ПОСТКВАНТОВЫЙ АЛГЕБРАИЧЕСКИЙ АЛГОРИТМ ЭЦП С ТРЕМЯ СКРЫТЫМИ ГРУППАМИ

Молдовян А. А.[1]

DOI: 10.21681/2311-3456-2025-5-78-87

Цель работы: *создание дополнительных предпосылок для разработки постквантового стандарта на алгоритмы ЭЦП, основанные на вычислительной сложности решения больших систем нелинейных уравнений (БСНУ) в конечном поле.*

Метод исследования: *применение трех скрытых коммутативных групп, элементы каждой из которых некоммутативны с элементами другой, для реализации усиленной рандомизации подписи в алгебраических схемах ЭЦП, стойкость которых базируется на вычислительной трудности решения БСНУ в простом конечном поле $GF(p)$. Вычисление подгоночного элемента подписи в виде матрицы* $\mathbf{S}$ *в зависимости от трех попарно некоммутативных матриц, выбираемых случайным образом из скрытых групп. Применение конечных алгебры матриц 3×3 и 5×5, заданных над полем $GF(p)$ с 64-битным и 40-битным простым порядком p.*

Результаты исследования: *предложен новый механизм усиленной рандомизации подгоночного элемента подписи и разработан алгебраический алгоритм ЭЦП, перспективный в качестве прототипа практичного постквантового стандарта ЭЦП. Выбор случайных матриц из скрытых групп задается посредством возведения генераторов соответствующих скрытых групп в случайные степени, вычисляемые в зависимости от параметров рандомизации и рандомизирующего элемента ЭЦП. Впервые для повышения уровня стойкости к потенциальным атакам на основе альтернативных секретных ключей указанные степени вычисляются как решение системы линейных уравнений. Представлены оценки стойкости к прямой атаке и атаке на основе известных подписей. Приведено сравнение параметров разработанного алгоритма ЭЦП с известными алгоритмами, использующими трудность решения БСНУ, и обсуждаются способы повышения его производительности.*

Научная и практическая значимость *полученных результатов заключается в создании новой предпосылки для обоснования выбора алгебраических алгоритмов ЭЦП со скрытыми группами в качестве основы для разработки практичного постквантового стандарта ЭЦП, состоящей в повышении уровня стойкости к потенциальным атакам на основе эквивалентных ключей.*

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

Введение

В ходе технического прогресса возрастает значение электронной цифровой подписи (ЭЦП), которая имеет важную роль в современных информационных технологиях, применяемых в различных сферах общественной деятельности. Существующие стандарты на алгоритмы ЭЦП основаны на вычислительной трудности задачи факторизации (ЗФ) и задачи дискретного логарифмирования (ЗДЛ). Последние результаты в области квантовых вычислений дают основание для прогнозирования появления в ближайшем будущем практически доступного квантового компьютера, на котором ЗФ и ЗДЛ будут решаться за полиномиальное время. С этого момента криптографические алгоритмы с открытым ключом, стойкость которых ограничена сверху вычислительной сложностью ЗФ и ЗДЛ, включая действующие стандарты ЭЦП, перестают быть безопасными. Такая ситуация делает актуальной задачу разработки постквантовых двухключевых криптоалгоритмов и стандартов на их основе, которые являются стойкими к атакам с использованием квантовых компьютеров. Исследования в этом направлении относятся к постквантовой криптографии, тематика которой привлекает внимание и усилия многих исследователей [1–3]. Для обеспечения стойкости к атакам с использованием квантовых компьютеров разрабатываемые криптоалгоритмы должны базироваться на вычислительно трудных задачах, отличных от ЗФ и ЗДЛ. Переход к задачам другого типа обусловил существенный рост размеров открытого ключа и подписи, что поднимает вопрос о практичности использования постквантовых криптоалгоритмов с открытым ключом (в смысле снижения объемов оперативной памяти и количества вычислительных операций, т.е. издержек их практического применения).

В области постквантовой криптографии значительное внимание уделяется разработке алгоритмов открытого шифрования и ЭЦП на трудно обратимых отображениях с секретной лазейкой [4–8]. Стойкость таких алгоритмов основана на вычислительной сложности решения больших систем нелинейных уравнений (БСНУ), заданных над конечным полем

1 Молдовян Александр Андреевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0000-0001-5480-6016. E-mail: maa1305@yandex.ru

сравнительно малого порядка. Для нахождения решений БСНУ квантовый компьютер не является эффективным, что обеспечивает постквантовую стойкость разрабатываемых криптоалгоритмов. Несмотря на достаточно большое число разработанных алгоритмов ЭЦП такого типа, не удалось решить проблему чрезвычайно большого размера открытого ключа (от десятков килобайт до нескольких мегабайт в зависимости от уровня стойкости). Даже сравнительно новая парадигма построения криптоалгоритмов на трудно обратимых отображениях с секретной лазейкой дает только ограниченное решение данной проблеме [9–11].

Принципиально новый подход к использованию вычислительной сложности решения БСНУ связан с разработкой алгебраических алгоритмов со скрытой коммутативной группой [12–15]. Эти алгоритмы относятся к рандомизированным схемам ЭЦП, в которых подпись $(e, \mathbf{S})$ генерируется в зависимости от предварительно генерируемых случайных натуральных чисел и включает два элемента: 1) случайное число e (рандомизирующий элемент ЭЦП) и 2) элемент конечной алгебры $\mathbf{S}$, используемой в качестве алгебраического носителя (подгоночный элемент ЭЦП). При этом проверочное уравнение включает $\mathbf{S}$ два или более раза в качестве множителя. Формируемое в процессе генерации подписи значение e является уникальным, обусловливая уникальность значения $\mathbf{S}$. Однако в отличии от рандомизированных схем ЭЦП, стойкость которых основана на вычислительной сложности ЗДЛ или скрытой ЗДЛ [16–18], для рассматриваемых алгоритмов рандомизация ЭЦП является ограниченной (в смысле того, что $\mathbf{S}$ принимает значения из подмножества Ψ обратимых элементов алгебры, используемой в качестве алгебраического носителя, мощность которого ψ намного меньше порядка Ω мультипликативной группы алгебры).

