Filomat 40:1 (2026), 23–40
https://doi.org/10.2298/FIL2601023N

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Chains of time-dependent 3D matrices and applications to encryption systems

Bobomurad A. Narkuziev[a], M. Victoria Velasco[b,*]

[a] *Kimyo International University in Tashkent, Department of Exact Sciences, Shota Rustaveli street, 156, 100121 Tashkent, Uzbekistan*
[b] *Departamento de Análisis Matemático, Facultad de Ciencias, Universidad de Granada, 18071 Granada, Spain*

Abstract. This paper deals with chains of time-dependent 3D matrices and their applications. We introduce the 3D rotation-chain $2 \times 2 \times 2$ and describe the properties of each 3D matrix in this chain after identifying it with the non-associative algebra that it defines. To this end, we characterize when the algebra associated with a 3D matrix of dimension $2 \times 2 \times 2$ is associative, commutative, has a unit (or a one-sided unit), or is a division algebra, respectively. Based on the properties of the 3D rotation-chain $2 \times 2 \times 2$ we develop algorithms for encryption and decryption processes .

1. Introduction

The aim of this paper is to study chains of time-dependent 3D matrices with applications in encryption systems. Examples of such chains, centered on 3D rotation matrices of dimension $2\times2\times2$, are provided and used to illustrate a robust method for developing time-dependent encryption and decryption algorithms. Consequently, this approach, after some minor adaptations, can be applied to time-based encryption processes, such as the creation of temporary encryption keys, temporary access tokens, and programmed encryption systems, among others [1, 18, 33].

Three-dimensional matrices, commonly referred to as **3D matrices**, are mathematical structures that extend the concept of two-dimensional matrices (which have rows and columns) to three dimensions. Therefore, a 3D matrix consists of elements arranged in a three-dimensional grid, where each element is identifiable using three indices. The dimension of a 3D matrix is typically described as $m \times n \times p$, where m represents the number of rows (height), n the number of columns (width) and p the number of layers (depth).

In Cryptography, 3D matrices are employed for complex data transformations, adding layers of complexity to enhance the security of ciphers [23, 28]. Furthermore, 3D matrices are widely recognized as

2020 *Mathematics Subject Classification*. Primary 68P25; Secondary 16-04, 15A24.
Keywords. Time dependent 3D matrix, cubic matrix, Chapman-Kolmogorov equation.
Received: 26 May 2025; Accepted: 31 October 2025
Communicated by Dragan S. Djordjević
Research supported by the Agency for Innovative Development under the Ministry of Higher Education, Science, and Innovations of the Republic of Uzbekistan and Junta de Andalucía grant FQM-199, and the Spanish Ministry of Science and Innovation (MINECO/MICINN/FEDER), through the IMAG-Maria de Maeztu Excellence Grant CEX2020-001105M/AEI/10.13039/ .
* Corresponding author: M. Victoria Velasco
Email addresses: b.narkuziev@kiut.uz (Bobomurad A. Narkuziev), vvelasco@ugr.es (M. Victoria Velasco)
ORCID iDs: https://orcid.org/0000-0002-9203-7999 (Bobomurad A. Narkuziev),
https://orcid.org/0000-0003-4957-3275 (M. Victoria Velasco)

essential tools in several scientific fields [29] including Physics (for tensor calculus and space simulations [24]), Computer Graphics (for manipulating 3D models through operations such as translation, rotation, and scaling [11]), and Data Science (especially in Machine Learning for managing multi-dimensional data sets [9]). In Virtual Reality and Augmented Reality, 3D matrices are crucial for creating and managing 3D environments [6]. In Computer Vision, they are utilized for tasks such as object recognition, 3D reconstruction, and motion tracking [35]. This usage facilitates the understanding and interpretation of the structure of a 3D environment from 2D images [10]. In Medical Imaging, 3D matrices help reconstruct 3D models from 2D slices [31], while in Meteorology and geophysics they enable visualization of complex 3D phenomena [32]. The focus here is on **cubic matrices** (i.e., 3D matrices with dimension $n \times n \times n$). This preference arises from the fact that such matrices can be considered as n-dimensional algebras (not necessarily associative), allowing the use of algebraic tools to enhance our model. This aspect is crucial in the algorithms we develop here, particularly where the multiplication of two elements is involved. It is also worth noting that an asymmetric 3D matrix of dimension $m \times n \times p$ can be treated as a cubic matrix of dimension $s := \max\{m, n, p\}$ by filling the unoccupied spaces in the $s \times s \times s$ block with zeros.

We will pay special attention to 3D **rotation matrices,** as already mentioned. Rotation matrices are useful in various fields of science [7], including Computer graphics [2], Neural Networks [36] and Transformers [30], and of course in Cryptography [14]. Indeed, in data security, a basic idea is to represent data in matrix form and then apply various mathematical operations to encrypt or decrypt the data. Thus, the concept of rotating (or shifting) data elements is a common encryption technique. Moreover, the strength of a cryptographic algorithm often depends on the complexity of solving certain matrix problems [8], which is further increased by introducing time dependence, as we do here. In summary, although 3D matrices and rotation matrices are more commonly associated with Computer Graphics, they also play a significant role in the field of Cryptography.

The paper is structured as follows: Section 2 focuses on characterizing the algebraic properties of the two-dimensional algebra determined by a 3D matrix of dimension $2 \times 2 \times 2$. In this context, we explore properties including associativity, commutativity, the existence of a unit and one-sided units, as well as the criteria for being a division algebra. These characterizations are exclusively dependent on the 3D matrix that defines the multiplication of the given algebra.

In Section 3, we introduce the notion of a time-dependent chain of 3D matrices (Definition 3.1), and show an illustrative example called the 3D rotation-chain $2 \times 2 \times 2$ (Definition 3.3). After describing all the algebras associated with the cubic matrices of this particular time-dependent chain of 3D matrices, we classify them and present their algebraic properties based on the results of Section 2. Finally, we outline double-key and triple-key encryption and decryption algorithms, making use of the algebraic properties previously discussed.

2. Algebras associated to a 3D matrix of dimension $n \times n \times n$

Throughout this paper, $\mathbb{K}$ denotes either the field of real numbers, $\mathbb{R}$, or the field of complex numbers, $\mathbb{C}$. Formally, a **3D matrix** of dimension $n \times m \times p$ is a collection of elements $\omega_{ijk} \in \mathbb{K}$ where $i = 1, 2, ..., n$, $j = 1, 2, ..., m$, and $k = 1, 2, ..., p$. Therefore, each element in the matrix is identified by its three indices, i, j and k, which correspond to the matrix's three dimensions. In this context: n denotes the number of rows in each 2D matrix slice along the first dimension, m represents the number of columns in each 2D matrix slice along the second dimension, and p denotes the number of these 2D matrix slices arranged along the third dimension. Thus, a 3D matrix, M, of dimension $n \times m \times p$ is uniquely determined by p 2D matrices, $M_1, ..., M_p$, each of dimension $n \times m$, that is $M_k := (\omega_{ijk})_{ij}$ where $i = 1, 2, ..., n$, and $j = 1, 2, ..., m$, and we write $M = (M_1|...|M_p)$.

The set of all 3D matrices of dimension $n \times m \times p$ is a linear space equipped with the standard operations of addition and scalar multiplication. Thus, if $A = (a_{ijk})$, $B = (b_{ijk})$, and if $\lambda \in \mathbb{K}$, then $A + B := (a_{ijk} + b_{ijk})$ and $\lambda A := (\lambda a_{ijk})$.

From now on we will deal with 3D matrix of dimension $n \times n \times n$ and we assign a name to them.

Definition 2.1. *A **cubic matrix** of dimension n is 3D matrix of dimension $n \times n \times n$ with entries in $\mathbb{K}$. The set of all n-dimensional cubic matrices is denoted by $\mathfrak{C}_n$.*

The reason we focus on the class $\mathfrak{C}_n$ is due to the fact that, when considering an n-dimensional linear space $\mathcal{A}$ with a predetermined basis $B = \{e_1, ..., e_n\}$, each 3D matrix $M \in \mathfrak{C}_n$ determines a multiplication in $\mathcal{A}$ that endows $\mathcal{A}$ with an algebra structure (not necessarily associative). This fact significantly enriches our study.

We recall that a **multiplication** on a linear space $\mathcal{A}$ is a bilinear map $(a, b) \to ab$, from $\mathcal{A} \times \mathcal{A}$ to $\mathcal{A}$. It's important to note that the the algebra $\mathcal{A}$ does not need to be associative as the associative property of the product is not required (only bilinearity is assumed).

In relation to the basis $B = \{e_1, ..., e_n\}$, a multiplication in $\mathcal{A}$ is defined by the structure constants ω_{ijk} given by the equalities

$$e_i e_j = \sum_{k=1}^{n} \omega_{ijk} e_k. \tag{1}$$

The bilinear map $\pi_k : \mathcal{A} \times \mathcal{A} \to \mathbb{K}$ determined the equalities by $\pi_k(e_i, e_j) = \omega_{ijk}$, for every $i, j = 1, ..., n$, is the projection of the product of $\mathcal{A}$ over the subspace generated by e_k, for every $k = 1, ..., n$. The matrix associated to π_k with respect to the basis B is

$$M_k = \begin{pmatrix} \omega_{11k} & \cdots & \omega_{1nk} \\ \vdots & \ddots & \vdots \\ \omega_{n1k} & \cdots & \omega_{nnk} \end{pmatrix}$$

Thus, the multiplication $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ given by (1) can be identified with the cubic matrix $M = (M_1|\cdots|M_n)$ where $M_k = (\pi_k(e_i, e_j))_{i,j=1,\cdots,n}$ with $k = 1, \cdots, n$.

Conversely, every cubic matrix $M = (M_1|...|M_n)$ where $M_k = (\omega_{ijk})_{i,j=1...n}$, for $k = 1, \cdots, n$, defines a multiplication in $\mathcal{A}$ given by the equalities $e_i e_j := \sum_{k=1}^{n} \omega_{ijk} e_k$.

