International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 3, June 2025, pp. 2965∼2976
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i3.pp2965-2976

Structure of quaternion-type algebras and a post-quantum signature algorithm

May Thu Duong[1], Alexander Andreevich Moldovyan[2], Dmitriy Nikolaevich 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:

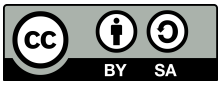
Received Jul 13, 2024
Revised Dec 22, 2024
Accepted Jan 16, 2025

Keywords:

Digital signature
Hidden group
Non-commutative
Post-quantum cryptography
Two-dimensional cyclicity

ABSTRACT

Algebraic digital signature algorithms with a commutative hidden group, which are based on the computational difficulty of solving large systems of power equations, are promising candidates for post-quantum cryptoschemes, especially in securing applications like the internet of things (IoT) and other information technologies. Associative finite non-commutative algebras are used as an algebraic support of the said algorithms. Among such algebras, finite quaternion-type algebras have been identified as strong candidates for providing algebraic support. This paper investigates the decomposition of these algebras into commutative subrings and explores their multiplicative groups, which can serve as potential hidden groups. The analysis reveals the existence of three distinct types of subrings, with derived formulas for the number of subrings and the orders of their multiplicative groups. These findings align with previous studies on four-dimensional algebras defined by sparse basis vector multiplication tables. Using the finite quaternion-type algebras as algebraic support, a novel post-quantum signature algorithm characterized in using two mutually non-commutative hidden groups has been developed.



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

The United States National Institute of Standards and Technology (NIST) has emphasized the critical importance of developing standards for post-quantum cryptography, underscoring the growing need for secure cryptosystems in the quantum computing era [1]–[4]. One of the major challenges in this field is designing practical post-quantum digital signature algorithms that are suitable for a wide range of information and communication technologies. This has led to the exploration of novel approaches, including the use of associative finite non-commutative algebras (AFNAs) as algebraic support for digital signature algorithms (DSAs) with a commutative hidden group [5]–[7]. Understanding the structure of AFNAs is crucial for assessing the security of that DSAs [8], [9]. For certain AFNAs, defined by sparse basis vector multiplication tables (BVMTs), this structural problem has been addressed in previous works [10], [11].

Quaternion-type algebras, introduced in [6], [12], have emerged as promising candidates for sup-

porting post-quantum electronic digital signature algorithms (DSAs) with hidden groups, which rely on the difficulty of solving large systems of power equations [7], [9]. This growing interest highlights the need for a deeper investigation into the structure of quaternion-type AFNAs, particularly focusing on their decomposition, where these algebras are viewed as finite non-commutative rings, into sets of commutative subrings. The relevance of this scientific problem lies in the significance of its results for the development of practical post-quantum DSAs on non-commutative associative algebras.

The present paper consideres decomposition of different versions of quaternion-type AFNAs, which represent finite non-commutative rings, into a set of commutative subrings and show the similarity of the structure of these algebras. Based on the obtained results, a novel post-quantum signature algorithm is introduced that uses two hidden commutative groups, where elements of one group are non-commutative with those of the other. The developed algorithm is of interest as a candidate for a prototype of a practical post-quantum DSA.

2. ASSOCIATIVE FINITE NON-COMMUTATIVE ALGEBRAS

A finite algebra can be defined as an m-dimensional vector space over a finite field, equipped with a closed vector multiplication operation that is both left and right distributive over vector addition. Any vector $\boldsymbol{A}$ in this space can commonly be represented in two ways: 1) As an ordered set of coordinates: $\boldsymbol{A} = (a_0, a_1, \ldots, a_{m-1})$, 2) As a sum of scalar multiples of basis vectors $a_i\boldsymbol{e}_i$: $\boldsymbol{A} = \sum_{i=0}^{m-1} a_i\boldsymbol{e}_i$, where $\boldsymbol{e}_i$ are basis vectors and a_i are elements of the finite field. This paper considers quaternion-type finite algebras set over the ground field $\mathrm{GF}(p)$, where p is an odd characteristic.

To ensure the properties of closure and two-sided distributivity in vector multiplication, we define the multiplication of two vectors $\boldsymbol{A}$ and $\boldsymbol{B}$ by multiplying each component of $\boldsymbol{A}$ with each component of $\boldsymbol{B}$ according to the following expression:

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

where every one of the products $\boldsymbol{e_i} \circ \boldsymbol{e_j}$ is substituted by a one-component vector $\lambda \boldsymbol{e_k}$ indicated in the cell at the intersection of the i-th row and the j-th column of some BVMT (for example, see Table 1). If the coordinate λ is not equal to 1, then it is called the structural constant.

If the defined multiplication operation is non-commutative and associative, then the resulting structure is an (AFNA). A unified method for generating AFNAs with a global two-sided unit (designated as E) for arbitrary even dimensions $m \geq 6$ was introduced in [12]. In the specific case of $m = 4$, this method produces symmetric BVMTs relative to the diagonal running from the upper-left to the lower-right corner. These symmetric BVMTs define commutative finite associative algebras.

However, as show in [12], it is possible to modify such BVMTs by introducing several different non-symmetric distributions of the structural constant $\lambda = 1$, which define non-commutative multiplication operations. One of these non-symmetric distributions is presented in Table 1 and corresponds to a four-dimensional AFNA known as a finite quaternion algebra. The use of AFNAs as algebraic support for digital signature algorithms (DSAs) is of particular interest due to their potential in developing practical algebraic post-quantum DSAs standard.

Table 1. Establishing the finite quaternion algebra with the unit element $E = (1, 0, 0, 0)$ [13]

$\circ$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$
$\boldsymbol{e}_0$	$\boldsymbol{e}_0$	$\boldsymbol{e}_1$	$\boldsymbol{e}_2$	$\boldsymbol{e}_3$
$\boldsymbol{e}_1$	$\boldsymbol{e}_1$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_3$	$-\boldsymbol{e}_2$
$\boldsymbol{e}_2$	$\boldsymbol{e}_2$	$-\boldsymbol{e}_3$	$-\boldsymbol{e}_0$	$\boldsymbol{e}_1$
$\boldsymbol{e}_3$	$\boldsymbol{e}_3$	$\boldsymbol{e}_2$	$-\boldsymbol{e}_1$	$-\boldsymbol{e}_0$

Post-quantum public key cryptography leverages computationally difficult problems beyond discrete logarithm and factorization problems. For instance, post-quantum algorithms have been developed based on groups [14], algebraic lattices [15], codes [16], and hash functions [17]. Of particular interest are post-quantum public key algorithms that rely on the computational difficulty of solving large systems of power equations involving many variables [18], [19], as quantum computers are inefficient at solving such systems. This area

of post-quantum cryptography is referred to as multivariate public key cryptography (MPKC) [20]. MPKC algorithms are typically designed using hard-to-reverse mappings with a secret trapdoor. These algorithms are known for their relatively high performance and compact digital signature sizes [21]. However, a significant drawback of MPKC algorithms lies in the exceptionally large size of the public key. Even with methods such as those described in [22], which reduce the size of the public key by an order of magnitude, the public key size remains substantially large.

