UDC 003.26
doi:10.31799/1684-8853-2023-1-29-40
EDN: KSCBTZ

Articles

Post-quantum algebraic signature algorithms with a hidden group

A. A. Moldovyan[a], *Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0001-5480-6016*
N. A. Moldovyan[a], *Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0002-4483-5048, nmold@mail.ru*
[a]*St. Petersburg Federal Research Center of the RAS, 39, 14th Line, 199178, Saint-Petersburg, Russian Federation*

Introduction: *The development of post-quantum standards on digital signature algorithms is one of the current challenges faced by the global cryptographic community. Recently, two types of algebraic signature schemes with a hidden group have been proposed, in which the finite non-commutative associative algebras set over the field GF(p) are used as an algebraic support. The design of that type of signature algorithms on the algebras set over the finite fields of Characteristic two represent significant interest for improving the performance and reducing the hardware implementation cost.* ***Purpose:*** *To develop post-quantum algebraic signature algorithms in which computations in a finite field of Characteristic two are used.* ***Results:*** *Several 4-dimensional finite non-commutative algebras set over the GF(2^z) fields are proposed as algebraic support of the signature schemes with a hidden group. We suggest some recommendations for choosing the value of the extension degree z. In particular cases the value of z represents a Mersenne degree. Compared with the signature algorithms which are based on the hidden logarithm problem, the algebraic signature algorithms based on the computational complexity of solving systems of many quadratic equations with many variables are considered to be a preferable type of cryptoschemes with a hidden group. We have introduced new practical signature algorithms with a hidden group. In two of the developed algorithms the signature (e,* ***S****) represents an integer e and a 4-dimensional vector* ***S*** *and is verified with vector equations with three and four entries of the signature element* ***S****.* ***Practical relevance:*** *Like other known signature schemes with a hidden group, the proposed two schemes have sufficiently small size of signature and public key. Due to comparatively small hardware implementation cost and high performance, the introduced candidates for post-quantum signature algorithms represent practical interest and are attractive as a potential prototype of a post-quantum digital signature standard.*

Keywords *— post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, multivariate cryptography, finite non-commutative algebras, associative algebras, cyclic groups, multidimensional cyclicity.*

For citation: Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. *Informatsionno-upravliaiushchiesistemy* [Information and Control Systems], 2023, no. 1, pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40, EDN: KSCBTZ

Introduction

The predicted emergence of quantum computers in practice in the near future and the availability of polynomial in time quantum algorithms for solving the discrete logarithm problem and the factorization problem [1–3] determine the high degree of relevance of the development of post-quantum public-key cryptographic schemes, which are resistant to quantum attacks (attacks with using ordinary and quantum computers). Post-quantum signature algorithms are to be based on hard problems different from discrete logarithm and factorization problems.

In particular, the quantum computer is not effective for finding solutions of systems of many quadratic equations with many unknowns and computational difficulty of this problem underlies the resistance of the multivariate signature algorithms [4–6]. There are known signature schemes on algebras [7, 8], on algebraic lattices [9], on codes [10, 11], and on hash functions [12]. A certain disadvantage of the known post-quantum signature schemes is a large size of public key and signature. In order to reduce the total size of the signature and the key, the signature schemes with a hidden group are proposed, in which finite non-commutative associative algebras (FNAA) are used as an algebraic support [13, 14]. One can distinguish two types of algorithms with a hidden group, which differ in the type of the used computationally difficult problem:

1) algorithms, security of which is based on the computational difficulty of the hidden discrete logarithm problem (HDLP) [13, 15];

2) algorithms, security of which is based on the computational difficulty of finding a solution of a system of many quadratic equations with many unknowns [14, 16].

A hidden group represents a subset of elements of some m-dimensional FNAA, which composes a commutative group. In the algorithms of the both types, the elements of the public key are computed as a masked (secret) element $\mathbf{H}$ of the hidden group. The masking is performed, for example, as the left and the right multiplications of the m-dimensional invertible vector $\mathbf{H}$ by some secret invertible vectors $\mathbf{A}$ and $\mathbf{B}$ which satisfy the following conditions $\mathbf{BA} \neq \mathbf{AB}$, $\mathbf{HA} \neq \mathbf{AH}$, $\mathbf{HB} \neq \mathbf{BH}$.

The FNAAs defined over a ground finite field $GF(p)$ with prime $p = 2q + 1$, where q is also a

prime, are used as algebraic supports of the known signature algorithms with a hidden group [7, 13]. To improve the performance and reduce the hardware implementation cost, development of the post-quantum algebraic signature algorithms on FNAAs set over finite fields of characteristic two, i. e. over the fields $GF(2^z)$, represents significant interest.

In this paper, three different 4-dimensional FNAAs, including the algebras defined by a sparse basis vector multiplication tables (BVMTs), set over the $GF(2^z)$ fields are used as algebraic support of the proposed three new algebraic signature algorithms with a hidden group: i) one HDLP-based algorithm and ii) two algorithms with a hidden group, which are based on computational difficulty of solving a system of many quadratic equations with many unknowns. Compared with the former one, the latter are considered as more preferable candidates for post-quantum signature schemes. Recommendations for choosing the value of the extension degree z of the $GF(2^z)$ field are suggested for each of two types of the signature algorithms with a hidden group.

Four-dimensional FNAA used as algebraic support

Brief explanation of the notion of FNAA is provided in [16]: "A vector space of dimension m, which is set over a finite field $GF(p)$ or $GF(2^z)$, with additionally defined vector multiplication operation (that possesses the property of distributivity at the left and at the right relatively the addition operation) is called m-dimensional algebra [16]. A vector $\mathbf{A}$ can be represented in the following two forms: i) as an ordered set of its coordinates: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$ and ii) as a sum of its components: $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ ($i = 0, 1, \ldots, m-1$) are basis vectors. If the defined multiplication operation is non-commutative and associative, then one gets m-dimensional FNAA. Usually, the product of the 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 formula $\mathbf{AB} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i\mathbf{e}_j$, where the values a_i and b_i are multiplied as the field elements 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 BVMT".

Usually, to perform one multiplication operation in some 4-dimensional algebra (see, for example, Table 1 [8]) one need to execute 16 multiplications and 12 additions in the field $GF(p)$ or $GF(2^z)$. However, computational complexity of this operation can be reduced, using sparse BVMTs (see, for example, Tables 2 [7] and 3 [16]).

■ ***Table 1.*** Multiplication of basis vectors ($\lambda\sigma \neq 1$, $\lambda \neq 0$, and $\sigma \neq 0$) in the 4-dimensional FNAA [8]

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

■ ***Table 2.*** Sparse BVMT ($\lambda \neq 0$) defining the 4-dimensional FNAA with global two-sided unit $\mathbf{E} = (1, 1, 0, 0)$ [7]

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

■ ***Table 3.*** Sparse BVMT ($\lambda \neq 0$) defining the 4-dimensional FNAA with global two-sided unit $\mathbf{E} = (0, 1, 1, 0)$ [16]

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

In addition to a faster multiplication operation, the 4-dimensional FNAAs defined by the sparse BVMTs are attractive to the fact that their detailed structure (in terms of decomposition into a set of commutative subalgebras) is known for the case of defining the algebras over the fields $GF(p)$ with arbitrary odd characteristics p. Besides, using the technique by [7, 8], one can show that, in the case of defining the algebras over the fields $GF(2^z)$, where $z > 0$, the 4-dimensional FNAAs set by Tables 1 and 2, possess the following common properties:

