Quasigroups and Related Systems **33** (2025), 71 – 83

https://doi.org/10.56415/qrs.v33.06

A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras

Alexandr A. Moldovyan and *Nikolay A. Moldovyan*

Abstract. The paradigm of algebraic signature schemes security of which is based on the computational difficulty of solving large systems of power equations is attractive for developing practical post-quantum signature algorithms. A significant drawback of the known algorithms of the mentioned type is the limited signature randomization, which creates preconditions for a decrease in security. A method for enhancing signature randomization is proposed and used for developing a digital signature algorithm that is free of the said drawback. The method is based on the use of three hidden commutative groups, such that in the general case the elements of one of them are non-commutative with the elements of the other two groups.

1. Introduction

The computational difficulty of solving large systems of power equations underlies the paradigm of developing post-quantum public-key cryptographic algorithms on nonlinear mappings with a secret trapdoor [2, 15]. Within this paradigm (known as multivariate public-key cryptography (MPKC)), post-quantum digital signature algorithms with a small signature size have been developed. However, they use an extremely large public key [4, 14], which makes them quite impractical. Even a recently proposed method [13, 8] for 10 to 100 times reducing the size of the public key does not completely eliminate this drawback. In general, in algorithms on hard-to-reverse mappings the public-key size is significantly larger than in other types of post-quantum algorithms.

2010 Mathematics Subject Classification: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50

Keywords: finite non-commutative algebra, associative algebra, computationally difficult problem, system of power equations, hidden commutative group, digital signature, signature randomization, post-quantum cryptography.

This work was finantially supported by Russian Science Foudation (project No. 24-41-04006).

A recently proposed new concept for developing algebraic digital signature algorithms based on the difficulty of solving large systems of power equations allows for relatively small sizes of the public key and signature [3, 6, 10]. Finite non-commutative associative algebras (FNAAs) of the dimensions $m \geqslant 4$ are used as algebraic support in those algorithms, the signature having the form (e, S), where e is a natural number representing a randomization parameter and S is an m-dimensional vector playing the role of a fitting parameter that has unique value computed depending on the value of e. A distinctive feature of algorithms [6, 10, 3] (that can be attributed to algebraic MPKC algorithms) is the use of a verification equation with multiple entry of the vector S as a multiplier.

The mentioned concept is of interest for the development of practical post-quantum digital signature algorithms, however, as shown in paper [5], the signature randomization mechanism used in the algorithms [6, 10] creates prerequisites for a significant decrease in security level compared to the expected one. Paper [5] proposed a method for enhancing randomization, but this method requires the use of a doubled verification equation, which leads to an increase in the size of the public key and a decrease in the performance of the digital signature generation and verification procedures. Thus, the task of developing a mechanism for enhancing randomization that does not require doubling the verification equation seems relevant.

This paper introduces a new mechanism for enhancing signature randomization in algebraic algorithms based on the computational difficulty of solving systems of many power equations with many unknowns. A new post-quantum digital signature algorithm implementing the proposed method is also presented.

2. Preliminaries

In an m-dimensional vector space over a finite field $GF(p^z)$, where p is a prime and the integer $z \geqslant 1$, we have two operations, addition and scalar multiplication. Defining additionally a vector multiplication operation which is closed and distributive at the left and at the right relatively addition operation, one gets an m-dimensional algebra. The multiplication of two vectors $A = (a_0, a_1, \ldots a_{m-1}) = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots, a_{m-1}\mathbf{e}_{m-1}$ and $B = (b_0, b_1, \ldots b_{m-1}) = b_0\mathbf{e}_0 + b_1\mathbf{e}_2 + \ldots, b_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{m-1}$ are basis vectors, posessing the said properties can be specified by the next formula:

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

where every product $\mathbf{e}_i\mathbf{e}_j$ is to be replaced by a one-component vector $\mu\mathbf{e}_k$ indicated in the cell at the intersection of the ith row and jth column of so called basis vector multilication table (BVMT).

In the algebraic MPKC signature algorithms the exponentiation operations to a large-size degree are used, therefore, the finite non-commutative associative algebras (FNAAs) with global two-sided unit E are used as algebraic support. For the case of associative multiplication and unknown form of the E unit one can very efficiently perform the exponentiation operation, for example, using the fast exponentiation algorithm described in [7], which is free from the use of an explicit unit vector. For the development of the algebraic MPKC signature algorithms and evaluating their security the information about structure of the FNAAs (from the point view of their decomposition into a set of commutative subalgebras) is very significant. A sufficiently complete picture of the structure of FNAAs is currently known only for the case $m = 4$ and $z = 1$. Therefore, in this article we consider the case of using four-dimensional FNAAs set over $GF(p)$ (where prime $p = 2q + 1$ with prime q) as an algebraic support, although it is of interest to use higher-dimensional algebras ($m \geqslant 6$) to increase the security of the developed post-quantum signature algorithm.

