Post-quantum Commutative Encryption Algorithm

Dmitriy N. Moldovyan[1], Alexandr A. Moldovyan[1], Han Ngoc Phieu[2], and Minh Hieu Nguyen[2(✉)]

[1] Laboratory of Cybersecurity and Post-quantum Cryptosystems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, St. Petersburg, Russia
mdn.spectr@mail.ru, maal305@yandex.ru

[2] Faculty of Electronics and Telecommunications, Academy of Cryptography Techniques, 141 Chien Thang, Tan Trieu, Thanh Tri, Hanoi, Vietnam
phieungochan@gmail.com, hieuminhmta@gmail.com

Abstract. It is considered an extended notion of the commutativity of the encryption. Using the computational difficulty of the hidden discrete logarithm problem, a new method and post-quantum probabilistic algorithm for commutative encryption are proposed. The finite non-commutative associative algebra containing a large set of the global left-sided unites is used as the algebraic carrier of the proposed method and probabilistic commutative cipher. The latter is secure to the known-plaintext attack and, therefore, efficient to implement on its base a post-quantum no-key encryption protocol. Main properties of the algebraic carrier, which are used in the commutative encryption method, are described.

Keywords: Post-quantum cryptography · Commutative probabilistic encryption · No-key protocol · Hidden logarithm problem · Finite non-commutative algebra · Associative algebra

1 Introduction

Currently the development of the practical post-quantum public-key cryptoschemes attracts significant attention of the cryptographic community [1, 2]. A cryptoscheme is called post-quantum, if it performs efficiently on ordinary computers and resists attacks with using hypothetic quantum computers (quantum attacks). Post-quantum public-key algorithms and protocols are to be based on some computationally difficult problems that are different from the factorization problem (FP) and discrete logarithm problem (DLP), since there are known polynomial in time algorithms for solving both the FP and the DLP [3, 4].

Many different post-quantum public-key algorithms and protocols have been designed and proposed as candidates for post-quantum public-key standards in frame of the world competition announced by NIST in the end of 2016 [2]. One should mention that the problem of providing post-quantum security relates also to the commutative

P. C. Vinh and A. Rakib (Eds.): ICCASA 2019/ICTCC 2019, LNICST 298, pp. 205–214, 2019.
https://doi.org/10.1007/978-3-030-34365-1_16

encryption algorithms possessing security to the known-plaintext attacks. Commutative ciphers possessing such property represent the base primitive of the no-key encryption protocols that are attractive for different practical applications. Development of the post-quantum commutative encryption algorithms is an open problem that is considered only in few papers. An interesting approach to the development of the post-quantum commutative cipher is the use of the computational difficulty of the hidden discrete logarithm problem (HDLP) [5]. However, the form of the HDLP defined in the finite algebra of quaternions and introduced in [5] can be reduced to the ordinary DLP in a finite field [6].

In the present paper it is introduced a new form of the HDLP that prevents the reductionist method developed in [6]. The paper is organized as follows. Section 2 presents the base notion connected with the HDLP. Section 3 introduces the 4-dimensional finite non-commutative associative algebra (FNAA) used as algebraic support of the proposed post-quantum commutative encryption method. Section 4 presents the novel interpretation of the notion of commutativity of the encryption and the proposed post-quantum commutative probabilistic encryption algorithm. Section 5 describes the post-quantum no-key encryption protocol based on the introduced commutative encryption algorithm. Final remarks are presented in the concluding Sect. 6.

2 Forms of the Hidden Discrete Logarithm Problem

The DLP consists in solving the equation $Y' = G'^x$ (where G' is the generator of the group and Y' is a group element) in a finite cyclic group relatively the unknown x. The HDLP is set in some m-dimensional FNAA, where $m \geq 4$ is an even number, which contains many different cyclic groups as subsets of the m-dimensional vectors (algebraic elements). The HDLP is defined as selection a base finite cyclic group with the generator G', generation a random integer x, performing the base exponentiation operation G'^x, and mapping one of the values G' and G'^x or both of them, using different map functions (operations) $\varphi(X)$ and $\psi(X)$. For example, (i) the values $Y = \varphi(G'^x)$ and G', (ii) $Y = \varphi(G'^x)$ and $G = \psi(G')$ are given and in each of the last two cases one should compute the value x.

