Quasigroups and Related Systems **32** (2024), 95 – 108

https://doi.org/10.56415/qrs.v32.08

Complete signature randomization in an algebraic cryptoscheme with a hidden group

Alexandr A. Moldovyan

Abstract. The issue of the signature randomization in algebraic cryptoschemes with a hidden group, which are based on the computational difficulty of solving large systems of power equations, is considered. To ensure complete randomization of the signature, the technique of doubling the verification equation was used to specify the hidden group. A specific signature algorithm is proposed that uses 4-dimensional non-commutative associative algebra as an algebraic support. Known results on the study of the structure of this algebra were used in constructing the proposed algorithm and estimating its security. The question of implementing similar algorithms on finite non-commutative associative algebras of dimensions $m \geqslant 6$ is related to the open problem of studying their structure from the point of view of decomposition into a set of commutative subalgebras.

1. Introduction

Design of algebraic signature algorithms with a hidden group [11, 17] had been proposed as a way to solve the current problem of developing practical post-quantum signature algorithms [1]. One can distinguish two main types of the said signature schemes, which use finite non-commutative associative algebras as their algebraic carrier: 1) based on the computational difficulty of solving the hidden discrete logarithm problem [13, 16] and 2) based on the computational difficulty of solving lage systems of power equations with many unknowns [4, 9, 17].

The latter computationally difficult problem has been well tested as a post-quantum primitive of multivariate-cryptography algorithms developed

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, hidden group, post-quantum cryptography, public-key cryptoscheme, signature randomization
This work was financially supported by Russian Science Foundation (project No. 24-21-00225).

from 1988 [8] to the present [7, 10]. However, the known multivariate-cryptography algorithms have a significant drawback for practical application, which is the very large size of the public key.

The second type of the said algebraic signature algorithms is of special interest as an approach to developing signature schemes possessing small-size public key, which are based on the computational complexity of systems of many power equations with many unknowns. In fact, only the first step has been taken in this direction and it is necessary to study various aspects of the design of the second type algebraic algorithms with a hidden group. A common feature of the known algorithms of this type is specifying a digital signature that includes a certain vector S as its element. In this case, a vector-type verification equation is used with the repeated entry of the vector S as a multiplier. In the next section it is shown that the said feature is connected with a restricted randomization of the signature (in sens that only a small part of the elements of the algebra used as algebraic support can be potentially spesified as the vector S).

The latter creates the preconditions for potential attacks on algorithms of the type under consideration, therefore this article proposes the design of algebraic signature schemes with a hidden group, which ensures complete randomization of the signature (in sens that all reversible vectors can be potentially spesified as the vector S).

2. Preliminaries

Some m-dimensional vector A usually is denoted as $A = (a_0, a_1, \ldots, a_{m-1})$ or as $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1}$ are coodinates taking on the values in some finite field (for example, in $GF(p)$); $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors. In a finite m-dimensional vector space we have two standard operations: 1) addition of vectors and 2) scalar multiplication. Suppose the vector multiplication operation is additionally specified so that it is closed and distributive at the right and at the left relatively the addition operation. Then we get a finite m-dimensional algebra.

The most interesting cases of the development of the algebraic signature algorithms with a hidden group relates to the use of finite non-commutative associative algebras (FNAA) with global two-sided unit. The property of associativity is required due to using the exponentiation operations in the signature-algorithms design (when multiplication is associative one can very efficiently perform the exponentiation to a degree of large size).

The operation of multiplying two vectors A and B (coordinates of which, for example, are elements of the field $GF(p)$) can be defined by the formula

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

where every of the products $\mathbf{e}_i \mathbf{e}_j$ is to be substituted by a vector (usually single-component vector $\lambda \mathbf{e}_k$, where $\lambda \in GF(p)$) indicated in the cell at the intersection of the ith row and jth column of basis vector multiplication table (BVMT). Table 1 shows a specific example of BVMTs. To define associative multiplication the BVMT should be composed so that multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$ satisfies the following equality:

$$(\mathbf{e}_i \mathbf{e}_j)\, \mathbf{e}_k = \mathbf{e}_i\, (\mathbf{e}_j \mathbf{e}_k)\,.$$