Как показано в статьях [19, 20], ограниченность рандомизации создает предпосылки для осуществления атаки на основе известных подписей (атака A1), которая состоит в вычислении элементов секретного ключа по некоторому набору известных подписей путем решения некоторой БСНУ, включающие уравнения, записываемые по формуле для вычисления подгоночного значения $\mathbf{S}$. При этом прямая атака на алгебраические алгоритмы со скрытой группой состоит в решении БСНУ, которая составляется по формулам генерации элементов открытого ключа в зависимости от элементов секретного ключа (атака A2). Атака A1 позволяет вычислить только часть секретного ключа, однако это позволяет существенно уменьшить вычислительную сложность атаки A2, т.е. снизить уровень стойкости алгоритма ЭЦП. Если сложность атаки A1 превышает сложность атаки A2, то используемый механизм рандомизации может рассматриваться приемлемым (достаточным) для данного конкретного алгебраического алгоритма ЭЦП (критерий достаточной полноты рандомизации по [21, 22]). В качестве количественной меры достигаемого уровня рандомизации в заданном алгоритме можно принять значение отношения $\log_2\Omega$ к разности $\log_2\Omega - \log_2\Psi$, а термин «усиление рандомизации» – трактовать как повышение уровня рандомизации при разработке нового механизма рандомизации ЭЦП. Следует отметить, что выполнение критерия достаточной полноты рандомизации не привязано к некоторому пороговому значению уровня рандомизации и требует рассмотрения вычислительной сложности атак A1 и A2 для конкретного алгебраического алгоритма ЭЦП. Тем не менее, усиление рандомизации можно трактовать как «приближение» к выполнению критерия полноты рандомизации.

Способ получения оценки стойкости к атаке A1 детально рассматривается в работах [21, 22], в которых в частности показано, что обеспечение полноты рандомизации подгоночного элемента $\mathbf{S}$ путем его вычисления в зависимости от случайного элемента $\mathbf{V}$, выбираемого из мультипликативной группы используемого алгебраического носителя, не приводит автоматически к достаточной полноте рандомизации ЭЦП, поскольку для корректности схемы ЭЦН элемент $\mathbf{V}$ должен входить в качестве множителя также и в формулу для вычисления вектора-фиксатора $\mathbf{R}$ при генерации ЭЦП. При этом значение $\mathbf{R}$ вычисляется в процессе верификации ЭЦП (т.е. $\mathbf{V}$ для данной известной подписи входит в качестве неизвестной в два независимых векторных уравнения). Для усиления рандомизации в схемах ЭЦП с удвоенным проверочным уравнением в работе [21] впервые применены две скрытые группы и вычисление элемента $\mathbf{S}$ в зависимости от двух случайных элементов, выбираемых из разных скрытых групп. В работе [22] эта идея использована для разработки алгоритма ЭЦП с одним проверочным уравнением, удовлетворяющего упомянутому критерию достаточной полноты рандомизации.

Механизм рандомизации, включающий вычисление элемента $\mathbf{S}$ в зависимости от случайного значения $\mathbf{V}$, при разработке алгоритма ЭЦП требует использования удвоенного проверочного уравнения, приводящего к существенному снижению производительности процедур генерации и верификации ЭЦП. По этой причине с практической точки зрения больший интерес представляют механизмы рандомизации [22], реализуемые в рамках схем ЭЦП с одним поверочным уравнением, в которое элемент $\mathbf{S}$ входит многократно (два и более раза).

В работах предложены механизмы рандомизации, использующие две скрытые циклические группы, элементы одной из которых некоммутативны с элементами другой. Данный механизм может быть представлен следующей формулой для вычисления подгоночного элемента подписи $\mathbf{S}$:

$$\mathbf{S} = \mathbf{D}\mathbf{P}^{b}\mathbf{G}^{n}\mathbf{F}, \quad (1)$$

где $\mathbf{D}$ и $\mathbf{F}$ – элементы секретного ключа; $\mathbf{P}$ и $\mathbf{G}$ – генераторы скрытых групп; b и n – случайные натуральные степени. Использование случайного выбора элементов из двух скрытых групп обеспечивает существенное увеличение параметра ψ, за счет чего повышается уровень рандомизации. В разработанных на основе формулы (1) алгоритмах ЭЦП [22], использующих четырехмерные конечные некоммутативные ассоциативные алгебры в качестве алгебраического носителя, выполняется критерий достаточной полноты рандомизации при обеспечении уровня стойкости 2^{100}. Разработка алгоритмов ЭЦП с двумя скрытыми группами потребовала использования одного или двух дополнительных подгоночных элементов в виде натуральных чисел, входящих в проверочное уравнение как степени при некоторых элементах открытого ключа, присутствующих в уравнении верификации ЭЦП.

