Computer Science Journal of Moldova, vol.**28**, no.3(84), 2020

Digital signature scheme set in a hidden cyclic group

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

Abstract

A new form of the hidden discrete logarithm problem is proposed as cryptographic primitive for the development of the post-quantum signature schemes, which is characterized in performing two masking operations over each of two elements from a hidden finite cyclic group used to compute the public-key elements. The latter is contained in the set of non-invertible elements of the finite non-commutative associative algebra with a two-sided unit. One of the said masking operations represents the automorphism-map operation and the other one is the left-sided (right-sided) multiplication by a local right-sided (left-sided) unit acting on the said hidden group. Two 4-dimensional algebras are considered as possible algebraic supports of the developed signature schemes. The formulas describing the sets of local left-sided and right-sided units are derived. Periodic functions set on the base of the public parameters of the signature scheme contain periods depending on the discrete logarithm value, but every of them takes on the values relating to different finite groups contained in the algebraic support. Therefore one can expect that the computational difficulty of breaking the introduced signature schemes on a hypothetic quantum computer is superpolinomial.

Keywords: finite associative algebra, non-commutative algebra, global unit, local unit, right-sided unit, left-sided unit, discrete logarithm problem, public-key cryptoscheme, digital signature, post-quantum cryptosystem.

MSC 2010: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50

1 Introduction

Currently, the development of the post-quantum (PQ) public key (PK) cryptographic algorithms and protocols is considered as one of challenges in the area of applied and theoretic cryptography [1], [2]. A response to this challenge is the world competition for the development of the PQ PK cryptoschemes, announced by NIST in 2016 [3], [4]. The problem of the development of the practical PQ PK cryptoschemes is connected with the following items: i) quantum computers can suddenly appear in practice in near future; ii) at present the most widely used PK cryptoschemes are based on computational difficulty of the discrete logarithm problem (DLP) and the factorization problem (FP), however, each of these problems can be solved on a hypothetic quantum computer in polynomial time [5]–[7].

Computationally hard problems, other than DLP and FP, are used as primitives of the PQ PK cryptoschemes [9], [10], one of which is the hidden DLP (HDLP) [8]. The HDLP seems to be a promising primitive for designing PQ signature schemes [11], [12], PQ public key-agreement protocols [13], [14], and PQ commutative ciphers [15]. For the first time the HDLP had been defined in finite algebra of quaternions using the automorphism-map as the operation masking the hidden cyclic group in which the basic exponentiation operation is performed [8]. However, that form of the HDLP can be reduced to the ordinary DLP in a finite field [16]. Therefore, in the design of the HDLP-based signature scheme [17], using the finite quaternion algebra as its algebraic support, a strengthened form of the HDLP was applied. In the signature scheme [17], the basic exponentiation operation N^x (where x is a private value) is performed in the hidden cyclic group generated by a non-invertible element N of the algebra and the PK includes two elements $Y = G \circ N^x \circ G^{-1}$ and $Z = Q \circ N \circ Q^{-1}$, where G and Q are two secret invertible elements that define two different automorphism-map operations each of which is mutually commutative with the exponentiation operation.

In the present paper we show that, setting the hidden cyclic group generated by a non-invertible element of the finite non-commutative associative algebra (FNAA) with a global two-sided unit, provides possibility to design the HDLP-based signature schemes in which, during the process of generating the PK, the left-sided (rightleft-sided) multiplication by a local right-sided (left-sided) unit is used as additional masking operation performed on the element N^x (N) of the hidden group. Two 4-dimensional FNAAs are considered as algebraic support of the developed signature scheme. The formulas describing the sets of local left-sided and right-sided units are derived.

2 The used algebraic support

Usually the multiplication operation in a m-dimensional FNAA (denoted as $\circ$) is defined by the following formula

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

where $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ are m-dimensional vectors; $\mathbf{e}_1, \mathbf{e}_2, \ldots \mathbf{e}_m$ are basis vectors. The product $\mathbf{e}_i \circ \mathbf{e}_j$ for all possible pairs of the integers i and j is to be replaced by some single-component vector $\lambda \mathbf{e}_k$ indicated in the cell at intersection of the ith row and the jth column of so called basis vector multiplication table (BVMT). The value $\lambda \neq 1$ is called structural coefficient.

