Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 11(2): 3724–3746.
DOI: 10.3934/math.2026151
Received: 01 November 2025
Revised: 20 January 2026
Accepted: 26 January 2026
Published: 06 February 2026

Research article

Applications of differential Kreb algebras in security protocol analysis

Ghulam Muhiuddin[1,*], **Nabilah Abughazalah**[2] **and Manivannan Balamurugan**[3]

[1] Department of Mathematics, Faculty of Science, University of Tabuk, P.O. Box 741, Tabuk 71491, Saudi Arabia

[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

[3] Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, Tamil Nadu, India

* **Correspondence:** Email: gmuhiuddin@ut.edu.sa, chishtygm@gmail.com.

Abstract: This paper introduces differential Kreb algebras, a novel extension of Kreb algebras incorporating higher-order derivation operators, and investigates their structural properties. By defining and analyzing differential terms of the form $\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)$, we establish results on symmetry, recurrence relations, and structural identities. Core morphisms—homomorphisms, isomorphisms, and automorphisms—are developed and their preservation properties. The framework is applied to security protocol analysis, where these terms model recursive permissions, access validation, and trust propagation. Numerical examples demonstrate both blocked and successful access decisions. This bridges algebraic theory and logic-driven system design for advances in applied algebra and security verification.

Keywords: BCI-algebra; Kreb algebras; differential Kreb algebras; morphism of differential Kreb algebras
Mathematics Subject Classification: 03E72, 08A72, 22E60, 62F07, 90C70

1. Introduction

The study of algebras of type $(2, 0)$ non-empty sets equipped with a binary operation and a constant element satisfying specific axioms, has led to the development of numerous algebraic systems in mathematical logic and abstract algebra. The evolution of these algebras can be traced through several milestones in the literature. The origins of this class date back to the works of Imai and Iseki in 1966. In [1], Imai et al. introduced BCI-algebras, which were subsequently generalized by Iseki in [2] to form the broader class of BCK-algebras. These algebras were motivated by two fundamental sources: set theory and propositional calculus. In set theory, operations such as union, intersection, and set difference led to the development of Boolean algebras and distributive lattices. However, the operation of set difference and its algebraic properties were not studied systematically studied until the introduction of BCI-algebras and BCK-algebras. In propositional calculus, logical systems involving only the implicational functor, such as the positive and weak positive implicational calculi as well as BCK and BCI-systems, provided a logical motivation for these algebras. The close correspondence between set difference in set theory and implication in logic laid the foundation for the algebraic framework of BCI-algebras.

In 1983, Hu et al. [3] introduced the concept of BCH-algebras, further generalizing BCI-algebras. Later, in 1999, Neggers et al. [4] developed d-algebras, providing another algebraic extension of the BCI structure. Subsequently in 2007, Kim et al. [5] introduced BE-algebras expanding the family of BCI-type algebras. The structural properties of BE-algebras were further explored by Ahn et al. [6, 7], who investigated ideals, upper sets, and generalized upper sets. In 2019, Kim et al. [8] proposed pre-commutative algebras, enriching the family of non-classical algebraic systems derived from BE-algebras. A subsequent development was the introduction of Fenyves BCI-algebras. Jaiyeola et al. [9] examined Bol–Moufang type varieties of quasi neutrosophic triplet loops related to Fenyves BCI-algebras. This study was extended by Jaiyeola et al. in [10], where isotopy classes of such varieties were investigated. Later, Ilojide et al. [11] studied the holomorphy of Fenyves BCI-algebras, providing a deeper understanding of their algebraic structure.

In parallel, several novel algebras of type $(2, 0)$ were proposed. Ilojide introduced Obic algebras [12] and later [13], developed Torian algebras, proving that Torian algebras form a broader generalization than Obic algebras. The study of Torian algebras continued with explorations of their ideals [14], right distributive structures [15], and isomorphism theorems [16]. Additionally, Ilojide [17] investigated Nayo algebras, introducing the concepts of monics and Krib maps. Ebrahimi et al. [18] demonstrated that BCI-algebras and their generalizations can be effectively applied in coding theory, particularly in the study of ideal entropy and binary linear codes. This work sparked renewed interest in the algebraic study of logical systems. Moreover, Neggers et al. [19] analyzed Q-algebras, outlining key results that motivate further exploration of related algebraic systems in logic. Rezaei et al. [20] investigated fuzzy congruence relations on pseudo BE-algebras, while Jun [21] studied positive implicative BE-filters based on Łukasiewicz fuzzy sets, highlighting the growing intersection between fuzzy logic and algebraic structures. Additionally, the construction of (n-fold) EQ-algebras using fuzzy n-fold filters was explored by Ganji Saffar et al. [22], further expanding the scope of fuzzy algebra. Jun, Muhiuddin, and Song [23] advanced filter theory within EQ-algebras based on soft sets, reinforcing the link between algebraic frameworks and fuzzy logic methodologies.

Inspired by these developments, Ilojide introduced Kreb algebras as a generalization of BCI-algebras [24]. Kreb algebras relax certain axioms—such as associativity and symmetry—allowing the study of inference systems with non-reversible or direction-sensitive implications. This extension encompasses a broader class of logical transformations, making it applicable to real-world reasoning and dynamic logical systems. Later Ilojide proposed Differential BCI-algebras [25], which incorporate higher-order derivations to model multi-stage inference and recursive reasoning in logical deduction. Additionally, Needham et al. [26] discussed encryption for authentication in large computer networks. The present work extends this idea by formulating differential Kreb algebras, combining the structural flexibility of Kreb algebras with the expressive power of differential operations.

1.1. Objectives

The main objectives of this study are

- To define and formalize the concept of differential Kreb algebras by extending the derivational structure introduced in differential BCI-algebras to the more general Kreb framework.
- To analyze and establish key algebraic properties of these structures, including derivational symmetry, recurrence relations, and the behavior of differential terms under composition.
- To introduce and classify morphisms (homomorphisms, isomorphisms, and automorphisms) in the context of differential Kreb algebras, and to determine how these preserve or reflect differential structures.
- To develop application scenarios, particularly in access control and security protocol verification, where the differential derivations model multi-level permission evaluation and trust propagation.
- To support the theoretical development with numerical examples and simulation patterns, showcasing the practicality and logic of differential Kreb operations.

