Computer Science Journal of Moldova, vol.**28**, no.1(82), 2020

Digital signature scheme with doubled verification equation

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

Abstract

A novel design of the signature schemes based on the hidden discrete logarithm problem is proposed, which is characterized in using special criterion oriented to providing security to potential quantum attacks. The criterion consists in the requirement to ensure practical intractability of the task of constructing a periodic function with a period depending on the value of a discrete logarithm in a hidden cyclic group. A signature scheme satisfying the mentioned criterion is introduced. A 4-dimensional finite non-commutative associative algebra is considered as algebraic support. To implement the signature scheme, a commutative hidden group defined by generator system $< N, Q >$, where vectors N and Q have the same prime order, is exploited. For further development of the introduced method, an 8-dimensional algebra is proposed.

Keywords: finite non-commutative algebra, hidden logarithm problem, public-key cryptoscheme, digital signature, post-quantum cryptoscheme.

MSC 2010: 94A60, 16Z05, 14G50, 11T71, 16S50.

1 Introduction

Development of practical post-quantum signature schemes represents a current challenge in the area of the applied and theoretic cryptography [1], [2]. Currently nine signature schemes proposed in framework of the NIST competition [3] are considered as candidates for post-quantum signature standard. A significant disadvantage of those schemes is a large size of public key and signature, except for GeMSS

and Rainbow signature schemes. In the latter, the signature size is relatively small, but the public key size is extremely large. In terms of the trade off between performance and size of the public key and the signature, the preferred post-quantum signature schemes are Falcon-512 (657-byte signature; 897-byte public key) and Dilithium-1024x768 (2044-byte signature; 1184-byte public key).

A promissing approach to the design of the public-key post-quantum cryptoschemes with sorter size of signature and public key represents using so called hidden discrete logarithm problem (HDLP) as the post-quantum cryptographic primitive [4], [5]. Several HDLP-based signature schemes are described in the papers [6], [7]. Usually the HDLP used in the signature schemes is set in the m-dimensional ($m = 4, 6$) finite non-commutative associative algebras (FNAAs) as follows.

One selects a random integer $x < q$ and a random cyclic group contained in the used FNAA and generated by some m-dimensional vector N having order equal to the prime q of sufficiently large size. Then he computes vector N^x and performs homomorphism-map operations ψ_1 and ψ_2 obtaining public key in the form of the following two vectors $Y = \psi_1(N^x)$ and $Z = \psi_2(N)$ or three vectors (Y, Z, T), where vector T plays the role of a fitting parameter in verification equation. The cyclic group generated by the vector N is called the base group. The vectors Y, Z, and T are contained in other three different cyclic groups (contained in the used FNAA as different subsets of vectors).

Due to mutual commutativity of each of the masking operations ψ_1 and ψ_2 with the exponentiation operation, different signature schemes based on the computational difficulty of the discrete logarithm problem (see, for example, [8], [9]) can be used as prototypes of the HDLP-based cryptoschemes.

The earlier proposed rationale of the security of the known HDLP-based signature schemes to the quantum attacks (attacks with using a hypothetic quantum computer) is quite straightforward: in the case of the HDLP-based signature schemes, potential attacker knows no elements of the base cyclic group in which the exponentiation operation is performed, therefore, to compute the value x, one cannot directly use

the Shor quantum algorithm [10] for finding logarithm in a cyclic group.

For a more convincing justification of the security to quantum attacks, an additional criterion can be adopted, which is aimed at preventing the possibility of constructing periodic functions with a period depending on the value of the discrete logarithm in the base cyclic group, regardless of the fact that the periodic function takes on only values from the same finite group. The HDLP-based signature schemes proposed in [6],[7],[11] do not satisfy this criterion, since one can define the following periodic function $F(i,j) = Y^i \circ T \circ Z^j$ in two integer variables i and j, which contains a period with the length equal to $(-1, x)$. Indeed, we have $Y^i \circ T \circ Z^j = Y^{i-1} \circ T \circ Z^{j+x}$. This function takes on values in different groups contained in the FNAA used as algebraic carrier of the signature scheme, however, one can suppose that an advanced quantum algorithm for evaluating the period of the function $F(i,j)$ can be potentially developed.

In the present paper a new HDLP-based signature scheme is proposed which meets the criterion of ensuring practical intractability of the task of constructing a periodic function with a period depending on the value of a discrete logarithm in a hidden cyclic group. The proposed criterion introduces significant limitations in the development of the HDLP-based signature schemes, which were overcome by using a three-element signature and doubling the verification equation. Besides, a commutative group defined by generator system $< N, Q >$, where the vectors N and Q have the same prime order, is applied as the hidden group in which the basic exponentiation operation is performed. A 4-dimensional FNAAs set over the ground finite field $GF(p)$, where prime $p = 2q + 1$ and q is a 255-bit prime, are proposed as algebraic support for implementing the proposed signature scheme. This algebra contains p^2 global left-sided units and p^2 different isomorphic commutative groups of the order $(p-1)^2$. As a promising algebraic support for further development of the proposed method for constructing post-quantum signature schemes, an 8-dimensional algebra with a global two-sided unit is proposed.