1) the 4-dimensional FNAA contains $2^{2z} + 2^z + 1$ of commutative subalgebras of the order 2^{2z}, every pair of which intersecting exactly in the set of scalar vectors $\{\mathbf{L}: \mathbf{L} = h\mathbf{E}, h = 0, 1, \ldots, 2^z - 1\}$, where $\mathbf{E}$ is the global two-sided unit;

2) the order of multiplicative group Γ of the algebra is equal to

$$\Omega = 2^z(2^{2z} - 1)(2^z - 1); \qquad (1)$$

3) the group Γ contains sufficiently large number ($> 2^z$) of commutative subgroups Γ_1 possessing

2-dimensional cyclicity (i. e., a minimum generator system of the subgroup Γ_1 contains two vectors of the same order) and having order equal to

$$\Omega_1 = (2^z - 1)^2; \quad (2)$$

4) the group Γ contains sufficiently large number ($> 2^z$) of commutative cyclic subgroups Γ_2 of the order

$$\Omega_2 = 2^{2z} - 1 = (2^z - 1)(2^z + 1); \quad (3)$$

5) the group Γ contains commutative cyclic subgroups Γ_3 of the order

$$\Omega_3 = 2^z(2^z - 1). \quad (4)$$

The condition of invertibility of some vector **A** in the FNAA set by Table 2 over a field $GF(p)$ [7] is also valid in the cased of defining the FNAA over the $GF(2^z)$ fields:

$$a_0a_1 \neq \lambda a_2a_3. \quad (5)$$

Similarly, we have the following invertibility condition for the FNAA set by Table 3 over the $GF(2^z)$ fields [16]:

$$a_1a_2 \neq \lambda a_0a_3. \quad (6)$$

For the 4-dimensional FNAA set by Table 1 over the $GF(2^z)$ fields (commutative groups of the Γ_1, Γ_2, and Γ_3 types are also contained in this algebra), from [8] one gets the invertibility condition

$$a_1a_2 \neq a_0a_3 \quad (7)$$

and the following formula for the two-sided global unit **E** depending on the structural constants λ and σ (that can be selected arbitrarily, but satisfying the conditions $\lambda\sigma \neq 1$, $\lambda \neq 0$, and $\sigma \neq 0$):

$$\mathbf{E} = \left(\frac{\sigma}{\sigma\lambda - 1}, \frac{1}{1 - \sigma\lambda}, \frac{1}{1 - \sigma\lambda}, \frac{\lambda}{\sigma\lambda - 1} \right). \quad (8)$$

To execute the exponentiation operation in FNAAs, i. e. for calculating the value $\mathbf{R} = \mathbf{W}^k$ (**W** is a vector; k is a non-negative integer), we propose the following modification of the fast-exponentiation algorithm, which is free of using the **E** value:

INPUT: **W** and $k > 0$.

1. Set $\mathbf{V} \leftarrow \mathbf{W}$, and $n \leftarrow k$.
2. If $n \bmod 2 = 1$, then go to step 4.
3. $\mathbf{V} \leftarrow \mathbf{V}^2$, $n \leftarrow n$ div 2, and go to step 2.
4. $\mathbf{R} \leftarrow \mathbf{V}$, $\mathbf{V} \leftarrow \mathbf{V}^2$, $n \leftarrow n$ div 2.
5. If $n = 0$, then STOP.
6. If $n \bmod 2 = 1$, then go to step 8.
7. $\mathbf{V} \leftarrow \mathbf{V}^2$, $n \leftarrow n$ div 2, and go to step 6.
8. $\mathbf{R} \leftarrow \mathbf{RV}$, $\mathbf{V} \leftarrow \mathbf{V}^2$, $n \leftarrow n$ div 2, and go to step 5.

OUTPUT: $\mathbf{R} = \mathbf{W}^k$.

Development of the algebraic signature algorithms with a hidden group, which are based on computational difficulty of the HDLP, is connected with the requirement of existence of a large-size prime factor of the order of the hidden group. Taking into account that the said algorithms use hidden groups which are subgroups of the commutative groups of the Γ_1 and Γ_2 types, one can recommend the values of z shown in Tables 4 and 5. The values z = 61, 89, 107, 127, 521, and 607 are Mersenne degrees that define prime values of $2^z - 1$.

Development of the algorithms with a hidden group, which are based on computational difficulty of solving a system of many quadratic equations with many unknowns, is free of the requirement of existence of a large-size prime factor of the order of the hidden group. Security of the algorithms of this type depends on the size of the order of the hidden group and is not dependent on the factorization of the order. However, to provide a higher performance the hidden group order should be free of small-size factors (for example, less than 20 bits). If the order of a group of the Γ_1-type is free of the said factors,

■ ***Table 4.*** The case of using the Γ_1-type and Γ_2-type commutative groups (or their subgroups) as a hidden group in the HDLP-based signature algorithms

Degree z	Number of prime factors of the value $2^z - 1$ (their size in bits)	Degree z	Number of prime factors of the value $2^z - 1$ (their size in bits)
61	1 (61)	281	2 (17 and 265)
89	1 (89)	373	2 (25 and 349)
107	1 (107)	421	2 (50 and 372)
127	1 (127)	457	2 (28 and 430)
131	2 (9 and 123)	521	1 (521)
197	2 (13 and 185)	607	1 (607)

■ ***Table 5.*** Additional values of z for the case of using the Γ_2-type commutative groups (or their subgroups) as a hidden group in the HDLP-based signature algorithms

Degree z	Number of prime factors of the value $2^z + 1$ (their size in bits)	Degree z	Number of prime factors of the value $2^z + 1$ (their size in bits)
101	1 (100)	311	2 (16 and 294)
127	1 (126)	313	1 (312)
179	2 (36 and 142)	347	1 (346)
199	1 (198)	433	2 (22 and 410)
229	2 (25 and 204)	–	–

■ ***Table 6.*** The case of using a hidden group of the Γ_1-type

Degree z	Number of β-bit prime ($\beta \geq 30$) factors of the value $2^z - 1$ (their size in bits)	Degree z	Number of β-bit prime ($\beta \geq 26$) factors of the value $2^z - 1$ (their size in bits)
89	Mersenne degree	257	3 (49, 80, and 129) [17]
101	2 (43 and 59) [17]	271	2 (34 and 238) [17]
103	2 (39 and 63) [17]	293	2 (86 and 208) [17]
107	Mersenne degree	307	4 (31, 42, 68, and 166)
109	2 (30 and 80) [17]	331	3 (44, 50, and 238) [17]
127	Mersenne degree	347	2 (74 and 274) [17]
137	2 (65 and 73) [17]	379	2 (38 and 342) [17]
139	2 (43 and 97) [17]	389	3 (26, 33, and 332) [17]
149	2 (67 and 83) [17]	421	2 (50 and 372)
173	3 (41, 56, and 78) [17]	433	4 (65, 80, 83, and 208)
199	2 (38 and 162) [17]	503	4 (52, 64, 71, and 318)

■ ***Table 7.*** The case of using a hidden group of the Γ_2-type

Degree z	Number of β-bit prime ($\beta \geq 36$) factors of the value $2^z + 1$ (their size in bits)	Degree z	Number of β-bit prime ($\beta \geq 22$) factors of the value $2^z + 1$ (their size in bits)
101	1 (100)	307	4 (31, 42, 68, and 166)
127	1 (126)	347	1 (346)
179	2 (36 and 142)	379	3 (44, 100, and 235)
199	1 (198)	389	4 (40, 51, 52, and 246)
257	3 (46, 69, and 142)	433	2 (22 and 410)
271	2 (45 and 231)	503	4 (52, 64, 71, and 318)

then each of them can be used as the hidden group of the designed signature scheme.

