Split logarithm problem and a candidate for a post-quantum signature scheme

A.A. Moldovyan, N.A. Moldovyan

Abstract

A new form of the hidden discrete logarithm problem, called split logarithm problem, is introduced as primitive of practical post-quantum digital signature schemes, which is characterized in using two non-permutable elements A and B of a finite non-commutative associative algebra, which are used to compute generators $Q = AB$ and $G = BQ$ of two finite cyclic groups of prime order q. The public key is calculated as a triple of vectors (Y, Z, T): $Y = Q^x$, $Z = G^w$, and $T = Q^a B^{-1} G^b$, where x, w, a, and b are random integers. Security of the signature scheme is defined by the computational difficulty of finding the pair of integers (x, w), although, using a quantum computer, one can easily find the ratio $x/w \bmod q$.

Keywords: finite associative algebra, non-commutative algebra, finite cyclic group, discrete logarithm problem, hidden logarithm problem, public key, digital signature, post-quantum cryptosystem.

MSC 2010: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50

1 Introduction

In the current field of development of post-quantum cryptographic algorithms and protocols [1], considerable attention of the world cryptographic community is paid to the development of two-key cryptographic schemes on algebras [2], [3], on Boolean functions [4], [5], and on linear codes [6], [7]. To develop a public-key cryptoscheme that is resistant to an attack including computations on a hypothetic quantum computer

doi:10.56415/csjm.v30.14

(quantum attack), one should use the computationally complex problems different from the factoring problem and the discrete logarithm problem (DLP), since each of them can be solved in polynomial time on a quantum computer [8]–[10].

The hidden discrete logarithm problem (HDLP) defined in the finite non-commutative associative algebras (FNAAs) is very attractive as a primitive of practical post-quantum digital signature (DS) schemes [11]–[13]. Several different forms of the HDLP and design criteria of the HDLP-bases DS schemes are considered in the papers [14], [15].

For a more complete understanding of the potential of the HDLP as a post-quantum cryptographic primitive, it is interesting to expand the set of forms of defining the HDLP. This article offers a new form called split logarithm problem (SLP). Next Section 2 considers the notions of DLP and HDLP and used notations. Section 3 introduces a novel form of the HDLP and a SLP-based signature scheme. Section 4 presents discussion and Section 5 concludes the paper.

2 Preliminaries

2.1 Use of the exponentiation as a base operation of public-key cryptoschemes

In the finite associative algebraic structures, the exponentiation can be performed sufficiently fastly and allows one to define a computationally complex problem, called DLP, well suitable for designing public-key cryptoschemes of different types (public key-agreement protocols, public encryption algarithms, signature schemes) and commutative encryption algorithms. The DLP is defined in a finite cyclic group as problem of finding an integer value x satisfying the equality

$$Y' = Q^x, \tag{1}$$

where Q is the group generator; Y' and Q are known elements of the group. Formula (1) is used to generate a public key in different DLP-based cryptoschemes. To set a required security of cryptoschemes, i. e., fairly high difficulty of the DLP, the group order should be prime and

have large size (256 to 2048 bits and more, depending on the type of the used cyclic group). In the known DLP-based DS schemes, the values Q and Y' are used as parameters of signature verification equations, i. e., usually they are public parameters of cryptoschemes. Since the Shor quantum algorithm [8] allows one to find effectively the logarithm value in any explicitly given cyclic group, the DLP-based cryptoschemes are not resistant to quantum attacks.

The idea of the HDLP consists in using the exponentiation as the base operation introducing the main contribution to the security of the public-key cryptoschemes and masking the parameters of the base cyclic group (the group in which the exponentiation operation is performed to calculate a public key). Thus, in the HDLP-based cryptoschemes the base cyclic group is hidden. Obviously, the HDLP must be set in some finite algebraic support, which includes a sufficiently large number of different cyclic groups, forming an environment in which some fixed cyclic group can be securely hidden. In addition, masking operations must have some special properties that ensure the correct operation of the cryptoscheme.

