Computer Science Journal of Moldova, vol.**27**, no.1(79), 2019

Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem*

D.N. Moldovyan

Abstract

A new form of the hidden discrete logarithm problem, proposed as primitive of the post-quantum public-key cryptoschemes, is defined over the 6-dimensional finite non-commutative associative algebra with a large set of the left-sided global units. The considered computationally difficult problem uses the mutual commutativity of the exponentiation operation and homomorphism mapping defined relatively a fixed unit element of the algebra. The related properties of the introduced algebra are described. Novel public key-agreement and zero-knowledge protocols based on the hidden logarithm problem are introduced as post-quantum cryptoschemes.

Keywords: finite non-commutative algebra, associative algebra, computationally difficult problem, homomorphism, key agreement scheme, zero-knowledge protocol, post-quantum cryptoscheme

MSC 2010: 94A60, 16Z05, 14G50, 11T71, 16S50.

1 Introduction

Currently the most widely used in practice public key cryptographic algorithms and protocols are based on computational difficulty of the factoring problem (FP) and discrete logarithm problem (DLP) [1]. The FP and DLP are universal cryptographic primitives that allow

*The work is supported by the Russian Foundation for Basic Research grant # 18-07-00932-a.

designing on their base cryptoschemes of different types: public encryption and digital signature algorithms, public key-agreement and zero-knowledge authentication protocols, blind signature and multisignature schemes.

Both the FP and the DLP can be solved in polynomial time on a quantum computer [2], [3], therefore due to the latest progress in the quantum computation technology the cryptographic community has faced the challenge of developing the post-quantum public-key cryptoschemes, i. e., the cryptoschemes that resist the attacks with using both the ordinary computers and the quantum ones [4], [5]. Developers of the post-quantum public-key cryptoschemes look for suitable computational difficult problems different from the FP and DLP, which have superpolynomial computational difficulty when solving them on a quantum computer.

One of the latter computationally difficult problems, called conjugacy search problem, had been defined over braid groups representing a particular type of non-commutative groups [6], [7]. Using computations in the braid groups a number of different public-key cryptoschemes have been developed [8], [9]. The articles [10], [11] highlight some fundamental difficulties in using the conjugacy problem for developing cryptoschemes with superpolynomial security.

A promising approach to design the post-quantum cryptoschemes relates to combining the DLP with the problem of finding the conjugating element, which leads to the so-called hidden DLP (HDLP), i. e., to the DLP in a cyclic group hidden in the finite algebra of quaternions defined over the ground field $GF(p)$ [12], [13]. The computational complexity of the HDLP is superpolynomial in solving it on conventional computers. However, in [14] the polynomial reducibility of the HDLP in finite algebra of quaternions to the DLP in the field $GF(p^2)$ was shown. Therefore, using the form of the HDLP described in [12], [13] and the finite algebra of quaternions as its algebraic support can not be considered as a direct way to developing the post-quantum public-key algorithms and protocols. The search for new algebraic supports and new forms of the HDLP was noted in [14]–[16] as one of the conditions for the development of post-quantum cryptoschemes based on the

HDLP. In papers [15],[16] different types of the finite non-commutative associative algebras (FNAAs) are proposed as algebraic supports of the HDLP defined in new forms. New forms of the HDLP proposed in [16] are used as the base primitive for two different post-quantum digital signature schemes, however that forms of the HDLP do not suite for designing the public key-agreement schemes.

In present paper it is introduced a new form of the HDLP defined over the 6-dimensional FNAA containing a large set of the global left-sided units. The HDLP is defined relatively some specified left-sided unit and properties of the used FNAA connected with its unit elements are investigated. The public key-agreement scheme and zero-knowledge protocol based on the proposed form of the HDLP are introduced as candidates of the public-key post-quantum cryptoschemes.