The functions $\varphi(X)$ and $\psi(X)$ are called masking operations. To have possibility to design some public-key protocols and algorithms with the use of the values $Y = \varphi(G'^x)$ and $G = \psi(G')$ as parameters of the cryptoscheme, the masking operations should possess respective properties. The main requirement for the masking function is the mutual commutativity with the base exponentiation operation.

Finite non-commutative associative algebras of different types are very attractive for using them as algebraic supports of the HDLP. Automorphism-map functions and homomorphism-map function defined in some given FNAA can be used as masking operations.

The specific form of the HDLP is determined by the choice of a particular pair of the map functions $\varphi(X)$ and $\psi(X)$.

The known form [5, 7] of the HDLP can be characterized as the case $Y = \varphi(G'^x) = KG'^xK^{-1}$ and $G' = \psi(G')$, where the values K and x are elements of the private key; Y is the public key.

3 Algebraic Support of the Proposed Post-quantum Commutative Cipher

Let us consider a finite m-dimensional vector space defined over the ground finite field $GF(p)$. In the vector space there are defined two operations: (i) addition of vectors and (ii) multiplying a vector by a scalar. If one defines the additional operation (denoted as $\circ$) for multiplying arbitrary two vectors, which is distributive relatively the addition operation, then the considered vector space represents a new algebraic structure called finite m-dimensional algebra. Such complemented finite vector space is called finite algebra. If the multiplication operation is non-commutative and associative, then the algebra is FNAA. Suppose $\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{m-1}$ are the basis vectors. The vector A is denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1}$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$.

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

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

where products of all pairs of basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ are to be substituted by a single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$ is the structural constant, indicated in the so called basis vector multiplication table (BVMT). The intersection of the ith row and jth column defines the cell indicating the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$.

For defining the HDLP of a new type we have set the BVMT describing the vector multiplication operation in the finite 4-dimensional vector space, which is presented as Table 1. This BVMT defines the 4-dimensional FNAA, containing p^2 different global left-sided units. To derive the formula describing the all such units one should solve the following vector equation:

$$X \circ A = A, \tag{1}$$

where $A = (a_0, a_1, a_2, a_3)$ is a fixed 4-dimensional vector and $X = (x_0, x_1, x_2, x_3)$ is the unknown. Using Table 1 one can reduce the vector Eq. (1) to the following two systems of two linear equations:

$$\begin{cases} (x_1 + x_2)a_0 + (x_0 + x_3)a_2 = a_0; \\ \lambda(x_0 + x_3)a_0 + (x_1 + x_2)a_2 = a_2; \end{cases} \tag{2}$$

$$\begin{cases} (x_1+x_2)a_1+\lambda(x_0+x_3)a_3=a_1; \\ (x_0+x_3)a_1+(x_1+x_2)a_3=a_3. \end{cases} \tag{3}$$

Table 1. Defining the multiplication operation in the 4-dimensional vector space (λ is quadratic non-residue in *GF*(*p*))

∘	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$

Performing the variable substitution $u_1 = x_1 + x_2$ and $u_2 = x_0 + x_3$ one can establish that for all vectors A in the considered FNAA the set of the vectors L described with the formula

$$L = (l_0, l_1, l_2, l_3) = (x_0, x_1, 1 - x_1, -x_0), \tag{4}$$

where x_0, x_1 = 0, 1, …. p − 1, represents solutions of the Eq. (1), i.e., each of the p^2 different values L is the global left-sided unit of the algebra (global means that the unit acts on each element of the algebra).

The right-sided units relating to some vector A can be computed from the vector equation

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

that can be reduced to the following two independent systems of two linear equations with the unknowns x_0, x_2 and x_1, x_3 correspondingly:

$$\begin{cases} (a_1+a_2)x_0+(a_0+a_3)x_2=a_0; \\ \lambda(a_0+a_3)x_0+(a_1+a_2)x_2=a_2; \end{cases} \tag{6}$$

$$\begin{cases} (a_1+a_2)x_1+\lambda(a_0+a_3)x_3=a_1; \\ (a_0+a_3)x_1+(a_1+a_2)x_3=a_3. \end{cases} \tag{7}$$

