Journal of Computer Science and Cybernetics, V.37, N.4 (2021), 495–509
DOI 10.15625/1813-9663/37/4/16023

POST-QUANTUM BLIND SIGNATURE PROTOCOL ON NON-COMMUTATIVE ALGEBRAS

MINH N.H[1,*], MOLDOVYAN D.N[2], MOLDOVYAN N.A[2], KOSTINA A.A[2], MINH L.Q[3], HUONG L.H[4], GIANG N.L[5]

[1]*Institute of Cryptographic Science and Technology, Ha Noi, Viet Nam*
[2]*St. Petersburg Federal Research Center of the Russian Academy of Sciences, Russia*
[3]*Information Technology Institute, Vietnam National University, 144 Xuan Thuy Street, Cau Giay District, Ha Noi, Viet Nam*
[4]*Academy of Cryptography Techniques, 141 Chien Thang Street, Tan Trieu Ward, Thanh Tri District, Ha Noi, Viet Nam*
[5]*Institute of Information Technology, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet Street, Cau Giay District, Ha Noi, Viet Nam*

Abstract. A method for constructing a blind signature scheme based on a hidden discrete logarithm problem defined in finite non-commutative associative algebras is proposed. Blind signature protocols are constructed using four-dimensional and six-dimensional algebras defined over a ground finite field $GF(p)$ and containing a global two-sided unit as an algebraic support. The basic properties of the used algebra, which determine the choice of protocol parameters, are described.

Keywords. Information security, post-quantum cryptography, digital signature, blind signature, finite associative algebra, non-commutative algebra.

1. INTRODUCTION

Modern standards of electronic digital signature with a public key, adopted in the leading countries of the world, are based on the computational problem of discrete logarithm (DL) [1], however, significant progress in the development of quantum computing and the creation of experimental computers for which polynomial algorithms for solving the DL problem and the factorization problem (FP) have been developed [2, 3]. That result caused the urgent problem of the development of post-quantum two-key cryptoschemes, including electronic digital signature (EDS) schemes and blind EDS protocols. Post-quantum cryptoschemes,

Dedicated to Professor Phan Dinh Dieu on the occasion of his 85th birth anniversary.

*Corresponding author.
E-mail addresses: hieuminhmta@gmail.com (Minh N.H); nmold@mail.ru (Moldovyan D.N, Moldovyan N.A, Kostina A.A); lqminh78@gmail.com (Minh L.Q); lehaihuongvn@actvn.edu.vn (Huong L.H); nl-giang75@gmail.com (Giang N.L).

algorithms and protocols are those that are resistant to attacks using hypothetical (at the moment) quantum computers capable of solving FP and DL problem in polynomial time.

The response to the said problem was the announcement by the US National Institute of Standards and Technology (NIST) in December 2016 of a worldwide competition for the development of post-quantum public-key agreement and digital signature schemes with the aim of adopting post-quantum cryptographic standards by 2024 [4], as well as 2010 to 2020 annual international thematic conference "Post-Quantum Cryptography" [5].

One of the promising approaches to the development of post-quantum public-key cryptoschemes is the use of the computational difficulty of the hidden discrete logarithm problem (HDLP) specified in finite non-commutative associative algebras (FNAA) [6]. Resistance to quantum attacks of the HDLP is justified in [7, 8]. On the basis of HDLP, public-key agreement schemes [9], commutative ciphers [10] and EDS schemes [11, 12] have been developed, which are of interest as practical post-quantum cryptoschemes, free from a number of shortcomings of their counterparts participating in the NIST competition. It is of interest to develop cryptoschemes of other types based on HDLP.

This article proposes a method for constructing blind EDS schemes using the computational complexity of the HDLP and describes a post-quantum blind signature protocol implemented on its basis. As an algebraic carrier of the developed protocol, we used four-dimensional and six-dimensional FNAA, containing a global two-sided unit.

2. THE CONCEPT AND APPLICATION OF A BLIND DIGITAL SIGNATURE

The concept of a blind digital signature was first proposed in [13] to solve problems of ensuring the non-traceability (anonymity) of users that arise in some special information technologies, for example, electronic money systems and secret electronic voting. Blind EDS is calculated by the signer in the process of interacting with some user (client). The signer uses his personal private key to calculate the blind signature and transfers the latter to the client. The latter computes, based on the blind signature, the authentic signature of the signer to some document to which the signer does not have access during the protocol execution. The signature received by the client is standard and its authenticity is verified according to the same algorithm as the verification of a regular signature.

For the first time, the blind signature protocol was implemented on the basis of the RSA signature scheme [13] based on the FP. Subsequently, blind signature protocols based on the DL problem have been proposed [14]. In both cases, the anonymity of the client is ensured by the fact that during the protocol he introduces one or two random blinding factors into the blind signature. After receiving a blind signature from the signer, the client removes the blinding factors, thereby calculating the true signature.

3. THE USED ALGEBRAIC SUPPORTS

3.1. Definition of finite non-commutative associative algebras

An arbitrary vector A of some finite m-dimensional vector space defined over a finite field $GF(p)$, can be written as an ordered set of elements of the field $GF(p)$: $A = (a_0, a_1, \ldots, a_{m-1})$ or as a sum of its component: $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $\mathbf{e}_i$ are basis vectors; $a_i \in GF(p)$ are

coordinated of the vector. A vector space in which, in addition to the operations of addition of vectors and multiplication of a vector by a scalar, an operation of multiplication of two vectors is defined, which has the property of distributivity with respect to the operation of addition, is called algebra.

