Computer Science Journal of Moldova, vol.**27**, no.3(81), 2019

Post-quantum commutative encryption algorithm

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

Abstract

To provide possibility to design the commutative encryption algorithms on the basis of new versions of the hidden discrete logarithm problem, the term "commutativity" is interpreted in the extended sense. Namely, the encryption algorithm is called commutative, if the double encryption on two different keys produces the ciphertext that can be correctly decrypted using the keys in arbitrary order. The introduced commutative encryption method is characterized in using the single-use random subkeys. This feature defines probabilistic nature of the encryption process. A candidate for post-quantum commutative encryption algorithm is proposed, using the computations in the 6-dimensional finite non-commutative associative algebra with a large set of the right-sided global units. The proposed algorithm is used as the base of the post-quantum no-key protocol.

Keywords: commutative encryption, post-quantum cryptoscheme, no-key protocol, finite non-commutative algebra, associative algebra, homomorphism

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

1 Introduction

The most widely used public-key cryptoschemes are based on the computational difficulty of the factoring problem (FP) and the discrete logarithm problem (DLP). However, both the FP and the DLP can be solved in polynomial time on a quantum computer [1]. This means that cryptographic schemes based on the FP and on the DLP will not

be secure in the coming era of quantum computing [2]. Future practice needs post-quantum public-key cryptoschemes. A cryptographic algorithm or protocol is called post-quantum, if it runs efficiently on classical computers but will resist quantum attacks [3],[4], i. e., attacks performed with using hypothetic quantum computers.

Currently, post-quantum cryptographic research efforts are mainly focused on developing practical public-key cryptoschemes based on the computationally difficult problems different from the FP and DLP. In the frame of the competition announced by NIST (in the end of 2016) on development of the post-quantum public-key cryptoschemes suitable as candidates for new cryptographic standards several dozen of signature schemes, public encryption algorithms, and public key-agreement protocols have been selected for further research [5].

The commutative encryption algorithms possessing security to the known-plaintext attacks are attractive for different practical applications. The known commutative ciphers 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 a challenge in the area of 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.

The first attempt to solve the noted problem relates to the work [6] in which a commutative cipher was proposed, based on the hidden discrete logarithm problem (HDLP) defined in a finite quaternion algebra. In the recent paper [7] it is shown that that version of the HDLP can be polynomially reduced to the DLP in a finite field.

In the present paper a new form of the HDLP is applied to design the post-quantum commutative encryption algorithm suitable as the base primitive of the post-quantum no-key protocols. The used form of the HDLP is formulated in the 6-dimensional finite non-commutative associative algebra (FNAA) containing a large set of the global right-sided units. The introduced encryption method represents a specific probabilistic transformation, therefore it has been required to extend the interpretation of the notion of commutative encryption. Namely,

we call the encryption algorithm commutative, if the double encryption on two different keys produces the ciphertext that can be correctly decrypted with using the keys in arbitrary order. Such type of commutative ciphers can be used in the no-key encryption protocols.

2 Preliminaries

2.1 Algebraic carriers of the HDLP

In a finite m-dimensional vector space defined over a finite field, for example, $GF(p)$ there are defined two standard operations: addition of two vectors and multiplication of some given vector A by a scalar $d \in GF(p)$. The vector space with the additionally defined operation of multiplying two arbitrary vectors which is distributive relatively the addition operation is called the m-dimensional finite algebra. If the multiplication operation (denoted as $\circ$) is non-commutative and associative, then we have an m-dimensional FNAA. Suppose $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are the basis vectors. The vector A is 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.

Usually the multiplication operation of two vectors A and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined with the formula

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

in which products of different pairs of basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ are to be substituted by a single-component vector indicated in the so called basis vector multiplication table (BVMT). Every cell of the BVMT contains some single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$ is called structural coefficient. If $\lambda = 1$, then the content of the cell is denoted as $\mathbf{e}_k$. One usually assumes that the left operand $\mathbf{e}_i$ defines the row and the right one $\mathbf{e}_j$ defines the column. The intersection of the ith row and jth column defines the cell indicating the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$. To define associative multiplication one should compose the

BVMT that defines associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) .$$

2.2 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). Thus, it is supposed the cyclic group Γ is a subset of elements 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 operations used to mask the values G and Y' are called the masking operations. To provide possibility to design a public-key cryptoscheme on the basis 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 operations.

