MSC 94A60, 16Z05, 14G50, 11T71, 16S50 DOI: 10.14529/mmp190106

FINITE NON-COMMUTATIVE ASSOCIATIVE ALGEBRAS AS CARRIERS OF HIDDEN DISCRETE LOGARITHM PROBLEM

N.A. Moldovyan[1]***, A.A. Moldovyan***[1]
[1] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, St. Petersburg, Russian Federation
E-mails: nmold@mail.ru, maa1305@yandex.ru

The article introduces new finite algebras attractive as carriers of the discrete logarithm problem in a hidden group. In particular new 4-dimensional and 6-dimensional finite non-commutative algebras with associative multiplication operation and their properties are described. It is also proposed a general method for defining finite non-commutative associative algebras of arbitrary even dimension $m \geq 2$. Some of the considered algebras contain a global unit, but the other ones include no global unit element. In the last case the elements of the algebra are invertible locally relatively local bi-side units that act in the frame of some subsets of elements of algebra. For algebras of the last type there have been derived formulas describing the sets of the (right-side, left-side, and bi-side) local units. Algebras containing a large set of the global single-side (left-side and right-side) units and no global bi-side unit are also introduced. Since the known form of defining the hidden discrete logarithm problem uses invertibility of the elements of algebra relatively global unit, there are introduced new forms of defining this computationally difficult problem. The results of the article can be applied for designing public-key cryptographic algorithms and protocols, including the post-quantum ones. For the first time it is proposed a digital signature scheme based on the hidden discrete logarithm problem.

Keywords: finite associative algebra; non-commutative algebra; global unit; left-side units; local unit; local invertibility; discrete logarithm problem; public-key cryptoscheme; digital signature; post-quantum cryptography.

Introduction

The public-key cryptographic algorithms and protocols are widely used for solving different security problems of information and telecommunication technologies [1, 2]. A large part of such cryptoschemes is based on the following two computationally difficult problems: factorization and finding discrete logarithm [3]. However each of these two problems can be solved on a quantum computer in polynomial time [5]. Since quantum computing develops towards efficient practical implementations [4], one of actual challenges in the area of cryptography is development of public-key cryptoschemes based on other computationally difficult problems solution of which will remain infeasible even while solving them on a quantum computer. The response to this challenge was the announcement (December 20, 2016) by the National Institute of Standards and Technology (NIST) of the competition of the post-quantum public-key cryptograms development and the appearance of regularly held thematic conferences [6, 7]. The current results of the NIST competition have shown the following:

– no difficult computational problem suitable as single primitive for desgning the post-quantum cryptoschemes of the main types (algorithms and protocols for public encryption, public key distribution, commutative encryption, and digital signature) had been proposed;

– the hidden discrete logarithm problem (HDLP) defined in the finite non-commutative associative algebras (FNAAs), which are promising as a universal primitive of the post-quantum cryptoschemes of different types, have remained outside the scope of attention of participants of the NIST competition.

The purpose of this article is to attract the attention of researchers and developers of cryptographic schemes to the HDLP as to a universal cryptographic primitive, providing the possibility of building the post-quantum cryptographic algorithms and protocols of various types, which are convenient for practical application.

To achieve this goal, the following scientific tasks are considered in the article:

– construction of new FNAAs as potential carriers of the HDLP;
– studying of the properties of the proposed algebras;
– setting new forms of the HDLP;
– designing the digital signature scheme based on the HDLP.

1. Non-Commutative Finite Groups and Associative Algebras for Post-Quantum Cryptography

In a number of articles the cojugacy-search problem defined over the braid groups was considered as the base of post-quantum cryptoschemes [8] and was used to design digital signature protocols [9]. Unfortunately it had been shown possibility to reduce the cojugacy-search problem to solving a system of linear equations [10]. Such reduction means existance of principal problems with providing high security of the cryptoschemes based on the mentioned computational problem.

Another proposal for post-quantum primitives is the discrete logarithm problem in a hidden group, which is defined over finite non-commutative associative algebras [11, 12] and can be called HDLP. The HDLP is described as follows.

Suppose a finite non-commutative group Γ contains element Q having large prime order q and we have a method for an easy selection of the elements from commutative subgroup $\Gamma' \subset \Gamma$. To construct a public key-agreement cryptoscheme in [12] it is proposed to select a private key composed of two parts, random invertible element $W \in \Gamma'$ satisfying condition $W \circ Q \neq Q \circ W$ and random number $x < q$. Then the public key Y can be computed as follows

$$Y = W \circ Q^x \circ W^{-1}. \tag{1}$$

Finding pair (W, x) (where $W \in \Gamma'$) from the last equation, while there are known values Q and Y, is a computationally difficult problem that can be called the HDLP. The HDLP represents interest as the base primitive for constructing the public-key post-quantum cryptoschemes. The HDLP suits also well for designing post-quantum commutative encryption algorithms.

Public key-agreement scheme [13] is decribed as follows. Suppose the elements $G \in \Gamma$ and $Q \in \Gamma$ having sufficiently large prime order are specified and two remote users have intensions to generate a shared secret key using a public channel. The first user selects his private key as pair of random numbers (w_1, x_1), computes his public key $Y_1 = G^{w_1} \circ Q^{x_1} \circ G^{-w_1}$ and sends Y_1 to the second user. The last selects his private key (w_2, x_2), computes his public key $Y_2 = G^{w_2} \circ Q^{x_2} \circ G^{-w_2}$ and sends Y_2 to the first user. Then the first user computes value

$$K_{12} = G^{w_1} \circ (Y_2)^{x_1} \circ G^{-w_1} = G^{w_1+w_2} \circ Q^{x_2 x_1} \circ G^{-w_1-w_2}.$$

The second user computes value

$$K_{21} = G^{w_2} \circ (Y_1)^{x_2} \circ G^{-w_2} = G^{w_2+w_1} \circ Q^{x_1 x_2} \circ G^{-w_2-w_1}.$$

Thus, $K_{21} = K_{12} = K$, i.e., the users have generated securely common secret key K interacting via a public channel.

Suppose a user has published his public-key $Y = G^w \circ Q^x \circ G^{-w}$, where pair (w, x) is his private key, and a symmetric encryption algorithm F_K with key K is specified. Using a public communication channel and public key Y any person can send securely confidential message M to the user as follows [13]:

1. Sender generates two random numbers r and u, then computes elements $R = G^r \circ Q^u \circ G^{-r}$ and $K = G^r \circ Y^u \circ G^{-r} = G^{r+w} \circ Q^{xu} \circ G^{-r-w}$.