Логическим расширение такого приема усиления рандомизации является переход к механизму, включающему случайный выбор элементов из трех скрытых циклических групп и описываемому следующей формулой:

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

где $\mathbf{D}$ и $\mathbf{F}$ – элементы секретного ключа; $\mathbf{P}$, $\mathbf{G}$ и $\mathbf{J}$ – генераторы скрытых групп, таких, что элементы каждой из них некоммутативны с элементами двух других; b, n и d – случайные натуральные степени. Достаточно очевидно, что это расширение дает существенное увеличение уровня рандомизации и потенциальную возможность разработки алгоритмов ЭЦП, удовлетворяющих критерию достаточной полноты рандомизации подписи при обеспечиваемом уровне стойкости 2^{192} и более и сохраняющих высокую производительность процедур генерации и верификации ЭЦП. Однако, разработка алгоритмов ЭЦП на основе формулы (2) требует применения новых конструктивных приемов.

Целью настоящей работы является создание дополнительных предпосылок, дающих обоснование целесообразности разработки проекта постквантового стандарта ЭЦП на основе алгебраических алгоритмов ЭЦП, основанных на вычислительной сложности решения БСНУ, что потенциально позволит принять практичный с точки зрения размеров открытого ключа и подписи и производительности стандарт ЭЦП для применения в постквантовую эру. В качестве таких дополнительных предпосылок предполагается разработка алгоритма, обладающего стойкость 2^{192} и 2^{256} в различных его модификациях, и расширение множества приемов построения алгоритмов ЭЦП со скрытыми группами.

Для достижения этой цели применяется механизм рандомизации, описываемый формулой (2), и применяются новые конструктивные приемы разработки алгоритма ЭЦП, реализующего этот механизм при выполнении критерия достаточной полноты рандомизации.

Основные приемы, используемые при разработке алгоритма ЭЦП

1. В качестве основного механизма для предотвращения подделки подписи на основе решения проверочного уравнения относительно неизвестного значения $\mathbf{S}$ предполагается использовать значение хеш-функции Φ от $\mathbf{S}$ в качестве степени одной из операций экспоненцирования, присутствующих в проверочном уравнении. Данный прием ранее использован в работах [21, 22]. Его алгоритмическая реализация предполагает использование вспомогательного подгоночного элемента подписи в виде натурального числа s, поскольку значение степени $\rho = \Phi(\mathbf{S})$ является псевдослучайным и становится известным только после фиксирования значения подгоночного элемента $\mathbf{S}$.

2. Задается двухкратное вхождение в проверочное уравнение элемента $\mathbf{S}$ как множителя первой степени. Многократное вхождение в уравнение верификации элемента $\mathbf{S}$ без его возведения в большую степень, не может обеспечить приемлемую стойкость к подделке подписи, поэтому использование второго конструктивного приема становится возможным только одновременно с первым.

3. В используемой для вычисления значения $\mathbf{S}$ формуле (2) в качестве генератора циклической группы $\mathbf{G}$ выбирается произведение $\mathbf{J}^{x}\mathbf{P}^{z}$ (где $\mathbf{P}$ и $\mathbf{J}$ – обратимые матрицы, удовлетворяющие условию $\mathbf{JP} \neq \mathbf{PJ}$) с секретными степенями x и z. Третий прием требует выполнения переборной процедуры, состоящей в подборе таких степеней x и z, при которых порядок матрицы $\mathbf{G} = \mathbf{J}^{x}\mathbf{P}^{z}$ имеет достаточно большой размер. Благодаря тому, что доля матриц большого порядка является преобладающей, указанная процедура незначительно увеличивает вычислительную сложность процесса формирования открытого и секретного ключей. Выполнимость требуемых условий $\mathbf{GP} \neq \mathbf{PG}$ и $\mathbf{GJ} \neq \mathbf{JG}$ является достаточно очевидной.

Используемый алгебраический носитель

В известных алгоритмах ЭЦП со скрытой группой в качестве алгебраического носителя используются m-мерные конечные некоммутативные ассоциативные алгебры (КНАА), обычно заданные над конечным

полем нечетной характеристики $GF(p)$, а в отдельных случаях характеристики два [23]. При этом более детальный анализ стойкости к атакам А1 и А2 выполнен для случая использования четырехмерных КНАА, поскольку в этом анализе существенно используется возможность описания координат векторов из скрытой группы по координатам некоторого представителя скрытой группы и значениям η ($\eta < m$) скалярных переменных. Для задания КНАА произвольных четных размерностей известны унифицированные способы их задания [24, 25], причем с ростом значения размерности m ожидается существенное повышение стойкости алгебраических алгоритмов, основанных на вычислительной трудности решения БСНУ. Однако, для размерностей $m > 4$ строение КНАА, заданных по способам [24, 25], является мало изученным, что не позволяет получить приемлемых оценок стойкости.

В работе [26] возможность разработки алгоритма ЭЦП на КНАА большой размерности $m = 9$ и получения приемлемых оценок стойкости, в качестве КНАА используется конечная алгебра матриц 3×3, заданная над простым полем $GF(p)$ с 80-битной характеристикой p. Действительно, легко видно, что умножение матриц размера $\mu\times\mu$ может быть представлено как умножение векторов размерности $m = \mu^2$, заданное по таблице умножения базисных векторов специального вида (см. [26] для случая $\mu = 3$).

В настоящей работе в качестве алгебраического носителя разрабатываемого постквантового алгоритма ЭЦП используется конечная алгебра матриц, заданная над полем $GF(p)$ с 64-битной характеристикой p и алгоритмы генерации матриц требуемого порядка, описанные в [26]. Для задания более высокого уровня стойкости предполагается реализация разработанного алгоритма на алгебре матриц 5×5, заданной над полем $GF(p)$ с 40-битной характеристикой p. Более высокий уровень стойкости обеспечивается существенным возрастанием числа уравнений в БСНУ, задача решения которой возникает в атаках А1 и А2.

Далее в статье вместо термина «элементы матриц» будем использовать термин «координаты матриц», резервируя слово «элементы» для использования терминов «элементы (конечного) поля» и «элементы открытого (секретного) ключа».