A number of studied four-dimensional FNAAs [9] (including the FNAA set by Table 1) have a typical structure that can be described as follows:

1. There are only three types of the commutative subalgebras of order p^2:

i) $\eta_1 = \frac{p(p-1)}{2}$ different subalgebras of the first type characterized in that their multiplicative group is cyclic and has order $\Omega_1 = (p^2 - 1)$;

ii) $\eta_2 = \frac{p(p+1)}{2}$ different subalgebras of the second type characterized in that their multiplicative group is generated by a minimum generator system containing two vectors of order $p - 1$, the order of the group being $\Omega_2 = (p - 1)^2$;

iii) $\eta_3 = p + 1$ different subalgebras of the third type characterized in that their multiplicative group is cyclic and has order $\Omega_3 = p(p - 1)$.

2. Arbitrary two subalgebras intersect exactly in the set of scalar vectors $L = \lambda E$, where $\lambda \in GF(p)$.

3. A given non-scalar vector A contained in some subalgebra Ψ (the vector A is called a representative of Ψ) defines all vectors contained in

Ψ. Namely, the coordinates of every of the lasts are determined by four coordinates of the representatve A and unique pair of integer values $i, j \in \{0, 1, \ldots p-1\}$.

The four-dimensional FNAA [9] set by Table 1 contains the global two-sided unit $E = (0, 0, 1, 1)$ and all vectors contained in a subalgebra of the first type or of the second type are described via coordinates of its representative $A = (a_0, a_1, a_2, a_3)$ by the following formula [9]:

$$X = (x_0, x_1, x_2, x_3) = \left(i, \ \frac{a_1}{a_0} i, \ j, j + \frac{a_3 - a_2}{a_0} i \right). \tag{1}$$

Formula (1) is taken into account when estimating security of the developed post-quantum signature algorithm.

Table 1

A sparse BVMT ($\lambda \neq 0$) defining a four-dimensional FNAA [9].

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

3. Technique for inhancing the signature randomization

The algebraic MPKC signature algorithms [10, 3] belong to the type of randomized cryptalgorithms and the randomization mechanism used is important to ensure a sufficient level of security. The signature calculation procedure begins with generating a random vector R (called fixator), for example, by the formula

$$R = AG^k H^t B, \tag{2}$$

where k and t are random natural numbers ($k, t < p - 1$); A, B, G, and H are secret vectors, the pair $<G, H>$ being a minimum generator system of the multiplicative group of a C2-subalgebra (subalgebra of the second type). The fixator R is attached to the document M to be signed and the randomization signature element e is calculated as the hash value $e =$

$\Phi(\mathrm{M}, R)$, where Φ is a collision resistant hash function. The fitting signature element S, satisfying the verification equation with multiple entry of the vector S as a factor, is computed by the following formula

$$S = CG^nH^dD, \tag{3}$$

where n and d are random natural numbers $(n, d < p - 1)$ pre-calculated depending on the value of e; vectors C and D are elements of the secret key. Formulas (2) and (3) describes the signature randomization mechanism used in [6, 10].

During the signature verification process, the value of the fixator vector R is calculated, therefore, every valid signature defines a pair of vector equations specified by formulas (2) and (3), in which the unknowns A, B, C, and D are fixed for all known signatures and the unknown vectors G^kH^t and G^nH^d are unique unknowns. Since the last two vectors are contained in the hidden commutative group of the order $\approx p^2$, for some number α of known signatures it becomes potentially possible to find the secret key elements A, B, C, and D. Indeed, consider a representative X of the hidden group as the fifth unknown. Then the system of power vector equations can be reduced to a system of power scalar equations in which you have 8α scalar equations with 20 fixed scalar unknowns (coordinates of the fixed vector unknowns A, B, C, D and X) and 4α unique scalar unknowns (two pairs of scalar values i and j that decribe by formula (1) the unknown vectors G^kH^t and G^nH^d).

