УДК654.1 DOI:10.31854/1813-324X-2021-7-2-85-93

Схема цифровой подписи со скрытой группой, обладающей двухмерной цикличностью

Д.Н. Молдовян[1], Р.Ш. Фахрутдинов[1], А.Ю. Мирин[1], А.А. Костина[1]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация
*Адрес для переписки: fahr@cobra.ru

Информация о статье
Поступила в редакцию 29.04.2021
Принята к публикации 23.05.2021

Ссылка для цитирования: Молдовян Д.Н., Фахрутдинов Р.Ш., Мирин А.Ю., Костина А.А. Схема цифровой подписи со скрытой группой, обладающей двухмерной цикличностью // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 85–93. DOI:10.31854/1813-324X-2021-7-2-85-93

Аннотация: *Предложен способ построения схем цифровой подписи, основанных на скрытой задаче дискретного логарифмирования, удовлетворяющих общему критерию постквантовой стойкости, который обеспечивает сравнительно малые размеры открытого ключа и подписи. На основе способа разработана практичная схема цифровой подписи, в которой операция экспоненцирования в скрытой группе с двухмерной цикличностью является базовым криптографическим примитивом. Алгебраический носитель криптосхемы представляет собой четырехмерную конечную некоммутативную алгебру с ассоциативной операцией умножения. Благодаря заданию алгебры по прореженной таблице умножения базисных векторов, обеспечивается повышение производительности процедур генерации и проверки подлинности подписи. Открытым ключом является тройка четырехмерных векторов, вычисляемых как образы элементов скрытой группы, отображаемые с помощью маскирующих операций двух типов: 1) взаимно коммутативных с операцией экспоненциирования и 2) не обладающих этим свойством.*

Ключевые слова: *защита информации, компьютерная безопасность, криптография, цифровая подпись, постквантовая криптосхема, задача дискретного логарифмирования, конечная ассоциативная алгебра, некоммутативная алгебра, скрытая группа.*

Введение

Одной из актуальных текущих проблем теоретической и практической криптографии является разработка двухключевых алгоритмов и протоколов [1, 2], стойких к атакам с использованием квантовых компьютеров. Криптосхемы такого типа называются постквантовыми. Всемирный конкурс на разработку постквантовых схем цифровой подписи и открытого согласования ключа, объявленный Национальным институтом стандартов и технологий США (НИСТ), ориентирован на получение к 2024 г. черновых версий постквантовых криптографических стандартов. Однако общим минусом предложенных кандидатов на постквантовые схемы электронной подписи является их недостаточная практичность, в частности большие размеры открытого ключа и подписи.

Сравнительно новым и многообещающим подходом к разработке практичных постквантовых схем цифровой подписи является использование скрытой задачи дискретного логарифмирования (СЗДЛ), задаваемой в конечных некоммутативных ассоциативных алгебрах (КНАА), в качестве базового примитива [3–6]. Обоснование использования СЗДЛ, как постквантового криптографического примитива, объясняется тем, что задание по открытым параметрам криптосхемы периодической функции с периодом, зависящим от значения дискретного логарифма, приводит к тому, что эта функция принимает значения из многочисленных различных циклических групп, содержащихся в КНАА. Благодаря этому обстоятельству обеспечивается стойкость к квантовым атакам (атаки с использованием квантового компьютера), использующим известные полиномиальные по времени квантовые алгоритмы нахождения длины периодов периодических функций, значения которых лежат в одной явно заданной конечной циклической группе [7–9].

В первых постквантовых схемах цифровой подписи [4, 5], базирующихся на СЗДЛ и допускающих задание периодических функций, включающих период, зависящий от значения дискретного логарифма в скрытой группе, использован следующий

критерий построения: *вычислительно невыполнимо построение периодической функции на основе открытых параметров схемы цифровой подписи, содержащих период с длиной, зависящей от значения дискретного логарифма, и с достаточно высокой вероятностью, принимающих значения в некоторой фиксированной циклической группе.*

В расширенной постановке вопроса обеспечения достаточно высокой стойкости к квантовым атакам (постквантовой стойкости) [10] следует учесть потенциальную возможность разработки новых квантовых алгоритмов нахождения длины периода периодических функций, принимающих значения в различных коммутативных группах, содержащихся в фиксированной КНАА, используемой в качестве алгебраического носителя схемы цифровой подписи. В работе [10] предложен общий критерий постквантовой стойкости схем цифровой подписи, базирующихся на СЗДЛ: *по открытым параметрам схемы цифровой подписи вычислительно невыполнима задача построения периодической функции, содержащей период, зависящий от значения логарифма в скрытой циклической группе*.

При выполнении общего критерия постквантовой стойкости, разрабатываемая схема цифровой подписи будет защищенной от атак, использующих как известные, так и новые квантовые алгоритмы нахождения длины периода периодических функций. В работе [10] предложен механизм реализации общего критерия, включающий использование коммутативной группы, обладающей двухмерной цикличностью (частный тип групп с двумя порождающими элементами, характеризующийся тем, что порождающие элементы имеют одинаковый порядок, см., например, [11]) в качестве скрытой группы.

Постановка задачи

Известные схемы цифровой подписи [10, 12], удовлетворяющие общему критерию постквантовой стойкости, построены с удвоением открытого ключа и удвоением проверочного уравнения, а также использованием вектора, в качестве дополнительного элемента подписи. Это приводит к удвоению размера открытого ключа и увеличению длины подписи в 3 раза при одновременном снижении производительности криптосхемы по сравнению со схемами цифровой подписи, основанными на первом критерии.

В настоящей статье предлагается способ реализации схем цифровой подписи, удовлетворяющих общему критерию постквантовой стойкости и свободных от недостатков их аналогов, предложенных ранее в работах [10, 12].

