A novel method for developing post-quantum cryptoschemes and a practical signature algorithm

Nikolay Andreevich Moldovyan
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia, and
Dmitriy Nikolaevich Moldovyan
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia

Received 14 February 2021
Revised 18 May 2021
15 June 2021
Accepted 27 June 2021

Abstract

Purpose – The practical purpose of this research is to propose a candidate for post-quantum signature standard that is free of significant drawback of the finalists of the NIST world competition, which consists in the large size of the signature and the public key. The practical purpose is to propose a fundamentally new method for development of algebraic digital signature algorithms.

Design/methodology/approach – The proposed method is distinguished by the use of two different finite commutative associative algebras as a single algebraic support of the digital signature scheme and setting two different verification equation for a single signature. A single public key is computed as the first and the second public keys, elements of which are computed exponentiating two different generators of cyclic groups in each of the algebras.

Findings – Additionally, a scalar multiplication by a private integer is performed as final step of calculation of every element of the public key. The same powers and the same scalar values are used to compute the first and the second public keys by the same mathematic formulas. Due to such design, the said generators are kept in secret, providing resistance to quantum attacks. Two new finite commutative associative algebras, multiplicative group of which possesses four-dimensional cyclicity, have been proposed as a suitable algebraic support.

Originality/value – The introduced method is novel and includes new techniques for designing algebraic signature schemes that resist quantum attacks. On its base, a new practical post-quantum signature scheme with relatively small size of signature and public key is developed.

Keywords Information protection, Computer security, Digital signature, Post-quantum cryptography, Finite associative algebra, Commutative algebra, Multi-dimensional cyclicity groups

Paper type Research paper

1. Introduction

Public-key cryptographic algorithms and protocols are of great importance in modern practical informatics and computer science. They provide basic primitives for solving fundamental problems of information security and are a source of new information technologies. In the last three decades, most developed countries have used cryptographic standards for public key distribution and digital signature, based on the computational

Applied Computing and Informatics
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1108/ACI-02-2021-0036

complexity of the discrete logarithm problem (DLP) and the factorization problem (FP). However, both of these problems can be effectively solved on a quantum computer [1–3], the appearance of which is predicted in the fairly near future.

The implementation of this expectation will mean that the specified cryptographic standards cease to be secure. Therefore, the development of practical public-key post-quantum cryptoschemes that resist quantum attacks (attacks with using quantum and ordinary computers) attracts much attention of the cryptographic community [4]. A notable event was NIST's announcement of a worldwide competition to develop candidates for post-quantum public-key standards for (1) digital signature algorithms and (2) public-key encryption and key-establishment algorithms during 2017–2024 [5].

At the moment, 3 signature schemes and 4 public-key encryption and key-establishment algorithms have been selected as finalists out of 69 initially submitted candidates for post-quantum public-key standards [6]. However, the former have a significant drawback for a wide practical application, which consists in the large size of the signature and the public key.

The article is organized as follows. In Section 2, different approaches to design of post-quantum public key cryptoschemes are mentioned. Section 3 describes the overall idea of the proposed method for development of the post-quantum signature algorithm. Section 4 presents a new algebraic post-quantum signature scheme. Next Section 5 provides preliminary security estimation. Section 6 concludes the paper.

2. Preliminaries

For the development of post-quantum public-key cryptographic algorithms and protocols one should use computationally difficult problems that are different from the FP and DLP, since polynomial algorithms for solving FP and DLP on a quantum computer are known [1–3]. Considerable attention of the developers is paid to the development of cryptoschemes on algebras [6, 7], on Boolean functions [8], on lattices [9] and on linear codes [10, 11].

One of attractive approaches to the development of post-quantum signature algorithm relates to exploiting computational difficulty of the so-called hidden discrete logarithm problem (HDLP) defined usually in non-commutative finite associative algebras (FAAs). Different forms of the HDLP were used to develop signature algorithms on non-commutative FAAs [7, 12, 13]. For the first time, a HDLP-based signature algorithm on a commutative FAA was proposed in [14].

A common feature of the HDLP-based signature algorithms is the use of exponentiation operations in a hidden cyclic group, but the masking mechanisms used to hide this group are fundamentally different when using non-commutative and commutative algebras. More extensive possibilities for setting various forms of the HDLP in non-commutative FAAs are associated with the possibility of setting automorphisms and homomorphisms in non-commutative algebras, which can be used as masking operations. The latter is not possible when using commutative FAAs and other masking mechanisms should be proposed when developing a HDLP-based signature algorithm on commutative algebras.