2.1 A first 4-dimensional FNAA

One can easily show that the BVMT, shown as Table 1, defines over the ground finite field $GF(p)$ the 4-dimensional FNAA containing the global two-sided unit

$$E = \left(\frac{1}{\lambda - 1}, \frac{1}{1 - \lambda}, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1} \right). \qquad (2)$$

The global means that the value E acts as unit element on every vector of the algebra. If each of the vector equations $A \circ X = E$ and $X \circ A =$

Table 1. The BVMT setting the 4-dimensional FNAA ($\lambda \neq 0$; $\lambda \neq 1$).

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

E has the same solution A^{-1}, then the vector A is called invertible and the vector A^{-1} is called inverse to the vector A. In the FNAA with the multiplication operation defined by Table 1 the vector $A = (a_0, a_1, a_2, a_3)$ is invertible, if the following invertibility condition holds true

$$a_1 a_2 \neq a_0 a_3. \tag{3}$$

Correspondingly, the non-invertibility condition is as follows

$$a_1 a_2 = a_0 a_3. \tag{4}$$

Using the condition (4) one can easily compute the number of the non-invertible vectors that is equal to $\eta = p^3 + p^2 - p$. Therefore, for the order Ω of the multiplicative group of the considered algebra (number of its invertible vectors) one can get $\Omega = p^4 - \eta$:

$$\Omega = p(p-1)\left(p^2 - 1\right). \tag{5}$$

In the algebra there exists no other element, except the global unit E, which acts as unit element on an invertible vector. On the contrary, there exists a variety of local left-sided and local right-sided units acting on some fixed non-invertible vector N and some subsets of non-invertible vectors connected with the vector N.

To derive the formula describing the set of the local left-sided units, one should consider the solutions of the vector equation $X \circ N = N$, where $N = (n_0, n_1, n_2, n_3)$ is a vector satisfying the non-invertibility condition $n_1 n_2 = n_0 n_3$, which can be reduced to the following two independent systems of two linear equations:

$$\begin{cases} (\lambda n_0 + n_2)\, x_0 + (n_0 + n_2)\, x_1 = n_0; \\ (\lambda n_1 + n_3)\, x_0 + (n_1 + n_3)\, x_1 = n_1; \end{cases} \tag{6}$$

$$\begin{cases} (\lambda n_0 + n_2)\, x_2 + (n_0 + n_2)\, x_3 = n_2; \\ (\lambda n_1 + n_3)\, x_2 + (n_1 + n_3)\, x_3 = n_3. \end{cases} \tag{7}$$

The main determinant of each of the latter systems is equal to zero. The auxiliary determinants of the system (6) are

$$\Delta_0 = n_0\,(n_1 + n_3) - n_1\,(n_0 + n_2) = (n_0 n_3 - n_1 n_2) = 0.$$

$$\Delta_1 = n_1\,(\lambda n_0 + n_2) - n_0\,(\lambda n_1 + n_3) = n_1 n_2 - n_0 n_3 = 0.$$

For the system (6) we have p solutions described by the formula

$$x_1 = \frac{n_0 - (\lambda n_0 + n_2)\, x_0}{n_0 + n_2},$$

where $x_0 = 0, 1, \ldots, p-1$, if $n_0 + n_2 \neq 0$, or by the formula

$$x_0 = \frac{n_0 - (n_0 + n_2)\, x_1}{\lambda n_0 + n_2},$$

where $x_1 = 0, 1, \ldots, p-1$, if $\lambda n_0 + n_2 \neq 0$. The auxiliary determinants of the system (7) are also equal to zero:

$$\Delta_2 = n_2\,(n_1 + n_3) - n_3\,(n_0 + n_2) = n_1 n_2 - n_0 n_3 = 0.$$

$$\Delta_3 = n_3\,(\lambda n_0 + n_2) - n_2\,(\lambda n_1 + n_3) = \lambda\,(n_0 n_3 - n_1 n_2) = 0.$$

The system (7) has p solutions described by the formula $x_3 = \frac{n_2 - (\lambda n_0 + n_2) x_2}{n_0 + n_2}$, where $x_2 = 0, 1, \ldots, p-1$, if $n_0 + n_2 \neq 0$, or by the formula $x_2 = \frac{n_2 - (n_0 + n_2) x_3}{\lambda n_0 + n_2}$, where $x_3 = 0, 1, \ldots, p-1$, if $\lambda n_0 + n_2 \neq 0$.

