Digital Signature Algorithms Based on Hidden Discrete Logarithm Problem

Alexandr Andreevich Moldovyan[1], Nikolay Andreevich Moldovyan[1], Ngoc Han Phieu[2], Cong Manh Tran[3], and Hieu Minh Nguyen[2(✉)]

[1] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, St. Petersburg, Russia
{maa, nmold}@mail.ru
[2] Academy of Cryptography Techniques, Hanoi, Vietnam
{phieungochan, hieuminhmta}@gmail.com
[3] Le Quy Don Technical University, Hanoi, Vietnam

Abstract. The discrete logarithm problem in a hidden group, which is defined over finite non-commutative associative algebras, represents interest for constructing post-quantum public-key cryptoschemes. The currently known form of the hidden logarithm problem suits well for designing the public-key agreement protocols and public encryption algorithms, but not suits for designing the digital signature algorithms. In the present paper, there are introduced novel forms of defining the hidden discrete logarithm problem, on the base of which two digital signature algorithms are proposed. Two different four-dimensional finite non-commutative associative algebras have been used in the proposed signature algorithms. In one of the proposed algorithms, there are used globally non-invertible vectors that are invertible locally. A large set of the left-side and a large set of the right-side local units relates to some fixed globally non-invertible vector. Several different local units are used to define one of the proposed forms of the hidden logarithm problem.

Keywords: Cryptography · Public-key cryptosystems · Post-quantum cryptoschemes · Discrete logarithm problem · Digital signature

1 Introduction

Currently, digital signature algorithms (DSAs) [1, 2] based on the computational difficulty of the factorization problem (FP) [3] and the discrete logarithm problem (DLP) [4] have wide practical application. The security of the DSAs based on the FP and DLP is determined by the fact that the most efficient known algorithms for solving these problems have subexponential (factorization and DLP in finite fields) or exponential difficulty (DLP on elliptic curves).

In connection with the significant progress in the development of quantum computations [5, 6], interest in estimating the computational complexity of the DLP and FP at solving these problems on a quantum computer has arisen. It has been shown that solving the FP and the DLP on quantum computer has polynomial computation difficulty [7, 8]. This result means that attacks with using quantum computers will break

S. C. Satapathy et al. (eds.), *Frontiers in Intelligent Computing: Theory and Applications*, Advances in Intelligent Systems and Computing 1014,
https://doi.org/10.1007/978-981-13-9920-6_1

the DSAs based on computational difficulty of the FP and DLP. Waiting for the emergence of practically working quantum computers in the middle or in the second half of the 2020s [9] leads to the current challenge of applied and theoretical cryptography for the development of the post-quantum DSAs that will resist the attacks based on using quantum computers.

To ensure sufficiently, high security level of the DSAs requires that computationally difficult problems other than the FP and the DLP can be used as their base cryptographic primitive. The response to this challenge was the announcement by the National Institute of Standards and Technology (NIST) of the competition for developing the post-quantum public-key cryptosystems (public-key agreement protocols, public encryption algorithms, and DSAs) [9, 10] and the appearance of regularly held thematic conferences [11, 12].

This paper extends the approach to the design of the post-quantum public-key cryptoschemes, which relates to the use of so-called hidden DLP (HDLP) as the base cryptographic primitive. Section 2 introduces the known form of the HDLP and describes the finite quaternion algebra. Section 3 describes a new 4-dimensional FNAA. Sections 4 and 5 describe the first (second) proposed DSA. In Sect. 6, the proposed DSAs are discussed as candidates for the post-quantum signature algorithms. Section 7 concludes the paper.

The main contribution of the paper is introducing two new forms of the HDLP, applicable to the design of the post-quantum signature schemes, and proposing two new DSAs as candidates of the post-quantum signature schemes.

2 Non-commutative Finite Algebras as Carriers of the Post-quantum Cryptoschemes

For the development of post-quantum public-key cryptoschemes, it was suggested to use the problem of finding the conjugating element in non-commutative braid groups [13, 14]. However, in this approach, there are fundamental difficulties associated with the fact that this problem reduces to solving systems of linear equations [15]. The latter casts doubt on the security of the numerous two-key cryptosystems based on calculations in braid groups [16, 17].

