BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(98), 2022, Pages 56–65
ISSN 1024–7696, E-ISSN 2587–4322

A New Method for Developing Signature Algorithms on Finite Non-commutative Algebras

Alexandr A. Moldovyan, Dmitriy N. Moldovyan

Abstract. A new method for developing signature schemes on finite non-commutative associative algebras is introduced. A signature algorithm is developed on a 4-dimensional algebra defined over the ground field $GF(p)$. The public key element and one of the signature elements represent vectors calculated using exponentiation operations in a hidden commutative group. Decomposition of the algebra into commutative subalgebras is taken into account while designing the algorithm. The method extends the class of algebraic digital signature schemes and opens up the possibility of developing a number of practical post-quantum digital signature algorithms, the main merit of which is comparatively small size of the public key, secret key, and signature.

Mathematics subject classification: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50.
Keywords and phrases: Finite associative algebras, non-commutative algebras, discrete logarithm problem, hidden logarithm problem, multivariate cryptography, public-key cryptoscheme, digital signature, post-quantum signature algorithm.

Introduction

At present the widely used digital signature and public key-agreement protocols are based on the computational complexity of the factorization [3, 19] and the discrete logarithm problem [6, 20]. However, the expected breakthrough in quantum computation technology in the near future makes it extremely urgent to develop cryptoschemes that are resistant to attacks using quantum computers. The post-quantum public-key algorithms and protocols should be based on computationally hard problems different from the mentioned two problems, since polynomial algorithms for solving each of them are known [5, 21, 23].

Currently in the field of post-quantum cryptography, considerable attention of the cryptographic community is paid to the development of cryptoschemes on algebras [9, 13], on Boolean functions [1], on lattices [8], and on linear codes [2]. In the framework of the world competition on developing the candidates for post-quantum cryptographic standards the following digital signature schemes have been selected as finalists [17, 18]: CRYSTALS-DILITHIUM, FALCON, and Rainbow. A significant disadvantage of these finalists is the large size of the public key, private key, and signature. Therefore, the search for new more practical signature schemes is of interest.

DOI: https://doi.org/10.56415/basm.y2022.i1.p56

One of attractive approaches to development of the practical post-quantum signature schemes is the use of hidden discrete logarithm problem (HDLP) defined usually in finite non-commutative associative algebras (FNAAs). Different forms of the HDLP were proposed to develop signature schemes on FNAAs [11–13]. The interest in the HDLP problem is related to the fact that the HDLP-based signature schemes have relatively small sizes of the public key and signature. This area of research is quite new, and for a deeper and more complete understanding of the possibilities for the development of practical post-quantum HDLP-based signature schemes, it is of significant interest to search for new forms of the HDLP, especially for the case of using 4-dimensional FNAAs as a carrier of the HDLP, which are defined using sparse basis vector multiplication tables (BVMT) [10, 14]. The main feature of the HDLP-based signature schemes is the use of a hidden group in which the exponentiation operations are executed, while generating the public key and generating and verifying signatures.

In this paper we propose a new method for designing algebraic signature algorithms including exponentiation operations performed in a hidden group. Security of the signature schemes, developed in line with the method, are based on computational difficulty of solving a system of many quadratic equations with many unknowns. This is a principal difference from the HDLP-based signature schemes. A new practical post-quantum signature algorithm, using a 4-dimensional FNAA as algebraic support, is developed.

1 Preliminaries

The discrete logarithm problem is defined in a finite cyclic group as solution of the equation $Y = G^x$, where G is a generator of the cyclic group; Y is a known element of the group; and x is an unknown integer. Usually, the HDLP is set in an m-dimensional ($m = 4, 6, 8$) FNAA as follows. One selects at random an integer $x < q$ and a generator G of a finite cyclic group of prime order q, which is contained in the FNAA. To provide a required level of secutity the prime q should have sufficiently large size (≥ 128 bits). Then the vector G^x is computed and two elements of the public key are formed: $Y = \varphi_1(G^x)$ and $Z = \varphi_2(G)$, where φ_1 and φ_2 are two different homomorphism-map (or automorphism-map) operations. The operations φ_1 and φ_2 are secret, therefore, the potential attacker does not know the basic finite group in which the exponentiation operation had been performed. The masking operations φ_1 and φ_2 possess the property of mutual commutativity with the exponentiation operation that contributes mainly to the security, therefore, different known DLP-base signature algorithms can be used as prototypes of the HDLP-based algorithms. Particular designs [12] use masking operations that a free from the property of mutual commutativity with the exponentiation operation.

