A New Method for Designing Post-Quantum Signature Schemes

Minh Nguyen Hieu[1], Moldovyan Alexander Andreevich[2], Moldovyan Nikolay Andreevich[2], and Canh Hoang Ngoc[3]
[1] Institute of Cryptographic Science and Technology, Hanoi, Vietnam
[2] St.Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, St.Petersburg, Russian
[3] Thuongmai University, Hanoi, Vietnam
Email: hieuminhmta@gmail.com; maa1305@yandex.ru; nmold@mail.ru; canhhn@tmu.edu.vn

Abstract**—**The current standards of the digital signature algorithms are based on computational difficulty of the discrete logarithm and factorization problems. Expected appearance in near future of the quantum computer that is able to solve in polynomial time each of the said computational puts forward the actual task of the development of the post-quantum signature algorithms that resist the attacks using the quantum computers. Recently, the signature schemes based on the hidden discrete logarithm problem set in finite non-commutative associative algebras had been proposed. The paper is devoted to a further development of this approach and introduces a new practical post-quantum signature scheme possessing small size of public key and signature. The main contribution of the paper is the developed new method for defining the hidden discrete logarithm problem that allows applying the finite commutative groups as algebraic support of the post-quantum digital signature schemes. The method uses idea of applying multipliers that mask the periodicity connected with the value of discrete logarithm of periodic functions set on the base of the public parameters of the signature scheme. The finite 4-dimensional commutative associative algebra the multiplicative group of which possesses 4-dimensional cyclicity is used as algebraic support of the developed signature scheme.

Index Terms**—**Post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, finite commutative algebra, hidden logarithm problem

I. Introduction

Currently, cryptographic algorithms have found wide application for solving various problems of information protection [1]-[3]. Public-key cryptographic schemes [4], [5], including digital signature protocols [6]-[8] are of particular importance for ensuring information security. The predicted appearance in the near future of a quantum computer capable of solving the computationally difficult discrete logarithm problem (DLP) [9] and factorization problem [10], [11] in polynomial time has led to a high degree of urgency of the problem of developing post-quantum public-key cryptoschemes, which include algorithms and protocols with public key, which are resistant to attacks using calculations on a quantum computer [12], [13]. At the end of 2016 the US National Institute of Standards and Technology (NIST) announced a program of the development of the post-quantum standards for key agreement scheme and digital signature (DS) scheme. In the framework of the program a worldwide competition [14] on the development of cryptoschemes such types was announced. From the 69 proposed candidates for post-quantum cryptoschemes for participation in the second stage of the competition [15], 17 key agreement schemes and 9 DS schemes were selected [16]. All of these cryptoschemes are based on computationally difficult tasks other than DL and the factorization problem.

The main drawback of the proposed post-quantum DS schemes is the large total size of the public key and digital signature that exceeds 2400 bytes ([16]). The approach to the development of post-quantum DS schemes, based on the computational complexity of the hidden discrete logarithm problem (HDLP), was out of the competition participants, although more practical post-quantum cryptoschemes could potentially be developed within this approach.

The well-known forms of HDLP are formulated in finite non-commutative associative algebras (FNAAs) defined over a ground finite field GF(p) [17]-[21]. The extension of the class of algebraic carriers of the HDLP and the development of its new forms is of significant interest for the development of new practical post-quantum cryptoschemes. In this paper, we propose a new way of defining the HDLP, in which the property of non-commutativity of the multiplication operation is not exploited, namely, finite commutative groups with multidimensional cyclicity are used as an algebraic support [22], [23]. A finite group whose minimum generator system includes m ($m \geq 2$) group elements, every one of which has the same order, is called group with m-dimensional cyclicity.

II. The HDLP as a Basic Primitive of Post-Quantum Cryptoschemes

The known polynomial algorithms for solving DL and factorization problems on a quantum computer are based on reducing each of them to the problem of finding the period length of a periodic function constructed using public parameters of a cryptographic scheme. In the case

Manuscript received March 24, 2020; revised September 4, 2020.
Corresponding author email: canhhn@tmu.edu.vn.
doi:10.12720/jcm.15.10.747-754

of DLP, a periodic function is constructed that contains a period that depends on the value of the logarithm. A sufficiently fast calculation of the period length is ensured by the fact that in the case of functions that take on values in a finite cyclic group, the quantum computer very efficiently performs the discrete Fourier transform [21], [24].

