MSC 94A60, 16Z05, 14G50, 11T71, 16S50 10.14529/mmp200205

COMMUTATIVE ENCRYPTION METHOD BASED ON HIDDEN LOGARITHM PROBLEM

D.N. Moldovyan[1]***, 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: mdn.spectr@mail.ru, nmold@mail.ru, maa1305@yandex.ru

A candidate for post-quantum commutative encryption algorithm is proposed, which is based on the hidden discrete logarithm problem defined in a new 6-dimensional finite non-commutative associative algebra. The properties of the algebra are investigated in detail and used in the design of the proposed commutative cipher. The formulas describing the set of p^2 different global right-sided units contained in the algebra and local left-sided units are derived. Homomorphisms of two different types are considered and used in the commutative cipher. The encrypted message is represented in the form of a locally invertible element T of the algebra and encryption procedure includes performing the exponentiation operation and homomorphism map followed by the left-sided multiplication by a randomly selected local right-sided unit. The introduced commutative cipher is secure to the known-plaintext attacks and has been used to develop the post-quantum no-key encryption protocol providing possibility to send securely a secret message via a public channel without using any pre-agreed key. The proposed commutative encryption algorithm is characterized in using the single-use keys that are selected at random directly during the encryption process.

Keywords: commutative encryption; probabilistic cipher; post-quantum cryptoscheme; no-key protocol; finite non-commutative algebra; associative algebra; global unit; right-sided unit.

Introduction

The public-key cryptographic algorithms and protocols which are based on the computational difficulty of the factoring problem (FP) and the discrete logarithm problem (DLP) are the most widely used cryptoschemes. However, they will not be secure in the coming era of quantum computations [1, 2], since both the FP and the DLP can be solved in polynomial time on a quantum computer [3]. Therefore, development of practical post-quantum public-key cryptoschemes is considered as one of challenges in the area of the applied and theoretic cryptography. However, the problem of the development of the post-quantum commutative encryption algorithms has practically remained outside the attention of researchers. This particular problem is connected with the fact that practical applications have commutative encryption algorithms possessing security to the known-plaintext attacks. The known ciphers satisfying the last demand are based on the computational difficulty of the DLP, therefore they do not provide security against quantum attacks. Development of the post-quantum versions of the commutative ciphers is also an open problem.

The first attempt to solve this problem relates to designing the commutative cipher on the base of the hidden discrete logarithm problem (HDLP) defined in a finite quaternion algebra [4] set over the finite ground field $GF(p)$. The recent paper [5] has shown: that form of the HDLP is polynomially reducible to the DLP in a finite field $GF(p^2)$.

The present paper introduces a new form of the HDLP that is applied to development of the post-quantum commutative encryption algorithms suitable for using them in frame of the no-key protocols. The used form of the HDLP is formulated in the concrete 6-dimensional finite non-commutative associative algebra (FNAA) containing a large set of the global righ-tsided units, which is used as algebraic support of the proposed post-quantum commutative-encryption algorithm. The introduced method is charecterized in ussing the exponentiation operation as the main encryption procedure and the masking homomorphism-map operations.

1. The Used 6-Dimensional Finite Algebra

The finite m-dimensional vector space with the additionally defined operation of multiplying arbitrary two vectors, which is distributive relatively the addition operation, represents the algebraic structure called the m-dimensional finite algebra. Suppose $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are the basis vectors. The vector A of a vector space defined over the finite field $GF(p)$ can be denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \cdots + a_{m-1}\mathbf{e}_{m-1}$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates. The multiplication operation (denoted as $\circ$) of two vectors A and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is usually defined as follows

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

where every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be substituted by a single-component vector $\lambda\mathbf{e}_\mathbf{k}$, where $\lambda \in GF(p)$ is called structural constant, indicated in the respective cell of so called basis vector multiplication table (BVMT). It is usually assumed that the intersection of the ith row and jth column defines the cell indicating the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$. In the developed commutative encryption method we use computations in the 6-dimensional FNAA, in which the vector multiplication is defined by BVMT shown as Table.

Table

The BVMT defining the FNAA with p^2 global right-sided units ($\lambda \neq 1$)

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

1.1. The Set of Global Right-Sided Units

The 6-dimensional FNAA defined by Table, where $\lambda \neq 1$, contains p^2 different global right-sided units R (global means that these units act on all elements of the algebra) which represent solutions of the vector equation $A \circ X = A$ that, using Table, can be represented in the form of the following system of six linear equations with coordinates of the right operand $x_0, x_1, x_2, x_3, x_4, x_5$ as the unknown values:

$$\begin{cases} a_0x_0 + a_1x_0 + a_0x_2 + \lambda a_1x_2 + a_0x_4 + a_1x_4 = a_0; \\ a_0x_1 + a_1x_1 + a_0x_3 + a_1x_3 + a_0x_5 + \lambda a_1x_5 = a_1; \\ a_2x_0 + a_5x_0 + a_2x_2 + \lambda a_5x_2 + a_2x_4 + a_5x_4 = a_2; \\ a_3x_1 + a_4x_1 + a_3x_3 + a_4x_3 + \lambda a_3x_5 + a_4x_5 = a_3; \\ a_3x_0 + a_4x_0 + \lambda a_3x_2 + a_4x_2 + a_3x_4 + a_4x_4 = a_4; \\ a_2x_1 + a_5x_1 + a_2x_3 + a_5x_3 + a_2x_5 + \lambda a_5x_5 = a_5. \end{cases} \tag{1}$$

Performong the variable substitution $u_1 = x_0+x_2+x_4$, $u_2 = x_0+\lambda x_2+x_4$, $u_3 = x_1+x_3+x_5$, and $u_4 = x_1 + x_3 + \lambda x_5$, one can show that for arbitrary vector A the system (1) holds true for the values $u_1 = 1$, $u_2 = 0$, $u_3 = 0$, and $u_4 = 1$. From the last conditions one can write the following formula describing p^2 global right-sided units $R = (r_0, r_1, r_2, r_3, r_4, r_5)$:

$$R = \left(h, k, \frac{1}{1-\lambda}, -k + \frac{1}{1-\lambda}, -h + \frac{\lambda}{\lambda-1}, \frac{1}{\lambda-1}\right), \tag{2}$$

