UDC 003.26

doi:10.31799/1684-8853-2021-2-43-51

A post-quantum digital signature scheme on groups with four-dimensional cyclicity

D. N. Moldovyan[a]*, PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198*
N. A. Moldovyan[a]*, Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0002-4483-5048, nmold@mail.ru*
[a]*Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation*

Introduction: *Development of practical post-quantum signature schemes is a current challenge in the applied cryptography. Recently, several different forms of the hidden discrete logarithm problem were proposed as primitive of signature schemes resistant to quantum attacks.* ***Purpose:*** *Development of a new form of the hidden discrete logarithm problem set in finite commutative groups possessing multi-dimensional cyclicity, and a method for designing post-quantum signature schemes.* ***Results:*** *A new form of the hidden discrete logarithm problem is introduced as the base primitive of practical post-quantum digital signature algorithms. Two new four-dimensional finite commutative associative algebras have been proposed as algebraic support for the introduced computationally complex problem. A method for designing signature schemes on the base of the latter problem is developed. The method consists in using a doubled public key and two similar equations for the verification of the same signature. To generate a pair of public keys, two secret minimum generator systems <**G**, **Q**> and <**H**, **V**> of two different finite groups* $\Gamma_{<G,\,Q>}$ *and* $\Gamma_{<H,\,V>}$ *possessing two-dimensional cyclicity are selected at random. The first public key (**Y**, **Z**, **U**) is computed as follows:* $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$, $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$, $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$, *where the set of integers* $(y_1, y_2, \alpha, z_1, z_2, \beta, u_1, u_2, \gamma)$ *is a private key. The second public key (**Y**′, **Z**′, **U**′) is computed as follows:* $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$. *Using the same parameters to calculate the corresponding elements belonging to different public keys makes it possible to calculate a single signature which satisfies two similar verification equations specified in different finite commutative associative algebras.* ***Practical relevance:*** *Due to a smaller size of the public key, private key and signature, as well as approximately equal performance as compared to the known analogues, the proposed digital signature scheme can be used in the development of post-quantum signature algorithms.*

Keywords *— post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, finite commutative groups, associative algebras, multi-dimensional cyclicity.*

For citation: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 43–51. doi:10.31799/1684-8853-2021-2-43-51

Introduction

Currently the most widely used public-key cryptoschemes exploit the computational complexity of the factoring problem (FP) [1, 2] and the discrete logarithm problem (DLP) [3, 4]. However, the expected breakthrough in quantum computing technology in the near future makes it extremely urgent to develop cryptosystems that are resistant to attacks using quantum computers. Post-quantum public-key cryptosystems should be based on computationally difficult problems other than FP and DLP, since efficient polynomial algorithms for solving FP and DLP on a quantum computer are known [5–7].

In the current field of development of public-key post-quantum cryptoschemes, considerable attention of the cryptographers is paid to the development of cryptoschemes on algebras [8, 9], on boolean functions [10, 11], and on linear codes [12, 13].

One of attractive post-quantum primitives is the hidden discrete logarithm problem (HDLP) defined usually in non-commutative finite associative algebras (FAAs). Different forms of the HDLP were proposed to develop signature schemes on non-commutative FAAs [9, 14, 15]. For the first time, a signature scheme on a commutative FAA was proposed in [16]. The interest in the HDLP problem is related to the fact that the HDLP-based signature schemes have relatively small sizes of the public key and signature. This area of research is quite new, and for a deeper and more complete understanding of the possibilities for the development of practical post-quantum HDLP-based, it is of significant interest to search for new forms, especially for the case of using commutative FAAs as a carrier of the HDLP.

In this paper, we propose a new form of setting the HDLP in commutative FAAs characterized in that the multiplicative group of the algebras possesses four-dimentional cyclicity in terms of the paper [17]: a finite commutative group whose minimum generator system includes μ (μ ≥ 2) elements that have the same order is called group with μ-dimensional cyclicity. The method of setting the proposed form of the HDLP is fundamentally different from the method introduced earlier in the paper [16] for development of the HDLP-based signature on a commutative algebra.

Two commutative FAAs used as algebraic support

A finite m-dimensional vector space over the finite ground field $GF(p)$, in which a vector multiplication operation is defined additionally to the scalar multiplication and addition operations, is called m-dimensional algebra, if the vector multiplication is distributive at the left and at the right relatively the addition. A vector $\mathbf{A}$ is presented as an ordered set of its coordinates: $\mathbf{A}=(a_0, a_1, ..., a_{m-1})$ or as a sum of its components: $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + ... + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ ($i = 0, 1, ..., m - 1$) are formal basis vectors. Defining additionally the operation of vector multiplication ($\circ$) possessing the property of the two-sided distributivity relatively the addition operation, one gets the finite m-dimensional algebra.

Usually, the multiplication of two vectors $\mathbf{A}=\sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $\mathbf{B}=\sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined by the following formula: $\mathbf{A}\circ\mathbf{B}=\sum_{j=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i\circ\mathbf{e}_j$, where the coordinates a_i and b_i are multiplied as elements of the field $GF(p)$ and every the product of two formal basis vectors is to be replaced by an one-component vector indicated in a cell at the intersection of the i-th row and j-th column of so called basis vector multiplication table, for example, see Table 1 [16]. Each of these tables defines a four-dimensional commutative FAA, multiplicative group of which has order Ω that can be computed as number of invertible vectors. Consider, for example, the algebra defined by Table 1.