In this paper, we consider a method for designing post-quantum signature schemes on commutative FAAs characterized in exploiting a novel masking mechanism to hide cyclic groups in which the base exponentiation operations are performed. The main requirement to the FAAs suitable for their using as algebraic support for implementing the introduced method is that their multiplicative group possesses multidimensional cyclicity.

Consider the setting of FAAs. Suppose in a finite m-dimensional vector space over a finite field (ground field $GF(p)$ or extension of the binary field $GF(2^n)$), in which a vector multiplication operation is defined additionally to the scalar multiplication and addition operations. If the vector multiplication is distributive at the left and at the right relatively the addition operation, then the said vector space is called m-dimensional algebra. A vector $\mathbf{A}$ is

presented as an ordered set of its coordinates: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$ or as a sum of its components: $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \cdots + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i (i = 0, 1, \ldots, m-1)$ are formal basis vectors.

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:

$$\mathbf{AB} = \sum_{i,j=0}^{m-1} a_i b_j \mathbf{e}_i\mathbf{e}_j, \tag{1}$$

where the coordinates a_i and b_i are multiplied as elements of the finite field, for example $GF(p)$, and every of the products $\mathbf{e}_i\mathbf{e}_j$ is to be substituted by an one-component vector $\lambda\mathbf{e}_k$ indicated in a cell in the intersection of the ith row and jth column of so called basis vector multiplication table (BVMT), for example, see Table 1. The value $\lambda \in GF(p)$ is called structural coefficient.

The use of the exponentiation operation in the procedures of public key computation and of signature generation and verification implies the possibility of using a fast exponentiation algorithm. To ensure the correct operation of the latter, the associativity condition of the multiplication operation must be met. Formula (1) shows that one can define the associative vector multiplication operation imposing the following conditions on the BVMT:

$$(\mathbf{e}_i\mathbf{e}_j)\mathbf{e}_k = \mathbf{e}_i(\mathbf{e}_j\mathbf{e}_k) \tag{2}$$

for all possible triples of basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$.

To construct an algebra suitable for our purpose, we used a unified method [15] for defining algebras of arbitrary even dimensions, which results in non-commutative/commutative FAAs of the dimensions $m \geq 6/m = 2, 4$. From a single general formula introduced in [15] for case $m = 4$ we get the following formula for generating a BVMT:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{i+j\bmod 4}, & \text{if } i\bmod 2 = 0; \\ \mathbf{e}_{i-j\bmod 4}, & \text{if } i\bmod 2 = 1,\ j\bmod 2 = 0; \\ \lambda\mathbf{e}_{i-j\bmod 4}, & \text{if } i\bmod 2 = 1,\ j\bmod 2 = 1. \end{cases} \tag{3}$$

that defines Table 1a. To construct the second four-dimensional commutative FAA, we propose the following formula:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \lambda\mathbf{e}_{i+j-2\bmod 4}, & \text{if } i\bmod 2 = 0,\ j\bmod 2 = 0; \\ \mathbf{e}_{i+j-2\bmod 4}, & \text{if } i\bmod 2 = 0,\ j\bmod 2 = 1; \\ \mathbf{e}_{i-j+2\bmod 4}, & \text{if } i\bmod 2 = 1. \end{cases} \tag{4}$$

that defines Table 1b. It is easy to show the latter formula (3) sets the satisfiability of condition (2). The validity of the following two statements can be easily verified:

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

(a)

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

(b)

Table 1. Defining associative vector multiplication operation in the first (a) and second (b) FAAs used as algebraic support ($\lambda \neq 0$)

Proposition 1. The vector $\mathbf{E} = (1,0,0,0)$ is the unit of the commutative FAA set by Table 1a.

Proposition 2. The vector $\mathbf{E} = (0,0,1,0)$ is the unit of the commutative FAA set by Table 1b.

Each of the defined commutative FAA contains a multiplicative group possessing μ-dimensional cyclicity with $\mu = 2$, if λ is a quadratic non-residue modulo p, or $\mu = 4$, if λ is a quadratic residue. Notion of the multidimensional cyclicity was introduced in [16], namely, a finite commutative group the minimum generator system (group basis) of which includes μ group elements of the same order is called a μ-dimensional cyclicity group (a group possessing μ-dimensional cyclicity).

