UDC 003.26
doi:10.31799/1684-8853-2020-6-21-29

A novel method for development of post-quantum digital signature schemes

D. N. Moldovyan[a], *PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru*
A. A. Moldovyan[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-5480-6016*
N. A. Moldovyan[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0002-4483-5048*
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: *Development of post-quantum digital signature standards represents a current challenge in the area of cryptography. Recently, the signature schemes based on the hidden discrete logarithm problem had been proposed. Further development of this approach represents significant practical interest, since it provides possibility of designing practical signature schemes possessing small size of public key and signature.* ***Purpose:*** *Development of the method for designing post-quantum signature schemes and new forms of the hidden discrete logarithm problem, corresponding to the method.* ***Results:*** *A method for designing post-quantum signature schemes is proposed. The method consists in setting the dependence of the public-key elements on masking multipliers that eliminates the periodicity connected with the value of discrete logarithm of periodic functions constructed on the base of the public parameters of the cryptoscheme. Two novel forms for defining the hidden discrete logarithm problem in finite associative algebras are proposed. The first (second) form has allowed to use the finite commutative (non-commutative) algebra as algebraic support of the developed signature schemes.* ***Practical relevance:*** *Due to significantly smaller size of public key and signature and approximately equal performance in comparison with the known analogues, the developed signature algorithms represent interest as candidates for practical post-quantum cryptoschemes.*

Keywords *— post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, finite commutative groups, non-commutative associative algebras.*

For citation: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29

Introduction

Since the mid-1990s, cryptographic algorithms and protocols have been widely used to solve information security problems [1, 2]. Public key cryptosystems are of particular importance in electronic document management technologies [3, 4]. The most widely used public-key algorithms and protocols are based on the computational complexity of the factorization problem (FP) [5, 6] and the discrete logarithm problem (DLP) [7, 8]. However, progress in the theory and technology of quantum computing suggests that in the fairly near future, a quantum computer will be available and can be used to solve FP and DLP.

Since polynomial algorithms for solving FP and DLP are known for a quantum computer [9, 10], the implementation of this forecast will make it insecure to use public-key cryptographic algorithms and protocols based on FP and DLP [11, 12]. This raises the problem of the development of post-quantum public-key cryptoschemes based on the computationally hard problems of other types

Over the past decade the global cryptographic community has been actively developing the post-quantum public-key cryptosystems [13, 14]. As a basic primitive, a number of studies consider the problem of searching for a conjugating element in non-commutative braid groups [15, 16]. This problem has been studied in numerous papers and fundamental difficulties associated with the development of practical post-quantum cryptosystems based on it have been identified [17].

At the end of 2016, the National Institute of Standards and Technology of the United States (NIST) announced a program on the developing a project for post-quantum standards for public key-agreement and electronic digital signature (EDS) schemes by 2024, within which a world competition was announced [18] for the development of cryptoschemes of the said type. Out of 69 proposed candidates for post-quantum cryptographic schemes 17 public key-agreement schemes and 9 EDS schemes were selected for participation in the second stage of the competition [19, 20].

The main drawback of the proposed post-quantum EDS schemes is the large total size of the public key and digital signature. A promising approach to the development of post-quantum EDS schemes, based on the use of the computational complexity of the hidden discrete logarithm problem (HDLP), remained out of the attention of the participants of the NIST competition.

The known forms of HDLP are given in finite non-commutative associative algebras (FNAA) given over a ground finite field $GF(p)$ [21]. The extention of the class of algebraic carriers of HDLP and the development of new forms of HDLP is of significant interest for the development of practical post-quantum cryptosystems [22, 23]. In this paper, we propose two new forms of setting the HDLP, which differ in that they use a commutative group with μ-dimensional cyclicity ($\mu \ge 2$) as a hidden group. One of the forms is set in a commutative group with multidimensional cyclicity [24, 25] (a finite group whose basis includes two or more group elements that have the same order is called group with multidimensional cyclicity). The second form of HDLP is set in the FNAAs, various types of which are considered in the works [22, 26, 27].

The hidden discrete logarithm problem as base primitive of post-qantum cryptoschemes

The well-known polynomial algorithms for solving DLP and FP on a quantum computer are based on reducing each of them to the problem of finding the period length of a periodic function constructed using public parameters of the cryptosystem. When solving DLP, a periodic function is constructed that contains a period that depends on the value of the logarithm. A sufficiently fast calculation of the period length is provided by the fact that for functions that take values in a finite cyclic group, a quantum computer effectively performs a discrete Fourier transform [28, 29].

The DLP is formulated as follows: given a public key Y', which is an element of a cyclic group of prime order and calculated by the formula $Y' = G^x$, where G is the group generator, x is the private key ($x < q$). You need to calculate the value of x from the known G and Y'. For a classical computer, polynomial algorithms for finding discrete logarithm are unknown in the multiplicative group of the field $GF(p)$ and in the groups of elliptic curve points.