Thus, for the non-invertible vector N that satisfies the condition $n_0 + n_2 \neq 0$ there exist p^2 different left-sided units $L = (l_0, l_1, l_2, l_3)$ described by the formula

$$L = \left(d, \frac{n_0 - (\lambda n_0 + n_2)\, d}{n_0 + n_2}, h, \frac{n_2 - (\lambda n_0 + n_2)\, h}{n_0 + n_2} \right), \tag{8}$$

where $d, h = 0, 1, \ldots, p-1$. Using the non-invertibility condition (5), one can easily derive the following formula describing all local left-sided units that are non-invertible vectors:

$$L' = \left(d, \frac{n_0 - (\lambda n_0 + n_2)\, d}{n_0 + n_2}, \frac{n_2}{n_0} d, \frac{n_0 n_2 - (\lambda n_0 + n_2)\, n_2 d}{n_0^2 + n_0 n_2} \right), \qquad (9)$$

where $d = 0, 1, \ldots, p-1$. Since the set (9) includes p different non-invertible vectors, one can conclude that the set (8) contains $p^2 - p$ invertible and p non-invertible elements of the considered 4-dimensional FNAA.

To derive the formula describing all local right-sided units relating to the non-invertible vector N, one is to consider the solutions of the vector equation $N \circ X = N$ that can be reduced to the following two systems of equations:

$$\begin{cases} (\lambda n_0 + n_1)\, x_0 + (n_0 + n_1)\, x_2 = n_0; \\ (\lambda n_2 + n_3)\, x_0 + (n_2 + n_3)\, x_2 = n_2; \end{cases} \qquad (10)$$

$$\begin{cases} (\lambda n_0 + n_1)\, x_1 + (n_0 + n_1)\, x_3 = n_1; \\ (\lambda n_2 + n_3)\, x_1 + (n_2 + n_3)\, x_3 = n_3. \end{cases} \qquad (11)$$

Each of the systems (10) and (11) has the main determinant equal to zero. The auxiliary determinants of each of the systems (10) and (11) are equal to zero. Therefore, for the system (10) we have p solutions described by the formula $x_2 = \frac{n_0 - (\lambda n_0 + n_1) x_0}{n_0 + n_1}$, where $x_0 = 0, 1, \ldots, p-1$, if $n_0 + n_1 \neq 0$, or by the formula $x_0 = \frac{n_0 - (n_0 + n_1) x_2}{\lambda n_0 + n_1}$, where $x_1 = 0, 1, \ldots, p-1$, if $\lambda n_0 + n_1 \neq 0$.

For the system (11) we have p solutions described by the formula $x_3 = \frac{n_1 - (\lambda n_0 + n_1) x_1}{n_0 + n_1}$, where $x_2 = 0, 1, \ldots, p-1$, if $n_0 + n_1 \neq 0$, or by the formula $x_1 = \frac{n_1 - (n_0 + n_1) x_3}{\lambda n_0 + n_1}$, where $x_3 = 0, 1, \ldots, p-1$, if $\lambda n_0 + n_1 \neq 0$.

Thus, p^2 different right-sided units $R = (r_0, r_1, r_2, r_3)$ relate to the non-invertible vector N satisfying the condition $n_0 + n_1 \neq 0$, and the set of the R-units is described by the formula

$$R = \left(d, h, \frac{n_0 - (\lambda n_0 + n_1)\, d}{n_0 + n_1}, \frac{n_1 - (\lambda n_0 + n_1)\, h}{n_0 + n_1} \right), \qquad (12)$$

where $d, h = 0, 1, \ldots, p-1$. One can easily derive the formula describing all of p local right-sided units that are non-invertible vectors and show that the set (12) includes $p^2 - p$ invertible and p non-invertible 4-dimensional vectors. The sets (8) and (12) contain p common vectors among which only one vector E_N is non-invertible. These p units are local two-sided units. The single local two-sided unit E_N relating to the vector N represents the unit of the cyclic group generated by N.