Different types of the FNAAs of different even dimensions have been proposed for their use as algebraic support of the HDLP-based cryptoschemes [3], [16]. The non-commutativity of the multiplication operation is a principal property of the FNAAs for defining the HDLP, which allows one to set the masking operations possessing the required properties, one of which is mutual commutativity with the exponentiation operation. The latter is provided when using the automorphism-map φ_A and homomorphism-map ψ_H operations for masking the base cyclic group. Masking operations are secret, therefore they should be dependent on selection of some random values.

The φ_A operation, parameterized by an invertible algebra element A, is defined in an FNAA containing a two-sided global unit E by the formula

$$\varphi_A(X) = AXA^{-1}, \tag{2}$$

where X takes on all values in the algebra. The $\psi_{L,H}$ operation, parameterized by a left-sided unit L and a locally invertible element H, can be defined in an FNAA containing a large set of left-sided global

units [17] by the formula

$$\psi_{L,H}(X) = HXH', \tag{3}$$

where X takes on all values in the algebra and the algebra element H' is such that $HH' = H'H = L$. It is easy to see that each of the masking operations set by the formulas (2) and (3) is mutually commutative with the exponentiation operation: $\varphi_A\left(X^k\right) = \left(\varphi_A(X)\right)^k$ and $\psi_{L,H}\left(X^k\right) = \left(\psi_{L,H}(X)\right)^k$. Some other types of masking operations are considered in [11], [13].

When using masking operation set by the formula (2), in the DS scheme [12] on a 4-dimensional FNAA the public key is formed as follows:

1. Select at random a non-invertible vector B generating a cyclic group of prime order q having fairly large size and a random non-negative integer $x < q$.

2. Select at random an invertible element G such that $GB \neq BG$ and calculate the first element Y of the public key: $Y = GB^xG^{-1}$.

3. Select at random an invertible element H such that $HB \neq BH$ and $GH \neq HG$ and calculate the second element Z of the public key: $Z = HBH^{-1}$.

4. Calculate the third element T of the public key: $T = GRH^{-1}$, where R is an invertible vector representing a local right-sided unit of the vector B (formulas describing sets of local right-sided anf left-sided units are presented in [12]).

The elements of the public key (Y, Z, T) are contained in three different cyclic groups and no element of the hidden group generated by the non-invertible vector B is known. To generate a signature only one secret parameter (the integer x) can be used, although many other secret values are used to calculate the public key. Therefore, one can define this form of the HDLP as finding the private key x that is discrete logarithm in a hidden group.

A certain disadvantage of the signature scheme [12] is the use of a hidden group generated by a non-invertible element of the FNAA used as algebraic support. However, in the signature scheme [12] based on this form of the HDLP, the said flaw seems to be unavoidable. In

section 3 of this paper, a new form of the HDLP, called SLP, is proposed, the application of which makes it possible to avoid using the signature scheme parameters that are non-invertible elements of the algebra. This possibility is due to the used new masking mechanism that consists in performing two exponentiation operations in two different cyclic groups of the same prime order, which are set by some two fixed secret elements of the FNAA.

2.2 The used algebraic support

To be used as algebraic support of the HDLP form proposed in the present paper, an FNAA should i) contain a two-sided global unit and ii) contain a sufficiently large set of cyclic groups of prime order q having a sufficiently large size (256 bits or more). Many FNAAs satisfying the first requirement are described in the literature, for example, see [11], [12], [16]. To satisfy the second criterion, an FNAA can be set over the finite ground field $GF(p)$, the characteristic of which has the structure $p = eq+1$, where q is a 256-bit prime; e is a small even number (usually $e = 2$).

As the used algebraic support, we have chosen the 4-dimensional FNAA defined over $GF(p)$ and described in [18]. We also use notations of [18]: $\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2$, and $\mathbf{e}_3$ are formal basis vectors; $a_0, a_1, a_2, a_3 \in GF(p)$ are coordinates of a vector $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + a_3\mathbf{e}_3$ that can be alternatively written as $A = (a_0, a_1, a_2, a_3)$. The vector multiplication operation of two vectors A and $B = b_0\mathbf{e}_0 + b_1\mathbf{e}_1 + b_2\mathbf{e}_2 + b_3\mathbf{e}_3$ is defined by the following formula

