BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(93), 2020, Pages 62–67
ISSN 1024–7696

Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security

N. A. Moldovyan

Abstract. The paper introduces an enhanced criterion of the post-quantum security for designing post-quantum digital signature schemes based on the hidden discrete logarithm problem. The proposed criterion requires that it is computationally impossible to construct a periodic function containing a period whose length depends on the value of a discrete logarithm in a hidden cyclic group when using public parameters of the signature scheme. A practical post-quantum signature scheme which satisfies the criterion is proposed.

Mathematics subject classification: 94A60, 16Z05, 14G50, 11T71, 16S50.
Keywords and phrases: finite associative algebra, non-commutative algebra, discrete logarithm problem, hidden logarithm problem, post-quantum cryptography, digital signature.

1 Introduction

Currently the development of practical signature schemes is one of the challenges in the field of cryptography [1, 2]. A signature scheme is called post-quantum if it resists attacks that use hypothetic quantum computers. Signature schemes based on the computational difficulty of the discrete logarithm problem (DLP) and the factorization problem (FP), which are widely used at the present time, are not post-quantum because both the DLP and the FP can be solved in polynomial time with quantum computer [3, 4]. The quantum algorithms for solving each of these problems are based on the extremely high efficiency of a quantum computer to perform discrete Fourier transform of periodic functions that take on values in some fixed finite group [5, 6]. The algorithms for solving the DLP (the FP) use the reducibility of each of these two problems to the problem of finding length of the period depending on the value of the discrete logarithm (divisor of the integer to be factorized) [3, 7]. A post-quantum signature scheme is to be based on a problem that is different from the DLP and the FP, which has superpolynomial computational complexity when solving it with quantum computer.

The hidden DLP (HDLP) was proposed as the base primitive of the post-quantum public key-agreement protocols [8, 9] and post-quantum digital signature schemes [10, 11]. The HDLP-based signature algorithms introduced earlier satisfy the following criterion of the post-quantum security, which requires that periodic functions, constructed on the basis of public parameters of the signature scheme, take on values that lie in a sufficiently large number of different groups contained in the finite algebra used as the algebraic carrier of the cryptoscheme. However, in the future new quantum algorithms are assumed to be developed for finding the period length of a periodic function whose values are not limited to a single finite group or a sufficiently small number of different finite groups.

We can propose the following enhanced criterion of post-quantum security for designing the HDLP-based signature algorithms: construction of the periodic functions containing a period depending on the value of the discrete logarithm should be a computationally intractable problem, when using the public parameters of the signature scheme.

This paper presents the developed signature scheme that implements the introduced enhanced criterion of the post-quantum security, which is of interest for application as a practical post-quantum signature scheme having high performance and comparatively small size (1550 bits).

2 Notion of the HDLP and its algebraic supports

Usual DLP is defined in a finite cyclic group as finding the value x in the equation $Y = G^x$, where the group elements Y and G are known; G is the generator of the group. For example, in the Schnorr signature algorithm [12] the value G having prime order q of sufficiently large size (≥ 160 bits) is a common parameter, Y is a public key, and x ($x < q$) is the private key of the owner of the public key Y. The quantum algorithm for finding the value x uses the periodic function $f(i,j) = Y^i G^j$ that contains a period of the length $(-1, x)$: $f(i-1, j+x) = Y^{i-1} G^{j+x} = f(i,j)$, where the function $f(i,j)$ takes on the values in the said group.

The HDLP is set in finite non-commutative associative algebras (FNAAs) [10,11] in frame of which one can set sufficintly large number of different cyclic groups. A hidden cyclic group of large prime order q is selected, in it the basic exponentiation operation is performed $Y = G^x$. Then the masking operations ψ_1 and ψ_2 (each of them is mutually commutative with the exponentiation operation) are performed over the values Y and G: $W = \psi_1(Y)$ and $Z = \psi_2(G)$. The values W and Z are elements of the public key in the signature schemes introduced in [10, 11]. In some other signature algorithms [13, 14] the public key includes the third element T that is a matching element needed to provide correctness of the signature scheme. The value T is defined by the selected private operations ψ_1 and ψ_2. Using the public parameters of the known HDLP-based signature schemes one can easily compose the periodic function $f'(i,j) = W^i \circ G^j$ or $f''(i,j) = W^i \circ T \circ G^j$ (where $\circ$ denotes the multiplication operation in the FNAA), which also contains a period of the length $(-1, x)$, however each of the functions $f'(i,j)$ and $f''(i,j)$ takes on the values related to sufficiently large number of different finite cyclic groups contained in the FNAA used as the algebraic support of the signature scheme, therefore, the known quantum algorithms can not be applied for finding the value x.

In the signature scheme introduced in the next section, which satisfies the enhanced criterion of the post-quantum security, it is assumed to use algebraic supports

Table 1. The BVMT setting the quaternion-like FNAA with the unit $(0, 1, 0, 0)$.