The order Ω_2 of the Γ_2 group contains factor 3 [see formula (3)]. If no other small-size factors are contained in $\Omega_2 = (2^z - 1)(2^z + 1)$, then the subgroup of the order $\Omega_2/3$ can be used as a hidden group. The values of z suitable for development of signature algorithms with a hidden group of the Γ_1-type, based on difficulty of solving a system of quadratic equations, are shown in Table 6 [17] (Γ_2-type – in Table 7). In the case of the hidden group of the Γ_2-type, one should use the z values that determine the absence of short divisors for the values $2^z - 1$ and $2^z + 1$ (except the two-bit divisor 3 for the second value).

When developing the signature schemes with a hidden group, it is assumed to use algorithms for generating a basis (minimum generator system) of the hidden group. For example, you can use the following algorithms.

Algorithm 1: generating a basis of the Γ_1-type group.

1. Using the invertibility condition [see formulas (5)–(7)], generate a random invertible vector $\mathbf{V}$ of the order $q = 2^z - 1$.

2. If the vector $\mathbf{V}$ is contained in the set of scalar vectors, i. e., if $\mathbf{V} = \sigma\mathbf{E}$ for some value $\sigma \in GF(2^z)$, then go to step 1.

3. Generate a random integer k ($0 < k < q$) and a random binary polynomial $\beta \in GF(2^z)$ of the order $2^z - 1$.

4. Compute the vector $\mathbf{H} = \beta\mathbf{V}^k$.

5. Output the pair of vectors $\mathbf{H}$ and $\mathbf{G} = \mathbf{V}$ as a basis $<\mathbf{G}, \mathbf{H}>$ of a random Γ_1-type group.

This algorithm works correctly, since the vectors of the order $2^z - 1$ in the groups of the Γ_2 and Γ_3-types are scalar vectors.

Algorithm 2: generating a basis of the Γ_2-type group.

1. Using the invertibility condition [see formulas (5)–(7)], generate a random invertible vector $\mathbf{V}$ of order the $q = (2^z - 1)(2^z + 1)$.

2. Output the vector $\mathbf{V}$ as a generator (basis $<\mathbf{V}>$) of a random Γ_2-type group.

This algorithm works correctly, since the Γ_1-type and Γ_3-type groups do not contain vectors of the order $(2^z - 1)(2^z + 1)$. Evidently, the vector $\mathbf{J} = \mathbf{V}^3$ is a generator of a commutative cyclic group Γ_2' of the order $q/3$, which is a subgroup of the Γ_2-type group generated by the vector $\mathbf{V}$.

The described 4-dimensional FNAAs are used as algebraic carrier of three new signature algorithms with a hidden group. Evidently the said FNAAs (set over $GF(2^z)$) could be used to update the known algorithms of such type, for example, described in [7, 13] (for the first type of the signature algorithms with a hidden group) and in [15] (for the second type of the signature algorithms with a hidden group). However, the authors prefer to illustrate existence of variety of possibilities, when designing algorithms with a hidden group.

A signature scheme based on HDLP

In this section it is introduced a HDLP-based signature algorithm (the first signature scheme) that illustrates the first type of the algebraic signa-

ture schemes with a hidden group. The development of various types of HDLP-based algorithms and methods for setting a hidden group formed the prerequisites on the basis of which the second type of signature algorithms with a hidden group was born. The reader can easily see the similar construction elements in the two types of the algorithms introduced in this paper (see also the next section).

Suppose a 4-dimensional FNAA is set by Table 2 over the field $GF(2^z)$, where $z = 521$ and $q = 2^z - 1$ is a prime number. Using a group of the Γ_1-type (set by some basis $<\mathbf{G}, \mathbf{H}>$), you can generate a public key in the form of three vectors **U**, **Y**, and **Z** as follows:

1. Generate two random invertible vectors **A** and **B** of the order $\omega \geq p - 1$, satisfying the conditions $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

2. Generate two random integers $x < q$ and $u < q$. Then calculate the first element **U** of the public key: $\mathbf{U} = \mathbf{AG}^x\mathbf{H}^u\mathbf{B}^{-1}$.

3. Calculate the second element **Y** of the public key: $\mathbf{Y} = \mathbf{BGB}^{-1}$.

4. Calculate the third element **Z** of the public key: $\mathbf{Z} = \mathbf{BHA}^{-1}$.

The pair of numbers (x, u) and the vectors **G**, **H**, **A**, and **B** compose a secret key (having size ≈ 1173 bytes) and are used for generating a signature to some electronic document M. The size of the public key represented by the triple of vectors (**U**, **Y**, **Z**) is equal to ≈ 782 bytes.

Algorithm for generating a signature.

1. Generate a random natural integer $k < q$ and calculate the vector $\mathbf{K} = \mathbf{G}^k$.

2. Generate a random natural integer $t < q$ and calculate the vector $\mathbf{R} = \mathbf{AKH}^t\mathbf{A}^{-1}$.

3. Using a specified 521-bit hash function f, calculate the first signature element e as a hash-function value from the document M to which the vector **R** is concatenated: $e = f(M, \mathbf{R})$.

4. Compute the second signature element s:

$$s = \sqrt{\frac{1}{e}\left(k - \frac{tx}{u+1}\right)} \bmod q.$$

5. If the value under the root is a quadratic non-residue modulo q, then go to step 2.

6. Compute the third signature element d:

$$d = \left(\frac{t}{s(u+1)} - 1\right) \bmod q.$$

This algorithm outputs a 196-byte signature in the form of a triple of 521-bit integers (e, s, d). Computational difficulty of the signature generation algorithm is defined mainly by exponentiation operations performed at steps 1 and 2. It is easy to see that on the average three exponentiations in the FNAA used as algebraic support (≈ 18 432 multiplications in $GF(2^{521})$) are executed to generate one signature.

Algorithm for verifying a signature.

1. Calculate the vector

$$\mathbf{R}' = \left(\mathbf{UY}^{es}\mathbf{Z}(\mathbf{UZ})^d\right)^s.$$

2. Calculate the hash-function value from the document M to which the vector $\mathbf{R}'$ is concatenated: $e' = f(M, \mathbf{R}')$.

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

Computational difficulty of the signature verification procedure can be estimate as three exponentiations in the 4-dimensional FNAA used as algebraic support (≈ 18 432 multiplications in $GF(2^{521})$).

Correctness proof of the described signature scheme is as follows (see formulas used at steps 4 and 6 of the signature generation algorithm):

$$\mathbf{R}' = \left(\mathbf{UY}^{es}\mathbf{Z}(\mathbf{UZ})^d\right)^s = \left(\mathbf{AG}^x\mathbf{H}^u\mathbf{B}^{-1}\mathbf{BG}^{es} \times \right.$$

$$\left. \times \mathbf{B}^{-1}\mathbf{BHA}^{-1}\left(\mathbf{AG}^x\mathbf{H}^u\mathbf{B}^{-1}\mathbf{BHA}^{-1}\right)^d\right)^s =$$

$$= \left(\mathbf{AG}^{x+es}\mathbf{H}^{u+1}\mathbf{A}^{-1}\mathbf{AG}^{xd}\mathbf{H}^{d(u+1)}\mathbf{A}^{-1}\right)^s =$$

$$= \left(\mathbf{AG}^{x+es+xd}\mathbf{H}^{u+1+d(u+1)}\mathbf{A}^{-1}\right)^s =$$

$$= \mathbf{AG}^{xs(d+1)+es^2}\mathbf{H}^{sd(u+1)+s(u+1)}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^{xs\frac{t}{s(u+1)}+e\frac{1}{e}\left(k-\frac{tx}{u+1}\right)}\mathbf{H}^{\left(\frac{t}{u+1}-s\right)(u+1)+s(u+1)} \times$$

$$\times \mathbf{A}^{-1} = \mathbf{AG}^k\mathbf{H}^t\mathbf{A}^{-1} = \mathbf{R} \Rightarrow$$

$$\Rightarrow f(M, \mathbf{R}') = f(M, \mathbf{R}) \Rightarrow e' = e.$$

A critical point of the consideration of the HDLP-based signature algorithms as candidates for post-quantum cryptoschemes is potential possibility of using algebraic methods to reduce the HDLP to ordinary DLP. Therefore, the second-type algebraic signature schemes with a hidden group, which are based on computational difficulty of solving a system of many quadratic equations with many unknowns (the problem for solving of which the quantum computer is not efficient), can be estimated as a more preferable candidates for post-quantum signature schemes.