2.2 A second 4-dimensional FNAA

To obtain a higher performance of the signature scheme one can define the vector multiplication operation using a BVMT containing eight cells with the structural constant equal to zero. The appropriate BVMT defining the 4-dimensional FNAA with global two-sided unit $E = \left(\mu^{-1}, \lambda^{-1}, 0, 0\right)$ is shown as Table 2. Every vector $A = (a_0, a_1, a_2, a_3)$ is invertible, if the following invertibility condition holds true

$$a_0 a_1 \neq a_2 a_3. \tag{13}$$

Respectively, the vector $N = (n_0, n_1, n_2, n_3)$ is a non-invertible vector, if the following non-invertibility condition holds true

$$n_0 n_1 = n_2 n_3. \tag{14}$$

The algebra contains $p^3 + p^2 - p$ non-invertible vectors and

$$\Omega = p(p-1)\left(p^2 - 1\right)$$

invertible ones, exactly like in the case of FNAA defined by Table 1.

One can derive the following formulas describing the sets of the local left-sided units, local right-sided units, and local two-sided units relating to the non-invertible vector N:

$$L_N = \left(d,\ h,\ \frac{n_1}{\mu n_3}\left(1 - \lambda h\right),\ \frac{n_0}{\lambda n_2}\left(1 - \mu d\right)\right), \tag{15}$$

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

Table 2. The BVMT setting the 4-dimensional FNAA ($\lambda \neq 0$; $\mu \neq 0$).

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mu\mathbf{e}_0$	0	0	$\mu\mathbf{e}_3$
$\mathbf{e}_1$	0	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mu\mathbf{e}_2$	0	0	$\mu\mathbf{e}_1$
$\mathbf{e}_3$	0	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_0$	0

$$R_N = \left(d, h,\ \frac{n_0}{\lambda n_3}\left(1-\mu d\right),\ \frac{n_1}{\mu n_2}\left(1-\lambda h\right)\right), \tag{16}$$

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

$$E_N = \left(d,\ \frac{\lambda n_1 - \mu n_0 + \mu^2 n_0 d}{\lambda^2 n_1},\ \frac{n_0}{\lambda n_3}\left(1-\mu d\right),\ \frac{n_0}{\lambda n_2}\left(1-\mu d\right)\right), \tag{17}$$

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

Each of the sets (15) and (16) includes $p^2 - p$ invertible vectors and p non-invertible ones. The set (17) includes $p-1$ invertible vectors and one non-invertible vector.

3 The hidden DLP and a masked form of it

The DLP is set in a cyclic group Γ of prime order q as follows: $Y' = Z'^x$, where Z' is a generator of the group Γ and the value $x < q$ is unknown integer. Computation of the value x, when the group elements Z' and Y' are known, is called DLP. The HDLP is set so that at least one of the values Z' and Y' is masked (hidden). When setting the HDLP, the cyclic group Γ is set as a subset of elements of a FNAA. The exponentiation operation Z'^x contributes mainly to the hardness of both the DLP and the HDLP, therefore it is called the base operation. The auxiliary operations used to mask the values Z' and Y' are called the masking operations. When developing the HDLP-based PK cryptoscheme, one should use the masking operations that are mutually commutative with the base exponentiation operation. The automorphism-map [8], [17] and homomorphism-map [14] operations are examples of masking operations. A particular form of the HDLP is defined by the used masking operations. Development of the PK cryptoschemes of different types is connected with applying different versions of the HDLP. When developing the PK cryptoschemes, to have possibility to select elements of order q having large size ($\geq$ 256 bits), usually there are used the FNAAs defined over the field $GF(p)$ with characteristic $p = 2q + 1$, where q is a prime.