We conclude in this way that, fixed an n-dimensional linear space $\mathcal{A}$ and a basis $B = \{e_1, ..., e_n\}$, every multiplication in $\mathcal{A}$ is one to one determined a matrix in $\mathfrak{C}_n$, and vice versa.

In this paper, we focus on matrices in $\mathfrak{C}_2$. The main goal of this section is to characterize the properties of a 2-dimensional algebra based on the cubic matrix that defines its multiplication, relative to a predetermined basis. We address the next subsection to this purpose.

2.1. 3D matrices of dimension $2 \times 2 \times 2$ and their associated algebras

From now on, a matrix $M \in \mathfrak{C}_2$ given by

$$M = \left(\begin{array}{cc|cc} \omega_{111} & \omega_{121} & \omega_{112} & \omega_{122} \\ \omega_{211} & \omega_{221} & \omega_{212} & \omega_{222} \end{array}\right) \in \mathfrak{C}_2$$

will also be denoted by $M = (M_1|M_2)$ where

$$M_1 := \begin{pmatrix} \omega_{111} & \omega_{121} \\ \omega_{211} & \omega_{221} \end{pmatrix} \text{ and } M_2 := \begin{pmatrix} \omega_{112} & \omega_{122} \\ \omega_{212} & \omega_{222} \end{pmatrix}. \tag{2}$$

In what follows, consider a fixed 2-dimensional vector space $\mathcal{A}$ over $\mathbb{K}$ and a basis $B = \{e_1, e_2\}$. Then, as already mentioned, every cubic matrix in $\mathfrak{C}_2$ define a multiplication in $\mathcal{A}$. More precisely, if $a = \alpha_1 e_1 + \alpha_2 e_2$ and $b = \beta_1 e_1 + \beta_2 e_2$, then $ab = \gamma_1 e_1 + \gamma_2 e_2$ where γ_1 and γ_2 are determined by

$$\begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} \omega_{111} & \omega_{121} \\ \omega_{211} & \omega_{221} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \gamma_1,$$

$$\begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} \omega_{112} & \omega_{122} \\ \omega_{212} & \omega_{222} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \gamma_2.$$

In this way, $\mathcal{A}$ becomes an algebra that we denote by $\mathcal{A}_M$ in order to refer to the cubic matrix that determines its product.

We recall $\mathcal{A}_M$ has a **left unit** (respectively, a **right unit**) if there exists $u \in \mathcal{A}_M$ such that $ua = a$, (respectively, $au = a$), for every $a \in \mathcal{A}_M$.

We say that $u \in \mathcal{A}_M$ is a **unit** for $\mathcal{A}_M$ if u is both, a left and a right unit.

If u_1 is a left unit of $\mathcal{A}_M$ and if u_2 is a right unit of $\mathcal{A}_M$, then $u_2 = u_1u_2 = u_1$, and therefore, this element is a unit for $\mathcal{A}_M$. This also proves that, if it exists, the unit of $\mathcal{A}_M$ must be unique.

Remark 2.2. *Let $\mathcal{A}_M$ be the algebra associated to the matrix $M = (M_1|M_2)$ given in (2), with respect to the basis $B = \{e_1, e_2\}$. Then $\mathcal{A}_M$ is commutative if and only if $M_1 = M_1^T$ and $M_2 = M_2^T$.*

Theorem 2.3. *Let $\mathcal{A}_M$ be the algebra associated to the matrix $M = (M_1|M_2)$, given in (2), with respect to the basis $B = \{e_1, e_2\}$. Then, $\mathcal{A}_M$ is associative if and only if the following equalities are satisfied, for $i, j = 1, 2$,*

$$\begin{pmatrix} \omega_{1i1} & \omega_{1i2} \\ \omega_{2i1} & \omega_{2i2} \end{pmatrix} M_j = M_j \begin{pmatrix} \omega_{i11} & \omega_{i21} \\ \omega_{i12} & \omega_{i22} \end{pmatrix}. \tag{3}$$

Proof. The algebra $\mathcal{A}_M$ is associative, if and only if $(e_ie_j)e_k = e_i(e_je_k)$ for every $i, j, k = 1, 2$, which means that the following equalities are satisfied for $i = 1, 2$.

$$\begin{aligned} (e_1e_i)e_1 &= e_1(e_ie_1), \qquad (e_1e_i)e_2 = e_1(e_ie_2) \\ (e_2e_i)e_1 &= e_2(e_ie_1), \qquad (e_2e_i)e_2 = e_2(e_ie_2), \end{aligned} \tag{4}$$

Setting

$$a_i =: \begin{pmatrix} \omega_{1i1} & \omega_{1i2} \end{pmatrix}, b_i =: \begin{pmatrix} \omega_{2i1} & \omega_{2i2} \end{pmatrix}, c_i := \begin{pmatrix} \omega_{i11} & \omega_{i12} \end{pmatrix}^T, d_i := \begin{pmatrix} \omega_{i21} & \omega_{i22} \end{pmatrix}^T,$$

and $v_1^T = \begin{pmatrix} 1 & 0 \end{pmatrix}$, $v_2^T = \begin{pmatrix} 0 & 1 \end{pmatrix}$, the equalities (4) can be written as

$$a_iM_jv_1 = v_1^TM_jc_i; \;\; a_iM_jv_2 = v_1^TM_jd_i; \;\; b_iM_jv_1 = v_2^TM_jc_i; \;\; b_iM_jv_2 = v_2^TM_jd_i.$$

for $j = 1, 2$. Consequently,

$$\begin{aligned} & \begin{pmatrix} \omega_{1i1} & \omega_{1i2} \\ \omega_{2i1} & \omega_{2i2} \end{pmatrix} M_j \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \\ = & \begin{pmatrix} a_iM_jv_1 & a_iM_jv_2 \\ b_iM_jv_1 & b_iM_jv_2 \end{pmatrix} = \begin{pmatrix} v_1^TM_jc_i & v_1^TM_jd_i \\ v_2^TM_jc_i & v_2^TM_jd_i \end{pmatrix} = \\ = & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} M_j \begin{pmatrix} \omega_{i11} & \omega_{i21} \\ \omega_{i12} & \omega_{i22} \end{pmatrix}, \end{aligned}$$

which proves the result. □

Corollary 2.4. *Let $\mathcal{A}_M$ be the algebra associated with the matrix $M = (M_1|M_2)$. Then, $\mathcal{A}_M$ is an associative and commutative algebra if and only if M is given by*

$$M = \left(\begin{array}{cc|cc} a & b & \alpha & \beta \\ b & c & \beta & \gamma \end{array}\right),$$

where $a, b, c, \alpha, \beta, \gamma \in \mathbb{K}$ and the following conditions are satisfied

$$\alpha c = b\beta; \quad \det M_1 = \beta c - \gamma b, \quad \det M_2 = \alpha b - a\beta. \tag{5}$$

Proof. By Theorem 2.2, the commutativity of $\mathcal{A}_M$ means that the matrices M_1 and M_2 are symmetric. Moreover, the equalities in (5) follow directly from equation (3) in Theorem 2.3. □

Our next goal is to characterize the existence of a unit in $\mathcal{A}_M$. To this end, we study first the existence of left and right units.

Theorem 2.5. *Let $\mathcal{A}_M$ be the algebra associated to the matrix $M = (M_1|M_2)$ given in (2), with respect to the basis $B = \{e_1, e_2\}$. Set*

$$v_1^T := \begin{pmatrix} 1 & 0 \end{pmatrix},\ v_2^T := \begin{pmatrix} 0 & 1 \end{pmatrix} \text{ and } u^T := \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T.$$

(i) *If $\det M_1 \neq 0$, then $\mathcal{A}_M$ has a left unit $u = u_1e_1 + u_2e_2$ if and only if $M_2^T(M_1^T)^{-1}v_1 = v_2$, in which case $u^T = (M_1^{-1})^T v_1$.*

(ii) *If $\det M_2 \neq 0$, then $\mathcal{A}_M$ has a left unit $u = u_1e_1 + u_2e_2$ if and only if $M_1^T(M_2^T)^{-1}v_2 = v_1$, in which case $u^T = (M_2^T)^{-1}v_2$.*

(iii) *If $\det M_1 = \det M_2 = 0$, then $\mathcal{A}_M$ has a left unit if and only if either assertion* (a) *or* (b) *is satisfied where:*

(a) $M = \left(\begin{array}{cc|cc} \omega_{111} & 0 & 0 & \omega_{122} \\ \omega_{211} & 0 & 0 & \omega_{222} \end{array}\right)$ *with* $\widetilde{M} = \begin{pmatrix} \omega_{111} & \omega_{122} \\ \omega_{211} & \omega_{222} \end{pmatrix}^T$ *saisfying that* $\det \widetilde{M} \neq 0$. *In this case, $u = u_1e_1 + u_2e_2$ with $u^T = \widetilde{M}^{-1}(v_1 + v_2)$ is the unique left unit of $\mathcal{A}_M$.*

(b) $M = \left(\begin{array}{cc|cc} a & 0 & 0 & a \\ b & 0 & 0 & b \end{array}\right)$ *with $a^2 + b^2 \neq 0$. Then, every $u = u_1e_1 + u_2e_2$ satisfying that $au_1 + bu_2 = 1$ is a left unit for $\mathcal{A}_M$.*

Proof. Suppose that $u = u_1e_1 + u_2e_2$ is a left unit of $\mathcal{A}_M$ with respect to the matrix $M = (M_1|M_2) \in \mathfrak{C}_2$. Then $ue_i = e_i$ for $i = 1, 2$. This means that

$$u^T M_1 v_1 = 1; \quad u^T M_2 v_1 = 0; \quad u^T M_1 v_2 = 0; \quad u^T M_2 v_2 = 1. \tag{6}$$