2. Using element K as encryption key and encryption algorithm F_K the sender encrypts message M into cryptogram $C = F_K(M)$ and sends group elements C and R to the user.

3. Using value R the user computes key K as follows $K = G^w \circ R^x \circ G^{-w} = G^{r+w} Q^{ux} \circ G^{-r-w}$ and discloses source message M from ciphertext C : $M = F_K^{-1}(C)$, where F_K^{-1} is the decryption function corresponding to encryption function F_K. The commutative-encryption algorithm is described as follows [14].

1. Represent a message as element $M \in \Gamma$.

2. Encrypt M with first encryption key (w_1, e_1, d_1) (where integers e_1 and d_1 satisfy condition $e_1 d_1 = 1 \bmod \Omega$; Ω is the order of group Γ), as follows: $C_1 = G^{w_1} \circ M^{e_1} \circ G^{-w_1}$.

3. Encrypt ciphertext C_1 with second encryption key (w_2, e_2, d_2) (where integers e_2 and d_2 satisfy condition $e_2 d_2 = 1 \bmod \Omega$; Ω is the order of group Γ) as follows:

$$C_2 = G^{w_2} \circ C_1^{e_2} \circ G^{-w_2} = G^{w_2+w_1} \circ M^{e_1 e_2} \circ G^{-w_1-w_2}.$$

It is easy to show the encryption of message M with second key (w_2, e_2, d_2) and then with first key (w_1, e_1, d_1) outputs the same ciphertext $C_{21} = C_{12}$, i.e. the described encryption algorithm is commutative (note key elements d_1 and d_2 are required to perform the decryption procedure).

Currently in literature no digital signature scheme is proposed. In the next sections of the paper we introduce new forms of the defining the HDLP and one of the last is used to propose a post-quantum digital signature scheme.

Proposed in literature post-quantum cryptoschemes are based on the HDLP defined over finite quaternion algebra [11] multiplicative group of which is used as non-commutative group Γ. Detailed study of the HDLP in finite quaternion algebra defined over ground field $GF(p)$ [15] had shown that the HDLP can be reduced to the problem of finding discrete logarithm in finite field $GF(p^2)$. To design post-quantum cryptoschemes on the base of the HDLP, in paper [15] it had been proposed to look for other finite non-commutative associative algebras (FNAAs) as carriers of the HDLP. However currently in literature there are considered only very few other FNAAs. The HDLP in 2-dimensional and 3-dimensional FNAAs over $GF(p)$, which are considered in [16,17], can be reduced to discrete logarithm in $GF(p)$.

In the present article there are introduced new 6-dimensional FNAAs possessing various properties and a general method for constructing FNAAs of arbitrary fixed even dimension $m \geq 2$. Some of the introduced algebras contain only local unit elements therefore there are proposed new forms of defining the HDLP which are different from the form considered in $[13, 15-17]$. The paper also proposes a digital signature scheme based on a new form of the HDLP. The paper is organized as follows. Section 1 describes the

HDLP as cryptographic primitive and several cryptoschemes based on the HDLP. Section 2 consideres general construction of the FNAAs. Section 3 introduces new 6-dimensional FNAAs and considers some of their properties. In one of the introduced FNAAs there is a large set of the global left-sided units and no global right-sided unite contained. In Section 4 it is proposed a unified method for constructing the FNAAs for the case of arbitrary even dimension. In Section 5 there are proposed new forms of defining the HDLP, including the case of using the global left-sided unites, and a new post-quantum signature scheme.

2. Finite Non-Commutative Associative Algebras

Let us consider finite m-dimensional vector space elements of which are vectors $A = (a_0, a_1, \dots a_{m-1})$ defined over some finite field, for example, over ground field $GF(p)$, i.e. $a_0, a_1, \dots a_{m-1} \in GF(p)$, where p is a prime number having sufficiently large size (256 to 512 bits). Suppose "+" is the addition operation in the vector space and the sum of vectors A and $B = (b_0, b_1, \dots b_{m-1})$ is defined as follows:

$$A + B = (a_0 + b_0, a_1 + b_1, \dots a_{m-1} + b_{m-1}),$$

where sign "+" designates both the addition in vector space and the addition in field $GF(p)$. Multiplying vector A by some scalar $\mu \in GF(p)$ is defined as follows

$$\mu A = (\mu a_0, \mu a_1, \dots \mu a_{m-1}).$$

The finite m-dimensional vector space becomes the finite m-dimensional algebra with defining the second binary operation that is distributive relatively the addition operation and is called multiplication. For defining the multiplication operation it is reasonable to use the notion of formal basis vectors denoted as $\mathbf{e}_0 = (1, 0, 0 \dots, 0, 0)$, $\mathbf{e}_1 = (0, 1, 0 \dots, 0, 0)$, ... $\mathbf{e}_{m-1} = (0, 0, 0 \dots, 0, 1)$ and representation of vectors A and B as follows: $A = \sum\limits_{i=0}^{m-1} a_i \mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$, where terms $a_i \mathbf{e}_i$ and $b_j \mathbf{e}_j$ are called components of vectors A and B correspondingly.

The multiplication operation "$\circ$" of m-dimensional vectors A and B is defined by the following formula

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

where product $\mathbf{e}_i \circ \mathbf{e}_j$ for all possible pairs of values i and j is to be replaced by some one-component vector in accordance with some basis vector multiplication table (BVMT) in every cell of which it is contained some one-component vector. The coordinate of the last is called structural coefficien. On definition it is assumed the following (where $\lambda \in GF(p)$):

$$(\mu \mathbf{e}_i) \circ (\lambda \mathbf{e}_j) = \mu\lambda \left(\mathbf{e}_i \circ \mathbf{e}_j \right) = \mu\lambda \mathbf{e}_i \circ \mathbf{e}_j.$$

In (2) it is assumed that the intersection of ith row and jth column of the BVMT defines the cell in which it is given the value of product $\mathbf{e}_i \circ \mathbf{e}_j$.

If the used BVMT defines associative multiplication, then the algebra is called associative. If the multiplication operation is non-commutative (commutative), then the algebra is called non-commutative (commutative). In case $m|p-1$ the BVMT can be composed so that algebra represents itself finite field $GF(p^m)$ [18].