1. Разработанный алгоритм ЭЦП

Формирование секретного и открытого ключей

Предлагается разработка двух вариантов алгоритма ЭЦП, отличающихся тем, что в первом варианте используется в качестве алгебраического носителя конечная алгебра матриц 3×3, заданная над полем $GF(p)$ с 64-битной характеристикой p, а во втором – алгебра матриц 5×5, заданная над полем $GF(p)$ с 40-битным простым числом p. Для первого варианта используется такое простое число p, что число $q = p^2 + p + 1$ также является, а для второго варианта – простое число p, при котором имеем простое значение $q = p^4 + p^3 + p^2 + p + 1$. Учитывая формулу для порядка Ω мультипликативной группы алгебры матриц размера $n\times n$, выражающую Ω через значения p и n (см., например, формулу (5) в [26]), легко показать существование матриц порядка q первого и второго случаев. Из указанной формулы легко установить возможные значения порядков матриц. При этом в [26] показано, что вычислительная сложность процедур генерации нужного простого значения p и матрицы порядка q для первого случая является сравнительно низкой. По аналогии с рассуждениями [26] легко показать, что во втором случае вычислительная сложность упомянутых процедур также является приемлемой для их использования в алгоритмах генерации секретного и открытого ключей. Обе версии разработанного алгоритма описываются одинаковыми математическими формулами.

Для генерации секретного ключа выбираются случайные натуральные числа $u < q$, $v < q$, $w < q$, $x < q$, $y < q$ и $z < q$ и случайные обратимые (невырожденные) нескалярные матрицы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{J}$ и $\mathbf{P}$, которые являются попарно некоммутативными, а матрицы $\mathbf{J}$ и $\mathbf{P}$ имеют одинаковый порядок q. Размер секретного ключа равен 528 (870) байт для первой (второй) версии алгоритма ЭЦП. При генерации ЭЦП используется вспомогательная секретная матрица $\mathbf{G}$, которая вычисляется по следующей формуле

$$\mathbf{G} = \mathbf{J}^x\mathbf{P}^z. \quad (3)$$

Формула (3) учитывается при генерации случайных положительных значений $x < q$ и $z < q$. Легко показать, что для любой пары значений $x > 0$ и $z > 0$ вычисляемая матрица $\mathbf{G}$ будет некоммутативным с каждой из матриц $\mathbf{J}$ и $\mathbf{P}$. При генерации различных пар значений (x, z) определяется значение порядка $\omega(\mathbf{G})$ матрицы $\mathbf{G}$ и в качестве элементов секретного ключа фиксируются значения x и z, при которых $\omega(\mathbf{G})$ является нечетным числом.

Открытый ключ формируется в виде набора из семи матриц ($\mathbf{Q}$, $\mathbf{U}$, $\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$), элементы которого вычисляются по следующим формулам:

$$\mathbf{Q} = \mathbf{B}\mathbf{J}^z\mathbf{B}^{-1};\ \mathbf{U} = \mathbf{F}^{-1}\mathbf{J}\mathbf{F};\ \mathbf{Y} = \mathbf{A}\mathbf{P}\mathbf{A}^{-1};\ \mathbf{Z} = \mathbf{D}\mathbf{P}^x\mathbf{D}^{-1}; \quad (4)$$

$$\mathbf{T}_1 = \mathbf{A}^{-1}\mathbf{P}^u\mathbf{D}^{-1};\ \mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{J}^u\mathbf{P}^w\mathbf{D}^{-1};\ \mathbf{T}_3 = \mathbf{F}^{-1}\mathbf{1}\mathbf{J}^v\mathbf{B}^{-1}. \quad (5)$$

Суммарный размер открытого ключа равен 504 (875) байт для первой (второй) версии алгоритма ЭЦП. В формулах (3) и (4) можно было бы использовать различные значения степеней x и z, однако этот вариант несколько увеличивает размер секретного ключа, но не влияет на оценку стойкости алгоритма.

В процедурах генерации и верификации ЭЦП используется некоторая специфицированная коллизионно стойкая 256-битная хеш-функции Φ, которая является частью рассматриваемого алгоритма ЭЦП.

Алгоритм генерации ЭЦП

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < q$, $t < q$ и $r < q$ и вычислить значение рандомизирующей матрицы $\mathbf{R}$ по формуле:

$$\mathbf{R} = \mathbf{A}\mathbf{P}^{t}\mathbf{G}^{k}\mathbf{J}^{r}\mathbf{B}^{-1}. \quad (6)$$

2. Вычислить хеш-значение от матрицы $\mathbf{R}$ с присоединенным к нему документом M: $e = e_1||e_2 = \Phi(M, \mathbf{R})$, где 256-битное хеш-значение e представлено в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.

3. Вычислить натуральное число d:

$$d = x - e_2 - u \bmod q. \quad (7)$$

4. Вычислить натуральные числа σ и b (удовлетворяющие одновременно уравнениям $\sigma + u + xe_1 + b = t$ и $w + x\sigma + b = z \bmod q$):

$$\sigma = (1 - x)^{-1}(t - xe_1 - u - z + w) \bmod q; \quad (8)$$

$$b = z - w - x\sigma \bmod q. \quad (9)$$

5. Вычислить натуральное число n:

$$n = 2^{-1}(k - 1) \bmod \omega(\mathbf{G}). \quad (10)$$

6. Вычислить матрицу $\mathbf{S} = \mathbf{D}\mathbf{P}^{b}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F}$.

7. Вычислить хеш-значение $\rho = \rho_1||\rho_2 = \Phi(\mathbf{S}, e)$, где значение ρ представлено в виде конкатенации двух 128-битных натуральных чисел ρ_1 и ρ_2.