The multiplication operation specified by Table 1 is associative, namely, we have a four-dimensional FNAA with the global two-sided unit $E = (0, 0, 1, 1)$, structure of which is well studied from the point view of decomposition into the set of commutative subalgebras [14]. Every of the latter has order p^2. The full number of the latter is $\eta = p^2 + p + 1$. Arbitrary two subalgebras intersect exactly in the set of scalar vectors $L = \lambda E$, where $\lambda \in GF(p)$. Exactly three types of commutative subalgebras of order p^2 exist [14]:

1) containing multiplicative group possessing two-dimensional cyclicity and having order $\Omega = (p-1)^2$;
2) containing cyclic multiplicative group of order $\Omega = p(p-1)$;
3) containing cyclic multiplicative group of order $\Omega = (p^2 - 1)$.

The number of commutative subalgebras of the first (η_1), second (η_2), and third (η_3) type is equal to [14]:

$$\eta_1 = \frac{p(p+1)}{2}; \quad \eta_2 = p + 1; \quad \eta_3 = \frac{p(p-1)}{2}. \tag{1}$$

In the paper [14] the formulas describing all elements of every type of the subalgebras are also derived, which provide possibility to express all elements of a subalgebra via coordinates of one given representtative (that is not a scalar vector) of the subalgebra.

The algebraic support of one of the algebraic signature schemes proposed in [17] represents a 4-dimensional FNAA (set over $GF(p)$ with $p = 2q + 1$, where q is a 128-bit prime) containing sufficiently large number of different

Table 1

The BVMT setting a sparse 4-dimensional FNAA over $GF(p)$; $\lambda \neq 0$ [14].

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

commutative groups having order q^2 and possessing two-dimensional cyclicity (a minimum generator system of such groups includes two vectors of the same order equal to q). In that signature scheme the public key represents the set of the vectors Y, Z, U, and W calculated as follows:

$$\begin{aligned} Y &= AGB, \quad & Z &= AG^{x_1}B; \\ U &= AHB, \quad & W &= AH^{x_2}A^{-1}, \end{aligned} \tag{2}$$

where $x_1 < q$ and $x_2 < q$ are random natural numbers; the vectors G and H compose a minimum generator system of the commutative hidden group; the vectors A and B satisfy the conditions $AB \neq BA$, $AG \neq GA$, and $BG \neq GB$. The values x_1, x_2, A, and B are elements of the private key connected with the public key. The signature (e_1, e_2, e_3, S) to an electronic document M is generated as follows [17]:

1. Using random natural numbers $k < q$ and $t < q$, calculate the vector

$$R = AG^kH^tA^{-1}. \tag{3}$$

2. Using a specified 384-bit hash function f_h, calculate the first signature element $e = e_1||e_2||e_3 = f_h(M, R)$ represented as concatenation of three 128-bit integers e_1, e_2, and e_3.

3. Calculate the integers n and u:

$$n = \frac{k - x_1e_2e_3 - e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q; \quad u = \frac{t - x_2e_2e_3 - e_1e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q.$$

4. Calculate the second signature element

$$S = B^{-1}G^nH^uA^{-1}. \tag{4}$$

The signature verification procedure includes the next steps:

1. Calculate the vector $R' = \left(YS\,(US)^{e_1}\,(ZSW)^{e_2}\right)^{e_3}$.

2. Concatenate the vector R' to the document M and compute the hash value $e' = f_h(M, R')$.

3. If $e' = e$ $(e' \neq e,)$, then the signature is genuine (false).

In the formulas (3) and (4) the integers k, t, n, and u are random, but the vectors G, H, A and B are fixed. Therefore, each of the vectors R and S takes only $q^2 = O(p^2)$, where $O(\cdot)$ is the order notation, different values in the FNAA containing p^4 different vectors. This shows that the signature randomization in the algorithm [17] is quite limitted. The latter creates potential preconditions for reducing security, which is assessed in [17] by the value of the computational difficulty of solving a system of quadratic equations connecting the elements of the public key with the elements of the secret key (see formulas (2)).