To find the value of the order Ω of multiplicative group one is to calculate the number of invertible elements in a FAA, which is equal to Ω. Consider the first FAA. For an invertible vector $\mathbf{A}$ vector the vector equation $\mathbf{AX} = E$ has a unique solution that is inverses of the vector $\mathbf{A}$ and is denoted as $\mathbf{A}^{-1}$. To obtain invertibility condition one can reduce the said vector equation to the following system of four linear equations with the unknown integers x_0, x_1, x_2, and x_3 as the coordinates of the vector $\mathbf{X}$:

$$\begin{cases} a_0x_0 + \lambda a_1x_1 + a_2x_2 + \lambda a_3x_3 = 1; \\ a_0x_1 + a_1x_0 + a_2x_3 + a_3x_2 = 0; \\ a_0x_2 + \lambda a_1x_3 + a_2x_0 + \lambda a_3x_1 = 0; \\ a_0x_3 + a_1x_2 + a_2x_1 + a_3x_0 = 0. \end{cases} \tag{5}$$

The main determinant of the system (5) is

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

$$+ a_2 \begin{vmatrix} a_1 & a_0 & a_2 \\ a_2 & \lambda a3 & \lambda a_1 \\ a_3 & a_2 & a_0 \end{vmatrix} - \lambda a_3 \begin{vmatrix} a_1 & a_0 & a_3 \\ a_2 & \lambda a_3 & a_0 \\ a_3 & a_2 & a_1 \end{vmatrix}$$

$$= a_0\left(a_0\left(a_0^2 - \lambda a_1^2\right) - a_3(\lambda a_0a_3 - \lambda a_1a_2) + a_2(\lambda a_1a_3 - a_0a_2)\right) -$$

$$- \lambda a_1\left(a_1(a_0^2 - \lambda a_1^2) - a_3(a_0a_2 - \lambda a_1a_3) + a_2(a_1a_2 - a_0a_3)\right) +$$

$$+ a_2\left(a_1(\lambda a_0a_3 - \lambda a_1a_2) - a_0(a_0a_2 - \lambda a_1a_3) + a_2\left(a_2^2 - \lambda a_3^2\right)\right) -$$

$$- \lambda a_3\left(a_1(\lambda a_1a_3 - a_0a_2) - a_0(a_1a_2 - a_0a_3) + a_3\left(a_2^2 - \lambda a_3^2\right)\right) = \ldots =$$

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

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

$$= \left(a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2\right)^2 - 4\lambda(a_0a_1 - a_2a_3)^2.$$

If $\Delta \neq 0$, then the system (5) has unique solution and we have the following invertibility condition:

$$\left(a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2\right)^2 - 4\lambda(a_0a_1 - a_2a_3)^2 \neq 0 \tag{6}$$

First, we will calculate the number η of non-invertible vectors and the compute the multiplicative group order as $\Omega = p^4 - \eta$. Taking into account the condition (6) we get the following non-invertibility condition

$$\left(a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2\right)^2 = 4\lambda(a_0 a_1 - a_2 a_3)^2. \quad (7)$$

Proposition 3. If the structural constant λ is equal to a quadratic non-residue modulo p, then the number of non-invertible vectors in the commutative FAA set by Table 1a equals to $\eta = 2p^2 - 1$ and the multiplicative group order equals to $\Omega = (p^2 - 1)^2$.

Proof. Formula (7) sets the following condition:

$$\begin{cases} a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2 = 0; \\ a_0 a_1 - a_2 a_3 = 0. \end{cases}$$

For the case $a_1 \neq 0$, substituting the value $a_0 = a_2 a_3 a_1^{-1}$ in the first equality we have $a_2^2(a_3^2 - a_1^2) = \lambda a_1^2(a_3^2 - a_1^2)$. from the latter formula one can see that in this case we have $2p^2 - 2p$ non-invertible vectors.

For the case $a_1 = 0$ we have $a_2 a_3 = 0$. If $a_2 = 0$, then $a_0^2 = \lambda a_3^2 \Rightarrow a_0 = a_3 = 0$ (this gives one more non-invertible vector, namely, the vector (0,0,0,0). If $a_3 = 0$, then $a_0^2 = a_2^2 \Rightarrow a_0 = \pm a_2$ and we have $2(p-1)$ additional non-invertible vectors. If $a_3 = 0$ and $a_2 = 0$, then $a_0 = 0$. The latter gives the vector (0,0,0,0).

In sum, for the considered cases one gets $\eta = 2p^2 - 2p + 2(p-1) + 1 = 2p^2 - 1$. Therefore, $\Omega = p^4 - \eta = (p^2 - 1)^2$. Proposition 3 is proven.

Proposition 4. If the structural constant λ is equal to a quadratic non-residue modulo p, then the number of non-invertible vectors in the commutative FAA set by Table 1a equals to $\eta = 4p^3 - 6p^2 + 4p^2 - 1$ and the multiplicative group order equals to $\Omega = (p-1)^4$.