$$AB = \left(\sum_{i=0}^{3} a_i\mathbf{e}_i\right)\left(\sum_{j=0}^{3} b_j\mathbf{e}_j\right) = \sum_{j=0}^{3}\sum_{i=0}^{3} a_i b_j\left(\mathbf{e}_i\mathbf{e}_j\right),$$

where the product $\mathbf{e}_i\mathbf{e}_j$ for all possible pairs of the integers i and j is to be replaced by some single-component vector $\lambda\mathbf{e}_k$ indicated in the cell at intersection of the ith row and the jth column of so called basis vector multiplication table (BVMT) shown as Table 1, where $\lambda \neq 0$. The value $\lambda \neq 1$ is called structural constant.

Our choice is due to the fact that the vector multiplication operation in this algebra is given by a sparse BVMT, which reduces the compu-

Table 1. Setting the multiplication operation in the used FNAA [18].

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

tational complexity of multiplication and exponentiation operations by two times. The latter leads to a twofold increase in the performance of the developed signature scheme. In addition, the structure of the said FNAA is investigated in detail, and results of [18] show the algebra includes only three types of commutative subalgebras having the same order equal to p^2:

i) multiplicative group of which is generated by a minimum generator system containing two vectors of order $p-1$, the group order being equal to $(p-1)^2$; number of such subalgebras is equal to $p(p+1)/2$;

ii) multiplicative group of which is cyclic and has order $p(p-1)$; number of these subalgebras is equal to $p+1$;

iii) multiplicative group of which is cyclic and has order p^2-1; number of these subalgebras is equal to $p(p-1)/2$.

In this paper, we consider the case of defining the FNAA over the finite ground field $GF(p)$ characteristic of which has the structure $p = 2q+1$, where q is a 512-bit prime, and of using the cyclic groups of the order q that is a divisor of $p-1$, which are contained in the set of the commutative subalgebras of the first type. The vector $E = (1,1,0,0)$ is the global two-sided unit of the algebra. A vector G satisfying the condition $g_0g_1 \neq \lambda g_2g_3$ is invertible.

3 The split logarithm problem and a SLP-based signature scheme

3.1 Proposed form of the HDLP

Proposition 1. Suppose invertible vectors A and B are not permutable, and the vector $Q = AB$ has prime order equal to q. Then the vector $G = BA$ also has order equal to q.

Proof. By the condition, $Q^q = E \Rightarrow A(BA)^{q-1}B = E \Rightarrow A(BA)^{q-1} = B^{-1} \Rightarrow (BA)^{q-1} = A^{-1}B^{-1} = (BA)^{-1} \Rightarrow G^{q-1} = G^{-1}$ and $G^q = E$. Proposition 1 is proven. □

Proposition 2. Suppose invertible vectors A and B are not permutable; $Q = AB$ and $G = BA$. Then the equality $Q^k = AG^{k-1}B$ holds true.

Proof. $Q^k = (AB)^k = A(BA)^{k-1}B \Rightarrow AG^{k-1}B$. Proposition 2 is proven. □

Using the algorithm [18] for the generation of a group having 2-dimensional cyclicity, one can easily generate at random a vector Q' of order $p-1$, which is not a scalar vector, and compute the vector $Q = Q'^2$ having order equal to q. Then, fixing a vector A that is not permutable with Q, one can compute the vectors $B = A^{-1}Q$ and $G = BA$. The proposed new form of the HDLP follows from the next procedure for generating a public key that will be used in the signature scheme described in the Subsection 3.2 of the article:

1. Generate two random vectors A and B such that both of the vectors $Q = AB$ and $G = BA \neq Q$ have the same order q and the vector G is not a scalar vector.

2. Select at random non-negative integer $x < q$ and a primitive element α (modulo p). Then compute the first public key element $Y = (AB)^x\alpha = Q^x\alpha$.

3. Select at random non-negative integer $w < q$ and compute the second public-key element $Z = (BA)^w = G^w$.

4. Generate two random integers $a < q$ and $b < q$ and calculate the third signature element $T = Q^aB^{-1}G^b$.

Note that each of the vectors Q and G together with a scalar vector

$N = (n, n, 0, 0)$, where $n \in GF(p)$ is an element of order q, compose a minimum generator system of a 2-dimensional cyclicity group (contained in a commutative subalgebra of the first type).