Indeed, one can show that a genuine signature $S_1 = B^{-1}G^{n_1}H^{u_1}A^{-1}$ defines four quadratic scalar equations with twelve fixed scalar uknowns (coordinates of the vectors B^{-1}, A^{-1}, and $G^{n_1}H^{u_1}$) and each additional genuine signature S_i $(i = 2, 3, \dots)$ adds four cubic scalar equations containing only two new scalar unknowns (due to limitted signature randomization). The latter describes an unknown vector $G^{n_i}H^{u_i}$ from the hidden group that is fixed by coordinates of the vector $G^{n_1}H^{u_1}$ (see formula (8) in [17], which describes all elements of commutative subalgebra containing multiplicative group with two-dimensional cyclicity). For example, five (six) different genuine signatures set a system of 20 (24) scalar equations (quadratic and cubic) with 20 (22) unknowns.

A similar consideration of the system of scalar power equations defined by the vector $R' = R$ (for genuine signatures) and by formula (3) leads to a smaller system of quadratic and cubic equations (note that formula (3) defines the equation $RA = AG^kH^t$). Namely, three (four) different genuine signatures set a system of 12 (16) scalar equations (quadratic and cubic) with 12 (14) unknowns, whereas formulas (2) with the additional equations $GG^{x_1} = G^{x_1}G$, $GH = HG$, and $GH^{x_2} = H^{x_2}G$ define a system of 28 power equations with 24 unknowns [17].

In the algebraic signature algorithm [4] based on difficulty of solving large systems of power equations, consideration of the systems of scalar equation composed for both the randomization vectors R and the genuine signatures S is similar to the above case.

Thus, the limitted randomization of the signature in the known algebraic algorithms based on computational difficulty of solving large systems of power equations leads to potential reduction of the security. Therefore, the

task of insuring the complete signature randomization is relevant.

3. Technique for complete randomization

Completeness of the signature randomization assumes the the signature element S can potentially take on arbitrary reversible value in the FNAA used as algebraic support. This can be provided with introducing a random reversible vector V as a multiplier in the formula for computation of the signature element S. However, this eliminates the possibility of using a verification equation with multiple entry of the signature element S. In order to get around this contradiction, you can use the technique of doubling the verification equation, which was previously used in the papers [12, 18] introducing specific signature algorithms with a hidden group, which are based on computational difficulty of the hidden discrete logarithm problem.

Namely, when using the FNAA specified by Table 1 over $GF(p)$, where $p = 2q+1$ with 192-bit prime q, we suppose the signature element S should satisfy the following two different verification equations in which the public key elements Y_1, T_1, Z_1, and U_1 in the first equation and Y_2, T_2, Z_2, and U_2 in the second equation are computed as masked elements of the hidden group $\Gamma_{<G,H>}$ set by the minumum generator system $<G, H>$:

$$\begin{cases} R'_1 = Y_1^{e_1\sigma_1} T_1 Z_1^{e_2\sigma_2} U_1 S Q_1^{h_1 h_2}; \\ R'_2 = Y_2^{e_1} T_2 Z_2^{e_2} U_2 S Q_2^{h}, \end{cases} \tag{5}$$

where Q_1 and Q_2 ($Q_1Q_2 \neq Q_2Q_1$) are two vectors of the order p^2-1, which represent common public parameters; $\sigma_1 < q$ and $\sigma_2 < q$ are auxiliary elements of the signature; $h = h_1||h_2 = f_h(M)$ is a 384-bit hash-function value represented as concatenation of two 192-bit integers h_1 and h_2.

The public key elements are computed as follows:

1. Generate a random pair of vectors $< G, H >$ of order q, which specify the minumum generator system of the hidden group of order q^2.

2. Generate at random natural numbers ($< q$) x_y, x_z, t_{11}, t_{12}, u_{11}, u_{12}, t_{21}, t_{22}, u_{21}, u_{22}.

3. Generate random vectors A, B, C, D, and F satisfying the inequalities $AB \neq BA$, $AG \neq GA$, $AC \neq CA$, $AD \neq DA$, $AF \neq FA$, $BG \neq GB$, $BC \neq CB$, $BD \neq DB$, $BF \neq FB$, $CG \neq GC$, $CD \neq DC$, $CF \neq FC$, $DG \neq GD$, $DF \neq FD$, and $FG \neq GF$.

4. Calculate the vectors $\{J_{t1}, J_{u1}, J_{t2}, J_{u2}\} \in \Gamma_{<G,H>}$: $J_{t1} = G^{t_{11}} H^{t_{12}}$, $J_{u1} = G^{u_{11}} H^{u_{12}}$, $J_{t2} = G^{t_{21}} H^{t_{22}}$, $J_{u2} = G^{u_{21}} H^{u_{22}}$.