2 Preliminaries

2.1 Defining FNAAs

Suppose the m-dimensional vector space is defined over the ground finite field $GF(p)$. Introducing the vector multiplication operation that is distributive at the left and at the right relatively the addition operation, one gets the m-dimensional finite algebra. If the defined multiplication operation is non-commutative and associative, then we have FNAA. To define the vector multiplication operation, one can use the notion of formal basis vectors denoted as $\mathbf{e}_0 = (1, 0, 0 \ldots, 0)$, $\mathbf{e}_1 = (0, 1, 0 \ldots, 0)$, ... $\mathbf{e}_{m-1} = (0, 0 \ldots, 0, 1)$ and representation of some two vectors $A = (a_0, a_1, \ldots a_{m-1})$ and $B = (b_0, b_1, \ldots b_{m-1})$ in the form of the following summs of the single component vectors $a_i\mathbf{e}_i$ and $b_i\mathbf{e}_i$: $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$.

The vector multiplication operation (denoted as $\circ$) is defined by the following formula $A \circ B = \sum_{j=0}^{m-1} \sum_{i=0}^{m-1} a_i b_j \, (\mathbf{e}_i \circ \mathbf{e}_j)$, where 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 $\lambda\mathbf{e}_k$. The rule of the mentioned substitution is usually given by so called basis vector multiplication table (BVMT), like Table 1 (see Subsection 2) and Table 2 (Section 3).

It is assumed that the intersection of the ith row and the jth column defines the cell which contains the value $\lambda\mathbf{e}_k = \mathbf{e}_i \circ \mathbf{e}_j$, where the value $\lambda \neq 1$ is called structural coefficient. To build a FNAA, one should compose and use some BVMT defining non-commutative associative multiplication operation. Clearly, to implement the associativity property, it is sufficient to use the BVMP for which the condition $(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)$ holds true for all possible triples (i, j, k).

2.2 Finite algebra with multiplicative group possessing two-dimensional cyclicity

In the paper [12] it is shown that the multiplicative group Γ of the finite 2-dimensional commutative algebra with the multiplication operation defined by Table 1, where the structural coefficient λ is a quadratic residue in $GF(p)$, has order $\Omega = (p-1)^2$ and includes the generator

system $< G'_1, G'_2 >$, where each of the vectors G'_1 and G'_2 has order $\omega = p - 1$. One can easily show the group Γ' contains p finite cyclic groups Γ'_c of the order $p-1$. The finite groups generated by a generator system in which each element has the same order value are called groups with multi-dimensional cyclicity [13].

When constructing public-key cryptosystems based on the computational complexity of the discrete logarithm problem, one uses cyclic groups whose order is equal to a prime number of sufficiently large size. This defines interest to the case of defining the finite algebras over the field $GF(p)$ whose characteristic p is such that the integer $p-1$ contains a large prime divisor, for example $p = 2q+1$, where q is a prime. In the last case the group Γ' contains the commutative subgroup Γ generated by the generator system $< G_1, G_2 >$, in which each of the vectors G_1 and G_2 has order q. Evidently, some fixed integers i and j ($0 < i < q$; $0 < j < q$) define the vector $G_{ij} = G_1^i \circ G_2^j$ 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 1. The BVMT setting the 2-dimensional commutative algebra.

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

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

Proposition 1 is used in the designed signature schemes (see Sections 4 and 5) to prevent construction of the periodic functions on the basis of using the elements of the public key, the period of which is defined by discrete logarithm in the hidden cyclic group. One can note that the subgroup Γ contains $q^2 - 1$ elements $G \neq (1, 0)$ that are distributed among $q + 1$ different cyclic groups of order q which include only one common element, namely, the unit element (1,0).

3 Algebraic support of the proposed signature scheme

3.1 The used 4-dimensional algebra

For development of the HDLP-based signature scheme satisfying the criterion of practical intractability of the task of constructing a periodic function with a period depending on the value of a discrete logarithm in a hidden cyclic group we have used the 4-dimensional FNAA containing p^2 different global left-sided units L, which is defined over the field $GF(p)$ using the BVMT presented as Table 2.

To obtain the formula describing the set of the L-units, the following vector equation is to be considered: $X \circ A = A$, where $A = (a_0, a_1, a_2, a_3)$ is a fixed 4-dimensional vector and $X = (x_0, x_1, x_2, x_3)$ is the unknown. Using Table 2, one can represent the vector equation in the form of the following system of four linear equations:

$$\begin{cases} (x_0 + x_1)\, a_0 + \lambda\, (x_2 + x_3)\, a_2 = a_0; \\ (x_0 + x_1)\, a_2 + (x_2 + x_3)\, a_0 = a_2; \\ (x_0 + x_1)\, a_1 + \lambda\, (x_2 + x_3)\, a_3 = a_1; \\ (x_0 + x_1)\, a_3 + (x_2 + x_3)\, a_1 = a_3. \end{cases} \tag{1}$$

Using the variable substitution $u_1 = x_0 + x_1$ and $u_2 = x_2 + x_3$, one can represent the system (1) in the form of the following two independent systems of two linear equations:

$$\begin{cases} u_1 a_0 + \lambda u_2 a_2 = a_0; \\ u_1 a_2 + u_2 a_0 = a_2; \end{cases} \tag{2}$$

$$\begin{cases} u_1 a_1 + \lambda u_2 a_3 = a_1; \\ u_1 a_3 + u_2 a_1 = a_3. \end{cases} \tag{3}$$

For arbitrary vector A satisfying the conditions $a_0^2 \neq \lambda a_1^2$ and $a_1^2 \neq \lambda a_3^2$, each of the systems (2) and (3) has the same unique solution $u_1 = 1$ and $u_2 = 0$. One can easily see that the indicated solution satisfies the systems (2) and (3) for all elements of the considered FNAA (in

Table 2. The BVMT for defining the 4-dimensional FNAA ($\lambda \neq 0$).