Signature schemes based on difficulty of solving a system of many quadratic equations

The second proposed signature scheme is described as follows. Suppose the 4-dimensional FNAA is set by Table 3 over the field $GF(2^z)$, where $z = 257$.

Then, generating a random secret basis <**G**, **H**> of a group of the Γ_1-type one can generate a public key in the form of six vectors ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$, $\mathbf{Z}_3$, **T**) as follows.

Public-key generation algorithm.

1. Using the invertibility condition (6), generate at random invertible vectors **A**, **B**, **D**, and **F** satisfying the following non-equalities: $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AF} \neq \mathbf{FA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BF} \neq \mathbf{FB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DF} \neq \mathbf{FD}$, $\mathbf{DG} \neq \mathbf{GD}$, and $\mathbf{FG} \neq \mathbf{GF}$.

2. Calculate the vectors $\mathbf{A}^{-1}$, $\mathbf{B}^{-1}$, $\mathbf{D}^{-1}$, and $\mathbf{F}^{-1}$.

3. Generate non-negative integers $x < q$ and $w < q$, where $q = 2^z - 1$ is a 256-bit number that is product of three primes having the size 49, 80, and 129 bits (see Table 6). Then compute the public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$, $\mathbf{Z}_3$, **T**) by formulas

$$\mathbf{Y}_1 = \mathbf{AGB};\ \mathbf{Z}_1 = \mathbf{DHA}^{-1};$$

$$\mathbf{Y}_2 = \mathbf{FH}^x\mathbf{B};\ \mathbf{Z}_2 = \mathbf{DH}^w\mathbf{GF}^{-1};$$

$$\mathbf{Y}_3 = \mathbf{AG}^w\mathbf{B};\ \mathbf{Z}_3 = \mathbf{DHGF}^{-1};\ \mathbf{T} = \mathbf{DHG}^x\mathbf{B}. \quad (9)$$

The secret key (with total size ≈ 833 bytes) represents two integers x, w and six vectors **G**, **H**, **A**, **B**, **D**, and **F**. The size of public key is equal to ≈ 900 bytes. Computation of a signature to some electronic document M is performed, using the following algorithm.

Signature generation algorithm.

1. Generate at random two natural numbers k ($k < q$) and t ($t < q$). Then calculate the vector

$$\mathbf{R} = \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1}. \quad (10)$$

2. Using a specified $2z$-bit hash function f, calculate the first signature element e as a hash-function value from the document M to which the vector **R** is concatenated: $e = e_1||e_2 = f(M, \mathbf{R})$, where the hash-value e is represented as concatenation of two z-bit integers e_1 and e_2.

3. If the integers $2e_1 + e_2 + 1$ and q are not mutually prime, then go to step 1. Otherwise, calculate the natural numbers n and d:

$$n = \frac{k - e_1 - xe_1 - e_2 - w - 1}{2e_1 + e_2 + 1} \bmod q; \quad (11)$$

$$d = \frac{t - 2e_1 - xe_2 - we_2 - 1}{2e_1 + e_2 + 1} \bmod q. \quad (12)$$

4. Calculate the second signature element in the form of the vector **S**:

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}. \quad (13)$$

Since the integer q contains three factors of sufficiently large size (≥ 49 bits), the probability of repeating the first step of the algorithm is negligible. Therefore, the computational complexity of this algorithm is determined mainly by 4 exponentiations in the used FNAA (≈ $48z$ = 12 336 multiplications in $GF(2^z)$). The size of the signature (e, **S**) is equal to $6z$ bits (≈ 193 bytes). Verification of the signature is performed, using the public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$, $\mathbf{Z}_3$, **T**) and the following procedure.

Signature verification algorithm.

1. Compute the vector $\mathbf{R}'$ by the following formula with four entries of the signature element **S**:

$$\mathbf{R}' = \left(\mathbf{Y}_1\mathbf{STSZ}_1\right)^{e_1}\mathbf{Y}_3\mathbf{SZ}_3\left(\mathbf{Y}_2\mathbf{SZ}_2\right)^{e_2}. \quad (14)$$

2. Calculate the hash-value e' from the document to which the vector $\mathbf{R}'$ is concatenated: $e' = f(M, \mathbf{R}')$.

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

The computational complexity of the signature verification algorithm is determined mainly by 2 exponentiations in the used FNAA (≈ $24z$ = 6168 multiplications in $GF(2^z)$).

Correctness of the signature scheme is proven as follows.

Signature scheme correctness proof.

Compute the vectors

$$\mathbf{J}_1 = \left(\mathbf{Y}_1\mathbf{STSZ}_1\right)^{e_1} = \left(\mathbf{AGBB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1} \times \right.$$

$$\left. \times\ \mathbf{DG}^x\mathbf{HBB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DHA}^{-1}\right)^{e_1} =$$

$$= \left(\mathbf{AGG}^n\mathbf{H}^d\mathbf{G}^x\mathbf{HG}^n\mathbf{H}^d\mathbf{HA}^{-1}\right)^{e_1} =$$

$$= \left(\mathbf{AG}^{2n+x+1}\mathbf{H}^{2d+2}\mathbf{A}^{-1}\right)^{e_1} =$$

$$= \mathbf{AG}^{2ne_1+xe_1+e_1}\mathbf{H}^{2de_1+2e_1}\mathbf{A}^{-1};$$

$$\mathbf{J}_2 = \mathbf{Y}_3\mathbf{SZ}_3 = \mathbf{AG}^w\mathbf{BB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DHGF}^{-1} =$$

$$= \mathbf{AG}^{n+w+1}\mathbf{H}^{d+1}\mathbf{F}^{-1};$$

$$\mathbf{J}_3 = \left(\mathbf{Y}_2\mathbf{SZ}_2\right)^{e_2} =$$

$$= \left(\mathbf{FH}^x\mathbf{BB}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DH}^w\mathbf{GF}^{-1}\right)^{e_2} =$$

$$= \left(\mathbf{FG}^{n+1}\mathbf{H}^{d+x+w}\mathbf{F}^{-1}\right)^{e_2} =$$

$$= \mathbf{FG}^{ne_2+e_2}\mathbf{H}^{de_2+xe_2+we_2}\mathbf{F}^{-1}.$$

Then compute the vector $\mathbf{R}'$:

$$\mathbf{R}' = \mathbf{J}_1\mathbf{J}_2\mathbf{J}_3 = \mathbf{AG}^{2ne_1+xe_1+e_1}\mathbf{H}^{2de_1+2e_1}\mathbf{A}^{-1} \times$$

$$\times\ \mathbf{AG}^{n+w+1}\mathbf{H}^{d+1}\mathbf{F}^{-1} \times \mathbf{FG}^{ne_2+e_2}\mathbf{H}^{de_2+xe_2+we_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{2ne_1+xe_1+e_1+n+w+1+ne_2+e_2} \times$$

$$\times\ \mathbf{H}^{2de_1+2e_1+d+1+de_2+xe_2+we_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{n(2e_1+e_2+1)+e_1+xe_1+e_2+w+1} \times$$

$$\times\ \mathbf{H}^{d(2e_1+e_2+1)+2e_1+xe_2+we_2+1}\mathbf{F}^{-1}.$$

Taking into account the formulas (11) and (12) we get:

$$\mathbf{R}' = \mathbf{A}\mathbf{G}^k\mathbf{H}^t\mathbf{F}^{-1} = \mathbf{R} \Rightarrow$$
$$\Rightarrow f\left(M \,\|\, \mathbf{R}'\right) = f\left(M \,\|\, \mathbf{R}\right) \Rightarrow e' = e.$$

The final equality means validity of the input signature.

