UDC 512.552.18+003.26
MSC 16P10

Structure of a 4-dimensional algebra and generating parameters of the hidden discrete logarithm problem

N. A. Moldovyan, A. A. Moldovyan

St Petersburg Federal Research Center of the Russian Academy of Sciences, 39, 14-ya liniya V. O., St Petersburg, 199178, Russian Federation

For citation: Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden discrete logarithm problem. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2022, vol. 18, iss. 2, pp. 209–217. https://doi.org/10.21638/11701/spbu10.2022.202

Structure of a 4-dimensional algebra and generating parameters of the hidden discrete logarithm problem the field $GF(p)$ is studied in connection with using it as algebraic support of the hidden discrete logarithm problem that is an attractive primitive of post-quantum signature schemes. It is shown that each invertible 4-dimensional vector that is not a scalar vector is included in a unique commutative group representing a subset of algebraic elements. Three types of commutative groups are contained in the algebra and formulas for computing the order and the number of groups are derived for each type. The obtained results are used to develop algorithms for generating parameters of digital signature schemes based on computational difficulty of the hidden logarithm problem.

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

1. Introduction. Currently the development of the public-key digital signature algorithms and protocols that are resistant to attacks with using computations on a quantum computer (quantum attacks) attracts significant attention of the cryptographic community [1].

Usually the research activity in the area of the post-quantum public-key cryptography is focused on the development of the public-key cryptoschemes based on the computationally complex problems different from the factoring problem (FP) and the discrete logarithm problem (DLP), since both the FP and the DLP can be solved in polynomial time on a quantum computer [2–4].

Recently it was shown that the hidden discrete logarithm problem (HDLP) defined in finite non-commutative associative algebras (FNAAs) set over a ground field $GF(p)$ represents an attactive primitive for designing practical post-quantum signature algorithms [5]. The design criteria of post-quantum resistance for development of the HDLP-based signature schemes are presented in [6]. Different FNAAs had been used to set different forms of the HDLP and to develop different types of post-quantum cryptoschemes based on computational difficulty of the HDLP: public key-agreement protocols [7], commutative encryption algorithms [8], and digital signature schemes [5, 9].

However, the rationale for using FNAAs as carriers of HDLP is intuitive and empirical. Namely, it is intuitively assumed that the used algebra contains a sufficiently large number of isomorphic finite commutative groups whose order is equal to the divisor of $p^2 - 1$ or to the divisor of $p(p - 1)$. A limited experimental verification of these assumptions is

performed. Thus, the problem of theoretical justification of these assumptions for some fixed FNAA chosen as algebraic carrier of the HDLP-based cryptoschemes is open.

In this paper the structure of the 4-dimensional FNAA proposed in [10] for reducing the hardware implementation cost of the HDLP-based signature scheme is studied and formulas for computing the number of different types of commutative groups contained in the algebra and for computing the order of the groups are obtained.

2. The studied 4-dimensional FNAA. Suppose in a finite m-dimensional vector space set over the field $GF(p)$ the vector multiplication of arbitrary two vectors is defined additionally. If the vector multiplication is distributive at the right and at the left relatively the addition operation, then we have a finite m-dimensional 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 defined with the following formula:

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

in which every of the products $\mathbf{e}_i \circ \mathbf{e}_j$ is to be substituted by a single-component vector $\lambda \mathbf{e}_\mathbf{k}$ (here $\lambda \in GF(p)$ is called structural coefficient) given in the cell at intersection of the i-th row and j-th column of specially composed basis vector multiplication table (BVMT). If the BVMT sets non-commutative vector multiplication possessing property of associativity, then we have a FNAA.