Используемый алгебраический носитель

В качестве алгебраического носителя алгоритмов цифровой подписи, основанных на скрытой задаче дискретного логарифмирования, обычно применяются КНАА четной размерности $m \geq 4$, в которых содержится достаточно большое число различных подмножеств элементов, представляющих собой конечные коммутативные группы. Конечные алгебры задаются путем определения в конечном векторном пространстве с операциями сложения векторов и скалярного умножения дополнительной операции векторного умножения, обладающей свойствами дистрибутивности слева и справа относительно операции сложения. Пусть некоторое m-мерное векторное пространство задано над простым конечным полем $GF(p)$, и имеется некоторый его базис в виде набора векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_i, \ldots, \boldsymbol{e}_m$. Некоторый вектор $\boldsymbol{A}$ можно записывать в виде:

1) упорядоченного множества его координат $a_i \in GF(p)$: $\boldsymbol{A} = (a_0, a_1, \ldots, a_{m-1})$;

2) суммы $\boldsymbol{A} = \sum_{i=0}^{m-1} a_i e_i$, где $a_i \boldsymbol{e}_i$ – компоненты вектора $\boldsymbol{A}$.

Операция умножения вектора $\boldsymbol{A} = \sum_{i=0}^{m-1} a_i \boldsymbol{e}_i$ на вектор $\boldsymbol{B} = \sum_{j=0}^{m-1} b_j e_j$ определяется по следующей формуле, в которой всевозможные произведения вида $\boldsymbol{e}_i \cdot \boldsymbol{e}_j$ заменяются по некоторому правилу на однокомпонентные векторы:

$$\boldsymbol{A} \cdot \boldsymbol{B} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\boldsymbol{e}_i \cdot \boldsymbol{e}_j), \qquad (1)$$

Указанное правило удобно представить в виде таблицы умножения базисных векторов (ТУБВ), предполагая, что вместо каждого из произведений $e_i \cdot e_j$ подставляется на некоторый вектор $\lambda \boldsymbol{e}_k$, указанный в ячейке на пересечение i-й строки и j-го столбца. Если $\lambda = 1$, то в ячейках ТУБВ указывается базисный вектор $\boldsymbol{e}_k$. Если $\lambda \neq 1$, то значение λ называется структурным коэффициентом.

Для задания КНАА разрабатывается ТУБВ, которая определяет операцию векторного умножения, обладающую свойствами некоммутативности и ассоциативности. При реализации последнего свойства для произвольной тройки векторов $\boldsymbol{A}$, $\boldsymbol{B}$ и $\boldsymbol{C}$ выполняется следующее равенство:

$$(\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{C} = \boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C}). \qquad (2)$$

С учетом формул (1) и (2) легко показать, что ТУБВ, которая задает выполнимость равенства для всевозможных троек базисных векторов, определяет ассоциативное векторное умножение:

$$(\boldsymbol{e}_i \cdot \boldsymbol{e}_j) \cdot \boldsymbol{e}_k = \boldsymbol{e}_i \cdot (\boldsymbol{e}_j \cdot \boldsymbol{e}_k).$$

С целью повышения производительности алгоритмов генерации и проверки подлинности цифровой подписи представляет интерес использование четырехмерных КНАА, в которых операция умножения задана по прореженным ТУБВ, т. е. по ТУБВ,

в ячейках которых присутствует структурный коэффициент $\lambda = 0$.

Таблица 1 дает пример прореженной ТУБВ и используется для задания алгебраического носителя в разрабатываемой схеме цифровой подписи, основанной на скрытой задаче дискретного логарифмирования и удовлетворяющей общему критерию постквантовой стойкости.

В случае, если равенство $\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{B} \cdot \boldsymbol{A}$ выполняется для произвольной пары векторов $\boldsymbol{A}$ и $\boldsymbol{B}$, операция умножения и задаваемая алгебра называются коммутативными, в противном случае – некоммутативными. В последнем случае имеем КНАА.

ТАБЛИЦА 1. Прореженная ТУБВ, задающая четырехмерную КНАА с глобальной единицей ($\mu^{-1}, \lambda^{-1}, 0, 0$), где $\mu \neq 0; \lambda \neq 0$ [12]

TABLE 1. A Sparse Basis Vector Multiplication Table that Defines a Four-Dimensional Non-Commutative Associative Algebra with Global Unit ($\mu^{-1}, \lambda^{-1}, 0, 0$), where $\mu \neq 0; \lambda \neq 0$ [12]

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

Конечные группы с многомерной цикличностью

Конечной группой с μ-мерной цикличностью называется коммутативная группа с μ порождающими элементами, имеющими одинаковый порядок [11, 13]. В работах [11, 13] приведены примеры групп с μ-мерной цикличностью ($\mu \geq 2$) и обсуждается их применение для построения схем цифровой подписи. Рассмотрим, например, двухмерную конечную ассоциативную алгебру с операцией умножения, заданной по таблице 2. Ее мультипликативная группа имеет строение, зависящее от структурного коэффициента λ. Если λ является квадратичным невычетом в $GF(p)$, то указанная группа является циклической и имеет порядок $\Omega = p^2 - 1$ [13]. Если λ является квадратичным вычетом в $GF(p)$, то она является группой с двухмерной цикличностью и имеет порядок $\Omega = (p-1)^2$ [13].