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

1.2. Local Left-Sided Units

Computing the local left-sided unit for some fixed vector A is connected with finding solutions of the vector equation

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

Using Table 1 one can represent (3) in the form of the following three independent systems of two linear equations with the pairs of the unknowns (x_0, x_1), (x_2, x_5), and (x_3, x_4) :

$$\begin{cases} (a_0 + a_2 + a_4)\, x_0 + (a_0 + \lambda a_2 + a_4)\, x_1 = a_0; \\ (a_1 + a_3 + a_5)\, x_0 + (a_1 + a_3 + \lambda a_5)\, x_1 = a_1; \end{cases} \tag{4}$$

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

$$\begin{cases} (a_1 + a_3 + \lambda a_5)\, x_3 + (a_1 + a_3 + a_5)\, x_4 = a_3; \\ (a_0 + \lambda a_2 + a_4)\, x_3 + (a_0 + a_2 + a_4)\, x_4 = a_4. \end{cases} \tag{6}$$

The same main determinant Δ_A corresponds to each of the systems (4) – (6):

$$\Delta_A = (a_0a_5 + a_4a_5 - a_1a_2 - a_2a_3)\,(\lambda - 1)\,. \tag{7}$$

If $\Delta_A \neq 0$, then every of the systems (4) – (6) has unique solution, i. e., the vector equation (5) also has unique solution as the single left-sided unit L_A related to the vector A. Solving the systems (4) – (6) one gets the following formulas describing the vector $L_A = (l_0, l_1, l_2, l_3, l_4, l_5)$:

$$\begin{aligned} l_0 &= \frac{a_0a_3 - a_1a_4 + \lambda\,(a_0a_5 - a_1a_2)}{\Delta_A};\ l_1 = \frac{a_1a_2 + a_1a_4 - a_0a_3 - a_0a_5}{\Delta_A}; \\ l_2 &= \frac{1}{1-\lambda}; \qquad l_3 = \frac{a_0a_3 + a_2a_3 - a_1a_4 - a_1a_5}{\Delta_A}; \\ l_4 &= \frac{a_1a_4 + \lambda a_4a_5 - a_0a_3 - \lambda a_2a_3}{\Delta_A};\ l_5 = \frac{1}{\lambda-1}. \end{aligned} \tag{8}$$

Proposition 1. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the local left-sided unit L_A relating to A is contained in the set of the global right-sided units, i. e., there exist the single local two-sided unit E_A relating to the vector A, which is equal to L_A.*

Proof. Let us consider the formulas (2) and (8). We have $r_2 = l_2 = (1-\lambda)^{-1}$ and $r_5 = l_5 = (\lambda-1)^{-1}$. Substituting the values $h = l_0 = \Delta_A^{-1}(a_0a_3 - a_1a_4 + \lambda(a_0a_5 - a_1a_2))$ and $k = l_1 = \Delta_A^{-1}(a_1a_2 + a_1a_4 - a_0a_3 - a_0a_5)$ in (2) we get $r_3 = l_3$ and $r_4 = l_4$.

□

Proposition 2. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the local left-sided unit L_A relating to A relates also to the vector A^i for arbitrary natural value i.*

Proof. $\{L_A \circ A = A \circ L_A = A\} \Rightarrow$
$\{L_A \circ A^i = L_A \circ A \circ A^{i-1} = A^i;\ A^i \circ L_A = A^{i-1} \circ A \circ L_A = A^i\}$.

□

Proposition 3. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the sequence $A, A^2, \ldots, A^i, \ldots$ is periodic and for some positive integer ω we have $A^\omega = L_A$.*

Proof. Suppose the sequence $A, A^2, \ldots, A^i, \ldots$ contains the zero vector $O = (0,0,0,0,0,0)$. Then for some natural number j (for example, $j = 2$) we have $A^{j-1} \neq O$ and $A^j = O$, i. e., $A^{j-1} \circ A = O$. Since $\Delta_A \neq 0$ and $X = O$ the equation $X \circ A = O$ has unique solution that is the following one: $X = O$. Therefore, $A^{j-1} = O$. The obtained contradiction proves that all values in the considered sequence are different from O. The last fact and the finiteness of the considered algebra shows that for some minimum natural number t the value A^t is equal to one of the previous values $A, A^2, \ldots, A^{t-1}$, namely, to the value A. If we suppose $A^t = A^h$, where $1 < h < t$, then we have $A \circ A^{t-1} = A \circ A^{h-1} \Rightarrow \left(A^{t-1} - A^{h-1}\right) \circ A = O$. Since $\Delta_A \neq 0$, we have $A^{t-1} - A^{h-1} = O \Rightarrow A^{t-1} = A^{h-1}$. The last equality contradicts to the fact that the value t is the first number for which we have a repetition. Thus, we have $A^t = A^{t-1} \circ A = A$ and $A^\omega = L_A$, where $\omega = t - 1$.

□

The Proposition 3 shows that every vector A such that $\Delta_A \neq 0$ generates a finite cyclic group with the unit element equal to the local left-sided unit of the vector A. The vector A is invertible relatively the unit L_A and can be called locally invertible element of the algebra. The value ω can be called local order of the vector A. Respectively, the vectors A such that $\Delta_A \neq 0$ can be called locally invertible vectors [8].