The vector multiplication operation $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_i \mathbf{e}_j$ is usually determined by the rule of multiplying each component of the first vector with each component of the second vector, namely, by the following formula

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

in which each product of the form $\mathbf{e}_i \circ \mathbf{e}_j$ must be replaced by a one-component vector $\lambda \mathbf{e}_k$, selected from the so-called multiplication table of basis vectors (MTBV), where $\lambda \in GF(p)$ is called structural constant. In the case $\lambda = 1$ only basis vector $\mathbf{e}_k$ is indicated in the MTBV. Left multiplier in the product $\mathbf{e}_i \circ \mathbf{e}_j$ specifies the row and the right one specifies the column, the intersection of which indicates the cell containing the value $\lambda \mathbf{e}_k$.

If the operation of multiplication has the properties of non-commutativity and associativity, then the case of specifying the FNAAs is realized [15, 12]. For the dimensions $m = 4$ and $m = 6$ the MTBV shown as tables 1 and 2 set the FNAAs used as algebraic carriers of blind signature protocols. These algebras contain a global two-sided unit and local units of various types related to subsets of non-invertible vectors. Global two-sided units are elements of algebra that act as two-sided units on all elements of the FNAA. Local units are elements of an algebra that act as unit elements within subsets of algebra element [16].

3.2. Four-dimensional FNAA

The algebra with the multiplication of elements given in Table 1 contains a two-sided global unit E, which is described by the following formula

$$E = \left(\frac{1}{\lambda - 1}, \frac{1}{1 - \lambda}, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1} \right).$$

The validity in the above formula is proved by direct substitution of the value E instead of the unknown X in the vector equations $X \circ A = A$ and $A \circ X = A$ for an arbitrary value A.

For use as an algebraic support, it is important that the FNAA contains vectors of a sufficiently large prime order. To implement the latter, the four-dimensional FNAA will be defined over the field $GF(p)$, whose characteristic is equal to a prime number $p = 2q + 1$, where q is a 512-bit prime. The generation of the required primes p is done by generating many different 512-bit primes q and testing the values $p = 2q + 1$ for primality.

Table 1: Setting a 4-dimensional FNAA with a global two-sided unit ($\lambda \neq 1$)

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

When specifying new versions of HDLP and building EDS protocols, unit elements of various types will be used, which are contained in the FNAAs applied as carriers of signature schemes. In the algebra discussed in this section, there are many local left-sided, right-sided, and two-sided units. The condition of invertibility of some vector $A = (a_0, a_1, a_2, a_3)$ is determined by the fact that vector equations of the forms $X \circ A = E$ and $A \circ X = E$ have a unique solution. The first of these equations reduces to the following system of four linear equations with unknowns x_0, x_1, x_2, and x_3, representing the coordinates of the vector X

$$\begin{cases} (\lambda a_0 + a_2)x_0 + (a_0 + a_2)x_1 & = \dfrac{1}{\lambda - 1}, \\ (\lambda a_1 + a_3)x_0 + (a_1 + a_3)x_1 & = \dfrac{1}{1 - \lambda}, \\ (\lambda a_0 + a_2)x_2 + (a_0 + a_2)x_3 & = \dfrac{1}{1 - \lambda}, \\ (\lambda a_1 + a_3)x_2 + (a_1 + a_3)x_3 & = \dfrac{\lambda}{\lambda - 1}. \end{cases} \tag{1}$$

It is easy to see that system (1) splits into two independent systems of two equations, the main determinant of each of which is equal to the same value

$$\Delta = (1 - \lambda)\,(a_1 a_2 - a_0 a_3)\,. \tag{2}$$

From formula (2), we obtain the following invertibility condition for the vector $A = (a_0, a_1, a_2, a_3)$

$$a_1 a_2 \neq a_0 a_3. \tag{3}$$

Consider the non-invertible vectors $G = (g_0, g_1, g_2, g_3)$, for which the equality $g_1 g_2 = g_0 g_3$ holds true. The FNAA under consideration contains a set of elements that act on some given non-invertible vector G as left-sided local units. Many such units can be found by solving a vector equation of the form

$$X \circ G = G, \tag{4}$$

which reduces to solving the following system of four linear equations

$$\begin{cases} (\lambda g_0 + g_2)x_0 + (g_0 + g_2)x_1 & = g_0, \\ (\lambda g_1 + g_3)x_0 + (g_1 + g_3)x_1 & = g_1, \\ (\lambda g_0 + g_2)x_2 + (g_0 + g_2)x_3 & = g_2, \\ (\lambda g_1 + g_3)x_2 + (g_1 + g_3)x_3 & = g_3. \end{cases} \tag{5}$$

System (5) splits into two independent systems of two equations with two unknowns, each of which has p different solutions giving p^2 different solutions of the system (5), which describe the following set of local left-sided units L corresponding to the vector G and all possible powers G^k

$$L = (l_0, l_1, l_2, l_3) = \left(x_0, \frac{g_0 - (\lambda g_0 + g_2)x_0}{g_0 + g_2}, x_2, \frac{g_2 - (\lambda g_0 + g_2)x_2}{g_0 + g_2}\right), \tag{6}$$

where $x_0,\ x_2 = 0, 1, \ldots, p - 1$. The set of local left-sided units (6) includes $p^2 - p$ invertible vectors and p non- invertible vectors.

Set of right-sided local units corresponding to a vector G and to vectors G^k, can be found as solutions to the vector equation

$$G \circ X = G. \tag{7}$$

Vector equation (7) is reduced to the following system of four linear equations

$$\begin{cases} (\lambda g_0 + g_1)x_0 + (g_0 + g_1)x_2 & = g_0, \\ (\lambda g_2 + g_3)x_0 + (g_2 + g_3)x_2 & = g_2, \\ (\lambda g_0 + g_1)x_2 + (g_0 + g_1)x_3 & = g_1, \\ (\lambda g_2 + g_3)x_2 + (g_2 + g_3)x_3 & = g_3. \end{cases} \tag{8}$$

System (8) splits into two independent systems of two equations with two unknowns, each of which has p solutions that define p^2 different solutions of the system (8). The latter determine the following set of right-sided local units R

$$R = (r_0, r_1, r_2, r_3) = \left(x_0, x_1, \frac{g_0 - (\lambda g_0 + g_1)x_0}{g_0 + g_1}, \frac{g_1 - (\lambda g_0 + g_1)x_1}{g_0 + g_1} \right), \tag{9}$$

where $x_0,\ x_1 = 0, 1, \ldots, p-1$. The set of local right-sided units (9) includes $p^2 - p$ invertible vectors and p non-invertible vectors.

The intersection of sets (6) and (9) describes p different two-sided local units E, corresponding to vectors of the form G^k (for $k = 1, 2, \ldots$). This intersection of sets is described by the following formula

$$E = \left(x_0, \frac{g_0 - (\lambda g_0 + g_2)x_0}{g_0 + g_2}, \frac{g_0 - (\lambda g_0 + g_1)x_0}{g_0 + g_1}, \frac{g_1 g_2 - \lambda g_0^2}{(g_0 + g_1)(g_0 + g_2)} + \frac{(\lambda g_0 + g_1)(\lambda g_0 + g_2)x_0}{(g_0 + g_1)(g_0 + g_2)} \right), \tag{10}$$

where $x_0 = 0, 1, 2, \ldots, p-1$. The set (10) includes $p-1$ invertible vectors and unique vector E_G that is a non-invertible element of the algebra. The vector E_G is the unit of the cyclic group generated by all possible all possible powers of the vector G. The E_G value can be calculated using the formula $E_G = G^{\omega}$ where ω is a devisor of the number $p^2 - 1$. From expressions (6) and (9) it is easy to obtain one more formula for calculating the value E_G

$$E_G = \left(k, \frac{g_1}{g_0}k, \frac{g_0 - (\lambda g_0 + g_1)k}{g_0 + g_1}, \frac{g_0 g_1 - (\lambda g_0 + g_1)g_1 k}{g_0^2 + g_0 g_1} \right), \tag{11}$$

where $k = g_0^2 \left(\lambda g_0^2 + g_0 g_1 + g_0 g_2 + g_1 g_2 \right)^{-1}$. Finding the value of E_G by formula (11) has a significantly lower computational complexity.

3.3. Six-dimensional FNAA

The 6-dimensional FNAA used in this article was obtained as a particular representative of the FNAA class of arbitrary even dimension, given by the general method proposed in [15]. This FNAA is defined over the field $GF(p)$, whose characteristic is equal to a prime number $p = 2q + 1$, where q is a 512-bit prime number.

The global two-sided unit of this six-dimensional FNAA is the vector $E = (1, 0, 0, 0, 0, 0)$. The invertible 6-dimensional vectors of a this algebra have the order ω, that is a divisor of the integer $p^2 - 1$, includingly the value $p^2 - 1$. Finding vectors having order $\omega = p^2 - 1$ is carried out by choosing random invertible vectors Q and checking that the condition $Q^{\frac{p^2-1}{d}} \neq E$ holds true for all prime divisors $d \mid p^2 - 1$.

When developing a blind signature protocol on a 6-dimensional FNAA, non-invertible vectors that have a local order equal to a prime number q of large size and a value of the structural coefficient λ, which is a quadratic residue in $GF(p)$, are used. In [15], the existence of two types of non-invertible vectors was shown. Non-invertible vectors $G = (g_0, g_1, g_2, g_3, g_4, g_5)$ of the first type satisfy the following condition

Table 2: Setting a 6-dimensional FNAA over $GF(p)$ by method [15]

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e_3}$	$\lambda\mathbf{e_2}$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e_5}$	$\lambda\mathbf{e_4}$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e_2}$	$\mathbf{e_3}$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e_1}$	$\lambda\mathbf{e_0}$

$$(g_0+g_2+g_4)^2=\lambda(g_1+g_3+g_5)^2. \tag{12}$$

Non-invertible vectors $G=(g_0,g_1,g_2,g_3,g_4,g_5)$ of the second type satisfy the following condition

$$(g_0-g_2)^2+(g_0-g_4)^2+(g_2-g_4)^2=\lambda((g_1-g_3)^2+(g_1-g_5)^2+(g_3-g_5)^2). \tag{13}$$

If the structure coefficient λ is a quadratic non-residue in the field $GF(p)$, then there is a single non-invertible vector $(0,0,0,0,0,0)$ of the first type. If the structure coefficient λ is a quadratic residue, then there are a set of non-invertible vectors of both the first and second types. For large sizes of the characteristic of the field $GF(p)$, the probability of obtaining a non-invertible vector by randomly choosing 6-dimensional vectors is very low; therefore, to find non-invertible vectors in the considered 6-dimensional FNAA in [15] algorithms for generating non-invertible vectors are proposed, in which relations (12) and (13) are used.

The non-invertible 6-dimensional vectors of the considered FNAA are of the order ω equal to all possible divisors of the number p^2-1, includingly the value p^2-1. Finding non-invertible vectors of order $\omega=q$ is performed by choosing random non-invertible vectors N and checking whether the condition $G=N^{\frac{p^2-1}{q}}\neq E$ holds true.

4. BLIND SIGNATURE PROTOCOLS

4.1. Initial signature scheme on the four-dimensional algebra

We will assume that the 4-dimensional FNAA used as an algebraic carrier of the proposed digital signature scheme is given over a ground finite field $GF(p)$, where a 512-bit prime with the structure $p=2q+1$, is used as a characteristic p, where q is a prime number of a large size, for example equal to 512 bits. To construct a post-quantum EDS scheme with the possibility of performing a formal reductionist security proof proposed earlier in [17] for EDS schemes based on the computational difficulty of the DL problem, we will use the Schnorr signature scheme [18] as a prototype. Unlike the prototype, in which the base cyclic group is explicitly set as an algebraic carrier of the cryptoscheme, in the EDS scheme based on the HDLP the base cyclic group is hidden and the EDS authentication includes calculations in two other cyclic groups. The values obtained in the latter are interconnected through the values of the elements of the basic cyclic group. Due to the said interconnection the correct operation of the EDS scheme based on the proposed version of the HDLP is ensured.

The mutual commutativity of masking operations with the exponentiation operation is used in the following procedure for generating a public key in the form of a triplet of vectors (Y,Z,T):

1. Generating various random coordinate values g_0, g_1, g_2 and g_3, satisfying the condition $g_1 g_2 = g_0 g_3$, choose a random non-invertible vector G, whose local order is equal to $p-1$.
2. Using the formula (10) and choosing random values of the variable x_0, generate an invertible vector Q^* of the order q, which is a local two-sided unite of the non-invertible vector G.
3. Generate a random natural number $\alpha < q$ that is a primitive element in the finite field $GF(p)$ and compute an invertible vector Q of the order q, which possesses the property if permutability with the non-invertible vector G: $Q = \alpha^{\frac{p-1}{q}} Q^*$. One can easily see that the vector Q has order equal to the prime q.
4. Generate two random 4-dimensional vectors A and B of the order q, for which the no-equalities $A \circ B \neq B \circ A$, $A \circ Q \neq Q \circ A$, and $B \circ Q \neq Q \circ B$, hold true.
5. Generate at random natural number $x < q$ and calculate the first element of the public key in the form of the vector $Y = A \circ Q^x \circ A^{-1}$.
6. Calculate the second element of the public key in the form of the vector $Z = B \circ Q \circ B^{-1}$.
7. Calculate the third element of the public key in the form of the vector $T = A \circ G \circ B^{-1}$.

When generating the public key in the form of a triplet of vectors (Y, Z, T), the following random elements were selected, which are secret parameters: the generator of the basic cyclic group Q, non-invertible vector G (permutable with vector Q), invertible vectors A and B, and natural number x. It is assumed that after the formation of the public key, its owner only needs to store as his private secret key the values x, Q, A and $D = G \circ B^{-1}$, which are used in the digital signature generation procedure.

In the proposed initial signature scheme, the procedure for generating a signature in the form of a pair of numbers (e, s) to some electronic document M includes the following steps:

1. Generate at random an integer $k < q$.
2. Calculate the vector-fixator $V = A \circ Q^k \circ D$.
3. Calculate the first signature element in the form of number $e = F_h(M, V)$, where F_h is a specified hash function.
4. Calculate the second signature element in the form of the number s

$$s = k - ex \mod q.$$

The procedure for verifying the authenticity of the signature (e, s) to the document M is performed using the public key (Y, Z, T) as follows:

1. Calculate the vector $\tilde{V} = Y^e \circ T \circ Z^s$.
2. Calculate the value $\tilde{e} = F_h(M, \tilde{V})$.
3. Compare values $\tilde{e}$ and e. If $\tilde{e} = e$ then the signature (e, s) is recognized as genuine. Otherwise, the signature is rejected.

The formal proof of the correctness of the proposed EDS scheme is to show that substitution of the signature value, calculated correctly in accordance with the signature generation

procedure, to the input of the authentication procedure will lead to confirmation of the EDS authenticity. This substitution sets the following

$$\begin{aligned}\tilde{V} &= Y^{-e} \circ T \circ Z^s = \left(A \circ Q^x \circ A^{-1}\right)^e \circ A \circ G \circ B^{-1} \left(B \circ Q \circ B^{-1}\right)^s \\ &= A \circ Q^{ex} \circ G \circ Q^s \circ B^{-1} = A \circ Q^{ex} \circ Q^s \circ G \circ B^{-1} \\ &= A \circ Q^{ex} \circ Q^{k-ex} \circ D = A \circ Q^k \circ D \\ &= V \\ \Rightarrow \quad & F_h\left(M, \tilde{R}\right) = F_h\left(M, R\right) \quad \Rightarrow \quad \tilde{e} = e\,.\end{aligned}$$

To understand the method of implementing the blind signature protocol based on the described initial EDS scheme, it is useful to consider an alternative signature generation procedure, in which only one secret value is used, namely, the discrete logarithm value in the hidden group, i.e. the value x. An alternative procedure for generating EDS requires one additional exponentiation operation and is described as follows:

1. Generate a pair of random non-negative integers $t < q$ and $u < q$.
2. Calculate the vector-fixator $V = Y^t \circ T \circ Z^u$.
3. Calculate the first signature element $e = F_h(M, V)$.
4. Calculate the second signature element s

$$s = u + (t - e)x \mod q.$$

4.2. Initial signature scheme on the six-dimensional algebra

We assume that the 6-dimensional FNAA used as an algebraic support is given over a ground finite field $GF(p)$, where the characteristic p represents a prime number having the structure $p = 2q+1$ with a prime q of sufficiently large size (384 or more bits). To construct a post-quantum EDS scheme with the possibility of performing a formal reductionist security proof, proposed earlier in [17] for EDS schemes based on the computational complexity of DL problem, we use the Schnorr signature scheme [18] as a prototype. In contrast to the prototype, in which the basic cyclic group is explicitly defined as the algebraic carrier of the cryptoscheme, in the EDS scheme based on the HDLP, the basic cyclic group is hidden and EDS authentication involves calculations in two other cyclic groups. The values obtained in the latter are interfaced through the values of the elements of the basic cyclic group, which ensures the correct operation of the EDS scheme based on the proposed version of the HDLP.

The mutual commutativity of masking operations with exponentiation is used in the following procedure for generating a public key in the form of a triplet of vectors (Y, Z, T):

1. Generating different random values for the coordinates g_0, g_1, g_2, g_3, g_4, and g_5, for which equality (12) holds true, choose a random non-invertible vector G, whose local order is equal to a prime number q.
2. Generating different random values for the coordinates a_0, a_1, a_2, a_3, a_4, and a_5, for which equalities (12) and (13) do not hold simultaneously, choose a random invertible vector A, whose order is equal to the number p^2-1, and the non-equality $A \circ G \neq G \circ A$ is fulfilled.
3. Calculate a vector equal to the inverse value of the vector A: $A^{-1} = A^{p^2-2}$.

4. Generating different random values for the coordinates b_0, b_1, b_2, b_3, b_4, and b_5, for which equalities (12) and (13) do not hold simultaneously, choose a random invertible vector B, whose order is equal to the number $p^2 - 1$, and the non-equality $B \circ G \neq G \circ B$ is fulfilled.
5. Calculate a vector equal to the inverse value of the vector B: $B^{-1} = B^{p^2-2}$.
6. Generate a random natural number $x < q$ and calculate the first element of the public key as a vector $Y = A \circ G^x \circ A^{-1}$.
7. Calculate the second element of the public key as a vector $Z = B \circ G \circ B^{-1}$.
8. Generate a random natural number $d < q$ and calculate the third element of the public key as a vector $T = A \circ G^d \circ B^{-1}$.

When forming a public key in the form of triplet of vectors (Y, Z, T) the following random elements, which are secret parameters, were selected: the generator of the basic cyclic group G, invertible vectors A and B and non-negative integers x and d. It is assumed that after the formation of a public key, its owner only needs to store the following values as his personal secret key x, d, G, A, and B^{-1}, which are used in the digital signature generation procedure.

In the proposed initial signature scheme, the procedure for generating a signature in the form of a pair of numbers (e, s) to some electronic document M includes the following steps:

1. Generate a random natural number $k < q$.
2. Calculate the fixator-vector $V = A \circ G^k \circ B^{-1}$.
3. Compute the first signature element as the binary number $e = F_h(M, V)$ where F_h is a specified hash-function.
4. Compute the second signature element as the binary number s
$$s = k - d - ex \mod q.$$

Procedure for verifying a signature (e, s) to the document M is executed using the public key (Y, Z, T) as follows:

1. Calculate the vector $\tilde{V} = Y^e \circ T \circ Z^s$
2. Calculate the value $\tilde{e} = F_h(M, \tilde{V})$
3. Compare values $\tilde{e}$ and e. If $\tilde{e} = e$ then the signature (e, s) is recognized as genuine. Otherwise, the signature is rejected.

Formal proof of the correctness of the proposed EDS scheme is performed as follows

$$\begin{aligned}
\tilde{V} &= Y^{-e} \circ T \circ Z^s = \left(A \circ G^x \circ A^{-1}\right)^e \circ A \circ G^u \circ B^{-1} \left(B \circ G \circ B^{-1}\right)^s \\
&= A \circ G^{ex} \circ G^d \circ G^s \circ B^{-1} = A \circ G^{ex+d} \circ G^{k-d-ex} \circ B^{-1} \\
&= A \circ G^k \circ B^{-1} \\
&= V \\
\Rightarrow \quad & F_h\left(M, \tilde{R}\right) = F_h\left(M, R\right) \\
\Rightarrow \quad & \tilde{e} = e.
\end{aligned}$$

Just as in the EDS scheme on the 4-dimensional algebra, an alternative EDS generation procedure can be used to calculate the signature, which includes the following steps:

1. Generate a pair of random natural numbers $t < q$ and $u < q$.
2. Calculate the fixator-vector $V = Y^t \circ T \circ Z^u$.

3. Compute the first signature element as the binary number $e = F_h(M, V)$
4. Compute the second signature element as the binary number s

$$s = u + (t - e)x \mod q.$$

Note that the alternative procedures for generating a signature in both the signature schemes match.

4.3. Method of applying blinding multipliers

In general, the DL problem is formulated in a finite cyclic group Γ contained, for example, in some given FNAA, as a solution of an equation of the form $W = G^x$, where W and G are some given elements of the group Γ, x is an unknown natural number. If over one of the elements W and G or over both of them the operations of automorphic or homomorphic mapping of FNAA using secret parameters is performed, then the specified two elements will be mapped in the vectors of Y and Z correspondingly. The HDLP consists in calculating the value x using the known values Y and Z. The latter generally lie in different cyclic groups contained in the FNAA and different from Γ. The main contribution to the security of cryptosystems based on HDLP is made by the exponentiation operation to an integer power of large size. This operation is called basic.

The use of functions of automorphic or homomorphic mapping of FNAA as masking operations is determined by the fact that in order to ensure the possibility of constructing cryptosystems based on HDLP, it is necessary to provide the property of mutual commutativity of the base operation with each of the masking operations. If this requirement is met, [6, 7]. Within the framework of this analogy, the following method of constructing a blind signature scheme based on the DL problem is proposed. Select an EDS scheme based on the DL problem and constructed by analogy with the Schnorr EDS scheme [18], for which a method is known for constructing a blind EDS scheme using two different types of blinding multipliers: 1) the multiplier formed as a result of exponentiating the value of the signer's public key to a random power μ and 2) the multiplier formed as a result of exponentiating the generator G to a random power ε. In the well-known blind signature protocol [17], at the first step, the signer generates a fixator (his one-time public key) and passes it to the user, who forms two blinding multipliers of the specified types and sequentially multiplies the fixator by each of them. The same mechanism can also be used when constructing a blind signature scheme based on the HDLP, introducing the following clarification: when performing multiplication by blinding multipliers, it should be taken into account that the EDS verification equation is set in a non-commutative algebra, so multiplication by each of the blinding multipliers should be performed strictly on the right or strictly on the left, depending on the multiplier and the original EDS scheme used.

The initial signature schemes introduced in Subsections 4.1 and 4.2 are analogs of the Schnorr EDS scheme implemented on the basis of the HDLP. It should be noted that in the initial EDS schemes based on the computational complexity of the HDLP, for forging a signature it is enough to calculate the values x and d when using the public key. Indeed, to calculate the signature, you can use the alternative procedure for generating a signature, in which the fixator-vector is calculated using three elements of the public key Y, Z and T in correspondence with the formula $\bar{V} = Y^t \circ T \circ Z^u$, where $t < q$ and $u < q$ are random natural numbers. Taking into account the existence of an alternative procedure for generating EDS,

it is possible to formulate the version of the HDLP, used in the introduced EDS scheme as the calculation of a natural number x when using a known public key.

In the blind signature protocol, the value of the fixator-vector $\bar{V} = Y^t \circ T \circ Z^u$ generated by the signer, is passed to the client to inset blinding multipliers. The last formula tells us that a blind digital signature protocol should include a step at which the client generates a random natural numbers $\mu < q$ and $\varepsilon < q$ and forms blinding multipliers Y^μ and Z^ε, and then calculates the value of the fixator-vector $V = Y^\mu \circ \bar{V} \circ Z^\varepsilon$, associated with the genuine signature, which will be used by the client to calculate the first element e of the authentic signature and calculate the first element $\bar{e}$ of the blind signature (the calculation of the first element does not require knowledge of the secret key associated with the public key). An important distinguishing feature is the use of the multiplier Y^μ as the left operand, and the multiplier Z^ε as the right operand.

4.4. A blind signature protocol on the four-dimensional algebra

To build a blind EDS protocol, we will use the basic digital signature scheme described in Subsection 4.1.

The proposed blind digital signature protocol includes the following steps:

1. The signer generates a random number $k < q$ and calculates the fixator-vector $\bar{V} = A \circ G^k \circ D$. Then he sends the value of $\bar{V}$ to client who wish to obtain from the signer a digital signature to the document M.
2. The client generates two random natural numbers $\mu < q$ and $\varepsilon < q$ and calculates the vector $V = Y^\mu \circ \bar{V} \circ Z^\varepsilon$ and the first element of genuine signature $e = F_h(M, V)$.
3. The client then calculates the first element of the blind signature $\bar{e} = e - \mu \mod q$ and sends it to the signer.
4. Using his private secret key x, the signer calculates the second element $\bar{s}$ of blind signature:$\bar{s} = k - \bar{e}x \mod q$. He then sends the value $\bar{s}$ to the client.
5. By value $\bar{s}$, the client calculates the second element s of the authentic signature to the document M: $s = \bar{s} + \varepsilon \mod q$.

Procedure for verifying a signature (e, s) to the document M is executed using the public key (Y, Z, T) as follows:

1. Calculate the vector $\tilde{V} = Y^e \circ T \circ Z^s$
2. Calculate the value $\tilde{e} = F_h(M, \tilde{V})$
3. If $\tilde{e} = e$ then the signature (e, s) is accepted as genuine one. Otherwise, the signature is rejected.

The correctness of the described blind EDS protocol is proved by substituting the signature for the input of the specified verification procedure and demonstrating that it passes verification as a genuine signature.

The proof of correctness of the blind digital signature protocol

$$\begin{aligned}\tilde{V} &= Y^e \circ T \circ Z^s = Y^{\bar{e}+\mu} \circ T \circ Z^{\bar{s}+\varepsilon} \\ &= Y^\mu Y^{\bar{e}} \circ T \circ Z^{\bar{s}} \circ Z^\varepsilon = Y^\mu \circ \bar{V} \circ Z^\varepsilon = V \\ &\Rightarrow \tilde{e} = F_h\left(M, \tilde{V}\right) = F_h(M, V) = e.\end{aligned}$$

4.5. The blind signature protocol on the six-dimensional algebra

To build a blind EDS protocol, we will use the basic digital signature scheme described in Subsection 4.2.

The proposed blind signature protocol on the 6-dimensional algebra includes the following steps:

1. The signer generates a random number $k < q$ and calculates the fixator-vector $\bar{V} = A \circ G^k \circ B^{-1}$. He then directs the value $\bar{V}$ to the client who wants to receive the signer's EDS to the document M.
2. The client generates two random natural numbers $\mu < q$ and $\varepsilon < q$ and computes the vector $V = Y^{\mu} \circ \bar{V} \circ Z^{\varepsilon}$ and the first element of the authentic signature $e = F_h(M, V)$.
3. The client then calculates the first element of the blind signature $\bar{e} = e - \mu \mod q$ and sends it to the signer.
4. Using his private secret key x, the signer calculates the second element $\bar{s}$ of blind signature $\bar{s} = k - d - \bar{s}x \mod q$. He then directs the value $\bar{s}$ to the client.
5. By the value of $\bar{s}$ the client calculates the second element s of the authentic signature to the document M $s = \bar{s} + \varepsilon \mod q$.

Procedure for verifying a signature (e, s) to the document M is executed, using the public key (Y, Z, T), in full compliance with the verification procedure of the initial signature scheme described in Section 4.2. The proof of correctness of the protocol is identical to the proof of correctness of the blind signature protocol described in Subsection 4.4.

5. DISCUSSION

When developing the signature schemes described in Section 4, a design criterion was used, which can be formulated as follows: *based on the use of public parameters of the EDS scheme, it should be computationally impossible to specify a periodic function that takes values in an explicitly specified cyclic group and contains a period that depends on the value of the discrete logarithm* x.

In both described EDS schemes, the public key elements Y and Z are generators of various cyclic groups contained in the algebraic support of the cryptoscheme. The groups generated by the vectors Y and Z are associated with a hidden cyclic group, so when using the matching element T of the public key, you can specify a periodic function from two integer variables i and j with a period $(-1, x)$, the length of which depends on the value of x: $F(i, j) = Y^i \circ T \circ Z^j = Y^{i-1} \circ T \circ Z^{j+x}$. However, the values of the function $F(i, j)$ lie in many different cyclic groups contained in the FNAA used as an algebraic support. At the same time, it is impossible to distinguish any fixed cyclic group, which with a significant probability includes the values of the function $F(i, j)$. This circumstance does not allow us to apply the quantum Shor algorithm [2] to find the value of x.

An important technique for constructing EDS schemes based on the HDLP is to use the matching element T of the public key, which is a non-invertible vector. This technique eliminates the possibility of calculating the inverse value T^{-1}, with which it would be possible to construct a periodic function $F^*(i, j) = Y^i \circ (Z^*)^j = Y \circ (T \circ Z \circ T^{-1})^j$.

In the case of a blind signature protocol on the 4-dimensional FNAA, a hidden group generated by an invertible element of the Q algebra is used, and the matching parameter

is calculated by the formula $T = A \circ G \circ B^{-1}$, which uses a non-invertible element G that is mutually permutable with the vector Q. The permutability property of these elements is necessary to ensure the correctness of the EDS scheme. When forming a public key, a non-invertible vector G is first generated, which has a local order equal to a sufficiently large prime number, and then a two-sided local unit is selected Q^*, corresponding to the vector G and being permutable with G. Since the vector Q is computed by scalar multiplication of the invertible vector Q^* of order q and number $\alpha^{\frac{p-1}{q}}$, the order of which is also equal to q, then the order of the vector Q is equal to q. Evidently the vector Q is permutable with the vector G. When using a 4-dimensional FNAA as algebraic support of the HDLP-based signature schemes one obtains higher performance than in the case of using the FNAA having dimensions $m \geq 6$. However, one can expect that in the latter case some possible future attacks on the signature schemes on 4-dimensional FNAAs will be potentially inefficient. The use of the 6-dimensional FNAA as an algebraic support illustrates some features of the signature scheme design.

In the case of a blind signature protocol on the 6-dimensional FNAA, it is not obvious how one can generate an invertible vector Q that would be permutable with a non-invertible vector G, therefore, as a hidden group, the group generated by the non-invertible vector G is used, which is also used to specify the non-invertible matching element T of the public key $T = A \circ G^d \circ B^{-1}$. Exponentiation of the vector G to power d when computing the vector T is connected with the fact that without this exponentiation operation, there would be a linear relationship between the elements T and Z of the public key through the vector $X = A \circ B^{-1} : T = X \circ Z$. The latter equation can be solved reducing it to the solving a system of six linear equations. After finding the value of X one can compute the vector $Z' = X \circ Z \circ X^{-1}$, such that $Y = Z'^x$, i. e. the HDLP could be reduced to ordinary DL problem.