Proof. Since the structural constant λ is a quadratic residue, formula (7) defines the following two cases:

(1) $$a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2 = 2\sqrt{\lambda}(a_0 a_1 - a_2 a_3) \Rightarrow (a_0 - \sqrt{\lambda}\, a_1)^2 = (a_2 - \sqrt{\lambda}\, a_3)^2 \Rightarrow$$
$$\Rightarrow a_0 - \sqrt{\lambda} a_1 = \pm(a_2 - \sqrt{\lambda}\, a_3);$$

(2) $$a_0^2 + \lambda a_1^2 - a_2^2 - \lambda a_3^2 = -2\sqrt{\lambda}(a_0 a_1 - a_2 a_3) \Rightarrow (a_0 + \sqrt{\lambda}\, a_1)^2 = (a_2 + \sqrt{\lambda}\, a_3)^2 \Rightarrow$$
$$\Rightarrow a_0 + \sqrt{\lambda} a_1 = \pm(a_2 + \sqrt{\lambda}\, a_3).$$

These cases define four conditions for the values of coordinates (a_0, a_1, a_2, a_3) of non-invertible vectors, which are presented in Table 2 together with the number of vectors coordinates of which relates to a fixed condition.

Totally, number of non-invertible vectors is equal to

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

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

Table 2. Number of non-invertible vectors relating to every of four conditions

Therefore, one gets $\Omega = p^4 - \eta = (p-1)^4$. Proposition 4 is proven.

In a similar way, we can prove that the Propositions 3 and 4 are also valid for the case of the second commutative FAA, in which the vector multiplication operation is defined by Table 1b.

It is easy to see that the multiplicative group of each of the algebras is generated by a group basis containing two (four) vectors of order $\omega = p^2 - 1$ ($\omega = p - 1$), if the value of λ is a quadratic non-residue (residue) modulo p. When developing a digital signature scheme it is assumed that the structural constant is equal to a residue and each of the considered commutative FAAs is defined over the same field $GF(p)$ with characteristic equal to a prime $p = 2q + 1$, where q is a 256-bit prime.

Suppose the multiplicative group of the first FAA is generated by a basis $< \mathbf{B}'_1, \mathbf{B}'_2, \mathbf{B}'_3, \mathbf{B}'_4 >$. Then the following four vectors $\mathbf{B}_1 = \mathbf{B}'^2_1$, $\mathbf{B}_2 = \mathbf{B}'^2_2$, $\mathbf{B}_3 = \mathbf{B}'^2_3$, and $\mathbf{B}_4 = \mathbf{B}'^2_4$ compose a basis of a primary group of order q^4, which contains $q + 1$ cyclic groups of order q. Each element $\mathbf{V}$ of the said primary group can be uniquely represented as a product of some powers of the elements of the basis $< \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4 >: \mathbf{V} = \mathbf{B}^i_1, \mathbf{B}^j_2, \mathbf{B}^k_3, \mathbf{B}^h_4$, where $i, j, k, h = 0, 1, 2, \ldots, q-1$. The power vector (i, j, k, h) can be called four-dimensional logarithm (or simply logarithm) of the vector $\mathbf{V}$ over the basis $< \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4 >$. Evidently the value of the logarithm of the vector $\mathbf{V}$ depends on the fixed basis, *i.* e., for different bases the logarithm of a fixed vector $\mathbf{V}$ has different values.

Let us make the following remark about the logarithm of the scalar vector, which is essential for understanding the method of constructing post-quantum digital signature schemes described below. Selection of a random basis leads to a random value of the logarithm of the scalar vector $\mathbf{S} = \mathbf{E}\alpha$, where α is a scalar multiplier. Therefore, fixing at random a basis in the first FAA and a basis in the second FAA for the fixed scalar vector $\mathbf{S}$ one gets different values of log $\mathbf{S}$.

3. Proposed method

The method is based on the idea of selecting random bases of primary groups of order 2 in the first and second algebras, and then calculating the first and second public keys as a product of powers of the elements of the corresponding basis, the same powers being used to calculate corresponding element of the first and second public key. The latter is to provide possibility to generate a single digital signature, for which one verification equation (written for the first public key) and another verification equation (written for the second public key) are satisfied.

Such doubling of the verification equation should force a potential signature forger to calculate the same values of logarithms of the corresponding public-key elements. However, the fact that the corresponding public-key elements are computed using the same powers of the exponentiation operation can be potentially used to compute bases over which the logarithms of the corresponding public-key elements are equal.