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

Table 2. The BVMT of the quaternion-like FNAA with the unit $(0, 0, 1, 0)$.

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

being 4-dimensional FNAAs containing global two-sided unit, which are defined over the ground finite field $GF(p)$ with the characteristic equal to the prime $p = 2q - 1$, where q is a 256-bit prime. For example, one can use the FNAAs described in [10,14] or quaternion-like FNAAs with the multiplication operation defined with the basis vector multiplication tables (BVMTs) shown as Tables 1, 2, and 3, where $\lambda \neq 0$. (Description of the procedure for performing the multiplication operation in FNAAs is given, for example, in [10]).

Usually the multiplication operation of two vectors A and $B = \sum_{i=0}^{m-1} b_i\mathbf{e}_i$ is defined with the formula $A \circ B = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} a_i b_j(\mathbf{e}_i \circ \mathbf{e}_j)$, in which products of different pairs of basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ are to be substituted by a single-component vector indicated in the so-called basis vector multiplication table (BVMT), namely, at the intersection of the ith row and jth column.

In every of the FNAAs defined with Tables 1, 2, and 3 the set of all invertible 4-dimensional vectors forms a finite non-commutative group with the group operation

Table 3. The BVMT of the quaternion-like FNAA with the unit $(0, 0, 0, 1)$.

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

$\circ$, the order Ω of which is described by the following formula:

$$\Omega = p(p-1)\left(p^2-1\right).$$

Due to the used structure of the prime p, the prime value q divides the value Ω, therefore the group contains elements of the order q. In the above group the maximum order of the group elements is equal to p^2-1, like in the case of the finite quaternion algebra defined over the field $GF(p)$ [8].

3 The proposed post-quantum signature scheme

The procedure for generating the public key includes the following steps:

1. Select at random an invertible vector U that is a generator of certain finite cyclic group with the order p^2-1 and compute the vector $G = U^{\frac{p^2-1}{q}}$ that has order equal to the prime q.

2. Select at random invertible vectors X and D with the order p^2-1, which satisfy the conditions $X \circ D \neq D \circ X$, $X \circ G \neq G \circ X$, and $D \circ G \neq G \circ D$.

3. Generate two random natural numbers $x < q$ and $t < q$.

4. Compute the vectors $Z_1 = \psi_D(G \circ U) = D \circ G \circ U \circ D^{-1}$ and $Z_2 = \psi_X\left(G^t \circ U\right) = X \circ G^t \circ U \circ X^{-1}$.

5. Compute the vectors $W_1 = \psi_X(G^x) = X \circ G^x \circ X^{-1}$ and $W_2 = \psi_D\left(G^{tx}\right) = D \circ G^{tx} \circ D^{-1}$.

The public key constitutes two pairs of the vectors (Z_1, W_1) and (Z_2, W_2). All other values used in the public-key generation procedure, except the integers q and p, are secret. The set of secret values that are needed to compute a signature (i. e., the vectors X, D, G, U, and the integers x and t) represent the private key. Computing the private key from the public one is the proposed version of the HDLP that is used as the base primitive of the developed signature scheme described as follows.

Procedure for generation of the signature (h, s, S) to the electronic document M:

1. Select two random integers $w < q$ and $u < q$ and compute the vector $K = G^w \circ U^u$.

2. Generate a random integer $k < q$ and compute the vectors $V_1 = X \circ G^k \circ K \circ D^{-1}$ and $V_2 = X \circ G^{tk} \circ K \circ D^{-1}$.

3. Using some specified 256-bit hash-function f_h compute the hash value h from the document M to which the vectors V_1 and V_2 are concatenated: $h = f_h(M, V_1, V_2)$. The value h is the first signature element.

4. Then compute the second signature element s: $s = k - xh \bmod q$.

5. Compute the third signature element in the form of the vector $S = X \circ G^w \circ U^{u-s} \circ D^{-1}$.

Signature verification procedure is executed as follows:

1. Compute the vector $V_1' = W_1^h \circ S \circ Z_1^s$.

2. Compute the vector $V_2' = Z_2^s \circ S \circ W_2^h$.

3. Compute the value $h' = f_h\left(M, V_1', V_2'\right)$.

4. If $h' = h$, then the signature is accepted as genuine. Otherwise it is rejected.

The masking operations ψ_X and ψ_D define two different automomorphism maps of the FNAA used as algebraic support of the developed signature scheme, therefore each of the above two operations is mutually commutative with the exponentiation operation and the signature scheme performs correctly.

Correctness proof of the signature scheme is as follows:

$$\begin{aligned}
V_1' &= \left(X \circ G^x \circ X^{-1}\right)^h \circ \left(X \circ G^w \circ U^{u-s} \circ D^{-1}\right) \circ \left(D \circ G \circ U \circ D^{-1}\right)^s = \\
&= X \circ G^{xh} \circ G^w \circ U^{u-s} \circ G^s \circ U^s \circ D^{-1} = X \circ G^{xh} \circ G^{k-xh} \circ G^w \circ U^u \circ D^{-1} = \\
&= X \circ G^k \circ G^w \circ U^u \circ D^{-1} = X \circ G^k \circ K \circ D^{-1} = V_1; \\
V_2' &= \left(X \circ G^t \circ U \circ X^{-1}\right)^s \circ \left(X \circ G^w \circ U^{u-s} \circ D^{-1}\right) \circ \left(D \circ G^t \circ D^{-1}\right)^h = \\
&= X \circ G^{ts} \circ U^s \circ G^w \circ U^{u-s} \circ G^{txh} \circ D^{-1} = \\
&= X \circ G^{t(k-xh)} \circ G^{txh} \circ U^u \circ G^w \circ D^{-1} = X \circ G^{tk} \circ K \circ D^{-1} = V_2; \\
&\left\{V_1' = V_1;\ V_2' = V_2\right\} \Rightarrow f_h\left(M, V_1', V_2'\right) = f_h\left(M, V_1, V_2\right) \Rightarrow h' = h.
\end{aligned}$$

Thus, the correctly computed signature (h, s, S) passes the verification procedure as genuine signature.

4 Discussion and conclusion

To define computaional complexity of constructing a periodic function containing period depending on the value x, the value U has been imbedded in the public key elements Z_1 and Z_2, which masks well the potential periodicity connected with x. However, when performing the signature verification you need to eliminate the influence of the vector U, which depends on a random value s, so the third element of the signature is used in the form of the vector S calculated depending on the value U^s. To prevent the possibility of using the third element of the signature (which is included as a multiplier of the first degree in the signature verification equation) for signature forgery, the proposed signature scheme uses a double verification equation as compared with the signature schemes [11,13] used as prototype.

The proposed post-quantum signature scheme is of practical interest, since it has sufficiently high performance and low size of the public key (about 4100 bits) and of the signature (about 1550 bits) in comparison with the candidates for post-quantum signature standard which were proposed in the framework of the world competition for the development of post-quantum two-key cryptosystems [2,16].

The introduced signature scheme uses computations in cyclic hidden group. A more efficient masking of the periodicity of the periodic functions, which depends on the private value x, is supposed to be provided when using the commutative hidden group with 2-dimensional cyclicity (a group generated by the generator system containing two elements G and U of the same order). However, some particular FNAA are to be used as algebraic carries to implement this idea. To set new specific FNAAs one can use unified methods [10,17] for defining FNAAs of an arbitrary even dimension.

References

[1] *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018 Proceedings.* Fort Lauderdale, FL, USA, April 9-11, 2018. Springer Verlag LNCS, 2018, **10786**.

[2] *Post-Quantum Cryptography. Proceedings of the 10th International Conference, PQCrypto 2019.* Chongqing, China, May 8−10, 2019. Springer Verlag LNCS, 2019, **11505**.

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

[4] Smolin J. A., Smith G., Vargo A. *Oversimplifying quantum factoring*, Nature. **499** (2013), No. 7457, 163–165.

[5] A. Ekert, R. Jozsa, *Quantum computation and Shorś factoring algorithm.* Rev. Mod. Phys. **68** (1996), 733.

[6] Jozsa R. *Quantum algorithms and the Fourier transform.* Proc. Roy. Soc. London Ser A, **454** (1998), 323–337.

[7] Yan S. Y. *Quantum Attacks on Public-Key Cryptosystems*, Springer, 2014. 207 p.

[8] Moldovyan D. N. *Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes.* Quasigroups and Related Systems, 2010, **18**, No. 2, 165–176.

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

[10] Moldovyan N. A., Moldovyan A. A. *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, 2019, **12**, No. 1, 66–81.

[11] Moldovyan N. A. *Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base.* Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, 2019, No. 1 (89), 71 − 78.

[12] Schnorr C.P. *Efficient signature generation by smart cards.* J. Cryptology, 1991, **4**, 161–174.

[13] Moldovyan A. A., Moldovyan N. A. *Post-quantum signature algorithms based on the hidden discrete logarithm problem.* Computer Science J. of Moldova, 2018, **26**, No. 3(78), 301–313.

[14] Moldovyan N. A., Abrosimov I. K. *Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem.* Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2019, **15**, No. 2, 212–220

[15] D. N. Moldovyan *New Form of the Hidden Logarithm Problem and Its Algebraic Support.* Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, 2020, No. 2 (93), 3–10.

[16] First NIST standardization conference – April 11–13, 2018. http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html

[17] Moldovyan N. A. *Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions*, Quasigroups and Related Systems, 2018, **26**, No. 2. P. 263-270.

Nikolay Moldovyan
St. Petersburg Institute for Informatics and Automation of
Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg
Russia
E-mail: *nmold@mail.ru*

Received February 6, 2020