НОВАЯ КОНЦЕПЦИЯ РАЗРАБОТКИ ПОСТКВАНТОВЫХ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ НА НЕКОММУТАТИВНЫХ АЛГЕБРАХ

Молдовян Д.Н.[1], Молдовян А.А.[2], Молдовян Н.А.[3]

Цель *работы: разработка нового подхода к построению постквантовых алгоритмов цифровой подписи, свободных от недостатков известных аналогов – больших размеров подписи и открытого ключа.*

Метод *исследования: использование степенных векторных уравнений с многократным вхождением подписи S в качестве проверочного соотношения. Вычислительная трудность решения уравнений данного типа относительно неизвестного значения S обеспечивает стойкость схемы подписи к атакам с использованием S как подгоночного параметра. Возможность вычисление значения S по секретному ключу обеспечивается использованием открытого ключа в виде набора секретных элементов скрытой группы, маскируемых путем выполнения левых и правых умножений на согласованные обратимые векторы.*

Результаты *исследования: предложена новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах с использованием скрытой коммутативной группы. Ее основным отличием является использование секретного ключа в виде набора векторов, знание которых позволяет вычислить правильное значение подписи для случайных степеней присутствующих в проверочном уравнении. Вид проверочного уравнения задает систему квадратных векторных уравнений, связывающих открытый ключ с секретным, которая сводится к системе из многих квадратных уравнений с многими неизвестными, заданной над конечным полем. Вычислительная трудность нахождения решения последней системы определяет стойкость алгоритмов, разработанных в рамках предложенной концепции. Квантовый компьютер неэффективен для решения данной задачи, поэтому указанные алгоритмы являются постквантовыми. В качестве аналогов по построению рассматриваются алгоритмы цифровой подписи, основанные на вычислительной трудности скрытой задачи дискретного логарифмирования, однако использование скрытой группы и операций экспоненцирования составляет общий технический прием обеспечения корректности разрабатываемых в рамках концепции, а не для задания базовой вычислительно трудной задачи. Для повышения производительности процедур генерации и проверки подлинности подписи в качестве алгебраического носителя предложены четырехмерные алгебры, заданные по прореженным таблицам умножения базисных векторов. Предложенная концепция подтверждена разработкой конкретного постквантового алгоритма, обеспечивающего существенное уменьшение размеров открытого ключа и подписи по сравнению с финалистами всемирного конкурса НИСТ в номинации постквантовых алгоритмов цифровой подписи.*

Научная и практическая значимость *результатов статьи состоит в разработке новой концепции построения постквантовых алгоритмов цифровой подписи, расширяющих области их применения в условиях ограниченных вычислительных ресурсов.*

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

DOI: 10.21681/2311-3456-2022-1-18-25

Введение

Широко используемые в настоящее время криптосхемы с открытым ключом, включая алгоритмы электронной цифровой подписи (ЭЦП), основаны на вычислительной трудности задачи дискретного логарифмирования (ЗДЛ) или задачи факторизации (ЗФ). Однако, текущий прогресс в технологии создания квантовых вычислителей позволяет сделать прогноз, что в ближайшем будущем появится реально действующий квантовый компьютер, который может быть использован для выполнения полиномиальных алго-

1 Молдовян Дмитрий Николаевич, кандидат технических наук, научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, orcid.org/0000-0001-5039-7198. E-mail: mdn.spectr@mail.ru

2 Молдовян Александр Андреевич, доктор технических наук, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, orcid.org/0000-0001-5480-6016. E-mail: maa1305@yandex.ru

3 Молдовян Николай Андреевич, доктор технических наук, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, orcid.org/0000-0002-4483-5048, E-mail: nmold@mail.ru