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

The calculation of the value of x on a quantum computer consists in constructing the periodic function $f(i,j) = (Y')^i G^j$ in two variables i and j that take on natural values. This function contains periods of the following lengths: (0, q), (q, 0), (q, q) and (-1, x). The first three values are associated with the order value of the cyclic group, and the last with the discrete logarithm:

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

For a function f (i, j) that takes on values in a given cyclic group, the quantum algorithm finds a period of length (-1, x) in polynomial time.

To construct DS schemes based on HDLP, FNAA of various dimensions m (usually m = 4 and m = 6), which contain a sufficiently large number of isomorphic cyclic groups, are used as algebraic carriers [19], [20]. To generate the public key, a secret cyclic group of prime order is selected. Some group element N that is different from the unit element is selected and the element N^x is calculated. Two secret masking operations ψ_1 and ψ_2, are formed, each of which is mutually commutative with the basic exponentiation operation, and the following two elements Y and Z of the algebra are calculated:

$$Y = \psi_1(N^x), Z = \psi_2(N)$$

belonging to two other cyclic groups of the algebra. To ensure the correct functioning of the digital signature scheme, the selected operations ψ_1 and ψ_2 satisfy special condition. Thanks to the last the function

$$f(i,j) = Y^i Z^j$$

is periodic and contains a period with the length (-1, x). However, this function takes on arbitrary values in the FNAA, used as an algebraic support, i.e. the values f function are not limited to some fixed finite group. This conditions the resistance of DS schemes based on HDLP to quantum attacks using the currently known algorithms for finding the length of a period on a quantum computer. For the said known algorithms the essential point is the boundedness of the values of the periodic function by the framework of one fixed group.

The criterion for constructing post-quantum DS schemes described in [17]-[20] is the following: *defining periodic functions based on public parameters of the DS schemes should lead to the fact that these functions with a rather low probability take values belonging to some fixed group*.

However, the question arises of the possibility of the appearance in the future of quantum algorithms for finding the length of a period for a wider class of periodic functions. The possibility of maintaining high security of DS schemes with the appearance of such quantum algorithms can potentially be provided by the computational complexity of constructing periodic functions with a period length that depends on the value of the discrete logarithm.

Thus, the enhanced criterion for ensuring resistance to quantum attacks can be formulated as follows: *the cryptographic scheme should be designed in such a way that the construction of periodic functions based on public parameters of the cryptographic scheme should lead to the fact that these functions will be free of the period, depending on the value of the discrete logarithm, although they will have periods whose lengths are defined by the prime order of the hidden cyclic group.*

To implement the first criterion, finite commutative associative algebras and finite groups cannot be used as an algebraic support, however, to implement the second criterion, the non-commutative property of the multiplication operation is not necessary, since the masking of the periodicity associated with the value of the discrete logarithm can be performed by multiplying the elements of the basic cyclic groups on elements belonging to another cyclic group. The implementation of this idea is associated with the presence of many different cyclic groups having the same order value. Obviously, the latter also holds in finite commutative associative algebras and commutative groups whose minimum generator system includes two or more elements having the same order value.

The finite commutative groups with multidimensional cyclicity, considered in [22], [23], appear to be the most interesting for the development of new methods and forms of defining the HDLP. Groups of this type include groups whose minimum generator system includes two or more elements having the same order value. Finite groups with m-dimensional cyclicity can be set as multiplicative groups of m-dimensional finite algebras defined over the field GF(p), where p is a prime number, if p - 1 is divisible by m.

III. Finite Commutative Groups with Multidimensional Cyclicity

The set of all m-dimensional vectors whose coordinates are elements of a finite ground field GF(p), where p is a prime number, with the operations of addition of vectors and scalar multiplication form a finite m-dimensional vector space. Vectors are usually represented as an ordered set of coordinates $A = (a_0, a_1, \ldots, a_{m-1})$ or in the form of all possible sums of one-component vectors $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ are basis vectors. When an additional operation of vector multiplication ($\circ$) of vectors is specified in a vector space with the property of two-sided distributivity relatively the addition operation, a finite algebraic structure called a finite *m*-dimensional algebra is formed.