Calculating the value of x on a quantum computer consists in constructing a periodic function $f(i, j) = (Y')^i G^j$ from two variables i and j, taking integer values, which contains periods of the following lengths: $(0, q)$, $(q, 0)$, (q, q) and $(-1, x)$. The first three values are related to the order value of the cyclic group, and the last one is related to the discrete logarithm:

$$(Y')^i G^j = (Y')^{i-1} G^{j+x} \Rightarrow f(i, j) = f(i-1, j+x).$$

For a function $f(i, j)$, that takes values in an explicitly defined cyclic group of any nature, the quantum algorithm finds the period of length $(-1, x)$ in polynomial time.

For the construction of HDLP-based EDS schemes, FNAAs of various dimensions m are used as algebraic carriers (usually $m = 4$ and $m = 6$), which contain a sufficiently large number of isomorphic cyclic groups [22, 26, 27]. A secret cyclic group of prime order is selected to generate the public key. Some group element $\mathbf{N}$ that is different from the unit element of the group is selected, and the element $\mathbf{N}^x$ is calculated, two secret masking operations ψ_1 and ψ_2 are formed, each of which is mutually commutative with the base exponentiation operation, and two elements of the algebra are calculated $\mathbf{Y}$ and $\mathbf{Z}$: $\mathbf{Y} = \psi_1(\mathbf{N}^x)$, $\mathbf{Z} = \psi_2(\mathbf{N})$, belonging to two other cyclic groups of algebra. To ensure the correct operation of the EDS scheme coordinated operations ψ_1 and ψ_2 are selected. Thanks to this feature the function $f(i, j) = \mathbf{Y}^i\mathbf{Z}^j$ is periodic and contains a period of length $(-1, x)$, however, it takes arbitrary values in the FNAA used as an algebraic carrier, i. e. the values are not restricted to some fixed finite group. This determines the security of the HDLP-based EDS schemes to attacks using known algorithms for finding the length of a period on a quantum computer.

The design criterion of the post-quantum signature schemes, described in [22, 26], this is the following: *setting periodic functions constructed on the base of public parameters of the EDS scheme should lead to the fact that these functions with a fairly low probability take values that belong to any one fixed group.*

However, quantum algorithms for finding the period length for a broader class of periodic functions may appear in the future. The possibility of maintaining high security of EDS schemes with the appearance of such quantum algorithms can potentially be provided by specifying the computational impossibility of constructing periodic functions with a period length that depends on the value of the discrete logarithm.

Thus, the wording of the strengthened criterion of providing resistance to quantum attacks can be shown as follows: *cryptoscheme should be constructed in such a way that the construction of periodic functions based on public parameters of the cryptoscheme should cause these functions will be free from period, depending on the value of discrete logarithm, although there will be periods whose lengths are set by prime order of hidden cyclic group.*

In this paper, finite associative algebras containing finite commutative groups with multidimensional cyclicity are used as the algebraic carrier of the cryptosystem to develop EDS schemes that satisfy the enhanced criterion. Groups of this type include groups whose basis includes two or more elements, the order of each of which is equal to the same value [24, 25].

Setting the finite commutative groups with multidimensional cyclicity

Suppose a finite m-dimensional vector space is set over the field $GF(p)$, where p is a prime. Usually, a vector is presented as an ordered set of coordinates $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$ or as a sum of one-component vectors $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ $(i = 0, 1, \ldots, m-1)$ are basis vectors. Defining additionally the operation of vector multiplication ($\circ$) possessing the property of the two-sided distributivity relatively the addition operation of vectors, one gets the finite m-dimensional algebra.

The multiplication operation of the vectors $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is set with the following formula: $\mathbf{A} \circ \mathbf{B} = \sum_{j=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j$, where each pair of the basis vectors is replaced by the one-component vector indicated in the intersection of the i-th row and j-th column of the so called basis vector multiplication table.

Setting the hidden discrete logarithm problem in a finite commutative group with multi-dimensional cyclicity

In commutative groups, the method of masking the base cyclic group, in which it is supposed to perform the exponentiation operation, should be focused on the implementation of the mentioned earlier strengthened criterion of providing resistance to quantum attacks. Indeed, in commutative groups, it is not possible to perform the automorphic and homomorphic mapping operations used in FNAA [22, 26], therefore we need to offer a new method of masking.

The hidden logarithm problem is set at the stage of forming a public key, which includes the selection of a secret base cyclic group by generating a random vector $\mathbf{G}$, considered as the generator of this group. After performing the basic exponentiation operation (which makes the main contribution to the security of the cryptosystem), we get the vector $\mathbf{G}^x$, which together with the vector $\mathbf{G}$ is subject to masking, which will give two vectors that are elements of the public key. The proposed masking method uses the idea of multiplying vectors $\mathbf{G}$ and $\mathbf{G}^x$ by randomly selected vectors $\mathbf{U}$ and $\mathbf{D}$ of order q, which belong to different cyclic groups other than the base one, and such that the triple of vectors $(\mathbf{G}, \mathbf{U}, \mathbf{D})$ forms the basis of a primary subgroup of order q^3. Thus, one gets the public key as a pair of vectors $\mathbf{Y} = \mathbf{G}^x \circ \mathbf{U}$ and $\mathbf{Z} = \mathbf{G} \circ \mathbf{D}$.

