Computer Science Journal of Moldova, vol.**29**, no.2(86), 2021

A practical digital signature scheme based on the hidden logarithm problem

D.N. Moldovyan

Abstract

A candidate for practical post-quantum digital signature algorithm based on computational difficulty of the hidden discrete logarithm problem is introduced. The used algebraic carrier represents a 4-dimensional finite non-commutative associative algebra defined over the field $GF(p)$, which is caracterized in using a sparse basis vector multiplication table for defining the vector multiplication operation. Structure of the algebra is studied. Three types of the commutative groups are contained in the algebra and formulas for number of groups of every type are obtained. One of the types represents groups of the order $(p-1)^2$, possessing 2-dimensional cyclicity, and one of them is used as a hidden group in the signature scheme developed using a new method for implementing a general criterion of post-quantum resistance proposed earlier.

Keywords: finite associative algebra, non-commutative algebra, commutative finite group, discrete logarithm problem, hidden logarithm problem, public key, digital signature, post-quantum cryptosystem.

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

1 Introduction

Currently the development of the public-key digital signature algorithms and protocols that are resistant to quantum attacks (i. e., attacks including computations on a hypothetic quantum computer) attracts significant attention of the cryptographic community [1], [2].

Usually the research activity in the area of the post-quantum cryptography is focused on the development of the practical public-key cryptoschemes based on the computationally complex problems different from the factoring problem and the discrete logarithm problem (DLP). Actually, both the factoring problem and the DLP can be solved in polynomial time on a quantum computer [3]–[5].

Recently it was shown that the hidden discrete logarithm problem (HDLP) defined in finite non-commutative associative algebras (FNAAs) represents an attactive primitive for designing practical post-quantum cryptoschemes of the following types: commutative encryption algorithms [6], public key-agreement protocols [7], and digital signature schemes [8]–[10].

In the papers [11], [12] a general criterion for ensuring resistance of the HDLP-based signature schemes to hypothetic future quantum attacks based on quantum algorithms for computing the length of the periods of periodic functions was proposed. However, the signature schemes [11], [12] satisfying the said criterion had been developed using a method of doubling the signature verification equation.

In this paper a signature scheme implementing the said general design criteria without doubling the verification equation is developed. In addition a 4-dimensional FNAA is used as algebraic carrier of the signature scheme. Due to these features, the procedures of signature generation and verification are significantly faster and the size of the public key and size of signature are significantly smaller in comparision with the signature schemes [11], [12].

2 Preliminaries

2.1 Forms of the HDLP and design criteria

Usually the HDLP is defined in the m-dimensional ($m = 4, 6$, and 8) FNAAs as follows. One selects at random an integer $x < q$ and a generator G of a finite cyclic group of prime order q, which is contained in the used FNAA. To provide a required level of secutity the prime q should have sufficiently large size (≥ 256 bits). Then the vector G^x is

computed and two elements of the public key are formed: $Y = \psi_1(G^x)$ and $Z = \psi_2(G)$, where ψ_1 and ψ_2 are two different automorphism-map (or homomorphism-map) operations. The operations ψ_1 and ψ_2 are secret, therefore the potential attacker does not know the basic finite group in which the exponentiation operation had been performed. The masking operations ψ_1 and ψ_2 possess the property of mutual commutativity with the exponentiation operation that contributes mainly to the security, therefore, different known DLP-base signature algorithms can be used as prototypes of the HDLP-based algorithms.

In some of the HDLP-based signature schemes there is used the public key representing the triple of vectors (Y, Z, T), where the vector T is a fitting parameter in the verification equation. The hidden cyclic group is called the base group. The vectors Y, Z, and T are contained in other three different cyclic groups.

The rationale of the post-quantum resistance of the known HDLP-based signature schemes is quite straightforward: potential attacker knows no elements of the hidden cyclic group in which the exponentiation operation is performed, therefore, to compute the logarithm value x the Shor quantum algorithm [3] cannot be directly applied. Indeed, that algorithm is based on the ability of a quantum computer to perform a discrete Fourier transform (used to compute the period length of periodic functions) extremely efficiently for functions that take on values in a finite cyclic group [5]. In particular, to find the logarithm value x one constructs a periodic function whose values lie in a fixed cyclic group, which contains a period with the length depending on the value x.

For the case of the HDLP-based signature algorithms described in papers [8], [9] one can define the periodic function $F(i, j) = Y^i \circ T \circ Z^j$ in two integer variables i and j. This function contains a period with the length equal to $(-1, x)$:

$$F(i, j) = Y^i \circ T \circ Z^j = Y^{i-1} \circ T \circ Z^{j+x} = F(i - 1, j + x).$$

Thus, the design criterion related to the known HDLP-based signature algorithms can be formulated as follows.