Suppose number ω is the minimum one from the set natural numbers γ that for some invertible vector A, contained in a FNAA with global bi-side unit E, it holds $A^\gamma = E$.

Then the value ω is called order of vector A. If vector B is contained in a subset of algebra elements, which contains local bi-side unit $E' \neq E$, and for some minimum integer ω' we have $B^{\omega'} = E'$, then value ω' is called local order of vector B and the last is called locally invertible.

In the next section there are introduced several 6-dimensional FNAAs containing no global bi-side unit:

i) algebras with large set of the global single-side units,

ii) algebra with compressing multiplication operation.

The proposed 6-dimensional FNAAs are attractive for application as carriers of the HDLP, however one should introduce new forms of the HDLP.

3. New Carriers of the Hidden Discrete Logarithm Problem

3.1. The 6-Dimension FNAA with Set of Global Right-Side Unites

For case $m = 6$ the associative multiplication operation can be defined with the BVMT presented as Table 1. The associativity of the multiplication can be easily proved using formula (2) and considering fulfillment of the following condition for arbitrary three vectors A, B, and $C = \sum_{k=0}^{m-1} c_k \mathbf{e}_k$: $(A \circ B) \circ C = A \circ (B \circ C)$.

Table 1

The BVMT defining the 6-dimensional FNAA with local invertibility of its elements

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

From vector equation $A \circ X = A$, where $X = \sum_{k=0}^{m-1} x_j \mathbf{e}_j$ is the unknown vector, with using Table 1 one can get the following system of six linear equations with unknown values $x_j \in GF(p),\ j = 0, 1, \ldots, m-1$:

$$\begin{cases} a_0x_0 + \tau\mu a_3x_1 + a_0x_2 + \mu a_3x_3 + \tau a_0x_4 + \mu a_3x_5 = a_0; \\ a_1x_0 + \tau a_4x_1 + a_1x_2 + a_4x_3 + \tau a_1x_4 + a_4x_5 = a_1; \\ a_2x_0 + \tau\mu a_5x_1 + a_2x_2 + \mu a_5x_3 + \tau a_2x_4 + \mu a_5x_5 = a_2; \\ a_3x_0 + \tau a_0x_1 + a_3x_2 + a_0x_3 + \tau a_3x_4 + a_0x_5 = a_3; \\ a_4x_0 + \tau\mu a_1x_1 + a_4x_2 + \mu a_1x_3 + \tau a_4x_4 + \mu a_1x_5 = a_4; \\ a_5x_0 + \tau a_2x_1 + a_5x_2 + a_2x_3 + \tau a_5x_4 + a_2x_5 = a_5. \end{cases} \quad (3)$$

The system of equations (3) can be represented in the following form:

$$\begin{cases} a_0\left(x_0 + x_2 + \tau x_4\right) + \mu a_3\left(\tau x_1 + x_3 + x_5\right) = a_0; \\ a_1\left(x_0 + x_2 + \tau x_4\right) + a_4\left(\tau x_1 + x_3 + x_5\right) = a_1; \\ a_2\left(x_0 + x_2 + \tau x_4\right) + \mu a_5\left(\tau x_1 + x_3 + x_5\right) = a_2; \\ a_3\left(x_0 + x_2 + \tau x_4\right) + a_0\left(\tau x_1 + x_3 + x_5\right) = a_3; \\ a_4\left(x_0 + x_2 + \tau x_4\right) + \mu a_1\left(\tau x_1 + x_3 + x_5\right) = a_4; \\ a_5\left(x_0 + x_2 + \tau x_4\right) + a_2\left(\tau x_1 + x_3 + x_5\right) = a_5. \end{cases} \quad (4)$$

It is easy to see the solutions of the last system satisfy the following two equations:

$$\begin{cases} x_0 + x_2 + \tau x_4 = 1; \\ \tau x_1 + x_3 + x_5 = 0. \end{cases} \tag{5}$$

From (5) one can write the following formula describing the set of local right-side units E_r relating to vector A:

$$E_r = \left(i,\ k,\ j,\ h, \frac{1-i-j}{\tau},\ -\tau k - h \right). \tag{6}$$

it is esy to see that each vector from set (6) is the global right-side unit, since it acts as the right unit on all elements of the considered FNAA.

To get the formula for the left-side units corresponding to vector A one should consider the following vector equation

$$X \circ A = A$$

that can be rewritten in the form of the following system of six linear equations with unknowns $x_0, x_1, x_2, x_3, x_4, x_5$:

$$\begin{cases} \Phi x_0 + \mu \Psi x_3 = a_0; \\ \Phi x_1 + \Psi x_4 = a_1; \\ \Phi x_2 + \mu \Psi x_5 = a_2; \\ \Psi x_0 + \Phi x_3 = a_3; \\ \mu \Psi x_1 + \Phi x_4 = a_4; \\ \Psi x_2 + \Phi x_5 = a_5, \end{cases} \tag{7}$$

where $\Phi = a_0 + a_2 + \tau a_4$ and $\Psi = \tau a_1 + a_3 + a_5$.

There exists the single solution of system (7) that defines the following formula for the left-side local unit corresponding to vector A:

$$E_l = \left(\frac{\Phi a_0 - \mu \Psi a_3}{\Phi^2 - \mu \Psi^2}, \frac{\Phi a_1 - \Psi a_4}{\Phi^2 - \mu \Psi^2}, \frac{\Phi a_2 - \mu \Psi a_5}{\Phi^2 - \mu \Psi^2}, \frac{\Phi a_3 - \Psi a_0}{\Phi^2 - \mu \Psi^2}, \frac{\Phi a_4 - \mu \Psi a_1}{\Phi^2 - \mu \Psi^2}, \frac{\Phi a_5 - \Psi a_2}{\Phi^2 - \mu \Psi^2} \right). \tag{8}$$

It is easy to see that value E_l is included in set (6). Thus, to vector A such that

$$(a_0 + a_2 + \tau a_4)^2 \neq \mu \left(\tau a_1 + a_3 + a_5 \right)^2 \tag{9}$$

it correspons the single bi-side local unit, i.e. every of such vectors is locally invertible.