To develop post-quantum DSAs with a small public key size, the studies in [5] and [6] propose utilizing the computational complexity of the so-called hidden discrete logarithm problem. This class of algorithms is referred to as algebraic algorithms with a hidden group. However, detailed analyses in [23], [24], and [25] have demonstrated the possibility of reducing known forms of the hidden discrete logarithm problem to the standard discrete logarithm problem, rendering these algorithms vulnerable to quantum attacks. Another class of algebraic algorithms with a hidden group, as described in [8] and [9], also achieves a small size for both the signature and the public key by leveraging the computational complexity of solving large systems of power equations. These algorithms can be classified as algebraic MPKC algorithms. This approach effectively addresses the limitations of existing MPKC algorithms based on hard-to-reverse mappings and represents a promising new direction in multivariate cryptography. It is particularly oriented toward the development of practical post-quantum signature algorithms on AFNAs with a global two-sided unit.

A unique research problem associated with the development of algebraic digital signature algorithms with a hidden group (that is commutative) lies in describing the possible types of commutative groups contained within the AFNA used as algebraic support. This problem can be formalized as studying the decomposition of a non-commutative ring, represented by the AFNA, into a set of commutative subrings. The papers [10] and [11] propose a methodology for such studies and provide a detailed description of the structure (from this perspective) of certain four-dimensional AFNAs defined by sparse BVMTs. When AFNAs defined by complete BVMTs (i.e., BVMTs without zero values for structural constants) are used as algebraic support, a strengthened interdependence is observed in the power equations describing the connection between elements of the secret and public keys. This characteristic makes AFNAs defined by complete BVMTs particularly interesting for cryptographic applications. Quaternion-like algebras belong to this latter type of AFNAs.

This article focuses on the development of signature algorithms on quaternion-type algebras. Consequently, studying the structure of such algebras forms a significant part of the research. Based on the obtained results, a new post-quantum algebraic MPKC signature algorithm is introduced. The novel features of this algorithm include the following: i) the use of two hidden groups, where the elements of one group are non-commutative with those of the other; ii) the incorporation of an auxiliary randomizing signature element in the form of a hash function computed from the value of the fitting signature element; and iii) the use of an auxiliary fitting signature element, represented by an integer, that serves as a degree in the verification equation.

3. QUATERNION-TYPE FINITE ALGEBRAS

The multiplication operation in the finite quaternion algebra is defined by Table 1 possessing the following distinguishing features:

a. Symmetry of basis vector distribution: The basis vectors are symmetrically arranged along the main diagonal, which extends from the upper-left corner to the lower-right corner of the BVMT.
b. Asymmetry of the distribution of the structural constant $\boldsymbol{\lambda = -1}$: The structural coefficient λ, equal to -1, is distributed asymmetrically across the BVMT cells. This asymmetry results in the non-commutative nature of the multiplication operation.
c. Associativity of multiplication: The multiplication operation within the algebra is associative.

In this paper, we refer to four-dimensional AFNAs defined by BVMTs exhibiting these properties as quaternion-type (QT) algebras. Examples of such algebras can be found in references [6], [12]. It is evident that quaternion-type AFNAs should be defined over finite fields $\mathrm{GF}(p^z)$, where z is a natural number, with an odd characteristic because, in the fields $\mathrm{GF}(2^z)$, the values 1 and -1 are equal.

The QT-type algebras presented in [6] and [12] ccan be extended by independently distributing the structural constants, including -1 and other arbitrary non-zero values. This extension results in four distinct versions of quaternion-type AFNAs, detailed in Tables 2, 3, 4, and 5. Key characteristics of these versions are as follows: i) Structural constants k, q, p, s, t, and u are independently assigned values of either -1 or 1; ii)

Each constant is positioned asymmetrically relative to the main diagonal and is repeated in exactly four cells within the BVMT; and iii) The design ensures that -1 is allocated to asymmetrically positioned cells, which guarantees the non-commutative nature of the algebra.

Table 2. Establishing the QT-algebras of the $\boldsymbol{e}$-version with the unit element $E = (1, 0, 0, 0)$ [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_1}$	$\boldsymbol{e_1}$	$qu\alpha\lambda\boldsymbol{e_0}$	$kqs\alpha\boldsymbol{e_3}$	$ksu\lambda\boldsymbol{e_2}$
$\boldsymbol{e_2}$	$\boldsymbol{e_2}$	$rtu\alpha\boldsymbol{e_3}$	$rs\alpha\beta\boldsymbol{e_0}$	$stu\beta\boldsymbol{e_1}$
$\boldsymbol{e_3}$	$\boldsymbol{e_3}$	$qrt\lambda\boldsymbol{e_2}$	$kqr\beta\boldsymbol{e_1}$	$kt\lambda\beta\boldsymbol{e_0}$

Table 3. Establishing the QT-algebras of the $\boldsymbol{i}$-version with the unit element $E = (0, 1, 0, 0)$ [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$ru\alpha\lambda\boldsymbol{e_1}$	$\boldsymbol{e_0}$	$krt\lambda\boldsymbol{e_3}$	$ktu\alpha\boldsymbol{e_2}$
$\boldsymbol{e_1}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_2}$	$qsu\lambda\boldsymbol{e_3}$	$\boldsymbol{e_2}$	$kq\beta\lambda\boldsymbol{e_1}$	$ksu\beta\boldsymbol{e_0}$
$\boldsymbol{e_3}$	$qrs\alpha\boldsymbol{e_2}$	$\boldsymbol{e_3}$	$qrt\beta\boldsymbol{e_0}$	$st\alpha\beta\boldsymbol{e_1}$

