Algebraic Supports and New Forms of the Hidden Discrete Logarithm Problem for Post-quantum Public-key Cryptoschemes

Dmitriy Moldovyan[1], Nashwan Al-Majmar[2], and Alexander Moldovyan[1]
[1]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia
[2]Computer Sciences and Information Technology Department, Ibb University, Yemen

Abstract: *This paper introduces two new forms of the hidden discrete logarithm problem defined over a finite non-commutative associative algebras containing a large set of global single-sided units. The proposed forms are promising for development on their base practical post-quantum public key-agreement schemes and are characterized in performing two different masking operations over the output value of the base exponentiation operation that is executed in framework of the public key computation. The masking operations represent homomorphisms and each of them is mutually commutative with the exponentiation operation. Parameters of the masking operations are used as private key elements. A 6-dimensional algebra containing a set of p^3 global left-sided units is used as algebraic support of one of the hidden logarithm problem form and a 4-dimensional algebra with p^2 global right-sided units is used to implement the other form of the said problem. The result of this paper is the proposed two methods for strengthened masking of the exponentiation operation and two new post-quantum public key-agreement cryptoschemes.*
Mathematics subject classification: 94A60, 16Z05, 14G50, 11T71, 16S50.

Keywords: *Finite associative algebra, non-commutative algebra, right-sided unit, left-sided unit, global units, discrete logarithm problem, post-quantum cryptography, public key-agreement.*

Received December 23, 2019; accepted November 24, 2020
https://doi.org/10.34028/iajit/18/3/14

1. Introduction

Development of the practical post-quantum public-key cryptoschemes is considered by the cryptographic community as a current challenge in the area of theoretic and applied cryptography [1, 8]. A crypto-scheme is called post-quantum, if it runs efficiently on classical computers but will resist quantum attacks, performed with using hypothetic quantum computers. Post-quantum crypto-schemes should not be based on the factorization problem nor on the Discrete Logarithm Problem (DLP) [10], since both of the latter two computational problems can be solved by a quantum computer in polynomial time [20, 21].

The Public Key-Agreement (PKA) schemes Classic McEliece, CRYSTALS-KYBER, NTRU, and SABER considered currently as candidates for a post-quantum PKA standard [19] resist well quantum attacks, however, they are not very practical because of very large size of the public and secret key (700 to 3000 bytes).

The Hidden DLP (HDLP) is very attractive as the base primitive of the practical post-quantum cryptoschemes with relatively small size of public and secret keys [12, 14]. However, the first implementation of a HDLP-based PKA scheme was not successful and an efficient attack was proposed in [7].

Estimation of potentiality of the HDLP as post-quantum cryptographic primitive is connected with developing new forms of the HDLP and with the search for new NFAAs as their algebraic supports [7].

In this paper, we introduce two new forms of HDLP, suitable to design post-quantum PKA schemes with small enough size of public and secret keys. New types of algebraic supports, namely, the NFAAs containing a large set of the global left-sided units (called algebras of *L*-type) and the NFAA containing the right-sided units (called algebras of *R*-type), are applied as algebraic supports of the proposed forms of the HDLP, each of which resists attack [7] due to performing two different masking operations instead of one in the known versions of the HDLP used earlier to develop PKA schemes.

2. State of the art of the HDLP-based PKA Schemes

2.1. Notion of Hidden Logarithm Problem

The DLP is defined in a finite cyclic group as follows:

$Y = G^x$; where G is a generator of the group and the value x is an 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 [14, 15] or both of them [11, 16] are masked.

Masking is possible if the considered cyclic group is contained in some other set of algebraic elements, which contains many different cyclic groups as its subsets. Non-commutative Finite Associative Algebras (NFAAs) represent significant practical interest as algebraic supports of the HDLP [17]. Different types of the NFAAs are used to define different forms of the HDLP [13, 18].

Initially the HDLP was defined in the finite algebra of quaternions and applied to design a Public Key-Agreement (PKA) scheme [12, 14]. Reducibility of the first form of the HDLP to the DLP in a finite field was shown in the paper [7], where the search for new algebraic supports of the HDLP has been recommended as a next stage in the direction of post-quantum public-key cryptoschemes development, based on a computational difficulty of the HDLP. Recently, several new NFAAs and new forms of the HDLP were introduced and used as the base primitive of post-quantum digital signature protocols [11, 16].

