Post-quantum Commutative Deniable Encryption Algorithm

Nguyen Hieu Minh, Dmitriy Nikolaevich Moldovyan,
Nikolay Andreevich Moldovyan, Quang Minh Le, Sy Tan Ho,
Long Giang Nguyen, Hai Vinh Nguyen and Cong Manh Tran

Abstract There is proposed a new post-quantum commutative encryption algorithm based on the hidden discrete logarithm problem. The introduced cipher is suitable for implementing post-quantum pseudo-probabilistic deniable encryption protocol. The proposed commutative cipher belongs to the class of the algebraic ciphers. Its algebraic support represents a finite noncommutative associative algebra of special type. The used algebra is characterized in existence of a large set of the global right-sided units that are used to define the homomorphism map of the algebra and then to define the hidden discrete logarithm problem using the mutual commutativity of the homomorphism-map operation and the exponentiation operation. The proposed commutative cipher is the first implementation of the post-quantum commutative ciphers based on the hidden discrete logarithm problem defined in a finite algebra that contains no two-sided global unit.

Keywords Commutative cipher · Deniable encryption · Hidden discrete logarithm problem · No-key encryption protocol · Post-quantum commutative encryption · Pseudo-probabilistic commutative encryption

N. H. Minh (✉) · S. T. Ho
Academy of Cryptography Techniques, Hanoi, Vietnam
e-mail: hieuminhmta@gmail.com

D. N. Moldovyan · N. A. Moldovyan
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg 199178, Russia

Q. M. Le
The Information Technology Institute (ITI), Vietnam National University, Hanoi, Vietnam

L. G. Nguyen
Institute of Information Technology, Vietnam Academy of Science and Technology, Hanoi, Vietnam

H. V. Nguyen
VNU University of Science, Hanoi, Vietnam

C. M. Tran
Le Qui Don Technical University, Hanoi, Vietnam

V. K. Solanki et al. (eds.), *Intelligent Computing in Engineering*,
Advances in Intelligent Systems and Computing 1125,
https://doi.org/10.1007/978-981-15-2780-7_104

1 Introduction

Commutative encryption algorithms (called also commutative ciphers) represent significant practical interest for application in the case of passive potential attacks, since they can be put into the base of the so-called no-key encryption protocols that provide possibility of secure transmission of secret messages via public channels without using public and secret keys shared by the parties of communication session.

In order to provide resistance of the no-key encryption protocol to passive attacks it should be based on a commutative cipher that is resistant to the known plaintext attack. The exponentiation cipher by Pohlig-Hellman [1] represents an example of commutative encryption algorithms that satisfies the indicated requirement. The problem of providing resistance of the no-key encryption protocols to the coercive attacks was discussed in papers [2, 3]. To provide resistance to attacks of such type it had been proposed to include in the no-key encryption protocols procedures of the pseudo-probabilistic encryption [4].

The notion of the pseudo-probabilistic ciphering relates to implementing the shared-key deniable encryption [5]. The deniable encryption is a method for providing resistance of the public-key and shared-key encryption protocols to coercive attacks [2], i.e., to attacks from the part of some coercive adversary (coercer) that has power to force a party of the communication protocol or the both parties simultaneously to open the encryption key and the source text after the ciphertext has been sent via a public channel.

The public-key deniable encryption protocols [3, 6] represent significant practical interest as a method for preventing vote-buying in the internet-voting systems [7] and a method for providing secure multiparty computations [8]. The recent paper [9] initiated the development of the pseudo-probabilistic encryption as a particular form of the shared-key deniable encryption which is oriented to application as an individual method for providing the information protection in communication and computer systems. The concept of the pseudo-probabilistic encryption is considered in detail in the papers [9]. The design of fast block pseudo-probabilistic ciphers had been introduced in [10]. The design of the synchronous stream pseudo-probabilistic ciphers was considered in the papers [11].

