АЛГЕБРАИЧЕСКИЕ АЛГОРИТМЫ ЭЦП, ОСНОВАННЫЕ НА ТРУДНОСТИ РЕШЕНИЯ СИСТЕМ УРАВНЕНИЙ

Молдовян Д.Н.[1], Молдовян А.А.[2]

Цель *работы: разработка постквантовых алгоритмов ЭЦП, обладающих высокой производительностью и малыми размерами подписи и открытого и секретного ключей.*

Метод *исследования: использование новой концепции построения алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах, отличающейся многократным вхождением подписи S в степенное проверочное уравнение. Генерация открытого ключа в виде набора векторов, вычисляемых как произведения различных троек секретных векторов. При специальном выборе указанных троек обеспечивается возможность вычисления подписи, удовлетворяющей проверочному уравнению.*

Результаты *исследования: предложены два новых алгебраических постквантовых алгоритма ЭЦП со скрытой группой, отличающиеся от известных аналогов тем, что их стойкость основана на вычислительной трудности решения систем квадратных уравнений с многими неизвестными. Отличием от двухключевых алгоритмов многомерной криптографии является то, что система квадратных уравнений выводится из формул генерации элементов открытого ключа в виде набора векторов m-мерной конечной некоммутативной алгебры с ассоциативной операцией векторного умножения. Указанные формулы задают систему из n квадратных векторных уравнений, которая сводится к системе из mn квадратных уравнений над конечным полем. Благодаря «естественному» механизму возникновения указанной системы она задается над полем, порядок которого имеет большой размер (97 и 129 бит). Используемые процедуры генерации открытого ключа и подписи включают операции возведения в степень большого размера (96 и 128 бит) элементов секретной (скрытой) коммутативной группы, содержащейся в алгебре. Подпись формируется в виде двух элементов – рандомизирующего натурального числа e и «подгоночного» вектора S. Уравнение проверки подлинности подписи включает трехкратное вхождение вектора S. При этом каждое вхождение связано с формированием произведения, возводимого в степень, зависящую от значения e. Достигнуто существенное уменьшение размеров открытого и секретного ключей и подписи, а также повышение производительности по сравнению с зарубежными аналогами, рассматриваемыми в качестве базовых алгоритмов для принятия постквантовых стандартов ЭЦП.*

Научная и практическая значимость *результатов статьи состоит в разработке двух новых практичных постквантовых алгоритмов ЭЦП, в которых устранены основные недостатки известных аналогов, за счет чего они могут быть применяться в условиях доступности 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: 10.21681/2311-3456-2022-2-7-17

Введение

Аутентификация и конфиденциальность сообщений, передаваемых по каналам связи, имеет важное значение в системах телемедицины [1], электронного правительства, интернета вещей [2], облачных [3] и туманных [4] вычислений. Решение этих задач обеспечивается различными способами, включая технологию «блокчейна» [5,6], при этом наиболее удобными и универсальными являются методы криптогра-

1 Молдовян Дмитрий Николаевич, кандидат технических наук, научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. 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, Санкт-Петербург, Россия. Orcid. org/0000-0001-5480-6016. E-mail: maa1305@yandex.ru

фии с открытым ключом. В настоящее время широко применяемые двухключевые криптографические алгоритмы и протоколы основаны на вычислительной трудности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ).

До конца 2016 г. доминировало мнение о том, что появление практически действующего квантового компьютера в обозримом будущем является достаточно маловероятным событием, поэтому существование полиномиальных по времени квантовых алгоритмов решения ЗДЛ и ЗФ, предложенные П. Шором[3], включая наличие эффективных алгоритмов решения ЗДЛ на эллиптических кривых [7], не принималось во внимание для оценки практической безопасности существующих стандартов на криптографические алгоритмы с открытым ключом, включая алгоритмы электронной цифровой подписи (ЭЦП). Однако значительный технологический прогресс в области квантовых вычислений дал основание Национальному институту стандартов и технологий США (НИСТ) прийти к мнению, что после 2025 г. квантовый вычислитель, с помощью которого можно будет решать ЗДЛ и ЗФ, возникающие при криптоанализе широко используемых криптосхем с открытым ключом, может неожиданно появиться. С этого момента указанные криптосхемы перестанут быть безопасными и системы обеспечения информационной безопасности, включая кибербезопасность, останутся без двух важнейших своих инструментов: 1) механизмов согласования секретного ключа по открытому каналу, включая открытое шифрование и 2) механизмов аутентификации информации и ее источника с использованием ЭЦП.

Переход к широкому использованию постквантовых (т. е. стойких к атакам с использованием квантовых компьютеров) механизмов указанных двух типов требует принятия постквантовых стандартов. Учитывая, что процедура разработки криптографических алгоритмов, включая их криптоанализ, является исходным этапом перехода на постквантовые стандарты и требует длительных по времени исследований, НИСТ в декабре 2016 г. анонсировал программу на период 2017–2024 гг. [8] по созданию постквантовых стандартов на криптоалгоритмы с открытым ключом, в рамках которой был объявлен всемирный конкурс по разработке 1) постквантовых алгоритмов открытого согласования ключа и открытого шифрования и 2) постквантовых алгоритмов ЭЦП.

К настоящему моменту завершились первые три этапа конкурса [9], в результате которых были выбраны алгоритмы для углубленного исследования на четвертом этапе, результатом которого должны стать проекты постквантовых стандартов на указанные два типа алгоритмов. В номинации постквантовых ЭЦП выбраны 3 финалиста, алгоритмы Falcon, Crystals-Dilithium, Rainbow, и 3 альтернативных алгоритма GeMSS, Picnic, Sphincs+ (на случай, если у всех финалистов обнаружатся неприемлемые недостатки). При этом НИСТ рассматривает возможность объявить дополнительное представление в ходе четвертого этапа новых заявок на участие в конкурсе по номинации постквантовых ЭЦП [10]. Видимо это связано с пониманием того, что для принятия стандарта выбранные финалисты и альтернативные варианты не являются достаточно практичными, главным образом из-за больших размеров подписи и/или открытого ключа.