More promising is the approach consisting in combining the DLP with the problem of finding the conjugating element, leading to the HDLP, i.e., to the DLP in the hidden cyclic group of a finite non-commutative associative algebra (FNAA) [18, 19]. However, the form of the HDLP proposed in papers [18, 19] suits well for designing the public-key agreement protocols, public encryption, and commutative encryption algorithms, but not suits to design the DSA.

The HDLP is defined over some finite non-commutative algebraic structure containing sufficiently large number of different cyclic groups as its subsets. The FNAAs represent the most attractive case of the carriers of the HDLP. Let us consider a finite m-dimensional vector space defined over a ground finite field GF(p). An arbitrary vector V can be represented as an ordered set of m elements of the field GF(p)$V = (a, b, \ldots, q)$ or as the following sum of the single-component vectors $a\mathbf{e}$, $b\mathbf{i}$, …, $q\mathbf{v}$: $V = a\mathbf{e} \oplus b\mathbf{i} \oplus \cdots \oplus q\mathbf{v}$, where $\mathbf{e}$, $\mathbf{i}$, and $\mathbf{v}$ are formal basis vectors; $a\mathbf{e} = (a, 0, \ldots, 0)$,

$b\mathbf{i} = (0, b, 0, \ldots, 0)$, and $q\mathbf{v} = (0, \ldots, 0, q)$. The terms $a\mathbf{e}$, $b\mathbf{i}$, …, $q\mathbf{v}$ are called the components of the vector V. The addition of vectors V and $V' = (a', b', \ldots, q')$ is denoted as $\oplus$ and is defined with the following formula:

$$V \oplus V' = (a, b, \ldots, q) \oplus (a', b', \ldots, q') = (a + a', b + b' + \cdots + q + q').$$

The operation of multiplying two vectors $a\mathbf{e} \oplus b\mathbf{i} \oplus \cdots \oplus q\mathbf{v}$ and $x\mathbf{e} \oplus y\mathbf{i} \oplus \cdots \oplus w\mathbf{v}$ is defined as the multiplication of each component of the first operand with each component of the second operand in accordance with the following formula (the multiplication operation is denoted as $\circ$):

$$\begin{aligned}(a\mathbf{e} \oplus b\mathbf{i} \oplus \cdots \oplus q\mathbf{v}) \circ (x\mathbf{e} \oplus y\mathbf{i} \oplus \cdots \oplus w\mathbf{v}) \\ = ax\mathbf{e} \circ \mathbf{e} \oplus ay\mathbf{e} \circ \mathbf{i} \oplus \cdots \oplus aw\mathbf{e} \circ \mathbf{v} \oplus bx\mathbf{i} \circ \mathbf{e} \oplus by\mathrm{i} \circ \mathbf{i} \\ \oplus \cdots \oplus bw\mathbf{i} \circ \mathrm{v} \oplus \cdots \oplus qx\mathbf{v} \circ \mathbf{e} \oplus qy\mathbf{v} \circ \mathbf{i} \oplus \cdots \oplus qw\mathbf{v} \circ \mathbf{v},\end{aligned}$$

in which in each term the product of two basis vectors is to be replaced by some single-component vector indicated in a cell of some table called basis-vector multiplication table (BVMT) [18, 19]. The indicated cell locates at intersection of the row defined by the left basis vector and the column defined by the right basis vector. The coordinates of the single-component vectors, which are not equal to 1, are called structural coefficients. After the mentioned replacement was performed, the right-hand side of the last expression will represent the sum of the single-component vectors. Addition of all of the lasts yields some vector $V'' = (a'', b'', \ldots, q'') = a''\mathbf{e} \oplus b''\mathbf{i} \oplus \cdots \oplus q''\mathbf{v}$. The finite vector space with the described multiplication operation is called finite m-dimensional algebra. If the operation of multiplication in a finite algebra is associative and non-commutative, then the last one is called FNAA.