2 The used 6-dimensional FNAA

Suppose the m-dimensional vector space is defined over the finite ground field $GF(p)$. Defining additionally the multiplication operation that is distributive relatively the addition operation one gets the m-dimensional finite algebra. If the multiplication operation is associative and non-commutative, then the algebra is called FNAA. To define the multiplication operation in the vector space one can use the representation of some vector $A = (a_0, a_1, \dots a_{m-1})$ in the form of the following summ of the single component vectors $a_i\mathbf{e}_i$: $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$, where $\mathbf{e}_0 = (1, 0, 0 \dots, 0)$, $\mathbf{e}_1 = (0, 1, 0 \dots, 0)$, ... $\mathbf{e}_{m-1} = (0, 0 \dots, 0, 1)$ are formal basis vectors.

The multiplication operation $\circ$ of two m-dimensional vectors A and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined as follows:

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

where every product of two babis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by some single-component vector $\lambda\mathbf{e}_k$ that is taken from the so called basis

vector multiplication table (BVMT), like Table 1. It is assumed that the intersection of the ith row and the jth column defines the cell indicating the value $\lambda\mathbf{e}_k = \mathbf{e}_i \circ \mathbf{e}_j$. If the structural coefficient $\lambda = 1$, then the mentioned single-component vector is written as $\mathbf{e}_k$.

To define a FNAA one should compose respective BVMT that defines non-commutative asssociative multiplication operation. A unified method for defining the FNAAs of arbitrary dimensions $m > 1$ is proposed in [17]. Investigation of the general properties of that FNAAs had shown that their characteristic property is the existence of large set of the global single-sided units. The FNAAs possessing such property are very interesting for using them as algebraic support of the public key-agreement schemes, in this case a new form of the HDLP is to be proposed though. The last is because the known form of the HDLP used in such type of cryptoschemes exploits existance of the global two-sided unit.

Since the FNAAs described in [17] allows trivial reduction of the HDLP to the DLP in the finite field $GF(p)$, in this paper a new 6-dimensional FNAA containing p^4 global left-sided units is introduced with the BVMT composed as follows. Initially a preliminary BVMT have been built using the following formula:

$$\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_{3i+j}, \tag{2}$$

where $i, j = 0, 1, \ldots, 5$ and computation of the value $3i+j$ is performed modulo 6.

Proposition 1. The formula (2) together with the formula (1) defines non-commutative associative multiplication operation of the 6-dimensional vectors.

Proof. Using the formula (1) one can get the following formula describing the product of the vectors A, B, and $C = \sum_{k=0}^{5} c_k\mathbf{e}_k$:

$$(A \circ B) \circ C = \sum_{i=0}^{5}\sum_{j=0}^{5}\sum_{k=0}^{5} a_i b_j c_k \left(\mathbf{e}_i \circ \mathbf{e}_j\right) \circ \mathbf{e}_k;$$

$$A \circ (B \circ C) = \sum_{i=0}^{5}\sum_{j=0}^{5}\sum_{k=0}^{5} a_i b_j c_k \mathbf{e}_i \circ \left(\mathbf{e}_j \circ \mathbf{e}_k\right).$$

This formula shows the multiplication operation is associative, since the formula (2) defines associative multiplication of every possible triple of the basis vectors. Indeed, for arbitrary possible three values i, j, and k we have the following

$$\left.\begin{array}{l}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{3i+j} \circ \mathbf{e}_k = \mathbf{e}_{9i+3j+k} = \mathbf{e}_{3i+3j+k} \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{3j+k} = \mathbf{e}_{3i+3j+k}\end{array}\right\} \Rightarrow$$

$$\Rightarrow (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)\,.$$

Thus, the formula (2) describes some preliminary BVMT defining the associative multiplication of the basis vectors. Then we have found experimentally the distributions of the structural coefficients $\lambda \neq 1$ and $\epsilon \neq 1$, which retain the property of the associativity of the multiplication operation. The resultant BVMT is shown as Table 1.

Table 1. The BVMT defining the 6-dimensional FNAA with p^4 different global left-sided units.