5. Calculate the public key as the set of vectors $\{Y_1,Z_1,T_1,U_1,Y_2,Z_2,T_2,U_2\}$ (with total size equal to ≈768 bytes):

$$\begin{aligned} &Y_1 = AG^{x_y}A^{-1}; Z_1 = BH^{x_z}B^{-1}; T_1 = AJ_{t1}B^{-1}; U_1 = BJ_{u1}F^{-1}; \\ &Y_2 = CGC^{-1}; Z_2 = DHD^{-1}; T_2 = CJ_{t2}D^{-1}; U_2 = DJ_{u2}F^{-1}. \end{aligned} \tag{6}$$

The private key corresponding to the public key is the next set of elements $\{x_y, x_u, G, H, J_{t1}, J_{u1}, J_{t2}, J_{u2}, A, B, C, D, F$ with total size equal to ≈1104 bytes.

If we specify computation of the pair of randomization vectors $R_1 = AG^{k_1}H^{r_1}J_{t1}J_{u1}VQ_1^{h_1h_2}$ and $R_2 = CG^{k_2}H^{r_2}J_{t2}J_{u2}VQ_2^{h}$ (where k_1, r_1, k_2, and r_2 are random natural numbers; h is the 384-bit hash value $h = h_1||h_2 = f_h(M)$ computed from the document M to be signed), then with the pair of verification equations (5) and with public key elements (6) the required signature element S is to be calculated as

$$S = FG^nH^uV, \tag{7}$$

where V is a random reversible vector and the integers n and u are precomputed, depending on the signature randomization elements e_1 and e_2, such that $e_1||e_2 = f_h(M, R_1, R_2)$, and on random integers k_1, r_1, k_2, and r_2.

Thus, the signature element S is computed depending on a random multiplier V, thefore complete signature randomization is provided.

4. The proposed signature scheme

The used algebraic support, the common public parameters Q_1, Q_2, the private key, and the public key have been presented in Section 3. The signature generation algorithm is described as follows:

1. Generate at random natural numbers k_1, r_1, k_2, and r_2 ($< q$) and calculate the 384-bit hash-function value $h = h_1||h_2 = f_h(M)$ (where M is a signed document; h_1 and h_2 are 192-bit integers) and the vectors R_1 and R_2:

$$\begin{aligned} &R_1 = AG^{k_1}H^{r_1}J_{t1}J_{u1}VQ_1^{h_1h_2}; \\ &R_2 = CG^{k_2}H^{r_2}J_{t2}J_{u2}VQ_2^{h}. \end{aligned} \tag{8}$$

2. Compute the hash-function value $e = e_1||e_2$ (the first signature element), where $||$ denotes the concatenation operation, from the document M to which the vectors R_1 and R_2 are concatenated: $e = e_1||e_2 = f_h(M, R_1, R_2)$, where e_1 and e_2 are 192-bit integers.

3. Calculate the integers n, u, σ_1, and σ_2:

$$n = k_2 - e_1 \bmod q; \quad u = r_2 - e_2 \bmod q;$$
$$\sigma_1 = \frac{k_1 - k_2 + e_1}{x_y e_1} \bmod q; \quad \sigma_2 = \frac{r_1 - r_2 + e_2}{x_z e_2} \bmod q.$$

4. Calculate the second signature element S:

$$S = FG^n H^u V.$$

The signature is $e_1, e_2, \sigma_1, \sigma_2, S$ and has total size equal to ≈192 bytes. Computational complexity w of the signature generation alorithm is roughly equal to six exponentiations in the FNAA set by Table 1, i. e., to $w \approx 13,824$ multiplications modulo a 193-bit prime p.

The verification of the signature $e_1, e_2, \sigma_1, \sigma_2, S$ to the document M is performed with the following algorithm:

1. Calculate the hash-function value $h = h_1||h_2 = f_h(M)$ from the document M. Then calculate the vectors R'_1 and R'_2 by formulas (5).

2. Compute the hash-function value e' from the document M to which the vectors R'_1 and R'_2 are concatenated: $e' = f(M, R'_1, R'_2)$.