Criterion 1. *The periodic functions constructed on the base of public parameters of the signature algorithm and containing a period with the length depending on the discrete logarithm value should take on values in different finite cyclic groups contained in the FNAA. Besides, no cyclic group can be pointed out as a preferable finite group for the values of the function* $F(i,j)$.

It is reasonable to assume that in the future, quantum algorithms will be developed that will effectively find the period length for functions that take on values within the framework of the whole FNAA used as algebraic support of the signature scheme. Taking into accoun such potential possibility, the following *advanced* criterion of the post-quantum resistance had been proposed in [11], [12].

Criterion 2. *Based on the public parameters of the signature scheme, the construction of a periodic function containing a period with the length depending on the discrete logarithm value should be a computationally intractable task.*

To implement a signature scheme satisfying the advanced criterion, one can use the idea of masking periodicity depending on the discrete logarithm value. To implement this idea, in the signature schemes proposed in [11], [12] a commutative group with two-dimensional cyclicity had been used as a hidden group. A finite commutative group is called group with the μ-dimensional cyclicity, if the group is generated by a generator system of μ independent elements possessing the same order value.

Suppose, in a hypothetic signature scheme the public key (Y, Z) includes elements computed as fallows: $Y = \psi_1(G^x)$ and $Z = \psi_2(GQ)$, where elements G and Q are generators of two different cyclic groups contained in the hidden commutative group with 2-dimensional cyclicity. Since each of the values G and Q has the same order, you cannot eliminate the Q multiplier effect by performing an exponentiation operation. Therefore, periodic functions, like the functions $F(i,j) = Y^i \circ Z^j$ or $F(i,j) = Y^i \circ T \circ Z^j$, will only show the periodicity associated with the value of the order of the elements G and Q.

This idea is quite trivial, but when it is implemented in specific signature algorithms, there are a number of complications that

must be overcome. The implementation of this idea in signature schemes [11], [12] required doubling the size of the public key and doubling the verification equation. At the same time, the size of the signature increased by three or more times compared to signature schemes that meet the Criterion 1.

In Section 3, a new 4-dimensional FNAA with a fast vector multiplication operation is proposed as an algebraic carrier of the HDLP-based signature algorithms. This algebra contains sufficiently large number of the commutative groups of the order $(p-1)^2$, which possess 2-dimensional cyclicity. Section 4 presents a novel method for designing HDLP-based signature schemes satisfying Criterion 2, which are free from the disadvantages of the implementations [11], [12].

2.2 Setting finite non-commutative algebras

Suppose a finite m-dimensional vector space is defined over the ground finite field $GF(p)$ and, additionally to the addition operation and scalar multiplication, a vector multiplication operation is defined so that it is distributive at the right and at the left relatively the addition operation. Then we have the algebraic structure called the m-dimensional finite algebra. Some algebra element A can be denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors.

The vector multiplication operation ($\circ$) of two m-dimensional vectors A and B is set as $A \circ B = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \circ \mathbf{e}_j)$, where each of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be substituted by a single-component vector $\lambda \mathbf{e_k}$, where $\lambda \in GF(p)$, which is indicated in the cell at the intersection of the ith row and jth column of the so-called basis vector multiplication table (BVMT). To define associative vector multiplication operation, the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$: $(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)$.

The BVMT shown as Table 1 sets 2-dimensional finite commutative associative algebra that is a finite field $GF(p^2)$, if the structural constant $\lambda \neq 0$ is a quadratic non-residue in $GF(p)$ [14]. If λ is a

Table 1. The BVMT setting the 2-dimensional commutative algebra

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

quadratic residue, the set of invertible elements of the said algebra represents the multiplicative group Γ' possessing 2-dimensional cyclicity and having order equal to $(p-1)^2$. In general, a finite group is called group with μ-dimensional cyclicity if its minimum generator system includes μ independent elements of the same order [15].