ТАБЛИЦА 2. Задание двухмерной ассоциативной алгебры над полем $GF(p)$ ($\lambda \neq 0$)

TABLE 2. Setting Two-Dimensional Associative Algebra Over Field GF(p) ($\lambda \neq 0$)

·	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$
$\boldsymbol{e}_0$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$
$\boldsymbol{e}_1$	$\boldsymbol{e}_1$	$\lambda\boldsymbol{e}_0$

В настоящей работе разрабатывается схема цифровой подписи, основанная на СЗДЛ и использующая коммутативную группу с двухмерной цикличностью в качестве скрытой группы. Важным моментом является задание скрытой группы, содержащей элементы достаточно большого простого порядка. Это может быть реализовано при выборе характеристики p поля $GF(p)$, равной простому числу вида $p = 2q + 1$, где q – 256-битное простое число. При таком выборе и значении λ, являющимся квадратичным вычетом, мультипликативная группа двухмерной алгебры, заданной по таблице 2, имеет двухмерное циклическое строение и содержит подгруппу $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$ порядка q^2, генерируемую некоторым базисом $<\boldsymbol{G}, \boldsymbol{Q}>$, где каждый из двухмерных векторов $\boldsymbol{G}$ и $\boldsymbol{Q}$ имеет порядок, равный простому числу q. Легко установить, что группа $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$ включает единичный вектор $(1, 0)$ и $q^2 - 1$ различных векторов, имеющих одно и тоже значение порядка, равное простому числу q. Группа $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$ включает $q + 1$ циклических подгрупп порядка q. Любой фиксированный вектор, отличный от $(1, 0)$, содержится в единственной циклической подгруппе.

Свойства алгебраического носителя

В работе [14] показано, что двухсторонней глобальной единицей четырехмерной КНАА, заданной по таблице 1, является вектор $\boldsymbol{E} = (\mu^{-1}, \lambda^{-1}, 0, 0)$, а порядок мультипликативной группы этой алгебры равен значению:

$$\Omega = p(p-1)(p^2-1). \tag{3}$$

При этом для произвольного заданного вектора $\boldsymbol{Q} = (q_0, q_1, q_2, q_3)$ доказаны следующие положения:

1) условие обратимости вектора $\boldsymbol{Q}$ выражается формулой $q_0 q_1 \neq q_2 q_3$ [14];

2) условие необратимости вектора $\boldsymbol{Q}$ выражается формулой $q_0 q_1 = q_2 q_3$ [14];

3) множество всех векторов, перестановочных с $\boldsymbol{Q}$, описывается следующей формулой [14]:

$$\boldsymbol{X} = (x_0, x_1, x_2, x_3) = \\ = \left(d, \frac{\mu q_2 d + (\lambda q_1 - \mu q_0)h}{\lambda q_2}, h, \frac{q_3}{q_2} h\right), \tag{4}$$

где $d, h = 0,1, \ldots, p-1$.

Множество (4) включает p^2 различных векторов, в том числе вектор $\boldsymbol{Q}$, нулевой элемент (0,0,0,0) и единицу $\boldsymbol{E}$.

Утверждение 1 [14]. Любые два элемента $\boldsymbol{V}$ и $\boldsymbol{W}$, входящие в множество (4), являются взаимно перестановочными, т. е. имеет место равенство $\boldsymbol{W} \cdot \boldsymbol{V} = \boldsymbol{V} \cdot \boldsymbol{W}$.

Утверждение 2 [15]. Подмножество обратимых векторов, входящих в множество (4) образуют мультипликативную коммутативную группу с единицей $\boldsymbol{E}$.

Утверждение 3 [15]. Координаты ненулевых необратимых векторов, содержащихся в множестве (4) удовлетворяют следующему равенству:

$$h = \left(\frac{\lambda q_1 - \mu q_0}{2\lambda q_3} \pm \sqrt{\frac{(\lambda q_1 - \mu q_0)^2}{4\lambda^2 q_3^2} + \frac{\mu q_2}{\lambda q_3}} \right) d. \qquad (5)$$

Используя равенство (5), можно подсчитать число необратимых и обратимых векторов, содержащихся в множестве (4).

Рассмотрим следующие два случая.

Случай 1. *Вектор **Q** является обратимым элементом*. Если координаты **Q** таковы, что подкоренное выражение в (5) является квадратичным невычетом в поле $GF(p)$, то все ненулевые векторы, входящие в (4), являются обратимыми. Легко заметить, что в этом случае операции умножения и сложения векторов являются замкнутыми в (4) и удовлетворяют свойствам операций конечного поля характеристики p, т. е. множество векторов (4) образует поле $GF(p^2)$, мультипликативная группа которого является циклической и имеет порядок $p^2 - 1$. Для построения схемы цифровой подписи важным является существование обратимых векторов, порядок которых равен $p^2 - 1$ и произвольному заданному делителю $p^2 - 1$.

Если подкоренное выражение в (5) является квадратичным вычетом в поле $GF(p)$, то формула (4) для каждого из значений $d = 0,1, \ldots, p - 1$ при двух различных значениях h, определяемых формулой (5), задает пару ненулевых необратимых векторов, т. е. с учетом нулевого вектора в множестве (4) имеем $2p - 1$ необратимых векторов и $p^2 - (2p - 1) = (p - 1)^2$ обратимых. Значение порядка группы обратимых векторов $\Omega = (p - 1)^2$ подсказывает, что они образуют конечную группу с двухмерной цикличностью. Пусть α — примитивный элемент поля $GF(p)$, тогда вектор-скаляр $\alpha\boldsymbol{E}$ входит в указанную группу и имеет порядок $p - 1$. Всевозможные степени вектора $\alpha\boldsymbol{E}$ генерируют $p - 1$ различных векторов. Пусть обратимый вектор $\boldsymbol{V}$ (например, $\boldsymbol{V} = \boldsymbol{Q}$), входящий в множество (4) и непредставимый в виде степени вектора $\alpha\boldsymbol{E}$ имеет порядок $p - 1$. Тогда легко показать, что базис $<\alpha\boldsymbol{E}, \boldsymbol{V}>$ генерирует коммутативную группу $\Gamma_{<\alpha\boldsymbol{E},\boldsymbol{V}>}$ порядка $(p - 1)^2$, имеющую двухмерное циклическое строение. Единицей группы $\Gamma_{<\alpha\boldsymbol{E},\boldsymbol{V}>}$ является вектор $\boldsymbol{E}$. Так как $\Gamma_{<\alpha\boldsymbol{E},\boldsymbol{V}>}$ включает только обратимые векторы, перестановочные с $\boldsymbol{Q}$, то $\Gamma_{<\alpha\boldsymbol{E},\boldsymbol{V}>}$ является группой обратимых векторов множества (4). Для построения предлагаемой схемы цифровой подписи важным является наличие в используемом алгебраическом носителе достаточно большого числа коммутативных групп с двухмерной цикличностью как подмножеств алгебраических элементов. (В общем случае различные векторы **Q** задают различные группы с двухмерной цикличностью.)