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 [6],[8] as follows:

$$Y = Q^w \circ G^x \circ Q^{-w} = \alpha\left(G^x\right), \tag{1}$$

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 described by the formula (1) was applied to design a public key-agreement scheme and commutative encryption algorithm [6],[8]. However, reducibility of the first form of the HDLP to the DLP in the finite field $GF(p^2)$ was shown in the paper [7].

Recently [9],[10] 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, T) defined as follows [9]:

$$Y = Q \circ G^x \circ Q^{-1}, \quad Z = H \circ G \circ H^{-1}; \quad T = Q \circ E \circ H^{-1}, \qquad (2)$$

where $Q \circ G \neq G \circ Q$; $H \circ G \neq H \circ Q$; E is a randomly selected vector from the set of local units related to the non-invertible vector G. The HDLP 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 [10]:

$$Y = H \circ G^x \circ D, \quad Z = J \circ G \circ T, \qquad (3)$$

where $D \circ G \neq G \circ D$; $D \circ H = L_1$; $D \circ J = L_2$; $T \circ J = L_3$; L_1, L_2, and L_3 are global left-sided units. The HDLP 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 [7] for reducing the HDLP to the DLP in a finite field does not work.

2.3 Commutative encryption

Encryption function (algorithm) F is called commutative, if for arbitrary encryption keys K_1 and $K_2 \neq K_1$ it satisfies the following condition

$$F_{K_1}[F_{K_2}(M)] = F_{K_2}[F_{K_1}(M)], \qquad (4)$$

where M is a plaintext. Commutative ciphers resisting the known plaintext attack can be used to implement Shamir's no-key protocol (also called Shamir's three-pass protocol [11]) described as follows. Suppose Alice wishes to send the secret message M to Bob, using a public channel and no shared key. For this purpose they can use the following protocol:

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

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

3. Alice decrypts the ciphertext C_2 obtaining the ciphertext $C_3 = F^{-1}_{K_1}(C_2)$. Then she sends the ciphertext C_3 to Bob.

Having received the ciphertext C_3 Bob computes the value $M' = F^{-1}_{K_2}(C_3)$. Due to commutativity of the encryption function F we have $M' = M$:

$$\begin{aligned} M' &= F^{-1}_{K_2}(C_3) = F^{-1}_{K_2}[F^{-1}_{K_1}(C_2)] = F^{-1}_{K_2}[F^{-1}_{K_1}[F_{K_2}(C_1)]] = \\ &= F^{-1}_{K_2}[F^{-1}_{K_1}[F_{K_2}(F_{K_1}(M))]] = F^{-1}_{K_2}[F^{-1}_{K_1}[F_{K_1}(F_{K_2}(M))]] = \\ &= F^{-1}_{K_2}[F_{K_2}(M)] = M. \end{aligned}$$

This protocol provides security to passive attacks (an adversary only intercepts the ciphertexts sent via a channel), if the used commutative encryption function F is secure to the know-plaintext attack. The appropriate commutative encryption function is provided by the exponentiation cipher proposed by Pohlig and Hellman in [12], which is described as follows. Suppose p is a 2464-bit prime such that number $(p-1)$ contains a large prime divisor q, for example, $p = 2q + 1$.

To generate an encryption/decryption key (e, d) one selects a random number e (having size equal to 256 bit or more) that is mutually prime with the value $(p-1)$ and then computes the value $d = e^{-1} \bmod p - 1$. The encryption is defined by the formula

$$C = M^e \bmod p.$$

The next formula defines the decryption operation:

$$M = C^d \bmod p.$$

The Pohlig-Hellman commutative encryption algorithm is as secure as the DLP modulo p is difficult. In this paper we use the notion of the commutativity in the extended sense, namely, we call the encryption

algorithm commutative, if the consecutive encryption of the paintext with using two different keys produces the ciphertext which can be decrypted correctly using the keys in arbitrary order. The ciphers possessing such property can be used for imlementation of the three-pass no-key protocol.

The indicated interpretation of the notion of the commutative encryption covers the commutative encryption functions defined by the formula (4) Only deterministic encryption functions can be commutative in the sense defined by the formula (4). In the proposed extended sense of commutativity both the deterministic encryption functions and the probabilistic encryption functions can be commutative.