It is easy to see that a pair of vectors $(\mathbf{Y}, \mathbf{Z})$ forms the basis of a primitive subgroup of order q^2, therefore, the periodic function $f_r(i, j) = \mathbf{Y}^i \circ \mathbf{Z}^j$ takes on all q^2 values of the specified primitive subgroup with a period of length (q, q). This function also contains length periods $(q, 0)$ and $(0, q)$ and is free of explicit periodicity, the length of which depends on the discrete logarithm. The latter is determined by the masking influence of multipliers $\mathbf{U}$ and $\mathbf{D}$.

The principal point is that these multipliers have the same order as the vectors $\mathbf{G}$ and $\mathbf{G}^x$. If this condition is violated, for example, if the multipliers are vectors $\mathbf{U}$ and $\mathbf{D}$ have a prime order $r \neq q$, then their masking influence can be completely eliminated by exponentiating the vectors $\mathbf{Y}$ and $\mathbf{Z}$ to the degree r and defining the periodic function $f_r(i, j) = \mathbf{Y}^{ri} \circ \mathbf{Z}^{rj}$, that contains a period of the length $(-1, x)$: $\mathbf{Y}^{r(i-1)} \circ \mathbf{Z}^{r(j+x)} = \mathbf{Y}^{ri}\mathbf{Z}^{-rx} \circ \mathbf{Z}^{r(j+x)} = \mathbf{Y}^{ri} \circ \mathbf{Z}^{rj}$.

Masking multipliers contribute to the digital-signature verification equation. This effect must be compensated for ensuring the correct functioning of the EDS algorithm. The latter is supposed to be provided by calculating an additional element of the digital signature in the form of a vector $\mathbf{S}$, that is included as a multiplier in the verification equation.

If there is a multiplier that is a signature element, it is possible to easily forge the signature using the vector $\mathbf{S}$ as a fitting parameter, the random value of which is calculated as unknown in the EDS authentication equation. To prevent this method of the EDS forgery, the idea of doubling the verification equation can be used, i. e. instead of one verification equation, two similar equations will be used, which use different pairs of the values $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$ and the same signature in the form of triple of the values $(e, s, \mathbf{S})$. In this case forgery of the signature for the first and second verification equations will lead to different values of the fitting parameter $\mathbf{S}$, which makes the specified method of EDS forgery computationally infeasible.

The proposed mechanism for doubling the verification ratio assumes the calculation of the public key in the form of two pairs of vectors $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$, which ensure that the verification equation will be satisfied for the same signature value. This is ensured by the fact that the first and second elements in each of the pairs $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$ are connected by the same value of the discrete logarithm x and the same values of masking factors $\mathbf{U}$ and $\mathbf{D}$. Independence of the pairs $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$ is ensured by the fact that independent base cyclic groups are used for calculating the said pairs, and random multipliers $\mathbf{U}$ and $\mathbf{D}$ are chosen such that the four vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form the basis of a primary group of order q^4. The latter provides the implementation of the enhanced post-quantum resistance criterion (the computational infeasibility of constructing a periodic function with a period defined by the value x).

In the versions of the HDLP specified in the FNAAs and used for designing EDS schemes in [22, 26], the calculation of the value of the discrete logarithm x in the secret base cyclic group can be performed using the baby-step-giant-step algorithm. This is directly connected with the possibility of constructing a periodic function containing a period whose length depends on the x. This circumstance makes it necessary to use a hidden cyclic group of prime order, the size of which is 256 bits while providing 128-bit security.

The proposed version of the HDLP, set in finite commutative groups, implements the enhanced criterion for ensuring post-quantum resistance, i. e. periodic functions constructed on the base of public parameters of the EDS scheme are free from the periodicity associated with the value of the discrete logarithm x. The calculation of the value x by the baby-step-giant-step method and other known analogues can not be carried out due to the fact that the calculation of the value of x can not be separated from the calculation of at least one of the secret vectors **G**, **U**, and **D**. Thus, you can expect that a 128-bit value q is sufficient to provide 128-bit security. However, due to the fact that the new version of the HDLP is little studied, we will consider the implementation of the HDLP-based EDS algorithm for the case of using 256-bit values q.

Digital signature scheme using calculations in a finite group with four-dimensional cyclicity

As the algebraic carrier of the EDS scheme, we will use a four-dimensional finite commutative algebra defined over a field $GF(p)$, where $p = 2q + 1$ with the 256-bit prime q, when using BVMT shown as Table 1, where the structural coefficient $\lambda = 4$.

The unit of this associative algebra is the vector (0, 0, 1, 0), and its multiplicative group has a four-dimensional (two-dimensional) cyclicity at the value λ equal to the quadratic residue (non-residue) in the field $GF(p)$. In the case of forming a group with two-dimensional cyclicity, its basis includes two vectors, each of which has the order $p^2 - 1$, and the group order is equal to $(p^2 - 1)^2$. When developing the EDS scheme in this section, we will consider the case of four-dimensional cyclicity, when the basis of the multiplicative group includes four vectors, each of which has an order $p - 1$, and the group order is equal to $(p - 1)^4$.