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

2.1 Some properties related to defining the HDLP

The left-sided units of the algebra introduced in Section 2 can be described as solutions of the following vector equation

$$X \circ A = A. \tag{3}$$

Using Table 1 one can represent (3) in the form of the following system of six linear equations with coordinates of the left operand $x_0, x_1, \ldots, x_5$

as the unknown values:

$$\begin{cases} \lambda x_0 a_0 + \epsilon x_1 a_3 + x_2 a_0 + \lambda x_3 a_3 + \epsilon x_4 a_0 + x_5 a_3 = a_0; \\ \lambda x_0 a_1 + \epsilon x_1 a_4 + x_2 a_1 + \lambda x_3 a_4 + \epsilon x_4 a_1 + x_5 a_4 = a_1; \\ \lambda x_0 a_2 + \epsilon x_1 a_5 + x_2 a_2 + \lambda x_3 a_5 + \epsilon x_4 a_2 + x_5 a_5 = a_2; \\ \lambda x_0 a_3 + \epsilon x_1 a_0 + x_2 a_3 + \lambda x_3 a_0 + \epsilon x_4 a_3 + x_5 a_0 = a_3; \\ \lambda x_0 a_4 + \epsilon x_1 a_1 + x_2 a_4 + \lambda x_3 a_1 + \epsilon x_4 a_4 + x_5 a_1 = a_4; \\ \lambda x_0 a_5 + \epsilon x_1 a_2 + x_2 a_5 + \lambda x_3 a_2 + \epsilon x_4 a_5 + x_5 a_2 = a_5. \end{cases} \tag{4}$$

The system (4) can be rewritten in the following form

$$\begin{cases} (\lambda x_0 + x_2 + \epsilon x_4)\, a_0 + (\epsilon x_1 + \lambda x_3 + x_5)\, a_3 = a_0; \\ (\epsilon x_1 + \lambda x_3 + x_5)\, a_0 + (\lambda x_0 + x_2 + \epsilon x_4)\, a_3 = a_3; \\ (\lambda x_0 + x_2 + \epsilon x_4)\, a_1 + (\epsilon x_1 + \lambda x_3 + x_5)\, a_4 = a_1; \\ (\epsilon x_1 + \lambda x_3 + x_5)\, a_1 + (\lambda x_0 + x_2 + \epsilon x_4)\, a_4 = a_4; \\ (\lambda x_0 + x_2 + \epsilon x_4)\, a_2 + (\epsilon x_1 + \lambda x_3 + x_5)\, a_5 = a_2; \\ (\epsilon x_1 + \lambda x_3 + x_5)\, a_2 + (\lambda x_0 + x_2 + \epsilon x_4)\, a_5 = a_5. \end{cases} \tag{5}$$

Performing the variable substitution $u_0 = \lambda x_0 + x_2 + \epsilon x_4$ and $u_1 = \epsilon x_1 + \lambda x_3 + x_5$ in the system (5) one gets the following three systems of two linear equations

$$\begin{cases} a_0 u_0 + a_3 u_1 = a_0; \\ a_3 u_0 + a_0 u_1 = a_3; \end{cases} \tag{6}$$

$$\begin{cases} a_1 u_0 + a_4 u_1 = a_1; \\ a_4 u_0 + a_1 u_1 = a_4; \end{cases} \tag{7}$$

$$\begin{cases} a_2 u_0 + a_5 u_1 = a_2; \\ a_5 u_0 + a_2 u_1 = a_5. \end{cases} \tag{8}$$

It is easy to see that for arbitrary vector A each of the equations of every of the systems (6), (7), and (8) holds true for the values of the unknowns

$u_0 = 1$ and $u_1 = 0$. This means that every vector X coordinates of which satisfy the conditions

$$u_0 = \lambda x_0 + x_2 + \epsilon x_4 = 1 \quad \text{and} \quad u_1 = \epsilon x_1 + \lambda x_3 + x_5 = 0 \qquad (9)$$

acts as the global left-sided units of the considered FNAA, i. e., the left-sided units acting on all elements of the algebra. Thus, we have the following formula describing the set of all p^4 global left-sided unit elements $L = (l_0, l_1, l_2, l_3, l_4, l_5)$:

$$L = (x_0, x_1, 1 - \lambda x_0 - \epsilon x_4, x_3, x_4, -\epsilon x_1 - \lambda x_3)\,, \qquad (10)$$

where $x_0, x_1, x_3, x_4 = 0, 1, 2, \ldots, p-1$.