The Schnorr signature scheme [18] and the blind signature protocols [14, 17] use computation in the finite ground field $GF(p)$. To provide 109-bit security level one should set the size of the prime p equal to 2048 or more bits. The computational complexity of the multiplication operation modulo p is a quadratic function of the size of p. Taking into account the latter, one can state that the proposed initial signature schemes and blind signature protocols on the 4-dimensional (6-dimensional) FNAA have significantly higher (about the same) performance. However the cryptoschemes [17, 18], are not resistant to quantum attacks. Post-quantum resistance is the main advantage of the proposed cryptoschemes against the blind signature protocols [14, 13, 17].

One can expect that post-quantum resistance can be provided by the blind signature protocols designed on the base of post-quantum signature schemes Falcon [19], Crystals-Dilithium [20], and Rainbow [21] (finalists of the NIST competition in nomination of post-quantum signature algorithms [22]). However, in the latter case the sum size of public key and signature is very large (> 3000 bytes) that is a significant disadvantage for many practical applications of blind signatures.

To improve significantly the performance of the proposed cryptoschemes one can use a FNAAs set over the field $GF(p)$ with prime $p = 2q + 1$, where the prime $q = 2^{256} + \frac{(c-1)}{2}$ with an odd 32-bit integer c (selected so that the value $p = 2^{257} + c$ is prime). In this case the multiplication modulo p can be performed without executing the arithmetic division operation. Selection of the other cryptoscheme parameters do not affect on the performance.

6. CONCLUSIONS

A method for constructing blind EDS protocols based on the HDLP is proposed and a specific version of such a protocol is developed when using two different algebraic carriers each of which contains a global two-sided unit: a 4-dimensional and a 6-dimensional FNAAs set over a finite ground field $GF(p)$. A characteristic feature of the proposed blind signature protocols based on the hidden discrete logarithm problem is the use of left-sided and right-sided masking multipliers, which is determined by the fact that the vectors that are elements of the public key are non-permutable.

The proposed protocols are of practical interest as post-quantum blind signature protocols, due to the fact that they have a fairly high performance and relatively small size of the public parameters of the cryptoscheme.

ACKNOWLEDGMENT

This research is supported by RFBR (project # 21-57-54001-Vietnam) and by Vietnam Academy of Science and Technology (project # QTRU01.13/21-22).

REFERENCES

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography.* Boca Raton: CRC Press (5th printing), 2001.

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

[3] S. Y. Yan, *Quantum Attacks on Public-key Cryptosystems.* Springer US, 2014.

[4] Federal Register, "Announcing request for nominations for public-key post-quantum cryptographic algorithms." [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf

[5] T. Lange and R. Steinwandt, "Post-quantum cryptography," in *9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, ser. Lecture Notes in Computer Science, vol. 10786. Springer, 2018.

[6] D. N. Moldovyan and N. A. Moldovyan, "Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms," *Quasigroups and Related Systems*, vol. 18, no. 2, pp. 177–186, 2010.

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

[8] N. A. Moldovyan and A. A. Moldovyan, "Candidate for practical post-quantum signature scheme," *Vestnik of Saint Petersburg State University. Applied Mathematics. Computer Science. Control Processes*, vol. 16, pp. 455–461, 2020.

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

[10] D. N. Moldovyan and N. A. Moldovyan, "A new hard problem over non-commutative finite groups for cryptographic protocols," in *5th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS 2010 Proceedings. St.Petersburg*, vol. 6258, September 8-11, 2010, pp. 183–194.

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

[12] N. A. Moldovyan and A. A Moldovyan, "Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem," *Bulletin of the South Ural State University.Mathematical Modelling, Programming & Computer Software*, vol. 12, no. 1, 2019.

[13] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press*, 1983, pp. 199–203.

[14] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in *Advances in Crypology - EUROCRYPT'94*, vol. 950. Springer Verlang, 1995, pp. 428–432.

[15] N. A. Moldovyan, "Unified method for defining finite associative algebras of arbitraty even dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263–270, 2018.

[16] D. N. Moldovyan, "New form of the hidden logarithm problem and its algebraic support," *Bulletin of Academy of Sciences of Moldova. Mathematics*, vol. 2, no. 2(93), pp. 3–10, 2020.

[17] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[18] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[19] P. Fouque, J. Hoffstein, P. Kirchner *et al.*, "Fast-fourier lattice-based compact signatures over ntru," accessed July 11, 2021. [Online]. Available: https://www.falcon-sign.info/

[20] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: A lattice-based digital signature scheme," accessed July 11, 2021. [Online]. Available: https://eprint.iacr.org/2017/633.pdf

[21] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Applied Cryptography and Network Security. ACNS 2005*, ser. Lecture Notes in Computer Science, Y. M. Ioannidis J., Keromytis A., Ed., vol. 3531, 2005, pp. 164–175.

[22] Post-Quantum Cryptography. Round 3 Submissions. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms, accessed July 11, 2021. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

Received on April 19, 2021
Accepted on August 02, 2021