The operation of vector multiplication of arbitrary two vectors $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is usually given by the formula:

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

in which all kinds of products of ordered pairs of basis vectors are replaced by a one-component vector at the intersection of the *i*-th row and the *j*-th column in the so-called multiplication table of basis vectors (MTBV).

It is easy to see from formula (1) that the associativity property of the vector multiplication operation is ensured if the used MTBV is such that for all possible triples of basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$ and $\mathbf{e}_k$ the following equality holds true:

$$\left(\mathbf{e}_i \circ \mathbf{e}_j\right) \circ \mathbf{e}_k = \mathbf{e}_\mathbf{i} \circ \left(\mathbf{e}_j \circ \mathbf{e}_k\right). \qquad (2)$$

Various types of FNAA and their application for development of the public-key cryptoschemes were considered in [19], [20]. The rest of this paper considers finite commutative associative algebras whose multiplicative group has multidimensional cyclicity. To define *m*-dimensional algebras of the latter type, MTBV presented as a Table I can be used, where the structural coefficient $\lambda \in GF(p)$ is not equal to zero.

TABLE I: GENERAL VIEW OF THE MTBV DEFINING A COMMUTATIVE ASSOCIATIVE OPERATION OF VECTOR MULTIPLICATION IN *M*-DIMENSIONAL ALGEBRA [22]

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	...	$\mathbf{e}_{m-1}$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	...	$\mathbf{e}_{m-1}$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	...	$\mathbf{e}_{m-1}$	$\lambda\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	...	$\mathbf{e}_{m-1}$	...	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	...	$\mathbf{e}_{m-1}$	$\lambda\mathbf{e}_0$	...	$\lambda\mathbf{e}_2$
...	...	$\mathbf{e}_{m-1}$	...	...	...	...
$\mathbf{e}_{m-1}$	$\mathbf{e}_{m-1}$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	...	$\lambda\mathbf{e}_{m-2}$

It was shown in [22], [23] that, if the divisibility condition $m|p$ - 1 is satisfied, the following two cases take place:

1. The *m*-dimensional commutative algebra with the multiplication operation given by Table I is a finite field GF(p^m), if the value λ is a non-residue of all degrees *d* that are divisors of dimension *m*. In this case, the multiplicative group of this algebra is cyclic and has the order p^m - 1.

2. If the structure coefficient λ is a residue of degree *m* in the field GF(*p*), then the finite algebra under consideration is a ring whose multiplicative group has *m*-dimensional cyclicity, i.e. it is generated by all possible degrees of some *m* different vectors, every of which has order equal to the value (*p* - 1). Moreover, the order of the multiplicative group of the algebra is $(p - 1)^m$. The said *m* different vectors form a minimum generator system. Any vector belonging to the multiplicative group can be represented as the product of the degrees of the elements included in the basis. Taking into account that each vector included in the basis is of order *p* - 1, it is easy to understand from the latter that reversible algebra vectors can only have a value of order equal to a divisor of *p* - 1.

In this paper, we use a 4-dimensional commutative algebra defined using a special form of MTBV, where the structural coefficient λ is equal to a quadratic residue in *GF*(*p*). The multiplicative group of the algebra has 4-dimensional cyclicity. The particular type of MTBV used does not require the fulfillment of the divisibility condition $m|p$ - 1 to implement the case of 4-dimensional cyclicity, which allows the use of arbitrary values of the prime number *p*.

When designing cryptoschemes based on computational difficulty of the DLP, usually the cyclic groups of prime order having a large bit length (usually 256 bits or more, depending on the type of the used finite group and of the cryptoschemes being implemented) are used. Therefore, when defining multiplicative groups of this type, it is preferable to use prime values *p* having the following structure: *p* = 2*q* + 1, where *q* is also a prime number. Possible 128-bit (256-bit) primes *p* are presented in Table II and Table III.

