BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(89), 2019, Pages 71–78
ISSN 1024–7696

Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on its Base

N. A. Moldovyan

Abstract. The paper considers finite non-commutative associative algebras every of which contains a large set of the global one-sided (right and left) units. Formulas describing all of the global units are derived for each of the algebras. Finite algebras of such type are introduced as carriers of the hidden discrete logarithm problem that is defined in three new forms. One of them is used to design the post-quantum cryptoscheme for public key-distribution. Two others are applied to design the post-quantum digital signature schemes.

Mathematics subject classification: 94A60, 16Z05, 14G50, 11T71, 16S50.
Keywords and phrases: Finite associative algebra, non-commutative algebra, right unit, set of global units, discrete logarithm problem, digital signature, post-quantum cryptography.

1 Introduction

Finite non-commutative groups and associative algebras represent significant practical interest as carriers of the hidden discrete logarithm problem (HDLP) that potentially can be used to design the post-quantum public-key cryptoschemes [1–3]. The known form of the HDLP definition is described by the formula

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

where $\circ$ is multiplication operation; w and x are integers; Y, Q, and G are elements of a finite non-commutative group or of a finite non-commutative associative algebra (FNAA) containing the global two-sided unit. Finding the integers w and x gives the known form of the HDLP.

Formula (1) was used to design the public key-distribution protocols and public encryption algorithms [2]. In the both cryptoschemes the public key Y is computed using formula (1), where the pair of integers (w, x) represents the private key. No digital signature scheme based on the HDLP is described in the literature.

The present paper introduces the 4-dimensional and 6-dimensional FNAAs containg sufficiently large set of the one-sided units and no global two-sided unit. The described FNAAs represent interest as carriers of the HDLP difined with formulas different from (1). Two of the proposed new forms of the HDLP are used in the introduced post-quantum digital signature schemes. Results of the paper contribute to the actual problem of designing public-key post-quantum cryptoschemes [4, 5].

2 Defining FNAA with the set of global one-sided units

Suppose an m-dimensional vector space is defined over the field $GF(p)$ and $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are some formal basis vectors. To denote a vector V one can use notations $V = (v_0, v_1, \ldots, v_{m-1})$ and $V = v_0\mathbf{e}_0 + v_1\mathbf{e}_1 + \cdots + v_{m-1}\mathbf{e}_{m-1}$, where $v_0, v_1, \ldots, v_{m-1} \in GF(p)$. A finite vector space becomes a finite algebra after the operation for multiplying two arbitrary vectors is defined as the second operation that is distributive relative to the addition operation. If non-commutative associative multiplication operation is defined, then we have an FNAA.

Usually the multiplication operation (denoted by $\circ$) of two vectors $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $B = \sum_{i=0}^{m-1} b_i\mathbf{e}_i$ in an m-dimensional FNAA is defined as follows:

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

where the products of different pairs of formal basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ are to be replaced by a one-component vector in accordance with one so called basis vector multiplication table (BVMT). We will assume that the left operand $\mathbf{e}_i$ defines the row and the right one $\mathbf{e}_j$ defines the column. The cell of the BVMT at the intersection of the ith row and jth column defines the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$.

Table 1 defines a 4-dimensional FNAA with the set of global right units. Formula describing all global right unites can be obtained from the following vector equation with the unknown vector $X = (x_0, x_1, x_2, x_3)$:

$$A \circ X = A. \tag{2}$$

The vector equation (2) defines the following system of four linear equations:

$$\begin{cases} a_0x_1 + a_0x_2 + a_2x_0 + a_2x_3 = a_0; \\ \mu a_3x_0 + a_1x_1 + a_1x_2 + \mu a_3x_3 = a_1; \\ \mu a_1x_1 + a_2x_1 + a_2x_2 + \mu a_0x_3 = a_2; \\ a_1x_0 + a_3x_1 + a_3x_2 + a_1x_3 = a_3. \end{cases} \tag{3}$$

The system (3) can be rewritten as two independent systems of two equations:

$$\begin{cases} (x_1 + x_2)\, a_0 + (x_0 + x_3)\, a_2 = a_0; \\ \mu\,(x_0 + x_3)\, a_0 + (x_1 + x_2)\, a_2 = a_2. \end{cases} \tag{4}$$

$$\begin{cases} (x_1 + x_2)\, a_1 + \mu\,(x_0 + x_3)\, a_3 = a_1; \\ (x_0 + x_3)\, a_1 + (x_1 + x_2)\, a_3 = a_3. \end{cases} \tag{5}$$