For the first time the design of the pseudo-probabilistic no-key encryption protocol was proposed in [12]. That protocol uses the Pohlig-Hellman exponentiation cipher based on the computational difficulty of the discrete logarithm problem (DLP) to perform the procedure of commutative encryption. The DLP in any evidently defined cyclic group can be solved on a quantum computer in polynomial time due to the Short algorithm [13]. Therefore, the pseudo-probabilistic no-key encryption protocols [4, 12] is not secure to quantum attacks. Taking into account that currently the development of the post-quantum cryptographic algorithms and protocols is considered as a challenge in the area of computer security and cryptography [14, 15] one can conclude that the design of the post-quantum versions of the commutative ciphers, no-key encryption protocols, and pseudo-probabilistic no-key protocols represents significant practical and theoretic interest. In the frame of this task, the core item relates to the design of the post-quantum commutative encryption algorithm, i.e., the commutative cipher that runs efficiently on ordinary computers and are resistant to attacks using the quantum computers. For the first time, the post-quantum commutative ciphers had been proposed in [16] using the so-called hidden DLP (HDLP) defined in the finite algebra of quaternions. However, a method for reducing the HDLP in the finite algebra of quaternions to the ordinary DLP in a finite field was proposed in [17]. The last means that the problem of designing the post-quantum commutative ciphers is open.

This paper introduces the design of the post-quantum commutative encryption algorithms based on the HDLP set in a new form in the finite noncommutative associative algebra (FNAA) that contains no global two-sided unit. Due to using the algebraic support of a new type the quantum attacks based on the method [17] for reduction of the HDLP to the DLP are prevented. Thus, the proposed commutative cipher is a candidate for post-quantum commutative encryption algorithms. It has been used to develop a post-quantum no-key protocol. A post-quantum pseudo-probabilistic commutative encryption cipher has been also proposed.

This paper is organized as follows. Section 2 describes the algebraic support of the proposed post-quantum commutative cipher. Section 3 introduces the HDLP used as the base primitive and the proposed post-quantum commutative encryption algorithm. Section 4 presents the proposed post-quantum no-key encryption protocol. Section 5 describes the pseudo-probabilistic no-key encryption protocol. Final remarks are presented in the concluding Sect. 6.

2 The Used Algebraic Support

Suppose a finite m-dimensional vector space is defined over the ground finite field $GF(p)$, in which the addition operation and operation of the multiplying vectors by the scalars (elements of the base finite field). Then defining additionally the vector multiplication operation that is distributive relatively the addition operation one gets the finite m-dimensional algebra. The additional operation for multiplying arbitrary two vectors, which is distributive relatively the addition operation, is usually defined as follows. Suppose the set $\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{m-1}\}$ represents the base of the vector space, i.e., $\mathbf{e}_0$, $\mathbf{e}_1$, …, $\mathbf{e}_{m-1}$ are the basis vectors. Some m-dimensional vector A is usually 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 $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are coordinates of the vector A.

The multiplication operation of two vectors $A = \sum_{i=0}^{m-1} a_i \mathrm{e}_i$ and $B = \sum_{j=0}^{m-1} b_j \mathrm{e}_j$ is defined with the following 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 every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ of basis vectors is to be replaced by a single-component vector indicated in the so-called basis vector multiplication table (BVMT) that is composed as follows. Every cell of the BVMT contains some single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$ is called structural constant. If $\lambda = 1$, then in the respective cell its content is denoted as $\mathbf{e}_k$. Usually it is assumed the left operand $\mathbf{e}_i$ defines the row and the right operand $\mathbf{e}_j$ defines the column of the BVMT. The intersection of the ith row and jth column indicates the cell containing the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$.

For defining the HDLP one should use the BVMTs that define the vector multiplication operation possessing the properties of the noncommutativity and associativity. The multiplication operation is associative if for arbitrary three vectors A, B, and $C = \sum_{k=0}^{m-1} c_k \mathrm{e}_k$ the following condition holds true:

$$(A \circ B) \circ C = \sum_{i,j,k=0}^{m-1} a_i b_j c_k \left(\mathrm{e}_i \circ \mathrm{e}_j\right) \circ \mathrm{e}_k; \quad A \circ (B \circ C) = \sum_{i,j,k=0}^{m-1} a_i b_j c_k \mathrm{e}_i \circ \left(\mathrm{e}_j \circ \mathrm{e}_k\right).$$