3.2. The 6-Dimension FNAA with Compressing Multiplication Operation

Table 2 defines the multiplication operation possessing property of the compressing map of the 6-dimensional FNAA into some subset of the algebra elements, which can be described with the following formula

$$A \circ V = H, \tag{10}$$

where operands A and $V = \sum\limits_{j=0}^{m-1} v_j \mathbf{e}_j$ take on all possible values of the considered FNAA and vector $H = \sum\limits_{k=0}^{m-1} h_k \mathbf{e}_k$ is an element from some subset representing all possible results

of the multiplication operation. Such property is sufficiently specific and illustrates that constructing different types of the BVMTs one can define FNAAs possessing significantly different properties.

Table 2

The BVMT for Defining FNAA with Compressing Multiplication Operation

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

Using Table 2 one can represent vector equation (10) in the form of the system of six linear equations with coordinates of the right operand $v_0, v_1, \ldots, v_5$ as the unknown values. It is easy to show that the last system contains the following three independent systems of two linear equations:

$$\begin{cases} \mu v_0 (a_0 + a_2 + a_4) + v_1 (a_0 + a_2 + a_4) = h_0; \\ \mu v_0 (a_1 + a_3 + a_5) + v_1 (a_1 + a_3 + a_5) = h_1; \end{cases} \tag{11}$$

$$\begin{cases} \mu v_2 (a_0 + a_2 + a_4) + v_3 (a_0 + a_2 + a_4) = h_2; \\ \mu v_2 (a_1 + a_3 + a_5) + v_3 (a_1 + a_3 + a_5) = h_3; \end{cases} \tag{12}$$

$$\begin{cases} \mu v_4 (a_0 + a_2 + a_4) + v_5 (a_0 + a_2 + a_4) = h_4; \\ \mu v_4 (a_1 + a_3 + a_5) + v_5 (a_1 + a_3 + a_5) = h_5. \end{cases} \tag{13}$$

From systems (11), (12), and (13) we get

$$\frac{h_0}{h_1} = \frac{h_2}{h_3} = \frac{h_4}{h_5} = \frac{a_0 + a_2 + a_4}{a_1 + a_3 + a_5} = \rho, \tag{14}$$

where ρ $(1 \le \rho \le p-1)$ depends only on the left operand in the left part of (10). It is easy to estimate the number $\#\{H\}$ of possible different values at output of multiplication operation: $\#\{H\} < p^4$.

3.3. The FNAA Containing a Set of Global Left-Side Units

Another example of the 6-dimensional FNAAs possessing interesting properties is defined by Table 3. If structural coefficient μ is equal to 1, then the defined multiplication operation possesses compressing property, like in the FNAA described in previous subsection. If $\mu \neq 1$, then the algebra defined with Table 3 contains a large set of the left-side units acting on each element of the algebra (such units can be called the global left-side units). At the same time, the algebra contains no global bi-side unit and no global right-side unit. The single local bi-side unit corresponds to each locally invertible element of the considered FNAA. Let us consider case $\mu \neq 1$.

Table 3

The BVMT defining FNAA with set of the global left-side units ($\mu \neq 1$)

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

For some left-side unit X acting on vector A it holds the vector equation

$$X \circ A = A. \tag{15}$$

Using Table 3 one can represent (15) 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 unknown values:

$$\begin{cases} a_0 (x_0 + \mu x_2 + x_4) + a_5 (x_0 + x_2 + x_4) = a_0; \\ a_1 (x_1 + x_3 + x_5) + a_4 (x_1 + \mu x_3 + x_5) = a_1; \\ a_2 (x_0 + \mu x_2 + x_4) + a_3 (x_0 + x_2 + x_4) = a_2; \\ a_2 (x_1 + \mu x_3 + x_5) + a_3 (x_1 + x_3 + x_5) = a_3; \\ a_1 (x_0 + x_2 + x_4) + a_4 (x_0 + \mu x_2 + x_4) = a_4; \\ a_0 (x_1 + \mu x_3 + x_5) + a_5 (x_1 + x_3 + x_5) = a_5. \end{cases} \tag{16}$$

System (16) has the same solutions as the following system of four linear equations with six unknowns:

$$\begin{cases} x_0 + x_2 + x_4 = 0; \\ x_0 + \mu x_2 + x_4 = 1; \\ x_1 + x_3 + x_5 = 1; \\ x_1 + \mu x_3 + x_5 = 0. \end{cases} \tag{17}$$

The solution of system (17) does not depend on value A and describes the following set of global left-side units:

$$E_l = (x_0, x_1, x_2, x_3, x_4, x_5) = \left(d, h, \frac{1}{\mu - 1}, \frac{1}{1 - \mu}, \frac{1}{1 - \mu} - d, \frac{\mu}{\mu - 1} - h \right), \tag{18}$$

where $d, h = 0, 1, \ldots, p - 1$.

Finding the right-side units acting on vector A is connected with solving the following vector equation:

$$A \circ X = A. \tag{19}$$

Using Table 3 one can represent (19) in the form of the following three independent systems each of which contains two linear equations:

$$\begin{cases} x_0 (a_0 + \mu a_2 + a_4) + x_5 (a_0 + a_2 + a_4) = a_0; \\ x_0 (a_1 + \mu a_3 + a_5) + x_5 (a_1 + a_3 + a_5) = a_5; \end{cases} \tag{20}$$

$$\begin{cases} x_1 (a_1 + a_3 + a_5) + x_4 (a_1 + \mu a_3 + a_5) = a_1; \\ x_1 (a_0 + a_2 + a_4) + x_4 (a_0 + \mu a_2 + a_4) = a_4; \end{cases} \tag{21}$$

$$\begin{cases} x_2 (a_0 + \mu a_2 + a_4) + x_3 (a_0 + a_2 + a_4) = a_2; \\ x_2 (a_1 + \mu a_3 + a_5) + x_3 (a_1 + a_3 + a_5) = a_3. \end{cases} \tag{22}$$

Each of systems (20), (21), and (22) has the single solution, therefore for vector A there exists single right-side unit

$$E_r = (x_0, x_1, x_2, x_3, x_4, x_5),$$

where:

$$x_0 = \frac{a_0\,(a_1 + a_3) - a_5\,(a_2 + a_4)}{(\mu - 1)\,(a_1a_2 + a_2a_5 - a_0a_3 - a_3a_4)}; \quad x_1 = \frac{a_0a_1 + \mu a_1a_2 - \mu a_3a_4 - a_4a_5}{(\mu - 1)\,(a_1a_2 + a_2a_5 - a_0a_3 - a_3a_4)};$$

$$x_2 = \frac{1}{\mu - 1}; \qquad x_3 = \frac{1}{1 - \mu};$$

$$x_4 = \frac{a_3a_4 + a_4a_5 - a_0a_1 - a_1a_2}{(\mu - 1)\,(a_1a_2 + a_2a_5 - a_0a_3 - a_3a_4)}; \quad x_5 = \frac{\mu a_2a_5 + a_4a_5 - a_0a_1 - \mu a_0a_3}{(\mu - 1)\,(a_1a_2 + a_2a_5 - a_0a_3 - a_3a_4)}.$$

It is easy to show that the right-side unit related to an arbitrary vector A is contained in the set of global left-side units (18). The last means the right-side local units are simultaneously the bi-side local units.