It is easy to see that each of the systems (4) and (5) has the same set of p^2 different solutions satisfying the following two conditions:

$$x_0 + x_3 = 0 \quad \text{and} \quad x_1 + x_2 = 1. \tag{6}$$

These solutions do not depend on the value A. The last means that every solution acts as a global right unit, i.e., we have the set of p^2 global right units described by the following formula (defined by (6)):

$$R = (x_0, x_1, 1 - x_1, -x_0), \tag{7}$$

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

Table 1. The BVMT setting the 4-dimensional FNAA containing the set of global right units

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

Consideration of the vector equation

$$X \circ A = A \tag{8}$$

gives the following formula for the single local left unit related to the vector A :

$$\begin{aligned} L_A = \Bigg(& \frac{a_0a_1 - a_2a_3}{\Delta}, \frac{a_1^2 + a_1a_2 - \mu a_3a_0 - \mu a_3^2}{\Delta}, \\ & \frac{a_2^2 + a_1a_2 - \mu a_0^2 - \mu a_0a_3}{\Delta}, \frac{a_2a_3 - a_0a_1}{\Delta} \Bigg), \end{aligned} \tag{9}$$

where $\Delta = (a_1 + a_2)^2 - \mu (a_0 + a_3)^2 \neq 0$. Thus, the single local left unit corresponds to any vector A coordinates of which satisfy condition $\Delta \neq 0$. Evidently, the formula (9) defines the vector L_A that is included in the set (7). The last means the local left unit of the vector A is simultaneously its local two-sided unit E_A. Besides, in the considered 4-dimensional FNAA there exist $\leq p^2$ different local two-sided units.

For fixed vector A and arbitrary integer $i \geq 1$ the local left unit L_A corresponds to every vector A^i, i.e., $L_{A^i} = L_A = E_A$. For some minimum integer ω we have $A^\omega = E_A$. The value ω can be called the local order of the vector A. All possible powers of the vector A compose a finite cyclic group contained in the considered 4-dimensional FNAA. Vectors for which a local two-sided unit exists can be called locally invertible.

The multiplication operation defined with Table 2 sets a 4-dimensional FNAA containing the set of global left units described by the following formula:

$$L = \left(x_0, \frac{1 - \tau x_0}{\mu}, x_2, -\frac{\mu x_2}{\tau} \right), \tag{10}$$

where $x_0, x_2 = 0, 1, \ldots p-1$. The single local right unit R_A relates to an arbitrary vector $A = (a_0, a_1, a_2, a_3)$ coordinates of which satisfy condition $\Delta = (\tau a_0 + \mu a_1)^2 - (\mu a_2 + \tau a_3)^2 \neq 0$. The value R_A is expressed by the formula

$$R_A = \left(\frac{\mu a_1 a_3 - \mu a_0 a_2}{\Delta}, \frac{\tau a_0 a_1 + \mu a_1^2 - \mu a_2^2 - \tau a_2 a_3}{\Delta}, \frac{\tau a_0 a_2 - \tau a_1 a_3}{\Delta}, \frac{\mu a_1 a_3 - \mu a_0 a_2}{\Delta} \right). \tag{11}$$

One can easily show the formula (11) defines the vector R_A that is included in the set (10), i.e., the local unit R_A is simultaneously the local two-sided unit E_A of the vector A. Any vector A satisfying the condition $\Delta \neq 0$ is a generator of a finite cyclic group contained in the FNAA.

Table 2. The BVMT setting the 4-dimensional FNAA containing the set of global left units.

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

The 6-dimensional FNAAs containing the set of global one-sided units also represent interest for application in the design of the public-key cryptoscheme based on the HDLP. Table 3 defines a non-commutative and associative multiplication operation and sets the FNAA with the set of global left units. The formula describing the last set can be derived considering the vector equation (8) written for the 6-dimensional vectors A and X. Taking into account Table 3 we get directly the following system of six linear equations:

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

All solutions of the last system can be found considering the following two independent systems of three linear equations:

$$\begin{cases} a_0 (\mu x_0 + \tau x_3) + a_2 (\tau x_1 + \mu x_4) + a_4 (\mu x_2 + \tau x_5) = a_0; \\ a_0 (\mu x_2 + \tau x_5) + a_2 (\mu x_0 + \tau x_3) + a_4 (\tau x_1 + \mu x_4) = a_2; \\ a_0 (\tau x_1 + \mu x_4) + a_2 (\mu x_2 + \tau x_5) + a_4 (\mu x_0 + \tau x_3) = a_4. \end{cases} \tag{12}$$

$$\begin{cases} a_1(\mu x_0 + \tau x_3) + a_3(\tau x_1 + \mu x_4) + a_5(\mu x_2 + \tau x_5) = a_1; \\ a_1(\mu x_2 + \tau x_5) + a_3(\mu x_0 + \tau x_3) + a_5(\tau x_1 + \mu x_4) = a_3; \\ a_1(\tau x_1 + \mu x_4) + a_3(\mu x_2 + \tau x_5) + a_5(\mu x_0 + \tau x_3) = a_5. \end{cases} \quad (13)$$