1.2. Novelty

This research introduces several new contributions:

- Extension of higher-order derivations to Kreb algebras via terms $\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)$.
- Development of symmetry and recurrence results within a non-associative logical algebraic system.
- Formalization of structure-preserving morphisms (homomorphisms, isomorphisms, automorphisms) specifically for differential Kreb algebras.
- Application of differential Kreb structures in access control and logical verification systems.

1.3. Research gap

This work addresses several unexplored areas:

- No prior literature has generalized differential derivations to the broader class of Kreb algebras.
- Existing studies on Kreb algebras lack a derivational calculus or structural symmetry framework.
- Limited work connects algebraic derivations with secure access modeling and policy logic.
- There is no established theory linking higher-order algebraic derivations to multi-stage authorization or dynamic trust propagation in security systems.

The motivation for studying differential Kreb algebras is twofold:

Theoretical: To generalize and unify structures in non-classical logic through recursive derivation terms $\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)$, which encode multi-level logical interactions.

Applied: To develop algebraic models for access control, trust evaluation, and policy propagation in secure and dynamic computational systems.

The remainder of the paper is organized as follows. Section 2 defines differential Kreb algebras and their key derivation operations. Section 3 develops the main algebraic properties, including lemmas and recurrence rules. Section 4 introduces morphisms—homomorphisms, isomorphisms, and automorphisms—and examines their preservation of differential structures. Section 5 presents real-world applications in security protocol analysis, illustrated with computational examples. Section 6 develops an algebraic analysis of the Needham–Schroeder Public-Key Protocol using differential Kreb filters. Comparison with formal methods for protocol analysis in Section 7. Section 8 concludes with a summary of findings and directions for future research.

2. Preliminaries

Definition 2.1. [25] A BCI-algebra is a non-void set $\mathcal{K}$ together with a binary operation $\rtimes : \mathcal{K}\times\mathcal{K} \to \mathcal{K}$ and a distinguished element $0 \in \mathcal{K}$, such that for all $\varpi, \zeta, \xi \in \mathcal{K}$, the following conditions hold:

(1) $((\varpi \rtimes \zeta) \rtimes (\varpi \rtimes \xi)) = \varpi \rtimes (\zeta \rtimes \xi)$ (left self-distributivity),
(2) $(\varpi \rtimes \zeta) \rtimes \zeta = \varpi \rtimes \zeta$ (right absorption),
(3) $\varpi \rtimes \varpi = 0$ (idempotent identity),
(4) $\varpi \rtimes 0 = \varpi$ (zero element property).

Definition 2.2. [24] An algebra $(\mathcal{K}; \rtimes, 0)$ is called a Kreb algebra if the following hold:

(1) $(\mathcal{K}; \rtimes, 0)$ is a BCI-algebra;
(2) $(\varpi \rtimes (\zeta \rtimes \xi)) \rtimes \varpi = \varpi \rtimes (\zeta \rtimes (\xi \rtimes \varpi))$ for all $\varpi, \zeta, \xi \in \mathcal{K}$.

The second condition is known as the Kreb identity.

Example 2.3. Consider $\mathcal{K} = \{0, 1, 2\}$ equipped with $\rtimes : \mathcal{K} \times \mathcal{K} \to \mathcal{K}$ defined by

$$\varpi \rtimes \zeta = 0 \vee \varpi - \zeta, \text{ for all } \varpi, \zeta \in \mathcal{K},$$

and the distinguished element $0 \in \mathcal{K}$.

Let $\mathcal{K} = \{0, 1, 2\}$ be a set with the Cayley table which is given in Table 1.

Table 1. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	1	2
0	0	0	0
1	1	0	1
2	2	1	0

It can be verified that $\mathcal{K}$ satisfies all the axioms of a BCI-algebra.

Next, consider the elements $\varpi = 1$, $\zeta = 2$, and $\xi = 0$. We compute the Kreb identity:

$$(\varpi \rtimes (\zeta \rtimes \xi)) \rtimes \varpi = 0$$

and

$$\varpi \rtimes (\zeta \rtimes (\xi \rtimes \varpi)) = 1.$$

Since

$$(\varpi \rtimes (\zeta \rtimes \xi)) \rtimes \varpi \neq \varpi \rtimes (\zeta \rtimes (\xi \rtimes \varpi)),$$

the Kreb identity fails for these elements.

Hence, $\mathcal{K}$ is a BCI-algebra but not a Kreb algebra.

Example 2.4. Consider a Kreb algebra $\mathcal{K} = \{0, \psi, \mu, \lambda\}$ with the Cayley table which is given in Table 2.

Table 2. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	ψ	μ	λ
0	0	ψ	μ	λ
ψ	ψ	0	λ	μ
μ	μ	λ	0	ψ
λ	λ	μ	ψ	0

It is easy to check that $\mathcal{K}$ satisfies all the axioms of a BCI-algebra. In addition, for all $\varpi, \zeta, \xi \in \mathcal{K}$, we have

$$(\varpi \rtimes (\zeta \rtimes \xi)) \rtimes \varpi = \varpi \rtimes (\zeta \rtimes (\xi \rtimes \varpi)),$$

which shows that the Kreb identity holds. Therefore, $\mathcal{K}$ is a Kreb algebra.

3. Differential Kreb algebras

Definition 3.1. Let $\mathcal{K}$ be a Kreb algebra and let $\varpi, \zeta \in \mathcal{K}$. For a non-negative integer γ, define the γ-fold Kreb-$\rtimes$ operation is recursively by

$$\varpi \rtimes \zeta^{[\gamma]} = \begin{cases} \varpi, & \text{if } \gamma = 0, \\ (\varpi \rtimes \zeta^{[\gamma-1]}) \rtimes \zeta, & \text{if } \gamma \geq 1, \end{cases}$$

where ζ is repeated γ times and $\rtimes$ denotes the binary operation of the algebra $\mathcal{K}$.

Remark 3.2. Let $\mathcal{K}$ be a Kreb algebra, and let $\varpi, \zeta \in \mathcal{K}$. For any natural number γ, the following holds:

$$\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma]}; = \underbrace{((\cdots((\varpi \rtimes (\varpi \rtimes \zeta)) \rtimes (\varpi \rtimes \zeta)) \rtimes \cdots) \rtimes (\varpi \rtimes \zeta))}_{\gamma \text{ times}},$$

where the term $(\varpi \rtimes \zeta)$ is repeated γ times in the nested operation.

