Quasigroups and Related Systems **29** (2021), 97 – 106

A new design of the signature schemes based on the hidden discrete logarithm problem

Dmitriy N. Moldovyan, Alexandr A. Moldovyan, Nikolay A. Moldovyan

Abstract. A new design of the signature scheme based on the computational complexity of the hidden discrete logarithm problem, which meets the criterion of elimination of periodicity associated with the value of the discrete logarithm, is introduced as a candidate for post-quantum public-key cryptoscheme. The used design criterion is oriented to provide security to the known and potential future quantum attacks. Three different 6-dimensional finite non-commutative associative algebras sets over the field $GF(p)$ are considered as the algebraic support of the developed signature have algorithm that is characterized in using a commutative finite group possessing 2-dimensional cyclicity as a hidden group. Besides, the following two different types of masking operations are applied: i) operations that are mutual commutative with the exponentiation operation and ii) operations that are free of this property.

1. Introduction

Development of practical post-quantum (PQ) public-key (PK) cryptosystems is a current challenge in the area of cryptography, which attracts considerable attention from the research community [15, 16]. The most widely used in practice, PK cryptographic algorithms and protocols are not resistant to quantum attacks (attacks on computations on a quantum computer), since they are based on the computational difficulty of the factoring problem (FP) and the discrete logarithm problem (DLP) each of which can be solved in polynomial time on a quantum computer [2, 18]. Quantum algorithms for solving the FP and DLP exploit the extremely high efficiency of quantum computers to perform a discrete Fourier transform [3] which is used to calculate the period length of periodic functions. In particular, to solve DLP, one constructs a periodic function containing a period with the length depending on the value of the logarithm.

Among the computationally difficult problems used as a basic primitive of PQ PK cryptoschemes the hidden discrete logarithm problem (HDLP) [4, 6, 8] is of particular interest for the development of PQ signature schemes [13, 7] having high performance and comparetively small size of the PK and signature.

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, single-sided units, post-quantum cryptography, public-key cryptoscheme, signature scheme, discrete logarithm problem, hidden logarithm problem

Recently [10], an enhanced design criterion has been proposed to provide the resistance of the HDLP-based signature schemes to quantum attacks. That criterion consists in the requirement to eliminate periodicities depending on the value of the discrete logarithm when defining periodic functions on the base of public parameters of the signature scheme. The signature scheme proposed in [10] meets the said design criterion, however, that scheme uses a doubled verification equation reducing the rate and increasing the signature size.

The present paper consideres another design of HDP-based signature schemes meeting the advanced criterion of PQ resistance. The introduced new signature scheme has significantly smaller size of signature and PK.

2. Preliminaries

2.1. Masking operations and hidden logarithm problem

Usually the HDLP is defined in finite non-commutative associative algebras (FNAAs) [6, 7, 13]. The HDLP can be briefly described as follows. It is a selected a random cyclic group having sufficiently large prime order, which is represented by its generator G. Then one computes the PK in the form of the pair of vectors $Z = \psi_1(G)$ and $Y = \psi_2(G^x)$, where x is private key; ψ_1 and ψ_2 are masking operations representing two different homomorphism-map (or automorphism-map) operations which are mutually commutative with the exponentiation operation.

Due to using the masking operations ψ_1 and ψ_2 the vectors Z and Y are contained in different cyclic groups. Each of the masking operations is mutually comutative with the exponentiation operation, therefore, one can use a DLP-based signature (for example, well-known Schnorr signature algorithm [17]) and replace in it the signature verification procedure using the values G and G^x by a signature verification procedure using the values Z and Y. To compute a signature, a potential forger needs to know only the value x that is a discrete logarithm value in a hidden cyclic group, no element of which is known to the forger. The rationale of the security of the HDLP-based signature scheme is connected with the fact that every set of periodic functions constructed using the public parameters of the signature scheme takes on values in many different cyclic groups contained in FNAA used as algebraic support. Therefore, the Shor quantum algorithm is not directly applicable to compute the value x, even in the case when a periodic function contains a period depending on the value x although.

For example, in the case of the signature scheme [13] the function $F(i,j) = Y^i \circ Z^j$, where $\circ$ denotes the multiplication operation in the FNAA, contains a period of the length $(-1, x)$, however one cannot select a fixed cyclic group such that the function $F(i,j)$ take on with sufficiently high probability the values in the fixed cyclic group.