The unit element of this commutative FAA is the vector $\mathbf{E} = (0, 0, 1, 0)$. If for some vector $\mathbf{A}$ the vector equation

$$\mathbf{AX}=\mathbf{E} \qquad (1)$$

has a unique solution, then the vector $\mathbf{A}$ is called invertible. For a fixed invertible vector $\mathbf{A}$ the vector equation $\mathbf{AX} = \mathbf{E}$ has a unique solution denoted as $\mathbf{A}^{-1}$ (called inverses of $\mathbf{A}$). Evidently, $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$. An invertibility condition can be derived from equation (1) that can be reduced to the following system of four linear equations, where the unknowns are coordinates of the vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$:

$$\begin{cases} a_2x_0+a_3x_1+a_0x_2+a_1x_3=1\\ \lambda a_3x_0+a_2x_1+a_1x_2+\lambda a_0x_3=0\\ \lambda a_0x_0+a_1x_1+a_2x_2+\lambda a_3x_3=0\\ a_1x_0+a_0x_1+a_3x_2+a_2x_3=0 \end{cases}. \qquad (2)$$

■ ***Table 1.*** Setting the multiplication operation in the first used FAA multiplicative group of which possesses multi-dimensional cyclicity ($\lambda \neq 0$)

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

The main determinant of the system (2) is

$$\Delta=\begin{vmatrix} a_2 & a_3 & a_0 & a_1\\ \lambda a_3 & a_2 & a_1 & \lambda a_0\\ \lambda a_0 & a_1 & a_2 & \lambda a_3\\ a_1 & a_0 & a_3 & a_2 \end{vmatrix}=a_2\begin{vmatrix} a_2 & a_1 & \lambda a_0\\ a_1 & a_2 & \lambda a_3\\ a_0 & a_3 & a_2 \end{vmatrix}-$$

$$-a_3\begin{vmatrix} \lambda a_3 & a_1 & \lambda a_0\\ \lambda a_0 & a_2 & \lambda a_3\\ a_1 & a_3 & a_2 \end{vmatrix}+a_0\begin{vmatrix} \lambda a_3 & a_2 & \lambda a_0\\ \lambda a_0 & a_1 & \lambda a_3\\ a_1 & a_0 & a_2 \end{vmatrix}-$$

$$-a_1\begin{vmatrix} \lambda a_3 & a_2 & a_1\\ \lambda a_0 & a_1 & a_2\\ a_1 & a_0 & a_3 \end{vmatrix}=a_2\left(a_2\left(a_2^2-\lambda a_3^2\right)-\right.$$

$$-a_1\left(a_1a_2-\lambda a_0a_3\right)+\lambda a_0\left(a_1a_3-a_0a_2\right)\Big)-$$

$$-a_3\left(\lambda a_3\left(a_2^2-\lambda a_3^2\right)-a_1\left(\lambda a_0a_2-\lambda a_1a_3\right)+\right.$$

$$+\lambda a_0\left(\lambda a_0a_3-a_1a_2\right)\Big)+a_0\left(\lambda a_3\left(a_1a_2-\lambda a_0a_3\right)-\right.$$

$$-a_2\left(\lambda a_0a_2-\lambda a_1a_3\right)+\lambda a_0\left(\lambda a_0^2-a_1^2\right)\Big)-$$

$$-a_1\left(\lambda a_3\left(a_1a_3-a_0a_2\right)-a_2\left(\lambda a_0a_3-a_1a_2\right)+\right.$$

$$+a_1\left(\lambda a_0^2-a_1^2\right)\Big)=\ldots=\lambda^2\left(a_0^2+a_3^2\right)^2-4\lambda a_0^2a_3^2+$$

$$+\left(a_1^2+a_2^2\right)^2-4\lambda a_0^2a_3^2-2\lambda\left(a_0^2+a_3^2\right)\left(a_1^2+a_2^2\right)+$$

$$+8\lambda a_0a_1a_2a_3=\ldots=\left(\lambda a_0^2-a_1^2-a_2^2+\lambda a_3^2\right)^2-$$

$$-4\left(\lambda a_0a_3-a_1a_2\right)^2.$$

The case $\Delta \neq 0$ defines the following invertibility condition:

$$\left(\lambda a_0^2-a_1^2-a_2^2+\lambda a_3^2\right)^2-4\left(\lambda a_0a_3-a_1a_2\right)^2\neq 0. \qquad (3)$$

The case $\Delta = 0$ defines the following non-invertibility condition:

$$\left(\lambda a_0^2-a_1^2-a_2^2+\lambda a_3^2\right)^2=4\left(\lambda a_0a_3-a_1a_2\right)^2. \qquad (4)$$

Proposition 1. Suppose the structural constant λ is a quadratic non-residue in $GF(p)$. Then the number of different non-invertible vectors in the four-dimensional FAA set by Table 1 is equal to $\eta = 2p^2 - 1$.

Proof: The non-invertibility condition (4) sets the following two cases:

i) $\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = 2\lambda a_0 a_3 - 2a_1 a_2 \Rightarrow$

$\Rightarrow \lambda(a_0 - a_3)^2 = (a_1 - a_2)^2$;

ii) $\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = -2\lambda a_0 a_3 + 2a_1 a_2 \Rightarrow$

$\Rightarrow \lambda(a_0 + a_3)^2 = (a_1 + a_2)^2$.

If the structural constant λ is a quadratic non-residue modulo p, then for the first case the equality holds true only if $(a_0 - a_3)^2 = (a_1 - a_2)^2 = 0$. This gives p different sets of coordinates a_0 and a_1 and p different sets of coordinates a_2 and a_3, including the zero vector (0, 0, 0, 0). Totally, in the first case we have $p^2 - 1$ non-inverible vectors. In the second case the equality holds true only if $(a_0 + a_3)^2 = (a_1 + a_2)^2 = 0$. This defines other p^2 sets of coordinates a_0, a_1, a_2, and a_3, including (0, 0, 0, 0). Therefore we have $\eta = 2p^2 - 1$. Proposition 1 is proven.