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

the cases $a_0^2 \neq \lambda a_1^2$ and $a_1^2 \neq \lambda a_3^2$ there exist some additional solutions defining local left-sided units). Thus, the solution $(u_1, u_2) = (1, 0)$ defines the set of the global left-sided units X, the coordinates of which satisfy the conditions $x_0 + x_1 = u_1 = 1$ and $x_2 + x_3 = u_2 = 0$. These left-sided units are called global, since every of them acts as the left-sided unit on every vector in the FNAA. The set of p^2 global left-sided units L is described as follows:

$$L = (l_0, l_1, l_2, l_3) = (h, 1-h, k, -k)\,, \tag{4}$$

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

The considered FNAA contains local right-sided units R acting in some subsets of the algebra elements. The local right-sided unit R_A relating to some vector A can be computed as solution of the vector equation $A \circ X = A$ that can be easily reduced to the following two systems of two linear equations:

$$\begin{cases} (a_0 + a_1)\, x_0 + \lambda\,(a_2 + a_3)\, x_2 = a_0; \\ (a_2 + a_3)\, x_0 + (a_0 + a_1)\, x_2 = a_2; \end{cases} \tag{5}$$

$$\begin{cases} (a_0 + a_1)\, x_1 + \lambda\,(a_2 + a_3)\, x_3 = a_1; \\ (a_2 + a_3)\, x_1 + (a_0 + a_1)\, x_3 = a_3. \end{cases} \tag{6}$$

Each of the systems (5) and (6) has the same main determinant Δ_A:

$$\Delta_A = (a_0 + a_1)^2 - \lambda\,(a_2 + a_3)^2\,. \tag{7}$$

Thus, in the case $\Delta_A \neq 0$, the equation $A \circ X = A$ has a unique solution $X = R_A$ and the single right-sided unit $R_A = (r_0, a_1, r_2, a_3)$ relates to the vector A. One can obtain the following formula for computing the value R_A:

$$R_A = \left(\frac{a_0 (a_0 + a_1) - \lambda a_2 (a_2 + a_3)}{\Delta}, \frac{a_1 (a_0 + a_1) - \lambda a_3 (a_2 + a_3)}{\Delta}, \right.$$
$$\left. \frac{a_1 a_2 - a_0 a_3}{\Delta}, \frac{a_0 a_3 - a_1 a_2}{\Delta} \right). \tag{8}$$

The value R_A acts as the local right-sided unit in the frame of the sequence of the vectors $A, A^2, \ldots, A^i, \ldots$. Besides, the latter sequence is periodic and composes a finite cyclic group with the unit R_A, i. e., the element R_A is the single local two-sided unit E_A relating to the vector A (and to cyclic group generated by the vector A).

Proposition 2. *The local right-sided unit R_A is simultaneously the local two-sided unit E_A relating to the vector A.*

Proof. It is sufficient to show that the vector R_A is contained in the set (4) of the global left-sided units. Suppose in (4) we have $h = r_0$ and $k = r_2$. Then one can compute

$$1 - h = 1 - r_0 = 1 - \frac{a_0 (a_0 + a_1) - \lambda a_2 (a_2 + a_3)}{\Delta} =$$
$$= \frac{a_1 (a_0 + a_1) - \lambda a_3 (a_2 + a_3)}{\Delta} = r_1;$$

$$-k = -r_2 = -\frac{a_1 a_2 - a_0 a_3}{\Delta} = \frac{a_0 a_3 - a_1 a_2}{\Delta} = r_3.$$

Thus, the vector R_A is equal to the global left-sided unit corresponding to the integers $h = r_0$ and $k = r_2$. □

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 the unit of the cyclic group generated by the vector A.*

Proof. Let us consider the sequence of the vectors $A, A^2, \dots A^h, \dots A^k, \dots$. For all integer values i one has $A^i \neq O$, where $O = (0,0,0,0)$, since $\Delta_A \neq 0$. Due to finiteness of the considered algebras and condition $\Delta_A \neq 0$, the indicated sequence is periodic, i. e., for some integer h and some minimum integer $k > h$ we have the following:

$$A^k = A^h \Rightarrow A^h \circ A^{k-h} = A^h \Rightarrow A^{h-1} \circ \Big(A \circ A^{k-h} - A\Big) = O \Rightarrow$$
$$A \circ A^{k-h} - A = O \Rightarrow A \circ A^{k-h} = A \Rightarrow A^{k-h} = R_A,$$
$$A \circ A^{k-h} = A \Rightarrow A^{k-h} \circ A = A \Rightarrow A^{k-h} = L_A = R_A = E_A.$$

Thus, the vector E_A is the unit of the cyclic group containing elements $\big\{A, A^2, \dots A^\omega\big\}$, where $\omega = k - h$, and Proposition 3 holds true. □

The Proposition 3 shows $A^{\omega-i} \circ A^i = A^i \circ A^{\omega-i} = E_A$, i. e., the vector $A^{\omega-i}$ is the inverse value of the vector A^i relatively the local two-sided unit E_A. Therefore, the value ω can be called the local order of the vector A and the last can be called a locally invertible vector.