■ ***Table 1.*** Setting the multiplication operation in finite algebra multiplicative group of which possesses multidimensional cyclicity

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

The public key is generated as follows:

1. Generate random vectors **G**, **Q**, **U** and **D**, the order of each of which is equal to the same prime number q.

2. Generate random natural number $x < q$ and calculate vectors $\mathbf{Y}_1 = \mathbf{G}^x \circ \mathbf{U}$ and $\mathbf{Y}_2 = \mathbf{Q}^x \circ \mathbf{U}$.

3. Calculate vectors $\mathbf{Z}_1 = \mathbf{G} \circ \mathbf{D}$ and $\mathbf{Z}_2 = \mathbf{Q} \circ \mathbf{D}$.

The public key is two pairs of vectors $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$. The private key of the owner of this public key is a set of the following values x, **G**, **Q**, **U**, and **D**, knowledge of which is required for calculation of the signature. The probability that the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form the basis of a primary group of order q^4, practically is equal to 1. Indeed, the said four vectors are random because they depend on random vectors **G**, **Q**, **U** and **D**. The probability that the products of all possible degrees of the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form a primary subgroup of order q^3 or q^2 is negligible and equal to $\approx q^{-1}$ (if the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ are independent and form a primary group of order q^3, then the probability that a random vector $\mathbf{Z}_2$ is contained in this primary group is equal to the ratio of its order to the number of all vectors of order q, which are contained in the multiplicative group of the four-dimensional algebra under consideration (accounting for case when the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ form a primary group of order q^2 makes a small adjustment to the value q^{-1}).

Let an electronic document M be given, to which a digital signature of owner of the public key $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$ is to be created. To do this, the following procedure is performed, which uses some pre-defined secure 256-bit hash function f_h (the algorithm for calculating a hash value is part of the EDS scheme under consideration):

1. Generate three random natural numbers $k < q$, $t < q$ and $u < q$.

2. Calculate two vector fixators $\mathbf{V}_1$ and $\mathbf{V}_2$ using the following formulas:

$\mathbf{V}_1 = \mathbf{G}^k \circ \mathbf{D}^t \circ \mathbf{U}^u$ and $\mathbf{V}_2 = \mathbf{Q}^k \circ \mathbf{D}^t \circ \mathbf{U}^u$.

3. Calculate the value $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (the first signature element).

4. Calculate the value $s = k - ex \bmod q$ (the second signature element).

5. Calculate the vector $\mathbf{S} = \mathbf{D}^{t-e} \circ \mathbf{U}^{u-s}$ (the third signature element).

At the output of this algorithm we get the digital signature $(e, s, \mathbf{S})$. The main contribution to the computational complexity W of the algorithm is made by exponentiation operations in the four-dimensional algebra under consideration, i. e. one can accept the estimate $W = 8$ exponentiation operations.

Algorithm for verifying triples of values (e, s, $\mathbf{S}$) as a genuine signature to a document M includes the following steps:

1. Using the public key, namely, two pairs of the vectors ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$), calculate the vectors $\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s$ and $\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s$.

2. Attaching vectors $\tilde{\mathbf{V}}_1$ and $\tilde{\mathbf{V}}_2$ to the document M, calculate the hash-function value $\tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right)$.

3. Check whether the equality is valid $\tilde{e} = e$. If it is true, the EDS (e, s, $\mathbf{S}$) is accepted as a genuine one. If $\tilde{e} \neq e$, the signature (e, s, $\mathbf{S}$) is rejected.

The computational complexity of the EDS authentication algorithm is equal to $W = 4$ exponentiation operations. Demonstration of the correctness of the considered EDS scheme involves performing a proof that the signature calculated by the owner of the public key successfully passes the signature authentication procedure. Let the signature (e, s, $\mathbf{S}$) be obtained in accordance with the signature generation procedure when using the correct signer's private key. Then, submitting the signature (e, s, $\mathbf{S}$) to the input of the verification procedure, we have the following proof of the correctness of the proposed signature scheme:

$$\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s = \left(\mathbf{G}^x \circ \mathbf{U}\right)^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ (\mathbf{G} \circ \mathbf{D})^s =$$
$$= \mathbf{G}^{xe} \circ \mathbf{U}^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ \mathbf{G}^s \circ \mathbf{D}^s = \mathbf{G}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{G}^s =$$
$$= \mathbf{G}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{G}^{k-xe} = \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{D}^u = \mathbf{V}_1;$$

$$\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s = \left(\mathbf{Q}^x \circ \mathbf{U}\right)^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ (\mathbf{Q} \circ \mathbf{D})^s =$$
$$= \mathbf{Q}^{xe} \circ \mathbf{U}^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ \mathbf{Q}^s \circ \mathbf{D}^s = \mathbf{Q}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{Q}^s =$$
$$= \mathbf{Q}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{Q}^{k-xe} = \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{D}^u = \mathbf{V}_2 \Rightarrow$$
$$\Rightarrow \tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = e.$$

The obtained equality $\tilde{e} = e$ means the signature (e, s, $\mathbf{S}$) passes the verification procedure as a genuine one.

