UDC 512.552.18+003.26 Вестник СПбГУ. Прикладная математика. Информатика ... 2020. Т. 16. Вып. 4
MSC 16P10

Candidate for practical post-quantum signature scheme

N. A. Moldovyan, A. A. Moldovyan

St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39, 14-ia linia, St. Petersburg, 199178, Russian Federation

For citation: Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2020, vol. 16, iss. 4, pp. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410

A new criterion of post-quantum security is used to design a practical signature scheme based on the computational complexity of the hidden discrete logarithm problem. A 4-dimensional finite non-commutative associative algebra is applied as algebraic support of the cryptoscheme. The criterion is formulated as computational intractability of the task of constructing a periodic function containing a period depending on the discrete logarithm value. To meet the criterion, the hidden commutative group possessing the 2-dimensional cyclicity is exploited in the developed signature scheme. The public-key elements are computed depending on two vectors that are generators of two different cyclic groups contained in the hidden group. When computing the public key two types of masking operations are used: *i*) possessing the property of mutual commutativity with the exponentiation operation and *ii*) being free of such property. The signature represents two integers and one vector S used as a multiplier in the verification equation. To prevent attacks using the value S as a fitting element the signature verification equation is doubled.

Keywords: digital signature, post-quantum cryptoscheme, public key, hidden logarithm problem, finite non-commutative algebra, associative algebra.

1. Introduction. Current cryptographic standards of the digital signature algorithms and public key-agreement protocols do not provide post-quantum resistance, since they are based on the computational difficulty of the factoring problem and of the discrete logarithm problem which can be solved on a hypothetic quantum computer in polynomial time [1, 2]. The development of practical public-key post-quantum cryptoschemes attracts much attention of the cryptographic community [3, 4].

One of the attractive approches to the development of post-quantum signature schemes is applying the hidden discrete logarithm problem (HDLP) as the base cryptographic primitive [5–7]. The rationale of the post-quantum security of the known signature algorithms based on the HDLP takes into account that the quantum algorithm for finding the discrete logarithm value exploits the extremely high efficiency of quantum computer to perform a discrete Fourier transform for a function that takes values in a finite cyclic group [1, 8]. To solve the problem of finding the logarithm value x, i. e., to solve the equation $Y = G^x$, where $x < q$ is the unknown integer; Y and G are known elements of a finite cyclic group of the prime order q, one constructs a periodic function $F(i,j) = Y^i \circ G^j$ in two integer variables i and j, which contains a period with the length $(-1,x)$: $F(i,j) = Y^i G^j = Y^{i-1} G^{j+x} = F(i-1, j+x)$. From the discrete Fourier transform results the perion length $(-1,x)$ is easily computed.

For the case of the HDLP-based signature schemes considered in papers [5–7] one can construct the periodic function $F(i,j) = Y^i \circ T \circ Z^j$, where Y, T and Z are m-dimensional

vectors; $\circ$ is the multiplication operation in the finite non-commutative associative algebra (FNAA) used as algebraic support of the signature scheme. This function includes period with the length $(-1, x)$, however, the function $F(i, j)$ takes on the values that lie in different cyclic groups and there is no preferable cyclic group for the values of this function.

Thus, the design criterion related to the know HDLP-based signature algorithms can be formulated as the following one.

Criterion 1. *The periodic functions $F(i, j)$ constructed on the base of public parameters of the signature scheme and containing a period with the length depending on the discrete logarithm value should take on values in different finite cyclic groups contained in the FNAA. Besides, no cyclic group can be pointed out as a preferable finite group for the values of the function $F(i, j)$.*

In present paper we use another design criterion for providing post-quantum resistance of the HDLP-based signature algorithms. To meet the accepted criterion, a new method of setting the HDLP is used, which is characterized by the use of a hidden commutative group with two-dimensional cyclicity and masking operations of the following types: *i*) having the property of mutual commutativity with the exponentiation operation in the hidden group; *ii*) not having such a property.

