Post-quantum Cryptoschemes: New Finite Non-commutative Algebras for Defining Hidden Logarithm Problem

Hieu Minh Nguyen[1(✉)], Nikolay Andreevich Moldovyan[2], Alexandr Andreevich Moldovyan[2], Nam Hai Nguyen[1], Cong Manh Tran[3], and Ngoc Han Phieu[1]

[1] Academy of Cryptography Techniques, 141 Chien Thang Street, Hanoi, Vietnam
hieuminhmta@gmail.com, nnhaivn61@gmail.com, phieungochan@gmail.com
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 14-th line 39, 199178 St. Petersburg, Russia
nmold@mail.ru, maa1305@yandex.ru
[3] Le Quy Don Technical University, No 236 Hoang Quoc Viet Road, Hanoi, Vietnam
manhtc@gmail.com

Abstract. In the article we present some properties of non-commutative finite algebras of four-dimension vectors with parameterized multiplication operation characterized in that different modifications of the multiplication operation are mutually associative. One of the introduced finite algebras represents ring. Other algebra contains no global unit element, its elements are invertible locally, and is characterized in that the multiplication operation possess compression property. Regarding the investigated ring, the detailed attention is paid to properties of the set of non-invertible elements of the ring. Formulas for zero-divisors and unit elements of different types are derived. The introduced finite algebras represent interest to define over them the hidden discrete logarithm problem that is a promising cryptographic primitive for post-quantum cryptography.

Keywords: Finite algebra · Ring · Galois field · Vector
Local left unit element · Bi-side unit element
Associative multiplication · Parameterized multiplication
Cryptoscheme

1 Introduction

Cryptographic algorithms and protocols [1,2], including cryptosystems with public key, based on the computational difficulty of the factorization problem for numbers of a special type [3] and the discrete logarithm problem (DLP) [4] have found a wide practical application for solving problems of providing information-safe modern computer technologies. The security of cryptosystems based on

P. Cong Vinh and V. Alagar (Eds.): ICCASA 2018/ICTCC 2018, LNICST 266, pp. 1–12, 2019.
https://doi.org/10.1007/978-3-030-06152-4_16

these problems is determined by the fact that the most effective algorithms for solving these problems, known at the present time and implemented with the use of existing computer technology, have a subexponential (factorization and DLP in finite fields) or exponential complexity (DLP on an elliptic curve). In connection with the significant progress in the development of quantum computations [5,6], interest in estimating the complexity of discrete logarithmic and factorization in solving these problems on a quantum computer has arisen. It was shown that both of these problems have a polynomial complexity in the model of quantum computations [7,8]. These results and the expectation of the appearance of practically functioning quantum computers capable of effectively solving the problem of cracking existing cryptoschemes based on the DLP and the factorization problem, raises the problem of creating an arsenal of the electronic digital signature, public key distribution, and public encryption protocols, which would be convenient for practical use and resistant to attacks using quantum computers. Algorithms of cryptography with a secret key, for example block ciphers, according to experts will remain resistant to cryptanalysis using quantum computers. However, to ensure sufficient security of the public key cryptoschemes it is required to put into their basis computationally difficult problems of another type whose computational complexity of solution would be of superpolynomial complexity when using both conventional and quantum computers. The response to this challenge was the announcement by the National Institute of Standards and Technology (NIST) of the competition but the post-quantum two-key cryptograms development [9] and the appearance of regularly held thematic conference [10].

Finite non-commutative rings (FNRs) are interesting for designing public-key cryptoschemes based on the discrete logarithm problem in hidden commutative subgroup [11–14] that represents interest as potential primitive of the post-quantum cryptography. Earlier, for the development of post-quantum cryptosystems based on the computational difficulty of the hidden discrete logarithm problem, the finite algebra of quaternions was applied [12,13]. However, realizing the potential of this computationally difficult problem as a primitive of the post-quantum cryptography requires significantly expanding the class of its carriers [14]. Present paper introduces two novel carriers of the hidden discrete logarithm problem and discusses their properties. Different FNR can be constructed in the form of associative finite algebras (AFAs), defining multiplication operation of vectors in some finite vector space.