For the first time HDLP was applied for development of the public key-agreement scheme [8]. That form of HDLP includes masking only one of two elements Z' and Y' and can be defined as follows:

HDLP: Given a FNAA, an algebra element Z' generating a cyclic group of prime order q, an invertible element Q of order q, which satisfies condition $Z' \circ Q \neq Q \circ Z'$, and an element $Y = \psi_{Q^w}(Z'^x) = Q^w \circ Z'^x \circ Q^{-w}$, where $w < q$ and $x < q$ are non-negative integers; ψ_{Q^w} is an automorphism-map operation; find the algebra element Q^w and integer x.

In the signature scheme [17] an enhanced form of the HDLP is used, which is characterized in masking both the element Z' and the element Y'.

Enhanced HDLP: Given a FNAA and non-invertible algebra elements $Z = \psi_G(Z'^x) = G \circ Z'^x \circ G^{-1}$, $Y = \psi_Q(Y'^x) = Q \circ Z'^x \circ Q^{-1}$, and invertible element $T = Q \circ G^{-1}$, where invertible elements Q and G have order q; the conditions $Z' \circ Q \neq Q \circ Z'$, $Z' \circ G \neq G \circ Z'$, and $G \circ Q \neq Q \circ G$ holds true; $1 < x < q$ is a non-negative integer; find the value of x.

One can note that in the latter definition only the value x is to be found, since the signature can be computed using the value x (discrete logarithm in the hidden cyclic group generated by the element Z') and the public parameters Z and Y. When using a non-invertible algebra element N as parameter Z', one can hide each of the elements $Z' = N$ and $Y' = N^x$ performing on it two different masking operations, namely, the ψ operation and an additional operation connected with multiplication by a local single-sided unit.

For example, the first masking operation can be implemented in the form $\varphi_L(N^x) = N^x \circ L_N$ to transform the vector N^x and in the form $\varphi_R(N) = R_N \circ N$ to transform the vector N. The automorphism-map operations ψ_Q and ψ_G can be used as the second masking operation when transforming the vectors N^x and N correspondingly: $Y = \psi_Q(\varphi_L(N^x)) = Q \circ N^x \circ L_N \circ Q^{-1}$ and $Z = \psi_G((\varphi_R(N))) = G \circ R_N \circ N \circ G^{-1}$. One can easily show that the following equalities hold true for arbitrary non-negative integers k and x:

$$(\varphi_L(N^x))^k = \varphi_L\left((N^x)^k\right); \quad (\varphi_R(N))^k = \varphi_R\left(N^k\right).$$

Thus, each of the said additional masking operations is mutually commutative with ψ operation. Due to such property of the used masking operations the developed signature scheme (see next Section 4) performs correctly. The introduced signature scheme is based on the following form of the HDLP.

Masked HDLP: Given a FNAA, non-invertible algebra elements $Z = \psi_G(\varphi_L(N)) = G \circ N \circ L_N \circ G^{-1}$ and $Y = \psi_Q(\varphi_R(N^x)) = Q \circ R_N \circ N^x \circ Q^{-1}$, and invertible element $T = Q \circ L_N^{-1} \circ G^{-1}$, where N is a non-invertible algebra element generating a cyclic group of order q; L_N is local left-sided unit for N; R_N is local right-sided unit for N; the invertible algebra elements Q and G have order q and satisfy the conditions $N \circ Q \neq Q \circ N$, $N \circ G \neq G \circ N$, and $G \circ Q \neq Q \circ G$; $1 < x < q$ is non-negative integer; find the value of x.

In Subsection 4.4, it is described method for computing the signature using public parameters Z and Y and the value x, therefore, to break the proposed signature scheme, it is sufficient to find only the unknown value of discrete logarithm in the hidden cyclic group generated by the unknown element N. In Subsection 4.5, it is shown that an algorithm for forging a signature can be used to compute the value x, i.e. the proposed signature scheme is as secure as the masked HDLP is computationally difficult.