Evidently, if the condition $\left(\mathbf{e}_i \circ \mathbf{e}_j\right) \circ \mathbf{e}_k = \mathbf{e}_i \circ \left(\mathbf{e}_j \circ \mathbf{e}_k\right)$ holds true for all possible triples of the indices (i, j, k), then the vector multiplication operation is associative. Examples of the BVMT defining the noncommutative and associative vector multiplication for different values of the dimension are presented in papers [18–20]. The dimension value should not be large to provide faster computations and higher performance of the designed encryption algorithm. In this paper we use the value $m = 4$ and the BVMT shown as Table 1, which define the noncommutative and associative vector multiplication, i.e., the finite noncommutative associative algebra (FNAA). The used FNAA defined over the field $GF(p)$ is characterized in that it contains p^2 different global left-sided units (the term "global" means that every of these units acts as a left-sided unit on all elements of the algebra).

To derive the formula describing the set of the global left-sided units one should consider the 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 system of four linear equations:

Table 1 The BVMT defining the 4-dimensional FNAA (where the structural coefficient λ is equal to a non-residue in $GF(p)$)

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

$$\begin{cases} (x_1 + x_2)a_0 + (x_0 + x_3)a_2 = a_0; \\ (x_1 + x_2)a_1 + \lambda(x_0 + x_3)a_3 = a_1; \\ (x_1 + x_2)a_2 + \lambda(x_0 + x_3)a_0 = a_2; \\ (x_1 + x_2)a_3 + (x_0 + x_3)a_1 = a_3. \end{cases}, \tag{2}$$

Performing the variable substitution $u_1 = x_1 + x_2$ and $u_2 = x_0 + x_3$ one can represent the system (2) in the following form of two independent systems of two equations:

$$\begin{cases} a_0u_1 + a_2u_2 = a_0; \\ a_2u_1 + \lambda a_0u_2 = a_2; \end{cases}, \tag{3}$$

$$\begin{cases} a_1u_1 + \lambda a_3u_2 = a_1; \\ a_3u_1 + a_1u_2 = a_3. \end{cases}, \tag{4}$$

It is easy to see that the solution $u_1 = 1$ and $u_2 = 0$ satisfies both the system (3) and the system (4) for all possible values A. Performing the inverse substitution we get the following formula that describes all p^2 global left-sided units in the considered 4-dimensional FNAA:

$$L = (l_0,\ l_1,\ l_2,\ l_3) = (h,\ k,\ 1 - k,\ -h), \tag{5}$$

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

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

$$A \circ X = A \tag{6}$$

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

$$\begin{cases} (a_1 + a_2)x_0 + (a_0 + a_3)x_3 = a_0; \\ \lambda(a_0 + a_3)x_0 + (a_1 + a_2)x_3 = a_2; \end{cases}, \tag{7}$$

$$\begin{cases} (a_1 + a_2)x_1 + \lambda(a_0 + a_3)x_3 = a_1; \\ (a_0 + a_3)x_1 + (a_1 + a_2)x_3 = a_3. \end{cases}, \tag{8}$$

The main determinant of each of the systems (7) and (8) is the same and equal to

$$\Delta_A = (a_1 + a_2)^2 - \lambda(a_0 + a_3)^2. \tag{9}$$

The algebra contains only p^2 different vectors A for which we have $\Delta_A = 0$. Such vectors we will denote as A' and call them “marginal”, since they will not be used in the developed encryption algorithm. Suppose $\{A'\}$ denotes the set of all “marginal” vectors. One can easily prove the following propositions:

Proposition 1 If $A \notin \{A'\}$, then to the vector A relates the single local right-sided unit R_A.

Proposition 2 Suppose $A \notin \{A'\}$. Then the local right-sided unit R_A is contained in the set (5) of the global left-sided units.

Proposition 3 If $A \notin \{A'\}$, then to the vector A relates the single local two-sided unit E_A and $E_A = R_A$.

Proposition 4 If $A \notin \{A'\}$, then local two-sided unit E_A and local right-sided unit R_A act as local units on the vectors A^k for arbitrary natural values k.