Thus, for the development of the HDLP-based signature schemes, one can formulate the following design criterion:

Criterion 1. *The periodic functions constructed on the base of public parameters of the signature scheme and containing a period with the length depending on the discrete logarithm value should take on values in different finite cyclic groups contained in the FNAA used as algebraic support. Besides, no cyclic group can be pointed out as a preferable finite group for the values of the function $F(i, j)$.*

However, the future progress in quantum computations can lead to developing new quantum algorithms that will allow one to compute the period length for periodic functions that take on values in algebraic sets that are not groups. Possible emergence of such quantum algorithms will mean breaking the known HDLP-based signature schemes.

In the paper [10] the following strengthened criterion for ensuring the security of the HDLP-based cryptoschemes to hypothetic quantum attacks is proposed:

Criterion 2. *Based on the public parameters of the signature scheme, the construction of a periodic function containing a period with the length depending on the discrete logarithm value should be a computationally intractable task.*

Using Criterion 2, in the present paper, a new HDLP-base signature scheme is developed which has smaller sizes of signature and PK.

2.2. The used 6-dimensional FNAAs

Suppose a finite m-dimensional vector space is defined over the ground finite field $GF(p)$. Then defining additionally the vector multiplication that is distributive at the right and at the left relatively the addition operation one gets a finite m-dimensional algebra. Some algebra element (m-dimensional vector) 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 ($\circ$) of two m-dimensional vectors A and B is defined as follows:

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

where every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by a 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 so called basis vector multiplication table (BVMT) like Tables 1, 2, and 3. To define the associative vector multiplication operation, the BVMT should define the associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

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

Three different 6-dimensional FNAAs defined by Tables 1, 2, and 3 with the structural constant $\lambda \neq 0$ are considered as the algebraic support of the HDLP-based signature scheme described in the next Section 3. The BVMT shown as

Tablea 1 is constructed using a unified method [12] for setting FNAA of arbitrary even dimensions. Other two BVMTs are presented as alternative variants of setting the 6-dimensional FNAAs which also suit well for applying them as an algebraic support of the proposed signature scheme.

Every of these FNAAs contains a global two-sided unit. The unit in the algebra defined by Tables 1 and 3 represents the vector $E = (1, 0, 0, 0, 0, 0)$. The unit in the algebras defined by Table 2 is the vector $E = (0, 0, 0, 1, 0, 0)$. Invertible vectors having prime order of sufficiently large size are used as parameters of the signature scheme. In every of the said FNAAs the maximum order of the elements is equal to $\omega_{\max} = p\left(p^2 - 1\right)$ and the algebras are set over the field $GF(p)$ with characteristic equal to prime $p = 2q + 1$, where q is a 255-bit prime number.

It is easy to see that every of the considered FNAAs contains a large number of different commutative groups possessing 2-dimensional cyclicity. The notion of μ-dimensional cyclicity was proposed in [11, 14] in order to highlight the finite groups generated by a minimum generator system including μ elements of the same order.

Consider the vector $V_d = (d, 0, 0, 0, 0, 0)$, where d is primitive element in $GF(p)$. Evidently, the vector V_d is generator of the cyclic group Γ_d including all vectors of the form $(i, 0, 0, 0, 0, 0)$, where $i \neq 0$, and every vector $V \in \Gamma_d$ satisfies the condition $A \circ V = V \circ A$, since multiplication by V represents the scalar multiplication.

Suppose the vector $J \notin \Gamma_d$ has order equal to $p - 1$. Then the minimum generator system $< J, V_d >$ defines the finite commutative group possessing 2-dimensional cyclicity and having the order $\Omega = (p-1)^2$. Every of the considered 6-dimensional FNAAs contains a large number of different commutative groups of the said type and the cyclic group Γ_d is contained in every of these commutative groups.

Table 1

The BVMT [12] setting the 6-dimensional FNAA used as algebraic support

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

Table 2

The BVMT setting the first alternative 6-dimensional FNAA; $\lambda \neq 0$.

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

Table 3

The BVMT setting the second alternative 6-dimensional FNAA; $\lambda \neq 0$.

