A new type of digital signature algorithms with a hidden group

Dmitriy N. Moldovyan

Abstract

The known designs of digital signature schemes with a hidden group, which use finite non-commutative algebras as algebraic support, are based on the computational complexity of the so-called hidden discrete logarithm problem. A similar design, used to develop a signature algorithm based on the difficulty of solving a system of many quadratic equations in many variables, is introduced. The significant advantage of the proposed method compared with multivariate-cryptography signature algorithms is that the said system of equations, which occurs as the result of performing the exponentiation operations in the hidden group, has a random look and is specified in a finite field of a higher order. This provides the ability to develop post-quantum signature schemes with significantly smaller public-key sizes at a given level of security.

Keywords: finite associative algebra, non-commutative algebra, commutative finite group, discrete logarithm problem, hidden logarithm problem, public key, digital signature, multivariate cryptography, post-quantum cryptosystem.

MSC 2010: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50.

1 Introduction

Multivariate public key cryptosystems (MPKCs) represent a class of post-quantum cryptographic algorithms since they are based on the computational complexity of solving a system of non-linear (usually quadratic) equations in many variables, which is set over a finite field [1],[2]. Hypothetic quantum computers are not efficient at solving

doi:10.56415/csjm.v31.06

the said computational problem. One of three finalists of the NIST competition on developing post-quantum public-key algorithms [3] in the nomination of digital signatures, namely the algorithm Rainbow, is a prominent example of the said class of cryptosystems. The problem of solving a system of quadratic equations is in general an NP-hard problem; however, while designing an MPKC, one should use a set of quadratic polynomials defining a map in a finite field, which has a trapdoor. The design of the MPKCs consists mainly of the development of secure multivariate trapdoors. Inversion of a map with a trapdoor is connected with solving a system belonging to a subclass of systems of quadratic equations. Therefore, the security of the MPKCs is not guaranteed by the NP-hardness of the random or generic systems of quadratic equations and requires expert evaluation.

Currently, the development of the public-key digital signature algorithms, the security of which is based on the so-called hidden discrete logarithm problem (HDLP) defined in a finite non-commutative algebra (FNAA), is also considered an attractive approach to designing practical post-quantum public-key cryptoschemes [4], [5], [7]. A specific feature of the HDLP-based signature schemes is the use of a hidden (secret) group in which exponentiation operations are executed when generating a public key and signature [6]–[8]. Usually, the signature is calculated in the form of two integers (e, s), where e is a randomization element and s is a fitting one. Several HDLP-based signature schemes use an additional fitting element of the signature, which represents an algebra element S [9], [10] used as one of the multipliers of the signature verification equation. The latter potentially is a source of forging signature algorithms. To prevent such attacks, the technique of doubling the verification equation is proposed [9]. A general problem of the HDLP-based approach is a justification of the post-quantum security since, in any case, we have a problem of finding a discrete logarithm value, which can be solved on a quantum computer in polynomial time [11]–[13].

The present article introduces a new design of signature algorithms with a hidden group, in which the single fitting element of the signature represents an algebra element S, and the attacks of the mentioned type are prevented due to using a verification equation with three entries of

the signature element S. The introduced signature scheme uses the exponentiation operations executed in a hidden commutative group; however, its security is based on the computational difficulty of solving a system of many quadratic equations in many variables (unknowns), which is set over the ground finite field $GF(p)$. The mentioned type of the underlying computational problem defines post-quantum security of the developed signature scheme, a significant merit of which relates to the fact that the said system is not directly connected with the used trapdoor, since the latter is set at the level of FNAA, when selecting random masking (secret) m-dimensional vectors.

2 The FNAAs used as algebraic support

Suppose a finite m-dimensional vector space is defined over a finite field, for example, the ground field $GF(p)$. If, in addition to the operation of addition and scalar multiplication, a vector multiplication operation is defined so that it is distributive at the right and at the left relative to the addition operation, then the full set of the m-dimensional vector composes an m-dimensional finite algebra. Some 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 as $AB = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \mathbf{e}_j)$, where every of the products $\mathbf{e}_i \mathbf{e}_j$ is to be substituted by a 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 the 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 $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) : (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)$.