TABLE II: EXAMPLES PRIMES *P* AND *Q* HAVING THE LENGTH ≈128 BITS

p	$q = \frac{p-1}{2}$
240548035568971429741317911022065104259	120274017784485714870658955511032552129
9561335598278095553365871159737995388 7	47806677991390477766829355798689976943

TABLE III: EXAMPLES OF 256-BIT PRIMES *P*

p	$q = \frac{p-1}{2}$
7807267206046456146937368234167254112722284252029606594561099496053577747695 9	390363360302322807346868411708362705636114212601480329728054974802678887 38479
9805592033996934210908264533442413320338732569105266285131823549694262411105 9	490279601699846710545413226672120666016936628455263314256591177484713120 55529

Consider the case of *m*-dimensional cyclicity. When choosing *p* = 2*q* + 1, a finite group with *m*-dimensional cyclicity (for example, *m* = 4) contains a primary group of order q^m generated by a minimum generator system including *m* vectors of prime order *q*. This primary group contains $q^m - 1$ vectors of order *q*, each of which is included in only one of $q^{m-1} + q^{m-2} + \ldots + q + 1$ cyclic groups of order *q* contained in the said primary group. The unit vector (1, 0, ..., 0) is common for all the cyclic groups mentioned.

Some random cyclic group of order *q* can be defined by choosing some random vector *R* of order *q*. The vector

R can be found by choosing an arbitrary vector V that is not equal to the unit (1, 0, ..., 0) and zero (0, 0, ..., 0) vectors, and calculating the square of the vector V: $R = V^2$. If m - 1 vectors of order q are selected, then, if one more vector of the order q is randomly selected, the probability that it can be represented as the product of some degrees of the indicated m - 1 vectors is

$$\frac{q^{m-1}-1}{q^m-1} \approx \frac{1}{q}.$$

For the primes used, p and q, the probability that the selected m random vectors of order q will not form the minimum generator system of a primary group of order q^m is negligible. Therefore, in this paper, deterministic methods for generating the basis of the primary group are not considered, although when developing specific digital signature schemes recommended for practical use, it is preferable to use the deterministic procedure for specifying the minimum generator system.

IV. A Method for Defining HDLP in a Finite Commutative Group with Multidimensional Cyclicity

In groups of the type under consideration, the method of masking the basic cyclic group, in which it is supposed to perform the exponentiation operation, should be focused on the fulfillment of the strengthened criterion for ensuring post-quantum resistance (see Section 2). This is due to the fact that in commutative groups there is no possibility of performing the operations of the automorphic [17] and homomorphic [19] map which are used when defining the HDLP in FNAAs. Thus, a new masking method is required.

Setting the HDLP is directly connected with the stage of generating the public key, which includes the selection of the secret basic cyclic group by generating a random vector G, considered as a generator of this group. After performing the basic operation of exponentiation (which introduces the main contribution to the security of the designed cryptoscheme), we obtain the vector G^x, which, together with the vector G, must be masked. After performing the masking operations one gets two vectors that are elements of the public key. The proposed masking method uses the idea of multiplying each of the vectors G and G^x by randomly selected vectors U and D of order q which belong to different cyclic groups other than the basic cyclic group one. Thus, the triple of vectors (G, U, D) forms the minimum generator system of a primary subgroup of order q^3. One gets the public key in the form of a pair of vectors

$$Y = G^x \circ U \text{ and } Z = G \circ D.$$

It is easy to see that the pair of vectors (Y, Z) forms the minimum generator system of a primary subgroup of order q^2; therefore, the periodic function $f_r(i, j) = Y^i \circ Z^j$ runs through all q^2 values of the indicated primary subgroup with a period of length (q, q). This function also contains periods of lengths (q, 0) and (0, q) and is free of explicit periodicity, the length of which depends on the discrete logarithm. The latter is determined by the masking influence of the factors U and D.

The fundamental point is that these factors have the same order as the vectors G and G^x. If this condition is violated, for example, if the vector factors U and D have a prime order $r \neq q$, then their masking effect can be completely eliminated by exponentiating the vectors Y and Z to the power r and constructing a periodic function

$$f_r(i, j) = Y^{ri} \circ Z^{rj},$$

which contains a period of length (-1, x): $Y^{r(i-1)} \circ Z^{r(j+x)} = Y^{ri}Z^{-rx} \circ Z^{r(j+x)} = Y^{ri} \circ Z^{rj}$.

However, masking factors will contribute to the signature verification equation and this contribution must be compensated to ensure the correct operation of the DS scheme. It is supposed the latter is to be ensured by calculating an additional element of the digital signature in the form of some vector S included in the verification equation in the form of an auxiliary factor.