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

3. The proposed signature scheme

3.1. Setting the hidden commutative group

One can use different values of the structural constant $\lambda \neq 0$ in the BVMTs defining the 6-dimensional FNAAs used as an algebraic support of the developed signature scheme. For any fixed value λ every of the said algebras contains sufficiently large number of commutative groups with 2-dimensional cyclicity. Computation of the private and public parameters of the signature scheme begins with setting a private hidden finite commutative group $\Gamma_{<G,Q>}$ that is generated by the minimum generator system $< G, Q >$ that includes two vectors G and Q each of which has order equal to the prime q. Actually, the group $\Gamma_{<G,Q>}$ of the order q^2 is set as computation of the vectors G and Q of the order q, which is performed as follows:

1. Select a random invertible vector R_1 and compute $G_1 = R_1^{2p(p+1)} \neq E$.
2. Select a random invertible vector R_2 and compute $G_2 = R_2^{2p(p+1)} \neq E$.
3. If $G_1 \circ G_2 = G_2 \circ G_1$, then go to step 1. Otherwise, take $G = G_1$.
4. Select a random integer r and compute $b = r^2 \bmod p \neq 1$.
5. Performing scalar multiplication, compute the vector $Q = bG$.

One can easily see that the order of each of the vectors G and Q is equal

to the prime q, therefore we have the minimum generator system $< G, Q >$ of the commutative group with 2-dimensional cyclicity, which has order equal to the value q^2.

3.2. Masking operations and computation of the public key.

Two different types of masking operations are used:

i) the automorphism map operation $\psi_B(X) = B \circ X \circ B^{-1}$, where B is an invertible vector (private value), which is a mutually commutative the exponentiation operation;

ii) map operations that are not mutually commutative with the exponentiation operation, which are defined as $F_{AB}(X) = A \circ X \circ B^{-1}$ and $F_{BA}(X) = B \circ X \circ A^{-1}$.

Computation of the PK in the form of the triple of vectors (U, Y, Z) is performed as follows:

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

2. Generate at random the invertible vector B of the order $p^2 - 1$, , which satisfies the conditions $G \circ B \neq B \circ G$, and compute the vector $Y = B \circ G \circ B^{-1}$.

3. Generate at random the integers x $(1 < x < q)$ and w $(1 < w < q)$ and the invertible vector A of the order $p^2 - 1$, which satisfies the conditions $A \circ B \neq B \circ A$ and $A \circ G \neq G \circ A$. Then compute the vectors $U = A \circ G^x \circ Q \circ B^{-1}$ and $Z = B \circ Q^w \circ A^{-1}$.

The integers x, w and the vectors G, Q, A, and B are the private parameters of the signature scheme. The private key represents the subset $\{x, w, G, Q, A\}$ of private elements that are used when computing a signature. The size of the PK (U, Y, Z) is equal to 576 bytes.

3.3. Signature generation algorithm:

1. Generate at random the integers k $(1 < k < q)$ and t $(1 < t < q)$. Then compute $V = A \circ G^k Q^t \circ A^{-1}$.

2. Using a specified hash function f_H, compute the first signature element e: $e = f_H(M, V)$, where M is a document to be signed.

3. Compute the second s and third σ signature elements as one of the two solutions of the following system of two congruences

$$\begin{cases} es^2 + xs + x\sigma = k \bmod q; \\ s + ws + \sigma + w\sigma = t \bmod q. \end{cases}$$

If this system has no solution, then go to step 1.

On average, computation of one 96-byte signature (e, s, σ) requires performing the signature generation procedure two times. On the whole, the computational difficulty of the signature computation procedure is roughly equal to four exponentiation operations in the 6-dimensional FNAA selected as the algebraic support of the signature scheme.

3.4. Verification and correctness of the signature scheme

Signature verification procedure includes the following steps:

1. Using the signature (e, s, σ) and the PK (U, Y, Z), compute the vector

$$V' = (U \circ Y^{es} \circ Z)^s \circ (U \circ Z)^{\sigma}.$$

2. Compute the hash function value $e' = f_H(M, V')$.

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

The computational difficulty of the signature verification procedure is roughly equal to three exponentiation operations in the 6-dimensional FNAA. Correctness proof of the signature scheme consists in proving that the signature (e, s, σ) computed correctly will pass the verification procedure as a genuine signature.