3 Algebraic carrier of the proposed post-quantum commutative cipher

The BVMT shown as Table 1 defines the 6-dimensional FNAA which contains p^3 different global right-sided units that can be computed from the following vector equation:

$$A \circ X = A, \tag{5}$$

where $X = (x_0, x_1, \ldots, x_5)$ is the unknown. Using Table 1 one can represent the equation (5) in the form of the following system of six linear equations with six unknowns $x_0, x_1, x_2, x_3, x_4, x_5$:

$$\begin{cases} \tau a_0 x_1 + a_0 x_4 + a_2 x_2 + \tau a_2 x_5 + a_4 x_0 + \tau a_4 x_3 = a_0; \\ \tau a_1 x_1 + a_1 x_4 + a_3 x_2 + \tau a_3 x_5 + a_5 x_0 + \tau a_5 x_3 = a_1; \\ a_0 x_0 + \tau a_0 x_3 + \tau a_2 x_1 + a_2 x_4 + a_4 x_2 + \tau a_4 x_5 = a_2; \\ a_1 x_0 + \tau a_1 x_3 + \tau a_3 x_1 + a_3 x_4 + a_5 x_2 + \tau a_5 x_5 = a_3; \\ a_0 x_2 + \tau a_0 x_5 + a_2 x_0 + \tau a_2 x_3 + \tau a_4 x_1 + a_4 x_4 = a_4; \\ a_1 x_2 + \tau a_1 x_5 + a_3 x_0 + \tau a_3 x_3 + \tau a_5 x_1 + a_5 x_4 = a_5 \end{cases} \tag{6}$$

Performing the variable substitution $u_1 = \tau x_1 + x_4$, $u_2 = x_2 + \tau x_5$, and $u_3 = x_0 + \tau x_3$ one can represent the system (6) in the form of the

following two systems of linear equations:

$$\begin{cases} u_1a_0 + u_2a_2 + u_3a_4 = a_0; \\ u_1a_2 + u_2a_4 + u_3a_0 = a_2; \\ u_1a_4 + u_2a_0 + u_3a_2 = a_4; \end{cases} \tag{7}$$

$$\begin{cases} u_1a_1 + u_2a_3 + u_3a_5 = a_1; \\ u_1a_3 + u_2a_5 + u_3a_1 = a_3; \\ u_1a_5 + u_2a_1 + u_3a_3 = a_5. \end{cases} \tag{8}$$

Table 1

The BVMT defining the FNAA containing p^3 global right-sided units

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

One can easily see that the systems (7) and (8) are simultaneously satisfied for arbitrary vector A with the values of the unknowns $u_1 = 1$, $u_2 = 0$, and $u_3 = 0$. Thus, every vector $X = (x_0, x_1, x_2, x_3, x_4, x_5)$ coordinates of which satisfy the conditions

$$\begin{cases} \tau x_1 + x_4 = u_1 = 1; \\ x_2 + \tau x_5 = u_2 = 0; \\ x_0 + \tau x_3 = u_3 = 0; \end{cases} \Rightarrow \begin{cases} x_4 = 1 - \tau x_1; \\ x_2 = -\tau x_5; \\ x_0 = -\tau x_3 \end{cases} \tag{9}$$

is one of the solutions of the system (6) for every possible value A, i. e., every of such vectors X represent a right-sided unit acting on all elements of the considered FNAA (in this sense such units are global).

From the conditions (9) we get the following formula describing the set of p^3 different global right-sided units contained in the algebra:

$$R = (r_0, r_1, r_2, r_3, r_4, r_5) = (-\tau x_3,\ x_1,\ -\tau x_5,\ x_3,\ 1 - \tau x_1,\ x_5)\,, \tag{10}$$

where $x_1, x_3, x_5 = 0, 1, \ldots p-1$.

Evidently the considered FNAA contains neither global left-sided unit nor global two-sided unit. However, the algebra contains local left-sided units acting in the frame of some subsets of the elements. The local left-sided unit corresponding to some 6-dimensional vector A can be computed as solution of the following vector equation:

$$X \circ A = A. \tag{11}$$

The vector equation (11) can be represented in the form of the following two systems each of which contains three equations:

$$\begin{cases} (\tau a_1 + a_4)\, x_0 + (a_2 + \tau a_5)\, x_2 + (a_0 + \tau a_3)\, x_4 = a_0; \\ (a_0 + \tau a_3)\, x_0 + (\tau a_1 + a_4)\, x_2 + (a_2 + \tau a_5)\, x_4 = a_2; \\ (a_2 + \tau a_5)\, x_0 + (a_0 + \tau a_3)\, x_2 + (\tau a_1 + a_4)\, x_4 = a_4; \end{cases} \tag{12}$$

$$\begin{cases} (\tau a_1 + a_4)\, x_1 + (a_2 + \tau a_5)\, x_3 + (a_0 + \tau a_3)\, x_5 = a_1; \\ (a_0 + \tau a_3)\, x_1 + (\tau a_1 + a_4)\, x_3 + (a_2 + \tau a_5)\, x_5 = a_3; \\ (a_2 + \tau a_5)\, x_1 + (a_0 + \tau a_3)\, x_3 + (\tau a_1 + a_4)\, x_5 = a_5. \end{cases} \tag{13}$$