When constructing the HDLP-based public-key cryptoschemes, one uses hidden cyclic groups whose order is equal to a prime of sufficiently large size. Therefore the used FNAAs are defined over the field $GF(p)$ whose characteristic is equal to a prime $p = 2q + 1$, where q is also a prime. In the last case the group Γ' includes the commutative subgroup Γ with the minimum generator system $< G_1, G_2 >$, in which the elements G_1 and G_2 have prime order q. Different pairs of integers i and j, such that $0 < i < q$ and $0 < j < q$, define different elements $G_{ij} = G_1^i \circ G_2^j$ having order q. Every element G_{ij} is a generator of some cyclic group of the prime order q. For a fixed pair of integers (i, j), where $i, j = 1, 2, \ldots, q-1$, each of the formulas $G_k = G_{ij} \circ G_1^k$ and $G_k = G_{ij} \circ G_2^k$, where $k = 0, 1, \ldots, q-1$, sets q generators of q different cyclic groups of the order q.

To set FNAAs of arbitrary even dimensions m, one can use two unified methods, [8], [16], each of which is represented by a simple mathematical formula parameterized by values $m = 2, 4, 6, \ldots 2i$, which describes the content of all cells of the BVMT as the basis vector $\mathbf{e}_{f_m(i,j)} = \mathbf{e}_i \circ \mathbf{e}_j$, where the function $f_m(i, j)$ takes on the values from the set $0, 1, 2, \ldots m-1$. For a fixed value m, each of that methods sets an m-dimensional FNAA in which the computational complexity of the vector multiplication operation is approximately equal to m^2 multiplications in $GF(p)$.

In order to provide a higher performance of the developed signature

scheme, in the present paper it is used a specially composed particular BVMT defining a 4-dimensional FNAA with the vector multiplication operation having complexity equal to ≈ 8 multiplications in $GF(p)$.

3 The used algebraic support and its properties

The 4-dimensional FNAA used as algebraic carrier is set by a sparse BVMT represented by Table 2, where the structural constant $\lambda \neq 0$. This algebra contains the global two-sided unit $E = (1, 1, 0, 0)$. The vectors $G = (g_0, g_1, g_2, g_3)$ satisfying the non-equality $g_0 g_1 \neq \lambda g_2 g_3$ are invertible. The vectors $N = (n_0, n_1, n_2, n_3)$ satisfying the condition $n_0 n_1 = \lambda n_2 n_3$ are non-invertible. It is easy to show that the number of non-invertible vectors is equal to $\eta_N = p^3 + p^2 - p$. Correspondingly, the number of invertible vectors, i. e. the order of the multiplicative group of the algebra, is equal to

$$\Omega = p^4 - \eta_N = p(p-1)\left(p^2 - 1\right). \tag{1}$$

To study structure of the algabra, consider different sets of the algebra elements X that are mutually permutable with a fixed vector A. The elements $X = (x_0, x_1, x_2, x_3)$ can be computed from the vector equation $A \circ X = X \circ A$ that can be reduced to solving the following system of three linear equations with the unknowns x_0, x_1, x_2, and x_3:

$$\begin{cases} \lambda\left(a_3 x_2 - x_3 a_2\right) = 0; \\ a_2\left(x_0 - x_1\right) + x_2\left(a_1 - a_0\right) = 0; \\ a_3\left(x_1 - x_0\right) + x_3\left(a_0 - a_1\right) = 0. \end{cases} \tag{2}$$

Consider the following cases: i) $a_0 = a_1 = s$ and $a_2 = a_3 = 0$; ii) $a_0 \neq a_1$ and $a_2 = a_3 = 0$; iii) $a_2 = 0$, and $a_3 \neq 0$; iv) $a_2 \neq 0$, and $a_3 = 0$; v) $a_2 \neq 0$, and $a_3 \neq 0$.

Case i) relates to the set of the scalar vectors $S = sE$. Evidently, every vector of the considered 4-dimensional FNAA is permutable with every scalar vector. The set of scalar vectors Ψ is contained in every set of pairwise permutable vectors.

Table 2. The sparse BVMT setting a 4-dimensional FNAA ($\lambda \neq 0$)

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

Case ii). From system (2) one can easily see that the solution space includes p^2 vectors $X = (x_0, x_1, 0, 0)$, where $x_0, x_1 = 0, 1, \dots p-1$. This set of vectors X represents a commutative subalgebra containing $2p-1$ non-invertible vectors, multiplicative group of which has 2-dimensional cyclicity and order equal to $\Omega_1 = (p-1)^2$.

Case iii). System (2) is reduced to the following system of two equations:

$$\begin{cases} x_2 = 0; \\ x_1 = x_0 - x_3 \dfrac{a_0 - a_1}{a_3}, \end{cases} \tag{3}$$

which defines the solution space

$$X = (x_0, x_1, x_2, x_3) = \left(d, d - h\frac{a_0 - a_1}{a_3}, 0, h \right), \tag{4}$$

where $d, h = 0, 1, \dots p-1$. For the fixed value $h = 0$, formula (6) defines the set of scalar vectors. For the values $h \neq 0$, every vector V of set (4) satisfies the condition of the Case iii), therefore V defines the set of vectors Φ_V permutable with V, which coincides with set (4) that represents a commutative subalgebra Φ_A of the considered 4-dimensional FNAA.