Proposition 5 If $A \notin \{A'\}$, then for some minimum nonnegative integer $\omega$the condition $A^{\omega} = E_A$ holds true. (Such value ω is called local order of the vector A.)

Thus, the non-"marginal" vectors $A \notin \{A'\}$ which satisfy condition $\Delta_A \notin 0$ are generators of some cyclic groups $\{A, A^2, \ldots, A^i, \ldots, A^{\omega}\}$ of the order ω. Evidently, every vector A is invertible in the indicated cyclic group. Such vectors A will be called locally invertible.

3 The Hidden Discrete Logarithm Problem and Commutative Cipher on Its Base

The known form of the HDLP is defined if the multiplicative group Γ of the finite algebra of quaternions as follows [16]. Suppose the elements $G \in \Gamma$ and $Q \in \Gamma$ are the group elements of sufficiently large prime order q and they satisfy the condition $Q \circ G \neq G \circ Q$. To compute a public key one should generate two random nonnegative integers $x < q$ and $w < q$ as his private key and computes his public key in the form of the group element Y:

$$Y = Q^w \circ G^x \circ Q^{-w}. \tag{10}$$

Finding the values x and Q^w (or x and w) from the Eq. (10) is called the HDLP. The exponentiation operation G^x introduces the main contribution to the computational difficulty of the HDLP. The left-sided multiplication by the element Q^w and the right-sided multiplication by the element Q^{-w} are used as mechanism of masking the value G^x.

In the definition of a new form of the HDLP in the FNAA described in the previous section there are used the following propositions:

Proposition 6 Suppose $A \circ B = L$, where L is a global left-sided unit. Then for arbitrary natural number t the equality $A^t \circ B^t = L$ holds true.

Proof

$$\begin{aligned} A' \circ B' &= A^{-1}\mathrm{O}(A \circ B) \circ B^{-1} = A^{-1} \circ L \circ B^{-1} = A^{-1} \circ B^{-1} = A^{-2} \circ (A \circ B) \circ B'^{-2} \\ &= A^{t-2} \circ L \circ B^{t-2} = A^{t-2} \circ B^{t-2} = \ldots = A \circ B = L. \end{aligned}$$

The Proposition 6 is proven.

Proposition 7 Suppose $A \circ B = L$ and t is an arbitrary natural number. 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 a homomorphism map.

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

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

The Proposition 7 is proven.

Proposition 8 The homomorphism-map operation $\psi_L = B \circ X \circ A$ 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 7 we have $\psi_L(X^i) = (\psi_L(X))^i$, i.e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The Proposition 8 is proven.

To define commutative encryption algorithm based on performing computations in the 4-dimensional FNAA introduced in Sect. 2 one should set the method for mapping a message M into a 4-dimensional vector (m_0, m_1, m_2, m_3) with coordinates $m_i < p$, where $i = 0, 1, 2, 3$ and p is a 512-bit prime such that $p = 2q + 1$, where q is a prime. We define that encryption algorithm will process 500-bit messages M' divided into four data blocks M_0, M_1, M_2, and M_3, where the first three blocks have size equal to 128 bits and the fourth block M_3 has size equal to 116 bits. Besides, to the data block M_3 a 12-bit random binary number ρ is concatenated. Then the message is considered as the four-dimensional vector $M = (m_0, m_1, m_2, m_3)$, where $m_0 = M_0$, $m_1 = M_1$, $m_2 = M_2$, and $m_3 = M_3 \| \rho$.

Suppose the vector A such that $\Delta_A \neq 0$ is invertible and has order equal to $2q$ and L is a randomly selected global left-sided unit. Then solving the equation

$$A \circ B = L \tag{11}$$

one computes the vector B. The values, A, B, and L will be used as common parameters of the commutative encryption algorithm. The secret encryption key represents a triple of random natural numbers (e, d, t) such that $e < q$, $t < q$ and $d = e^{-1} \bmod q$. The procedure of encrypting a 500-bit message M' is performed as follows:

1. Select a random 12-bit string ρ such that the message M' is mapped into the 4-dimensional vector M satisfying the conditions $A \circ M \neq M \circ A$ and $\Delta_M = (m_1 + m_2)^2 - \lambda(m_0 + m_3)^2 \neq 0$.
2. Solving the vector Eq. (6) written for the vector M compute the local two-sided unit $E_M = R_M$ relating to M. The vector R_M is the first part of the ciphertext.
3. Compute the second part C of the ciphertext: $C = B^t \circ M^e \circ A^t$.