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

Proof. $(S \circ L_i) \circ A = S \circ (L_i \circ A) = S \circ A = B$. Suppose $S \circ L_i = S \circ L_j$, then $S \circ (L_i - L_j) = (0,0,0,0)$ and $L_i = L_j$. Therefore, the number of different solutions is equal to the number of different L-units, i. e., to p^2. The Proposition 4 is proven. □

Proposition 5. *Suppose the vector L is a global left-sided unit. Then the map of the FNAA defined by the formula $\varphi_L(X) = X \circ L$, where the vector X takes on all values in the algebra, is a homomorphism.*

Proof. For two arbitrary vectors X_1 and X_2 we have
$$\varphi_L(X_1 \circ X_2) = (X_1 \circ X_2) \circ L = (X_1 \circ L) \circ (X_2 \circ L) =$$
$$= \varphi_L(X_1) \circ \varphi_L(X_2);$$
$$\varphi_L(X_1 + X_2) = (X_1 + X_2) \circ L = X_1 \circ L + X_2 \circ L =$$
$$= \varphi_L(X_1) + \varphi_L(X_2).$$
□

Proposition 6. *All locally invertible vectors of the considered 4-dimensional FNAA form p^2 different groups with p^2 different units $E = (h, 1-h, k, -k)$, where $h, k = 0, 1, 2, \dots p-1$.*

Proof. Suppose the set $\{A_1, A_2, \dots A_i, \dots A_\Omega\}$ of locally invertible vectors includes all vectors relating to a fixed local two-sided unit E (including the vector E) and only such vectors. It is easy to see this set is the group Γ_E with the unit E. Every fixed global left-sided unit L' from the set (4) is the unit E' of some group $\Gamma_{E'}$ representing a set of locally invertible vectors $\{A'_1, A'_2, \dots A'_i, \dots A'_\Omega\}$. Indeed, due to the Proposition 5, we have $A'_i = A_i \circ L'$ for $i = 1, 2, \dots \Omega$, and $E' = E \circ L' = L'$. The considered FNAA contains p^2 different global left sided units $E = (h, 1-h, k, -k)$, where $h, k = 0, 1, 2, \dots p-1$, every one of which defines a unique group of the order Ω. □

Proposition 7. *If the structural coefficient λ is a quadratic non-residue, then the considered 4-dimensional FNAA contains $p^2\left(p^2-1\right)$ locally invertible vectors. If λ is a quadratic residue, then the algebra contains $p^2\left(p-1\right)^2$ locally invertible vectors.*

Proof. Condition of the local invertibility of the vector A is $\Delta_A \neq 0$. Let us compute the number of non-invertible vectors using the condition $\Delta_A = 0$. Using the formula (7), one can represent the last condition in the form of the following equation

$$a_0^2 + 2a_0a_1 + a_1^2 - \lambda\left(a_2 + a_3\right)^2 = 0.$$

If the coordinates of the vector A satisfy the last equation, then A is a non-invertible vector. Solving the equation relatively the unknown value a_0, one can get $a_0 = -a_1 \pm \sqrt{\lambda\left(a_2 + a_3\right)^2}$.

If λ is a quadratic non-residue, then solution exists only in the case $a_2 + a_3 = 0$, i. e. we have p different variants of the values of coodinates a_2 and a_3. In every of such variants the solution exists for arbitrary value a_1. Thus, the number of non-invertible vectors is equal to p^2. Correspondingly, the number μ of invertible vectors contained in the algebra is equal to $\mu = p^4 - p^2 = p^2\left(p^2-1\right)$.

If λ is a quadratic residue, then we have one value of the square root for the case $a_2 + a_3 = 0$ (p variants of the pairs of the values (a_2, a_3) : $a_2 + a_3 = 0$) and p^2 variants of the triples (a_1, a_2, a_3) for which the considered equation has a solution, i. e., p^2 non-invertible vectors. For the case $a_2 + a_3 \neq 0$ we have two values of the square root ($p^2 - p$ variants of the pairs of the values (a_2, a_3) : $a_2 + a_3 \neq 0$) and $2p\left(p^2 - p\right)$ variants of the triples (a_1, a_2, a_3) for which the considered equation has a solution, i. e., in the second case we have $2p\left(p^2 - p\right)$ non-invertible vectors.

Thus, taking into account both of the cases, one gets the number of non-invertible vectors equal to $2p\left(p^2 - p\right) + p^2 = 2p^3 - p^2$ and the value $\mu = p^4 - \left(2p^3 - p^2\right) = p^2\left(p - 1\right)^2$. The Proposition 7 is proven. □

Proposition 8. *The considered 4-dimensional FNAA contains p^2 isomorphic commutative groups and every locally invertible vector of the algebra is contained only in one of these groups. If the structural coefficient λ is a quadratic residue (non-residue), then every of these groups is cyclic (has 2-dimensional cyclicity) and its order is equal to $\Omega = p^2 - 1$ $\left(\Omega = (p-1)^2\right)$.*

Proof. Due to the Proposition 6, one should only derive a formula for the order Ω of every of p^2 isomorphic groups contained in the considered algebra and show that the algebra contains at least one cyclic group or one commutative group having 2-dimensional cyclicity.

Clearly we have $\Omega = \frac{\mu}{p^2} = p^2 - 1$, if the value λ is a quadratic residue, and $\Omega = \frac{\mu}{p^2} = (p-1)^2$, if the value λ is a quadratic non-residue.

One can easily see that the set of the vectors $(h, 0, k, 0)$, where $h, k = 0, 1, 2, \ldots p - 1$, represents subalgebra that is isomorphic with the commutative 2-dimensional algebra described in Subsection 2.2, therefore, the set of the invertible vectors in this subalgebra represents a cyclic group, if the value λ is a quadratic non-residue, or commutative group with 2-dimensional cyclicity, if the value λ is a quadratic residue [12]. The Proposition 8 is proven. □

Suppose the vector B is such that $\Delta_B \neq 0$ and L is a random global left-sided unit L. One can compute the single vector A that satisfies

the condition

$$B \circ A = L. \tag{9}$$

The main determinant of the system of linear equations, which corresponds to the vector equation (9), is equal to $\Delta_B \neq 0$, therefore, the equation (9) has a unique solution.

