Quasigroups and Related Systems **28** (2020), 269 – 284

An enhanced version of the hidden discrete logarithm problem and its algebraic support

Dmitriy N. Moldovyan, Alexandr A. Moldovyan, Nikolay A. Moldovyan

Abstract. A new approach is proposed to the development of the signature schemes based on the computational difficulty of the hidden discrete logarithm problem, which is characterized in the adoption of the criterion of elimination of periodicity associated with the value of the discrete logarithm in the construction of periodic functions based on the public parameters of the signature scheme. In line with the approach, a new signature scheme is proposed as candidate for post-quantum public-key cryptoscheme. Its algebraic support represents a 6-dimensional finite non-commutative associative algebra set over the field $GF(p)$, which contains p^2 global right-sided units. Every one of the lasts is the unit of one of p^2 isomorphic finite non-commutative groups contained in the algebra. Every of the said groups contains commutative subgroups possessing 2-dimensional cyclicity and this feature is exploited to implement the enhanced criterion of providing security to the known and potential future quantum attacks.

1. Introduction

In the last few years the development of practical post-quantum (PQ) public-key (PK) cryptosystems has attracted considerable attention from the cryptographic community [11, 12]. Post-quantum are called cryptographic algorithms and protocols that run efficiently on classical computers but will resist attacks performed with using hypothetic quantum computers (quantum attacks). Currently, the most widely used in practice cryptographic algorithms and protocols are based on computationally difficult problems of finding discrete logarithm and factorization, however, in the PQ era, such cryptosystems are insecure. The latter is due to the fact that polynomial algorithms for solving the said computational problems are known for a quantum computer [14].

Quantum algorithms for solving both the factoring problem (FP) [1] and the discrete logarithm problem (DLP) [14, 15] are based on the extremely high efficiency of a quantum computer to perform a discrete Fourier transform [2], which is used to calculate the period length of periodic functions. In particular, to solve the problem of finding the value of a discrete logarithm, one constructs a peri-

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, single-sided units, post-quantum cryptography, public-key cryptoscheme, signature scheme, discrete logarithm problem, hidden logarithm problem
This work was supported by the budget theme No. 0060-2019-010.

odic function whose values lie in an explicitly given cyclic group, which contains a period with the length depending on the value of the logarithm.

Developers of the PQ PK cryptoschemes usually use difficult computational problems that are different from the FP and DLP. An interesting approach to the designing of the PQ PK cryptoschemes and PQ commutative ciphers relates to using so called hidden DLP (HDLP) [3, 6, 7]. Different versions of the HDLP are used in the design of different PK cryptosystems. In the case of development of the signature schemes [9], the idea of that approach consists in selecting a cyclic group having sufficiently large prime order, which is generated by some vector N as a subset of elements of a finite non-commutative associative algebra (FNAA) followed by computing the PK in the form of the pair of the vectors $Q = \psi_1(N)$ and $Y = \psi_2(N^x)$, where x is private key; ψ_1 and ψ_2 are masking operations representing two different homomorphism-map (or automorphism-map) operations.

Due to using the masking operations ψ_1 and ψ_2 the vectors Q and Y are elements of two different cyclic groups each of which is different from the group generated by the vector N. Since the masking operations defines homormorphism maps, every one of them is mutually comutative with the exponentiation operation. Due to the last, one can use a DLP-based signature (for example, well known Schnorr signature algorithm [13]) and replace in it the signature verification procedure using the values N and N^x by the the signature verification procedure using the values Q and Y. To compute a signature a potential forger needs to know only the value x that is a discrete logarithm value in a hidden cyclic group, no element of which is known to the forger. The rationale of the security of the HDLP-based signature schemes consists in the fact that a periodic function $f(i,j)$ constructed as computation of product of the values Q^i and Y^j (for example, $f(i,j) = Q^i Y^j$) take on the values contained in numerous different groups contained in the FNAA used as algebraic support of the signature scheme. Therefore, the Shor quantum algorithm is not directly applicable to compute the value x, the function $f(i,j)$ contains a period depending on the value x though.

However, the question arises about the possibility of developing new quantum algorithms that allow us to calculate the period length for periodic functions that take values in algebraic sets that are not groups. In future, the emergence of such quantum algorithms will mean breaking the known HDLP-based signature schemes.

In this paper, we propose to adopt a strengthened criterion for ensuring security of the HDLP-based cryptoschemes to hypothetic quantum attacks based on the said advanced quantum algorithms for computing the lenth of the periods of periodic funcions related to a wider class of such functions. Namey, we propose the following advanced criterion of designing the HDLP-based PK cryptosystems: construction of the periodic functions on the base of the publicly know parameters of the cryptoscheme, which contain a period with the length depending on the value of the discrete logarithm in the hidden group, should be a computationally intractable problem.

To develop algorithms that meet this criterion, we propose to use the idea of masking periodicity with a period length different from the value of the prime order q of the cyclic group in which the hidden discrete logarithm problem is given. Namely, one is to design a signature scheme with such public parameters that using them to build periodic functions will give the period length equal to the order of the hidden cyclic group. As a concrete way to implement this idea, we propose to define a base cyclic group as a subgroup of a hidden commutative group having 2-dimensional cyclicity (i.e., group generated by a minimum generator system of two elements U and N having the same order value; in our case, the order is equal to the prime q). This makes it possible to form such a PK that the construction of periodic functions using its elements will define the value of the period equal to the value q. The latter is achieved by the fact that the elements of the PK are calculated by the formulas $Q = \psi_1(NU)$ and $Y = \psi_2(N^x)$.