Therefore, the technique of scalar multiplication is used. This technique consists in including an additional scalar multiplication of the public-key elements. Different scalar multipliers are used for computing different element of the same public key, but the same scalar multiplier is used for computing corresponding elements of the first and second public keys. Due to scalar multiplications the logarithms of the corresponding elements of public keys (over randomly selected bases in the first and second FAAs) become different. The multiplications by scalars acts as masking operations that hide the 2-dimensional cyclicity groups set by the initially selected bases in each of the commutative FAA.

Introducing an additional signature element we provide correctness of the signature scheme the doubled verification equation complemented with the technique of scalar multiplication.

4. Post-quantum signature scheme

An arbitrary vector **G** of order q generates a cyclic group including $q - 1$ vectors of the order q. The multiplicative group of each of the FAAs includes $q^4 - 1$ different vectors of the order q. Therefore, with probability $\approx 1 - q^{-3}$ a random vector **Q** of the order q sets a basis <**G**, **Q**> of primary group of order q^2, including $q^2 - 1$ different vectors of the order q. Then with probability $\approx 1 - q^{-2}$ a random vector **V** of the order q sets a basis <**G**, **Q**, **V**> of primary group of order q^3, including $q^3 - 1$ different vectors of the order q. Then with probability $\approx 1 - q^{-1}$ a random vector **W** of the order q sets a basis <**G**, **Q**, **V**, **W**> of primary group of order q^4. Thus, most likely is the case, when two (four) random vectors of order q set a basis of a primary group of order q^2 (q^4), which has two-dimensional (four-dimensional) cyclicity. However there is a probability that two (four) random vectors set a generator system of the primary group of order q ($\leq q^3$). The latter probability can be called a failure probability.

In each of the commutative FAAs used as algebraic support of the developed signature algorithm, the failure probability is negligibly small, i.e., equals to $\approx q^{-3}$ ($\approx q^{-1}$) when setting the basis of two-dimensional (four-dimensional) cyclicity by selection of two (four) random vectors of order q.

Calculation of the first and second public keys that compose a single public key is performed as follows:

(1) Generate two uniformly random vectors **G** and **Q** of order q in the first FAA and two uniformly random vectors **D** and **H** of order q in the second FAA.

(2) Generate at random three 256-bit integers $y_1 < q$, $y_2 < q$, and $\alpha < p$, where α is a primitive element modulo p, and calculate the first element of the first public key $\mathbf{Y}_1 = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$ and the first element of the second public key $\mathbf{Y}_2 = \mathbf{D}^{y_1}\mathbf{H}^{y_2}\alpha$.

(3) Generate at random three 256-bit integers $z_1 < q$, $z_2 < q$, and $\beta < p$, where β is a primitive element modulo p, and calculate the second element of the first public key $\mathbf{Z}_1 = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$ and the second element of the second public key $\mathbf{Z}_2 = \mathbf{D}^{z_1}\mathbf{H}^{z_2}\beta$.

(4) Generate at random two 256-bit integers $u < q$ and $\gamma < p$, where γ is a primitive element modulo p, and calculate the third element of the first public key $\mathbf{U}_1 = \mathbf{G}^{u}\gamma$ and the third element of the second public key $\mathbf{U}_2 = \mathbf{D}^{u}\gamma$.

This algorithm outputs the first 384-byte public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$) and the second 384-byte public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$). These two key compose a single 768-byte public key. The private key represents the set of eight 32-byte integers (y_1, y_2, α, z_1, z_2, β, u, γ) and the set of four 128-byte vectors (**G**, **Q**, **D**, **H**). Total size of the private key is equal to 768 bytes.

To generate (and then verify) a signature to an electronic document M, a secure 256-bit hash function f_H is supposed to be used.

4.1 Signature generation algorithm

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

(2) Calculate the vector $\mathbf{R}_1 = \mathbf{G}^k\mathbf{Q}^t\rho$.

(3) Calculate the vector $\mathbf{R}_2 = \mathbf{D}^k\mathbf{H}^t\rho$.

(4) Calculate the first signature element e that is a hash-function value calculated from the document M, to which the vectors $\mathbf{R}_1$ and $\mathbf{R}_2$ are concatenated: $e = f_H(M, \mathbf{R}_1, \mathbf{R}_2)$.

(5) Calculate the second signature element s: $s = z_2^{-1}(t - y_2 e) \bmod q$.

(6) Calculate the third signature element d: $d = u^{-1}(k - y_1 e - z_1 s) \bmod q$.