However, that forms of the HDLP are not suitable for developing the PKA. Development of new forms of the HDLP suitable for developing the HDLP-base PKA schemes is a task of practical interest. In present paper we propose two new forms of the HDLP and develop on their base PKA schemes. For the first time two masking operations are used to set the HDLP forms suitable for developing the PKA schemes.

2.2. The NFAAs of the *L*-Type and *R*-Type

A finite *m*-dimensional vector space defined over the field $GF(p)$ can be complemented with an additional operation, namely, with the vector multiplication that is distributive relatively the addition operation. A finite vector space complemented with the said multiplication operation is called finite algebra. If the multiplication operation (denoted as $\circ$) is non-commutative and associative, then the algebra is a NFAA. A vector A can be denoted in the following two forms: $A=(a_0, a_1, ..., a_{m-1})$ and $A=a_0e_0+a_1e_1+...,a_{m-1}e_{m-1})$; where $e_0, e_1, ..., e_{m-1}$ are the basis vectors and $a_0, a_1, \ldots, a_{m-1} \in GF(p)$.

Usually the multiplication operation of two vectors A and $B=\sum_{i=0}^{m-1} b_i e_i$, is defined by the formula [13, 15]: $A \circ B = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} a_i b_j (e_i \circ e_j)$, in which products of different pairs of basis vectors $e_i \circ e_j$ are 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 λe_k, where $\lambda \in GF(p)$ is called structural coefficient.

If $\lambda = 1$, then the content of the cell is denoted as e_k. One usually assumes that the left operand e_i defines the row and the right one e_j defines the column. The intersection of the *i*-th row and *j*-th column defines the cell indicating the value of the product $e_i \circ e_j$.

Table 1 defines the 6-dimensional *L*-type NFAA, containing p^3 of different global left-sided units described by the following formula [16]:

$$L=\left(d, h, k, \frac{1-\mu d}{\tau}, -\frac{\tau h}{\mu}, -\frac{\mu k}{\tau}\right) \quad (1)$$

Where $d, h, k=0,1,...p-1$. Every unit of set (1) acts as a left-sided unit on all vectors in the considered NFAA, i.e., equality $A \circ L = A$ holds true for all vectors A. The algebra contains no global right-sided unit nor global right-sided one. However, for a fixed set of algebra elements there exists an element acting as a right-sided unit. The latter is called a local right-sided unit. Generally, different right-sided units act in different subsets of algebraic elements.

Consider a vector $A = (a_0, a_1, a_2, a_3, a_4, a_5)$. A right-sided unit can be calculated from the following vector equation with the unknown value $R = (r_0, r_1, r_2, r_3, r_4, r_5)$:

$$A \circ R = A \quad (2)$$

Table 1. The BVMT setting a 6-dimensional NFAA containing p^3 different global left-sided units [16].

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	μe_0	μe_1	μe_2	μe_3	μe_4	μe_5
e_1	τe_4	τe_5	τe_0	τe_1	τe_2	τe_3
e_2	μe_2	μe_3	μe_4	μe_5	μe_0	μe_1
e_3	τe_0	τe_1	τe_2	τe_3	τe_4	τe_5
e_4	μe_4	μe_5	μe_0	μe_1	μe_2	μe_3
e_5	τe_2	τe_3	τe_4	τe_5	τe_0	τe_1

Using Table 1, one can reduce the Equation (2) to the following system of six linear equations with the unknowns $r_0, r_1, r_2, r_3, r_4, r_5 \in GF(p)$ [16]:

$$\begin{cases} \mu a_0 r_0 + \tau a_1 r_2 + \mu a_2 r_4 + \tau a_3 r_0 + \mu a_4 r_2 + \tau a_5 r_4 = a_0 \\ \mu a_0 r_1 + \tau a_1 r_3 + \mu a_2 r_5 + \tau a_3 r_1 + \mu a_4 r_3 + \tau a_5 r_5 = a_1 \\ \mu a_0 r_2 + \tau a_1 r_2 + \mu a_2 r_0 + \tau a_3 r_2 + \mu a_4 r_4 + \tau a_5 r_0 = a_2 \\ \mu a_0 r_3 + \tau a_1 r_2 + \mu a_2 r_1 + \tau a_3 r_3 + \mu a_4 r_5 + \tau a_5 r_1 = a_3 \\ \mu a_0 r_4 + \tau a_1 r_2 + \mu a_2 r_2 + \tau a_3 r_4 + \mu a_4 r_0 + \tau a_5 r_2 = a_4 \\ \mu a_0 r_5 + \tau a_1 r_2 + \mu a_2 r_3 + \tau a_3 r_5 + \mu a_4 r_1 + \tau a_5 r_3 = a_5 \end{cases} \quad (3)$$

If vector A is such that the main determinant of the system (3) Δ_A satisfies the condition:

$$\Delta_A \neq 0, \quad (4)$$

Then the system (3) has a unique solution κ_A. Evidently, for all integer values i the following equality $A^i \circ R_A = A^i$ holds true. It is easy to show

that for a vector A satisfying the condition (4) the sequence A, A^2 ...A^i,... is periodic and for some integer w we have $A^w = R_A$ and $R_A \circ A = A$, like in NFAA considered in [15], i.e., the unit element R_A is a two-sided unit $E_A = R_A$ One can easily see that all possible integer powers of the vector A compose a multiplicative cyclic group with the unit element E_A, like in [18]. Since the vector A is invertible in the mentioned cyclic group, it is called locally invertible [18]. It is also easy to show that the value E_A is contained in set (1) [16].

Table 2. The BVMT setting a 4-dimensional NFAA containing p^2 global right-sided units [16].

$\circ$	e_0	e_1	e_2	e_3
e_0	μe_2	e_0	e_0	μe_2
e_1	e_3	e_1	e_1	e_3
e_2	e_0	e_2	e_2	e_0
e_3	μe_1	e_3	e_3	μe_1

An algebra containing a set of global right-sided (left-sided) units is called *R*-type (*L*-type) algebra. Table 2 defines the 4-dimensional *R*-type NFAA, containing P^2 of different global right-sided units described by the following formula [16]:

$$R = (d, h, 1-h, -d), \quad (5)$$

Where d,h=0,1,...p-1. Every unit from the set (5) acts as a right-sided unit on all 4-dimensional vectors. The considered 4-dimensional algebra contains no global left-sided unit no global two-sided one. In some subsets of algebra elements some of vectors L act as local left-sided units that can be calculated from the following vector equation, where vector $L = (l_0, l_1, l_2, l_3)$ is unknown:

$$L \circ A = A \quad (6)$$

Consider a vector $A = (a_0, a_1, a_2, a_3)$ the coordinates of which satisfy the following condition [16]:

$$(a_1 + a_2)^2 - \mu(a_0 + a_3)^2 \neq 0 \quad (7)$$

In this case the vector Equation (6) has unique solution L_A which represents the single local two-sided unit, relating to the vector A and to all integer powers A^i. One can easily demonstrate that L_A is contained in the set of the global right-sided units (5), therefore, L_A is a local two-sided unit E_A, relating to the vectors A^i , i.e., $E_A = L_A$ The value E_A is the unit element of the multiplicative cyclic group generated by the vector A, which is a subset of elements of the considered 4-dimensional NFAA.

2.3. The known forms of the HDLP Suitable for Designing the PKA Schemes

For the first time, the HDLP was defined in multiplicative group Γ of the finite algebra of quaternions in the form described by the following formula [12, 14]:

$$Y = G^{\omega} \circ Q^{x} \circ G^{-\omega}, \quad (8)$$

Where the known values Y (the public key), G, and Q are elements of the group Γ and have order equal to a prime number of sufficiently large size; the unknown natural numbers w and x represent the private key.

Another form of the HDLP was defined in the *L*-type NFAA and was described by the following formula [14] for computation of the public key Y:

$$Y = B^{t} \circ N^{x} \circ A^{t} = (B^{t} \circ N^{x} \circ A^{t})^{x}, \quad (9)$$

Where the vectors N, A, and B are such that the following conditions $\Delta_N \neq 0$, $\Delta_A \neq 0$, $A \circ N \neq N \circ A$, and $A \circ B = L$ hold true; besides the local order of the vector N contains a prime divisor having a fairly large size. Finding the values x and t, when all other values in the Equation (9) are known, represent the HDLP.