Definition 3.3. Let $\mathcal{K}$ be a Kreb algebra, and let $\varpi, \zeta \in \mathcal{K}$. For any natural number $\gamma \in \mathbb{N}$, define the γ-fold Kreb-derived operation by

$$\varpi \rtimes_\gamma \zeta := \varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma]},$$

where $(\varpi \rtimes \zeta)^{[\gamma]}$ represents the γ-fold operation of the term $\varpi \rtimes \zeta$, that is,

$$(\varpi \rtimes \zeta)^{[\gamma]} = \underbrace{(\varpi \rtimes \zeta) \rtimes (\varpi \rtimes \zeta) \rtimes \cdots \rtimes (\varpi \rtimes \zeta)}_{\gamma \text{ times}}.$$

Definition 3.4. Let $\mathcal{K}$ be a Kreb algebra, and let $\mathbb{N}^*$ denote the set of non-negative integers. For elements $\varpi, \zeta \in \mathcal{K}$ and integers $\gamma, \delta \in \mathbb{N}^*$, define the differential operation $\mathcal{D}^{\gamma,\delta}$ recursively as follows:

(1) $\mathcal{D}^{0,0}(\varpi, \zeta) := \varpi \rtimes (\varpi \rtimes \zeta)$.

(2) For $\gamma, \delta \geq 0$,

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) := (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]},$$

where the right Kreb operation $(\varpi \rtimes \zeta)^{[\dot{\hat{\mathrm{n}}}]}$ is defined recursively by

$$(\varpi \rtimes \zeta)^{[0]} := \varpi, \quad (\varpi \rtimes \zeta)^{[\dot{\hat{\mathrm{n}}}]} := (\varpi \rtimes \zeta)^{[\dot{\hat{\mathrm{n}}}-1]} \rtimes \zeta, \dot{\hat{\mathrm{n}}} \geq 1.$$

(3) Similarly,

$$\mathcal{D}^{\gamma,\delta}(\zeta, \varpi) := (\zeta \rtimes (\zeta \rtimes \varpi)^{[\gamma+1]}) \rtimes (\varpi \rtimes \zeta)^{[\delta]}.$$

(4) The operations can be extended recursively as

$$\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta) := \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\varpi \rtimes \zeta),$$

$$\mathcal{D}^{\gamma,\delta+1}(\varpi, \zeta) := \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\zeta \rtimes \varpi).$$

Definition 3.5. Let $\mathcal{K}$ be a Kreb algebra. We say that $\mathcal{K}$ is a differential Kreb algebra if there exist non-negative integers $\gamma, \delta, \alpha, \beta \in \mathbb{N}^*$ such that

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi),$$

where

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) := (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]}, \quad \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) := (\zeta \rtimes (\zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}.$$

This equation is referred to as the differential form of $\mathcal{K}$, and the corresponding identity

$$(\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]} = (\zeta \rtimes (\zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}$$

is called the derivative of $\mathcal{K}$.

Example 3.6. Consider a Kreb algebra $\mathcal{K} = \{0, 1, 2\}$ with the Cayley table which is given in Table 3.

Table 3. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	1	2
0	0	1	2
1	1	0	0
2	2	0	0

This structure is a Kreb algebra. Choose $\varpi = \zeta = 1$. Then

$$\mathcal{D}^{0,0}(1, 1) = 1 \rtimes (1 \rtimes 1) = 1 \rtimes 0 = 1,$$

and

$$\mathcal{D}^{0,0}(1, 1) = 1 \rtimes (1 \rtimes 1) = 1 \rtimes 0 = 1.$$

Thus,

$$\mathcal{D}^{0,0}(\varpi, \zeta) = \mathcal{D}^{0,0}(\zeta, \varpi),$$

and so $\mathcal{K}$ is a differential Kreb algebra.

Example 3.7. Consider a Kreb Algebra $\mathcal{K} = \{0, 1, 2, 3, 4\}$ with the Cayley table which is given in Table 4.

Table 4. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	2	4	3
2	2	4	0	1	3
3	3	1	4	0	2
4	4	3	1	2	0

This structure is a Kreb algebra. For $\varpi = \zeta = 0$, we have

$$\mathcal{D}^{0,0}(0, 0) = 0 \rtimes (0 \rtimes 0) = 0 \rtimes 0 = 0,$$

and

$$\mathcal{D}^{0,0}(0, 0) = \mathcal{D}^{0,0}(0, 0) = 0.$$

Hence, $\mathcal{K}$ is a differential Kreb algebra.

Lemma 3.8. *Let $\mathcal{K}$ be a Kreb algebra. The family of differential terms*

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) := (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]}$$

satisfies the following recurrence relations for all $\gamma, \delta \in \mathbb{N}^*$:

$$\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta) = \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\varpi \rtimes \zeta), \tag{3.1}$$

$$\mathcal{D}^{\gamma,\delta+1}(\varpi, \zeta) = \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\zeta \rtimes \varpi). \tag{3.2}$$

Similarly, the terms $\mathcal{D}^{\alpha,\beta}(\zeta, \varpi)$ satisfy:

$$\mathcal{D}^{\alpha+1,\beta}(\zeta, \varpi) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) \rtimes (\zeta \rtimes \varpi), \tag{3.3}$$

$$\mathcal{D}^{\alpha,\beta+1}(\zeta, \varpi) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) \rtimes (\varpi \rtimes \zeta). \tag{3.4}$$

Proof. We first verify the recurrence for $\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta)$:

$$\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+2]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]}.$$

By Definition 3.1,

$$(\varpi \rtimes \zeta)^{[\gamma+2]} = (\varpi \rtimes \zeta)^{[\gamma+1]} \rtimes \zeta.$$

Hence,

$$\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+2]} = \varpi \rtimes ((\varpi \rtimes \zeta)^{[\gamma+1]} \rtimes \zeta).$$

Using associativity in accordance with the Kreb identity, we can write

$$\varpi \rtimes ((\varpi \rtimes \zeta)^{[\gamma+1]} \rtimes \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\varpi \rtimes \zeta).$$