For some fixed values of the dimension and of the characteristic of the field GF(p), finite algebras of various types can be defined using different BVMTs. The finite quaternion algebra, a particular case of the four-dimensional FNAAs, is defined with the BVMT shown as Table 1.

Table 1. BVMT defining the finite quaternion algebra ($\tau \in$ GF(p)) [18]

$\circ$	**e**	**i**	**j**	**k**
e	**e**	**i**	**j**	**k**
i	**i**	$-\tau$**e**	**k**	$-\tau$**j**
j	**j**	−**k**	−**e**	**i**
k	**k**	τ**j**	−**i**	$-\tau$**e**

The vector E = (1, 0, 0, 0) is the global bi-side unit (unit acting on all elements of the algebra). This finite algebra contains:

$$\Omega = p(p-1)(p^2-1) \tag{1}$$

different vectors that are invertible relatively the global unit and $p^3 + p^2 - p$ vectors that are non-invertible relatively E. The set of the globally non-invertible vectors contains many different subsets of the locally invertible vectors, i.e., vectors invertible in the frame of some subset including the local bi-side unit. Results of the paper [19] show that such locally invertible vectors represent special interest for using them as parameters of the HDLP.

Initially, the HDLP was introduced over the finite non-commutative multiplicative group Γ of the quaternion algebra as follows. Suppose that two invertible vectors Q and G have sufficiently large prime order q (such that q divides Ω) and satisfy condition $Q \circ G \neq G \circ Q$. Then, one can define computation of the public key as follows:

$$Y = Q^{q-t} \circ G^x \circ Q^t = (Q^{q-t} \circ G \circ Q^t)^x, \tag{2}$$

where the pair of integers x ($x < q$) and t ($t < q$) represents the private key. The vectors Y and G are contained in different cyclic groups contained as subgroups in the group Γ; therefore, the problem of finding the values x and t in the vector Eq. (2) is called HDLP.

The public-key agreement scheme constructed on the base of this form of the HDLP is as follows. Two remote users A and B select their private keys (x_A, t_A) and (x_B, t_B) correspondingly. Then, using the formula (2), they compute their public keys Y_A and Y_B. After exchanging with the public keys, the user A computes the vector

$$Z = Q^{q-t_A} \circ Y_B^{x_A} \circ Q^{t_A} = Q^{q-t_A-t_B} \circ G^{x_B x_A} \circ Q^{t+t_B+t_A},$$

and the user B computes the same vector

$$Z = Q^{q-t_B} \circ Y_A^{x_B} \circ Q^{t_B} = Q^{q-t_B-t_A} \circ G^{x_A x_B} \circ Q^{t+t_A+t_B}.$$

The HDLP defined in the form of the formula (2) over the finite quaternion algebra has super-polynomial difficulty at solving it using the ordinary computers, but it can be reduced to the DLP in the finite field GF(p^2) [20]. Therefore, to provide post-quantum security one should look for new FNAAs as carriers of the HDLP [20].

One can expect that defining the HDLP in new forms is also an attractive approach for providing post-quantum security. For example, in new forms of the HDLP one can use non-invertible vectors of the finite quaternion algebra or of some other FNAA with global unit. Using non-invertible vectors represents interest to provide security to attacks using homomorphism of the FNAA into the finite field GF(p) or into the finite field GF(p^2) [19].

3 Proposed New FNAA

We propose the four-dimensional FNAA in which the multiplication operation is defined with Table 2 as a new carrier of the HDLP.

Table 2. BVMT defining the four-dimensional FNAA with bi-side global unit ($\tau\mu \neq 1$)

∘	**e**	**i**	**j**	**k**
e	**e**	μ**k**	μ**e**	**k**
i	τ**j**	**i**	**j**	τ**i**
j	**j**	μ**i**	μ**j**	**i**
k	τ**e**	**k**	**e**	τ**k**

Solving the vector equations:

$$V \circ X = V \quad \text{and} \quad X \circ V = V \tag{3}$$

for the case $\tau\mu \neq 1$, we have derived the following formula for the bi-side global unit E:

$$E = \left(\frac{1}{1-\tau\mu}, \frac{1}{1-\tau\mu}, \frac{\tau}{\tau\mu-1}, \frac{\mu}{\tau\mu-1}\right) \tag{4}$$