Security of the described signature scheme is based on computational difficulty of solving the system of 13 vector quadratic equations with the following 11 unknowns: **A**, **B**, **D**, **F**, **G**, **H**, $\mathbf{H}' = \mathbf{H}^x$, $\mathbf{H}'' = \mathbf{H}^w\mathbf{G}$, $\mathbf{G}' = \mathbf{G}^w$, $\mathbf{G}'' = \mathbf{G}\mathbf{H}$, and $\mathbf{G}''' = \mathbf{G}^x\mathbf{H}$, which are determined by the formulas (9) and the pair-wise permutability of the unknowns **G**, **H**, **H**′, **H**″, **G**′, **G**″, and **G**‴: $\mathbf{G}\mathbf{H} = \mathbf{H}\mathbf{G}$, $\mathbf{G}\mathbf{H}' = \mathbf{H}'\mathbf{G}$, $\mathbf{G}\mathbf{H}'' = \mathbf{H}''\mathbf{G}$, $\mathbf{G}\mathbf{G}' = \mathbf{G}''\mathbf{G}$, $\mathbf{G}\mathbf{G}'' = \mathbf{G}'\mathbf{G}$, and $\mathbf{G}\mathbf{G}''' = \mathbf{G}'''\mathbf{G}$. Using Table 3, the latter system reduces to a system of 52 quadratic equations (with 44 unknowns) in the field $GF(2^z)$.

A remarkable feature of the algebraic algorithms with a hidden group is the multiple entries of the signature element **S** in the vector verification equation set over a non-commutative algebra. This provides resistance to forging signature attacks base on using the value **S** as a fitting parameter. In the algorithm describe above we have four entries of the vector **S**. The number η of entries should satisfy the condition $\eta \geq 2$. The next digital signature scheme uses the value $\eta = 3$.

The third developed signature scheme is described as follows. Suppose the 4-dimensional FNAA is set by Table 1 over the field $GF(2^z)$, where $z = 199$ (see Tables 6 and 7). Then, generating a random secret basis <**G**> of a cyclic group of the Γ_2'-type (subgroup of a Γ_2-type group), which has order $q = \Omega_2/3 = 3^{-1}(2^z - 1)(2^z + 1)$, one can generate a public key in the form of seven vectors ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}_2$, **V**) as follows.

Public-key generation algorithm.

1. Using the invertibility condition (8), generate at random invertible vectors **A**, **B**, **D**, and **F** satisfying the following non-equalities: $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AF} \neq \mathbf{FA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BF} \neq \mathbf{FB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{FD} \neq \mathbf{DF}$, and $\mathbf{GF} \neq \mathbf{FG}$.

2. Calculate the vectors $\mathbf{A}^{-1}$, $\mathbf{B}^{-1}$, $\mathbf{D}^{-1}$, and $\mathbf{F}^{-1}$.

3. Calculate the vector $\mathbf{J} = \mathbf{G}^{q\left(2^z-1\right)^{-1}}$ of the order $q' = 3^{-1}(2^z + 1)$ and the vector $\mathbf{I} = \mathbf{G}^{3q\left(2^z+1\right)^{-1}}$ of the order $q'' = 2^z - 1$.

4. Generate at random non-negative integers x ($x < q'$) and w ($w < q''$), where q' is a 198-bit prime number and q'' is a product of two primes having the size 38 and 162 bits (see Tables 6 and 7). Then compute the public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}_2$, **V**) by formulas

$$\mathbf{Y}_1 = \mathbf{B}^{-1}\mathbf{J}\mathbf{A}^{-1};\ \mathbf{Z}_1 = \mathbf{B}^{-1}\mathbf{I}\mathbf{B};\ \mathbf{U}_1 = \mathbf{B}^{-1}\mathbf{J}^x\mathbf{F}^{-1};$$
$$\mathbf{Y}_2 = \mathbf{D}\mathbf{J}\mathbf{I}\mathbf{A}^{-1};\ \mathbf{Z}_2 = \mathbf{F}\mathbf{J}^w\mathbf{I}\,\mathbf{D}^{-1};$$
$$\mathbf{U}_2 = \mathbf{D}\mathbf{J}\mathbf{I}^x\mathbf{A}^{-1};\ \mathbf{V} = \mathbf{B}^{-1}\mathbf{I}^w\mathbf{D}^{-1}. \qquad (15)$$

The secret key (with total size ≈ 650 bytes) represents two integers x, w and six vectors **J**, **I**, **A**, **B**, **D**, and **F**. The size of public key is equal to ≈ 700 bytes. Computation of a signature to some electronic document M is performed, using the following algorithm.

Signature generation algorithm.

1. Generate at random two natural numbers k ($k < q'$) and t ($t < q''$). Then calculate the vector

$$\mathbf{R} = \mathbf{F}\mathbf{J}^k\mathbf{I}^t\mathbf{F}^{-1}. \qquad (16)$$

2. Using a specified $3z$-bit hash function f, calculate the first signature element e as a hash-function value from the document M to which the vector **R** is concatenated: $e = e_1||e_2||e_3 = f(M, \mathbf{R})$, where the hash-value e is represented as concatenation of tree z-bit integers e_1, e_2, and e_3.

3. If the integer $e_1e_2e_3 + e_2e_3 + e_3$ is not mutually prime with q' or with q'', then go to step 1. Otherwise, calculate the natural numbers n and d:

$$n = \left(\frac{k - we_3 - xe_3}{e_1e_2e_3 + e_2e_3 + e_3} - 1\right) \bmod q'; \qquad (17)$$

$$d = \left(\frac{t - we_2e_3 - xe_3}{e_1e_2e_3 + e_2e_3 + e_3} - 1\right) \bmod q''. \qquad (18)$$

4. Calculate the second signature element in the form of the vector **S**:

$$\mathbf{S} = \mathbf{A}\mathbf{J}^n\mathbf{I}^d\mathbf{B}. \qquad (19)$$

Since the integer q' is prime and q'' contains two factors of sufficiently large size (38 and 162 bits), the probability of repeating the first step of the algorithm is negligible. Therefore, the computational complexity of this algorithm is determined mainly by 4 exponentiations in the used FNAA (≈ $96z$ = 19 104 multiplications in $GF(2^z)$). The size of the signature (e, **S**) is equal to ≈ $7z$ bits (≈ 175 bytes). Verification of the signature is performed, using the public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}_2$, **V**) and the following procedure.

Signature verification algorithm.

1. Compute the vector **R**′ by the following formula with three entries of the signature element **S**:

$$\mathbf{R}' = \left[\mathbf{Z}_2\left(\mathbf{Y}_2\mathbf{S}\left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\mathbf{V}\right)^{e_2}\mathbf{U}_2\mathbf{S}\mathbf{U}_1\right]^{e_3}. \qquad (20)$$

2. Calculate the hash-value e' from the document to which the vector **R**′ is concatenated: $e' = f(M, \mathbf{R}')$.

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

The computational complexity of the signature verification algorithm is determined mainly by 3 exponentiations in the used FNAA ($\approx 72z$ = = 14 328 multiplications in $GF(2^z)$).

