УДК 003.26 DOI: 10.17587/it.26.577-585

Р. Ш. Фахрутдинов, канд. техн. наук, зав. лабораторией, e-mail: fahr@cobra.ru,
А. Ю. Мирин, канд. техн. наук, ст. науч. сотр., e-mail: mirin@cobra.ru,
Д. Н. Молдовян, канд. техн. наук, науч. сотр., e-mail: mdn.spectr@mail.ru,
А. А. Костина, науч. сотр., e-mail: anna-kostina1805@mail.ru,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
г. Санкт-Петербург

Схемы открытого согласования ключей на основе скрытой задачи дискретного логарифмирования[1]

Рассмотрены схемы открытого согласования ключа, основанные на вычислительной сложности скрытой задачи дискретного логарифмирования, задаваемой в конечных некоммутативных ассоциативных алгебрах. Для повышения производительности предложены алгебры с заданием операции векторного умножения с помощью прореженных таблиц умножения базисных векторов и процедура генерации перестановочных ключевых элементов, свободная от операций экспоненцирования.

Ключевые слова: *защита информации, криптография, открытое согласование ключей, задача дискретного логарифмирования, конечная ассоциативная алгебра, некоммутативная алгебра, глобальная единица, локальная единица, левосторонняя единица*

Введение

В настоящее время прогресс в области квантовых вычислений достиг такого уровня, при котором высокую степень актуальности приобрела проблема разработки криптографических алгоритмов и протоколов с открытым ключом, обеспечивающих высокую стойкость к квантовым атакам, т.е. атакам с использованием квантового компьютера [1—3]. Криптосхемы, удовлетворяющие этому условию, называются постквантовыми, т.е. ориентированными на применение в эпоху квантовых вычислений, наступление которой прогнозируется на ближайшее будущее [4].

Указанная проблема связана с тем, что современные двухключевые криптосхемы, имеющие широкое применение для решения многочисленных задач в области обеспечения информационной безопасности и кибербезопасности, основаны на вычислительной трудности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), которые на квантовом компьютере могут быть решены за полиномиальное время [5—8]. Полиномиальные квантовые алгоритмы решения ЗДЛ и ЗФ используют возможность сведения этих задач к задаче определения длины периода некоторой периодической функции, принимающей дискретные значения в рамках явно заданной конечной циклической группы. В частности, при решении ЗДЛ строится периодическая функция, длина одного из периодов которой зависит от искомого значения логарифма. Квантовый компьютер чрезвычайно эффективно реализует дискретное преобразование Фурье, из максимумов которого вычисляются длины периодов преобразованной функции [9, 10].

Для разработки постквантовых криптографических алгоритмов и протоколов используют вычислительно трудные задачи, отличные от ЗДЛ и ЗФ. Перспективным подходом к разработке постквантовых двухключевых криптосхем является применение в качестве базового криптографического примитива скрытой задачи дискретного логарифмирования (СЗДЛ) [11—13]. На основе этого примитива предложены протоколы открытого согласования ключа [14] и электронной цифровой подписи (ЭЦП) [15, 16], а также алгоритмы коммутативного

[1] Работа выполнена при поддержке бюджетной темы № 0060-2019-0010.

шифрования [17, 18]. В качестве алгебраического носителя таких криптосхем используются некоммутативные конечные ассоциативные алгебры (НКАА) [19—22], содержащие в себе большое число различных конечных циклических групп в качестве подмножеств элементов алгебры.

В данной статье рассматриваются известные протоколы открытого согласования ключа, построенные на основе вычислительной трудности СЗДЛ, и предлагается и обосновывается новый способ построения криптосхем данного типа, который позволяет повысить их вычислительную эффективность. Предлагаемый способ отличается использованием в качестве алгебраического носителя криптосхем НКАА с операцией умножения, задаваемой по прореженным таблицам умножения базисных векторов (ТУБВ).

1. Задание скрытой задачи дискретного логарифмирования

Традиционная ЗДЛ формулируется следующим образом. Известен открытый ключ Y', представляющий собой некоторый элемент конечной циклической группы, вычисленный путем выполнения операции возведения в целочисленную степень достаточно большой разрядности:

$$Y' = N^x,$$

где N — генератор конечной циклической группы; x — секретный ключ. Нахождение значения x по известным элементам N и Y' называется ЗДЛ. В случае группы, имеющей значение ее порядка, равное многоразрядному простому числу q (длиной 256 бит и более), для обычного компьютера известны только сверхполиномиальные алгоритмы решения ЗДЛ, задаваемой в мультипликативной группе поля $GF(p)$ и в ряде других конечных групп.

На квантовом компьютере ЗДЛ решается как задача вычисления длины периода функции $f(i, j) = Y'^i N^j$ с натуральными значениями i и j, которая содержит период длины $(-1, x)$:

$$Y'^i N^j = Y'^{i-1} N^{j+x} \Rightarrow f(i, j) = f(i-1, j+x).$$

Для функции $f(i, j)$ со значениями в явно заданной конечной циклической группе квантовый компьютер эффективно выполняет дискретное преобразование Фурье, что позволяет за полиномиальное время найти длины всех периодов функции $f(i, j)$, в том числе и значение $(-1, x)$, а следовательно, и значение дискретного логарифма x.

Различные формы СЗДЛ возникают при построении двухключевых криптосхем, в которых основной операцией, определяющей высокий уровень стойкости, является операция возведения в степень, выполняемая в некоторой скрытой циклической группе, содержащейся в НКАА. Маскирование этой группы реализуется тем, что оба элемента N и N^x группы или один из них предоставляются в виде открытых параметров Y и Z криптосхемы после дополнительного маскирующего преобразования с помощью операций ψ_1 и ψ_2, являющихся взаимно коммутативными с операцией возведения в степень экспоненцирования: $Y = \psi_1(N^x)$ и $Z = \psi_2(N)$. При этом секретные маскирующие операции выбираются такими, что значения Y и Z лежат в разных циклических группах, каждая из которых отлична от группы, генерируемой всевозможными степенями элемента N.