Таким образом, разработка практичных постквантовых алгоритмов ЭЦП сохраняет высокую степень актуальности в мировом масштабе. При этом неочевидно как известные подходы, использованные командными участниками конкурса НИСТ, могут обеспечить решение указанной актуальной задачи. Для решения этой задачи более перспективным представляется использование новой концепции построения алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах (КНАА), предложенной недавно в статье [11]. В основе концепции лежит идея использования вычислений, включая операции экспоненцирования, в скрытой группе для формирования подписи таким способом, что для взлома алгоритма требуется решать не скрытую ЗДЛ [12,13], а систему из многих квадратных уравнений с многими переменными – постквантовую вычислительно трудную задачу [14,15], использованную при разработке алгоритмов Rainbow [16] и GeMSS [GeMSS: A Great Multivariate Short Signature. https://www-polsys.lip6.fr/Links/NIST/GeMSS.html].

Постановка цели исследования

Предложенная в работе [11] концепция построения постквантовых алгоритмов ЭЦП на КНАА подтверждена реализацией схемы ЭЦП с использованием четырехмерных КНАА, заданных над простым конечным полем $GF(p)$ с 257-битным значением порядка p, и проверочного уравнения с двумя вхождениями «подгоночного» элемента подписи $\mathbf{S}$. Выбор сравнительно большого размера порядка поля, над которым возникает базовая вычислительно трудная задача нахожде-

3 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

ния решения системы из 28 квадратных уравнений с 28 неизвестными, связан с обеспечением стойкости к способу подделки подписи (вычисление подписи без знания секретного ключа) с использованием значения $\mathbf{S}$ как подгоночного параметра. При этом произведение размера порядка поля на число квадратичных уравнений в системе равно значению $\Psi \approx 7200$, что от 5 до 16 раз больше, чем в случае апробированных постквантовых алгоритмов ЭЦП [14,15,16] многомерной криптографии, которые также основаны на вычислительно трудной задаче указанного типа.

Отвлекаясь от конкретного вида квадратичных уравнений, значение указанного произведения можно принять в качестве неформального показателя ожидаемого уровня стойкости, т.е. для различных алгоритмов с примерно одинаковым значением этого неформального показателя можно ожидать примерно одинаковый уровень стойкости. Последний следует скорректировать по результатам детального рассмотрения вычислительной трудности решения системы квадратных уравнений с учетом их конкретного вида. Однако детализированное исследование стойкости является самостоятельной достаточно трудоемкой задачей и на этапе рассмотрения разнообразных конкретных алгоритмов, разрабатываемых в рамках концепции [11], представляется оправданным принятие во внимание упомянутого неформального показателя Ψ.

В алгоритме ЭЦП из работы [11] используется избыточно большое значение показателя Y, которое в принципе может быть существенно уменьшено, сохраняя приемлемый уровень стойкости, если предложить варианты алгоритмов, для которых усиливается защищенность от атак с использованием элемента подписи $\mathbf{S}$ в качестве подгоночного параметра. Для такого усиления представляется естественным применение проверочных уравнений с числом вхождений значения $\mathbf{S}$ более двух.

В настоящей статье решается задача разработки постквантовых алгоритмов ЭЦП в соответствии с концепцией [11] при использовании проверочных уравнений с тремя вхождениями элемента подписи $\mathbf{S}$. При этом в качестве алгебраического носителя используется четырехмерная (шестимерная) КНАА, заданная над полем $GF(p)$ со 129-битным (97-битным) значением порядка p, за счет чего обеспечивается повышение производительности, уменьшение размеров подписи и открытого и секретного ключей при сохранении приемлемого значения показателя $\Psi \approx 3600$ ($\Psi \approx 3500$).

1. Используемые алгебраические носители

Если в m-мерном векторном пространстве определить *дополнительную операцию векторного умножения*, обладающую свойством дистрибутивности слева и справа *относительно операции сложения, то получим алгебраическую структуру, называемую* m-мерной алгеброй. Операция умножения векторов $\mathrm{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ и $\mathrm{B} = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$, где $\mathbf{e}_i$ – *формальные базисные векторы*, может быть определена по следующей формуле:

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

где каждое из всевозможных произведений пар базисных векторов заменяется на однокомпонентный вектор по правилу, задаваемому некоторой таблицей умножения базисных векторов (ТУББВ). Для построения алгоритмов ЭЦП, использующих операции возведения в степень большого размера, следует использовать алгебры с ассоциативным умножением (это свойство необходимо для реализации процедуры быстрого возведения в степень). Таким образом, в качестве алгебраического носителя разрабатываемых схем подписи используются КНАА, а именно, четырехмерные и шестимерные алгебры с векторным умножением, заданным над простым конечным полем $GF(p)$ по табл. 1 и табл. 2 соответственно. В качестве характеристики поля берется постое число $p = 2q + 1$, где q - 128-битное (для случая $m = 4$) или 96-битное (для случая $m = 6$) простое число.