Table from [10] sets a 4-dimensional FNAA proposed as algebraic carrier of the HDLP-based signature scheme suitable for efficient hardware implementation (due to comparatively low computational complexity of the vector multiplication). That FNAA contains the global two-sided unit $E = \left(\mu^{-1}, \lambda^{-1}, 0, 0\right)$. Vectors A satisfying the condition $a_0 a_1 \neq a_2 a_3$ are invertible. Vectors $N = (n_0, n_1, n_2, n_3)$ satisfying the condition $n_0 n_1 = n_2 n_3$ are non-invertible. A non-invertible vector N such that $n_1 \neq 0$ and $\mu n_0 \neq -\lambda n_1$ is locally invertible relatively a local two sided unit E''_N for which the following formula is derived in [10]:

$$E''_N = \left(\frac{n_0}{\mu n_0 + \lambda n_1}, \frac{n_1}{\mu n_0 + \lambda n_1}, \frac{n_2}{\mu n_0 + \lambda n_1}, \frac{n_3}{\mu n_0 + \lambda n_1} \right).$$

The vector E''_N is unit of some cyclic multiplicative group Γ_N which is generated by the vector N and represents a subset of the set of non-invertible vectors. Supposedly, the considered FNAA contains sufficiently large number of the cyclic groups isomorphic to Γ_N and the latter is used as a hidden group in one of the HDLP-based signature schemes described in [10]. One can easily show that the number of non-invertible vectors contained in the algebra is equal to $p^3 + p^2 - p$ and the order Ω of the non-commutative multiplicative group of the algebra is described by the formula

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

3. Commutative subalgebras. A fixed 4-dimensional vector $Q = (q_0, q_1, q_2, q_3)$ defines a set of pairwise permutable algebraic elements X such that $Q \circ X = X \circ Q$. Using Table, one can represent the latter vector equation as the following system of four linear equations with unknown coordinates of the vector $X = (x_0, x_1, x_2, x_3)$:

$$\begin{aligned}
\mu x_0 q_0 + \lambda x_3 q_2 - \mu x_0 q_0 - \lambda x_2 q_3 &= 0,\\
\lambda x_1 q_1 + \mu x_2 q_3 - \lambda x_1 q_1 - \mu x_3 q_2 &= 0,\\
\lambda x_1 q_2 + \mu x_2 q_0 - \lambda x_2 q_1 - \mu x_0 q_2 &= 0,\\
\mu x_0 q_3 + \lambda x_3 q_1 - \mu x_3 q_0 - \lambda x_1 q_3 &= 0.
\end{aligned} \tag{1}$$

Consider the case $(q_2, q_3) = (0, 0)$ for which the system (1) reduces to the system of two linear equations:

$$\begin{aligned}
x_2 (\mu q_0 - \lambda q_1) &= 0,\\
x_3 (\mu q_0 - \lambda q_1) &= 0.
\end{aligned}$$

From (1) one can easily see that for the vectors Q satisfying the condition $\mu q_0 = \lambda q_1$ every 4-dimensional vector satisfies this system. Evidently, the said vectors Q compose the set of scalar vectors $S = \left(s\mu^{-1}, s\lambda^{-1}, 0, 0\right)$, where $s = 0, 1, \ldots, p-1$. For the vectors $Q = (q_0, q_1, 0, 0)$ satisfying the condition $\mu q_0 \neq \lambda q_1$ the solution space of the system (1) is the set Φ of p^2 vectors $X = (i, j, 0, 0)$, where $i, j = 0, 1, \ldots, p-1$. The latter set contains $2p-1$ non-invertible vectors and $(p-1)^2$ invertible ones (for invertible vectors we have $i \neq 0$ and $j \neq 0$). The sum and product of arbitrary two elements of the set Φ are contained in Φ, therefore Φ represents associative subalgebra that is comutative (see Table). Multiplicative group Γ_1 of this algebra has order $\Omega = (p-1)^2$. A minimum generator system of the group Γ_1 includes two vectors of the order $\omega = p-1$, for example $(w, 0, 0, 0)$ and $(0, z, 0, 0)$, where w and z are primitive elements modulo p.