Setting the HDLP in non-commutative algebra and the EDS scheme based on it

Used in the previous section mechanism of doubling the signature authentication equation can also be applied to develop the EDS algorithms based on the computational complexity of the HDLP set in FNAAs. Let's consider the implementation of an EDS scheme of this type as a doubling of the cryptosystem described earlier in the paper [26] and using the four-dimensional FNAA as its algebraic carrier, in which the vector multiplication operation is set by Table 2 over the field $GF(p)$. As in the previous signature scheme, we assume $p = 2q + 1$ for a 256-bit prime value q.

■ ***Table 2.*** Setting the multiplication operation in 4-dimensional non-commutative algebra [26] ($\lambda \neq 0$; $\lambda \neq 1$)

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

The said four-dimensional FNAA contains a global two-sided unit $\mathbf{E} = ((1 - \lambda)^{-1}, (1 - \lambda)^{-1}, \lambda(\lambda - 1)^{-1}, (\lambda - 1)^{-1})$ and $p(p + 1)(p - 1)^2$ invertible vectors. A sign of the invertibility of a certain vector $\mathbf{A} = (a_0, a_1, a_2, a_3)$ is non-equality $a_0a_1 \neq a_2a_3$. Multiplying a certain vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$ by vectors of the form $\mathbf{D} = (d(1 - \lambda)^{-1}, d(1 - \lambda)^{-1}, d\lambda(\lambda - 1)^{-1}, d(\lambda - 1)^{-1}) = d\mathbf{E}$ is actually a multiplication by a scalar d: $\mathbf{D} \circ \mathbf{X} = d\mathbf{X}$. The latter means that for any value $d \in GF(p)$ the vector $\mathbf{D}$ is permutable with each vector $\mathbf{X}$ in the considered FNAA: $\mathbf{D} \circ \mathbf{X} = \mathbf{X} \circ \mathbf{D}$. Obviously, the equation $\mathbf{D}^i = d^i\mathbf{E}$ holds true. When choosing an integer d, which is a primitive root modulo p, one gets the vector $\mathbf{D}$ that is a generator of a cyclic group $\Gamma_{\mathbf{D}}$ having order equal to $p - 1$.

The maximum order of invertible vectors of the multiplicative group of the considered FNAA is $p^2 - 1$. In this group you can find many different pairs of vectors $\mathbf{G} \notin \Gamma_{\mathbf{D}}$ and $\mathbf{Q} \notin \Gamma_{\mathbf{D}}$ of the order $p - 1$, for which the non-equality $\mathbf{G} \circ \mathbf{Q} \neq \mathbf{Q} \circ \mathbf{G}$ holds true. Each of the pairs of vectors $<\mathbf{G}, \mathbf{D}>$ and $<\mathbf{Q}, \mathbf{D}>$ forms a minimal system of generators (basis) of some commutative group $\Gamma_{<\mathbf{G},\mathbf{D}>}$ and $\Gamma_{<\mathbf{Q},\mathbf{D}>}$, correspondingly, of order $(p - 1)^2$. Intersection of the groups $\Gamma_{<\mathbf{G},\mathbf{D}>}$ and $\Gamma_{<\mathbf{Q},\mathbf{D}>}$ represents the cyclic group $\Gamma_{\mathbf{D}}$. Thus, the four-dimensional algebra under consideration contains a large number of different commutative groups with two-dimensional cyclicity, and the cyclic group $\Gamma_{\mathbf{D}}$ being a subgroup of each of them. This structure of the algebra allows for such modification of the EDS scheme [26], in which a new form of HDLP is specified, which implements an enhanced criterion for ensuring post-quantum security.

This modification is based on the idea of using a commutative group with two-dimensional cyclicity (instead of a cyclic group in the analog [26]) as a hidden group. The proposed version of the EDS scheme is described as follows.

Procedure of generating the public key includes the following steps:

1. Generate random vectors $\mathbf{G} \notin \Gamma_{\mathbf{D}}$ and $\mathbf{B} \in \Gamma_{\mathbf{D}}$, whose order is equal to a prime number q. (These two vectors form the basis $<\mathbf{G}, \mathbf{B}>$ of the group

$\Gamma_{<\mathbf{G},\mathbf{B}>}$ that is commutative, has two-dimensional cyclicity, and has order equal to q^2.)

2. Generate two random numbers r_1 ($r_1 < q$) and r_2 ($r_2 < q$) and calculate the vector $\mathbf{Q} = \mathbf{G}^{r_1} \circ \mathbf{B}^{r_2} \in \Gamma_{<\mathbf{G},\mathbf{B}>}$.

3. Generate two random numbers u_1 ($u_1 < q$) and u_2 ($u_2 < q$) and calculate the vector $\mathbf{U} = \mathbf{G}^{u_1} \circ \mathbf{B}^{u_2} \in \Gamma_{<\mathbf{G},\mathbf{B}>}$.