If $a_0 \neq a_1$, then set (4) includes $2p-1$ non-invertible vectors and $p^2-(2p-1)$ invertible ones that compose multiplicative group of subalgebra Φ_A, which possesses 2-dimensional cyclicity and has order equal to $(p-1)^2$. Below, commutative groups of this type are denoted as Γ_1 and are called groups of the Γ_1 type.

If $a_0 = a_1$, then set (4) includes p non-invertible vectors and (p^2-p) invertible ones that compose a cyclic multiplicative group of the order $p(p-1)$. Commutative groups of this type are denoted as Γ_2 and are attributed to the Γ_2 type.

Case iv). System (2) is reduced to the following system of two equations:

$$\begin{cases} x_3 = 0; \\ x_1 = x_0 + x_2 \dfrac{a_1 - a_0}{a_2}, \end{cases} \tag{5}$$

which defines the solution space

$$X = (x_0, x_1, x_2, x_3) = \left(d, d + h\frac{a_1 - a_0}{a_2}, h, 0 \right), \tag{6}$$

where $d, h = 0, 1, \ldots p-1$. For the values $h \neq 0$, every vector V of set (6) satisfies the condition of the Case iv), therefore V defines the set of vectors Φ_V permutable with V, which coincides with set (6) that is a commutative subalgebra Φ_A. Note that for $h = 0$ formula (6) defines the scalar vectors.

If $a_0 \neq a_1$, then set (6) includes $2p-1$ non-invertible vectors and $(p-1)^2$ invertible ones that compose a multiplicative group of the Γ_1 type. If $a_0 = a_1$, then set (6) includes p non-invertible vectors and $p(p-1)$ invertible ones that compose a multiplicative group of the Γ_2 type.

Case v). System (2) is reduced to the following system of two equations:

$$\begin{cases} x_3 = x_2 \dfrac{a_3}{a_2}; \\ x_1 = x_0 + x_2 \dfrac{a_1 - a_0}{a_2}, \end{cases} \tag{7}$$

which defines the solution space

$$X = (x_0, x_1, x_2, x_3) = \left(d,\ d + h\frac{a_1 - a_0}{a_2},\ h,\ h\frac{a_3}{a_2} \right), \tag{8}$$

where $d, h = 0, 1, \ldots p-1$. For arbitrarily fixed integers d and $h \neq 0$, every vector V of set (8) satisfies the condition of the Case v),

therefore V defines the set of vectors Φ_V permutable with V, which is described by formula (8) written for coordinates of the vector $V = (v_0, v_1, v_2, v_3) = \left(d,\ d + h\frac{a_1 - a_0}{a_2},\ h,\ h\frac{a_3}{a_2}\right)$:

$$X' = \left(x'_0, x'_1, x'_2, x'_3\right) = \left(d',\ d' + h'\frac{v_1 - v_0}{v_2},\ h',\ h'\frac{v_3}{v_2}\right), \qquad (9)$$

where $d', h' = 0, 1, \ldots p-1$. Substitution of the coordinates $v_0 = d$, $v_1 = d + h\frac{a_1 - a_0}{a_2}$, $v_2 = h$, and $v_3 = h\frac{a_3}{a_2}$ in formula (9) gives $\Phi_V = \Phi_A$. Due to the latter result one can conclude that Φ_A is the set of pairwise permutable vectors. Actually, Φ_A is a commutative subalgebra of the order p^2. Like in the cases ii), iii), and iv), for the fixed value $h = 0$ formula (8) describes the set of scalar vectors: $X = (d,\ d,\ 0,\ 0)$, where $d = 0, 1, \ldots p-1$. Thus we have come to the following conclusion:

Proposition 1. Every 4-dimensional vector, except scalar vectors, is included in a single commutative subalgebra Φ.

Consider possible types of the Φ_A relating to the Case v). Using the non-invertibility condition, one can write the following equation for coordinates of non-invertible vectors contained in Φ_A:

$$d\left(d + h\frac{a_1 - a_0}{a_2}\right) = \lambda h^2 \frac{a_3}{a_2}, \qquad (10)$$

where different pairs of integers (d, h) that satisfy equation (10) set different non-invertible vectors contained in Φ_A, that is a commutative subalgebra. Consider solution of equation (10) relatively the unknown value d for a fixed value of h:

$$d = \left(\frac{a_0 - a_1}{a_2} \pm \frac{\sqrt{(a_0 - a_1)^2 + 4\lambda a_2 a_3}}{2a_2}\right) h. \qquad (11)$$

The number of non-invertible vectors that are contained in Φ_A depends on the value $\Delta = (a_0 - a_1)^2 + 4\lambda a_2 a_3$.