For vectors $V = (a, b, c, d)$ coordinates of which satisfy condition $ab \neq dc$, Eq. (3) has the single solution $X = E$. For these vectors, the vector equations $V \circ X = E$ and $X \circ V = E$ also have same single solution that defines the vector $X = V^{-1}$. If there is $dc - ab = 0$, then the vector V irreversible. From the last condition, it is easy to find the number of irreversible vectors, which is equal to $p^3 + p^2 - p$, and the value of the order of the non-commutative multiplicative ring called inverses of the vector V. Thus, the condition $ab \neq dc$ defines the globally invertible vectors V, i.e., the vectors that are invertible relatively the bi-side global unit. We add the word "globally" since the condition $ab = dc$ defines the vectors V that are non-invertible relatively the unit E, but invertible relatively some local bi-side units acting in the frame of some subsets of the algebra elements. Such globally non-invertible vectors we denote as $N = (a', b', c', d')$. For vectors N (that are not the left zero divisors nor the right zero divisors), there exists a large set of the local bi-side units, which contains only one element $E' = (x, y, z, w)$ that is a globally non-invertible vector relating to the case $xy = zw$. The vector E' depends on the coordinates of the vector N and can be computed using the following formula:

$$E' = (x, y, z, w) = \left(h, \frac{d'}{a'\mu + d'} - \frac{a' + d'\tau}{a'\mu + d'} \cdot \frac{d'}{a'} h, \frac{d'}{a'\mu + d'} - \frac{a' + d'\tau}{a'\mu + d'} h, \frac{d'}{a'} h\right), \tag{5}$$

where $h = a'(a' + b' + c'\mu + d'\tau)^{-1}$. All other local bi-side units of the vector N are globally invertible.

It is easy to show that the local unit E' is the local bi-side unit for every vector N^u, where u is an arbitrary natural number. Taking into account the finiteness of the considered FNAA, one can be shown that for some minimum value of the degree $u = \omega$, the condition $N^{\omega} = E'$ holds. This value ω is called local order of the vector

N. The set of the vectors N^i, where $i = 1, 2, \ldots, \omega$, compose a cyclic group having order ω and containing the unit element E'. Thus, if some globally non-invertible vector N is not a zero divisor, then N generated a cyclic finite group contained in the considered FNAA. Such cyclic groups represent interest for using them as the hidden group to define the HDLP.

In one of the proposed DSAs (see Sect. 5), the local right-side units of some locally invertible vector are used as secret parameters. All local right-side units of the vector $N = (a', b', c', d')$ are described by the following formula:

$$E_r = (x, y, z, w) = \left(h, \frac{d'}{a'\mu + d'} - \frac{a' + d'\tau}{a'\mu + d'} n, \frac{a'}{a'\mu + d'} - \frac{a' + d'\tau}{a'\mu + d'} h, n \right), \qquad (6)$$

where $h, n = 0, 1, 2, \ldots, p - 1$. The set (6) includes p^2 different right-side units of the vector N and only p of such units are globally non-invertible vectors. Coordinates of the lasts satisfy condition $hd' = na'$. All other units in the set (6) are globally invertible vectors.

4 Digital Signature Scheme on the Base of the First New Form of the HDLP

In the first proposed DSA, we use a new form of the HDLP in the frame of which the formula, like formula (2), is used to compute two of three elements of the public key. Suppose a user selects at random three invertible vectors P, Q, and G (while using one of the finite quaternion algebra considered in Sect. 2) which have sufficiently large prime order q (that divides the number $p + 1$) and satisfy the following conditions: $Q \circ G \neq G \circ Q, P \circ G \neq G \circ P$, and $Q \circ P \neq P \circ Q$. Then, he can generate the triple of random integers (x, t, u), where $x < q$; $t < q$; $u < q$, and compute his public key as following triple of the vectors (Y, U, F):

$$Y = Q^{q-t} \circ G^x \circ Q^t, U = P^{q-u} \circ G \circ P^u, F = Q^{u-t} \circ P^u. \qquad (7)$$

To compute a signature to some electronic document M, the owner of the public key uses the integers x, t, and u and the vectors Q, G, and P. The last six values compose the private key of the user. The problem of representation of the public key in the form (7) is the first proposed new form of the HDLP.