Like in the HDLP-based signature algorithms, the method for development of the signature schemes on FNAAs, which is introduced in present paper, also uses exponentiation operations in a hidden group. However, security of the signature algorithms designed in line with the proposed method are based on the computational

difficulty of finding a solution of system of quadratic equations with a large number of unknowns, rather than on the difficulty of HDLP. One can speak about certain connection between the introduced method and the multivariate cryptography [22].

The FNAAs are set as follows. Suppose a finite m-dimensional vector space is defined over a finite field (for example, the ground field $GF(p)$) and additionally to the addition operation and scalar multiplication the vector multiplication is defined so that it is distributive at the right and at the left relative to the addition operation. Then we have the algebraic structure called an m-dimensional finite algebra. An algebra element A can be denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ..., $\mathbf{e}_{m-1}$ are basis vectors.

The vector multiplication operation of two m-dimensional vectors A and B is set by the formula

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

in which every product $\mathbf{e}_i \mathbf{e}_j$ is to be replaced by a single-component vector $\lambda \mathbf{e}_\mathbf{k}$, where $\lambda \in GF(p)$, indicated in the cell at the intersection of the ith row and jth column of so called basis vector multiplication table (BVMT). To define associative vector multiplication operation the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

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

The BVMT shown as Table 1 sets a 2-dimensional finite commutative associative algebra that is a finite field $GF(p^2)$ if the structural constant $\lambda \neq 0$ is a quadratic non-residue in $GF(p)$ [15]. If λ is a quadratic residue, the set of invertible elements of the said algebra represents a multiplicative group possessing 2-dimentional cyclicity and having order equal to $(p-1)^2$. In general, a finite group is called group with μ-dimensional cyclicity if its minimum generator system includes μ independent elements of the same order [16].

Table 1

The BVMT setting a 2-dimensional commutative algebra; $\lambda \neq 0$.

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

In this paper we develop a post-quantum signature scheme using a 4-dimensional FNAA as an algebraic support, in which the vector multiplication operation is set over $GF(p)$, where $p = 2q + 1$ and q is a 256-bit prime, by a sparse BVMT (in order to get a higher performance of the post-quantum signature scheme). Table 2 [10] and Table 3 [14] suit well as an algebraic support of the developed algorithm. Note

that in the case of Table 3 and structural coefficient $\lambda = 1$ we have 2x2 matrix algebra. The introduced method for designing signature algorithms unites the technique of the HDLP-based signature schemes with the multivariate cryptography [22]. Namely, it uses exponentiation operations in a hidden commutative group and masking multiplications, whereas the security of the developed signature scheme is based on the difficulty of solving a system of quadratic equations in many variables.

2 The algebraic support and introduced design method

From the point of view of the decomposition into a set of commutative subalgebras the FNAAs set by Tables 2 and 3 have a similar structure. Each of these algebras is divided into commutative subalgebras of order p^2, which are attributed exactly to the following three types [10, 14]:

i) subalgebras of Ψ_1 type include a multiplicative group of the order $(p-1)^2$, which has 2-dimensional cyclicity;

ii) subalgebras of Ψ_2 type include a cyclic multiplicative group of the order p^2-1;

iii) subalgebras of Ψ_3 type include a cyclic multiplicative group of the order $p(p-1)$.