Therefore, it follows that

$$\begin{pmatrix} \omega_{111} & \omega_{121} \\ \omega_{211} & \omega_{221} \end{pmatrix}^T \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad \begin{pmatrix} \omega_{112} & \omega_{122} \\ \omega_{212} & \omega_{222} \end{pmatrix}^T \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{7}$$

Consequently:
(i) If $\det M_1 \neq 0$, then $\mathcal{A}_M$ has a left unit if and only if $M_2^T(M_1^T)^{-1}v_1 = v_2$.
(ii) If $\det M_2 \neq 0$, then $\mathcal{A}_M$ has a left unit if and only if $M_1^T(M_2^T)^{-1}v_2 = v_1$.
(iii) If $\det M_1 = \det M_2 = 0$, then from (6) it follows that

$$\omega_{121} = \omega_{221} = \omega_{112} = \omega_{212} = 0.$$

(Indeed, otherwhise the system (7) has no solution). Moreover, either

$$\omega_{111}\omega_{222} - \omega_{211}\omega_{122} \neq 0$$

and hence

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} \omega_{111} & \omega_{211} \\ \omega_{122} & \omega_{222} \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

or, otherwise, $\omega_{111}\omega_{222} - \omega_{122}\omega_{211} = 0$ and consequently $\omega_{111} = \omega_{122} = a$, and $\omega_{211} = \omega_{222} = b$. In this last case, $\mathcal{A}_M$ has a unit if and only if $a^2 + b^2 \neq 0$ and then, every $u = u_1e_1 + u_2e_2$ satisfying that $au_1 + bu_2 = 1$ is a left unit for $\mathcal{A}_M$. □

Theorem 2.6. *Let $\mathcal{A}_M$ be the algebra associated with the matrix $M = (M_1|M_2)$ given in (2), with respect to the basis $B = \{e_1, e_2\}$. Set*

$$v_1^T := \begin{pmatrix} 1 & 0 \end{pmatrix},\ v_2^T := \begin{pmatrix} 0 & 1 \end{pmatrix} \text{ and } u^T := \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T.$$

(i) *If $\det M_1 \neq 0$, then $\mathcal{A}_M$ has a right unit $u = u_1e_1 + u_2e_2$ if and only if $M_2M_1^{-1}v_1 = v_2$, in which case with $u^T = M_1^{-1}v_1$.*

(ii) *If $\det M_2 \neq 0$, then $\mathcal{A}_M$ has a right unit $u = u_1e_1 + u_2e_2$ if and only if $M_1M_2^{-1}v_2 = v_1$, in which case $u^T = M_2^{-1}v_2$.*

(iii) *If $\det M_1 = \det M_2 = 0$, then $\mathcal{A}_M$ has a right unit if and only if either assertion* (a) *or* (b) *is satisfied where:*

(a) $M = \left(\begin{array}{cc|cc} \omega_{111} & \omega_{121} & 0 & 0 \\ 0 & 0 & \omega_{212} & \omega_{222} \end{array}\right)$ *and* $\widetilde{M} = \begin{pmatrix} \omega_{111} & \omega_{121} \\ \omega_{212} & \omega_{222} \end{pmatrix}$ *is such that* $\det \widetilde{M} \neq 0$. *In this case, $u = u_1e_1 + u_2e$ where $u^T = \widetilde{M}^{-1}(v_1 + v_2)$ is the unique right unit of $\mathcal{A}_M$.*

(b) $M = \left(\begin{array}{cc|cc} a & b & 0 & 0 \\ 0 & 0 & a & b \end{array}\right)$ *with $a^2 + b^2 \neq 0$. In this case, every $u = u_1e_1 + u_2e_2$ satisfying $au_1 + bu_2 = 1$ is a right unit for $\mathcal{A}_M$.*

Proof. The proof of this theorem is similar to the proof of Theorem 2.5. □

Corollary 2.7. *Let $\mathcal{A}_M$ be the algebra associated to the matrix $M = (M_1|M_2)$, with respect to the basis $B = \{e_1, e_2\}$. Then $\mathcal{A}_M$ has a unit if and only if $M_1 = M_1^T$, $M_2 = M_2^T$ and one of the following assertions is satisfied:*

(i) *$\det M_1 \neq 0$ and $M_2M_1^{-1}v_1 = v_2$, in which case $u = u_1e_1 + u_2e_2$ is the unit of $\mathcal{A}_M$, where $u^T := \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T$ is given by $u^T = M_1^{-1}v_1$.*

(ii) *$\det M_2 \neq 0$ and $M_1M_2^{-1}v_2 = v_1$, in which case $u = u_1e_1 + u_2e_2$ is the unit of $\mathcal{A}_M$, where $u^T := \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T$ is given by $u^T = M_2^{-1}v_2$.*

Consequently, if $\det M_1 \neq 0$ and $\det M_2 \neq 0$ then, $\mathcal{A}_M$ has a unit if and only if $M_1 = M_1^T$, $M_2 = M_2^T$ and $M_1^{-1}v_1 = M_2^{-1}v_2$.

(iii) *If $\det M_1 = 0 = \det M_2 = 0$ then, $\mathcal{A}_M$ has a unit if and only if*

$$M = \left(\begin{array}{cc|cc} a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \end{array}\right) \tag{8}$$

with $ab \neq 0$, in which case $u = \frac{1}{a}e_1 + \frac{1}{b}e_2$ is the unit of $\mathcal{A}_M$.

Proof. Suppose that $\det M_1 \neq 0$. From Theorem 2.5.(i) and Theorem 2.6.(i) the unique possible left (respectively right) unit for $\mathcal{A}_M$ is $u = u_1e_1 + u_2e_2$ where, if

$$u^T := \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T$$

then, $u^T = (M_1^T)^{-1}v_1$ (respectively, $u^T = M_1^{-1}v_1$). Consequently, a necessary condition for the existence of a unit is

$$M_1^{-1}v_1 = (M_1^T)^{-1}v_1.$$

From this last equality we obtain that $M_1 = M_1^T$. Moreover, according to the mentioned theorems, for the existence of a unit we also need that

$$M_2{M_1}^{-1}v_1 = M_2^T(M_1^T)^{-1}v_1 = v_2.$$

Therefore, $(M_2 - M_2^T)M_1^{-1}v_1 = 0$ and we deduce that $M_2 = M_2^T$. Consequently, a necessary condition for the existence of a unit in $\mathcal{A}_M$ is that $M_1 = M_1^T$ and $M_2 = M_2^T$ in which case, $u^T = M_1^{-1}v_1$ is both a left and a right unit if and only if $M_2M_1^{-1}v_1 = v_2$. This proves (i).

To prove (ii) suppose that $\det M_2 \neq 0$. Similarly, we obtain that $M_1 = M_1^T$ and $M_2 = M_2^T$ are necessary conditions for the existence of a unit for $\mathcal{A}_M$, and also that $u = u_1e_1 + u_2e_2$ is a unit for $\mathcal{A}_M$, where $u^T = M_2^{-1}v_2$, if and only if $M_1M_2^{-1}v_2 = v_1$.

Particularly, if $\det M_1 \neq 0$ and $\det M_2 \neq 0$, then it follows straightforwardly that $\mathcal{A}_M$ has a unit if and only if $M_1 = M_1^T$, $M_2 = M_2^T$, and $M_1^{-1}v_1 = M_2^{-1}v_2$.

Finally, note that if $\det M_1 = 0 = \det M_2$, then the only way to simultaneously satisfy assertion (iii) in both Theorem 2.5 and Theorem 2.6 is that assertion (b) be satisfied in both results. This means that M is of the type (8) and, therefore, $u = \frac{1}{a}e_1 + \frac{1}{b}e_2$ is the unit of $\mathcal{A}_M$. □

Theorem 2.8. *Let $\mathcal{A}_M$ be the algebra associated to the matrix $M = (M_1|M_2)$, with respect to the basis $B = \{e_1, e_2\}$. Then $\mathcal{A}_M$ is an associative and commutative algebra with a unit if and only if one of the following conditions is satisfied:*

(i) $M = \left(\begin{array}{cc|cc} a & b & 0 & 0 \\ b & c & 0 & \frac{-\det M_1}{b} \end{array}\right)$ *with $b \neq 0$ and $\det M_1 \neq 0$. In this case, the unit of $\mathcal{A}_M$ is given by*

$$u = \frac{1}{\det M_1}(ce_1 - be_2).$$

(ii) $M := \left(\begin{array}{cc|cc} \frac{-\det M_2}{\beta} & 0 & \alpha & \beta \\ 0 & 0 & \beta & \gamma \end{array}\right)$ *with $\beta \neq 0$ and $\det M_2 \neq 0$. In this case, the unit of $\mathcal{A}_M$ is given by*

$$u = \frac{1}{\det M_2}(-\beta e_1 + \alpha e_2).$$

(iii) $M = \left(\begin{array}{cc|cc} a & b & -b\lambda & -c\lambda \\ b & c & -c\lambda & d\lambda \end{array}\right)$, *for $a, b, c, d, \lambda \in \mathbb{K}$, with $(ac - b^2)(bd + c^2) \neq 0$, and $\lambda = -\frac{ac-b^2}{bd+c^2}$. In this case, the unit of $\mathcal{A}_M$ is given by*

$$u = \frac{1}{\det M_1}(ce_1 - be_2).$$

(iv) $M = \left(\begin{array}{cc|cc} a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \end{array}\right)$ *with $ab \neq 0$. In this case, the unit of $\mathcal{A}_M$ is given by*

$$u = \frac{1}{a}e_1 + \frac{1}{b}e_2.$$

Proof. Since $M = (M_1|M_2)$ defines the product of $\mathcal{A}_M$ by Corollary 2.4, we have

$$M = (M_1|M_2) = \left(\begin{array}{cc|cc} a & b & \alpha & \beta \\ b & c & \beta & \gamma \end{array}\right)$$

where

$$\begin{aligned} \alpha c &= b\beta \\ \det M_1 &= \beta c - \gamma b, \\ \det M_2 &= \alpha b - a\beta, \end{aligned} \tag{9}$$

Case 1. $\det M_1 \neq 0$ and $\det M_2 = 0$.