Proposition 2. Suppose the structural constant λ is a quadratic non-residue in $GF(p)$. Then the order of the multiplicative group of the FAA set by the Table 1 is equal to $\Omega = (p^2 - 1)^2$.

Proof: Among p^4 different vectors of the algebra you have $\eta = 2p^2 - 1$ non-invertible ones, therefore $\Omega = p^4 - \eta = (p^2 - 1)^2$. Proposition 2 is proven.

Proposition 3. Suppose the structural constant λ is a quadratic residue in $GF(p)$. Then the number of non-invertible vectors in the four-dimensional FFA set by Table 1 is equal to $\eta = 4p^3 - 6p^2 + 4p^2 - 1$.

Proof: Since the structural constant λ is a quadratic residue, formula (4) defines the following two cases:

i) $\left(a_0\sqrt{\lambda} - a_3\sqrt{\lambda}\right)^2 = (a_1 - a_2)^2 \Rightarrow a_0\sqrt{\lambda} - a_3\sqrt{\lambda} =$

$= \pm(a_1 - a_2)$;

ii) $\left(a_0\sqrt{\lambda} + a_3\sqrt{\lambda}\right)^2 = (a_1 + a_2)^2 \Rightarrow a_0\sqrt{\lambda} + a_3\sqrt{\lambda} =$

$= \pm(a_1 + a_2)$.

Sets of coordinates (a_0, a_1, a_2, a_3) satisfying one of four conditions defined by the said two cases represent non-invertible vectors. The following Table 2 shows the number of vectors coordinates of which satisfy a condition indicated in the left column.

Totally, we have

$$\eta = p^2 + p^2 + 2p(p-1)^2 + 2p(p-1)^2 =$$
$$= 4p^3 - 6p^2 + 4p - 1.$$

Proposition 3 is proven.

■ *Table 2.* Number of non-invertible vectors relating to different subsets for the case when λ is a quadratic residue

Condition	# of different combinations of coordinates (a_0, a_1, a_2, a_3) satisfying the condition at the left
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = a_1 - a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = a_1 + a_2 = 0$	p^2 including (0, 0, 0, 0)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = \pm(a_1 - a_2) \neq 0$	$2p(p-1)^2$
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = \pm(a_1 + a_2) \neq 0$	$2p(p-1)^2$

Proposition 4. Suppose the structural constant λ is a quadratic residue in $GF(p)$. Then the order of the multiplicative group of the FAA set by the Table 1 is equal to $\Omega = (p - 1)^4$.

Proof: Among p^4 different vectors of the algebra you have $\eta = 4p^3 - 6p^2 + 4p^2 - 1$ non-invertible ones, therefore $\Omega = p^4 - \eta = p^4 - (4p^3 - 6p^2 + 4p^2 - 1) = (p - 1)^4$. Proposition 4 is proven.

Thus, if the structural constant λ is equal to a quadratic residue modulo p, then the multiplicative group of the considered algebra has order $(p - 1)^4$ and possesses four-dimensional cyclicity [16]. If the structural constant λ is equal to a quadratic non-residue modulo p, then the multiplicative group of the considered algebra has order $(p^2 - 1)^2$ and possesses two-dimensional cyclicity [16].

In the developed signature scheme, it is assumed that the first commutative FAA is set by Table 1, where λ is equal to a quadratic residue, and the characteristic of the field $GF(p)$ is a prime having the following structure $p = 2q + 1$ with 256-bit prime q. In this case the integer q divides $p - 1$ and one can generate a minimum generator system <**G**, **Q**>, where **G** and **Q** are vectors of the order q, which sets a two-dimensional cyclicity subgroup of order q^2.

We also use another commutative FAA possessing the properties similar to that of the algebra set by Table 1. The second used commutative FAA is set by basis vector multiplication table represented as Table 3, where λ is equal to a quadratic residue, and includes the unit vector **E** = (0, 0, 0, 1). Consideration of the number of invertible vectors in the second commutative FAA shows that for the latter the Propositions 1 to 4 are also true. Thus, we have two different commutative FAAs multiplicative group each of which possesses four-dimensional cyclicity. The latter group contains a large num-

■ ***Table 3.*** Setting the second used FAA ($\lambda \neq 0$)

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

ber of two-dimensional cyclicity subgroups of the order q^2.

Example 1. In the case of the first FAA with $p = 2q + 1 = 307771779467$ (prime $q = 153885889733$) and $\lambda = 3$ (quadratic residue) one can select the following minimum generator system <**G**, **Q**, **H**, **V**> setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>} = q^4 = 560783464662101934272226806080639851841841521$:

$$\mathbf{G} = (0, 0, 3, 0);\ \mathbf{Q} = (0, 2, 5, 0);\ \mathbf{H} = (2, 7, 3, 0);$$

$$\mathbf{V} = (13, 12, 10, 17).$$

For $\lambda = 2$ (quadratic non-residue) one can select the following minimum generator system <**G**, **Q**> setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q}>} = q^2 = 94723468236283682804089$:

$$\mathbf{G} = (0, 0, 3, 0) \text{ and } \mathbf{Q} = (0, 1, 2, 0).$$

Example 2. In the case of the second FAA with $p = 2q + 1 = 273413518347119$ (prime $q = 136706759173559$) and $\lambda = 2$ (quadratic residue) one can select the following minimum generator system <**G**, **Q**, **H**, **V**> setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q},\mathbf{H},\mathbf{V}>} = q^4 = 34926892817234073926\ 007473842204106\ 865502885395378264336 1$:

$$\mathbf{G} = (0, 0, 0, 2);\ \mathbf{Q} = (0, 0, 1, 2);\ \mathbf{H} = (0, 1, 4, 7);$$

$$\mathbf{V} = (1, 3, 7, 10).$$

For $\lambda = 13$ (quadratic non-residue) one can select the following minimum generator system <**G**, **Q**> setting a primary group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ of the order $\Omega_{<\mathbf{G},\mathbf{Q}>} = q^2 = 18688738003737457800684726481$:

$$\mathbf{G} = (0, 189, 0, 222) \text{ and } \mathbf{Q} = (0, 0, 0, 2).$$

Consider a method for generating a minimun generator system of a two-dimensional cyclicity subgroup of order q^2. The following procedure outputs a random vector of the order q:

1. Generate a random vector **R** and compute the vector $\mathbf{Q} = \mathbf{R}^2$.

2. If $\mathbf{Q} \neq \mathbf{E}$, then output **Q**. Else go to step 1.

The next probabilistic procedure outputs the minimum generator system:

1. Generate a uniformly random vector **G** of prime order q.

2. Generate a uniformly random vector **Q** of order q.

The multiplicative group of the algebra contains $q^4 - 1$ vectors of order q. The cyclic group generated by the vector **G** includes $q - 1$ vectors of order q, therefore, probability that the vector **Q** is an element of the cyclic group generated by the vector **G** is equal approximately to q^{-3}. In another case the pair of vectors <**G**, **Q**> represents a minimum generator system of a primary subgroup of order q^2 that is contained in the multiplicative group of the algebra. For the case of 256-bit prime q the probability q^{-3} that the latter procedure fails is negligible.

A new HDLP-based signature scheme

In the developed signature scheme a 256-bit collision-resistant hash function f_H is assumed to be used. Computation of the public key is proposed as the following procedure.

Public-key generation algorithm.

1. Generate at random a minimum generator system <**G**, **Q**> of the group of order q^2, which is contained in the first commutative FAA.

2. Generate at random integers $y_1 < q$, $y_2 < q$, and $\alpha < p$, where α is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$.

3. Generate at random integers $z_1 < q$, $z_2 < q$, and $\beta < p$, where β is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$.

4. Generate at random integers $\gamma < p$, $u_1 < q$, and $u_2 < q$, such that non-equality $z_1u_2 \neq z_2u_1$ holds true and γ is a primitive element in $GF(p)$. Then calculate the vector $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$.

5. Generate at random a minimum generator system <**H**, **V**> of the group of order q^2, which is contained in the second commutative FAA.

6. Calculate the vectors $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, and $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$.

7. Output the public key in the form of two triples of vectors: (**Y**, **Z**, **U**) and (**Y**′, **Z**′, **U**′).

In the developed signature scheme, we use the idea of doubling the signature verification equation connected with doubling the public key. Therefore, the triple (**Y**, **Z**, **U**) will be called in this paper the first public key. Respectively, the triple (**Y**′, **Z**′, **U**′) will be called the second public key. Each of the public keys has been calculated with using the same private key representing nine 256-bit integers (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ) and the same formulas. The first (second) public key is computed in the first (second) commutative FAAs. The size of each of public keys is equal to 384 bytes, and the size of doubled public key equals to 768 bytes.

The vectors **G**, **Q**, **H**, and **V** are secret, but the developed signature scheme offers the possibility to choose one of two signature generation procedures. In the first one, only four exponentiation operations are executed in FAAs, however, the vectors **G**, **Q**, **H**, and **V** must be stored by the owner of the public key (the person who generated the public key) as additional elements of his private key. In this case the size of private key is equal to 704 bytes.

In the second version of the signature generation procedures, six exponentiation operations are to be performed in FAAs, but the vectors **G**, **Q**, **H**, and **V** are not needed and the set of nine integers (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ) represent the full private key having the size equal to 192 bytes.

Usually, finding the integer x satisfying the exponential equation $Y' = G'^x$, where Y' and G' are known group elements, which is set in a finite cyclic group is called discrete logarithm problem. If one of the elements Y' and G' or both of them is not directly given, then we have a number of problems we call HDLPs. Different forms of the HDLP are considered in [9, 15]. The HDLP form exploited in the present paper is defined as follows:

Given a triple of vectors (**Y**, **Z**, **U**) contained in the first FAA and a triple of vectors (**Y**′, **Z**′, **U**′) contained in the second FAA. Find the set of integer powers (y_1, y_2, z_1, z_2, u_1, u_2) and the set of scalars (α, β, γ) such that equations $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$, $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$, $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$ (in the first FAA), $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, and $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$ (in the second FAA) hold true for i) some secret vectors **G** and **Q** generating two different cyclic groups of prime order q in the first FAA; ii) some secret vectors **H** and **V** generating two different cyclic groups of prime order q in the second FAA.

One can easily show that, due to using random vectors **G** and **Q** (**H** and **V**) and scalar multiplications, the vectors **Y**, **Z**, and **U** (**Y**′, **Z**′ and **U**′) compose a basis of a three-dimensional cyclicity group in the first (second) FAA. Therefore the vector **Y** (**Y**′) cannot be represented as a product of some powers of the vectors **Z** and **U** (**Z**′ and **U**′) and a periodic function set on the base of the known parameters has periods defined by the order of the public key elements, i. e., by the prime q. The latter means that the Shor quantum algorithm [5] is not applicable to find one of the values y_1, y_2, z_1, z_2, u_1, and u_2.

The said computationally complex problem underlying the developed signature scheme is a new one and currently the authors have no proposal for solving it (except exhaustive search). However, the importance of finding effective solutions allows us to hope that this article will stimulate independent researchers to address this issue. At the moment, the authors expect that choosing a 256-bit prime number q will provide a 128-bit level of security for the proposed signature algorithm.