3. If $e' = e_1||e_2$, then the signature is genuine, else the signature is false.

The computational complexity w' of the signature verification algorithm is roughly equal to four exponentiations in the 4-dimensional FNAA used as algebraic support, i. e., $w' \approx 9,216$ multiplications modulo a 193-bit prime p.

Correctness proof of the signature scheme.
Taking into account that the vectors $G, H, J_{t1}, J_{u1}, J_{t2}, J_{u2}$ are elements of the commutative group $\Gamma_{<G,H>}$ and have order q, one can show that the correctly computed signature $e_1, e_2, \sigma_1, \sigma_2, S$ passes the verification procedure as genuine one:

$$\begin{aligned}
R'_1 &= Y_1^{e_1\sigma_1} T_1 Z_1^{e_2\sigma_2} U_1 S Q_1^{h_1 h_2} \\
&= \left(AG^{x_y} A^{-1}\right)^{e_1\sigma_1} A J_{t1} B^{-1} \left(BH^{x_z} B^{-1}\right)^{e_2\sigma_2} B J_{u1} F^{-1} \left(FG^n H^u V\right) Q_1^{h_1 h_2} \\
&= AG^{x_y e_1 \sigma_1} J_{t1} H^{x_z e_2 \sigma_2} J_{u1} G^n H^u V Q_1^{h_1 h_2} \\
&= AG^{x_y e_1 \frac{k_1 - k_2 + e_1}{x_y e_1}} J_{t1} H^{x_z e_2 \frac{r_1 - r_2 + e_2}{x_z e_2}} J_{u1} G^{k_2 - e_1} H^{r_2 - e_2} V Q_1^{h_1 h_2} \\
&= AG^{k_1 - k_2 + e_1} H^{r_1 - r_2 + e_2} G^{k_2 - e_1} H^{r_2 - e_2} J_{t1} J_{u1} V Q_1^{h_1 h_2} \\
&= AG^{k_1} H^{r_1} J_{t1} J_{u1} V Q_1^{h_1 h_2} = R_1;
\end{aligned}$$

$$R'_2 = Y_2^{e_1} T_2 Z_2^{e_2} U_2 S Q_2^{h}$$

$$= \left(CGC^{-1}\right)^{e_1} CJ_{t2}D^{-1} \left(DHD^{-1}\right)^{e_2} DJ_{u2}F^{-1} \left(FG^nH^uV\right) Q_1^{h_1h_2}$$
$$= CG^{e_1}J_{t2}H^{e_2}J_{u2}G^{k_2-e_1}H^{r_2-e_2}VQ_2^h = R_2;$$

$$\{R_1' = R_1;\ R_2' = R_2\} \ \Rightarrow\ f_h(M, R_1', R_2') = f_h(M, R_1, R_2) \ \Rightarrow\ e' = e_1||e_2.$$

5. Disscussion

The completeness of signature randomization in the algorithm described in Section 4 is connected with the fact that calculating a value of genuine signature involves multiplying by a random vector V, therefore, for arbitrary fixed set of values of the vectors F, G^n, and H^u (see formula (7)) the value of the signature can take any reversible value in the FNAA used as an algebraic support. However, for a certain number of genuine signatures it is possible to calculate the unknown value F (the unknown vectors G^n and H^u are not element of the private key).

The latter can be done by constructing a systems of vector equations set by formulas (7) and (8) for different signatures S connected with different pairs of the vectors R_1 and R_2. For example, one signature S defines the following three quadratic vector equations

$$\begin{aligned} SV^{-1} &= F\left(G^nH^u\right) \\ R_1V^{-1}Q_1^{-h_1h_2} &= A\left(G^{k_1}H^{r_1}J_{t1}J_{u1}\right); \\ R_2V^{-1}Q_2^{-h} &= C\left(G^{k_2}H^{r_2}J_{t2}J_{u2}\right), \end{aligned} \tag{9}$$

where the vectors R_1, R_2, $Q_1^{h_1h_2}$, and Q_2^h are calculated in framework of the signature verification procedure.