Case 1.1. If $\beta = 0$, then $\gamma \neq 0$, $b \neq 0$ and $\alpha = 0$, therefore, $\gamma = \frac{-\det M_1}{b}$. This means that

$$M_1 = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \text{ with } b \neq 0, \text{ and } M_2 = \begin{pmatrix} 0 & 0 \\ 0 & \frac{-\det M_1}{b} \end{pmatrix}.$$

Since the equality $M_2 M_1^{-1} v_1 = v_2$ holds we obtain, from Corollary 2.7, that the unit of $\mathcal{A}_M$ is given by $u = \frac{1}{\det M_1}(ce_1 - be_2)$.

Case 1.2. If $\beta \neq 0$, then $\alpha \neq 0$ and $\gamma \neq 0$ as $\beta^2 = \alpha\gamma$ because $\det M_2 = 0$. Since $\alpha c = b\beta$, by (9), we have that if $b = 0$, then $c = 0$ and $\det M_1 = 0$, a contradiction. Therefore, $b \neq 0$ and hence $\beta = \frac{\alpha c}{b}$. Consequently,

$$0 = \det M_2 = \alpha b - a\beta = \alpha b - \frac{\alpha a c}{b} = -\alpha \frac{\det M_1}{b} \neq 0,$$

a contradiction.

Case 2. $\det M_1 = 0$ and $\det M_2 \neq 0$.

Case 2.1 If $b = 0$ then, $a \neq 0$ and $\beta \neq 0$. Consequently, $b = \frac{\alpha c}{\beta}$ and

$$\det M_1 = \beta c - \gamma b = \beta c - \gamma \frac{\alpha c}{\beta} = \frac{c}{\beta}(\beta^2 - \alpha\gamma) = 0.$$

Therefore $c = 0$ and $a = \frac{-\det M_2}{\beta}$. Hence,

$$M_2 = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}, \text{ with } \beta \neq 0 \text{ and } M_1 = \begin{pmatrix} \frac{-\det M_2}{\beta} & 0 \\ 0 & 0 \end{pmatrix}.$$

In this case, $u^T = M_2^{-1} v_2$ so that $u = \frac{1}{\det M_2}(-\beta e_1 + \alpha e_2)$ is the unit of $\mathcal{A}_M$.

Case 2.2. $b \neq 0$.

Case 2.2.1. If $\alpha = 0$ then $\beta = 0$ as $\alpha c = b\beta$ by (9) and thus $\det M_2 = 0$, a contradiction.

Case 2.2.2 If $\alpha \neq 0$ then, since $\beta = \frac{\alpha c}{b}$, it follows that

$$0 \neq \det M_2 = \alpha b - a\beta = \alpha b - a\frac{\alpha c}{b} = \frac{\alpha}{b}(b^2 - ac) = 0,$$

a contradiction.

Case 3. $\det M_1 \neq 0$ and $\det M_2 \neq 0$. Then, in order to have a unit, we need that $M_1^{-1} v_1 = M_2^{-1} v_2$ so that

$$\frac{1}{\det M_1}\begin{pmatrix} c & -b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\det M_2}\begin{pmatrix} \gamma & -\beta \\ -\beta & \alpha \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and it follows that $\alpha = -\lambda b$ and $\beta = -\lambda c$ with $\lambda = \frac{\det M_2}{\det M_1} \neq 0$. Setting $d := \frac{\gamma}{\lambda}$,

$$M = \left(\begin{array}{cc|cc} a & b & -b\lambda & -c\lambda \\ b & c & -c\lambda & d\lambda \end{array}\right).$$

Since $\lambda = \frac{\det M_2}{\det M_1} = -\lambda^2 \frac{bd+c^2}{\det M_1}$, we have that $1 = -\lambda \frac{bd+c^2}{\det M_1}$. Thus, $\lambda = -\frac{ac-b^2}{bd+c^2}$. Moreover, since the unit is defined by the equality $M_1^{-1} v_1 = M_2^{-1} v_2$, we conclude that such a unit is $u = \frac{1}{\det M_1}(ce_1 - be_2)$.

Case 4. If $\det M_1 = 0 = \det M_2$ then, according with Corollary 2.7, a necessary and sufficient condition for $\mathcal{A}_M$ to have a unit is that

$$M = \left(\begin{array}{cc|cc} a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \end{array}\right)$$

with $ab \neq 0$. In this case $u = \frac{1}{a}e_1 + \frac{1}{b}e_2$ is the unit of $\mathcal{A}_M$. □

We recall that a **division** algebra is an algebra equipped with a unit, in which every nonzero element has an inverse. For non-associative algebras the notion of an invertible element is a delicate matter (see [20, 34]). Next we characterize when a real algebra $\mathcal{A}_M$ is an associative and commutative division algebra.

Theorem 2.9. *Let $\mathcal{A}_M$ be an algebra over $\mathbb{R}$, whose multiplication with respect to the basis $B = \{e_1, e_2\}$ is given by the cubic matrix $M = (M_1|M_2)$, where M_1 and M_2 are real matrices of dimension 2×2. Then, $\mathcal{A}_M$ is an associative, commutative division algebra if and only if*

$$M = \left(\begin{array}{cc|cc} a & b & -b\lambda & -c\lambda \\ b & c & -c\lambda & d\lambda \end{array}\right), \tag{10}$$

for $a, b, c, d, \lambda \in \mathbb{R}$, where $(ac - b^2)(bd + c^2) \neq 0$, $\lambda = -\frac{ac-b^2}{bd+c^2}$, and

$$(ad + bc)^2 < 4(b^2 - ac)(bd + c^2).$$

Proof. Since the algebra $\mathcal{A}_M$ that we are considering is associative, commutative and has a unit, we have that $\mathcal{A}_M$ have to satisfy one of the assertions (i) − (iv) stated in the Theorem 2.8.

Assertions (i), (ii), or (iv) correspond to an associative, commutative algebra with a unit that is not a division algebra. This is because e_1 (in cases (i) and (iv)) and e_2 (in cases (ii) and (iv)) are not invertible elements in $\mathcal{A}_M$. Consequently, we conclude that $\mathcal{A}_M$ satisfies (iii) so that M is like (10), for $a, b, c, d, \lambda \in \mathbb{R}$, where $(ac - b^2)(bd + c^2) \neq 0$ and $\lambda = -\frac{ac-b^2}{bd+c^2}$.

To prove that $\mathcal{A}_M$ is a division algebra, let $a = a_1e_1 + a_2e_2$ be any nonzero element of $\mathcal{A}_M$ and $a^{-1} = xe_1 + ye_2$ be its inverse. If the unit is given by $u = u_1e_1 + u_2e_2$ then, since since $\mathcal{A}_M$ is commutative, we have that $aa^{-1} = u$ which means that

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = u_1 \text{ and } \begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} -b\lambda & -c\lambda \\ -c\lambda & \lambda d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = u_2. \tag{11}$$

If we set

$$c_{11} := a_1a + a_2b,\ c_{12} := a_1b + a_2c,\ c_{21} := -a_1b\lambda - a_2c\lambda,\ c_{22} := -a_1c\lambda + a_2\lambda d, \tag{12}$$

then the system (11) can be written as

$$\begin{cases} c_{11}x + c_{12}y = u_1 \\ c_{21}x + c_{22}y = u_2. \end{cases} \tag{13}$$

Let $C := \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$. Then,

$$\begin{aligned} \det C &= c_{11}c_{22} - c_{12}c_{21} = \\ &= a_1^2\lambda(b^2 - ac) + a_2^2\lambda(bd + c^2) + a_1a_2\lambda(ad + bc) = \\ &= -a_1^2\lambda \det M_1 - a_2^2\frac{\det M_2}{\lambda} + a_1a_2(ad + bc)\lambda. \end{aligned} \tag{14}$$

The condition $\det C \neq 0$ is necessary and sufficient for the system to have a unique solution. (If the solution is not unique, then $\mathcal{A}_M$ contains divisors of zero, which implies that $\mathcal{A}_M$ is not a division algebra). We study when (13) has a unique solution by considering the following cases:

Case 1. $a_1 \neq 0$ and $a_2 = 0$. Then the unique solution of (13) is given by

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} \frac{\lambda cu_1 + bu_2}{a_1 \det M_2} & -\frac{b\lambda u_1 + au_2}{a_1 \det M_2} \end{pmatrix}.$$

Case 2. $a_1 = 0$ and $a_2 \neq 0$. Then the unique solution of (13) is given by

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} \frac{-\lambda d u_1 + c u_2}{a_2 \det M_1} & -\frac{\lambda c u_1 + b u_2}{a_2 \det M_1} \end{pmatrix}.$$

Case 3. $a_1 \neq 0$ and $a_2 \neq 0$. Then (13) has a unique solution if $\det C \neq 0$. If we fix a_2, then $\det C = 0$ if and only if

$$-a_1^2 \det M_1 + a_2^2(bd + c^2) + a_1 a_2(ad + bc) = 0. \tag{15}$$

This equation always has a real solution unless the discriminant is negative, that is

$$a_2^2(ad + bc)^2 + 4a_2^2 \det M_1(bd + c^2) < 0.$$

Consequently

$$(ad + bc)^2 < 4(b^2 - ac)(bd + c^2),$$

In this case, the inverse of $a = a_1 e_1 + a_2 e_2$ is given by $a^{-1} = x e_1 + y e_2$ where

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} \frac{c_{22}u_1 - c_{12}u_2}{\det C} & \frac{-c_{21}u_1 + c_{11}u_2}{\det C} \end{pmatrix},$$

with c_{ij} (for $i, j = 1, 2$) and $\det C$ determined by (12) and (14), respectively. □

Remark 2.10. *That there are no complex division algebras of dimension 2 is very well known [13], as finite-dimensional division algebras over an algebraically closed field $\mathbb{F}$ are isomorphic to $\mathbb{F}$ (note that $\mathbb{C}$ has dimension 1 as a complex algebra). In the above proof we obtain a justification of this fact. Indeed, since the equation (15) always have solution in $\mathbb{C}$, it follows that the associative and commutative algebra $\mathcal{A}_M$ is not a division algebra.*

3. Chains of time dependent 3D matrices

When working with time-dependent 3D matrices, it is advisable to select models where the temporal dependency is consistent. Drawing inspiration from Markov chain processes [5], we introduce below the notion of a chain of 3D matrices. These are time-dependent cubic matrices whose temporal dependency is robust, as guaranteed by the Chapman-Kolmogorov equation. For this purpose, we need to establish the product of two 3D-matrices in $\mathfrak{C}_n$.