It is easy to see that the specified system of vector equations is divided into two independent systems, including i) equations defined by formula (1), and ii) equations defined by formula (2). For example, for the first case we have α vector equations with 3α fixed vector unknowns and α unique vector unknowns. When reduced to a system of scalar equations, we obtain 4α scalar equations and 3α fixed scalar unknowns (coordinates of the vectors A, B, and X) and $2(\alpha - 1)$ unique unknowns (minus 1 takes into account the fact that the unknown vector G^kH^t in the first signature is considered as a representative X of the hidden group).

For the first case, to perform an attack based on known signatures, the required value of α can be estimated from the condition of equality of the number of equations (4α) and the number of unknowns ($12+2(\alpha-1)$) in the solved system of power scalar equations. In accordance with this condition, we obtain the equation $4\alpha = 10 + 2\alpha$ from which we have the value $\alpha = 5$ and a system of 20 power scalar equations, which should be solved to find the secret vectors A and B. Computational complexity of such attack is rather low, therefore, one should conclude that the signature randomization in algorithms [6, 10] is not satisfactory.

Consider the case of using the four-dimensional FNAA set over $GF(p)$, where $p = 2q + 1$ with 128-bit prime q. To enhance the signature randomization, the following formula can be proposed for calculating the fixator vector R:

$$R = AP^u G^k Q^t B, \tag{4}$$

where u, k, and t are random natural numbers ($u, t < p^2 - 1$ and $k < q$); P and Q are non-scalar vectors of the order $p^2 - 1$, such that $PQ \neq QP$; G is a non-scalar vector of the order q (such vectors are contained in the multiplicative group of the C2-subalgebras that have order $4q^2$). The corresponding formula for calculating the fitting signature element is as follows:

$$S = CP^b G^n Q^d D, \tag{5}$$

where b, n, and d are random natural numbers ($b, d < p^2 - 1$ and $n < q$) which are calculated depending on the fixator vector R and electronic document M to be signed.

In a known signature attack, each known signature specifies by formula (4) a vector equation with a unique vector unknown $P^u G^k Q^t$ and also specifies by formula (5) a vector equation with a unique vector unknown $P^b G^n Q^d$. These unique unknowns take on values within the entire FNAA used as an algebraic support of the digital signature algorithm. When reducing a system of vector equations to a system of scalar equations, each unique vector unknown specifies four unique scalar unknowns. Given the presence of fixed unknowns, it is easy to see that in the systems of scalar equations formed during a known signature attack, the number of unknowns will exceed the number of equations. Therefore, the system will have multiple solutions for arbitrary value of α. For the system including equations set by formula (4) or (5), you can estimate roughly the number of solutions as $\approx p^{4g}$, where g is the number of fixed vector unknowns.

The share of solutions associated with elements of the secret key and elements of potentially possible equivalent keys is presumably negligibly small for the case $p > 2^{100}$. The latter gives grounds for the assumption that the level of signature randomization specified by formulas (4) and (5) is sufficient. The following section presents a digital signature algorithm that implements this method of signature randomization and uses the signature verification equation with two entries of the fitting signature element S.

4. A candidate for a practical post-quantum signature algorithm

Formation of the public key begins with generation of the secret vectors P, Q, and G. The first two are generators of two different multiplicative groups of the subalgebras of the first type. Since the portion of the lasts is $\approx 50\%$, the vectors P and Q can be selected at random untill each of them has order $p^2 - 1$ and the inequality $PQ \neq QP$ holds true. The vectors of the order q are contained in the C2-subalgebras the portion of which is $\approx$50%. Besides, the portion of the vectors of order q in some fixed multiplicative group of the C2-subalgebras is $\approx$50% (note that the multiplicative group of a C2-subalgebra contains vectors of orders 2, q, and $2q$), therefore the vector G can be selected at random (from the set of invertible non-scalar vectors) with checking its order.

Suppose we have generated the secret vectors P, Q, and G. The rest of the secret key represents the random vectors A, B, C, D, F that are pairwise non-commutative (and non-commutative with the vectors P, Q, and G) and three natural numbers $w < p^2 - 1$, $x < p^2 - 1$, and $v < q$. The total size of the secret key equals to 592 bytes. The 576-byte public key includes nine vectors Y, T, Z, N, U, K, V, J, and W computed by the following formulas:

$$\begin{aligned} &Y = APA^{-1};\;\; T = AP^xC^{-1};\;\; Z = D^{-1}QD;\\ &N = D^{-1}Q^wF^{-1};\;\; U = FGF^{-1};\;\; K = FG^vP^wC^{-1};\\ &V = CPC^{-1},\;\; J = D^{-1}Q^xB;\;\; W = B^{-1}Q^wB. \end{aligned} \tag{6}$$

Using some specified 256-bit hash-function Φ, one can generate a signature to the electronic document M as follows:

The signature generation procedure.