Proposition 9. *Suppose $B \circ A = L$. Then the formula $\psi_L = A \circ X \circ B$, where the vector X takes on all values in the considered 4-dimensional FNAA, sets the homomorphism map.*

Proof. For two arbitrary 4-dimensional vectors X_1 and X_2, one can get the following:
$\psi_L(X_1 \circ X_2) = A \circ (X_1 \circ X_2) \circ B = A \circ (X_1 \circ L \circ X_2) \circ B =$
$= (A \circ X_1 \circ B) \circ \left(A \circ X_2 \circ B^t\right) = \psi_L(X_1) \circ \psi_L(X_2)$;
$\psi_L(X_1 + X_2) = A \circ (X_1 + X_2) \circ B = (A \circ X_1 \circ B) + (A \circ X_2 \circ B) =$
$= \psi_L(X_1) + \psi_L(X_2)$. □

Proposition 10. *The homomorphism-map operation $\psi_L(X) = A \circ X \circ B$ 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 9, we have $\psi_L(X^k) = (\psi_L(X))^k$, i. e., $A \circ X^k \circ B = (A \circ X \circ B)^k$. □

3.2 Perspective 8-dimensional algebra

In algebras with a global two-sided unit, local masking operations can be applied that operate within the set of non-invertible elements of the algebra. Methods for setting local masking operations are quite diverse and are of interest for building digital signature schemes (see, for example, [14]). The possibility of setting new types of masking operations is due to the fact that a large number of local left-sided units and a large number of local right-sided units operate simultaneously on some fixed subsets of non-invertible elements. Implementation of the signature schemes with doubled verification equation on the base on FNAAs of such type represent significant interest. However, the

developer needs to use FNAAs containing commutative groups with two-dimensional cyclicity.

Algebra with the multiplication operation specified in Table 3 solves this problem when selecting a structural coefficient λ equal to the quadratic residue in the field $GF(p)$. However, this algebra is an object of independent research focused on obtaining formulas that define the criterion of non-invertibility of vectors and describe the sets of local right-sided and local left-sided units for a fixed non-invertible vector, as it had been done for 4-dimensional FNAAs considered in the works [6], [14].

Besides, one should develop a procedure for computing the generator system $< N, Q >$ defining the hidden commutative group with two-dimensional cyclicity. The following three possibilities represent interest for implementing the signature schemes with doubled verification equation: i) N is a non-invertible vector and Q is invertible; ii) N and Q are non-invertible vectors; iii) N and Q are invertible vectors. In each of the cases for many different fixed pairs of integers (u, w) the vectors $N^u \circ Q^w$ are generators of different cyclic groups of the same order q.

Table 3. The BVMT defining the 8-dimensional FNAA with global two-sided unit ($\lambda \neq 0$, $\mu \neq 0$, $\mu \neq 1$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mu\mathbf{e}_6$	$\mu\mathbf{e}_7$	$\mu\mathbf{e}_0$	$\mu\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mu\mathbf{e}_7$	$\lambda\mu\mathbf{e}_6$	$\mu\mathbf{e}_1$	$\lambda\mu\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$
$\mathbf{e}_2$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mu\mathbf{e}_3$	$\lambda\mu\mathbf{e}_2$	$\mu\mathbf{e}_5$	$\lambda\mu\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_6$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_7$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$

For the said 8-dimensional algebra, one can select a random invertible vector N of the order q and number β having order q in $GF(p)$, for

which the pair of the vectors N and $Q = \beta N$ (scalar multiplication) with high probability compose the generator system of some commutative group with two-dimensional cyclicity. When using this pair of vectors and various variants of the automorphism map operation as masking operations, the said 8-dimensional FNAA can be used as algebraic support for implementing some versions of the signature scheme described in the next section.

For example, in the case of prime $p = 2q + 1 = 501659$, prime $q = 250829$, $\lambda = 4$, $\mu = 2$, and $\beta = 123456$ we have:
$N = (22334; 57857; 35656; 45457; 17645; 61268; 62597; 57864)$
$Q = \beta N =$
$= (148440; 172950; 391070; 381818; 177742; 389465; 419996; 33824)$
$N^q = Q^q = E = (501658;\ 0;\ 501658;\ 0;\ 1;\ 0;\ 2;\ 0)$,
where E is the global two-sided unit.

4 The proposed signature scheme

4.1 Generation of the hidden commutative group

The 4-dimensional FNAA described in Section 3 and defined over the field $GF(p)$ with characteristic $p = 2q + 1$, where q is a 255-bit prime, is used as algebraic support of the designed signature scheme. The hidden finite group $\Gamma_{<N,Q>}$ is generated as computation of its basis $< N, Q >$ that includes two vectors N and Q each of which has order equal to the prime q. The basis $< N, Q >$ is computed as follows:

1. Generate a random value d that is a primitive element modulo p. The primitive element d defines a locally invertible vector $G_1 = (d, 0, 0, 0)^z \neq (1, 0, 0, 0)$, where $z = \frac{p-1}{q}$, having order equal to the prime q.

2. Generate the vector $G_2 = (b, 0, r, 0)^z$, where $b < p - 1$ and $r < p - 1$ are such random numbers that the vector G_2 has order equal to q. (For example, generate several different pairs of random numbers b' and r' and compute $G'_2 = (b', 0, r', 0)^z$ and take the value $G'_2 \neq (1, 0, 0, 0)$ as the vector G_2.)