In the system of equations (9) each of the products G^nH^u, $G^{k_1}H^{r_1}J_{t1}J_{u1}$, and $G^{k_2}H^{r_2}J_{t2}J_{u2}$ sets a random selection of an element from a hidden group $\Gamma_{<G,H>}$. The latter is fixed, if we fix the unknown $G = (g_0,\ g_1,\ g_2,\ g_3)$. All elements $X = (x_0,\ x_1,\ x_2,\ x_3)$ of the commutative subalgebra that contains the group $\Gamma_{<G,H>}$ are described by the following formula including fixed coordinates (g_0, g_1, g_2, g_3) and two scalar variables $i, j \in \{0, 1, ..., p-1\}$ (see formula (8) in [14]):

$$X = (x_0, x_1, x_2, x_3) = \left(i,\ \frac{g_1}{g_0}i,\ j, j + \frac{g_3 - g_2}{g_0}i\right). \tag{10}$$

Therefore, a random selection from the hidden group can be described with the scalar unknowns i and j. Using formula (10) we can reduce the number

of scalar unknowns, but the respective scalar equations become cubic (however, the computational complexity of solving a system of quadratic and of cubic equation is of the same order for the same number of equations [3]). Taking into account these remarks, we have four fixed vector unknowns A, C, F, and G (setting 16 scalar unknowns that are coodinates of the said vectors), a unique vector unknown V^{-1} for a triple of equations related to the same signature, and unique pair of scalar unknowns i and j in each vector equation of the considered system. If we have b different genuine signatures, then we can compose a system of $3b$ different vector equations and represent it as a system of $12b$ cubic scalar equations with d unknowns, where

$$d = 16 + 4b + 2{\cdot}3b = 16 + 10b.$$

From the condition $d = 12b$ we can fined the number of signatures $b = 8$, when the nuber of scalar unknowns is equal to the number of scalar equations and the system includes 96 power (quadratic and cubic) scalar equations.

A system of quadratic vector equations composed using formulas (6) describing connection of the public-key elements with the private-key elements is as follows:

$$\begin{cases} Y_1A = AG^{x_y}; \quad Z_1B = BH^{x_z}; \quad T_1B = AJ_{t1}; \quad U_1F = BJ_{u1}; \\ Y_2C = CG; \quad Z_2D = DH; \quad T_2D = CJ_{t2}; \quad U_2F = DJ_{u2}; \\ GH = HG; \quad GJ_{t2} = J_{t2}G; \quad GJ_{u2} = J_{u2}G; \\ GG^{x_y} = G^{x_y}G; \quad GH^{x_z} = H^{x_z}G; \quad GJ_{t1} = J_{t1}G; \quad GJ_{u1} = J_{u1}G, \end{cases} \tag{11}$$

where the last seven equations reflect the fact that the unknown vectors G, G^{x_y}, H, H^{x_z}, J_{t1}, J_{u1}, J_{t2}, and J_{u2} are selected from the hidden group $\Gamma_{<G,H>}$. When representing this system of vector equation as a system of scalar equations, the last seven equations in (11) can be reduced with using formula (10) and considering the unknown vector $G = (g_0,\ g_1,\ g_2,\ g_3)$ as element fixing the group $\Gamma_{<G,H>}$ (coordinates of arbitrary vector included in the hidden group can be described via coordinates of G and a unique pair of scalar unknowns i and j). For example, using Table 1, the first vector equation in (11), namely, $Y_1A = AG^{x_y}$ (where $Y_1 = (y_0, y_1, y_2, y_3)$ and

$A = (a_0, a_1, a_2, a_3))$ is represented by the following four scalar equations:

$$\begin{cases} y_0 a_2 + y_3 a_0 = a_0 j + a_3 i; \\ y_2 a_1 g_0 + y_1 a_3 g_0 = a_2 g_1 i + a_1 g_0 j + a_1 g_3 - a_1 g_2; \\ \lambda y_1 a_0 + y_2 a_2 = \lambda a_1 i + a_2 j; \\ \lambda y_0 a_1 g_0 + y_3 a_3 g_0 = \lambda a_0 g_1 i + a_3 g_0 j + a_3 g_3 - a_3 g_2, \end{cases}$$

Each of the other vector equations in (11) is transformed into a similar four scalar equations.

In this way we get a system of 32 quadratic and cubic scalar equations with 40 scalar unknowns. The latter suggests that there are numerous solutions defining many equivalent keys. However, their calculation involves solving a system of 32 cubic equations. The complexity of solving a system of power equations depends exponentially on the number of equation (and weakly depends on the degree of equations [3]) and determines the security of the algorithm under consideration to a direct attack.