2. Advanced criterion of post-quantum resistance. Criterion 1 takes into account the currently known quantum algorithm for finding the period length for a periodic function which values lie in some fixed finite cyclic group. However, one can assume that in the future, novel quantum algorithms will be developed that will effectively find the period length for functions that take on values within the framework of the whole FNAA used as algebraic support of the signature scheme. Taking into account such potential possibility the following *advanced* criterion of the post-quantum resistance is applied in this paper for the development of a post-quantum signature scheme.

Criterion 2. *Based on the public parameters of the signature scheme, the construction of a periodic function containing a period with the length depending on the discrete logarithm value should be a computationally intractable task.*

To design a signature scheme satisfying this criterion it is used the idea of masking periodicity depending on the discrete logarithm value. To implement this idea, we propose to perform the exponentiation operation, which introduces the main contribution to the security, in a cyclic group (called basic cyclic group) that is a subgroup of a hidden commutative group having two-dimensional cyclicity. (A finite commutative group is called group with the μ-dimensional cyclicity, if its minimum generator system includes μ elements possessing the same order value [9].)

To implement the said idea, there is used a hidden commutative group having order q^2, in which every element (except the unit) possesses order equal to the prime q. The public-key elements are calculated based on two independent elements of the hidden group. One of the latter is the generator of the base cyclic group, and the second is used as a masking multiplier that imposes a periodicity having length equal to the value q.

3. The used FNAA. Consider a finite m-dimensional vector space defined over the field $GF(p)$. Defining additionally the vector multiplication operation that is distributive at the right and at the left relatively the addition operation, one gets the m-dimensional finite algebra. Some vector A can be represented in two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ... , $\mathbf{e}_{m-1}$ are basis vectors. The vector multiplication operation ($\circ$) of two m-dimensional vectors A and B is set as follows:

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

where every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by a single-component vector $\lambda \mathbf{e_k}$, here $\lambda \in GF(p)$, indicated in the cell at the intersection of the i-th row and j-th column of so called basis vector multiplication table (BVMT), like Table 1. To define associative vector multiplication operation one should construct the BVMT that defines associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$: $(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)$.

Table 1. **The BVMT defining the used FNAA ($\lambda \neq 1$; $\lambda \neq 0$)**

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

To develop the signature scheme that meets Criterion 2 we have used the 4-dimensional FNAA with the multiplication operation defined by the BVMT shown in Table 1, where $\lambda \neq 1$; $\lambda \neq 0$ [5]. This FNAA contains global two-sided unit E that can be computed as

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

The vectors A satisfying the condition $a_0 a_1 \neq a_2 a_3$ are invertible. The vectors N satisfying condition $n_0 n_1 = n_2 n_3$ are non-invertible.

Proposition. The number of the invertible vectors in the considered 4-dimensional FNAA is equal to $\Omega = p\,(p+1)\,(p-1)^2$.

P r o o f. The number of the locally invertible vectors is equal to the number of all elements of the algebra (p^4) minus the number on non-invertible vectors N. Let us compute the number of the vectors N for which we have $n_0 n_1 = n_2 n_3$. For the case $n_1 \neq 0$ ($p-1$ different values of n_1) the coordinades n_2 and n_3 are arbitrary (p^2 variants) and $n_0 = n_2 n_3 n_1^{-1}$, therefore, we have $(p-1)p^2$ non-invertible vectors related to this case. For the case $n_1 = 0$, at least, one of the values n_2 and n_3 should be equal to 0 ($2p-1$ variants) and in every of such variants the coordinate n_0 is arbitrary. Therefore, the last case gives $p(2p-1)$ more non-invertible vectors. Totally, there exists $(p-1)p^2 + p(2p-1) = p^3 + p^2 - p$ different non-invertible vectors. For the value Ω we get: $\Omega = p^4 - p^3 - p^2 + p = p\,(p+1)\,(p-1)^2$. □

The value Ω is the order of multiplicative group of the algebra. The maximum possible order of the invertible vectors in the considered algebra is equal to $\left(p^2 - 1\right)$. To have possibility to define the hidden commutative group containing cyclic groups of the prime order q having sufficiently large size, we suppose the considered FNAA is defined over the finite field $GF(p)$ with 256-bit characteristic $p = 2q + 1$, where q is a 255-bit prime.