The first signature generation algorithm.

1. Generate three uniformly random integers $k < q$, $t < q$, and $\rho < p$.

2. Calculate the vector $\mathbf{R} = \mathbf{G}^k\mathbf{Q}^t\rho$.

3. Calculate the vector $\mathbf{R}' = \mathbf{H}^k\mathbf{V}^t\rho$.

4. Compute the first signature element e that is a hash-function value calculated from the document M to be signed, to which the vectors **R** and **R**′ are concatenated: $e = f_H(M, \mathbf{R}, \mathbf{R}')$.

5. Interpreting the hash value as a 256-bit binary number e, calculate the second s and third d signature elements, which represent the solution of the following system of two linear equations:

$$\begin{cases} z_1 s + u_1 d = k - e y_1 \bmod q \\ z_2 s + u_2 d = t - e y_2 \bmod q \end{cases}. \qquad (5)$$

It is easy to get the following formulas for computation of the second and third signature elements:

$$s = \frac{u_2(k - ey_1) - u_1(t - ey_2)}{z_1 u_2 - z_2 u_1} \bmod q; \qquad (6)$$

$$d = \frac{z_1(t - ey_2) - z_2(k - ey_1)}{z_1 u_2 - z_2 u_1} \bmod q. \qquad (7)$$

6. Compute the fourth signature element $\sigma = \rho\alpha^{-e}\beta^{-s}\gamma^{-d}$.

The output signature is four 256-bit numbers (e, s, d, σ) with total size equal to 128 bytes.

The second signature generation algorithm.

1. Generate four uniformly random integers $a < q$, $b < q$, $c < q$, and $\rho < p$.

2. Calculate the vector $\mathbf{R} = \mathbf{Y}^a\mathbf{Z}^b\mathbf{U}^c\rho$.

3. Calculate the vector $\mathbf{R}' = \mathbf{Y}'^a\mathbf{Z}'^b\mathbf{U}'^c\rho$.

4. Compute the first signature element e that is a hash-function value calculated from the document M to be signed, to which the vectors **R** and **R**′ are concatenated: $e = f_H(M, \mathbf{R}, \mathbf{R}')$.

5. Interpreting the hash value as a 256-bit binary number e, calculate the second s and third d signature elements, which represent the solution of the system (5) and can be computed by formulas (6) and (7), substituting the following values of the randomization integers k and t:

$$k = ay_1 + bz_1 + cu_1 \bmod q \text{ and}$$

$$t = ay_2 + bz_2 + cu_2 \bmod q.$$

6. Compute the fourth signature element $\sigma = \rho\alpha^{a-e}\beta^{b-s}\gamma^{c-d}$.

The main contribution to the computational complexity of the signature generation procedure is introduced by the exponentiation operations.

The exponentiation in each of the four-dimensional FAAs takes about 6144 multiplications in $GF(p)$. One exponentiation in $GF(p)$ takes on the average about 384 multiplications. One can roughly estimate the execution time of the first and second signature generation procedures as 25728 and 38016 multiplications in $GF(p)$, correspondingly.

The signature verification algorithm.

1. Calculate the vector $\mathbf{R}^* = \mathbf{Y}^e\mathbf{Z}^s\mathbf{U}^d\sigma$.

2. Calculate the vector $\mathbf{R}'^* = \mathbf{Y}'^e\mathbf{Z}'^s\mathbf{U}'^d\sigma$.

3. Compute the hash-function value from the document M to which the vectors $\mathbf{R}^*$ and $\mathbf{R}'^*$are concatenated: $e^* = f_H(M, \mathbf{R}^*, \mathbf{R}'^*)$.

4. If $e^* = e$, then the signature is accepted as a genuine one, otherwise the signature is rejected as a false one.

One can roughly estimate the computational complexity (execution time) of the signature verification procedure as six exponentiations in the used four-dimensional algebras or as 37248 multiplications in $GF(p)$.

Signature scheme correctness proof.

To prove correctness of the introduced signature scheme, consider a signature (e, s, d, σ) computed in full correspondence with the first signature generation procedure when using the correct signer's private key. When, submitting the signature (e, s, d, σ) to the input of the verification procedure, we have the following proof of the correctness of the proposed signature scheme with the first signature generation algorithm [take into account formulas in the system (5)]:

$$\mathbf{R}^* = \mathbf{Y}^e\mathbf{Z}^s\mathbf{U}^d\sigma =$$

$$= \mathbf{G}^{ey_1}\mathbf{Q}^{ey_2}\alpha^e\mathbf{G}^{sz_1}\mathbf{Q}^{sz_2}\beta^s\mathbf{G}^{du_1}\mathbf{Q}^{du_2}\gamma^d\sigma =$$

$$= \mathbf{G}^{ey_1+sz_1+du_1}\mathbf{Q}^{ey_2+sz_2+du_2}\alpha^e\beta^s\gamma^d\sigma =$$

$$= \mathbf{G}^{ey_1+(k-ey_1)}\mathbf{Q}^{ey_2+(t-ey_2)}\alpha^e\beta^s\gamma^d\rho\alpha^{-e}\beta^{-s}\gamma^{-d} =$$

$$= \mathbf{G}^k\mathbf{Q}^t\rho = \mathbf{R};$$

$$\mathbf{R}'^* = \mathbf{Y}'^e\mathbf{Z}'^s\mathbf{U}'^d\sigma =$$

$$= \mathbf{H}^{ey_1}\mathbf{V}^{ey_2}\alpha^e\mathbf{H}^{sz_1}\mathbf{V}^{sz_2}\beta^s\mathbf{H}^{du_1}\mathbf{V}^{du_2}\gamma^d\sigma =$$

$$= \mathbf{H}^{ey_1+sz_1+du_1}\mathbf{V}^{ey_2+sz_2+du_2}\alpha^e\beta^s\gamma^d\sigma =$$

$$= \mathbf{H}^{ey_1+(k-ey_1)}\mathrm{V}^{ey_2+(t-ey_2)}\alpha^e\beta^s\gamma^d\rho\alpha^{-e}\beta^{-s}\gamma^{-d} =$$

$$= \mathbf{H}^k\mathrm{V}^t\rho = \mathbf{R}';$$

$$\left\{\mathbf{R}'^* = \mathbf{R}'; \mathbf{R}^* = \mathbf{R}\right\} \Rightarrow e^* = e.$$