ритмов, предложенных П. Шором[4] для решения ЗДЛ и ЗФ. С этого момента упомянутые криптосхемы перестают быть безопасными, поэтому в настоящее время ведутся актуальные исследования по разработке постквантовых двухключевых криптосхем, основанных на вычислительно трудных задачах других типов [1,2,3]. Наиболее ярким и масштабным за последнее время событием в области постквантовой криптографии является проведение Национальным институтом стандартов и технологий (НИСТ) США конкурса [4] по разработке постквантовых стандартов на криптосхемы с открытым ключом в период 2017—2024 гг. На данный момент времени завершены три этапа конкурса и выбраны алгоритмы для разработки на их основе постквантовых стандартов, что составит содержание завершающего четвертого этапа конкурса. Однако, НИСТ заявил, что кроме отобранных алгоритмов-финалистов он готов рассматривать новые предложения по номинации постквантовых ЭЦП, основанных на новых механизмах, даже за временными рамками четвертого этапа [5]. Это показывает, что НИСТ признает определенные недостатки алгоритмов ЭЦП, выбранных в качестве финалистов конкурса, и понимает, что более удачные решения вполне вероятны. С точки зрения авторов настоящей статьи конечные некоммутативные ассоциативные алгебры (КНАА) как носители постквантовых двухключевых алгоритмов [6,7] со сравнительно малыми размерами открытого ключа и подписи незаслуженно остались вне внимания участников конкурса НИСТ.

Целью настоящего исследования является разработка нового подхода к построению постквантовых алгоритмов ЭЦП с использованием КНАА в качестве алгебраического носителя, свободных от основных недостатков финалистов конкурса НИСТ – больших размеров подписи и открытого ключа.

Для достижения поставленной цели решается задача обоснования нового механизма генерации и верификации цифровой подписи, который, по сути, задает новую концепцию построения постквантовых алгоритмов ЭЦП с использованием КНАА в качестве алгебраического носителя. Источником данной концепции является ряд разработанных схем цифровой подписи, основанных на вычислительной сложности скрытой задачи дискретного логарифмирования [8,9] и использующих подпись, в которой рандомизирующий и подгоночный элементы представляют собой натуральные числа, играющие роль степеней в проверочном уравнении. Одно из важных отличий нового подхода состоит том, что в качестве подгоночного элемента служит вектор, входящий в проверочное векторное уравнение два или более раза, причем каждое вхождение связано с формированием произведения, возводимого в рандомизирующую степень. Другим важным отличием является то, что алгоритмы разработанные в рамках концепции основаны на вычислительной трудности решения систем многих квадратичных уравнений с многими переменными. Для решения этой вычислительной задачи квантовый компьютер не является эффективным, поэтому алгоритмы цифровой подписи, разрабатываемые в рамках предложенной концепции, являются постквантовыми. Для повышения производительности предлагается использовать четырехмерные КНАА, в которых операция векторного умножения задается по прореженными таблицам умножения базисных векторов (ТУБВ). Для подтверждения разработанной концепции разработан конкретный практичный постквантовый алгоритм ЭЦП.

1. Строение используемых КНАА

Пусть в m-мерном векторном пространстве дополнительно к стандартным операциям сложения векторов и умножения вектора на скаляр определена операция векторного умножения векторов $A=\sum_{i=0}^{m-1} a_i \mathrm{e}_i$ и $B=\sum_{j=0}^{m-1} b_j \mathrm{e}_j$, где e_i – формальные базисные векторы, в соответствии со следующей формулой:

$$AB=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \left(\mathrm{e}_i \mathrm{e}_j\right), \qquad (1)$$

где каждое из всевозможных произведений пар базисных векторов заменяется на однокомпонентный вектор в соответствии с некоторым правилом, задаваемым некоторой ТУБВ. Векторное пространство с определенной таким образом операцией умножения векторов, являющейся дистрибутивной слева и справа относительно операции сложения, называется m-мерной алгеброй. Для построения криптосхем, использующих операции экспоненцирования, интерес представляют КНАА, поэтому мы будем использовать ТУБВ, задающие ассоциативное векторное умножение, а для снижения вычислительной сложности этой операции – прореженные ТУБВ.

В качестве алгебраического носителя разработанного нового постквантового алгоритма ЭЦП может быть использована одна из четырех четырехмерных КНАА с глобальной двухсторонней единицей, задаваемых над конечным простым полем $GF(p)$ с характеристикой $p=2q+1$, где q - 256-битное простое число, по табл. 1–4. Выполненное авторами изучение строения каждой из этих алгебр показало, что они имеют сходное разбиение на множества коммутативных подалгебр. Последние имеют порядок, равный p^2, и относятся к трем различным типам, различающимся строением мультипликативной группы. Важными для данной статьи результатами исследования строения являются следующие.