The described two forms of the HDLP suit well to design the PKA schemes, but they do not suit well to be used as the base primitive of the signature schemes. Several different forms of the HDLP and new NFAAs, including the algebras containing a large set of the global single-sided units, have been proposed and used to design the post-quantum signature protocols in [11, 18].

However, the HDLP forms introduced in [11, 18] are not suitable for designing the PKA schemes. Section 4 presents two new forms of the HDLP used for development of the PKA schemes. Next section 3 describes the homomorphisms used to set the masking operations.

3. Homomorphisms of the *L*-type and *R*-Type

In the NFAAs containing a set of global left-sided units there is a particular type homomorphism.

- *Proposition* 1. Suppose the vector L is a global left-sided unit. Then the map of the *L*-type NFAA defined by the formula $\varphi_L(X) = X \circ L$, where the vector X takes on all values in algebra, is a homomorphism.
  - *Proof*. For two arbitrary vectors X_1 and X_2, one can get the following:

$\varphi_L(X_1 \circ X_2) = (X_1 \circ X_2) \circ L = (X_1 \circ L) \circ (X_2 \circ L) = \varphi_L(X_1) \circ \varphi_L(X_2)$,
$\varphi_L(X_1 + X_2) = (X_1 + X_2) \circ L = X_1 \circ L + X_2 \circ L = \varphi_L(X_1) + \varphi_L(X_2)$

The Proposition 1 is proven. The φ_L map is called the *L*-type homomorphism.

- *Proposition* 2. Suppose a homomorphism-map operation of the *L*-type $\varphi_L(X) = X \circ L$, where *L* is a global left-sided unit, is given. Then for an arbitrary integer i the exponentiation operation X^i and the φ_L operation are mutually commutative, i. e., the equality $X^i \circ L = (X \circ L)^i$ holds true.
  - *Proof.* Due to Proposition 1 we have $\varphi_L(X^i) = (\varphi_L(X))^i$, i. e., $X^i \circ L = (X \circ L)^i$. The Proposition 2 is proven.
- *Proposition* 3. Suppose the vector *N* satisfies the condition $\Delta_N \neq 0$. Then the non-equality $N \circ L_i \neq N \circ L_j$ holds true for arbitrary two global left-sided units L_i and L_j that satisfy the condition $L_j \neq L_i$.
  - *Proof.* Suppose $N \circ L_i = N \circ L_i$, then $N \circ (L_i - L_i) = 0$, where $0 = (0,0,...,0)$ is zero vector. Since $\Delta_N \neq 0$, the equation $N \circ X = 0$ has unique solution $X = 0$. Therefore, we have $L_i - L_j = O \Rightarrow L_i = L_j$. The obtained contradiction proves the proposition 3.
- *Proposition* 4. Suppose $\{L\}$ is the set of global left-sided units and the vector equation $X \circ W = Z$, where *Z* is a non-zero vector, has a solution $X = S$. Then $\#\{L\}$ different values $X_i = S \circ L_i$, where L_i takes on all values from the set $\{L\}$, also are solutions for the given equation.
  - *Proof.* Due to associativity property of the multiplication operation we have $(S \circ L_i) \circ W = S \circ (L_i \circ W) = S \circ W = Z$. Thus, the proposition 4 is proven.

For example, in the case of the 6-dimensional NFAA algebra described in subsection 2.1. an equation like $X \circ W = Z$ has p^3 different solutions.

In the NFAAs containing a set of the global right-sided units one can define the *R*-type homomorphisms as in the following proposition.

- *Proposition* 5. Suppose the vector *R* is a global right-sided unit. Then the map of the *R*-type NFAA defined by the formula $\varphi_R = R \circ X$, where the vector *X* takes on all values in the algebra, is a homomorphism.
  - *Proof.* For two arbitrary vectors X_1 and X_2, one can get the following:

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

the proposition 5 is proven. The φ_R map is called the *R*-type homomorphism.