The Ψ subalgebras intersect exactly in the set of scalar vectors. The number η of the Ψ_1, Ψ_2, and Ψ_3 subalgebras are equal respectively to (see [10, 14]):

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

Table 2

Setting the 4-dimensional FNAA with the two-sided unit $(1, 1, 0, 0)$ [10]; $\lambda \neq 0$.

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

When using one of these two FNAAs as algebraic support of a signature scheme, in framework of the present paper it is supposed that these FNAAs are defined over the field $GF(p)$ with prime characteristic $p = 2q + 1$, where 256-bit integer q is also a prime number. The proposed method exploits the idea of using a verification equation (set in an FNAA) with two occurrences of the signature element S that is non-permutable with every element of the public key calculated in a form of four vectors Y_1, Z_1, Y_2, and Z_2. The first and the second occurrence is connected with computation of the vectors Y_1SZ_1 and Y_2SZ_2 which are exponentiated to different powers depending on a natural number that represents the randomization element of the signature (e, S). Thus, procedure for generating a signature to an electronic

Table 3

Setting the 4-dimensional FNAA with the two-sided unit $(1,0,0,1)$ [14]; $\lambda \neq 0$.

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

document M should output a number e and a vector S that satisfy, for example, the following verification equation

$$R = (Y_1 S Z_1)^{e_1} (Y_2 S Z_2)^{e_2}, \tag{1}$$

where (for some pre-agreed 512-bit hash-function f and a genuine signature) the condition $e = e_1||e_2 = f(M,R)$ is satisfied (note the 512-bit number e is represented as concatenation of two 256-bit numbers e_1 and e_2).

Possibility to compute the signature element S that satisfies the verification equation is provided by calculation of the public-key elements and the vector S as masked elements of a hidden commutative group. To provide smaller size of the first signature element, one can propose to use a primary group of order q^2 contained in the multiplicative group of an algebra of the Ψ_1 type. Algorithm for generating a minimum generator system of a group with 2-dimensional cyclicity in each of the FNAAs, defined by Table 2 and Table 3, is described in [10] and [14], correspondingly.

Te following procedure for generation of the public key in the form of four vectors Y_1, Z_1, Y_2, and Z_2 is proposed:

1. Generate at random a minimum generator system $< G', H' >$ of a commutative group $\Gamma_{<G',H'>}$ possessing the 2-dimensional cyclicity.

2. Compute vectors $G = G'^2$ and $H = H'^2$ that compose a minimum generator system $< G, H >$ of a hidden commutative group $\Gamma_{<G,H>}$ of the order q^2, which possesses the 2-dimensional cyclicity.

3. Generate two random invertible vectors A, B, and D satisfying the conditions $AB \neq BA$, $AD \neq DA$, $BD \neq DB$, $AG \neq GA$, $HB \neq BH$, and $HD \neq DH$ and calculate the vector A^{-1}.

4. Generate at random non-negative integers u and w ($u < q$ and $w < q$) and, using the vectors A and B as masking multipliers compute the public-key elements $Y_1 = AG^u B$ and $Y_2 = AH^w B$.

5. Using the vectors A^{-1} and D as masking multipliers compute the public-key elements $Z_1 = DHA^{-1}$ and $Z_2 = DGA^{-1}$.

The size of public key is equal to ≈ 4096 bits (512 bytes). The integers u and w and vectors G, H, A, B, and D represent a private key of the ≈ 5632 bits (704 bytes) size.

The randomization vector R is computed by the following formula $R = AG^kH^tA^{-1}$, where integers k and t ($k < q$ and $t < q$) are generated at random. The vector R and document M set unique value of the randomization element of the signature. Computation of the signature element S satisfying the verification equation (1) is executed in accordance with the formula

$$S = B^{-1}G^nH^mD^{-1}, \tag{2}$$

where natural numbers n and m are preliminary computed from the following two equations in $GF(p)$:

$$n\,(e_1 + e_2) + ue_1 + e_2 = k \bmod q; \tag{3}$$

$$m\,(e_1 + e_2) + we_2 + e_1 = t \bmod q. \tag{4}$$

3 The proposed post-quantum signature scheme

Signature generation algorithm

1. Generate at random the integers k ($1 < k < q$) and t ($1 < t < q$). Then compute the vector $R = AG^kQ^tA^{-1}$.

2. Using a specified 512-bit hash function f, compute the first signature element e: $e = e_1||e_2 = f(M, R)$, where M is a document to be signed.