There are many standard multiplication operations for cubic matrices (see [3, 17, 19]) that endow the linear space $\mathfrak{C}_n$ with the structure of an algebra. Particularly, in [3], the authors identifiy 15 associative multiplication rules for cubic matrices giving rise to five non-isomorphic associative algebras.

In this paper, we will consider in $\mathfrak{C}_n$ the algebraic structure derived from the following multiplication: Given $A = (a_{ijk})$ and $B = (b_{ijk})$ in $\mathfrak{C}_n$ we define multiplication of A and B as the matrix $A * B \in \mathfrak{C}_n$ given by

$$A * B := (c_{ijr})_{i,j,r} \quad \text{where } c_{ijr} = \sum_{k=1}^{n} a_{ijk} b_{kjr}, \text{ with } i, j, r = 1, \cdots, n. \tag{16}$$

In the case of matrices $A = (a_{ijk})$ and $B = (b_{ijk})$ in $\mathfrak{C}_2$, the above multiplication is $A * B = (C_1|C_2)$ where

$$\begin{aligned} C_1 &: = \begin{pmatrix} a_{111}b_{111} + a_{112}b_{211} & a_{121}b_{121} + a_{122}b_{221} \\ a_{211}b_{111} + a_{212}b_{211} & a_{221}b_{121} + a_{222}b_{221} \end{pmatrix} \\ C_2 &: = \begin{pmatrix} a_{111}b_{112} + a_{112}b_{212} & a_{121}b_{122} + a_{122}b_{222} \\ a_{211}b_{112} + a_{212}b_{212} & a_{221}b_{122} + a_{222}b_{222} \end{pmatrix}. \end{aligned} \tag{17}$$

That is, $A * B := (c_{ijr})_{i,j,r}$ with $i, j, r = 1, 2$, where

$$\begin{pmatrix} a_{1j1} & a_{1j2} \\ a_{2j1} & a_{2j2} \end{pmatrix} \begin{pmatrix} b_{1j1} & b_{1j2} \\ b_{2j1} & b_{2j2} \end{pmatrix} = \begin{pmatrix} c_{1j1} & c_{1j2} \\ c_{2j1} & c_{2j2} \end{pmatrix}, \quad j = 1, 2. \tag{18}$$

Definition 3.1. *Let $a, b \in \mathbb{R}_0^+$ with $a < b$. We define a **chain of 3D matrices** in $\mathfrak{C}_n$, associated to the time-range $[a, b]$, as a family of cubic matrices over $\mathbb{K} = \mathbb{R}$*

$$\mathcal{CH}_{[a,b]}^{n,*} := \{M^{[s,t]} \in \mathfrak{C}_n : a \le s < t \le b\}$$

satisfying the Chapman-Kolmogorov equation, which means that

$$\mathcal{M}^{[s,t]} = \mathcal{M}^{[s,\tau]} * \mathcal{M}^{[\tau,t]}, \tag{19}$$

for all $a \le s < \tau < t \le b$, where $*$ is a predefined product of cubic matrices in $\mathfrak{C}_n$.

We extend this definition straightforwardly to the case of a time interval given by $[a, +\infty]$ (as well as for $\mathbb{K} = \mathbb{C}$).

As said before, the product $*$ that we will consider in this work is (16).

Constructing examples of chains of 3D matrices is challenging, even in dimension 2. In fact, to define a chain $\mathcal{CH}_{[a,b]}^{n,*} := \{M^{[s,t]} \in \mathfrak{C}_2 : a \le s < t \le b\}$, where the matrices

$$\mathcal{M}^{[s,t]} = \left(\begin{array}{cc|cc} c_{111}^{[s,t]} & c_{121}^{[s,t]} & c_{112}^{[s,t]} & c_{122}^{[s,t]} \\ c_{211}^{[s,t]} & c_{221}^{[s,t]} & c_{212}^{[s,t]} & c_{222}^{[s,t]} \end{array}\right) \in \mathfrak{C}_2,$$

satisfy the Chapman-Kolmogorov equation with respect to the product (16), it is necessary that the following equations derived from (19), be satisfied:

$$c_{ijr}^{[s,t]} = c_{ij1}^{[s,\tau]} c_{1jr}^{[\tau,t]} + c_{ij2}^{[s,\tau]} c_{2jr}^{[\tau,t]}, \qquad i, j, r = 1, 2.$$

If we consider the four equations with $j = 1$, the unknowns in them do not participate in the other four equations with $j = 2$. Therefore, the equations for $j = 1$ and $j = 2$ are independent. Hence it suffices to solve the system only for $j = 1$. Denote $a_{ir}^{[s,t]} = c_{i1r}^{[s,t]}$ to obtain the following system:

$$\begin{cases} a_{11}^{[s,t]} = a_{11}^{[s,\tau]} a_{11}^{[\tau,t]} + a_{12}^{[s,\tau]} a_{21}^{[\tau,t]} \\ a_{12}^{[s,t]} = a_{11}^{[s,\tau]} a_{12}^{[\tau,t]} + a_{12}^{[s,\tau]} a_{22}^{[\tau,t]} \\ a_{21}^{[s,t]} = a_{21}^{[s,\tau]} a_{11}^{[\tau,t]} + a_{22}^{[s,\tau]} a_{21}^{[\tau,t]} \\ a_{22}^{[s,t]} = a_{21}^{[s,\tau]} a_{12}^{[\tau,t]} + a_{22}^{[s,\tau]} a_{22}^{[\tau,t]}. \end{cases} \tag{20}$$

The complete set of solutions of the system (20) has not yet been fully determined. However, a broad class of solutions exists, as explored in [4, 12, 16, 21, 22, 25, 26]. In the next result, we present a particular solution for (20) taken from [15].

Remark 3.2. *The matrices $M^{[s,t]}$ given by*

$$M^{[s,t]} = \left(\begin{array}{cc|cc} \cos(t-s) & \cos(t-s) & \sin(t-s) & -\sin(t-s) \\ -\sin(t-s) & \sin(t-s) & \cos(t-s) & \cos(t-s) \end{array}\right), \tag{21}$$

for $s, t \in \mathbb{R}_0^+$ with $s < t$, define a chain

$$\mathcal{CH}_{[0,+\infty[}^{2,*} := \{M^{[s,t]} : 0 \le s < t < +\infty\},$$

of 3D matrices in $\mathfrak{C}_2$ (with $\mathbb{K} = \mathbb{R}$) with respect to the product given by (17).

To make a direct reference to the chain provided by Remark 3.2, we introduce the following definition.

Definition 3.3. *We define the **3D rotation chain of dimension** $2 \times 2 \times 2$ as the 3D chain*

$$\mathcal{CH}_{[0,+\infty[}^{2,rot} := \{M^{[s,t]} : 0 \le s < t < +\infty\}$$

of matrices in $\mathfrak{C}_2$ (with $\mathbb{K} = \mathbb{R}$) defined by the matrices $M^{[s,t]}$ given in (21), with the matrix product in $\mathfrak{C}_2$ determined by (17).

Our next goal is to study the properties of the algebras associated with the cubic matrices that determine the 3D rotation chain of dimension $2 \times 2 \times 2$.

3.1. The rotation chain of dimension 2

As previously mentioned, fixed a 2-dimensional linear space $\mathcal{A}$ with a basis $B = \{e_1, e_2\}$, every matrix

$$M = \left(\begin{array}{cc|cc} a_{111} & a_{121} & a_{112} & a_{122} \\ a_{211} & a_{221} & a_{212} & a_{222} \end{array}\right) \in \mathfrak{C}_2$$

define a product in $\mathcal{A}$. In fact, if $a = \alpha_1 e_1 + \alpha_2 e_2$ and $b = \beta_1 e_1 + \beta_2 e_2$ then $ab = \gamma_1 e_1 +_2 \gamma e_2$ where

$$\begin{aligned} \gamma_1 &= (\alpha_1, \alpha_2)\left(\begin{array}{cc} a_{111} & a_{121} \\ a_{211} & a_{221} \end{array}\right)\left(\begin{array}{c} \beta_1 \\ \beta_2 \end{array}\right); \\ \gamma_2 &= (\alpha_1, \alpha_2)\left(\begin{array}{cc} a_{112} & a_{122} \\ a_{212} & a_{222} \end{array}\right)\left(\begin{array}{c} \beta_1 \\ \beta_2 \end{array}\right). \end{aligned} \tag{22}$$

This product endows $\mathcal{A}$ with the structure of an algebra that does not need to be associative.

