UDC 003.26
doi:10.31799/1684-8853-2022-1-44-53

Articles

A novel method for developing post-quantum digital signature algorithms on non-commutative associative algebras

A. A. Moldovyan[a], *Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0001-5480-6016, maa1305@yandex.ru*
D. N. Moldovyan[a], *PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198*
N. A. Moldovyan[a], *Dr. Sc., Tech., Professor, Chief Researcher, orcid.org/0000-0002-4483-5048*
[a]*St. Petersburg Federal Research Center of the RAS, 39, 14th Line, V. O., 199178, Saint-Petersburg, Russian Federation*

Introduction: *Development of practical post-quantum signature algorithms is a current challenge in the area of cryptography. Recently, several candidates on post-quantum signature schemes, in which the exponentiation operations in a hidden commutative group contained in a non-commutative algebra is used, were proposed. Search for new mechanisms of using a hidden group, while developing signature schemes resistant to quantum attacks, is of significant practical interest.* ***Purpose:*** *Development of a new method for designing post-quantum signature algorithms on finite non-commutative associative algebras.* ***Results:*** *A novel method for developing digital signature algorithms on non-commutative algebras. A new four-dimensional finite non-commutative associative algebra set over the ground field GF(p) have been proposed as algebraic support of the signature algorithms. To provide a higher performance of the algorithm, in the introduced algebra the vector multiplication is defined by a sparse basis vector multiplication table. Study of the algebra structure has shown that it can be represented as a set of commutative subalgebras of three different types, which intersect exactly in the set of scalar vectors. Using the proposed method and introduced algebra, a new post-quantum signature scheme has been designed. The introduced method is characterized in using one of the elements of the signature (e, S) in form of the four-dimensional vector* $\mathbf{S}$ *that is computed as a masked product of two exponentiated elements* $\mathbf{G}$ *and* $\mathbf{H}$ *of a hidden commutative group:* $\mathbf{S} = \boldsymbol{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{r}\mathbf{C}^{-1}$*, where non-permutable vectors* $\mathbf{B}$ *and* $\mathbf{C}$ *are masking multipliers; the natural numbers n and r are calculated depending on the signed document M and public key. The pair* $\langle \mathbf{G}, \mathbf{H} \rangle$ *composes a minimum generator systems of the hidden group. The signature verification equation has the form* $\mathbf{R} = (\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1)^{e}(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2)^{e^2}$*, where pairwise non-permutable vectors* $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, *and* $\mathbf{Z}_2$ *are element of the public key and natural number e that is computed depending on the value M and the vector* $\mathbf{R}$. ***Practical relevance:*** *Due to sufficiently small size of public key and signature and high performance, the developed digital signature scheme represents interest as a practical post-quantum signature algorithm. The introduced method is very attractive to develop a post-quantum digital signature standard.*

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

For citation: Moldovyan A. A., Moldovyan D. N., Moldovyan N. A. A novel method for developing post-quantum digital signature algorithms on non-commutative associative algebras. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 44–53. doi:10.31799/1684-8853-2022-1-44-53

Introduction

At present the most widely used digital signature algorithms are based on the computational complexity of the integer factorization problem [1, 2] and the discrete logarithm problem (DLP) [3, 4]. However, both of the said problems can be solved in polynomial time on a quantum computer [5–7]. The expected breakthrough in the technology of quantum computations in the near future makes it extremely urgent to develop practical post-quantum public-key signature algorithms (post-quantum are called algorithms that are resistant to attacks using quantum computers) [8]. Computationally difficult problems other than factorization problem and DLP are to be used as the base cryptographic primitive of post-quantum digital signature algorithms.

In the current field of development of public-key post-quantum cryptoschemes, considerable attention of the cryptographers is paid to the development of cryptoschemes on algebras [9, 10], on Boolean functions [11, 12], and on linear codes [13, 14].

A landmark event in the area of post-quantum cryptography is the worldwide algorithm competition announced by the US National Institute of Standards and Technology (NIST) for the period 2017–2024 with the aim of developing post-quantum standards for digital signature algorithms and public key agreement algorithms. The first round [15] of the competition ended with the selection of 10 signature algorithms and 16 public key agreement algorithms (i. e. 26 public-key algorithms out of 69 initially submitted for participation in the competition) as potential candidates for post-quantum standards. The second round [16] ended with the selection of three signature algorithms and four public key-agreement algorithms (called finalists) for the in-depth analysis in the third round. In addition, three alternative signature algorithms and five alternative key agreement algorithms were selected for consideration at the fourth round of the

competition. For the first time in the NIST cryptographic competitions, along with the finalists, alternative cryptoschemes were selected for final consideration.

However, the most interesting thing is that according to the results of the third round of the competition NIST intends to accept new post-quantum signature algorithms for consideration at the fourth round [17]. In a brief overview of the current results of the competition [17], it is noted: "We are most interested in a general purpose digital signature scheme which is not based on structured lattices". Taking into account that algorithms Dilithium and Falcon, which are based on lattices, are considered the most promising for adopting the post-quantum signature standard, one can conclude that NIST remained somewhat dissatisfied with the current results of the competition in the nomination of signature algorithms. Thus, search for new methods, mechanisms, and algebraic supports for the development of practical post-quantum digital signature algorithms is still an urgent task.

One of attractive primitives of the post-quantum signature algorithms is the hidden discrete logarithm problem (HDLP) defined usually in finite non-commutative associative algebras (FNAAs). Earlier, many different forms of the HDLP were proposed to develop signature algorithms on FNAAs [18–20]. The main feature of the HDLP-based signature schemes is the use of the exponentiation operations in hidden commutative groups and computing the signature in the form of two integers. The latter defines possibility to forge signatures in the case of known secret value of the discrete logarithm in a hidden group, for calculation of the public key secret vectors are used as masking multipliers though. Separate HDLP-based algorithms are characterized by using an auxiliary signature element in the form of a vector **S**. In the last type algorithms for eliminating attacks associated with the use of the vector **S** as a fitting parameter, a doubling of the signature verification equation is proposed [20].

In this paper, we propose a new method for developing the signature algorithms including the exponentiation operations in a hidden group, which is characterized in using a vector **S** as a main element of the signature (*e*, **S**) including the randomization integer *e*. The vector **S** is included in the verification equation two or more times. The latter defines computational infeasibility of forging a signature by calculating the value of **S** from the verification equation. At the same time, with the knowledge of secret masking vectors, it is possible to calculate the vector **S** satisfying the verification equation for arbitrary fixed value of the randomizing signature element *e*. Using the proposed method, a new candidate for post-quantum signature algorithm is developed. To provide higher performance a new four-dimensional FNAA set by a sparse basis vector multiplication table (BVMT) is proposed and used as algebraic support of the signature algorithm.

Four-dimensional FNAA used as algebraic support

A vector space of dimension m, which is set over a finite ground field $GF(p)$, with the additionally defined vector multiplication operation that is distributive at the left and at the right relatively the addition operation is called m-dimensional algebra. A vector $\mathbf{A}$ is presented as an ordered set of its coordinates: $\mathbf{A} = (a_0, a_1, ..., a_{m-1})$ or as a sum of its components: $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + ... + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ ($i = 0, 1, ..., m - 1$) are formal basis vectors. If the vector multiplication is non-commutative and associative, then one gets m-dimensional FNAA.

Usually, the multiplication of two 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 defined by the following formula: $\mathbf{AB} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i\mathbf{e}_j$, where the coordinates a_i and b_i are multiplied as elements of the field $GF(p)$ and every the product of two formal basis vectors is to be replaced by an one-component vector indicated in a cell at the intersection of the i-th row and j-th column of so called BVMT. In general for the case $m = 4$, one vector multiplication operation is implemented as executing about 16 multiplications and 12 additions in $GF(p)$. To reduce computational complexity of the vector multiplication we propose a new sparse BVMT shown as Table 1, which defines a four-dimensional FNAA with reduced two times complexity of the vector multiplication.

A left-sided unit $\mathbf{E}_L$ of the said algebra can be computed from the vector equation $\mathbf{XA} = \mathbf{A}$ that can be reduced to the following two independent systems of two linear equations with unknown values of the coordinates of the vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$:

■ ***Table 1***. Multiplication of basis vectors ($\lambda \neq 0$) in the proposed four-dimensional FNAA with global two-sided unit $\mathbf{E} = (0, 1, 1, 0)$

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

$$\begin{cases} a_1x_0 + a_0x_2 = a_0; \\ a_2x_2 + \lambda a_3x_0 = a_2; \end{cases}$$
$$\begin{cases} a_1x_1 + \lambda a_0x_3 = a_1; \\ a_3x_1 + a_2x_3 = a_2. \end{cases}$$

From the last two systems one easily gets $\mathbf{E}_L = (0, 1, 1, 0)$. The right-sided unit $\mathbf{E}_R$ can be computed from the vector equation $\mathbf{AX} = \mathbf{A}$. The latter gives $\mathbf{E}_R = (0, 1, 1, 0) = \mathbf{E}_L$. One can easily see that the vector $\mathbf{E} = (0, 1, 1, 0)$ acts as global two-sided unit in the considered four-dimensional FNAA. One can show that for different fixed values $\mathbf{A}$ the vector equation $\mathbf{AX} = \mathbf{E}$ has a unique solution or has no solutions. In the first case the vector $\mathbf{A}$ is called invertible and in the second case it is called non-invertible. Inverse value of $\mathbf{A}$ is denoted as the vector $\mathbf{A}^{-1}$. Considering the vector equation $\mathbf{AX} = \mathbf{E}$ or equation $\mathbf{XA} = \mathbf{E}$, one can obtain the invertibility (non-invertibility) condition of the vector $\mathbf{A}$:

$$a_1a_2 \neq \lambda a_0a_3 \ (a_1a_2 = \lambda a_0a_3). \qquad (1)$$

Using the formulas (1) it is easy to find the number on non-invertible vectors (equal to $p^3 + p^2 - p$) and then the number Ω of invertible vectors (order of the multiplicative group of the algebra):

$$\Omega = p(p^2 - 1)(p - 1). \qquad (2)$$

The structure of a FNAA from the view point of its decomposition into a set of commutative subalgebras represents significant interest while using it as algebraic support of the HDLP-based signature algorithms [18]. Next section describes the structure of the introduced four-dimensional FNAA.

Structure of the algebra used as algebraic support

To study the structure of the FNAA set by Table 1, we apply the method used earlier in the paper [18]. Consider the set of the vectors $\mathbf{X}$ that are permutable with a fixed vector $\mathbf{A} = (a_0, a_1, a_2, a_3)$. The set of vectors $\mathbf{X} = (x_0, x_1, x_2, x_3)$ can be computed as solution space of the following vector equation:

$$\mathbf{AX} - \mathbf{XA} = (0, 0, 0, 0). \qquad (3)$$

If $\mathbf{X}_1$ and $\mathbf{X}_2$ are two solutions, then $\mathbf{X}_1 \pm \mathbf{X}_2$ and $\mathbf{X}_1\mathbf{X}_2$ are also solutions. One can show that the set of solutions of the equation (3) represents a subalgebra $\Psi_{\mathbf{A}}$. The said vector equation can be reduced to the following system of four linear equations with the unknowns x_0, x_1, x_2, and x_3:

$$\begin{cases} a_1x_0 + a_0x_2 - a_0x_1 - a_2x_0 + \lambda a_3x_0 = 0; \\ a_1x_1 + \lambda a_0x_3 - a_1x_1 - \lambda a_3x_0 = 0; \\ a_1x_2 + \lambda a_3x_0 - a_2x_2 - \lambda a_0x_3 = 0; \\ a_3x_1 + a_2x_3 - a_1x_3 - a_3x_2 = 0. \end{cases} \qquad (4)$$

The system (4) reduces to the following system of three linear equations:

$$\begin{cases} a_3x_0 - a_0x_3 = 0; \\ (a_1 - a_2)x_0 + a_0(x_2 - x_1) = 0; \\ a_3(x_1 - x_2) + (a_2 - a_1)x_3 = 0. \end{cases} \qquad (5)$$

Depending on the vector $\mathbf{A}$ there are possible the following cases.

I. Case $a_0 = a_3 = 0$. The system (5) reduces to the system

$$\begin{cases} (a_1 - a_2)x_0 = 0; \\ (a_1 - a_2)x_3 = 0. \end{cases}$$

If $a_1 \neq a_2$, then the subalgebra $\Psi_{\mathbf{A}}$ includes the set of vectors described by the following formula:

$$\mathbf{X} = (x_0, x_1, x_2, x_3) = (0, d, h, 0), \qquad (6)$$

where $d, h = 0, 1, ..., p - 1$. The set (6) contains $2p - 1$ non-invertible vectors of the forms $(0, 0, h, 0)$ and $(0, d, 0, 0)$ and $(p - 1)^2$ invertible vectors, i. e., the multiplicative group Γ_1 of the $\Psi_{\mathbf{A}}$ subalgebra has order $\Omega_1 = (p - 1)^2$. A generator system of the group Γ_1 includes two vectors or order $p - 1$. Such group is called a group possessing two-dimensional cyclicity. Subalgebras containing a multiplicative group of the Γ_1 type are called subalgebras of the Ψ_1 type.

If $a_1 = a_2$, then every vector of the considered FNAA is permutable with $\mathbf{A}$. Indeed, in this subcase we have a scalar vector $\mathbf{A} = (0, a_1, a_1, 0)$.

II. Case $a_0 \neq 0$; $a_3 = 0$. The system (5) reduces to the system

$$\begin{cases} x_3 = 0; \\ x_2 = x_1 - \dfrac{a_1 - a_2}{a_0}x_0. \end{cases}$$

The set of elements of the subalgebra $\Psi_{\mathbf{A}}$ is described by the following formula

$$\mathbf{X} = \left(d, h, h - \frac{a_1 - a_2}{a_0}d, 0\right), \qquad (7)$$

where $d, h = 0, 1, ..., p - 1$. Taking into account the non-invertibility condition in (1), for the non-invertible vectors contained in (6) one can write

$$h\left(h-\frac{a_1-a_2}{a_0}d\right)=0.$$

For the subcase $a_1 \neq a_2$, from the latter formula one can conclude that the set (7) contains $2p-1$ non-invertible vectors and we have subalgebra of the Ψ_1 type.

For the subcase $a_1 = a_2$, from the non-invertibility condition in (1) we have $h = 0$ and p non-invertible vectors of the form $(d, 0, 0, 0)$. Respectively, the order of multiplicative group of the subalgebra $\Psi_{\mathbf{A}}$ is equal to $\Omega_2 = p^2 - p = p(p-1)$. The multiplicative group is cyclic and is attributed to the Γ_2 type. Subalgebra containing a multiplicative group of the Γ_2 type is attributed to the Ψ_2 type.

III. Case $a_0 = 0$; $a_3 \neq 0$. The system (5) reduces to the system

$$\begin{cases} x_3 = 0; \\ x_2 = x_1 - \dfrac{a_1-a_2}{a_3}x_3. \end{cases}$$

The set of elements of the subalgebra $\Psi_{\mathbf{A}}$ is described by the following formula:

$$\mathbf{X}=\left(0, d, d-h\frac{a_1-a_2}{a_3}, h\right), \tag{8}$$

where d, $h = 0, 1, \ldots, p-1$. Taking into account the non-invertibility condition in (1), for the non-invertible vectors contained in (8) one can write

$$d\left(d-h\frac{a_1-a_2}{a_3}d\right)=0.$$

For the subcase $a_1 \neq a_2$, from the latter formula one can conclude that the set (8) contains $2p-1$ non-invertible vectors and we have subalgebra of the Ψ_1 type.

For the subcase $a_1 = a_2$, from the non-invertibility condition in (1) we have $d = 0$ and p non-invertible vectors of the form $(0, 0, 0, h)$. Respectively, the order of multiplicative group of the subalgebra $\Psi_{\mathbf{A}}$ is equal to $\Omega_2 = p^2 - p = p(p-1)$. The multiplicative group is cyclic and is attributed to the Γ_2 type. Subalgebra containing a multiplicative group of the Γ_2 type is attributed to the Ψ_2 type.

IV. Case $a_0 \neq 0$; $a_3 \neq 0$. The system (5) reduces to the system

$$\begin{cases} x_3 = x_0\dfrac{a_3}{a_0}; \\ x_2 = x_1 - \dfrac{a_1-a_2}{a_0}x_0. \end{cases}$$

The set of all elements of the subalgebra $\Psi_{\mathbf{A}}$ is described by the following formula:

$$\mathbf{X}=\left(d, h, h+\frac{a_2-a_1}{a_0}d, \frac{a_3}{a_0}d\right), \tag{9}$$

where d, $h = 0, 1, \ldots, p-1$. Taking into account the conditions (1), for the non-invertible vectors contained in (9) we have

$$\lambda d^2\frac{a_3}{a_0}=h^2+dh\frac{a_2-a_1}{a_0}. \tag{10}$$

From the quadratic equation (10) one has solution

$$h=\frac{a_1-a_2}{2a_0}d\pm\sqrt{\frac{(a_1-a_2)^2}{4a_0^2}d^2+\lambda d^2\frac{a_3}{a_0}}= \\ =\frac{a_1-a_2\pm\sqrt{\Delta}}{2a_0}d, \tag{11}$$

where

$$\Delta=(a_1-a_2)^2+4\lambda a_0 a_3. \tag{12}$$

Depending on the value Δ we have the following subcases.

IVa. Subcase Δ is quadratic residue modulo p ($\Delta \neq 0$). From (11) one can see that for every value of $d = 1, 2, \ldots, p-1$ we have two different values of h. This gives $2(p-1)$ nonzero non-invertible vectors. Totally, the number of non-invertible vectors is equal to $2p-1$, therefore the set (9) describes subalgebras of the Ψ_1 type containing multiplicative group of Γ_1 type.

IVb. Subcase Δ is quadratic non-residue modulo p ($\Delta \neq 0$). The equation (11) has no solutions and the set (9) contains only one non-invertible vector, namely, the zero vector (0, 0, 0, 0). The order of multiplicative group of the $\Psi_{\mathbf{A}}$ algebra is $\Omega_3 = p^2 - 1$. This group is attributed to the third type denoted as Γ_3. A subalgebra described by formula (9) represents a field that is isomorphic to $GF(p^2)$. Therefore, the groups of the Γ_3 type are cyclic.

IVc. Subcase $\Delta = 0$. From (11) one can see that for every value of $d = 0, 1, \ldots, p-1$ we have exactly one value of h. This gives p non-invertible vectors, therefore, the set (9) describes subalgebras of the Ψ_2 type containing multiplicative group of Γ_2 type, which has order equal to $\Omega_2 = p(p-1)$.

Like it has been shown in [18], one can prove the following formulas:

i) for the number η of different $\Psi_{\mathbf{A}}$ subalgebras: $\eta = p^2 + p + 1$;

ii) for the number η_1 of different subalgebras of the Ψ_1 type:

$$\eta_1=\frac{p(p+1)}{2}; \tag{13}$$

iii) for the number η_2 of different Ψ_2 subalgebras:

$$\eta_2 = p+1; \quad (14)$$

iv) for the number η_3 of different Ψ_3 subalgebras:

$$\eta_3 = \frac{p(p-1)}{2}. \quad (15)$$

The number of commutative groups of the types Γ_1, Γ_2 and Γ_3, in which the group operation is the vector multiplication, is defined by the formulas (13)–(15), correspondingly.

Proposed method

Into the base of the proposed method for development post-quantum digital signature algorithm is put the idea of using the vectors **G** and **H** contained in a hidden group to compute both the public key in the form of several vectors, for example, $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$ (which are pairwise non-permutable) and the signature element of the form of vector $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^r\mathbf{C}^{-1}$, where non-permutable vectors **B** and **C** are masking multipliers. The design of concrete signature scheme should be so that computation of the non-negative integers n and m allows one to get the value of **S**, which satisfies the signature verification equation with several occurrences of the signature element **S** that is non-permutable with every element of the public key. For example, in the case of two occurrences of the vector **S** one can use the verification equation of the following form

$$\mathbf{R} = (\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1)^e (\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2)^{e^2}, \quad (16)$$

where e is the signature randomization element in the form of a natural number computed as a hash function value from an electronic document M (to be signed) and the vector **R**. Including in the signature generation procedure a step of computation of the vector **R** in the form $\mathbf{R} = \mathbf{A}\mathbf{G}^k\mathbf{H}^t\mathbf{A}^{-1}$ provides potential possibility of finding the required values of the vector **S**.

To implement this method one needs to use a FNAA containing sufficiently large number of commutative groups. The proposed four-dimensional FNAA suits well as algabraic support of the method. Using the results on study its structure one can propose algorithms for generation of the vectors **G** and **H** defining the type of the hidden group (Γ_1, Γ_2, or Γ_3). In accordance with the formulas (13), (14), and (15), it appears that the most attractive is the use of hidden groups of the types Γ_1 and Γ_3. In the next section we describe a signature scheme in which the hidden group of the Γ_1 type is used. However, the number of the Γ_2 groups is also sufficiently large, therefore the use of a hidden group of the Γ_2 type seems to be not critical from the security point of view. Besides, there is no need to fix the hidden group type and the user can select it at stage of generating the public key.

Proposed candidate for post-quantum signature scheme

Suppose that the four-dimensional FNAA is defined over the field $GF(p)$ with prime characteristic $p = 2q + 1$, where q is a 256-bit prime. It is easy to generate such primes, including the case, when the structure of primes q and p is such that the multiplication modulo p and modulo q can be executed without using the arithmetic division operation (this item has practical significance to get significantly higher performance of the digital signature algorithm described below). In the developed signature scheme a hidden group of the Γ_1 type is used as a hidden group. To set the latter the following algorithm for generating its minimum generator system $\langle \mathbf{G}, \mathbf{H} \rangle$ is used.

1. Select at random an invertible vector $\mathbf{A} = (a_0, a_1, a_2, a_3)$ such that $a_1a_3 \neq \lambda a_0a_3$ and, using the formula (12), compute the value of Δ.

2. If $\Delta \neq 0$ is a quadratic non-residue, then go to step 1. Otherwise set integer variable $d = 1$.

3. Using the formula (11), compute the integer h.

4. Using the formula (9), compute the vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$.

5. If $a_1a_3 = \lambda a_0a_3$, then set the variable $d \leftarrow d + 1$ and go to step 3. Otherwise compute the vector $\mathbf{H} = \mathbf{X}^{(p-1)/q} = \mathbf{X}^2 = (h_0, h_1, h_2, h_3)$.

6. If $\mathbf{H} = \mathbf{E}$ or $(h_0, h_3) = (0, 0)$, then set the variable $d \leftarrow d + 1$ and go to step 3. Otherwise generate a primitive element $\alpha \in GF(p)$ and compute the scalar vector $\mathbf{L} = (0, \alpha, \alpha, 0)$.

7. Generate a random integer $k < q$ and compute the vector $\mathbf{G} = \mathbf{L}^k\mathbf{H}$. Then output the vectors **H** and **G**.

In line with the proposed method, the following procedure of computing the public key is proposed.

Algorithm for computation of the public key.

1. Generate private vectors **G** and **H** that compose a minimum generator system $\langle \mathbf{G}, \mathbf{H} \rangle$ of a of hidden group of the Γ_1 type (i. e. a primary group of order q^2, which possesses two-dimensional cyclicity).

2. Generate at random invertible vectors **A**, **B**, and **C** that are pairwise non-permutable, every of which in also non-permutable with each of the vectors **G** and **H**.

3. Generate uniformly random integers $u < q$ and $w < q$. Then compute the following four vectors serving as elements of the public key ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$):

$$\mathbf{Y}_1 = \mathbf{AG}^u\mathbf{B};\ \mathbf{Z}_1 = \mathbf{CHA}^{-1};$$

$$\mathbf{Y}_2 = \mathbf{AH}^w\mathbf{B};\ \mathbf{Z}_1 = \mathbf{CGA}^{-1}. \quad (17)$$

(Calculation of the vector $\mathbf{A}^{-1}$ can be executed as finding solution of the vector equation $\mathbf{AX} = \mathbf{E}$.)

The size of the public key is equal approximately to 4096 bits (512 bytes). The private key is the following set of values: u, w, **G**, **H**, **A**, **B**, and **C**. The size of the private key is equal approximately to 5632 bits (704 bytes).

Signature generation algorithm.

Suppose the owner of the public key wishes to sign an electronic document M. Then he can use the following algorithm.

1. Generate uniformly random integers $k < q$ and $t < q$ and compute the vector **R**:

$$\mathbf{R} = \mathbf{AG}^k\mathbf{H}^t\mathbf{A}^{-1}. \quad (18)$$

2. Using a pre-agreed hash function f, compute the first signature element $e = f(M, \mathbf{R})$.

3. Calculate the integers n and r as follows:

$$n = \frac{k - ue - e^2}{e + e^2} \bmod q;$$

$$r = \frac{t - we^2 - e}{e + e^2} \bmod q.$$

4. Calculate the second signature element in the form of vector **S**:

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^r\mathbf{C}^{-1}. \quad (19)$$

The size of the signature $(e, \mathbf{S})$ is equal approximately to 1280 bits (160 bytes). Computational complexity of the signature generation algorithm can be estimated as 4 exponentiation operations in the FNAA set by Table 1 (≈12 288 multiplications in $GF(p)$).

Signature verification algorithm.

To verify the signature $(e, \mathbf{S})$ assigned to document M one can use the following procedure.

1. Compute the vector **R***:

$$\mathbf{R}^* = \left(\mathbf{Y}_1\mathbf{SZ}_1\right)^e\left(\mathbf{Y}_2\mathbf{SZ}_2\right)^{e^2}. \quad (20)$$

2. Using a pre-agreed hash function f, compute the value $e^* = f(M, \mathbf{R}^*)$.

3. Compare the values e^* and e. If $e^* = e$, then the signature $(e, \mathbf{S})$ is accepted as genuine. Otherwise the signature is rejected.

Computational complexity of the signature verification algorithm can be estimated as 2 exponentiations in the FNAA used as algebraic support (≈6144 multiplications modulo p).

Proof of the signature scheme correctness.

Consider a signature $(e, \mathbf{S})$ to document M, which is computed correctly in full correspondence with the signature generation procedure, while using the correct signer's private key. In line with the signature verification algorithm, for the signature $(e, \mathbf{S})$ one can write the following:

$$\mathbf{R}^* = \left(\mathbf{Y}_1\mathbf{SZ}_1\right)^e\left(\mathbf{Y}_2\mathbf{SZ}_2\right)^{e^2} =$$

$$= \left(\mathbf{AG}^u\mathbf{BB}^{-1}\mathbf{G}^n\mathbf{H}^r\mathbf{C}^{-1}\mathbf{CHA}^{-1}\right)^e \times$$

$$\times \left(\mathbf{AH}^w\mathbf{BB}^{-1}\mathbf{G}^n\mathbf{H}^r\mathbf{C}^{-1}\mathbf{CGA}^{-1}\right)^{e^2} =$$

$$= \left(\mathbf{AG}^{u+n}\mathbf{H}^{r+1}\mathbf{A}^{-1}\right)^e\left(\mathbf{AH}^{w+r}\mathbf{G}^{n+1}\mathbf{A}^{-1}\right)^{e^2} =$$

$$= \left(\mathbf{AG}^{(u+n)e}\mathbf{H}^{(r+1)e}\mathbf{A}^{-1}\right)\left(\mathbf{AH}^{(w+r)e^2}\mathbf{G}^{(n+1)e^2}\mathbf{A}^{-1}\right) =$$

$$= \mathbf{AG}^{(u+n)e+(n+1)e^2}\mathbf{H}^{(r+1)e+(w+r)e^2}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^{n\left(e+e^2\right)+eu+e^2}\mathbf{H}^{r\left(e+e^2\right)+we^2+e}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^{\frac{k-eu-e^2}{e+e^2}\left(e+e^2\right)+eu+e^2}\mathbf{H}^{\frac{k-we^2-e}{e+e^2}\left(e+e^2\right)+we^2+e}\mathbf{A}^{-1} =$$

$$= \mathbf{AG}^k\mathbf{H}^t\mathbf{A}^{-1} = \mathbf{R} \Rightarrow$$

$$\Rightarrow f\left(M, \mathbf{R}^*\right) = f\left(M, \mathbf{R}\right) \Rightarrow e^* = e.$$

The final equality means the input signature passes the verification procedure as a genuine signature, i. e., the signature scheme performs correctly.

Discussion

The developed signature algorithm uses the exponentiation operation in a hidden commutative group and powers of these operations are secret, like in the known HDLP-based signature schemes [18–20]. However, in the latter schemes for computing a signature it is sufficient to use only the values of the said powers, while in the signature scheme described in the previous section, without using the secret vectors **G**, **H**, **A**, **B**, and **C** a valid signature cannot be directly generated. This is due to a new mechanism used for masking the hidden group, which is presented by formulas (17).

If a potential forger knows the powers u and w and the minimum generator system of the hidden group $\langle \mathbf{G}, \mathbf{H} \rangle$, then he will be able to forge signatures as follows:

1. Compute the vectors $\mathbf{U} = \mathbf{G}^u$ and $\mathbf{W} = \mathbf{H}^w$.

2. Using the public key elements and considering the vectors $\mathbf{A}'$, $\mathbf{B}'^{-1}$, and $\mathbf{C}'$ as unknowns compose the following system of four linear vector equations:

$$\begin{cases} \mathbf{Y}_1\mathbf{B}'^{-1} = \mathbf{A}'\mathbf{U}; \\ \mathbf{Z}_1\mathbf{A}' = \mathbf{C}'\mathbf{H}; \\ \mathbf{Y}_2\mathbf{B}'^{-1} = \mathbf{A}'\mathbf{W}; \\ \mathbf{Z}_2\mathbf{A}' = \mathbf{C}'\mathbf{G}. \end{cases} \quad (21)$$

[The system (21) reduces to a system of 16 linear equations in $GF(p)$ with 12 unknown coordinates of the vectors $\mathbf{A}'$, $\mathbf{B}'^{-1}$, and $\mathbf{C}'$. Evidently, the system (21) has a solution, namely, $\mathbf{A}' = \mathbf{A}$, $\mathbf{B}'^{-1} = \mathbf{B}^{-1}$, and $\mathbf{C}' = \mathbf{C}$.]

3. Solve the system (21). Then, using the found values of $\mathbf{A}$, $\mathbf{B}^{-1}$, $\mathbf{C}$ and signature generation procedure from previous section, generate a signature. [If the system (21) has a solution different from $(\mathbf{A}', \mathbf{B}'^{-1}, \mathbf{C}') = (\mathbf{A}, \mathbf{B}^{-1}, \mathbf{C})$, then it will also provide generation of a valid signature.]

Currently, the proposed method and the algorithm of the case is quite new and is still unclear what way the signature scheme can be efficiently attached, when no element of the private key is known for the attacker. One can propose the next general approach for forging a signature, which consists in finding an alternative representation of the public key, i. e., finding the values $\mathbf{A}'$, $\mathbf{B}'$, $\mathbf{C}'$, $\mathbf{G}'$, $\mathbf{G}_w$, $\mathbf{H}'$, $\mathbf{H}_w$, where $\mathbf{G}'$, $\mathbf{G}_w$, $\mathbf{H}'$, and $\mathbf{H}_w$ are pairwise permutable vectors, such that they satisfy the following system of the vector equations

$$\begin{cases} \mathbf{Y}_1\mathbf{B}'^{-1} = \mathbf{A}'\mathbf{G}_u; \\ \mathbf{Z}_1\mathbf{A}' = \mathbf{C}'\mathbf{H}'; \\ \mathbf{Y}_2\mathbf{B}'^{-1} = \mathbf{A}'\mathbf{H}_w; \\ \mathbf{Z}_2\mathbf{A}' = \mathbf{C}'\mathbf{G}'. \end{cases} \quad (22)$$

One can easily show that for such alternative representation of the public key a valid signature can be calculated using a signature verification algorithm which is similar to that described in previous section. However, all of the equations in (22) contain products of a couple of unknowns, therefore, solving the system (22) appears to be a computationally hard problem.

Indeed, the requirement of permutability on the unknown vectors $\mathbf{G}'$, $\mathbf{G}_w$, $\mathbf{H}'$, and $\mathbf{H}_w$ adds three vector equations to (22) and one gets the system of seven equations in the FNAA, which reduces to the system of 28 quadratic equations in $GF(p)$ with 28 unknowns. Finding a solution for such systems is a computationally difficult problem [21, 22]. One can suppose that the computational complexity of finding a solution of the system (22) defines the security level of the proposed signature scheme.

Development of the methods for solving the system (22) and estimation of their computational complexity is an independent research task. We would only like to note that improving the complexity of the solution of the mentioned computational problem can be achieved by increasing the size of the prime p and/or increasing the public key size. The latter can be implemented by calculating two additional public-key elements $\mathbf{Y}_3$ and $\mathbf{Z}_3$, using additional private integers $b < q$ and $d < q$, which are also uniformly random values: $\mathbf{Y}_3 = \mathbf{A}\mathbf{H}^b\mathbf{B}$; $\mathbf{Z}_3 = \mathbf{C}\mathbf{G}^d\mathbf{A}^{-1}$. Respectively, such modification of the public key requires updating the verification equation. For example the following one can be used:

$$\mathbf{R} = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^e \left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e^2} \left(\mathbf{Y}_3\mathbf{S}\mathbf{Z}_3\right)^{e+e^2}. \quad (23)$$

(In line with the method presented in Section "Proposed method" and signature algorithm described in previous Section "Proposed candidate for post-quantum signature scheme", the reader can easily update the signature generation procedure in correspondence with the modified versions of the public key and verification equation.)

The use of a hypothetical quantum computer is not effective for solving the specified problem of solving the system of equations (22). In addition, when analyzing the security of the proposed digital signature algorithm, there is no need to solve DLP or HDLP, despite the fact that the exponential operations play a significant role in the developed algorithm. For example, in contrast to the known

■ ***Table 2***. Comparison with some known post-quantum digital signature algorithms

Signature scheme	Signature size, byte	Public key size, byte	Signature generation rate, arb. un.	Signature verification rate, arb. un.
Falcon [24]	1280	1793	50	25
Dilithium [25]	2701	1472	15	2
HDLP-based [19]	192	768	50	80
HDLP-based [20]	192	512	40	80
HDLP-based [26]	96	576	30	40
Proposed	160	512	140	290

HDLP-based algorithms in which the exponentiations plays a fundamental role, the proposed algorithm can be modified in such a way that, when generating a public key, exponentiation operations will not be used.

Thus, in comparison with the known HDLP-based algorithms, the introduced method and the developed digital signature algorithm is characterized in that the appearance of computationally efficient algorithms for solving DLP and HLP does not mean that the signature algorithm has ceased to be safe. In this connection one can notice that the presence of a large-sized prime divisor in the decomposition of the order of the multiplicative group of the $GF(p)$ field is not a critical requirement. This feature simplifies the implementation of the algorithm when using the FNAA, set over a field $GF(2^s)$, as algebraic support.

A draft comparison of the developed signature algorithm with two finalists (Falcon and Dilithium) of the NIST competition [23] and some of the HDLP-based signature schemes are presented in Table 2. The algorithm proposed in this article has a significant advantage in the sizes of the signature and public key. Besides, it has higher performance.

Conclusion

Like in a number of known HDLP-based signature schemes, in the developed algorithm a hidden group is used, but the latter algorithm more precisely should be called an algorithm with a hidden group. The proposed method can be used to develop many different algorithms with a hidden group, which are attractive as candidates for practical post-quantum signature algorithms.

The results of this article can be considered as a starting point for the formation of a new concept of the development of post-quantum digital signature algorithms on non-commutative algebras, in framework of which one will be able potentially to reduce significantly the size of the public key and the signature while simultaneous increasing performance.

Financial support

This research is partially supported by RFBR (project No 21-57-54001-Вьет_а) and budget theme No FFZF-2022-0007.

References

1. 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.
2. 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.
3. 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.
4. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
5. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
6. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
7. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
8. *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 24 November 2021).
9. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
10. Moldovyan D. N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. *Computer Science Journal of Moldova*, 2019, vol. 27, no. 1(79), pp. 56–72.
11. Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions. *Prikl. Diskr. Mat.*, 2018, no. 40, pp. 23–33. doi:10.17223/20710410/40/3
12. Agibalov G. P. ElGamal cryptosystems on Boolean functions. *Prikl. Diskr. Mat.*, 2018, no. 42, pp. 57–65. doi:10.17223/20710410/42/4
13. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. *Designs, Codes and Cryptography*, 2017, vol. 82, no. 1–2, pp. 469–493.
14. Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem. *Prikl. Diskr. Mat.*, 2019, no. 45, pp. 33–43. doi:10.17223/20710410/45/4
15. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., and Liu Y. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. Ser. NIST Interagency/Internal Report (NISTIR). National Institute of Standards and Technology, Gaithersburg, MD, 2019. https://doi.org/10.6028/NIST.IR.8240. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (accessed 24 November 2021).