Table 4. Establishing the QT-algebras of the $\boldsymbol{j}$-version with the unit element $E = (0, 0, 1, 0)$ [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$kr\alpha\lambda\boldsymbol{e_2}$	$ktu\alpha\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$rtu\lambda\boldsymbol{e_1}$
$\boldsymbol{e_1}$	$qrs\alpha\boldsymbol{e_3}$	$qt\alpha\beta\boldsymbol{e_2}$	$\boldsymbol{e_1}$	$rst\beta\boldsymbol{e_0}$
$\boldsymbol{e_2}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_3}$	$kqs\lambda\boldsymbol{e_1}$	$kqu\beta\boldsymbol{e_0}$	$\boldsymbol{e_3}$	$su\beta\lambda\boldsymbol{e_2}$

Table 5. Establishing the QT-algebras of the $\boldsymbol{k}$-version with unity $E = (0, 0, 0, 1)$ [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$kr\beta\lambda\boldsymbol{e_3}$	$kts\beta\boldsymbol{e_2}$	$rts\lambda\boldsymbol{e_1}$	$\boldsymbol{e_0}$
$\boldsymbol{e_1}$	$rqu\beta\boldsymbol{e_2}$	$qs\alpha\beta\boldsymbol{e_3}$	$rsu\alpha\boldsymbol{e_0}$	$\boldsymbol{e_1}$
$\boldsymbol{e_2}$	$kqu\lambda\boldsymbol{e_1}$	$kqt\alpha\boldsymbol{e_0}$	$ut\alpha\lambda\boldsymbol{e_3}$	$\boldsymbol{e_2}$
$\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$

The structural constants α, β, and λ are symmetrically distributed along the main diagonal and can assume any non-zero values. If any of these constants is zero, the algebra becomes degenerate. In quaternion algebras, the basis vectors $\boldsymbol{e_0}, \boldsymbol{e_1}, \boldsymbol{e_2}$, and $\boldsymbol{e_3}$ are commonly denoted as $\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}$, and $\boldsymbol{k}$, respectively. QT-algebras are classified based on the specific vector, such as $\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}$, or $\boldsymbol{k}$, that consistently appears along the main diagonal, as shown in the titles of Tables 2, 3, 4, and 5. By varying the combinations of the structural constants $k, q, r, s, t, u, \alpha, \beta$, and λ, a diverse range of AFNAs can be created, corresponding to distinct quaternion-type algebras like $\boldsymbol{e}$-, $\boldsymbol{i}$-, $\boldsymbol{j}$-, and $\boldsymbol{k}$-based structures. In [12], the $\boldsymbol{e}$-quaternion algebra was introduced as a specific case in constructing an AFNA using a unified framework for defining associative algebras of even dimensions. This approach results in non-commutative algebras for dimensions $m \geq 6$ and commutative algebras for $m = 2$ and $m = 4$. However, in the four-dimensional case, [12] highlights that non-commutativity in multiplication can be achieved by assigning the structural constant -1 in an asymmetrical distribution. Several examples of four-dimensional AFNAs are provided in [12], one of which corresponds to a quaternion algebra. Implementations are presented in Table 2. The $\boldsymbol{i}$-, $\boldsymbol{j}$-, and $\boldsymbol{k}$-versions of the QT-algebras are explored in [6], where they serve as algebraic support for DSAs with a hidden group. The authors provide extended variations of these three versions of quaternion-type AFNAs, detailed in Tables 3, 4, and 5. It is straightforward to demonstrate that, for each studied algebra, the vector equations $\boldsymbol{X} \circ \boldsymbol{A} = \boldsymbol{A}$ and $\boldsymbol{A} \circ \boldsymbol{X} = \boldsymbol{A}$, where $\boldsymbol{X}$ is the unknown vector, have the same unique solution: the global two-sided unit $\boldsymbol{E}$. Furthermore, the specific value of $\boldsymbol{E}$ differs among the various versions of QT-algebras. These values are indicated in the titles of Tables 2, 3, 4, and 5.

Additionally, it can be shown that in all QT-algebras, the equations $\boldsymbol{X} \circ \boldsymbol{A} = \boldsymbol{E}$ and $\boldsymbol{A} \circ \boldsymbol{X} = \boldsymbol{E}$ either both lack solutions or both share the same unique solution $\boldsymbol{X} = \boldsymbol{A}^{-1}$, referred to as the inverse vector

of $\boldsymbol{A}$. In the first scenario, where no solution exists, $\boldsymbol{A}$ is called an irreversible vector; in the second scenario, where a unique solution exists, $\boldsymbol{A}$ is considered reversible. It is evident that the vectors $\boldsymbol{A}$ and $\boldsymbol{A}^{-1}$ commute with each other.

Vectors of the form $\boldsymbol{L} = \lambda \boldsymbol{E}$, where λ is a scalar factor from the field $\mathrm{GF}(p)$, are referred to as scalar vectors. It is straightforward to demonstrate that any fixed scalar vector commutes with all four-dimensional vectors within any given QT-algebra. The scalar vectors form a finite group of order $p-1$, which is a subgroup of every finite commutative group contained in the algebra.

4. STRUCTURE OF THE QUATERNION-TYPE ALGEBRAS OF THE J-VERSION

An examination of several arbitrarily chosen special cases of the k-version QT-algebras reveals that the unit vector in these algebras is $\boldsymbol{E} = (0, 0, 0, 1)$. This unit acts as a global two-sided unit for all possible combinations of the structural constants $k, q, r, s, t, u, \alpha, \beta$, and λ, with each fixed combination specifying a unique instance of the k-version QT-algebra. Previously, the case of the k-version QT-algebras, as specified in Table 6, was investigated in detail from the perspective of decomposition into a set of commutative subrings [13]. The method described in [13] involves fixing $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$ and solving the following vector equation for an unknown vector $\boldsymbol{X} = (x_0, x_1, x_2, x_3)$:

$$\boldsymbol{X} \circ \boldsymbol{A} = \boldsymbol{A} \circ \boldsymbol{X}. \tag{2}$$

Table 6. The investigated case of $\boldsymbol{k}$-version QT-algebras [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$\lambda \boldsymbol{e_3}$	$\boldsymbol{e_2}$	$\lambda \boldsymbol{e_1}$	$\boldsymbol{e_0}$
$\boldsymbol{e_1}$	$-\boldsymbol{e_2}$	$\boldsymbol{e_3}$	$-\boldsymbol{e_0}$	$\boldsymbol{e_1}$
$\boldsymbol{e_2}$	$-\lambda \boldsymbol{e_1}$	$\boldsymbol{e_0}$	$-\lambda \boldsymbol{e_3}$	$\boldsymbol{e_2}$
$\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$