8. Вычислить вспомогательный подгоночный элемент ЭЦП в виде натурального числа s:

$$s = z^{-1}(r - d - v - \rho_1) - \rho_2 \bmod q. \quad (11)$$

Сгенерированная подпись представляет собой четверку значений $(e, \sigma, s, \mathbf{S})$ с суммарным размером 136 (197) байт для первой (второй) версии алгоритма ЭЦП. Вычислительную трудность алгоритма генерации ЭЦП можно оценить как три операции возведения в степень в конечной алгебре матриц (вычисление матриц $\mathbf{P}^{t}$, $\mathbf{G}^{k}$, $\mathbf{J}^{d}$), что составляет ≈15500 (90000) операций умножения в поле $GF(p)$ для первой (второй) версии алгоритма. Учитывая, что в первой версии алгоритма используется 64-битное простое число p, а во второй – 40-битое, легко видеть, что производительность второй версии примерно в 2,3 раза меньше.

Алгоритм верификации ЭЦП

Верификация подписи $(e, \sigma, s, \mathbf{S})$ к документу M выполняется по открытому ключу $(\mathbf{Q}, \mathbf{U}, \mathbf{Y}, \mathbf{Z}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$ с использованием следующего алгоритма:

1. Вычислить хеш-значение $\rho = \rho_1||\rho_2 = \Phi(\mathbf{S}, e)$.

2. Вычислить матрицу $\mathbf{R}'$ по следующему проверочному уравнению:

$$\mathbf{R}' = \mathbf{Y}^{\sigma}\mathbf{T}_1\mathbf{Z}^{e_1}\mathbf{S}\mathbf{U}^{e_2}\mathbf{T}_2\mathbf{Z}^{\sigma}\mathbf{S}\mathbf{U}^{\rho_1}\mathbf{T}_3\mathbf{Q}^{s+\rho_2}. \quad (12)$$

3. Вычислить хеш-функцию от матрицы $\mathbf{R}'$ с присоединенным к нему документом M: $\varepsilon = \varepsilon_1||\varepsilon_2 = \Phi(\mathbf{R}', M)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.

4. При справедливости равенств $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$ ЭЦП делается вывод о подлинности подписи, в противном случае – о ложности.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как шесть операций экспоненцирования в конечной алгебре матриц. что составляет ≈31000 (180000) операций умножения в поле $GF(p)$ для первой (второй) версии алгоритма.

Корректность разработанного алгоритма

Корректность предложенного алгоритма ЭЦП можно показать, выполняя подстановку в уравнении (12) матриц $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{T}_1$, $\mathbf{T}_2$ и $\mathbf{T}_3$, выраженных через элементы секретного ключа по формулам (4) и (5):

$$\mathbf{R}' = (\mathbf{A}\mathbf{P}\mathbf{A}^{-1})^{\sigma}\,\mathbf{A}^{-1}\mathbf{P}^{u}\mathbf{D}^{-1}(\mathbf{D}\mathbf{P}^{x}\mathbf{D}^{-1})^{e_1} \times$$
$$\times (\mathbf{D}\mathbf{P}^{b}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F})\,(\mathbf{F}^{-1}\mathbf{J}\mathbf{F})^{e_2}\,\mathbf{F}^{-1}\mathbf{J}^{u}\mathbf{P}^{w}\mathbf{D}^{-1}(\mathbf{D}\mathbf{P}^{x}\mathbf{D}^{-1})^{\sigma} \times$$
$$\times (\mathbf{D}\mathbf{P}^{b}\mathbf{G}^{n}\mathbf{J}^{d}\mathbf{F})(\mathbf{F}^{-1}\mathbf{J}\mathbf{F})^{\rho_2}\,\mathbf{F}^{-1}\mathbf{J}^{v}\mathbf{B}^{-1}(\mathbf{B}\mathbf{J}^{z}\mathbf{B}^{-1})^{s+\rho_2} =$$
$$= \mathbf{A}\mathbf{P}^{\sigma+u+xe_1+b}\mathbf{G}^{n}\mathbf{J}^{d+e_1+u} \times \mathbf{P}^{w+x\sigma+b}\mathbf{G}^{n}\mathbf{J}^{d+x+\rho_1+z(s+\rho_2)}\mathbf{B}^{-1}.$$

Заменяя в последнем уравнении значения d, σ, b, n и s правой частью соответствующих формул (7)–(11) и учитывая равенство (3), получаем:

$$\mathbf{R}' = \mathbf{A}\mathbf{P}^{t}\mathbf{G}^{n}\mathbf{J}^{x}\mathbf{P}^{z}\mathbf{G}^{n}\mathbf{J}^{r}\mathbf{B}^{-1} = \mathbf{A}\mathbf{P}^{t}\mathbf{G}^{2n+1}\mathbf{J}^{r}\mathbf{B}^{-1} =$$
$$= \mathbf{A}\mathbf{P}^{t}\mathbf{G}^{k}\mathbf{J}^{r}\mathbf{B}^{-1} = \mathbf{R}.$$

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

2. Обсуждение стойкости

В основе стойкости разработанного алгоритма лежит вычислительная сложность решения БСНУ. В случае прямой атаки (атака А2) БСНУ записывается по формулам (4) и (5), связывающем матрицы секретного ключа (неизвестные) с элементами открытого ключа. Если степени u, v, w, x, y и z принять как неизвестные, то будем иметь систему степенных и экспоненциальных матричных уравнений. Чтобы свести атаку А1 к решению системы, включающих только степенные матричные уравнения, в формулах (4) и (5) значения $\mathbf{J}^{z}$, $\mathbf{J}^{u}$ и $\mathbf{J}^{v}$ следует рассматривать как неизвестные матрицы, выбираемые из коммутативной скрытой группы, генерируемой матрицей $\mathbf{J}$,

