Quasigroups and Related Systems **27** (2017), 293 – 308

A unified method for setting finite non-commutative associative algebras and their properties

Dmitriy Moldovyan

Abstract. A unified method for defining a class of the finite non-commutative associative algebras of different even dimensions $m \geqslant 6$ is proposed to extend the set of potential algebraic supports of the public-key cryptographic algorithms and protocols based on the hidden discrete logarithm problem. The introduced method sets the algebras containing a large set of the global left-sided units. A particular version of the method defines the algebras with parametrizable multiplication operation all modification of which are mutually associative. The cases $m = 6$ and $m = 10$ are detaily considered.

1. Introduction

One of the current challenges in the area of theoretic and applied cryptography represents developing the public-key cryptographic algorithms and protocols that run efficiently on classical computers but will resist quantum attacks [1, 2], i. e., attacks performed with using hypothetical quantum computers that can be used to solve the factorization problem (FP) and the discrete logarithm problem (DLP) in polynomial time [15]. Development of the post-quantum public-key cryptoschemes is connected with looking for difficult computational problems that are different from the FP and DLP and can be used as primitives of the public-key cryptoschemes.

Much attention of the researchers has gained the conjugacy search problem (CSP) in braid groups representing a particular type of non-commutative groups [3, 6]. On the base of the computational difficulty of that problem a number of the public-key cryptoschemes have been designed [4, 16]. Another promising approach to the development of the post-quantum digital signature schemes [8, 9] and public key-agreement protocols is connected with exploiting so called hidden DLP (HDLP). For the first time the HDLP was proposed in the form of combining the DLP with the CSP as follows [11, 12]:

$$Y = G^w \circ Q^x \circ G^{-w}, \tag{1}$$

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, single-sided units, parametrizable multiplication, post-quantum cryptography, public-key cryptoscheme, hidden logarithm problem, discrete logarithm problem

where the known values Y (the public key), G, and Q are elements of some finite non-commutative group Γ; the unknown natural numbers w and x represent the private key. The public key-agreement scheme, the public encryption and commutative encryption algorithms have been introduced in [11, 12] using the multiplicative group of the finite algebra of quaternions, defined over the ground field $CF(p)$, as the group Γ. Detailed investigation [5] of the security of that cryptoschemes have revealed possibility of the polynomial reduction of the HDLP to the LP in the field $CF(p^2)$. That result had shown fundamental difficulties for development of the post-quantum public-key cryptoschemes on the base of the HDLP defined in the form (1) when using the finite algebra of quaternions as the algebraic support of the HDLP. Therefore, the further research of the HDLP as potential post-quantum cryptographic primitive is connected with looking for new forms of the HDLP and/or new finite non-commutative associative algebras (FNAAs) as algebraic supports of the HDLP.

In present paper a unified method for setting a class of the FNAAs of different even dimensions $m \geqslant 6$ is proposed. The introduced FNAAs possess two features that are interesting for cryptographic applications: i) the algebras contain a large set of the global left-sided units and ii) the algebras can be set so that that the multiplication operation is parametrizable and arbitrary two modifications of the multiplication operation are mutually associative. The last property is very attractive for potential application in the public-key cryptoschemes in which the modifications of the multiplication operation are used as a part of the private key. The properties of the 6-dimensional and 10-dimensional FNAAs are investigated in detail.

2. A method for setting a class of the FNAAs

2.1. Preliminaries

The FNAAs of small dimension m, which contain a large set of the global single-sided units, are described in [10] ($m = 2$) and [13] ($m = 3$). However for developing public-key cryptosystems based on the HDLP it is preferably to apply the FNAAs of the dimensions $m \geq 4$, which are defined over the field $GF(p)$ with sufficiently large characteristic p (for example, having the size equal to 256 to 512 bits).

The m-dimensional finite algebra represents the m-dimensional vector space over the field $GF(p)$, in which the multiplication operation (that is distributive relatively the addition operation) is additionally defined. The multiplication operation (denoted as $\circ$) can be defined with using the representation of arbitrary vector $A = (a_0, a_1, \ldots a_{m-1})$ as the following sum of the single-component vectors $a_i\mathbf{e}_i$:

$$A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i,$$

where $\mathbf{e}_0 = (1, 0, 0 \ldots, 0)$, $\mathbf{e}_1 = (0, 1, 0 \ldots, 0)$, ... $\mathbf{e}_{m-1} = (0, 0 \ldots, 0, 1)$ are the basis vectors; $a_0, a_1, \ldots a_{m-1}$ are coordinates of the vector A.

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

$$A \circ B = \left(\sum_{i=0}^{m-1} a_i \mathbf{e}_i \right) \circ \left(\sum_{j=0}^{m-1} b_j \mathbf{e}_j \right) = \sum_{j=0}^{m-1} \sum_{i=0}^{m-1} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j \right), \tag{2}$$

where the product of every pair of the basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by some single-component vector $\mu \mathbf{e}_k$ that is taken from the so called basis vector multiplication table (BVMT), like Tables 2, 3 (see Section 3), and 4 (Section4). When performing such replacement, one assumes that the intersection of the ith row and the jth column defines the value $\mu \mathbf{e}_k = \mathbf{e}_i \circ \mathbf{e}_j$. The value $\mu \neq 1$ is called structural coefficient. If the BVMT defines the multiplication operation that is associative and non-commutative, then the algebra is called FNAA. The element L (the element R) satisfying the vector equation $L \circ A = A$ ($A = A \circ R$) for every element A of the algebra is called the global left-sided (right-sided) unit.