A commutative group of the order q^2 can be set as computation of its basis $< G, Q >$ including two independent vectors of the same order q. The procedure of setting the basis $< G, Q >$ is as follows:

a) select a random invertible vector R_1 and compute $G_1 = R_1^{2(p+1)} \neq E$;

b) select a random invertible vector R_2 and compute $G_2 = R_2^{2(p+1)} \neq E$;

c) if $G_1 \circ G_2 = G_2 \circ G_1$, then go to step 1. Otherwise take $G = G_1$;

d) select a random integer r and compute $b = r^{2(p+1)} \bmod p \neq 1$;

e) performing scalar multiplication, compute the vector $Q = bG$.

At the output of this procedure we have the basis $< G, Q >$ of the commutative group of the order q^2 which possesses the 2-dimensional cyclicity. One can easily see that the order of each of the vectors G and Q is equal to the prime q.

4. Computation of the public-key. The public-key represents two triples of the 4-dimensional vectors (U_1, Y_1, Z_1) and (U_2, Y_2, Z_2) that are computed as follows.

1. Generate at random the basis $< G, Q >$ of the hidden commutative group Γ possessing the 2-dimensional cyclicity.

2. Select two random integers r_1 and r_2 and compute the vector $J = G^{r_1} \circ Q^{r_2} \in \Gamma$.

3. Generate at random the invertible vector B_1 and compute the vector $Y_1 = B_1 \circ G \circ B_1^{-1}$.

4. Generate at random the invertible vector A_1 and the integer x $(1 < x < q)$. Then compute the vectors $U_1 = A_1 \circ G^x \circ B_1^{-1}$ and $Z_1 = B_1 \circ Q \circ A_1^{-1}$.

5. Generate at random the invertible vector B_2 and compute the vector $Y_2 = B_2 \circ J \circ B_2^{-1}$.

6. Generate at random integer w $(1 < w < q)$. Then compute the vectors $W = Q^w$, $A_2 = A_1 \circ W$, $U_2 = A_2 \circ J^x \circ B_2^{-1}$, and $Z_2 = B_2 \circ Q \circ A_2^{-1}$.

The integers x, w and the vectors G, Q, J, A_1, B_1, A_2, B_2, and W are private elements. The private key represents the subset $\{x, G, Q, J, A_1, A_2, W\}$ of private elements that are used when computing a signature. The size of the public-key (U_1, Y_1, Z_1); (U_2, Y_2, Z_2) is equal to 768 bytes.

Signature generation procedure:

• Generate at random the integer k $(1 < k < q)$ and the invertible vector K. Then compute $V_1 = A_1 \circ G^k \circ K$ and $V_2 = A_2 \circ J^k \circ W^{-1} \circ K$.

• Using a specified hash function f_H, compute the first signature element e: $e = f_H(M, V_1, V_2)$, where M is a document to be signed.

• Compute the second signature element s as one of two solutions of the equation $s^2 + xs = k \bmod q$. If the equation has no solution, then go to step 1.

• Compute the third signature element $S = A_1 \circ Q^{-s} \circ K$. (Note $S = A_2 \circ W^{-1} \circ Q^{-s} \circ K$.)

On the average, computation of one 192-byte signature (e, s, S) requires performing the signature generation procedure two times. On the whole the computational difficulty of the signature generation procedure is roughly equal to four exponentiation operations in the 4-dimensional in FNAA.

Signature verification procedure:

• Using the signature (e, s, S) and the public-key (Y_1, Z_1, T_1); (Y_2, Z_2, T_2) compute the vectors $V_1' = (U_1 \circ Y_1^{es} \circ Z_1)^s \circ S$ and $V_2' = (U_2 \circ Y_2^{es} \circ Z_2)^s \circ S$.

• Compute the hash-function value $e' = f_H(M, V_1', V_2')$.

• If $e' = e$ and $S = (s_0, s_1, s_2, s_3)$ is such that $s_0 s_1 \neq s_2 s_3$, then the signature is genuine. Otherwise the signature is rejected.