а значения $\mathbf{P}^x$, $\mathbf{P}^u$ и $\mathbf{P}^w$ – как неизвестные матрицы, выбираемые из коммутативной скрытой группы, генерируемой матрицей $\mathbf{P}$. В статье [26] приводится обоснование, того, что координаты матриц 3×3, выбираемых из коммутативной группы могут быть описаны по координатам известной нескалярной матрицы (представителя коммутативной группы), содержащейся в этой группе, и $\eta = \mu$ ($\mu = 3$) скалярным переменным, т.е. толкование каждой из матриц $\mathbf{J}^z$, $\mathbf{J}^u$, $\mathbf{J}^v$. $\mathbf{P}^x$, $\mathbf{P}^u$ и $\mathbf{P}^w$ в качестве матричной неизвестной дает μ уникальных скалярных неизвестных при сведении решения системы матричных уравнений к системе скалярных уравнений (уравнений в поле $GF(p)$). По аналогии со случаем алгебры матриц 3×3 можно показать, что координаты матриц, содержащихся в заданной коммутативной группе конечной алгебры матриц 5×5 описываются по координатам нескалярного представителя этой группы и $\eta = \mu = 5$ скалярным переменным.

При таком толковании повышается степень матричных уравнений в БСНУ, однако повышением вычислительной сложности решения БСНУ за счет этого момента не будем принимать во внимание при выполнении оценки стойкости разработанного алгоритма ЭЦП (сложность решения БСНУ несущественно увеличивается за счет увеличения степени некоторых уравнений). Каждая из матричных неизвестных $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{J}$ и $\mathbf{P}$ дает μ^2 скалярных неизвестных, а каждая из матричных неизвестных $\mathbf{J}^z$, $\mathbf{J}^u$, $\mathbf{J}^v$. $\mathbf{P}^x$, $\mathbf{P}^u$ и $\mathbf{P}^w$ – μ скалярных неизвестных. Всего в скалярной БСНУ получаем $6\mu^2 + 6\mu$ неизвестных и $7\mu^2$ уравнений. Для случая, когда число уравнений превышает число неизвестных, сложность решения БСНУ может быть оценена по числу степенных уравнений, содержащихся в БСНУ. В этом случае с учетом оценок [4] получаем значение уровня стойкости разработанного алгоритма к атаке A2, равное 2^{192} для первой версии ($\mu = 3$) и 2^{256} – для второй версии ($\mu = 5$) разработанного алгоритма.

Применяя способ оценивания стойкости к атаке на основе известных подписей (атака A1), описанный в [21, 22], получаем следующее. В рамках атаки A1 уравнения, записываемые по формуле (2), и уравнения, записываемые по формуле (6), образуют две независимые и похожие системы степенных уравнений. Поэтому для оценки сложности атаки A1 достаточно рассмотреть только одну из них, например, относящуюся к формуле (2). Последняя задает для первой из N известных подписей пять фиксированных матричных неизвестных $\mathbf{D}$, $\mathbf{P}^{b_1}$, $\mathbf{G}^{n_1}$, $\mathbf{J}^{d_1}$ и $\mathbf{F}$. Действительно, неизвестные $\mathbf{D}$ и $\mathbf{F}$ присутствуют в уравнении, составляемом по формуле (2) для каждой известной подписи, а неизвестные $\mathbf{P}^{b_1}$, $\mathbf{G}^{n_1}$ и $\mathbf{J}^{d_1}$ фиксируют представителей трех неизвестных коммутативных групп. Для каждой i-й подписи ($i = 2, 3, \ldots, N$) выбор случайных значений $\mathbf{P}^{b_1}$, $\mathbf{G}^{n_1}$ и $\mathbf{J}^{d_1}$ из соответствующих скрытых групп описывается через координаты соответствующих представителей $\mathbf{P}^{b_1}$, $\mathbf{G}^{n_1}$ и $\mathbf{J}^{d_1}$ и μ уникальных скалярных неизвестных.

Таким образом, первая подпись задает $5\mu^2$ фиксированных скалярных неизвестных, а каждая из остальных – 3μ уникальных скалярных неизвестных. Для N известных подписей получаем систему из $N\mu^2$ скалярных уравнений, включающую $5\mu^2 + 3\mu(N-1)$ скалярных неизвестных. Из условия равенства числа уравнений и числа неизвестных получаем формулу для вычисления числа N_0 известных подписей, нужных для выполнения атаки A1:

$$N_0 = (\mu - 3)^{-1}(5\mu - 3). \qquad (13)$$

Для второй версии алгоритма $\mu = 5$ и $N_0 = 11$, что соответствует БСНУ, включающей 275 степенных уравнений в поле $GF(p)$ 40-битного порядка, и уровню стойкости $>2^{256}$. Для первой версии алгоритма $\mu = 3$ при любом значении N_0 условие равенства числа уравнений и неизвестных является недостижимым. По причине нелинейности уравнений, входящих в БСНУ, можно предположить, что при достаточно большом значении N_0 в процессе решения БСНУ ($N_0 > 11$) в принципе могут быть найдены значения секретных матриц $\mathbf{D}$ и $\mathbf{F}$, однако оцениваемая вычислительная сложность решения этой системы $>>2^{256}$ битовых операций. Таким образом, для обеих версий разработанного алгоритма стойкость к атаке A1 превышает стойкость к атаке A2, т.е. критерий достаточности рандомизации ЭЦП выполняется.