The *signature generation algorithm* is as follows:

Input: document M.

1. Generate a random integer $k < q$ and compute the vector $R = Q^{q-t} \circ G^k \circ P^u$.
2. Compute the first signature element e: $e = f(M, R)$, where f is some specified hash function (the hash function value e is computed from the document M that is to be signed, to which the vector R is concatenated).
3. Compute the second signature element s: $s = k - ex \bmod q$.

Output: digital signature in the form of the pair of integers (e, s).

The *signature verification algorithm* is as follows:

Input: the public key (Y, U, F); document M; and digital signature (e, s).

1. Compute the vector $\tilde{R} = Y^e \circ F \circ U^s$.
2. Compute the value $\tilde{e}$: $\tilde{e} = f(M, \tilde{R})$.
3. Compare the values e and $\tilde{e}$.
4. If $\tilde{e} = e$, then output message "The signature is valid". Otherwise, output "The signature is false".

Proof of the correctness of the algorithm is as follows:

$$\begin{aligned}\tilde{R} &= Y^e \circ F \circ U^s = (Q^{q-t} \circ G^x \circ Q^t)^e \circ Q^{-t} \circ P^u \circ (P^{q-u} \circ G \circ P^u)^s \\ &= Q^{q-t} \circ G^{xe} \circ Q^t \circ Q^{-t} \circ P^u \circ P^{q-u} \circ G^s \circ P^u = Q^{q-t} \circ G^{xe} \circ G^s \circ P^u \\ &= Q^{q-t} \circ G^{xe+s} \circ P^u = Q^{q-t} \circ G^{xe+k-ex} \circ P^u = Q^{q-t} \circ G^k \circ P^u \\ &= R \Rightarrow \tilde{e} = e.\end{aligned}$$

Thus, if the signature is computed correctly, then it will pass the signature verification procedure as genie one.

5 Digital Signature Scheme on the Base of the Second New Form of the HDLP

In the second proposed DSA, we use the FNAA defined with Table 2. Suppose a user selects at random one globally invertible vector Q, having sufficiently large prime order, and one locally invertible vector $N = (a', b', c', d')$ such that $a'\mu + d' \neq 0$, which has a large prime local order q and relates to the bi-side local unit E' defined by the formula (5). While selecting the vectors Q and N, the following condition is to be satisfied: $Q \circ N \neq N \circ Q$. Then, the user selects at random three pairs of integers (h_1, n_1), (h_2, n_2), and (h_3, n_3) such that the conditions $h_1 d' \neq n_1 a'$, $h_2 d' \neq n_2 a'$, and $h_3 d' \neq n_3 a'$ hold and, using the formula (6), computes the local right-side units E_{r1}, E_{r2}, and E_{r3} relating to the vector N. Due to the indicated conditions, the computed units E_{r1}, E_{r2}, and E_{r3} represent globally invertible vectors. The vectors Q, N, E_{r1}, E_{r2}, and E_{r3} are secret elements used for computing the public key.

Algorithm for computing the public key is described as follows:

1. Generate a random integer $x < q$.
2. Compute the vectors (T, P, L): $T = E_{r1} \circ Q^{-1}$; $P = T^{-1} \circ E_{r2}$; $L = E_{r3} \circ P^{-1}$.
3. Compute the public key as the following pair of the vectors Y and U:

$$Y = Q \circ N^x \circ T; \quad U = P \circ N \circ L. \tag{8}$$

The pair of the vectors (Y, U) represents the public key. The vectors T and P are also secret; however, they are used only in the procedure for computing the public key. The private key used for computing digital signatures represents the integer x and the triple of the four-dimensional vectors (N, Q, L). The problem of representation of the public key in the form (8) is the second proposed new form of the HDLP.

The *signature generation algorithm* is as follows:

Input: document M.