A system of power equations composed for a set of known genuine signatures includes significantly larger number of equations than the system composed from formulas describing connection of public-key elements with the private-key elements, therefore one can conclude that using the known signatures can not be used to reduce the security level of the introduced signature algorithm, i. e. the proposed signature randomization technique is efficient.

The best-known methods for solving a large system of power equations use the algorithms F4 [5] and F5 [6]. Taken into account the latter algorithms, the paper [2] presents the minimum number of power equations in different fields $GF(q')$ that is requiered to get the security level (ψ) 2^{80}, 2^{100}, $2^{128,}$ 2^{192}, and 2^{256} for the case when the number of equations is approximately equal to the number of unknowns (see Table 2). Using that results, security of the introduced signature algorithm to direct attack can be estimeted as $\approx 2^{100}$. To improve the security level one can try to implement the algorithm from Section 4 on FNAAs having dimensions $m \geq 6$. Suitable non-commutative algebras are described, for example, in [15]. However, the decomposition of that FNAAs into the set of commutative subalgebras (results of which are useful for both the design and the security evaluation) has not been studied yet, therefore, for such versions of the algorithm it is not entirely clear how one can minimize the number of equations in the system of scalar equations, to which the system of vector equations (11) is reduced.

Table 2

The minimum number of equations in $GF(q')$ by [2].

$\psi = \ldots$	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
$q' = 16$	30	39	51	80	110
$q' = 31$	28	36	49	75	103
$q' = 256$	26	33	43	68	93

Leaving the said implementations for future research, we note that at the moment, the assessment of the security level of the proposed algorithm is quite rough and applies only to direct attacks related to solving a system of quadratic vector equations (11) connecting elements of public and private keys. Obviously, further analysis of resistance to attacks of various types is required. At the moment we only claim that the randomization technique used ensures sufficient completeness of the signature randomization.

In the first and second verification equations (5) the most right multipliers $Q_1^{h_1h_2}$ and Q_2^h are used to insure security to the following algorithm for forging a signature. Suppose a genuine signature $e_1, e_2, \sigma_1, \sigma_2, S$ is available and an attacker is intended to forge a signature $e_1'', e_2'', \sigma_1'', \sigma_2'', S''$ to the document M''. From equations (5) he can calculate the vectors $R_1'' = R_1'$ and $R_2'' = R_2'$, the values $e'' = e_1''||e_2'' = f_h(M'', R_1'', R_2'')$ and $h'' = h_1''||h_2'' = f_h(M'')$, where e_1'', e_2'', h_1'', and h_2'' are 192-bit integers.

Since $R_1'' = R_1'$, from the first of equations (5) one gets the value $S'' = S_1''$:

$$Y_1^{e_1\sigma_1}T_1Z_1^{e_2\sigma_2}U_1SQ_1^{h_1h_2} = Y_1^{e_1''\sigma_1''}T_1Z_1^{e_2''\sigma_2''}U_1S_1''Q_1^{h_1''h_2''} \Rightarrow$$
$$\Rightarrow S_1'' = FG^{x_y(e_1\sigma_1 - e_1''\sigma_1'')}H^{x_z(e_2\sigma_2 - e_2''\sigma_2'')}F^{-1}SQ_1^{h_1h_2 - h''_1h_2''},$$

Since $R_2'' = R_2'$, from the second of equations (5) one gets the value $S'' = S_2''$:

$$Y_2^{e_1\sigma_1}T_2Z_2^{e_2\sigma_2}U_2SQ_2^h = Y_2^{e_1''\sigma_1''}T_2Z_2^{e_2''\sigma_2''}U_2S_2''Q_2^{h''} \Rightarrow$$
$$\Rightarrow S_2'' = FG^{e_1\sigma_1 - e_1''\sigma_1''}H^{e_2\sigma_2 - e_2''\sigma_2''}F^{-1}SQ_2^{h-h''}.$$

Then the attacker calculates the signature elements $\sigma_1'' = \sigma_1 e_1 e_1''^{-1}$ and $\sigma_2'' = \sigma_2 e_2 e_2''^{-1}$ for which he has $S_1''Q_1^{h_1''h_2'' - h_1h_2} = S_2''Q_2^{h''-h}$.