The final equality means the input signature passes the verification procedure as a genuine signature, i. e., the signature scheme performs correctly. The correctness proof of the signature scheme with the second signature generation algorithm is similar to the presented one.

Discussion

The fact that the same signature satisfies two similar, but different, verification equations is ensured by the same pairs of powers (y_1, y_2), (z_1, z_2), and (u_1, u_2) and the same multipliers α, β, and γ, which are used to compute the corresponding elements of the first $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ and second $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$ public keys. The public keys are computed after selection random minimum generator systems $<\mathbf{G}, \mathbf{Q}>$ (in the first FAA) and $<\mathbf{H}, \mathbf{V}>$ (in the second FAA) which are secret. Every of the element of the first (second) public key is calculated as an element of the two-dimensional cyclicity group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ $(\Gamma_{<\mathbf{H},\mathbf{V}>})$, which is multiplied by a random scalar. After scalar multiplication we get with a high probability a vector outside the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ $(\Gamma_{<\mathbf{H},\mathbf{V}>})$. Thus, the elements of the first (second) public key are not elements of the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$ $(\Gamma_{<\mathbf{H},\mathbf{V}>})$.

Suppose a vector $\mathbf{W}$ is an element of the group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$. The problem of finding the powers w_1 and w_2 such that $\mathbf{W} = \mathbf{G}^{w1}\mathbf{Q}^{w2}$ is called discrete logarithm problem in a two-dimensional cyclicity group $\Gamma_{<\mathbf{G},\mathbf{Q}>}$. In this paper we assume that a potential signature forger can efficiently solve this problem, i. e., if a minimum generator system is given, then a forger can efficiently express any group element as product of some powers of two generators.

Consider an arbitrary minimum generator system $<\mathbf{G}_i, \mathbf{Q}_i>$ of the primary group of order q^2 in the first algebra. The forger can generate random integers α_i, β_i, γ_i and efficiently compute the values $(y_{i1}, y_{i2}, z_{i1}, z_{i2}, u_{i1}, u_{i2})$ such that $\mathbf{Y}\alpha_i^{-1} = \mathbf{G}_i^{y_{i1}}\mathbf{Q}_i^{y_{i2}}$, $\mathbf{Z}\beta_i^{-1} = \mathbf{G}_i^{z_{i1}}\mathbf{Q}_i^{z_{i2}}$, and $\mathbf{U}\gamma_i^{-1} = \mathbf{G}_i^{u_{i1}}\mathbf{Q}_i^{u_{i2}}$. Then, using the formulas (6) and (7), he can compute a signature satisfying the first verification equation. However, this signature will satisfy the second verification equation only if the primary group of order q^2 of the second algebra contains a minimum generator system $<\mathbf{H}_i, \mathbf{V}_i>$ such that $\mathbf{Y}'\alpha_i^{-1} = \mathbf{H}_i^{y_{i1}}\mathbf{V}_i^{y_{i2}}$, $\mathbf{Z}'\beta_i^{-1} = \mathbf{H}_i^{z_{i1}}\mathbf{V}^{z_{i2}}$, and $\mathbf{U}'\gamma_i^{-1} = \mathbf{H}_i^{u_{i1}}\mathbf{V}_i^{u_{i2}}$. However, in fact, the fixed four values $(y_{i1}, y_{i2}, z_{i1}, z_{i2})$ define one minimum generator system $<\mathbf{H}_i, \mathbf{V}_i>$ (that can be supposedly computed) such that $\mathbf{Y}'\alpha_i^{-1} = \mathbf{H}_i^{y_{i1}}\mathbf{V}_i^{y_{i2}}$ and $\mathbf{Z}'\beta_i^{-1} = \mathbf{H}_i^{z_{i1}}\mathbf{V}_i^{z_{i2}}$. For the fixed values of the vectors $\mathbf{H}_i$ and $\mathbf{V}_i$ one will get $\mathbf{U}'\gamma_i^{-1} = \mathbf{H}_i^{u'_{i1}}\mathbf{V}_i^{u'_{i2}}$, where the values u'_{i1} and u'_{i2} are random. Since the first and second commutative FAAs are independent, the equalities $u'_{i1} = u_{i1}$ and $u'_{i2} = u_{i2}$ of two pairs of 256-bit numbers can take place only at random with probability about 2^{-512}.

Therefore, we expect that the signature forger is unable to find efficiently the required alternative pair of vectors $<\mathbf{G}_i, \mathbf{Q}_i>$ or to guess the secret elements $<\mathbf{G}, \mathbf{Q}>$. A quantum computer will not provide much help to the forger, since the discrete logarithm problem that arises is hidden (the "bases" of logarithms, i. e., $<\mathbf{G}, \mathbf{Q}>$ and $<\mathbf{H}, \mathbf{V}>$ are unknown).

In fact, breaking the proposed signature scheme is to find two minimum generator systems of two different two-dimensional cyclicity groups (contained in two different FAAs) which are consistent with each other. These two minimum generator systems are connected by the mechanism of doubling the verification equation, i. e., by a single digital signature, which must satisfy the verification equation given in two different independent commutative FAAs.