In the developed digital signature scheme, it is proposed to use i) the 4-dimensional FNAA with the multiplication operation set by the BVMT shown in Table 1 or ii) the 6-dimensional FNAA defined by the BVMT shown in Table 2. In the first (second) case, the algebra is defined over the field $GF(p)$ of prime order $p = 2q + 1$, where q is a 256-bit (128-bit) prime.

Table 1. The sparse BVMT [14] setting the used 4-dimensional FNAA ($\lambda \neq 0$)

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

The structure of the used 4-dimensional FNAA had been studied in detail in [14], where it had been proven that this algebra contains p^2+p+1 different commutative subalgebras of order p^2, including i) $\frac{p(p+1)}{2}$ subalgebras with multiplicative groups of order $(p-1)^2$, every one of the latter is generated by a minimum generator system containing two vectors of the same order (such groups are called groups having 2-dimensional cyclicity); ii) $\frac{p(p-1)}{2}$ subalgebras with cyclic multiplicative groups of order p^2-1, and iii) $p+1$ subalgebras with cyclic multiplicative groups of order $p(p-1)$. This algebra contains the global two-sided unit $E=(1,1,0,0)$. The scalar vectors have the form $(j,j,0,0)$, where $j=1,2,\ldots p-1$. A vector $G=(g_0,g_1,g_2,g_3)$ is invertible, if its coordinates satisfy the following invertibility condition [14]:

$$g_0 g_1 \neq \lambda g_2 g_3. \tag{1}$$

The used 6-dimensional FNAA had been earlier considered as a particular case generated applying a unified method for defining associative algebras of arbitrary even dimensions [15]. The latter algebra also contains a sufficiently large number of commutative groups of orders $(p-1)^2$, p^2-1, and $p(p-1)$; however, its decomposition into the set of commutative algebras had not been studied in detail. The global two-sided unit of the algebra is the vector $E=(1,0,0,0,0,0)$. The scalar vectors have the form $(j,0,0,0,0,0)$, where $j=1,2,\ldots p-1$. A vector $G=(g_0,g_1,g_2,g_3,g_4,g_5)$ is invertible, if its coordinates satisfy

Table 2. The BVMT [15] setting the used 6-dimensional FNAA ($\lambda \neq 0$)

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

the following invertibility condition [15]:

$$\begin{aligned} &\frac{1}{4}((g_0+g_2+g_4)^2-\lambda\,(g_1+g_3+g_5)^2)\times \\ &\times\,((g_0-g_2)^2+(g_0-g_4)^2+(g_2-g_4)^2- \\ &-\lambda\,(g_1-g_3)^2-\lambda\,(g_1-g_5)^2-\lambda\,(g_3-g_5)^2)^2\neq 0. \end{aligned} \tag{2}$$

3 The developed post-quantum signature algorithm

3.1 Generation of the public key

The first step of the procedure for generating a public key consists in selecting a random minimum generator system $<G, H>$ of a commutative hidden group, which contains two vectors of the same order equal to q. For the case of the 4-dimensional FNAA, a suitable algorithm is described in [14]. For each of the cases of 4-dimensional and 6-dimensional FNAAs, one can apply the following algorithm for selecting a random pair of vectors G and H setting a hidden commutative group of order q^2 possessing 2-dimensional cyclicity:

1. Generate a random invertible vector R.
2. Calculate the vector $G' = R^{p(p+1)}$.
3. If the vector G' is a scalar vector or has order $\omega_{G'} < p-1$, then go to step1.

4. Generate at random an integer k and a primitive element α modulo p and compute the scalar vector $L = \alpha E$ and the vector $H' = G'^k L$.