4. Unified Method for Defining FNAAs for Arbitrary Even Dimension

For the case of even dimension m of the finite vector space the FNAAs can be defined by the following general method that consists in defining the multiplication of formal basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$ for $i, j = 0, 1, \ldots, m-1$ with formula

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \mathbf{e}_i, & \text{if the value } \ i + j \ \text{ is even,} \\ \mathbf{e}_{m-1-i}, & \text{if the value } \ i + j \ \text{ is odd,} \end{cases} \tag{23}$$

where addition and subtraction are performed modulo m.

Proposition 1. *Formulas (2) and (23) define the associative multiplication operation for arbitrary even value of dimension m.*

Proof. Suppose $i,\ j,\ k$ denote even integers and $i',\ j',\ k'$ denote odd integers. While multiplying three formal basis vectors we have the following cases:

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

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_{k'} = \mathbf{e}_i \circ \mathbf{e}_{k'} = \mathbf{e}_{m-1-i}, \qquad \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_{k'}) = \mathbf{e}_i \circ \mathbf{e}_{m-1-j} = \mathbf{e}_{m-1-i};$$

$$(\mathbf{e}_i \circ \mathbf{e}_{j'}) \circ \mathbf{e}_k = \mathbf{e}_{m-1-i} \circ \mathbf{e}_k = \mathbf{e}_{m-1-(m-1-i)} = \mathbf{e}_i, \quad \mathbf{e}_i \circ (\mathbf{e}_{j'} \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{m-1-j'} = \mathbf{e}_i;$$

$$(\mathbf{e}_{i'} \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{m-1-i'} \circ \mathbf{e}_k = \mathbf{e}_{m-1-i'}, \qquad \mathbf{e}_{i'} \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_{i'} \circ \mathbf{e}_j = \mathbf{e}_{m-1-i'};$$

$$(\mathbf{e}_{i'} \circ \mathbf{e}_j) \circ \mathbf{e}_{k'} = \mathbf{e}_{m-1-i'} \circ \mathbf{e}_{k'} = \mathbf{e}_{i'}, \qquad \mathbf{e}_{i'} \circ (\mathbf{e}_j \circ \mathbf{e}_{k'}) = \mathbf{e}_{i'} \circ \mathbf{e}_{m-1-j} = \mathbf{e}_{i'};$$

$$(\mathbf{e}_{i'} \circ \mathbf{e}_{j'}) \circ \mathbf{e}_k = \mathbf{e}_{i'} \circ \mathbf{e}_k = \mathbf{e}_{m-1-i'}, \qquad \mathbf{e}_{i'} \circ (\mathbf{e}_{j'} \circ \mathbf{e}_k) = \mathbf{e}_{i'} \circ \mathbf{e}_{m-1-j'} = \mathbf{e}_{m-1-i'};$$

$$(\mathbf{e}_{i'} \circ \mathbf{e}_{j'}) \circ \mathbf{e}_{k'} = \mathbf{e}_{i'} \circ \mathbf{e}_{k'} = \mathbf{e}_{i'}, \qquad \mathbf{e}_{i'} \circ (\mathbf{e}_{j'} \circ \mathbf{e}_{k'}) = \mathbf{e}_{i'} \circ \mathbf{e}_{j'} = \mathbf{e}_{i'};$$

$$(\mathbf{e}_i \circ \mathbf{e}_{j'}) \circ \mathbf{e}_{k'} = \mathbf{e}_{m-1-i} \circ \mathbf{e}_{k'} = \mathbf{e}_{m-1-i}, \qquad \mathbf{e}_i \circ (\mathbf{e}_{j'} \circ \mathbf{e}_{k'}) = \mathbf{e}_i \circ \mathbf{e}_{j'} = \mathbf{e}_{m-1-i}.$$

Thus, for multiplying all possible ordered triples of the basis vectors it holds the property of associativity.

□

Formula (23) defines structure of the BVMT for arbitrary fixed even dimension $m \geq 2$. After the BVMT will have been constructed one can add one or several structural coefficients in some of the cells of the table so that the property of associativity will be saved. Tables 4, 5, and 6 presents some examples of the BVMT constructed in line with such unified method for cases $m = 2, 4$ and 6 respectively.

Table 4

The BVMT for the case $m = 2$

$\circ$	$\mathbf{e_0}$	$\mathbf{e_1}$
$\mathbf{e_0}$	$\mu\mathbf{e}_0$	$\mu\mathbf{e}_1$
$\mathbf{e}_1$	$\tau\mathbf{e}_0$	$\tau\mathbf{e}_1$

The 4-dimensional FNAA defined by Table 5, where $\mu\tau \neq 1$, represents itself a ring with global bi-side unit

$$E = \left(\frac{1}{1-\mu\tau}, \frac{1}{1-\mu\tau}, \frac{\tau}{\mu\tau-1}, \frac{\mu}{\mu\tau-1}\right)$$

such that for arbitrary 4-dimensional vector A the following equations $V \circ E = E \circ V = V$ hold true. In this ring 4-dimension vectors $A = (a_0, a_1, a_2, a_3)$ such that $a_0 a_1 \neq a_2 a_3$ are invertible. All invertible 4-dimensional vectors compose a finite group order of which is equal to $p(p-1)\left(p^2-1\right)$. If $a_0 a_1 = a_2 a_3$ vector A is non-invertible. In the ring there exist $p^3 + p^2 - p$ different non-invertible vectors. In the subset of the non-invertible vectors there exists the single local bi-side unit E' corresponding to some fixed non-invertible vector A. The local bi-side unit E' depends on the coordinates of vector A as follows:

Table 5

The BVMT for the case $m = 4$

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

$$E' = \left(x_0, \frac{a_3}{a_0\mu + a_3} - \frac{a_0 + a_3\tau}{a_0\mu + a_3} \cdot \frac{a_3}{a_0} x_0, \frac{a_3}{a_0\mu + a_3} - \frac{a_0 + a_3}{a\mu + d} x_0, \frac{a_3}{a_0} x_0\right),$$

where $x_0 = a_0 \left(a_0 + a_1 + \mu a_2 + \tau a_3\right)^{-1}$.