The systems (6) and (7) have the same main determinant that is equal to

$$\Delta_A = (a_1+a_2)^2 - \lambda(a_0+a_3)^2. \tag{8}$$

The value of the structural constant λ is selected from the set of non-residues modulo p (see Table 1), therefore only for p^2 different vectors A', namely, for vectors satisfying the conditions $a'_1 = -a'_2$ and $a'_1 = -a'_3$ we have $\Delta_{A'} \neq 0$. For all other vectors A we have $\Delta_A \neq 0$. Such vectors we call locally invertible, since for every of them Eq. (5) has one solution that defines unique local right-sided unit R_A= (r_0, r_1, r_2,

r_3) related to the vector A. Solving the systems (6) and (7) one can derive the following formulas describing the value R_A:

$$r_0 = \frac{a_0a_1 - a_2a_3}{\Delta_A}, \quad r_1 = \frac{a_1(a_1 + a_2) - \lambda a_3(a_0 + a_3)}{\Delta_A}, \tag{9}$$

$$r_2 = \frac{a_2(a_1 + a_2) - \lambda a_0(a_0 + a_3)}{\Delta_A}, \quad r_3 = \frac{a_2a_3 - a_0a_1}{\Delta_A}. \tag{10}$$

One can easily show that the formulas $r_2 = 1 - r_1$ and $r_3 = -r_0$ hold true, i.e., the vector R_A is contained in the set (4). Therefore, actually R_A is the local two-sided unit relating to the vector A. Evidently, the vector R_A is the local two-sided unit relating to the vectors A^i for all natural values i. Let us consider the sequence of the values A, A^2, …, A^i, … (generated by the vector A such that $\Delta_A \neq 0$). This sequence is periodic and do not contain the zero element $O = (0, 0, 0, 0)$. Indeed, assumption that for some minimum natural number j we have $A^{j-1} \neq O$ and $A^j = O$ leads to the following (due to the condition $\Delta_A \neq 0$):

$$A \circ A^{j-1} = O \;\Rightarrow\; A^{j-1} = O,$$

Proposition 1. Suppose for some vector A we have $\Delta_A \neq 0$. Then for some minimum natural number ω_A the condition $A^{\omega_A} = R_A$ holds true and the set of the vectors $\{A, A^2, \ldots, A^i, \ldots, A^{\omega_A}\}$ represents a finite cyclic group with the unit element R_A.

Proof. Since the sequence A, A^2, …, A^i, … is periodic, for some minimum natural $h > i$ we have $\{A^h = A^i\} \Rightarrow \{A^i \circ A^{h-i} = A^i\} \Rightarrow \{R_{A^i} = A^{h-i}\}$. For the right-sided unit R_A corresponding to the element A we have $\{A^i \circ R_A = A^{i-1} \circ (A \circ R_A) = A^i\} \Rightarrow \{R_{A^i} = R_A\} \Rightarrow \{R_A = A^{h-i}\}$. Thus, we have $R_A = A^{\omega_A}$, where $\omega_A = h - i$. Evidently, the vector R_A acts as two-sided unit on all elements of the set $\{A, A^2, \ldots, A^{\omega_A}\}$, therefore the element $A^{\omega - i}$ is inverses of the element A^i. Taking into account the associativity of the multiplication operation we conclude the set $\{A, A^2, \ldots, A^{\omega_A}\}$ is a finite cyclic group with the unit element equal to R_A. The Proposition 1 is proven.

Proposition 2. Suppose the vector L is a global left-sided unit. Then the map of the FNAA defined by the formula $\varphi_L(X) = X \circ L$, 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:

$$\begin{aligned}\varphi_L(X_1 \circ X_2) &= (X_1 \circ X_2) \circ L = (X_1 \circ L) \circ (X_2 \circ L)\\ &= \varphi_L(X_1) \circ \varphi_L(X_2);\\ \varphi_L(X_1 + X_2) &= (X_1 + X_2) \circ L = (X_1 \circ L) + (X_2 \circ L)\\ &= \varphi_L(X_1) + \varphi_L(X_2).\end{aligned}$$

The Proposition 2 is proven.

Proposition 3. Suppose $A \circ B = L$. Then for arbitrary natural number t the equality $A^t \circ B^t = L$ holds true.

Proof. $A^t \circ B^t = A^{t-1} \circ (A \circ B) \circ B^{t-1} = A^{t-1} \circ B^{t-1} = A^{t-2} \circ (A \circ B) \circ B^{t-2} = A^{t-2} \circ B^{t-2} = A \circ B = L'$. The Proposition 3 is proven.

Proposition 4. Suppose $A \circ B = L$. Then the formula $\psi_L = B \circ X \circ A$, where the vector X takes on all values in the considered 4-dimensional FNAA, sets the homomorphism map.