Independently of the value $A \neq (0,0,0,0,0,0)$ each of the systems (12) and (13) has the same solutions defined by the following three conditions:

$$\mu x_0 + \tau x_3 = 1; \quad \tau x_1 + \mu x_4 = 0; \quad \mu x_2 + \tau x_5 = 0.$$

The last conditions define the following formula describing the set of all p^3 different global left units

$$L = \left(x_0, x_1, x_2, \frac{1 - \mu x_0}{\tau}, -\frac{\tau x_1}{\mu}, -\frac{\mu x_2}{\tau} \right), \quad (14)$$

where $x_0, x_1, x_2 = 0, 1, \ldots p-1$. If the vector A is locally invertible, then the single local right unit R_A corresponds to A. The vector R_A is contained in the set (14) and it represents the local two-sided unit of the vector A. Only the vectors from the set (14) can act as local two-sided units. On the average about p^3 different vectors of the considered 6-dimensional FNAA correspond to a fixed value from (14) as to local two-sided unit.

Table 3. The BVMT setting the 6-dimensional FNAA containing p^3 different global left units.

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

It is sufficiently evident that every element of the considered FNAAs, which relates to a fixed local two-sided unit generates a finite multiplicative group and every locally invertible vector of the FNAA is included only in one such group.

3 New forms of the HDLP and public-key cryptoschemes based on them

Let us consider some locally invertible elements N and T of the 6-dimensional FNAA considered in the previous section, such that $T \circ N \neq N \circ T$. Suppose the local orders of the vectors N and T are equal to integers ω and τ correspondingly. Suppose also that the characteristic of the field $GF(p)$ is sufficiently large and the integers ω and τ have size 512 bits, besides the number ω is a prime. The following equation holds $N^\omega = E_N$, where E_N is the local two-sided unit relative to N. Then

the set of vectors $\left\{N, N^2, ..., N^{\omega-1}, E_N\right\}$ together with the operation $\circ$ compose a finite cyclic group of the order ω. For some left-sided unit from the set (14) one can easily compute the 6-dimensional vector U such that $T \circ U = L$. Using the vectors N, T, and U as known parameters one can construct the following public key-agreement scheme.

The first (second) user selects a pair of uniformly random integers w_1 and x_1 (w_2 and x_2) as his private key and then computes his public key as follows:

$$\begin{array}{l} Y_1 = U^{w_1} \circ N^{x_1} \circ T^{w_1} = (U^{w_1} \circ N \circ T^{w_1})^{x_1} \\ (Y_2 = (U^{w_2} \circ N \circ T^{w_2})^{x_2} = U^{w_2} \circ N^{x_2} \circ T^{w_2}) . \end{array} \tag{15}$$

The users exchange their public keys via a public channel. Then each of them can compute the common secret value Z using his private key. The first (second) user performs computations as follows:

$$\begin{array}{l} Z = U^{w_1} \circ Y_2^{x_1} \circ T^{w_1} = U^{w_1+w_2} \circ N^{x_1 x_2} \circ T^{w_1+w_2} \\ \left(Z = U^{w_2} \circ Y_1^{x_2} \circ T^{w_2} = U^{w_2+w_1} \circ N^{x_2 x_1} \circ T^{w_2+w_1}\right) . \end{array}$$

The proposed form of the HDLP described by equation (15) with unknown values w and x is suitable to be defined in FNAAs that contain the set of global one-sided units and no global two-sided unit which is needed for defining the HDLP of the known form (see equation (1)).

The second proposed new form of the HDLP relates to constructing the digital signature schemes and is also defined over FNAAs containing the set of global one-sided units, for example, the 4-dimensional FNAA with the multiplication operation set by Table 1, which contains the set of global right units $\{R_i : \ R_i \circ V = V\}$, where i is an integer and V is an arbitrary 4-dimensional vector. Like in the case of the considered public key-agreement scheme we assume that the vector space is defined over $GF(p)$, where prime p has a large size (for example, 768 bits).

Evidently, for arbitrary right unit R_i and arbitrary integer j $R_i^j = R_i$ holds. Suppose N is a vector having sufficiently large prime local order ω and vectors U, U', T, and D satisfy the following conditions $T \circ U = R_1$, $T \circ U' = R_2$, and $D \circ U' = R_3$, where R_1, R_2, and R_3 ($R_1 \neq R_2$; $R_1 \neq R_3$; $R_2 \neq R_3$) are some global right units. The signer's private key is a uniformly random integer $x < \omega$ and the set of the vectors N, U, and D. The public key represents the pair of the vectors Y and Q that are computed as follows:

$$Y = U \circ N^x \circ T = (U \circ N \circ T)^x ; \quad Q = U' \circ N \circ D. \tag{16}$$

The digital signature to some document M is computed as follows:

1. Select a random integer $k < \omega$ and compute the vector $K = U \circ N^k \circ D$.

2. Compute the first signature element $e = F_h(M, K)$, where F_h is a specified hash function.

3. Calculate the second signature element $s = k - xe \bmod \omega$, where the bit string e is interpreted as a binary number.