3. Generate a random global left-sided unit L_r and a random num-

ber $u < q$ and compute the vectors N and Q of the order q as follows:

$$N = G_1 \circ G_2^u \circ L_r; \qquad Q = G_2 \circ L_r.$$

The vectors G_1 and G_2 represent the basis $< G_1, G_2 >$ of the commutative group with the unit element equal to $E = (1, 0, 0, 0)$ (see the proof of the Proposition 8). Since the multiplication at the right by any global left-sided unit defines a homomorphism map of the algebra, the vectors N and Q define the basis $< N, Q >$ of some commutative group of the order equal to q^2, which has 2-dimensional cyclicity. It is easy to see the unit element of the hidden commutative group $\Gamma_{<N,Q>}$ is the vector $E = (1, 0, 0, 0) \circ L_r = L_r$.

4.2 Generation of parameters of masking operations

The exponentiation operations performed in two different cyclic groups contained in the hidden commutative group are used as base operations. Vector N is used as generator of the first of these cyclic groups. Generator J of the second cyclic group is computed as follows:

1. Generate two random integers $t < q$ and $u < q$.
2. Compute the vector $J = N^t \circ Q^u$.

The values N, J, N^x, and J^x, where $x < q$ is an element of the private key, are used to compute the elements $\psi_0 (N \circ Q)$, $\psi_1 (N^x)$, $\psi_0 (J \circ Q)$, and $\psi_2 (J^x)$, of the public key. Thus, the elements N and J are masked performing multiplication by the vector Q followed by performing the ψ_0-map operation, and the vectors N^x and J^x are masked performing the ψ_1-map and ψ_2-map operations, correspondingly. Parameters of the homomorphism-map operations $\psi_0(X) = C \circ X \circ D$, $\psi_1(X) = A_1 \circ X \circ B_1$, and $\psi_2(X) = A_2 \circ X \circ B_2$ are computed as follows:

1. Select a random global left-sided unit L_0 (for example, using the formula (4)), generate a random locally invertible vector D, and compute the value C as solution of the following vector equation $D \circ C = L_0$. (It has a unique solution, since $\Delta_D \neq 0$.)

2. Select a random global left-sided unit L_1, generate a random locally invertible vector B_1, and compute the value A_1 as solution of the vector equation $B_1 \circ A_1 = L_1$.

3. Generate two random integers $h < p - 1$ and $k < p - 1$, take the

global left-sided unit $L_2 = (h, 1-h, k, -k)$, generate a random locally invertible vector B_2 ($\Delta_{B_2} \neq 0$), and compute the value A_2 as solution of the vector equation $B_2 \circ A_2 = L_2$.

4.3 Public and private kyes

Public key represents the following two triples of the vectors (Y_1, Z_1, T_1) and (Y_2, Z_2, T_2) which are computed as follows:

1. $Y_1 = A_1 \circ N^x \circ B_1$; $\quad Z_1 = C \circ N \circ Q \circ D$.
2. $Y_2 = A_2 \circ J^x \circ B_2$: $\quad Z_2 = C \circ J \circ Q \circ D$.
3. $T_1 = A_1 \circ D \circ L$, where L is a random global left-sided unit.
4. $T_2 = A_2 \circ D \circ L'$, where L' is a random global left-sided unit.

One can consider private key as the set of all secret elements used to compute the public key and the signature. In another interpretation, the private key is a set of secret elements that are needed to calculate only the signature. We will use the second interpretation for which we have the private key representing the set of the values N, J, x, Q, A_1, A_2, and D.

4.4 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 generation algorithm is as follows:

1. Generate a random integer $k < q$ and a random locally invertible 4-dimensional vector K. Then compute the vectors V_1 and V_2:

$$\begin{cases} V_1 = A_1 \circ N^k \circ K; \\ V_2 = A_2 \circ J^k \circ K. \end{cases}$$

2. Compute the hash-function value e (the first signature element) from the document M to which the vectors V_1 and V_2 are concatenated: $e = f_H(M, V_1, V_2)$.

3. Compute the second signature element $s = k + xe \bmod q$.

4. Compute the third signature element S as solution of the following vector equation: $Q^s \circ D \circ S = K$.

The last vector equation has a unique solution, since the product of the locally invertible vectors Q^s and D is a locally invertible vector, i. e., the main determinant Δ of the system of four linear equations corresponding to the last vector equation satisfies the condition $\Delta \neq 0$. The major contribution to the computational complexity of the fourth step in the last procedure is introduced by the exponentiation operation.

Thus, in the introduced signature scheme the digital signature is composed from three elements, two 256-bit integers e and s and one vector S. On the whole, the computational difficulty of the signature generation procedure can be estimated as three exponentiation operations in the FNAA used as algebraic support (roughly equal to three exponentiations mod$p$ for 1024-bit prime p, for example, in the Schnorr signature scheme [8]).

