Computer Science Journal of Moldova, vol.**26**, no.3(78), 2018

Post-quantum signature algorithms based on the hidden discrete logarithm problem

A.A. Moldovyan N.A. Moldovyan

Abstract

New options of the hidden discrete logarithm problem are proposed as cryptographic primitive of the post-quantum signature algorithms. Two signature schemes using computations in finite non-commutative algebras with associative multiplication operation are introduced. The main feature of the proposed signature algorithms consists in using locally invertible elements of algebras. Two different types of algebras are used: i) containing global bi-side unit and ii) containing a large set of global right-side units.

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

MSC 2000: 94A60, 16Z05, 14G50, 11T71, 16S50.

1 Introduction

Development of the post-quantum public-key cryptographic algorithms and protocols is a current challenge of the applied and theoretic cryptography [1], [2]. A well-known response to this challenge is the competition for the development of the post-quantum public-key cryptoschemes, announced by NIST in 2016 [3]. The current outcome of this competition is a set of post-quantum cryptoschemes, chosen as candidates for the adoption of post-quantum cryptographic standards on their basis [4]. At the next stage it is expected to initiate an all-round discussion of candidates from the wide cryptographic community. It is

assumed that the main point at this three-year stage will be research on the resistance of selected candidates to attacks using a hypothetical quantum computer.

The problem of discrete logarithm in a hidden cyclic group [5] remained outside the attention of NIST participants, although it seems to be an interesting primitive for constructing practical post-quantum cryptoschemes. Apparently this is due to the fact that in the literature this problem, which can be called the hidden discrete logarithm problem (HDLP), is little illuminated. Another reason is a relatively small number of known carriers of this problem, which are finite noncommutative associative algebras (FNAAs). The urgency of the problem of finding new carriers of the HDLP is underlined in the paper [6].

The purpose of this work is to attract the attention of cryptographic community to the HDLP as a post-quantum cryptographic primitive. To achieve this goal, new types of algebras are being developed (Section 2), new variants of the HDLP are introduced (Section 3), and algorithms for digital signature based on the proposed options of the HDLP are being developed for the first time (Section 4). In the concluding Section 5 we estimate that the application of the HDLP for the design of the post-quantum public-key algorithms and protocols is a promising direction.

2 New carriers of the HDLP

The known option of the HDLP [5] is formulated in a finite noncommutative group Γ as follows. Suppose the group Γ contains elements Q and G having large prime order q and satisfying the condition $G \circ Q \neq Q \circ G$. In [5] it is proposed to compute a public key Y as follows $Y = G^w \circ Q^x \circ G^{-w}$, where the pair of integers (w, x) represents the private key. Computing the values $w < q$ and $x < q$, while the elements Y, Q, and G are known, is called HDLP. The paper [5] decribes the public key-agreement protocol, the public encryption algorithm, and the commutative cipher based on the HDLP formulated in the finite algebra of quaternions. No proposals for digital signature schemes are known in the literature.

While considering new FNAAs of the dimensions $m = 4$ and $m = 6$ the following common description is used. The m-dimensional vector space defined over the finite field $GF(p)$ becomes the m-dimensional finite algebra after the operation for multiplying arbitrary two vectors is defined, which is distributive relatively the addition operation. To set the multiplication operation one can use the notion of formal basis vectors denoted as $\mathbf{e}_0 = (1, 0, 0 \ldots, 0)$, $\mathbf{e}_1 = (0, 1, 0 \ldots, 0)$, ... $\mathbf{e}_{m-1} = (0, 0 \ldots, 0, 1)$ and representation of some vector $A = (a_0, a_1, \ldots a_{m-1})$ in the form of the following summ of the single component vectors $a_i\mathbf{e}_i$: $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$.

The multiplication operation $\circ$ of the m-dimensional vectors A and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined by the following formula

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

where product $\mathbf{e}_i \circ \mathbf{e}_j$ for all possible pairs of the integers i and j is to be replaced by some single-component vector $\lambda\mathbf{e}_k$ indicated by so called basis vector multiplication table (BVMT). In formula (1) it is ussumed that the intersection of the ith row and the jth column defines the cell which contains the value $\lambda\mathbf{e}_k = \mathbf{e}_i \circ \mathbf{e}_j$. If the coordinate $\lambda \neq 1$, then λ is called structural coefficient. To build a FNAA we should compose and use some BVMT defining non-commutative associative multiplication operation.