Thus, due to using the multiplications by $Q_1^{h_1h_2}$ and Q_2^h (such that $Q_1Q_2 \neq Q_2Q_1$) in the first and second verification equations, correspondingly, the probability of the equality $S_1'' = S_2'' = S''$ that take place, if $h'' = h$ (i. e., probability of successful signature forgery) is negligible ($\approx 2^{-384}$ for the used 384-bit hash function).

6. Conclusion

The proposed technique for complete signature randomization can be implemented in algebraic signature algorithms with a hidden group and doubled verification equation. The structure of the algebra used as an algebraic carrier, from the point of view of decomposition into a set of commutative subalgebras, is essential for the development of signature schemes and assessment of their security. To develop new versions of the proposed algorithm on FNAAs of dimension $m \geq 6$, it is of interest to study the structure of the latter.

Acknowledgement. The author sincerely thanks the anonymous Referee for his comments on improving the content of the article.

References

[1] **G. Alagic, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, D. Apon**, *Status report on the third round of the NIST post-quantum cryptography standardization process* (2022) NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8413, (Accessed December 23, 2023)

[2] **J. Ding, A. Petzoldt**, *Current state of multivariate cryptography*, IEEE Security and Privacy Magazine, **15** (2017), no. 4, 28 – 36.

[3] **J. Ding, A. Petzoldt, D.S. Schmidt**, *Solving polynomial systems*, In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. **80** (2020), 185 – 248.

[4] **M.T. Duong, D.N. Moldovyan, B.V. Do, M.H. Nguyen**, *post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations*, Computer Standards and Interfaces, **86** (2023), 103740.

[5] **J.-C. Faugére**, *A new efficient algorithm for computing Gröbner basis* ($F4$), J. Pure Appl. Algebra, **139** (1999), no. 1-3, 61 – 88.

[6] **J.-C. Faugére**, *A new efficient algorithm for computing Gröbner basis without reduction to zero* ($F5$). In: Proceedings of the International Symposium on Symbolic and Algebraic Computation (2002), 75 – 83.

[7] **Y. Ikematsu, S. Nakamura, T. Takagi**, *Recent progress in the security evaluation of multivariate publickey cryptography*, IET Information Security, (2022), 1 – 17.

[8] **T. Matsumoto, H. Imai**, *Public quadratic polynomial-tuples for efficient signature verification and message-encryption*, Advances in Cryptology (Eurocrypt'88), Springer Berlin Heidelberg, (1988), 419 – 453.

[9] **A.A. Moldovyan, D.N. Moldovyan**, *A new method for developing signature algorithms*, Bul. Acad. Sci. Moldova, Mathematics, (2022), no. 1(98), 56 – 65.

[10] **A.A. Moldovyan, N.A. Moldovyan**, *Vector finite fields of characteristic two as algebraic support of multivariate cryptography*, Computer Sci. J. Moldova, **32** (2024), no. 1(94), 46 – 60.

[11] **D.N. Moldovyan**, *A practical digital signature scheme based on the hidden logarithm problem*, Computer Sci. J. Moldova, **29** (2021), no. 2(86), 206 – 226.

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

[13] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *A new design of the signature schemes based on the hidden discrete logarithm problem*, Quasigroups and Related Systems, **29** (2021), no. 1, 97 – 106.

[14] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *Structure of a finite non-commutative algebra set by a sparse multiplication table*, Quasigroups and Related Systems, **30** (2022), no. 1, 133 – 140.

[15] **N.A. Moldovyan**, *Unifed method for defining fnite associative algebras of arbitrary even dimensions*, Quasigroups and Related Systems, **26** (2018), no. 2, 263 – 270.

[16] **N.A. Moldovyan**, *Signature schemes on algebras, satisfying enhanced criterion of post-quantum security*, Bull. Acad. Sci. Moldova, Mathematics, (2020), no. 2(93), 62 – 67.

[17] **N.A. Moldovyan**, *Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations*, Quasigroups and Related Systems, **30** (2022), no. 2, 287 – 298.

[18] **N.A. Moldovyan, A.A. Moldovyan**, *Candidate for practical post-quantum signature scheme*, Vestnik Saint Petersburg Univ., Applied Math., Computer Sci., Control Processes, **16** (2020), no. 4, 455 – 464.

Received January 8, 2024

St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
e-mail: maa1305@yandex.ru