1. Все коммутативные подалгебры попарно пересекаются строго в множестве всех скалярных векторов.

2. Подалгебры первого типа являются полем, которое изоморфно полю $GF(p^2)$, и их мультипликативная

4 Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing, 1997. Vol. 26. P. 1484–1509.

группа Γ_1 имеет циклическое строение и порядок, равный $\Omega_1 = p^2 - 1$. Содержат единственный необратимый вектор (0, 0, 0, 0).

3. Подалгебры второго типа содержат мультипликативную группу Γ_2, имеющую двухмерное циклическое строение (базис включает два вектора одного и того же порядка) и порядок, равный $\Omega_2 = (p - 1)^2$. Подалгебра данного типа содержит $2p - 1$ необратимых векторов, включая нулевой вектор.

4. Подалгебры третьего типа содержат мультипликативную группу Γ_3, имеющую циклическое строение и порядок, равный $\Omega_3 = p(p - 1)$. Подалгебра данного типа содержит p необратимых векторов.

Для числа коммутативных подалгебр первого n_1, второго n_2 и третьего n_3 типов получены следующие формулы [8,9]:

$$n_1 = \frac{p(p-1)}{2}; \quad (2)$$

$$n_2 = \frac{p(p+1)}{2}; \quad (3)$$

$$n_3 = p + 1. \quad (4)$$

Таблица 1

Задание первой четырехмерной КНАА (λ ≠ 0) с единицей вида (0, 1, 1, 0)

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

Таблица 2

Задание второй четырехмерной КНАА (λ ≠ 0) с единицей вида (0, 0, 1, 1)

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

Таблица 3

Задание четырехмерной КНАА (λ ≠ 0) с единицей вида (1, 0, 0, 1) [8]

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	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 четырехмерной КНАА (λ ≠ 0) единицей вида (1, 1, 0, 0) [9]

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

2. Алгоритмы-аналоги

В качестве аналогов разработанного алгоритма могут быть указаны схемы ЭЦП, описанные в статьях [8–10] и использующие коммутативную группу с двухмерной цикличностью в качестве скрытой группы. При реализации этих аналогов на алгебрах заданных по прореженным табл. 1–4 алгоритм генерации открытого ключа схемы подписи следует составить таким образом, чтобы задавался случайный выбор скрытой группы, содержащийся в одной из n_2 мультипликативных групп коммутативных подалгебр второго типа.

В качестве другого аналога может быть рассмотрен алгоритм ЭЦП, описанный в работе [7] и использующий в качестве алгебраического носителя некоторую КНАА с глобальной двухсторонней единицей и открытый ключ в виде тройки векторов (Y, Z, T), вычисляемой по формулам

$$Y = AN^xA^{-1}; \quad Z = BNB^{-1}; \quad T = AE_NB^{-1}, \quad (5)$$

где N – генератор скрытой циклической группы, являющийся необратимым вектором; A и B – обратимые векторы; E_N – необратимый вектор, являющийся одной из локальных единиц, относящихся к N. Вектор T является согласующим параметром алгоритма ЭЦП и является необратимым вектором. Проверочное уравнение имеет вид

$$R = Y^eTZ^s, \quad (6)$$

где e и s – рандомизирующий и подгоночный элементы подписи, причем для подписанного электронного документе M выполняется условие $e = f(M,R)$ для некоторой хеш-функции, являющейся частью схемы ЭЦП. Значение s вычисляется в зависимости от e и x.

Необратимость вектора T является важным требованием, поскольку в противном случае нахождение неизвестное значение x может быть легко сведено к решению ЗДЛ, заданной в циклической группе, генерируемой вектором $Z' = TZT^{-1}$, т. е. к решению уравнения $Y = Z'^{x}$, что выполняется на гипотетическом квантовом компьютере с помощью алгоритма П. Шора за полиномиальное время. Выбор в качестве генератора скрытой циклической группы необратимого вектора N связано с предотвращением возможности сведения СЗДЛ к ЗДЛ в поле $GF(p)$ путем вычисления значений функции нормы η (•) от векторов Y и Z, которая задает гомоморфное отображение алгебры в поле $GF(p)$: $\eta(Y) = (\eta(Z))^{x}$.

Вычисление открытого ключа в виде тройки необратимых векторов накладывает требование использования в качестве алгебраического носителя КНАА, имеющих размерность $m \geq 6$, поскольку в КНАА размерности $m = 4$ мощность множества взаимно перестановочных необратимых векторов является достаточно ограниченным. Например, в КНАА, заданных по прореженным табл. 1–4, в коммутативных подалгебрах содержится не более $2p$ необратимых векторов.

В алгоритмах ЭЦП, разработанных в соответствии с предложенной концепцией, предполагается использование только обратимых векторов, поэтому указанное ограничение снимается.

3. Предлагаемая концепция и постквантовый алгоритм ЭЦП

Идея предлагаемой концепции построения постквантовых схем ЭЦП на некоммутативных алгебрах заключается в задании проверочного уравнения, включающего два (и более) вхождениями одного из элементов подписи, являющегося некоторым обратимым вектором S. При этом проверочное уравнение имеет такой вид, что без знания секретного ключа, связанного с открытым ключом, при фиксировании остальных параметров этого уравнения обеспечивается практическая невозможность вычисления значения S как неизвестного. При этом открытый ключ формируется в виде векторов, каждый из которых вычисляется путем умножения элементов скрытой (секретной) коммутативной группы слева и справа на секретные обратимые векторы, взаимно перестановочные. Благодаря последнему указанная пара умножений задает маскирующую операцию, свободную от свойства взаимной коммутативности с операцией возведения в степень. Однако, пары векторов, используемые при вычисление различных элементов открытого ключа связаны между собой таким образом, что при знании векторов, использованных для вычисления открытого ключа, при соответствующем задании вектора S можно вычислительно эффективно найти значение S, удовлетворяющее проверочному уравнению и играющее роль подгоночного элемента подписи. Для вычисления значения S требуется явное использование элементов скрытой группы, поэтому задача разработки полиномиальных алгоритмов подделки подписи (ее вычисление без знания секретного ключа) для квантового компьютера предположительно является невыполнимой. Следующая схема ЭЦП разработана в соответствии с представленной концепцией, в которой в качестве алгебраического носителя предполагается использование одной из четырехмерных КНАА, задаваемых по табл. 1–4.

Открытый ключ формируется в виде двух пар обратимых векторов (Y_1, Z_1) и (Y_2, Z_2) по следующим формулам:

$$Y_1 = AG^{x}B;\ Z_1 = DQA^{-1};\ Y_2 = AQ^{w}B;\ Z_2 = DGA^{-1}, \quad (7)$$

где x и w – случайные натуральные значения, не превосходящие число q; G и Q – случайные обратимые векторы порядка q, выбранные из случайной коммутативной подалгебры второго типа; A, B и D – случайные обратимые попарно неперестановочные векторы, принадлежащие другим подалгебрам. Алгоритмы генерации векторов, принадлежащих подалгебре заданного типа, описаны в работах [8,9]. Все значения, используемые для вычисления открытого ключа, являются секретными.

Процедура генерации подписи в виде натурального числа e и вектора S включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < q$ и $t < q$ и вычислить вектор R:

$$R = AG^{k}Q^{t}A^{-1} \quad (8)$$

и рандомизирующий элемент подписи $e = f(M,R)$, где f – 256-битная хеш-функция.

2. Вычислить значения d и d:

$$d = (e + e^2)^{-1}(k - ex - e^2) \bmod q; \quad (9)$$

$$d = (e + e^2)^{-1}(t - e^2w - e) \bmod q. \quad (10)$$

3. Вычислить подгоночный элемент подписи в виде вектора S:

$$S = B^{-1}G^{d}Q^{d}D^{-1}. \quad (11)$$

Процедура проверки подлинности (верификации) ЭЦП (e, S) к документу M имеет вид:

1. Вычислить вектор

$$R' = (Y_1SZ_1)^{e}(Y_2SZ_2)^{e^2}. \quad (12)$$

2. Вычислить значение $e' = f(M,R')$.

3. Если $e' = e$, то подпись признается подлинной, иначе она отвергается.