Для корректности работы схемы ЭЦП маскирующие операции ψ_1 и ψ_2 должны быть согласованы между собой, что дает возможность построения периодических функций по значениям элементов открытого ключа. Например, в схемах ЭЦП, описанных в работах [23—25], открытым ключом является пара значений Y и Z, по которым может быть построена периодическая функция $f(i, j) = Y^i Z$, включающая период, имеющий длину $(-1, x)$, однако эта функция принимает значения, лежащие во многих различных циклических группах. Это обеспечивает стойкость к квантовым атакам на основе известных квантовых алгоритмов вычисления длины периода.

В схемах открытого согласования ключей предполагается, что независимые пользователи выполняют базовую операцию экспоненцирования в одной и той же циклической группе, поэтому кроме открытого ключа в криптосхемах данного типа должен быть задан другой известный параметр, позволяющий выполнить указанное условие. В рассматриваемом случае маскирование базовой циклической группы обеспечивается только маскированием результата выполнения операции экспоненцирования, т.е. открытый ключ включает элементы $Y = \psi_1(N^x)$ и N. Однако, несмотря на кажущуюся ослабленной маскировку, периодические функции, построенные с использованием значений Y и N, не содержат период, определяемый значением дискретного логарифма, а включают периоды, связанные со значением порядка q базовой циклической группы.

2. Некоммутативные конечные алгебры с ассоциативной операцией умножения

Конечные m-мерные алгебры представляют собой конечные m-мерные векторные пространства, заданные над конечным полем, например, над простым конечным полем $GF(p)$, в которых дополнительно к имеющимся операциям сложения векторов и скалярного умножения определена операция векторного умножения (далее операция умножения), которая является дистрибутивной слева и справа относительно операции сложения. Для построения двухключевых криптосхем на основе СЗДЛ используются НКАА, поэтому при задании операции умножения в векторном пространстве применяется способ определения этой операции по таблицам умножения базисных векторов (ТУБВ), позволяющий обеспечить свойство ассоциативности операции умножения.

Элементами m-мерного векторного пространства являются всевозможные векторы вида

$$\mathbf{A} = (a_0, a_1, \ldots, a_{m-1}) = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1},$$

где $a_i \in GF(p)$, где p — простое число; $\mathbf{e}_i$ — формальные базисные векторы. Операция умножения ($\circ$) векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ определяется по следующей формуле

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

где каждое из произведений пар базисных векторов заменяется на однокомпонентный вектор $\lambda\mathbf{e}_k$, задаваемый специально разработанной ТУБВ. Значение $\lambda \in GF(p)$ называется структурной константой. Рассмотрим произведение трех векторов $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C} = \sum_{k=0}^{m-1} c_k\mathbf{e}_k$, осуществляемое в соответствии со следующими двумя вариантами:

$$(\mathbf{A} \circ \mathbf{B}) \circ \mathbf{C} = \left(\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j\right) \circ \sum_{k=0}^{m-1} c_k\mathbf{e}_k = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} a_i b_j c_k (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k; \qquad (2)$$

$$\mathbf{A} \circ (\mathbf{B} \circ \mathbf{C}) = \left(\sum_{i=0}^{m-1} a_i\mathbf{e}_i\right) \circ \left(\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} b_j c_k \mathbf{e}_i \circ \mathbf{e}_j\right) = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} a_i b_j c_k \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k). \qquad (3)$$

Таблица 1

Задание операции умножения четырехмерной НКАА ($\mu \neq 0$; $\lambda \neq 0$)

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

Таблица 2

Задание операции умножения в шестимерной НКАА ($\lambda \neq 0$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	$\mathbf{e}_2$	0	$\mathbf{e}_4$	0
$\mathbf{e}_1$	$\lambda\mathbf{e}_3$	0	$\lambda\mathbf{e}_5$	0	$\lambda\mathbf{e}_1$	0
$\mathbf{e}_2$	0	$\mathbf{e}_4$	0	$\mathbf{e}_0$	0	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_3$	0	$\mathbf{e}_5$	0	$\mathbf{e}_1$	0
$\mathbf{e}_4$	$\lambda\mathbf{e}_0$	0	$\lambda\mathbf{e}_2$	0	$\lambda\mathbf{e}_4$	0
$\mathbf{e}_5$	0	$\mathbf{e}_1$	0	$\mathbf{e}_3$	0	$\mathbf{e}_5$

Равенство правых частей выражений (2) и (3) имеет место, если используемая ТУБВ обеспечивает выполнение равенства

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) \qquad (4)$$

для всех возможных троек значений (i, j, k).

Известен ряд частных ТУБВ для реализации НКАА с фиксированным значением размерности векторов [19] и унифицированные способы построения ТУБВ [20—22] для произвольных четных значений размерности m. Из формулы (1) легко видеть, что вычислительная сложность операции умножения определяется вычислительной сложностью операции умножения в поле $GF(p)$ и числом этих операций, поэтому для уменьшения сложности базовой операции экспоненцирования (т.е. для повышения производительности разрабатываемых криптосхем) представляет интерес разработка прореженных ТУБВ, в которых в достаточно большом числе ячеек содержится структурный коэффициент, равный нулю.

Для случаев размерностей $m = 4$ и $m = 6$ в данном исследовании разработаны и используются ТУБВ указанного типа, которые показаны как табл. 1 и табл. 2.