- *Proposition* 6. Suppose a homomorphism-map operation of the *R*-type $\varphi_R(X) = R \circ X$, where *R* is a global right-sided unit, is given. Then for an arbitrary non-negative integer *i* the exponentiation operation X^i and the φ_L operation are mutually commutative, i.e., the equality $R \circ X^i = R \circ X)^i$ holds true.
  - *Proof.* Due to proposition 5, we have $\varphi_R(X^i) = (\varphi_R(X))^i$; i.e., $R \circ X^i = (R \circ X)^i$. The proposition 6 is proven.
- *Proposition* 7. Suppose the vector *N* satisfies the condition $\Delta_N \neq 0$. Then the non-equality $R_i \circ N \neq R_j \circ N$ holds true for arbitrary two global right-sided units R_i and R_j that satisfy the condition $R_j \neq R_i$.
  - *Proof.* Suppose $R_i \circ N = R_j \circ N$, then $(R_i - R_j) \circ N = 0$, where the equation $X \circ N = 0$ has a unique solution $X = 0$. Therefore, we have $R_i - R_j = O \Rightarrow R_i = R_j$, then the obtained contradiction proves proposition 7.
- *Proposition* 8. Suppose $\{R\}$ is the set of global right-sided units $\{R\}$ and the vector equation $W \circ X = Z$, where *Z* is a non-zero vector, has a solution $X = S$. Then $\#\{R\}$ different values $X_i = R_i \circ S$, where R_i takes on all values from the set $\{R\}$, also are solutions for the given equation.
  - *Proof.* $W \circ (R_i \circ S) = (W \circ R_i) \circ S) = W \circ X = S$. The proposition 8 is proven.

For example, in the case of the 4-dimensional NFAA described in subsection 1.2 the equation like $X \circ W = Z$ has p^2 different solutions.

4. New Forms of the HDLP and Double Masking

In the NFAAs, containing a set of global left-sided units the Equation (9) defines different homomorphism dependent on the selected global left-sided unit *L*.

- *Proposition* 9. Suppose a map of the NFAA is defined by the formula $\varphi_L(X) = B \circ X \circ A$, where the vectors *A* and *B* are such that the condition $A \circ B = L$ holds true for some fixed global left-sided unit *L* and the vector *X* takes on all values in algebra. Then the map $\varphi_L(X)$ is a

homomorphism, called the L^+ -type homomorphism.

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

$$\varphi_L(X_1 \circ X_2) = B \circ (X_1 \circ X_2) \circ A = B \circ (X_1 \circ L \circ X_2) \circ A$$
$$= (B \circ X_1 \circ A) \circ (B \circ X_2 \circ A) = \varphi_L(X_1) \circ \varphi_L(X_2);$$
$$\varphi_L(X_1 + X_2) = B \circ (X_1 + X_2) \circ A = (B \circ X_1 \circ A) + (B \circ X_2 \circ A)$$
$$= \varphi_L(X_1) + \varphi_L(X_2);$$

The proposition 9 is proven.

- *Proposition* 10. Suppose the formula $\varphi_L(X) = B \circ X \circ A$ sets a homomorphism-map operation of the L^+-type. Then for arbitrary non-negative integer i the exponentiation operation X^i and the φ_L operation 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 9 we have $\varphi_L(X^i) = (\varphi_L(X))^i$, i.e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The proposition 10 is proven.

- *Proposition* 11. Suppose the vectors A and B are such that the equality $A \circ B = L$, where L is a global left-sided unit holds true. Then, for arbitrary natural number $t \geq 1$ the equality $A^t \circ B^t = L$ holds true.

- *Proof*: $A^t \circ B^t = A^{t-1} \circ B^{t-1} = A^{t-1} \circ A \circ B \circ B^{t-1} =$ $A^{t-1} \circ L \circ B^{t-1} = A^{t-1} \circ B^{t-1} = ... = A \circ B = L$

the proposition 11 is proven.