Using (2) and Table 6, the vector (4) can be reduced to the following system of three linear equations in the finite field $\mathrm{GF}(p)$:

$$\begin{cases} a_1 x_2 = a_2 x_1, \\ a_2 x_0 = a_0 x_2, \\ a_1 x_0 = a_0 x_1. \end{cases} \tag{3}$$

All solutions of the system (4.) compose the set $\boldsymbol{\Psi_A}$ of vectors that commute with the vector A, the set $\boldsymbol{\Psi_A}$ being a finite ring. The results obtained in [13] show the following:

a. If $\boldsymbol{A}$ is a scalar vector, then $\boldsymbol{\Psi_A}$ contains all vectors of the considered AFNA.
b. If $\boldsymbol{A}$ is a non-scalar vector, then $\boldsymbol{\Psi_A}$ contains exactly p^2 distinct vectors. The set $\boldsymbol{\Psi_A}$ forms a finite commutative subring of the considered AFNA, representing a substructure within the finite non-commutative ring.
c. Every commutative subring of order p^2 includes all scalar vectors and $p^2 - p$ unique non-scalar vectors.
d. The total number of commutative subrings $\boldsymbol{\Psi_A}$ of order p^2 is given by $\eta = p^2 + p + 1$.
e. There are three distinct types of commutative subrings $\boldsymbol{\Psi_A}$ of order p^2, each characterized by the structure of their multiplicative group:

- The first type consists of a cyclic multiplicative group of order $p^2 - 1$. The number of subrings $\boldsymbol{\Psi_A}$ of the first type is:

$$\eta_1 = \frac{p(p-1)}{2}. \tag{4}$$

- The second type consists of a multiplicative group of order $(p-1)^2$, which exhibits two-dimensional cyclicity (as defined in [26]), i.e., it is generated by two vectors of order $p-1$. The number of subrings $\boldsymbol{\Psi_A}$ of the second type is:

$$\eta_2 = \frac{p(p+1)}{2}. \tag{5}$$

- The third type consists of a cyclic multiplicative group of order $p(p-1)$. The number of subrings $\boldsymbol{\Psi_A}$ of the third type is:

$$\eta_3 = p + 1. \tag{6}$$

For the security analysis of the developed DSAs on the QT-algebras, it is useful to describe all elements of the $\boldsymbol{\Psi_A}$ subring using the coordinates of the non-scalar vector $\boldsymbol{A}$. In the case $a_1 \neq 0$, the set $\boldsymbol{\Psi_A}$ is described by the following formula [13]:

$$\boldsymbol{X} = (x_0, x_1, x_2, x_3) = \left(\frac{a_0}{a_1} j, j, \frac{a_2}{a_1} j, k\right), \tag{7}$$

where $j, k = 0, 1, 2, \ldots, p-1$. The irreversibility condition for the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$ is given by:

$$\lambda a_0^2 + a_1^2 - a_2^2 - \lambda a_3^2 = 0. \tag{8}$$

5. THE DECOMPOSITION OF QUATERNION-TYPE ALGEBRAS OF OTHER VERSIONS

By applying the method described in [13], we analyzed the decomposition of AFNAs for various quaternion-type AFNAs of the $\boldsymbol{e}$-, $\boldsymbol{i}$-, and $\boldsymbol{j}$-versions. Our study revealed structural similarities across all specific cases of QT-algebras with the results presented in section 4 of [13]. For instance, the AFNA of the $\boldsymbol{e}$-version, defined by the BVMT in Table 7, contains vectors in the subring $\boldsymbol{\Psi_A}$, generated by the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$. In the case $a_3 \neq 0$, the subring is described by the following expression:

$$\boldsymbol{X} = (x_0, x_1, x_2, x_3) = \left(j, \frac{a_1}{a_3} k, \frac{a_2}{a_3} k, k\right), \tag{9}$$

The condition for the irreversibility of the vector $\boldsymbol{A}$ in the case $a_3 \neq 0$ is given by:

$$a_0^2 - \lambda a_1^2 - a_2^2 + \lambda a_3^2 = 0. \tag{10}$$

Table 7. A representative model of the $\boldsymbol{e}$-version QT-algebra [13].

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_1}$	$\boldsymbol{e_1}$	$\lambda \boldsymbol{e_0}$	$-\boldsymbol{e_3}$	$-\lambda \boldsymbol{e_2}$
$\boldsymbol{e_2}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$
$\boldsymbol{e_3}$	$\boldsymbol{e_3}$	$\lambda \boldsymbol{e_2}$	$-\boldsymbol{e_1}$	$-\lambda \boldsymbol{e_0}$

For the $\boldsymbol{i}$-version QT-algebra, defined by Table 8, the subring $\boldsymbol{\Psi_A}$, generated by the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$, is described by:

$$\boldsymbol{X} = (x_0, x_1, x_2, x_3) = \left(j, k, \frac{a_2}{a_0} j, \frac{a_3}{a_0} j\right), \tag{11}$$

The irreversibility condition for the vector $\boldsymbol{A}$ is given by:

$$\lambda a_0^2 + a_1^2 - \lambda a_2^2 - a_3^2 = 0. \tag{12}$$

Table 8. A representative model of the $\boldsymbol{i}$-version QT-algebra [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$-\lambda \boldsymbol{e_1}$	$\boldsymbol{e_0}$	$\lambda \boldsymbol{e_3}$	$-\boldsymbol{e_2}$
$\boldsymbol{e_1}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_2}$	$-\lambda \boldsymbol{e_3}$	$\boldsymbol{e_2}$	$\lambda \boldsymbol{e_1}$	$-\boldsymbol{e_0}$
$\boldsymbol{e_3}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$

For the $\boldsymbol{j}$-version QT-algebra, defined by Table 9, the subring $\boldsymbol{\Psi_A}$, generated by the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$, is given by:

$$\boldsymbol{X} = (x_0, x_1, x_2, x_3) = \left(\frac{a_0}{a_1} j, j, k, \frac{a_3}{a_1} j\right), \tag{13}$$

The irreversibility condition for the vector $\boldsymbol{A}$ is expressed as:

$$\lambda a_0^2 + a_1^2 - a_2^2 - \lambda a_3^2 = 0. \tag{14}$$

Table 9. A representative model of the $\boldsymbol{j}$-version QT-algebra [13]