2.2. Proposed unified method for defining FNAAs of different even dimensions

The paper [7] describes a general method for defining a class of the FNAAs over the field $GF(p)$, which contain a large class of the single-sided units, for arbitrary dimensions $m > 1$. However, using the general properties of such algebras, which are described in [7], one can show that for arbitrary value of the dimension the HDLP can be easily reduced to the DLP in the field $GF(p)$. Therefore, in order to extend the class of potential algebraic supports of the HDLP-based cryptoschemes one can propose the following unified method for defining the FNAAs over the ground field $GF(p)$.

The proposed method consists in using the BVMT described by the following formula for multiplying the basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$ in the m-dimensional vector space:

$$\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_{j-di}, \tag{3}$$

where the value $j - di$ is computed modulo m. For arbitrary even value m one can fined the values d such that the BVMT described by the formula (3) will define non-commutative associative multiplication operation.

Let us consider three m-dimensional vectors A, B, and $C = \sum_{k=1}^{m} c_k \mathbf{e}_k$. Taking into account the formula (2), for product of the vectors A, B, and $C = \sum_{k=0}^{m} c_k \mathbf{e}_k$ one can get the following

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

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

The last formula shows the multiplication operation is associative, if the BVMT defines associative multiplication of the basis vectors.

For multiplication of three basis vectors $\mathbf{e}_i, \mathbf{e}_j$, and $\mathbf{e}_k$, which is performed in accordance with the formula (3), one can write

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{j-di} \circ \mathbf{e}_k = \mathbf{e}_{k-dj+d^2 i};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{k-dj} = \mathbf{e}_{k-dj-di}.$$

Thus, the formula (3) defines associative multiplication of the basis vectors, if the condition

$$d^2 \equiv -d \mod m. \tag{4}$$

holds true.

For all values $m \geqslant 2$ the value $d \equiv -1 \mod m$ satisfies the condition (4) and defines associative multiplication, however in this case we have commutative multiplication. Non-commutative associative multiplication operation can be obtained for even values of the dimension $m \geqslant 6$, for example, when $m = 6, 10, 12, 14$. Table 1 shows the values of the parameter d at which we have the m-dimensional FNAAs.

Table 1

Suitable values d for different dimensions m

m	6	10	12	14	18	20	30	40	62
d	2; 3	4; 5	3; 8	6; 7	8; 9	4; 15	5; 24	6; 35	30; 31

It is easy to show that for the values $m = 2q$, where q is a prime, we have the following two values of the parameter d: $d_1 = q$ and $d_2 = q - 1$ (note that in this case we have $q^2 \equiv q \equiv -q \mod m$ and $(q-1)^2 \equiv 1 - q \mod m$).

The formula (3) generates the BVMTs that are free from structural coefficients, but one can experimentally find different distributions of the inserted structural coefficients, which retain the property of the associativity of the multiplication operation. After such modification of the source BVMT constructed for the case $m = 6$ and $d = 2$ one obtains the BVMT defining the 6-dimensional FNAA (that contains p^3 global left-sided units) used as algebraic support of the post-quantum signature scheme in [14].

For the case of even values of the parameter d one can propose the following version of the proposed unified method, which is described by the following formula for defining the BVMTs containing the structural coefficients λ and ϵ :

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \lambda \mathbf{e}_{j-di}, \text{ if } i \equiv 0 \bmod 2 \\ \epsilon \mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2, \end{cases} \tag{5}$$

Proposition 2.1. *The formula* (5) *defines the m-dimensional FNAAs, if m and d are even natural numbers and the condition* (4) *holds true.*

Thus, the version of the considered unified method described with the formula (5) introduces a set of the FNAAs corresponding to the same distribution of the basis vectors in the BVMT and different pairs of the values of structural coefficients λ and ϵ. One can call such set of FNAAs the algebra with parametrizable multiplication operation. Concrete version of the multiplication operation is set by selecting two fixed values the structural coefficients λ and ϵ. In the considered case of the FNAA with parametrizable multiplication operation we have the following interesting property that can be called mutual associativity of arbitrary two modifications of the multiplication operation (earlier the mutual associativity of different modifications of the multiplication operation in FNAAs was considered in [7]).

Proposition 2.2. *Suppose m and d are even natural numbers and the condition* (4) *holds true. Then the formula* (5) *defines the m-dimensional FNAA with parametrizable multiplication operation and with mutual associativity of all possible pairs of the modifications $\circ$ and $\star$ of the multiplication operation.*

Proof. Suppose the structural coefficients λ and ϵ define the $\circ$-version of the multiplication operation and the structural coefficients λ' and ϵ' define the $\star$-version of the multiplication operation. One should consider the influence of the pairs of structural coefficients (λ, ϵ) and (λ', ϵ') in the following two products: i) $(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k$ and ii) $\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k)$. In each of these two cases the oddness of the value k does not influences the result in the indicated two cases. Therefore, one should consider the following four cases.