Table. **The BVMT defining the considered FNAA ($\lambda \neq 0$, $\mu \neq 0$)**

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

Consider the case $(q_2, q_3) \neq (0, 0)$. In the system (1) the first and second equations coincide. In addition, in the solution space of the first and second equations, the third and fourth equations also coincide. Thus, the solution space of the system (1) coincide with the solution space of the next system of two linear equations:

$$\begin{aligned}
\lambda x_3 q_2 - x_2 q_3 &= 0,\\
\lambda x_1 q_2 + \mu x_2 q_0 - \lambda x_2 q_1 - \mu x_0 q_2 &= 0.
\end{aligned} \tag{2}$$

If $q_2 \neq 0$, then $x_3 = q_3 q_2^{-1} x_2$ and the solution space of the system (2) is described by the following formula:

$$X = (x_0, x_1, x_2, x_3) = \left(i, \frac{\mu q_2 i + (\lambda q_1 - \mu q_0)\, j}{\lambda q_2}, j, \frac{q_3}{q_2} j\right), \tag{3}$$

where $i, j = 0, 1, \ldots, p-1$. If $q_3 \neq 0$, then $x_2 = q_2 q_3^{-1} x_3$ and the solution space of the system (2) is described by the formula

$$X = (x_0, x_1, x_2, x_3) = \left(i, \frac{\mu q_3 i + (\lambda q_1 - \mu q_0)\, j}{\lambda q_3}, \frac{q_2}{q_3} j, j\right). \tag{4}$$

Note that for the case $q_2 \neq 0$ and $q_3 \neq 0$ the formulas (3) and (4) define the same set of vectors X that are permutable with the vector Q. For certainty, consider the formula (3).

Proposition 1. Arbitrary two vectors X_1 and X_2 from the set (3) are permutable, i. e. $X_1 \circ X_2 = X_2 \circ X_1$.

P r o o f. Suppose $X_1 = \left(i_1, (\mu q_2 i_1 + (\lambda q_1 - \mu q_0)\, j_1)\, \lambda^{-1} q_2^{-1}, j_1, q_3 q_2^{-1} j_1\right)$ and $X_2 = \left(i_2, (\mu q_2 i_2 + (\lambda q_1 - \mu q_0)\, j_2)\, \lambda^{-1} q_2^{-1}, j_2, q_3 q_2^{-1} j_2\right)$. Using Table and perfoming direct computation of the values $V_1 = X_1 \circ X_2$ and $V_2 = X_2 \circ X_1$ we will obtain $V_1 = V_2$. □

Suppose Σ denotes the set of scalar vectors $S = sE$ $(s = 0, 1, \ldots, p-1)$ and Φ_Q denotes the set of mutually permutable vectors defined by the formula (3). Arbitrary vector V from the set $\Phi_Q \backslash \Sigma$ defines the set Φ_V including p^2 different vectors every of which is permutable with V. Since, due to the Proposition 1, the set Φ_Q contains p^2 different vectors permutable with V (including V) we have come to the two conclusions.

Proposition 2. Arbitrary vector $V \in \Phi_Q \backslash \Sigma$ defines the set Φ_V of vectors permutable with V, which coincides with Φ_Q, i. e. $\Phi_V = \Phi_Q$.

Proposition 3. Arbitrary vector V that is not a scalar vector is included in a unique set of paiwise permutable vectors.

Arbitrary fixed set Φ represents a commutative associative subalgebra of the considered 4-dimensional FNAA. Evidently, every scalar vector S is included in each of the sets of pairwise permutable vectors. Other $p^4 - p$ non-zero vectors are distributed among η_Φ different sets Φ each of which contains $p^2 - p$ unique non-scalar vectors, therefore, we have the following formula for the number of the Φ subalgebras:

$$\eta_\Phi = \frac{p^4 - p}{p^2 - p} = p^2 + p + 1. \tag{5}$$

In general case different subalgebras contain finite multiplicative groups Γ_Φ of different orders Ω_{Γ_Φ} and types.

4. Three types of commutative groups. Consider a fixed Φ_Q subalgebra for some vector Q that satisfies the non-equalities $q_2 \neq 0$ and $q_3 \neq 0$. The order of its multiplicative group is equal to p^2 minus the number η_N of non-invertible vectors contained in the subalgebra. From the non-invertibility condition $x_0 x_1 = x_2 x_3$ and the formula (3) we have the equation

$$\lambda q_3 j^2 - (\lambda q_1 - \mu q_0)\, ij - \mu q_2 i^2 = 0. \tag{6}$$

The number of different pairs (i, j) satisfying the equation (6) gives the value of η_N. For $i = 0$ we get $j = 0$. In the case $i \neq 0$, solving the equation (6) relatively the unknown value j, we get

$$j = \left(\frac{(\lambda q_1 - \mu q_0)}{2\lambda q_3} \pm \sqrt{\Delta} \right), \; i = 0, \tag{7}$$

$$\Delta = \frac{(\lambda q_1 - \mu q_0)^2}{4\lambda^2 q_3^2} + \frac{\mu q_2}{\lambda q_3}. \tag{8}$$

The value of Δ defines three types of multiplicative group of the commutative subalgebras Φ: i) Δ is a quadratic non-residue modulo p; ii) Δ is a quadratic residue modulo p; iii) $\Delta = 0$.