3. Using formulas (3) and (4), compute the numbers n and m:

$$n = \frac{k - ue_1 - e_2}{e_1 + e_2} \bmod q;$$
$$m = \frac{t - we_2 - e_1}{e_1 + e_2} \bmod q.$$

4. Calculate the vectors A^{-1} and D^{-1} and the second signature element S:

$$S = B^{-1}G^nH^mD^{-1}.$$

The size of the output signature (e, S) is approximately equal to 1536 bits (192 bytes). Computational difficulty of the signature computation procedure is roughly equal to four exponentiation operations in the 4-dimensional FNAA selected as algebraic support of the signature scheme (12,288 multiplications in GF(p)).

Signature verification algorithm

1. Using a signature $(e, S) = (e_1||e_2, S)$ to an electronic document M, compute the vector

$$R' = (Y_1SZ_1)^{e_1}\,(Y_2SZ_2)^{e_2}\,.$$

2. Compute the hash-function value $e' = f\,(M, R')\,.$

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

The computational difficulty of the signature verification procedure is roughly equal to two exponentiation operations in the 4-dimensional FNAA (6,144 multiplications in $GF(p)$).

Correctness proof of the signature scheme consists in proving that the signature $(e_1||e_2, S)$ computed correctly will pass the verification procedure as genuine signature. The proof is as follows.

Suppose $(e, S) = (e_1||e_2, S)$ is a correctly computed signature to an electronic document M. Then, taking into account the formulas (3) and (4), the public-key and signature generation procedures, and signature verification procedure, we have:

$$
\begin{aligned}
R'_1 &= (Y_1 S Z_1)^{e_1} (Y_2 S Z_2)^{e_2} = \\
&= \left(AG^u B \left(B^{-1} G^n H^m D^{-1}\right) DHA^{-1}\right)^{e_1} \left(AH^w B \left(B^{-1} G^n H^m D^{-1}\right) DGA^{-1}\right)^{e_2} = \\
&= \left(AG^{u+n} H^{m+1} A^{-1}\right)^{e_1} \left(AG^{n+1} H^{w+m} A^{-1}\right)^{e_2} = \\
&= AG^{(n+u)e_1+(n+1)e_2} H^{(m+1)e_1+(m+w)e_2} A^{-1} = \\
&= AG^{n(e_1+e_2)+ue_1+e_2} H^{m(e_1+e_2)+we_2+e_1} A^{-1} = \\
&= AG^k H^t A^{-1} = R \quad \Rightarrow \quad e' = f\left(M, R'\right) = f\left(M, R\right) = e = e_1||e_2.
\end{aligned}
$$

4 Discussion

In the proposed method and the developed digital signature algorithm, the basic operation is the exponentiation one, like in the HDLP-based signature schemes. The exponentiations used while generating the public key and signature are performed in a hidden commutative group, however the developed signature algorithm is not based on computational difficulty of some form of the HDLP. Indeed, in the introduced method the exponentiation operation is used as a technique of generating different vectors contained in the hidden group, when computing the public key. For this purpose one can use formulas derived in [14] and [10], which directly describe the set of elements of the commutative subalgebras of the Ψ_1 type in the case of the FNAAs defined by Table 2 and Table 3, correspondingly. Thus, using those formulas one can directly select four different random elements G, H, J, and L contained in the hidden group and compute the public key as $Y_1 = AJB$, $Y_2 = ALB$, $Z_1 = DHA^{-1}$, and $Z_2 = DGA^{-1}$. When using the last technique for generating the public key, one should respectively modify the signature generation procedure.