Случай 2. *Вектор **Q** является необратимым элементом*. Допустим, что координаты вектора **Q** удовлетворяют условию $q_0q_1 = q_2q_3$, т. е. он является необратимым. Из условия необратимости получаем $q_2 = q_3^{-1}q_0q_1$ и представление формулы (5) в следующем виде:

$$h = \begin{cases} \dfrac{q_1}{q_3} d \\ -\dfrac{\mu q_0}{\lambda q_3} d \end{cases}, \qquad (6)$$

где $d = 1, 2, \ldots, p - 1$. Из (6) следует, что множество (4) включает $2(p - 1)$ необратимых векторов, отличных от нулевого вектора, и $p^2 - 2(p - 1) - 1 = (p - 1)^2$ обратимых векторов. Множество последних включает все вектор-скаляры $i\boldsymbol{E}$, где $i = 1, 2, \ldots, p - 1$, и образует конечную коммутативную группу порядка $(p - 1)^2$, обладающую двухмерной цикличностью.

Таким образом, группу с двухмерной цикличностью (ее базис) можно задать, генерируя необратимый вектор **Q** и вычисляя по формулам (4) и (6) некоторый вектор **X** порядка $p - 1$ (для различных значений d проверяем значение порядка вектора **X**), т. е. имеем еще один способ задания группы с двухмерной цикличностью. В работе [15] доказано, что в случае необратимого вектора **Q** множество (4) действительно содержит обратимый вектор, отличный от вектор-скаляра и имеющий значение порядка $p - 1$.

Способ выполнения критерия постквантовой стойкости

Для построения схемы цифровой подписи, удовлетворяющей общему критерию постквантовой стойкости, представляет интерес использовать идею, предложенную ранее в работе [10] и заключающуюся в применении маскирующего умножения элементов скрытой циклической группы простого порядка q на перестановочные с ними элементы из другой циклической группы, также имеющей порядок q. В принципе данная идея может быть реализована при задании скрытой группы, имеющей двухмерное или многомерное циклическое строение. При этом могут быть применены различные способы формирования открытых параметров схемы цифровой подписи с использованием указанного маскирующего умножения. Однако практический интерес представляют способы, которые обеспечивают существенное уменьшение размера подписи по сравнению со схемой цифровой подписи [10]. С этой целью предлагается следующий способ формирования открытого ключа при использовании КНАА, заданной по таблице 1, в качестве алгебраического носителя:

1) сформировать базис $<\boldsymbol{G}, \boldsymbol{Q}>$ коммутативной группы $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$, включающий векторы порядка q; обратимые векторы **G** и **Q** являются секретными и задают скрытую группу $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$, обладающую двухмерной цикличностью;

2) сгенерировать случайные обратимые четырехмерные векторы $\boldsymbol{A}$ и $\boldsymbol{B}$ порядка $p^2 - 1$;

3) сгенерировать случайное натуральное число $x < q$ и вычислить вектор $\boldsymbol{U} = \boldsymbol{A} \cdot \boldsymbol{G}^x \cdot \boldsymbol{B}^{-1}$ (умножение слева на $\boldsymbol{A}$ и умножение справа на $\boldsymbol{B}^{-1}$ маскируют группу $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$, в которой выполняется операция экспоненцирования в степень x; при этом отображение вектора $\boldsymbol{G}^x$ в вектор $\boldsymbol{U}$ не является коммутативным с операцией экспоненцирования);

4) вычислить вектор $\boldsymbol{Y} = \boldsymbol{B} \cdot \boldsymbol{G} \cdot \boldsymbol{Q} \cdot \boldsymbol{B}^{-1}$ (эта формула задает автоморфное отображение вектора $\boldsymbol{G} \cdot \boldsymbol{Q}$, которое является взаимно коммутативным с операцией экспоненцирования);

5) сгенерировать случайное натуральное число $u < q$ ($u \neq x$) и вычислить вектор $\boldsymbol{Z} = \boldsymbol{B} \cdot \boldsymbol{Q}^u \cdot \boldsymbol{A}^{-1}$.

Левое умножение на $\boldsymbol{B}$ и правое на $\boldsymbol{A}^{-1}$ задает маскирующее отображение вектора $\boldsymbol{Q}^u$, которое не является коммутативным с операцией экспоненцирования. Однако это отображение и отображение, используемое в ходе применения указанного выше способа формирования открытого ключа, позволяют построить композиционные отображения, обладающие свойством взаимной коммутативности с операцией экспоненцирования. Последнее используется в процедуре проверки подлинности цифровой подписи и для обеспечения корректности разработанной схемы цифровой подписи. Открытым ключом является тройка векторов $\boldsymbol{U}$, $\boldsymbol{Y}$ и $\boldsymbol{G}$. Размер открытого ключа ($\boldsymbol{U}$, $\boldsymbol{Y}$, $\boldsymbol{Z}$) равен 768 байт.

Первый этап формирования открытого ключа состоит в генерация базиса $<\boldsymbol{G}, \boldsymbol{Q}>$ скрытой коммутативной группы с двухмерной цикличностью. Для задания группы $\Gamma_{<\boldsymbol{G},\boldsymbol{Q}>}$ предлагается следующий алгоритм генерации двух независимых порождающих векторов $\boldsymbol{G}$ и $\boldsymbol{Q}$.

Шаг 1.1. Сгенерировать случайный необратимый вектор $\boldsymbol{R}$.