Suppose $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ be some formal basis vectors and $a, b, c, d \in GF(p)$, where prime $p \geq 3$, are coordinates. The vectors are denoted as $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ or as (a, b, c, d). The terms $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, are called components of the vector.

The operation of addition of two vectors (a, b, c, d) and (x, y, z, v) is defined via addition of the corresponding coordinates according to the following formula: $(a, b, c, d) + (x, y, z, v) = (a + x, b + y, c + z, d + v)$.

The multiplication of two vectors $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ and $x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + v\mathbf{k}$ is defined with the following formula:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + v\mathbf{k})$$
$$= ax\mathbf{e} \circ \mathbf{e} + bx\mathbf{i} \circ \mathbf{e} + cx\mathbf{j} \circ \mathbf{e} + dx\mathbf{k} \circ ... \circ \mathbf{j} + av\mathbf{e} \circ \mathbf{k} + bv\mathbf{i} \circ \mathbf{k} + cv\mathbf{j} \circ \mathbf{k} + dv\mathbf{k} \circ \mathbf{k},$$

where $\circ$ denotes the vector multiplication operation and each product of two basis vectors is to be replaced by some basis vector or by a one-component vector in accordance with the basis-vector multiplication table (BVMT) defining associative and non-commutative multiplication. In this paper there are introduced two novel BVMTs that define parameterized multiplication operations, different modifications of which are mutually associative. The proposed BVMTs are shown in Tables 1 and 2, where $\mu \in GF(p)$ and $\tau \in GF(p)$ are structural coefficients. In the last formula it is assumed that in every product of two basis vectors the left (right) operant indicates the row (column) of the BVMT and the intersection of the indicated row and column defines the cell of the BVMT in which it is given the value of the product. The AFA defined with Table 2 is characterized in that the multiplication operation possesses property of compression, i.e. multiplication of arbitrary two non-zero elements of the AFA gives as the result a vector (a, b, c, d) satisfying the condition $ac = bd$.

Table 1. The basis-vector multiplication table defining a finite ring

$\circ$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$	$\overrightarrow{k}$
$\overrightarrow{e}$	$\mathbf{e}$	$\mu\mathbf{k}$	$\mu\mathbf{e}$	$\mathbf{k}$
$\overrightarrow{i}$	$\tau\mathbf{j}$	$\mathbf{i}$	$\mathbf{j}$	$\tau\mathbf{i}$
$\overrightarrow{j}$	$\mathbf{j}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mathbf{i}$
$\overrightarrow{k}$	$\tau\mathbf{e}$	$\mathbf{k}$	$\mathbf{e}$	$\tau\mathbf{k}$

Table 2. The basis-vector multiplication table defining a finite algebra with compressing multiplication operation

$\circ$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$	$\overrightarrow{k}$
$\overrightarrow{e}$	$\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{i}$	$\mu\mathbf{e}$
$\overrightarrow{i}$	$\tau\mathbf{e}$	$\tau\mathbf{i}$	$\tau\mathbf{i}$	$\tau\mathbf{e}$
$\overrightarrow{j}$	$\tau\mathbf{k}$	$\tau\mathbf{j}$	$\tau\mathbf{j}$	$\tau\mathbf{k}$
$\overrightarrow{k}$	$\mu\mathbf{k}$	$\mu\mathbf{j}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$

The paper is organized as follows: Sect. 2 describes the properties of the introduced FNR, Sect. 3 describes briefly properties of the introduced AFA, Sect. 4 presents a homomorphic map of the non-invertible vectors of the FNR for defining the discrete logarithm problem in hidden cyclic group, and Sect. 5 concludes the paper.

2 Properties of the Introduced Ring

Lemma 1. *Suppose* $\circ$ *and* $\star$ *are two arbitrary modifications of the vector multiplication operation, which correspond to different pairs of structural coefficients* (μ_1, τ_1) *and* $(\mu_2, \tau_2) \neq (\mu_1, \tau_1)$*. Then for arbitrary three vectors* A*,* B*, and* C *the following formula* $(A \circ B) \star C = A \circ (B \star C)$ *holds.*

Proof of this lemma consists in straightforward using the definition of the multiplication operation and Table 1.