4 A new signature scheme

4.1 Private and public keys

Each of the FNAA described in Section 2 can be used as algebraic support of the proposed signature scheme. The algebras are to be defined over the field $GF(p)$, where $p = 2q + 1$ and q are two prime numbers having large size (≥ 256 bits). One can easily generate a random non-invertible vector N that has order equal to the prime q. Such vector defines a finite cyclic group of the order q. The vector N is one of the elements of private key. The next element of private key is the non-negative integer $x < q$ which is used to compute the vector N^x.

Procedure of the PK generation is as follows:

1. Generate a random invertible vector Q of the order q and a random local left-sided unit L_N, that is an invertible vector, which satisfy the following conditions: $Q \circ N \neq N \circ Q$ and $R_N \circ N \neq N \circ R_N$.

2. Compute the first element Y of the PK:

$$Y = Q \circ N^x \circ L_N \circ Q^{-1}$$

3. Generate a random invertible vector G of the order q and a random local right-sided unit R_N, that is an invertible vector, which satisfy the following conditions: $G \circ N \neq N \circ G$ and $R_N \circ N \neq N \circ R_N$.

4. Compute the second element Z of the PK:

$$Z = G \circ R_N \circ N \circ G^{-1}.$$

5. Compute the third element T of the PK:

$$T = Q \circ L_N^{-1} \circ G^{-1}.$$

This procedure outputs the PK in form of the triple of the vectors (Y, Z, T).

All other elements used to generate the PK are secrete and part of them represent the private key in the form of the integer x and the triple of the vectors $\left(Q, N, G^{-1}\right)$. Other secret elements are not attributed to the private key, since they are not used in the signature computation procedure.

4.2 Signature generation and verification procedures

Generation of the signature (e, s) to the electronic document M is to be performed as follows:

1. Select a random integer $k < q$ and, using the elements Q and G^{-1} of the private key, compute the vector

$$V = Q \circ N^k \circ G^{-1}.$$

2. Using a specified hash-function F_h that satisfies the collision-resistance requirement, compute the value e of the hash function from the document M to which the vector V is attached: $e = F_h(M, V)$.

3. Compute the value $s = k - xe \bmod q$.

One should note that for signing a document M unique integer k is to be used. If two different documents are signed using the same value k, then one can compute the private value x from two signatures. Therefore the value of k is to be generated at random.

Signature verification procedure is executed as follows:

1. Using the PK (Y, Z, T) compute the vector

$$V' = Y^e \circ T \circ Z^s.$$

2. Compute the value $e' = F_h(M, V')$.

3. If $e' = e$, then the signature is accepted as genuine. Otherwise it is rejected.

4.3 Correctness of the signature scheme

Correctness proof of the signature scheme is as follows:

$$\begin{aligned} &V' = Y^e \circ (T) \circ Z^s = \\ &= \left(Q \circ N^x \circ L_N \circ Q^{-1}\right)^e \circ (T) \circ \left(G \circ R_N \circ N \circ G^{-1}\right)^s = \\ &= Q \circ N^{ex} \circ L_N \circ Q^{-1} \circ Q \circ L_N^{-1} \circ G^{-1} \circ G \circ R_N \circ N^s \circ G^{-1} = \\ &= Q \circ N^{ex+s} \circ G^{-1} = Q \circ N^{ex+k-ex} \circ G^{-1} = Q \circ N^k \circ G^{-1} = V \Rightarrow \\ &\qquad \Rightarrow F_h(M, V') = F_h(M, v) \Rightarrow e' = e. \end{aligned} \tag{18}$$

Thus, the signature (e, s) computed correctly will pass the verification procedure as genuine signature.

4.4 Alternative procedure for computing a signature

One can significantly reduce the size of the private key replacing the described signature verification procedure by the following one:

1. Select two random integers $k_1 < q$ and $k_2 < q$. Then, using the PK (Y, Z, T), compute the vector

$$V = Y^{k_1} \circ T \circ Z^{k_2}.$$

2. Compute the value $e = F_h(M, V)$.

3. Compute the value $s = k_2 + (k_1 - e)\, x \bmod q$.

Using the last version of the signature generation procedure one gets the private key in the form of one integer value x. However, after such modification, computing the signature will require performing one additional exponentiation operation.