If $\Delta = \delta \neq 0$ is a quadratic residue in $FG(p)$, then for every value $h = 1, 2, \ldots p-1$, formula (11) gives two different values of d, i. e.

$2(p-1)$ non-invertible vectors different from $(0,0,0,0)$. Taking the zero vector into account we have $\eta_N = 2p-1$. The multiplicative group of the subalgebra has order $\Omega_1 = (p-1)^2$ and possesses 2-dimensional cyclicity, i. e. it is a group of Γ_1 type.

If $\Delta = 0$, then for every value $h = 0, 1, \ldots p-1$ formula (11) gives the single value of d, i. e. p non-invertible vectors including the zero vector. Thus, the number of non-invertible vectors is equal to $\eta_N = p$. The multiplicative group is cyclic and has order $\Omega_2 = p^2 - p = p(p-1)$, i. e. it is a group of Γ_2 type.

If $a_0 \neq a_1$, then set (5) includes $2p-1$ non-invertible vectors and $(p-1)^2$ invertible ones that compose a multiplicative group of the Γ_1 type. If $a_0 = a_1$, then set (5) includes p non-invertible vectors and $p(p-1)$ invertible ones that compose a multiplicative group of the Γ_2 type.

If $\Delta = \delta \neq 0$ is a quadratic non-residue in $FG(p)$, then for every value $h = 1, 2, \ldots p-1$ formula (11) gives no solution of equation (10), with exception $(d,h) = (0,0)$ corresponding to the zero vector $(0,0,0,0)$. Subalgebra Φ_A represents a finite ground field $GF(p^2)$, the multiplicative group of which is cyclic and has the order $\Omega_3 = p^2 - 1$. A group of this type is called a group of the Γ_3 type.

Thus, the considered 4-dimensional FNAA contains commutative groups of the types Γ_1, Γ_2, and Γ_3.

4 The number of commutative groups of every type

Proposition 2. Number η_Φ of the commutative Φ subalgebras equals to $p^2 + p + 1$.

Proof. The set of the scalar vectors Ψ is contained in every Φ subalgebra. Due to the Proposition 1, every vector that is different from a scalar vector is contained in a single subalgebra of Φ type. Therefore, for the number η_Φ of the Φ subalgebras one can write:

$$\eta_\Phi = \frac{p^4 - p}{p^2 - p} = p^2 + p + 1. \qquad (12)$$

The Proposition 2 is proven.

Suppose k, t, and u denote number of different commutative groups of the types Γ_1, Γ_2, and Γ_3 correspondingly. Then we have $\eta_\Phi = k+t+u$ and

$$k + t + u = p^2 + p + 1. \tag{13}$$

Due to the Proposition 1 and formula (1) one can write:

$$\begin{aligned}
&(\Omega_1 - (\#\Psi - 1))\, k + (\Omega_2 - (\#\Psi - 1))\, t + (\Omega_3 - (\#\Psi - 1))\, u = \\
&\qquad = \Omega - (\#\Psi - 1)\,; \\
&\Big((p-1)^2 - (p-1)\Big)\, k + (p(p-1) - (p-1))\, t + \\
&+ \big(p^2 - 1 - (p-1)\big)\, u = p(p-1)\left(p^2 - 1\right) - (p-1);
\end{aligned}$$

$$(p-2)k + (p-1)t + pu = p^3 - p - 1. \tag{14}$$

Using formulas (13) and (14) one can easily derive the following two equations:

$$2k + t = (p+1)^2; \tag{15}$$

$$2u + t = p^2 + 1. \tag{16}$$

To find the value t, consider the number of non-invertible vectors A relating to the Case v), which define the Φ_A subalgebras containing multiplicative groups of the Γ_2 type. Such vectors satisfy the conditions $a_0 a_1 = \lambda a_2 a_3 \neq 0$ and $\Delta = (a_0 - a_1)^2 + 4\lambda a_2 a_3 = 0$ from which it is easy to get the conditions

$$a_0 \neq 0; \quad a_1 \neq 0; \quad a_1 = -a_0; \quad a_3 = \frac{a_0 a_1}{\lambda a_2},$$