В связи с использованием 256-битой хеш-функции возникает вопрос об обеспечении достаточного уровня стойкости к атаке на основе парадокса о днях рождения (превышающего стойкость к атаке A2). Сценарий этой атаки включает генерацию большого числа документов, получение к им подлинных подписей и нахождением одинаковых подписей вида (e, σ, s, $\mathbf{S}$) к двум различным документам. Из алгоритма генерации ЭЦП видно, что для получения одинакового значения элемента $\mathbf{S}$ в двух различных подписях, в ходе в ходе вычисления каждой из них должны быть использованы 1) одинаковые значения e и 2) одинаковые значения случайных натуральных чисел $k < q$, $t < q$ и $r < q$ (поскольку вычисляется как в зависимости от e, так и в зависимости от k, t и r). Вероятность первого события равна 2^{-256}, а второго – $q-3 < 2^{-384}$ (для каждой из версий разработанного алгоритма). Поскольку данные события независимы (значение e зависит не только от значений k, t и r, но и от документа M), то вероятность того, что для двух различных подписей значения всех соответствующих четырех параметров совпадают,

Таблица 1.

Сравнение двух версий разработанного алгоритма ЭЦП с известными аналогами

Алгоритм	Размер открытого ключа, байт	Размер подписи, байт	Скорость генерации ЭЦП, отн.ед.	Скорость верификации ЭЦП, отн.ед.	Уровень стойкости
Версия 1	504	136	25,2	12,6	2^{192}
Версия 2	875	197	11,1	5,6	2^{256}
[26]	630	170	9,6	7,6	2^{192}
[22]	512	144	10,6	7,1	2^{100}
[14]	387	97	7,9	16,0	2^{100}
[15]	256	113	7,9	10,6	2^{80}
[13]	768	160	2,0	7,1	2^{80}

равна $<2^{-640}$. В соответствии с парадоксом о днях рождения для получения вероятности существования двух различных документов с одинаковыми значениями подписи должны быть сгенерированы 2^{320} подписей к различным документам, что определяет уровень стойкости 2^{320} к атаке на основе парадокса о днях рождения.

Таким образом, в рамках обеих версий разработанного алгоритма ЭЦП использование 256-битной хеш-функции является достаточным и не требуется увеличения разрядности функции Ф. Более того, можно применить 192-битную хеш-функцию Ф. При этом для первой (второй) версии алгоритма можно использовать алгебру матриц 3×3 (5×5), заданную над простым полем, имеющим 96-битный (32-битный) порядок p, обеспечивая более высокий уровень стойкости к атаке на основе парадокса о днях рождения по сравнению с атакой A2, значение которой при таком модифицировании не изменяется, поскольку не изменяется число степенных уравнений в БСНУ, решение которой выполняется в ходе атаки A2. Последнее замечание относится также и к атаке A1, поэтому указанное модифицирование сохраняет выполнимость критерия полноты рандомизации ЭЦП, приводя к повышению производительности процедур генерации и верификации подписи в 1,8 (1,6) раза для первой (второй) версии разработанного алгоритма.

Приводимое в табл. 1 сравнение разработанного алгоритма с известными алгебраическими алгоритмами ЭЦП, основанными на вычислительной трудности решения БСНУ, обладает более привлекательным сочетанием значений основных параметров. С учетом указанной возможности повышения производительности каждой из двух версий алгоритма можно сделать вывод о его достаточной практичности.

Выводы

Впервые реализован алгебраический алгоритм ЭЦП, основанный на вычислительной сложности решения БСНУ и использующий три скрытые коммутативные группы. В алгоритме предусмотрены две версии реализации с различным уровнем стойкости (2^{192} и 2^{256}). Обе версии обладают относительно малыми размерами подписи и открытого ключа (в сравнении с известными постквантовыми алгоритмами ЭЦП для заданного уровня стойкости) и достаточно высокой производительностью. Выполненная алгоритмическая разработка и использованные приемы расширяют предпосылки для решения о целесообразности приложения усилий по разработке постквантового стандарта ЭЦП на конечных некоммутативных алгебрах.

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. 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.

4. J. Ding, A. Petzoldt. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. N. 4. P. 28–36.
5. 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. V. 33. P. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
6. 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.
7. Øygarden M., Felke P., Raddum H. Analysis of multivariate encryption schemes: Application to Dob and C* // Journal of Cryptology. 2024. V. 37. N. 3. Article 20. DOI: 10,1007/s00145-024-09501-w.
8. Omar S., Padhye S., Dey D. Cryptanalysis of multivariate threshold ring signature schemes // Information Processing Letters.2023. V. 181. Article 106357. DOI: 10.1016/j.ipl.2022.106357.
9. 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.
10. Moldovyan N. A. Parameterized method for specifying vector finite fields of arbitrary dimensions // Quasigroups and related systems. 2024. Vol. 32. N. 2. P.299–312. DOI: 10.56415/qrs.v32.21.
11. 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.
12. Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022. Vol. 30. N. 2(48). P. 287–298. DOI: 10.56415/qrs.v30.24.
13. Moldovyan D. N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023. V. 31. N. 1(91). P. 111–124. doi:10.56415/csjm.v31.06.
14. 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 & Interfaces. 2023. V. 86. Article 103740. DOI: 10.1016/j.csi.2023.103740.
15. 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.
16. 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.
17. 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.
18. Moldovyan N. A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2020. N. 2(93). P. 62–67.
19. Moldovyan A. A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. N. 1. P. 95–108. DOI: DOI: 10.56415/qrs.v32.08.
20. 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.
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. 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.
23. Duong M. T., Do B. T., Nguyen M. H., Kurysheva A. A., Kostina A. A., Moldovyan D. N. Signature Algorithms on Non-commutative Algebras Over Finite Fields of Characteristic Two // Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. Springer Nature Singapore, 2022. P. 273–284, DOI: 10.1007/978-981-19-8069-5-18.
24. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. N. 2, pp. 293–308.
25. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018. V. 26. N. 2. P. 263–270.
26. Захаров Д. В., Костина А. А., Морозова Е. В., Молдовян Д. Н. Алгоритм ЭЦП на алгебре матриц 3x3, использующий две скрытые группы // Вопросы кибербезопасности. 2025. № 3(67). С. 45–54. DOI: 10.21681/2311-3456-2025-3-45-54.