The existence of an alternative signature generation procedure shows that it is sufficient to know only one secret value to forge a signature, namely, the value of x. In Subsection 4.5 this fact is used to perform formal security proof for the developed signature scheme.

4.5 On formal security proof

The method [19], proposed for providing formal security proof of the Schnorr DLP-based signature scheme [18], is well applicable to the developed HDLP-based signature scheme. Like in the Schnorr signature algorithm [18], in the developed signature scheme during the signature generation process the base exponentiation operation N^k is performed before computation of the first signature element that is the hash value $e = F_h(M, V)$, where $V = Q \circ N^k \circ G^{-1}$. In the formal security proof [19] one supposes that the hash function F_h is free of some properties that the signature forger can take advantage of [20]. Such assumption is reasonable in the case of using a collision-resistant hash-function.

In the method [19] it is considered a forger that can compute the signature element equally well for different hash functions F_h and F'_h. Suppose the forger runs two computer programs that use the same input data and the same random integer k, but different hash functions.

He will get two signatures (e, s) and (e', s') with the fixed value V and values $e = F_h(M, V)$ and $e' = F'_h(M, V)$. For some fixed integer k and fixed hash-function value e (e') there exists unique value of the second signature element s (s'). Therefore, for two signatures computed by hypothetic forging computer program one can write the following equalities: $s = k - ex \bmod q$ and $s' = k - e'x \bmod q$ from which the forger can easily compute the private value $x = (s - s')(e' - e)^{-1} \bmod q$.

The question of how a computer program can calculate the value of V when the values of Q, N, and G are unknown requires explanation. From the alternative procedure for calculating the signature, it can be seen that the calculation by the formula $V = Y^{k_1} \circ T \circ Z^{k_2}$ gives the same result as the calculation by the formula $V = Q \circ N^k \circ G^{-1}$ at $k = k_1 x + k_2 \bmod q$. Thus, fixing two values k_1 and k_2 results in fixing the value k. Actually, due to the existence of an alternative signature regeneration procedure, the reductionist security proof method [19] works well for the developed signature scheme.

4.6 Computational complexity of the signature scheme

Computational complexity of the procedures for i) generating private and public keys, ii) computing a signature, and iii) verifying a signature can be estimated in multiplication operations in the field $GF(p)$ and in exponentiation operations in the used FNAA (see Table 3) taking into account that i) one exponentiation in the FNAA used as algebraic support equals on the average to 384 multiplications $\circ$, ii) computation of the value U^{-1} for some invertible vector U is performed as solving the vector equation $U \circ X = E$, and iii) the local units R_N and L_N are computed with the use of formulas (8) and (12) for the case of the first 4-dimensional algebra and (15) and (16) for the case of the second 4-dimensional algebra.

The obtained estimate results show that the proposed signature scheme is sufficiently fast. For example, computational complexity of the signature generation (signature verification for the case of 64-bit public exponent) in the 2048-bit RSA cryptoscheme can be evaluated as $\approx 3 \cdot 2^{16}$ ($\approx 3 \cdot 2^{11}$) multiplications in $GF(p)$ with 256-bit prime p.

Table 3. A rough estimate of the implementation complexity.

Procedure for	# multiplications in $GF(p)$ for the first (second) FNAA	# exponentia- tions in FNAA
generating keys	$< 3 \cdot 2^{11}$ $(< 3 \cdot 2^{10})$	< 2
computing signature	$3 \cdot 2^{10}$ $(3 \cdot 2^{9})$	1
verifying signature	$3 \cdot 2^{11}$ $(3 \cdot 2^{10})$	2
alternative computing signature	$3 \cdot 2^{11}$ $(3 \cdot 2^{10})$	2