Substituting back, we obtain

$$\mathcal{D}^{\gamma+1,\delta}(\varpi,\zeta) = \mathcal{D}^{\gamma,\delta}(\varpi,\zeta) \rtimes (\varpi \rtimes \zeta).$$

Next, for $\mathcal{D}^{\gamma,\delta+1}(\varpi,\zeta)$:

$$\mathcal{D}^{\gamma,\delta+1}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta+1]}.$$

Also,

$$(\zeta \rtimes \varpi)^{[\delta+1]} = (\zeta \rtimes \varpi)^{[\delta]} \rtimes (\zeta \rtimes \varpi).$$

Therefore,

$$\mathcal{D}^{\gamma,\delta+1}(\varpi,\zeta) = \mathcal{D}^{\gamma,\delta}(\varpi,\zeta) \rtimes (\zeta \rtimes \varpi).$$

The recurrence relations for $\mathcal{D}^{\alpha,\beta}(\zeta,\varpi)$ follow analogously by symmetry. This completes the proof. □

Lemma 3.9. *Let $\mathcal{K}$ be a differential Kreb algebra. Then for any $\varpi \in \mathcal{K}$,*

$$\mathcal{D}^{0,0}(\varpi,\varpi) = \varpi.$$

Proof. By Definition 3.5, we have

$$\mathcal{D}^{0,0}(\varpi,\varpi) = (\varpi \rtimes (\varpi \rtimes \varpi)^{[1]}) \rtimes (\varpi \rtimes \varpi)^{[0]}.$$

From Definition 3.4,

$$(\varpi \rtimes \varpi)^{[1]} = \varpi \rtimes \varpi, \quad (\varpi \rtimes \varpi)^{[0]} = \varpi.$$

Substituting these values gives

$$\mathcal{D}^{0,0}(\varpi,\varpi) = (\varpi \rtimes (\varpi \rtimes \varpi)) \rtimes \varpi.$$

Applying the Kreb identity, we obtain

$$(\varpi \rtimes (\varpi \rtimes \varpi)) \rtimes \varpi = \varpi \rtimes (\varpi \rtimes (\varpi \rtimes \varpi)) = \varpi.$$

Hence, $\mathcal{D}^{0,0}(\varpi,\varpi) = \varpi$. □

Lemma 3.10. *Let $\mathcal{K}$ be a differential Kreb algebra. For all $\varpi,\zeta \in \mathcal{K}$ and $\gamma,\delta \in \mathbb{N}^*$, the differential terms $\mathcal{D}^{\gamma,\delta}(\varpi,\zeta)$ satisfy the recurrence relations*

$$\mathcal{D}^{\gamma+1,\delta}(\varpi,\zeta) = \mathcal{D}^{\gamma,\delta}(\varpi,\zeta) \rtimes (\varpi \rtimes \zeta), \quad \mathcal{D}^{\gamma,\delta+1}(\varpi,\zeta) = \mathcal{D}^{\gamma,\delta}(\varpi,\zeta) \rtimes (\zeta \rtimes \varpi).$$

Proof. By Definition 3.5,

$$\mathcal{D}^{\gamma+1,\delta}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+2]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]}.$$

Using the recursive rule for the Kreb-$\rtimes$ operation,

$$(\varpi \rtimes \zeta)^{[\gamma+2]} = (\varpi \rtimes \zeta)^{[\gamma+1]} \rtimes \zeta,$$

it follows that

$$\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+2]} = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes \zeta.$$

Substituting this into $\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta)$, we obtain

$$\mathcal{D}^{\gamma+1,\delta}(\varpi, \zeta) = ((\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes \zeta) \rtimes (\zeta \rtimes \varpi)^{[\delta]} = \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\varpi \rtimes \zeta).$$

Similarly,

$$\mathcal{D}^{\gamma,\delta+1}(\varpi, \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta+1]}.$$

Also,

$$(\zeta \rtimes \varpi)^{[\delta+1]} = (\zeta \rtimes \varpi)^{[\delta]} \rtimes (\zeta \rtimes \varpi),$$

which gives

$$\mathcal{D}^{\gamma,\delta+1}(\varpi, \zeta) = \mathcal{D}^{\gamma,\delta}(\varpi, \zeta) \rtimes (\zeta \rtimes \varpi).$$

Thus, both recurrence relations are satisfied. □

Lemma 3.11. (Symmetry lemma) Let $\mathcal{K}$ be a differential Kreb algebra. If the binary operation $\rtimes$ is commutative on $\mathcal{K}$, that is,

$$\varpi \rtimes \zeta = \zeta \rtimes \varpi \quad \text{for all } \varpi, \zeta \in \mathcal{K},$$

then for all $\gamma, \delta \in \mathbb{N}^*$, the differential terms satisfy

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\gamma,\delta}(\zeta, \varpi).$$

Proof. Assume that $\rtimes$ is commutative on $\mathcal{K}$. Then, by induction on the Kreb-$\rtimes$ operation,

$$(\varpi \rtimes \zeta)^{[\dot{\hat{\mathrm{n}}}]} = (\zeta \rtimes \varpi)^{[\dot{\hat{\mathrm{n}}}]} \quad \text{for all } n \in \mathbb{N}.$$

Consequently,

$$\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]} = \varpi \rtimes (\zeta \rtimes \varpi)^{[\gamma+1]}.$$

Combining these observations, we have

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]} = (\zeta \rtimes (\zeta \rtimes \varpi)^{[\gamma+1]}) \rtimes (\varpi \rtimes \zeta)^{[\delta]} = \mathcal{D}^{\gamma,\delta}(\zeta, \varpi).$$

Hence, the differential terms are symmetric under the commutativity of $\rtimes$. □

Theorem 3.12. (Differential stability) If $\mathcal{K}$ is a differential Kreb algebra and $\varpi \rtimes \zeta = \varpi$ for all $\zeta \in \mathcal{K}$, then for any $\gamma, \delta \in \mathbb{N}^*$,

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \varpi.$$

Proof. If $\varpi \rtimes \zeta = \varpi$, then $(\varpi \rtimes \zeta)^{[\dot{\hat{\mathrm{n}}}]} = \varpi$ for all $\dot{\hat{\mathrm{n}}}$, since:

$$(\varpi \rtimes \zeta)^{[1]} = \varpi \rtimes \zeta = \varpi, \quad (\varpi \rtimes \zeta)^{[2]} = \varpi \rtimes \zeta = \varpi, \text{ etc.}$$

Hence,

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = (\varpi \rtimes \varpi) \rtimes \varpi = \varpi \rtimes \varpi = \varpi.$$

□

Remark 3.13. The stability theorem shows that elements that are idempotent or act trivially under $\rtimes$ stabilize differential expressions to fixed values.