Шаг 1.2. Выбирая случайное значение d ($1 < d < p - 1$) и используя формулы (4) и (6), вычислить обратимый вектор $\boldsymbol{X}$.

Шаг 1.3. Проверить, является ли число q порядком вектора $\boldsymbol{X}$. Если порядок вектора $\boldsymbol{X}$ не равен q или $\boldsymbol{X}$ является вектор-скаляром, то перейти к шагу 1.2. (с учетом того, что $p = 2q + 1$, легко показать, что в среднем потребуется выполнить ≈4 раза шаги 1.2 и 1.3 для перехода к шагу 1.4).

Шаг 1.4. Взять в качестве первого элемента базиса скрытой группы вектор $\boldsymbol{G} = \boldsymbol{X}$.

Шаг 1.5. Сгенерировать натуральное число β, где ($1 < \beta < p - 1$), и порядок которого по модулю p равен значению q; затем вычислить второй элемент $\boldsymbol{Q}$ базиса скрытой группы: $\boldsymbol{Q} = \beta \boldsymbol{E} \cdot \boldsymbol{X}$.

Второй этап формирования открытого ключа состоит в генерации случайных обратимых векторов $\boldsymbol{A}$ и $\boldsymbol{B}$ порядка $p^2 - 1$ и выполняется следующим образом.

Шаг 2.1. Сгенерировать случайный обратимый вектор $\boldsymbol{R} = (r_0, r_1, r_2, r_3)$ с координатами $r_2 \neq 0$ и $r_3 \neq 0$.

2.2. Вычислить значения (см. формулу (5)):

$$\delta = \left(\frac{(\lambda r_1 - \mu r_0)^2}{4\lambda^2 r_3^2} + \frac{\mu r_2}{\lambda r_3}\right) \mathrm{mod} p,$$

$$\varepsilon = \delta^q \mathrm{mod} p.$$

Шаг 2.3. Если $\varepsilon = p - 1$, то значение подкоренного выражения формулы (5), записанной для вектора $\boldsymbol{R}$, является квадратичным невычетом (в соответствии с критерием Эйлера) и множество векторов, перестановочных с $\boldsymbol{R}$, содержат векторы порядка $p^2 - 1$.

Шаг 2.4. Если $\varepsilon = 1$, то перейти к шагу 2.1.

Шаг 2.5. Сгенерировать пару случайных значений d ($1 < d < p - 1$) и h ($1 < h < p - 1$).

Шаг 2.6. В соответствии с формулой (3) вычислить вектор:

$$\boldsymbol{X} = \left(d, \frac{\mu r_2 d + (\lambda r_1 - \mu r_0) h}{\lambda r_2}, h, \frac{r_3}{r_2} h\right).$$

Шаг 2.7. Если одновременно выполняются неравенства $\boldsymbol{X}^2 \neq \boldsymbol{E}$ и $\boldsymbol{X}^q \neq \boldsymbol{E}$, то в качестве вектора порядка $p^2 - 1$ взять вектор $\boldsymbol{V} = \boldsymbol{X}$.

Все случайно генерируемые векторы и числа, использованные в ходе процесса вычисления открытого ключа, относятся к секретным параметрам. Открытыми параметрами схемы цифровой подписи являются элементы открытого ключа и параметры задания четырехмерной алгебры, используемой в качестве алгебраического носителя криптосхемы.

Соответствие общему критерию стойкости к квантовым атакам и корректность разработанной схемы цифровой подписи обеспечивается комбинированием согласованных маскирующих операций двух различных типов: 1) свободных от свойства взаимной коммутативности с операцией экспоненцирования и 2) обладающих этим свойством. Без знания секретных векторов $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{G}$ и $\boldsymbol{Q}$ предположительно задание периодической функции, в которой содержатся периоды с длиной, зависящей от значений x и u, является вычислительно невыполнимой задачей (нахождение x и u представляет собой задачу дискретного логарифмирования в скрытой группе).

Так, рассмотрим периодическую функцию:

$$F_1(i, j) = (\boldsymbol{U} \cdot \boldsymbol{Y} \cdot \boldsymbol{Z})^i (\boldsymbol{U} \cdot \boldsymbol{Z})^j =$$
$$= \boldsymbol{A} \cdot \boldsymbol{G}^{xi+i+xj} \cdot \boldsymbol{Q}^{i+ui+uj} \cdot \boldsymbol{A}^{-1}.$$

Пусть длина периода этой функции равна (δ_i, δ_j). Тогда в силу независимости векторов $\boldsymbol{G}$ и $\boldsymbol{Q}$ при условии $\Delta = (1 + x)u - (1 + u)x \neq 0$ (Δ — главный детерминант следующей системы линейных уравнений с неизвестными δ_i и δ_j) имеем:

$$\begin{cases} x\delta_i + \delta_i + x\delta_j \equiv 0 \bmod q \\ \delta_i + u\delta_i + u\delta_j \equiv 0 \bmod q \end{cases} \Rightarrow \begin{cases} \delta_i \equiv 0 \bmod q \\ \delta_j \equiv 0 \bmod q \end{cases},$$

т. е. функция $F_1(i, j)$ содержит только периоды, длина которых равны значениям (kq, tq) при целочисленных значениях k и t (вероятность выполнения условия $\Delta = 0$ пренебрежимо мала). Легко показать, что последнее относится и к следующим двум периодическим функциям:

$$F_2(i,j) = (\boldsymbol{Z} \cdot \boldsymbol{U})^i \boldsymbol{Y}^j = \boldsymbol{B} \cdot \boldsymbol{Q}^{ui+j} \cdot \boldsymbol{G}^{xi+j} \cdot \boldsymbol{B}^{-1};$$

$$F_3(i,j) = (\boldsymbol{U} \cdot \boldsymbol{Z})^i \cdot \boldsymbol{U} \cdot \boldsymbol{Y}^j = \boldsymbol{A} \cdot \boldsymbol{G}^{xi+x+j} \cdot \boldsymbol{Q}^{ui+j} \cdot \boldsymbol{B}^{-1}.$$