1. Generate three random natural numbers k ($k < q$), t ($t < p^2 - 1$), and u ($u < p^2 - 1$). Then calculate the fixator vector by formula (4):

$$R = AP^uG^kQ^tB.$$

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 vector R is concatenated: $e = e_1||e_2 = \Phi\,(\mathrm{M}, R)\,,$ where e_1 and e_2 are 128-bit integers.

3. Calculate the integers b, d, and n by the following formulas (where $\delta = p^2 - 1$):

$$b = u - e - x \bmod \delta; \quad d = -e_1 e_2 - w \bmod \delta.$$
$$n = \frac{k - e_1 - v}{2} \bmod q.$$

4. Calculate the fitting signature element S:

$$S = CP^b G^n Q^d D.$$

5. Calculate the hash value from the from the signature element S to which the randomization signature element e is concatenated:

$$\rho = \Phi\left(S, e\right).$$

6. Calculate the auxiliary fitting elements s and σ of the signature:

$$s = -b - w \bmod \delta; \quad \sigma = \frac{t - d - x - \rho}{w} \bmod \delta.$$

The size of the output signature (e, s, σ, S) is equal to $\approx$ 160 bytes. Computational difficulty μ of the signature generation procedure is roughly equal to six exponentiation operations in the four-dimensional FNAA used as algebraic support of the signature algorithm (four exponentiations to the 256-bit degree and two exponentiations to the 128-bit degree), i. e., to $\approx 15,400$ multiplications modulo a 129-bit prime p. The verification of the signature (e, s, σ, S) to the document M is performed using the public key $(Y, T, Z, N, U, K, V, J, W)$ as folows:

The signature verification procedure.

1. Calculate the vector R':

$$R' = Y^e T S Z^{e_1 e_2} N U^{e_2} K V^s S Z^{\Phi(S,e)} J W^\sigma. \tag{7}$$

2. Compute the hash-function value e' from the document M to which the vector R' is concatenated: $e' = \Phi\left(\mathrm{M}, R'\right)$.

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

At the first step of the signature verification algorithm the computations are performed in accordance with a verification equation with two entries of the signature element S. The computational complexity μ' of the signature verification procedure is roughly equal to six exponentiation operations in the four-dimensional FNAA used as algebraic support, one exponentiation to the 128-bit degree e_1 and five exponentiations to the 256-bit degree, i. e., we have $\mu' \approx 16,900$ multiplications modulo a 129-bit prime.

Correctness proof. Suppose (e, s, σ, S) is a correctly calculated signature to document M. Then you have:

$$\begin{aligned}
&R_1' = \left(APA^{-1}\right)^e \left(AP^xC^{-1}\right) \left(CP^bG^nQ^dD\right) \left(D^{-1}QD\right)^{e_1e_2} \times\\
&\times \left(D^{-1}Q^wF^{-1}\right) \left(FGF^{-1}\right)^{e_1} \left(FG^vP^wC^{-1}\right) \left(CPC^{-1}\right)^s \times\\
&\times \left(CP^bG^nQ^dD\right) \left(D^{-1}QD\right)^\rho \left(D^{-1}Q^xB\right) \left(B^{-1}Q^wB\right)^\sigma =\\
&= AP^eP^xP^bG^nQ^dQ^{e_1e_2}Q^wG^{e_1}G^vP^wP^sP^bG^nQ^dQ^\rho Q^xQ^{w\sigma}B =\\
&= AP^{e+x+b}G^nQ^{d+e_1e_2+w}G^{e_1+v}P^{w+s+b}G^nQ^{d+\rho+x+w\sigma}B =\\
&= AP^{e+x+u-e-x}G^nQ^0G^{e_1+v}P^0G^nQ^{d+\rho+x+t-d-x-\rho}B =\\
&= (AP^uG^{2n+e_1+v}Q^tB = AP^uG^kQ^tB = R \;\Rightarrow\; e' = e.
\end{aligned}$$

The last equality means that the signature calculated correctly in accordance with the signature generation algorithm passes the verification procedure as a genuine signature, i. e., the introduced signature algorithm performs correctly.