If there is a factor that is a signature element, it becomes possible to easily fake a signature using the vector S as a fitting parameter, a random value of which is calculated as unknown in the DS verification equation. To prevent such a method of forging DS, the idea of doubling the verification equation can be used, i.e., instead of one verification equation, one will use two similar equations in which different pairs of the values (Y_1, Z_1) and (Y_2, Z_2) are used and the same signature value (e, s, S). In this case, the forging of the signature according to the first and second verification equations will lead to different values of the fitting parameter S, which makes the indicated method of forging the signature practically impossible.

In the proposed mechanism for doubling the verification equation, it is assumed that the public key is calculated in the form of two pairs of vectors (Y_1, Z_1) and (Y_2, Z_2), which ensure the validity of the verification equation for the same value of the DS. This is ensured by the fact that the first and second elements in each of the pairs (Y_1, Z_1) and (Y_2, Z_2) are connected by one value of the discrete logarithm of x and the same values of the masking factors U and D. The independence of the pairs (Y_1, Z_1) and (Y_2, Z_2) is ensured by using independent basic cyclic groups to calculate these pairs, and random factors U and D are chosen such that the four vectors Y_1, Z_1, Y_2 and Z_2 form the basis of a primary group of order q^4. The latter provides the implementation of the enhanced criterion of post-quantum security (the computational impossibility of constructing a periodic function with a period determined by the value of x).

In the HDLP versions specified in the FNAA and used to construct DS schemes in [17], [19], the discrete logarithm x value in the secret basic cyclic group can be calculated using the baby-step-giant-step algorithm for finding the value x. Such possibility is directly connected with the possibility of constructing (on the basis of the public parameters of the DS scheme) a periodic function containing a period whose length depends on x. This circumstance necessitates the use of a hidden cyclic group of prime order, the size of which is 256 bits while ensuring 128-bit security (the computational complexity of forging a signature equal to 2^{128} multiplication operations).

In the proposed version of the HDLP set in finite commutative groups, an enhanced criterion for ensuring post-quantum resistance is implemented and the discrete logarithm cannot be computed using the baby-step-giant-step algorithm and other known analogues of the last. This is due to the fact that the calculation of the value of x cannot be separated from the calculation of at least one of the secret vectors G, U, and D. Thus, we can expect that to ensure 128-bit security, it is sufficient to use the q value having the 128-bit length.

However, due to the fact that the new version of the HDLP is poorly studied, we can consider the implementation of DS algorithms based on it using the 256-bit values q and raise the question of the level of security achieved in this case (128-bit or 256-bit?). The question of evaluating the security of DS algorithms based on the HDLP set in finite commutative groups is of independent interest. Even in the case of using the 256-bit values q, the proposed DS algorithm seems quite practical. The total size of the public key and signature in them is about 710 bytes, which is 3 or more times smaller in comparison with the candidates for post-quantum DS schemes proposed during the NIST competition [14].

V. Digital Signature Scheme over a Finite Group with Four-Dimensional Cyclicity

Consider the case of defining a 4-dimensional finite commutative algebra over the field GF(p), where $p = 2q + 1$ for the 256-bit prime value q, using the MTBV presented as Table IV, where the structural coefficient is $\lambda = 4$.

TABLE IV: THE MTBV SETTING A FINITE ALGEBRA WHOSE MULTIPLICATIVE GROUP HAS 4-DIMENSIONAL CYCLICITY

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

When defining an algebra according to this table, its multiplicative group has the 4-dimensional cyclicity, if the structural coefficient λ is a quadratic residue in the field GF(p). If the structural coefficient λ is a quadratic non-residue the multiplicative group of the algebra has the 2-dimensional cyclicity and the minimum generator system of the group contains two vectors of the order $p^2 - 1$ (the order of the group is equal to $(p^2 - 1)^2$). When designing the DS scheme in this section, we will consider the case of four-dimensional cyclicity.

The public key is generated as follows:

1. Generate four random vectors G, Q, U, and D, each of which has order equal to the prime q.

2. Generate a random positive integer $x<q$ and calculate the vectors $Y_1 = G^x \circ U$ and $Y_2 = Q^x \circ U$.

3. Calculate the vectors $Z_1 = G \circ D$ and $Z_2 = Q \circ D$.

The public key is two pairs of vectors (Y_1, Z_1) and (Y_2, Z_2). The private key of the owner of this public key is a set of the following values x, G, Q, U and D, the knowledge of which is required to calculate the digital signature. As already noted, the probability that the vectors Y_1, Z_1, Y_2, and Z_2 form the minimum generator system of a primary group of order q^4 is practically equal to 1 (the probability that the products of all possible degrees of these vectors form a primary subgroup of order q^3 is negligible and is equal to the value q^{-1}).