Considering the systems (6), (7), and (8) one can state existence of two particular sets of the vectors $A = (a_0, a_1, a_2, a_3, a_4, a_5)$. The first particular set includes the vectors coordinates of which satisfy simultaneously the following three conditions $a_0 = a_3$, $a_1 = a_4$, and $a_2 = a_5$. The second particular set includes vectors satisfying simultaneously the conditions $a_0 = -a_3$, $a_1 = -a_4$, and $a_2 = -a_5$. To each of these particular sets there corresponds a large set of local left-sided units, i. e., the left-sided units acting only on vectors contained in the particular sets.

The local units acting on the vectors from the first set is described as follows

$$L' = (x_0, x_1, x_2, x_3, x_4, 1 - \lambda x_0 - x_2 - \epsilon x_4 - \epsilon x_1 - \lambda x_3)\,,$$

where $x_0, x_1, x_2, x_3, x_4 = 0, 1, 2, \ldots, p-1$.

The local units acting on the vectors from the second set is described as follows

$$L'' = (x_0, x_1, x_2, x_3, x_4, \lambda x_0 + x_2 + \epsilon x_4 - \epsilon x_1 - \lambda x_3 - 1)\,,$$

where $x_0, x_1, x_2, x_3, x_4 = 0, 1, 2, \ldots, p-1$.

For every vector A that is not contained in the first nor in the second set, the systems (6), (7), and (8) are satisfied simultaneously only for the case $u_0 = 1$ and $u_1 = 0$. Therefore, only the global left-sided units

act on every vector A that is not contained in the indicated particular sets.

Computing the right-sided units for some fixed vector A is connected with finding solutions of the vector equation

$$A \circ X = A. \tag{11}$$

Using Table 1 one can represent (11) in the form of the following system of six linear equations with coordinates of the right operand $x_0, x_1, \ldots, x_5$ as the unknown values:

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

The system (12) can be represented in the form of the following three independent systems of two linear equations

$$\begin{cases} (\lambda a_0 + a_2 + \epsilon a_4)\, x_0 + (\epsilon a_1 + \lambda a_3 + a_5)\, x_3 = a_0; \\ (\epsilon a_1 + \lambda a_3 + a_5)\, x_0 + (\lambda a_0 + a_2 + \epsilon a_4)\, x_3 = a_3; \end{cases} \tag{13}$$

$$\begin{cases} (\lambda a_0 + a_2 + \epsilon a_4)\, x_1 + (\epsilon a_1 + \lambda a_3 + a_5)\, x_4 = a_1; \\ (\epsilon a_1 + \lambda a_3 + a_5)\, x_1 + (\lambda a_0 + a_2 + \epsilon a_4)\, x_4 = a_4; \end{cases} \tag{14}$$

$$\begin{cases} (\lambda a_0 + a_2 + \epsilon a_4)\, x_2 + (\epsilon a_1 + \lambda a_3 + a_5)\, x_5 = a_2; \\ (\epsilon a_1 + \lambda a_3 + a_5)\, x_2 + (\lambda a_0 + a_2 + \epsilon a_4)\, x_5 = a_5. \end{cases} \tag{15}$$

The same main determinant Δ corresponds to each of the systems (13), (14), and (15):

$$\Delta_A = \alpha^2 - \beta^2, \tag{16}$$

where $\alpha = \lambda a_0 + a_2 + \epsilon a_4$ and $\beta = \epsilon a_1 + \lambda a_3 + a_5$. If $\Delta \neq 0$, then every of the systems (13), (14), and (15) has a unique solution, i. e., the vector

equation (11) also has a unique solution as the single right-sided unit R related to the vector A. It is easy to write the following formulas describing the vector $R_A = (r_0, r_1, r_2, r_3, r_4, r_5)$:

$$\begin{array}{lll} r_0 = \dfrac{a_0\alpha - a_3\beta}{\Delta_A}; & r_1 = \dfrac{a_1\alpha - a_4\beta}{\Delta_A}; & r_2 = \dfrac{a_2\alpha - a_5\beta}{\Delta_A}; \\ r_3 = \dfrac{a_3\alpha - a_0\beta}{\Delta_A}; & r_4 = \dfrac{a_4\alpha - a_1\beta}{\Delta_A}; & r_5 = \dfrac{a_5\alpha - a_2\beta}{\Delta_A}. \end{array} \tag{17}$$

Proposition 2. Suppose the vector A is such that $\Delta_A \neq 0$. Then the local right-sided unit R_A relating to A is contained in the set of the global left-sided units, i. e., there exists the single local two-sided unit E_A relating to the vector A that is equal to R_A.

Proof. Let us consider the formula (10) describing the set of the global left-sided units. Suppose $x_0 = r_0$, $x_1 = r_1$, $x_3 = r_3$, $x_4 = r_4$. Taking into account the formulas (17) computation of the coordinate x_2 gives the following

$$x_2 = 1 - \lambda r_0 - \epsilon r_4 = \frac{1}{\Delta_A}\left(\alpha^2 - \beta^2 - \lambda a_0\alpha + \lambda a_3\beta - \epsilon a_4\alpha + \epsilon a_1\beta\right) = \\ = \frac{1}{\Delta_A}\left(a_2\alpha - a_5\beta\right) = r_2.$$

Computation of the coordinate x_5 gives the following

$$x_5 = 1 - \epsilon r_1 - \lambda r_3 = \frac{1}{\Delta_A}\left(-\epsilon a_1\alpha + \epsilon a_4\beta - \lambda a_3\alpha + \lambda a_0\beta\right) = \\ = \frac{1}{\Delta_A}\left(a_5\left(\lambda a_0 + \epsilon a_4\right) - a_2\left(\epsilon a_1 + \lambda a_3\right)\right) = r_5.$$

Thus, the vector R_A is contained in the set of the global right-sided units (10). Proposition 2 is proven.

Proposition 3. Suppose the vector A is such that $\Delta_A \neq 0$. Then the local right-sided unit R_A relating to A relates also to the vector A^i for arbitrary natural value i.

Proof.

$$\left\{A \circ R_A = R_A \circ A = A\right\} \Rightarrow \\ \left\{A^i \circ R_A = A^{i-1} \circ A \circ R_A = A^i;\ R_A \circ A^i = R_A \circ A \circ A^{i-1} = A^i\right\}.$$

Proposition 4. Suppose the vector A is such that $\Delta_A \neq 0$. Then the sequence $A, A^2, \ldots, A^i, \ldots$ is periodic and for some positive integer ω we have $A^\omega = R_A$.

Proof. Suppose the sequence $A, A^2, \ldots, A^i, \ldots$ contains the zero vector $O = (0, 0, 0, 0, 0, 0)$. Then for some natural number j (for example, $j = 2$) we have $A^{j-1} \neq O$ and $A^j = O$, i. e., $A \circ A^{j-1} = O$. Since $\Delta_A \neq 0$ and $X = O$ satisfies the equation $A \circ X = O$, the last equation has a unique solution $X = O$. Therefore, $A^{j-1} = O$. The obtained contradiction proves that all values in the considered sequence are different from O.

The last fact and the finiteness of the considered algebra shows that for some natural numbers i and $t > i$ we have

$$\left\{A^i = A^t = A^{t-i} \circ A^i = A^i \circ A^{t-i}\right\} \Rightarrow E_{A^i} = A^{t-i}.$$

Due to uniqueness of the local two-sided unit and Proposition 3 we have $E_A = E_{A^i} = A^{t-i}$. Evidently, in the considered sequence there exists some minimum integer $t > i$ which defines some minimum integer $\omega = t - i$ such that $A^\omega = E_A = R_A$. The proposition 4 is proven.

The value ω can be called local order of the vector A. Respectively, the vectors A such that $\Delta_A \neq 0$ can be called locally invertible vectors.

Proposition 5. Suppose the vector A is such that $\Delta_A \neq 0$. Then $A \circ L_i \neq A \circ L_j$, if L_i and $L_j \neq L_i$ are arbitrary two different global left-sided units.

Proof. Suppose $A \circ L_i = A \circ L_j$. Then $A \circ (L_i - L_j) = O$. Since $\Delta_A \neq 0$, the vector equation $A \circ X = O$ has a unique solution $X = O$. Therefore, we have $L_i - L_j = O \Rightarrow L_i = L_j$. The obtained contradiction proves the Proposition 5.