The main determinant of the systems (12) and (13) is the same and equal to the value

$$\begin{aligned} \Delta_A = (a_0 + \tau a_3)^3 + (\tau a_1 + a_4)^3 + (a_2 + \tau a_5)^3 - \\ - 3\,(a_0 + \tau a_3)\,(\tau a_1 + a_4)\,(a_2 + \tau a_5)\,. \end{aligned} \tag{14}$$

If $\Delta_A \neq 0$, then there exists the single solution $X = L_A$ that represents the local left-sided unit of the vector A.

Proposition 1. Suppose the vector A is such that $\Delta_A \neq 0$. Then there exists some integer ω such that $A^\omega = L_A$ and the vector L_A is simultaneously one of the global right-sided units.

Proof. Let us consider the sequence of the vectors $A, A^2, \ldots A^h, \ldots A^k, \ldots$. For all integer values i one has $A^i \neq O$, where $O = (0,0,0,0,0,0)$, since $\Delta_A \neq 0$. Due to finiteness of the considered algebras and condition $\Delta_A \neq 0$ the indicated sequence is periodic, i. e., for some integer h and minimum integer $k > h$ we have the following:

$$A^k = A^h \Rightarrow A^{k-h} \circ A^h = A^h \Rightarrow \Big(A^{k-h} \circ A - A\Big) \circ A^{h-1} = O \Rightarrow$$
$$A^{k-h} \circ A - A = O \Rightarrow A^{k-h} \circ A = A \Rightarrow A^{k-h} = L_A,$$
$$A^{k-h} \circ A = A \Rightarrow A \circ A^{k-h} = A \Rightarrow A^{k-h} = R_A = L_A = E_A,$$

where R_A is one of the global right-sided units described by the formula (10); L_A is the local left-sided unit related to the vector A; E_A is the local two-sided unit related to A. Thus, Proposition 1 holds true.

The single local two-sided unit E_A corresponds to the vector A such that $\Delta_A \neq 0$, since $E_A = L_A$ and we have the single local left-sided unit relating to the vector A. The value $\omega = k - h$ such that $A^\omega = E_A$ can be called the local order of the vector A. Proposition 1 shows $A^{\omega-1} \circ A = A \circ A^{\omega-1} = E_A$, i. e., the vector $A^{\omega-1}$ is the inverse value of the vector A relatively the local two-sided unit E_A.

In the next section a new method for commutative encryption is proposed, at the development of which the following propositions have been used.

Proposition 2. If the vector equation $A \circ X = B$ has solution $X = S$, then p^3 different values $X_i = R_i \circ S$, where R_i takes on all values from the set (10), also are solutions of the given equation.

Proof. $A \circ (R_i \circ S) = (A \circ R_i) \circ S = A \circ S = B$. The Proposition 2 is proven.

Proposition 3. If $A \circ B = R$, where R is a global right-sided unit, then the equality $A^i \circ B^i = R$ holds true for arbitrary natural value i.

Proof.

$A^i \circ B^i = \big(A^{i-1} \circ R\big) \circ B^{i-1} = A^{i-1} \circ B^{i-1} = A^{i-2} \circ B^{i-2} = \ldots$

$\cdots = A \circ B = R$. The Proposition 3 is proven.

Proposition 4. If $A \circ B = R$, where R is a global right-sided unit, then the map defined by the formula $\psi(X) = B \circ X \circ A$, where the

vector X takes on all values in the considered algebra, represents a homomorphism.

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

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

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

The Proposition 4 is proven.

Proposition 5. The homomorphism-map operation $\psi(X) = B \circ X \circ A$, where $A \circ B = R$, and the exponentiation operation X^i are mutually commutative, i. e., the equality $B \circ X^i \circ A = (B \circ X \circ A)^i$ holds true.

Proof. Due to Proposition 4 we have $\psi(X^i) = (\psi(X))^i$, i. e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The Proposition 5 is proven.

Proposition 6. Suppose the vector R is an arbitrary global right-sided unit and the vector X takes on all values in the considered FNAA. Then the map defined by the formula $\varphi(X) = R \circ X$ is a homomorphism.