Let an electronic document M is given, to which it is necessary to generate a digital signature of the owner of the public (Y_1, Z_1) and (Y_2, Z_2). To do this, the following procedure is performed, in which some previously agreed secure hash function f_h is used (the algorithm for computing a hash value is part of the DS scheme under consideration):

1. Generate three random positive integers $k < q$, $t < q$ and $u < q$.

2. Calculate the two vector-fixators V_1 and V_2 using the following formulas:

$$V_1 = G^k \circ D^t \circ U^u \text{ and } V_2 = Q^{\,k} \circ D^t \circ U^u.$$

3. Calculate the first element of the digital signature as the value of the hash function $e = f_h(M, V_1, V_2)$, where f_h is a specified hash function.

4. Calculate the second element of the digital signature as a binary number s:

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

5. Calculate the third element of the digital signature in the form of a vector S:

$$S = D^{t-e} \circ U^{u-s}.$$

The result of this algorithm is the signature (e, s, S).

Verification of the signature (e, s, S) to document M is performed using the public key (Y_1, Z_1) and (Y_2, Z_2) according to the following algorithm:

1. Calculate the value of the vectors $\tilde{V}_1 = Y_1^{-e} \circ S \circ Z_1^s$ and $\tilde{V}_2 = Y_2^{-e} \circ S \circ Z_2^s$.

2. Concatenate the vectors $\tilde{V}_1$ and $\tilde{V}_2$ to the document and calculate the value of the hash function $\tilde{e} = f_h(M, \tilde{V}_1, \tilde{V}_2)$.

3. Compare the values $\tilde{e}$ and e. If $\tilde{e} = e$, the signature (e, s, S) is accepted as a genuine digital signature. If $\tilde{e} \neq e$,the signature (e, s, S) is rejected as a false digital signature.

The demonstration of the correctness of the considered DS scheme involves performing a proof that the signature calculated by the owner of the public key successfully passes the signature verification procedure. Let the signature (*e*, *s*, *S*) has been obtained in accordance with the procedure for generating the signature using the correct private key of the signer. Then, by submitting the signature (*e*, *s*, *S*) to the input of the verification procedure, we have the following proof of the correct operation of the proposed signature scheme:

$$\begin{aligned}
\tilde{V}_1 = Y_1^{-e} \circ S \circ Z_1^s &= (G^x \circ U)^e \circ U^{t-e} \circ D^{u-s} \circ (G \circ D)^s \\
&= G^{xe} \circ U^e \circ U^{t-e} \circ D^{u-s} \circ G^s \circ D^s \\
&= G^{xe} \circ U^t \circ D^u \circ G^s = \\
&= G^{xe} \circ U^t \circ D^u \circ G^{k-xe} = \; G^k \circ U^t \circ D^u = V_1; \\
\tilde{V}_2 = Y_2^{-e} \circ S \circ Z_2^s &= (Q^x \circ U)^e \circ U^{t-e} \circ D^{u-s} \circ (Q \circ D)^s \\
&= Q^{xe} \circ U^e \circ U^{t-e} \circ D^{u-s} \circ Q^s \circ D^s \\
&= Q^{xe} \circ U^t \circ D^u \circ Q^s = \\
&= Q^{xe} \circ U^t \circ D^u \circ Q^{k-xe} = \; Q^k \circ U^t \circ D^u = V_2 \quad \Rightarrow \\
&\Rightarrow \; \tilde{e} = f_h(M, \tilde{V}_1, \tilde{V}_2) = f_h(M, V_1, V_2) = e.
\end{aligned}$$

Since the condition is fulfilled, the signature (*e*, *s*, *S*) is accepted as a genuine digital signature to document *M*.

VI. Discussion

As part of the NIST competition [14], currently, 9 different digital signature schemes are being considered as a candidate for the post-quantum DS standard [16]. The most attractive DS schemes from the point of view of compromise between performance and public key size and signature are: Falcon [25], Dilithium [26], and qTESLA [27]. Table V presents an approximate comparison of the developed two signature schemes with the listed candidates for the post-quantum standard of DS, namely, their versions Falcon-512, Dilithium-1024x768, and qTESLA-p-I corresponding to the level of 128-bit security.