Процедуры генерации и проверки подлинности цифровой подписи

Вычисление подписи к электронному документу M предлагается выполнять по следующему алгоритму (рисунок 1a):

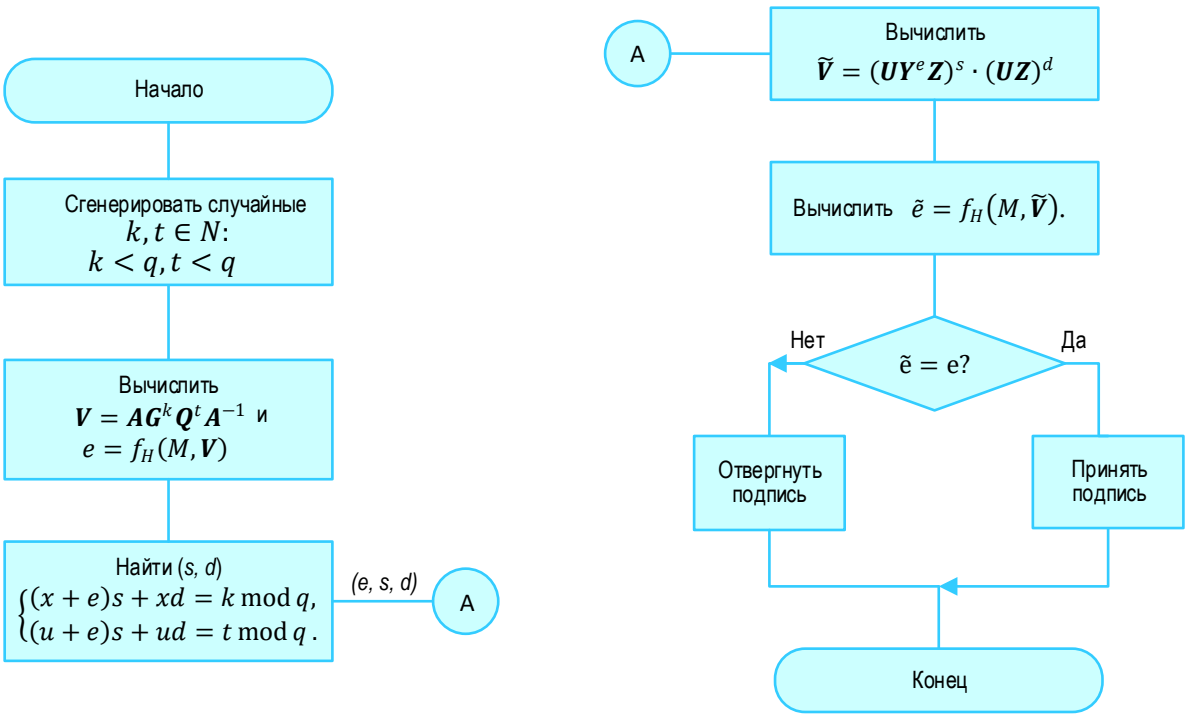
1) сгенерировать случайные натуральные числа $k < q$ и $t < q$ и вычислить вектор $\boldsymbol{V}$:

$$\boldsymbol{V} = \boldsymbol{A} \cdot \boldsymbol{G}^k \cdot \boldsymbol{Q}^t \cdot \boldsymbol{A}^{-1};$$

2) вычислить первый элемент подписи в виде двоичного числа $e = f_H(M, \boldsymbol{V})$, где f_H – некоторая специфицированная 256-битная хэш-функция, удовлетворяющая требованию строгой коллизионной стойкости;

3) вычислить второй s и третий d элементы цифровой подписи как решение следующей системы уравнений первой степени:

$$\begin{cases} (x+e)s + xd = k \bmod q; \\ (u+e)s + ud = t \bmod q. \end{cases}$$



a) b)

Рис. 1. Алгоритм вычисления (a) и проверка (b) цифровой подписи

Fig. 1. Calculation Algorithm (a) and Verification Algorithm (b) of Digital Signature

Подписью является тройка 256-битных чисел (e, s, d) и имеет длину 96 байт. Вычислительная сложность процедуры вычисления подписи приближенно может быть оценена как две операции возведения четырехмерных векторов в 256-битную степень.

Проверка подлинности цифровой подписи (рисунок 1b) осуществляется по открытому ключу $(\boldsymbol{U}, \boldsymbol{Y}, \boldsymbol{Z})$, используя следующий алгоритм:

1) вычислить значение $\widetilde{\boldsymbol{V}}$:

$$\widetilde{\boldsymbol{V}} = (\boldsymbol{U} \cdot \boldsymbol{Y}^e \cdot \boldsymbol{Z})^s \cdot (\boldsymbol{U} \cdot \boldsymbol{Z})^d;$$

2) вычислить значение хэш-функции от документа с присоединенным к нему вектором $\widetilde{\boldsymbol{V}}$:

$$\tilde{e} = f_H(M, \widetilde{\boldsymbol{V}});$$

3) при выполнении равенства $\tilde{e} = e$ подпись признается подлинной (в противном случае подпись признается ложной).