The produced ciphertext represents the pair of the vectors (R_M, C).

The decryption of the ciphertext (R_M, C) is performed as follows:

1. Compute the vector N: $N = A^t \circ C^d \circ B^t$.
2. Compute the vector $M^* = N \circ R_M$.

Correctness proof of the encryption scheme is as follows:

$$\begin{aligned} M^* &= N \circ R_M = A^t \circ C^d \circ B^t \circ R_M = A^t \circ \left(B^t \circ M^e \circ A^t\right)^d \circ B^t \circ R_M \\ &= A^t \circ \left(B^t \circ M^{ed} \circ A^t\right) \circ B^t \circ R_M = A^t \circ B^t \circ M^{ed} \circ A^t \circ B^t \circ R_M \\ &= L \circ M \circ L \circ R_M = M \circ R_M = M. \end{aligned}$$

When performing encryption on two different keys (e_1, d_1, t_1) and (e_2, d_2, t_2), the first element of the ciphertext is computed only once, namely, at moment of the first encryption procedure:

1. Using the key (e_1, d_1, t_1) compute the ciphertext (R_M, C_1), where $C_1 = B^{t_1} \circ M^{e_1} \circ A^{t_1}$.
2. Using the key (e_2, d_2, t_2) compute the ciphertext (R_M, C_{12}), where

$$\begin{aligned} C_{12} &= B^{t_2} \circ C_1^{e_2} \circ A^{t_2} = B^{t_2} \circ \left(B^{t_1} \circ M^{e_1} \circ A^{t_1}\right)^{e_2} \circ A^{t_2} \\ &= B^{t_2} \circ B^{t_1} \circ M^{e_1 e_2} \circ A^{t_1} \circ A^{t_2} = B^{t_2 + t_1} \circ M^{e_1 e_2} \circ A^{t_1 + t_2}. \end{aligned}$$

Double encryption with using the keys in other order gives:

1. Using the key (e_2, d_2, t_2) compute the ciphertext (R_M, C_2), where $C_2 = B^{t_2} \circ M^{e_2} \circ A^{t_2}$.
2. Using the key (e_1, d_1, t_1) compute the ciphertext (R_M, C_{21}), where

$$
\begin{aligned}
C_{21} &= B^{t_1} \circ C_2^{e_1} \circ A^{t_1} = B^{t_1} \circ \left(B^{t_2} \circ M^{e_2} \circ A^{t_2}\right)^{e_1} \circ A^{t_1} \\
&= B^{t_1} \circ B^{t_2} \circ M^{e_2 e_1} \circ A^{t_2} \circ A^{t_1} = B^{t_1 + t_2} \circ M^{e_1 e_2} \circ A^{t_2 + t_1} = C_{12}.
\end{aligned}
$$

Thus, the double encryption outputs the ciphertext $(R_M, C_{21}) = (R_M, C_{12})$, i.e., the encryption algorithm possesses property of commutativity.

4 Post-quantum No-key Encryption Protocol

No-key encryption 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. The encryption function is called commutative, if the following equality holds:

$$
E_{K_{\mathrm{A}}}\left(E_{K_{\mathrm{B}}}(M)\right) = E_{K_{\mathrm{B}}}\left(E_{K_{\mathrm{A}}}(M)\right)
$$

where K_{A} and K_{B} ($K_{\mathrm{B}} \neq K_{\mathrm{A}}$) are different encryption keys. Shamir's no-key protocol (also called Shamir's three-pass protocol) includes the following three steps [10]:

1. The sender (Alice) of the message M generates a random key K_{A} and calculates the ciphertext $C_1 = E_{K_{\mathrm{A}}}(M)$. Then he sends C_1 to the receiver via an open channel.
2. The receiver (Bob) generates a random key K_{B}, encrypts the ciphertext C_1 with the key K_{B} as follows $C_2 = E_{K_{\mathrm{B}}}(C_1) = E_{K_{\mathrm{B}}}\left(E_{K_{\mathrm{A}}}(M)\right)$ and sends C_2 to the sender.
3. The sender, using decryption procedure $D = E^{-1}$, calculates the ciphertext $C_3 = D_{K_{\mathrm{A}}}(C_2) = D_{K_{\mathrm{A}}}\left(E_{K_{\mathrm{B}}}\left(E_{K_{\mathrm{A}}}(M)\right)\right) = D_{K_{\mathrm{A}}}\left(E_{K_{\mathrm{A}}}\left(E_{K_{\mathrm{B}}}(M)\right)\right) = E_{K_{\mathrm{B}}}(M)$ and sends C_3 to the receiver of the message M.

Using the received ciphertext C_3 the receiver recovers message M accordingly to the formula $M = D_{K_{\mathrm{B}}}(C_3) = D_{K_{\mathrm{B}}}\left(E_{K_{\mathrm{B}}}(M)\right) = M$.

In this protocol, the used keys K_{A} and K_{B} represent local parameters (local keys) of commutative transformations. Since the parties of the protocol use no pre-agreed key the protocol is called the no-key protocol. If one uses the Pohlig-Hellman exponentiation cipher [1] 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.

The post-quantum version of the no-key protocol should be based on the commutative ciphers that are resistant to quantum attacks. Using the post-quantum commutative encryption algorithm described in Sect. 3 one can propose the following post-quantum version of the no-key protocol:

1. Alice generates a random the key (e_1, d_1, t_1) and calculates the ciphertext (R_M, C_1), where $C_1 = B^{t_1} \circ M^{e_1} \circ A^{t_1}$. Then he sends (R_M, C_1) to Bob via a public channel.
2. Bob generates a random key (e_2, d_2, t_2), encrypts the ciphertext C_2 as follows $C_2 = B^{t_2} \circ C_1^{e_2} \circ A^{t_2}$ and sends C_2 to Alice.
3. Alice decrypts the ciphertext C_2 and obtains the ciphertext C_3: $C_3 = A^{t_1} \circ C_2^{e_1} \circ B^{t_1}$. Then she sends C_3 to Bob.

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

5 Post-quantum Pseudo-probabilistic Commutative Encryption Protocol

Like in the case of pseudo-probabilistic block ciphers [10], the pseudo-probabilistic commutative encryption algorithm can be constructed as some deterministic procedure of simultaneous commutative encryption of two independent messages, fake and secret messages, using two different key, the fake and secret keys. The post-quantum version of the pseudo-probabilistic commutative encryption algorithm can be designed on the base of the post-quantum commutative encryption algorithm describe in Sect. 3. Suppose the sender of the message (Alice) and the receiver (Bob) share the fake key (e, d, t, μ) and the secret key (e', d', t', μ'), where μ and μ' are mutually irreducible binary polynomials. Then the following pseudo-probabilistic commutative encryption protocol can be used to provide resistance to the coercive attacks with using quantum computers, which is implemented as process of simultaneous encryption of the fake $M = (m_0, m_1, m_2, m_3)$ and secret messages $H = (h_0, h_1, h_2, h_3)$.

1. Alice compute two intermediate ciphertexts (R_M, C_M) and (R_H, C_H), where $R_M = \left(r_{M_0}, r_{M_1}, r_{M_2}, r_{M_3}\right)$ and $R_H = \left(r_{H_0}, r_{H_1}, r_{H_2}, r_{H_3}\right)$ are local two-sided units relating to the vectors M and H correspondingly (R_M and R_H are computed as solutions of the vector Eq. (6) written for M and H);

$$C_M = \left(c_{M_0}, c_{M_1}, c_{M_2}, c_{M_3}\right) = B^t \circ M^e \circ A^t; \text{ and}$$

$$C_H = \left(c_{H_0} c_{H_1}, c_{H_2}, c_{H_3}\right) = B^{t'} \circ H^{e'} \circ A^{t'}.$$