The comparison shows that the proposed signature scheme has significantly smaller total size of the public key and signature and higher performance. However, it is less studied from the point of view of their security and only after performing cryptanalytic studies by independent experts it will be possible to give a more reasonable estimate of the practicality of the proposed DS algorithms. At the moment, the performed comparison gives the base for the assumption about the validity of the assumption that the cryptographic community will pay attention to the developed DS scheme based on the HDLP.

TABLE V: COMPARISON OF THE PROPOSED SCHEMES WITH CANDIDATES FOR THE POST-QUANTUM DS STANDARDS

DS Scheme	Signature Length, byte	Public key length byte	Signature generation rate, arb. units	Signature verification rate, arb. units
Falcon-512	657	897	50	25
Dilithium	2044	1184	15	1
qTESLA-p-I	2592	15000	20	40
Proposed	192	512	50	75

Consider the construction of periodic functions based on the public parameters of the proposed DS schemes. We have the following public parameters $Y_1 = G^x \circ U$, $Y_2 = Q^x \circ U$, $Z_1 = G \circ D$ and $Z_2 = Q \circ D$, where every pair of the public-key elements depends on some three vectors from the minimum generator system <*Q*, *U*, *G*, *D*>, and each triple of the public-key elements depends on some three vectors from the set <*Q*, *U*, *G*, *D*>. Therefore, periodic functions constructed as products of the natural degrees of two and three public parameters can contain only periods whose lengths depend on the order of the elements *Q*, *U*, *G*, and *D*, i.e. on the prime value *q*.

Consider a periodic function $F(i,j,k,h) = Y_1^i \circ Z_1^j \circ Y_1^k \circ Z_1^h$. Expressing this function of integer variables through the minimum generator system <*Q*, *U*, *G*, *D*> of the multiplicative group of the 4-dimensional algebra set by Table IV, we get:

$$F(i,j,k,h) = G^{xi+k} \circ U^{i+j} \circ Q^{xj+h} \circ D^{k+h}.$$

Let this function have a period $(\delta_i, \delta_j, \delta_k, \delta_h)$. Since all the basis vectors are independent, we have the following system of linear congruencies with unknowns $\delta_i, \delta_j, \delta_k, \delta_h$:

$$\begin{cases} x\delta_i + \delta_k \equiv 0 \mod q\,; \\ \delta_i + \delta_j \equiv 0 \mod q\,; \\ x\delta_j + \delta_h \equiv 0 \mod q\,;^{\cdot} \\ \delta_k + \delta_h \equiv 0 \mod q\,; \end{cases}$$

The main determinant of this system is nonzero, therefore there is a unique solution $(\delta_i, \delta_j, \delta_k, \delta_h) = (0,0,0,0)$, which means that the considered function contains only periods whose length depends only on the value *q*.

Thus, the proposed DS scheme meets the enhanced criterion of post-quantum resistance.

VII. Conclusion

The construction of a signature scheme based on HDLP using finite commutative algebra was performed for the first time. At the same time, the proposed signature scheme satisfies the enhanced criterion of post-quantum resistance. The introduced method for defining the HDLP in a finite commutative algebra, the multiplicative group of which has a multidimensional cyclic structure, can be extended to the case of other dimensions of algebras and other dimensions of the cyclic structure of their multiplicative group.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

All authors contributed equally to this paper, and were cooperatively involved in conceptualization, investigation, formal analysis and writing. All authors have read and agreed to the published version of the manuscript.

Acknowledgment

This research was funded by the Ministry of Science and Technology (MOST) under grant KC.01.22/16-20.

References

[1] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, p. 816.

[2] Y. Y. Song, *Cybercryptography: Applicable Cryptography for Cyberspace Security*, 1st ed. Springer, 2018, p. 436.

[3] Public-Key Cryptography – PKC 2019. 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14–17, 2019, Proceedings. Lecture Notes in Computer Science series. Springer, vol. 11443, 2019.

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[5] S. Y. Chiou, "Novel digital signature schemes based on factoring and discrete logarithms," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 295–310, 2016.

[6] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, no. 4. pp. 469–472, 1985.

[7] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, pp. 161–174, 1991.