4.5 Signature verification procedure

Suppose one is to verify the signature (e, s, S) to the document M, using the public key $(Y_1, Z_1, T_1;\ \ Y_2, Z_2, T_2)$. The signature verification procedure is as follows:

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

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

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

3. Compute the value Δ_S (see formula (7)) 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 the false one.

4.6 Correctness proof

Correctness proof of the signature scheme consists in proving that the signature (e, s, S) computed correctly will pass the verification proce-

dure 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:

$$\begin{aligned}
V_1' &= Y_1^{-e} \circ T_1 \circ Z_1^s \circ S = \\
&= (A_1 \circ N^x \circ B_1)^{-e} \circ T_1 \circ (C \circ (N \circ Q) \circ D)^s \circ S = \\
&= A_1 \circ N^{-ex} \circ B_1 \circ A_1 \circ D \circ L \circ C \circ (N^s \circ Q^s) \circ D \circ S = \\
&= A_1 \circ N^{-ex} \circ L_1 \circ D \circ C \circ N^s \circ D \circ C \circ Q^s \circ D \circ S = \\
&= A_1 \circ N^{-ex} \circ L_0 \circ N^{k+ex} \circ L_0 \circ Q^s \circ D \circ S = \\
&= A_1 \circ N^{-ex+k+ex} \circ K = A_1 \circ N^k \circ K = V_1; \\
V_2' &= Y_2^{-e} \circ T_2 \circ Z_2^s \circ S = \\
&= (A_2 \circ J^x \circ B_2)^{-e} \circ T_2 \circ (C \circ (J \circ Q) \circ D)^s \circ S = \\
&= A_2 \circ J^{-ex} \circ B_2 \circ A_2 \circ D \circ L' \circ C \circ (J^s \circ Q^s) \circ D \circ S = \\
&= A_2 \circ J^{-ex} \circ L_2 \circ D \circ C \circ J^s \circ D \circ C \circ Q^s \circ D \circ S = \\
&= A_2 \circ J^{-ex} \circ L_0 \circ J^{k+ex} \circ L_0 \circ Q^s \circ D \circ S = \\
&= A_2 \circ N^{-ex+k+ex} \circ K = A_2 \circ N^k \circ K = V_2.
\end{aligned}$$

Since $V_1' = V_1$ and $V_2' = V_2$, the equality $e' = e$ holds true. Besides, the correctly computed signature element S is a locally invertible vector, therefore, the inequality $\Delta_S \neq 0$ holds true.

5 Alternative design

When using the 8-dimensional FNAA with global two-sided unit as algebraic support, one can propose the following signature scheme with doubled verification equation, in which automorphism-map operations $\alpha_V(X) = V \circ X \circ V^{-1}$ (mutually commutative with the exponentiation operation) are used as masking ones.

Computation of the public key is performed as follows:

1. Generate at random the invertible vector N of the order q and integer $\beta \in GF(p)$ of the order q and compute the vectors $Q = \beta N$

and $J = N \circ Q^z$, where z is a random integer ($z < q$).

2. Generate at random the integer $x < q$ and the invertible vectors A_1 and A_2. Then compute the public-key elements $Y_1 = A_1 \circ N^x \circ A_1^{-1}$ and $Y_2 = A_2 \circ J^x \circ A_2^{-1}$.

3. Generate at random the integer $u < q$ and the invertible vector B_1. Then compute the vector $B_2 = B_1 \circ Q^u$ and the public-key elements $Z_1 = B_1 \circ N \circ Q \circ B_1^{-1}$, $T_1 = A_1 \circ B_1^{-1}$, $Z_2 = B_2 \circ J \circ Q \circ B_2^{-1}$, and $T_2 = A_2 \circ B_2^{-1}$.

The signature generation is performed as follows:

1. Generate at random the integer $k < q$ and the invertible vector K. Then compute $V_1 = A_1 \circ N^k \circ K$ and $V_2 = A_2 \circ J^k \circ Q^{-u} \circ K$.

2. Using a specified hash function f_H, compute the first signature element e: $e = f_H(M, V_1, V_2)$, where M is a document to be signed.

3. Compute the second signature element s: $s = k + ex \bmod q$.

4. Compute the third signature element $S = B_1 \circ Q^{-s} \circ K$.

The signature verification is performed as follows:

1. Using the signature (e, s, S) and the public key $(Y_1, Z_1, T_1;\ \ Y_2, Z_2, T_2)$, compute the vectors V_1' and V_2': $V_1' = Y_1^{-e} \circ T_1 \circ Z_1^s \circ S;\ \ V_2' = Y_2^{-e} \circ T_2 \circ Z_2^s \circ S$.

2. Compute the hash-function value $e' = f_H(M, V_1', V_2')$.

3. If $e' = e$ and S is an invertible vector, then the signature is genuine. Otherwise the signature is rejected.

Correctness proof of the signature scheme:

$$
\begin{aligned}
V_1' &= Y_1^{-e} \circ T_1 \circ Z_1^s \circ S = \\
&= \left(A_1 \circ N^x \circ A_1^{-1}\right)^{-e} \circ A_1 \circ B_1^{-1} \circ \left(B_1 \circ (N \circ Q) \circ B_1^{-1}\right)^s \circ S = \\
&= A_1 \circ N^{-ex} \circ N^s \circ Q^s \circ B_1^{-1} \circ S = \\
&= A_1 \circ N^{-ex+k+ex} \circ Q^s \circ B_1^{-1} \circ B_1 \circ Q^{-s} \circ K = \\
&= A_1 \circ N^k \circ K = V_1;
\end{aligned}
$$

$$
\begin{aligned}
V_2' &= Y_2^{-e} \circ T_2 \circ Z_2^s \circ S = \\
&= \left(A_2 \circ J^x \circ A_2^{-1}\right)^{-e} \circ A_2 \circ B_2^{-1} \circ \left(B_2 \circ (J \circ Q) \circ B_2^{-1}\right)^s \circ S = \\
&= A_2 \circ J^{-ex} \circ J^s \circ Q^s \circ B_2^{-1} \circ S = \\
&= A_2 \circ J^{-ex+k+ex} \circ Q^s \circ Q^{-u} \circ B_1^{-1} \circ B_1 \circ Q^{-s} \circ K = \\
&= A_2 \circ J^k \circ Q^{-u} \circ K = V_2.
\end{aligned}
$$