Proof. For two arbitrary 4-dimensional vectors X_1 and X_2 one can get the following:

$$\begin{aligned}\psi_L(X_1 \circ X_2) &= B \circ (X_1 \circ X_2) \circ A = B \circ (X_1 \circ L' \circ X_2) \circ A \\ &= (B \circ X_1 \circ A) \circ (B \circ X_2 \circ A) = \psi_{L'}(X_1) \circ \psi_{L'}(X_2); \\ \psi_L(X_1 + X_2) &= B \circ (X_1 + X_2) \circ A = (B \circ X_1 \circ A) \\ &+ (B \circ X_2 \circ A) = \psi_{L'}(X_1) + \psi_{L'}(X_2).\end{aligned}$$

The Proposition 4 is proven.

We will use the homomorphism maps φ_L and ψ_L as masking operations in the post-quantum commutative encryption algorithm described in the next section. Evidently, each of these operations is mutually commutative with the exponentiation operation.

The algebra described in this section suits well as the algebraic support to implement an encryption algorithms based on the HDLP. The considered FNAA contains very large number of the finite cyclic groups having the same value of the order, that is equal to a divisor of the value $p^2 - 1$. Respectively, the order ω_A of some locally invertible vector A is a divisor of the value $p^2 - 1$.

4 Commutative Encryption Algorithm

Some message to be encrypted is represented in the form of the 4-dimensional vector $M = (m_0, m_1, m_2, m_3)$ coordinates of which are elements of the field $GF(p)$, where $p = 2q + 1$ and q is a 256-bit prime number. Probability that $\Delta_M = 0$ is negligible (is equal to p^{-2}), therefore we will consider that the vector M is locally invertible ($\Delta_M \neq 0$). Like in the Pohlig-Hellman exponentiation cipher [8], the encryption/decryption key is generated as the triple of non-negative numbers (e, d, t) such that $ed \equiv 1 \mod p^2 - 1$. Besides the used FNAA, two vectors A and B such that $A \circ B = L_0$, where L_0 is some given global left-sided unit, are specified as common parameters of the proposed post-quantum cipher.

The encryption is performed as computation of two vectors R_M and C. The value R_M represents the right-sided unit related to the vector M and is computed using the formulas (9) and (10). To transform the message into the vector C, the single-use key in the form of randomly selected global left-sided unit is generated and then the value C is computed as follows:

$$C = B^t \circ M^e \circ A^t \circ L. \tag{11}$$

In the last formula the value L is the single-use subkey that is selected at random, i.e., the proposed encryption method relates to the probabilistic encryption procedures for which the value of the ciphertext is not predetermined even in the case, when the same source message is encrypted two times. The known interpretation of the commutativity of the encryption relates to the deterministic encryption procedures, namely, it is assumed that a cipher is commutative, if the double encryption of some fixed input message on two different fixed keys produces the same ciphertext independently of the order of using the keys [8, 9]. In the case of such definition of the commutativity of the encryption no probabilistic commutative ciphers are possible.

Thus, in this paper we use the extended interpretation of the commutative-encryption notion. We call an encryption algorithm commutative, if the double encryption of some fixed input message on two different fixed keys produces the ciphertext the can be correctly decrypted using the keys in each of two possible orders. below it is shown that the formula (11) defines the commutative encryption process.

Decryption of the ciphertext (R_M, C) is performed as computation of the vector M' with using the following formula:

$$M' = A^t \circ C^d \circ B^t \circ R_M. \tag{12}$$

Correctness proof of the proposed encryption method is as follows:

$$\begin{aligned} M' &= A^t \circ C^d \circ B^t \circ R_M = A^t \circ (B^t \circ M^e \circ A^t \circ L)^d \circ B^t \circ R_M \\ &= A^t \circ B^t \circ M^{ed} \circ A^t \circ B^t \circ R_M = L_0 \circ M \circ L_0 \circ R_M = M. \end{aligned}$$

Let us show that the proposed encryption algorithm is commutative. Since the first encryption with the key (e, d, t) and the second encryption with the key $(\varepsilon, \delta, \tau)$ relates to the data having different size (because the ciphertext includes the vector R_M as the first part), we accept on definition that the value R_M is computed in frame of the first encryption and at the second encryption the value R_M is not transformed.

The double encryption with the key (e, d, t) and then with the key $(\varepsilon, \delta, \tau)$ produces the ciphertext (R_M, C'), where C' is computed as follows:

$$C' = B^{t+\tau} \circ M^{e\varepsilon} \circ A^{t+\tau} \circ L', \tag{13}$$

where L' is some random global left-sided unit used as the single-use key at the second encryption.