5. Calculate the vectors $G = G'^2$ and $H = H'^2$.

6. Output the pair of vectors $<G, H>$, each of which possesses order q, as a minimum generator system of a hidden group possessing 2-dimensonal cyclicity and having order q^2.

The public key represents the set of six vectors Y_1, Z_1, Y_2, Z_2, T, and U and is calculated as follows:

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

2. Using the invertibility conditions (1) and (2), generate random invertible vectors A, B, D, and F satisfying the following inequalities $AB \neq BA$, $AD \neq DA$, $AF \neq FA$, $BD \neq DB$, $BF \neq FB$, $DF \neq FD$, $AG \neq GA$, $BG \neq GB$, $GD \neq DG$, and $GF \neq FG$. Then calculate the vectors A^{-1}, B^{-1}, D^{-1}, and F^{-1}.

3. Generate random integers $y_1, y_2, z_1, z_2 \in GF(p)$ and calculate the vectors Y_1, Z_1, Y_2, Z_2, T, and U:

$$\begin{aligned} &Y_1 = AG^{y_1}B, \quad Z_1 = FH^{z_1}A^{-1}; \\ &Y_2 = DH^{y_2}B, \quad Z_2 = FG^{z_2}D^{-1}; \\ &T = AHB, \ \text{ and } \ U = FGD^{-1}. \end{aligned} \tag{3}$$

The size of public key is equal to ≈ 6144 bits (768 bytes) in the case of the 4-dimensional FNAA used as algebraic support and to ≈ 4608 bits (576 bytes) in the case of the 6-dimensional FNAA. The integers y_1, y_2, z_1, z_2 and vectors G, H, A, B^{-1}, D^{-1}, and F^{-1} represent a private key having the size equal to ≈ 7168 bits (896 bytes) in the case $m = 4$ and to ≈ 5120 bits (640 bytes) in the case $m = 6$.

3.2 The signature generation procedure

Suppose the owner of the public key $(Y_1, Z_1, Y_2, Z_2, T, U)$ is to compute a signature to the electronic document M, using some specified h-bit hash-function f (where $h = 512$ bits and $h = 256$ bits for the cases of 4-dimensional and 6-diensional FNAAs, correspondingly). Then the

digital signature is computed using the secret values y_1, y_2, z_1, z_2, G, H, A, B^{-1}, D^{-1}, and F^{-1} and the following algorithm:

1. Generate at random integers $k < q$ and $t < q$ and compute the vector

$$R = AG^k H^t D^{-1}.$$

2. Compute the hash-function value $e = e_1||e_2$ (the first signature element) from the document M to which the vector R is concatenated: $e = e_1||e_2 = f(M, R)$, where e_1 and e_2 are $(h/2)$-bit non-negative integers.

3. Calculate the integers n and u:

$$n = \frac{k - y_1 e_1 - z_2 e_2 - 1}{e_1 + e_2 + 1} \bmod q;$$
$$u = \frac{t - z_1 e_1 - y_2 e_2 - 1}{e_1 + e_2 + 1} \bmod q.$$

4. Calculate the second signature element S:

$$S = B^{-1} G^n H^u F^{-1}.$$

The size of the output signature (e, S) is equal to $\approx$ 1280 bits (160 bytes) in the case $m = 4$ and to $\approx$ 896 bits (112 bytes) in the case $m = 6$. Computational difficulty w of the signature computation procedure is roughly equal to four exponentiation operations in the FNAA used as algebraic support of the signature scheme. For the case of 4-dimensional FNAA, we have $w \approx 12,288$ multiplications modulo a 257-bit prime or $w \approx 49,152$ multiplications modulo a 129-bit prime. For the case of 6-dimensional FNAA, we have $w \approx 27,648$ multiplications modulo a 129-bit prime or $w \approx 6,912$ multiplications modulo a 257-bit prime.