Proposition 4. *The number of the locally invertible vectors in the considered 6-dimensional FNAA is equal to $\Omega = p^3(p-1)(p^2-1)$.*

Proof. The number of the locally invertible vectors is equal to the number of all elements of the algebra (p^6) minus the number on non-invertible vectors A for which we have $\Delta_A = 0$. Let us compute the number of the vectors A for which we have $\Delta_A = 0$. From (7) we have $a_0a_5 = (a_1 + a_3)a_2 - a_4a_5$. In the case $a_5 \neq 0$ we have $p^4(p-1)$ non-invertible vectors satisfying the last equation. One can easily computed that in the case $a_5 = 0$ the number of the non-invertible vectors is equal to $p^2(2p^2 - p)$. Totally, we have $n = p^4(p-1) + p^2(2p^2 - p) = p^5 + p^4 - p^3$ non-invertible vectors and $\Omega = p^6 - n = p^3(p-1)(p^2-1)$ locally invertible ones.

□

Proposition 5. *The set of the locally invertible vectors relating to the same fixed local left-sided unit L represent a finite group.*

Proof. The value L is the group unit. The vector multiplication operation is associative. For every of the considered locally invertible vectors V there exists natural number ω such that $V^{\omega} = L$. The inverses of the vector V is the vector $V^{\omega-1}$ for which we have $V \circ V^{\omega-1} = V^{\omega-1} \circ V$.

□

1.3. Structure of the Considered FNAA

Finding the solutions of the vector equation $A \circ D = O$, where $O = (0,0,0,0,0,0)$, one can easily show that the considered FNAA contains p^2 different global right-sided zero divisors D which are described with the formula

$$D = (d_0, d_1, d_2, d_3, d_4, d_5) = (h, k, 0, -k, -h, 0)\,, \tag{9}$$

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

An arbitrary fixed global right-sided unit R sets a homomorphism map of the considered FNAA, which can be called the homomorphism of the φ_R-type.

Proposition 6. *Suppose the vector R is a global right-sided unit. Then the map of the FNAA defined by the formula $\varphi_R(X) = R \circ X$, where the vector X takes on all values in the algebra, is a homomorphism.*

Proof. For two arbitrary vectors X_1 and X_2 one can get the following:

$$\varphi_R(X_1 \circ X_2) = R \circ (X_1 \circ X_2) = (R \circ X_1) \circ (R \circ X_2) = \varphi_R(X_1) \circ \varphi_R(X_2)\,;$$
$$\varphi_R(X_1 + X_2) = R \circ (X_1 + X_2) = R \circ X_1 + R \circ X_2 = \varphi_R(X_1) + \varphi_R(X_2)\,.$$

□

Proposition 7. *The homomorphism-map operation $\varphi_R(X) = R \circ X$, where R is a global right-sided unit, and the exponentiation operation X^i are mutually commutative, i. e., the equality $R \circ X^i = (R \circ X)^i$ holds true.*

Proof. Due to Proposition 6: $\varphi_R(X^i) = (\varphi_R(X))^i$, i. e., $R \circ X^i = (R \circ X)^i$.

□

Proposition 8. *Suppose for some fixed global right-sided unit R we have $\varphi_R(X) = R \circ X = U$. Then $L_U = R$, i. e. the function $\varphi_R(X)$ takes on the values the local left-sided unit of which is equal to R.*

Proof. For an arbitrary value X we have $R \circ U = R \circ R \circ X = R \circ X = U$.

□

Proposition 9. *Suppose for some fixed vector X and the global right-sided unit R we have $\varphi_R(X) = R \circ X = U$. Then for all p^2 vectors of the form $V_U = R' \circ U$, where R' takes on all values from the set (2), the equality $\varphi_R(V_U) = R \circ V_U = U$ holds true.*

Proof. $\varphi_R(V_U) = R \circ R' \circ U = R \circ U = U$.

□

Proposition 10. *Suppose for some fixed vector X global right-sided unit R we have $\varphi_R(X) = R \circ X = U$, where U is such that $\Delta_U \neq 0$. Then the vector X can be represented in the form $X = R' \circ U$, where R' is a global right-sided unit.*

Proof. An arbitrary global right-sided zero divisor D can be represented in the form $D = D' \circ U$, where D' is also a global right-sided zero divisor. Indeed, the equation $X \circ U = D$

has unique solution $X = D'$, since $\Delta_U \neq 0$. Evidently, for an arbitrary vector V such that $\Delta_V \neq 0$ we have the following: $V \circ (D' \circ U) = (V \circ D') \circ U = O$. Since $\Delta_U \neq 0$, from the last equality we have $V \circ D' = O$, hence D' is a global right-sided zero divisor. One can write: $\{R \circ X = U;\ R \circ U = U\} \Rightarrow R \circ (X - U) = O \Rightarrow (X - U) = D \Rightarrow X = U + D$, where D is a global right-sided zero divisor. The last equality can be represented in the form $X = R \circ U + D' \circ U = (R + D') \circ U = R' \circ U$, where R' is a global right-sided unit. □

The Propositions 9 and 10 show that exactly p^2 different vectors of the considered 6-dimensional FNAA are mapped into the fixed value U.

Proposition 11. *If the vector G satisfying the condition $\Delta_G \neq 0$ is not a global right-sided unit, then for an arbitrary natural number k such that $G^k \neq G$ the non-equality $\varphi_R(G^k) \neq \varphi_R(G)$ holds true.*

Proof. The map $\varphi_R(X)$ is a homomorphism, therefore $\varphi_R(G^k - G) = \varphi_R(G^k) - \varphi_R(G)$. Suppose $\varphi_R(G^k) = \varphi_R(G)$. Then $\varphi_R(G^k - G) = O \Rightarrow G^k - G = D$, where D is a global right-sided zero-divisor. Therefore $\big(G \circ G^k - G\big) = O \Rightarrow \big(G^k - G\big) \circ G = O$. Since $\Delta_G \neq 0$, from the last equation we have $G^k - G = O \Rightarrow G^k = G$. The obtained contradiction proves the Proposition 11. □

Proposition 12. *If the vector equation $V \circ X = Z$ has solution $X = S$, then p^2 different values $X_i = R_i \circ S$, where R_i takes on all values from the set (2), also are solutions of the given equation.*

Proof. $V \circ (R_i \circ S) = (V \circ R_i) \circ S = V \circ S = Z$. □

Evidently, for every global right-sided unit R' we have $\varphi_R(R') = R$ and for every global right-sided zero divisor D we have $\varphi_R(D) = O$. From the Proposition 11 it is easy to see that some fixed cyclic group contained in the algebra is maped with the function $\varphi_R(X)$ into another cyclic group of the same order. The finite group Γ contained in the considered algebra as subset of the algbra elements the local left-sided unit of which is equal to a fixed global right-sided unit R_f (the group unit) is maped with the function $\varphi_R(X)$ into the finite group having the same order Ω' and unit equal to the vector $R \circ R_f = R$. Selecting different values R_f one can fix p^2 different groups having order Ω'.