Calculation of a signature in the modified signature algorithm includes, for example, the following steps:

1. Generate at random the integers k $(1 < k < q)$, j $(1 < j < q)$ and t $(1 < t < q)$, and l $(1 < l < q)$. Then compute the vector $R = AG^k Q^t J^j L^l A^{-1}$.

2. Using a specified 512-bit hash function f, compute the first signature element e: $e = e_1||e_2 = f(M, R)$, where M is a document to be signed.

3. Compute the numbers n, m, n', and m':

$$
n = \frac{k - e_2}{e_1 + e_2} \bmod q; \;\; m = \frac{t - e_1}{e_1 + e_2} \bmod q; \;\; n' = \frac{j - e_1}{e_1 + e_2} \bmod q; \;\; m' = \frac{l - e_2}{e_1 + e_2} \bmod q.
$$

4. Calculate the second signature element S: $S = B^{-1} G^n H^m J^{n'} L^{m'} D^{-1}$.

To verify a signature in the modified signature scheme the signature verification algorithm of the source signature scheme needs no modification. The modified signature scheme evidently shows that computation of the private key from the public one is not connected with solving a HDLP.

To forge a signature one can propose an attack connected with computation of the private key (or alternative private key) using the following system of quadratic vector equations with the unkowns A, B^{-1}, D, G, H, J, and L:

$$\begin{cases} Y_1 B^{-1} = AJ; \\ Y_2 B^{-1} = AL; \\ Z_1 A = DH; \\ Z_2 A = DG; \\ GH = HG; \\ GJ = JG; \\ JL = LJ, \end{cases} \tag{5}$$

where the last three equations define the pairwise permutability of the unknowns G, H, J, and L (for details see [14] and [10]). The system (5) reduces to the system of 28 quadratic equations (over the field $GF(p)$) with 28 unknowns, which has (by construction) at least one solution.

Computational difficulty of the systems of quadratic equations set over a finite field is used in multivariate public-key cryptosystems [22] attractive as post-quantum ones. However, estimation of the computational difficulty of solving the system (5) represents a topic of individual study.

A rough comparison of the proposed DS scheme with some known candidates for post-quantum signature schemes is presented in Table 4, where a procedure execution time* is estimated in multiplications in $GF(p)$. One can see that the developed signature algorithm has advantages in the size of parameters and performance (lower execution time) against algorithms Falcon [7] and Dilithium [4] which are finalists of the NIST's competition on development of the post-quantum signature standard [18]. The HDLP-based signature schemes look more practical. However, one can expect that the proposed method for development of post-quantum signature algorithm has an internal potential to optimize the design and to get more practical signature schemes. For example, if a further research will show that finding a solution of the system (5) is an infeasible computational problem in the case of 128-bit or 192-bit prime p.

Conclusion

The proposed method and developed signature algorithm can be attributed to the cryptoschemes with a hidden group, however not to the HDLP-based signature schemes. The calculation in the hidden group is used as a technique that provides setting a system of many quadratic equations in many unknowns, which is to be

Table 4

The BVMT setting the 2-dimensional commutative algebra; $\lambda \neq 0$.

Signature scheme	signature size, bytes	public-key size, bytes	sign. gener. time*	sign. verific. time*
HDLP-based [10]	96	384	$\approx 12,300$	$\approx 9,200$
HDLP-based [14]	96	384	$\approx 3,100$	$\approx 6,200$
Falcon [7]	1280	1793	$\approx 20,000$	$\approx 40,000$
Dilithium [4]	2701	1472	$\approx 50,000$	$\approx 90,000$
Proposed	192	704	$\approx 12,300$	$\approx 6,150$

evaluated from the point of view of computational difficulty in order to estimate security of the developed signature algorithm. The latter can be considered as a candidate for practical post-quantum cryptoschemes, since its security is based on a problem for solving of which a hypothetical quantum computer is not efficient. Actually, the proposed method introduces a new approach to development of post-quantum signature algorithms on FNAAs.