To find the unit element of the considered ring one can solve the following vector equation:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}), \tag{1}$$

where $V = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})$ is an arbitrary vector and $X = (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k})$ is the unknown.

Equation (1) can be reduced to solving the following two systems of linear equations:

$$\begin{cases} (a + d\tau)x + (a\mu + d)z = a \\ (c + b\tau)x + (c\mu + b)z = c \end{cases} \tag{2}$$

and

$$\begin{cases} (b + c\mu)y + (b\tau + c)w = b \\ (a\mu + d)y + (a + d\tau)w = d. \end{cases} \tag{3}$$

Each of the systems has the same main determinant

$$\Delta = ab(1 - \mu\tau) + dc(\mu\tau - 1) = (\mu\tau - 1)(dc - ab)$$

and the same auxiliary determinants

$$\Delta_x = ab - cd; \Delta_z = \tau(cd - ab); \Delta_y = ab - cd; \Delta_w = \mu(cd - ab).$$

For the case $dc - ab \neq 0$ there exists the unique solution of each of the systems:

$$\begin{aligned} x = \frac{\Delta_x}{\Delta} = \frac{1}{1 - \mu\tau}; y = \frac{\Delta_y}{\Delta} = \frac{1}{1 - \mu\tau}; \\ z = \frac{\Delta_z}{\Delta} = \frac{\tau}{\mu\tau - 1}; w = \frac{\Delta_w}{\Delta} = \frac{\tau}{\mu\tau - 1}. \end{aligned} \tag{4}$$

The vector $E = (\frac{1}{1-\mu\tau}, \frac{1}{1-\mu\tau}, \frac{\tau}{\mu\tau-1}, \frac{\tau}{\mu\tau-1})$ has been computed as the right unit element of the ring.

Considering the vector equation

$$X \circ V = V \tag{5}$$

gives the same solution $X = E$ as the left unit element.

For the case $dc - ab = 0$ there exists p different solutions of each of the systems (2) and (3), which include the solution (4). Thus we have come to the following lemma:

Lemma 2. *The vector* $E = \left(\frac{1}{1-\mu\tau}, \frac{1}{1-\mu\tau}, \frac{\tau}{\mu\tau-1}, \frac{\mu}{\mu\tau-1}\right)$ *is the (global) unit element of the considered ring, i.e. for arbitrary vector* V *the following equations* $V \circ E = E \circ V = V$ *hold.*

The examination of the vector equation $V \circ X = E$ leads to the following

Lemma 3. *Vectors* $V = (a, b, c, d)$, *where* $ab \neq cd$, *are invertible.*

Calculating number of the vectors satisfying condition $ab \neq cd$ one can get

Lemma 4. *The order* Ω *of the multiplicative group of the considered ring is equal to* $\Omega = p(p-1)(p^2-1)$.

Examination of the vector Eqs. (1) and (5) for the case $ab = cd$ leads to the following two lemmas:

Lemma 5. *For an arbitrary vector* $N = (a, b, c, d)$ *such that* $ab = cd$ *and* $a\tau + c \neq 0$, *each of the vectors*

$$E_l = \left(x, \frac{c}{a\tau + c} - \frac{a + c\mu}{a\tau + c}z, z, \frac{a}{a\tau + c} - \frac{a + c\mu}{a\tau + c}x\right),$$

where $x, y \in GF(p)$ *acts as the left local unit element on all elements of the set* N^i, *where* i *is an arbitrary natural number, i.e., equalities* $E_l \circ N^i = N^i$ *hold true.*

Lemma 6. *For an arbitrary vector* $N = (a, b, c, d)$ *such that* $ab = cd$ *and* $a\mu + d \neq 0$, *each of the vectors*

$$E_r = \left(x, \frac{d}{a\mu + d} - \frac{a + d\tau}{a\mu + d}w, \frac{a}{a\mu + d} - \frac{a + d\tau}{a\mu + d}x, w\right),$$

where $x, w \in GF(p)$ *acts as the right local unit element on all elements of the set* N^i, *where* i *is a natural number, i.e., equalities* $N^i \circ E_r = N^i$ *hold true.*

The sets of left and right local unit elements contain invertible and non-invertible vectors (a', b', c', d').