Then she computes the values $C = (c_0, c_1, c_2, c_3)$; $R = (r_0, r_1, r_2, r_3)$; where for $i = 0, 1, 2, 3$ the values c_i, and r_i are computed as solutions of the following two systems of congruencies:

$$\begin{cases} c_i \equiv c_{M_i} \bmod \mu; \\ c_i \equiv c_{H_i} \bmod \mu'; \end{cases} \quad \begin{cases} r_i \equiv r_{M_i} \bmod \mu; \\ r_i \equiv r_{H_i} \bmod \mu'; \end{cases}$$

The computed ciphertext (R, C) is sent to Bob via a public channel.

2. To open the fake message Bob computes the values $C_M = \left(c_{M_0}, c_{M_1}, c_{M_2}, c_{M_3}\right)$, where $c_{M_i} \equiv c_i \bmod \mu$ (for $i = 0, 1, 2, 3$), and $R_M = \left(r_{M_0}, r_{M_1}, r_{M_2}, r_{M_3}\right)$, where $r_{M_i} \equiv r_i \bmod \mu$ (for $i = 0, 1, 2, 3$). Then he computes the value $M = A^t \circ C_M^d \circ B^t \circ R_M$.
3. To open the secret message Bob computes the values $C_H = \left(c_{H_0}, c_{H_1}, c_{H_2}, c_{H_3}\right)$, where $c_{H_i} \equiv c_i \bmod \mu'$ (for $i = 0, 1, 2, 3$), and $R_H = \left(r_{H_0}, r_{H_1}, r_{H_2}, r_{H_3}\right)$, where $r_{H_i} \equiv r_i \bmod \mu'$ (for $i = 0, 1, 2, 3$). Then he computes the value $H = A^{t'} \circ C_H^{d'} \circ B^{t'} \circ R_H$.

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

The described protocol is computationally indistinguishable from the following probabilistic commutative encryption protocol with the shared key (e, d, t, μ).

1. Alice computes the ciphertexts (R_M, C_M), where $R_M = \left(r_{M_0}, r_{M_1}, r_{M_2}, r_{M_3}\right)$ is the local two-sided unit relating to the vector M (R_M is computed as solutions of the vector Eq. (6) written for M);

$$C_M = \left(c_{M_0}, c_{M_1}, c_{M_2}, c_{M_3}\right) = B^t \circ M^e \circ A^t.$$

Then she generates random binary polynomial μ' (such that it is mutually prime with μ), random vectors $C_H = \left(c_{H_0}, c_{H_1}, c_{H_2}, c_{H_3}\right)$ and $R_H = \left(r_{H_0}, r_{H_1}, r_{H_2}, r_{H_3}\right)$ and computes the values $C = (c_0, c_1, c_2, c_3)$; $R = (r_0, r_1, r_2, r_3)$; where for $i = 0, 1, 2, 3$ the values c_i and r_i are computed as solutions of the following two systems of congruencies:

$$\begin{cases} c_i \equiv c_{M_i} \bmod \mu; \\ c_i \equiv c_{H_i} \bmod \mu'; \end{cases} \quad \begin{cases} r_i \equiv r_{M_i} \bmod \mu; \\ r_i \equiv r_{H_i} \bmod \mu'; \end{cases}$$

The computed ciphertext (R, C) is sent to Bob via a public channel.

2. To open the message Bob computes the values $C_M = \left(c_{M_0}, c_{M_1}, c_{M_2}, c_{M_3}\right)$, where $c_{M_i} \equiv c_i \bmod \mu$ (for $i = 0, 1, 2, 3$), and $R_M = \left(r_{M_0}, r_{M_1}, r_{M_2}, r_{M_3}\right)$, where $r_{M_i} \equiv r_i \bmod \mu$ (for $i = 0, 1, 2, 3$). Then he computes the value $M = A^t \circ C_M^d \circ B^t \circ R_M$.