Легко доказать корректность описанной схемы ЭЦП, т.е. то, что ЭЦП, сформированная в соответствии

DOI:10.21681/2311-3456-2022-1-18-25

с процедурой генерации подписи проходит проверочную процедуру как подлинная подпись. Размер открытого ключа и подписи равен примерно 512 байт и 160 байт соответственно, что существенно меньше аналогичных размеров постквантовых схем ЭЦП, выбранных в качестве финалистов конкурса НИСТ [11].

В описанной схеме подписи операции экспоненцирования используются как средство задания элементов из выбранной скрытой группы и вычисления подгоночного элемента подписи S. Знание значения степеней операций экспоненцирования не позволяет выполнить подделку подписи. Это показывает, что в основу стойкости схемы положена задача вычисления использованных при формировании открытого ключа элементов скрытой группы.

Основными способами взлома предложенного алгоритма представляются следующие два.

1. Выбрать произвольное значение $e^* < p - 1$ и вычислить вектор R^*:

$$R^* = (Y_1 S_0 Z_1)^{e^*} (Y_2 S_0 Z_2)^{e^{*2}}, \quad (13)$$

где S_0 – подгоночный элемент некоторой подлинной подписи, сформированной владельцем открытого ключа. Затем вычислить значение $e = f(M,R^*)$ и решить уравнение

$$R^* = (Y_1 S Z_1)^e (Y_2 S Z_2)^{e^2} \quad (14)$$

относительно неизвестного вектора S. Очевидно, что вычисленная пара (e, S) проходит проверочную процедуру как подлинная подпись к документу M.

2. Выбрать случайную коммутативную подалгебру второго типа и произвольные три ее обратимых элемента G', Q', и Q''. Затем решить систему, включающую следующие три линейных векторных уравнения, определяемых формулами (7):

$$Y_1 B'^{-1} = A'G'; \; Z_1 A' = D'Q'; \; Y_2 B'^{-1} = A'Q'' \quad (15)$$

относительно трех неизвестных векторных значений B'^{-1}, D' и A'. После этого вычислить вектор $G'' = D'^{-1} Z_2 A'$. Если $G''G' = G'G''$, то найдено альтернативное представление открытого ключа, которое позволяет сформировать подлинную подпись (описанная ранее процедура генерации подписи легко может быть модифицирована для случая представления открытого ключа в виде $Y_1 = A'G'B'$; $Z_1 = D'Q'A'^{-1}$; $Y_2 = A'Q''B'$; $Z_2 = D'G''A'^{-1}$).

Для устранения переборной процедуры второй способ можно реализовать как решение системы из 7 векторных уравнений с 7 неизвестными A', G', G'', B'^{-1}, D', Q', Q''. В этом случае к четырем уравнениям (15) добавляются следующие три уравнения связанные с перестановочностью неизвестных элементов из коммутативной скрытой группы:

$$G'G'' = G''G', \; G'Q' = Q'G' \text{ и } G'Q'' = Q''G'. \quad (16)$$

В результате имеем систему 7 векторных квадратичных уравнений с 7 неизвестными, которые сводятся к системе из 28 квадратичных уравнений над простым полем $GF(p)$, порядок которого $p > 2^{256}$, с 28 неизвестными. Вычислительная сложность задач такого типа лежит в основе постквантовых двухключевых криптосхем многомерной криптографии, в которых используется вычислительная трудность решения системы квадратичных уравнений с числом неизвестных 27, заданные над полем порядка 2^{16} [12] или с числом неизвестных до 100 и более при задании над полем порядка 2^8 в различных вариантах постквантового алгоритма цифровой подписи Rainbow [13], финалиста конкурса НИСТ.

Детальное рассмотрение каждого из двух упомянутых способов подделки подписи представляет собой самостоятельную задачу. Однако уровень стойкости будет определяться вторым способом, поскольку в первом возникает задача решения векторного уравнения вида

$$SZ_1(Y_2 SZ_2)^e = R'' \quad (17)$$

относительно неизвестного вектора S, которое при 256-битной степени e практически несводимо к решению системы уравнений над полем $GF(p)$, поэтому первый способ представляется имеющим более высокую вычислительную сложность.