Procedure of the signature verification is executed as follows:

1. Using the signature (e, s) representing a pair of integers compute the vector $K^? = Y^e \circ Q^s$.

2. Compute the bit string $e^? = F_h(M, K^?)$.

3. If $e^? = e$, then the signature is accepted as a genuine. Otherwise the signature is rejected as false one.

The correctness proof of the proposed signature scheme is evident:

$$K^? = (U \circ N^x \circ T)^e \circ \left(U' \circ N \circ D\right)^{k-xe} = U \circ N^{xe} \circ T \circ U' \circ N^{k-xe} \circ D =$$
$$= U \circ N^{xe} \circ R_2 \circ N^{k-xe} \circ D = U \circ N^{xe+k-xe} \circ D = U \circ N^k \circ D = K \Rightarrow$$
$$\Rightarrow e^? = F_h(M, K^?) = F_h(M, K) = e.$$

The third proposed new form of the HDLP is also defined over FNAAs containing a set of global one-sided units and also relates to constructing the digital signature schemes. Let us use the 6-dimensional FNAA the multiplication operation in which is defined with Table 3. This algebra contains a set of global left units $\{L_i : \ L_i \circ V = V\}$, where V is an arbitrary 6-dimensional vector. The signer's private key is a random integer $x < \omega$ and the set of the vectors N, U, G, T, and D satisfy the following conditions $T \circ U = L_1$ and $D \circ G = L_2$, where L_1 and $L_2 \neq L_1$ are some global left units. The public key represents the triple of the vectors Y, H, and Q that are computed so that the follow equations hold:

$$Y = U \circ N^x \circ T = (U \circ N \circ T)^x ; \quad Q = G \circ N \circ D; \quad T \circ H \circ G = L_3, \tag{17}$$

where L_3 is a global left unit such that $L_3 \neq L_1$ and $L_3 \neq L_2$.

The digital signature (e, s) to a document M is computed as follows:

1. Select a random integer $k < \omega$ and compute the vector $K = U \circ N^k \circ D$.

2. Calculate the integers $e = F_h(M, K)$ and $s = k - xe \bmod \omega$.

Procedure of the signature verification is executed as follows:

1. Compute the vector $K^? = Y^e \circ H \circ Q^s$ and the bit string $e^? = F_h(M, K^?)$.

2. If $e^? = e$, then the signature is accepted. Otherwise it is rejected.

In the both proposed signature schemes the minimum signature size is 384 bits (128-bit value e and 256-bit value s) in the case of providing 128-bit security (2^{128} multiplications in the used FNAA). Like in the Schnorr digital signature algorithm [8], in two proposed signature schemes a finite cyclic group of the prime order there is used. The novelty consists in hiding this cyclic group in FNAAs. The public part of the proposed signature schemes is a fixed FNAA containing a set of global one-sided units and the vectors Y, H, and Q. The vectors Y and Q are connected with the hidden cyclic group generated by powers of the vector N that is an element of the private key.

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. The consideration of this item represents an individual task.

4 Conclusion

We have introduced the 4-dimensional and 6-dimentional FNAAs containing a large set of global one-sided units, which suit well to define the HDLP of new forms. New forms of the HDLP have been used in the proposed new post-quantum public-key cryptoschemes. For the first time the digital signature schemes based on the HDLP have been introduced. The proposed signature schemes are more practical than the post-quantum signature schemes selected in frame of the NIST PQCrypto project [6, 7] as candidates for future post-quantum signature standards.

Apparently, the FNAAs and the HDLP were undeservedly ignored by the developers of the public-key post-quantum cryptoschemes in the course of the NIST competition. However, the post-quantum cryptosystems proposed in this paper require a study of their resistance to quantum attacks by a wide cryptographic community, like it is envisaged for the selected candidates at the next three-year stage of the NIST PQCrypto project.

References

[1] 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, **223**, No. 5, 629–641.

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

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

[4] Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. *Lecture Notes in Computer Science series*. Springer, 2018. Vol. 10786.

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

[6] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST PQCrypto project. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

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

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

N. A. Moldovyan
St. Petersburg Institute for Informatics and Automation
of Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg
Russia
E-mail: *nmold@mail.ru*

Received September 05, 2018