where $a_0, a_2 = 1, 2, \ldots p-1$. Therefore, $(p-1)^2$ different non-invertible vectors A relating to the Case v) define the Φ subalgebras containing the multiplicative group of the Γ_2 type. Every one of the said Φ subalgebras includes $p-1$ non-invertible vectors that are different from the zero vector, therefore, the Case v) gives $\eta_{v)} = \frac{(p-1)^2}{p-1} = p-1$ different groups of the Γ_2 type. In addition, each of the Cases iii) and iv) gives one unique Γ_2-type group. Thus, we have got

$$t = p + 1.$$

Substituting the last value in (15) and (16) one gets:

$$k = \frac{p(p+1)}{2}; \tag{17}$$

$$u = \frac{p(p-1)}{2}. \tag{18}$$

5 Signature algorithm satisfying the advanced criterion of post-quantum resistance

The introduced 4-dimensional FNAA is well suited for development a HDLP-based digital signature scheme satisfying the advanced criterion of post-quantum resistance, since it contains a large number of the Γ_1-type commutative groups having 2-dimensional cyclicity. The proposed signature scheme is described as follows.

5.1 Computation of the signature scheme parameters

The FNAA used as algebraic support is defined over the finite ground field $GF(p)$ with prime $p = 2q + 1$, where q is a 256-bit prime. The required value p is set as generation of different 256-bit primes q until the value $2q + 1$ will satisfy a test for primality (for example, trying several arbitrary different integers $b < p$, one gets a value b such that $b^2 \bmod p \neq 1$ and $b^q \bmod p \neq 1$). Generation of the requiered prime p introduces the main contribution in the computational complexity of generating the parameters of the proposed signature scheme. Taking into account that on the average about 10^2 different primes q are to be tried, one can estimate that the generation of the value p takes about 10^7 multiplications modulo 257-bit prime.

The secret hidden group $\Gamma_{<G,U>}$ with 2-dimensional cyclicity is set as computation of its minimum generator system $< G, U >$ including invertible vectors G and U having order q.

Algorithm for generating a hidden group with 2-dimensional cyclicity:

1. Using the invertibility condition $a_0a_1 \neq a_2a_3$, generate a random invertible vector $A = (a_0, a_1, a_2, a_3)$ such that $\{a_2 \neq 0;\ a_3 \neq 0\}$ and compute the value

$$\Delta = (a_0 - a_1)^2 + 4\lambda a_2 a_3.$$

2. If $\Delta \neq 0$ is a quadratic non-residue, then go to step 1.

3. Calculate the vector $G = A^{\frac{p-1}{q}} = A^2$.

4. If $G = E$, then go to step 1. Otherwise generate a primitive element $s \in GF(p)$ and compute the scalar vector $S = sE = (s, s, 0, 0)$.

5. Generate a random integer $k < q$ and compute the vector

$$U = S^{\frac{p-1}{q}} \circ G^k.$$

6. Output the permutable vectors G and U each of which has order equal to 256-bit prime q.

Note the step 2 outputs a vector A that is an element of the commutative group of the Γ_1-type. This algorithm works quickly due to the fact that the number of the Γ_1-type groups is equal to $k = 2^{-1}p(p+1)$, and the latter contain about $k(p-1)^2 \approx 2^{-1}p^4$ elements of the used 4-dimensional FNAA, i. e. about half of all invertible 4-dimensional vectors.

Generation of the parameters of masking operations:

1. Select at random an invertible vector A possessing order equal to the value $p^2 - 1$, which satisfies the condition $G \circ A \neq A \circ G$.

2. Select at random an invertible vector B possessing order equal to the value $p^2 - 1$, which satisfies the conditions $B \circ A \neq A \circ B$ and $G \circ B \neq B \circ G$

The private values A and B are used as parameters of masking operations.

Computation of the public key (W, Y, Z):

1. Select a random integer $1 < x < q$ and compute the vector $W = A \circ G^x \circ B^{-1}$.

2. Compute the vectors $Y = B \circ G \circ B^{-1}$ and $Z = B \circ U \circ A^{-1}$.

The value x is an element of private key. The size of the public key (W, Y, Z) is equal to $\approx$ 384 bytes. Computational difficulty of the

public-key generation procedure is roughly equal to one exponentiation in the 4-dimensional FNAA (computational complexity of one exponention in the FNAA equals on the average to ≈ 3072 multiplications in $GF(p)$).

5.2 Signature generation procedure

Suppose one is to compute a signature to the electronic document M, using some specified 256-bit hash-function f_H.