It is of interest to consider subsets of non-invertible vectors. Imposing the condition $(a'b' = c'd')$ on the coordinates of the local unit elements leads to the following two formulas describing subsets of non-invertible local unit elements:

$$E_l^* = \left(x; \frac{c}{a\tau + c} - \frac{a + c\mu}{a\tau + c} \cdot \frac{c}{a}x; \frac{c}{a}x; \frac{a}{a\tau + c} - \frac{a + c\mu}{a\tau + c}x\right). \tag{6}$$

$$E_r^* = \left(x; \frac{d}{a\mu + d} - \frac{a + d\tau}{a\mu + d} \cdot \frac{d}{a}x; \frac{a}{a\mu + d} - \frac{a + d\tau}{a\mu + d}x; \frac{d}{a}x\right). \tag{7}$$

The elements included simultaneously in the sets (6) and (7) represent bi-side local unit elements of the vector (a, b, c, d). From condition $E_l^* = E_r^*$ one has four equations with the unknown value x which are satisfied simultaneously at some unique value $x = x_0$:

Lemma 7. *The local bi-side unit element E' is described with the following formula* $E' = \left(x_0, \frac{d}{a\mu+d} - \frac{a+d\tau}{a\mu+d} \cdot \frac{d}{a}x_0, \frac{d}{a\mu+d} - \frac{a+d\tau}{a\mu+d}x_0, \frac{d}{a}x_0\right)$, *where* $x_0 = \frac{a^2}{ca\mu+cd+a^2+ad\tau} = \frac{a}{c\mu+b+a+d\tau}$.

Proof of this statement is performed substituting the value x_0 in the formulas describing all possible values E_l^* and E_r^*.

It is evident that

$$(E' \circ N = N \circ E' = N) \Rightarrow \left(E' \circ N^i = N^i \circ E' = N^i\right)$$

for all integers i. Let us consider the sequence $N, N^2, ..., N^i$ (for $i = 1, 2, 3, ...$). If the vector N is not a zero-divisor relatively some its power (formulas describing zero-divisors are presented below), then for some two integers h and $k > h$ we have $N^k = N^h$ and $N^k = N^{k-h} \circ N^h = N^h \circ N^{k-h} = N^{k-h} \circ N^h$. Thus, we have the following:

Lemma 8. *Suppose $N = (a, b, c, d)$ be a non-invertible vector, i.e. $ab = cd$, such that there exists no integer k for which the condition $N^k = (0, 0, 0, 0)$ holds true. Then the sequence $N, N^2, ..., N^i, ...$, where $i = 1, 2, ...$, is periodic and for some integer ω we have $N^\omega = E'$, where E' is the local unit element such that $N \circ E' = E' \circ N = N$.*

If for some integer ω (that can be called order of the non-invertible vector N) $N^\omega = E'$ holds true, then the bi-side local unit element corresponding to the vector N can be computed as a power of N.

The following computational example illustrates this fact:

for $p = 241740125706839$ and $\mu = 1$; $\tau = 1$

$$N = (a, b, c, d) = (235252752952, 124252511124, 855846652525, 52660042235214). \tag{8}$$

Computation of the value E' as $E' = N^{p^2-1}$ and with using formula from Lemma 7 gives the same result:

$$E' = (152632284483677, 212707439691227, 72220177461588, 45920349777187). \tag{9}$$

Product of some two non-invertible vectors can be equal to zero $(0, 0, 0, 0)$ of the ring. Such vectors are called zero-divisors. For some non-invertible vector $N = (a, b, c, d)$ there exit sets of the left and right zero-divisors D such that the following equalities hold: $N \circ D = (0, 0, 0, 0)$ and $D \circ N = (0, 0, 0, 0)$.