POST-QUANTUM ALGEBRAIC SIGNATURE ALGORITHM WITH THREE HIDDEN GROUPS

Moldovyan A. A.[2]

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

Purpose of work *is the creation of additional prerequisites for the development of a post-quantum standard for digital signature algorithms based on the computational complexity of solving large systems of nonlinear equations (LSNE) in a finite field.*

2 Alexander A. Moldovyan, Dr. Sc. (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/0000-0001-5480-6016. E-mail: maa1305@yandex.ru

Research methods: *application of three hidden commutative groups, the elements of each of which are non-commutative with the elements of another one, for the implementation of enhanced signature randomization in algebraic digital signature schemes, the security of which is based on the computational difficulty of solving the LSNE in the ground finite field* $GF(p)$*. Calculation of the fitting signature element in the form of a matrix* $\mathbf{S}$ *depending on three pairwise non-commutative matrices selected randomly from the hidden groups. Application of the finite algebra of 3×3 and 5×5 matrices defined over the field* $GF(p)$ *with 64-bit and 40-bit prime order* p*.*

Results of the study: *a new mechanism for enhanced randomization of the signature fitting element is proposed and an algebraic algorithm for digital signature is developed, which is promising as a prototype of a practical post-quantum digital signature standard. The selection of random matrices from hidden groups is specified by exponentiating the generators of the corresponding hidden groups to random powers, calculated depending on the randomization parameters and the randomizing element of the digital signature. For the first time, to increase the security level to potential attacks based on alternative secret keys, the specified degrees are calculated as a solution to a system of linear equations. Estimates of the security to a direct attack and an attack based on known signatures are presented. A comparison of the parameters of the developed digital signature algorithm with known algorithms using the difficulty of solving the LSNE is given, and ways to improve its performance are discussed.*

Practical relevance: *the obtained results consist in creating a new premise for substantiating the choice of algebraic digital signature algorithms with hidden groups as a basis for developing a practical post-quantum digital signature standard, which consists in increasing the level of resistance to potential attacks based on equivalent keys.*

References

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. 2024, vol. 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, vol. 14154. Springer, Cham.
3. 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.
4. J. Ding, A. Petzoldt Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28–36.
5. 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, pp. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
6. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022, pp. 1–17. DOI: 10.1049/ise2.12092.
7. Øygarden M., Felke P., Raddum H. Analysis of multivariate encryption schemes: Application to Dob and C* // Journal of Cryptology. 2024, vol. 37, no. 3, article 20. DOI: 10,1007/s00145-024-09501-w.
8. Omar S., Padhye S., Dey D. Cryptanalysis of multivariate threshold ring signature schemes // Information Processing Letters.2023, vol. 181, article 106357. DOI: 10.1016/j.ipl.2022.106357.
9. Moldovyan N. A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023, no. 3(103), pp. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.
10. Moldovyan N. A. Parameterized method for specifying vector finite fields of arbitrary dimensions // Quasigroups and related systems. 2024, vol. 32, no. 2, pp. 299–312. DOI: 10.56415/qrs.v32.21.
11. Moldovyan A. A., Moldovyan N. A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024, vol. 32, no. 1(94), pp. 46–60. DOI: 10.56415/csjm.v32.04.
12. Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022, vol. 30 no. 2(48), pp. 287–298. DOI: 10.56415/qrs.v30.24.
13. 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.
14. 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 & Interfaces. 2023, vol. 86, article 103740. DOI: 10.1016/j.csi.2023.103740.
15. Moldovyan D. N., Moldovyan A. A. Algebraic signature algorithms based on difficulty of solving systems of equations. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2022, no. 2(48), pp. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
16. 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), pp. 3–10.
17. 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), pp. 206–226.
18. Moldovyan N. A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2020, no. 2(93), pp. 62–67.
19. 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. DOI: DOI: 10.56415/qrs.v32.08.
20. Moldovyan A. A., Moldovyan D. N., Kostina A. A. Algebraic signature algorithms with complete signature randomization. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2024, no. 2(60), pp. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.
21. Moldovyan D. N., Kostina A. A. A method for strengthening signature randomization in algebraic signature algorithms on noncommutative algebras. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2024, no. 4(62), pp. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.

22. Moldovyan N. A., Petrenko A. S. Algebraic signature algorithm with two hidden groups. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2024, no. 6(64), pp. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
23. Duong M. T.,, Do B. T., Nguyen M. H., Kurysheva A. A., Kostina A. A., Moldovyan D. N. Signature Algorithms on Non-commutative Algebras Over Finite Fields of Characteristic Two // Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. Springer Nature Singapore, 2022, pp. 273–284, DOI: 10.1007/978-981-19-8069-5-18.
24. 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.
25. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018, vol. 26, no. 2, pp. 263–270.
26. Zakharov D. V., Moldovyan D. N., Kostina A. A., Morozova E. V., Moldovyan D. N. A digital signature algorithm on the algebra of 3×3 matrices, which uses two hidden groups. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2025, no. 3(67), pp. 45–54. DOI: 10.21681/2311-3456-2025-3-45-54.