1. Generate a random integer $k < q$, and compute the vector $R = Q \circ N^k \circ L$.
2. Compute the first signature element e: $e = f(M, R)$, where f is some specified hash function.
3. Compute the second signature element s: $s = k - ex \bmod q$.

Output: digital signature in the form of the pair of integers (e, s).

The *signature verification algorithm* is as follows:

Input: the public key (Y, U); document M; and digital signature (e, s).

1. Compute the vector $\tilde{R} = Y^e \circ U^s$.
2. Compute the value $\tilde{e}$: $\tilde{e} = f(M, \tilde{R})$,
3. Compare the values e and $\tilde{e}$.
4. If $\tilde{e} = e$, then the signature is accepted as genie. Otherwise, the signature is rejected as false one.

Proof of the correctness of the algorithm is as follows.
Using the equality $Q \circ T = E_{r_1}$, one can show the following:

$$\begin{aligned}(Q \circ G^x \circ T)^e &= \left(Q \circ (G^x \circ T \circ Q)^{e-1} \circ G^x \circ T\right) \\ &= \left(Q \circ (G^x \circ E_{r1})^{e-1} \circ G^x \circ T\right) \\ &= \left(Q \circ (G^x)^{e-1} \circ G^x \circ T\right) \\ &= (Q \circ G^{xe} \circ T).\end{aligned}$$

Using the equality $L \circ P = E_{r_3}$, one can write the following:

$$\begin{aligned}(P \circ G \circ L)^s &= \left(P \circ (G \circ L \circ P)^{s-1} \circ G \circ L\right) \\ &= \left(P \circ (G \circ E_{r3})^{s-1} \circ G \circ L\right) = \left(P \circ G^{s-1} \circ G \circ L\right) \\ &= (P \circ G^s \circ L).\end{aligned}$$

For a genie signature (e, s), we have the following:

$$\begin{aligned}\tilde{R} &= Y^e \circ U^s = (Q \circ G^x \circ T)^e \circ (P \circ G \circ L)^s \\ &= Q \circ G^{xe} \circ T \circ P \circ G^s \circ L = Q \circ G^{xe} \circ E_{r2} \circ G^s \circ L \\ &= Q \circ G^{xe} \circ G^s \circ L = Q \circ G^{xe+s} \circ L = Q \circ G^{xe+k-ex} \circ L \\ &= Q \circ G^k \circ L = R \Rightarrow \tilde{e} = e.\end{aligned}$$

Thus, if the signature (e, s) is computed correctly, then it will pass the verification procedure as valid signature.

Because the generator N is private, the last proposed form of the HDLP does not suite for constructing the public-key agreement schemes.

One should note that in the second DSA, the local left-side units E_{l1}, E_{l2}, and E_{l3} representing globally invertible vectors can be used instead of the local right-side units E_{r1}, E_{r2}, and E_{r3}. In the case of the four-dimensional FNAA defined with Table 2, the set of all left-side units relating to the vector $N = (a', b', c', d')$, where $a'\tau + c' \neq 0$, is described by the following formula:

$$E_l = (x, y, z, w) = \left(h, \frac{c'}{a'\tau + c'} - \frac{a' + c'\mu}{a'\tau + c'}n, n, \frac{a'}{a'\tau + c'} - \frac{a' + c'\mu}{a'\tau + c'}h\right), \tag{9}$$

where h, $n = 0, 1, 2, \ldots, p - 1$. The set (8) includes p^2 different left-side units of the vector N and only p of such units are globally non-invertible vectors. Coordinates of the lasts satisfy condition $hc' = na'$. Selecting different pairs of the integers (h_i, n_i) satisfying condition $h_i c' \neq n_i a'$, one can define selection of the required vectors E_{li}, $i = 1, 2, 3$.

Each of the considered four-dimensional algebras can be used as a carrier of each of the two proposed forms of the HDLP. However, when using the finite quaternion algebra as the carrier of the HDLP of the second form, the formulas describing the sets of the local right-side or of the left-side units, like (6) or (9), are to be derived and used at designing the signature schemes.