The signature to the electronic document M is computed using the private key (x, A, B, G, U) as folows:

1. Using random integers $k < q$ and $t < q$, compute the vector

$$V = A \circ G^k \circ U^t \circ A^{-1}.$$

2. Compute the value e (the first signature element) from the document M to which the vector V is concatenated: $e = f_H(M, V)$, where f_H is a specified hash-function.

3. Compute the second signature element s as solution of the following quadratic equation

$$es^2 - s + xt + t = k \bmod q.$$

If the last equation has no solution, then go to step 1.

4. Compute the third signature element

$$d = s^{-1}(t - s) \bmod q.$$

On the average, computation of a signature (e, s, d) requires performing the first, second, and third steps of the signature generation procedure two times. Therefore, computational difficulty of the signature generation is roughly equal to four exponentiations in the 4-dimensional FNAA (≈ 12300 multiplications in $GF(p)$). The signature size is equal to ≈ 768 bits (96 bytes).

5.3 Signature verification procedure

The verification of the signature (e, s, d) to the document M is performed on the public key (W, Y, Z) as folows:

1. Using the public key, compute the vector V':

$$V' = \left(W \circ Y^{es} \circ Z \circ (W \circ Y \circ Z)^d\right)^s.$$

2. Compute the hash-function value e' from the document M to which the vector V' is concatenated: $e' = f_H(M, V')$.

3. If $e' = e$, then the signature is genuine. Otherwise reject the signature.

The computational difficulty of the signature verification procedure is roughly equal to three exponentiation operations in the FNAA ($\approx$ 9200 multiplications modulo p).

Correctness proof of the signature algorithm consists in proving that the correctly computed signature (e, s, d) will pass the verification procedure as a genuine signature. Due to the mutual commutativity of the automorphism-map operation with the exponentiation operation we have the following:

$$\begin{aligned}
V'_1 &= \left(W \circ Y^{es} \circ Z \circ (W \circ Y \circ Z)^d\right)^s = \\
&= \left(A \circ G^x \circ B^{-1} \circ \left(B \circ G \circ B^{-1}\right)^{es} \circ B \circ U \circ A^{-1} \circ \right. \\
&\quad \left. \circ \left(A \circ G^x \circ B^{-1} \circ B \circ G \circ B^{-1} \circ B \circ U \circ A^{-1}\right)^{s^{-1}(t-s)}\right)^s = \\
&= A \circ G^{xs} \circ G^{es^2} \circ U^s \circ G^{x(t-s)} \circ G^{t-s} \circ U^{t-s} \circ A^{-1} = \\
&= A \circ G^{es^2-s+xt+t} \circ U^t \circ A^{-1} = \\
&= A \circ G^k \circ U^t \circ A^{-1} = V \quad \Rightarrow \quad V' = V \;\Rightarrow\; e' = e.
\end{aligned}$$

6 Discussion

In the proposed signature scheme, the idea [11] of using a hidden commutative group possessing 2-dimensional cyclicity is exploited. However, the used method for implementing the advanced criterion of post-quantum security is different. Due to a novel design the signature size is reduced significantly and performance of the signature verification

procedure is improved. The used 4-dimensional FNAA set by a sparse BVMT provides about a twofold (and fourfold) increase in performance of the signature scheme in comparison with [11] (and [12]).

Like in the signature scheme [17], in the introduced one generation of the public key is performed using two different types of operations masking the hidden commutative group. The first type relates to the automorphism map operation possessing the property of mutual commutativity with the exponentiation operation (see the formula for computing the element Y of the public key). The second type relates to a map operation that is free of the property of mutual commutativity with the exponentiation operation (see formulas for computing the elements W and Z of the public key). However, masking operations of the second type are not arbitrary. Their parameters are chosen taking into account the fact that their compositions form a composite operation that has the said property of commutativity. An advantage of the introduced signature scheme against [17] is elimenation of doubling of both the verification equation and the public key.

An advantage of the introduced signature scheme is the use of the algebraic support for which one can evidently demonstrate the existence of the sufficiently large number of different commutative groups having 2-dimensional cyclicity (see formula (17)).

Table 3, where a procedure execution time* is estimated in multiplications in $GF(p)$, presents a rough comparison of the proposed signature scheme with the introduced earlier in [11], [12], [17]) ones (for the case of using a 257-bit prime).

To illustrate fulfillment of Criterion 1, consider the construction of some periodic functions based on public parameters of the proposed signature algorithm.