Proposition 6. Suppose the vector equation $X \circ A = B$ has solution $X = S$. Then p^4 different values $X_i = S \circ L_i$, where L_i takes on all values from the set of the global left-sided units (10), also represent solutions of the given equation.

Proof. $(S \circ L_i) \circ A = S \circ (L_i \circ A) = S \circ A = B$. The Proposition 6 is proven.

3 The proposed new form of the HDLP

The known form of the HDLP [12] used in the public-key cryptoschemes is defined in the multiplicative group Γ of some FNAA (finite algebra of quaternions) with global two-sided unit, which is defined over the ground field $GF(p)$, as follows. Two 4-dimensional vectors $Q, G \in \Gamma$ having large prime order ω, which satisfy condition $G \circ Q \neq Q \circ G$, are selected. Then two uniformly random integers $t < \omega$ and $x < \omega$ are generated as the private key and the vector Y is computed as the public key:

$$Y = Q^t \circ G^x \circ Q^{\omega - t} = \left(Q^t \circ G \circ Q^{\omega - t}\right)^x . \tag{18}$$

Finding the pair of integers t and x from equation (18) when the values Q, G, and Y are known is called the HDLP. Finding the value x from the known value G^x, contained in the cyclic subgroup generated by the vector G, represents the DLP, however the value G^x is hidden due to automophism map defined as $Y = TG^xT^{-1}$, where the vector $T = Q^t$ is unknown. The public-key cryptoschemes described in [12] perform correctly due to mutual commutativity of the automophism-map operation and exponentiation operation (see formula (18)). In the paper [13] a potential attack that uses the homomorphism of the group Γ in the multiplicative group of the field $GF(p)$ is proposed. To prevent that attack we propose to define the HDLP in the FNAAs containing no global two-sided unit element (i. e., no globally invertible elements), for example in the 6-dimensional FNAA introduced in Section 2.

In the proposed form of the HDLP the following facts are used: **Proposition 7.** Suppose the product of two 6-dimensional vectors A and B is equal to the global left-sided unit L, i. e. $A \circ B = L$. Then for arbitrary natural number i the equality $A^i \circ B^i = L$ holds true.

Proof.
$A^i \circ B^i = A^{i-1} \circ \left(L \circ B^{i-1}\right) = A^{i-1} \circ B^{i-1} = A^{i-2} \circ B^{i-2} = \cdots = A \circ B = L$.

The Proposition 7 is proven.

Proposition 8. Suppose the product of two 6-dimensional vectors A and B is equal to the global left-sided unit L, i. e. $A \circ B = L$. Then

the map defined by the formula $\psi(X) = B \circ X \circ A$, where the vector X takes on all values in the considered FNAA, is a homomorphism.

Proof. Suppose X_1 and X_2 are arbitrary two 6-dimensional vectors. Then we have

$$\psi(X_1 \circ X_2) = B \circ (X_1 \circ X_2) \circ A = (B \circ X_1 \circ A) \circ (B \circ X_2 \circ A) = \psi(X_1) \circ \psi(X_2);$$

$$\psi(X_1 + X_2) = B \circ (X_1 + X_2) \circ A = (B \circ X_1 \circ A) + (B \circ X_2 \circ A) = \psi(X_1) + \psi(X_2).$$

The Proposition 8 is proven.

Proposition 9. The homomorphism map operation $\psi(X) = B \circ X \circ A$, where $A \circ B = L$, and the exponentiation operation X^i are mutually commutative, i. e., the equality $B \circ X^i \circ A = (B \circ X \circ A)^i$ holds true.

Proof. Due to Proposition 8 we have $\psi(X^i) = (\psi(X))^i$, i. e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The Proposition 9 is proven.

We propose to use as post-quantum cryptographic primitive the HDLP defined with the following formula for computing the public key:

$$Y = B^t \circ N^x \circ A^t = \left(B^t \circ N \circ A^t\right)^x, \tag{19}$$

where the vector N is such that $\Delta_N \neq 0$, besides the local order of the vector N contains a prime divisor having sufficiently large size.