(7) Calculate the fourth signature element σ: $\sigma = \rho\alpha^{-e}\beta^{-s}\gamma^{-d} \bmod p$.

The signature represents the following set of four 32-byte integers (e, s, d, σ) with total size equal to 128 bytes. Computational complexity of the signature generation procedure can be roughly estimate as four exponentiations in the used four-dimensional FAAs and three exponentiations in $GF(p)$ or as ≈26000 multiplications in $GF(p)$.

4.2 The signature verification algorithm

(1) Calculate the vector $\mathbf{R}_1^* = \mathbf{Y}_1^e \mathbf{Z}_1^s \mathbf{U}_1^d \sigma$.

(2) Calculate the vector $\mathbf{R}_2^* = \mathbf{Y}_2^e \mathbf{Z}_2^s \mathbf{U}_2^d \sigma$.

(3) Compute the hash-function value from the document M to which the vectors $\mathbf{R}_1^*$ and $\mathbf{R}_2^*$ are concatenated: $e^* = f_H(M, \mathbf{R}_1^*, \mathbf{R}_2^*)$.

(4) If $e^* = e$, then the signature is genuine, else the signature is rejected.

Computational complexity of the signature verification procedure can be roughly estimate as six exponentiations in the used four-dimensional FAAs or as ≈37250 multiplications in $GF(p)$.

4.3 Signature scheme correctness proof

Consider a signature (e, s, d, σ) that has been computed in full correspondence with the signature generation procedure. Suppose the signature (e, s, d, σ) is submitted to the input of the verification procedure, then we have the following proof of the correctness of the introduced digital signature algorithm:

$$
\begin{aligned}
&\mathbf{R}_1{}^* = \mathbf{Y}_1^e \mathbf{Z}_1^s \mathbf{U}_1^d \sigma = \\
&= \mathbf{G}^{ey_1} \mathbf{Q}^{ey_2} \alpha^e \mathbf{G}^{sz_1} \mathbf{Q}^{sz_2} \beta^s \mathbf{G}^{du} \gamma^d \sigma = \\
&= \mathbf{G}^{ey_1 + sz_1 + du} \mathbf{Q}^{ey_2 + sz_2} \alpha^e \beta^s \gamma^d \rho \alpha^{-e} \beta^{-s} \gamma^{-d} = \\
&= \mathbf{G}^{ey_1 + sz_1 + (k - ey_1 - sz_1)} \mathbf{Q}^{ey_2 + (t - ey_2)} \rho = \\
&= \mathbf{G}^k \mathbf{Q}^t \rho = \mathbf{R}_1; \\
&\mathbf{R}_2{}^* = \mathbf{Y}_2^e \mathbf{Z}_2^s \mathbf{U}_2^d \sigma = \\
&= \mathbf{D}^{ey_1} \mathbf{H}^{ey_2} \alpha^e \mathbf{D}^{sz_1} \mathbf{H}^{sz_2} \beta^s \mathbf{D}^{du} \gamma^d \sigma = \\
&= \mathbf{D}^{ey_1 + sz_1 + du} \mathbf{H}^{ey_2 + sz_2} \alpha^e \beta^s \gamma^d \rho \alpha^{-e} \beta^{-s} \gamma^{-d} = \\
&= \mathbf{D}^{ey_1 + sz_1 + (k - ey_1 - sz_1)} \mathbf{H}^{ey_2 + (t - ey_2)} \rho = \\
&= \mathbf{D}^k \mathbf{H}^t \rho = \mathbf{R}_2; \\
&\{\mathbf{R}_1{}^* = \mathbf{R}_1; \mathbf{R}_2{}^* = \mathbf{R}_2\} \Rightarrow \mathbf{e}^* = \mathbf{e}
\end{aligned}
$$

The equality $e^* = e$ means that the input digital signature is accepted as a genuine signature, i.e. the developed signature scheme performs correctly.

5. Discussion

We refer the developed digital signature algorithm to type of HDLP-based signature schemes, since the vectors belonging to some primary two-dimensional cyclicity group, which is hidden in a primary four-dimensional cyclicity group, are used in calculating the elements of

the public key and generating the signature. In our case, the masking operations are scalar multiplications, which is a new technique for constructing HDLP-based signature schemes.

The technique of doubling the verification equation when designing a signature scheme was previously used in [12, 14], but in the proposed method it is extended to the case of using two different algebras as a single algebraic carrier of the signature scheme. At the same time, it has a new purpose, which is to provide binding of public key elements to a fixed hidden group in each of the used algebras.