In case $m = 6$ we found a variety of options for embedding structural coefficients. For example, in Table 6 three different structural coefficients are included, which are distributed in such a way that the associativity property of the multiplication operation is preserved. The FNAA defined by Table 6 contains a set of p^2 different global right-side units E_r described by the following formula:

Table 6

The BVMT defining the 6-dimensional FNAA with p^2 different global right-side units

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

$$E_r = \left(i, j, \frac{1 + (\lambda-1)i}{\tau-\mu}, \frac{1 + (\lambda-1)j}{\mu-\lambda\tau}, \frac{(\mu-\lambda\tau)i - \mu}{\tau-\mu}, \frac{(\tau-\mu)j - \tau}{\mu-\lambda\tau}\right),$$

where $i, j = 0, 1, \ldots, p-1$.

5. New Forms of Defining the Hidden Discrete Logarithm Problem

Using different types of the BVMTs for defining the associative multiplication operation one can define different types of m-dimensional FNAAs, including algebras

containing only locally invertible elements. The last does not suit to define the HDLP while using the known form of the formulation of the HDLP. To use such type of finite algebras as carriers of the HDLP it needs to propose another form for formulating the HDLP.

Suppose N be some locally invertible vector such that for some prime number ω we have $N^{\omega} = E'$, where E' is the local bi-side unit relating to N. Then the sequence $\{N, N^2, ..., N^{\omega}\}$ contains ω different elements of the considered FNAA and represents a cyclic finite group with the group operation $\circ$, therefore ω can be called local order of the element N. Using the local bi-side unit element E' one can define the following homomorphism $\varphi_{N,t}$ over the set of locally invertible elements $V_{E'}$ computed as

$$V_{E'} = V \circ E',$$

where V takes on all values in the considered FNAA (note the element E' acts in the frame of the set of elements $V_{E'}$ as the right-side unit).

Like standard automorphisms ψ_W in the finite non-commutative group described by the formula $\psi_W(V) = W^{-1} \circ V \circ W$, where W is an invertible element of the ring, the homomorphism $\varphi_{N,t}$ is defined as follows:

$$\varphi_{N,t}\left(V_{E'}\right) = N^{\omega-t} \circ V_{E'} \circ N^t.$$

Actually, the last formula defines homomorphism since with evidence the following holds true:

$$\varphi_{N,t}\left(V'_{E'} \circ V''_{E'}\right) = \varphi_{N,t}\left(V'_{E'}\right) \circ \varphi_t\left(V''_{E'}\right),$$
$$\varphi_{N,t}\left(V'_{E'} + V''_{E'}\right) = \varphi_{N,t}\left(V'_{E'}\right) + \varphi_{N,t}\left(V''_{E'}\right).$$

To define public-key cryptoschemes, like that described in [13, 15], one can select some locally invertible vector G having sufficiently large prime order g, which satisfies condition $G \circ N \neq N \circ G$, compute vector $G_{E'} = G \circ E'$ and use the formula

$$Y = N^{\omega-t} \circ G^x_{E'} \circ N^t, \tag{24}$$

where Y is a public key and the pair of numbers (t, x) is a private key (the integers $t < \omega$ and $x < g$ is to be selected at random). Finding values (t, x) from equation (24) represents a novel form of the HDLP. The FNAAs with local invertibility of all elements (except zero), like that described in subsection 3.2 (see case with structural coefficient equal to a quadratic non-residue) are especially attractive as carriers of the HDLP while the last is defined by formula (24).

The second proposed new form of defining the HDLP relates to using the 6-dimensional FNAA containing the set of the global left-side units $\{L_i : L_i \circ V = V\}$, where i is an integer and V is an arbitrary 6-dimensional vector. For arbitrary left-side unit L_i and arbitrary integer w it holds $L_i^w = L_i$. Suppose N is a vector having sufficiently large prime order relatively its local bi-side unit and vectors U and D satisfy the condition $D \circ U = L_1$, where L_1 is some global left-side unit. Then the public key Y can be computed as follows

$$Y = U^w \circ N^x \circ D^w = \left(U^w \circ N \circ D^w\right)^x, \tag{25}$$

where the pair of integers (w, x) is the private key. Finding values w and x from the equation (25) represents a kind of the HDLP. The last equation can be used to define the public key agreement protocol and public encryption algorithm.

To provide possibility to construct the digital signature scheme we propose the following form of the HDLP in which there is used a double masking mechanism as follows. Suppose the private key represents the set of values x, N, U, U', D, and T, where x is a random integer and the following two conditions are met $D \circ U = L_1$, $D \circ U' = L_2$, and $T \circ U' = L_3$ for some left-side units L_1, L_2, and L_3. Besides vector N has a local order equal to sufficiently large prime q. The required triple of vectors U, D, and T can be computed as follows:

1. Select values D, L_1 and L_2.
2. Compute vector U from vector equation $D \circ U = L_1$.
3. Compute vector U' from vector equation $T \circ U' = L_2$.
4. Compute vectors T and L_3 from vector equation $T \circ U' = L_3$.

The public key represents the pair of the 6-dimensional vectors Y and Q that can be computed using the following two formulas:

$$Y = U \circ N^x \circ D; \qquad Q = U' \circ N \circ T. \tag{26}$$

The signature generation procedure includes the following steps:

1. Generate random value k and compute vector $R = U \circ N^k \circ T$.
2. Using specified hash function F_h compute first signature element $e = F_h(M, R)$, where M is some signed document.
3. Considering bit string e as a binary number compute second signature element $s = k - xe \bmod q$.