Correctness proof:

$$\begin{aligned}
V_1' &= (U \circ Y^{es} \circ Z)^s \circ (U \circ Z)^{\sigma} = \\
&= \left(A \circ G^x \circ Q \circ B^{-1} \circ \left(B \circ G \circ B^{-1}\right)^{es} \circ B \circ Q^w \circ A^{-1}\right)^s \circ \\
&\quad \circ \left(A \circ G^x \circ Q \circ B^{-1} \circ B \circ Q^w \circ A^{-1}\right)^{\sigma} = \\
&= \left(A \circ G^x \circ Q \circ G^{es} \circ Q^w \circ A^{-1}\right)^s \circ A \circ G^{x\sigma} \circ Q^{\sigma} \circ Q^{w\sigma} \circ A^{-1} = \\
&= A \circ G^{xs} \circ Q^s \circ G^{es^2} \circ Q^{ws} \circ G^{x\sigma} \circ Q^{\sigma + w\sigma} \circ A^{-1} = \\
&= A \circ G^{es^2 + xs + x\sigma} \circ Q^{s + ws + \sigma + w\sigma} \circ A^{-1} = A \circ G^k \circ Q^t \circ A^{-1} = V.
\end{aligned}$$

Since $V' = V$, the equality $e' = e$ holds true, i. e. the signature is accepted as a genuine one.

4. Discussion

Consider some periodic functions composed on the base of public parameters of the introduced signature scheme.

1. Suppose the function $F_1(i, j) = (Z \circ U)^i \circ Y^j = B \circ G^{xi+j} \circ Q^{wi+i} \circ B^{-1}$ includes a period with the length (δ_i, δ_j). Then, we have

$$\begin{cases} x\delta_i + \delta_j \equiv 0 \bmod q; \\ (w+1)\delta_i \equiv 0 \bmod q. \end{cases}$$

From the last system, one gets $\delta_i \equiv \delta_j \equiv 0 \bmod q$. The last means the function $F_1(i, j)$ possesses only the periodicity connected with the value q that is the order of cyclic groups contained in the hidden commutative group with 2-dimensional cyclicity.

2. Suppose the function $F_2(i, j) = (U \circ Y \circ Z)^i \circ (U \circ Z)^j = A \circ G^{xi+i+xj} \circ Q^{i+wi+j+wj} \circ A^{-1}$ contains a period with the length (δ_i, δ_j). Then, taking into

account that G and Q are generators of different cyclic groups of the same order q, we have

$$\begin{cases}(x+1)\delta_i + x\delta_j \equiv 0 \bmod q;\\ (w+1)\delta_i + (w+1)\delta_j \equiv 0 \bmod q.\end{cases}$$

The main determinant of this system of two linear equations is not equal to zero, therefore, $\delta_i \equiv \delta_j \equiv 0 \bmod q$, i. e., the function $F_2(i,j)$ also possesses only the periodicity connected with the value q.

3. Suppose the function $F_3(i,j,k) = (U \circ Z)^i \circ \left(U \circ Y^j \circ Z\right)^k = B \circ G^{xi+xk+jk} \circ Q^{wi+i+k+wk} \circ B^{-1}$ contains a period with the length (δ_i, δ_j). Then we have

$$\begin{cases}x\delta_i + x\delta_k + j\delta_k + k\delta_j + \delta_j\delta_k \equiv 0 \bmod q;\\ (w+1)\delta_i + (w+1)\delta_k \equiv 0 \bmod q.\end{cases}$$

When solving the last system of two linear congruencies relatively, the unknowns δ_i, δ_j, and δ_k, one obtains solutions that depend on the values j and k, except the solution $(\delta_i, \delta_j, \delta_k) = (0,0,0)$. This means that the function $F_3(i,j,k)$ possesses only the periodicity with the length (q,q,q), i. e., the function $F_3(i,j,k)$ also possesses only the periodicity connected with the order of the vectors G and Q.

Thus, the proposed signature scheme meets the advanced design criterion of PQ resistance.