Correctness of the latter signature scheme is proven as follows.

Signature scheme correctness proof.

Calculate the values $\mathbf{X}_1$ and $\mathbf{X}_2$:

$$\mathbf{X}_1 = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1} = \left(\mathbf{B}^{-1}\mathbf{J}\mathbf{A}^{-1}\mathbf{A}\mathbf{J}^n\mathbf{I}^d\mathbf{B}\mathbf{B}^{-1}\mathbf{I}\mathbf{B}\right)^{e_1} =$$

$$= \mathbf{B}^{-1}\mathbf{J}^{e_1 n+e_1}\mathbf{I}^{e_1 d+e_1}\mathbf{B};$$

$$\mathbf{X}_2 = \left(\mathbf{Y}_2\mathbf{S}\mathbf{X}_1\mathbf{V}\right)^{e_2} =$$

$$= \left(\mathbf{D}\mathbf{J}\mathbf{I}\mathbf{A}^{-1}\mathbf{A}\mathbf{J}^n\mathbf{I}^d\mathbf{B}\mathbf{B}^{-1}\mathbf{J}^{e_1 n+e_1}\mathbf{I}^{e_1 d+e_1}\mathbf{B}\mathbf{B}^{-1}\mathbf{I}^w\mathbf{D}^{-1}\right)^{e_2} =$$

$$= \left(\mathbf{D}\mathbf{J}^{n(e_1+1)+e_1+1}\mathbf{I}^{d(e_1+1)+e_1+w+1}\mathbf{D}^{-1}\right)^{e_2} =$$

$$= \mathbf{D}\mathbf{J}^{n(e_1e_2+e_2)+e_1e_2+e_2}\mathbf{I}^{d(e_1e_2+e_2)+e_1e_2+we_2+e_2}\mathbf{D}^{-1}.$$

Then compute the vector $\mathbf{R}'$:

$$\mathbf{R}' = \left[\mathbf{Z}_2\mathbf{X}_2\mathbf{U}_2\mathbf{S}\mathbf{U}_1\right]^{e_3} =$$

$$= \begin{pmatrix} \mathbf{F}\mathbf{J}^w\mathbf{I}\mathbf{D}^{-1}\mathbf{D}\mathbf{J}^{n(e_1e_2+e_2)+e_1e_2+e_2} \times \\ \times\, \mathbf{I}^{d(e_1e_2+e_2)+e_1e_2+we_2+e_2} \times \\ \times\, \mathbf{D}^{-1}\mathbf{D}\mathbf{J}\mathbf{I}^x\mathbf{A}^{-1}\mathbf{A}\mathbf{J}^n\mathbf{I}^d\mathbf{B}\mathbf{B}^{-1}\mathbf{J}^x\mathbf{F}^{-1} \end{pmatrix}^{e_3} =$$

$$= \begin{pmatrix} \mathbf{F}\mathbf{J}^{n(e_1e_2+e_2+1)+e_1e_2+e_2+w+x+1} \times \\ \times\, \mathbf{I}^{d(e_1e_2+e_2+1)+e_1e_2+we_2+e_2+x+1}\mathbf{F}^{-1} \end{pmatrix}^{e_3} =$$

$$= \mathbf{F}\mathbf{J}^{n(e_1e_2e_3+e_2e_3+e_3)+e_1e_2e_3+e_2e_3+we_3+xe_3+e_3} \times$$

$$\times\, \mathbf{I}^{d(e_1e_2e_3+e_2e_3+e_3)+e_1e_2e_3+we_2e_3+e_2e_3+xe_3+e_3}\mathbf{F}^{-1}.$$

Taking into account the formulas (17) and (18) we get:

$$\mathbf{R}' = \mathbf{A}\mathbf{J}^k\mathbf{I}^t\mathbf{A}^{-1} = \mathbf{R} \Rightarrow f\left(M, \mathbf{R}'\right) = f\left(M, \mathbf{R}\right) \Rightarrow e' = e,$$

where the latter equality proves the correct performance of the signature scheme.

Discussion

In this paper, the first developed signature algorithm, based on HDLP, is considered as an illustration of signature schemes attributed to the first type of the algebraic signature algorithms with a hidden group. Comparison with the second-type algorithms shows that in the both cases the main operations used to generate the public key, to generate a signature, and to verify the signature are exponentiation operations. However, the signature algorithms of the second type have principal difference, namely, they are based on computational complexity of finding a solution of a system of many quadratic equations with many unknowns. To solve the latter problem, the quantum computer is not efficient [18]. This fact is used in the area of multivariate cryptography that is one of the directions in the development of post-quantum public-key cryptographic algorithms. The multivariate cryptography was initiated by the paper [19] in 1988.

Over the past 30 years of the research in the field of multivariate cryptography many multivariate signature algorithms are currently known. A merit of the multivariate signature schemes is small size of the signature. Unfortunately, their significant drawback is a very large size of the public key. The latter is associated with a specific method for developing the multivariate signature algorithms, including generation of the public key as a set of quadratic (or cubic) polynomials that describe a trapdoor one-way mapping of vectors of large dimensions (from 30 to 200), given over a finite field of sufficiently small order (from 2^2 to 2^{16}).

At present the cryptographic community has well worked out the basic methods for cryptanalysis of the multivariate-cryptography algorithms. The following two types of attacks are distinguished [18]: i) direct attacks based on the algorithms for solving systems of many power (quadratic in many cases) equations with many unknowns and ii) structural attacks that use the structural features of the cryptoscheme design.

Because of significantly different design of the signature algorithms with a hidden group and the multivariate-cryptography algorithms the structural attacks developed for cryptanalysis of the latter are hardly applicably to the former and novel types of structural attacks are to be developed. Therefore, for preliminary security estimation of the second and third proposed algebraic signature algorithms the known direct attacks can be considered. The most effective direct attack is the use of algorithms for solving systems of many power equations, based on the calculation of the Gröbner basis [20, 21]. Table 8 computed on the base of the results of the papers [20, 21] can be used to estimate security W of the introduced algebraic algorithms with a hidden group to the direct attack.

Security of the second introduced signature scheme (algorithm with the value $\eta = 4$) is based on difficulty of solving the system of 12 vector quadratic equations with 11 unknowns $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{H}$, $\mathbf{G}' = \mathbf{G}^w$, $\mathbf{H}' = \mathbf{H}^x$, $\mathbf{H}'' = \mathbf{H}^w$, $\mathbf{G}''' = \mathbf{G}\mathbf{H}$, and $\mathbf{G}'' = \mathbf{G}^w\mathbf{H}$, which are determined by the formulas (9) and the pair-wise permutability of the unknowns $\mathbf{G}$, $\mathbf{H}$, $\mathbf{G}'$, $\mathbf{H}'$, $\mathbf{H}''$, $\mathbf{G}''$, and $\mathbf{G}'''$: $\mathbf{G}\mathbf{H} = \mathbf{H}\mathbf{G}$, $\mathbf{G}\mathbf{G}' = \mathbf{G}'\mathbf{G}$, $\mathbf{G}\mathbf{H}' = \mathbf{H}'\mathbf{G}$, $\mathbf{G}\mathbf{H}'' = \mathbf{H}''\mathbf{G}$, and $\mathbf{G}\mathbf{G}'' = \mathbf{G}''\mathbf{G}$. Using

Table 3, the latter system reduces to a system of $\mu = 48$ quadratic equations (with $\delta = 44$ unknowns) in the field $GF(2^{257})$.