Таблица 1

Задание четырехмерной КНАА ($\lambda \neq 0; \lambda \neq 1$) [17]

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

Четырехмерная КНАА, заданная по табл. 1 содержит глобальную двухстороннюю единицу в виде вектора

$$E=\left(\frac{1}{1-\lambda},\frac{1}{1-\lambda},\frac{\lambda}{\lambda-1},\frac{1}{\lambda-1}\right). \quad (2)$$

Условием обратимости вектора $\mathbf{A} = (a_0, a_1, a_2, a_3)$ является выполнимость неравенства

$$a_0a_1 \neq a_2a_3. \quad (3)$$

Таблица 2

Задание шестимерной КНАА (λ ≠ 0) [18]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

Шестимерная КНАА, заданная по табл. 2, содержит глобальную двухстороннюю единицу в виде вектора $\mathbf{E} = (1, 0, 0, 0, 0, 0)$. Данная алгебра построена как частный случай реализации ассоциативных алгебр произвольной четной размерности с помощью унифицированного метода, предложенного в работе [18]. Условием обратимости вектора $\mathbf{A} = (a_0, a_1, a_2, a_3, a_4, a_5)$ является выполнимость неравенства

$$\begin{aligned}&\frac{1}{4}\left(\left(a_0+a_2+a_4\right)^2-\lambda\left(a_1+a_3+a_5\right)^2\right)\times\\ &\times\left(\left(a_0-a_2\right)^2+\left(a_0-a_4\right)^2+\left(a_2-a_4\right)^2-\right.\\ &\left.-\lambda\left(a_1-a_3\right)^2-\lambda\left(a_1-a_5\right)^2-\lambda\left(a_3-a_5\right)^2\right)^2\neq 0.\end{aligned} \quad (4)$$

Вычисление вектора $\mathbf{A}^{-1}$, обратного заданному вектору $\mathbf{A}$, выполняется как решение векторного уравнения $\mathbf{AX} = \mathrm{E}$, которое сводится к системе из четырех линейных уравнений над полем $GF(p)$.

Скалярные векторы в этих двух алгебрах имеют вид $\mathbf{L} = \alpha\mathbf{E}$, где $\alpha = 1, 2, \ldots p - 1$. Каждая из них содержит большое множество различных коммутативных групп порядков $(p^2 - 1)$ - циклические; $(p - 1)^2$ - порождаемые минимальной системой образующих (базисом) из двух векторов порядка $p - 1$; $p(p - 1)$ - циклические. В качестве скрытой (секретной) группы в предлагаемых постквантовых алгоритмах используются коммутативные группы, обладающие двухмерной цикличностью, т.е. порождаемые базисом <**G**, **H**>, включающим два вектора одного и того же порядка, равного простому числу q. Алгоритм генерации случайного базиса описывается следующим образом:

1. Сгенерировать случайный обратимый вектор **V** порядка $p - 1$.
2. Если вектор **V** содержится в множестве скалярных векторов, то перейти к шагу 1.
3. Вычислить вектор $\mathbf{G} = \mathbf{V}^2$.
4. Сгенерировать случайное целое число k $(0 < k < p - 1)$ и случайный примитивный элемент b по модулю p.
5. Вычислить вектор $\mathbf{H} = \beta^2\mathbf{G}^k$ (скалярное умножение).

2. Постквантовая схема подписи на четырехмерной КНАА

В первой разработанной схеме ЭЦП используется в качестве алгебраического носителя четырехмерная КНАА, заданная по табл. 1, и следующий алгоритм генерации открытого ключа.

Алгоритм формирования открытого ключа.

1. Сгенерировать базис <**G**, **H**> примарной коммутативной группы порядка q^2, обладающей двухмерной цикличностью.
2. Используя формулу (3). сгенерировать случайные обратимые векторы **A**, **B**, и **D**, которые удовлетворяют следующим неравенствам $\mathbf{AB} \neq \mathrm{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{DB} \neq \mathbf{BD}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DG} \neq \mathbf{GD}$.
3. Вычислить векторы $\mathbf{A}^{-1}$, $\mathbf{B}^{-1}$ и $\mathbf{D}^{-1}$.
4. Сгенерировать случайные неотрицательные целые числа $x < q$ и $w < q$. Затем вычислить открытый ключ в виде четверки векторов (**Y**, **Z**, **U**, **V**) по формулам:

$$\mathbf{Y} = \mathbf{B}^{-1}\mathbf{G}\mathbf{A}^{-1};\ \mathbf{Z} = \mathbf{B}^{-1}\mathbf{H}\mathbf{A}^{-1};$$
$$\mathbf{U} = \mathbf{B}^{-1}\mathbf{G}^x\mathbf{D}^{-1};\ \mathbf{V} = \mathbf{D}\mathbf{H}^w\mathbf{A}^{-1}. \quad (5)$$

Размер открытого ключа (**Y**, **Z**, **U**, **V**) равен 2064 бит (258 байт). Секретным ключом является набор значений x, w , **G**, **H**, **A**, **B** и **D**, общий размер которого составляет 2836 бит (≈355 байт). Для вычисления цифровой подписи к некоторому заданному электронному документу M следует использовать секретный ключ и следующий алгоритм.

Алгоритм генерации ЭЦП.

1. Сгенерировать случайные неотрицательные целые числа $k < q$ и $t < q$ и вычислить вектор

$$\mathbf{R} = \mathbf{D}\mathbf{G}^k\mathbf{H}^t\mathbf{D}^{-1}. \quad (6)$$

2. Используя некоторую специфицированную

384-битную хэш-функцию f, вычислить первый элемент подписи $e = e_1||e_2||e_3 = f(M, \mathbf{R})$, где хэш-значение e представлено как конкатенация трех 128-битных целых чисел e_1, e_2 и e_3.

3. Вычислить натуральные числа n и u:

$$n = \frac{k - e_1e_2e_3 - xe_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q; \quad (7)$$

$$u = \frac{t - e_2e_3 - we_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q. \quad (8)$$

4. Вычислить второй элемент подписи в виде вектора $\mathbf{S}$:

$$\mathbf{S} = \mathbf{A}\mathbf{G}^n\mathbf{H}^u\mathbf{B}. \quad (9)$$

Подписью к документу M является пара (e, $\mathbf{S}$), т. е. хэш-значение e и вектор $\mathbf{S}$. Длина подписи равна 900 бит (≈113 байт). Вычислительная сложность алгоритма генерации ЭЦП примерно равна 4 операциям возведения в 128-битную степень в КНАА, используемой в качестве алгебраического носителя (или 12288 умножений по модулю 129-битного простого числа p).