4 Candidates for post-quantum public-key cryptoschemes

4.1 The public key-agreement scheme

The common parameters of the formula (19) defining computation of the public key Y after selection of the private key (t, x) are generated as follows:

1. Generate a 256-bit prime number $p = 2q + 1$, where q is prime, for example,

$p = 61307880204127427930866981627885239778341924428642533948984609893264740644403;$
$q = 30653940102063713965433490813942619889170962214321266974492304946632370322201.$

2. Generate a random locally invertible vector N having order $\omega = q$.

3. Generate a random locally invertible vector A having order $\omega = q$, which satisfies the condition $A \circ N \neq N \circ A$.

4. Select a random left-sided unit L.

5. Compute the vector B as solution of the vector equation $A \circ X = L$ with the unknown value X.

The first and second users generate their private keys (t_1, x_1) and (t_2, x_2) correspondingly. Then, using the formula (19) they compute their public keys Y_1 and Y_2. The public key-agreement scheme is described as follows:

1. The users exchange their public keys via a public channel.

2. The first user computes the 6-dimensional vector $Z_1 = B^{t_1} \circ Y_2^{x_1} \circ A^{t_1}$.

3. The second user computes the 6-dimensional vector $Z_2 = B^{t_2} \circ Y_1^{x_2} \circ A^{t_2}$.

Correctness proof of the protocol consists in proving that the both users compute the same value Z:

$$Z_1 = B^{t_1} \circ \left(B^{t_2} \circ N^{x_2} \circ A^{t_2}\right)^{x_1} \circ A^{t_1} = B^{t_1+t_2} \circ N^{x_2 x_1} \circ A^{t_2+t_1};$$
$$Z_2 = B^{t_2} \circ \left(B^{t_1} \circ N^{x_1} \circ A^{t_1}\right)^{x_2} \circ A^{t_2} = B^{t_2+t_1} \circ N^{x_1 x_2} \circ A^{t_1+t_2}.$$

Thus, after performing computations in frame of the described cryptoscheme the users share the same secrete value $Z_1 = Z_2$.

4.2 Zero-knowledge protocol

Zero-knowledge protocol is used for authentication of the remote users. It is a public-key method by which one user, owner of the public key, (called the prover) can prove to another one (called the verifier) that he knows the private key connected with his public key, without conveying any information apart from the fact that he knows the private

key. Security of the zero-knowledge protocols is based on the computational difficulty of finding the private key, when the public key is known. Therefore, the post-quantum protocols of such type should be based on the computational problems that are intractable for quantum computers.

To implement a post-quantum zero-knowledge protocol one can use the HDLP described in Section 4 and the method [18] for transforming a public key-agreement scheme into respective zero-knowledge protocol. The idea of such transformation is based on i) ability of two users to compute a common secrete value after exchange of their public keys and ii) applying the single-use public key of the verifier. The proposed protocol is described as follows. The prover is the owner of public key Y computed in correspondence with the formula (19), i. e., he knows the private key (t, x) connected with the vector Y, and the protocol includes the following two steps:

1. The verifier generates a pair of uniformly random natural numbers (g, k) (his single-use private key) and computes his single-use public key D and, using the public key of the prover Y, the value Z:

$$D = B^g \circ N^k \circ A^g; \quad Z = B^g \circ Y^k \circ A^g.$$

Then, using some specified secure hash function F_h, he computes the hash value $h = F_h(Z)$ and sends the values D and h to the prover.

2. The prover computes the value Z' (that is the single-use shared key connected with the public keys Y and D):

$$Z' = B^t \circ D^x \circ A^t.$$

Then he computes the hash value $h' = F_h(Z')$. If $h' = h$, the prover sends the value Z' to the verifier. Otherwise the prover responses "The request is incorrect". The verifier compares the values Z' and Z. If $Z' = Z$, he concludes the prover is genuine. Evidently, the response of the prover contains no information, with exception of the fact that the prover knows the private key (t, x) connected with the public key Y. To ensure that the verifier knows the value of the response Z', Bob checks whether the equality $h' = h$ holds true.