Verification of signature (e, s) (representing a pair of integers) to document M is executed as follows:

1. Compute vector $R^?$: $R^? = Y^e \circ Q^s$.
2. Compute bit string $e^? = F_h(M, R^?)$.
3. Compare values $e^?$ and e. If $e^? = e$, then the signature is valid. Otherwise the signature is rejected as false one.

Corrctness proof of the proposed signature scheme is evident:

$$\begin{aligned} &R^? = (U \circ N^x \circ D)^e \circ (U' \circ N \circ T)^{k-xe} = U \circ N^{xe} \circ D \circ U' \circ N^{k-xe} \circ T = \\ &= U \circ N^{xe} \circ L_2 \circ N^{k-xe} \circ T = U \circ N^{xe+k-xe} \circ T = U \circ N^k \circ T = R \Rightarrow \\ &\Rightarrow e^? = F_h(M, R^?) = F_h(M, R) = e. \end{aligned}$$

Like in the case of the Schnorr digital signature protocol [19] in the described signature scheme there is use some cyclic group of the prime order. The difference consists in the hiding this cyclic group. The public part of the proposed signature scheme is the used FNAA and two its elements Y and Q that are connected with the hidden cyclic group generated by powers of vector N that is an element of a private key. Connection between vectors Y and Q can be represented as

$$Y = Z_l \circ Q^x \circ Z_r,$$

where integer x and vectors Z_l and Z_r are unknowns. The last formula shows vectors Y and Q belong to different cyclic groups contained in the used FNAA with set of the global left-side units. Therefore, the potential forgery of a signature should find a representation of public key elements Y and Q in a form like (26) and to solve the discrete logarithm

problem in a finite cyclic group contained in the FNAA. There exists many different variants of mentioned representation, however finding at least one of them appears to be a computationally difficult problem.

Estimation of the security of the propose signature scheme to attacks with using hypothetic quantum computer is connected with estimation of the computational difficulty of the reduction of the used HDLP to the discrete logarithm problem in some cyclic group. Consideration of this item represents an individual problem.

Conclusion

Several 6-dimensional FNAA have been introduced as novel carriers of the HDLP that is attractive as post-quantum primitive of the public-key cryptoschemes. Some properties of algebras, which relate to defining the HDLP, have been investigated. It also introduced a general method for constructing FNAAs of arbitrary even dimensions. Some of the introduced FNAA contain only vectors that are locally invertible. For the last case there are proposed new forms of the definition of the HDLP. One of the proposed novel forms of the HDLP has been used to design a digital signature scheme. The proposed new forms of the HDLP represent an interest as independent primitives of post-quantum cryptography. Comparing with the signature schemes proposed in frame of NIST project PQCrypto the introduced signature scheme based on the HDLP has the following significant advantages: a higher perfomance and smaller signature size. One can hope that due to the last merits the proposed signature scheme will attract attention of the researchers to the task of the estimating its security.

Acknowledgements. *The reported study was partially funded by Russian Foundation for Basic Research (project no. 18-07-00932-a).*

References

1. Sirwan A., Majeed N. New Algorithm for Wireless Network Communication Security. *International Journal on Cryptography and Information Security*, 2016, vol. 6, no. 3, pp. 1–8.
2. Yiteng Feng, Guomin Yang, Joseph K.Liu. A New Public Remote Integrity Checking Scheme with User and Data Privacy. *International Journal of Applied Cryptography*, 2017, vol. 3, no. 3, pp. 196–209. DOI: 10.1504/IJACT.2017.086232
3. Chiou S.Y. Novel Digital Signature Schemes Based on Factoring and Discrete Logarithms. *International Journal of Security and Its Applications*, 2016, vol. 10, no. 3, pp. 295–310. DOI: 10.14257/ijsia.2016.10.3.26
4. Yan S.Y. *Quantum Computational Number Theory*. N.Y., Springer, 2015. DOI: 10.1007/978-3-319-25823-2
5. Yan S.Y. *Quantum Attacks on Public-Key Cryptosystems*. N.Y., Springer, 2014.
6. *Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016*. Fukuoka, Springer, 2016.
7. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018*. Fort Lauderdale, Springer, 2018.
8. Hiranvanichakorn P. Provably Authenticated Group Key Agreement based on Braid Groups. The Dynamic Case. *International Journal of Network Security*, 2017, vol. 19, no. 4, pp. 517–527.

9. Verma G.K. Probable Security Proof of a Blind Signature Scheme over Braid Groups. *International Journal of Network Security*, 2011, vol. 1, no. 2, pp. 118–120.

10. Myasnikov A., Shpilrain V., Ushakov A. *A Practical Attack on a Braid Group Based Cryptographic Protocol*. 2005. Springer, vol. 3621, pp. 86–96.

11. Moldovyan D.N., Moldovyan N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols. Conference on Mathematical Methods, Models and Architectures for Computer Network Security. 2010, *Springer*, vol. 6258, pp. 183–194. DOI: 10.1007/978-3-642-14706-7_14

12. Sakalauskas E., Tvarijonas P., Raulynaitis A. Key Agreement Protocol Using Conjugacy and Discrete Logarithm Problems in Group Representation Level. *Informatica*, 2007, vol. 18, no. 1, pp. 115–124.

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

14. Moldovyan D.N., Moldovyan N.A. Cryptoschemes Over Hidden Conjugacy Search Problem and Attacks Using Homomorphisms. *Quasigroups Related Systems*, 2010, vol. 18, no. 2, pp. 177–186.

15. 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. DOI: 10.1007/s10958-017-3371-y

16. Moldovyan A.A., Moldovyan N.A., Shcherbacov V.A. Non-Commutative Finite Associative Algebras of 2-Dimension Vectors. *Computer Science Journal of Moldova*, 2017, vol. 25, no. 3, pp. 344–356.

17. Moldovyan D.N., Moldovyan N.A., Shcherbacov V.A. Non-Commutative Finite Associative Algebras of 3-Dimensional Vectors. *Quasigroups and Related Systems*, 2018, vol. 26, no. 1, pp. 109–120.

18. Moldovyan N.A., Moldovyan P.A. Vector Form of the Finite Fields $GF(p^m)$. *Bulletinul Academiei de stiinte a Republicii Moldova. Matematica*, 2009, no. 3, pp. 57–63.

19. Schnorr C.P. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174. DOI: 10.1007/BF00196725

Received September 11, 2018

УДК 512.624.5 **DOI: 10.14529/mmp190106**

КОНЕЧНЫЕ НЕКОММУТАТИВНЫЕ АССОЦИАТИВНЫЕ АЛГЕБРЫ КАК НОСИТЕЛИ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Н.А. Молдовян[1]***, А.А. Молдовян***[1]
[1]Санкт-Петербургский институт информатики и автоматизации РАН,
г. Санкт-Петербург, Российская Федерация

Статья рассматривает новые конечные алгебры, представляющие интерес в качестве носителей задачи дискретного логарифмирования в скрытой группе. В частности, предложены новые 4-мерные и 6-мерные конечные некоммутативные алгебры с ассоциативной операцией умножения и описаны их свойства. Также предложен общий метод

задания конечных некоммутативных ассоциативных алгебр произвольной четной размерности $m \geq 2$. Некоторые из рассмотренных алгебр содержат глобальную двухстороннюю единицу, а другие не содержат такой единицы. В последнем случае элементы алгебры обратимы локально относительно некоторой локальной двухсторонней единицы, действующей в рамках некоторого подмножества элементов алгебры. Для алгебр последнего типа выведены формулы, описывающие множества правосторонних, левосторонних и двухсторонних локальных единиц. Также представлены алгебры, содержащие большое множество глобальных левосторонних (правосторонних) единиц при отсутствии в них глобальной двухсторонней единицы. Поскольку известные формы задания крытой задачи дискретного логарифмирования используют обратимость элементов алгебры относительно глобальной двухсторонней единицы, были предложены новые формы задания этой вычислительно трудной задачи. Результаты статьи могут быть использованы для разработки криптографических алгоритмов и протоколов с открытым ключом, включая постквантовые криптосхемы. Впервые предложена схема цифровой подписи, основанная на скрытой задаче дискретного логарифмирования.

Ключевые слова: конечная ассоциативная алгебра; некоммутативная алгебра; глобальная единица; левосторонняя единица; локальная единица; локальная обратимость; задача дискретного логарифмирования; криптосхема с открытым ключом; цифровая подпись; постквантовая криптография.

Литература

1. Sirwan, A. New Algorithm for Wireless Network Communication Security / A. Sirwan, N. Majeed // International Journal on Cryptography and Information Security. – 2016. – Т. 6, № 3. – С. 1–8.
2. Feng, Yiteng. A New Public Remote Integrity Checking Scheme with User and Data Privacy / Yiteng Feng, Guomin Yang, Joseph K.Liu // International Journal of Applied Cryptography. – 2017. – Т. 3, № 3. – С. 196–209.
3. Chiou, S.Y. Novel Digital Signature Schemes Based on Factoring and Discrete Logarithms / S.Y. Chiou // International Journal of Security and Its Applications. – 2016. – Т. 10, № 3. – С. 295–310.
4. Yan, S.Y. Quantum Computational Number Theory / S.Y. Yan. – New York: Springer, 2015.
5. Yan, S.Y. Quantum Attacks on Public-Key Cryptosystems / S.Y. Yan. – New York: Springer, 2014.
6. Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24–26, 2016. – Springer, 2016.
7. Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. – Springer, 2018.
8. Hiranvanichakorn, P. Provably Authenticated Group Key Agreement Based on Braid Groups. The Dynamic Case / P. Hiranvanichakorn // International Journal of Network Security. – 2017. – Т. 19, № 4. – С. 517–527.
9. Verma, G.K. Probable Security Proof of a Blind Signature Scheme over Braid Groups / G.K. Verma // International Journal of Network Security. – 2011. – Т. 12, № 2. – С. 118–120.
10. Myasnikov, A. A Practical Attack on a Braid Group Based Cryptographic Protocol / A. Myasnikov, V. Shpilrain, A. Ushakov // Advances in Cryptology – CRYPTO'05. Springer, 2005. – Т. 3621. – С. 86–96.
11. Moldovyan, D.N. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols / D.N. Moldovyan, N.A. Moldovyan // 5th Int. Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS 2010 Proceedings. – Springer, 2010. – Т. 6258. – С. 183–194.

12. Sakalauskas, E. Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level / E. Sakalauskas, P. Tvarijonas, A. Raulynaitis // Informatica. – 2007. – Т. 18, № 1. – С. 115–124.
13. Moldovyan, D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes / D.N. Moldovyan // Quasigroups and Related Systems. – 2010. – Т. 18, № 2. – С. 165–176.
14. Moldovyan, D.N. Cryptoschemes over Hidden Conjugacy Search Problem and Attacks Using Homomorphisms / D.N. Moldovyan, N.A. Moldovyan // Quasigroups Related Systems. – 2010. – Т. 18, № 2. – С. 177–186.
15. Kuzmin, A.S. Cryptographic Algorithms on Groups and Algebras / A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev // Journal of Mathematical Sciences. – 2017. – V. 223, № 5. – С. 629–641.
16. Moldovyan, A.A. Non-Commutative Finite Associative Algebras of 2-Dimension Vectors / A.A. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov // Computer Science Journal of Moldova. – 2017. – Т. 25, № 3. – С. 344–356.
17. Moldovyan, D.N. Non-Commutative Finite Associative Algebras of 3-Dimensional Vectors / D.N. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov // Quasigroups and Related Systems. – 2018. – Т. 26, № 1. – С. 109–120.
18. Moldovyan, N.A. Vector Form of the Finite Fields $GF(p^m)$ / N.A. Moldovyan, P.A. Moldovyanu // Bulletinul Academiei de Stiinte a Republicii Moldova. Matematica. – 2009. – № 3. – С. 57–63.
19. Schnorr, C.P. Efficient Signature Generation by Smart Cards / C.P. Schnorr // Journal of Cryptology. – 1991. – V. 4. – P. 161–174.

Николай Андреевич Молдовян, доктор физико-математических наук, профессор, главный научный сотрудник, лаборатория «Кибербезопасность и постквантовая криптография», Санкт-Петербургский институт информатики и автоматизации Российской академии наук (г. Санкт-Петербург, Российская Федерация), nmold@mail.ru.

Александр Андреевич Молдовян, доктор физико-математических наук, профессор, главный научный сотрудник, лаборатория «Кибербезопасность и постквантовая криптография», Санкт-Петербургский институт информатики и автоматизации Российской академии наук (г. Санкт-Петербург, Российская Федерация), maa1305@yandex.ru.

Поступила в редакцию 11 сентября 2018 г.