The 3D rotation-chain is given by the family

$$\mathcal{CH}^{2,rot}_{[0,+\infty[} := \{M^{[s,t]} : 0 \le s < t < +\infty\},$$

where

$$M^{[s,t]} = \left(\begin{array}{cc|cc} \cos(t-s) & \cos(t-s) & \sin(t-s) & -\sin(t-s) \\ -\sin(t-s) & \sin(t-s) & \cos(t-s) & \cos(t-s) \end{array}\right).$$

The algebras $\mathcal{A}^{[0,t]}$ associated to the matrices $M^{[0,t]} \in \mathcal{CH}^{2,rot}_{[0,+\infty[}$, for $t \in \mathbb{R}^+_0$, have been described in [27]. Since

$$\mathcal{M}^{[0,t]} = \left(\begin{array}{cc|cc} \cos(t) & \cos(t) & \sin(t) & -\sin(t) \\ -\sin(t) & \sin(t) & \cos(t) & \cos(t) \end{array}\right),$$

we obtain that, having fixed the basis $B = \{e_1, e_2\}$, the multiplication table of $\mathcal{A}^{[0,t]}$ is given by

$$\begin{aligned} e_1e_1 &= c_{111}e_1 + c_{112}e_2 = \cos te_1 + \sin te_2, \\ e_1e_2 &= c_{121}e_1 + c_{122}e_2 = \cos te_1 - \sin te_2, \\ e_2e_1 &= c_{211}e_1 + c_{212}e_2 = -\sin te_1 + \cos te_2, \\ e_2e_2 &= c_{221}e_1 + c_{222}e_2 = \sin te_1 + \cos te_2. \end{aligned}$$

In order to describe these algebras for every $t \in \mathbb{R}^+_0$, we introduce the following notation.

Notation. Considering a fixed a 2-dimensional vector space $\mathcal{A}$ over $\mathbb{R}$ with basis $B = \{e_1, e_2\}$, let us denote by $\mathcal{A}^+_0$, $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}^+_{\cos t}$, and $\mathcal{A}^-_{\cos t}$, the real algebras associated, respectively, with the following cubic matrices:

$$\mathcal{M}^+_0 = \left(\begin{array}{cc|cc} 0 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 \end{array}\right), \quad \mathcal{M}_1 = \left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right),$$

$$\mathcal{M}_2 = \left(\begin{array}{cc|cc} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{array}\right),$$

$$\mathcal{M}^+_{\cos t} = \left(\begin{array}{cc|cc} \cos t & \cos t & \sqrt{1-\cos^2 t} & -\sqrt{1-\cos^2 t} \\ -\sqrt{1-\cos^2 t} & \sqrt{1-\cos^2 t} & \cos t & \cos t \end{array}\right) \quad \text{and}$$

$$\mathcal{M}^-_{\cos t} = \left(\begin{array}{cc|cc} \cos t & \cos t & -\sqrt{1-\cos^2 t} & \sqrt{1-\cos^2 t} \\ \sqrt{1-\cos^2 t} & -\sqrt{1-\cos^2 t} & \cos t & \cos t \end{array}\right).$$

The proof of the following result is derived from [27, Theorem 3].

Theorem 3.4. *The algebras $\mathcal{A}^{[0,t]}$ associated to the matrices $M^{[0,t]}$, for $t \in \mathbb{R}_0^+$, in the 3D rotation chain of dimension 2, are the following ones:*

$$\mathcal{A}^{[0,t]} \cong \begin{cases} \mathcal{A}_1, & if \quad t \in \{\pi k : k \in I\} \\ \mathcal{A}_0^+, & if \quad t \in \{\frac{\pi}{2} + \pi k : k \in I\} \\ \mathcal{A}_2, & if \quad t \in \{\frac{3\pi}{4} + \pi k : k \in I\} \\ \mathcal{A}^+_{\cos t}, & if \quad t \in \bigcup_{k\in I}(\pi k; \frac{\pi}{2} + \pi k) \\ \mathcal{A}^-_{\cos t}, & if \quad t \in \bigcup_{k\in I}((\frac{\pi}{2} + \pi k; \pi + \pi k) \setminus \{\frac{3\pi}{4} + \pi k\}) \end{cases}$$

where $I = \{0, 1, 2, ...\}$.

The essence of the theorem can be more clearly visualized in Figure 1.

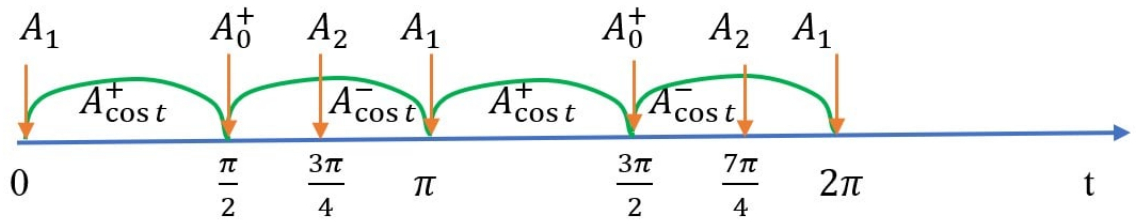

Figure 1: The partition of the time set $\{(0, t) : 0 \leq t\}$ corresponding to the classification of the algebras $\mathcal{A}^{[0,t]}$, with $t \geq 0$ in the rotation chain.

Our goal now is to describe the algebraic properties of the algebras $\mathcal{A}^{[0,t]}$, with $t \geq 0$, in order to use them in encryption-decryption purposes.

From a direct application of the theorems and corollaries in Section 2 we obtain the result presented in the following table, where

$$u_\alpha := \alpha e_1 + (1 - \alpha)e_2, \text{ for } \alpha \in \mathbb{R}, \quad u = \frac{1}{\sqrt{2}}(e_1 + e_2) \text{ and } \widetilde{u} = \frac{1}{2\cos t}(e_1 + e_2).$$

	$\mathcal{A}_0^+$	$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}^+_{\cos t}$	$\mathcal{A}^-_{\cos t}$
Associativity	No	Yes	Yes	No	No
Commutative	No	No	Yes	No	No
Left unit	No	No	u	No	No
Right unit	No	u_α	u	$\widetilde{u}$	$\widetilde{u}$
Unit	No	No	u	No	No

Regarding the determinants of layers M_1 and M_2 in $M = (M_1|M_2)$ where M is the cubic matrix defining the product of the corresponding algebra, we have the following information:

	$\mathcal{M}_0^+$	$\mathcal{M}_1$	$\mathcal{M}_2$	$\mathcal{M}^+_{\cos t}$	$\mathcal{M}^-_{\cos t}$
$\det M_1$	0	0	-1	$\sin(2t)$	$-\sin(2t)$
$\det M_2$	0	0	-1	$\sin(2t)$	$-\sin(2t)$

We summarize this information in the following result.

Theorem 3.5. *Let $\mathcal{CH}^{2,rot}_{[0,+\infty[} := \{M^{[s,t]} : 0 \leq s < t < +\infty\}$ be the 3D rotation chain of dimension $2 \times 2 \times 2$. Let $\mathcal{A}^{[0,t]}$ be the algebra associated with the cubic matrix $M^{[0,t]}$, for every $t \in \mathbb{R}^+_0$. Then:*

(i) *$\mathcal{A}^{[0,t]}$ has a unit if and only if $t \in \{\frac{3\pi}{4} + \pi k : k \in I\}$ with $I = \mathbb{N} \cup \{0\}$, in which case $\mathcal{A}^{[0,t]} = \mathcal{A}_2$.*

(ii) *$\mathcal{A}_2$ is an associative and commutative division algebra whose unit is given by $u = \frac{1}{\sqrt{2}}(e_1 + e_2)$. Moreover, the inverse of a nonzero element $a = a_1e_1 + a_2e_2 \in \mathcal{A}_2$ is given by $a^{-1} = \frac{a_2}{a_1^2+a_2^2}e_1 + \frac{a_1}{a_1^2+a_2^2}e_2$.*

3.2. Encrypting and decrypting with the 3D rotation chain

This subsection presents the use of algebraic properties of the algebras associated with the 3D rotation chain to develop time-dependent encryption and decryption algorithms. We will not provide a specific algorithm, but rather a general procedure for constructing algorithms based on predefined functions. Depending on these functions, different algorithms can be obtained under the same framework.

In $\mathcal{A} = \mathbb{R}^2$ we prefix a basis $B = \{e_1, e_2\}$. Then, every 3D matrix of dimension $2\times2\times2$ uniquely determines a multiplication in $\mathbb{R}^2$, endowing $\mathbb{R}^2$ with structure of an algebra (non necessarily associative). In particularly, this holds for every matrix of the 3D rotation chain $\mathcal{CH}^{2,rot}_{[0,+\infty[} := \{M^{[s,t]} : 0 \leq s < t < +\infty\}$ where $M^{[s,t]}$ is given by (21).

More precisely, our interest lies in the time-dependent two-dimensional algebras $\mathcal{A}^{[0,t]}$ obtained by considering in $\mathbb{R}^2$ the products associated to the cubic matrices $M^{[0,t]}$ with $t \geq 0$, given by

$$M^{[0,t]} := \left(\begin{array}{cc|cc} c^{[0,t]}_{111} & c^{[0,t]}_{121} & c^{[0,t]}_{112} & c^{[0,t]}_{122} \\ c^{[0,t]}_{211} & c^{[0,t]}_{221} & c^{[0,t]}_{212} & c^{[0,t]}_{222} \end{array}\right) = \left(\begin{array}{cc|cc} \cos(t) & \cos(t) & \sin(t) & -\sin(t) \\ -\sin(t) & \sin(t) & \cos(t) & \cos(t) \end{array}\right).$$

Thus, the product of $a = \alpha e_1 + \beta e_2$, and $b = \gamma e_1 + \delta e_2$, in the algebra $\mathcal{A}^{[0,t]}$ is given by $ab = \lambda e_1 + \mu e_2$ where, according with (22),

$$(\alpha,\beta)\begin{pmatrix} c^{[0,t]}_{111} & c^{[0,t]}_{121} \\ c^{[0,t]}_{211} & c^{[0,t]}_{221} \end{pmatrix}\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \lambda \text{ and } (\alpha,\beta)\begin{pmatrix} c^{[0,t]}_{112} & c^{[0,t]}_{122} \\ c^{[0,t]}_{212} & c^{[0,t]}_{222} \end{pmatrix}\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \mu.$$

The proposed encryption model works as follows. We consider that Alice has an input token represented by a vector $a := (\alpha, \beta) \in \mathbb{R}^2$. Therefore, associated with Alice's information, we have the vector $a = \alpha e_1 + \beta e_2$.