5 Conclusion

The introduced 6-dimensional FNAA does not contain the global two-sided unit, but includes p^4 different global left-sided units. Relatively the lasts one can define the operation of the homomorphism map, which is mutually commutative with the exponentiation operation. The mentioned commutativity and the local invertibility of the elements of the considered FNAA have been used to introduce a new form of the HDLP. The introduced form of the HDLP have been applied to develop the public key-agreement scheme and the zero-knowledge protocol that are proposed as candidates for the post-quantum public-key cryptoschemes. Estimation of their security to different possible quantum attacks appears to be an individual research task. One can suppose that the main approach in frame of such research is connected with the development of the potential quantum attacks on the proposed cryptoschemes which are connected with finding methods for reducing the used HDLP to the DLP in the extension field $GF(p^s)$ with the value $s = 1, 2, \ldots, 6$, like in the case of the HDLP in the finite algebra of quaternions [14].

References

[1] S. Y. Chiou, "Novel Digital Signature Schemes based on Factoring and Discrete Logarithms," *International Journal of Security and its Applications*, vol. 10, no. 3, pp. 295–310, 2016.

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

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

[4] *Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016, Fukuoka, Japan, February 24-26,*

2016 (Lecture Notes in Computer Science, vol. 9606), 2016, 270 p.

[5] *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018 Proceedings, Fort Lauderdale, FL, USA, April 9-11, 2018* (Lecture Notes in Computer Science, vol. 10786), 2018.

[6] I. Anshel, M. Anshel, and D. Goldfeld, "An Algebraic Method for Public Key Cryptography," *Mathematical Research Letters*, vol. 6, pp. 287–291, 1999.

[7] E. Lee and J. H. Park, "Cryptanalysis of the Public Key Encryption Based on Braid Groups," in *Advances in Cryptology – EUROCRYPT 2003* (Lecture Notes in Computer Science, vol. 2656), 2003, pp. 477–489.

[8] G. K. Verma, "Probable Security Proof of a Blind Signature Scheme over Braid Groups," *International Journal of Network Security*, vol. 12, no. 2, pp. 118–120, 2011.

[9] P. Hiranvanichakorn, "Provably Authenticated Group Key Agreement based on Braid Groups: The Dynamic Case," *International Journal of Network Security*, vol. 19, no. 4, pp. 517–527, 2017.

[10] A. Myasnikov, V. Shpilrain, and A. A Ushakov, "Practical Attack on a Braid Group Based Cryptographic Protocol," in *Advances in Cryptology ? CRYPTO'05* (Lecture Notes in Computer Science, vol. 3621), 2005, pp. 86–96.

[11] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, "Average-case complexity for the word and membership problems in group theory," *Advances in Mathematics*, vol. 190, pp. 343–359, 2005.

[12] D. N. Moldovyan, "Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes," *Quasigroups and Related Systems*, vol. 18, no. 2, pp. 165–176, 2010.

[13] D. N. Moldovyan and N. A. Moldovyan, "Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms," *Quasigroups Related Systems*, vol. 18, no. 2, pp. 177–186, 2010.

[14] A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, and A. A. Nechaev, "Cryptographic Algorithms on Groups and Algebras," *Journal of Mathematical Sciences*, vol. 223, no. 5, pp. 629–641, 2017.

[15] N. A. Moldovyan, "Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions," *Quasigroups Related Systems*, vol. 26, no. 2, pp. 263–270, 2018.

[16] A. A. Moldovyan and N. A. Moldovyan, "Post-quantum signature algorithms based on the hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 26, no. 3(78), pp. 301–313, 2018.

[17] A. A. Moldovyan, "General Method for Defining Finite Noncommutative Associative Algebras of Dimension $m > 1$," *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, no. 2(87), pp. 95–100, 2018.

[18] N. A. Moldovyan, A. A. Moldovyan, and A. N. Berezin, "On Using Mersenne Primes in Designing Cryptoschemes," *International Journal of Network Security*, vol. 18, no. 2, pp. 369–373, 2016.

Received September 29, 2018

D.N. Moldovyan,

St. Petersburg Institute for Informatics and Automation
of Russian Academy of Sciences,
14 Liniya, 39, St. Petersburg 199178, Russia
E–mail: mdn.spectr@mail.ru; http://www.spiiras.nw.ru