Легко видеть, что в рамках описанной схемы ЭЦП для задания скрытой коммутативной группы могут быть использованы коммутативные подалгебры различных типов, например, первого и третьего для случая четырехмерных КНАА, заданных по таблицам 1–4. Также можно отметить возможность разработки частных схем ЭЦП с использованием в качестве алгебраического носителя некоммутативных алгебр (с глобальной двухсторонней единицей) разнообразных типов, например, описанных в работе [14]. При этом значительный интерес представляет информация о типах коммутативных подалгебр, содержащихся в используемом алгебраическом носителе.

4. Выводы

Предложена новая концепция разработки постквантовых схем ЭЦП на некоммутативных алгебрах и в ее рамках разработан конкретный алгоритм, обеспечивающий существенное уменьшение размеров открытого ключа и подписи. Представленные два способа взлома описанного алгоритма ЭЦП представляются имеющими общее значение для анализа различных схем ЭЦП, разрабатываемых в соответствии с концепцией. Последняя предоставляет достаточно широкое пространство для разнообразных частных реализаций. При этом в качестве алгебраических носителей могут быть использованы КНАА различных типов и размерностей $m \geq 4$, включая алгебры матриц 2x2 и некоммутативные алгебры, заданные над конечными расширениями двоичного поля GF(2). Для повышения производительности разработанного алгоритма в качестве его алгебраического носителя использованы четырехмерные КНАА, операция векторного умножения в которых задана по прореженным ТУБВ.

Впервые на КНАА реализован алгоритм цифровой подписи со скрытой коммутативной группой, основан-

ный на вычислительной сложности решения систем квадратичных уравнений с многими неизвестными, т.е. на задаче, для решения которой квантовый компьютер неэффективен. Предложенная концепция задает новый подход и способ построения практичных постквантовых алгоритмов ЭЦП, свободных от недостатков присущих известным постквантовым алгоритмам ЭЦП и имеет существенное значение для теории и практики постквантовой криптографии.

Литература

1. 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.
2. Agibalov G.P. ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57–65. DOI: 10.17223/20710410/42/4.
3. Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Zh. Choosing parameters for NTRU Encrypt // Cryptographers› Track at the RSA Conference - CTA-RSA 2017. Springer LNCS. 2017. Vol. 10159, pp. 3–-18.
4. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register, December 20, 2016. Vol. 81. No. 244. P. 92787–92788. https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf. (обращение 4 декабря 2021).
5. Moody D. NIST Status Update on the 3rd Round. https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (обращение 4 декабря 2021).
6. Kuzmin A.S., Markov V.T., Mikhalev A.A., Mikhalev A.V., Nechaev A.A. Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. Vol. 223. No. 5, P. 629–641.
7. Moldovyan A.A., Moldovyan N.A. Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. Vol. 26, N. 3(78). P. 301–313.
8. 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. https://doi.org/10.21638/11701/spbu10.2021.303
9. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. N.2(86). P. 206–226.
10. Moldovyan N. A., Moldovyan A.A. Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410.
11. Moody D. , Alagic G. , Apon D. , Cooper D., Dang Q., Kelsey J., Liu Y., Miller C., Peralta R., Perlner R., Robinson A., Smith-Tone D. and Alperin-Sheriff J. (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8309 (обращение 4 декабря 2021).
12. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. Vol. 18. N. 1. P. 60-67.
13. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (обращение 4 декабря 2021)
14. Moldovyan N.A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. Vol. 26. N. 2. P. 263–270.

A NEW CONCEPT FOR DESIGNING POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS ON NON-COMMUTATIVE ALGEBRAS

Moldovyan D.N.[5], Moldovyan A.A.[6], and Moldovyan N.A.[7]

Abstract

Purpose of work *is the development of a new approach to designing post-quantum digital signature algorithms that are free from the shortcomings of known analogs – large sizes of the signature and public key.*

Research method *is the use of power vector equations with multiple occurrences of the signature S as a signature verification equation. The computational difficulty of solving equations of the said type relatively the unknown value of S ensures the resistance of the signature scheme to attacks using S as a fitting parameter. The possibility of calculating the value of S by the secret key is provided by using the public key in the form of a set of secret elements of the hidden group, masked by performing left and right multiplications by matched invertible vectors.*