References

[1] Agibalov G. P., Pankratova I. A. *Asymmetric cryptosystems on Boolean functions.* Prikl. Diskr. Mat., 2018, **40**, 23–33. DOI: 10.17223/20710410/40/3.

[2] Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. *A code-based group signature scheme.* Designs, Codes and Cryptography, 2017, **82**, 469–493.

[3] Chiou S. Y. *Novel digital signature schemes based on factoring and discrete logarithms.* International Journal of Security and Its Applications, 2016, **10**, 295–310.

[4] Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., and Stehle D. *"CRYSTALS-Dilithium: a lattice-based digital signature scheme*, https://eprint.iacr.org/2017/633.pdf (see also https://pq-crystals.org/dilithium/index.shtml).

[5] Ekert A., Jozsa R. *Quantum computation and Shor's factoring algorithm.* Reviews of Modern Physics, 1996, **68**, 733–752.

[6] ElGamal T. *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory, 1985 **IT-31**, 469–472.

[7] "Fast-Fourier lattice-based compact signatures over NTRU," https://falcon-sign.info/

[8] Hoffstein J., Pipher J., Schanck J. M., Silverman J. H., Whyte W, Zhang Zh. *Choosing parameters for NTRU Encrypt.* Cryptographers' Track at the RSA Conference – CTA-RSA 2017. Springer LNCS, vol. **10159**, 2017, pp. 3-18.

[9] Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. *Cryptographic algorithms on groups and algebras.* Journal of Mathematical Sciences, 2017, **223**, 629–641.

[10] Moldovyan D. N. *A practical digital signature scheme based on the hidden logarithm problem.* Computer Science Journal of Moldova, 2021, **29**, 206–226.

[11] Moldovyan D. N. *New form of the hidden logarithm problem and its algebraic support.* Bulletin of Academy of Sciences of Moldova. Mathematics, 2020, **2(93)**, 3–10.

[12] 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, **16**, 455–461. https://doi.org/10.21638/11701/spbu10.2020.410

[13] Moldovyan N. A., Moldovyan A. A. *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem.* Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software, 2019, **12**, 66–81. DOI: 10.14529/mmp190106.

[14] Moldovyan N. A., Moldovyan A. A. *Digital signature scheme on the 2x2 matrix algebra.* Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2021, **17**, 254–261.

[15] Moldovyan N. A., Moldovyanu P. A. *New primitives for digital signature algorithms.* Quasigroups and Related Systems, 2009, **17**, 271–282.

[16] Moldovyan N. A., *Fast signatures based on non-cyclic finite groups.* Quasigroups and Related Systems, 2010, **18**, 83–94.

[17] Moody D. *NIST Status Update on the 3rd Round*, 2021. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (accessed November 27, 2021).

[18] Post-Quantum Cryptography. Round 3 Submissions. Round 3 Finalists: Digital Signature Algorithms. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[19] Rivest R. L., Shamir A., Adleman L. M. *A method for obtaining digital signatures and public key cryptosystems.* Communications of the ACM, 1978, **21**, 120–126.

[20] Schnorr C. P. *Efficient signature generation by smart cards.* Journal of Cryptology, 1991, **4**, 161–174.

[21] Shor P.W. *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer.* SIAM Journal of Computing, 1997, **26**, 1484–1509.

[22] Shuaiting Qiao, Wenbao Han, Yifa Li, and Luyao Jiao *Construction of Extended Multivariate Public Key Cryptosystems.* International Journal of Network Security, 2016, **8**, 60–67.

[23] Smolin J. A., Smith G., Vargo A. *Oversimplifying quantum factoring.* Nature, 2013, **499**, 163–165.

Alexandr A. Moldovyan, Dmitriy N. Moldovyan
St. Petersburg Federal Research Center of the Russian
Academy of Sciences (SPC RAS),14 Liniya V.O., 39,
St.Petersburg, 199178, Russia
E-mail: *maa1305@yandex.ru*, *mdn.spectr@mail.ru*

Received December 7, 2021