Every locally invertible element of the algebra is contained only in one of these groups, therefore we have $\Omega = \Omega' p^2$ and the following formula for computing the value Ω' (see the Proposition 4): $\Omega' = p^{-2}\Omega = p\,(p-1)\,(p^2-1)$.

1.4. Homomorphism of the ψ_R Type

Suppose the vector B is such that $\Delta_B \neq 0$. Then one can select a random global right-sided unit R and compute the single vector A that satisfies the condition

$$A \circ B = R.$$

Solving the last equation relatively the unknown A gives the value A having local order ω that is equal to the local order of the vector B and satisfying the condition $A^\omega = R$.

Proposition 13. *Suppose $A \circ B = R$. Then for arbitrary natural number t the equality $A^t \circ B^t = R$ holds true.*

Proof. $A^t \circ B^t = A^{t-1} \circ (A \circ B) \circ B^{t-1} = A^{t-1} \circ B^{t-1} = \cdots = A \circ B = R$. □

Proposition 14. *Suppose $A \circ B = R$. Then the formula $\psi_R = B \circ X \circ A$, where the vector X takes on all values in the considered 6-dimensional FNAA, sets the homomorphism map, called the ψ_R-type homomorphism.*

Proof. For two arbitrary 6-dimensional vectors X_1 and X_2 one can get the following:

$$\psi_R(X_1 \circ X_2) = B \circ (X_1 \circ X_2) \circ A = B \circ (X_1 \circ R \circ X_2) \circ A = \\ = (B \circ X_1 \circ A) \circ (B \circ X_2 \circ A^t) = \psi_R(X_1) \circ \psi_R(X_2); \\ \psi_R(X_1 + X_2) = B \circ (X_1 + X_2) \circ A = (B \circ X_1 \circ A) + (B \circ X_2 \circ A) = \\ = \psi_R(X_1) + \psi_R(X_2).$$

□

Proposition 15. *The ψ_R-type homomorphism-map operation the $\psi_R(X) = B \circ X \circ A$ and the exponentiation operation X^k are mutually commutative, i. e., the equality $B \circ X^k \circ A = (B \circ X \circ A)^k$ holds true.*

Proof. $\psi_R(X^k) = (\psi_R(X))^k \Rightarrow B \circ X^k \circ A = (B \circ X \circ A)^k$.

□

Proposition 16. *Suppose V is an arbitrary fixed value. Then every one of the elements $V + D$, where D takes on all values from the set (9), is mapped with the function ψ_R into the value $\psi_R(V)$.*

Proof. We have $\psi_R(V + D) = \psi_R(V) + \psi_R(D) = \psi_R(V) + O = \psi_R(V)$.

□

Proposition 17. *Suppose V is an arbitrary fixed locally invertible element order of which is equal to ω. Then the local left-sided unit relating to the value $V + D$, where D takes on all values from the set (9), is equal to the value $L_{V+D} = L_V + D \circ V^{\omega-1}$, where L_V is the local left-sided unit related to the vector V.*

Proof. Taking into account that the local left-sided unit L_V is simultaneously one of the global right-sided units, we have $(L_V + D \circ V^{\omega-1}) \circ (V + D) = L_V \circ V + D \circ V^{\omega} = V + D \circ L_V = V + D$.

□

Proposition 18. *Suppose V is an arbitrary fixed locally invertible element order of which is equal to ω. Then the order of every of the values $V + D$, where D takes on all values from the set (9), is equal to ω.*

Proof. $(V + D)^{\omega} = (V + D)^{\omega-1} \circ (V + D) = (V + D)^{\omega-1} \circ V = (V + D)^{\omega-2} \circ V^2 = (V + D) \circ V^{\omega-1} = V^{\omega} + D \circ V^{\omega-1} = L_V + D \circ V^{\omega-1} = L_{V+D}$ (see the Proposition 17).

□

Proposition 19. *Suppose S is a solution of the equation $A \circ X = Z$, where A is an arbitrary fixed locally invertible vector, i. e., $\Delta_A \neq 0$. Then the vector $S' = S + D$, where D is an arbitrary global right-sided zero divisor from the set (9), is also a solution.*

Proof. We have $A \circ (S + D) = A \circ S + A \circ D = A \circ S + O = A \circ S = Z$.

□

Proposition 20. *Suppose S_1 and S_2 are two different solutions of the equation $A \circ X = Z$, where A is such that $\Delta_A \neq 0$. Then $S_2 = S_1 + D'$, where D' is a global right-sided zero divisor from the set (9), i. e., the formula $S = S_1 + D$, where D takes on all values from the set (9), describes all p^2 solutions of the given equation.*

Proof. We have $A \circ S_2 - A \circ S_1 = O \Rightarrow A \circ (S_2 - S_1) = O \Rightarrow S_2 - S_1 = D \Rightarrow S_2 = S_1 + D$, where D is an element from the set (9). Due to the Proposition 19 the value $S = S_1 + D'$ is also a solution of the given equation for arbitrary value D' from the set (9), therefore we have exactly p^2 different solutions.