2.1 The 4-dimensional FNAA

In this subsection we summarize in brief some results of the paper [7] relating to the case of the 4-dimensional non-commutative algebra. The FNAA defined by Table 1, where $\tau \neq 1$, contains the global bi-side unit

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

for which for every element of the algebra the formulas $A \circ E = A$ and $E \circ A = A$ hold. Every vector A of the algebra, coordinates of which

Table 1. The BVMT for defining the 4-dimensional algebra with the global unit ($\tau \neq 1$).

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

satisfy the condition $a_0a_1 \neq a_2a_3$, is invertible relatively the global unit E, i.e., for arbitrary vector of such a kind there exists the vector A^{-1} such that $A \circ A^{-1} = A^{-1} \circ A = E$ holds. The vectors B satisfying the condition $b_0b_1 = b_2b_3$ are non-invertible relatively the global unit E. However, the majority of vectors B are locally invertible, i.e., invertible relatively some local bi-side unit E_B acting as unit element in some subset of the algebra elements, which includes the vector B. Evidently, this subset is a finite group with the group operation $\circ$. There exists the single local bi-side unit in the subset of the non-invertible (globally) algebra elements. However, for some fixed non-invertible vector B there exists a large set of the vectors E'_B satisfying the condition $E'_B \circ B = B$. This set of the vectors E'_B can be called the set of the left-side units of the vector B and is described by the following formula:

$$E'_B = \left(d,\ \frac{b_2}{b_0+b_2} - \frac{b_0+b_2}{\tau b_0+b_2}h,\ h,\ \frac{b_0}{\tau b_0+b_2} - \frac{b_0+b_2}{\tau b_0+b_2}d \right), \qquad (2)$$

where $h, d = 0, 1, \ldots p-1$. Analogously, for the vector B there exists a large set of the vectors E''_B satisfying the condition $B \circ E''_B = B$. The last set can be called the set of the right-side units of the vector B and is described by the following formula:

$$E''_B = \left(d,\ \frac{b_3}{b_0+b_3} - \frac{b_0+\tau b_3}{b_0+b_3}h,\ \frac{b_0}{b_0+b_3} - \frac{b_0+\tau b_3}{b_0+b_3}d,\ h \right), \qquad (3)$$

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

The existence of many local units associated with a given non-invertible vector is an essential point in setting a new form of the HDLP proposed in Section 3.1. Earlier [8] the use of the non-invertible elements had been proposed in frame of the known form of the HDLP [5], however in that proposal there are not exploited the local units related to the used non-invertible element B.

2.2 The 6-dimensional FNAA

If the structural coefficients λ, μ, and τ in Table 2 satisfy the following two conditions $\mu \neq \tau$ and $\mu \neq \lambda\tau$, then this BVMT defines the multiplication operation in the 6-dimensional FNAAs containing a large set of the global right-side units. For some right-side unit X acting on the vector A the following vector equation holds:

$$A \circ X = A. \tag{4}$$

Using Table 2 one can represent (4) in the form of the following system of six linear equations with coordinates of the right operand $x_0, x_1, \ldots, x_5$ as the unknown values:

$$\begin{cases} a_0x_0 + \tau a_0x_2 + a_0x_4 + \lambda a_5x_0 + \mu a_5x_2 + a_5x_4 = a_0; \\ a_1x_1 + \mu a_1x_3 + \lambda a_1x_5 + a_4x_1 + \tau a_4x_3 + a_4x_5 = a_1; \\ a_2x_0 + \tau a_2x_2 + a_2x_4 + \lambda a_3x_0 + \mu a_3x_2 + a_3x_4 = a_2; \\ a_2x_1 + \tau a_2x_3 + a_2x_5 + a_3x_1 + \mu a_3x_3 + \lambda a_3x_5 = a_3; \\ a_0x_0 + \tau a_0x_2 + a_0x_4 + \lambda a_5x_0 + \mu a_5x_2 + a_5x_4 = a_4; \\ a_0x_1 + \tau a_0x_3 + a_0x_5 + a_5x_1 + \mu a_5x_3 + \lambda a_5x_5 = a_5. \end{cases} \tag{5}$$

The system (5) can be rewritten as the following system of six equations with four unknowns: $z_1 = x_0 + \tau x_2 + x_4$; $z_2 = \lambda x_0 + \mu x_2 + x_4$; $z_3 =$

$x_1 + \tau x_3 + x_5$; $z_4 = x_1 + \mu x_3 + \lambda x_5$:

$$\begin{cases} a_0 z_1 + a_5 z_2 = a_0; \\ a_1 z_4 + a_4 z_3 = a_1; \\ a_2 z_1 + a_3 z_2 = a_2; \\ a_2 z_3 + a_3 z_4 = a_3; \\ a_1 z_2 + a_4 z_1 = a_4; \\ a_0 z_3 + a_5 z_4 = a_5. \end{cases} \tag{6}$$