3.3 Signature verification procedure

The verification of the signature (e, S) to the document M is performed using the public key $(Y_1, Z_1, Y_2, Z_2, T, U)$ as folows:

1. Calculate the vector R':

$$R' = (Y_1 S Z_1)^{e_1} (TSU) (Y_2 S Z_2)^{e_2}.$$

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

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

The computational difficulty w' of the signature generation procedure is roughly equal to two exponentiation operations in the m-dimensional FNAA used as algebraic support of the signature scheme. For the case $m = 4$, we have $w' \approx 6,144$ multiplications modulo a 257-bit prime or $w' \approx 24,576$ multiplications modulo a 129-bit prime. For the case $m = 6$, we have $w' \approx 13,824$ multiplications modulo a 129-bit prime or $w' \approx 3,456$ multiplications modulo a 257-bit prime.

Correctness proof of the sigature algorrithm consists in proving that the correctly computed signature (e, S) will pass the verification procedure as genuine signature. Indeed, taking into account that the order of the mutually permutable vectors G and H is equal to the prime q, we have the following:

$$
\begin{aligned}
R'_1 &= (Y_1 S Z_1)^{e_1} (TSU) (Y_2 S Z_2)^{e_2} = \\
&= \left(AG^{y_1} BB^{-1} G^n H^u F^{-1} F H^{z_1} A^{-1}\right)^{e_1} \left(AHBB^{-1} G^n H^u F^{-1} FGD^{-1}\right) \times \\
&\qquad \times \left(DH^{y_2} BB^{-1} G^n H^u F^{-1} FG^{z_2} D^{-1}\right)^{e_2} = \\
&= \left(AG^{y_1+n} H^{u+z_1} A^{-1}\right)^{e_1} \left(AHG^n H^u GD^{-1}\right) \left(DH^{y_2+u} G^{n+z_2} D^{-1}\right)^{e_2} = \\
&= AG^{e_1(y_1+n)} H^{e_1(u+z_1)} A^{-1} AG^{n+1} H^{u+1} D^{-1} DH^{e_2(y_2+u)} G^{e_2(n+z_2)} D^{-1} = \\
&= AG^{e_1(y_1+n)+n+1+e_2(n+z_2)} H^{e_1(u+z_1)+u+1+e_2(y_2+u)} D^{-1} = \\
&= AG^{n(e_1+e_2+1)+e_1 y_1+e_2 z_2+1} H^{u(e_1++e_2+1)+e_1 z_1+e_2 y_2+1} D^{-1} = \\
&= AG^{\frac{k-y_1 e_1-z_2 e_2-1}{e_1+e_2+1}(e_1+e_2+1)+e_1 y_1+e_2 z_2+1} \times \\
&\qquad \times H^{\frac{t-z_1 e_1-y_2 e_2-1}{e_1+e_2+1}(e_1+e_2+1)+e_1 z_1+e_2 y_2+1} D^{-1} = \\
&= AG^k H^t D^{-1} = R \quad \Rightarrow \quad f(M, R') = f(M.R) \;\Rightarrow\; e' = e.
\end{aligned}
$$

4 Discussion

Like the known HDLP-based signature schemes, the proposed algorithm uses exponentiation operations in a hidden group. However, in the HDLP-based algorithms, exponentiations define the HDLP; whereas, in the introduced algorithm, the exponentiation operations

are used to set the randomization vector R in a form for which one can find a solution of the vector verification equation with three entries of the variable S (possibility to find a solution is also connected with the representation of the public-key elements in the form of formulas (3)). The random integers y_1, z_1, y_2, and z_2 that are degrees of respective exponentiation operations are used only in the framework of a technique for selecting random vectors $G' = G^{y_1}$, $H' = H^{z_1}$, $H'' = H^{y_2}$, and $G'' = G^{z_2}$ from the hidden group. This technique reduces the number of exponentiations when generating a signature. Actually, the developed signature scheme can be modified so that the randomization vector R is calculated as $R = G^{k_1}H^{t_1}G'^{k_2}H'^{t_2}G''^{k_3}H''^{t_3}$ (where integers k_1, k_2, k_3, t_1, t_2, and t_3 are generated at random), and for generating a signature, the values y_1, z_1, y_2, and z_2 are not needed. This illustrates that the HDLP is not an underlying computationally hard problem in the proposed signature scheme.