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

[9] J. A. Smolin, G. Smith, and A. Vargo, "Oversimplifying quantum factoring," *Nature*, vol. 499, no. 7457, pp. 163–165, 2013.

[10] S. Y. Yan, "Quantum attacks on public-key cryptosystems," *Springer US*, 2014, p. 207.

[11] Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Lecture Notes in Computer Science series. Springer, 2018, vol. 10786.

[12] Proceedings of the 10th International Workshop on Post-Quantum Cryptography, PQCrypto 2019. Chongqing, China, May 8-10, 2019. Lecture Notes in Computer Science (LNCS) series. Springer, vol. 11505, 2019. [Online]. Available: https://www.springer.com/gp/book/9783030255091

[13] 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

[14] Post-Quantum Cryptography. Round 2 Submissions. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

[15] D. Zimmer, NIST Round 2 and Post-Quantum Cryptography – The New Digital Signature Algorithms. [Online]. Available: https://www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantum-cryptography-the-new-digital-signature-algorithms/

[16] 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, pp. 301–313, 2018.

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

[18] N. H. Minh, N. A. Moldovyan, A. A. Moldovyan, N. N. Hai, T. C. Manh, and P. N. H. Phieu, "Post-quantum cryptoschemes: New finite non-commutative algebras for defining hidden logarithm problem," in *Proc. Context-Aware Systems and Applications, and Nature of Computation and Communication*, 2018, pp. 183–194.

[19] N. A. Moldovyan and A. A. Moldovyan, "New forms of defining the hidden discrete logarithm problem," *SPIIRAS Proceedings*, vol. 18, no. 2, pp. 504–529, 2019.

[20] N. A. Moldovyan and P. A. Moldovyanu, "New primitives for digital signature algorithms," *Quasigroups and Related Systems*, vol. 17, no. 2, pp. 271–282, 2009.

[21] D. N. Moldovyan, A. A. Moldovyan, P. N. Han, and N. H. Minh, "Post-quantum Commutative Encryption Algorithm," in *Proc. Context-Aware Systems and Applications, and Nature of Computation and Communication*, 2019, pp. 205–214.

[22] R. Jozsa, "Quantum algorithms and the fourier transform," *Proc. Roy. Soc. London. A*, vol. 454, pp. 323–337, 1998.

[23] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Reviews of Modern Physics*, vol. 68, pp. 733–752, 1996.

[24] N. A. Moldovyan, "Fast signatures based on non-cyclic finite groups," *Quasigroups and Related Systems*, vol. 18, no. 1, pp. 83–94, 2010.

[25] Falcon: Fast-Fourier Lattice-base Compact Signatures over NTRU. [Online]. Available: https://falcon-sign.info/

[26] CRYSTALS: Cryptographic Suite for Algebraic Lattices. [Online]. Available: https://pq-crystals.org/dilithium/

[27] qTESLA: Efficient And Post-Quantum Secure Lattice-Based Signature Scheme. [Online]. Available: https://qtesla.org/

Minh Nguyen Hieu is a Vice dean of Institute of Cryptographic Science and Technology, Hanoi, Vietnam. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2006). His research interests include cryptography, communication and network security. He has authored or co-authored more than 85 scientific articles, books chapters, reports and patents, in the areas of his research.

Alexander A. Moldovyan is a chief researcher with the St. Petersburg Institute for Informatics and Automation of RAS, and a Professor with the Saint Petersburg Electrical Engineering University. His research interests include information assurance, computer security and applied cryptography. He has authored or co-authored more than 35 patents and 150 scientific articles, books, and reports. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (1996). Contact him at: maa1305@yandex.ru.

Nikolay A. Moldovyan is an honored inventor of Russian Federation (2002), a chief researcher with the St. Petersburg Institute for Informatics and Automation of RAS, and a Professor with the Saint Petersburg Electrical Engineering University. His research interests include computer security and cryptography. He has authored or co-authored more than 50 patents and 200 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981). Contact him at: nmold@mail.ru.

Canh Hoang Ngoc is a Lecturer in the Thuongmai University, Hanoi, Vietnam. He received his master-degree in information systems from Le Quy Don Technical University of Vietnam in 2012. His research interests include cryptography, database, machine learning. Currently, besides teaching, he works as a network administrator and database administrator at Thuongmai University.