5 Discussion and conclusion

The expected PQ security of the proposed signature scheme is connected with the fact that a periodic function constructed on the basis of public parameters of the scheme takes on the values from many different groups contained in the FNAA used as algebraic support. For example, the function $f(i, j) = Y^i \circ T \circ Z^j$ contains a period with the length depending on the value x, however, the values of $f(i, j)$ are not limited to the values of any one group. Indeed, this function can be represented in the following form:

$$f(i, j) = Q \circ N^{ix+j} \circ G^{-1} = F(i, j) \circ V,$$

where $F(i, j) = Q \circ N^{ix+j} \circ Q^{-1}$ is the function taking on the values in frame of the cyclic group generated by the generator $Q \circ N \circ Q^{-1}$ and the vector $V = Q \circ G^{-1}$ is fixed. Due to multiplying different elements belonging to a fixed cyclic group by a fixed vector that has value out of this group, the function $f(i, j)$ takes on values belonging to different groups contained in the FNAA, whereas a quantum computer effectively finds the period lengths of a function whose values lie within a given finite group [6], [7].

Two different 4-dimensional FNAA with a global two-sided unit have been considered as algebraic supports of the proposed signature scheme. However, the 6-dimensional and 8-dimensional FNAAs represent significant interest for implementing other versions of the proposed signature scheme. Probably, using the FNAAs with dimension $m \geq 6$ it is reasonable to invent some other signature schemes such that their public parameters will not allow one to compose the periodic functions containing a period having the length depending on the private value x. Such potential signature schemes are particularly interesting as candidates for PQ PK cryptoschemes.

Acknowledgement. The authors sincerely thank the anonymous Referee for his comments and detailed advice on improving the content of the article.

This work was supported by the budget theme No. 0060-2019-010.

References

[1] *Post-Quantum Cryptography. 8th International Conference, PQCrypto 2017 Proceedings*, Utrecht, The Netherlands, June 26-28, 2017 (Lecture Notes in Computer Science, vol. 10346), 2017.

[2] *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018 Proceedings*, Fort Lauderdale, FL, USA, April 9-11, 2018 (Lecture Notes in Computer Science, vol. 10786), 2018.

[3] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST PQCrypto project. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[4] *Post-Quantum Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019*, (Lecture Notes in Computer Science, vol. 11505), 2019.

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

[6] A. Ekert and R. Jozsa, "Quantum computation and Shorś factoring algorithm," *Rev. Mod. Phys.*, vol. 68, p. 733, 1996.

[7] R. Jozsa, "Quantum algorithms and the fourier transform," *Proc. Roy. Soc. London Ser A*, vol. 454, pp. 323 – 337, 1998.

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

[9] Q. Alamelou, O. Blazy, S. Cauchie, and Ph. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, pp. 469–493, 2017.

[10] P. Hiranvanichakorn, "Provably Authenticated Group Key Agreement based on Braid Groups: The Dynamic Case," *International Journal of Network Security*, vol. 19, no. 4, pp. 517–527, 2017.

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

[12] N. A. Moldovyan, "Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base," *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, no. 1(89), pp. 71–78, 2019.

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

[14] D. N. Moldovyan, "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(79), pp. 56–72, 2019.

[15] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "Post-quantum commutative encryption algorithm," *Computer Science Journal of Moldova*, vol. 27, no. 3(81), pp. 299–317, 2019.

[16] A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, and A. A. Nechaev, "Cryptographic Algorithms on Groups and

Algebras," *Journal of Mathematical Sciences*, vol. 223, no. 5, pp. 629–641, 2017.

[17] N. A. Moldovyan and I. K. Abrosimov, "Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 15, no. 2, pp. 212–220, 2019. https://doi.org/10.21638/11702/spbu10.2019.205 (In Russian)

[18] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, pp. 161–174, 1991.

[19] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.

[20] N. Koblitz and A. J. Menezes, "Another Look at "Provable Security"," *Journal of Cryptology*, vol. 20, pp. 3–38, 2007.

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

Received January 18, 2020
Revised August 30, 2020
Accepted September 19, 2020

St. Petersburg Federal Research Center of
the Russian Academy of Sciences (SPC RAS),
St. Petersburg Institute for Informatics and
Automation of the Russian Academy of Sciences
14 Liniya, 39, St.Petersburg, 199178
Russia
E–mail: nmold@mail.ru