Докажем корректность предложенной схемы цифровой подписи. Допустим, что подпись (e, s, d) была вычислена в соответствии с алгоритмом генерации подписи. Тогда на первом шаге проверочной процедуры будет вычислен вектор:

$$\tilde{\boldsymbol{V}} = (\boldsymbol{U} \cdot \boldsymbol{Y}^e \cdot \boldsymbol{Z})^s \cdot (\boldsymbol{U} \cdot \boldsymbol{Z})^d =$$
$$= (\boldsymbol{A} \cdot \boldsymbol{G}^x \cdot \boldsymbol{B}^{-1} \cdot \boldsymbol{B} \cdot \boldsymbol{G} \cdot \boldsymbol{Q} \cdot \boldsymbol{B}^{-1}\boldsymbol{B} \cdot \boldsymbol{Q}^u \cdot \boldsymbol{A}^{-1})^s \cdot$$
$$\cdot (\boldsymbol{A} \cdot \boldsymbol{G}^x \cdot \boldsymbol{B}^{-1} \cdot \boldsymbol{B} \cdot \boldsymbol{Q}^u \cdot \boldsymbol{A}^{-1})^d =$$
$$= \boldsymbol{A} \cdot \boldsymbol{G}^{xs} \cdot \boldsymbol{G}^{es} \cdot \boldsymbol{Q}^{es} \cdot \boldsymbol{Q}^{us} \cdot \boldsymbol{G}^{xd} \cdot \boldsymbol{Q}^{ud} \cdot \boldsymbol{A}^{-1} =$$
$$= \boldsymbol{A} \cdot \boldsymbol{G}^{xs+es+xd} \cdot \boldsymbol{Q}^{es+us+ud} \cdot \boldsymbol{A}^{-1} =$$
$$= \boldsymbol{A} \cdot \boldsymbol{G}^{(x+e)s+xd} \cdot \boldsymbol{Q}^{(e+u)s+ud} \cdot \boldsymbol{A}^{-1} =$$
$$= \boldsymbol{A} \cdot \boldsymbol{G}^k \cdot \boldsymbol{Q}^t \cdot \boldsymbol{A}^{-1} = \boldsymbol{V}\,.$$

Поскольку $\tilde{V} = V$, то на втором шаге проверочной процедуры будет вычислено значение $\tilde{e}$, удовлетворяющие равенству $\tilde{e} = e$, т. е. подпись признается подлинной, что доказывает корректность разработанной схемы цифровой подписи.

Сопоставление с известными постквантовыми схемами цифровой подписи

С точки зрения компромисса между производительностью и размером открытого ключа и подписи предпочтительными представляются следующие два кандидата на постквантовый стандарт цифровой подписи, которые предложены в ходе конкурса НИСТ: Falcon [16] и Dilithium [17]. Сравнение разработанной постквантовой схемы цифровой подписи с указанными кандидатами и схемой цифровой подписи из работы [10] представлено в таблице 3 (сравнение выполнено для версий для версий алгоритмов Falcon и Dilithium, соответствующих уровню 128-битной стойкости). Схемы цифровой подписи, разработанные на основе СЗДЛ, обладают значительно меньшими размерами подписи и открытого ключа. При этом предложенная схема цифровой подписи является более производительной.

ТАБЛИЦА 3. Сравнение разработанной авторами схемы цифровой подписи с известными аналогами

TABLE 3. A Rough Comparison of the Developed by the Authors Signature Scheme with Known Analogues

Схема цифровой подписи	Длина, байт		Скорость, отн. ед.	
	цифровой подписи	открытого ключа	генерации цифровой подписи	верификации цифровой подписи
[16]	657	897	5	3
[17]	2044	1184	2	1
[10]	192	768	4	3
Авторская схема	96	384	15	10

Заключение

Предложен новый способ построения схем цифровой подписи, удовлетворяющих общему критерию постквантовой стойкости, который позволяет существенно сократить размер подписи по сравнению со способом, описанным в работе [10]. На основе способа разработана конкретная постквантовая схема цифровой подписи, которая представляется более практичной по сравнению с известными кандидатами на постквантовый стандарт цифровой подписи, предложенными в ходе конкурса НИСТ [2] по разработке постквантовых двухключевых криптосхем.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 21-57-54001-Вьет_а).

Список используемых источников

1. Ding J., Steinwandt R. Post-Quantum Cryptography // Revised Selected Papers of the 10th International Conference (PQCrypto 2019, Chongqing, China, 8–10 May 2019). Lecture Notes in Computer Science. Security and Cryptology. Springer, 2019. Vol. 11505. 418 p.

2. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register. 2016. Vol. 81. No. 244. Available from: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf [Accessed 24th May 2021]

3. Молдовян А.А., Молдовян Д.Н. Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2(125). С. 23–32.

4. Moldovyan N.A., Moldovyan A.A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // ВестникЮУрГУ. Серия «Математическое моделирование и программирование». 2019. Т. 12. № 1. С. 66–81. DOI:10.14529/mmp190106

5. Молдовян Н.А., Абросимов И.К Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18–22.

6. 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. No. 3(78). PP. 301–313.

7. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer // SIAM Review. 1999. Vol. 41. Iss. 2. PP. 303–332. DOI:10.1137/S0036144598347011

8. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm // Reviews of Modern Physics. 1996. Vol. 68. PP. 733. DOI:10.1103/RevModPhys.68.733

9. Jozsa R. Quantum algorithms and the Fourier transform // Proceedings of the Royal Society A. Mathematical, Physical and Engineering Sciences. 1998. Vol. 454. Iss. 1969. PP. 323–337. DOI:10.1098/rspa.1998.0163

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. №. 4. С. 455–461. DOI:10.21638/11701/spbu10.2020.410

11. 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.
12. Moldovyan N.A. Fast signatures based on non-cyclic finite groups // Quasigroups and Related Systems. 2010. Vol. 1. No. 18. PP. 83–94.
13. Moldovyan N.A., Moldovyanu P.A. New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. Vol. 2. No. 17. PP. 271–282.
14. Фахрутдинов Р.Ш., Мирин А.Ю, Молдовян Д.Н., Костина А.А. Схемы открытого согласования ключей на основе скрытой задачи дискретного логарифмирования // Информационные технологии. 2020. Т. 26. № 10. С. 577–585. DOI:10.17587/it.26
15. Гурьянов Д.Ю., Молдовян Д.Н., Молдовян А.А. Постквантовые схемы цифровой подписи: задание скрытой группы с двухмерной цикличностью // Информатизация и связь. 2020. № 4. С. 75–82. DOI:10.34219/2078-8320-2020-11-4-75-82
16. Fast-Fourier Lattice-Based Compact Signatures over NTRU // Falcon. URL: https://falcon-sign.info (дата обращения 24.05.2021)
17. Dilithium Home // CRYSTALS. Cryptographic Suite for Algebraic Lattices. URL: https://pq-crystals.org/dilithium/index.shtml (дата обращения 24.05.2021)