1. Suppose the function

$$F_1(i,j) = (W \circ Y \circ Z)^i \circ (W \circ Z)^j = A \circ G^{xi+i+j} \circ U^{i+j} \circ A^{-1}$$

includes a period with the length (δ_i, δ_j). Then, taking into account that G and U are generators of different cyclic groups of the same order q, we have $x\delta_i + \delta_i + \delta_j \equiv 0 \bmod q$ and $\delta_i + \delta_j \equiv 0 \bmod q$. From these two congruencies one gets: $x\delta_i \equiv 0 \bmod q \Rightarrow \delta_i \equiv \delta_j \equiv 0 \bmod q$. The last

Table 3. Comparison of the proposed and known signature schemes

Signature scheme	signature size, bytes	public-key size, bytes	sign. gener. time*	sign. verific. time*
[11]	192	768	18,432	24,576
[12]	256	1158	41,472	55,296
[17]	192	768	30,720	24,576
Proposed	96	384	12,300	9,200

means the function $F_1(i,j)$ possesses only the periodicity connected with the value q that is order of cyclic groups contained in the hidden commutative group with 2-dimensional cyclicity.

2. Suppose the function

$$F_2(i,j) = (Z \circ W)^i \circ Y^j = B \circ U^i \circ G^{xi} \circ G^j \circ B^{-1}$$

includes a period with the length (δ_i, δ_j). Then, we have $\delta_i \equiv 0 \bmod q$ and $x\delta_i + \delta_j \equiv 0 \bmod q \Rightarrow \delta_i \equiv \delta_j \equiv 0 \bmod q$, i. e., the function $F_2(i,j)$ also possesses only the periodicity connected with the value q.

7 Conclusion

An alternative design of the HDLP-based signature schemes satisfying the advanced criterion of post-quantum security is implemented in the introduced signature scheme. A new 4-dimensional FNAA set by a sparse BVMT is used as the algebraic carrier. For the first time, the types of the commutative groups contained in the algebraic carrier have been studied, and formulas for computing the number of the groups of every type have been obtained. To study the properties of the used FNAA, a method of computing sets of pairwise permutable vectors has been applied. This method is attractive to study properties of FNAAs of other types and dimensions.

The proposed signature scheme seems to be quite competitive with known candidates for post-quantum signature schemes. At the same time, one can suppose that other efficient designs for implementing Criterion 2 are possible.

Acknowledgement. *This work was partially supported by RSF and by the budget theme No. 0060-2019-010.*

References

[1] *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings* (Lecture Notes in Computer Science, vol. 10786, Security and Cryptology), Tanja Lange, Rainer Steinwandt, Eds. Springer International Publishing, 2018. ISBN: 978-3-319-79062-6.

[2] *Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers*, (Lecture Notes in Computer Science, vol. 11505, Security and Cryptology), Jintai Ding, Rainer Steinwandt, Eds. Springer International Publishing, 2019. ISBN: 978-3-030-25509-1.

[3] 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.

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

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

[6] D.N. Moldovyan, N. A. Moldovyan, and A. A. Moldovyan, "Commutative Encryption Method Based on Hidden Logarithm Problem," *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software*, vol. 13, no. 2, pp. 54–68, 2020. DOI: 10.14529/mmp200205.

[7] 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.

[8] 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*, vol. 12, no. 1, pp. 66–81, 2019. DOI: 10.14529/mmp190106.

[9] 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).

[10] 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. 2(93), pp. 62–67, 2020.

[11] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "Digital signature scheme with doubled verification equation," *Computer Science Journal of Moldova*, vol. 28, no. 1(82), pp. 80–103, 2020.

[12] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "An enhanced version of the hidden discrete logarithm problem and its algebraic support," *Quasigroups and Related Systems*, vol. 28, no. 2, pp. 269–284, 2020.

[13] 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.

[14] N.A. Moldovyan and P.A. Moldovyanu, "New primitives for digital signature algorithms," *Quasigroups and Related Systems*, vol. 17, no. 2, pp. 271–282, 2009.

[15] N.A. Moldovyan, "Fast signatures based on non-cyclic finite groups," *Quasigroups and Related Systems*, vol. 18, no. 1, pp. 83–94, 2010.

[16] N. A. Moldovyan, "Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263–270, 2020.

[17] N. A. Moldovyan and A. A. Moldovyan, "Candidate for practical post-quantum signature scheme," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 16, no. 4, pp. 455–461, 2020. https://doi.org/10.21638/11701/spbu10.2020.410 (in English).

D. N. Moldovyan

Received December 28, 2020
Accepted June 14, 2021

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: mdn.spectr@mail.ru