For the first case, finding vectors D is connected with solving the systems of two linear Eqs. (2) and (3) with the right part equal to zero of the field $GF(p)$.

Considering such modified systems of equations it is sufficiently easy to derive the following formula describing the set of the right zero-divisors

$$D_r = \left(x; y; -\frac{a+d\tau}{a\mu+d}x; -\frac{a\mu+d}{a+d\tau}y\right), \tag{10}$$

where x and y take on all values in the field $GF(p)$. Thus, for arbitrary given non-invertible vector such that $a\mu+d \neq 0$ and $a+d\tau \neq 0$ there exist p^2 different zero-divisors including the trivial one $(0,0,0,0)$. The analogous consideration of the left zero-divisors leads to the following formula

$$D_l = \left(x; y; -\frac{a\tau+c}{a+c\mu}y; -\frac{a+c\mu}{a\tau+c}x\right). \tag{11}$$

It is easy to see that sets of the right and left divisors include only non-invertible vectors. Let us find intersection of these two sets. The intersection corresponds to the pairs of the values (x, y) at which we have the following two equalities:

$$-\frac{a+d\tau}{a\mu+d}x = -\frac{a\tau+c}{a+c\mu}y; -\frac{a\mu+d}{a+d\tau}y = -\frac{a+c\mu}{a\tau+c}x.$$

Each of the following two equations gives the following:

$$\begin{aligned} &(a\mu+d)(a\tau+c)x = (a+c\mu)(a+d\tau)y \Rightarrow \\ &a^2(\mu\tau-1)x = cd(\mu\tau-1)y \Rightarrow y = \frac{a^2}{cd}x = \frac{a}{b}x. \end{aligned} \tag{12}$$

Thus, for the case $\mu\tau - 1 \neq 1$ and $cd \neq 0$ all bi-side zero-divisors of the vector N are described with the formula

$$D' = \left(x; \frac{a}{b}x; -\frac{a\tau+c}{a+c\mu}\cdot\frac{a}{b}x; -\frac{a+c\mu}{a\tau+c}x\right), \tag{13}$$

where x is an arbitrary element of the field $GF(p)$.

It is of interest to get formula describing square roots from zero of the ring, i.e., solutions of the vector equation

$$D \circ D = (0,0,0,0). \tag{14}$$

In the case $ab = cd$ the last equation defines the following system of linear equations:

$$\begin{cases} a(a+b+c\mu+d\tau) = 0 \\ b(a+b+c\mu+d\tau) = 0 \\ c(a+b+c\mu+d\tau) = 0 \\ d(a+b+c\mu+d\tau) = 0, \end{cases} \tag{15}$$

where $D = (a, b, c, d)$ is the unknown. From system (15) we have the following:

Lemma 9. *Square roots from the vector* $(0, 0, 0, 0)$ *are non-invertible vectors* $N = (a, b, c, d)$*, the coordinates of which satisfy the condition* $a+b+\mu c+\tau d = 0$.

Comparing Lemmas 7 and 9 one can see that for the non-invertible vectors that are square roots from the zero vector there exist no local bi-side unity elements. Taking into account this relation one can put forward the following hypothesis:

Lemma 10. *If the coordinates of the non-invertible vectors* $N = (a, b, c, d)$ *satisfy the condition* $a + b + \mu c + \tau d \neq 0$*, then the bi-side local unity element can be computed as* $E' = N^{\omega}$ *at some integer* ω.

Lemmas 5 to 8 show that the set of non-invertible vectors includes different cyclic groups with different bi-side local unit elements.

3 Finite Non-commutative Associative Algebra with Compressing Multiplication Operation

Lemma 11. *Lemma 1 is valid for the AFA defined over the field* $GF(p)$ *with Table 2 as the BVMT.*

Lemma 12. *Result of multiplying two arbitrary non-zero elements of the AFA represents a vector* (a, b, c, d) *satisfying condition* $ac = bd$.