$\circ$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_0}$	$\lambda \boldsymbol{e_2}$	$\boldsymbol{e_3}$	$\boldsymbol{e_0}$	$\lambda \boldsymbol{e_1}$
$\boldsymbol{e_1}$	$-\boldsymbol{e_3}$	$\boldsymbol{e_2}$	$\boldsymbol{e_1}$	$-\boldsymbol{e_0}$
$\boldsymbol{e_2}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
$\boldsymbol{e_3}$	$-\lambda \boldsymbol{e_1}$	$\boldsymbol{e_0}$	$\boldsymbol{e_3}$	$-\lambda \boldsymbol{e_2}$

6. A NEW ALGEBRAIC MPKC SIGNATURE ALGORITHM

The analysis of the decomposition of different versions of quaternion-type AFNAs into commutative subrings demonstrates a broad structural similarity, emphasizing their suitability as algebraic support for DSAs utilizing a commutative hidden group. This observed similarity holds significant promise for advancing practical post-quantum DSAs built on QT-algebras. Suppose a QT-algebra, for instance, defined by Table 6 over the field $\mathrm{GF}(p)$ with prime $p = 2q + 1$ (where q is a 128-bit prime), is used as algebraic support. In this case, to calculate a public key, one can generate two non-scalar vectors $\boldsymbol{P}$ and $\boldsymbol{G}$ of orders $p^2 - 1$ and q, respectively, such that $\boldsymbol{PG} \neq \boldsymbol{GP}$.

Algorithm 1. Algorithm for generating the vector $\boldsymbol{P}$

1: Select random integers $a_0, a_1, a_2, a_3 \neq 0$
2: If $\epsilon = a_1^{-2}(\lambda a_0^2 + a_1^2 - \lambda a_2^2)$ is a quadratic residue modulo p, then go back to step 1. (For such ϵ, the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$ is contained in the subring $\boldsymbol{\Psi_A}$ of the second type [13]; note that this step ensures that the output vector $\boldsymbol{A}$ is contained in the subring $\boldsymbol{\Psi_A}$ of the first type).
3: Select two random integers $j \neq 0$ and $k \neq 0$, and calculate the vector using formula 4.: $\boldsymbol{X} = (a_0 a_1^{-1} j, j, a_2 a_1^{-1} j, k)$.
4: If the order $\omega \boldsymbol{X} \neq p^2 - 1$ (where $\omega \boldsymbol{X}$ denotes the order of the vector $\boldsymbol{X}$), then return to step 3.
5: Output the vector $\boldsymbol{P} = \boldsymbol{X}$.

Algorithm 2. Algorithm for generating the vector $\boldsymbol{G}$)

1: Select random integers $a_0, a_1, a_2, a_3 \neq 0$.
2: If $\epsilon = a_1^{-2}(\lambda a_0^2 + a_1^2 - \lambda a_2^2)$ is a quadratic non-residue modulo p, then return to step 1. (For such ϵ, the vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$ is contained in the subring $\boldsymbol{\Psi_A}$ of the second type [13]. Note that this step ensures that the output vector $\boldsymbol{A} = (a_0, a_1, a_2, a_3)$ belongs to the subring $\boldsymbol{\Psi_A}$ of the second type).
3: Select two random integers $j \neq 0$ and $k \neq 0$, and calculate the vector using formula 4.: $\boldsymbol{X} = (a_0 a_1^{-1} j, j, a_2 a_1^{-1} j, k)$.
4: If the vector $\boldsymbol{X}$ is a scalar vector, then return to step 3.
5: If the order $\omega \boldsymbol{X} \neq q$ (where $\omega \boldsymbol{X}$ denotes the order of the vector $\boldsymbol{X}$), then return to step 3.
6: Output the vector $\boldsymbol{G} = \boldsymbol{X}$.

Algorithm 3. Algorithm for generating a public key

1: Generate three random integers: x ($x < p - 1$), u ($u < p - 1$), and w ($w < p^2 - 1$). Additionally, generate five reversible vectors $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{D}$, and $\boldsymbol{F}$, which are pairwise non-commutative. These vectors are used as secret masking vectors.
2: Compute the seven vectors $\boldsymbol{Y}, \boldsymbol{Z}, \boldsymbol{U}_Y, \boldsymbol{U}_Z, \boldsymbol{T}, \boldsymbol{T}_Y, \boldsymbol{T}_Z$, which compose the public key, using the following formulas:

$$\boldsymbol{Y} = \boldsymbol{APA}^{-1}, \quad \boldsymbol{Z} = \boldsymbol{B}^{-1}\boldsymbol{GB}, \quad \boldsymbol{U}_Y = \boldsymbol{B}^{-1}\boldsymbol{G}^x\boldsymbol{D}^{-1}, \quad \boldsymbol{U}_Z = \boldsymbol{B}^{-1}\boldsymbol{G}^u\boldsymbol{F}^{-1}, \tag{15}$$

$$\boldsymbol{T}_Y = \boldsymbol{DP}^w\boldsymbol{A}^{-1}, \quad \boldsymbol{T}_Z = \boldsymbol{FP}^{xu}\boldsymbol{A}^{-1}, \quad \boldsymbol{T} = \boldsymbol{DG}^{u-x}\boldsymbol{F}^{-1}. \tag{16}$$

Since the vectors $\boldsymbol{P}$ and $\boldsymbol{G}$ belong to different commutative subrings, the inequality $\boldsymbol{PG} \neq \boldsymbol{GP}$ holds. These vectors $\boldsymbol{P}$ and $\boldsymbol{G}$ are used as generators of two distinct commutative hidden groups for computing the public-key elements, which are masked elements of the first or second hidden group. Thus, the 450-byte secret key (including elements $x, u, w, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{D}, \boldsymbol{F}, \boldsymbol{G}$, and $\boldsymbol{P}$) is fully established in step 1 of the algorithm. The public key ($\boldsymbol{Y}, \boldsymbol{Z}, \boldsymbol{U}_Y, \boldsymbol{U}_Z, \boldsymbol{T}, \boldsymbol{T}_Y, \boldsymbol{T}_Z$) has a size of approximately 450 bytes. The calculation of a digital signature for an electronic document M is performed using the following algorithm.