One can note, that the method [18, 19] of the reductionist security proof that was applied to the Schnorr signature algorithm [20] can be also applied to the proposed signature scheme. Indeed, an assumption that a signature forger is able to calculate a signature equally well for six different hash functions leads to potential possibility to compute the private key (y_1, y_2, α, z_1, z_2, β, u_1, u_2, γ).

Indeed, like in [19], suppose a potential signature forger can compute signatures for different hash functions, when the values of the randomization parameters are k, t, and ρ are fixed. For four different hash functions he computes the signatures (e_1, s_1, d_1, σ_1), (e_2, s_2, d_2, σ_2), (e_3, s_3, d_3, σ_3), and (e_4, s_4, d_4, σ_4). Then the signature forger composes the following system of eight linear equations with eight unknowns y_1, y_2, z_1, z_2, u_1, u_2, k, and t [see (5)]:

$$\begin{cases} z_1s_1 + u_1d_1 = k - e_1y_1 \bmod q \\ z_2s_1 + u_2d_1 = t - e_1y_2 \bmod q \\ z_1s_2 + u_1d_2 = k - e_2y_1 \bmod q \\ z_2s_2 + u_2d_2 = t - e_2y_2 \bmod q \\ z_1s_3 + u_1d_3 = k - e_3y_1 \bmod q \\ z_2s_3 + u_2d_3 = t - e_3y_2 \bmod q \\ z_1s_4 + u_1d_4 = k - e_4y_1 \bmod q \\ z_2s_4 + u_2d_4 = t - e_4y_2 \bmod q \end{cases}.$$

Note, the probability that the main determinant of his system of equations equals to zero is negligibly small (q^{-1}). Solving the latter system one can get the values of y_1, y_2, z_1, z_2, u_1, and u_2. It easy to show that, using the formulas $\sigma_i = \rho\alpha^{-e_i}\beta^{-s_i}\gamma^{-d_i}$ for $i = 1, 2, 3, 4$ (see step 6 in the first signature generation algorithm) and finding roots from different ratio values σ_i/σ_j in $GF(p)$, one can calculate the values of scalars α, β, and γ. Thus, taking into account that operations of finding roots in $GF(p)$, where $p = 2q + 1$, have polynomial computational complexity, one can conclude that a polynomial algorithm for forging a signature is reducible to a polynomial algorithm of solving the HDLP underlying the introduced signature scheme.

The above provides a general idea for constructing a signature scheme and a general justification for its resistance to attacks using conventional and quantum computers. Detailed consideration of the security issue and obtaining detailed estimates is a separate independent task for the new study.

■ ***Table 4.*** Comparison with some known post-quantum signature schemes

Signature scheme	Signature size, byte	Public key size, byte	Rate of signature generation, arb. un.	Rate of signature verification, arb. un.
Falcon	1280	1793	50	25
Crystals-Dilithium	2701	1472	15	2
Rainbow	64	150 000	–	–
[15]	192	768	50	80
[16]	192	512	40	80
Proposed	128	768	70	80

It is important that the proposed fundamentally new method for setting the HDLP can be implemented in numerous different ways. The most obvious is the use of different pairs of finite associative algebras. In particular, pairs of algebras of different orders, different types and structures can be used. In particular, is interesting to consider the following versions:

i) one algebra is commutative and the other one is non-commutative;

ii) one algebra is defined over a ground finite field $GF(p)$, and the other one is defined over a finite extension of the binary field $GF(2^s)$.

The introduced design method opens up quite wide possibilities for implementing various design variants of digital signature schemes. The introduced signature scheme suites well for software implementation, since it uses only additions, multiplications, exponentiations and inversions (mod p and mod q).

Currently, the NIST competition [21] for the development of post-quantum public-key cryptosystems has entered the final stage [22]. The finalists in the category of post-quantum signatures were Falcon [23] and Crystals-Dilithium [24], and Rainbow [25]. It is interesting to compare the proposed signature scheme with the finalists and with other HDLP-based signatures. A rough comparison is presented in Table 4.

Conclusion

A new design method and a practical HDLP-based post-quantum signature scheme have been introduced. The proposed method is quite simple to understand and has fundamental differences from other known methods of designing post-quantum digital signature schemes. This reduces the complexity of the further stage of a detailed study of the security of the developed signature scheme. Another important advantage of the proposed method is that it opens up the possibility of developing a new class of practical post-quantum cryptosystems. The latter is of particular importance in the light of the widely conducted researches on the development of post-quantum digital signature standards.