Case i): subalgebra Φ_Q contains one non-invertible vector $(0, 0, 0, 0)$ and $\eta_N = 1$. Therefore, all non-zero vectors are ivertible and Φ_Q represents the finite field of the order p^2. The group Γ_Φ is cyclic as multiplicative group of a field and $\Omega_{\Gamma_\Phi} = p^2 - 1$. A group of such type is denoted as Γ_1.

Case ii): $\sqrt{\Delta} = \delta \neq 0$. For every value $i = 1, 2, \ldots, p-1$ we have two unique solutions of the equation (3): $j = \left((\lambda q_1 - \mu q_0)(2\lambda q_3)^{-1} \pm \delta\right) i$. Thus, taking into account zero vector, we have $\eta_N = 2p - 1$ and $\Omega_{\Gamma_\Phi} = p^2 - (2p-1) = (p-1)^2$. A vector $V = (a, b, 0, 0) \notin \Sigma$ defines a subalgebra Φ_V multiplicative group of which Γ_{Φ_V} has order equal to $(p-1)^2$ and contains a minimum generator system including two vectors G_1 and G_2 of the same order equal to $p-1$. Suppose the vector W is a generator of a cyclic group Γ_Φ of the order p^2-1. Then the formula $F(X) = W^{-i} \circ X \circ W^i$ defines p^2-1 different (in general case) isomorphic maps of the group Γ_{Φ_V} to different groups Γ_Φ. Evidently, every of the lasts contains a minimum generator system including two vectors of the order $p-1$. Thus, if Δ is a quadratic residue in $GF(p)$, then the formula (3) defines a Φ_Q algebra that contains a multiplicative group generated by a minimum generators system including two vectors of the order $p-1$ (in terms of the paper [11] a finite commutative group generated by a minimum generator system including k elements of the same order is called a group with k-dimensional cyclicity). A group of the second type is denoted as Γ_2.

Case iii): $\sqrt{\Delta} = 0$. For every value of $i = 0, 1, 2, \ldots, p-1$ we have one unique solutions of the equation (6): $j = (\lambda q_1 - \mu q_0)(2\lambda q_3)^{-1} i$. Thus, we have $\eta_N = p$ and $\Omega_{\Gamma_\Phi} = p^2 - p = p(p-1)$. For a primitive element $\alpha \in GF(p)$ the order of scalar vector $S = \alpha E$ is equal to $p-1$. Definitely, the group Γ_Φ contains a vector V of the order p. The vector $W = V \circ S$ is contained in Γ_Φ and has order equal to $p(p-1)$, since the values p and $p-1$ are mutually prime. The vectors W^i $(i = 1, 2, \ldots, p(p-1))$ are pairwise different and each of them is contained in Γ_Φ, therefore, one can conclude the group Γ_Φ is cyclic. A group of the third type is denoted as Γ_3.

5. On the number of groups of the same type. Due to the Proposition 3 one can write the equation

$$\begin{aligned}(\Omega_{\Gamma_1} - (\#\Sigma - 1))\, d + (\Omega_{\Gamma_2} - (\#\Sigma - 1))\, t + (\Omega_{\Gamma_3} - (\#\Sigma - 1))\, u = \\ = p(p-1)\left(p^2 - 1\right) - (\#\Sigma - 1)\,,\end{aligned} \tag{9}$$

where unknown integer values d, t, and u denote number of the groups Γ_1, Γ_2, and Γ_3, respectively, contained in the considered 4-dimensional FNAA. Substituting the values $\Omega_{\Gamma_1} = p^2 - 1$, $\Omega_{\Gamma_2} = (p-1)^2$, $\Omega_{\Gamma_3} = p(p-1)$, and $\#\Sigma = p$ in equation (9) one can get

$$pd + (p-2)t + (p-1)u = p^3 - p - 1. \tag{10}$$

The value of the sum $d + t + u$ is the number of different Φ subalgebras contained in the FNAA, therefore, due to equality (5) one can write

$$d + t + u = p^2 + p + 1. \tag{11}$$

From (10) and (11) it is easy to obtain the following equalities:

$$2t + u = (p+1)^2, \qquad 2d + u = p^2 + 1. \tag{12}$$

To find the unknown value u, consider the number of all non-invertible vectors Q that defines the Φ_Q algebras containing the groups of the Γ_3 type. For a non-invertible vector Q the equality $q_0 q_1 = q_2 q_3$ holds true and the formulas (7) and (8) can be represented in the form

$$j = \frac{\lambda q_1 - \mu q_0 \pm (\lambda q_1 + \mu q_0)}{2\lambda q_3} i, \quad \Delta = \frac{(\lambda q_1 + \mu q_0)^2}{4\lambda^2 q_3^2}.$$

The case $\Delta = 0$ corresponds to fulfillment of the condition $\lambda q_1 = -\mu q_0$. If $q_0 = q_1 = 0$, then the system (3) take on the following form:

$$\begin{aligned} \lambda x_3 q_2 - \lambda x_2 q_3 = 0, \\ \mu x_0 q_3 - \lambda x_1 q_3 = 0. \end{aligned} \tag{13}$$

Since additional condition $(q_2, q_3) = (0, 0)$ leads to trivial case $Q = (0, 0, 0, 0)$, at least, we have $q_3 \neq 0$ or $q_2 \neq 0$. For certainty, consider the case $q_3 \neq 0$ (the value of q_2 is arbitrary). The solution space of the system (13) that sets the Φ_Q subalgebra is described by the formula

$$X = (x_0, x_1, x_2, x_3) = \left(i,\ \frac{\mu}{\lambda} i,\ \frac{q_2}{q_3} j,\ j \right),$$

where $i, j = 0, 1, \ldots, p-1$. The non-invertible vectors contained in Φ_Q satisfy the condition

$$i^2 = \frac{\lambda q_2}{\mu q_3} j^2.$$

If the value $\lambda q_2 \left(\mu q_3\right)^{-1}$ is a quadratic non-residue, then Φ_Q includes only one non-invertible vector, namely, $(0, 0, 0, 0)$ and multiplicative group of the Γ_1-type. If the value $\lambda q_2 \left(\mu q_3\right)^{-1}$ is a quadratic residue and $i = \pm j \sqrt{\lambda q_2 \left(\mu q_3\right)^{-1}}$, then Φ_Q includes $2p - 1$ non-invertible vectors and multiplicative group of the Γ_2-type. If $q_3 \neq 0$ and $q_2 = 0$, then Φ_Q includes p non-invertible vectors having the form $(0, 0, 0, j)$ and multiplicative group of the Γ_3-type (evidently, every of the vectors $(0, 0, 0, j)$ sets subalgebra $\Phi_{(0,0,0,j)} = \Phi_Q$). Similarly, for the case $q_2 \neq 0$ and $q_3 = 0$, each of the vectors $Q = (0, 0, q_2, 0)$ defines a fixed Φ algebra that includes p non-invertible vectors having the form $(0, 0, j, 0)$ and a multiplicative group of the Γ_3-type.

Thus, the case $q_0 = q_1 = 0$ gives two different Φ_Q subalgebras each of which contains a group of the Γ_3 type. For the values $q_0 \neq 0$ and $q_1 \neq 0$ we have $p - 1$ different variants of fulfillment of the condition $\lambda q_1 = -\mu q_0$. Every of the said variants for each value $q_3 \in \{1, 2, \ldots, p-1\}$ defines a unique non-invertible vector Q setting a unique Φ_Q subalgebra containing a group of the Γ_3-type.

In the case $q_0 \neq 0$ or $q_1 \neq 0$, we have $(p-1)^2$ vectors defining the Φ_Q subalgebras containing a group of the Γ_3-type. For the case $q_0 = 0$ and $q_1 = 0$, we have $2(p-1)$ additional vectors of the said type. Totally, in the considered FNAA we have $(p-1)^2 + 2(p-1)$ non-invertible vectors defining the Φ_Q subalgebras each of which contains $p - 1$ vectors of the considered type. Therefore, we have

$$u = \frac{(p-1)^2 + 2(p-1)}{p-1} = p + 1. \tag{14}$$

Substituting the value of u in (12) we obtain:

$$d = \frac{p(p-1)}{2}, \qquad t = \frac{p(p+1)}{2}. \tag{15}$$

6. Discussion. The post-quantum signature schemes with a hidden group can be divided into the following two types: i) algorithms based on the computational difficulty of the HDLP; ii) algorithms based on computational difficulty of solving systems of many quadratic equations with many unknowns [12]. Post-quantum security of second type algorithms is related to the fact that the quantum computer is ineffective to solve systems

of many quadratic equations [13, 14]. Usually the FNAAs used as carriers of the algebraic signature algorithms with a hidden group are set over a ground field $GF(p)$ with characteristic p of sufficiently large size z ($z = 256$ to 512 bits). Besides, the value of p is to be selected so that one can select a hidden cyclic group of sufficiently large prime order. To implement a masking mechanism one should use an algebraic carrier containing sufficiently large number of cyclic groups of the same order. The larger this number, the more resistant the masking mechanism appears. The derived formulas (14) and (15) clearly show that the number of the commutative groups of every of the types Γ_1, Γ_2, and Γ_3 is sufficiently large, therefore the hidden group can be potentially selected in a set of groups of every of these types. However, it seems preferable to select a hidden group from one of the Γ_1 and Γ_2 sets, since the number of the Γ_3-type groups is significantly lower: $d/u \approx t/u \approx p$.

For designing a signature scheme with a cyclic hidden group one can generate a prime $p = 2q + 1$, where q is also a prime, and compute a vector H of order q as generator of the hidden cyclic group. The vector H can be selected from groups of Γ_1- or Γ_2-types. An alternative possibility of using a cyclic hidden group relate to generating a prime $p = 2q-1$ with prime q. In the latter case the generator H of hidden group of order q is to be chosen only from set of the Γ_1-type groups. Algorithm for generating a vector H of order q is as follows:

- select at random an invertible vector $R \neq E$;
- compute the vector $H = R^{\frac{p^2-1}{q}}$;
- if $H \neq E$, then output the vector H. Otherwise go to step 1.

For designing a signature scheme with commutative hidden group possessing 2-dimensional cyclicity (see, for example, [6, 12]) the considered 4-dimensional FNAA is to be set over $GF(p)$ with characteristic $p = 2q + 1$, where q is a prime. To set a hidden group of the order q^2, which possesses 2-dimensional cyclicity, one should compute generators H_1 and H_2 of the order q, which generate two different cyclic groups contained in the same group of the Γ_2-type. Algorithm for generating vectors H_1 and H_2 that represent a minimum generator system of the hidden group of the order q^2 is as follows:

- select at random an invertible vector $Q = (q_0, q_1, q_2, q_3)$ such that $\{q_2 \neq 0;\ q_3 \neq 0\}$ and, using the formula (8), compute the value of Δ;
- if Δ is a quadratic non-residue, then go to step 1. Otherwise set integer variable $i = 1$;
- using the formula (7), compute the integer j;
- using the formula (3), compute the vector $X = (x_0, x_1, x_2, x_3)$;
- if $x_0x_1 = x_2x_3$, then set the variable $i \leftarrow i+1$ and go to step 3. Otherwise compute the vector $H_1 = X^{\frac{p-1}{q}}$;
- if $H_1 = E$, then set the variable $i \leftarrow i+1$ and go to step 3. Otherwise generate a primitive element $\alpha \in GF(p)$ and compute the scalar vector $S = \alpha E = \left(\alpha\mu^{-1}, \alpha\lambda^{-1}, 0, 0\right)$;
- generate a random integer $k < q$ and compute the vector $H_2 = S^{\frac{p-1}{q}} \circ H_1^k$. Then output the vectors H_1 and H_2.