Theorem 3.14. (Identity equivalence theorem) Let $\mathcal{K}$ be a differential Kreb algebra. For all $\varpi, \zeta \in \mathcal{K}$ and $\gamma \in \mathbb{N}^{\rtimes}$, the following equivalence holds:

$$\mathcal{D}^{\gamma,0}(\varpi,\zeta) = \mathcal{D}^{0,\gamma}(\varpi,\zeta) \iff \varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]} = (\varpi \rtimes (\varpi \rtimes \zeta)) \rtimes (\zeta \rtimes \varpi)^{[\gamma-1]}.$$

Proof. By Definition 3.5, we have

$$\mathcal{D}^{\gamma,0}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]},$$

and

$$\mathcal{D}^{0,\gamma}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)) \rtimes (\zeta \rtimes \varpi)^{[\gamma]}.$$

Equating the two expressions gives

$$(\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) = (\varpi \rtimes (\varpi \rtimes \zeta)) \rtimes (\zeta \rtimes \varpi)^{[\gamma]}.$$

Observing that $(\zeta \rtimes \varpi)^{[\gamma]}$ can be written as

$$(\zeta \rtimes \varpi)^{[\gamma]} = (\zeta \rtimes \varpi)^{[\gamma-1]} \rtimes (\zeta \rtimes \varpi),$$

and noting the common factor ϖ on the right in $\mathcal{D}^{\gamma,0}$, we may simplify to obtain

$$\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]} = (\varpi \rtimes (\varpi \rtimes \zeta)) \rtimes (\zeta \rtimes \varpi)^{[\gamma-1]}.$$

This completes the proof. □

Lemma 3.15. (Fixed point lemma) Let $\mathcal{K}$ be a differential Kreb algebra. Suppose $\varpi, \zeta \in \mathcal{K}$ satisfy

$$\varpi \rtimes (\varpi \rtimes \zeta) = \varpi \quad \text{and} \quad \zeta \rtimes \varpi = \varpi.$$

Then

$$\mathcal{D}^{1,1}(\varpi,\zeta) = \varpi.$$

Proof. By Definition 3.5, we have

$$\mathcal{D}^{1,1}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[2]}) \rtimes (\zeta \rtimes \varpi).$$

Compute the two-fold iteration:

$$(\varpi \rtimes \zeta)^{[2]} = (\varpi \rtimes \zeta)^{[1]} \rtimes \zeta = \varpi \rtimes \zeta.$$

Using the hypothesis $\varpi \rtimes (\varpi \rtimes \zeta) = \varpi$ and $\zeta \rtimes \varpi = \varpi$, we have

$$\mathcal{D}^{1,1}(\varpi,\zeta) = (\varpi \rtimes \zeta) \rtimes \varpi = \varpi \rtimes \varpi = \varpi.$$

Hence, the lemma is proved. □

Definition 3.16. Let $\mathcal{K}$ be a Kreb algebra and let $\mathbb{M} \in \mathbb{N}^*$. We say that $\mathcal{K}$ is a bounded differential Kreb algebra if there exist integers $\gamma, \delta, \alpha, \beta \in \mathbb{N}^*$ with

$$1 \leq \gamma, \delta, \alpha, \beta \leq \mathbb{M}$$

such that, for all $\varpi, \zeta \in \mathcal{K}$,

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi),$$

where

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]} \quad \text{and} \quad \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) = (\zeta \rtimes (\zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}.$$

The above identity is called the bounded differential form of $\mathcal{K}$, and the corresponding equation

$$(\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]} = (\zeta \rtimes (\zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}$$

is called the bounded derivative of $\mathcal{K}$.

Theorem 3.17. (Bounded differential Kreb algebra) Let $\mathcal{K}$ be a Kreb algebra and let $M \in \mathbb{N}^*$. If there exist fixed integers $\gamma, \delta, \alpha, \beta \leq \mathbb{M}$ such that

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) \quad \text{for all } \varpi, \zeta \in \mathcal{K},$$

then $\mathcal{K}$ is a bounded differential Kreb algebra.

Proof. Let $\mathcal{K}$ be a Kreb algebra and let $\mathbb{M} \in \mathbb{N}^*$. Assume that there exist integers $\gamma, \delta, \alpha, \beta \leq \mathbb{M}$ such that

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\alpha,\beta}(\zeta, \beta)$$

for all $\varpi, \zeta \in \mathcal{K}$, where

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\gamma]} \quad \text{and} \quad \mathcal{D}^{\alpha,\beta}(\zeta, \varpi) = (\zeta \rtimes (zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}.$$

Since the indices $\gamma, \delta, \alpha, \beta$ are bounded above by $\mathbb{M}$, the differential iterations involved in the operators $\mathcal{D}^{\gamma,\delta}$ and $D^{\alpha,\beta}$ are finite. Hence, for every pair $(\varpi, \zeta) \in \mathcal{K} \times \mathcal{K}$, the expressions $(\varpi \rtimes \zeta)^{[\gamma+1]}$, $(\zeta \rtimes \varpi)^{[\delta]}$, $(\zeta \rtimes \varpi)^{[\alpha+1]}$, and $(\varpi \rtimes \zeta)^{[\beta]}$ are well defined in $\mathcal{K}$.

By the assumed identity, we have

$$(\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]} = (\zeta \rtimes (\zeta \rtimes \varpi)^{[\alpha+1]}) \rtimes (\varpi \rtimes \zeta)^{[\beta]}$$

for all $\varpi, \zeta \in \mathcal{K}$ and for bounded indices not exceeding $\mathbb{M}$. Therefore, the differential form of $\mathcal{K}$ holds within the bounded range $\{1, 2, \ldots, \mathbb{M}\}$.

Consequently, $\mathcal{K}$ satisfies the defining condition of a bounded differential Kreb algebra. This completes the proof. □

4. Morphism of differential Kreb algebras

Definition 4.1. Let $\mathcal{K}$ and $\mathcal{L}$ be differential Kreb algebras. A map

$$\phi : \mathcal{K} \longrightarrow \mathcal{L}$$

is called a homomorphism of differential Kreb algebras if, for all $\varpi, \zeta \in \mathcal{K}$ and all $\gamma, \delta \in \mathbb{N}^*$, the following condition holds:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)).$$

Example 4.2. Consider the sets $X = \{0, a, b\}$ and $Y = \{0, 1\}$, both equipped with a Kreb algebra structure where the operation $\rtimes$ is defined as

$$\varpi \rtimes \zeta = 0 \quad \text{for all } \varpi, \zeta \in \mathcal{K} \text{ or } Y.$$

Define a map $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ by

$$\phi(0) = 0, \quad \phi(a) = 1, \quad \phi(b) = 1.$$

Then, for every $\varpi, \zeta \in \mathcal{K}$ and $k, \delta \in \mathbb{N}^{\rtimes}$, we have

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = 0 \quad \text{and} \quad \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)) = 0.$$

Thus,

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)),$$

which shows that ϕ is a homomorphism of differential Kreb algebras.

Theorem 4.3. (Preservation under homomorphism) Let $\mathcal{K}$ and $\mathcal{L}$ be differential Kreb algebras, and let $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ be a homomorphism. If for some $\varpi, \zeta \in \mathcal{K}$ and $\gamma, \delta, \alpha, \beta \in \mathbb{N}^*$, the differential identity

$$\mathcal{D}^{\gamma,\delta}(\varpi, \zeta) = \mathcal{D}^{\alpha,\beta}(\zeta, \varpi)$$

holds in $\mathcal{K}$, then the identity is preserved in $\mathcal{L}$ under ϕ, i.e.,

$$\mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)) = \mathcal{D}^{\alpha,\beta}(\phi(\zeta), \phi(\varpi)).$$

Proof. Since ϕ is a homomorphism of differential Kreb algebras, it preserves all differential terms:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)), \quad \phi(\mathcal{D}^{\alpha,\beta}(\zeta, \varpi)) = \mathcal{D}^{\alpha,\beta}(\phi(\zeta), \phi(\varpi)).$$

Applying ϕ to both sides of the given identity in $\mathcal{K}$:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \phi(\mathcal{D}^{\alpha,\beta}(\zeta, \varpi)),$$

and substituting the images, we obtain

$$\mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)) = \mathcal{D}^{\alpha,\beta}(\phi(\zeta), \phi(\varpi)),$$

which proves that the differential identity is preserved under ϕ. □

Remark 4.4. The above theorem illustrates that any homomorphism between differential Kreb algebras maintains the differential symmetry property. Consequently, the collection of differential Kreb algebras together with their homomorphisms forms a mathematically well-structured category.

Theorem 4.5. (Converse preservation condition) Let $\mathcal{K}$ and $\mathcal{L}$ be differential Kreb algebras and let $\psi : \mathcal{K} \longrightarrow \mathcal{L}$ be a function such that for all $\varpi, \zeta \in \mathcal{K}$ and all $\gamma, \delta \in \mathbb{N}^*$,

$$\mathcal{D}^{\gamma,\delta}(\psi(\varpi), \psi(\zeta)) = \psi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)).$$

Then ψ is a homomorphism of differential Kreb algebras.

Proof. By the hypothesis, the function ψ satisfies:

$$\psi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\psi(\varpi), \psi(\zeta)) \quad \text{for all } \varpi, \zeta \in \mathcal{K},\ \gamma, \delta \in \mathbb{N}^*.$$

Hence, ψ is a homomorphism of differential Kreb algebras. □

Remark 4.6. The converse shows that any map that respects the differential operation in the image is necessarily a homomorphism, highlighting a strong equivalence between structure preservation and definitional homomorphism.

Definition 4.7. A homomorphism $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ of differential Kreb algebras is called an isomorphism if it is bijective. In this case, we say that $\mathcal{K}$ and $\mathcal{L}$ are isomorphic differential Kreb algebras, denoted $\mathcal{K} \cong \mathcal{L}$.

Example 4.8. Consider a differential Kreb algebras $\mathcal{K} = \{0, \psi, \mu\}$ and $\mathcal{L} = \{0, a, b\}$ with Cayley tables which is given in Tables 5 and 6.

Table 5. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	ψ	μ
0	0	0	0
ψ	ψ	0	ψ
μ	μ	0	0

Table 6. The Cayley table for the operation $\rtimes$.

$\rtimes$	0	a	b
0	0	0	0
a	a	0	0
b	b	0	0

Define a map $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ by

$$\phi(0) = 0, \quad \phi(\psi) = a, \quad \phi(\mu) = b.$$

Then ϕ is a bijection, and for all $a, b \in \mathcal{K}$,

$$\phi(a \rtimes b) = \phi(a) \rtimes \phi(b).$$

Moreover, for all $\gamma, \delta \in \mathbb{N}^{\rtimes}$,

$$\phi(\mathcal{D}^{\gamma,\delta}(a, b)) = \mathcal{D}^{\gamma,\delta}(\phi(a), \phi(b)).$$

Hence, ϕ is an isomorphism of differential Kreb algebras.

Theorem 4.9. (Isomorphism theorem for differential Kreb algebras) Let $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ be a bijective map between differential Kreb algebras. Then ϕ is an isomorphism of differential Kreb algebras if and only if for all $\varpi, \zeta \in \mathcal{K}$ and all $\gamma, \delta \in \mathbb{N}^*$,

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)).$$

Proof. (⇒) If ϕ is an isomorphism, then by definition it is a bijective homomorphism of differential Kreb algebras, and hence:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)) \quad \text{for all } \varpi, \zeta \in \mathcal{K}.$$

(⇐) Conversely, suppose ϕ is a bijection and satisfies the condition:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)) \quad \text{for all } \varpi, \zeta \in \mathcal{K},\ \gamma, \delta \in \mathbb{N}^*.$$

Then ϕ preserves the differential structure and thus is a homomorphism. Being bijective, it follows that ϕ is an isomorphism of differential Kreb algebras. □

Definition 4.10. An automorphism of a differential Kreb algebra $\mathcal{K}$ is an isomorphism $\phi : \mathcal{K} \to \mathcal{K}$, i.e., a bijective map from $\mathcal{K}$ to itself such that for all $\varpi, \zeta \in \mathcal{K}$ and $\gamma, \delta \in \mathbb{N}^*$,

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)).$$

The set of all such automorphisms forms a group under composition, denoted Aut(X).

Example 4.11. Let $\mathcal{K} = \{0, \psi, \mu\}$ be a differential Kreb algebra with operation $\rtimes$ defined as in Table 5. Define a map $\phi : \mathcal{K} \to \mathcal{K}$ by:

$$\phi(0) = 0, \quad \phi(\psi) = \mu, \quad \phi(\mu) = \psi.$$

Then ϕ is bijective and for all $\varpi, \zeta \in \mathcal{K}$,

$$\phi(\varpi \rtimes \zeta) = \phi(\varpi) \rtimes \phi(\zeta).$$

Hence,

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)).$$

Therefore, ϕ is an automorphism of the differential Kreb algebra $\mathcal{K}$.

Theorem 4.12. (Automorphism theorem for differential Kreb algebras) Let $\mathcal{K}$ be a differential Kreb algebra and let $\phi : \mathcal{K} \to \mathcal{K}$ be a bijective map. Then ϕ is an automorphism of $\mathcal{K}$ if and only if for all $\varpi, \zeta \in \mathcal{K}$ and all $\gamma, \delta \in \mathbb{N}^*$,

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi, \zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi), \phi(\zeta)).$$

Proof. ($\Rightarrow$) If ϕ is an automorphism, then it is by definition a bijective homomorphism, so it preserves all differential terms:

$$\phi(\mathcal{D}^{\gamma,\delta}(\varpi,\zeta)) = \mathcal{D}^{\gamma,\delta}(\phi(\varpi),\phi(\zeta)).$$

($\Leftarrow$) Conversely, suppose ϕ is bijective and satisfies the condition for all $\varpi,\zeta \in \mathcal{K}$; then it preserves the structure of all differential terms, so it is an automorphism. □

Theorem 4.13. (Composition theorem for differential Kreb algebra morphisms) Let $\mathcal{K},\mathcal{L},\mathcal{M}$ be differential Kreb algebras. If $\phi : \mathcal{K} \longrightarrow \mathcal{L}$ and $\psi : \mathcal{L} \longrightarrow \mathcal{M}$ are homomorphisms of differential Kreb algebras, then their composition $\psi \circ \phi : \mathcal{K} \to \mathcal{M}$ is also a homomorphism.

Moreover,

- If ϕ and ψ are isomorphisms, then $\psi \circ \phi$ is an isomorphism.
- If $\mathcal{K} = \mathcal{L} = \mathcal{M}$ and both ϕ and ψ are automorphisms, then $\psi \circ \phi$ is an automorphism.

Proof. For any $\varpi,\zeta \in \mathcal{K}$ and $\gamma,\delta \in \mathbb{N}^*$:

$$(\psi \circ \phi)(\mathcal{D}^{\gamma,\delta}(\varpi,\zeta)) = \psi(\phi(\mathcal{D}^{\gamma,\delta}(\varpi,\zeta))) = \psi(\mathcal{D}^{\gamma,\delta}(\phi(\varpi),\phi(\zeta))) = \mathcal{D}^{\gamma,\delta}(\psi(\phi(\varpi)),\psi(\phi(\zeta))).$$

So $\psi \circ \phi$ is a homomorphism.

If ϕ and ψ are bijective, then their composition is bijective, so $\psi \circ \phi$ is an isomorphism.

If $\mathcal{K} = \mathcal{L} = \mathcal{M}$, then ϕ and ψ are automorphisms, and their composition is also an automorphism of $\mathcal{K}$. □

5. Application of security protocol analysis using differential Kreb algebras

Differential Kreb algebras can be applied to model and analyze access permissions and information flows in security protocols. In such contexts, elements of the algebra represent access rights, while the operation $\rtimes$ and the derived terms $\mathcal{D}^{\gamma,\delta}(\varpi,\zeta)$ capture dynamic rules for permission propagation and conditional access.

In a network security protocol, γ models the strength of authentication and trust establishment among network entities, while δ captures adversarial or environmental disturbances such as message delay, interception, or replay attacks. These parameters jointly characterize secure state evolution under realistic network conditions.

Definition 5.1. (Differential Kreb filter) Let $\mathcal{K}$ be a differential Kreb algebra over a set of protocol state elements. A differential Kreb filter is a mapping

$$\mathcal{F} : \mathcal{K} \times \mathcal{K} \to \mathcal{K}$$

such that for any consecutive state expressions $E_i, E_{i+1} \in \mathcal{K}$,

$$\mathcal{F}(E_i, E_{i+1}) = \Delta(E_{i+1}) \ominus \Delta(E_i),$$

where $\Delta(\rtimes)$ is the differential operator in $\mathcal{K}$ and $\ominus$ is the inverse of the algebraic operation $\oplus$.

5.1. Modeling permission propagation

Suppose $\mathcal{K}$ represents a base permission (e.g., read access), and ζ represents a condition or policy (e.g., authentication token). Then, the differential term:

$$\mathcal{D}^{\gamma,\delta}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[\gamma+1]}) \rtimes (\zeta \rtimes \varpi)^{[\delta]}$$

can model a rule where access is granted after $\gamma + 1$ nested evaluations of a token and δ reflections of token validation against existing credentials.

5.2. Security policy symmetry

A protocol may require that access policies be symmetric (mutually valid) between components A and B. The differential symmetry condition:

$$\mathcal{D}^{\gamma,\delta}(\varpi,\zeta) = \mathcal{D}^{\alpha,\beta}(\zeta,\varpi)$$

expresses this balance. If it holds, neither party has a privileged view of the other, a desirable property in peer-to-peer systems.

5.3. Authentication and trust chains

In trust chain analysis, repeated derivations represent the flow of trust. For example:

$$\mathcal{D}^{3,2}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[4]}) \rtimes (\zeta \rtimes \varpi)^{[2]}$$

might represent that user ϖ is granted elevated access after four iterations of delegation through the user ζ, followed by two validation responses.