Algorithm 4. Signature generation algorithm

1: Generate two random natural numbers k ($k < p-1$) and t ($t < p^2-1$). Then calculate the vector:

$$\boldsymbol{R} = \boldsymbol{D}\boldsymbol{P}^t\boldsymbol{G}^k\boldsymbol{F}^{-1}. \tag{17}$$

2: Using a specified 256-bit hash function Φ, calculate the first signature element e as the hash value of the document M concatenated with the vector $\boldsymbol{R}$: $e = e_1 \,||\, e_2 = \Phi(M, \boldsymbol{R})$, where the hash value e is represented as the concatenation of two 128-bit integers e_1 and e_2.
3: If the integers $w + e - xu - e_1e_2$ and $p^2 - 1$ are not mutually prime, return to step 1.
4: Calculate the integers b and n: $b = -xu - e_1e_2 \mod (p^2-1)$, $\quad n = -x - e_2 \mod q$.
5: Calculate the fitting signature element as the vector $\boldsymbol{S}$:

$$\boldsymbol{S} = \boldsymbol{A}\boldsymbol{P}^b\boldsymbol{G}^n\boldsymbol{B}. \tag{18}$$

6: Calculate the auxiliary randomization number ρ as the hash value of the vector $\boldsymbol{S}$: $\rho = \Phi(\boldsymbol{S})$.
7: Calculate the first auxiliary fitting signature element as the integer s: $s = t(w + e - xu - e_1e_2)^{-1} \mod (p^2-1)$.
8: Calculate the second auxiliary fitting signature element as the integer σ: $\sigma = (k - u + x)(\rho + u - x - e_2)^{-1} \mod q$.
9: Output the digital signature $(e, s, \sigma, \boldsymbol{S})$.

The size of the generated signature is approximately 144 bytes. On average, step 1 is performed twice. Therefore, the computational complexity of the signature generation algorithm is primarily determined by three exponentiations to the 256-bit degree and three exponentiations to the 128-bit degree in the used finite quaternion-type algebra ($\approx 27,650$ multiplications in $\mathrm{GF}(p)$).

Algorithm 5. Signature verification algorithm

1: Calculate the hash value derived from the vector $\boldsymbol{S}$: $\rho = \Phi(\boldsymbol{S})$.
2: Compute the vector $\boldsymbol{R}'$ using the following formula, which involves two entries of the signature element $\boldsymbol{S}$:

$$\boldsymbol{R}' = (\boldsymbol{T}_Y\boldsymbol{Y}^e\boldsymbol{S}\boldsymbol{Z}^{e_2}\boldsymbol{U}_Y)^{\boldsymbol{S}}\,\boldsymbol{T}\,(\boldsymbol{T}_Z\boldsymbol{Y}^{e_1e_2}\boldsymbol{S}\boldsymbol{Z}^{\rho}\boldsymbol{U}_Z)^{\sigma}. \tag{19}$$

3: Calculate the hash value e' from the document concatenated with the vector $\boldsymbol{R}'$: $e' = f(M, \boldsymbol{R}')$.
4: Verify the signature: If $e' = e$, then the signature is genuine. Otherwise, reject the signature as invalid.

The computational complexity of the signature verification algorithm is primarily determined by three exponentiations to the 256-bit degree and three exponentiations to the 128-bit degree in the finite QT-algebra ($\approx 27,650$ multiplications in $\mathrm{GF}(p)$). By substituting into equation [19] the public key elements expressed in formulas [15] and [16], the correctness of the introduced signature scheme can be easily demonstrated. Specifically, note that any reversible vector $\boldsymbol{V}$ raised to the power of zero equals the unity vector $\boldsymbol{E}$, namely: $\boldsymbol{P}^0 = \boldsymbol{E}$ and $\boldsymbol{G}^0 = \boldsymbol{E}$.

Correctness Proof

$$\boldsymbol{R}' = \left(\boldsymbol{D}\boldsymbol{P}^w\boldsymbol{A}^{-1}(\boldsymbol{A}\boldsymbol{P}\boldsymbol{A}^{-1})^e\boldsymbol{A}\boldsymbol{P}^b\boldsymbol{G}^n\boldsymbol{B}\left(\boldsymbol{B}^{-1}\boldsymbol{G}\boldsymbol{B}\right)^{e_2}\boldsymbol{B}^{-1}\boldsymbol{G}^x\boldsymbol{D}^{-1}\right)^s\boldsymbol{D}\boldsymbol{G}^{u-x}\boldsymbol{F}^{-1}\times$$

$$\left(\boldsymbol{F}\boldsymbol{P}^{xu}\boldsymbol{A}^{-1}(\boldsymbol{A}\boldsymbol{P}\boldsymbol{A}^{-1})^{e_1e_2}\boldsymbol{A}\boldsymbol{P}^b\boldsymbol{G}^n\boldsymbol{B}\left(\boldsymbol{B}^{-1}\boldsymbol{G}\boldsymbol{B}\right)^{\rho}\boldsymbol{B}^{-1}\boldsymbol{G}^u\boldsymbol{F}^{-1}\right)^{\sigma} =$$

$$= \left(\boldsymbol{D}\boldsymbol{P}^{w+e+b}\boldsymbol{G}^{n+e_2+x}\boldsymbol{D}^{-1}\right)^s\boldsymbol{D}\boldsymbol{G}^{u-x}\boldsymbol{F}^{-1}\times\left(\boldsymbol{F}\boldsymbol{P}^{xu+e_1e_2+b}\boldsymbol{G}^{n+\rho+u}\boldsymbol{F}^{-1}\right)^{\sigma} =$$

$$= \left(\boldsymbol{D}\boldsymbol{P}^{w+e-xu-e_1e_2}\boldsymbol{G}^{-x-e_2+e_2+x}\boldsymbol{D}^{-1}\right)^s\boldsymbol{D}\boldsymbol{G}^{u-x}\boldsymbol{F}^{-1}\times\left(\boldsymbol{F}\boldsymbol{P}^{xu+e_1e_2-xu-e_1e_2}\boldsymbol{G}^{-x-e_2+\rho+u}\boldsymbol{F}^{-1}\right)^{\sigma} =$$

$$= \left(\boldsymbol{D}\boldsymbol{P}^{w+e-xu-e_1e_2}\boldsymbol{G}^{0}\boldsymbol{D}^{-1}\right)^s\boldsymbol{D}\boldsymbol{G}^{u-x}\boldsymbol{F}^{-1}\times\left(\boldsymbol{F}\boldsymbol{P}^{0}\boldsymbol{G}^{-x-e_2+\rho+u}\boldsymbol{F}^{-1}\right)^{\sigma} =$$

$$= \boldsymbol{DP}^{w+e-xu-e_1e_2}\boldsymbol{G}^0\boldsymbol{D}^{-1}\boldsymbol{DG}^{u-x}\boldsymbol{F}^{-1} = \boldsymbol{DP}^s\boldsymbol{G}^u\boldsymbol{G}^{-x-e_2+\rho+u}\boldsymbol{F}^{-1} = \boldsymbol{DP}^t\boldsymbol{G}^k\boldsymbol{F}^{-1} = \boldsymbol{R}.$$

$$\Longrightarrow\ e' = \Phi(M, \boldsymbol{R}') = \Phi(M, \boldsymbol{R}) = e.$$

