the CFS signature scheme // International Journal of Foundations of Computer Science. 2024. Vol. 35. N. 5. P. 501–512. DOI: 10.1142/S0129054123500132.
5. 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.
6. 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.
7. Li L., Lu X., Wang K. Hash-based signature revisited // Cybersecurity. 2022. V. 5. No. 13. https://doi.org/10.1186/s42400-022-00117-w.
8. 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.
9. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. Vol. 80. P. 7–23. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2.
10. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, 2021. Vol. 33. P. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
11. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. Vol. 93. No. 2. P. 3–10.
12. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. Moldovjan A.A., Moldovjan N.A. Algoritmy JeCP na konechnyh nekommutativnyh algebrah nad poljami harakteristiki dva // Voprosy kiberbezopasnosti. 2022. № 3(49). S. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
19. 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.
20. Moldovjan A.A., Moldovjan D.N., Kostina A.A. Algebraicheskie algoritmy JeCP s polnoj randomizaciej podpisi // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.

21. 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.
22. Moldovyan A. A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1, pp. 95–108. https://doi.org/10.56415/qrs.v32.08.
23. 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.
24. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T. (2024). Decomposition of Quaternion-Like Algebras into a Set of Commutative Subalgebras. In: Dang, T. K., Küng, J., Chung, T. M. (eds) Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2024. Communications in Computer and Information Science, vol 2310, p. 119–131. Springer, Singapore. https://doi.org/10.1007/978-981-96-0437-1_9.
25. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. Vol. 27. No. 2, pp. 293–308.
26. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018. vol. 26, no. 2. P. 263–270.
27. Duong M. T., Moldovyan D. N., Do B. V., 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.
28. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix 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.
29. 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.