5. Correctness proof. Correctness proof of the sigature scheme consists in proving that the signature (e, s, S) computed correctly will pass the verification procedure as genuine signature:

$$V_1' = (U_1 \circ Y_1^{es} \circ Z_1)^s \circ S =$$
$$= \left(A_1 \circ G^x \circ B_1^{-1} \circ \left(B_1 \circ G \circ B_1^{-1}\right)^{es} \circ B_1 \circ Q \circ A_1^{-1}\right)^s \circ A_1 \circ Q^{-s} \circ K =$$

$$= A_1 \circ G^{xs} \circ G^{es^2} \circ Q^s \circ A^{-1} \circ A_1 \circ Q^{-s} \circ K =$$
$$= A_1 \circ G^{es^2+xs} \circ K = A_1 \circ G^k \circ K = V_1;$$
$$V_2' = (U_2 \circ Y_2^{es} \circ Z_2)^s \circ S =$$
$$= \left(A_2 \circ J^x \circ B_2^{-1} \circ \left(B_2 \circ J \circ B_2^{-1}\right)^{es} \circ B_2 \circ Q \circ A_2^{-1}\right)^s \circ A_2 \circ W^{-1} \circ Q^{-s} \circ K =$$
$$= A_2 \circ J^{xs} \circ J^{es^2} \circ Q^s \circ A_2^{-1} \circ A_2 \circ Q^{-w} \circ Q^{-s} \circ K =$$
$$= A_2 \circ J^{es^2+xs} \circ Q^{-w} \circ K = A_2 \circ J^k \circ W^{-1} \circ K = V_2.$$

Since $V_1' = V_1$ and $V_2' = V_2$, the equality $e' = e$ holds true. Besides, in the signature (e, s, S) computed correctly the invertibility condition $s_0 s_1 \neq s_2 s_3$ is satisfied for the vector $S = (s_0, s_1, s_2, s_3)$.

6. Discussion. Among nine post-quantum signature schemes developed in framework of the NIST competition the algorithms Falcon [https://falcon-sign.info/] and Dilithium [https://pq-crystals.org/dilithium/index.shtml] attracts attention from the view point of the trade off between performance and size of the public-key and the signature. Table 2 presents a rough comparison of the proposed signature scheme with Falcon-512 and Dilithium-1024x768 (versions related to the 128-bit security level). The algorithm proposed in this article has a significant advantage in the size of the signature. Besides, it has higher performance of the signature verification procedure.

Table 2. **Comparison with the signature schemes Falcon-512, Dilithium-1024x768, RSA-2048**

Signature scheme	Signature size, bytes	Public-key size, bytes	Signature generation rate, arbitrary units	Signature verification rate, arbitrary units
Falcon-512	657	897	50	25
Dilithium-1024x768	2044	1184	15	10
RSA-2048	256	256	10	> 50
Proposed	192	768	40	60

Consider construction of some periodic functions on the base of public parameters of the proposed signature algorithm.

1. Suppose the function $F_1(i,j) = Y_1^i (Z_1 \circ U_1)^j = B_1 \circ G^{i+xj} \circ Q^j \circ B_1^{-1}$ contains a period with the length (δ_i, δ_j). Then, takin into account that G and Q are generators of different cyclic groups of the same order q, we have: $\delta_i + x\delta_j \equiv 0 \bmod q$ and $\delta_j \equiv 0 \bmod q \Rightarrow \delta_i \equiv \delta_j \equiv 0 \bmod q$. The last means the function $F_1(i,j)$ possesses only the periodicity connected with the value q that is order of cyclic groups contained in the hidden commutative group with 2-dimensional cyclicity.

2. Suppose the function $F_2(i,j) = (U_2 \circ Z_2)^i \circ (U_2 \circ Y_2 \circ Z_2)^j = A_2 \circ G^{xi+xj+j} \circ Q^{i+j} \circ A_2^{-1}$ includes a period with the length (δ_i, δ_j). Then, we have $x\delta_i + x\delta_j + \delta_j \equiv 0 \bmod q$ and $\delta_i + \delta_j \equiv 0 \bmod q \Rightarrow \delta_i \equiv \delta_j \equiv 0 \bmod q$. Thus, the function $F_1(i,j)$ possesses only the periodicity connected with the value q.