Proof of this lemma includes straightforward using the definition of the multiplication operation and Table 2. Naturally, squaring maps set of $p^2 - 1$ non-zero elements of the AFA into the subset of the four-dimension vectors (a, b, c, d) such that $ac = bd$ number of which is equal to $p^3 + p^2 - p$. Thus, on the average there exists approximately p different square roots from some element of the last subset.

Lemma 13. *The local right-side unit elements exist for vectors* (a, b, c, d) *such that* $ac = bd$, $\mu a + \tau b \neq 0$, $\mu d + \tau c \neq 0$ *and the set of the right-side units of the non-zero vector* (a, b, c, d) *is described with the following formula*

$$E_r = \left(x, y, \frac{b}{\mu a + \tau b} - y, \frac{a}{\mu a + \tau b} - x \right),$$

where $x, y \in GF(p)$.

Lemma 14. *The local left-side unit elements exist for vectors* (a, b, c, d) *such that* $ac = bd$, $a + d \neq 0$, $b + c \neq 0$ *and the set of the left-side units of some non-zero vector* (a, b, c, d) *is described with the following formula*

$$E_l = \left(x, \frac{a}{\tau(a + d)} - \frac{\mu}{\tau} x, z, \frac{d}{\tau(a + d)} - \frac{\tau}{\mu} z \right),$$

where $x, z \in GF(p)$.

Lemma 15. *The local bi-side unit elements of the non-zero vector* (a, b, c, d) *such that* $ac = bd$, $\mu a + \tau b \neq 0$, $\mu d + \tau c \neq 0$, $a + d \neq 0$, *and* $b + c \neq 0$ *is described with the following formula*

$$E' = \left(x, \frac{a}{\tau(a+d)} - \frac{\mu}{\tau}x, \frac{b}{\mu a + \tau b} - \frac{a}{\tau(a+d)} + \frac{\mu}{\tau}x, \frac{a}{\tau(a+d)} - x \right),$$

where $x \in GF(p)$.

Lemma 16. *For some non-zero vector* (a, b, c, d) *such that* $ac = bd$, $\mu a + \tau b \neq 0$, $\mu d + \tau c \neq 0$, $a + d \neq 0$, *and* $b + c \neq 0$ *there exists exactly one local bi-side unit element* $E' = (a', b', c', d')$ *such that* $a'c' = b'd'$. *The local bi-side unit* E' *can be computed using formula from Lemma 15 and substituting the value* $x = x_0$, *where*

$$x_0 = \frac{a^2}{(a+d)(\mu a + \tau b)}.$$

In the considered AFA the left, the right, and bi-side zero-divisors are global, i.e. they acts on each element of the AFA. The following three lemmas describes the sets of the mentioned three types of the zero-divisors.

Lemma 17. *The set of the right-side zero-divisors is described with the following formula*

$$D_r = (x, y, -y, -x),$$

where $x, y \in GF(p)$.

Lemma 18. *The set of the left-side zero-divisors is described with the following formula*

$$D_l = \left(x, -\frac{\mu}{\tau}x, z, -\frac{\tau}{\mu}z \right),$$

where $x, z \in GF(p)$.

Lemma 19. *The set of the bi-side zero-divisors is described with the following formula*

$$D' = \left(x, -\frac{\mu}{\tau}x, \frac{\mu}{\tau}x, -x \right),$$

where $x \in GF(p)$.

Lemma 20. *Suppose the non-zero vector* $V = (a, b, c, d)$ *and local bi-side unit* $E' = (a', b', c', d')$ *corresponding to* (a, b, c, d) *are such that* $ac = bd$, $\mu a + \tau b \neq 0$, $\mu d + \tau c \neq 0$, $a + d \neq 0$, $b + c \neq 0$, *and* $a'c' = b'd'$. *Then the local bi-side unit* E' *can be computed as* $E' = V^{\omega}$ *at some integer* ω.

Lemma 15 shows that the considered AFA includes different subsets of four-dimension vectors that represent cyclic groups the units of which are different in general case.