The use of the multiplier U allows one to fix the length q of the period of the constructed periodic functions, but the presence of such a multiplier should be taken into account when developing the verification equation of the signature scheme. In general, the HDLP-based cryptosystems developed taking into account the proposed enhanced design criterion have lower performance, longer PK and signature. However, they are significantly more attractive as candidates for PQ signature schemes.

The rest of the paper is organized as follows. Section 2 describes the suitable algebraic support of the developed signature scheme, which represents the 6-dimensional FNAA defined over the ground finite field $GF(p)$ and containing p^2 different global right-sided units and p^2 finite non-commutative groups every one of which contains commutative subgroups with 2-dimensional cyclicity. Section 3 introduces the developed candidate for PQ signature scheme, characterized in using a commutative group with 2-dimensional cyclicity as a hidden group.

2. The used 6-dimensional FNAA

2.1. Preliminaries

In general, the m-dimensional finite algebra represents the m-dimensional vector space over some finite field, in which the vector multiplication operation (that is distributive at the left and at the right) is defined. If the vector multiplication is non-commutative and associative we have the FNAAs. The FNAA used as the algebraic support of the developed PQ signature scheme is defined over the ground field $GF(p)$ the characteristic of which is equal to the prime $p = 2q + 1$, where q is a 256-bit prime. The multiplication operation (denoted as $\circ$) in the considered FNAA is defined using the following formula descibing the result of the multiplying two 6-dimensional vectors $A = \sum_{i=0}^{5} a_i \mathbf{e}_i$, and $B = \sum_{j=0}^{5} b_j \mathbf{e}_j$, where $\mathbf{e}_0, \mathbf{e}_1, \ldots \mathbf{e}_5$ are formal basis vectors, as follows:

$$A \circ B = \left(\sum_{i=0}^{5} a_i \mathbf{e}_i \right) \circ \left(\sum_{j=0}^{5} b_j \mathbf{e}_j \right) = \sum_{j=0}^{5} \sum_{i=0}^{5} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j \right), \qquad (1)$$

where coordinates a_0, $a_1, \ldots a_5$ of the vector A and coordinates b_0, $b_1, \ldots b_5$ of the vector B are elements of the field $GF(p)$. One assumes the product of every pair of the basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by some single-component vector $\lambda \mathbf{e}_k$ that is taken from the so called basis vector multiplication table (BVMT), namely, from the cell at the intersection of the ith row and the jth column. In present paper the BVMT shown as Table 1 is used to define the 6-dimensional FNAA with the required properties. This algebra contains p^2 isomorphic non-commutative groups every of which contains commutative subgroups having 2-dimensional cyclicity.

Table 1. The BVMT setting the FNAA with p^2 global right-sided units ($\lambda \geqslant 2$)

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

2.2. Finite commutative group with 2-dimensional cyclicity

The finite 2-dimentional commutative algebra with the associative multiplication operation defined by Table 2 was considered in the paper [10], where it had been shown that the multiplicative group Γ of the algebra is cyclic, if the structural coefficient λ is a quadratic non-residue in $GF(p)$. In this case this algebra represents a finite field $GF(p^2)$.

If the structural coefficient λ is a quadratic residue in $GF(p)$, then the order of the group Γ has order equal to the value $\Omega = (p-1)^2$. Besides, Γ is generated by the minimum generator system $< G'_1, G'_2 >$, including two vectors of the same order equal to the value $(p-1)$. In [8] it was proposed to call a commutative finite group containg the minimum generator system of m vectors having the same order the group having m-dimensional cyclicity. In this paper the said term is used.

For the case $p = 2q + 1$, where q is a prime, one can consider the commutative primary group of the order q^2 that has 2-dimensional cyclicity and is generated by the generator system $< G_1, G_2 >$, where each of the vectors G_1 and G_2 has order q: $G_1 = {G'_1}^2$ and $G_2 = {G'_2}^2$. Independenly of the value of the structural coefficient λ the multiplicative group of the considered 2-dimentional algebra contains the unit equal to the vector $(1, 0)$. The said primary group can be considered as a set of $q+1$ different cyclic groups of the prime order q all possible pairs of which contain only one common element, namely, the unit vector $(1, 0)$. Evidently, some fixed

pair of the integers i and j $(0 < i < q;\ 0 < j < q)$ define the vector $G_{ij} = G_1^i \circ G_1^j$ having order equal to q, which is a generator of some cyclic group Γ_c of the prime order q. One can easily see that the following proposition holds true.