The system (6) has the following single solution:

$$z_1 = 1; \quad z_2 = 0; \quad z_3 = 0; \quad z_4 = 1. \tag{7}$$

Using (7) one can write the following two independent systems:

$$\begin{cases} x_0 + \tau x_2 + x_4 = 1; \\ \lambda x_0 + \mu x_2 + x_4 = 0; \end{cases} \tag{8}$$

$$\begin{cases} x_1 + \mu x_3 + \lambda x_5 = 1; \\ x_1 + \tau x_3 + x_5 = 0. \end{cases} \tag{9}$$

Solution of the systems (8) and (9) defines all solutions of the system (5). The lasts can be described by the following formula:

$$R = \left(x_0, \quad x_1, \quad \frac{1 + (\lambda - 1)x_0}{\tau - \mu}, \quad \frac{1 + (\lambda - 1)x_1}{\mu - \lambda\tau}, \right. \\ \left. \frac{(\mu - \lambda\tau)x_0 - \mu}{\tau - \mu}, \quad \frac{(\tau - \mu)x_1 - \tau)}{\mu - \lambda\tau} \right), \tag{10}$$

where $x_0, x_1 = 0, 1, \ldots p - 1$. Thus, the solutions of the system (5) do not depend on the value A, therefore formula (10) describes the full set of the global right-side units in the considered FNAA.

One can easily prove the following propositions:

Proposition 1. For arbitrary global right-side unit R_i and arbitrary integer n the following equation holds $R_i^n = R_i$.

Propossition 2. For arbitrary two 6-dimensional vectors U and T such that $U \circ T = R_i$, where R_i is a global right-side unit, and arbitrary integer n the following equation holds $U^n \circ T^n = R_i$.

Propossition 3. For arbitrary global right-side unit R_i, arbitrary 6-dimensional vector U, and arbitrary integer n the following equation holds $(R_i \circ U)^n = R_i \circ U^n$.

Proposition 4. Arbitrary global right-side unit R_i is simultaneously the single local bi-side unit E_A for the vector $R_i \circ A$, where A is an arbitrary non-zero vector.

Table 2. The BVMT defining the 6-dimensional FNAA with p^2 different global right-side units ($\lambda \neq 1$, $\mu \neq 1$, $\tau \neq 1$, $\tau \neq \mu$, $\lambda\tau \neq \mu$)

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

Computation of the local bi-side unit E_A relating to the vector A can be executed as finding the local left-side unit of the vector A from the vector equation $X \circ A = A$, i.e., from the following system of six equations with six unknowns:

$$\begin{cases} (a_0 + \tau a_2 + a_4)\, x_0 + (\lambda a_0 + \mu a_2 + a_4)\, x_5 = a_0; \\ (a_1 + \mu a_3 + \lambda a_5)\, x_1 + (a_1 + \tau a_3 + a_5)\, x_4 = a_1; \\ (a_0 + \tau a_2 + a_4)\, x_2 + (\lambda a_0 + \mu a_2 + a_4)\, x_3 = a_2; \\ (a_1 + \tau a_3 + a_5)\, x_2 + (a_1 + \mu a_3 + \lambda a_5)\, x_3 = a_3; \\ (\lambda a_0 + \mu a_2 + a_4)\, x_1 + (a_0 + \tau a_2 + a_4)\, x_4 = a_4; \\ (a_1 + \tau a_3 + a_5)\, x_0 + (a_1 + \mu a_3 + \lambda a_5)\, x_5 = a_5. \end{cases} \tag{11}$$

It is easy to see that for the vectors A satisfying the condition

$$\begin{aligned}\Delta_A = (a_4a_5 - a_0a_1)(\lambda - 1) + (a_3a_4 - a_1a_2)(\mu - \tau) + \\ + (a_2a_5 - a_0a_3)(\lambda\tau - \mu) \neq 0\end{aligned} \tag{12}$$

the system (11) has the single solution, i.e., the single local left-side unit $L_A \neq (0, 0, \ldots, 0)$ relates to every such vector A.

Proposition 5. All vectors A satisfying the condition (12) and relating to a fixed local bi-side unit E_A compose a finite group (with the unit E_A and the group operation $\circ$) contained in the considered 6-dimensional FNAA.