The last point is important to ensure that the signature scheme is resistant to signature forgery by a person who has the ability to efficiently calculate a four-dimensional algorithm using a new type of quantum computer that may appear in the future. The resistance of the proposed algorithm to the attacks of the specified alleged person is due to the fact that the signature forger does not know the basis over which it is required to calculate four-dimensional logarithms.

As a substantiation of resistance to quantum attacks, it should be noted that the proposed signature scheme satisfies the general criterion of post-quantum security used to develop HDLP-based signature schemes described in the papers [12–14]. The mentioned criterion is formulated as follows [12]: "Based on the public parameters of the signature scheme, the construction of a periodic function containing a period with the length depending on the discrete logarithm value should be a computationally intractable task." The fulfillment of this criterion in the developed signature scheme is ensured by the fact that the elements of the first (second) public key form the basis of a primary group of the order q^3 in the first (second) algebra used as an algebraic carrier, therefore, all possible products $\mathbf{Y}_1^i\mathbf{Z}_1^j\mathbf{U}_1^k$ in the first FAA and $\mathbf{Y}_2^i\mathbf{Z}_2^j\mathbf{U}_2^k$ the second FAA for $i, j, k = 0, 1, 2 \ldots, q-1$ run through all the elements of the said primary group and periodic functions $\mathbf{F}_1\ (i,j,k) = \mathbf{Y}_1^i\mathbf{Z}_1^j\mathbf{U}_1^k$ and $\mathbf{F}_2\ (i,j,k) = \mathbf{Y}_2^i\mathbf{Z}_2^j\mathbf{U}_2^k$ contain periods having the lengths (aq, bq, cq), where $a, b, c \in \{0, 1\}$, i.e. these two functions do not contain periods associated with secret values y_1, y_2, α, z_1, z_2, β, u, γ. Thus, the Shor algorithm [1] based on efficiency of a quantum computer to find period length of periodic functions set in a finite cyclic group and possible future quantum algorithm for periodic function set in commutative groups of general type are not directly applicable for breaking the proposed signature scheme.

Our preliminary assessment of the security of the developed signature scheme shows that using a 256-bit value of the prime number q provides 256-bit security to signature forgery. For a more reasonable choice of parameters, it is necessary to perform a more detailed and comprehensive security study, which is an independent task of a separate work.

Using a non-optimized implementation on a common laptop computer with microprocessor Intel Core i7-6567U at 3.3 GHz, the developed HDLP-based signature generation algorithm outputs about 1,500 signatures per second. Its performance can be

Signature scheme	Signature size (byte)	Public key size (byte)	Signature generation performance (a.u.)	Signature verification performance (a.u.)
Falcon [17]	1,280	1,793	50	25
Dilithium [16]	2,701	1,472	15	2
Rainbow	64	150,000	–	–
HDLP-based [12]	192	768	50	80
HDLP-based [14]	192	512	40	80
2048-bit RSA	256	288	10	90
Proposed	128	768	70	50

Table 3. Comparison with some known post-quantum signature schemes

increased significantly when optimizing the software implementation, however the latter item is outside the scope of this paper. Using the said implementation, correctness of the introduced signature scheme had been experimentally demonstrated.

At present the NIST world competition [4] for the development of post-quantum public-key cryptosystems has entered the third stage [5]. The finalists in the category of post-quantum digital signatures were Falcon [17] and Crystals-Dilithium [16], and Rainbow [18]. It is interesting to compare the proposed signature scheme with the finalists, with other HDLP-based signatures [12, 14], and with 2048-bit RSA signature algorithm [19]. Table 3 presents a rough comparison which uses the published results of comparing the performance of the finalists with each other and with the algorithm RSA-2048. To get performance comparison of the proposed signature scheme with RSA-2048 we had taken into account that the private (public) exponent in RSA-2048 has length about 2048 (256) bits and computational difficulty of one multiplication modulo a 2048-bit can be roughly estimated as 64 multiplications modulo a 257-bit number.

This comparison shows that the proposed signature algorithm has significantly smaller sizes of the public key and signature relative to the finalists of the NIST competition. The exception is the algorithm Rainbow with the minimum signature size (64 bytes), but it has an excessively large public key size (150,000 bytes). At the same time, the above comparison does not take into account the possibility of using optimization mechanisms for specific implementations of the developed signature algorithm, the use of which will increase the performance of both the signature generation procedure and the signature verification procedure by a factor of 3–5.

The main advantage of the proposed algorithm compared to the finalists of the NIST competition is the smaller size of the public key and the signature. However, the finalists have successfully past a long time term of security testing and the proposed algorithm show potential possibility to reduce significantly the size of signature (by a factor of $\approx$10) and of public key (by a factor of $\approx$2), independent detailed security study of the introduced signature scheme is needed though.