Table 2. The BVMT setting 2-dimensional commutative associative algebra over $GF(p)$

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

Proposition 1. *For $k = 0, 1, \ldots, q-1$ each of the the formulas $G_k = G_{ij} \circ G_1^k$ and $G_k = G_{ij} \circ G_2^k$, where $i, j = 1, 2, \ldots, q-1$, defines q generators of q different cyclic groups having order q.*

Arbitrary two elements $N \neq (1, 0)$ and $U \neq (1, 0)$ of the said primary group, which are contained in different cyclic subgroups, represent the generator system of the primary group. Therefore, due to the Proposition 1, for arbitrary fixed integer i $(0 < i < q)$ q different cyclic groups are defined by the generators $U_k = N_i \circ U^k$, where $k = 0, 1, \ldots, q-1$. The last fact is used in the design of the proposed HDLP-based signature scheme.

2.3. Properties of the algebraic support

The FNAA defined over the field $GF(p)$ by Table 1, where $\lambda \neq 1$; $\lambda \neq 0$, contains p^2 global right-sided units R that can be computed from the vector equation

$$A \circ X = A \tag{2}$$

with the unknown 6-dimensional vector $X = (x_0, x_1, \ldots, x_5)$. Using Table 1 the equation (2) can be represented in the form of the following system of four linear equations:

$$\begin{cases} a_0 (x_0 + x_2 + x_4) + a_3 (\lambda x_0 + x_2 + x_4) = a_0; \\ a_1 (x_1 + \lambda x_3 + x_5) + a_2 (x_1 + x_3 + x_5) = a_1; \\ a_1 (\lambda x_0 + x_2 + x_4) + a_2 (x_0 + x_2 + x_4) = a_2; \\ a_0 (x_1 + x_3 + x_5) + a_3 (x_1 + \lambda x_3 + x_5) = a_3; \\ a_4 (x_0 + x_2 + x_4) + a_5 (\lambda x_0 + x_2 + x_4) = a_4; \\ a_4 (x_1 + x_3 + x_5) + a_5 (x_1 + \lambda x_3 + x_5) = a_5. \end{cases} \tag{3}$$

Performing the variable substitution $u_1 = x_0 + x_2 + x_4$, $u_2 = \lambda x_0 + x_2 + x_4$, $u_3 = x_1 + x_3 + x_5$, and $u_4 = x_1 + \lambda x_3 + x_5$, one can represent the system (3) in the following form:

$$\begin{cases} a_0u_1 + a_3u_2 = a_0; \\ a_1u_4 + a_2u_3 = a_1; \\ a_2u_1 + a_1u_2 = a_2; \\ a_0u_3 + a_3u_4 = a_3; \\ a_4u_1 + a_5u_2 = a_4; \\ a_4u_3 + a_5u_4 = a_5. \end{cases}$$

The solution $(u_1, u_2, u_3, u_4) = (1, 0, 0, 1)$ satisfies the last system for all 6-dimensional vectors, therefore, the conditions

$$\begin{cases} u_1 = x_0 + x_2 + x_4 = 1; \\ u_2 = \lambda x_0 + x_2 + x_4 = 0; \end{cases} \tag{4}$$

$$\begin{cases} u_3 = x_1 + x_3 + x_5 = 0; \\ u_4 = x_1 + \lambda x_3 + x_5 = 1. \end{cases} \tag{5}$$

define the ful set of the global right-sided units $R = (r_0, r_1, r_2, r_3, r_4, r_5)$ that satisfy the equation (2). Solving the systems of linear equations (4) and (5) one can get the following formula describing p^2 different global right-sided units:

$$R = \left(\frac{1}{1-\lambda}, \frac{h(\lambda-1)+1}{1-\lambda}, \frac{d(\lambda-1)-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, d, h \right), \tag{6}$$

where $d, h = 0, 1, \ldots, p-1$. Evidently, the considered algebra contains no global left-sided unit nor global two-sided unit, however it contains numerous local left-sided units L acting in some subsets of the 6-dimensional vectors. The local left-sided unit L_A corresponding to the set of the algebraic elements, which includes all possible powers of some fixed vector A, can be computed as solution of the vector equation

$$X \circ A = A. \tag{7}$$

Using Table 1 one can represent (7) in the form of the following three independent systems of two linear equations with the pairs of the unknowns (x_0, x_1), (x_2, x_5), and (x_3, x_4) :

$$\begin{cases} (a_0 + a_2 + a_4)\, x_0 + (a_0 + \lambda a_2 + a_4)\, x_1 = a_0; \\ (a_1 + a_3 + a_5)\, x_0 + (a_1 + a_3 + \lambda a_5)\, x_1 = a_1; \end{cases} \tag{8}$$

$$\begin{cases} (a_0 + a_2 + a_4)\, x_2 + (a_0 + \lambda a_2 + a_4)\, x_5 = a_2; \\ (a_1 + a_3 + a_5)\, x_2 + (a_1 + a_3 + \lambda a_5)\, x_5 = a_5; \end{cases} \tag{9}$$

$$\begin{cases} (a_1 + a_3 + \lambda a_5)\, x_3 + (a_1 + a_3 + a_5)\, x_4 = a_3; \\ (a_0 + \lambda a_2 + a_4)\, x_3 + (a_0 + a_2 + a_4)\, x_4 = a_4; \end{cases} \tag{10}$$