Для верификации ЭЦП к документу M следует воспользоваться открытым ключом ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{U}$, $\mathbf{V}$) и следующей вычислительной процедурой.

Алгоритм проверки подлинности ЭЦП.

1. Вычислить вектор

$$\mathrm{R}' = \left[\mathrm{V}\left(\mathrm{S}(\mathrm{YS})^{e_1}\,\mathrm{Z}\right)^{e_2}\mathrm{SU}\right]^{e_3} \quad (10)$$

2. Вычислить значение e' хэш-функции f от документа M с присоединенным к нему вектором $\mathbf{R}'$: $e' = f(M, \mathbf{R}')$.

3. Если $e' = e$, то подпись принимается как подлинная, в противном случае она отвергается.

Вычислительная сложность алгоритма верификации ЭЦП примерно равна 3 операциям возведения в 128-битную степень в четырехмерной КНАА (или 9216 умножений по модулю 129-битного простого числа p).

Корректность описанной схемы подписи может быть показана, рассматривая процедуру верификации подписи, сформированной в полном соответствии с процедурой генерации ЭЦП.

Доказательство корректности.

Вычислим значения $\left(\mathrm{YS}\right)^{e_1}$ и $\left(\mathrm{S}(\mathrm{YS})^{e_1}\,\mathrm{Z}\right)^{e_2}$:

$$\left(\mathrm{YS}\right)^{e_1} = \left(\mathrm{B}^{-1}\mathrm{G}\mathrm{A}^{-1}\mathrm{A}\mathrm{G}^n\mathrm{H}^u\mathrm{B}\right)^{e_1} = \mathrm{B}^{-1}\mathrm{G}^{e_1(n+1)}\mathrm{H}^{e_1u}\mathrm{B},$$

$$\mathrm{J} = \left(\mathrm{S}(\mathrm{YS})^{e_1}\,\mathrm{Z}\right)^{e_2} = \left(\mathrm{A}\mathrm{G}^n\mathrm{H}^u\mathrm{B}\mathrm{B}^{-1}\mathrm{G}^{e_1(n+1)}\mathrm{H}^{e_1u}\mathrm{B}\mathrm{B}^{-1}\mathrm{H}\mathrm{A}^{-1}\right)^{e_2} =$$

$$= \mathrm{A}\mathrm{G}^{n(e_1e_2+e_2)+e_1e_2}\mathrm{H}^{u(e_1e_2+e_2)+e_2}\mathrm{A}^{-1}.$$

Затем вычислим значение $\mathbf{R}'$:

$$\mathrm{R}' = \left(\mathrm{VJSU}\right)^{e_3} =$$

$$= \left(\mathrm{D}\mathrm{H}^w\mathrm{A}^{-1}\mathrm{A}\mathrm{G}^{n(e_1e_2+e_2)+e_1e_2}\mathrm{H}^{u(e_1e_2+e_2)+e_2}\mathrm{A}^{-1}\mathrm{A}\mathrm{G}^n\mathrm{H}^u\mathrm{B}\mathrm{B}^{-1}\mathrm{G}^x\mathrm{D}^{-1}\right)^{e_3} =$$

$$= \left(\mathrm{D}\mathrm{G}^{n(e_1e_2+e_2+1)+e_1e_2+x}\mathrm{H}^{u(e_1e_2+e_2+1)+e_2+w}\mathrm{D}^{-1}\right)^{e_3} =$$

$$= \mathrm{D}\mathrm{G}^{n(e_1e_2e_3+e_2e_3+e_3)+e_1e_2e_3+xe_3}\mathrm{H}^{u(e_1e_2e_3+e_2e_3+e_3)+e_2e_3+we_3}\mathrm{D}^{-1}.$$

С учетом формул (7) и (8) получаем:

$$\mathrm{R}' = \mathrm{D}\mathrm{G}^k\mathrm{H}^t\mathrm{D}^{-1} \Rightarrow f\left(M, \mathrm{R}'\right) = f\left(M, \mathrm{R}\right) \Rightarrow e' = e. \quad (11)$$

Таким образом, подпись, вычисленная в соответствии с алгоритмом генерации ЭЦП проходит процедуру верификации как подлинная ЭЦП, что доказывает корректность работы разработанной схемы ЭЦП.

3. Постквантовая схема ЭЦП на шестимерной КНАА

Для случая использования шестимерной КНАА, заданной по табл. 2, в качестве алгебраического носителя разработана схема ЭЦП, включающая следующий алгоритм генерации открытого ключа.

Алгоритм формирования открытого ключа.

1. Сгенерировать базис <$\mathbf{G}$, $\mathbf{H}$> примарной коммутативной группы порядка q^2, обладающей двухмерной цикличностью.

2. Используя условие обратимости (4), сгенерировать случайные обратимые векторы $\mathbf{A}$ и $\mathbf{B}$, которые удовлетворяют следующим неравенствам $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

3. Вычислить векторы $\mathbf{A}^{-1}$ и $\mathbf{B}^{-1}$.