1. The values i and j are even:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \lambda \mathbf{e}_{j-di} \star \mathbf{e}_k = \lambda\lambda' \mathbf{e}_{k-d(j-di)} = \lambda\lambda' \mathbf{e}_{k-dj+d^2 i} = \lambda\lambda' \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \lambda' \mathbf{e}_{k-dj} = \lambda'\lambda \mathbf{e}_{k-dj-di}.$$

2. The value i is even and the value j is odd:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \lambda \mathbf{e}_{j-di} \star \mathbf{e}_k = \epsilon' \lambda \mathbf{e}_{k-dj+d^2 i} = \epsilon' \lambda \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \epsilon' \mathbf{e}_{k-dj} = \lambda \epsilon' \mathbf{e}_{k-dj-di}.$$

3. The value i is odd and the value j is even:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \epsilon \mathbf{e}_{j-di} \star \mathbf{e}_k = \lambda' \epsilon \mathbf{e}_{k-dj+d^2 i} = \lambda' \epsilon \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \lambda' \mathbf{e}_{k-dj} = \epsilon\lambda' \mathbf{e}_{k-dj-di}.$$

4. The values i and j are odd:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \epsilon\mathbf{e}_{j-di} \star \mathbf{e}_k = \epsilon\epsilon'\mathbf{e}_{k-dj+d^2i)} = \epsilon\epsilon'\mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \epsilon'\mathbf{e}_{k-dj} = \epsilon'\epsilon\mathbf{e}_{k-dj-di}.$$

Thus, in all cases we have $(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k)$. The Proposition 2.2 is proved. □

Note that the Proposition 2.1 is direct corollary from the Proposition 2.2. Using the formula (5) one can define FNAAs with parametrizable multiplication operation, which have different dimensions. Table 1 provides the following examples: i) $m = 6$, $d = 2$; ii) $m = 10$, $d = 4$; iii) $m = 12$, $d = 8$; ... iv) $m = 62$, $d = 30$.

For the case of odd values of the parameter d in the formula (3) one can propose the following version of the considered uniform method which is described by the following formula:

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \mathbf{e}_{j-di}, \text{ if } i \equiv 0 \bmod 2 \\ \mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2 \text{ and } j \equiv 0 \bmod 2 \\ \lambda\mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2 \text{ and } j \equiv 1 \bmod 2, \end{cases} \tag{6}$$

The reader can easily prove the following proposition.

Proposition 2.3. *Suppose m is an even integer, d is an odd integer, and the condition* (4) *holds true. Then the formula* (6) *defines the m-dimensional FNAAs.*

Considering the fixed even value m and fixed odd value d we have many FNAAs relating to different values of the structural coefficient λ, which can be united by the notion of FNAA with the parametrizable multiplication operation. However, in such algebras different modifications of the multiplication operation are not mutually associative in general case.

3. The case of 6-dimensional FNAAs

3.1. The algebra with mutually associative modifications of the multiplication operation

In the case $m = 6$, $d = 2$, and $\lambda = 1$ we have the BVMT shown as Table 2. Due to the Proposition 2.2 this FNAA is an algebra is with parametrizable multiplication operation all modifications of which are mutually associative. The 6-dimensional FNAA defined with this table contains the set of p^3 global left-sided units $L = (l_0, l_1, l_2, l_3, l_4, l_5)$ described with the following formula [14]:

$$L = \left(h, k, t, (1-h)\epsilon^{-1}, -\epsilon k, -t\epsilon^{-1}\right),$$

where $h, k, t = 0, 1, \ldots p-1$. Evidently, the considered 6-dimensional FNAA contains no global right-sided unit. To find the formula describing local right-sided

units one should consider solution of the vector equation $A \circ X = A$, where $A = (a_0, a_1, a_2, a_3, a_4, a_5)$ is a fixed vector. The last equation can be reduced to the following two independent systems each of which contains three unknowns:

$$\begin{cases} (a_0 + \epsilon a_3)\, x_0 + (\epsilon a_1 + a_4)\, x_2 + (a_2 + \epsilon a_5)\, x_4 = a_0; \\ (a_2 + \epsilon a_5)\, x_0 + (a_0 + \epsilon a_3)\, x_2 + (\epsilon a_1 + a_4)\, x_4 = a_2; \\ (\epsilon a_1 + a_4)\, x_0 + (a_2 + \epsilon a_5)\, x_2 + (a_0 + \epsilon a_3)\, x_4 = a_4; \end{cases}$$

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

Table 2

The BVMT defining the FNAA containing p^3 global left-sided units [14]

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

The main determinant of each of the last two systems is equal to Δ_A:

$$\Delta_A = (a_0 + \epsilon a_3)^3 + (\epsilon a_1 + a_4)^3 + (a_2 + \epsilon a_5)^3 - 3\,(a_0 + \epsilon a_3)\,(a_2 + \epsilon a_5)\,(\epsilon a_1 + a_4)$$

If $\Delta_A \neq 0$, then there exists unique local right-sided unit corresponding to the vector A.