6 Discussion

In the known signature scheme [6] based on the computational difficulty of the HDLP the public key (Y, Z, T) is formed as a homomophism mapping of some elements N and N^x belonging to the same hidden cyclic group: $Z = \psi'(N)$ and $Y = \psi''(N^x)$, where ψ' and ψ'' are different homomorphism-map operations. Therefore, using these two values and the fitting element T of the public key, it is possible to construct a periodic function $f(i,j) = Y^i \circ T \circ Z^j$ containing a period that is determined by the value of the discrete logarithm x. Indeed, the condition $Y^{i-1} \circ T \circ Z^j = Y^i \circ Z \circ T^{j+x}$ holds true. In this case the assumed resistance to quantum attacks is justified by the fact that the values taken on by the function $f(i,j)$ lie in many different cyclic groups contained in the algebra.

To provide an advance justification of the HDLP-based signature scheme as candidates for post-quantum ones, a method for eliminating the periodicity with the period length depending on the value x is used. The method consists in using the commutative hidden group that is generated by the generator system $< N, Q >$ in which each of the vectors has order equal to the prime value q and computing the value Z as the vector $Z = \psi_0(N \circ Q)$. Multiplying by the vector Q destroys the periodicity associated with the value of the discrete logarithm. Indeed, the vector Q can not be represented as a power of the vector N, since these two vectors lie in different cyclic groups, so the construction of a periodic function with a period length other than the prime q, with the use of public key elements, seems computationally intractable.

However, the use of the product $N \circ Q$ as the preimage of the vector

Table 4. Comparison with the signature schemes Falcon-512, Dilithium-1024x768, and RSA-2048.

Signature scheme	signature size, bytes	publi-key size, bytes	sign. gener. rate, arb. un.	sign. verific. rate, arb. un.
Section 4	192	768	70	50
Section 5	320	1536	17	12
Falcon	657	897	50	25
Dilithium	2044	1184	15	10
RSA-2048	256	256	10	> 50

Z leads to the fact that the multiplier Q contributes also to the result of calculating the right part of the verification equation, which depends on the computed second signature element s. To compensate for this contribution, the calculation of the third element of the signature in the form of an invertible vector S is used. In order to prevent the possibility of signature forgery using the element S as a fitting parameter, the proposed signature scheme uses a doubled verification equation.

Table 4 presents a rough comparison of the proposed two signatures schemes (note different algebras used to implement these schemes) with the candidates for post-quantum signatures Falcon-512 and Dilithium-1024x768 [3].

In comparison with the known HDLP-based signature algorithms, a certain disadvantage of the proposed new signature scheme is the increased size of the signature and about two times higher computational complexity of the signature generation and verification algorithms. However, this disadvantage is quite acceptable in the light of ensuring the implementation of an enhanced criterion aimed at ensuring resistance to potential quantum attacks.

In the method [15] providing formal security proof of the Schnorr signature scheme [8] it is considered a forger that can compute the fitting signature element s equally well for different hash functions f_H and f_H^*. That model of the reductionist security proof is well applicable

to the HDLP-based signature schemes described in papers [6], [7], [14]. However, the said model is not applicable to the proposed signature schemes. In this connection, one can propose a topic for future development of the proposed design approach, i. e., development of the provably secure signature schemes satisfying the advanced criterion of postquantum resistance.

On the whole, it seems the post-quantum security estimate of the introduced two signature algorithms and known HDLP-based signatures is mainly connected with finding algebraic methods for reducing the HDLP to the ordinary HDLP in a finite field $GF(p^h)$ for some fixed value $h \geq 1$. This item represents a topic of individual study.

7 Conclusion

In this paper, a new design of the HDLP-based signature schemes is proposed, which is characterized in using the hidden commutative group having 2-dimensional cyclicity. Thanks to the latter, it is possible to specify the calculation of the corresponding elements Z_1 and Y_1 (Z_2 and Y_2, respectively) of the public key in such a way that, when constructing periodic functions using these two elements, we obtain a period length value equal to the prime order of the elements of the hidden commutative group. Method which provides masking the private value $x < q$ consists in calculation of elements Z_1 and Y_1 as homomorphic (or as automorphic) images of vectors belonging to different cyclic groups, available in the hidden group with the 2-dimensional cyclicity.

One of directions of the further development of the HDLP-based signature schemes is connected with finding new algebras providing possibility to set the hidden commutative groups with 2-dimensional and 3-dimensional cyclic structure.

Acknowledgement. The authors thank anonymous Referee for valuable remarks.

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

References

[1] *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, 420 p.

[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, 530 p.

[3] Derek Zimmer. *NIST Round 2 and Post-Quantum Cryptography – The New Digital Signature Algorithms*. (2019) [Online]. Available: https://www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantum-cryptography-the-new-digital-signature-algorithms/

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] *Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms*, International Standard ISO/IEC 14888-3:2006(E), 2006.

[10] 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.

[11] 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.

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

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

[14] D. N. Moldovyan, "New Form of the Hidden Logarithm Problem and Its Algebraic Support," *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, no. 1(92), pp. XX–XX, 2020, to be published.

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

D. N. Moldovyan, A. A. Moldovyan, N. A. Moldovyan Received December 11, 2019
Revised March 07, 2020

St. Petersburg Institute for Informatics and Automation of
Russian Academy of Sciences
14 Liniya, 39, St.Petersburg, 199178
Russia
E–mail: nmold@mail.ru