Thus, a pair of the vectors A and B satisfying the condition $A \circ B = L$ which defines a class of the homomorphism-map operations of the L^+-type. Selecting different values of the parameter t one can set different homomorphism-map operations. Using the mutual commutativity of the exponentiation operation and the homomorphism-map operations of the L-type and L^+-type, one can propose a new form of the HDLP that can be put into the base of the PKA scheme, in which the public key Y is computed as follows:

$$Y = (B^t \circ N^x \circ A^t) \circ L' = (B^t \circ N \circ A^t \circ L')^x, \quad (10)$$

Where the vector N is a locally invertible element of the L-type NFAA (used as algebraic support of the considered cryptoscheme) defined over the field $GF(p)$ with the characteristic p having a large size (for example, 256 to 384 bits); the global left-sided unit L' and the natural numbers x and t are selected randomly representing the elements of the private key connected with the public key Y.

Finding the pair of numbers x and t, when the parameters N, A, B and the public key Y are known, represents the proposed HDLP of the L-type. The value L' is not used to compute the common key. It serves only to make computation of the values x and t to be significantly more difficult. Based on the said form of the HDLP, one can propose the following PKA scheme using the 6-dimensional NFAA from subsection 2.1 (with τ=2 and μ=1) as its algebraic support.

1. The first and second users generate their private keys (x_1, t_1, L_1') and (x_1, t_1, L_2') correspondingly.
2. Using the formula (10), the users compute their public keys Y_1 and Y_2.
3. The users exchange their public keys via a public channel.
4. The first user calculates the 6-dimensional vector $Z_1 = B^{t_1} \circ Y_2^{x_1} \circ A^{t_1}$.
5. The second user calculates the 6-dimensional vector $Z_2 = B^{t_2} \circ Y_1^{x_2} \circ A^{t_2}$.

Correctness proof of the protocol consists in proving that each of the users can compute the same secret vector Z:

$$Z_1 = B^{t_1} \circ (B^{t_2} \circ N^{x_2} \circ A^{t_2} \circ L_2')^{x_1} \circ A^{t_1} = B^{t_1+t_2} \circ N^{x_2 x_1} \circ A^{t_2+t_1};$$
$$Z_2 = B^{t_2} \circ (B^{t_1} \circ N^{x_1} \circ A^{t_1} \circ L_1')^{x_2} \circ A^{t_2} = B^{t_2+t_1} \circ N^{x_1 x_2} \circ A^{t_1+t_2}.$$

Thus, each of the users gets the same secret value $Z=Z_1=Z_2$. The vector Z is calculated using only two elements of the private key. The elements L_1' and L_2' are used in the procedure for computing the public key in order to set a secret homomorphism map of the L-type as the second masking mechanism.

In the case of setting the used 6-dimensional FNAA over the $GF(p)$ with 384-bit prime p the size of public key (secrete key) in the latter PKA scheme is equal to 288 (384) bytes. These values are significantly smaller than the size of the keys in the post-quantum public key cryptoschemes [5, 6] based on the computationally complex problems other than HDLP, as well as in the post-quantum PKA schemes Classic McEliece [1], CRYSTALS-KYBER [2], NTRU [3], and SABER [4].

Using a non-optimized implementation on a common laptop computer with microprocessor Intel Core i7-6567U at 3.3 GHz, the described PKA algorithm generates about 1000 keys per second. Its performance can be increased significantly when optimizing software implementation, however the latter item is outside the scope of this paper.

In the NFAAs, containing the global right-sided units the Equation (9) also defines different homomorphism, but the latter depend on the selected global right-sided unit R and the vectors A and B should satisfy the condition $A \circ B = R$. The following propositions can be easily proved similarly to the proofs of the Propositions 9, 10, and 11.

- *Proposition* 12. Suppose a map of the NFAA is defined by the formula $\varphi_R(X) = B \circ X \circ A$, where the vectors A and B are such that the condition $A \circ B = R$ holds true for some fixed global right-sided unit R and the vector X takes on all values in

algebra. Then the map $\varphi_R(X)$ is a homomorphism, called, called the R^+-type homomorphism.

- *Proposition* 13. Suppose a homomorphism-map operation $\varphi_R(X)$ of the R^+-type is defined by the formula $\varphi_R(X) = B \circ X \circ A$. Then the $\varphi_R(X)$ operation 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.
- *Proposition* 14. Suppose the vectors A and B are such that the equality $A \circ B = R$, where R is a right-sided global unit, holds true. Then for arbitrary natural number t the equality $A^t \circ B^t = R$ holds true.