Results of the study *include a new proposed concept for the development of post-quantum digital signature algorithms on non-commutative algebras, which use a hidden commutative group. One of its main differences is the use of a secret key in the form of a set of vectors, the knowledge of which makes it possible to calculate the correct signature value for the random powers present in the verification equation. The form of the latter defines a system of quadratic vector equations connecting the public key with the secret, which is reduced to a system of many quadratic equations with many unknowns, given over a finite field. The computational difficulty of finding a solution to the latter system determines the security of the algorithms developed within the framework of the proposed concept. A quantum computer is ineffective for solving this problem, therefore, the said algorithms are post-quantum. As analogs in construction, digital signature algorithms based on the computational difficulty of the hidden discrete logarithm problem are considered, however, the use of a hidden group and exponentiation operations represent only a general technique for ensuring the correctness of the signature schemes developed within the framework of the concept, and not for specifying a basic computationally difficult problem. To improve the performance of the signature generation and verifications procedures, the four-dimensional algebras defined by sparse basis vector multiplication tables are used as an algebraic support. The proposed concept is confirmed by the development of a specific post-quantum algorithm that provides a significant reduction in the size of the public key and signature in comparison with the finalists of the NIST global competition in the nomination of post-quantum digital signature algorithms.*

Practical relevance: *The developed new concept for constructing post-quantum digital signature algorithms expands the areas of their application in conditions of limited computing resources*

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

References

1. Alamelou, Q., O. Blazy, S. Cauchie, and Ph. Gaborit. A code-based group signature scheme. Designs, Codes and Cryptography. 2017, vol. 82, no. 1–2, pp, 469–493.
2. Agibalov G.P. ElGamal cryptosystems on Boolean functions. Prikl. Diskr. Mat. 2018, no. 42, pp. 57–65. DOI: 10.17223/20710410/42/4.
3. Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Zh. Choosing parameters for NTRU Encrypt. Cryptographers' Track at the RSA Conference - CTA-RSA 2017. Springer LNCS. 2017, vol. 10159, pp. 3 18.
4. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. Federal Register, December 20, 2016. Vol. 81. No. 244. P. 92787–92788. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed December 4, 2021).
5. Moody, D. 2021. NIST Status Update on the 3rd Round. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (accessed December 4, 2021).
6. Kuzmin A.S., Markov V.T., Mikhalev A.A., Mikhalev A.V., Nechaev A.A. Cryptographic Algorithms on Groups and Algebras. Journal of Mathematical Sciences. 2017, vol. 223, no 5, pp. 629–641.

5 Dmitriy N. Moldovyan, Ph.D. (in Tech.) researcher of laboratory of cybersecurity and post-quantum cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: mdn.spectr@mail.ru

6 Alexander A. Moldovyan, Dr.Sc. (in Tech.) chief researcher of laboratory of cybersecurity and post-quantum cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: maa1305@yandex.ru

7 Nikolay A. Moldovyan, Dr.Sc. (in Tech.) chief researcher of laboratory of cybersecurity and post-quantum cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: nmold@mail.ru

7. Moldovyan, A.A. and N.A. Moldovyan. Post-quantum signature algorithms based on the hidden discrete logarithm problem. Computer Science Journal of Moldova. 2018, vol 26, no. 3, pp. 301–313.
8. Moldovyan, N. A. and A.A. Moldovyan. Digital signature scheme on the 2x2 matrix algebra. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2021, vol. 17, iss. 3, pp. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303
9. Moldovyan, D.N. A practical digital signature scheme based on the hidden logarithm problem. Computer Science Journal of Moldova. 2021, vol 29, no. 2, pp. 206–226.
10. Moldovyan N. A. and A.A. Moldovyan. Candidate for practical post-quantum signature scheme. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2020, vol. 16, iss. 4, pp. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410.
11. Moody, D., G. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y. Liu, C. Miller, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and J. Alperin-Sheriff. 2020. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online]. Available at: https://doi.org/10.6028/NIST.IR.8309 (accessed December 4, 2021).
12. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems. International Journal of Network Security. 2016, vol. 18, no. 1, pp. 60–67.
13. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (accessed December 4, 2021)
14. 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.