4. Сгенерировать случайные неотрицательные целые числа $x < q$ и $w < q$. Затем вычислить открытый ключ в виде четверки векторов ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{U}$, $\mathbf{V}$) по формулам:

$$\mathbf{Y} = \mathbf{B}^{-1}\mathbf{G}\mathbf{A}^{-1}; \ \mathbf{Z} = \mathbf{B}^{-1}\mathbf{H}\mathbf{B};$$
$$\mathbf{U} = \mathbf{B}^{-1}\mathbf{G}^x\mathbf{A}^{-1}; \ \mathbf{V} = \mathbf{B}^{-1}\mathbf{H}^w\mathbf{A}^{-1}. \quad (12)$$

Размер открытого ключа ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{U}$, $\mathbf{V}$) равен 2328 бит (291 байт). Секретным ключом является набор значений x, w , $\mathbf{G}$, $\mathbf{H}$, $\mathbf{A}$ и $\mathbf{B}$, общим размер которого составляет 2520 бит (315 байт). Для вычисления цифровой подписи к некоторому заданному электронному документу M следует использовать секретный ключ и следующий алгоритм.

Алгоритм генерации подписи.

1. Сгенерировать случайные неотрицательные целые числа $k < q$ и $t < q$ и вычислить вектор

$$\mathbf{R} = \mathbf{A}\mathbf{G}^k\mathbf{H}^t\mathbf{A}^{-1}. \quad (13)$$

2. Используя некоторую специфицированную 288-битную хэш-функцию f', вычислить первый элемент подписи $e = e_1||e_2||e_3 = f'(M, \mathbf{R})$, где значение e представлено как конкатенация трех 96-битных целых чисел e_1, e_2 и e_3.

3. Вычислить натуральные числа n и u:

$$n = \frac{k - e_1e_2e_3 - xe_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q; \quad (14)$$

$$u = \frac{t - e_1e_2e_3 - we_2e_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q. \quad (15)$$

4. Вычислить второй элемент подписи в виде вектора $\mathbf{S}$:

$$\mathbf{S} = \mathbf{AG}^n\mathbf{H}^u\mathbf{B}. \quad (16)$$

Подписью к документу M является пара (e, $\mathbf{S}$). Длина подписи равна 870 бит (≈109 байт). Вычислительная сложность алгоритма генерации ЭЦП примерно равна 4 операциям возведения в 96-битную степень (576 векторных умножений) в шестимерной КНАА (или 20736 умножений (≈11716 умножений) по модулю 97-битного (129-битного) простого числа p).

Верификация ЭЦП к документу M выполняется по открытому ключу ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{U}$, $\mathbf{V}$) с использованием следующего алгоритма.

Алгоритм проверки подлинности ЭЦП.

1. Вычислить вектор

$$\mathrm{R}' = \left[\left(\mathrm{S}(\mathrm{YSZ})^{e_1}\,\mathrm{V}\right)^{e_2}\mathrm{SU}\right]^{e_3} \quad (17)$$

2. Вычислить значение e' хэш-функции f': вычислить первый элемент подписи signature element $e' = f'(M, \mathbf{R}')$.

3. Если $e' = e$, то подпись принимается как подлинная, в противном случае она отвергается.

Вычислительная сложность алгоритма верификации ЭЦП примерно равна 3 операциям возведения в 96-битную степень (432 векторных умножения) в шестимерной КНАА (или 15552 умножений (≈8787 умножений) по модулю 97-битного (129-битного) простого числа p).

Доказательство корректности.

Вычислим значения $(\mathrm{YSZ})^{e_1}$ и $\mathrm{J} = \left(\mathrm{S}(\mathrm{YSZ})^{e_1}\,\mathrm{V}\right)^{e_2}$:

$$(\mathrm{YSZ})^{e_1} = \left(\mathrm{B}^{-1}\mathrm{GA}^{-1}\mathrm{AG}^n\mathrm{H}^u\mathrm{BB}^{-1}\mathrm{HB}\right)^{e_1} = \mathrm{B}^{-1}\mathrm{G}^{e_1n+e_1}\mathrm{H}^{e_1u+e_1}\mathrm{B};$$

$$\mathrm{J} = \left(\mathrm{S}(\mathrm{YSZ})^{e_1}\,\mathrm{V}\right)^{e_2} = \left(\mathrm{AG}^n\mathrm{H}^u\mathrm{BB}^{-1}\mathrm{G}^{e_1n+e_1}\mathrm{H}^{e_1u+e_1}\mathrm{BB}^{-1}\mathrm{H}^w\mathrm{A}^{-1}\right)^{e_2} =$$

$$= \mathrm{AG}^{n(e_1e_2+e_2)+e_1e_2}\mathrm{H}^{u(e_1e_2+e_2)+e_1e_2+we_2}\mathrm{A}^{-1}.$$

Затем вычислим значение $\mathbf{R}'$:

$$\mathrm{R}' = \left(\mathrm{JSU}\right)^{e_3} =$$

$$= \left(\mathrm{AG}^{n(e_1e_2+e_2)+e_1e_2}\mathrm{H}^{u(e_1e_2+e_2)+e_1e_2+we_2}\mathrm{A}^{-1}\mathrm{AG}^n\mathrm{H}^u\mathrm{BB}^{-1}\mathrm{G}^x\mathrm{A}^{-1}\right)^{e_3} =$$

$$= \left(\mathrm{AG}^{n(e_1e_2+e_2+1)+e_1e_2+x}\mathrm{H}^{u(e_1e_2+e_2+1)+e_1e_2+we_2}\mathrm{A}^{-1}\right)^{e_3} =$$

С учетом формул (14) и (15) получаем:

$$\mathrm{R}' = \mathrm{AG}^k\mathrm{H}^t\mathrm{A}^{-1} \Rightarrow f(M, \mathrm{R}') = f(M, \mathrm{R}) \Rightarrow e' = e, \quad (18)$$

где последнее равенство доказывает корректность работы разработанной схемы ЭЦП.