6 Conclusion

The paper has introduced post-quantum commutative cipher based on the HDLP, post-quantum no-key protocol and the post-quantum pseudo-probabilistic commutative encryption protocol. The HDLP is formulated in the 4-dimensional FNAA with a large set of global left-sided units, which has been used as algebraic support of the proposed algorithm and protocols.

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

References

1. Hellman ME, Pohlig SC (1984) Exponentiation cryptographic apparatus and method. US Patent # 4,424,414
2. Canetti R, Dwork C, Naor M, Ostrovsky R (1997) Deniable encryption. In: Proceedings advances in cryptology—CRYPTO 1997 (Lecture notes in computer science). Springer, Berlin, Heidelberg, New York, pp 90–104
3. Ibrahim MH (2009) A method for obtaining deniable public-key encryption. Int J Netw Secur 8:1–9
4. Nguyen NH, Moldovyan NA, Shcherbacov AV, Nguyen HM, Nguyen DT (2018) No-key protocol for deniable encryption. In: Proceedings of the fourth international conference INDIA 2017, advances in intelligent systems and computing information systems design and intelligent applications, vol 672. Springer, Berlin, pp 96–104. https://doi.org/10.1007/978-981-10-7512-4_10
5. Moldovyan NA, Al-Majmar NA, Nguyen DT, Nguyen NH, Nguyen HM (2018) Deniability of symmetric encryption based on computational indistinguishability from probabilistic ciphering. In: Proceedings of the fourth international conference INDIA 2017, advances in intelligent systems and computing, information systems design and intelligent applications. vol 672. Springer, Singapore, pp 209–218. https://doi.org/10.1007/978-981-10-7512-4_21
6. Barakat MT (2014) A new sender-side public-key deniable encryption scheme with fast decryption. KSII Trans Internet Inf Syst 8(9):3231–3249
7. Meng B (2009) A secure internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext. J Netw 370–377
8. Ishai Y, Kushilevits E, Ostrovsky R (2011) Efficient non-interactive secure computation. Advances in cryptology—EUROCRYPT 2011. (Lecture Notes in Computer Science). Springer, Berlin, Heidelberg, New York, pp 406–425
9. Andreevich MN, Andreevich MA, Duc TN, Nam HN, Hieu MN (2018) Method for pseudo-probabilistic block encryption. In: Proceedings of the conference INISCOM 2017/industrial networks and intelligent systems, Springer International Publishing. https://doi.org/10.1007/978-3-319-74176-5_28
10. Moldovyan NA, Moldovyan AA, Duc TN, Nam HN, Hieu MN (2018) Pseudo-probabilistic block ciphers and their randomization. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-018-0791-6
11. Moldovyan NA, Moldovyan AA, Moldovyan DN, Shcherbacov VA (2016) Stream deniable-encryption algorithms. Comput Sci J Moldova 24(70):68–82

12. Moldovyan NA, Shcherbacov AV, Eremeev MA (2017) Deniable-encryption protocols based on commutative ciphers. Quasigroups Relat Syst 25(1):95–108
13. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM J Comput 26:1484–1509
14. Post-quantum Cryptography (2018) Proceedings 9th international conference on PQCrypto 2018, Fort Lauderdale, FL, USA, Lecture Notes in Computer Science, vol 10786, Springer, Berlin
15. First NIST standardization conference—April 11–13, 2018 (2018). http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html
16. Moldovyan DN (2010) Non-commutative finite groups as primitive of public-key cryptoschemes. Quasigroups Relat Syst 18(2):165–176
17. Kuzmin AS, Markov VT, Mikhalev AA, Mikhalev AV, Nechaev AA (2017) Cryptographic algorithms on groups and algebras. J Math Sci 223(5):629–641
18. Moldovyan AA, Moldovyan NA (2019) Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. Bull South Ural State Univ Ser Math Model Program Comput Softw (Bulletin SUSU MMCS) 12(1):66–81
19. Moldovyan AA, Moldovyan NA (2018) Post-quantum signature algorithms based on the hidden discrete logarithm problem. Comput Sci J Moldova 26(78):301–313
20. Moldovyan NA (2018) Unified method for defining finite associative algebras of arbitrary even dimensions. Quasigroup Relat Syst 26(2):263–270