6 The Proposed DSAs as Candidates for Post-quantum Cryptoschemes

The proposed two DSAs and the public-key agreement protocol described in Sect. 2 are based on the HDLP, but the used forms of the last problem are different. In the key agreement scheme, the DLP arises in the finite cyclic group generated by the vector G. In this cryptoscheme, the public key Y is connected with the vector G^x; however, the last is hidden by the conjugacy vector Q^t (see the formula (2)). In the first DSA, there are hidden both the cyclic group generator G and the vector G^x [see the first and second formulas in (7)] by the conjugacy vectors Q^t and Q^u, respectively. The requirement that order q of the vector G divides the integer $p + 1$ (i.e., the integer q does not divide the integer $p - 1$) [19] is used in the first proposed DSA in order to prevent attacks based

on the homomorphism of the used FNAA into the finite ground field GF(p), over which the FNAA is defined [19].

Like in the case of the first DSA, security of the second DSA is also based on computational difficulty of finding the value x that represents the discrete logarithm of the value $Y' = N^x$; however, the value Y' is masked in the first element of the public key: $Y = Q \circ Y' \circ T$. Besides, the value N is also masked in the second element of the public key: $U = P \circ N \circ L$. In the case of the known values N and Y', one has the ordinary DLP, but in the case of known public key (Y, U) one has the HDLP.

One can interpret the second proposed DSA as implementation of the Schnorr signature scheme [21] in the finite cyclic group generated by the globally non-invertible vector N, which is hidden in the four-dimensional FNAA defined with Table 2. Approximately, the same can be said about the first proposed DSA. The both proposed signature schemes are very practical, since they define sufficiently short signatures and provide to generate arbitrary number of signatures using one registered public key. Besides, they have sufficiently high performance.

To estimate the performance of the proposed DSAs, let us consider the case of 128-bit security that can be provided with using the size of the primes p and q equal to 270 and 256 bits correspondingly. Using the HDLP in the hidden cyclic group having 256-bit prime order defines 128-bit security of the proposed signature schemes. He well approved Schnorr signature scheme defined over the field GF(p') with 2500-bit characteristic p' provides 128-bit security. In the Schnorr signature scheme and in the proposed DSAs, there is used approximately the same number of the exponentiation operation. Besides, the signature length is also the same; therefore, performance comparison of these three cryptoschemes is defined by the computational difficulty of the multiplication operation in the FNAAs and in GF(p'). Taking into account that computational difficulty of the modulo multiplication is proportional to the square of the size of the modulo and the multiplication operation in the used FNAAs includes 16 multiplications modulo p, it is easy to show the proposed DSAs are approximately 6 times faster than the Schnorr signature algorithm (in the case of providing security equal to 2^{128} multiplication operations, i.e., in the case of 128-bit security).

Using the non-invertible vector N as generator of the hidden cyclic group in the second proposed DSA serves to prevent potential attacks based on the homomorphism of used FNAA into the field GF(p), which are proposed in [19].

The supposed resistance of the described two DSAs to attacks based on using quantum computers is connected with hiding the cyclic group (in the frame of which a DLP-based signature scheme is constructed) in the four-dimensional FNAAs. However, like in the case of the signature schemes selected as candidates for post-quantum standards [10], estimation of the computational difficulty of the proposed forms of the HDLP for the case of solving them on a quantum computer represents a problem for independent research. The proposed DSAs have many practical advantages (short signature size, no limitation on signing many electronic documents with one public key, possibility to use the standard architecture of the public-key infrastructure) in comparison with the candidates for post-quantum signature standards; therefore, we suppose the task of estimating security of the proposed DSAs will attract much attention of the cryptographic community.

In the second proposed DSA, we have used the non-invertible vector N as generator of the hidden cyclic group in order to prevent potential attacks based on the homomorphism of used FNAA into the field GF(p), which are proposed in [19].

7 Conclusion

The performed research has contributed to the justification of the HDLP as an attractive primitive of the post-quantum public-key cryptography. The previously known form of the HDLP was used for designing post-quantum public-key agreement protocols and public encryption algorithms, but no signature scheme was proposed on its base. In this paper, two novel forms of the HDLP are proposed and used to design two DSAs.