The double encryption with the key $(\varepsilon, \delta, \tau)$ and then with the key (e, d, t) produces the ciphertext (R_M, C''), where C'' is computed as follows:

$$C'' = B^{\tau+t} \circ M^{\varepsilon e} \circ A^{\tau+t} \circ L'', \tag{14}$$

where L'' is some random global left-sided unit used as the single-use key at the second encryption. The ciphertexts (R_M, C') and (R_M, C'') are different, however one can easily

show that the double decryption of each of the ciphertexts (R_M, C') and (R_M, C'') outputs the source message M independently of the order of using the keys $(\varepsilon, \delta, \tau)$ and (e, d, t). For example, decryption of the ciphertext (R_M, C'') with the key $(\varepsilon, \delta, \tau)$ and then with the key (e, d, t) gives the following transformations:

$$\begin{aligned}
C^* &= A^{\tau} \circ C''^{\delta} \circ B^{\tau} \circ R_M \\
&= A^{\tau} \circ \left(B^{\tau+t} \circ M^{\varepsilon e} \circ A^{\tau+t} \circ L''\right)^{\delta} \circ B^{\tau} \circ R_M \\
&= A^{\tau} \circ B^{\tau+t} \circ M^{\varepsilon e \delta} \circ A^{\tau+t} \circ L'' \circ B^{\tau} \circ R_M \\
&= A^{\tau} \circ B^{t} \circ B^{\tau} \circ M^{e} \circ A^{t} \circ A^{\tau} \circ B^{\tau} \circ R_M \\
&= L_0 \circ B^{t} \circ M^{e} \circ A^{t} \circ L_0 \circ R_M = B^{t} \circ M^{e} \circ A^{t} \circ R_M; \\
M &= A^{t} \circ \left(C^*\right)^{d} \circ B^{t} \circ R_M \\
&= A^{t} \circ \left(B^{t} \circ M^{e} \circ A^{t} \circ R_M\right)^{d} \circ B^{t} \circ R_M \\
&= A^{t} \circ B^{t} \circ M^{ed} \circ A^{t} \circ R_M \circ B^{t} \circ R_M \\
&= L_0 \circ M^{ed} \circ L_0 \circ R_M = M.
\end{aligned}$$

Thus, we have proposed the post-quantum commutative cipher suitable for implementing the no-key encryption protocol. However, we interpret the term "commutativity" in the extended sense. Namely, we call the encryption algorithm commutative, if the double encryption on two different keys produces the ciphertext that can be correctly decrypted using the keys in a different order.

From the formula (11) one can see that the known-plaintext attack on the described commutative cipher, which assumes finding the value e, represents the HDLP that is characterized in masking the vector M^e, i.e., the output of the base exponentiation operation, with two consecutive homomorphism maps ψ_{L0} and φ_L.

5 Post-quantum No-key Encryption Protocol

Notion "no-key encryption" relates to implementing a secure communication session without using some pre-agreed key. No-key protocol uses some commutative encryption function $E_K(M)$, where M is the input message and K is the encryption key, which is secure to the known plaintext attacks [9]. Usually the encryption function is called commutative, if the following equality holds:

$$E_{K_A}(E_{K_B}(M)) = E_{K_B}(E_{K_A}(M))$$

where K_A and K_B ($K_B \neq K_A$) are different encryption keys. Shamir's no-key protocol includes the following three steps [9]:

1. The sender (Alice) of the message M generates a random key K_A and calculates the ciphertext $C_1 = E_{K_A}(M)$. Then she sends C_1 to the receiver (Bob) via an open channel.

2. Bob generates a random key K_B, encrypts the ciphertext C_1 with the key K_B as follows: $C_2 = E_{K_B}(C_1) = E_{K_B}(E_{K_A}(M))$. Then he sends the ciphertext C_2 to Alice.
3. Alice, using decryption procedure $D = E^{-1}$, calculates the ciphertext

$$C_3 = D_{K_A}(C_2) = D_{K_A}(E_{K_B}(E_{K_A}(M))) = D_{K_A}(E_{K_A}(E_{K_B}(M))) = E_{K_B}(M)$$

and sends C_3 to Bob.

Bob discloses the message as follows: $M = E_{K_B}^{-1}(C_3)$.

If one uses the Pohlig-Hellman exponentiation cipher [8] as the function $E_K(M)$ in this protocol, then the protocol is as secure as the DLP is hard. However, security to quantum attacks is not provided.