Using a Γ_3-type group to set a hidden cyclic group of order p is of potential interest to insure a higher perfomance of the computational procedures of the HDLP-based signature schemes, since for the values p having the structure $p = 2^z + c$, where value of c is small, the multiplication modulo p can be implemented without performing the arithmetic division operation. Algorithm for generating a vector H of order p is as follows:

a) select arbitrary three values $0 < q_0, q_1, q_3 < p - 1$ and compute the value $q_2 = -\left(\lambda q_1 - \mu q_0\right)^2 \left(4\lambda\mu q_3\right)^{-1}$ for which we have $\Delta = 0$ (see (8));

b) compute the vector $H = (q_0, q_1, q_2, q_3)^{p-1}$;

c) if $H = E$, then go to step 1. Else output the vector H as a generator of a hidden cyclic group.

7. Conclusion. The results obtained show the studied 4-dimensional FNAA defined by a sparse BVMT over a ground field $GF(p)$ can be represented as a set of commutative subalgebras intersecting in a set of scalar vectors. Three types of subalgebras can be distinguished: i) containing a cyclic group of the order $p^2 - 1$; ii) containing a group of the order $(p-1)^2$, which has a 2-dimensional cyclicity; iii) containing a cyclic group of the order $p(p-1)$. Formulas for the number of groups of each type were derived. Algorithms for generating the invertible vectors of the required order, wich are contained in a group of given type, are presented.

References

1. Post-quantum cryptography. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019, Proceedings. *Lecture Notes in Computer Science series*. Cham, Springer Publ., 2019, vol. 11505, pp. 1–269.

2. 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.

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

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

5. Moldovyan D. N. New form of the hidden logarithm problem and its algebraic support. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2020, no. 2(93), pp. 3–10.

6. 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

7. Moldovyan D. N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. *Computer Science Journal of Moldova*, 2019, vol. 27, no. 1(79), pp. 56–72.

8. Moldovyan A. A., Moldovyan D. N., Moldovyan N. A. Post-quantum commutative encryption algorithm. *Computer Science Journal of Moldova*, 2019, vol. 27, no. 3(81), pp. 299–317.

9. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties. *Quasigroups and Related Systems*, 2019, vol. 27, no. 2, pp. 293–308.

10. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Post-quantum signature schemes for efficient hardware implementation. *Microprocessors and Microsystems*, 2021, vol. 80, pp. 103487. https://doi.org/10.1016/j.micpro.2020.103487

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

12. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A new concept for designing post-quantum digital signature algorithms on non-commutative algebras. *Voprosy kiberbezopasnosti* [*Cibersecurity questions*], 2022, no. 1(47), pp. 18–25. https://doi.org/10.21681/2311-3456-2022-1-18-25

13. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.

14. Jintai D., Dieter S. Multivariable public key cryptosystems. 2004. https://eprint.iacr.org/2004/350.pdf (accessed: February 24, 2022).

Received: December 22, 2021.
Accepted: May 05, 2022.

Authors' information:

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

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

Структура одной четырехмерной алгебры и генерация параметров скрытой задачи дискретного логарифмирования

Н. А. Молдовян, А. А. Молдовян

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

Для цитирования: *Moldovyan N. A., Moldovyan A. A.* Structure of a 4-dimensional algebra and generating parameters of the hidden discrete logarithm problem // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2022. Т. 18. Вып. 2. С. 209–217. https://doi.org/10.21638/11701/spbu10.2022.202

Строение одной четырехмерной конечной некоммутативной ассоциативной алгебры, заданной над полем $GF(p)$, изучено в плане ее использования в качестве алгебраического носителя скрытой задачи дискретного логарифмирования. Показано, что каждый обратимый вектор, не относящийся к скалярным, включается в единственную коммутативную группу, которая является подмножеством алгебраических элементов. Три типа коммутативных групп содержатся в алгебре, и выведены формулы для вычисления порядка и числа групп каждого типа. Полученные результаты использованы для разработки алгоритмов генерации параметров схем цифровой подписи, основанных на вычислительной трудности скрытой задачи логарифмирования.

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

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