On the other hand, Bob (who encodes Alice's information) knows a predefined function $b : \mathbb{R}^+_0 \to \mathbb{R}^2\backslash\{0,0\}$. Note that there are no conditions on b except that

$$b(t) \neq (0,0), \text{ for every } t \geq 0.$$

Consequently, associated with $b(t) = (b_1(t), b_2(t)) \in \mathbb{R}^2$, we have the element

$$b(t) = b_1(t)e_1 + b_2(t)e_2 \in \mathcal{A}^{[0,t]}.$$

When Alice requests access to the encryption system managed by Bob, she inputs her data $a = \alpha e_1 + \beta e_2$ into the system at a specific instant of time t. A double first encryption of $a = (\alpha, \beta)$ is then obtained as follows:

$$\begin{aligned} (\alpha,\beta)\begin{pmatrix} c^{[0,t]}_{111} & c^{[0,t]}_{112} \\ c^{[0,t]}_{211} & c^{[0,t]}_{212} \end{pmatrix} &= (u^a_1(t), u^a_2(t)), \\ (\alpha,\beta)\begin{pmatrix} c^{[0,t]}_{121} & c^{[0,t]}_{122} \\ c^{[0,t]}_{221} & c^{[0,t]}_{222} \end{pmatrix} &= (v^a_1(t), v^a_2(t)). \end{aligned} \tag{23}$$

To decrypt this double encryption of $a = \alpha e_1 + \beta e_2$ (equivalently, of (α, β)), we consider another algebra that is well-behaved, since the algebra $\mathcal{A}^{[0,t]}$ used for encryption may be poorly behaved. To this end, note that for all

$$s \in \{\frac{3\pi}{4} + n\pi : n \in \mathbb{N}\},$$

the corresponding algebra $\mathcal{A}^{[0,s]}$ coincides with the algebra $\mathcal{A}_2$, which is the unique well-behaved algebra in the 3D rotation chain. Specifically, $\mathcal{A}^{[0,s]} = \mathcal{A}_2$ is the only associative and commutative division algebra. Consequently, for the decryption process, it is advisable to address the decryption problem to these concrete algebras. To achieve this, it is unnecessary for Alice to interact in the system again, as such intervention could introduce synchronization issues. Indeed, the Chapman-Kolmogorov equation allows us to obtain an algebra $\mathcal{A}^{[0,s]}$ for $s = \frac{3\pi}{4} + n\pi$ with $s > t$ and $n \in \mathbb{N} \cup \{0\}$ (for instance set $n = E(\frac{t}{\pi} - \frac{3}{4}) + 1$ if $t \geq \frac{3\pi}{4}$, and $n = 0$ otherwise, where E denotes the floor function). Since $M^{[0,t]} * M^{[t,s]} = M^{[0,s]}$, according with (18), we have that

$$\begin{pmatrix} c_{1i1}^{[0,t]} & c_{1i2}^{[0,t]} \\ c_{2i1}^{[0,t]} & c_{2i2}^{[0,t]} \end{pmatrix}\begin{pmatrix} c_{1i1}^{[t,s]} & c_{1i2}^{[t,s]} \\ c_{2i1}^{[t,s]} & c_{2i2}^{[t,s]} \end{pmatrix} = \begin{pmatrix} c_{1i1}^{[0,s]} & c_{1i2}^{[0,s]} \\ c_{2i1}^{[0,s]} & c_{2i2}^{[0,s]} \end{pmatrix}.$$

Hence, by defining

$$(w_1^a(s), w_2^a(s)) := (u_1^a(t), u_2^a(t))\begin{pmatrix} c_{111}^{[t,s]} & c_{112}^{[t,s]} \\ c_{211}^{[t,s]} & c_{212}^{[t,s]} \end{pmatrix} \text{ and}$$

$$(x_1^a(s), x_2^a(s)) := (v_1^a(t), v_2^a(t))\begin{pmatrix} c_{121}^{[t,s]} & c_{122}^{[t,s]} \\ c_{221}^{[t,s]} & c_{222}^{[t,s]} \end{pmatrix},$$

we have that

$$\begin{aligned} (\alpha, \beta)\begin{pmatrix} c_{111}^{[0,s]} & c_{112}^{[0,s]} \\ c_{211}^{[0,s]} & c_{212}^{[0,s]} \end{pmatrix} &= (w_1^a(s), w_2^a(s)) \text{ and} \\ (\alpha, \beta)\begin{pmatrix} c_{121}^{[0,s]} & c_{122}^{[0,s]} \\ c_{221}^{[0,s]} & c_{222}^{[0,s]} \end{pmatrix} &= (x_1^a(s), x_2^a(s)) \end{aligned}$$

and it follows that, in the algebra $\mathcal{A}^{[0,s]}$, the product of $\alpha e_1 + \beta e_2$ and $b_1(s)e_1 + b_2(s)e_2$ is given by $c^a(s) = c_1(s)e_1 + c_2(s)e_2$, where

$$\begin{aligned} c_1(s) &= w_1^a(s)b_1(s) + x_1^a(s)b_2(s) \text{ and} \\ c_2(s) &= w_2^a(s)b_1(s) + x_2^a(s)b_2(s). \end{aligned}$$

Since $\mathcal{A}^{[0,s]}$ is an associative and commutative, division algebra and $b(s)$ is nonzero, $c(s)$ can be easily decrypted. In fact, if $\cdot$ denotes the product in $\mathcal{A}^{[0,s]}$, then we have that

$$c^a(s) \cdot b(s)^{-1} = (a \cdot b(s)) \cdot b(s)^{-1} = a \cdot (b(s) \cdot b(s)^{-1}) = a \cdot e(s) = a.$$

More precisely, since $b(s) \in \mathcal{A}^{[0,s]}$ and $b(s) \neq 0$, by Theorem 3.5, we have that

$$b(s)^{-1} = \frac{b_2(s)}{b_1^2(s) + b_2^2(s)}e_1 + \frac{b_1(s)}{b_1^2(s) + b_2^2(s)}e_2.$$

Therefore

$$\begin{aligned} \alpha &= (c_1(s), c_2(s))\begin{pmatrix} c_{111}^{[0,s]} & c_{121}^{[0,s]} \\ c_{211}^{[0,s]} & c_{221}^{[0,s]} \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix} \text{ and} \\ \beta &= (c_1(s), c_2(s))\begin{pmatrix} c_{112}^{[0,s]} & c_{122}^{[0,s]} \\ c_{212}^{[0,s]} & c_{222}^{[0,s]} \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix}, \end{aligned}$$

as desired.

Regarding this model, we make the following observations to emphasize that we are not providing a single an algorithm but rather a general procedure from which multiple algorithms can be derived.

Remarks about the model.

(i) Each fixed basis in $\mathbb{R}^2$ induces a distinct encryption process based on the same approach..

(ii) Similarly, every function $b : \mathbb{R}_0^+ \to \mathbb{R}^2\backslash\{0,0\}$ defines a different encryption process, and we can take advantage of this fact to improve the process.

(iii) When dealing with the encryption and decryption of input tokens represented by vectors of length n, the vector can be partitioned into pairs (x_i, x_{i+1}), or the 3D rotation chain can be replaced by one of higher dimension, thereby extrapolating the method presented here.

(iv) Alice's code $a = \alpha e_1 + \beta e_2$ can be replaced by a time dependent vector code as follow.

Consider a mapping $h : \mathbb{R}^2 \times \mathbb{R}_0^+ \to \mathbb{R}^2$ such that, for every $t \in \mathbb{R}_0^+$, the function $h_t : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $h_t(\alpha,\beta) := h((\alpha,\beta),t)$ is bijective. Then, the encryption process can be strengthened by introducing $h_t(\alpha,\beta) = (\alpha_t,\beta_t)$ as Alice's time-dependent code instead of (α,β).

Such a function h is easy to construct. For instance, if $f, g : \mathbb{R} \to \mathbb{R}$ are functions that do not vanish simultaneously at the same point $t \in \mathbb{R}_0^+$, then the function $h : \mathbb{R}^2 \times \mathbb{R}_0^+ \to \mathbb{R}^2$ defined by

$$h((\alpha,\beta);t) = (f(t)\alpha + g(t)\beta, f(t)\beta - g(t)\alpha),$$

satisfies the required property. Indeed, if $h_t(\alpha,\beta) := h((\alpha,\beta),t) = (\alpha_t,\beta_t)$ then,

$$(\alpha,\beta) = \left(\frac{f(t)\alpha_t - g(t)\beta_t}{f^2(t)+g^2(t)}, \frac{g(t)\alpha_t + f(t)\beta_t}{f^2(t)+g^2(t)}\right). \tag{24}$$

In this case, to decrypt of Alice's code we first obtain $h_t(a) = (\alpha_t,\beta_t)$ from the equality $h_t(a) = c(s) * b(s)^{-1}$, and then recover $a = (\alpha,\beta)$ from $h_t(a) = (\alpha_t,\beta_t)$.

3.3. Algorithms.

In this section, we present encryption and decryption algorithms that implement the procedure described above. We begin with the simplest version (which ignors Remark (iv)).

Preliminaries:

(a) Define a function $b : \mathbb{R}_0^+ \to \mathbb{R}^2\backslash\{0,0\}$.

(b) Provide Alice with a vector $a = (\alpha,\beta) \in \mathbb{R}^2$.

For encryption:

(c) Determine the instant of time t in which Alice ask for codification.

(d) Compute $s > t$ such that $s = \frac{3\pi}{4} + n\pi$, for some integer n.

(e) Determine the double encryption $(u_1^a(t), u_2^a(t))$ and $(v_1^a(t), v_2^a(t))$ according to

$$\begin{aligned}(\alpha,\beta)\begin{pmatrix}\cos(t) & \sin(t)\\ -\sin(t) & \cos(t)\end{pmatrix} &= (u_1^a(t), u_2^a(t)),\\ (\alpha,\beta)\begin{pmatrix}\cos(t) & -\sin(t)\\ \sin(t) & \cos(t)\end{pmatrix} &= (v_1^a(t), v_2^a(t)).\end{aligned}$$

For decryption.