4 Discussion of the Potential Application

Designing different BVMTs for defining the multiplication operation in finite four-dimension vector space one can get different types of AFA, for example, finite rings, non-commutative [12] and commutative ones [15]. As a particular case of the lasts it is possible to define finite fields [15].

In accordance with the well-known Representation Theorem an m-dimension AFA over $GF(p)$ is isomorphic to an subalgebra of the $m \times m$ matrix algebra over $GF(p)$ (see, for example [16]).

In the case $m = 4$ one has the following illustration. For arbitrary given four-dimension AFA multiplication of all elements of the four-dimension vector space over $GF(p)$ by some fixed four-dimension vector V defines a map $\varphi_V(X) : X \to \varphi_V(X)$ of the vector space into itself (in particular cases, when the fixed vector is an invertible element of the AFA, such map represents linear transformation of the vector space). Indeed, from the definition of the multiplication operation in the AFA one can see that the result of multiplication of the vector X by V represents multiplication of the vector X by some 4×4 matrix M_V elements of which are defined by coordinates of the vector V and by the BVMT. Thus, it can be written the following:

$$\varphi_V(X) = X \circ V = X * M_V,$$

where $M_V = f(V)$ and $*$ denotes the matrix multiplication. Considering maps defined by two different vectors V_1 and V_2 we have

$$\varphi_{V_2}(\varphi_{V_1}(X)) = X \circ V_1 \circ V_2 = X \circ (V_1 \circ V_2) = \varphi_{V_1 \circ V_2}(X).$$

Considering the same two maps defined by the matrices $M_{V_1} = f(V_1)$ and $M_{V_2} = f(V_2)$ we get

$$\varphi_{M_{V_2}}\left(\varphi_{M_{V_1}}(X)\right) = X * M_{V_1} * M_{V_2} = X * (M_{V_1} * M_{V_2}) =$$
$$\varphi_{M_{V_1} * M_{V_2}}(X) = \varphi_{V_1 \circ V_2}(X) = \varphi_{f(V_1 \circ V_2)}(X).$$

Thus, we have

$$f(V_1 \circ V_2) = f(V_1) * f(V_2).$$

In analogous way it is easy to show the following

$$f(V_1 + V_2) = f(V_1) + f(V_2).$$

The last two formulas show that between any four-dimension AFA over $GF(p)$ and some subset of the 4×4 matrices there exists isomorphism, i.e. the results described in Sects. 2 and 3 relates to some subsets of the 4×4 matrices over $GF(p)$.

A characteristic feature of the ring considered in Sect. 2 and of the AFA considered in Sect. 3 is mutual associativity of different modifications of the parameterized multiplication operation. Such property is of interest for applications concerning the design of the cryptoschemes using the key-dependent operations.

It is also interesting to consider potential cryptographic applications concerning the definition of the hidden conjugacy search problem (it can be called alternatively the discrete logarithm problem in a hidden cyclic subgroup) over subset of the non-invertible vectors.

Suppose N be some non-invertible vector in the considered FNR (or element in the considered AFA) such that for some prime number q we have $N^q = E'$. Using the local unit element E' one can define the following homomorphism φ_t over set of non-invertible vectors $V_{E'}$, where $V_{E'} = V \circ E'$ and V takes on all values in the considered ring of the four-dimension vectors.

Like standard automorphisms ψ_W of the finite non-commutative ring described by the formula $\psi_W(V) = W^{-1} \circ V \circ W$, where W is an invertible element of the ring, the homomorphism φ_t is defined as follows:

$$\varphi_t\left(V_{E'}\right) = N^{q-t} \circ V_{E'} \circ N^t. \tag{16}$$

Actually, the last formula defines homomorphism since with evidence the following holds true:

$$\begin{aligned} &\varphi_t\left(V'_{E'} \circ V''_{E'}\right) = \\ &\varphi_t\left(V'_{E'}\right) \circ \varphi_t\left(V''_{E'}\right), \end{aligned} \tag{17}$$

$$\begin{aligned} &\varphi_t\left(V'_{E'} + V''_{E'}\right) = \\ &\varphi_t\left(V'_{E'}\right) + \varphi_t\left(V''_{E'}\right). \end{aligned} \tag{18}$$

To define public-key cryptoschemes, like that described in [11], one can select some invertible vector G having sufficiently large prime order g, which satisfies the condition $G \circ N \neq N \circ G$, and use the formula $Y = N^{q-t} \circ (G \circ E')^x \circ N^t$, where Y is public key and the pair of numbers (t, x) is private key (the integers $t < q$ and $x < g$ are to be selected at random).