References

1. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
2. Chiou S. Y. Novel digital signature schemes based on factoring and discrete logarithms. *International Journal of Security and its Applications*, 2016, vol. 10, no. 3, pp. 295–310.
3. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. IT-31, no. 4, pp. 469–472.
4. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
5. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
6. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
7. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
8. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
9. Moldovyan N. A., Moldovyan A. A. 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*, 2019, vol. 12, no. 1, pp. 66–81. doi:10.14529/mmp190106
10. Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions. *Prikl. Diskr. Mat.*, 2018, no. 40, pp. 23–33. doi:10.17223/20710410/40/3
11. Agibalov G. P. ElGamal cryptosystems on Boolean functions. *Prikl. Diskr. Mat*, 2018, no. 42, pp. 57–65. DOI:10.17223/20710410/42/4
12. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. *Designs, Codes and Cryptography*, 2017, vol. 82, no. 1–2, pp. 469–493.
13. Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem. *Prikl. Diskr. Mat.*, 2019, no. 45, pp. 33–43. doi:10.17223/20710410/45/4
14. Moldovyan N. A., Moldovyan A. A. New forms of defining the hidden discrete logarithm problem. *SPIIRAS Proceedings*, 2019, vol. 18, no. 2, pp. 504–529. doi:10.15622/sp.18.2.504-529
15. Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2020, vol. 16, iss. 4, pp. 455–461. doi:10.21638/11701/spbu10.2020.410
16. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29
17. Moldovyan N. A. Fast signatures based on non-cyclic finite groups. *Quasigroups and Related Systems*, 2010, vol. 18, no. 1, pp. 83–94.
18. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, vol. 13, pp. 361–396.
19. Koblitz N., Menezes A. J. Another look at "Provable Security". *Journal of Cryptology*, 2007, vol. 20, pp. 3–38.
20. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
21. *Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 27 January 2021).
22. *Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed 27 January 2021).
23. *Fast-Fourier Lattice-Based Compact Signatures over NTRU*. Available at: https://falcon-sign.info/ (accessed 27 January 2021).
24. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*. https://eprint.iacr.org/2017/633.pdf. Available at: https://pq-crystals.org/dilithium/index.shtml (accessed 27 January 2021).
25. Ding J., Schmidt D. *Rainbow, a New Multivariable Polynomial Signature Scheme*. In: Ioannidis J., Keromytis A., Yung M. (eds). *Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, 2005. Vol. 3531. Pp. 164–175.

УДК 003.26
doi:10.31799/1684-8853-2021-2-43-51

Постквантовая схема цифровой подписи на группе с четырехмерной цикличностью

Д. Н. Молдовян[a], канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048, nmold@mail.ru
[a]Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка практичных постквантовых схем подписи является одним из вызовов прикладной криптографии. Несколько различных форм скрытой задачи дискретного логарифмирования были предложены недавно в качестве примитива схем подписи, стойких к квантовым атакам. **Цель:** разработка новой формы скрытой задачи дискретного логарифмирования, заданной в коммутативной группе, обладающей многомерной цикличностью, и метода построения постквантовых схем подписи. **Результаты:** предложена новая форма скрытой задачи дискретного логарифмирования в качестве базового примитива для практичных постквантовых алгоритмов цифровой подписи. Представлены две новые четырехмерные конечные коммутативные ассоциативные алгебры в качестве алгебраического носителя предложенной новой вычислительно трудной задачи. Разработан метод построения схем подписи на основе последней. Суть метода состоит в использовании удвоенного открытого ключа и двух одинаковых уравнений для проверки подлинности одной и той же подписи. Для генерации пары открытых ключей выбираются случайным образом два базиса $<\mathbf{G}, \mathbf{Q}>$ и $<\mathbf{H}, \mathbf{V}>$ двух различных конечных групп $\Gamma_{<\mathbf{G}, \mathbf{Q}>}$ и $\Gamma_{<\mathbf{H}, \mathbf{V}>}$, обладающих двумерной цикличностью. Первый открытый ключ $(\mathbf{Y}, \mathbf{Z}, \mathbf{U})$ вычисляется следующим образом: $\mathbf{Y} = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$, $\mathbf{Z} = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$, $\mathbf{U} = \mathbf{G}^{u_1}\mathbf{Q}^{u_2}\gamma$, где набор целых чисел $(y_1, y_2, \alpha, z_1, z_2, \beta, u_1, u_2, \gamma)$ является секретным ключом. Второй открытый ключ $(\mathbf{Y}', \mathbf{Z}', \mathbf{U}')$ вычисляется следующим образом: $\mathbf{Y}' = \mathbf{H}^{y_1}\mathbf{V}^{y_2}\alpha$, $\mathbf{Z}' = \mathbf{H}^{z_1}\mathbf{V}^{z_2}\beta$, $\mathbf{U}' = \mathbf{H}^{u_1}\mathbf{V}^{u_2}\gamma$. Использование одинаковых параметров для вычисления соответствующих друг другу элементов, принадлежащих разным открытым ключам, обеспечивает возможность вычисления единой подписи, удовлетворяющей двум сходным проверочным уравнениям, заданным в различных конечных коммутативных ассоциативных алгебрах. **Практическая значимость:** предложенная схема цифровой подписи представляет практический интерес для разработки постквантовых алгоритмов подписи, обладающих сравнительно малыми размерами подписи, открытого и секретного ключей.

Ключевые слова — постквантовые криптосхемы, компьютерная безопасность, электронная цифровая подпись, задача дискретного логарифмирования, конечные коммутативные группы, ассоциативные алгебры, многомерная цикличность.

Для цитирования: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Информационно-управляющие системы*, 2021, № 2, с. 43–51. doi:10.31799/1684-8853-2021-2-43-51
For citation: Moldovyan D. N., Moldovyan N. A. A post-quantum digital signature scheme on groups with four-dimensional cyclicity. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 2, pp. 43–51. doi:10.31799/1684-8853-2021-2-43-51

УВАЖАЕМЫЕ АВТОРЫ!

Научная электронная библиотека (НЭБ) продолжает работу по реализации проекта SCIENCE INDEX. После того как Вы зарегистрируетесь на сайте НЭБ (http://elibrary.ru/defaultx.asp), будет создана Ваша личная страничка, содержание которой составят не только Ваши персональные данные, но и перечень всех Ваших печатных трудов, имеющихся в базе данных НЭБ, включая диссертации, патенты и тезисы к конференциям, а также сравнительные индексы цитирования: РИНЦ (Российский индекс научного цитирования), h (индекс Хирша) от Web of Science и h от Scopus. После создания базового варианта Вашей персональной страницы Вы получите код доступа, который позволит Вам редактировать информацию, помогая создавать максимально объективную картину Вашей научной активности и цитирования Ваших трудов.