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

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

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

The Proposition 6 is proven.

Proposition 7. The homomorphism-map operation $\varphi(X) = R \circ X$, 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 we have $\varphi(X^i) = (\varphi(X))^i$, i. e., $R \circ X^i = (R \circ X)^i$. The Proposition 7 is proven.

4 Probabilistic commutative encryption algorithm

Suppose the FNAA described in Section 3 is defined over the field $GF(p)$, where the prime $p = 2q + 1$; q is a 256-bit prime, and the encrypted message is represented in the form of the vector $T = (t_0, t_1, \ldots, t_5)$ such that $\Delta_T \neq 0$. (For some given message probability that $\Delta_A = 0$ is negligible. Besides, one can modify the message to satisfy the condition $\Delta_T \neq 0$.) The local two-sided unit E_T relating to the vector T can be computed from the vector equation

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

The vector E_T is contained in the set of global right-sided units (10). The algebra contains different vectors relating to some fixed value R from the set (10). All vectors such that the local two-sided unit of every of them is equal to R compose a finite group. The vector T is contained in a single of the mentioned finite groups and it generates a cyclic subgroup having the order ω that is a divisor of the value $p^2 - 1$. Therefore, the alternative method for computing the value E_T relates to using the formula

$$E_T = T^{p^2-1}. \tag{16}$$

However, finding the value E_T as solution of the vector equation (15) has significantly lower computational complexity. From (16) one can see that the message T can be encrypted and correctly decrypted with using the following two formulas:

$$C = T^e; \quad T = C^d, \tag{17}$$

where e and d are non-negative integers such that $ed \equiv 1 \bmod p^2 - 1$.

The formula (17) defines the commutative encryption function, the security of which to the known-plaintext attack is based on computational difficulty of the DLP. To develop a post-quantum commutative cipher one can use the masking operations, namely, the homomorphism-map operations ψ and φ.

4.1 Using the homomorphism map φ as encryption operations

The encryption of the message T with using the φ operation is performed with using the single-use subkey representing a randomly selected global right-sided unit R and is described as follows:

1. Compute the local two-sided unit E_T relating to the vector T.

2. Generate a random global right-sided unit R and compute the vector $C = R \circ T^e$.

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

This encryption procedure represents probabilistic ciphering process due to using a randomly selected single-use subkey R. The output ciphertext is two times larger in size than the input message T. The decryption is performed in accordance with the formula

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

Correctness proof of this decryption formula is as follows:

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

To consider the commutativity property of the introduced encryption function one should define the process of encrypting the message on two different keys. Evidently, the first element of the ciphertext, i. e., the vector E_T should not be transformed in the frame of the second encryption. Therefore, the encryption of the message T on the key (e_1, d_1) and then on the key (e_2, d_2) produces the ciphertext

$$C_{12} = (E_T, R_2 \circ T^{e_1 e_2}),$$

where R_2 is a global right-sided unit selected at random at the second encryption as the single-use subkey. The encryption of the message T on the key (e_2, d_2) and then on the key (e_1, d_1) produces the ciphertext

$$C_{21} = (E_T, R_1 \circ T^{e_2 e_1}),$$

where R_1 is a random global right-sided unit selected as the single-use subkey at the second encryption. Due to probabilistic nature of the

encryption function in the considered two cases we have got different output ciphertexts. However, one can easily show both the ciphertext C_{21} and the ciphertext C_{12} are decrypted correctly using the keys (e_1, d_1) and (e_2, d_2) in arbitrary order. Thus, the described encryption function is commutative.

4.2 Using the homomorphism map ψ as encryption operation

To implement encryption of the message T with using the ψ operation one should apply two common parameters representing the vectors A and B such that $A \circ B = R_0$, where R_0 is some fixed global right-sided unit, and additional subkey representing a non-negative integer $t < p^2 - 1$, i. e., the encryption key represents the triple of the natural numbers (e, d, t). The encryption procedure includes the following steps:

1. Compute the local two-sided unit E_T relating to the vector T.
2. Compute the vector $C = B^t \circ T^e \circ A^t$.
3. Output the ciphertext in the form of the pair of two vectors (E_T, C).