□

Proposition 21. *Suppose V is a locally invertible element of the considered algebra. Then an arbitrary global left-sided zero divisor D can be represented in the form $D = D' \circ V$, where D' is also a global left-sided zero divisor.*

Proof. The equation $X \circ V = D$ has unique solution $X = D'$, since $\Delta_V \neq 0$. Evidently, for an arbitrary vector A we have the following: $A \circ (D' \circ V) = (A \circ D') \circ V = O$. Since $\Delta_V \neq 0$, we have $A \circ D' = O$, hence D' is a global right-sided zero divisor.

□

Proposition 22. *Suppose the finite group Γ has order equal to Ω' and includes the locally invertible algebra elements $\{V_1, V_2, \ldots, V_i, \ldots V_{\Omega'}\}$ one of which is the group unit E. Then for the homomorphism map $\psi_R(X) = B \circ X \circ A$, where $A \circ B = R$, the non-equality $\psi_R(V_i) \neq \psi_R(V_j)$ holds true for the arbitrary two group elements V_i and $V_j \neq V_i$.*

Proof. Suppose $\psi_R(V_i) = \psi_R(V_j)$. Then we have $B \circ V_i \circ A - B \circ V_j \circ A = O \Rightarrow (B \circ V_i - B \circ V_j) \circ A = O \Rightarrow B \circ (V_i - V_j) = O \Rightarrow V_i - V_j = D$. Due to the Proposition 21 the last equality can be represented in the form $V_i = E \circ V_j + D' \circ V_j = (E + D') \circ V_j = R' \circ V_j$, where $R' = E + D'$ is a global right-sided unit. Since $V_i = R' \circ V_j$, we have $L_{V_i} = L_{R' \circ V_j} = R'$. Since $V_i \in \Gamma$, $L_{V_i} = E$. Thus, we have $R' = E \Rightarrow E + D' = E \Rightarrow D' = O \Rightarrow V_i = V_j$. The obtained contradiction proves the Proposition 22.

□

Proposition 23. *Suppose the set of the algebra elements $\{V_1, V_2, \ldots, V_i, \ldots V_{\Omega'}\}$ is a finite group with the group unit E, which has order equal to Ω'. Then all p^2 different groups contained in the considered algebra can be represented as the following p^2 sets of the algebra elements $\{R \circ V_1, R \circ V_2, \ldots, R \circ V_i, \ldots R \circ V_{\Omega'}\}$, where R takes on all values from the set (2) describing all right-sided units contained in the algebra.*

Proof. The inverses of every fixed value $R \circ V_i$ is the value $R \circ V_j$, where V_j is such that $V_i \circ V_j = E$. Indeed, $(R \circ V_i)(R \circ V_j) = R \circ (V_i \circ V_j) = R \circ E = R$, where R is the group unit of the set connected with the fixed value R. Every locally invertible element of the algebra is included only in one of the considered sets of the algebra elements, namely, in the group with the group unit $E = L_A$

□

Proposition 24. *Suppose the set of the algebra elements $\{V_1, V_2, \ldots, V_i, \ldots V_{\Omega'}\}$ is a finite group with the group unit E and the pairs of the values (A_k, B_k), where $k = 1, 2, \ldots, p^2$ are such that the vectors $R_k = A_k \circ B_k$ take on all values from the set (2) of the global right-sided units. Then the following p^2 sets $\{\psi_{R_k}(V_1), \psi_{R_k}(V_2), \ldots, \psi_{R_k}(V_{\Omega'})\}$ describe all p^2 different finite groups of the order Ω' contained in the considered 6-dimensional FNAA.*

Proof. For $k = 1, 2, \ldots, p^2$ we have p^2 different local two-sided unit elements $E_k = \psi_{R_k}(E) = B_k \circ E \circ A_k = R_k \circ E = R_k$.

□

From the Proposition 22 it is easy to see that every of p^2 finite groups of the order Ω' contained in the in the considered 6-dimensional FNAA is mapped with the function $\psi_R(X) = B \circ X \circ A$ into the single finite group with the unit equal to the value $R = A \circ B$.

For the fixed values A, B, and R selecting different non-negative integer values t one can define different homomorphism maps of the set of locally invertible algebra elements into the fixed finite group Γ, which can be described with the formula $\psi_R(X) = B^t \circ X \circ A^t$.

2. Forms of the HDLP

The DLP is defined in a finite cyclic group Γ as follows: $Y' = G^x$, where G is a generator of the group and the value x is unknown natural number. Finding the value x, when the values G and Y' are known, is called DLP. The HDLP is defined so that one of the values G and Y' or both of them are hidden (masked), namely, instead of the values G and Y' there are given some other values Z and Y correspondinly.

Thus, it is supposed the cyclic group Γ is a subset of elemets of some algebraic structure called carrier of the HDLP. The FNAAs suite well for defining different versions of the HDLP. The exponentiation operation G^x is the base operation in the HDLP. The operation used to mask the values G and Y' are called the masking operations. To provide possibility to design a public-key cryptoscheme on the base of HDLP one should use the masking operations that are mutually commutative with the base exponentiation operation. Therefore, the automorphism-map operations and the homomorphism-map operations are attractive to be applied as masking operations. A particular form of the HDLP is defined by the concrete set of the used masking operation.

The FNAAs are of significant interest as algebraic carriers of the HDLP and the cryptoschemes on its base. Different types of the FNAAs are used to define different forms of the HDLP. For the first time the HDLP was defined in the finite algebra of quaternions [4, 6] as follows:

$$Y = Q^w \circ G^x \circ Q^{-w} = \alpha\left(G^x\right), \tag{10}$$

where $Q \circ G \neq G \circ Q$; $\alpha(V)$ is the automorphism-map operation (V takes on all values in the quaternion algebra). The form of HDLP descibed by the formula (10) was applied to design a public key-agreement scheme and commutative encryption algorithm [4, 6]. However, reducibility of the first form of the HDLP to the DLP in the finite field $GF(p^2)$ was shown in the paper [5].

Recently [7,8] several new FNAAs and new versions of the HDLP were introduced and used to develop the post-quantum digital signature protocols. For example, in the digital signature scheme defined in the FNAA containing global two-sided unit the public key represents the triple of vectors (Y, Z, W) defined as follows [7]:

$$Y = Q \circ G^x \circ Q^{-1}, \quad Z = H \circ G \circ H^{-1}; \quad W = Q \circ E \circ H^{-1}, \tag{11}$$

where $Q \circ G \neq G \circ Q$; $H \circ G \neq G \circ H$; E is a randomly selected vector from the set of local units related to the non-invertible vector G. The HDLP defined with formula (11) consists in finding the value x in the case, when only the public key is known.

In the signature scheme defined in the FNAA containing a large set of global left-sided units the public key represents the pair of vectors (Y, Z) defined as follows [8]:

$$Y = H \circ G^x \circ D, \quad Z = J \circ G \circ W, \tag{12}$$

where $D \circ G \neq G \circ D$; $D \circ H = L_1$; $D \circ J = L_2$; $W \circ J = L_3$; L_1, L_2, and L_3 are global left-sided units. The HDLP defined with formula (12) consists in finding the value x in the case, when only the values Y and Z are known. In each of the last two versions of the HDLP no element of the base finite cyclic group is known, therefore the method [5] for reducing the HDLP to the DLP in a finite field do not work.

3. Commutative Encryption

Encryption algorithm F is called commutative, if for arbitrary two keys K_1 and $K_2 \neq K_1$ the following condition holds true:

$$F_{K_1}[F_{K_2}(T)] = F_{K_2}[F_{K_1}(T)], \tag{13}$$

where T is an encrypted message. Commutative encryption algorithms resisting the known-plaintext attacks are used as the base primitive of the Shamir's three-pass protocol [9]) for no-key encryption, described as follows. To send the secret message T to Bob, using a public channel and no pre-agreed key, Alice can use the following protocol:

1. Alice encrypts the message T using a random key K_1 and the commutative encryption function F: $C_1 = F_{K_1}(T)$. Then she sends the ciphertext C_1 to Bob.

2. Using a random key K_2 Bob encrypts the ciphertext C_1: $C_2 = F_{K_2}(C_1)$. Then he sends the ciphertext C_2 to Alice.

3. Using the decryption function $F_{K_1}^{-1}$ Alice decrypts the ciphertext C_2: $C_3 = F_{K_1}^{-1}(C_2)$ and sends the ciphertext C_3 to Bob.

After receiving the ciphertext C_3 Bob recovers the message $T = F_{K_2}^{-1}(C_3)$.

If the commutative cipher F is secure to the know-plaintext attack, then the described protocol provides security. However, the protocol do not provide authenticity and this fact is to be taken into account at practical applications of the protocol. The exponentiation cipher proposed by Pohlig and Hellman in [10] suits well for implementing the no-key encryption protocol. That commutative cipher uses the exponentiation operation modulo a large prime p, for example, having the size equal to 2048 bits and the structure described by the formula $p = 2q + 1$, where q is a large prime.

The encryption/decryption key (e, d) is generated as follows: 1) select at random a natural number e which has the size equal to 256 (or more) bits and is mutually prime with $(p-1)$; 2) compute the value $d = e^{-1} \bmod p - 1$. The encryption and decryption procedures are described by the formulas $C = T^e \bmod p$ and $T = C^d \bmod p$. Security of the Pohlig–Hellman cipher is defined by the computational difficulty of the DLP modulo p.

In the present paper we use the notion of the commutativity of the encryption function in the extended sense. We call the cipher commutative, if the consecutive encryption of the source message on two different keys produces the ciphertext which can be correctly decrypted using the keys in arbitrary order. The proposed definition of the commutativity also provides possibility to implement the no-key encryption protocols on the base of such commutative ciphers.

The introduced interpretation of the notion of the commutative encryption covers the deterministic commutative ciphers defined by the formula (13). The proposed extended interpretation of the notion of commutativity covers both the deterministic commutative ciphers and the probabilistic commutative ciphers.

4. Probabilistic Commutative Ecryption Algorithm

Suppose the FNAA described in Section 2 is defined over the field $GF(p)$, where $p = 2q + 1$ and q is a 256-bit prime, and the encrypted message is represented in the form of the 6-dimensional vector $T = (t_0, t_1, \ldots, t_5)$ which satisfies the condition $\Delta_T \neq 0$. The local two-sided unit E_T relating to the vector T can be computed as the local left-sided unit L_T from the formulas (8), since $E_T = L_T$.

The vector T is contained in one of p^2 finite groups of the order Ω' that are contained in the considered 6-dimensional FNAA. The order of the vector T is equal to a divisor of the integer $p\,(p^2-1)$. Therefore, the alternative method for finding the value E_T is performing computations defined by the following formula:

$$E_T = T^{p\left(p^2-1\right)}. \tag{14}$$

Evidently, computing the value E_T from the formulas (8) has significantly lower computational complexity than from the formula (14). The message T can be encrypted and then correctly decrypted with using the following two formulas:

$$C = T^e; \quad T = C^d, \tag{15}$$

where e and d are values satisfying the condition $ed \equiv 1 \bmod p\,(p^2-1)$.

Security of the commutative cipher defined by the formulas (15) is based on the computational difficulty of the DLP. To develop a post-quantum commutative cipher one can additionally use the masking homomorphism-map operations, for example, the φ operation.

The following probabilistic commutative cipher uses the ciphering key (e, d) and the single-use key representing a randomly selected global right-sided unit R and includes the following steps:

1. Using the formulas (8) compute the local two-sided unit E_T relating to the message T.

2. Using the formulas (2) compute a random global right-sided unit R and compute the value $C = R \circ T^e$.

3. Output the ciphertext representing the pair of two vectors (E_T, C).

This encryption algorithm defines a probabilistic encryption process due to using a randomly selected single-use key R. The ciphertext is two times large in size than the source message T. The value C is a part of the ciphertext that depends on the random value R. The decryption procedure is defined by the following formula:

$$T = E_T \circ C^d.$$

Correctness proof of this probabilistic cipher is as follows:

$$E_T \circ C^d = E_T \circ (R \circ T^e)^d = E_T \circ R \circ T^{ed} = E_T \circ T = T.$$

A feature of the described probabilistic cipher relates to the fact that the first part of the ciphertext is independent on the encryption key. Therefore, one should define the process of encrypting the message on two different keys. Evidently, the first part E_T of the ciphertext should be computed in frame of the first encrypton and in frame of the second encryption only the second part C of the ciphertext is to be encrypted.