5 Conclusion

In this paper, two new BVMTs have been introduced to define the parameterized non-commutative multiplication operation in finite space of four-dimension vectors defined over the field $GF(p)$.

The BVMTs are characterized that each of them defines mutual associativity of all possible modifications of the multiplication of the vectors. The first BVMT defines an AFA that represents a FNR. Formula for the order of the multiplicative group of the considered finite non-commutative ring of the four-dimension vectors has been got and some properties of the subset of the non-invertible vectors have been investigated.

The second BVMT defines an AFA with multiplication operation possessing compression property. The AFA contains no global unit, it contains many different subsets in frame of which local bi-side unit exists.

Using formula (16) and selecting different values t and different non-invertible vectors N it is possible to define a variety of homomorphic maps.

Like in papers [12,13], one can construct public-key crypto-schemes using the homomorphisms in the considered finite ring of four dimension vectors.

Future research in frame of the concerned topic is related with proving Statement 10, finding new BVMT defining other types of finite algebras of four-dimension vectors, consideration of the case of defining finite non-commutative algebras of the vectors having dimension $m > 4$.

References

1. Sirwan, A., Majeed, N.: New algorithm for wireless network communication security. Int. J. Cryptogr. Inf. Secur. **6**(3/4), 1–8 (2016)
2. Feng, Y., Yang, G., Liu, J.K.: A new public remote integrity checking scheme with user and data privacy. Int. J. Appl. Cryptogr. **3**(3), 196–209 (2017)
3. Chiou, S.Y.: Novel digital signature schemes based on factoring and discrete logarithms. Int. J. Secur. Appl. **10**(3), 295–310 (2016)
4. Poulakis, D.: A variant of digital signature algorithm. Des. Codes Cryptogr. **51**(1), 99–104 (2009)
5. Yan, S.Y.: Quantum Computational Number Theory, 1st edn. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25823-2
6. Yan, S.Y.: Quantum Attacks on Public-Key Cryptosystems, 1st edn. Springer, Boston (2013). https://doi.org/10.1007/978-1-4419-7722-9
7. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)
8. Smolin, J.A., Smith, G., Vargo, A.: Oversimplifying quantum factoring. Nature **499**(7457), 163–165 (2013)
9. Federal Register: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. The Daily journal of the United States Government. https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf. Accessed 6 June 2018
10. Takagi, T. (ed.): PQCrypto 2016. LNCS, vol. 9606. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29360-8
11. Sakalauskas, E., Tvarijonas, P., Raulynaitis, A.: Key Agreement Protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. Informatica **18**(1), 115–124 (2007)
12. Moldovyan, D.N.: Non-commutative finite groups as primitive of public-key cryptoschemes. Quasigroups Relat. Syst. **18**(2), 165–176 (2010)
13. Moldovyan, D.N., Moldovyan, N.A.: Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. Quasigroups Relat. Syst. **18**(2), 177–186 (2010)
14. Kuz'min, A.S., Markov, V.T., Mikhalev, A.A., Mikhalev, A.V., Nechaev, A.A.: Cryptographical algorithms on groups and algebras. J. Math. Sci. **223**(5), 629–641 (2017)
15. Moldovyan, N.A., Moldovyanu, P.A.: Vector form of the finite fields $GF(p^m)$. Bul. Acad. Ştiinţe Repub. Mold. Mat. **3**(61), 1–7 (2009)
16. Ronyai, L.: Computing the structure of finite algebras. J. Symb. Comput. **9**, 355–373 (1990)