4. Generate a random natural number x ($x < q$) and two random vectors $\mathbf{J}$ and $\mathbf{H}$ of order $p^2 - 1$, which satisfy the conditions $\mathbf{G} \circ \mathbf{J} \neq \mathbf{J} \circ \mathbf{G}$, $\mathbf{G} \circ \mathbf{H} \neq \mathbf{H} \circ \mathbf{G}$, and $\mathbf{H} \circ \mathbf{J} \neq \mathbf{J} \circ \mathbf{H}$. Then calculate the vectors $\mathbf{Z}_1 = \mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}$, $\mathbf{Y}_1 = \mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}$, $\mathbf{Y}_2 = \mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}$, and $\mathbf{Z}_2 = \mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}$.

The public key is a set of four vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, and $\mathbf{Z}_2$. All other parameters are secret. You can specify the integer number x and vectors $\mathbf{G}$, $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{H}$, $\mathbf{J}$ as private key of the owner of the public key. Calculation of the value x according to the public parameters of the EDS scheme, represents the HDLP, the specific form of which is determined by formulas describing the dependence of the public values $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, and $\mathbf{Z}_2$ on secret vectors $\mathbf{G}$, $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{H}$, $\mathbf{J}$.

Algorithm for creating EDS for an electronic document M:

1. Generate random integers k ($k < q$) and t ($t < q$) and calculate the vectors $\mathbf{V}_1 = \mathbf{J} \circ \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1}$ and $\mathbf{V}_2 = \mathbf{J} \circ \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1}$.

2. Calculate the value $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (the first signature element).

3. Calculate the value $s = k - ex \bmod q$ (the second signature element).

4. Calculate the vector $\mathbf{S} = \mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}$ (the third signature element).

The computational complexity of the signature generation algorithm is equal to $W = 5$ exponentiation operation.

Signature verification algorithm:

1. Calculate the vectors $\mathbf{V}'_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s$ and $\mathbf{V}'_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s$.

2. Calculate the hash-function value $e' = f_h(M, \mathbf{V}'_1, \mathbf{V}'_2)$.

3. If $e' = e$ and the vector $\mathbf{S}$ satisfies the invertibility condition, then the signature is accepted as genuine one. Otherwise the signature is rejected as false one.

The computational complexity of the signature verification algorithm is equal to $W = 4$ exponentiation operation.

Correctness proof of the signature scheme is as fallows:

$$\mathbf{V}'_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s =$$

$$= \left(\mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}\right)^e \circ \left(\mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}\right) \circ \left(\mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}\right)^s =$$

$$= \mathbf{J} \circ \mathbf{G}^{xe} \circ \mathbf{U}^{t-s}\mathbf{G}^s \circ \mathbf{U}^s \circ \mathbf{H}^{-1} = \mathbf{J} \circ \mathbf{G}^{xe} \circ \mathbf{U}^t\mathbf{G}^{k-ex} \circ \mathbf{H}^{-1} =$$

$$= \mathbf{J} \circ \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1} = \mathbf{V}_1;$$

$$\mathbf{V}'_2 = \mathbf{Z}_2^s \circ \mathbf{S} \circ \mathbf{Y}_2^e =$$

$$= \left(\mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}\right)^s \circ \left(\mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}\right) \circ \left(\mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}\right)^e =$$

$$= \mathbf{J} \circ \mathbf{Q}^s \circ \mathbf{U}^s \circ \mathbf{U}^{t-s} \circ \mathbf{Q}^{xe} \circ \mathbf{H}^{-1} = \mathbf{J} \circ \mathbf{Q}^{k-xe} \circ \mathbf{U}^t\mathbf{Q}^{ex} \circ \mathbf{H}^{-1} =$$

$$= \mathbf{J} \circ \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1} = \mathbf{V}_2;$$

$$\left\{\mathbf{V}'_1 = \mathbf{V}_1; \mathbf{V}'_2 = \mathbf{V}_2\right\} \Rightarrow e' = e.$$

The last equality means the correctly computed signature passes the verification procedure as a genuine one.

Discussion

Within the framework of the NIST competition [18], 9 different digital signature schemes are currently being considered as a candidate for the post-quantum EDS standard [20]. The most attractive from the point of view of a compromise between the performance and size of the public key and signature are the following EDS schemes: Falcon [https://falcon-sign.info/], Dilithium [https://pq-crystals.org/dilithium/index.shtml], Rainbow [30], and qTESLA [https://qtesla.org/]. Table 3 shows a rough comparison of the developed EDS schemes with the listed candidates for the post-quantum EDS standard, namely with their versions Falcon-512, Dilithium-1024x768, Rainbow, and qTESLA-p-I, corresponding to the level of 128-bit security. (The relative performance of the proposed signature schemes is estimated under the assumption that multiplication operations in 4-dimensional algebras and in finite ground field $GF(p')$ with 1024-bit characteristic p' have approximately the same computational complexity, when using literature data on the comparative perfor-

■ ***Table 3.*** Comparison with candidates for the post-quantum standard of EDS

Signature scheme	Signature size, byte	Public key size, byte	Rate of signature generation, arb. un.	Rate of signature verification, arb. un.
Falcon-512	657	897	50	25
Dilithium	2044	1184	15	2
Rainbow	64	150 000	–	–
qTESLA-p-I	2592	15 000	20	40
Section 5	192	512	40	80
Section 6	192	512	64	80

mance evaluation of the specified candidates for the post-quantum EDS standard and of the 2048-bit RSA cryptosystem.)