3. Suppose the function $F_3(i,j,k) = (U_2 \circ Z_2)^i \circ \left(U_2 \circ Y_2^j \circ Z_2\right)^k = A_2 \circ G^{xi+xj+jk} \circ Q^{i+j} \circ A_2^{-1}$ includes a period with the length $(\delta_i, \delta_j, \delta_k)$. Then, we have $x\delta_i + x\delta_j + j\delta_i - i\delta_j - \delta_i\delta_j \equiv 0 \bmod q$ and $\delta_i + \delta_j \equiv 0 \bmod q$. When solving simultaneously the last two congruencies relatively the unknowns δ_i and δ_j, one will obtain solutions that depends on the values i and j, except the solution $(\delta_i, \delta_j) = (0,0)$. This means that the function $F_3(i,j,k)$ possesses only the periodicity with the length (q,q).

7. Conclusion. An advanced criterion of post-quantum security has been applied to develop a new HDLP-based digital signature schemes that is a candidate for practical post-

quantum signature algorithms. The proposed design is characterized in applying the hidden commutative group possessing 2-dimensional cyclicity and masking operations that are not mutually commutative with the exponentiation operation. Besides, a doubled verification equation had been applied to prevent attacks using the signature element S as a fitting parameter.

References

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

2. Yan S. Y. *Quantum attacks on public-key cryptosystems*. Boston, Springer Publ., 2013, 207 p.

3. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018 Proceedings*. Fort Lauderdale, FL, USA, April 9–11, 2018. (Lecture Notes in Computer Science, 2018, vol. 10786.)

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

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

6. Moldovyan A. A., Moldovyan N. A. Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Series Mathematical Modelling, Programming & Computer Software*, 2019, vol. 12, no. 1, pp. 66–81.

7. Moldovyan N. A. Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2019, no. 1(89), pp. 71–78.

8. Jozsa R. Quantum algorithms and the fourier transform. *Proc. Roy. Soc. London. Series A*, 1998, vol. 454, pp. 323–337.

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

Received: January 27, 2020.
Accepted: October 23, 2020.

Authors' information:

Nikolay A. Moldovyan — Dr. Sci. in Technics, Professor, Chief Researcher; nmold@mail.ru

Alexandr A. Moldovyan — Dr. Sci. in Technics, Professor, Chief Researcher; maa1305@yandex.ru

Практичная постквантовая схема подписи

Н. А. Молдовян, А. А. Молдовян

Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Российская Федерация, 199178, Санкт-Петербург, 14-я линия, 39

Для цитирования: *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461.
https://doi.org/10.21638/11701/spbu10.2020.410

Для построения практичной схемы подписи, основанной на вычислительной сложности скрытой задачи дискретного логарифмирования, использован новый критерий постквантовой стойкости. В качестве алгебраического носителя криптосхемы применена четырехмерная конечная некоммутативная ассоциативная алгебра. Критерий сформулирован как вычислительная невозможность построения периодической функции, содержащей период, длина которого зависит от значения дискретного логарифма. Для выполнения критерия в разработанной схеме подписи используется скрытая коммутативная группа с двухмерной цикличностью. Элементы открытого ключа определяют-

ся в зависимости от двух векторов, которые являются генераторами двух различных циклических групп, содержащихся в скрытой группе. При вычислении открытого ключа применяются следующие типы маскирующих операций: 1) обладающих свойством взаимной коммутативности с операцией возведения в степень; 2) свободные от этого свойства. Подпись представляет собой два целых числа и вектор S, используемый в проверочном уравнении как множитель. Для предотвращения атак, применяющих значение S в качестве подгоночного параметра, проверочное уравнение удваивается.

Ключевые слова: цифровая подпись, постквантовая криптосхема, открытый ключ, скрытая задача логарифмирования, конечная некоммутативная алгебра, ассоциативная алгебра.

Контактная информация:

Молдовян Николай Андреевич — д-р техн. наук, проф., гл. науч. сотр.; nmold@mail.ru

Молдовян Александр Андреевич — д-р техн. наук, проф., гл. науч. сотр.; maa1305@yandex.ru