3.2. The algebra with p^4 global left-sided units

In the case $m = 6$ and $d = 3$ the formula (6) defines the BVMT in the form of Table 3. The left-sided units can be found from the vector equation $X \circ A = A$ that reduces to the following system with six unknowns x_0, x_1, x_2, x_3, x_4, and x_5:

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

Performing the variable substitution $u_1 = x_0 + x_2 + x_4$ and $u_2 = x_1 + x_3 + x_5$ one can easily find the following solution that is independent of the value A: $(u_1, u_2) = (1, 0)$. The solution in terms of the variables u_1 and u_2 defines p^4 solutions in terms of the variables x_0, x_1, x_2, x_3, x_4, and x_5. Every of the last solutions define a unique global left-sided unit. The set of all global left-sided units is described as follows (where $h, k, t, z = 0, 1, \ldots p-1$):

$$L = (l_0, l_1, l_2, l_3, l_4, l_5) = (h, k, t, z, 1-h-t, -k-z)\,.$$

The formula describing local right-sided units can be derived from the vector equation $A \circ X = A$ that can be reduced to the following three independent systems of two linear equations every one of which contains two unknowns:

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

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

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

Table 3

The BVMT of the 6-dimensional FNAA containing p^4 global left-sided units

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

The main determinant of each of the last three systems is equal to Δ_A:

$$\Delta_A = (a_0 + a_2 + a_4)^2 - \lambda\,(a_1 + a_3 + a_5)^2\,.$$

If $\Delta_A \neq 0$, then there exists unique local right-sided unit corresponding to the vector A.

4. The 10-dimensional FNAA

In the case $m = 10$, $d = 4$, $\lambda \neq 1$, and $\epsilon = 1$ the formula (5) defines the BVMT in the form of Table 4. The left-sided units can be found from the vector equation $X \circ A = A$ that reduces to the following system with ten unknowns $x_0, x_1, \ldots x_9$:

$$X \circ A = A. \tag{7}$$

Using Table 3 one can represent (7) in the form of the following system of 10 linear equations with coordinates of the left operand $x_0, x_1, \ldots, x_9$ as the unknown values:

$$\begin{cases} \lambda x_0a_0 + x_1a_4 + \lambda x_2a_8 + x_3a_2 + \lambda x_4a_6 + x_5a_0 + \lambda x_6a_4 + x_7a_8 + \lambda x_8a_2 + x_9a_6 = a_0; \\ \lambda x_0a_1 + x_1a_5 + \lambda x_2a_9 + x_3a_3 + \lambda x_4a_7 + x_5a_1 + \lambda x_6a_5 + x_7a_9 + \lambda x_8a_3 + x_9a_7 = a_1; \\ \lambda x_0a_2 + x_1a_6 + \lambda x_2a_0 + x_3a_4 + \lambda x_4a_8 + x_5a_0 + \lambda x_6a_6 + x_7a_0 + \lambda x_8a_4 + x_9a_8 = a_2; \\ \lambda x_0a_3 + x_1a_7 + \lambda x_2a_1 + x_3a_5 + \lambda x_4a_9 + x_5a_0 + \lambda x_6a_7 + x_7a_1 + \lambda x_8a_5 + x_9a_9 = a_3; \\ \lambda x_0a_4 + x_1a_8 + \lambda x_2a_2 + x_3a_6 + \lambda x_4a_0 + x_5a_0 + \lambda x_6a_8 + x_7a_2 + \lambda x_8a_6 + x_9a_0 = a_4; \\ \lambda x_0a_5 + x_1a_9 + \lambda x_2a_3 + x_3a_7 + \lambda x_4a_1 + x_5a_0 + \lambda x_6a_9 + x_7a_3 + \lambda x_8a_7 + x_9a_1 = a_5; \\ \lambda x_0a_6 + x_1a_0 + \lambda x_2a_4 + x_3a_8 + \lambda x_4a_2 + x_5a_0 + \lambda x_6a_0 + x_7a_4 + \lambda x_8a_8 + x_9a_2 = a_6; \\ \lambda x_0a_7 + x_1a_1 + \lambda x_2a_5 + x_3a_9 + \lambda x_4a_3 + x_5a_0 + \lambda x_6a_1 + x_7a_5 + \lambda x_8a_9 + x_9a_3 = a_7; \\ \lambda x_0a_8 + x_1a_2 + \lambda x_2a_6 + x_3a_0 + \lambda x_4a_4 + x_5a_0 + \lambda x_6a_2 + x_7a_6 + \lambda x_8a_0 + x_9a_4 = a_8; \\ \lambda x_0a_9 + x_1a_3 + \lambda x_2a_7 + x_3a_1 + \lambda x_4a_5 + x_5a_0 + \lambda x_6a_3 + x_7a_7 + \lambda x_8a_1 + x_9a_5 = a_9. \end{cases} \tag{8}$$