This encryption algorithm is a deterministic procedure; the ciphertext is two times larger in size than the source message though. The decryption is performed in accordance with the formula

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

Correctness proof of this decryption formula is as follows:

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

Let us consider the case of encryption of the message T on two independent keys (e_1, d_1, t_1) and (e_2, d_2, t_2). Like in the case of the encryption algorithm described in the previous subsection the first element of the ciphertext, i. e., the vector E_T should not be transformed in the frame of the second encryption. Encryption of the message T on the first key

and then on the second key produces the ciphertext

$$C_{12} = \left(E_T, B^{t_1+t_2} \circ T^{e_1e_2} \circ A^{t_1+t_2}\right).$$

Encryption of the message T on the second key and then on the first key produces the ciphertext

$$C_{21} = \left(E_T, B^{t_2+t_1} \circ T^{e_2e_1} \circ A^{t_2+t_1}\right) = C_{12}.$$

Thus, we have the same output ciphertext in the both cases, i. e., the described encryption algorithm is commutative.

4.3 Post-quantum commutative cipher and no-key protocol on its basis

In this section the post-quantum version of the commutative cipher is proposed, which is based on the HDLP defined with using both the masking φ-map operation and the masking ψ-map operation. The encryption procedure is performed using the key (e, d, t) as follows:

1. Compute the local two-sided unit E_T relating to the input message T.

2. Generate a random global right-sided unit and compute the vector $C = R \circ B^t \circ T^e \circ A^t$.

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

This encryption algorithm is a probabilistic procedure. The decryption is performed in accordance with the formula

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

Correctness proof of this decryption formula 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_1, d_1, t_1) and then on the key (e_2, d_2, t_2) produces the ciphertext

$$C_{12} = \left(E_T, R_2 \circ B^{t_2+t_1} \circ T^{e_1e_2} \circ A^{t_1+t_2}\right),$$

where R_2 is a random global right-sided unit used at the second encryption as the single-use subkey. Encryption of the message T on the key (e_2, d_2, t_2) and then on the key (e_1, d_1, t_1) produces the ciphertext

$$C_{21} = \left(E_T, R_1 \circ B^{t_1+t_2} \circ T^{e_2 e_1} \circ A^{t_2+t_1}\right),$$

where R_1 is a random global right-sided unit used at the second encryption as the single-use subkey.

In the considered two cases of double encryption we have different output ciphertexts. However, each of the ciphertexts is decrypted correctly, when performing the double decryption with using the keys in arbitrary order. Thus, 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 M:

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

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.

Having received the ciphertext C_3 Bob computes the value

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

Correctness proof of this decryption formula is as follows:

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

5 Conclusion

Interpreting the notion of commutative encryption in the wider sense, for the first time the probabilistic commutative encryption algorithm has been developed. The 6-dimensional FNAA containing p^3 different global right-sided units, which is defined over the finite ground field $GF(p)$, have been used as the algebraic carrier of the proposed post-quantum probabilistic commutative cipher based on the HDLP. The base encryption operation is the exponentiation operation complemented with two different masking homomorphism-map operations. One more novel feature of the commutative encryption method is the application of the single-use subkeys selected at random from the set of the global right-sided units.

On the basis of the introduced commutative cipher a post-quantum no-key protocol have been developed that seems more attractive for practical applications than the recently proposed one [13].

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer," *SIAM Journal of Computing*, vol. 26, pp. 1484–1509, 1997.

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

[3] 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.

[4] *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.

[5] PQC Standardization Process: Second Round Candidate Announcement. https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

[6] 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.

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

[8] D. N. Moldovyan and 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 and N. A. Moldovyan, "Post-quantum signature algorithms based on the hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 26, no. 3(78), pp. 301–313, 2018.

[10] N. A. Moldovyan and A. A. Moldovyan, "Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem," *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS)*, vol. 12, no. 1, pp. 66–81, 2019.

[11] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Applied cryptography*, New York, London: CRC Press, 1996, 780 p.

[12] M. E. Hellman and S. C. Pohlig, "Exponentiation Cryptographic Apparatus and Method," U.S. Patent # 4,424,414. 3 Jan. 1984.

[13] N. A. Moldovyan, A. A. Moldovyan, and V. A. Shcherbacov, "Post-quantum No-key Protocol," *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, no. 3(85), pp. 115–119, 2017.

A.A. Moldovyan, D.N. Moldovyan, N.A. Moldovyan, Received April 15, 2019

St. Petersburg Institute for Informatics and Automation
of Russian Academy of Sciences,
14 Liniya, 39, St. Petersburg 199178, Russia
E–mail: maa1305@yandex.ru; mdn.spectr@mail.ru; nmold@mail.ru;
http://www.spiiras.nw.ru