5. Discussion

In terms of a hidden group [3, 5] you can say that the proposed signature randomization method and the algorithm on its base use three different hidden groups contained in different commutative subalgebras of the FNAA set by Table 1. The known signature attack on the introduced algorithm is prevented due to the used strengthened signature randomization method described in Section 4. This attack relates to the structural attacke exploiting design features of the signature algorithm. Consider the direct attack that consists in solving the computationally difficult problem put into the base of the algorithm. In our case we have a system of power vector equations defined by formulas (6) connecting the public-key elements with the secret-key elements, the latter being the vector unknowns. Formulas (6) set the following system of power vector equations:

$$\begin{aligned}
&YA = AP; \;\; TC = AP^x; \;\; DZ = QD;\\
&DNF = Q^w; \;\; UF = FG; \;\; KC = FG^vP^w;\\
&VC = CP, \;\; DJ = Q^xB; \;\; BW = Q^wB.
\end{aligned} \tag{8}$$

When solving such a system of nine power vector equations with nine vector unknowns (vectors A, B, C, D, F, N, G, P, and Q), we must determine the unknown 128-bit natural numbers x, v, and w. If we consider them unknown, then our system will already be a system of exponential equations, the complexity of the solution of which seems to be significantly greater than the complexity of the system of power vector equations (at least the authors do not know of any computationally efficient ways to solve large systems involving power and exponential equations, like that present in system (8)). Therefore, consider the system of power vector equations in which the vectors $P_x = P^x$, $P_w = P^w$, $Q_x = Q^x$, $Q_w = Q^w$, and $G_v = G^v$ are unknown vectors satisfying the following five equations: $P_xP = PP_x$, $P_wP = PP_w$, $Q_xQ = QQ_x$, $Q_wQ = QQ_w$, and $G_vG = GG_v$. Adding the last five equations to system (8) we have a large system including 14 power vector equations with 14 vector unknowns. Such system reduces to a system of 56 power scalar equations with 56 scalar unknowns. Computational difficulty of solving such system determins the security Θ (to a direct attack) of the developed signature algorithm $2^{128} < \Theta < 2^{192}$ (see table 1 in [1]).

To reduce computational complexity of the direct attack, you can use formula (1) to set selection of the vectors P_w and P_x from the hidden group generated by the vector P as well as selection of the vectors Q_w and Q_x from the hidden group generated by Q and selection of the vector G_v from the hidden group generated by G. With this technique, the consideration of five vector unknowns is reduced to the consideration of only ten independent scalar unknowns (five different pairs (i, j) of independent scalar unknowns in formula (1) with coefficients determined by coodinates of the vectors P, Q, and G).

This allows us to exclude from consideration five vector equations describing the selection of unknown vectors from hidden groups and reduce the direct attack to solving a system that includes 36 scalar equations with 46 scalar unknowns. Since the number of equations is less than the number of unknowns, the algorithm is characterized by the presence of equivalent keys. However, to calculate one of the equivalent keys, it is necessary to find at least one solution. For example, you can fix the values of 10 scalar unknowns and proceed to solving a system with 36 scalar unknowns. In this case, you can use estimates [1] of the value of the security Θ to direct attacks, which depends on the number of power equations in the system. Taking into account the estimates by [1], you get $2^{100} < \Theta < 2^{128}$.

It is of interest to evaluate the security to forging signature attack performed by solving the verification equation (7) with respect to the vector unknown S. Forgery is performed by selecting and fixing a certain value of the fixator vector R' and scalar values s and σ. After that, the value of the randomizing parameter of the signature is calculated: $e = e_1||e_2 = \Phi(\mathrm{M}, R)$. As a result, we obtain a verification equation with specific values of the factors and powers, except for the power $\Phi(S, e)$, which depends on the unknown vector S. However, such an attack is computationally infeasible due to the two-fold entry of the unknown vector S into the verification equation which includes the exponentiation operation to the power $\Phi(S, e)$ that depends on the unknown S. Thus, the introduced MPKC signature algorithm appears to be secure to the forging signature attack.

To develop a version of the introduced algorithm with enhanced security level ($\geqslant 2^{128}$; up to 2^{256}) you can use as algebraic support the FNAAs having dimensions $m = 6, 8, 10, 12$ (a method for setting FNAA of arbitrary even dimensions is described in [11]). Indeed, the number of power scalar equations which are solved simultaneously in framework of the direct attack (and in framework of the attack based on using known signatures) is proportional to the value of m. However, to perform a security estimation you should study preliminary the structure of such FNAAs from the point of view of their decomposition into a set of commutative subalgebras.