Earlier [9] the analogous 6-dimensional FNAA containing p^4 different global right-side units have been considered, however units of such type had not been used at defining the HDLP.

3 Novel forms of defining the HDLP

3.1 The HDLP in FNAA containing the global unit

Over a FNAA with the global unit (for example, over the 4-dimensional algebra considered in Subsection 2.1) one can define the HDLP as follows. Suppose the vector B is a non-invertible one and has sufficiently large prime local order ω, the invertible vectors G and H are such that the following conditions $G \circ B \neq B \circ G$, $G \circ H \neq H \circ G$, and $H \circ B \neq B \circ H$ hold. Then one can select at random an integer $x < \omega$ and an invertible vector E from the sets of the local single-side units of the vector B, i.e., from the sets (2) and (3) in the case of considered 4-dimensional FNAA, and compute the vectors Z, Y, and T:

$$Z = H \circ B \circ H^{-1}; \quad Y = G \circ B^x \circ G^{-1}; \quad T = G \circ E \circ H^{-1}. \tag{13}$$

The triple (Z, Y, T) can be used as public key to which the private key representing the set of values x, B, H, and G corresponds. The value E is also secret, however it is used only at step of computing the public-key element T. Computationally difficult problem consists in finding the private key or alternative four values x', B', H', and G' with which the public key can be expressed in accordance with the formulas (13).

3.2 The HDLP in FNAA containing large set of the global single-side units

Over a FNAA with the set of the single-side global units (for example, over the 6-dimensional algebra considered in Subsection 2.2, which contains a large set of the global right-side units) an option of the HDLP can be defined as follows. Suppose the vector A satisfying the condition (12) has sufficiently large prime local order ω and the vectors G, P, H, and Q are selected so that the following conditions $G \circ A \neq A \circ G$, $H \circ A \neq A \circ H$, $P \circ G = R_1$, and $Q \circ H = R_2$, where R_1 and $R_2 \neq R_1$ are arbitrary global right-side units, hold. Then one can select at random an integer $x < \omega$ and a global right-side unit R_3, such that $R_3 \neq R_2$ and $R_3 \neq R_1$, and compute the triple of the vectors Z, Y, and T satisfying the following equations:

$$Z = H \circ A \circ Q; \quad Y = G \circ A^x \circ P; \quad P \circ T \circ H = R_3. \qquad (14)$$

The triple (Z, Y, T) represents a public key connected with the private key representing the set of values x, G, A, and Q. The values P, H, and R_3 are also secret, however they are needed to the owner of the public key only in frame of the process of computing the values Z, Y, and T.

Finding the private key or some alternative four values x', G', A', and Q', with which the public key can be expressed in accordance with the formulas (14), represents a difficult computation problem. The last is called HDLP due to using the exponentiation operation performed in the finite cyclic group generated by the vector A, which is hidden in the FNAA. The used exponentiation operation contributes significantly to the difficulty of the considered variants of the HDLP.

4 Digital signature algorithms

In the case of using the HDLP introduced in Subsection 3.1 and the 4-dimensional FNAA described in Subsection 2.1 and defined over the field $GF(p)$ with 512-bit prime p one can propose the following signa-

ture generation algorithm in which some specified hash function F_h is used:

1. Generate a uniformly random value $k < \omega$ and compute the vector $V = G \circ B^k \circ H^{-1}$.

2. Compute the first signature element $e = F_h(M, V)$, where M is the electronic document to be signed.

3. While interpreting the bit string e as a binary number, compute the second signature element $s = k - xe \bmod \omega$.

The respective signature verification algorithm is performed as follows:

1. Using the signature (e, s) to the document M, compute the vector V': $V' = Y^e \circ T \circ Z^s$.

2. Compute the hash value $e' = F_h(M, V')$.

3. If $e' = e$, then the signature is accepted as genuine. Otherwise the signature is rejected.

Correctness proof of the proposed signature scheme is as follows:

$$V' = \left(G \circ B^x \circ G^{-1}\right)^e \circ T \circ \left(H \circ B \circ H^{-1}\right)^{(k-xe)} =$$
$$G \circ B^{xe} \circ G^{-1} \circ T \circ H \circ B^{k-xe} \circ H^{-1} = G \circ B^{xe} \circ E \circ B^{k-xe} \circ H^{-1} =$$
$$G \circ B^{xe+k-xe} \circ H^{-1} = G \circ B^k \circ H^{-1} = V \;\Rightarrow\; e' = e.$$

While using the HDLP, set in the 6-dimensional FNAA defined over the field $GF(p)$ with 384-bit characteristic p (see Subsection 3.2), the following algorithm can be proposed for generating a signature to document M:

1. Select at random an integer $k < \omega$ and compute the vector $V = G \circ A^k \circ Q$.

2. Compute the first signature element $v = F_h(V)$, where F_h is the used hash function.

3. Compute the hash function value e from the document M and the second signature element s: $e = F_h(M)$ and $s = ke - xv \bmod \omega$.