Security of the third developed signature scheme (algorithm with the value $\eta = 3$) is based on difficulty of solving the system of 13 vector quadratic equations with the unknowns $\mathbf{A}$, $\mathbf{B}$, $\mathbf{J}$, $\mathbf{I}$, $\mathbf{J}' = \mathbf{J}^x$, $\mathbf{I}' = \mathbf{I}^w$, which are determined by the formulas (15) and the pair-wise permutability of the following 11 unknowns $\mathbf{J}$, $\mathbf{I}$, $\mathbf{J}'$, and $\mathbf{H}'$: $\mathbf{JI} = \mathbf{IJ}$, $\mathbf{JI}' = \mathbf{I}'\mathbf{J}$, $\mathbf{JJ}' = \mathbf{J}'\mathbf{J}$. Using Table 1, the latter system reduces to a system of 52 quadratic equations (with 44 unknowns) in the field $GF(2^{199})$.

Thus, one can take the number of equations μ equal to the number of the unknowns δ, and use the recommended minimum values of μ presented in the Table 8 for different values of the order of the field $GF(n)$ in which the system of quadratic equation is given. Since the system of quadratic equations related to the proposed signature algorithms is set in the fields $GF(2^z)$, where $2^z \gg 256$, one can use the values μ that relates to the case $n = 256$. In this case, we get overstated requirements for the minimum value, however, this overestimation can be considered insignificant due to relatively weak dependence on the value n. For the second and third proposed signature algorithms we get the value $W > 2^{128}$.

Since the value μ is proportional to the FNAA dimension, one can propose an evident way to improve the value W that is using six-dimensional and eight-dimensional FNAAs (set over the fields $GF(2^z)$ with smaller values of z) as algebraic support of the proposed signature algorithms, however, this way is connected with the study of the decomposition of the said FNAAs into the set of commutative subalgebras or to provide another method for justifying existence of sufficiently large number of commutative groups of a certain type. Potentially, using the 8-dimensional FNAAs as algebraic support of the second and third proposed signature algorithms for each of latter one gets the values $\mu = 104$, $\delta = 88$ and $W > 2^{192}$.

In the developed signature scheme with $\eta = 4$ the vectors $\mathbf{G}'$, $\mathbf{H}'$, $\mathbf{H}''$, $\mathbf{G}''$, and $\mathbf{G}'''$ are computed as $\mathbf{G}' = \mathbf{G}^w$, $\mathbf{H}' = \mathbf{H}^x$, $\mathbf{H}'' = \mathbf{H}^w$, $\mathbf{G}'' = \mathbf{G}^w\mathbf{H}$, and $\mathbf{G}''' = \mathbf{GH}$, correspondingly. This technique improves the performance of the signature generation algorithm. Actually, when generating a signature, you can select at random the vectors $\mathbf{G}'$, $\mathbf{H}'$, $\mathbf{H}''$, $\mathbf{G}''$, and $\mathbf{G}'''$ from the hidden group and use an alternative signature generation algorithm with many additional exponentiation operations (the reader can easily compose such algorithm), while the signature verification algorithm retains its original form. The analogous remark is valid for the algorithm with $\eta = 4$ entries of the $\mathbf{S}$ signature element in the signature verification equation. The noted remark clearly shows that the exponentiation operations are used as a part of the mechanism for calculating the signature element $\mathbf{S}$ that satisfies the verification equation with its multiple occurrences (entries) in the latter.

Table 9 shows a rough comparison of the developed post-quantum signature algorithms with the algorithms selected as finalists of the NIST world competition on the development of the post-quantum public-key algorithms [22]. Table 10 (where W denotes security to direct attack, which is estimated using Table 8) shows a rough comparison of the introduced signature algorithms based on computational difficulty of solving a system of quadratic equations with some known multivariate signature algorithms. The post-quantum algorithms introduced in this article have a significant advantage in the sizes of the signature and

■ ***Table 8.*** Minimum number of equations providing a given security level to the direct attack for different values of the order of the field $GF(n)$ in the case $\mu = \delta$ [18]

n	W				
	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
16	30	39	51	80	110
31	28	36	48	75	103
256	26	33	43	68	93

■ ***Table 9.*** Comparison with some known digital signature algorithms

Signature scheme	Signature size, bytes	Public key size, bytes	Signature generation rate, arb. un.	Signature verification rate, arb. un.
Falcon [23]	1280	1793	50	25
CRYSTALS-Dilithium [24]	2701	1472	15	2
Rainbow [25] (3 different versions)	66… 204	> 150 000 … > 1 900 000	–	–
The first proposed (HDLP-based)	196	782	25	25
The second proposed ($\eta = 4$)	193	900	150	300
The third proposed ($\eta = 3$)	175	700	150	200

■ ***Table 10.*** Comparison with some known digital signature algorithms

Signature algorithm	Signature size, bytes	Public key size, bytes	# quadratic equations μ (unknowns δ)	Order of the field over which the quadratic equations are set	W
[5]	–	–	27 (27)	2^{16}	$\approx 2^{80}$
Rainbow [26]	33	16 065	27 (33)	2^{8}	$\approx 2^{80}$
QUARTZ [6]	16	72 704	100 (107)	2^{4}	$> 2^{192}$
Rainbow [25] (3 different versions)	66… 204	> 150 000 … > 1 900 000	64 (96)… 128 (204)	2^{4}, 31, 2^{8}	2^{128}… 2^{256}
With a hidden group [16] η = 2	160	512	28 (28)	$> 2^{256}$	$\approx 2^{80}$
The second proposed (η = 4)	193	900	52 (44)	2^{257}	$> 2^{128}$
The third proposed (η = 3)	175	700	52 (44)	2^{199}	$> 2^{128}$

public key. Besides, the developed algebraic algorithms based on computational difficulty of solving a system of quadratic equations have significantly higher performance than finalists Falcon [23] and CRYSTALS-Dilithium [24]. However, a detailed security estimation of the introduced signature algorithms are to be performed as an independent research work.

The signature schemes with a hidden group, which are based on computational difficulty of solving a system of many quadratic equations, suite well for using the 6-dimensional and 8-dimensional FNAAs as algebraic support. The latter allows to define the FNAAs over the fields $GF(2^z)$ with comparatively small values of z. For composing the BVMTs defining the FNAAs of such dimensions, you can use the unified methods by [27, 28]. Using the FNAAs with a large set of global single-sided units (see, for example, [29]) as algebraic support of the signature algorithms with a hidden group also represent an item of a future study.

It should be noted that in passing to using FNAAs with a higher dimension value m (in order to get a higher security to the direct attack) as an algebraic support, we have the possibility to define algebras over the fields $GF(2^z)$ with lower degrees of z (for example, $z = 101$ and $z = 128$; see Tables 6 and 7). For a fixed value m, a decrease in the value of z has little effect on the resistance to direct attacks, however, we assume that this will lead to a significant decrease in the resistance to potential structural attacks. For this reason, sufficiently large values of z are used in the developed signature algorithms on the four-dimensional FNAAs.

The results of this study complement the results of the papers [14, 16] and give grounds to consider signature algorithms with a hidden group as candidates for practical post-quantum cryptoschemes with small signature size. The latter is a motive for the cryptographic community to pay attention to the issue of considering structural attacks on signature algorithms of the type considered.