Using the post-quantum commutative encryption algorithm described in Sect. 4 one can propose the following post-quantum version of the no-key protocol:

1. Alice generates a random key (e, d, t), the single-use key L and calculates the ciphertext (R_M, C_1), where $C_1 = B^t \circ M^e \circ A^t \circ L$. Then she sends (R_M, C_1) to Bob via a public channel.
2. Bob generates a random key $(\varepsilon, \delta, \tau)$, the single-use key L' and encrypts the ciphertext C_1 as follows: $C_2 = B^\tau \circ C_1^\varepsilon \circ A^\tau \circ L'$ and sends C_2 to Alice.
3. Alice generates the single-use key L'' and decrypts the ciphertext C_2 obtaining the ciphertext C_3: $C_3 = A^t \circ C_2^d \circ B^t \circ L''$. Then she sends C_3 to Bob.

Using the received ciphertext C_3 the receiver (i.e., Bob) recovers message M accordingly to the formula $M = A^{t_2} \circ C^{d_2} \circ B^{t_2} \circ R_M$.

The practical application of the no-key protocol relates to sending confidential messages via public (insecure) channels without using pre-agreed keys. Since security of the no-key protocol is based on the hardness of the underlying difficult problem (HDLP in the proposed version of the no-key protocol), only conditional (practical) security is provided. To provide unconditional (theoretical) security one should use secure communication channels and protocols of other types, for example, the quantum three-stage protocol [10] that is based on the quantum physics laws.

6 Conclusion

For the first time it is proposed a probabilistic commutative encryption method and a post-quantum commutative cipher based on the introduced method. Security of the proposed cipher is based on computational difficulty of the HDLP set in a new form using the 4-dimensional FNAA containing a large set of the global left-sided units as the algebraic support of the proposed encryption algorithm. The proposed commutative cipher have been used to design a post-quantum version of the no-key encryption protocol.

The proposed encryption method is very attractive to be combined with the pseudo-probabilistic method propose earlier in the papers [11, 12].

Acknowledgements. The reported study was partially funded by Russian Foundation for Basic Research (project #18-57-54002-Viet_a) and by VietNam Academy of Science and Technology (project # QTRU01.08/18-19).

References

1. Lange, T., Steinwandt, R. (eds.): PQCrypto 2018. LNCS, vol. 10786. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-79063-3
2. First NIST Standardization Conference, 11–13 April 2018 (2018). http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html
3. Yan, S.Y.: Quantum Computational Number Theory, p. 252. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25823-2
4. Yan, S.Y.: Quantum Attacks on Public-Key Cryptosystems, p. 207. Springer, Cham (2013). https://doi.org/10.1007/978-1-4419-7722-9
5. Moldovyan, D.N.: Non-commutative finite groups as primitive of public-key cryptoschemes. Quasigroups Relat. Syst. **18**(2), 165–176 (2010)
6. Kuzmin, A.S., Markov, V.T., Mikhalev, A.A., Mikhalev, A.V., Nechaev, A.A.: Cryptographic algorithms on groups and algebras. J. Math. Sci. **223**(5), 629–641 (2017)
7. Moldovyan, D.N., Moldovyan, N.A.: Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. Quasigroups Relat. Syst. **18**(2), 177–186 (2010)
8. Hellman, M.E., Pohlig, S.C.: Exponentiation cryptographic apparatus and method. U.S. Patent # 4,424,414. (1984)
9. Menezes, A.J., Oorschot, P.C., Vanstone, S.A.: Applied Cryptography. CRC Press, New York (1996)
10. Nguyen, D.M., Kim, S.: Multi-bits transfer based on the quantum three-stage protocol with quantum error correction codes. Int. J. Theor. Phys. **58**(6), 2043–2053 (2019)
11. Moldovyan, N.A., Moldovyan, D.N., Le, Q.M., Nguyen, L.G., Ho, S.T., Nguyen, H.M.: Stream pseudo-probabilistic ciphers. In: Cong Vinh, P., Alagar, V. (eds.) ICCASA/ICTCC - 2018. LNICST, vol. 266, pp. 36–47. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-06152-4_4
12. Moldovyan, N.A., Moldovyan, A.A., Nguyen, N.H., Tran, M.C., Nguyen, H.M.: Pseudo-probabilistic block ciphers and their randomization. J. Ambient Intell. Hum. Comput. **10**(5), 1977–1984 (2019)