* * *

Digital Signature Scheme with Hidden Group Possessing Two-Dimensional Cyclicity

D. Moldovyan[1], R. Fahrutdinov[1], A. Mirin[1], A. Kostina[1]

[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-2-85-93
Received 29th April 2021
Accepted 23rd May 2021

For citation: Moldovyan D., Fahrutdinov R., Mirin A., Kostina A. Digital Signature Scheme with Hidden Group Possessing Two-Dimensional Cyclicity. *Proc. of Telecom. Universities.* 2021;7(2):85–93. (in Russ.) DOI:10.31854/1813-324X-2021-7-2-85-93

Abstract: *A method is proposed for constructing digital signature schemes based on the hidden discrete logarithm problem, which meet ageneral criterion of post-quantum resistance. The method provides a relatively small size of the public key and signature. Based on the method, a practical digital signature scheme has been developed, in which the exponentiation operation in a hidden group with two-dimensional cyclicity is the basic cryptographic primitive. The algebraic support of a cryptoscheme is a four-dimensional finite non-commutative algebra with associative multiplication operation. By specifying algebra using abasis vector multiplication table with half of empty cells, the performance of signature generation and authentication procedures is improved. A public key is a triple of four-dimensional vectors calculated as images of elements of a hidden group which are mapped using two types of masking operations: 1) mutually commutative with the exponentiation operation and 2) not having this property.*

Keywords: *information protection, computer security, cryptography, digital signature, post-quantum cryptoscheme, discrete logarithm problem, finite associative algebra, non-commutative algebra, hidden group.*

FUNDING

This research was funded by RFBR according to the research project 21-57-54001 Viet_a.

References

1. Ding J., Steinwandt R. Post-Quantum Cryptography. *Revised Selected Papers of the 10th International Conference, PQCrypto 2019, Chongqing, China, 8–10 May 2019. Lecture Notes in Computer Science. Security and Cryptology*. Springer; 2019. vol.11505. 418 p.
2. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. *Federal Register*. 2016;81(244). Available from: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf [Accessed 24th May 2021]

3. Moldovyan A.A., Moldovyan D.N. Post-Quantum Digital Signature Protocols Based on the Hidden Discrete Logarithm Problem. *Information Security Questions* (Voprosy zaŝity informacii). 2019;2(125):23–32.

4. Moldovyan N.A., Moldovyan A.A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem. *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software*. 2019;12(1):66–81. DOI:10.14529/mmp190106

5. Молдовян Н.А., Молдовян Д.Н. Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18–22.

6. Moldovyan A.A., Moldovyan N.A. Post-quantum signature algorithms based on the hidden discrete logarithm problem. *Computer Science Journal of Moldova*. 2018;26(3(78)):301–313.

7. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer. *SIAM Review*. 1999;41(2):303–332. DOI:10.1137/S0036144598347011

8. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*. 1996;68:733. DOI:10.1103/RevModPhys.68.733

9. Jozsa R. Quantum algorithms and the Fourier transform. *Proceedings of the Royal Society A. Mathematical, Physical and Engineering Sciences*. 1998;454(1969):323–337. DOI:10.1098/rspa.1998.0163

10. Moldovyan N.A., Moldovyan A.A. Candidate for practical post-quantum signature scheme. *Vestnik of St Petersburg University. Applied Mathematics. Computer Science. Control Processes*. 2020;16(4):455–461. DOI:10.21638/11701/spbu10.2020.410

11. Moldovyan N.A. Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security. *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*. 2020;2(93):62–67.

12. Moldovyan N.A. Fast signatures based on non-cyclic finite groups. *Quasigroups and Related Systems*. 2010;1(18):83–94.

13. Moldovyan N.A., Moldovyanu P.A. New primitives for digital signature algorithms. *Quasigroups and Related Systems*. 2009;2(17):271–282.

14. Fahrutdinov R.S., Mirin A. Yu., Moldovyan D.N., Kostina A.A. Public Key – Agreement Schemes Based on the Hidden Discrete Logarithm Problem. *Information Technologies* (Informacionnye Tehnologii). 2020;26(10):577–585. DOI:10.17587/it.26

15. Guryanov D.Yu., Moldovyan D.N., Moldovyan A.A. Post-Quantum Digital Signature Schemes: Setting a Hidden Group with Two-Dimensional Cyclicity. *Informatizatsiia i sviaz*. 2020;4:75–82. DOI:10.34219/2078-8320-2020-11-4-75-82

16. Fast-Fourier Lattice-Based Compact Signatures over NTRU. *Falcon*. URL: https://falcon-sign.info [Accessed 24th May 2021]

17. Dilithium Home. *CRYSTALS. Cryptographic Suite for Algebraic Lattices*. URL: https://pq-crystals.org/dilithium/index.shtml [Accessed 24th May 2021]

Сведения об авторах:

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

ФАХРУТДИНОВ Роман Шафкатович
кандидат технических наук, заведующий лабораторией кибербезопасности и постквантовых криптосистем Санкт-Петербургского Федерального исследовательского центра Российской академии наук, fahr@cobra.ru

МИРИН Анатолий Юрьевич
кандидат технических наук, старший научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского Федерального исследовательского центра Российской академии наук, mirin@cobra.ru

КОСТИНА Анна Александровна
научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского Федерального исследовательского центра Российской академии наук, anna-kostina1805@mail.ru