A comparison of the developed algorithm with other known algebraic MPKC signature algorithms on four-dimensional FNAAs is presented in Table 2 (where μ and μ' denotes computational complexity in multiplications modulo a 129-bit prime). The comparison shows that the proposed algorithm implementing enhanced signature randomization looks rather practical as a candidate for a practical post-quantum cryptoscheme.

Table 2

Comparison of the proposed and known algebraic MPKC signature algorithms.

Signature algorithm	signature size, bytes	public-key size, bytes	private-key size, bytes	signature generation μ	signature verification μ'
[6]	160	768	290	$\approx$12,300	$\approx$9,200
[10]	160	768	896	$\approx$49,150	$\approx$24,600
[3]	97	387	451	$\approx$12,300	$\approx$6,150
[5]	192	768	1,104	$\approx$31,500	$\approx$20,700
[12]	160	258	290	$\approx$12,300	$\approx$9,200
Proposed	160	576	592	$\approx$15,400	$\approx$16,900

6. Conclusion

A new method for enhancing the randomization in algebraic MPKC signature algorithms based on computational complexity of solving large systems of power equations has been developed. The main feature of the method is the use of three different hidden commutative groups such that the vectors contained in every one of them are non-commutative with vectors contained in other two hidden groups, the signature being calculated depending on the product of three random representatives of the hidden groups. Based on the new randomization mechanism, a novel candidate for practical post-quantum signature algorithm has been proposed, in which the sizes of the public key and signature are rather small. The algorithm uses one verification equation with two entries of the fitting signature element S. Two auxiliary signature elements s and σ and auxiliary randomization parameter ρ (calculated as a hash value from S) are used as powers in the verification equation. Performed security evaluation shows that the introduced algebraic signature algorithm is resistant to direct attacks, to known signature attacks, and to forging signature attacks. Compared with the known MPKC signature algorithms on hard-to-reverse mappings the proposed one is more attractive as a practical post-quantum cryptoscheme. However the design of the algebaraic MPKC signature algorithm is principally different and more detailed study of its security is to be performed. Another task for future research is to study the structure of FNAAs of dimensions $m = 6, 8, 10, 12$ from the point of view of their decomposition into a set of commutative subrings, which will allow us to establish the values of the orders of hidden groups when developing algorithms that implement the considered randomization method on FNAAs of dimensions $m \geqslant 6$.

References

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

[2] **J. Ding, A. Petzoldt, D.S. Schmidt**, *Multivariate Public Key Cryptosystems. Advances in Information Security*, Springer. New York. **80** (2020).

[3] **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 & Interfaces. **86** (2023), 103740.

[4] **GeMSS**, A Great Multivariate Short Signature. [Online]. Available: https://www-polsys.lip6.fr/Links/NIST/GeMSS.html.

[5] **A.A. Moldovyan**, *Complete signature randomization in an algebraic cryptoscheme with a hidden group*, Quasigroups and Related Systems. **32** (2024), 95 – 108.

[6] **A.A. Moldovyan, D.N. Moldovyan**, *A new method for developing signature algorithms*, Bull. Acad. Sci. Moldova, Mathematics, **1(94)** (2022),46 – 60.

[7] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum algebraic signature algorithms with a hidden group*, Informatsionno-upravliaiushchie sistemy [Information and Control Systems]. (2023) no. 1, 29 – 40.

[8] **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.

[9] **A.A. Moldovyan, D.N. Moldovyan, N.A. Moldovyan**, *Structure of a finite non-commutative algebra set by a sparse multiplication table*, Quasigroups and Related Systems. **30** (2022), 133 – 140.

[10] **D.N. Moldovyan**, *A new type of digital signature algorithms with a hidden group*, Computer Sci. J. Moldova, **31** (2023), 111 – 124.

[11] **N.A. Moldovyan**, *Unifed method for defining finite associative algebras of arbitrary even dimensions*, Quasigroups and Related Systems. **26** (2018), 263 – 270.

[12] **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), 287 – 298.

[13] **N.A. Moldovyan**, *Finite algebras in the design of multivariate cryptography algorithms*, Bull. Acad. Sci. Moldova. Mathematics, **3(103)** (2023), 80 – 89.

[14] **Rainbow Signature**, One of three NIST Post-quantum Signature Finalists, 2021. [Online]. Available: https://www.pqcrainbow.org/.

[15] **Q. Shuaiting, H. Wenbao, Li Yifa, J. Luyao**, *Construction of extended multivariate public key cryptosystems*, International J. Network Security, **18** (2016), no. 1, 60 – 67.

Received February 20, 2025

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