The equality $e' = e$ proves that the signature is genuine, i.e., every correctly computed digital signature passes the verification procedure as a valid one. In comparison with the MPKC algorithms [7], [9], the introduced algorithm is characterized by: i) Utilizing two commutative hidden groups associated with different commutative subrings (of types $\boldsymbol{\Gamma}_1$ and $\boldsymbol{\Gamma}_2$); ii) Employing the auxiliary randomization parameter ρ, calculated as a hash value $\Phi(\boldsymbol{S})$ derived from the fitting signature element $\boldsymbol{S}$; iii) Incorporating two auxiliary fitting signature elements $\boldsymbol{s}$ and $\boldsymbol{\sigma}$. The security of the described signature scheme relies on the computational difficulty of solving a system of 12 vector power equations (as defined by formulas (15)) with the following 11 unknowns: $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{D}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{P}, \boldsymbol{G}_x = \boldsymbol{G}^x, \boldsymbol{G}_u = \boldsymbol{G}^u, \boldsymbol{G}_{u-x} = \boldsymbol{G}^{u-x}, \boldsymbol{P}_w = \boldsymbol{P}^w, \boldsymbol{G}_{ux} = \boldsymbol{G}^{ux}$, which are determined by the formulas (26) and the pairwise commutativity relationships among the unknowns: $\boldsymbol{G}, \boldsymbol{G}_x, \boldsymbol{G}_u : \boldsymbol{GG}_x = \boldsymbol{G}_x\boldsymbol{G}, \quad \boldsymbol{GG}_u = \boldsymbol{G}_u\boldsymbol{G}, \quad \boldsymbol{GG}_{u-x} = \boldsymbol{G}_{u-x}\boldsymbol{G}$, and similarly: $\boldsymbol{P}, \boldsymbol{P}_w, \boldsymbol{P}_{ux} : \boldsymbol{PP}_w = \boldsymbol{P}_w\boldsymbol{P}, \quad \boldsymbol{PP}_{xu} = \boldsymbol{P}_{xu}\boldsymbol{P}$. Using Table 6, this system reduces to 48 quadratic equations with 44 unknowns over the finite field $\mathrm{GF}(p)$, where p is a 129-bit prime. Based on the estimations provided in [27] (see Table 1 in [27]), the security level of the proposed post-quantum signature algorithm is evaluated to be $\geq 2^{128}$.

A more efficient attack involves exploiting the decomposition of quaternion algebras into commutative subrings. Instead of solving the equations: $\boldsymbol{GG}_x = \boldsymbol{G}_x\boldsymbol{G}, \quad \boldsymbol{GG}_u = \boldsymbol{G}_u\boldsymbol{G}, \quad \boldsymbol{GG}_{u-x} = \boldsymbol{G}_{u-x}\boldsymbol{G}, \quad \boldsymbol{PP}_w = \boldsymbol{P}_w\boldsymbol{P}, \quad \boldsymbol{PP}_{xu} = \boldsymbol{P}_{xu}\boldsymbol{P}$, an attacker can represent each of the vector unknowns $\boldsymbol{G}_x, \boldsymbol{G}_u, \boldsymbol{G}_{u-x}$ using four coordinates of the vector $\boldsymbol{G}$ and two scalar unknowns (refer to formulas [7], [11], and [13] for details on different QT-algebra versions used as algebraic support for the proposed DSA). Similarly, the vector unknowns $\boldsymbol{P}_w$ and $\boldsymbol{P}_{xu}$ can be expressed through four coordinates of the vector $\boldsymbol{P}$ and two scalar unknowns. In the framework of such a modified attack, the system reduces to 24 power scalar equations with 30 scalar unknowns, yielding a security estimation of $\approx 2^{80}$. A comparison of these two attacks demonstrates that incorporating the results from the decomposition of quaternion-like algebras significantly reduces the expected computational complexity of the attack on the developed signature algorithm. This highlights a promising approach for constructing post-quantum algebraic DSAs with two hidden commutative groups. While this method can be adapted for various algorithmic implementations, exploring these possibilities is a subject for future research. Moreover, to properly assess the security of the algorithms under development, it is crucial to understand the structural properties of the algebras used as algebraic support.

Additionally, the applied novel technique, which utilizes the exponentiation operation to the degree ρ, computed as a hash function value from the fitting signature element $\boldsymbol{S}$, plays a significant role in providing high-level security against forging signature attacks. Such attacks involve solving the signature verification equation for fixed values of $\boldsymbol{R}', e, s$, and $\boldsymbol{\sigma}$, with the vector $\boldsymbol{S}$ being the unknown. In the developed algebraic post-quantum DSA, this type of attack is mitigated by the following two factors: i) The vector $\boldsymbol{S}$ appears twice in the signature verification equation; and ii) One of the degrees in the verification equation explicitly depends on the value of $\boldsymbol{S}$.

7. CONCLUSION

The results of the investigation into the structure of various versions of QT-algebras reveal a significant structural similarity, highlighting their potential for the development of post-quantum digital signatures with a commutative secret group. The observed similarities in the decomposition of different versions of QT-algebras indicate that various types and versions of QT-algebras can be utilized in the proposed digital signature scheme with two hidden commutative groups. Furthermore, a comparison of these findings with previous studies on four-dimensional AFNAs defined by sparse BVMTs reveals a general similarity in the decomposition of such algebras into commutative subrings when a global two-sided unit is present. Based on this, it can be concluded that the developed algorithm has the potential to be implemented using a four-dimensional AFNAs defined by a sparse BVMT, achieving an approximate twofold increase in performance. However, this optimization represents an independent research task of practical significance. Even without this potential optimization, the developed post-quantum DSA remains practically attractive due to the small size of the public key and signature, along with sufficiently high performance. The proposed scheme is characterized by the use of two hidden commutative groups that are mutually non-commutative.