Thus, a pair of the vectors A and B satisfying the condition $A \circ B = R$ defines a class of the homomorphism-map operations of the R^+-type. Selecting different values of the parameter t, one can set different homomorphism-map operations. Using the mutual commutativity of the exponentiation operation and the homomorphism-map operations of the R-type and R^+-type one can propose a new form of the HDLP that can be put into the base of the PKA scheme, in which the public key Y is computed as follows:

$$Y = R' \circ (B^t \circ N^x \circ A^t) = (R' \circ B^t \circ N \circ A^t)^x \qquad (11)$$

Where the vector N is a locally invertible element of the R-type NFAA defined over the field $GF(p)$ with the characteristic p having large size (for example, 384 bits); a random global right-sided unit R' and random integers $x < q$ and $t < q$ are elements of private key. Finding the pair of numbers x and t, when the parameters N, A, B, and the public key Y are known, represents the proposed HDLP of the R-type. On the base of the Equation (11) for computing the public key, one can propose the following PKA scheme using the 4-dimensional NFAA from subsection 2.1. (with $\mu = 2$) as its algebraic support.

1. The first and second users generate their private keys (x_1, t_1, R_1') and (x_2, t_2, R_2') correspondingly.
2. Using the formula (11), the users compute their public keys Y_1 and Y_2.
3. The users exchange their public keys via a public channel.
4. The first user calculates the 4-dimensional vector $Z_1 = B^{t_1} \circ Y_2^{x_1} \circ A^{t_1}$.
5. The second user calculates the 4-dimensional vector $Z_2 = B^{t_2} \circ Y_1^{x_2} \circ A^{t_2}$.

It is easy to prove that $Z_1 = Z_2$. In the proposed PKA schemes there are used the NFAAs described in subsection 2.1., however other L-type and R-type NFAAs can be also used as algebraic supports of the proposed cryptoschemes. For example, the suitable algebras of such types are considered in [13].

In the case of setting the used FNAA over the $GF(p)$ with 256-bit prime p the size of public key (secrete key) in the latter PKA scheme is equal to 128 (192) bytes. On a common laptop computer with microprocessor Intel Core i7-6567U at 3.3 GHz, the latter PKA algorithm generates about 6000 keys per second. Such performance is high enough for many practical applications, besides it can be increased significantly when optimizing software implementation of the algorithm.

5. Conclusions

Using the NFAAs, containing a large set of the global single-sided units as algebraic support, two new forms of the HDLP are introduced as the base primitive of the post-quantum PKA schemes. A theoretic result of this paper consists in the proposed forms of the HDLP that are characterized in using two different homomorphism maps as a single strengthened masking operation for hiding the output value of the base exponentiation operation that is performed in frame of the computation of the public key.

A practical result consists in two PKA schemes are proposed as candidates for post-quantum public-key cryptoschemes with a relatively small size of the public and secret keys. Detailed security analysis of the introduced PKA schemes represent a task of individual research.

Another result is that in this study, the possibility of expanding the set of forms of the HDLP suitable to developing the PKA schemes was shown. This result is a new starting point for further searching for novel methods and techniques for setting HLP forms as primitives of the PKA algorithms.

Acknowledgement

The authors thank anonymous Referee for valuable remarks.

References

[1] Attema T., "First NIST Standardization Conference- April 11-13, 2018," http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html, Last Visited, 2021.

[2] Avanzi R., Bos J., Ducas L., Kiltz K., Lepoint T., Lyubashevsky V., Schanck J., Schwabe P., Seiler G., and Stehlé D., "CRYSTALS-Kyber. Algorithm Specifications and Supporting Documentation," https://cryptojedi.org/papers/kybernist-20171130.pdf, Last Visited, 2021.

[3] Chen C., "NTRU: Second Round Update," https://ntru.org/talks/20190823_nist_round2.pdf, Last Visited, 2021.

[4] D'Anvers J., Karmakar A., Roy S., and Vercauteren F., "Saber: Module-LWR Based

Key Exchange, CPA-Secure Encryption and CCA-Secure KEM," http://pure-oai.bham.ac.uk/ws/files/70656269/Saber._Module_LWR.pdf, Last Visited, 2021.

[5] Jalali A., Azarderakhsh R., Kermani M., and Jao D., "Supersingular Isogeny Key Encapsulation." https://sike.org/files/SIDH-spec.pdf, Last Visited, 2021.

[6] Kosolapov Y. and Turchenko O., "On the Construction of A Semantically Secure Modification of The Mceliece Cryptosystem," *Prikl. Diskr. Mat*., no. 45, pp. 33-43, 2019.

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

[8] Langer T. and Steinwandt R., "Post-Quantum Cryptography," *in Proceedings of 9th International Conference on Post-Quantum Cryptography*, Fort Lauderdale, 2018.

[9] Li Y., Deng R., and Wang X., "The Equivalence of McEliece's and Niederreiter's Publickey Cryptosystems," *IEEE Transactions on Information*, vol. 40, no. 1, pp. 271-273, 1994.

[10] Lu Y., Zhang Q., and Li J., "A Certificate-Based AKA Protocol Secure Against Public Key Replacement Attacks," *The International Arab Journal of Information Technology*, vol. 16, no. 4, pp. 754-765, 2019.

[11] Moldovyan A. and Moldovyan N., "Post-Quantum Signature Algorithms Based on The Hidden Discrete Logarithm Problem," *Computer Science Journal of Moldova*, vol. 26, no. 3, pp. 301-313, 2018.

[12] Moldovyan D., "Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes," *Quasigroups and Related Systems*, vol. 18, no. 2, pp. 165-176, 2010.

[13] Moldovyan D., "Post-Quantum Public Key-Agreement Scheme Based on A New form of The Hidden Logarithm Problem," *Computer Science Journal of Moldova*, vol. 27, no. 1, pp. 56-72, 2019.

[14] Moldovyan D. and Moldovyan N., "Cryptosche mes over Hidden Conjugacy Search Problem and Attacks Using Homomorphisms," *Quasigroups and Related Systems*, vol. 18, no. 2, pp. 177-186, 2010.

[15] Moldovyan D. and Moldovyan N., "A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols," *in Proceedings of 5th Intentional Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, St.Petersburg, pp. 183-194, 2010.

[16] Moldovyan N. and Moldovyan A., "Finite Non-Commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-Quantum Cryptoschemes on its Base," *Bulletin of Academy of Sciences of Moldova Mathematics*, no. 1, pp. 71-78, 2019.

[17] Moldovyan N., "Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263-270, 2018.

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

[19] Post-Quantum Cryptography. Round 3 Submissions. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions, Last Visited, 2021.

[20] Yan S., *Quantum Attacks on Public-Key Cryptosystems*, Springer, 2014.

[21] Yan S., *Quantum Computational Number Theory*, Springer, 2015.

Dmitriy Moldovyan A research fellow of the Laboratory of Cybersecurity and Post-quantum Cryptosystems (LCPC) of St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS) and a associate professor with the Saint-Petersburg Electro-technical University "LETI". His research interests include computer security, digital signature algorithms, and post-quantum public-key cryptoschemes. He is author or co-author of 7 inventions and 65 scientific articles, books, and reports. He received his Ph.D. from SPIIRAS (2012).

Nashwan Al-Majmar, An associate professor with department of Computer Sciences and Information Technology, Ibb University, Yemen. He received his B.S. degree in Computer Systems Engineering and Informatics, in 2003, the M.S. degree in Computer Systems Engineering and Informatics, in 2006 from Saint-Petersburg Electro-technical University "LETI", Saint-Petersburg, Russia, and the Ph.D. degree in Methods and Systems of Information Protection and Security from Saint-Petersburg State University of Information Technologies, Mechanics and Optics, Saint-Petersburg, Russia, in 2010. His research interests include "information security", "AI" and "software development".

Alexander Moldovyan, A chief researcher of the LCPC of SPIIRAS at SPC RAS and a professor with the Saint-Petersburg Electro-technical University "LETI". His research interests include information security and cryptographic protocols. He has authored or co-authored more than 60 inventions and 220 scientific articles, books, and reports. He received his Ph.D. from the "LETI" University (1996).