To forge a signature, a forger can propose an attack connected with the computation of the private key (or alternative private key) using the following system of 11 quadratic vector equations (defined by formulas (3)) with 10 unknowns A, B^{-1}, D, F, G, G', G'', H, H', H'':

$$\begin{cases} Y_1B^{-1} = AG'; & Y_2B^{-1} = DH''; \\ Z_1A = FH'; & Z_2D = FG''; \\ TB^{-1} = AH; & UD = FG; \\ GG' = G'G; & GG'' = G''G; \\ GH = HG; & GH' = H'G; \\ GH'' = H''G, & \end{cases} \tag{4}$$

where the last five equations define the pairwise permutability of the vectors G, G', G'', H, H', H''. The system (4) reduces to i) the system of 44 quadratic equations (over the field $GF(p)$) with 40 unknowns for the case of the 4-dimensional FNAA used as algebraic support and ii) the system of 66 quadratic equations (over the field $GF(p)$) with 60 unknowns for the case of the 6-dimensional FNAA. Evidently, the system (4) has (on construction) at least one solution.

For the case $m = 4$, in the system of 44 quadratic equations in the field $GF(p)$ every one of the lasts contains 4 members. A comparatively small number of members is defined by the use of the algebra defined by a sparse BVMT. Therefore, for this case, we propose to define the 4-dimensional FNAA over the finite field $GF(p)$ with 257-bit characteristic p; whereas, for the case of 6-dimensional FNAA used as algebraic support, we specify using 129-bit characteristic p. For the case $m = 6$, in the system of 66 quadratic equations in the field $GF(p)$, every one of the lasts contains 12 members.

Taking into account that for the signature algorithm Rainbow (one the finalists of the NIST competition), it is used hardness of solving a system of 96 quadratic equations in 188 variables, which is set in a finite field of order 2^8; one can suppose that in the $m = 4$ ($m = 6$) version of the proposed signature algorithm, it is sufficient to use a 128-bit (64-bit) characteristic p. However, a detailed security analysis of the proposed signature scheme should be performed as independent research work.

The computational difficulty of the systems of quadratic equations set over a finite field is used in multivariate public-key cryptosystems [1], [2] that are attractive as post-quantum ones. However, the estimation of the computational difficulty of solving the system (4) represents a topic of individual study.

A rough comparison of the proposed signature scheme with some known candidates for post-quantum signature schemes is presented in Table 3, where a procedure execution time* is estimated in multiplications in $GF(p)$ with 129-bit characteristic. One can see that the developed signature algorithm has advantages in the size of parameters and performance (lower execution time) against algorithms Falcon [17], Dilithium [18], and Rainbow [3] which are finalists of the NIST's competition on the development of the post-quantum signature standard [19]. The HDLP-based signature algorithms introduced in [14], [16] look more practical. However, one can expect that the proposed method for development of the post-quantum signature algorithms has an internal potential to optimize the design and to get more practical signature schemes. For example, if further research will show that finding a solution to the system (4) is an infeasible compu-

Table 3. Comparison of the proposed and known signature schemes

Signature scheme	signature size, bytes	public-key size, bytes	signature generation time*	signature verification time*
HDLP-based [14]	96	384	$\approx 49,200$	$\approx 36,800$
HDLP-based [16]	96	384	$\approx 12,400$	$\approx 24,800$
Falcon [17]	1280	1793	$\approx 80,000$	$\approx 160,000$
Dilithium [18]	2701	1472	$\approx 200,000$	$\approx 350,000$
Rainbow [3]	1,632	1,683 kB	–	–
Proposed ($m = 4$)	160	768	$\approx 49,152$	$\approx 24,576$
Proposed ($m = 6$)	112	576	$\approx 27,648$	$\approx 13,824$

tational problem in the case of 64-bit (128-bit) prime p for the case of 6-dimensional (4-dimensional) FNAA used as algebraic support.