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	√	√		√	√	√		√	√	√	√	√	√	√
Dmitriy Nikolaevich Moldovyan	√	√		√	√	√		√	√	√	√	√	√	√
Minh Hieu Nguyen	√	√		√	√	√		√	√	√	√		√	√
Bac Thi Do	√	√		√	√	√		√	√	√	√	√	√	√

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

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] M.-J. Saarinen and D. Smith-Tone, Eds., *Post-Quantum Cryptography: 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings*, Lecture Notes in Computer Science. Springer, Cham, 2024, V. 14771/14772. Springer, Cham.

[2] G. Alagic *et al.*, "Status report on the first round of the NIST post-quantum cryptography standardization process," Gaithersburg, MD, Jan. 2019. doi: 10.6028/NIST.IR.8240.

[3] D. Moody *et al.*, "Status report on the second round of the NIST post-quantum cryptography standardization process." *NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology*, Gaithersburg, MD, 2020.

[4] G. Alagic *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," July 2022, doi: 10.6028/NIST.IR.8413-upd1.

[5] N. A. Moldovyan, "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*, vol. 89, no. 1, pp. 71–78, 2019.

[6] N. A. Moldovyan, "Signature schemes on algebras, satisfying enhanced criterion of post-quantum security," *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, vol. 93, no. 2, pp. 62–67, 2020.

[7] N. A. Moldovyan, "Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations," *Quasigroups and Related Systems*, vol. 30, no. 2, pp. 287–298, 2022, doi: 10.56415/qrs.v30.24.

[8] A. Moldovyan, D. Moldovyan, N. Moldovyan, and A. Kurysheva, "A method for specifying complete signature randomization and an algebraic algorithm based on it," *Mathematics*, vol. 12, no. 13, 2024, doi: 10.3390/math12131970.

[9] M. T. Duong, D. N. Moldovyan, B. V. Do, and M. H. Nguyen, "Post-quantum signature algorithms on non-commutative algebras, using difficulty of solving systems of quadratic equations," *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4169407.

[10] N. A. Moldovyan and A. A. Moldovyan, "Digital signature scheme on the 2 × 2 matrix algebra," *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, vol. 17, no. 3, pp. 254–261, 2021, doi: 10.21638/11701/spbu10.2021.303.

[11] D. Moldovyan, A. Moldovyan, and N. Moldovyan, "Structure of a finite non-commutative algebra set by a sparse multiplication table," *Quasigroups and Related Systems*, vol. 30, no. 1, pp. 133–140, 2022, doi: 10.56415/qrs.v30.11.

[12] N. Moldovyan, "Unified method for defining finite associative algebras of arbitrary even dimensions," *Quasigroups and Related Systems*, vol. 26, no. 2, pp. 263–270, 2018.

[13] M. T. Duong, A. A. Moldovyan, D. N. Moldovyan, M. H. Nguyen, and B. T. Do, "Decomposition of quaternion-like algebras into a set of commutative subalgebras," *Communications in Computer and Information Science*, vol. 2310 CCIS, pp. 119–131, 2024, doi: 10.1007/978-981-96-0437-1_9.
[14] C. Battarbee, D. Kahrobaei, L. Perret, and S. F. Shahandashti, "Towards efficient, post-quantum group-based signatures," in *SPDH-Sign*, 2023, pp. 113–138. doi: 10.1007/978-3-031-40003-2_5.
[15] J. Gärtner, "NTWE: a natural combination of NTRU and LWE," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 14154, pp. 321–353, 2023, doi: 10.1007/978-3-031-40003-2_12.
[16] Q. Alamélou, O. Blazy, S. Cauchie, and P. Gaborit, "A code-based group signature scheme," *Designs, Codes, and Cryptography*, vol. 82, no. 1–2, pp. 469–493, 2017, doi: 10.1007/s10623-016-0276-6.
[17] B. Hamlin and F. Song, "Quantum security of hash functions and property-preservation of iterated hashing," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11505, pp. 329–349, 2019, doi: 10.1007/978-3-030-25510-7_18.
[18] A. Moldovyan and N. Moldovyan, "Vector finite fields of characteristic two as algebraic support of multivariate cryptography," *Computer Science Journal of Moldova*, vol. 32, no. 1, pp. 46–60, 2024, doi: 10.56415/csjm.v32.04.
[19] Y. Hashimoto, Recent developments in multivariate public key cryptosystems BT - International Symposium on Mathematics, Quantum Theory, and Cryptography. Singapore: *Springer*, 2021.
[20] 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, 2020, doi: 10.1016/j.jisa.2020.102512.
[21] J. Ding, A. Petzoldt, and D. S. Schmidt, "Oil and vinegar," in *Multivariate Public Key Cryptosystems. Advances in Information Security, ser. Advances in Information Security*. Springer, New York, 2020, vol. 80, pp. 89–151. doi: 10.1007/978-1-0716-0987-3_5
[22] N. A. Moldovyan, "Finite algebras in the design of multivariate cryptography algorithms," *Buletinul Academiei de Ştiinţe a Republicii Moldova. Matematica*, pp. 80–89, Jun. 2024, doi: 10.56415/basm.y2023.i3.p80.
[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, 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, Jun. 2017, doi: 10.1007/s10958-017-3371-y.
[25] Y. Ma, "Cryptanalysis of the cryptosystems based on the generalized hidden discrete logarithm problem," *Computer Science Journal of Moldova*, vol. 32, no. 2, pp. 289–307, 2024, doi: 10.56415/csjm.v32.15.
[26] N. A. Moldovyan, "Fast signatures based on non-cyclic nite groups," *Quasigroups and Related Systems*, vol. 18, pp. 83–94, 2010.
[27] J. Ding and A. Petzoldt, "Current state of multivariate cryptography," *IEEE Security and Privacy*, vol. 15, no. 4, pp. 28–36, 2017, doi: 10.1109/MSP.2017.3151328.

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, Thai Nguyen, 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 computer security problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences and a Professor with the St. Petersburg Electrotechnical Univeristy LETI, St. Petersburg, Russia. 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 can be contacted via email at: maa1305@yandex.ru.

Dmitriy Nikolaevich Moldovyan is an Associate Professor Professor with the St. Petersburg Electrotechnical Univeristy LETI and a researcher at the Laboratory of computer security problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. His research interests include information security and post-quantum cryptography. He has authored or co-authored 8 inventions and 60 scientific articles and books. He can be contacted via email at: mdn.spectr@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 via email at: 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 via email at: dtbac@ictu.edu.vn.