Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 3, June 2025, pp. 2017∼2030
ISSN: 2302-9285, DOI: 10.11591/eei.v14i3.9064

Structure of 6-dimensional finite non-commutative algebras with many single-sided units

May Thu Duong[1], Alexander Andreevich Moldovyan[2], Nikolay Andreevich Moldovyan[2], Minh Hieu Nguyen[3], Bac Thi Do[4]

[1]Faculty of Information Technology, Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam
[2]Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia
[3]Academy of Cryptography Techniques, Hanoi, Vietnam
[4]Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam

Article Info

Article history:

Received Jul 29, 2024
Revised Nov 11, 2024
Accepted Nov 19, 2024

Keywords:

Finite associative algebra
Homomorphisms
Noncommutative algebra
Post-quantum cryptography
Single-sided units

ABSTRACT

Finite Associative Noncommutative Algebras (FANAs) have gained considerable attention as a key foundational element for post-quantum (PQ) public-key (PK) cryptosystems, particularly those with a hidden group. These systems exploit the complexity of the hidden discrete logarithm problem (HDLP) and the challenge of solving large system of power equations. The structure of 6-dimensional FANAs over the finite field $GF(p)$, which can include global single-sided units in different configurations (p^2, p^3, and p^4), plays an essential role in assessing the security of these cryptosystems. A novel PQ signature algorithm has been proposed based on FANAs with p^2 global single-sided units, while the others have been deemed less suitable for supporting the proposed algorithm. The decomposition of these algebras into isomorphic subalgebras, each with a global two-sided unit, significantly contributes to understanding the design of PQ cryptosystems that use FANAs with a large number of global single-sided units as their algebraic framework.

Corresponding Author:

Bac Thi Do
Thai Nguyen University of Information and Communication Technology
Z115 Street, Quyet Thang Commmune, Thai Nguyen City, Thai Nguyen Province, Vietnam
Email: dtbac@ictu.edu.vn

1. INTRODUCTION

Currently, the advancement of practical post-quantum (PQ) public-key (PK) cryptosystems has garnered significant attention from the cryptographic community [1]-[9]. Recently, the hidden discrete logarithm problem (HDLP) [10]-[17] has been proposed as a novel basic primitive for practical PQ signature schemes. The HDLP is set in Finite Associative Noncommutative Algebras (FANAs) of dimensions $m \geq 4$. Different forms of the HDLP are connected with using different types of FANAs and different types of unit elements in the algebras. Several different 6-dimensional FANAs are proposed as algebraic supports of the PQ PK cryptoschemes. The structure of the FANAs has significant importance when estimating the security of the HDLP-based cryptoschemes [18].

The present paper considers for the first time the structure of 6-dimensional FANAs (defined over the finite ground field $GF(p)$ of three different types containing different numbers of single-sided units: i) p^2 [19], ii) p^3 [20], and iii) p^4 [10]. It is shown the connection between the structure of algebras and the security of the

PK cryptographic algorithms on 6-dimensional FANAs of the said types. Using the FANA with p^2 global right-sided (GRS) units as algebraic support, a novel algebraic signature algorithm with a hidden group is introduced as a candidate for practical PQ cryptoschemes.

The paper makes the following research contribution: the practical significance of the results of the paper is that, for the first time, the structure of a series of 6-dimensional finite noncommutative associative algebras with a set of global single-sided units, defined over a ground field, is studied from the point of view of decomposition into a set of isomorphic subalgebras, each of which contains a global two-sided unit. The theoretical significance of the results of the paper is the possibility of using them for security estimations of the PK cryptographic algorithms using 6-dimensional FANAs as an algebraic support. In particular, it has been established that only algebras with a number of global single-sided units equal to p^2 can provide a high level of security for PQ digital signature algorithms. An algorithm of such type is introduced.

2. PRELIMINARIES

An m-dimensional finite algebra represents an m-dimensional vector space over a finite field where the multiplication operation on vectors is defined as distributive on both sides. If this multiplication is associative and noncommutative, we get a FANA. Similar to the case of four-dimensional algebras [21]–[24], the multiplication operation (denoted as $\circ$) in the given FANA is expressed using the following formula, which defines the product of two 6-dimensional vectors $A = \sum_{i=0}^{5} a_i e_i$ and $B = \sum_{j=0}^{5} b_j e_j$, whith $\boldsymbol{e}_0, \ldots, e_5$ are formal being the basis vectors:

$$A \circ B = \left(\sum_{i=0}^{5} a_i e_i\right) \circ \left(\sum_{j=0}^{5} b_j e_j\right) = \sum_{j=0}^{5}\sum_{i=0}^{5} a_i b_j \left(e_i \circ e_j\right),$$

where $a_0, a_1, \ldots, a_5$ are the coordinates of vector A and $b_0, b_1, \ldots, b_5$ are those of vector B, are elements of the field $GF(p)$. The product of each pair of basis vectors $\boldsymbol{e}_i \circ \boldsymbol{e}_j$ is replaced by a single-component vector $\lambda \boldsymbol{e}_k$, derived from the table for multiplying basis vectors (TMBVs) located at the intersection of the i-th row and the j-th column. In this paper, TMBVs from Tables 1–3 are used to define three different types of 6-dimensional FANAs.

Table 1. Defining 6-dimensional algebra with p^2 GRS units ($\lambda \geq 2$) [19]

$\circ$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$
$\boldsymbol{e}_0$	$\boldsymbol{e}_0$	$\boldsymbol{e}_3$	$\boldsymbol{e}_0$	$\boldsymbol{e}_3$	$\boldsymbol{e}_0$	$\boldsymbol{e}_3$
$\boldsymbol{e}_1$	$\lambda\boldsymbol{e}_2$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\lambda\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_1$
$\boldsymbol{e}_2$	$\boldsymbol{e}_2$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_1$
$\boldsymbol{e}_3$	$\lambda\boldsymbol{e}_0$	$\boldsymbol{e}_3$	$\boldsymbol{e}_0$	$\lambda\boldsymbol{e}_3$	$\boldsymbol{e}_0$	$\boldsymbol{e}_3$
$\boldsymbol{e}_4$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$
$\boldsymbol{e}_5$	$\lambda\boldsymbol{e}_4$	$\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$\lambda\boldsymbol{e}_5$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$

Table 2. Defining FANA with p^3 GRS units ($\lambda \geq 2$) [20]

$\circ$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$	$\boldsymbol{e}_4$	$\boldsymbol{e}_5$
$\boldsymbol{e}_0$	$\boldsymbol{e}_2$	$\lambda\boldsymbol{e}_0$	$\boldsymbol{e}_4$	$\lambda\boldsymbol{e}_2$	$\boldsymbol{e}_0$	$\lambda\boldsymbol{e}_4$
$\boldsymbol{e}_1$	$\boldsymbol{e}_3$	$\lambda\boldsymbol{e}_1$	$\boldsymbol{e}_5$	$\lambda\boldsymbol{e}_3$	$\boldsymbol{e}_1$	$\lambda\boldsymbol{e}_5$
$\boldsymbol{e}_2$	$\boldsymbol{e}_4$	$\lambda\boldsymbol{e}_2$	$\boldsymbol{e}_0$	$\lambda\boldsymbol{e}_4$	$\boldsymbol{e}_2$	$\lambda\boldsymbol{e}_0$
$\boldsymbol{e}_3$	$\boldsymbol{e}_5$	$\lambda\boldsymbol{e}_3$	$\boldsymbol{e}_1$	$\lambda\boldsymbol{e}_5$	$\boldsymbol{e}_3$	$\lambda\boldsymbol{e}_1$
$\boldsymbol{e}_4$	$\boldsymbol{e}_0$	$\lambda\boldsymbol{e}_4$	$\boldsymbol{e}_2$	$\lambda\boldsymbol{e}_0$	$\boldsymbol{e}_4$	$\lambda\boldsymbol{e}_2$
$\boldsymbol{e}_5$	$\boldsymbol{e}_1$	$\lambda\boldsymbol{e}_5$	$\boldsymbol{e}_3$	$\lambda\boldsymbol{e}_1$	$\boldsymbol{e}_5$	$\lambda\boldsymbol{e}_3$

Consider the FANA set by Table 1 representing a case of algebra containing p^2 GRS units. The right-sided units satisfy (1):

$$A \circ X = A \tag{1}$$

which, using Table 1, for some vector $A = (a_0, a_1, a_2, a_3, a_4, a_5)$ can be reformulated as the following system of six linear equations, where the unknowns are the coordinates of the vector $X = (x_0, x_1, x_2, x_3, x_4, x_5)$:

$$\begin{cases} x_0a_0 + x_2a_0 + x_4a_0 + \lambda x_0a_3 + x_2a_3 + x_4a_3 = a_0; \\ x_1a_1 + \lambda x_3a_1 + x_5a_1 + x_1a_2 + x_3a_2 + x_5a_2 = a_1; \\ \lambda x_0a_1 + x_2a_1 + x_4a_1 + x_0a_2 + x_2a_2 + x_4a_2 = a_2; \\ x_1a_0 + x_3a_0 + x_5a_0 + x_1a_3 + \lambda x_3a_3 + x_5a_3 = a_3; \\ x_0a_4 + x_2a_4 + x_4a_4 + \lambda x_0a_5 + x_2a_5 + x_4a_5 = a_4; \\ x_1a_4 + x_3a_4 + x_5a_4 + x_1a_5 + \lambda x_3a_5 + x_5a_5 = a_5. \end{cases} \tag{2}$$

Table 3. Defining FANA with p^4 GRS units $(\lambda \geq 2)$ [10]

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	e_0	λe_3	e_0	e_3	λe_0	e_3
e_1	e_1	λe_4	e_1	e_4	λe_1	e_4
e_2	e_2	λe_5	e_2	e_5	λe_2	e_5
e_3	e_3	λe_0	e_3	e_0	λe_3	e_0
e_4	e_4	λe_1	e_4	e_1	λe_4	e_1
e_5	e_5	λe_2	e_5	e_2	λe_5	e_2

System (2) can be represented as (3):

$$\begin{cases} (x_0 + x_2 + x_4)a_0 + (\lambda x_0 + x_2 + x_4)a_3 = a_0; \\ (x_1 + \lambda x_3 + x_5)a_1 + (x_1 + x_3 + x_5)a_2 = a_1; \\ (\lambda x_0 + x_2 + x_4)a_1 + (x_0 + x_2 + x_4)a_2 = a_2; \\ (x_1 + x_3 + x_5)a_0 + (x_1 + \lambda x_3 + x_5)a_3 = a_3; \\ (x_0 + x_2 + x_4)a_4 + (\lambda x_0 + x_2 + x_4)a_5 = a_4; \\ (x_1 + x_3 + x_5)a_4 + (x_1 + \lambda x_3 + x_5)a_5 = a_5. \end{cases} \tag{3}$$

The solutions of the system of (3) can be obtained by performing the variable substitution defined by the formulas $z_1 = x_0 + x_2 + x_4$, $z_2 = \lambda x_0 + x_2 + x_4$, $z_3 = x_1 + x_3 + x_5$ and $z_4 = x_1 + \lambda x_3 + x_5$. After such substitution, the system (3) has the next form:

$$\begin{cases} z_1a_0 + z_2a_3 = a_0; \\ z_4a_1 + z_3a_2 = a_1; \\ z_1a_2 + z_2a_1 = a_2; \\ z_3a_0 + z_4a_3 = a_3; \\ z_1a_4 + z_2a_5 = a_4; \\ z_3a_4 + z_4a_5 = a_5. \end{cases} \tag{4}$$

System (4) has the solution $z_1 = z_4 = 1$ and $z_2 = z_3 = 0$, applicable for any chosen value of the vector A. Reversing the variable substitution results in a set of GRS units $R = (r_0, r_1, r_2, r_3, r_4, r_5)$, coordinates fulfill the following two independent systems of (5), (6):

$$\begin{cases} \;x_0 + x_2 = 1 - x_4; \\ \lambda x_0 + x_2 = -x_4. \end{cases} \tag{5}$$

$$\begin{cases} \;x_1 + x_3 = -x_5; \\ x_1 + \lambda x_3 = 1 - x_5. \end{cases} \tag{6}$$

System (5) includes unknowns x_0, x_2, and x_4 and has solutions defined by (7):

$$x_0 = \frac{1}{1-\lambda}; \quad x_2 = \frac{x_4(\lambda - 1) - \lambda}{1 - \lambda}; \quad x_4 = 0, 1, 2, \ldots, p-1. \tag{7}$$

System (6) includes unknowns x_1, x_3, and x_5 and has solutions defined by (8):

$$x_1 = \frac{x_5(1-\lambda)+1}{1-\lambda}; \quad x_3 = \frac{-1}{1-\lambda}; \quad x_5 = 0, 1, 2, \ldots, p-1. \tag{8}$$

Formulas (7) and (8) describe a set of GRS units $R = (r_0, r_1, r_2, r_3, r_4, r_5)$ with (9):

$$r_0 = \frac{1}{1-\lambda}; \quad r_1 = \frac{k(\lambda-1)+1}{1-\lambda}; \quad r_2 = \frac{d(\lambda-1)-\lambda}{1-\lambda}; r_3 = \frac{-1}{1-\lambda}; \quad r_4 = d; \quad r_5 = k \tag{9}$$

where the integers d and k take on all possible pairs of values from the set $\{0, 1, \ldots, p-1\}$.
Thus, the FANA specified by Table 1 includes $\rho = p^2$ distinct GRS units R defined by (10):

$$R = \left(\frac{1}{1-\lambda}, \frac{k(\lambda-1)+1}{1-\lambda}, \frac{d(\lambda-1)-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, d, k\right), \tag{10}$$

where $d, k = 0, 1, \ldots, p-1$.
The left-sided units L corresponding to vector A satisfy (11):

$$X \circ A = A \tag{11}$$

which simplifies into three independent systems of two equations each:

$$\begin{cases} (a_0 + a_2 + a_4)x_0 + (\lambda a_0 + a_2 + a_4)x_3 = a_0; \\ (a_1 + a_3 + a_5)x_0 + (a_1 + \lambda a_3 + a_5)x_3 = a_3; \end{cases} \tag{12}$$

$$\begin{cases} (a_1 + \lambda a_3 + a_5)x_1 + (a_1 + a_3 + a_5)x_2 = a_1; \\ (\lambda a_0 + a_2 + a_4)x_1 + (a_0 + a_2 + a_4)x_2 = a_2; \end{cases} \tag{13}$$

$$\begin{cases} (a_0 + a_2 + a_4)x_4 + (\lambda a_0 + a_2 + a_4)x_5 = a_4; \\ (a_1 + a_3 + a_5)x_4 + (a_1 + \lambda a_3 + a_5)x_5 = a_5. \end{cases} \tag{14}$$

Every one of the latter three systems has the same main determinant depending on the coordinates of the vector A:

$$\begin{aligned} \Delta_A &= (a_0 + a_2 + a_4)(a_1 + \lambda a_3 + a_5) - (a_1 + a_3 + a_5)(\lambda a_0 + a_2 + a_4) \\ &= a_0a_1(1-\lambda) + a_2a_3(\lambda-1) + a_3a_4(\lambda-1) + a_0a_5(1-\lambda) \\ &= (a_2a_3 + a_3a_4 - a_0a_1 - a_0a_5)(\lambda-1) \end{aligned} \tag{15}$$

if $\Delta_A \neq 0$, a unique local left-sided unit exists for vector A, which is referred to as a locally reversible vector.
From (15) provides the local reversibility condition for the vector $A = (a_0, a_1, a_2, a_3, a_4, a_5)$:

$$\Delta_{\boldsymbol{A}} = (a_2a_3 + a_3a_4 - a_0a_1 - a_0a_5)(\lambda-1) \neq 0. \tag{16}$$

It can be shown that each vector L_A representing the left-sided unit of a locally reversible vector A is part of the set (10). This unit L_A also serves as the unique local two-sided unit E_A for vector A and for A^i where $i \geq 2$.
The FANA defined by Table 2 contains $\rho = p^3$ different GRS units R described by (17) [20]:

$$R = (r_0, r_1, r_2, r_3, r_4, r_5) = (-\lambda k, d, -\lambda t, k, 1-\lambda d, t). \tag{17}$$

where $d, k, t = 0, 1, \ldots, p-1$. The vectors A satisfying the condition:

$$\Delta_A = (a_0 + \lambda a_3)^3 + (\lambda a_1 + a_4)^3 + (a_2 + \lambda a_5)^3 - 3(a_0 + \lambda a_3)(\lambda a_1 + a_4)(a_2 + \lambda a_5) \neq 0 \tag{18}$$

are locally reversible. For each such vector, the local left-sided unit L_A corresponds, and all vectors L_A are contained in the set (17). Each L_A is also the unique local two-sided unit E_A for vectors A^i where $i \geq 1$.

The FANA defined by Table 3 contains $\rho = p^4$ different GRS units R given by (19) [10]:

$$R_r = \left(d, k, t, u, \frac{1-d-t}{\lambda}, -\lambda t - u\right) \tag{19}$$

where $d, k, t, u = 0, 1, \dots, p-1$. The vectors A satisfying the condition:

$$\Delta_A = (a_0 + a_2 + \lambda a_3)^2 - (\lambda a_1 + a_3 + a_5)^2, \tag{20}$$

are locally reversible. Each such vector has a corresponding local left-sided unit L_A and all these vectors are part of set (19), making L_A is simultaneously the single local two-sided unit L_A simultaneously the local two-sided unit A^i where $i \geq 1$.

3. COMMON PROPERTIES OF THE CONSIDERED ALGEBRA

One can easily show that the condition $\Delta_A \neq 0$ defines the existence of a unique solution of the vector equation:

$$X \circ A = V$$

for arbitrary vector V. For every one of the said three FANAs, the following propositions hold:

Proposition 1. Assume vector A satisfies the condition $\Delta_A \neq 0$. In this case, there exists an integer ω such that $A^\omega = E_A$, where E_A is the local two-sided unit, which also serves as the unit of the cyclic group generated by vector A.

Proof: the vector L_A functions as a local two-sided unit for each vector in the sequence $A, A^2, \dots,$ $, A^i, \dots$. Given that $\Delta_A \neq 0$, a unique value for L_A exists for the fixed vector A, and the sequence follows a periodic cycle with a length of ω. Suppose $A^j = A^i$, where $j > i$. Then, we have $A^{j-i} \circ A^i = A^i \Rightarrow A^{j-i} \circ A = A$. Since $\Delta_A \neq 0$, the equation $X \circ A = A$ has a single solution $X = L_A$; meaning, $A^{j-i} = L_A$. The collection of vectors within one full cycle forms a finite cyclic group generated by A, with the unit element $E_A = L_A$. Therefore, E_A can be expressed as $E_A = A^\omega$. For any integer i ($0 < i < \omega$), the vector $A^{\omega-i}$ acts as the inverse of A^i with respect to the local two-sided unit E_A; therefore, making vector A locally reversible. Proposition 1 is established.

Proposition 2. Assume that vector R is a GRS unit. Then, the map of the FANA, defined by the formula $\varphi_R(X) = R \circ X$, where X takes on all values in the FANA, is a homomorphism.

Proof: for any two vectors X_1 and X_2, we have:

$$\varphi_R(X_1 \circ X_2) = R \circ (X_1 \circ X_2) = (R \circ X_1) \circ (R \circ X_2) = \varphi_R(X_1) \circ \varphi_R(X_2),$$

$$\varphi_R(X_1 + X_2) = R \circ (X_1 + X_2) = (R \circ X_1) + (R \circ X_2) = \varphi_R(X_1) + \varphi_R(X_2).$$

Proposition 3. In every one of the considered 6-dimensional FANAs, the set of the locally reversible vectors composes ρ different groups with ρ different units that compose the set of GRS units.

Proof: suppose the set $\{A_1, A_2, \dots, A_i, \dots, A_\Omega\}$ includes all vectors associated with a fixed local two-sided unit E (including E itself) and only such vectors. This set forms a group Γ_E with unit E. Each GRS unit R' corresponds to the unit E' of a group Γ'_E consisting of locally reversible vectors $\{A'_1, A'_2, \dots, A'_\Omega\}$. According to Proposition 2, for $i = 1, 2, \dots, \Omega$, we have $\varphi_R(A_i) = R' \circ A_i = A'_i$, $R' \circ E = E'$, and $R' \circ E = R'$, therefore $R' = E'$. Thus, the set $\{A'_1, A'_2, \dots, A'_\Omega\}$ is a group with the unit R'. We have ρ different GRS units R, evidently, each defining a unique group of order Ω. Proposition 3 is proven.

4. STRUCTURE OF THE ALGEBRAS

Consider the order Ω of each of the isomorphic groups (see Proposition 3). Clearly, $\Omega = \Omega' p^{-2}$, where Ω' represents the total number of locally reversible vectors in the algebra. This value can be computed as $\Omega' = p^6 - \Omega''$, with Ω'' being the number of all irreversible vectors, i.e., vectors that meet certain conditions.

$$\Delta_A = 0 \tag{21}$$

4.1. FANA with p^2 global right-sided units

Using (15), condition (21) reduces to the:

$$a_2a_3 + a_4a_3 - a_0a_1 - a_0a_5 = 0$$

if $a_3 \neq 0$, then for arbitrary values of a_0, a_1, a_3, and a_4, there is a unique value of a_2 that satisfies the equation, giving $p^4(p-1)$ distinct irreversible vectors. For $a_3 = 0$, the equation holds true for any a_2 and a_4 when $a_1a_0 + a_0a_5 = 0$. This leads to two subcases: i) $a_0 \neq 0$ resulting in $p^3(p-1)$ irreversible vectors and ii) $a_0 = 0$ which gives p^4 irreversible vectors. Thus, the total number of irreversible vectors is $\Omega'' = p^4(p-1) + p^3(p-1) + p^4 = p^5 + p^4 - p^3$.

Proposition 4. Each of the p^2 isomorphic groups, associated with a fixed GRS unit R and containing all corresponding reversible vectors, has an order of $\Omega = p(p-1)^2(p-1)$.

Proof: the number of locally reversible vectors is $\Omega' = p^6 - \Omega'' = p^6 - (p^5 + p^4 - p^3) = p^3(p-1)(p^2-1)$ and therefore $\Omega = \Omega' p^{-2} = p(p-1)(p^2-1)$.

It is evident that all 6-dimensional vectors of the form $A' = (a_0, a_1, a_2, a_3, 0, 0)$ make up a 4-dimensional noncommutative subalgebra, with multiplication defined by the TMBV shown in Table 4. This subalgebra contains one global two-sided unit E_{00}, which is part of the set (10) and corresponds to $d = 0$ and $k = 0$.

$$E_{00} = \left(\frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, 0, 0\right)$$

This subalgebra is similar to the 4-dimensional FANA described in [16], which is used as the algebraic foundation for HDLP-based signature schemes. The multiplicative group Γ_{00}, which belongs to the subalgebra, is one of the p^2 isomorphic groups within 6-dimensional FANA.

Table 4. The TMBV for the 4-dimensional subalgebra with a global two-sided unit

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	e_0	e_3	e_0	e_3	-	-
e_1	λe_2	e_1	e_2	λe_1	-	-
e_2	e_2	e_1	e_2	e_1	-	-
e_3	λe_0	e_3	e_0	λe_3	-	-
e_4	-	-	-	-	-	-
e_5	-	-	-	-	-	-

4.2. FANA with p^3 global right-sided units

Taking into account (18), condition (21) reduces to (22):

$$\beta_1^3 + \beta_2^3 + \beta_3^3 - 3\beta_1\beta_2\beta_3 = 0 \tag{22}$$

where $\beta_1 = a_0 + \lambda a_3$, $\beta_2 = a_1 + a_4$, and $\beta_3 = a_2 + \lambda a_5$. Suppose we have n_β different triples $(\beta_1, \beta_2, \beta_3)$ satisfying the last equality. Then, we have $\Omega'' = p^3 n_\beta$ irreversible vectors in the considered FANA. For some fixed values β_2 and β_3, one can compute the values β_1 satisfying (22) as solutions of the following cubic equation in $GF(p)$:

$$\beta_1^3 - (3\beta_2\beta_3)\beta_1 + (\beta_2^3 + \beta_3^3) = 0. \tag{23}$$

The number of solutions of the cubic (23) is considered in [21]. The discriminant Dt of the cubic equation represents the value:

$$Dt = \frac{(\beta_2^3 + \beta_3^3)^2}{4} + \frac{-3(\beta_2\beta_3)^3}{27} = \frac{(\beta_2^3 - \beta_3^3)^2}{4}$$

that is, the quadratic residue in $GF(p)$. One should consider the following two cases: i) number 3 divides the value $p-1$ and ii) number 3 does not divide the value $p-1$.

Case 1. Consider subcases 1a), $Dt = 0$, and 1b), $Dt \neq 0$.

Subcase 1a. If $\beta_2\beta_3 \neq (0,0)$, then we have $3(p-1)$ different pairs $(\beta_2\beta_3)$ for which the condition $Dt = 0$ holds true (coefficient 3 is due to the existence of 3 different cubic roots from β_3^3). For every one of the said pairs $(\beta_2\beta_3)$, there exist 2 different solutions of (23); therefore, we have $6(p-1)$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23). If $\beta_2\beta_3 \neq (0,0)$, then only the value $\beta_1 = 0$ satisfies (23). Thus, in subcase 1a, we have $6(p-1)+1$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23).

Subcase 1b. We have $3(p-1)+1$ different pairs $(\beta_2\beta_3)$ such that $D_t = 0$ (see subcase 1a). Therefore, $p^2 - 3(p-1) - 1 = p^2 - 3p + 2$ different pairs $(\beta_2\beta_3)$ correspond to the values $D_t \neq 0$. If $D_t \neq 0$, then the cubic (23) has three different solutions [21]; therefore, in subcase 1b, we have $n_\beta = 3(p^2 - 3(p-1) + 2)$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23).

Totally, in case 1 we have $6(p-1)+1+3\left(p^2-3p+2\right) = 3p^2-3p+1$ different triples $(\beta_2, \beta_2, \beta_3)$ satisfying (23) and relating to $\Omega'' = p^3\left(3p^2-3p+1\right)$ irreversible vectors. The number of locally reversible vectors is equal to $\Omega' = p^6 - \Omega'' = p^3\,(p-1)^3$. Correspondingly, the order of every of p^3 different isomorphic groups is equal to $\Omega = (p-1)^3$.

Case 2. Consider subcases 2a, $Dt = 0$, and 2b), $Dt \neq 0$.

Subcase 2a. If $(\beta_2\beta_3) \neq (0,0)$, then we have $(p-1)$ different pairs $(\beta_2\beta_3)$ for which the condition $Dt = 0$ holds true (we have only one cubic root from β_3^3). For every one of the said pairs $(\beta_2\beta_3)$, there exist 2 different solutions of (23); therefore, we have $2(p-1)$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23). If $(\beta_2\beta_3) \neq (0,0)$, then only the value $\beta_1 = 0$ satisfies (23). Thus, in subcase 2a, we have $2(p-1)+1 = 2p-1$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23).

Subcase 2b. We have $(p-1)+1 = p$ different pairs $(\beta_2\beta_3)$ such that $Dt = 0$ (see subcase 1a). Therefore, $p^2 - p$ different pairs $(\beta_2\beta_3)$ correspond to the values $Dt \neq 0$. If $Dt \neq 0$, then the cubic (23) has one root in $GF(p)$ [21]; therefore, in subcase 2b, we have $n_\beta = p^2 - p$ different triples (β_2, β_3) satisfying (23).

In case 2, we have $2p - 1 + p^2 - p = p^2 + p - 1$ different triples $(\beta_1, \beta_2, \beta_3)$ satisfying (23) and relating to $\Omega'' = p^3(3p^2 - 3p + 1)$ irreversible vectors. The number of locally reversible vectors is equal to $\Omega' = p^6 - \Omega'' = p^3(p-1)(p^2-1)$. Correspondingly, the order of every p^3 different isomorphic groups contained in the considered FANA is equal to $\Omega = (p-1)(p^2-1)$.

It is clear that the set of all 6-dimensional vectors in the form $A' = (0, a_1, 0, a_3, 0, a_5)$ forms a 3-dimensional commutative subalgebra, with the multiplication defined by the TMBV shown in Table 5. This subalgebra includes a global two-sided unit $E_{000} = (0, \lambda^{-1}, 0, 0, 0, 0)$, all elements of which are contained in the set (17), where the E_{000} vector corresponds to the integer values $d = \lambda^{-1}$, $k = 0$, and $t = 0$. Actually, this subalgebra represents a 3-dimensional finite commutative associative algebra isomorphic to that described in [16]. The multiplicative group Γ_{000} of this subalgebra is one of the p^3 isomorphic groups within the 6-dimensional FANA under consideration.

Table 5. The TMBV setting the 3-dimensional subalgebra

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	0	0	0	0	0	0
e_1	0	λe_1	0	λe_3	0	λe_5
e_2	0	0	0	0	0	0
e_3	0	λe_3	0	λe_5	0	λe_1
e_4	0	0	0	0	0	0
e_5	0	λe_5	0	λe_1	0	λe_3

4.3. FANA with p^4 global right-sided units

Taking into account (20) condition (21) reduces to the following equation:

$$(a_0 + a_2 + \lambda a_4)^2 = (\lambda a_1 + a_3 + a_5)^2$$

consider the following two cases.

Case 1. If $\lambda a_1 + a_3 + a_5 = 0$ (p^2 different variants), then the value $a_0 + a_2 + \lambda a_4$ is also equal to zero (p^2 different variants), and in this case, we have p^4 different irreversible vectors.

Case 2. If $\lambda a_1 + a_3 + a_5 = s \neq 0$ ($p^3 - p^2$ different variants), then $a_0 + a_2 + \lambda a_4 = s$ (p^2 different variants) or $a_0 + a_2 + \lambda a_4 = -s$ (p^2 different variants). Thus, in case 2 , we have $2p^2(p^3 - p^2) = 2p^4(p-1)$ different irreversible vectors.

Thus, we have $p^4 + 2p^4(p-1) = 2p^5 - p^4$ irreversible vectors. In total, the algebra contains $\Omega'' = p^4 + 2p^4(p-1) = 2p^5 - p^4$ irreversible vectors.

Proposition 5. Each one of the p^4 isomorphic groups, associated with a fixed GRS unit R and containing all reversible vectors related to R, has an order $\Omega = (p-1)^2$.

Proof: the number of locally reversible vectors is given by $\Omega' = p^6 - \Omega'' = p^6 - (2p^5 - p^4) = p^4(p-1)^2$ and hence $\Omega = \Omega' p^{-4} = (p-1)^2$.

It is evident that the set of all 6-dimensional vectors in the form $A' = (a_0, 0, a_3, 0, 0, 0)$ constitutes a 2-dimensional commutative subalgebra, with the multiplication defined by the TMBV presented in Table 6. This subalgebra includes a global two-sided unit $E_{0000} = (1, 0, 0, 0, 0, 0)$, which belongs to the set (19) and corresponds to $d = 1$, $k = 0$, $t = 0$, and $u = 0$. This 2-dimensional subalgebra is isomorphic to the corresponding commutative algebras discussed in [16].

Table 6. The TMBV of the 2-dimensional commutative subalgebra

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	e_0	0	0	e_3	0	0
e_1	0	0	0	0	0	0
e_2	0	0	0	0	0	0
e_3	e_3	0	0	e_0	0	0
e_4	0	0	0	0	0	0
e_5	0	0	0	0	0	0

5. A CASE OF THE 6-DIMENSIONAL ALGEBRA CONTAINING A SET OF GLOBAL LEFT-SIDED UNITS

Consider the 6-dimensional FANA containing p^3 GLS units, which is set by Table 7.

Table 7. TMBV defining the FANA with p^3 GLS units ($\lambda \geq 2$)

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	e_0	e_1	e_2	e_3	e_4	e_5
e_1	λe_4	λe_3	λe_0	λe_5	λe_2	λe_1
e_2	e_2	e_5	e_4	e_1	e_0	e_3
e_3	λe_2	λe_5	λe_4	λe_1	λe_0	λe_3
e_4	e_4	e_3	e_0	e_5	e_2	e_1
e_5	λe_0	λe_1	λe_2	λe_3	λe_4	λe_5

The left-sided units satisfy:

$$X \circ A = A$$

which for some vector $A = (a_0, a_1, a_2, a_3, a_4, a_5)$ can be reduced to the next system of linear equations with unknown coordinates of the vector $X = (x_0, x_1, x_2, x_3, x_4, x_5)$:

$$\begin{cases} x_0a_0 + \lambda x_1a_2 + x_2a_4 + \lambda x_3a_4 + x_4a_2 + \lambda x_5a_0 = a_0; \\ x_0a_1 + \lambda x_1a_5 + x_2a_3 + \lambda x_3a_3 + x_4a_5 + x_5a_1 = a_1; \\ x_0a_2 + \lambda x_1a_4 + x_2a_0 + \lambda x_3a_0 + x_4a_4 + \lambda x_5a_2 = a_2; \\ x_0a_3 + \lambda x_1a_1 + x_2a_5 + \lambda x_3a_5 + x_4a_1 + \lambda x_5a_3 = a_3; \\ x_0a_4 + \lambda x_1a_0 + x_2a_2 + \lambda x_3a_2 + x_4a_0 + \lambda x_5a_4 = a_4; \\ x_0a_5 + \lambda x_1a_3 + x_2a_1 + \lambda x_3a_1 + x_4a_3 + \lambda x_5a_5 = a_5. \end{cases} \tag{24}$$

System (24) can be rewritten as two independent systems, each consisting of three unknown variables:

$$\begin{cases} (x_0 + \lambda x_5)a_0 + (\lambda x_1 + x_4)a_2 + (x_2 + \lambda x_3)a_4 = a_0; \\ (x_2 + \lambda x_3)a_0 + (x_0 + \lambda x_5)a_2 + (\lambda x_1 + x_4)a_4 = a_2; \\ (\lambda x_1 + x_4)a_0 + (x_2 + \lambda x_3)a_2 + (x_0 + \lambda x_5)a_4 = a_4; \end{cases} \tag{25}$$

$$\begin{cases} (x_0 + \lambda x_5)a_1 + (x_2 + \lambda x_3)a_3 + (x_4 + \lambda x_1)a_5 = a_1; \\ (\lambda x_1 + x_4)a_1 + (x_0 + \lambda x_5)a_3 + (x_2 + \lambda x_3)a_5 = a_3; \\ (x_2 + \lambda x_3)a_1 + (\lambda x_1 + x_4)a_3 + (x_0 + \lambda x_5)a_5 = a_5. \end{cases} \tag{26}$$

The solutions of (25) and (26) can be obtained by performing the variable substitution defined by the formulas $z_1 = x_0 + \lambda x_5$, $z_2 = \lambda x_1 + x_4$, and $z_3 = x_2 + \lambda x_3$. After such substitution, the systems (25) and (26) have (27), (28):

$$\begin{cases} z_1 a_0 + z_2 a_2 + z_3 a_4 = a_0; \\ z_3 a_0 + z_1 a_2 + z_2 a_4 = a_2; \\ z_2 a_0 + z_3 a_2 + z_1 a_4 = a_4; \end{cases} \tag{27}$$

$$\begin{cases} z_1 a_1 + z_3 a_3 + z_2 a_5 = a_1; \\ z_2 a_1 + z_1 a_3 + z_3 a_5 = a_3; \\ z_2 a_1 + z_2 a_3 + z_1 a_5 = a_5. \end{cases} \tag{28}$$

The latter two systems have the same solution, that is $z_1 = 1$, $z_2 = z_3 = 0$. Note that this solution is valid for an arbitrary value of the vector A, i.e., the inverse variable substitution $x_0 + \lambda x_5 = z_1$, $\lambda x_1 + x_4 = z_2$; $x_2 + \lambda x_3 = z_3$ gives a set of GLS units $L = (l_0, l_1, l_2, l_3, l_4, l_5)$ coordinates of which satisfy the system, including the $x_0 + \lambda x_5 = 1$; $\lambda x_1 + x_4 = 0$; and $x_2 + \lambda x_3 = 0$. The latter system defines the set of GLS units described by (29):

$$L = (1 - \lambda k, d, -\lambda h, h, -\lambda d, k), \tag{29}$$

where the integers d, h, and k take on all possible triples of values from the set $\{0, 1, \ldots, p-1\}$.
The right-sided unit associated with vector A satisfies (30)-(32):

$$A \circ X = A \tag{30}$$

$$\begin{cases} (a_0 + \lambda a_5)x_0 + (\lambda a_1 + a_4)x_2 + (a_2 + \lambda a_3)x_4 = a_0; \\ (a_2 + \lambda a_3)x_0 + (a_0 + \lambda a_5)x_2 + (\lambda a_1 + a_4)x_4 = a_2; \\ (\lambda a_1 + a_4)x_0 + (a_2 + \lambda a_3)x_2 + (a_0 + \lambda a_5)x_4 = a_4; \end{cases} \tag{31}$$

$$\begin{cases} (a_0 + \lambda a_5)x_1 + (a_2 + \lambda a_3)x_3 + (a_4 + \lambda a_1)x_5 = a_1; \\ (\lambda a_1 + a_4)x_1 + (a_0 + \lambda a_5)x_3 + (a_2 + \lambda a_3)x_5 = a_3; \\ (a_2 + \lambda a_3)x_1 + (\lambda a_1 + a_4)x_3 + (a_0 + \lambda a_5)x_5 = a_5. \end{cases} \tag{32}$$

Each of the latter two systems has the same main determinant that can be represented in the form:

$$\Delta_A = \beta_1^3 + \beta_2^3 + \beta_3^3 - 3\beta_1\beta_2\beta_3 = 0. \tag{33}$$

where $\beta_1 = a_0 + \lambda a_5$; $\beta_2 = \lambda a_1 + a_4$ and $\beta_3 = a_2 + \lambda a_3$. If $\Delta_A \neq 0$, then a unique right-sided unit R_A relates to the vector A. You can easily show that the vector R_A is contained in the set of GLS units (29). Thus, the vector R_A is simultaneously a unique local two-sided unit E_A corresponding to some fixed vector A. Relatively, the unit E_A to the vector A is locally reversible. Consideration of the number of locally reversible vectors in the FANA set by Table 7 leads to an analysis of to (22) and (23), which is presented in subsection 4.2. Therefore, the results similar to those obtained in subsection 4.2 are also true for the case of the algebra set by Table 7.

For instance, the set of all 6-dimensional vectors in the form $A' = (a_0, 0, a_2, 0, a_4, 0)$ forms a 3-dimensional commutative subalgebra, where the multiplication is governed by Table 8. This subalgebra includes a global two-sided unit $E_{000} = (1, 0, 0, 0, 0, 0)$, which belongs to the set (16) and corresponds to the values $d = 0$, $h = 0$ and $k = 0$. In fact, this subalgebra is a 3-dimensional finite commutative associative algebra, isomorphic to the one described in [16]. The multiplicative group Γ_{000} of the subalgebra is one of the p^3 isomorphic groups within the 6-dimensional FANA defined by Table 7.

Table 8. The TMBV setting the 3-dimensional subalgebra

$\circ$	e_0	e_1	e_2	e_3	e_4	e_5
e_0	e_0	0	e_2	0	e_4	0
e_1	0	0	0	0	0	0
e_2	e_2	0	e_4	0	e_0	0
e_3	0	0	0	0	0	0
e_4	e_4	0	e_0	0	e_2	0
e_5	0	0	0	0	0	0

6. DISCUSSION

For the construction of algebraic PK public key-cryptographic schemes, the noncommutativity property of the multiplication operation is essential. For example, in the HDLP-base public key agreement schemes the public key is computed as vector $Y = A^w Q^k A^{-w}$, where A and Q are non-commutative vectors; x and k represent the private key (in section 6 the notation $\circ$ for the multiplication operation is omitted). Since for the case of the 6-dimensional FANAs with p^3 and p^4 global single-sided units analyzed there exists homomorphism into a commutative subalgebra of dimension $m = 3$ and $m = 2$, respectively, you can make a general conclusion that these types of 6-dimensional FANAs do not provide PQ security.

Construction of PQ cryptoschemes is possible using the considered 6-dimensional FANA with p^2 global single-sided units, since for this algebra there is a homomorphic mapping into a four-dimensional non-commutative subalgebra with a global two-sided unit. Obviously, the 6-dimensional algebras with a global two-sided unit are also of interest for construction of PQ cryptoschemes, but this case is beyond the scope of the algebras under consideration. For example, construction of a PQ digital signature scheme on 6-dimensional FANAs with p^2 global single-sided units can be performed as follows.

Suppose you use the 6-dimensional FANA set by Table 1 over the field $GF(p)$, where $p = 2q+1$ with a 128-bit prime q. Due to the fact that the used 6-dimensional FANA represents the set of p^2 different isomorphic 4-dimensional subalgebras with unique global two-sided unit, you can conclude that a fixed vector acts as an element of the 6-dimensional FANA and as an element of a 4-dimensional non-commutative subalgebra that has the same order. The 4-dimensional FANAs (of all known types [16], [22]-[25]) with a global two-sided unit include vectors having orders equal to different divisors of the values $p^2 - 1$ and $p(p-1)$. For calculating a public key, two uniformly random non-scalar vectors P and H (such that $PH \neq HP$ and $\varphi(P)\varphi(H) \neq \varphi(H)\varphi(P)$ for every of p^2 existing homomorphisms in the considered 6-dimensional FANA) of the order q are generated. These vectors are used as generators of two different commutative hidden groups for computing the PK elements. The required non-equality $\varphi(P)\varphi(H) \neq \varphi(H)\varphi(P)$ provides resistance to quantum attacks, but is not fulfilled in the 6-dimensional FANAs with p^3 and with p^4 global single-sided units (since these two algebras are mapped by φ into a commutative subalgebras), therefore, the latter two algebras do not suit for using them as algebraic support in the following practical PQ signature algorithm.

6.1. Generation of the public key

In order to be able to sign electronic documents, you should generate a secret key and calculate the corresponding public key. To do this, the following computational steps are performed:

- Generate at random three integers x ($x < q$), u ($u < q$), and w ($w < q$) and three locally reversible vectors A, D, and F (used as private-key elements) such that you have the private key in the form of three integers x, u, w and five vectors A, D, F, P, H that are pair-wise non-commutative.
- Calculate six vectors Y, Z, U, T, N, K (composing the public key) by (24):

$$Y = AHA^{-1}; \quad Z = DPD^{-1}; \quad U = F^{-1}H^xF; \quad T = AH^uP^wD^{-1}; \\ N = F^{-1}H^wP^xD^{-1}; \quad K = F^{-1}H^{w+x}P^uD. \qquad (34)$$

6.2. Signature generation algorithm

Calculation of a digital signature to the document M is performed using the signer's private key (x, u, w, A, D, F, P, H) as follows:

- Randomly generate two natural numbers k ($k < q$) and t ($t < q$). Then, calculate the vector:

$$R = AH^kP^tD^{-1}. \qquad (35)$$

- Use a 256-bit collision-resistant hash function Φ to compute the signature's randomization element e as the hash value from the document M concatenated with the vector R: $e = e_1||e_2 = \Phi(M, R)$, where the hash-value e is represented as concatenation of two 128-bit integers e_1 and e_2.
- Calculate the integer $b : b = -w - e_2 \mod q$.
- Calculate the integer $n : n = k - xe_1e_2 - w - e_1 - u \mod q$.
- Calculate the vector S representing the fitting signature element:

$$S = DP^bH^nF. \qquad (36)$$

- Calculate the auxiliary 256-bit randomization parameter ρ in the form of the hash value calculated from the vector S: $\rho = \rho_1 || \rho_2 = \Phi(S)$, where ρ is also a concatenation of two 128-bit integers ρ_1 and ρ_2.
- Calculate the first auxiliary fitting signature element $s : s = -x^{-1}(w + x + n) \mod q$.
- Calculate the second auxiliary fitting signature element $\sigma : \sigma = (t - x - \rho_1)(b + u + \rho_2)^{-1} \mod q$.
- Output the 128-byte signature (e, s, σ, S).

The computational complexity of this algorithm mainly involves 4 exponentiations (see (35) and (36) to the 128-bit degrees in the used 6-dimensional FANA ($\approx$ 27,700 multiplications in $GF(p)$).

6.3. Signature verification algorithm

Authentication of the signature (e, s, σ, S) to document M is performed using the signer's public key (Y, Z, U, T, N, K) according to the following computational procedure:

- Compute the hash value ρ from the vector S: $\rho = \rho_1 || \rho_2 = \Phi(S)$.
- Calculate the vector R' using the signature elements s as (37):

$$R' = Y^{e_1} T Z^{e_2} S U^{e_1 e_2} N Z^{\rho_1} (S U^s K Z^{\rho_2})^{\sigma}. \tag{37}$$

- Calculate the 256-bit hash value e' from the document to which the vector R' is concatenated: $e' = \Phi(M, R')$.
- If $e' = e$, the signature is valid; otherwise, it is rejected.

The computational complexity for the verification process is primarily determined by 7 exponentiations to 128-bit degrees in the used 6-dimensional FANA ($\approx$ 48,400 multiplications in $GF(p)$). Substituting in (37) the public key elements expressed by (34), you can easily prove correctness of the introduced PQ signature algorithm.

The resistance of the latter to quantum attacks, including those using quantum computers, is based on the computational complexity of solving large systems of power equations over the field $GF(p)$. The system is set by (34), written for the unknown coordinates of 12 vectors: $A, D, F, P, P^u, P^w, P^x, H, H^u, H^w, H^{w+x}$, when considering these vectors raised to unknown powers, the system becomes one of power exponential equations, for which no efficient solution methods are known in current literature. The inability of quantum computers to solve large systems of power equations is exploited in multivariate PK cryptography (MPKC), a well-established area of PQ cryptography [26]–[29]. The introduced signature algorithm represents a new implementation of algebraic MPKC, featuring signature algorithms that use hidden commutative groups. A key novelty of the introduced MPKC algorithm is the use of two distinct commutative hidden groups, where elements of one group do not commute with those of the other.

The primary factor contributing to the security of MPKC algorithms is the number of equations in the power equation system that must be solved to break the algorithms [29]. In the case of algebraic MPKC signature algorithms, this number is proportional to the dimension of the FANAs. For the development of signature algorithms using a hidden group, the decomposition of FANAs into commutative subalgebras is crucial. However, such decomposition is effectively applied only in the case of 4-dimensional FANAs (of different types) with a global two-sided unit [13], [25]. When utilizing 6-dimensional FANAs with p^2 global single-sided units as the algebraic support for cryptographic algorithms, the results from [13], [25] can still be applied, thanks to the existing homomorphisms into 4-dimensional subalgebras.

7. CONCLUSION

In the 6-dimensional FANAs analyzed, we discovered that the presence of a substantial set of single-sided units correlates strongly with a large array of isomorphic subalgebras within each algebra. This observation suggests that our findings might be extendable to other FANAs (including other 6-dimensional FANAs) that also feature global single-sided (GRS or GLS) units. A new algebraic MPKC signature algorithm on the 6-dimensional FANA with p^2 global right-sided units is introduced as a candidate for a practical PQ signature algorithm as well as an illustration of the applying the obtained results on the structure of FANAs for estimating the resistance to quantum attacks and security level. In particular, it has been shown that the studied 6-dimensional FANAs with p^3 and p^4 global right-sided units do not suit for using them as algebraic support of the introduced PQ signature algorithm.

ACKNOWLEDGEMENTS

The authors are grateful to the anonymous referees for their valuable feedback.

FUNDING INFORMATION

This research was partially funded by the Russian Science Foundation (grant number: 24-41-04006; section 6), and by Vietnam Academy of Science and Technology (grant number: QTRU06.09/24-26; sections 2-7). The Russian authors were financially supported by the Russian Science Foundation.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	**C**	**M**	**So**	**Va**	**Fo**	**I**	**R**	**D**	**O**	**E**	**Vi**	**Su**	**P**	**Fu**
May Thu Duong	✓	✓		✓	✓	✓		✓	✓	✓			✓	
Alexander Andreevich Moldovyan	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Nikolay Andreevich Moldovyan	✓	✓		✓	✓	✓			✓	✓	✓	✓	✓	✓
Minh Hieu Nguyen	✓	✓		✓	✓	✓			✓	✓	✓		✓	✓
Bac Thi Do	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject Administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding Acquisition
Fo	: **Fo**rmal Analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] J. Ding and R. Steinwandt, "Post-Quantum Cryptography," *10th International Conference, PQCrypto 2019*, Chongqing, China, May 8–10, 2019, doi: 10.1007/978-3-030-25510-7.

[2] T. Lange and R. Steinwandt, "Post-Quantum Cryptography," *9th International Conference, PQCrypto 2018*, Fort Lauderdale, FL, USA, Apr. 2018, doi: 10.1007/978-3-319-79063-3.

[3] K. Kimball, "Announcing request for nominations for public-key post-quantum cryptographic algorithms," *Federal Register*, vol. 81, no. 244, pp. 92 787–92 788, 2016.

[4] M.-J. Saarinen and D. Smith-Tone, Eds., Post-Quantum Cryptography: 15th International Workshop, PQCrypto 2024, Oxford, UK, *Proceedings, Part I/II, ser. Lecture Notes in Computer Science. Springer, Cham*, vol. 14771/14772, 2024.

[5] G. Alagic *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *National Institute of Standards and Technology*, Tech. Rep. NIST IR 8413-upd1, Jul. 2022, doi: 10.6028/NIST.IR.8413-upd1.

[6] C. Battarbee, D. Kahrobaei, L. Perret, and S. F. Shahandashti, "SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures," *SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures*, Cham: Springer Nature Switzerland, 2023, vol. 14154, pp. 113–138, doi: 10.1007/978-3-031-40003-2_5.

[7] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," *Applied Cryptography and Network Security (ACNS 2005)*, 2005, pp. 164–175.

[8] N. Kundu, S. K. Debnath, D. Mishra, and T. Choudhury, "Post-quantum digital signature scheme based on multivariate cubic problem," *Journal of Information Security and Applications*, vol. 53, p. 102512, 2020.

[9] Q. Alamelou, O. Blazy, S. Cauchie, and P. Gaborit, "A code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, pp. 1–25, 2017.

[10] 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 Series Mathematical Modelling Programming and Computer Software*, vol. 12, no. 7, pp. 66–81, 2019, doi: 10.14529/mmp190106.

[11] Y. Ma, "Cryptanalysis of the cryptosystems based on the generalized hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 32, no. 2(95), pp. 289–307, 2024, doi: 10.56415/csjm.v32.15.

[12] V. Shpilrain and A. Ushakov, "The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, pp. 285–289, 2006, doi: 10.1007/s00200-006-0009-6.

[13] D. N. Moldovyan, "A new type of digital signature algorithms with a hidden group," *Computer Science Journal of Moldova*, vol. 31, no. 1, pp. 111–124, 2023, doi: 10.56415/csjm.v31.06.

[14] V. Shpilrain and G. Zapata, "Using decision problems in public key cryptography," *Groups Complexity Cryptology*, vol. 1, no. 1, pp. 33–49, 2009, doi: 10.1515/GCC.2009.33.

[15] V. Roman'kov, "Cryptanalysis of a Combinatorial Public Key Cryptosystem," *Groups, Complexity, Cryptology*, vol. 9, no. 2, pp. 125–135, 2017, doi: 10.1515/gcc-2017-0013.

[16] M. H. Nguyen, C. N. Hoang, A. A. Moldovyan, N. A. Moldovyan, H. Q. Vu, and D. K. Le Tran, "A novel version of the hidden logarithm problem for post-quantum signature algorithms," *Theoretical Computer Science*, vol. 921, pp. 36–49, 2022, doi:10.1016/j.tcs.2022.03.040.

[17] E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis, "Key agreement protocol (kap) using conjugacy and discrete logarithms problems in group representation level," *Informatica*, vol. 18, no. 1, pp. 115–124, 2007.

[18] 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, pp. 56–72, 2019.

[19] 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.

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

[21] N. A. Moldovyan, A. A. Moldovyan, and V. A. Shcherbacov, "Generating cubic equations as a method for public encryption," *Bulletin of the Academy of Sciences of Moldova. Mathematics*, vol. 3, no. 79, pp. 60–71, 2015.

[22] A. Pandey, I. Gupta, and D. K. Singh, "On the Security of DLCSP over $GL_n(\mathbb{F}_q[S_r])$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 34, pp. 619–628, 2023, doi: 10.1007/s00200-021-00523-6.

[23] V. Roman'kov, A. Ushakov, and V. Shpilrain, "Algebraic and quantum attacks on two digital signature schemes," *Journal of Mathematical Cryptology*, vol. 17, no. 1, p. 20220023, 2023, doi: 10.1515/jmc-2022-0023.

[24] 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.

[25] 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.

[26] J. Ding, A. Petzoldt, and D. S. Schmidt, "Multivariate Public Key Cryptosystems," *Springer New York*, 2020, doi: 10.1007/978-1-0716-0987-3.

[27] S. Qin, W. Han, Y. Li, and L. Jia, "Construction of Extended Multivariate Public Key Cryptosystems," *International Journal of Network Security*, vol. 18, no. 1, pp. 60–67, 2016.

[28] Y. Hashimoto, "Recent developments in multivariate public key cryptosystems," *International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019*, 2021, pp. 209–229, doi: 10.1007/978-981-15-5191-8_16.

[29] J. Ding and A. Petzoldt, "Current state of multivariate cryptography," *IEEE Security and Privacy Magazine*, vol. 15, pp. 28–36, 2017.

BIOGRAPHIES OF AUTHORS

May Thu Duong is a Ph.D. student at the Faculty of Information Technology, Thai Nguyen University of Information and Communication Technology, Vietnam. She received her M.Sc. degree in network and telecommunications from the University of Paris XI, France. Her research interests include computer science, computer networking, digital signature, and post-quantum cryptography. She can be contacted at email: dtmay@ictu.edu.vn.

Alexander Andreevich Moldovyan Chief Researcher of Laboratory of cybersecurity and post-quantum cryptosystems at St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences and a Professor with the St. Petersburg Electrotechnical University (LETI). His research interests include computer security. His research interests include information security and cryptographic protocols. He has authored or co-authored more than 60 inventions and 220 scientific articles, books, and reports. He received his Ph.D. from SPIIRAS (2012). He can be contacted at email: maa1305@yandex.ru.

Nikolay Andreevich Moldovyan is an honored inventor of the Russian Federation (2002), a Chief Researcher of the Laboratory of Cybersecurity and Post-Quantum Cryptosystems at St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, and a Professor at St. Petersburg Electrotechnical University (LETI). His research interests include computer security and cryptography. He has authored or co-authored more than 80 inventions and 250 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981). He can be contacted at email: nmold@mail.ru.

Minh Hieu Nguyen is a Vice Dean at the Academy of Cryptography Techniques, Hanoi, Vietnam. He received his Ph.D. from Saint Petersburg Electrotechnical University in 2006. His research interests include cryptography, communication, and network security. He has authored or co-authored more than 95 scientific articles, book chapters, reports, and patents in his research areas. He can be contacted at email: hieuminhmta@gmail.com.

Bac Thi Do is a Senior Lecturer at the Thai Nguyen University of Information and Communication Technology, Vietnam. Her research areas include cryptography, communication, and network security. She received her Ph.D. from Le Quy Don Technical University in 2014. She can be contacted at email: dtbac@ictu.edu.vn.