16. Moody D., Alagic G., Apon D., Cooper D., Dang Q., Kelsey J., Liu Y., Miller C., Peralta R., Perlner R., Robinson A., Smith-Tone D., and Alperin-Sheriff J. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. Ser. NIST Interagency/Internal Report (NISTIR). National Institute of Standards and Technology, Gaithersburg, MD, 2020. Available at: https://doi.org/10.6028/NIST.IR.8309 (accessed 24 November 2021).
17. Moody D. *NIST Status Update on the 3rd Round*. National Institute of Standards and Technology, Gaithersburg, MD, 2020. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (accessed 24 November 2021).
18. Moldovyan D. N. A practical digital signature scheme based on the hidden logarithm problem. *Computer Science Journal of Moldova*, 2021, vol. 29, no. 2(86), pp. 206–226.
19. Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2020, vol. 16, iss. 4, pp. 455–461. doi: 10.21638/11701/spbu10.2020.410
20. 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
21. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.
22. Jintai D., Dieter S. *Multivariable Public Key Cryptosystems*. 2004. Available at: https://eprint.iacr.org/2004/350.pdf (accessed 24 November 2021).
23. *Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed 24 November 2021).
24. *Fast-Fourier lattice-based compact signatures over NTRU*. Available at: https://falcon-sign.info/ (accessed 24 November 2021).
25. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*. https://eprint.iacr.org/2017/633.pdf Available at: https://pq-crystals.org/dilithium/index.shtml (accessed 24 November 2021).
26. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A new design of the signature schemes based on the hidden discrete logarithm problem. *Quasigroups and Related Systems*, 2021, vol. 29, no. 1, pp. 97–106.

УДК 003.26
doi:10.31799/1684-8853-2022-1-44-53

Новый способ построения постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах

А. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0001-5480-6016, maa1305@yandex.ru
Д. Н. Молдовян[a], канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048
[a]Санкт-Петербургский Федеральный исследовательский центр РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка практичных постквантовых схем подписи является одним из текущих вызовов в области криптографии. Недавно предложены несколько кандидатов на постквантовые схемы цифровой подписи, в которых используется операция экспоненцирования в скрытой группе, содержащейся в некоммутативной алгебре. Поиск новых механизмов использования скрытой группы при разработке схем цифровой подписи, стойких к квантовым атакам, представляет существенный практический интерес. **Цель:** разработать новый способ построения постквантовых алгоритмов цифровой подписи на конечных некоммутативных ассоциативных алгебрах. **Результаты:** предложены новый способ разработки алгоритмов цифровой подписи на некоммутативных алгебрах и новая четырехмерная некоммутативная алгебра, заданная над простым полем $GF(p)$, в качестве носителя указанных алгоритмов. Благодаря заданию операции векторного умножения по прореженным таблицам умножения базисных векторов обеспечивается повышение производительности алгоритмов. Изучение строения алгебры показало, что она представима в виде множества коммутативных подалгебр, попарно пересекающихся строго в множестве всех скалярных векторов. Предложенный метод отличается использованием одного из элементов подписи $(e, \mathbf{S})$ в виде вектора $\mathbf{S}$, вычисляемого как замаскированное произведение степеней двух элементов $\mathbf{G}$ и $\mathbf{H}$ скрытой коммутативной группы: $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{r}\mathbf{C}^{-1}$, где неперестановочные векторы $\mathbf{B}$ и $\mathbf{C}$ являются маскирующими множителями; натуральные числа n и r вычисляются в зависимости от подписываемого документа M и открытого ключа. Пара $<\mathbf{G}, \mathbf{H}>$ составляет базис скрытой группы. Уравнение верификации подписи имеет вид $\mathbf{R} = (\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1)^{e}(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2)^{e^2}$, где попарно неперестановочные векторы $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ и $\mathbf{Z}_2$ являются элементами открытого ключа; натуральное число e вычисляется в зависимости от значения M и вектора $\mathbf{R}$. **Практическая значимость:** благодаря достаточно малым размерам подписи и открытого ключа и высокой производительности разработанная схема цифровой подписи представляет интерес как практичный постквантовый алгоритм подписи. Предложенный метод может быть использован для разработки стандарта на постквантовый алгоритм цифровой подписи.

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

Для цитирования: Moldovyan A. A., Moldovyan D. N., Moldovyan N. A. A novel method for developing post-quantum digital signature algorithms on non-commutative associative algebras. *Информационно-управляющие системы*, 2022, № 1, с. 44–53. doi:10.31799/1684-8853-2022-1-44-53
For citation: Moldovyan A. A., Moldovyan D. N., Moldovyan N. A. A novel method for developing post-quantum digital signature algorithms on non-commutative associative algebras. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 44–53. doi:10.31799/1684-8853-2022-1-44-53

Финансовая поддержка
Исследование частично поддержано РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темой № FFZF-2022-0007.

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.).

Текст рукописи должен быть оригинальным, а цитирование и самоцитирование корректно оформлено.

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.

Простые **формулы** набирайте в Word, сложные с помощью редактора Mathtype или Equation. 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 в Mathtype никогда не пользуйтесь вкладкой Other, Smaller, Larger, 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; пробелы в формуле ставьте только после запятых при перечислении с помощью Ctrl+Shift+Space (пробел); не отделяйте пробелами знаки: + = − ×, а также пространство внутри скобок; для выделения греческих символов в Mathtype полужирным начертанием используйте Style → Other → bold.

Для набора формул в Word никогда не используйте вкладки: «Уравнение», «Конструктор», «Формула» (на верхней панели: «Вставка» — «Уравнение»), 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.

Подробнее см. pdf-файл «Правила подготовки рукописей» (стр. 11) на сайте https://guap.ru/ric

Иллюстрации:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Adobe Illustrator (*.ai); Coreldraw (*.cdr, версия не выше 15); Excel (*.xls); Word (*.docx); AutoCad, Matlab (экспорт в PDF, EPS, SVG, WMF, EMF); Компас (экспорт в PDF), веб-портал DRAW.IO (экспорт в PDF);

— 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, *.jpg 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 «Руководство 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