(h) Determine $c^a(s) = (c_1(s), c_2(s))$. To this end, compute

$$\begin{aligned}(u_1^a(t), u_2^a(t))\begin{pmatrix} \cos(s-t) & \sin(s-t) \\ -\sin(s-t) & \cos(s-t) \end{pmatrix} &= (w_1^a(s), w_2^a(s)),\\ (v_1^a(t), v_2^a(t))\begin{pmatrix} \cos(s-t) & -\sin(s-t) \\ \sin(s-t) & \cos(s-t) \end{pmatrix} &= (x_1^a(s), x_2^a(s)),\end{aligned}$$

then define $c_1(s) = w_1^a(s)b_1(s) + x_1^a(s)b_2(s)$ and $c_2(s) = w_2^a(s)b_1(s) + x_2^a(s)b_2(s)$.

(i) Recover $a = (\alpha, \beta)$ using the formula $a = c_s(a) * b(s)^{-1}$. That is,

$$\begin{aligned}\alpha &= (c_1(s), c_2(s))\begin{pmatrix} \cos(s) & \cos(s) \\ -\sin(s) & \sin(s) \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix} \text{ and}\\ \beta &= (c_1(s), c_2(s))\begin{pmatrix} \sin(s) & -\sin(s) \\ \cos(s) & \cos(s) \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix}.\end{aligned}$$

Algorithm for triple encryption:

For a triple codification of $a = (\alpha, \beta)$, according to Remark (iv), replace steps (a), (e), and (i), in the algorithm above with the modified counterparts (a-bis), (e-bis), and (i-bis) below, respectively.

(a-bis). Define $b : \mathbb{R}_0^+ \to \mathbb{R}^2\backslash\{0,0\}$ and $h : \mathbb{R}^2 \times \mathbb{R}_0^+ \to \mathbb{R}^2$ satisfying that the mapping $h_t : \mathbb{R}^2 \to \mathbb{R}^2$ given by $h_t(a) := h(a, t)$ is bijective for every $t \in \mathbb{R}_0^+$.

(For obtaining the above algoritm take h_t as the identity on $\mathbb{R}^2$ so that $h_t(a) := a$ for every $t \in \mathbb{R}_0^+$ and every $a \in \mathbb{R}^2$).

(e-bis). Determine the encryption $h_t(a) = (\alpha_t, \beta_t)$ and its corresponding double encryption, given by $(u_1^a(t), u_2^a(t))$ and $(v_1^a(t), v_2^a(t))$, according to (23). Thus,

$$\begin{aligned}(\alpha_t, \beta_t)\begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix} &= (u_1^a(t), u_2^a(t))\\ (\alpha_t, \beta_t)\begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} &= (v_1^a(t), v_2^a(t)).\end{aligned}$$

(i-bis). Determine $h_t(a) = (\alpha_t, \beta_t)$ using the formula $h_t(a) = c_s(a) * b(s)^{-1}$. Therefore,

$$\begin{aligned}\alpha_t &= (c_1(s), c_2(s))\begin{pmatrix} \cos(s) & \cos(s) \\ -\sin(s) & \sin(s) \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix} \text{ and}\\ \beta_t &= (c_1(s), c_2(s))\begin{pmatrix} \sin(s) & -\sin(s) \\ \cos(s) & \cos(s) \end{pmatrix}\begin{pmatrix} \frac{b_2(s)}{b_1^2(s)+b_2^2(s)} \\ \frac{b_1(s)}{b_1^2(s)+b_2^2(s)} \end{pmatrix}.\end{aligned}$$

Finally, we recover $a = (\alpha, \beta)$ from $h_t(a) = (\alpha_t, \beta_t)$, as in (24).

References

[1] M. Abdalla, M. Bellare *et al.*, *Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions*, Adv. Cryptol. – CRYPTO 2005, Conf. Paper (2005).

[2] E. Angel, D. Shreiner, *Interactive Computer Graphics: A Top-Down Approach with WebGL*, 7th ed., Addison-Wesley, 2015.

[3] R. Bai, H. Liu, M. Zhang, *3-Lie algebras realized by cubic matrices*, Chin. Ann. Math. Ser. B **35** (2014), no. 2, 261–270.

[4] J. M. Casas, M. Ladra, U. A. Rozikov, *A chain of evolution algebras*, Linear Algebra Appl. **435** (2011), no. 4, 852–870.

[5] J. M. Casas, M. Ladra, U. A. Rozikov, *Markov processes of cubic stochastic matrices: quadratic stochastic processes*, Linear Algebra Appl. **575** (2019), 273–298.
[6] A. B. Craig, *Understanding Augmented Reality: Concepts and Applications*, 1st ed., Elsevier, 2013.
[7] P. B. Davenport, *A vector approach to the algebra of rotations with applications: Vector representation of rotations and their algebra*, NASA Goddard Space Flight Center, Greenbelt, MD, 1968.
[8] A. M. Deshpande, M. S. Deshpande, D. N. Kayatanavar, *FPGA implementation of AES encryption and decryption*, Proc. 2009 Int. Conf. Control, Autom., Commun. Energy Conserv., Perundurai, India (2009), 1–6.
[9] I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, 2016.
[10] R. Hartley, A. Zisserman, *Multiple View Geometry in Computer Vision*, Cambridge Univ. Press, 2004.
[11] J. F. Hughes, A. Van Dam, M. McGuire, D. F. Sklar, J. D. Foley, S. K. Feiner, K. Akeley, *Computer Graphics: Principles and Practice*, Addison-Wesley, 2014.
[12] A. N. Imomkulov, M. V. Velasco, *Chain of three-dimensional evolution algebras*, Filomat **34** (2020), no. 10, 3175–3190.
[13] N. Jacobson, *Lie Algebras*, Interscience Tracts Pure Appl. Math., vol. 10, Interscience Publ. (John Wiley & Sons), New York–London, 1962.
[14] S. Kiran *et al.*, *Analysis of in-place matrix rotation of square matrix for information security applications*, Procedia Comput. Sci. **215** (2022), 131–139.
[15] M. Ladra, U. A. Rozikov, *Flow of finite-dimensional algebras*, J. Algebra **470** (2017), 263–288.
[16] M. Ladra, U. A. Rozikov, *Construction of flows of finite-dimensional algebras*, J. Algebra **492** (2017), 475–489.
[17] M. Ladra, U. A. Rozikov, *Algebras of cubic matrices*, Linear Multilinear Algebra **65** (2017), no. 7, 1316–1328.
[18] Q. Liu, G. Wang, J. Wu, *Time-based proxy re-encryption scheme for secure data sharing in a cloud environment*, Inf. Sci. **258** (2014), 355–370.
[19] V. M. Maksimov, *Cubic stochastic matrices and their probability interpretations*, Theory Probab. Appl. **41** (1996), no. 1, 55–69.
[20] J. C. Marcos, M. V. Velasco, *The multiplicative spectrum and the uniqueness of the complete norm topology*, Filomat **28** (2014), 473–485.
[21] B. A. Narkuziyev, U. A. Rozikov, *Classification in chains of three-dimensional real evolution algebras*, Linear Multilinear Algebra **71** (2023), no. 2, 265–300.
[22] B. A. Omirov, U. A. Rozikov, K. M. Tulenbayev, *On real chains of evolution algebras*, Linear Multilinear Algebra **63** (2015), no. 3, 586–600.
[23] F. Regazzoni, B. Mazumdar, S. Parameswaran, *Security, Privacy, and Applied Cryptography Engineering*, Proc. 13th Int. Conf. SPACE 2023, Roorkee, India (2023), 14–17.
[24] K. F. Riley, M. P. Hobson, S. J. Bence, *Mathematical Methods for Physics and Engineering*, Cambridge Univ. Press, 2010.
[25] U. A. Rozikov, *Population Dynamics: Algebraic and Probabilistic Approach*, World Sci. Publ., Singapore, 2020.
[26] U. A. Rozikov, Sh. N. Murodov, *Dynamics of two-dimensional evolution algebras*, Lobachevskii J. Math. **34** (2013), no. 4, 344–358.
[27] U. A. Rozikov, M. V. Velasco, B. A. Narkuziev, *Classification in a rotational flow of two-dimensional algebras*, `arXiv:2204.13910v3` (2024).
[28] J. Sen, *Cryptography and Security in Computing*, CRC Press, 2012.
[29] N. H. Shah, F. A. Thakkar, *Matrix and Determinant: Fundamentals and Applications*, Springer, 2020.
[30] J. Su *et al.*, *Roformer: Enhanced transformer with rotary position embedding*, Neurocomputing **568** (2024), 127063–127065.
[31] P. Suetens, *Fundamentals of Medical Imaging*, Cambridge Univ. Press, 2009.
[32] A. Tarantola, *Inverse Problem Theory and Methods for Model Parameter Estimation*, Soc. Indust. Appl. Math. (SIAM), Philadelphia, 2005.
[33] S. Tuecke *et al.*, *Globus auth: A research identity and access management platform*, Proc. 12th IEEE Int. Conf. e-Sci. (e-Science), Baltimore, MD, USA (2016), 203–212.
[34] M. V. Velasco, *Spectral theory for non-associative complete normed algebras and automatic continuity*, J. Math. Anal. Appl. **351** (2009), 97–106.
[35] Y. Wang, T. Jiang, S. Ma, W. Gao, *Novel spatio-temporal structural information-based video quality metric*, IEEE Trans. Circuits Syst. Video Technol. **22** (2012), 989–998.
[36] Y. Zhou, C. Barnes, J. Lu, J. Yang, H. Li, *On the continuity of rotation representations in neural networks*, Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Long Beach, CA, USA (2019), 5738–5746.