The proposed forms of the HDLP suit well to construct signature schemes, but on the basis of them it is not possible to construct the public-key agreement schemes. The latter is caused by the fact that the hidden finite cyclic group used as the core part of the signature scheme represents a secret element. The last moment contributes significantly to the security of the proposed DSAs.

The FNAAs of the dimensions $m \geq 6$ also represent interest as carriers of the proposed two new forms of the HDLP. A unified method for constructing FNAAs of arbitrary even dimensions $m > 4$ is proposed in the paper [22]. Using different types of the FNAAs for designing the DSAs based on the proposed forms of the HDLP represent a task of independent research in the area of post-quantum cryptography.

Support for Research. This work was partially supported by the Russian Foundation for Basic Research in the framework of the project No. 18-07-00932-a.

References

1. Sirwan, A., Majeed, N.: New algorithm for wireless network communication security. Int. J. Cryptogr. Inf. Secur. **6**(3/4), 1–8 (2016)
2. Yiteng, F., Guomin, Y., Joseph, K.L.: A new public remote integrity checking scheme with user and data privacy. Int. J. Appl. Cryptography. **3**(3), 196–209 (2017)
3. Chiou, S.Y.: Novel digital signature schemes based on factoring and discrete logarithms. Int. J. Secur. Appl. **10**(3), 295–310 (2016)
4. Poulakis, D.: A Variant of digital signature algorithm. Des. Codes Crypt. **51**(1), 99–104 (2009)
5. Yan, S.Y.: Quantum Computational Number Theory, 252 p. Springer, Berlin (2015)
6. Yan, S.Y.: Quantum Attacks on Public-Key Cryptosystems, 207 p. Springer, Berlin (2014)
7. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)
8. Smolin, J.A., Smith, G., Vargo, A.: Oversimplifying quantum factoring. Nature **499**(7457), 163–165 (2013)
9. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST PQCrypto project. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

10. First NIST standardization conference—April 11–13, 2018. http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html
11. Post-Quantum Cryptography. In: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. Lecture Notes in Computer Science Series, vol. 10786. Springer, Berlin (2018)
12. Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24–26, 2016, Lecture Notes in Computer Science (LNCS) Series, vol. 9606, 270 p. Springer, Berlin (2016)
13. Verma, G.K.: A proxy blind signature scheme over braid groups. Int. J. Netw. Secur. **9**(3), 214–217 (2009)
14. Hiranvanichakorn, P.: Provably authenticated group key agreement based on braid groups—the dynamic case. Int. J. Netw. Secur. **19**(4), 517–527 (2017)
15. Myasnikov, A., Shpilrain, V., Ushakov, A.: A practical attack on a braid group based cryptographic protocol. In: Advances in Cryptology—CRYPTO'05/Lecture Notes in Computer Science, vol. 3621, pp. 86–96. Springer, Berlin (2005)
16. Chaturvedi, A., Lal, S.: An authenticated key agreement protocol using conjugacy problem in braid groups. Int. J. Netw. Secur. **6**(2), 181–184 (2008)
17. Verma, G.K.: Probable security proof of a blind signature scheme over braid groups. Int. J. Netw. Secur. **12**(2), 118–120 (2011)
18. Moldovyan, D.N.: Non-commutative finite groups as primitive of public-key cryptoschemes. Quasigroups Relat. Syst. **18**, 165–176 (2010)
19. Moldovyan, D.N., Moldovyan, N.A.: Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. Quasigroups Relat. Syst. **18**, 177–186 (2010)
20. Kuzmin, A.S., Markov, V.T., Mikhalev, A.A., Mikhalev, A.V., Nechaev, A.A.: cryptographic algorithms on groups and algebras. J. Math. Sci. **223**(5), 629–641 (2017)
21. Schnorr, C.P.: Efficient signature generation by smart cards. J. Cryptol. **4**, 161–174 (1991)
22. Moldovyan, N.A.: Unified method for defining finite associative algebras of arbitrary even dimensions. Quasigroups Relat. Syst. **26**(2), 263–270 (2018)