Among the nine signature algorithms developed in framework of the NIST competition as candidates for PQ signature standard the algorithms Falcon [https://falcon-sign.info/], Dilithium [https://pq-crystals.org/dilithium/index.shtml], Rainbow [1], and qTESLA [https://qtesla.org/] attracts attention from the view point of the trade off between rate and size of the PK and the signature. Table 4 presents a rough comparison of the proposed signature algorithm with Falcon-512, Dilithium-1024x768, Rainbow, and qTESLA-p-I (versions related to the 128-bit security level).

The signature algorithm proposed in this article has a significant advantage in the size of the signature, but it is inferior in performance than Falcon-512. However, for potential versions of the proposed signature scheme, which will be implemented using a 4-dimensional FNAA with two-sided global unit as the algebraic support, the rate can be increased by 2.25 times (with simultaneous reducing the PK size to the value 384 bytes). Suitable 4-dimensional FNAAs are presented, for example, in papers [5, 9]. When using a 256-bit prime integer as the value q, one can expect the 128-bit security is provided for the both cases of the algebra dimension $m = 6$ and $m = 4$. However consideration of the security of the proposed signature scheme represents a task of individual study.

5. Conclusion

This paper introduces a HDLP-based signature scheme that meets the advanced design criterion of PQ resistance, significant merit of which is the significantly

TABLE 4

Comparison with the NIST candidates for PQ signature standard

Signature scheme	signature size, bytes	publi-key size, bytes	sign. gener. rate, arb. un.	sign. verific. rate, arb. un.
Falcon-512	657	897	50	25
Dilithium	2044	1184	15	10
Rainbow	64	150000	–	–
qTESLA-p-I	2592	15000	20	40
Proposed $m = 6$	96	576	30	40
Proposed $m = 4$	96	384	65	90
[10]	192	768	85	65

smaller size of both the signature and the PK in comparison with the earlier proposed analog [10]. The used design method is characterized in applying both the masking operations that are mutually commutative with the exponentiation operation and the masking operations that are free of such properties. Another feature of the introduced cryptoscheme is the use of the signature verification equation with cascade exponentiation.

In comparison with the PQ signature schemes that are currently considered as candidates for PQ signature standards, the propose scheme is significantly more practical. Besides, implementation of the last one on the base of one of the 4-dimensional FNAA with two-sided global units, which are described in [5, 9], will supposedly also provide 128-bit security, but will have 2.25 times higher performance rate.

References

[1] **J. Ding, D. Schmidt**, *Rainbow, a new multivariable polynomial signature scheme*, Lecture Notes Computer Sci., **3531** (2005), 164 – 175.

[2] **A. Ekert, R. Jozsa**, *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys., **68** (1996), 733.

[3] **R. Jozsa**, *Quantum algorithms and the fourier transform*, Proc. Roy. Soc. London Ser A, **454** (1998), 323 – 337.

[4] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Cryptographic algorithms on groups and algebras*, J. Math. Sci., **223** (2017), no. 5, 629 – 641.

[5] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova, **26** (2018), no. 3(78), 301 – 313.

[6] **A.A. Moldovyan, N.A. Moldovyan**, *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem*, Bull. South Ural State Univ., Ser. Mathematical Modelling, Programming & Computer Software, **12** (2019), 66 – 81.

[7] **A.A. Moldovyan, N.A. Moldovyan**, *New forms of defining the hidden discrete logarithm problem*, SPIIRAS Proceedings, **18** (2019), no 2, 504 – 529.

[8] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems, **18** (2010), 165 – 176.

[9] **D.N. Moldovyan**, *A unified method for setting finite none-commutative associative algebras and their properties*, Quasigroups and Related Systems, **27** (2019), 293 – 308.

[10] **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), 269 – 284.

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

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

[13] **N.A. Moldovyan**, *Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base*, Bul. Acad.e Stiinte Republ. Moldova. Matematica, **1(89)** (2019), 71 – 78.

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

[15] *Post-Quantum Cryptography*, Lecture Notes Computer Sci., **10786**, (2018).

[16] *Post-Quantum Cryptography*, Lecture Notes Computer Sci., **11505** (2019).

[17] **C.P. Schnorr** *Efficient signature generation by smart cards*, Cryptology, **4** (1991), 161 – 174.

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

Received March 25, 2020

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS),
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
14-th line 39, 199178, St. Petersburg, Russia

E-mails: mdn.spectr@mail.ru, nmold@mail.ru