4. Обсуждение

Предложенные два алгоритма ЭЦП, использующие КНАА в качестве алгебраического носителя, построены в соответствии с недавно предложенной концепцией использования проверочного уравнения с несколькими вхождениями значения подписи и вычислений в скрытой коммутативной группе для задания секретного ключа в виде набора векторов. При этом в процедурах генерации и верификации подписи используются операции экспоненцирования, однако роль данных операций состоит не в задании ЗДЛ в скрытой группе, как в алгоритмах ЭЦП [12,13], а в обеспечении возможности вычисления подписи, удовлетворяющей проверочному уравнению с несколькими вхождениями элемента $\mathbf{S}$.

В предложенных двух новых алгоритмах ЭЦП используются проверочные уравнения с тремя вхождениями вектора $\mathbf{S}$, которые обусловливают необходимость использования специальных согласованных механизмов вычисления открытого ключа, генерации рандомизирующего вектора $\mathbf{R}$ и вычисления вектора $\mathbf{S}$, при которых обеспечивается выполнимость проверочного уравнения. Согласование обеспечивается тем, что элементы открытого ключа, входящие в проверочное уравнение как известные параметры и векторы $\mathbf{R}$ и $\mathbf{S}$ вычисляются как замаскированные элементы скрытой группы. Маскирование выполняется путем выполнения левостороннего и правостороннего умножений на согласованные секретные обратимые векторы.

Таким образом, при знании секретного ключа имеется возможность вычислить к данному документу правильную подпись в соответствии с описанным механизмом. При этом наличие других полиномиальных по времени способов генерации подписи неочевидно. В случае атак на предложенные алгоритмы ЭЦП, т. е. в случае подделки подписи без знания секретного ключа, другие способы еще менее очевидны. Наиболее эффективной атакой представляется вычисление секретного ключа по открытому ключу, причем в

общем случае может существовать другой набор векторов, которые удовлетворяют свойствам векторов, которые являются элементами секретного ключа. В этом случае мы будем иметь некоторый альтернативный секретный ключ, использование которого в процедуре генерации ЭЦП, обеспечивает возможность вычисления правильной подписи.

Вычисление секретного ключа или альтернативного секретного ключа связано с решением системы векторных квадратных уравнений с многими неизвестными. Для алгоритма ЭЦП на четырехмерной КНАА эта система включает 7 уравнений и имеет следующий вид:

$$\begin{cases} YA = B^{-1}G; & ZA = B^{-1}H; \\ UD = B^{-1}G_x; & VA = DH_w \\ GG_x = G_xG; & GH = HG; \\ GH_w = H_wG. \end{cases} \quad (19)$$

Первые 4 квадратных уравнения задаются формулами (5), по которым вычисляются элементы открытого ключа, а последние 3 уравнения определяются требованием выбора векторов $\mathbf{G}$, $\mathbf{H}$, $\mathbf{G}_x$ и $\mathbf{H}_w$ (где $\mathbf{G}_x = \mathbf{G}^x$ и $\mathbf{H}_w = \mathbf{H}^w$) из одной и той же коммутативной группы. Если для системы (19) будет найдено одно из решений, то вычисление подписи может быть легко осуществлено без представления векторов $\mathbf{G}_x$ и $\mathbf{H}_w$ в виде степеней векторов $\mathbf{G}$ и $\mathbf{H}$. В предложенных алгоритмах ЭЦП векторы, представленные в виде $\mathbf{G}^x$ и $\mathbf{H}^w$, используются только для того, чтобы уменьшить число операций возведения в степень при генерации подписи. На уровень стойкости это не влияет. Этот момент явно иллюстрирует тот факт, что предложенные два алгоритма ЭЦП основаны не на вычислительной сложности ЗДЛ, а на вычислительной сложности решения систем квадратных уравнений с многими переменными как это имеет место в двухключевых криптосхемах многомерной криптографии [14,15,16].

Последняя задача является вычислительно трудной также и для случая использования квантовых компьютеров, поэтому предложенные два алгоритма относятся к постквантовым двухключевым криптосхемам, также как и двухключевые криптоалгоритмы многомерной криптографии. Сложность решения систем квадратных уравнений зависит от их вида, числа уравнений входящих в систему, числа неизвестных и порядка поля, над которым заданы уравнения. Используя таблицу 1, система (21), включающая 7 векторных уравнений с 7 неизвестными $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{G}$, $\mathbf{G}_x$, $\mathbf{H}$ и $\mathbf{H}_w$, легко сводится к системе из 28 квадратных уравнений над полем $GF(p)$ с 28 неизвестными (которыми являются координаты векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{G}$, $\mathbf{G}_x$, $\mathbf{H}$ и $\mathbf{H}_w$,). В качестве альтернативных алгебраических носителей для реализации постквантового алгоритма ЭЦП из раздела 3 можно рассмотреть четырехмерные КНАА, предложенные в работе [19].

Алгоритм ЭЦП на шестимерной КНАА основан на вычислительной трудности решения следующей системы из 7 квадратных уравнений с 6 неизвестными (которыми являются шестимерные векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$, $\mathbf{G}_x$, $\mathbf{H}$ и $\mathbf{H}_w$) над упомянутой алгеброй:

$$\begin{cases} YA = B^{-1}G; & ZB = B^{-1}H; \\ UA = B^{-1}G_x; & VA = B^{-1}H_w \\ GG_x = G_xG; & GH = HG; \\ GH_w = H_wG. \end{cases} \quad (20)$$

Используя табл. 2, система (20) сводится к системе над полем $GF(p)$, включающей 42 уравнения и 36 неизвестных. Учитывая, что системы квадратных уравнений, вычислительная трудность решения которых лежит в основе разработанных двух алгоритмов, включают достаточно большое число уравнений и неизвестных, причем они задаются над полем $GF(p)$, порядок которого имеет большой размер (129 бит для первого и 97 бит для второго алгоритма), можно сделать предположение, что предложенные алгоритмы обладают стойкостью не ниже известных алгоритмов ЭЦП, относящихся к многомерной криптографии.