The system (8) can be rewritten in the form of two systems each of which contains five linear equations with 10 unknowns:

$$\begin{cases} (\lambda x_0 + x_5)\, a_0 + (x_3 + \lambda x_8)\, a_2 + (x_1 + \lambda x_6)\, a_4 + (\lambda x_4 + x_9)\, a_6 + (\lambda x_2 + x_7)\, a_8 = a_0; \\ (\lambda x_0 + x_5)\, a_2 + (x_3 + \lambda x_8)\, a_4 + (x_1 + \lambda x_6)\, a_6 + (\lambda x_4 + x_9)\, a_8 + (\lambda x_2 + x_7)\, a_0 = a_2; \\ (\lambda x_0 + x_5)\, a_4 + (x_3 + \lambda x_8)\, a_6 + (x_1 + \lambda x_6)\, a_8 + (\lambda x_4 + x_9)\, a_0 + (\lambda x_2 + x_7)\, a_2 = a_4; \\ (\lambda x_0 + x_5)\, a_6 + (x_3 + \lambda x_8)\, a_8 + (x_1 + \lambda x_6)\, a_0 + (\lambda x_4 + x_9)\, a_2 + (\lambda x_2 + x_7)\, a_4 = a_6; \\ (\lambda x_0 + x_5)\, a_8 + (x_3 + \lambda x_8)\, a_0 + (x_1 + \lambda x_6)\, a_2 + (\lambda x_4 + x_9)\, a_4 + (\lambda x_2 + x_7)\, a_6 = a_8; \end{cases} \tag{9}$$

$$\begin{cases} (\lambda x_0 + x_5)\, a_1 + (x_3 + \lambda x_8)\, a_3 + (x_1 + \lambda x_6)\, a_5 + (\lambda x_4 + x_9)\, a_7 + (\lambda x_2 + x_7)\, a_9 = a_1; \\ (\lambda x_0 + x_5)\, a_3 + (x_3 + \lambda x_8)\, a_5 + (x_1 + \lambda x_6)\, a_7 + (\lambda x_4 + x_9)\, a_9 + (\lambda x_2 + x_7)\, a_1 = a_3; \\ (\lambda x_0 + x_5)\, a_5 + (x_3 + \lambda x_8)\, a_7 + (x_1 + \lambda x_6)\, a_9 + (\lambda x_4 + x_9)\, a_1 + (\lambda x_2 + x_7)\, a_3 = a_5; \\ (\lambda x_0 + x_5)\, a_7 + (x_3 + \lambda x_8)\, a_9 + (x_1 + \lambda x_6)\, a_1 + (\lambda x_4 + x_9)\, a_3 + (\lambda x_2 + x_7)\, a_5 = a_7; \\ (\lambda x_0 + x_5)\, a_9 + (x_3 + \lambda x_8)\, a_1 + (x_1 + \lambda x_6)\, a_3 + (\lambda x_4 + x_9)\, a_5 + (\lambda x_2 + x_7)\, a_7 = a_9. \end{cases} \tag{10}$$

Performing the variable substitution

$$u_0 = \lambda x_0 + x_5;\ \ u_1 = x_3 + \lambda x_8;\ \ u_2 = x_1 + \lambda x_6;\ \ u_3 = \lambda x_4 + x_9;\ \ u_4 = \lambda x_2 + x_7 \tag{11}$$

in the systems (9) and (10) one can easily see that the solution

$$u_0 = 1;\ \ u_1 = 0;\ \ u_2 = 0;\ \ u_3 = 0;\ \ u_4 = 0 \tag{12}$$

satisfies simultaneously the systems (9) and (10) for all elements A of the considered FNAA. Besides, if the vector A is such that the main determinant of the system (9) Δ'_A satisfies condition $\Delta'_A \neq 0$ or the main determinant of the system (10) Δ''_A satisfies condition $\Delta''_A \neq 0$, then the indicated solution is unique relatively the unknowns u_0, u_1, u_2, u_3, and u_0.

For very small portion of the vectors A, coordinates of which satisfy the both conditions $\Delta'_A = 0$ and $\Delta''_A = 0$, many other solutions exists. However, such "marginal" vectors are to be not involved in the computations in frame of the potential public-key cryptoschemes based on the considered FNAA. The additional solutions define the local left-sided units acting only in frame of the subset of the "marginal" vectors. One can easily derive the formula describing the local left-sided units, but we will describe only the set of global left-sided units (that act as the left-sided units on every 10-dimensional vector).

Taking into account the formulas (11) and the solutions (12) one can get the formula describing all p^5 global left-sided units $L = (l_0, l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8, l_9)$:

$$L = (x_0, -\lambda x_6, x_2, -\lambda x_8, x_4, 1 - \lambda x_0, x_6, -\lambda x_2, x_8, -\lambda x_4), \tag{13}$$

where $x_0, x_2, x_4, x_6, x_8 = 0, 1, \ldots, p-1$.

Table 4

Defining the 10-dimensional FNAA containing p^5 global left-sided units

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$
$\mathbf{e}_0$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$
$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_2$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_4$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$
$\mathbf{e}_6$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$
$\mathbf{e}_7$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_8$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$
$\mathbf{e}_9$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Consideration of the right-sided units is connected with solving the vector equation

$$A \circ X = A. \tag{14}$$

Using Table 3 one can represent (14) in the form of the following system of 10 linear equations with coordinates of the right operand $x_0, x_1, \ldots, x_9$ as the unknown

values:

$$\begin{cases} \lambda a_0x_0 + a_1x_4 + \lambda a_2x_8 + a_3x_2 + \lambda a_4x_6 + a_5x_0 + \lambda a_6x_4 + a_7x_8 + \lambda a_8x_2 + a_9x_6 = a_0; \\ \lambda a_0x_1 + a_1x_5 + \lambda a_2x_9 + a_3x_3 + \lambda a_4x_7 + a_5x_1 + \lambda a_6x_5 + a_7x_9 + \lambda a_8x_3 + a_9x_7 = a_1; \\ \lambda a_0x_2 + a_1x_7 + \lambda a_2x_0 + a_3x_4 + \lambda a_4x_8 + a_5x_2 + \lambda a_6x_6 + a_7x_0 + \lambda a_8x_4 + a_9x_8 = a_2; \\ \lambda a_0x_3 + a_1x_8 + \lambda a_2x_1 + a_3x_5 + \lambda a_4x_9 + a_5x_3 + \lambda a_6x_7 + a_7x_1 + \lambda a_8x_5 + a_9x_9 = a_3; \\ \lambda a_0x_4 + a_1x_9 + \lambda a_2x_2 + a_3x_6 + \lambda a_4x_0 + a_5x_4 + \lambda a_6x_8 + a_7x_2 + \lambda a_8x_6 + a_9x_0 = a_4; \\ \lambda a_0x_5 + a_1x_0 + \lambda a_2x_3 + a_3x_7 + \lambda a_4x_1 + a_5x_5 + \lambda a_6x_9 + a_7x_3 + \lambda a_8x_7 + a_9x_1 = a_5; \\ \lambda a_0x_6 + a_1x_1 + \lambda a_2x_4 + a_3x_8 + \lambda a_4x_2 + a_5x_6 + \lambda a_6x_0 + a_7x_4 + \lambda a_8x_8 + a_9x_2 = a_6; \\ \lambda a_0x_7 + a_1x_2 + \lambda a_2x_5 + a_3x_9 + \lambda a_4x_3 + a_5x_7 + \lambda a_6x_1 + a_7x_5 + \lambda a_8x_9 + a_9x_3 = a_7; \\ \lambda a_0x_8 + a_1x_3 + \lambda a_2x_6 + a_3x_0 + \lambda a_4x_4 + a_5x_8 + \lambda a_6x_2 + a_7x_6 + \lambda a_8x_0 + a_9x_4 = a_8; \\ \lambda a_0x_9 + a_1x_4 + \lambda a_2x_7 + a_3x_1 + \lambda a_4x_5 + a_5x_9 + \lambda a_6x_3 + a_7x_7 + \lambda a_8x_1 + a_9x_5 = a_9. \end{cases} \tag{15}$$

If the main determinant of the system (15) $\Delta_A \neq 0$, then there exists unique solution $X = R_A$ which depends on the vector A, i. e., R_A is the local right-sided unit element.

5. Common properties of the 6-dimensional and 10-dimensional FNAAs

Sections 3 and 4 describe the 6-dimensional and 10-dimensional FNAAs defined applying the proposed unified method for setting FNAAs. It is shown that the considered algebras contain a large set of global left-sided units. One can expect that for all even values of the dimension $m \geqslant 6$ the proposed method will define the FNAAs, containing a large set of the global left-sided units. In this section we present some common properties of the described 6-dimensional and 10-dimensional FNAAs. One can suppose that the introduced propositions are valid for other values of the dimension of the FNAAs defined using the both versions (see the Propositions 2.1 and 2.2) of the proposed unified method.

Proposition 5.1. *If the vector A satisfies condition $\Delta_A \neq 0$, then $A \circ L_i \neq A \circ L_j$, for arbitrary two global left-sided units L_i and $L_j \neq L_i$.*

Proof. Suppose $A \circ L_i = A \circ L_j$. Then $A \circ (L_i - L_j) = O$. Since $\Delta_A \neq 0$, the equation $A \circ X = O$ has unique solution $X = O$. Therefore, we have $L_i - L_j = O \Rightarrow L_i = L_j$. The obtained contradiction proves the Proposition 5.1. □

Proposition 5.2. *If the vector equation $X \circ A = B$ has solution $X = S$, then different values $X_i = S \circ L_i$, where L_i takes on all values from the set of global left-sided units, also are solutions of the given equation.*

Proof. $(S \circ L_i) \circ A = S \circ (L_i \circ A) = S \circ A = B$. The Proposition 5.2 is proved. □

Proposition 5.3. *If $A \circ B = L$, where L is a global left-sided unit, then the equality $A^i \circ B^i = L$ holds true for arbitrary natural value i.*

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 5.3 is proved. □

Proposition 5.4. *If $A \circ B = L$, where L is a global left-sided unit, 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 algebra, represents a homomorphism.*

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

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

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

The Proposition 5.4 is proved. □

Proposition 5.5. *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 5.4 we have $\psi(X^i) = (\psi(X))^i$, i. e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The Proposition 5.5 is proved. □

Multiplication of the elements of the considered FNAA by any fixed global left-sided unit L at right represents a homomorphism map that is mutually commutative with the exponentiation operation. This fact is due to the following two propositions.

Proposition 5.6. *Suppose the vector L is an arbitrary global left-sided unit and the vector X takes on all values in the considered FNAA. Then the map defined by the formula $\varphi(X) = X \circ L$ is a homomorphism.*

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

$$\varphi(X_1 \circ X_2) = (X_1 \circ X_2) \circ L = (X_1 \circ L) \circ (X_2 \circ L) = \varphi(X_1) \circ \varphi(X_2);$$

$$\varphi(X_1 + X_2) = (X_1 + X_2) \circ L = X_1 \circ L + X_2 \circ L = \varphi(X_1) + \varphi(X_2).$$

The Proposition 5.6 is proved. □

Proposition 5.7. *The homomorphism-map operation $\varphi(X) = X \circ L$, where L is a global left sided unit, and the exponentiation operation X^i are mutually commutative, i. e., the equality $X^i \circ L = (X \circ L)^i$ holds true.*

Proof. Due to Proposition 5.6 we have $\varphi(X^i) = (\varphi(X))^i$, i. e., $X^i \circ L = (X \circ L)^i$. The Proposition 5.7 is proved. □

Every global left sided unit L is connected with different homomorphism map operations of other type which can be described with the following formula:

$$\psi(X) = A^i \circ X \circ B^i,$$

where $i \geqslant 1$ is an arbitrary non-negative integer and the vectors A and B are such that $A \circ B = L$ holds true.

Each of the homomorphism map operations $\psi(X)$ and $\varphi(X)$ is mutually commutative with the exponentiation operation and represents interest for using it as masking operation at setting new types of the HDLP. The next propositions show that the local right-sided unit R_A related the the vector A such that $\Delta_A \neq 0$ (the main determinant of the system of linear equation written for computing the right-sided units) is contained in the set of the global left-sided units, i. e. the value R_A is simultaneously the local two-sided unit of the vector A. Therefore the vectors A for which we have $\Delta_A \neq 0$ are called locally invertible vectors.

Proposition 5.8. *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. Assumption that the sequence $A, A^2, \ldots, A^i, \ldots$ contains the zero vector $O = (0, 0, 0, 0, 0, 0)$ leads to a contradiction. Indeed, due to the condition $\Delta_A \neq 0$ we have $A \neq O$. If for some natural number $j > 1$ we have $A^j = O$, then for some positive integer $k \leq j$ the conditions $A^{k-1} \neq O$ and $A^k = O$ holds true. Therefore, $A \circ A^{k-1} = O$. Since $\Delta_A \neq 0$ and $X = O$ satisfies the equation $A \circ X = O$, the last equation has unique solution $X = O$, i. e., $A^{k-1} = O$. The obtained contradiction proves that the considered sequence does not include the zero vector O. Therefore, due to finiteness of the considered algebra the indicated sequence is periodic. Then for some minimum $t > 1$ we have

$$\left\{A = A^t = A^{t-1} \circ A = A \circ A^{t-1}\right\} \Rightarrow E_A = A^{t-1},$$

where E_A is the local two-sided unit connected with the vector A. Evidently, due to condition $\Delta_A \neq 0$ we have $A \circ E_A - A \circ R_A = A \circ (E_A - R_A) = O \;\Rightarrow\; E_A - R_A = O \;\Rightarrow\; E_A = R_A$. Therefore, for $\omega = t - 1$ we have $A^\omega = R_A$. □

Proposition 5.9. *Suppose the vector A is such that the conditions $\Delta_A \neq 0$, $\Delta'_A \neq 0$, and $\Delta''_A \neq 0$ holds true. Then the local right-sided unit R_A is contained in the set of the global left-sided units.*

Proof. Due to the Proposition 5.8 we have $R_A = E_A$ and $E_A \circ A = A$, i. e., R_A acts on the vector A as the left-sided unit, but all left sided units of the vector A are included in the set of global left-sided units. □

6. On potential cryptographic application of the introduced FNAAs

In the case of defining of the HDLP in the 6-dimensional FNAAs containing many different global left-sided units, which are described in Section 3, the formula (1) cannot be used because these algebras contains no globally invertible element. However by analogy with the formula (1) one can use the mutual commutativity of the homomorphism-map operations ψ and φ with the exponentiation operation (see the Propositions 5.5 and 5.7) as follows.

Suppose the vectors A and B are such that $\Delta_A \neq 0$ and $A \circ B = L_0$, where L_0 is a global left-sided unit. Then using some locally invertible vector N satisfying the conditions $\Delta_N \neq 0$ and $N \circ A \neq A \circ N$ one can define computation of the public key Y by the next formula:

$$Y = B^t \circ N^x \circ A^t = \left(B^t \circ N \circ A^t\right)^x, \tag{16}$$

where the vectors A, B, and N are the known parameters and the positive integers (t, x) are the unknown values generated at random and used as the private key.

The formula (16) defines a particular form of the HDLP which can be used in the public key-agreement scheme in frame of which the common secret shared by some two users is calculated as follows

$$Z = B^{t_1} \circ Y_2^{x_1} \circ A^{t_1} = B^{t_2} \circ Y_1^{x_2} \circ A^{t_2},$$

where the vectors Y_1 and Y_2 (the pairs (t_1, x_1) and (t_2, x_2)) are the public (private) keys of the first and the second users correspondingly. Thus, this public key-agreement scheme performs correctly, however estimating its security is currently an open problem that require individual study.

For the development of the post-quantum public key-agreement schemes one can propose another form of the HDLP in which the connection between the public and private keys is complicated by introducing the additional masking element of the private key, which represents the unit element L selected at random from the set of the global left-sided units. The element L is used in the formula for calculating the public key as the *rightmost* operand, therefore the value L significantly influences the value Y. The proposed form of the HDLP is described by the following formula for computing the public key:

$$Y = B^t \circ N^x \circ A^t \circ L = \left(B^t \circ N \circ A^t\right)^x \circ L,$$

where the integers t and x and the vector L represent three elements of the corresponding private key. One can easily show that the public keys represented in the last form also provide possibility of the public key-agreement. Investigation of the security of such modified public key-agreement scheme also is an open problem for independent study.

The idea of using the modifications of the multiplication operation as elements of the private key in the public-key cryptoschemes represents special interest. For example, such key operations can be used as additional masking operations for setting novel forms of the HDLP in the FNAAs with parametrizable multiplication operation with mutual associativity of all pairs of the modifications of the multiplication operation. In future research we will pay significant attention to the design of the public-key cryptoschemes in which the modifications of the multiplication operation are used as the elements of private key.

7. Conclusion

The proposed unified method for defining FNAAs provides possibility to set a class of algebras every one of which contains a large set global left sided units. The method is implemented in two versions that are described by formulas (5) and (6) relating to even and odd value of the parameter d correspondingly. In the case of even values d there are set FNAAs with parametrizable multiplication operation characterized in that all pairs of the modifications of the multiplication operation are mutually associative. This subclass of algebras is very attractive as algebraic support of the public-key cryptoschemes in which the modifications of the multiplication operation are used as elements of the private key. However, the design of the cryptoschemes of such type is a task of individual research.

In general case the FNAAs containing a large set of the global left-sided units can be applied as algebraic support of the HDLP-based public-key cryptoschemes and new forms of the HDLP characterized in using the homomorphism-map operations of the ψ-type and φ-type as masking operations. Estimation of the security of the cryptoschemes of the last type to quantum attacks represents an attractive task of independent work.

Acknowledgments. The author thanks anonymous Referee for valuable remarks.

References

[1] First NIST standardization conference - April 11–13, 2018. http://prometheuscrypt.gforge.inria.fr/2018-04- 18.pqc2018.html

[2] *Post-Quantum Cryptography*, Lecture Notes Computer Sci., **10786** (2018).

[3] **I. Anshel, M. Anshel, D. Goldfeld**, *An algebraic method for public key cryptography*, Math. Research Letters, **6** (1999), 287 – 291.

[4] **P. Hiranvanichakorn**, *Provably authenticated group key agreement based on braid groups: The dynamic case*, Intern. J. Network Security, **19** (2017), 517 – 527.

[5] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Cryptographic algorithms on groups and algebras*, J. Math. Sci., **223** (2017), 629 – 641.

[6] **E. Lee, J.H. Park**, *Cryptanalysis of the public key encryption based on braid groups*, Lecture Notes Computer Sci., **2656** (2003), 477 – 489.

[7] **A.A. Moldovyan**, *General method for defining finite non-commutative associative algebras of dimension m>1*, Bul. Acad. Sti. Republ. Moldova. Matematica, **2(87)** (2018), 95 – 100.

[8] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova, **26** (2018), 301 – 313.

[9] **A.A. Moldovyan, N.A. Moldovyan**, *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem*, Bull. South ural State Univ., ser. Math. Modelling, Programming ana Computer Software, **12** (2019), no. 1, 66 – 81.

[10] **A.A. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov**, *Non-commutative finite associative algebras of 2-dimension vectors*, Computer Sci. J. Moldova, **25** (2017), 344 – 356.

[11] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems, **18** (2010), 165 – 176.

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

[13] **D.N. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov**, *Non-commutative finite associative algebras of 3-dimensional vectors*, Quasigroups and Related Systems, **26** (2018), 109 – 120.

[14] **N.A. Moldovyan**, *Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base*, Bul. Acad. Sti. Republ. Moldova, Matematica, **1** (2019), 71 – 78.

[15] **P.W. Shor**, *Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing, **26** (1997), 1484 – 1509.

[16] **G.K. Verma**, *Probable security proof of a blind signature scheme over braid groups*, Intern. J. Network Security, **12** (2011), no. 2, 118 – 120.

Received January 2, 2019

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
E-mail: mdn.spectr@mail.ru