The same main determinant Δ_A corresponds to each of the systems (8), (9), and (10):

$$\Delta_A = (a_0a_5 + a_4a_5 - a_1a_2 - a_2a_3)(\lambda - 1). \tag{11}$$

If $\Delta_A \neq 0$, then every of the systems (8), (9), and (10) has unique solution, i. e., the vector equation (7) has unique solution as the local left-sided unit L_A related to the vector A. Solving the systems (8), (9), and (10) one gets the following formulas describing the value $L_A = (l_0, l_1, l_2, l_3, l_4, l_5)$:

$$\begin{aligned} l_0 &= \frac{1}{1-\lambda}; \quad l_1 = \frac{a_0a_1 + a_1a_4 - a_2a_3 - a_2a_5}{\Delta_A}; \\ l_2 &= \frac{\lambda a_2a_3 + a_2a_5 - \lambda a_0a_1 - a_1a_4}{\Delta_A}; \quad l_3 = \frac{-1}{1-\lambda}; \\ l_4 &= \frac{a_0a_4 + \lambda a_3a_4 - \lambda a_0a_5 - a_2a_5}{\Delta_A}; \; l_5 = \frac{a_0a_5 + a_2a_5 - a_1a_4 - a_3a_4}{\Delta_A}. \end{aligned} \tag{12}$$

Proposition 2. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the local left-sided unit L_A is simultaneously the local two-sided unit E_A relating to the vector A.*

Proof. It is sufficient to show that the vector L_A is contained in the set (6) of the global right-sided units. Suppose in (6) we have $d = l_4$ and $h = l_5$. Then one can compute

$$r_1 = \frac{h(\lambda - 1) + 1}{1 - \lambda} = l_1; \quad r_2 = \frac{d(\lambda - 1) - \lambda}{1 - \lambda} = l_2.$$

Since $r_0 = l_0$ and $r_3 = l_3$, the local left-sided unit L_A is equal to the global right-sided unit corresponding to the integer values $d = l_4$ and $h = l_5$ in (6) and the vector L_A is the local two-sided unit E_A relating to the vector A. □

Due to the last proposition, one can conclude that the vector L_A acts on every vector form the set $A, A^2, \ldots, A^i, \ldots$ as local two-sided unit. Since $\Delta_A \neq 0$, for the fixed value A one has unique value L_A and the said sequence is periodic with the period length equal to some integer ω. The set of all vectors included in a fixed period compose a finite cyclic group (generated by the vector A) with the unit element equal to $E_A = L_A$, i. e., the element L_A can be computed using the formula $L_A = E_A = A^\omega$. For the integer value i $(0 < i < \omega)$the vector $A^{\omega - i}$ is the inverse value of the vector A^i relatively the local two-sided unit E_A, therefore, the vector A can be called a locally invertible vector. One can easily prove the following proposition:

Proposition 3. *Suppose the vector A is such that $\Delta_A \neq 0$. Then there exists some integer ω such that $A^\omega = E_A$ and the local two sided-unit E_A is simultaneously the unit of the cyclic group generated by the vector A.*

Proposition 4. *If the vector equation $A \circ X = B$ has solution $X = S$ such that $\Delta_S \neq 0$, then p^2 different values $X_i = R_i \circ S$, where R_i takes on all values from the set* (6)*, also represents solutions of the given equation.*

Proof. $A \circ (R_i \circ S) = (A \circ R_i) \circ S = A \circ S = B$. Suppose $R_i \circ S = R_j \circ S$, then $(R_i - R_j) \circ S = (0,0,0,0,0,0)$ and $R_i = R_j$, i. e., the number of different solutions $X_i = R_i \circ S$ is equal to the number of different global right-sided units, which is equal to p^2. The Proposition 4 is proven. □

Proposition 5. *Suppose the vector R is a global right-sided unit. Then the map of the FNAA, which is defined by the formula $\varphi_R(X) = R \circ X$, where the vector X takes on all values in the considered FNAA, is a homomorphism.*

Proof. For two arbitrary vectors X_1 and X_2 we have

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

$$\varphi_R(X_1 + X_2) = R \circ (X_1 + X_2) = R \circ X_1 + R \circ X_2 = \varphi_R(X_1) + \varphi_R(X_2). \quad \square$$

Proposition 6. *All locally invertible vectors of the considered 6-dimensional FNAA compose p^2 different groups with p^2 different units*

$$E = R = \left(\frac{1}{1-\lambda},\ \frac{h(\lambda-1)+1}{1-\lambda},\ \frac{d(\lambda-1)-\lambda}{1-\lambda},\ \frac{-1}{1-\lambda},\ \ d,\ \ h \right),$$

where $d, h = 0, 1, 2, \ldots p-1$.

Proof. Suppose the set $\{A_1, A_2, \ldots A_i, \ldots A_\Omega\}$ of locally invertible vectors includes all vectors relating to a fixed local two-sided unit E (including the vector E) and only such vectors. One can easily see that the said set is the group Γ_E with the unit E. Every fixed global right-sided unit R' from the set (6) is the unit E' of some group $\Gamma_{E'}$ representing a set locally invertible vectors $\{A'_1, A'_2, \ldots A'_i, \ldots A'_\Omega\}$. Indeed, due to the Proposition 5 we have $A'_i = R' \circ A_i$ for $i = 1, 2, \ldots \Omega$, and $E' = R' \circ E = R'$. We have p^2 different global right-sided units R described by the formula (6). Every of these units defines a unique group of the order Ω. The Proposition 6 is proven. □

Consider the order Ω of every of the said isomorphic groups. Evidently $\Omega = \Omega' p^{-2}$, where Ω' is the number of all locally invertible vectors contained in the algebra. One can compute the last value as $\Omega' = p^6 - \Omega''$, where Ω'' is the number of all non-invertible vectors, i. e., vectors satisfying the condition $\Delta_A = 0$. The last condition reduces to the following equation:

$$a_0 a_5 + a_4 a_5 - a_1 a_2 - a_2 a_3 = 0.$$

If $a_5 \neq 0$, then for arbitrary values a_1, a_2, a_3, a_4 there exists unique value a_0 that satisfies the last equality (in this case we have $p^4(p-1)$ different non-invertible vectors). For the case $a_5 = 0$ the equality holds true for arbitrary values a_0 and a_4, if $a_1 a_2 + a_2 a_3 = 0$. Consideration of two subcases i) $a_2 \neq 0$ and ii) $a_2 = 0$ gives respectively $p^3(p-1)$ and p^4 different non-invertible vectors. Totally the algebra contains $\Omega'' = p^4(p-1) + p^3(p-1) + p^4 = p^5 + p^4 - p^3$ non-invertible vectors.

Proposition 7. *Every one of p^2 isomorphic groups, which relates to some fixed global right-sided unit R and includes all invertible vectors relating to R, has order $\Omega = p(p-1)^2(p-1)$.*

Proof. We have $\Omega' = p^6 - \Omega'' = p^6 - \left(p^5 + p^4 - p^3\right) = p^3(p-1)\left(p^2-1\right)$ and $\Omega = \Omega' p^{-2} = p(p-1)\left(p^2-1\right)$. □

One can easily see that the set of all 6-dimensional vectors of the form $A' = (a_0, a_1, a_2, a_3, 0, 0)$ compose the 4-dimensional non-commutative subalgebra with the multiplication operation set by the BVMT shown as Table 3. This subalgebra contains one global two-sided unit E_{00} that is contained in the set (6) and corresponds to the integer values $d = 0$ and $h = 0$:

$$E_{00} = \left(\frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, 0, 0\right).$$

Actually, this subalgebra represents the 4-dimensional FNAA described in [4] and used as algebraic support of the HDLP-based signature schemes. The multiplicative group Γ_{00} of the subalgebra is one of the p^2 isomorphic groups contained in the considered 6-dimensional FNAA.

The group Γ_{00} includes a large number of commutative subgroups possessing 2-dimensional cyclicity. Indeed, for arbitrary value $\alpha \in GF(p)$ the vector $V_\alpha = \alpha E_{00}$ (scalar multiplication) is permutable with every vector in the group Γ_{00}. If α is a primitive element in $GF(p)$, then the vector V_α generates a cyclis subgroup Γ_α of the order $p-1$. Suppose $G \notin \Gamma_{00}$ ($G \notin \Gamma_\alpha$) is a vector of the order $p-1$. Then the generator system $< V_\alpha, G >$ generates the commutative subgroup possessing the order $(p-1)^2$ and having 2-dimensional cyclicity.

Table 3. The BVMT of the 4-dimensional subalgebra containing a global two-sided unit

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

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

$$B \circ A = R. \tag{13}$$

Evidently, the main determinant of the system of linear equations, which corresponds to the vector equation (13) is equal to $\Delta_A \neq 0$, therefore, the equation (13) has unique solution.

Proposition 8. *Suppose $B \circ A = R$. Then the formula*

$$\psi_R(X) = A \circ X \circ B,$$

where the vector X takes on all values in the considered 6-dimensional FNAA, sets the homomorphism map.

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

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

□

Proposition 9. *The homomorphism-map operation $\psi_R(X) = A \circ X \circ B$ and the exponentiation operation X^k are mutually commutative, i.e., the equality $A \circ X^k \circ B = (A \circ X \circ B)^k$ holds true.*

Proof. Due to Proposition 8 we have $\psi_R(X^k) = (\psi_R(X))^k$, i. e., $A \circ X^k \circ B = (A \circ X \circ B)^k$. □

3. The proposed HDLP-based signature scheme

3.1. Setting the hidden commutative group

The algebraic support of the introduced signature scheme represents the 6-dimensional FNAA described in Subsection 2.3 and defined over the field $GF(p)$ with characteristic $p = 2q + 1$, where q is a 256-bit prime. In the BVMT defining the multiplication operation (see Table 1) it is used the structural coefficient $\lambda \geqslant 2$, for example, $\lambda = 2$. Computation of the private and public parameters of the signature scheme begins with setting a private hidden finite commutative group $\Gamma_{<N,U>}$. The group $\Gamma_{<N,U>}$ is set as computation of its generator system $< N, U >$ that includes two vectors N and U each of which has order equal to the prime q. The generator system $< N, U >$ can be computed as follows:

1. Generate at random a locally invertible vector $U = (u_0, u_1, \ldots, u_5)$ of the order equal to q and, using the formulas (12), compute the global left-sided unit $L_U = (l_{U0}, l_{U1}, \ldots, l_{U5})$.

2. If the condition $\frac{u_0}{l_{U0}} = \frac{u_i}{l_{Ui}}$ holds true for all $i = 1, 2, \ldots, 5$, then go to step 1 (probability of this event is equal to $\approx q^{-1}$).

3. Select at random an integer value α $(1 < \alpha < p - 1)$ that is a primitive element modulo p. The primitive element α defines a locally invertible vector $G = \alpha^2 L_U$ having order equal to the prime q.

4. Generate a random integer k $(1 < k < q)$ and compute the vectors $N = G \circ U^k$.

One can easily see that each of the vectors N and U has order equal to the value q and the generator system $< N, U >$ defines a commutative primary group

$\Gamma_{<N,U>}$ the unit element of which is equal to L_U. The group $\Gamma_{<N,U>}$ has structure with the 2-dimensional cyclicity and the group order is equal to $\Omega = q^2$.

3.2. Computing parameters of the masking operations

The main contribution to the security of the developed signature scheme is introduced by two exponentiation operations performed in two different cyclic groups contained in the hidden commutative group $\Gamma_{<N,U>}$. The vector N sets the first of the said cyclic groups. The second cyclic group is set by the generator J that is computed as follows:

$$J = N^t \circ U^w,$$

where t and w ($1 < t < q$; $1 < w < q$) are two integer values selected at random. The vectors N, J, N^x, and $J^{x/2}$, where $x < q$ is an integer representing one of the elements of the private key, are used for computing the vectors $\psi_1(N \circ U)$, $\psi_2(N^x)$, $\psi_3\left(J \circ U^2\right)$, and $\psi_4\left(J^{x/2}\right)$ that are elements of the PK. Four different homomorphism-map operations ψ_1, ψ_2, ψ_3, and ψ_4 are used to compute four elements of the PK, which are elements of four different commutative groups contained in the algebra.

Parameters of the homomorphism-map operations $\psi_1(X) = A_1 \circ X \circ B_1$, $\psi_2(X) = A_2 \circ X \circ B_2$, $\psi_3(X) = A_1 \circ X \circ B_3$, and $\psi_4(X) = A_4 \circ X \circ B_4$, are computed as follows:

1. Select at random a global right-sided unit R_1 (for example, using the formula (6)), generate at random a locally invertible vector A_1, and compute the vector B_1 as solution of the vector equation $B_1 \circ A_1 = R_1$ (that has unique solution B_1, since $\Delta_{A_1} \neq 0$).
2. Select at random a global right-sided unit R_2, generate at random a locally invertible vector A_2, and compute the vector B_2 as solution of the vector equation $B_2 \circ A_2 = R_2$.
3. Select at random a global right-sided unit R_3 and compute the vector B_3 as solution of the vector equation $B_3 \circ A_1 = R_3$, where the vector A_1 has been generated at step 1.
4. Select at random a global right-sided unit R_4, generate at random a locally invertible vector A_4, and compute the vector B_4 as solution of the vector equation $B_4 \circ A_4 = R_4$.

3.3. Computation of the public key

The PK represents a set of six 6-dimensional vectors $(Z_1, Y_1, T_1; Z_2, Y_2, T_2)$ which are computed as follows:

1. $Z_1 = A_1 \circ N \circ U \circ B_1$ and $Y_1 = A_2 \circ N^x \circ B_2$.
2. $T_1 = R \circ A_1 \circ B_2$, where R is a random global right-sided unit.
3. $Z_2 = A_1 \circ J \circ U^2 \circ B_3$ and $Y_2 = A_4 \circ J^{x/2} \circ B_4$.
4. $T_2 = R' \circ A_1 \circ B_4$, where R' is a random global right-sided unit.

One can consider the private key as the set of all of secret elements that are needed to compute the signature. With such interpretation in the developed signature scheme the private key represents the set of the values x, N, J, U, A_1, B_2, and B_4.

3.4. Algorithm for signature generation

Suppose one should sign an electronic document M, using some fixed secure 256-bit hash-function f_H. The signature includes the following three elements: two 256-bit integers e and s and a 6-dimensional vector S. The elements of the signature are computed using the following signature generation algorithm:

1. Generate a random integer $k < q$ and a random locally invertible 6-dimensional vector K. Then compute the vectors V_1 and V_2:

$$\begin{cases} V_1 = K \circ N^k \circ B_2; \\ V_2 = K \circ J^{k/2} \circ B_4. \end{cases}$$

2. Calculate the first signature element e as the hash-function value computed from the document M to which the vectors V_1 and V_2 are concatenated:

$$e = f_H\left(M, V_1, V_2\right).$$

3. Calculate the second signature element s as follows: $s = k + xe \bmod q$.

4. Calculate the third signature element S as solution of the following vector equation:

$$S \circ A_1 \circ U^s = K.$$

In the last vector equation every of the values U^s, A_1, and K is a locally invetible vector, therefore, the equation has unique solution. At the output of the last algorithm one gets the signature (e, s, S) to the document M.

3.5. Algorithm for signature verification

Using the PK $(Y_1, Z_1, T_1;\ Y_2, Z_2, T_2)$, one can verify the signature (e, s, S) to the document M with the following signature verification algorithm:

1. Using the PK, compute the vectors V_1' and V_2':

$$\begin{cases} V_1' = S \circ Z_1^s \circ T_1 Y_1^{-e}; \\ V_2' = S \circ Z_2^{s/2} \circ T_2 \circ Y_2^{-e}. \end{cases}$$

2. Calculate the hash-function value e' from the document M to which the vectors V_1' and V_2' are concatenated: $e' = f_H\left(M, V_1', V_2'\right)$.

3. Using the formula (10), calculate the value Δ_S corresponding to the locally invertible vector $S = (s_0, s_1, s_2, s_3)$.

4. If $e' = e$ and $\Delta_S \neq 0$, then the signature is genuine. Otherwise the signature is rejected as false one.

3.6. Correctness proof

Correctness proof of the sigature scheme consists in proving that the signature (e, s, S) computed correctly will pass the verification procedure as genuine signature. Taking into account the mutual commutativity of the ψ-map operation with the exponentiation operation, for the vectors V_1' and V_2' computed at the first step of the signature verification procedure we have the following:

$$\begin{aligned} V_1' &= S \circ Z_1^s \circ T_1 \circ Y_1^{-e} \\ &= S \circ (A_1 \circ N \circ U \circ B_1)^s \circ R \circ A_1 \circ B_2 \circ (A_2 \circ N^x \circ B_2)^{-e} \\ &= S \circ A_1 \circ U^s \circ N^s \circ B_1 \circ A_1 \circ B_2 \circ A_2 \circ N^{-es} \circ B_2 \\ &= K \circ N^s \circ R_1 \circ R_2 \circ N^{-es} \circ B_2 = K \circ N^{k+ex} \circ N^{-ex} \circ B_2 \\ &= K \circ N^k \circ B_2 = V_1; \end{aligned}$$

$$\begin{aligned} V_2' &= S \circ Z_2^{s/2} \circ T_2 \circ Y_2^{-e} \\ &= S \circ \left(A_1 \circ J \circ U^2 \circ B_3\right)^{s/2} \circ R' \circ A_1 \circ B_4 \circ \left(A_4 \circ J^{x/2} \circ B_4\right)^{-e} \\ &= S \circ A_1 \circ U^s \circ J^{s/2} \circ B_3 \circ A_1 \circ B_4 \circ A_4 \circ (J^{-ex/2}) \circ B_4 \\ &= K \circ J^{(k+ex)/2} \circ R_3 \circ R_4 \circ J^{-ex/2} \circ B_4 = K \circ J^{(k+ex)/2-ex/2} \circ B_4 \\ &= K \circ J^{k/2} \circ B_4 = V_2. \end{aligned}$$

For $V_1' = V_1$ and $V_2' = V_2$ we have $f_H\,(M, V_1', V_2') = f_H\,(M, V_1, V_2)$ and the equality $e' = e$ holds true. For the signature (e, s, S) computed correctly inequality $\Delta_S \neq 0$ is satisfied. Thus, the signature scheme performes correctly.

4. Discussion

In the known signature schemes based on the computational difficulty of the HDLP, security to potential quantum attacks is provided by such design that sets the public signature-scheme parameters contained in different finite groups of some FNAA used as algebraic support of the cryptoscheme. Therefore, the use of the public parameters of the signature scheme in constructing periodic function causes the lasts to take values from many different groups, so the known quantum algorithms for finding the discret logarithm cannot be applied, the functions with the period length depending on the discrete logarithm value can be easily constructed though. The emergence of each new quantum algorithm will require a separate consideration of the security issue.

To obtain stronger guarantees of security to quantum attacks based on quantum algorithms for finding the length of periods of periodic functions, which can be developed in the future, it is reasonable to construct such signature schemes that periodic functions constructed using public parameters of the signature scheme will

be free of periods whose length is associated with the value of the discrete logarithm. The signature scheme described in Section 3 is an attempt of implementing this idea.

The proposed design can be considered as modification of the signature scheme described in [9], in which the PK represents three vectors $Z = \psi'(N)$, $Y = \psi''(N^x)$, and T, where ψ' and ψ'', are different homomorphism-map operations satisfying the condition $Y^i \circ T \circ Z^j = W_1 \circ N^{xj+i} \circ W_2$ for some fixed vectors W_1 and W_2 defining a map-operation of arbitrary type. Due to the last condition the periodic function $f(i,j) = Y^i \circ T \circ Z^j$ contains a period that is determined by the value of the discrete logarithm x. Indeed, the condition $Y^i \circ T \circ Z^j = Y^{i-1} \circ T \circ Z^{j+x}$ holds true. To eliminate periodicity connected with the value x, in the present paper for computing the vector Z it is proposed to use the formula $Z = \psi'(N \circ U)$, where the vectors N and U have the same prime order and are selected from hidden commutative group, besides these two vectors are contained in different cyclic groups. After such modification the periodic function $f(i,j) = Y^i \circ T \circ Z^j$ becomes free from periods connected with the value x, since $Y^i \circ T \circ Z^j = W_1 \circ N^{xj+i} \circ U^j \circ W_2$, where U cannot be represented in the form of some power of the vector N. Indeed, if the equation $N^{xj+i} \circ U^j = N^{xj'+i'} \circ U^{j'}$ holds true, then we have $j' \equiv j \bmod q$ and $i' \equiv i \bmod q$.

The said modification requires to introduce corresponding modification of the signature verification equation and such modfication has been performed as introducing the left-sided multiplication by the vector S that is the third signature element. This modification gives the following signature verification equation: $V' = S \circ Z^s \circ Y^{-e}$. However, after the modification a potential attacker can easily forge a signature using the value S as a fitting parameter, for example, using the following algorithm:

1. Generate at random a locally invertible vector V and compute $e = f_H(M, V)$.
2. Select at random a 256-bit number $s < q$.
3. Compute the vector S from the vector equation $S \circ Z^s \circ Y^{-e} = V$.

In order to prevent attacks based on using the signature element S as a fitting parameter in the introduced signature scheme the signature verification procedure includes two different verification equations.

Up to this point, we have focused attention on the fact that the calculation of the value x by public parameters of the HDLP-based schemes cannot be performed using known quantum algorithms for calculating the discrete logarithm. However, suppose a forger knows the value x. In the case of the HDLP-based signature schemes described in [5, 9] one can easily compose the signature generation algorithm using the value x and public parameters. In the case of the introduced signature scheme, knowledge of the value of x is not sufficient to simply calculate a genuine signature. In this connection one has an interesting research item on estimation of the computationally difficulty of forging a signature, when the private value x is known to the forger.

In comparison with the known HDLP-based signature schemes [5, 9], disadvantages of the proposed new signature scheme is the increased size of the signature

(about 3 times), the increased size of the PK (about 3 times), the reduced performance of the signature generation procedure (about 3 times) and signature verification procedure (about 2 times). However, these disadvantages are offset by the main advantage of the new scheme, which consists in the proposed significantly higher security to future quantum attacks and a more rigorous justification of such expectation.

5. Conclusion

This paper introduces a new approach to the design of the HDLP-based signature schemes and describes a signature scheme that illustrates a method used to satisfy the adopted criterion of eliminating periods having length connected with the value of discrete logarithm in construction of the periodic functions on the base of the public parameters of the signature scheme. The main difference of the proposed design from the earlier known deigns of the HDLP-based signature schemes is the use of the hidden commutative group possessing 2-dimensional cyclicity instead of using a hidden cyclic group. The 6-dimensial FNAA used as algebraic support of the developed signature scheme contains very large number of isomorphic commutative groups with 2-dimensional cyclicity.

One can suppose that FNAAs containing a large set of commutative groups with 3-dimensional cyclicity provide more space in designing the HDLP-based candidates for PQ signatures. This assumption sets the theme of a new study in the development of the proposed approach, but it is associated with the use of the FNAAs possessing a suitable structure. New designs in the line with the introduced approach, which are based on using 4-dimensional FNAAs with global two-sided unit, also represent practical interest.

Acknowledgement. The authors thank anonymous Referee for valuable remarks.

References

[1] **A. Ekert, R. Jozsa**, *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68** (1996), 733.

[2] **R. Jozsa**, *Quantum algorithms and the fourier transform*, Proc. Roy. Soc. London Ser A, **454** (1998), 323 – 337.

[3] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Cryptographic algorithms on groups and algebras*, J. Math. Sci. **223** (2017), no. 5, 629 – 641.

[4] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova. **26** (2018), 301 – 313.

[5] **A.A. Moldovyan, N.A. Moldovyan**, *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem*, Bull. South Ural State Univ. Ser. Math. Modelling, Programming & Computer Software. **12** (2019), 66 – 81.

[6] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems, **18** (2010), 165 – 176.

[7] **D.N. Moldovyan**, *A unified method for setting finite none-commutative associative algebras and their properties*, Quasigroups and Related Systems, **27** (2019), 293 – 308.

[8] **N.A. Moldovyan**, *Fast signatures based on non-cyclic finite groups*, Quasigroups and Related Systems, **18** (2010), 83 – 94.

[9] **N.A. Moldovyan**, *Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base*, Bul. Acad. Stiinte Republ. Moldova. Matematica, **1(89)** (2019), 71 – 78.

[10] **N.A. Moldovyan, P.A. Moldovyanu**, *New primitives for digital signature algorithms*, Quasigroups and Related Systems, **17** (2009), 271 – 282.

[11] *Post-quantum cryptography*, Lecture Notes Comp. Sci. **10786** (2018).

[12] *Post-quantum cryptography*, Lecture Notes Comp. Sci. **11505**, (2019).

[13] **C.P. Schnorr** *Efficient signature generation by smart cards*, J. Cryptology, **4** (1991), 161 – 174.

[14] **P.W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing, **26** (1997), 1484 – 1509.

[15] **S.Y. Yan**, *Quantum Attacks on Public-Key Cryptosystems*, Springer (2014).

Received December 16, 2019

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
14-th line 39, 199178, St. Petersburg, Russia
E-mails: maa1305@yandex.ru, mdn.spectr@mail.ru, nmold@mail.ru