В табл. 3 приведено сравнение некоторых параметров разработанных и известных алгоритмов ЭЦП, основанных на вычислительной трудности решения систем квадратных уравнений. При этом в приведенных известных алгоритмах размер секретного ключа превышает десятки и сотни килобайт, что существенно больше размера секретного ключа в схемах ЭЦП, описанных в разделах 2 и 3. Последние обладают более высоким значением неформального показателя ожидаемого уровня стойкости Ψ по сравнению с алгоритмами многомерной криптографии, описанными в работах [14,15,16,20]. В целом сопоставление показывает, что предложенные алгоритмы являются более практичными, благодаря существенно меньшему общему размеру открытого ключа, секретного ключа и подписи.

В табл. 4 приведено сравнение предложенных алгоритмов с финалистами конкурса НИСТ (алгоритмы Falcon, CRYSTALS-Dilithium и Rainbow) в номинации постквантовых алгоритмов ЭЦП и криптосистемой RSA-2048, которое также показывает существенные преимущества предложенных алгоритмов. Схемы

ЭЦП на кодах исправляющих ошибки [21,22] также являются постквантовыми, однако из-за чрезвычайно больших размеров подписи и открытого ключа (мегабайты) они представляются менее практичными, чем все упоминаемые в табл. 3 и 4 алгоритмы.

Выводы

На основе основных положений концепции [11] разработаны два постквантовых алгоритма ЭЦП, использующие КНАА в качестве их алгебраического носителя и основанные на вычислительной трудности решения системы многих квадратных уравнений с многими неизвестными, заданной над полем большого порядка. Они являются существенно более практичными по сравнению с известными постквантовыми алгоритмами ЭЦП, включая финалистов конкурса НИСТ. Это обусловливает интерес к детальному исследованию их стойкости и разработке рекомендаций по оптимизации выбора размера порядка поля, над которым задаются КНАА, используемые в качестве алгебраического носителя, для заданного уровня стойкости. Однако эти вопросы составляют предмет самостоятельного изучения.

В целом свойства разработанных двух алгоритмов дают подтверждение концепции [11] как нового перспективного направления в области постквантовой криптографии и показывают, что ее использование представляется перспективным для разработки стандартов на постквантовые алгоритмы ЭЦП.

Таблица 3

Сравнение с известными алгоритмами ЭЦП многомерной криптографии

Алгоритм ЭЦП	**Размер подписи, байт**	**Размер открытого ключа, байт**	**Число квадратных уравнений (неизвестных)**	**Порядок поля, над которым заданы уравнения**	Ψ
[14]	--	--	27 (27)	2^{16}	432
Rainbow [16]	33	16065	27 (33)	2^{8}	264
QUARTZ [15]	16	72704	100 (107)	2^{4}	428
Rainbow [20] (3 разных версии)	66... 204	>150000 ... >1900000	64 (96)... 128 (204)	2^{4}, 31, 2^{8}	384... 1632
[11]	160	512	28 (28)	$>2^{256}$	>7168
из раздела 2	113	258	28 (28)	$>2^{128}$	>3584
из раздела 3	109	291	42 (36)	$>2^{96}$	>3456

Таблица 4

Сравнение с финалистами конкурса НИСТ [9] в номинации постквантовых ЭЦП

Алгоритм ЭЦП	**Размер подписи, байт**	**Размер открытого ключа, байт**	**Скорость генерации подписи, отн. ед.**	**Скорость верификации подписи, отн. ед.**
Falcon	1280	1793	50	25
CRYSTALS-Dilithium	2701	1472	15	2
Rainbow	64	150000	--	--
RSA-2048	256	>256	10	100
из раздела 2	113	258	630	840
из раздела 3	109	291	660	880

Литература

1. Griggs K.N., Ossipova O., Kohlios C.P., Baccarini A.N., Howson E.A., Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring // Journal of Medical Systems. 2018. Vol. 42. Iss. 7. Article 130. DOI: 10.1007/s10916-018-0982-x
2. Zhang G., Shen F., Liu Z., Yang Y., Wang K., Zhou M.T. Femto: Fair and energy-minimized task offloading for fog-enabled IoT networks // IEEE Internet of Things Journal. 2018. Vol. 6. No. 3, pp. 4388–4400. DOI: 10.1109/JIOT.2018.2887229.
3. Xia Q., Sifah E.B., Asamoah K.O., Gao J., Du X., Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain // IEEE Access. 2017. Vol. 5. P. 14757–14767. DOI: 10.1109/ACCESS.2017.2730843.
4. Yao X., Kong H., Liu H., Qiu T., Ning H. An attribute credential based public key scheme for fog computing in digital manufacturing. IEEE Transactions on Industrial Informatics. 2019, vol. 15, no. 4, pp. 2297–2307. DOI: 10.1109/TII.2019.2891079.
5. Kaur H., Alam M.A., Jameel R., Mourya A.K., Chang V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of Medical Systems. 2018, vol. 42, iss. 8, article 156. DOI: 10.1007/s10916-018-1007-5.
6. Shahnaz C A., Qamar U., Khalid A. Using Blockchain for Electronic Health Records. IEEE Access. 2019, vol. 7, pp. 147782–147795. DOI: 10.1109/ACCESS.2019.2946373.
7. Galbraith S.D. and Gaudry P. Recent progress on the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography. 2016, vol. 78, no. 1, pp. 5172. DOI: 10.1007/s10623-015-0146-7.
8. 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 16 декабря 2021).
9. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed December 27, 2021)
10. 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 16 декабря 2021).
11. Молдовян Д.Н., Молдовян А.А., Молдовян Н.А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 10–17.
12. 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.
13. 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.
14. 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.
15. Jintai D., Dieter S. Multivariable Public Key Cryptosystems (2004) https://eprint.iacr.org/2004/350.pdf (accessed December 27, 2021)
16. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme // In Conference on Applied Cryptography and Network Security - ACNS 2005. Springer Lecture Notes in Computer Science. 2005. Vol. 3531. P. 164–175.
17. 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.
18. 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.
19. Moldovyan N.A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. No. 2(93). P. 62-67.
20. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (обращение 16 декабря 2021)
21. 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. DOI: 10.1007/s10623-016-0276-6.
22. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Прикладная дискретная математика. 2019. № 45. С. 33–43. DOI: 10.17223/20710410/45/4.