Conclusion

Within the framework of the methods [13, 16], new post-quantum algebraic signature algorithms with a hidden group has been developed, using 4-dimensional FNAAs, defined over finite fields of characteristic two, as algebraic support. It is shown that there are quite ample opportunities to choose suitable fields $GF(2^z)$ with different degrees of extension. The use of FNAAs, set over the fields $GF(2^z)$, as algebraic support of post-quantum signature algorithms with a hidden group is an essential moment for improving the performance and reducing the hardware implementation cost compared to the case of using FNAAs defined over the ground finite fields $GF(p)$.

An additional increase in performance can be achieved by using 6-dimensional and 8-dimensional FNAAs defined over the fields $GF(2^z)$ with the value of z from 80 to 150 as an algebraic support, including the case of defining FNAAs by sparse BVMTs. However, this is the subject of an independent study, which includes the study of the structure of such FNAAs and developing new forms of the signature verification equations.

References

1. 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.
2. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
3. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
4. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme. *Conf. on Applied Cryptography and Network Security — ACNS 2005*, Springer Lecture Notes in Computer Science, 2005, vol. 3531, pp. 164–175.
5. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.
6. Jintai D., Dieter S. *Multivariable Public Key Cryptosystems*. 2004. Available at: https://eprint.iacr.org/2004/350.pdf (accessed 09 March 2022).
7. Moldovyan D. N. A practical digital signature scheme based on the hidden logarithm problem. *Computer Science Journal of Moldova*, 2021, vol. 29, no. 2(86), pp. 206–226.
8. Moldovyan D. N. New form of the hidden logarithm problem and its algebraic support. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2020, no. 2 (93), pp. 3–10.
9. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*. Available at: https://eprint.iacr.org/2017/633.pdf (accessed 09 March 2022).
10. 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. doi:10.1007/s10623-016-0276-6
11. 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
12. Dahmen E., Okeya K., Takagi T., Vuillaume C. Digital signatures out of second-preimage resistant hash functions. *Proc. of the Second Intern. Workshop on Post-Quantum Cryptography, PQCrypto 2008*, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2008, vol. 5299, pp. 109–123. Available at: http://dblp.uni-trier.de/db/conf/pqcrypto/pqcrypto2008.html#DahmenOTV08 (accessed 09 March 2022).
13. 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
14. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A new concept for designing post-quantum digital signature algorithms on non-commutative algebras. *Voprosy kiberbezopasnosti*, 2022, no. 1(47), pp. 18–25 (In Russian). doi:10.21681/2311-3456-2022-1-18-25
15. 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
16. Moldovyan A. A., Moldovyan D. N., Moldovyan N. A. A novel method for developing post-quantum digital signature algorithms on non-commutative associative algebras. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 44–53. doi:10.31799/1684-8853-2022-1-44-53
17. Moldovyan A. A., Moldovyan N. A. Signature algorithms on finite non-commutative algebras over fields of characteristic two. *Voprosy kiberbezopasnosti*, 2022, no. 3(49), pp. 58–68 (In Russian). doi:10.21681/2311-3456-2022-3-58-68
18. Ding J., Petzoldt A. Current state of multivariate cryptography. *IEEE Security and Privacy Magazine*, 2017, vol. 15, no. 4, pp. 28–36.
19. Matsumoto T., Imai H. Public quadratic polynomial-tuples for efficient signature verification and message-encryption. *Proc. of Conf. Advances in Cryptology – Eurocrypt'88*, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1988, vol. 330, pp. 419–453. https://doi.org/10.1007/3-540-45961-8_39
20. Faugére J.-C. A new efficient algorithm for computing Gröbner basis (*F*4). *J. Pure Appl. Algebra*, 1999, vol. 139, no. 1–3, pp. 61–88.
21. Faugére J.-C. A new efficient algorithm for computing Gröbner basis without reduction to zero (*F*5). *Proc. of the Intern. Symp. on Symbolic and Algebraic Computation*, 2002, pp. 75–83. doi:10.1145/780506.780516
22. Moody D., Alagic G., Apon D., Cooper D., Dang Q., Kelsey J., Liu Y., Miller C., Peralta R., Perlner R., Robinson A., Smith-Tone D., and Alperin-Sheriff J. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR)*. National Institute of Standards and Technology, Gaithersburg, MD, 2020. https://doi.org/10.6028/NIST.IR.8309. Available at: https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf (accessed 09 March 2022).
23. *Fast-Fourier lattice-based compact signatures over NTRU*. Available at: https://falcon-sign.info/ (accessed 09 March 2022).
24. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*. Available at: https://eprint.iacr.org/2017/633.pdf https://pq-crystals.org/dilithium/index.shtml (accessed 09 March 2022).

25. *Rainbow Signature. One of three NIST Post-quantum Signature Finalists*. 2021. Available at: https://www.pqcrainbow.org/ (accessed 09 March 2022).
26. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme. *Proc. of Conf. on Applied Cryptography and Network Security — ACNS 2005*, Springer Lecture Notes in Computer Science, 2005, vol. 3531, pp. 164–175.
27. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties. *Quasigroups and Related Systems*, 2019, vol. 27, no. 2, pp. 293–308.
28. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions. *Quasigroups and Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.
29. Moldovyan D. N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. *Computer Science Journal of Moldova*, 2019, vol. 27, no. 1(79), pp. 56–72.

УДК 003.26
doi:10.31799/1684-8853-2023-1-29-40
EDN: KSCBTZ

Постквантовые алгебраические алгоритмы цифровой подписи со скрытой группой

А. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0001-5480-6016
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048, nmold@mail.ru
[a]Санкт-Петербургский Федеральный исследовательский центр РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка постквантовых стандартов на алгоритмы цифровой подписи является одним из современных вызовов для мирового криптографического сообщества. Недавно предложены два типа алгебраических схем подписи со скрытой группой, в которых конечные некоммутативные ассоциативные алгебры над полем $GF(p)$ используются в качестве алгебраического носителя. Построение алгоритмов этого типа на алгебрах, заданных над конечными полями характеристики два, представляет значительный интерес для повышения производительности и снижения схемотехнической сложности аппаратной реализации. **Цель:** разработать постквантовые алгоритмы цифровой подписи, в которых выполняются вычисления в конечных полях характеристики два. **Результаты:** предложены несколько четырехмерных конечных некоммутативных алгебр, заданных над полем $GF(2^z)$, в качестве алгебраических носителей схем цифровой подписи со скрытой группой. Разработаны рекомендации по выбору значения степени расширения z. В частных случаях значение z является степенью Мерсенна. По сравнению со схемами подписи, основанными на скрытой задаче дискретного логарифмирования, алгебраические алгоритмы подписи со скрытой группой, основанные на вычислительной сложности решения систем многих квадратных уравнений с многими неизвестными, рассматриваются как предпочтительные кандидаты на постквантовые криптосхемы. Предложены новые практичные алгоритмы подписи со скрытой группой. В двух алгоритмах подпись (e, $\mathbf{S}$) представляет собой целое число e и четырехмерный вектор $\mathbf{S}$. Верификация подписи выполняется по векторным уравнениям с тремя и четырьмя вхождениями элемента подписи $\mathbf{S}$. **Практическая значимость:** как и другие известные схемы подписи со скрытой группой, предложенные две схемы имеют достаточно малый размер подписи и открытого ключа. Благодаря сравнительно малой схемотехнической сложности аппаратной реализации и высокой производительности разработанные алгоритмы цифровой подписи представляют практический интерес и привлекательны как потенциальный прототип стандарта на постквантовые алгоритмы цифровой подписи.

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

Для цитирования: Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. *Информационно-управляющие системы*, 2023, no. 1, pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40, EDN: KSCBTZ
For citation: Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 1, pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40, EDN: KSCBTZ