3. Свойства четырехмерной НКАА

Решение векторных уравнений вида

$$\mathbf{X} \circ \mathbf{A} = \mathbf{A} \qquad (5)$$

и

$$\mathbf{A} \circ \mathbf{X} = \mathbf{A}, \qquad (6)$$

где $\mathbf{A} = (a_0, a_1, a_2, a_3)$ — некоторый заданный четырехмерный вектор; $\mathbf{X} = (x_0, x_1, x_2, x_3)$ — неизвестный вектор, приводит к получению следующей формулы для глобальной двухсторонней единицы **E**, содержащейся в алгебре:

$$\mathbf{E} = (\mu^{-1}, \lambda^{-1}, 0, 0). \quad (7)$$

Здесь используется термин "глобальная" для обозначения того, что данная единица действует на все элементы алгебры как двухсторонняя единица (в отличии от локальных единиц, действующих в подмножествах элементов алгебры).

Для преобладающего множества четырехмерных векторов рассматриваемой алгебры, координаты которых удовлетворяют условию $a_0a_1 \neq a_2a_3$, уравнения (5) и (6) имеют единственное решение $\mathbf{X} = \mathbf{E}$ (в случае $a_0a_1 = a_2a_3$ кроме этого решения имеется много других решений). Векторы, удовлетворяющие условию $a_0a_1 \neq a_2a_3$, являются обратимыми, т. е. для них каждое из векторных уравнений $\mathbf{X} \circ \mathbf{A} = \mathbf{A}$ и $\mathbf{A} \circ \mathbf{X} = \mathbf{A}$, имеет единственное решение $\mathbf{X} = \mathbf{A}^{-1}$, которое называется обратным значением вектора **A**. В случае $a_0a_1 = a_2a_3$ последние два векторных уравнения не имеют решений. Векторы, удовлетворяющие последнему условию, называются необратимыми. Из условия необратимости легко установить число необратимых векторов, которое равно $p^3 + p^2 - p$. Число всех четырехмерных векторов равно значению p^4, поэтому для числа обратимых векторов Ω (порядок мультипликативной группы алгебры) получаем следующую формулу:

$$\Omega = p(p-1)(p^2-1). \quad (8)$$

Каждый обратимый вектор $\mathbf{V} = (v_0, v_1, v_2, v_3)$ задает операцию автоморфного отображения, описываемую формулой

$$\varphi(\mathbf{X}) = \mathbf{V} \circ \mathbf{X} \circ \mathbf{V}^{-1}, \quad (9)$$

где переменная **X** пробегает все значения алгебры, которая является взаимно коммутативной с операцией экспоненцирования и представляет интерес как маскирующая операция при задании СЗДЛ.

В случае построения схем открытого согласования ключей маскирующие операции выполняются двумя пользователями в различной очередности, и порядок их выполнения не должен влиять на значение получаемого результата (общего секретного ключа), поэтому выбираемые пользователями маскирующие операции должны быть взаимно коммутативными, оставаясь при этом секретными. Взаимная коммутативность маскирующих операций, выбираемых любыми двумя пользователями, может быть обеспечена, если задать выбор вектора **V** как параметра операции автоморфного отображения из одной и той же коммутативной группы, содержащейся в алгебре. При этом порядок этой коммутативной группы должен быть достаточно большим. В работах [23, 24] эта проблема решается путем задания в качестве открытого параметра криптосхемы некоторого вектора **Q**, имеющего достаточно большой порядок ω, и механизма выбора вектора **V** путем использования случайного натурального числа $x < \omega$ и вычисления значения $\mathbf{V} = \mathbf{Q}^x$.

Недостатками этого способа являются ограничение множества потенциально возможных значений **V** и необходимость выполнения операции экспоненцирования, что повышает вычислительную трудоемкость процедуры формирования ключевых параметров пользователей. Для устранения этих недостатков предлагается способ задания полной коммутативной группы для выбора параметров маскирующей операции автоморфного отображения алгебры. Способ описывается следующим образом:

1) выбирается некоторый вектор

$$\mathbf{Q} = (q_0, q_1, q_2, q_3);$$

2) выводится формула, описывающая все векторы, которые перестановочны с **Q**;

3) по указанной формуле каждый пользователь вычисляет случайный вектор **V**, используемый для задания секретной операции маскирования.

Для векторов **X**, являющихся перестановочными с **Q**, выполняется условие $\mathbf{X} \circ \mathbf{Q} = \mathbf{Q} \circ \mathbf{X}$, т. е. множество векторов **X** являются решениями векторного уравнения $\mathbf{X} \circ \mathbf{Q} - \mathbf{Q} \circ \mathbf{X} = (0,0,0,0)$, которое сводится к решению следующей системы из четырех линейных уравнений с неизвестными x_0, x_1, x_2 и x_3:

$$\begin{cases} \mu x_0 q_0 + \lambda x_3 q_2 - \mu x_0 q_0 - \lambda x_2 q_3 = 0; \\ \lambda x_1 q_1 + \mu x_2 q_3 - \lambda x_1 q_1 - \mu x_3 q_2 = 0; \\ \lambda x_1 q_2 + \mu x_2 q_0 - \lambda x_2 q_1 - \mu x_0 q_2 = 0; \\ \mu x_0 q_3 + \lambda x_3 q_1 - \mu x_3 q_0 - \lambda x_1 q_3 = 0. \end{cases} \quad (10)$$

В этой системе первое уравнение совпадает со вторым, а третье — с четвертым. Легко установить, что все решения системы (10) описываются формулой

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = \left(d, \frac{\mu q_2 d + (\lambda q_1 - \mu q_0) h}{\lambda q_2}, h, \frac{q_3}{q_2} h \right), \quad (11)$$

где d, $h = 0,1, \ldots, p-1$. Множество (11) содержит p^2 различных векторов, включая нулевой элемент (0, 0, 0, 0) и единицу $(\mu^{-1}, \lambda^{-1}, 0, 0)$ алгебры.

Утверждение 1. Любые два вектора **V** и **W** из множества (11) являются перестановочными, т. е. для них выполняется условие $\mathbf{W} \circ \mathbf{V} = \mathbf{V} \circ \mathbf{W}$.

Доказательство. Выполняется непосредственной проверкой с использованием формулы (11) для двух произвольных пар значений (d_1, h_1) и (d_2, h_2).