ALGEBRAIC SIGNATURE ALGORITHMS BASED ON DIFFICULTY OF SOLVING SYSTEMS OF EQUATIONS

Moldovyan D.N.[4] and Moldovyan A.A.[5]

Abstract

Purpose *of work is the development of post-quantum digital signature algorithms with comparatively small sizes of the public and secret keys and the signature.*

Research method *is the use of a new concept for constructing signature algorithms on finite non-commutative associative algebras, which is distinguished by the multiple occurrences of the signature S in the power verification equation. A public key is generated in the form of a set of vectors every of which is calculated as the product of triples of secret vectors. With a special choice of these triples, it is possible to calculate a signature that satisfies the verification equation.*

Results *of the study are two developed algebraic post-quantum digital signature algorithms of a new type, security of which is based on the computational difficulty of solving systems of many quadratic equations with many unknowns. The difference from the public-key algorithms of multivariate cryptography is that the system of quadratic equations is derived from the formulas for generating the public-key elements in the form of a set of vectors of m-dimensional finite non-commutative algebra with an associative vector multiplication operation. The said formulas define the system of n quadratic vector equations, which reduces to the system of mn quadratic equations over a finite field. Thanks to the "natural" mechanism for the occurrence of the specified system, it is set above the field, the order of which has a large size (97 and 129 bits). The used procedures for generating the public key and signature include the exponentiation operations to the degree of a large size (96 and 128 bits), which are performed over the elements of the secret (hidden) commutative group contained in the algebra. The signature is formed in the form of two elements: a randomizing natural number e and a "fitting" vector S. The signature authentication equation includes a multiple occurrence of the S element and every entry of the vector S is associated with the formation of a product that is exponentiated to a degree dependent on the value of the e element. A significant reduction in the size of public and secret keys and signatures has been achieved, as well as an increase in performance compared to foreign analogues, considered currently as basic algorithms for the adoption of post-quantum digital signature standards.*

Practical relevance: *The developed two new practical post-quantum digital signature algorithms are free from the main disadvantages of known analogues and can be applied under the availability 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. Griggs K.N., Ossipova O., Kohlios C.P., Baccarini A.N., Howson E.A., Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems. 2018, vol. 42, iss. 7, article 130. DOI: 10.1007/s10916-018-0982-x
2. Zhang G., Shen F., Liu Z., Yang Y., Wang K., Zhou M.T. Femto: Fair and energy-minimized task offloading for fog-enabled IoT networks. IEEE Internet of Things Journal. 2018, vol. 6, no. 3, pp. 4388–4400. DOI: 10.1109/JIOT.2018.2887229.
3. Xia Q., Sifah E.B., Asamoah K.O., Gao J., Du X., Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017, vol. 5, pp. 14757–14767. DOI: 10.1109/ACCESS.2017.2730843.
4. Yao X., Kong H., Liu H., Qiu T., Ning H. An attribute credential based public key scheme for fog computing in digital manufacturing. IEEE Transactions on Industrial Informatics. 2019, vol. 15, no. 4, pp. 2297–2307. DOI: 10.1109/TII.2019.2891079.

4 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 orcid.org/0000-0001-5480-6016

5 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 orcid.org/0000-0001-5039-7198

5. Kaur H., Alam M.A., Jameel R., Mourya A.K., Chang V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of Medical Systems. 2018, vol. 42, iss. 8, article 156. DOI: 10.1007/s10916-018-1007-5.
6. Shahnaz C A., Qamar U., Khalid A. Using Blockchain for Electronic Health Records. IEEE Access. 2019, vol. 7, pp. 147782–147795. DOI: 10.1109/ACCESS.2019.2946373.
7. Galbraith S.D. and Gaudry P. Recent progress on the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography. 2016, vol. 78, no. 1, pp. 51-72. DOI: 10.1007/s10623-015-0146-7.
8. 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 27, 2021).
9. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed December 27, 2021)
10. Moody D. NIST Status Update on the 3rd Round.2021. 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 27, 2021).
11. Moldovyan D.N. Moldovyan A.A., Moldovyan N.A. A new concept for designing post-quantum digital signature algorithms on non-commutative algebras. Voprosy kiberbezopasnosti [Cibersecurity questtions]. 2022, no. 1(47), pp. 10–17.
12. 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. DOI: 10.21638/11701/spbu10.2021.303.
13. 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.
14. 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.
15. Jintai D., Dieter S. Multivariable Public Key Cryptosystems (2004) https://eprint.iacr.org/2004/350.pdf (accessed December 27, 2021)
16. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme. In Conference on Applied Cryptography and Network Security - ACNS 2005. Springer Lecture Notes in Computer Science. 2005, vol. 3531, pp. 164–175.
17. 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.
18. 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.
19. Moldovyan N.A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security. Bulletin of Academy of Sciences of Moldova. Mathematics. 2020, no. 2(93), pp. 62-67.
20. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (accessed December 27, 2021)
21. 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. DOI: 10.1007/s10623-016-0276-6.
22. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem. Prikl. Diskr. Mat. 2019, no. 45, pp. 33–43. DOI: 10.17223/20710410/45/4.