Verification of the signature (v, s) to the document M is to be performed with the following algorithm:

1. Compute the hash value e from the document $e = F_h(M)$.

2. Compute the vector $V' : V' = Y^{ve^{-1}} \circ T \circ Z^{se^{-1}}$.

3. Compute the hash value v' from the vector V': $v' = F_h(V')$.

4. If $v' = v$, then the signature is accepted as genuine. Otherwise the signature is rejected as false one.

Proof of the correctness of the last signature scheme is as follows:

$$V' = (G \circ A^x \circ P)^{ve^{-1}} \circ T \circ (H \circ A \circ Q)^{se^{-1}} =$$
$$G \circ A^{xve^{-1}} \circ P \circ T \circ H \circ A^{se^{-1}} \circ Q =$$
$$G \circ A^{xve^{-1}} \circ R_3 \circ A^{(ke-xv)e^{-1}} \circ Q =$$
$$G \circ A^{xve^{-1}+k-xve^{-1}} \circ Q = G \circ A^k \circ Q = V \Rightarrow v' = v.$$

Like in the Schnorr digital signature protocol [10] and in the discrete logarithm based standards [11], in the described signature schemes there is used some cyclic group of the prime order. However, in the proposed signature algorithms the used cyclic group is hidden in a FNAA. The public part of the introduced new signature algorithms is the used FNAA and three its elements Y, Z, and T that are connected with the hidden cyclic group generated by powers of the hidden-group generator (the vector B in the first signature scheme and the vector A in the second scheme) that is an element of the private key.

5 Conclusion

In this paper, two new FNAAs have been introduced as carries of the HDLP defined in two novel forms. One should note that the proposed two variants of the HDLP suit well to design digital signature schemes, however it is not evident, how they can be used for designing the public key agreement protocols. The known form of the HDLP [5] suits well to design the last type of protocols, however at present no proposals for signature schemes on its base are known. In the compared forms of the HDLP there are used different mechanisms for hiding a cyclic group.

Estimation of the security of the proposed signature algorithms to quantum attacks is connected with estimation of the computational difficulty of the reduction of the used HDLP to the discrete logarithm

problem in $GF(p)$. Consideration of this item represents an individual task. If the polynomial-time algorithms for such reduction will not be found for several years after publication of the proposed forms of the HDLP and signature schemes on their base, then one can hope the attractive candidates for post-quantum signature standards will be available. Significant advantage of the proposed signature schemes relatively the candidates selected in frame of the NIST PQCrypto project [3] is smaller signature size (384 to 512 bits in the case of 128-bit security) and higher performance of the signature generation and verification procedures.

Besides analysis of the resistance to quantum attacks, future development of the performed research can be also related to justification of the parameters of the FNAAs applied as carriers of the HDLP used as cryptographic primitive as well as to justification of the parameters of the HDLP.

References

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

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

[3] Federal Information Security Management Act (FISMA) of 2002. *Public Law 107347. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST PQCrypto project.* [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

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

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

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

[7] A. A. Moldovyan, N. A. Moldovyan, V. A. Shcherbacov, "Non-commutative finite rings with several mutually associative multiplication operations," in *Proceedings of The Fourth Conference of Mathematical Society of the Republic of Moldova dedicated to the centenary of Vladimir Andrunachievici (1917-1997), June 28 - July 2, 2017*, (Chisinau), 2017, pp. 133–136.

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

[9] A. A. Moldovyan, N. A. Moldovyan, V. A. Shcherbacov, "Non-commutative 6-dimensional associative algebras of two different types," in *Proceedings of the Workshop on Foundations of Informatics, July 2-6, 2018*, (Chisinau), 2018, pp. 154–163.

[10] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, pp. 161–174, 1991.

[11] *Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms*, International Standard ISO/IEC 14888-3:2006(E), 2006.

A. A. Moldovyan, N. A. Moldovyan,

Received September 5, 2018

St. Petersburg Institute for Informatics and Automation of
Russian Academy of Sciences
14 Liniya, 39, St.Petersburg, 199178
Russia
E–mail: nmold@mail.ru