Let's consider the construction of periodic functions based on the public parameters of the proposed EDS schemes. In the case of the signature scheme using computations in the finite commutative group with four-dimensional cyclicity we have the following public parameters $\mathbf{Y}_1 = \mathbf{G}^x \circ \mathbf{U}$, $\mathbf{Y}_2 = \mathbf{Q}^x \circ \mathbf{U}$, $\mathbf{Z}_1 = \mathbf{G} \circ \mathbf{D}$, and $\mathbf{Z}_2 = \mathbf{Q} \circ \mathbf{D}$, where each pair of public key elements depends on some three vectors from the basis <**Q**, **U**, **G**, **D**>, and where each triple of the elements depends on four vectors from the basis. Therefore, periodic functions constructed as products of natural powers of two and three public parameters can only contain periods whose lengths depend on the order of the basis elements, i. e. on the prime value q.

Consider the periodic function $F(i, j, k, h) = \mathbf{Y}_1^i \circ \mathbf{Z}_1^j \circ \mathbf{Y}_2^k \circ \mathbf{Z}_2^h$. Expressing this function from integer variables in terms of the basis of the multiplicative group of the four-dimensional algebra given in Table 3, we obtain: $F(i, j, k, h) = \mathbf{G}^{xi+k} \circ \mathbf{U}^{i+j} \circ \mathbf{Q}^{xj+h} \circ \mathbf{D}^{k+h}$. Let this function have a period $(\delta_i, \delta_j, \delta_k, \delta_h)$. Since all basis vectors are independent, we have the following system of linear congruencies with the unknowns δ_i, δ_j, δ_k, δ_h:

$$\begin{cases} x\delta_i + \delta_k \equiv 0 \bmod q \\ \delta_i + \delta_j \equiv 0 \bmod q \\ x\delta_j + \delta_h \equiv 0 \bmod q \\ \delta_k + \delta_h \equiv 0 \bmod q \end{cases}.$$

The main determinant of this system is different from zero, so there is the single solution $(\delta_i, \delta_j, \delta_k, \delta_h) = (0, 0, 0, 0)$, which means that the function in question contains only periods whose length depends only on the value q.

For the EDS scheme using computations in the four-dimensional FNAA we have the following public parameters $\mathbf{Z}_1 = \mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}$, $\mathbf{Y}_1 = \mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}$, $\mathbf{Y}_2 = \mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}$, and $\mathbf{Z}_2 = \mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}$. Consider the periodic function $F_1(i, j) = \mathbf{Y}_1^i \circ \mathbf{Z}_2^j = \mathbf{J} \circ \mathbf{G}^{xi} \circ (\mathbf{Q} \circ \mathbf{U})^j \circ \mathbf{J}^{-1}$. Since the vector **G** and the vector $\mathbf{Q} \circ \mathbf{U}$ are generators of different cyclic groups of the order q, the function F_1 can only contain periods associated with the value q.

The same situation holds for the function $F_2(i, j) = \mathbf{Y}_2^i \circ \mathbf{Z}_1^j = \mathbf{H} \circ \mathbf{Q}^{xi} \circ (\mathbf{G} \circ \mathbf{U})^j \circ \mathbf{H}^{-1}$. Setting other periodic functions based on the public parameters also does not result in functions containing a period that depends on the value x.

Conclusion

This is the first time that a HDLP-based signature using a finite commutative algebra has been constructed. Thus, the proposed signature scheme satisfies the enhanced criteria of post-quantum security. An EDS scheme is also proposed that meets the enhanced post-quantum security criterion and is based on the computational complexity of the HDLP set in the FNAA. The specified criterion is met by using a commutative finite group with two-dimensional cyclicity as a hidden group.

Financial support

This work was supported by the budget theme No. 0060-2019-010.

References

1. *Advances in Cryptology — CRYPT0'95. 15th Annual International Cryptology Conference*, Santa Barbara, California, USA, August 27–31, 1995, Proceedings. Lecture Notes in Computer Science series, Springer, 1995, vol. 963.
2. *Advances in Cryptology — CRYPTO 2019. 39th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings. Lecture Notes in Computer Science series, Springer, Cham, 2019, vol. 11692.
3. *Public Key Cryptography, PKC'98. The First International Workshop on Practice and Theory of Public-Key Cryptography*, Pacifico Yokohama, Japan, February 1998, Proceedings. Lecture Notes in Computer Science series, Springer, 1998, vol. 1431.
4. *Public-Key Cryptography — PKC 2019. 22nd IACR International* Conference *on Practice and Theory of Public-Key Cryptography*, Beijing, China, April 14–17, 2019, Proceedings. Lecture Notes in Computer Science series, Springer, 2019, vol. 11443.
5. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
6. Chiou S. Y. Novel digital signature schemes based on factoring and discrete logarithms. *International Journal of Security and its Applications*, 2016, vol. 10, no. 3, pp. 295–310.
7. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. IT-31, no. 4, pp. 469–472.
8. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
9. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum com-

puter. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.

10. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
11. Yan S. Y. *Quantum Computational Number Theory*. Springer, 2015. 252 p.
12. Yan S. Y. *Quantum Attacks on Public-Key Cryptosystems*. Springer, 2014. 207 p.
13. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018*, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. Lecture Notes in Computer Science series, Springer, 2018, vol. 10786.
14. *Proceedings of the 10th International Workshop on Post-Quantum Cryptography, PQCrypto 2019*, Chongqing, China, May 8–10, 2019. Lecture Notes in Computer Science series, Springer, 2019, vol. 11505.
15. Verma G. K. A proxy blind signature scheme over braid groups. *International Journal of Network Security*, 2009. vol. 9, no. 3, pp. 214–217.
16. Hiranvanichakorn P. Provably authenticated group key agreement based on braid groups – the dynamic case. *International Journal of Network Security*, 2017, vol. 19, no. 4, pp. 517–527.
17. Myasnikov A., Shpilrain V., Ushakov A. *A Practical Attack on a Braid Group Based Cryptographic Protocol*. In: *Advances in Cryptology – CRYPTO'05*. Lecture Notes in Computer Science series, Springer-Verlag, 2005. Vol. 3621. Pp. 86–96.
18. *Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 03 September 2020).
19. *Post-Quantum Cryptography. Round 2 Submissions*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (accessed 03 September 2020).
20. Zimmer D. *NIST Round 2 and Post-Quantum Cryptography — The New Digital Signature Algorithms*. 2019. Available at: https://www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantum-cryptography-the-new-digital-signature-algorithms/ (accessed 03 September 2020).
21. 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, vol. 223, no. 5, pp. 629–641.
22. 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 (Bulletin SUSU MMCS)*, 2019, vol. 12, no. 1, pp. 66–81. doi:10.14529/mmp190106
23. Moldovyan N. A., Moldovyan A. A. New forms of defining the hidden discrete logarithm problem. *SPIIRAS Proceedings*, 2019, vol. 18, no. 2, pp. 504–529. doi:10.15622/sp.18.2.504-529
24. Moldovyan N. A., Moldovyanu P. A. New primitives for digital signature algorithms. *Quasigroups and Related Systems*, 2009, vol. 17, no. 2, pp. 271–282.
25. Moldovyan N. A. Fast signatures based on non-cyclic finite groups. *Quasigroups and Related Systems*, 2010, vol. 18, no. 1, pp. 83–94.
26. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem. *Computer Science Journal of Moldova*, 2018, vol. 26, no. 3(78), pp. 301–313.
27. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions. *Quasigroups and Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.
28. Jozsa R. Quantum algorithms and the fourier transform. *Proc. Roy. Soc. London*, *Ser A*, 1988, vol. 454, pp. 323–337.
29. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
30. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2005, vol. 3531, pp. 164–175.

УДК 003.26
doi:10.31799/1684-8853-2020-6-21-29

Новый метод построения постквантовых схем цифровой подписи

Д. Н. Молдовян[a], канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru
А. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0001-5480-6016
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048
[a]Санкт-Петербургский институт информатики и автоматики РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка постквантовых схем цифровой подписи является одним из вызовов в области криптографии. Недавно предложены схемы цифровой подписи, основанные на скрытой задаче дискретного логарифмирования. Развитие этого подхода представляет существенный прикладной интерес, поскольку он позволяет разработать практичные схемы подписи, обладающие малыми размерами открытого ключа и подписи в сравнении с известными аналогами. **Цель:** разработка метода построения постквантовых схем подписи, соответствующих ему новых форм задания скрытой задачи дискретного логарифмирования и схем подписи на его основе. **Результаты:** предложен метод построения постквантовых схем цифровой подписи. Суть метода состоит в задании зависимости элементов открытого ключа от маскирующих множителей, устраняющих периодичность, зависящую от значения дискретного логарифма, в периодических функциях, построенных на основе открытых параметров криптосхемы. На основе метода разработаны две новые формы задания скрытой задачи дискретного логарифмирования в конечных ассоциативных алгебрах. Первая позволила использовать коммутативные алгебры, а вторая — некоммутативные алгебры в качестве алгебраического носителя разработанных схем цифровой подписи. **Практическая значимость:** разработанные алгоритмы цифровой подписи представляют интерес как кандидаты на практичные постквантовые криптосхемы, обладающие существенно меньшим размером открытого ключа и подписи при примерно равной производительности в сравнении с известными аналогами.

Ключевые слова — постквантовые криптосхемы, компьютерная безопасность, электронная цифровая подпись, задача дискретного логарифмирования, конечные коммутативные группы, некоммутативные ассоциативные алгебры.

Для цитирования: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Информационно-управляющие системы*, 2020, № 6, с. 21–29. doi:10.31799/1684-8853-2020-6-21-29

For citation: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = –.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Coreldraw (*.cdr); Excel (*.xls); Word (*.docx); Adobe Illustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Правила для авторов».

Контакты

Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru