BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(93), 2020, Pages 3–10
ISSN 1024–7696

New Form of the Hidden Logarithm Problem and its Algebraic Support

D. N. Moldovyan

Abstract. The paper introduces a new form of the hidden discrete logarithm problem defined over finite non-commutative associative algebras containing two-sided global unit and sets of local left-sided and right-sided units. The proposed form is characterized in using a new mechanism for masking the finite cyclic group in which the base exponentiation operation is performed. Local units act in frame of subsets of non-invertible vectors and are used as elements of the private key in the proposed post-quantum digital signature scheme. A new 4-dimensional algebra is introduced as algebraic support of the proposed cryptoscheme. Formulas describing units of different types are derived.

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

1 Introduction

One of current challenges in the area of cryptography relates to the development of the post-quantum public-key cryptoschemes suitable for wide practical application [1, 2]. A cryptographic scheme is called post-quantum if it can resist attacks performed with using hypothetic quantum computers for which there are known algorithms solving the discrete logarithm problem (DLP) and factorization problem in polynomial time [3, 4]. The post-quantum public-key cryptoschemes should be based on computationally difficult problems having superpolynomial complexity when solving them on quantum computers.

Earlier the hidden DLP (HDLP) was proposed as the base primitive for post-quantum public key-agreement protocols [5, 6]. That form of the HDLP has been defined in a finite non-commutative group Γ as follows. Suppose G is a generator of some finite cyclic group having prime order of sufficiently large size. Then the DLP is set as finding a natural number $x < q$ satisfying the equation $Y = G^x$, where the values G and Y are known. In the HDLP [5] the value Y is masked, i. e. instead of the value Y other value Y' is given that is an element of another cyclic group representing a subset of elements of the group Γ.

Recently [7,8] new forms of the HDLP have been proposed, in which both values G and Y are masked in some given values G' and Y' contained in two different finite cyclic groups representing subsets of a finite non-commutative associative algebra

(FNAA). The last forms have been used as the base primitive of the proposed post-quantum digital signature schemes. The last forms of the HDLP have been set in the FNAAs containing large sets of the global single-sided units. Homomorphism maps have been used as the masking mechanism.

The present paper introduces a new form of the HDLP with masking the both values Y and G, which suits well for designing the signature schemes. The proposed form is characterized in using two simple masking mechanisms each of which is performed as one multiplication operation, namely, as the multiplication by the right-sided unit used as the left operand or the multiplication by the left-sided unit used as the right operand. The next section of the paper describes a new 4-dimensional FNAA as an appropriate algebraic support of the proposed form of the HDLP and the intoduced postquantum signature scheme.

2 A 4-dimensional FNAA used as algebraic support

A finite m-dimensional algebra represents a vector space defined over a finite field, for example, over the ground finite field $GF(p)$, in which the vector multiplication operation (distributive relative to the addition operation) is additionally defined. If the multiplication operation (denoted as $\circ$) is non-commutative and associative, then the algebra is FNAA. Suppose $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are the basis vectors. A vector V is denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \cdots + a_{m-1}\mathbf{e}_{m-1}$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$.

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). Every cell of the BVMT contains a single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$ is called a structural coefficient. If $\lambda = 1$, then the content of the cell is denoted as $\mathbf{e}_k$. One usually assumes that the left operand $\mathbf{e}_i$ defines the row and the right one $\mathbf{e}_j$ defines the column. The intersection of the ith row and jth column defines the cell indicating the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$.

2.1 The BVMT and the invertibility condition

In the case of using the BVMT shown in Table 1 the vector equation defining the value of left-sided units and having the form $X \circ A = A$, where the vector $X = (x_0, x_1, x_2, x_3)$ is an unknown value, can be reduced to the following system of

Table 1. The BVMT setting the 4-dimensional FNAA ($\lambda\sigma \neq 1$).

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

four linear equations with the unknowns (x_0, x_1, x_2, x_3) :

$$\begin{cases} (\lambda x_0 + x_1)\, a_0 + (x_0 + \sigma x_1)\, a_2 = a_0; \\ (\lambda x_2 + x_3)\, a_0 + (x_2 + \sigma x_3)\, a_2 = a_2; \\ (\lambda x_0 + x_1)\, a_1 + (x_0 + \sigma x_1)\, a_3 = a_1; \\ (\lambda x_2 + x_3)\, a_1 + (x_2 + \sigma x_3)\, a_3 = a_3. \end{cases} \tag{1}$$

Perfoming the following substitution of the variables $u_1 = (\lambda x_0 + x_1)$; $u_2 = (x_0 + \sigma x_1)$; $u_3 = (\lambda x_2 + x_3)$; and $u_4 = (x_2 + \sigma x_3)$ one can get the solution $u_1 = 1$; $u_2 = 0$; $u_3 = 0$; and $u_4 = 1$ that is independent of the value A. From the last solution we get the following two independent systems of two linear equations with the unknowns (x_0, x_1) and (x_2, x_3) respectively:

$$\begin{cases} \lambda x_0 + x_1 = 1; \\ x_0 + \sigma x_1 = 0; \end{cases} \tag{2}$$

$$\begin{cases} \lambda x_2 + x_3 = 0; \\ x_2 + \sigma x_3 = 1. \end{cases} \tag{3}$$

Solving the last two systems we get the following value of the global left-sided unit (it is called global since it acts on all elements of the considered FNAA):

$$E_L = \left(\frac{\sigma}{\lambda\sigma - 1}, \frac{1}{1 - \lambda\sigma}, \frac{1}{1 - \lambda\sigma}, \frac{\lambda}{\lambda\sigma - 1} \right). \tag{4}$$

The vector equation $A \circ X = A$ defining the value of the right-sided units reduces to the following system with the unknowns (x_0, x_1, x_2, x_3) :

$$\begin{cases} (\lambda x_0 + x_2)\, a_0 + (x_0 + \sigma x_2)\, a_1 = a_0; \\ (\lambda x_1 + x_3)\, a_0 + (x_1 + \sigma x_3)\, a_1 = a_1; \\ (\lambda x_0 + x_2)\, a_2 + (x_0 + \sigma x_2)\, a_3 = a_2; \\ (\lambda x_1 + x_3)\, a_2 + (x_1 + \sigma x_3)\, a_3 = a_3. \end{cases} \tag{5}$$

Perfoming the following substitution of the variables $z_1 = (\lambda x_0 + x_2)$; $z_2 = (x_0 + \sigma x_2)$; $z_3 = (\lambda x_1 + x_3)$; and $z_4 = (x_1 + \sigma x_3)$ one can get the solution $z_1 = 1$;

$z_2 = 0$; $z_3 = 0$; and $z_4 = 1$ that is independent of the value A. Computation of the inverse variable substitution gives the following formula for the global right-sided unit

$$E_R = \left(\frac{\sigma}{\lambda\sigma - 1}, \frac{1}{1 - \lambda\sigma}, \frac{1}{1 - \lambda\sigma}, \frac{\lambda}{\lambda\sigma - 1} \right). \tag{6}$$

Comparison of the formulas (4) and (6) shows that the considered algebra contains the unique global two-sided unit $E = E_L = E_R = (e_0, e_1, e_2, e_3)$.

If for a vector A the equation $X \circ A = E$ has a solution, then the vector A is called invertible. The last vector equation reduces to the following two independent systems of two linear equations with the unknowns (x_0, x_1) and (x_2, x_3) correspondingly:

$$\begin{cases} (\lambda a_0 + a_2)\, x_0 + (a_0 + \sigma a_2)\, x_1 = e_0; \\ (\lambda a_1 + a_3)\, x_0 + (a_1 + \sigma a_3)\, x_1 = e_1; \end{cases} \tag{7}$$

$$\begin{cases} (\lambda a_0 + a_2)\, x_2 + (a_0 + \sigma a_2)\, x_3 = e_2; \\ (\lambda a_1 + a_3)\, x_2 + (a_1 + \sigma a_3)\, x_3 = e_3. \end{cases} \tag{8}$$

Each of the last two systems has the same determinant Δ_A :

$$\Delta_A = (\lambda a_0 + a_2)(a_1 + \sigma a_3) - (\lambda a_1 + a_3)(a_0 + \sigma a_2) = (1 - \lambda\sigma)(a_1 a_2 - a_0 a_3) \tag{9}$$

If $\Delta_A \neq 0$, then the vector A is invertible, i. e. we have the following invertibility condition:

$$a_1 a_2 \neq a_0 a_3. \tag{10}$$

2.2 Local units connected with non-invertible vectors

If coordinates of a vector $G = (g_0, g_1, g_2, g_3)$ satisfy the condition $g_1 g_2 = g_0 g_3$, then the vector G is non-invertible. However, some non-invertible vectors can be locally invertible. Such non-invertible vectors are generators of finite cyclic groups contained in the considered FNAA. Besides, to some fixed locally invertible vector G a large set of local left-sided units and a large set of right-sided units may relate. Each of the latter sets contains invertible and non-invertible 4-dimensional vectors.

To derive the formula describing local left-sided units one should consider the solutions of the vector equation $X \circ G = G$ that reduces to the following two independent systems:

$$\begin{cases} (\lambda g_0 + g_2)\, x_0 + (g_0 + \sigma g_2)\, x_1 = g_0; \\ (\lambda g_1 + g_3)\, x_0 + (g_1 + \sigma g_3)\, x_1 = g_1; \end{cases} \tag{11}$$

$$\begin{cases} (\lambda g_0 + g_2)\, x_2 + (g_0 + \sigma g_2)\, x_3 = g_2; \\ (\lambda g_1 + g_3)\, x_2 + (g_1 + \sigma g_3)\, x_3 = g_3. \end{cases} \tag{12}$$

The determinant of each of the latter systems is equal to zero. The auxiliary determinants of the system (11) are

$$\Delta_0 = g_0 (g_1 + \sigma g_3) - g_1 (g_0 + \sigma g_2) = \sigma (g_0 g_3 - g_1 g_2) = 0.$$

$$\Delta_1 = g_1\left(\lambda g_0 + g_2\right) - g_0\left(\lambda g_1 + g_3\right) = g_1 g_2 - g_0 g_3 = 0.$$

For the system (11) we have p solutions described by the formula $x_1 = \frac{g_0 - (\lambda g_0 + g_2)x_0}{g_0 + \sigma g_2}$, where $x_0 = 0, 1, \ldots, p-1$, if $g_0 + \sigma g_2 \neq 0$, or by the formula $x_0 = \frac{g_0 - (g_0 + \sigma g_2)x_1}{\lambda g_0 + g_2}$, where $x_1 = 0, 1, \ldots, p-1$, if $\lambda g_0 + g_2 \neq 0$.

The auxiliary determinants of the system (12) are also equal to zero:

$$\Delta_2 = g_2\left(g_1 + \sigma g_3\right) - g_3\left(g_0 + \sigma g_2\right) = g_1 g_2 - g_0 g_3 = 0.$$

$$\Delta_3 = g_3\left(\lambda g_0 + g_2\right) - g_2\left(\lambda g_1 + g_3\right) = \lambda\left(g_0 g_3 - g_1 g_2\right) = 0.$$

For the system (12) we have p solutions described by the formula $x_3 = \frac{g_2 - (\lambda g_0 + g_2)x_2}{g_0 + \sigma g_2}$, where $x_2 = 0, 1, \ldots, p-1$, if $g_0 + \sigma g_2 \neq 0$, or by the formula $x_2 = \frac{g_2 - (g_0 + \sigma g_2)x_3}{\lambda g_0 + g_2}$, where $x_3 = 0, 1, \ldots, p-1$, if $\lambda g_0 + g_2 \neq 0$.

Thus, for the non-invetible vector G coordinates of which satisfy the condition $g_0 + \sigma g_2 \neq 0$ there exist p^2 different left-sided units $L = (l_0, l_1, l_2, l_3)$ described by the formula

$$L = \left(x_0, \frac{g_0 - \left(\lambda g_0 + g_2\right)x_0}{g_0 + \sigma g_2}, x_2, \frac{g_2 - \left(\lambda g_0 + g_2\right)x_2}{g_0 + \sigma g_2}\right), \tag{13}$$

where $x_0, x_2 = 0, 1, \ldots, p-1$. One can easily show that the set (13) contains $p^2 - p$ invertible and p non-invertible elements of the considered FNAA. The subset of the local left-sided units L' that are non-invertible vectors of the considered 4-dimensinal FNAA is described as follows (for the case $g_0 \neq 0$):

$$L' = \left(x_0, \frac{g_0 - \left(\lambda g_0 + g_2\right)x_0}{g_0 + \sigma g_2}, \frac{g_2}{g_0}x_0, \frac{g_0 g_2 - \left(\lambda g_0 + g_2\right)g_2 x_0}{g_0^2 + \sigma g_0 g_2}\right), \tag{14}$$

where $x_0 = 0, 1, \ldots, p-1$.

The formula describing the set of the local right-sided units relating to the non-invertible vector G can be derived from the vector equation $G \circ X = X$ that reduces to the following two independent systems of two linear equations

$$\begin{cases} \left(\lambda g_0 + g_1\right)x_0 + \left(g_0 + \sigma g_1\right)x_2 = g_0; \\ \left(\lambda g_2 + g_3\right)x_0 + \left(g_2 + \sigma g_3\right)x_2 = g_2; \end{cases} \tag{15}$$

$$\begin{cases} \left(\lambda g_0 + g_1\right)x_1 + \left(g_0 + \sigma g_1\right)x_3 = g_1; \\ \left(\lambda g_2 + g_3\right)x_1 + \left(g_2 + \sigma g_3\right)x_3 = g_3. \end{cases} \tag{16}$$

The main determinant of each of the systems (15) and (16) is equal to zero. The auxiliary determinants of the system (15) are

$$\Delta_0 = g_0\left(g_2 + \sigma g_3\right) - g_2\left(g_0 + \sigma g_1\right) = \sigma\left(g_0 g_3 - g_1 g_2\right) = 0.$$

$$\Delta_2 = g_2\left(\lambda g_0 + g_1\right) - g_0\left(\lambda g_2 + g_3\right) = g_1 g_2 - g_0 g_3 = 0.$$

For the system (15) we have p solutions described by the formula $x_2 = \frac{g_0-(\lambda g_0+g_1)x_0}{g_0+\sigma g_1}$, where $x_0 = 0, 1, \ldots, p-1$, if $g_0 + \sigma g_1 \neq 0$, or by the formula $x_0 = \frac{g_0-(g_0+\sigma g_1)x_2}{\lambda g_0+g_1}$, where $x_1 = 0, 1, \ldots, p-1$, if $\lambda g_0 + g_1 \neq 0$.

The auxiliary determinants of the system (16) are also equal to zero:

$$\Delta_1 = g_1 (g_2 + \sigma g_3) - g_3 (g_0 + \sigma g_1) = g_1 g_2 - g_0 g_3 = 0.$$

$$\Delta_3 = g_3 (\lambda g_0 + g_1) - g_1 (\lambda g_2 + g_3) = \lambda (g_0 g_3 - g_1 g_2) = 0.$$

For the system (16) we have p solutions described by the formula $x_3 = \frac{g_1-(\lambda g_0+g_1)x_1}{g_0+\sigma g_1}$, where $x_2 = 0, 1, \ldots, p-1$, if $g_0 + \sigma g_1 \neq 0$, or by the formula $x_1 = \frac{g_1-(g_0+\sigma g_1)x_3}{\lambda g_0+g_1}$, where $x_3 = 0, 1, \ldots, p-1$, if $\lambda g_0 + g_1 \neq 0$.

Thus, for the non-invetible vector G coordinates of which satisfy the condition $g_0 + \sigma g_1 \neq 0$ there exist p^2 different right-sided units $R = (r_0, r_1, r_2, r_3)$ described by the formula

$$R = \left(x_0, x_1, \frac{g_0 - (\lambda g_0 + g_1) x_0}{g_0 + \sigma g_1}, \frac{g_1 - (\lambda g_0 + g_1) x_1}{g_0 + \sigma g_1} \right), \tag{17}$$

where $x_0, x_1 = 0, 1, \ldots, p-1$. One can easily show that the set (17) contains $p^2 - p$ invertible and p non-invertible elements of the considered FNAA.

The subset of the local right-sided units R' that are non-invertible vectors of the considered 4-dimensinal FNAA is described as follows (for the case $g_0 \neq 0$):

$$R' = \left(x_0, \frac{g_1}{g_0} x_0, \frac{g_0 - (\lambda g_0 + g_1) x_0}{g_0 + \sigma g_1}, \frac{g_0 g_1 - (\lambda g_0 + g_1) g_1 x_0}{g_0^2 + \sigma g_0 g_1} \right), \tag{18}$$

where $x_0 = 0, 1, \ldots, p-1$.

Let us consider the non-invertible vector G satisfying the conditions $g_0 + \sigma g_2 \neq 0$ and $g_0 + \sigma g_1 \neq 0$. Only one non-invertible vector E' is contained simultaneously in the sets (14) and (18). The value E' can be computed substituting the value

$$x_0 = \frac{g_0^2}{\lambda g_0^2 + g_0 g_1 + g_0 g_2 + \sigma g_1 g_2} \tag{19}$$

in (14) or in (18).

The vector E' is the unit of the cyclic group generated by the vector G. For example, for the fixed values $p = 2q + 1$, where $q = 30894397013$ is a prime, $\lambda = 1234567$, $\sigma = 809$, and $G = (160, 800, 400, 2000)$ computation of the value E' using the formulas (18) and (19) gives the same result as computation of the value

$$G^{p-1} = (52415881640, 14924232092, 7462116046, 37310580230) = E'.$$

3 The proposed form of the HDLP and post-quantum signature scheme

Suppose there are given the 512-bit prime $p = 2q + 1$, where q is also prime, the structural coefficients λ and σ such that $\lambda\sigma \neq 1$. Then one can generate the public key in the form of two vectors Y' and G' as follows:

1. Select at random the non-invertible vector G that is a generator of some finite cyclic group having the order equal to q.

2. Generate two random natural numbers x_0, x_2 and, using the formula (13), compute the local left-sided unit L.

3. Generate two random natural numbers x_0, x_1 and, using the formula (17), compute the local right-sided unit R.

4. Compute the vector $G' = G \circ L$.

5. Generate a random natural number x and compute the vector $Y' = R \circ G^x$.

The private key connected with the public key Y', G' represents the values G, L, R, and x. Finding the private key from the public key represent the proposed form of the HDLP that is put into the base of the following digital signature scheme.

Generation of the signature (v, s) to the electronic document M is to be performed as follows:

1. Select a random integer $k < q$ and compute the vector $U = R \circ G^k \circ L$.

2. Using some specified hash-function F_h compute the hash value v from the document M to which the vector U is cocatenated: $v = F_h(M, U)$. Then compute the value $s = k - xv \bmod q$.

Signature verification procedure is executed as follows:

1. Compute the vector $U^? = Y'^v \circ G'^s$ and the value $v^? = F_h(M, U^?)$.

2. If $e^? = e$, then the signature is accepted as genuine. Otherwise it is rejected.

The signature scheme performs correctly due to the commutativity of the exponentiation operation G^t and the left (right) multiplication by a right-sided (left-sided) unit $R \circ G$ $(G \circ L)$: $\quad (R \circ G)^t = R \circ G^t; \quad (G \circ L)^t = G^t \circ L$.

Correctness proof of the signature scheme is as follows:

$$U^? = Y'^v \circ G'^s = R \circ G^{xv} \circ G \circ L^s = R \circ G^{xv} \circ G^s \circ L = R \circ G^{xv} \circ G^{k-xv} \circ L = \\ = R \circ G^k \circ L = U \Rightarrow F_h(M, U^?) = F_h(M, U) \Rightarrow v^? = v. \tag{20}$$

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

4 Conclusion

A new form of the HDLP and a post-quantum signature scheme on its base have been introduced. A new 4-dimensional FNAA with two-sided global unit has been considered as algebraic support of the introduced HDLP. The proposed design of the signature scheme can be potentially implemented using different algebraic supports, for example, finite algebra of quaternions and 6-dimensional FNAA described in [9].

Another direction of an independent research can be attributed to combining the masking mechanism of the proposed form of the HDLP with the masking mechanisms described in [8, 10]

References

[1] First NIST standardization conference - April 11–13, 2018.

http://prometheuscrypt.gforge.inria.fr/2018-04- 18.pqc2018.html

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

[3] Yan S. Y. *Quantum Computational Number Theory*. Springer, 2015, 252 p.

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

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

[6] 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.

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

[8] 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 (Bulletin SUSU MMCS), 2019, **12**, No. 1, 66–81.

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

[10] 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.

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

Received February 8, 2019