4. Свойства шестимерной НКАА

Характерной особенностью шестимерной НКАА, задаваемой табл. 2, является наличие в ней большого множества глобальных левосторонних единиц. Для нахождения формулы, описывающей это множество, следует рассмотреть векторное уравнение $\mathbf{X} \circ \mathbf{A} = \mathbf{A}$ при некотором фиксированном шестимерном векторе $\mathbf{A} = (a_0, a_1, a_2, a_3, a_4, a_5)$. С использованием табл. 2 указанное векторное уравнение сводится к следующей системе из шести линейных уравнений с неизвестными координатами вектора $\mathbf{X} = (x_0, x_1, x_2, x_3, x_4, x_5)$:

$$\begin{cases} (x_0 + \lambda x_4)a_0 + x_2 a_3 = a_0; \\ (\lambda x_1 + x_3)a_4 + x_5 a_1 = a_1; \\ (x_0 + \lambda x_4)a_2 + x_2 a_5 = a_2; \\ (\lambda x_1 + x_3)a_0 + x_5 a_3 = a_3; \\ (x_0 + \lambda x_4)a_4 + x_2 a_1 = a_4; \\ (\lambda x_1 + x_3)a_2 + x_5 a_5 = a_5. \end{cases} \quad (12)$$

Используя замену переменных по формулам $u_1 = x_0 + \lambda x_4$ и $u_2 = \lambda x_1 + x_3$, систему (12) можно представить в виде двух независимых систем из трех линейных уравнений:

$$\begin{cases} u_1 a_0 + x_2 a_3 = a_0; \\ u_1 a_2 + x_2 a_5 = a_2; \\ u_1 a_4 + x_2 a_1 = a_4; \end{cases} \quad (13)$$

$$\begin{cases} u_2 a_4 + x_5 a_1 = a_1; \\ u_2 a_0 + x_5 a_3 = a_3; \\ u_2 a_2 + x_5 a_5 = a_5. \end{cases} \quad (14)$$

Для произвольного вектора $\mathbf{A}=(a_0, a_1, a_2, a_3, a_4, a_5)$ система (13) имеет решение $(u_1, x_2) = (1, 0)$, а система (14) — решение $(u_2, x_5) = (0, 1)$. Путем обратной замены переменных получаем следующую формулу, описывающую множество p^2 глобальных левосторонних единиц $\mathbf{L} = (l_0, l_1, l_2, l_3, l_4, l_5)$, содержащихся в рассматриваемой НКАА:

$$\begin{aligned} &L = (d, h, 0, -\lambda h, \lambda^{-1}(1-d), 1), \\ &d, h = 0, 1, \ldots, p-1. \end{aligned} \quad (15)$$

Алгебра содержит локальные правосторонние единицы, которые могут быть вычислены из векторного уравнения $\mathbf{A} \circ \mathbf{X} = \mathbf{A}$, которое сводится к следующей тройке независимых систем из двух линейных уравнений с парами неизвестных значений (x_0, x_3), (x_1, x_4) и (x_2, x_5) соответственно:

$$\begin{cases} (a_0 + \lambda a_4)x_0 + a_2 x_3 = a_0; \\ (\lambda a_1 + a_3)x_0 + a_5 x_3 = a_3; \end{cases} \quad (16)$$

$$\begin{cases} a_5 x_1 + (\lambda a_1 + a_3)x_2 = a_1; \\ a_2 x_1 + (a_0 + \lambda a_4)x_2 = a_4; \end{cases} \quad (17)$$

$$\begin{cases} (a_0 + \lambda a_4)x_2 + a_2 x_5 = a_2; \\ (\lambda a_1 + a_3)x_2 + a_5 x_5 = a_5. \end{cases} \quad (18)$$

Главные определители систем (16), (17) и (18) равны $\Delta^{(16)} = -\Delta^{(17)} = \Delta^{(18)} = a_5(a_0 + \lambda a_4) - a_2(\lambda a_1 + a_3)$. Если координаты вектора **A** удовлетворяют условию $\Delta_A = \Delta^{(16)} \neq 0$, то к вектору **A** относится единственная локальная правосторонняя единица $\mathbf{R}_A = (r_0, r_1, r_2, r_3, r_4, r_5)$, координаты которой могут быть вычислены по следующим формулам:

$$r_0 = \frac{a_0 a_5 - a_2 a_3}{\Delta^{(16)}}; \; r_1 = \frac{a_0 a_1 - a_3 a_4}{\Delta^{(17)}};$$

$$r_1 = \frac{a_0 a_1 - a_3 a_4}{\Delta^{(17)}}; \; r_2 = 0;$$

$$r_3 = \frac{\lambda(a_3 a_4 - a_1 a_0)}{\Delta^{(16)}}; \; r_4 = \frac{a_4 a_5 - a_1 a_2}{\Delta^{(17)}};$$

$$r_5 = 1.$$

Легко доказать, что единица $\mathbf{R}_A$, относящаяся к произвольному вектору **A**, содержится в множестве глобальных левосторонних единиц (15). Следующие два утверждения достаточно очевидны.

Утверждение 2. Локальная правосторонняя единица $\mathbf{R}_A$ одновременно является локальной двухсторонней единицей $\mathbf{E}_A$, относящейся к вектору **A**.

Очевидно, что вектор **A** является обратимым относительно единицы $\mathbf{E}_A$, которая является единичным вектором конечной циклической группы, генерируемой степенями вектора **A**. Поэтому вектор **A** называется локально обратимым, если он удовлетворяет условию $\Delta_A = \Delta^{(16)} \neq 0$, т. е. условию

$$a_5(a_0 + \lambda a_4) - a_2(\lambda a_1 + a_3) \neq 0 \quad (19)$$

Утверждение 3. Пусть вектор **L** — глобальная левосторонняя единица. Тогда отображение алгебры, задаваемое формулой $\varphi_L(\mathbf{X}) = \mathbf{X} \circ \mathbf{L}$, где **X** пробегает все значения в рассматриваемой алгебре, является гомоморфизмом.

Доказательство. Для двух произвольных векторов $\mathbf{X}_1$ и $\mathbf{X}_2$ имеем:

$$\varphi_L(\mathbf{X}_1 \circ \mathbf{X}_2) = (\mathbf{X}_1 \circ \mathbf{X}_2) \circ \mathbf{L} =$$
$$= (\mathbf{X}_1 \circ \mathbf{L}) \circ (\mathbf{X}_2 \circ \mathbf{L}) = \varphi_L(\mathbf{X}_1) \circ \varphi_L(\mathbf{X}_2);$$
$$\varphi_L(\mathbf{X}_1 + \mathbf{X}_2) = (\mathbf{X}_1 + \mathbf{X}_2) \circ \mathbf{L} =$$
$$= (\mathbf{X}_1 \circ \mathbf{L}) + (\mathbf{X}_2 \circ \mathbf{L}) = \varphi_L(\mathbf{X}_1) + \varphi_L(\mathbf{X}_2).$$

Утверждение 4. Число локально обратимых векторов, содержащихся в рассматриваемой шестимерной алгебре, равно значению $\Omega = p^3(p-1)(p^2-1)$..

Доказательство. Найдем число η необратимых векторов. Координаты необратимого вектора $\mathbf{A} = (a_0, a_1, a_2, a_3, a_4, a_5)$ удовлетворяют условию $a_5(a_0 + \lambda a_4) - a_2(\lambda a_1 + a_3) = 0$. Число решений последнего уравнения с неизвестными a_0, a_1, a_2, a_3, a_4 и a_5 равно искомому значению η. В случае $a_5 \neq 0$ (имеем $p-1$ различных значений a_5) для каждого возможного набора значений координат a_0, a_1, a_3 и a_4 (p^4 вариантов) имеется единственное значение a_2, удовлетворяющее рассматриваемому уравнению, т. е. в случае $a_5 \neq 0$ имеется $p^4(p-1)$ необратимых векторов. В случае $a_5 = 0$ координаты a_0 и a_4 могут принимать произвольные значения (p^2 вариантов) при обязательном выполнении условия $a_2(\lambda a_1 + a_3) = 0$. Последнее дает $p^2 + p(p-1)$ вариантов, а в случае $a_5 = 0$ всего имеем $2p^4 - p^3$ необратимых векторов. Принимая во внимание оба рассмотренных случая, получаем $\eta = p^5 + p^4 - p^3$. В алгебре всего содержится p^6 различных векторов, из которых следует вычесть необратимые векторы, что дает следующее число локально обратимых векторов: $\Omega = p^6 - \eta = p^3(p-1)(p^2-1)$.

Пусть задана локальная правосторонняя единица $\mathbf{R}_A$. Она одновременно является и локальной двухсторонней единицей $\mathbf{E}_A$, относящейся к вектору $\mathbf{A}$. Очевидно, что полное подмножество векторов, относящихся к $\mathbf{E}_A$, составляет конечную группу Г с групповой единицей $\mathbf{E}_A$. Умножая каждый элемент группы Г на произвольную фиксированную глобальную левостороннюю единицу $\mathbf{L}$, получаем другую конечную группу, изоморфную с Г, единицей которой является вектор $\mathbf{R} \circ \mathbf{L} = \mathbf{L}$ (см. утверждение 3). Таким образом, каждая глобальная левосторонняя единица $\mathbf{L}$ задает существование в алгебре уникальной конечной группы с единицей $\mathbf{L}$. Поскольку имеется p^2 различных глобальных левосторонних единиц, то рассматриваемая шестимерная алгебра содержит p^2 различных изоморфных групп, порядок которых равен одному и тому же значению Ω'. Так как каждый локально обратимый вектор содержится только в одной из указанных групп, имеем $\Omega = p^2\Omega'$, откуда получаем формулу для порядка конечных групп, содержащихся в алгебре:

$$\Omega' = p(p-1)(p^2-1). \qquad (20)$$

Утверждение 5. Пусть $\mathbf{A} \circ \mathbf{B} = \mathbf{L}'$, где $\mathbf{L}'$ — глобальная левосторонняя единица. Тогда для произвольного натурального числа t выполняется равенство $\mathbf{A}^t \circ \mathbf{B}^t = \mathbf{L}'$.

Доказательство:

$$\mathbf{A}^t \circ \mathbf{B} = \mathbf{A}^{t-1} \circ (\mathbf{A} \circ \mathbf{B}) \circ \mathbf{B}^{t-1} = \mathbf{A}^{t-1} \circ \mathbf{B}^{t-1} =$$
$$= \mathbf{A}^{t-2} \circ (\mathbf{A} \circ \mathbf{B}) \circ \mathbf{B}^{t-2} = \mathbf{A}^{t-2} \circ \mathbf{B}^{t-2} = \mathbf{A} \circ \mathbf{B} = \mathbf{L}'.$$

Утверждение 6. Пусть $\mathbf{A} \circ \mathbf{B} = \mathbf{L}'$ и t — произвольнее натуральное число. Тогда формула $\psi_{L'} = \mathbf{B} \circ \mathbf{X} \circ \mathbf{A}$, где $\mathbf{X}$ пробегает все значения в рассматриваемой алгебре, является гомоморфизмом.

Доказательство. Для двух произвольных векторов $\mathbf{X}_1$ и $\mathbf{X}_2$ имеем:

$$\psi_{L'}(\mathbf{X}_1 \circ \mathbf{X}_2) = \mathbf{B} \circ (\mathbf{X}_1 \circ \mathbf{X}_2) \circ \mathbf{A} =$$
$$= \mathbf{B} \circ (\mathbf{X}_1 \circ \mathbf{L}' \circ \mathbf{X}_2) \circ \mathbf{A} =$$
$$= (\mathbf{B} \circ \mathbf{X}_1 \circ \mathbf{A}) \circ (\mathbf{B} \circ \mathbf{X}_2 \circ \mathbf{A}) =$$
$$= \psi_{L'}(\mathbf{X}_1) \circ \psi_{L'}(\mathbf{X}_2);$$
$$\psi_{L'}(\mathbf{X}_1 + \mathbf{X}_2) = \mathbf{B} \circ (\mathbf{X}_1 + \mathbf{X}_2) \circ \mathbf{A} =$$
$$= (\mathbf{B} \circ \mathbf{X}_1 \circ \mathbf{A}) + (\mathbf{B} \circ \mathbf{X}_2 \circ \mathbf{A}) =$$
$$= \psi_{L'}(\mathbf{X}_1) + \psi_{L'}(\mathbf{X}_2).$$

При использовании рассматриваемой шестимерной НКАА в качестве алгебраического носителя схемы открытого согласования ключей, основанной на СЗДЛ, маскирование базовой операции возведения в степень можно осуществить с помощью операции гомоморфного отображения $\psi_{L'}(\mathbf{X})$ с использованием в качестве общей пары векторов $\mathbf{A}$ и $\mathbf{B}$, удовлетворяющих условию $\mathbf{A} \circ \mathbf{B} = \mathbf{L}'$. В этом случае секретной является конкретная модификация данной операции, определяемая выбором секретного значения степени t, задающей конкретное гомоморфное преобразование, определяемое формулой $\psi_{L'}(\mathbf{X}) = \mathbf{B}^t \circ \mathbf{X} \circ \mathbf{A}^t$.

5. Схема открытого согласования ключа на основе СЗДЛ в четырехмерной алгебре

При использовании четырехмерной НКАА с операцией умножения, задаваемой по табл. 1, в качестве общих параметров схемы открытого согласования ключей выбирается 1) характеристика простого конечного поля $GF(p)$,

равная значению $p = 2q - 1$, где q — 256-битовое простое число; 2) обратимый вектор $\mathbf{N} = (n_0, n_1, n_2, n_3)$, порядок которого равен q; 3) обратимый вектор $\mathbf{Q}$, удовлетворяющий условию $\mathbf{N} \circ \mathbf{Q} \neq \mathbf{Q} \circ \mathbf{N}$, координаты которого q_0, q_1, q_2 и q_3 используются для выполнения вычисления случайных векторов $\mathbf{X}$ по формуле (11).

Генерация открытого ключа пользователя выполняется следующим образом:

1. Пользователь выбирает случайные натуральные числа $x < q$, $d < p$ и $h < p$.

2. По формуле (11) и случайно выбранным значениям d и h вычисляет вектор $\mathbf{X}$.

3. Вычисляет открытый ключ $\mathbf{Y} = \mathbf{X} \circ \mathbf{N}^x \circ \mathbf{X}^{-1}$.

Личным секретным ключом пользователя является число x и вектор $\mathbf{X}$. Общий секретный ключ двух пользователей формируется следующим образом. Первый пользователь, используя свой секретный ключ (x_1, $\mathbf{X}_1$) и открытый ключ $\mathbf{Y}_2$ второго пользователя, вычисляет вектор

$$\begin{aligned}\mathbf{Z}_1 &= \mathbf{X}_1 \circ \mathbf{Y}_2^{x_1} \circ \mathbf{X}_1^{-1} = \\ &= \mathbf{X}_1 \circ (\mathbf{X}_2 \circ \mathbf{N}^{x_2} \circ \mathbf{X}_2^{-1})^{x_1} \circ \mathbf{X}_1^{-1} = \\ &= \mathbf{X}_1 \circ \mathbf{X}_2 \circ \mathbf{N}^{x_2 x_1} \circ \mathbf{X}_2^{-1} \circ \mathbf{X}_1^{-1}.\end{aligned}$$

Второй пользователь, используя свой секретный ключ (x_2, $\mathbf{X}_2$) и открытый ключ $\mathbf{Y}_1$ первого пользователя, вычисляет вектор

$$\begin{aligned}\mathbf{Z}_2 &= \mathbf{X}_2 \circ \mathbf{Y}_1^{x_2} \circ \mathbf{X}_2^{-1} = \\ &= \mathbf{X}_2 \circ (\mathbf{X}_1 \circ \mathbf{N}^{x_1} \circ \mathbf{X}_1^{-1})^{x_2} \circ \mathbf{X}_2^{-1} = \\ &= \mathbf{X}_2 \circ \mathbf{X}_1 \circ \mathbf{N}^{x_1 x_2} \circ \mathbf{X}_1^{-1} \circ \mathbf{X}_2^{-1}.\end{aligned}$$

Учитывая перестановочность векторов $\mathbf{X}_1$ и $\mathbf{X}_2$, легко показать, что выполняется условие $\mathbf{Z}_1 = \mathbf{Z}_2$, т. е. оба пользователя вычисляют один и тот же вектор, который служит общим секретным ключом, согласованным по открытому каналу связи. При практическом использовании этой криптосхемы предполагается применение механизмов проверки подлинности открытых ключей пользователей, что является стандартным условием применения протоколов данного типа. Например, пользователи пересылают друг другу цифровые сертификаты, содержащие значения их открытых ключей и подписанные цифровой подписью удостоверяющего центра.

6. Схема открытого согласования ключа на основе СЗДЛ в шестимерной алгебре

При использовании шестимерной НКАА с операцией умножения, задаваемой по табл. 2, в качестве общих параметров схемы открытого согласования ключей выбирается 1) характеристика простого конечного поля $GF(p)$, равная значению $p = 2q - 1$, где q — 256-битовое простое число; 2) локально обратимый вектор $\mathbf{N} = (n_0, n_1, n_2, n_3)$, порядок которого равен q; 3) пара локально обратимых векторов $\mathbf{A}$ и $\mathbf{B}$, удовлетворяющих условию $\mathbf{A} \circ \mathbf{B} = \mathbf{L}$, , где $\mathbf{L}$ — глобальная левосторонняя единица.

Генерация открытого ключа пользователя выполняется следующим образом:

1. Пользователь выбирает случайные натуральные числа $x < q$ и $t < q$.

2. Вычисляет открытый ключ $\mathbf{Y} = \mathbf{B}^t \circ \mathbf{N}^x \circ \mathbf{A}^t$.

Личным секретным ключом пользователя является пара чисел x и t. Общий секретный ключ двух пользователей формируется следующим образом. Первый пользователь, используя свой секретный ключ (x_1, t_1) и открытый ключ $\mathbf{Y}_2$ второго пользователя, вычисляет вектор

$$\begin{aligned}\mathbf{Z}_1 &= \mathbf{B}^{t_1} \circ \mathbf{Y}_2^{x_1} \circ \mathbf{A}^{t_1} = \\ &= \mathbf{B}^{t_1} \circ (\mathbf{B}^{t_2} \circ \mathbf{N}^{x_2} \mathbf{A}^{t_2})^{x_1} \circ \mathbf{A}^{t_1} = \\ &= \mathbf{B}^{t_1 + t_2} \circ \mathbf{N}^{x_2 x_1} \circ \mathbf{A}^{t_2 + t_1}\end{aligned}$$

Второй пользователь, используя свой секретный ключ (x_2, t_2) и открытый ключ $\mathbf{Y}_1$ первого пользователя, вычисляет вектор

$$\begin{aligned}\mathbf{Z}_2 &= \mathbf{B}^{t_2} \circ \mathbf{Y}_1^{x_2} \circ \mathbf{A}^{t_2} = \\ &= \mathbf{B}^{t_2} \circ (\mathbf{B}^{t_1} \circ \mathbf{N}^{x_1} \mathbf{A}^{t_1})^{x_2} \circ \mathbf{A}^{t_2} = \\ &= \mathbf{B}^{t_2 + t_1} \circ \mathbf{N}^{x_1 x_2} \circ \mathbf{A}^{t_1 + t_2} = \mathbf{Z}_1.\end{aligned}$$

Таким образом, оба пользователя вычисляют один и тот же вектор, который служит общим секретным ключом, согласованным по открытому каналу связи.

Заключение

Предложены новые реализации схем открытого согласования ключа, основанные на вычислительной трудности скрытой задачи дискретного логарифмирования, в которых для повышения их производительности в качестве алгебраических носителей используются НКАА с операцией умножения, заданной по прореженным ТУБВ. Первая предложенная криптосхема использует вычисления в НКАА с глобальной двухсторонней единицей и новый механизм формирования маскирующей операции. Вторая предложенная криптосхема реализует маскирующие операции, ранее предложенные в работе [14], и отличается применением шестимерных НКАА, заданных по прореженной ТУБВ. Ранее прореженные ТУБВ использовались для задания четырехмерных НКАА.

Построение шестимерных НКАА, заданных по прореженной ТУББ, выполнено впервые.

Дальнейшее развитие протоколов открытого согласования ключа, основанных на СЗДЛ, представляет интерес в направлении применения новых типов маскирующих операций и использования в качестве алгебраических носителей НКАА, заданных над конечными расширениями двоичного поля $GF(2^s)$.

Список литературы

1. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24-26, 2016 // Lecture Notes in Computer Science (LNCS) series. Springer, 2016. Vol. 9606. 270 p.
2. **Federal Register**. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. URL: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения 16.04.2020).
3. **Post-Quantum** Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings // Lecture Notes in Computer Science series. Springer, 2018. Vol. 10786.
7. **Post-Quantum** Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019 // Lecture Notes in Computer Science. 2019. Vol. 11505. 420 p.
5. **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.
6. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring // Nature. 2013. Vol. 499, N. 7457. P. 163—165.
7. **Yan S. Y.** Quantum Computational Number Theory. Springer, 2015. 252 p.
8. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems. Springer, 2014. 207 p.
9. **Ekert A., Jozsa R.** Quantum computation and Shor's factoring algorithm // Rev. Mod. Phys. 1996. Vol. 68. P. 733.
10. **Jozsa R.** Quantum algorithms and the fourier transform // Proc. Roy. Soc. London Ser A. 1998. Vol. 454. P. 323-337.
11. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165—176.
12. **Кузьмин А. С., Марков В. Т., Михалев А. А., Михалев А. В., Нечаев А. А.** Криптографические алгоритмы на группах и алгебрах // Фундаментальная и прикладная математика. 2015. Т. 20, № 1. С. 205—222.
13. **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, N. 5. P. 629—641.
14. **Moldovyan D. N.** Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V.27, N. 1(79). P. 56—72.
15. **Moldovyan A. A., Moldovyan N. A.** Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. V. 26, N. 3(78). P. 301—313.
16. **Молдовян А. А., Молдовян Н. А.** Новые формы задания скрытой задачи дискретного логарифмирования // Труды СПИИРАН. 2019. № 2 (18). С. 504—529.
17. **Moldovyan A. A., Moldovyan D. N., Moldovyan N. A.** Post-quantum commutative encryption algorithm // Computer Science Journal of Moldova. 2019. V. 27, N. 3(81). P. 299—317.
18. **Абросимов И. К., Ковалева И. В., Молдовян Н. А.** Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3—13.
19. **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 (Bulletin SUSU MMCS). 2019. Vol. 12, N. 1. P. 66—81.
20. **Moldovyan A. A.** General Method for Defining Finite Non-commutative Associative Algebras of Dimension m>1 // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2018. N. 2 (87). P. 95—100.
21. **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.
22. **Moldovyan D. N.** A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. Vol. 27, N. 2. P. 293—308.
23. **Молдовян Н. А., Абросимов И. К.** Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15, Вып. 2. С. 212—220.
24. **Молдовян Н. А., Абросимов И. К.** Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
25. **Молдовян А. 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.

R. S. Fahrutdinov, Head of Laboratory, e-mail: fahr@cobra.ru,
A. Yu. Mirin, Senior Researcher, e-mail: mirin@cobra.ru,
D. N. Moldovyan, Researcher, e-mail: mdn.spectr@mail.ru,
A. A. Kostina, Researcher, e-mail: anna-kostina1805@mail.ru,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Public Key-Agreement Schemes Based on the Hidden Discrete Logarithm Problem

There is considered the problem of increasing the performance of the public kley-agreement schemes based on the computational complexity of the hidden discrete logarithm problem defined in finite non-commutative associative algebras of various types. To increase the rate of cryptoschemes of the said type, it is proposed to use algebras as their algebraic support, in which the associative multiplication operation is specified using sparse multiplication tables of basis vectors. In framework of this method the rate increase is achieved by a significant reduction in the number of multiplications in the finite field, over which the algebra is specified, which are necessary to perform one multiplication operation in the algebra. The principal realizability of this method has

been demonstrated for cases of four-dimensional and six-dimensional algebras, for which the sparse tables are given that specify the associative multiplication operation and providing two-times reduction of the number of multiplications in the field. Another proposed way to increase the rate is to specify the procedure for generating permutable key elements in the form of a computational procedure performed according to specially derived mathematical formulas, free from the operation of exponentiation to a large-size integer power. The second method is based on the idea of defining a set of mutually permutable vectors of a finite non-commutative associative algebra, described by a fairly compact mathematical formula. Moreover, the latter defines a procedure for calculating a random vector from the indicated set of vectors, which has significantly lower computational complexity compared to the exponentiation operation used in well-known cryptoschemes of the considered type to generate random pairs of permutable vectors. The potential feasibility of the second method is demonstrated by the derivation of the indicated formula for a four-dimensional algebra given by sparse multiplication tables of basis vectors. Specific public key-agreement cryptoschemes have been developed that implement the developed methods for increasing performance, which are of interest for practical use as post-quantum public key-agreement schemes. To further increase the performance of cryptoschemes of the considered type, it is proposed to use the algebras set over finite extensions of a binary field.

Keywords: *information protection, cryptography, public key-agreement, discrete logarithm problem, finite associative algebra, non-commutative algebra, global unit, local unit, left-sided unit*

Acknowledgements: This work was supported by the budget theme № 0060-2019-0010.

DOI: 10.17587/it.26.577-585

References

1. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24—26, 2016, *Lecture Notes in Computer Science (LNCS) series*, Springer, 2016, vol. 9606, 270 p.

2. **Federal** Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (date of access 16.04.2020).

3. **Post-Quantum** Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9—11, 2018, Proceedings, *Lecture Notes in Computer Science series*, Springer, 2018, vol. 10786.

4. **Post-Quantum** Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019, *Lecture Notes in Computer Science*, 2019, vol. 11505, 420 p.

5. **Shor P. W.** Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer, *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484—1509.

6. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring, *Nature*, 2013, vol. 499, no. 7457, pp. 163—165.

7. **Yan S. Y.** Quantum Computational Number Theory, Springer, 2015, 252 p.

8. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems, Springer, 2014, 207 p.

9. **Ekert A., Jozsa R.** Quantum computation and Shor's factoring algorithm, *Rev. Mod. Phys.*, 1996, vol. 68, pp. 733.

10. **Jozsa R.** Quantum algorithms and the fourier transform, *Proc. Roy. Soc. London Ser A*, 1998, vol. 454, pp. 323—337.

11. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes, *Quasigroups and Related Systems,* 2010, vol. 18, pp. 165—176.

12. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras, *Fundamental'naja i prikladnaja matematika*, 2015, vol. 20, no. 1, pp. 205—222 (in Russian).

13. **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.

14. **Moldovyan D. N.** Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem, *Computer Science Journal of Moldova,* 2019, vol.27, no. 1(79), pp. 56—72.

15. **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.

16. **Moldovyan A. A., Moldovyan N. A.** New Forms of Defining the Hidden Discrete Logarithm Problem, *Trudy SPIIRAN,* 2019, no. 2 (18), pp. 504—529 (in Russian).

17. **Moldovyan A. A., Moldovyan D. N., Moldovyan N. A.** Post-quantum commutative encryption algorithm, *Computer Science Journal of Moldova,* 2019, vol.27, no. 3(81), pp. 299—317.

18. **Abrosimov I. K., Kovaleva I. V., Moldovyan N. A.** Post-quantum protocol of keyless encryption, *Voprosy Zashhity Informacii,* 2017, no. 3, pp. 3—13 (in Russian).

19. **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 (Bulletin SUSU MMCS)*, 2019, vol. 12, no. 1, pp. 66—81.

20. **Moldovyan A. A.** General Method for Defining Finite Non-commutative Associative Algebras of Dimension m>1, *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica,* 2018, no. 2 (87), pp. 95—100.

21. **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.

22. **Moldovyan D. N.** A unified method for setting finite non-commutative associative algebras and their properties, *Quasigroups and Related Systems,* 2019, vol. 27, no. 2, pp. 293—308.

23. **Moldovyan N. A., Abrosimov I. K.** Post-quantum digital signature schemes based on the enhanced form of the hidden discrete logarithm problem, *Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja Matematika. Informatika. Processy Upravlenija,* 2019, vol. 15, iss. 2, pp. 212—220 (in Russian).

24. **Moldovyan N. A., Abrosimov I. K.** Post-quantum digital signature protocols based on the hidden discrete logarithm problem, *Voprosy Zashhity Informacii,* 2019, no. 2, pp. 23—32 (in Russian).

25. **Moldovyan A. A., Moldovyan D. N.** Post-quantum digital signature schemes based on the hidden discrete logarithm problem in four-dimensional finite algebra, *Voprosy Zashhity Informacii,* 2019, no. 2, pp. 18—22 (in Russian).