Thus, the encryption on the key (e_A, d_A) and then on the key (e_B, d_B) produces the ciphertext

$$C_{AB} = (E_T, R_B \circ T^{e_A e_B}),$$

where R_B is the single-use subkey selected at random at the second encryption. The encryption on the key (e_B, d_B) and then on the key (e_A, d_A) produces the ciphertext

$$C_{BA} = (E_T, R_A \circ T^{e_B e_A}),$$

where R_A is the single-use subkey at the second encryption. Due to using the single-use key selected at random in the considered two cases the output ciphertexts have different values. Nevertheless, both the ciphertext C_{AB} and the ciphertext C_{BA} are decrypted correcly using the keys (e_A, d_A) and (e_B, d_B) in arbitrary order, i. e. the described probabilistic cipher is commutative.

5. Post-Quantum Commutative Cipher

To implement encryption of the message T using both the ψ-map operation and the φ-map operation one should specify two vectors A and B such that $A \circ B = R_0$, where R_0 is some fixed global right-sided unit, as common parameters of the encryption function. Besides, the additional subkey representing a natural number $t < p^2 - 1$ is to be used in the encryption process, i. e., the encryption key represents the triple of non-negative integers (e, d, t). The proposed post-quantum commutative cipher is describe as follows:

1. Using the formulas (8) compute the local two-sided unit E_T relating to the encrypted message T.

2. Using the formula (2) compute a random global right-sided unit R as the value of the single-use key and compute the ciphertxt $C = R \circ B^t \circ T^e \circ A^t$.

3. Output the ciphertext in the form of the pair of two vectors (E_T, C).

This encryption procedure is probabilistic. The decryption procedure is described by the following formula:

$$T = E_T \circ A^t \circ C^d \circ B^t.$$

Correctness proof of the decryption process is as follows:

$$E_T \circ A^t \circ C^d \circ B^t = E_T \circ A^t \circ \left(R \circ B^t \circ T^{ed} \circ A^t\right) \circ B^t =$$
$$= E_T \circ R_0 \circ T \circ R_0 = E_T \circ T = T.$$

Encrypting the message T on the key (e_A, d_A, t_A) and then on the key (e_B, d_B, t_B) outputs the ciphertext

$$C_{AB} = \left(E_T, R_B \circ B^{t_B + t_A} \circ T^{e_A e_B} \circ A^{t_A + t_B}\right),$$

where R_B is the single-use key used at the second encryption. Encrypting the message T on the key (e_B, d_B, t_B) and then on the key (e_A, d_A, t_A) produces the ciphertext

$$C_{BA} = \left(E_T, R_A \circ B^{t_A + t_B} \circ T^{e_B e_A} \circ A^{t_B + t_A}\right),$$

where R_A is the single-use key used at the second encryption. One can easily show that each of the ciphertexts C_{AB} and C_{BA} can be decrypted correctly using the keys (e_A, d_A, t_A) and (e_B, d_B, t_B) in different order and, therefore, the proposed post-quantum encryption algorithm is commutative. It can be used as the base encryption function in the following post-quantum no-key protocol:

1. Alice selects her local key (e_A, d_A, t_A), generates at random the single-use subkey R_A, computes the two-sided local unit relating to the vector T, and encrypts the message T :

$$C_1 = R_A \circ B^{t_A} \circ T^{e_A} \circ A^{t_A}.$$

Then she sends the ciphertext (E_T, C_1) to Bob.

2. Bob selects his local key (e_B, d_B, t_B), generates at random the single-use subkey R_B, and encrypts the vector C_1 :

$$C_2 = R_B \circ B^{t_B} \circ C_1^{e_B} \circ A^{t_B}.$$

Then he sends the vector C_2 to Alice.

3. Alice generates at random the single-use subkey R'_A and decrypts the vector C_2 obtaining the ciphertext

$$C_3 = R'_A \circ A^{t_A} \circ C_2^{d_A} \circ B^{t_A}.$$

Then she sends the vector C_3 to Bob.

After receiving the ciphertext C_3 Bob computes the value

$$T = E_T \circ A^{t_B} \circ C_3^{d_B} \circ B^{t_B}.$$

Correctness proof of the protocol is as follows:

$$\begin{aligned}
C_2 &= R_B \circ B^{t_B} \circ C_1^{e_B} \circ A^{t_B} = R_B \circ B^{t_B} \circ \left(R_A \circ B^{t_A} \circ T^{e_A} \circ A^{t_A}\right)^{e_B} \circ A^{t_B} = \\
&= R_B \circ B^{t_B} \circ \left(B^{t_A} \circ T^{e_A e_B} \circ A^{t_A}\right) \circ A^{t_B} = R_B \circ B^{t_A} B^{t_B} \circ T^{e_A e_B} \circ A^{t_B} A^{t_A} \;\Rightarrow \\
C_3 &= R'_A \circ A^{t_A} \circ \left(R_B \circ B^{t_A} B^{t_B} \circ T^{e_A e_B} \circ A^{t_B} A^{t_A}\right)^{d_A} \circ B^{t_A} = \\
&= R'_A \circ R_0 \circ B^{t_B} \circ T^{e_A e_B d_A} \circ A^{t_B} \circ R_0 = R'_A \circ B^{t_B} \circ T^{e_B} \circ A^{t_B} \quad \Rightarrow \\
E_T &\circ A^{t_B} \circ C_3^{d_B} \circ B^{t_B} = E_T \circ A^{t_B} \circ \left(R'_A \circ B^{t_B} \circ T^{e_B d_B} \circ A^{t_B}\right) \circ B^{t_B} = \\
&= E_T \circ R_0 \circ T \circ R_0 = E_T \circ T = T.
\end{aligned}$$

Conclusion

It is proposed a new more wider interpretation of the notion of commutative encryption and for the fist time the probabilistic commutative cipher has been developed. A new 6-dimensional FNAA (defined over the finite ground field $GF(p)$) containing p^2 different global right-sided units is introduced as the algebraic carrier of the post-quantum cryptoschemes based on computational difficulty of the HDLP. The structure and respective properties of the algebra have been studied and used in the design of the proposed post-quantum commutative cipher. The exponentiation operation is used as the base encryption operation which is complemented with two different masking homomorphism-map operations. A novel feature of the proposed commutative encryption method is the application of the single-use subkeys selected at random from the set of p^2 global right-sided units contaned in the used algebraic carrier.

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

References

1. Song Y. Yan. *Quantum Computational Number Theory.* N.Y., Springer, 2015.
2. Song Y. Yan. *Quantum Attacks on Public-Key Cryptosystems.* N.Y., Springer, 2014.

3. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
4. 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.
5. 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.
6. 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.
7. Moldovyan A.A., Moldovyan N.A. Post-Quantum Signature Algorithms Based on the Hidden Discrete Logarithm Problem. *Computer Science Journal of Moldova*, 2018, vol. 26, no. 3 (78), pp. 301–313.
8. Moldovyan N.A., Moldovyan A.A. Finite Non-Commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem. *Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software*, 2019, vol. 12, no. 1, pp. 66–81.
9. Menezes A.J., Oorschot P.C., Vanstone S.A. *Applied Cryptography*. N.Y., London, CRC Press, 1996.
10. Hellman M.E., Pohlig S.C. *Exponentiation Cryptographic Apparatus and Method*. U.S. Patent no. 4,424,414, 3 January 1984.

Received June 17, 2019

УДК 681.3 **10.14529/mmp200205**

КОНЕЧНЫЕ НЕКОММУТАТИВНЫЕ АССОЦИАТИВНЫЕ АЛГЕБРЫ КАК НОСИТЕЛИ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

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

Предложен кандидат на постквантовый алгоритм коммутативного шифрования, основанный на скрытой задаче дискретного логарифмирования, заданной в новой шестимерной конечной некоммутативной ассоциативной алгебре. Свойства алгебры детально исследованы и использованы при разработке предложенного коммутативного шифра. Выведены формулы, описывающие p^2 глобальных правосторонних единиц, содержащихся в алгебре. Рассмотрены и использованы в шифре гомоморфизмы двух различных типов. Шифруемое сообщение представлено в виде локально обратимого элемента T алгебры, а процедура шифрования включает выполнение операции возведения в степень и гомоморфное отображение, за которым следует левостороннее умножение на случайно выбранную глобальную правостороннюю единицу. Предложенный шифр является стойким к атакам на основе известного исходного текста и использован для разработки протокола бесключевого шифрования, обеспечивающего возможность безопасной передачи секретных сообщений по открытым каналам без использования предварительно согласованных ключей. Предложенный коммутативный шифр отличается использованием одноразовых подключей, выбираемых случайным образом непосредственно в ходе процесса зашифровывания.

Ключевые слова: коммутативное шифрование; вероятностный шифр; постквантовая криптосхема; конечная некоммутативная алгебра; ассоциативная алгебра; глобальная единица; правосторонняя единица.

Литература

1. Song Y. Yan. Quantum Computational Number Theory / Song Y. Yan. – N.Y.: Springer, 2015.
2. Song Y. Yan. Quantum Attacks on Public-Key Cryptosystems / Song Y. Yan. – N.Y.: Springer, 2014.
3. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer / P.W. Shor // SIAM Journal of Computing. – 1997. – V. 26. – P. 1484–1509.
4. Moldovyan, D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes / D.N. Moldovyan // Quasigroups and Related Systems. – 2010. – V. 18, № 2. – P. 165–176.
5. 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. – P. 629–641.
6. Moldovyan, D.N. Cryptoschemes over Hidden Conjugacy Search Problem and Attacks Using Homomorphisms / D.N. Moldovyan, N.A. Moldovyan // Quasigroups Related Systems. – 2010. – V. 18, № 2. – P. 177–186.
7. Moldovyan, A.A. Post-Quantum Signature Algorithms Based on the Hidden Discrete Logarithm Problem / A.A. Moldovyan, N.A. Moldovyan // Computer Science Journal of Moldova. – 2018. – V. 26, № 3 (78). – P. 301–313.
8. Moldovyan, N.A. Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem. / N.A. Moldovyan, A.A. Moldovyan // Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. – 2019. – V. 12, № 1. – P. 66–81.
9. Menezes, A.J. Applied cryptography / A.J. Menezes, P.C. Oorschot, S.A. Vanstone. – N.Y., London: CRC Press, 1996.
10. Hellman, M.E., Pohlig, S.C. Exponentiation Cryptographic Apparatus and Method. U.S. Patent № 4,424,414, 3 January 1984.

Дмитрий Николаевич Молдовян, кандидат техических наук, научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем, Санкт-Петербургский институт информатики и автоматизации РАН (г. Санкт-Петербург, Российская Федерация), mdn.spectr@mail.ru.

Николай Андреевич Молдовян, доктор техических наук, профессор, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем, Санкт-Петербургский институт информатики и автоматизации РАН (г. Санкт-Петербург, Российская Федерация), nmold@mail.ru.

Александр Андреевич Молдовян, доктор техических наук, профессор, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем, Санкт-Петербургский институт информатики и автоматизации РАН (г. Санкт-Петербург, Российская Федерация), maa1305@yandex.ru.

Поступила в редакцию 17 июня 2019 г.