Nevertheless, the finalists have successfully passed long security testing. Like, the recently introduced HDLP-based post-quantum signature schemes [12, 14], the proposed algorithm only show a potential possibility to significantly reduce the size of the signature and public key. If further independent security investigation confirm the authors' expectations, then we can say that there is a way to solve the said important practical problem. The reader can make a significant contribution to clarifying this issue.

As compared with the analogous [12, 14], the proposed signature scheme provides shorter signatures, a bit higher signature generation performance and a bit lower signature verification performance.

6. Conclusion

A fundamentally new design method and a practical HDLP-based post-quantum digital signature algorithm has been introduced. The proposed method and signature scheme are quite simple to understand. One can suppose that the proposed method opens up the possibility of developing a new class of practical post-quantum signature algorithms. The latter represents a significant interest in the light of the widely conducted researches on the development of candidates for post-quantum digital signature standards.

References

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM J Comput. 1997; 26: 1484-509.
2. Ekert A, Jozsa R. Quantum computation and Shor's factoring algorithm. Rev Mod Phys. 1996; 68: 733-52.

3. Smolin JA, Smith G, Vargo A. Oversimplifying quantum factoring. Nature. 2013; 499(7457): 163-65.
4. Federal Register. Announcing request for nominations for public-key post-quantum cryptographic algorithms. Available from: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 13 February 2021).
5. Round 3 Finalists. Public-key encryption and key-establishment algorithms. Available from: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed 13 February 2021).
6. Kuzmin AS, Markov VT, Mikhalev AA, Mikhalev AV, Nechaev AA. Cryptographic algorithms on groups and algebras. J Math Sci. 2017; 223(5): 629-41.
7. Moldovyan NA, Moldovyan AA. Finite non-commutative associative algebras as carriers of hidden Discrete logarithm problem. Bull South Ural State Univ Ser Math Model Program Comp Softw. 2019; 12(1): 66-81. doi: 10.14529/mmp190106.
8. Agibalov GP. ElGamal cryptosystems on Boolean functions. Prikl Diskr Mat. 2018(42): 57-65. doi: 10.17223/20710410/42/4.
9. Hoffstein J, Pipher J, Schanck JM, Silverman JH, Whyte W, Zhang Z. Choosing parameters for NTRU encrypt. Cryptographers' Track at the RSA Conference – CTA-RSA 2017. Springer LNCS. 2017; 10159: 3-18.
10. Alamelou Q, Blazy O, Cauchie S, Gaborit P. A code-based group signature scheme. Des Codes Cryptogr. 2017; 82(1–2): 469-93.
11. Kosolapov YV, Turchenko OY. On the construction of a semantically secure modification of the McEliece cryptosystem. Prikl Diskr Mat. 2019(45): 33-43. doi 10.17223/20710410/45/4.
12. Moldovyan NA, Moldovyan AA. Candidate for practical post-quantum signature scheme. Vestnik Saint Petersburg Univ Appl Math Comp Sci Control Process. 2020; 16(4): 455-61. doi: 10.21638/11701/spbu10.2020.410.
13. Moldovyan DN, Moldovyan AA, Moldovyan NA. An enhanced version of the hidden discrete logarithm problem and its algebraic support. Quasigr Relat Syst. 2020; 28(2): 269-84. Available from: http://www.quasigroups.eu/.
14. Moldovyan DN, Moldovyan AA, Moldovyan NA. A novel method for development of post-quantum digital signature schemes. Informatsionno-upravliaiushchie sistemy [Inform Control Syst], 2020(6): 21-29. doi: 10.31799/1684-8853-2020-6-21-29.
15. Moldovyan NA. A unified method for setting finite non-commutative associative algebras and their properties. Quasigr Relat Syst. 2018; 26(2): 263-70. http://www.quasigroups.eu/.
16. Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehlé D. CRYSTALS-Dilithium: a lattice-based Digital signature scheme. Available from: https://eprint.iacr.org/2017/633.pdf https://pq-crystals.org/dilithium/index.shtml (accessed 15 February 2021).
17. Fast-Fourier lattice-based compact signatures over NTRU. https://falcon-sign.info/ (accessed 15 February 2021).
18. 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; 3531: 164-175.
19. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public key cryptosystems. Commun ACM. 1978; 21: 120-26.

Corresponding author
Nikolay Andreevich Moldovyan can be contacted at: nmold@mail.ru