5 Conclusion

The proposed versions of the signature algorithm on FNAAs can be attributed to the cryptoschemes with a hidden group and to the MPKCs, but not to the HDLP-based signature algorithms. First shown as the development of digital signature algorithms on FNAAs leads to the creation of a MPKC. The introduced digital signature scheme has principal differences from both the known MPKCs and the known HDLP-based signature algorithms and can serve as a promising starting point that can be used for preparing a new application for participating in the NIST competition on developing a standard on a post-quantum signature algorithm (NIST is going to propose such possibility at the fourth round of its competition [19]).

References

[1] Q. Shuaiting, H. Wenbao, Li Yifa, and J. Luyao, “Construction of Extended Multivariate Public Key Cryptosystems,” *International*

Journal of Network Security, vol. 18, no. 1, pp. 60–67, 2016.

[2] D. Jintai and S. Dieter, "Multivariable Public Key Cryptosystems," 2004. [Online]. Available: https://eprint.iacr.org/2004/350.pdf. Accessed on: December 14, 2021.

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

[4] A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, and A. A. Nechaev, "Cryptographic Algorithms on Groups and Algebras," *Journal of Mathematical Sciences*, vol. 223, no. 5, pp. 629–641, 2017.

[5] D. N. Moldovyan, "Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem," *Computer Science Journal of Moldova*, vol. 27, no. 1(79), pp. 56–72, 2019.

[6] A. A. Moldovyan and N. A. Moldovyan, "Post-quantum signature algorithms based on the hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 26, no. 3(78), pp. 301–313, 2018.

[7] N. A. Moldovyan and A. A. Moldovyan, "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*, vol. 12, no. 1, pp. 66–81, 2019. DOI: 10.14529/mmp190106.

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

[9] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "Digital signature scheme with doubled verification equation," *Computer Science Journal of Moldova*, vol. 28, no. 1(82), pp. 80–103, 2020.

[10] N. A. Moldovyan and A. A. Moldovyan, "Candidate for practical post-quantum signature scheme," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 16, no. 4, pp. 455–461, 2020. https://doi.org/10.21638/11701/spbu10.2020.410.

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

[12] A. Ekert and R. Jozsa, "Quantum computation and Shorś factoring algorithm," *Rev. Mod. Phys.*, vol. 68, p. 733, 1996.

[13] R. Jozsa, "Quantum algorithms and the fourier transform," *Proc. Roy. Soc. London Ser A*, vol. 454, pp. 323–337, 1998.

[14] D. N. Moldovyan, "A practical digital signature scheme based on the hidden logarithm problem," *Computer Science Journal of Moldova*, vol. 29, no. 2(86), pp. 206–226, 2021.

[15] N. A. Moldovyan, "Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263–270, 2020.

[16] N. A. Moldovyan and A. A. Moldovyan, "Digital signature scheme on the 2x2 matrix algebra," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 17, no. 3, pp. 254–261, 2021. https://doi.org/10.21638/11701/spbu10.2021.303.

[17] "Fast-Fourier lattice-based compact signatures over NTRU," [Online]. Available: https://falcon-sign.info/. Accessed on: December 14, 2021.

[18] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme." [Online]. Available: https://eprint.iacr.org/2017/633.pdf. Accessed on: December 14, 2021. (see also https://pq-crystals.org/dilithium/index.shtml).

[19] D. Moody, “NIST Status Update on the 3rd Round.” [Online]. Available: 2021. https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/ images-media/session-1-moody-nist-round-3-update.pdf. Accessed on: December 14, 2021.

Dmitriy N. Moldovyan

Received December 14, 2021
Accepted June 07, 2022

ORCID: https://orcid.org/0000-0001-5039-7198
Department of Information Systems,
Saint Petersburg Electrotechnical University ”LETI”,
Prof. Popov, 5, St. Petersburg, 197022,
Russia
E–mail: mdn.spectr@mail.ru