The calculated public key (Y, Z, T) is intended for use in a DS scheme in which the known parameters are the parameters for setting the algebraic support and the public key elements, i. e., the vectors Y, Z, and T. The values x and w represent logarithms of the values Y and Z contained in two different cyclic groups (in the case, when the basis of logarithm is hidden, i. e., unknown). All other values used while calculating the public key are secret. The known value T connects the said cyclic groups. The logarithms x and w are connected via the public-key element T and one can propose a method for generating a signature, when using the values of the ratio $x/w \bmod q$ and α (see alternative signature generation algorithm in the next Subsection 3.2). Therefore, the introduced form of the HDLP can be called split logarithm problem (SLP).

3.2 Candidate for a practical post-quantum DS scheme

To generate a signature to some electronic document M, the owner of public key (Y, Z, T) (a person that had supposedly generated this key) should use some secret parameters, the set of which is called a private key. In the proposed SLP-based signature scheme it is sufficient to use only three secret values, namely, integers x, w, and α. However, in this case, an alternative signature generation procedure is to be applied, in which two exponentiation operations are executed; whereas, when using the private key, including the values A, G, x, w, α, and d $(d = a + b \bmod q)$, the following signature generation procedure, including only two exponentiation operations, outputs a genuine signature.

Algorithm for generating a signature.

1. Generate at random an integer $k < q$ and an integer $\rho < p$. Then calculate the vector $R = AG^k\rho$.

2. Compute the first 512-bit signature element e from the document M to which the vector R is concatenated: $e = f_H(M, R)$, where f_H is a pre-agreed collision-resistant 512-bit hash-function.

3. Compute the second 512-bit signature element s:

$$s = \frac{k - d - ex + 1}{x + we} \bmod q.$$

4. Compute the third 512-bit signature element σ: $\sigma = \rho\alpha^{-(e+s)}$.

On the average, computation of a 1024-bit signature (e, s, σ) requires performing one exponentiation operation in the FNAA (6144 multiplications modulo p) which makes a major contribution to the computational complexity of the signature generation procedure and one exponentiation operation in $GF(p)$ (768 multiplications modulo p). The verification of the signature (e, s, σ) to the document M is performed using the public key (Y, Z, T) and the following algorithm.

Signature verification algorithm.

1. Using the public key, compute the vector R':

$$R' = Y^{e+s}TZ^{se}\sigma.$$

2. Compute the hash-function value $e' = f_H(M, R')$.

3. If $e' = e$, then the signature is accepted as a genuine one. Otherwise, the signature is rejected.

The computational complexity of the signature verification procedure is roughly equal to two exponentiation operations in the FNAA used as algebraic support and one exponentiation operation in $GF(p)$ (totally, ≈ 13056 multiplications modulo p).

Correctness proof of the developed SLP-based signature scheme implies demonstrating that the correctly computed signature (e, s) passes the verification procedure as a genuine one. Due to Propositions 1 and 2, we have the following:

$$\begin{aligned} R' = Y^{e+s}TZ^{se}\sigma &= Q^{xe+xs}\alpha^{e+s}Q^aB^{-1}G^bG^{wse}\rho\alpha^{-(e+s)} = \\ &= Q^{xe+xs+a}B^{-1}G^{wse+b} = AG^{xe+xs+a-1}BB^{-1}G^{wse+b} = \\ &= AG^{s(x+we)+xe+d-1}\rho = A \circ G^k\rho = R \;\Rightarrow\; R' = R \;\Rightarrow\; e' = e. \end{aligned}$$

Alternative signature generation algorithm.

1. Generate at random integers t $(0 < t < q)$, u $(0 < u < q)$, and ρ $(0 < \rho < p)$. Then calculate the vector $R = Y^t T Z^u \rho$ (note: $R = AG^k \rho$, where $k = tx - 1 + a + b + wu \bmod q$).

2. Compute the value $e = f_H(M, R)$.

3. Compute the value s:

$$s = \frac{(t-e)x + wu}{(x + we)} \bmod q = \frac{(t-e)xw^{-1} + u}{(xw^{-1} + e)} \bmod q. \qquad (4)$$

4. Compute the third signature element σ: $\sigma = \rho\alpha^{-(e+s)} \bmod p$

4 Discussion

One of the features of the proposed signature scheme is the use of the scalar multiplication operation when calculating the first element Y of the public key and vectors R (in the signature generation algorithm) and R' (in the signature verification algorithm). Without introducing scalar multiplication operations, the signature scheme is somewhat simplified, but the rationale for using multiplications by scalars is that they make it computationally feasible to construct a periodic function with a period length that depends on the values of x and w. Consider a simplified version of the proposed signature scheme with the signature (e, s), when calculation of the first public-key element and the said vectors is executed by the following formulas: $Y_0 = (AB)^x = Q^x$, $R = AG^k$, and $R' = Y^{e+s} T Z^{se}$.

Proposition 3. The private key elements A and G satisfy the inequality $AG \neq GA$, i. e. they are not permutable.

Proof. Assume the opposite: $AG = GA$. Taking into account that $G = BA$, we have: $ABA = BA^2 \Rightarrow ABAA^{-1} = BA^2A^{-1} \Rightarrow AB = BA$. The latter equality contradicts the fact that in the proposed signature scheme, the vectors A and B are not permutable. Proposition 3 is proven. □

Proposition 4. For integer variable $k = 0, 1, \ldots q-1$, the function $F(k) = AG^k$, where A and G are elements of the private key of the introduced signature scheme, takes on values in q different cyclic groups.

Proof. Assume the opposite: for some two integes k and t, satisfying the conditions $0 \le k < q$ and $0 \le t < k$, the vectors $F(k)$ and $F(t)$ are contained in the same cyclic group Γ of some order ω. The latter means that for some two integers i and j (suppose for the sake of certainty that $i > j$) we have $F(k) = V^i$ and $F(t) = V^j$, where V is a generator of the cyclic group Γ, i. e., $AG^k = V^i$ and $AG^t = V^j$. Therefore, $AG^k = V^i = V^j V^{i-j} = AG^t V^{i-j} \Rightarrow G^{k-t} = V^{i-j}$. Since $k - t$ and q are mutually prime numbers, one can write $G = V^{\frac{i-j}{k-t}} = V^z$, where z is an integer number.

Thus, $AG^k = V^i \Rightarrow AV^{kz} = V^i \Rightarrow AV^{kz-i \bmod \omega} = E \Rightarrow A = V^{-(kz-i) \bmod \omega}$. The latter equality means that $A \in \Gamma$; therefore, A and V are permutable: $AV = VA \Rightarrow AG^k = AV^{zk} = V^{zk}A = G^k A$, i. e. $AG^k = G^k A$. Taking into account that $G = \left(G^k\right)^{z'}$, where the integer $z' = k^{-1} \bmod q$, one gets: $A\left(G^k\right) = \left(G^k\right)A \Rightarrow AG = GA$, i. e. the vectors A and G are permutable. However, this contradics Proposition 3. The resulting contradiction proves Proposition 4. $\square$

According to the public parameters of the simplified signature scheme, you can directly set a periodic function containing a period with a length that depends on the values of x and w, namely, the function $F_0(i, j) = Y_0^i T Z^j$ in two integer variables i and j. Proposition 4 shows the values of this function are distributed evenly across q different cyclic groups (note: $F_0(i, j) = AG^{i+j}$).

However, one can specify a periodic function, the use of which makes it possible to calculate the ratio of secret values x and w on a hypothetic quantum computer. Indeed, it is easy to show: $Z^* = TZT^{-1} = Q^w$ and the periodic function $F_0(i, j) = Y_0^i Z^{*j}$ in two integer variables i and j contains a period with the length $(-1, xw^{-1})$:

$$F_0(i-1, j+xw^{-1}) = Y_0^{i-1} Z^{*j+xw^{-1}} = Q^{x(i-1)} Q^{w(j-xw^{-1})} =$$
$$= Q^{xi} Q^x Q^{wj} Q^{-x} = Y_0^i Z^{*j} = F_0(i, j).$$

This function takes on the values in an explicitly specified cyclic group (that is generated by the vector Z^*). Therefore, using the Shor quantum algorithm, one can easily find the period length $(-1, xw^{-1})$ and, using the value of the ratio $\frac{x}{w}$, compute signatures, using the alternative signature generation algorithm.

Using an additional scalar multiplication, when computing the $Y = Q^x\alpha$ element of the public key, constructon of the periodic functions taking on the values in a fixed cyclic group and containing a period depending on the value x or/and w becomes computationally infeasible. Indeed, it is easy to see that the vectors Y and Z^* compose a minimum generator system of a commutative 2-dimensional cyclicity group of order q^2 (since the vectors Y_0 and Z^* are elements of the same cyclic group of order q). Therefore, the function $F(i,j) = Y^i Z^{*j}$ takes on all values in the said group and has a period with the length (q,q). Thus, the criterion of post-quantum resistance [14] is satisfied in the proposed SDL-based signature scheme. This explains why the proposed signature scheme uses vectors Q and G belonging to commutative subalgebras of the first type.

The reductionist security-proof method [19] that was applied to the Schnorr DLP-based signature scheme [20] can also be applied to the developed SLP-based DS scheme. Like in the Schnorr DS scheme, in the developed one, during the signature generation process the base exponentiation operation G^k is performed before calculating the first signature element $e = f_H(M,R)$, where $R = AG^k$.

In the model [19] of reductionist security-proof, it is assumed a signature forger is able to calculate the second signature element s equally well for two different hash functions f_H and f'_H (it is supposed that the hash function f_H is collision-resistant and free of properties that can be used to forge a signature [21]). Using the same input data, the forger executes two computer programs, each of which uses the same value of k, but different hash functions. The forger obtains two different signatures (e,s) and (e',s') for fixed value k and different values e and e'. Thus, the forger gets two linear equations with the unknown value of k and the unknown value of the discrete logarithm x. In the Schnorr signature scheme [20], the discrete logarithm represents one integer x and the second signature element $s = k + ex \bmod q$, therefore, the forger, using the obtained two equations, can calculate the private key x.

In the case of the proposed SLP-based DS scheme, the second signature element can be calculated by the formula (4) with three unknowns $x/w \bmod q$, t, and u, where the ratio x/w represents the split logarithm.

Therefore, the security-proof method [19] is to be extended to the case of forger's computing three different signatures (e_1, s_1, σ_1), (e_2, s_2, σ_2), and (e_3, s_3, σ_3), when using three different hash functions and fixed values of t, u, and ρ (the latter fixes the vector R in the alternative signature generation algorithm). As a result, the forger composes a system of three linear equations with three unknowns: $x/w \bmod q$, t, and u. Then, solving this system, the forger gets the values of every of the indicated unknowns. The unknown value of α is computed as follows:

$$\alpha = \left(\frac{\sigma_1}{\sigma_2}\right)^{(e_2+s_2-e_1-s_1)^{-1} \bmod q}.$$

Thus, an assumption of the existence of an algorithm for breaking the proposed signature scheme leads to the conclusion that there is an effective algorithm for calculating the values of $x/w \bmod q$ and α. This means that the analysis of the security of the proposed signature scheme is reduced to the analysis of the computational complexity of solving the SLP. The latter is the task of independent research.

A rough comparison of the proposed DS scheme with some known candidates for post-quantum signature schemes is presented in Table 2 (in the case of setting the used FNAAs over $GF(p)$ with 512-bit prime p) which demonstrates the introduced SLP-based DS scheme has advantages in the size of parameters and peformance (lower execution time; *estimated in multiplications modulo p), which are significant from a practical point of view.

5 Conclusion

A new form of the HDLP, called SLP, has been proposed as a primitive for developing post-quantum cryptoschemes. A comparison of the developed SLP-based DS scheme with other candidates for post-quantum signature algorithms shows the former is more attractive from a practical point of view due to its smaller size of public key and signature. However, more detailed security analysis is to be performed as independent research work. Developing new forms of the SLP and combining the current version of the SLP with a known form of the HDLP in

Table 2. A rough comparison of some DS schemes.

Signature scheme	signature size, bytes	public-key size, bytes	sign. gener. time*	sign. verific. time*
[14]	256	1536	$\approx 37,000$	$\approx 49,000$
[15]	320	2316	$\approx 83,000$	$\approx 110,600$
[11]	256	1536	$\approx 61,400$	$\approx 49,200$
[12]	128	768	$\approx 12,300$	$\approx 24,600$
Falcon [22]	1280	1793	–	–
Dilithium [23]	2701	1472	–	–
Proposed	128	768	$\approx 6,000$	$\approx 12,300$

framework a single signature scheme also represent interest for further research.

Acknowledgement. *This work was supported by the budget theme No. FFZF-2022-007.*

References

[1] *Post-Quantum Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019*, (Lecture Notes in Computer Science, vol. 11505), 2019.

[2] A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, and A. A. Nechaev, "Cryptographic Algorithms on Groups and Algebras," *Journal of Mathematical Sciences*, vol. 223, no. 5, pp. 629–641, 2017.

[3] 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. Ser. Mathematical Modelling, Programming & Computer Software*, vol. 12, no. 1, pp. 66–81, 2019. DOI: 10.14529/mmp190106.

[4] G. P. Agibalov and I. A. Pankratova, "Asymmetric cryptosystems on Boolean functions," *Prikl. Diskr. Mat.*, no. 40, pp. 23–33, 2018. DOI: 10.17223/20710410/40/3.

[5] G. P. Agibalov, "ElGamal cryptosystems on Boolean functions," *Prikl. Diskr. Mat.*, no. 42, pp. 57–65, 2018. DOI: 10.17223/20710410/42/4.

[6] Q. Alamelou, O. Blazy, S. Cauchie, and Ph. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, pp. 469–493, 2017.

[7] Y. V. Kosolapov and O. Y. Turchenko, "On the construction of a semantically secure modification of the McEliece cryptosystem," *Prikl. Diskr. Mat.*, no. 45, pp. 33–43, 2019. DOI: 10.17223/20710410/45/4.

[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] A. Ekert and R. Jozsa, "Quantum computation and Shorś factoring algorithm," *Rev. Mod. Phys.*, vol. 68, p. 733, 1996.

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

[11] N.A. Moldovyan and A.A. Moldovyan, "Candidate for practical post-quantum signature scheme," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 16, no. 4, pp. 455–461, 2020. https://doi.org/10.21638/11701/spbu10.2020.410

[12] 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.

[13] D.N. Moldovyan, "New Form of the Hidden Logarithm Problem and Its Algebraic Support," *Bulletin of Academy of Sciences of Moldova. Mathematics*, no. 2(93), pp.3–10, 2020.

[14] 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.

[15] D. N. Moldovyan, A. A. Moldovyan, and N. A. Moldovyan, "An enhanced version of the hidden discrete logarithm problem and its algebraic support," *Quasigroups and Related Systems*, vol. 28, no. 2, pp. 269–284, 2020.

[16] 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, 2020.

[17] 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.

[18] D. N. Moldovyan, "A practical digital signature scheme based on the hidden logarithm problem," *Computer Science Journal of Moldova*, vol. 29, no. 2(86), pp. 206–226, 2021.

[19] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.

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

[21] N. Koblitz and A. J. Menezes, "Another Look at "Provable Security"," *Journal of Cryptology*, vol. 20, pp. 3–38, 2007.

[22] "Fast-Fourier lattice-based compact signatures over NTRU," https://falcon-sign.info/

[23] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A Lattice-Based DigitalSignature Scheme," https://eprint.iacr.org/2017/633.pdf (see also https://pq-crystals.org/dilithium/index.shtml).

A. A. Moldovyan, N. A. Moldovyan

Received January 21, 2021
Accepted February 21, 2022

St. Petersburg Federal Research Center of
the Russian Academy of Sciences (SPC RAS)
14 Liniya, 39, St.Petersburg, 199178
Russia
E–mail: nmold@mail.ru