5.4. Numerical example: Blocked access

Let $\mathcal{K} = \{0, \psi, \mu\}$ be a differential Kreb algebra with the cayley table which is given in Table 5. Let $\varpi = \psi$ (read permission), $\zeta = \mu$ (authentication token), and compute:

$$\mathcal{D}^{1,1}(\varpi,\zeta) = (\varpi \rtimes (\varpi \rtimes \zeta)^{[2]}) \rtimes (\zeta \rtimes \varpi).$$

We compute step by step:

$$\begin{aligned}
\varpi \rtimes \zeta &= \psi \rtimes \mu = 0, \\
(\varpi \rtimes \zeta)^{[2]} &= (\varpi \rtimes \zeta) \rtimes \zeta = 0 \rtimes \mu = 0, \\
\varpi \rtimes (\varpi \rtimes \zeta)^{[2]} &= \psi \rtimes 0 = 0, \\
\zeta \rtimes \varpi &= \mu \rtimes \psi = 0, \\
\Rightarrow \mathcal{D}^{1,1}(\varpi,\zeta) &= 0 \rtimes 0 = 0.
\end{aligned}$$

This indicates that under the current token structure, access cannot be escalated, representing a blocked permission path.

5.5. *Numerical example: Successful access escalation*

Consider a differential Kreb algebra $\mathcal{K} = \{0, \psi, \mu\}$ with the Cayley table which is given in Table 7.

Table 7. The Cayley table for the operation $\rtimes\!\!\!\ltimes$.

$\rtimes\!\!\!\ltimes$	0	ψ	μ
0	0	0	0
ψ	ψ	0	0
μ	μ	0	0

Let $\varpi = \psi$ and $\zeta = \mu$, and compute:

$$\mathcal{D}^{1,1}(\varpi, \zeta) = (\varpi \rtimes\!\!\!\ltimes (\varpi \rtimes\!\!\!\ltimes \zeta)^{[2]}) \rtimes\!\!\!\ltimes (\zeta \rtimes\!\!\!\ltimes \varpi).$$

Now

$$\begin{aligned}
\psi \rtimes\!\!\!\ltimes \mu &= 0, \\
(\psi \rtimes\!\!\!\ltimes \mu)^{[2]} &= 0 \rtimes\!\!\!\ltimes 0 = 0, \\
\psi \rtimes\!\!\!\ltimes (\psi \rtimes\!\!\!\ltimes \mu)^{[2]} &= \psi \rtimes\!\!\!\ltimes 0 = \psi, \\
\mu \rtimes\!\!\!\ltimes \psi &= 0, \\
\Rightarrow \mathcal{D}^{1,1}(\psi, \mu) &= \psi \rtimes\!\!\!\ltimes 0 = \psi.
\end{aligned}$$

Thus,

$$\mathcal{D}^{1,1}(\psi, \mu) = \psi \neq 0.$$

This indicates that, under the current token structure, access can be escalated.

6. Algebraic analysis of the Needham–Schroeder public-key protocol using differential Kreb filters

To demonstrate the practical applicability of the proposed differential Kreb algebra framework, we apply it to the classical Needham–Schroeder public-key protocol [26]. This protocol well known for its susceptibility to a man-in-the-middle attack, providing an excellent test case for demonstrating the framework's capability to identify subtle structural weaknesses.

6.1. *Protocol overview*

The simplified steps of the Needham–Schroeder public-key protocol between two principals A and B are:

(1) $A \to B : \{N_A, A\}_{K_B}$,
(2) $B \to A : \{N_A, N_B\}_{K_A}$,
(3) $A \to B : \{N_B\}_{K_B}$,

where N_A and N_B are nonces, and K_A and K_B are the public keys of A and B, respectively.

6.2. *Mapping protocol states to differential Kreb filters*

We represent each protocol state E_i as an algebraic expression in the differential Kreb algebra $\mathcal{K}$. For instance:

$$\begin{aligned} E_1 &= \text{encrypt}(N_A \oplus A, K_B), \\ E_2 &= \text{encrypt}(N_A \oplus N_B, K_A), \\ E_3 &= \text{encrypt}(N_B, K_B). \end{aligned}$$

The differential Kreb filter $\mathcal{F}(E_i, E_{i+1})$ captures the change between consecutive states:

$$\begin{aligned} \mathcal{F}_{1,2} &= \Delta(E_2) \ominus \Delta(E_1) = \Delta(N_B) \ominus \Delta(A), \\ \mathcal{F}_{2,3} &= \Delta(E_3) \ominus \Delta(E_2) = \Delta(N_B) \ominus \Delta(N_A). \end{aligned}$$

6.3. *Detection of vulnerability*

Using the differential filters, we observe the following:

- $\mathcal{F}_{1,2}$ indicates that the nonce N_B introduced by B is algebraically independent of the initial message from A. This differential change can be exploited by an attacker to interpose messages, corresponding to the classical "man-in-the-middle attack" discovered by Lowe (1995).
- $\mathcal{F}_{2,3}$ shows that N_B is returned without proper binding to the origin of N_A. The algebraic difference highlights a potential "authentication breach", as an intruder can replay N_B to impersonate B.
- By systematically tracking these differentials, the framework identifies "structural vulnerabilities" that may be overlooked in purely symbolic or belief-based analyses.

This example demonstrates how the differential Kreb algebra framework can:

(1) Map protocol messages to algebraic expressions.
(2) Track state transitions using differential Kreb filters.
(3) Identify known vulnerabilities, such as man-in-the-middle attacks, in a systematic, algebraic manner.

7. Comparison with established formal methods for protocol analysis

In the security protocol literature, several well-established formal methods have been proposed to model and analyze cryptographic protocols. These methods differ substantially in their modeling assumptions, expressive power, and verification mechanisms. Accordingly, this section, we systematically compare the proposed Kreb algebra–based framework with representative and widely adopted approaches, including the Dolev–Yao model, BAN logic, and automated verification tools such as ProVerif and the Tamarin prover.

7.1. *Dolev–Yao model*

The Dolev–Yao model is a symbolic adversary framework in which cryptographic primitives are treated as idealized black boxes and messages are represented as algebraic terms. The adversary is assumed to have complete control over the communication network, allowing interception, modification replay, and fabrication of messages, subject only to the algebraic rules governing the cryptographic operations.

The proposed Kreb algebra–based approach also relies on algebraic abstractions, but places greater emphasis on the structural and operational relations defined intrinsically within the algebra itself. Whereas the Dolev–Yao model focuses primarily on explicit adversarial capabilities and term-rewriting rules, the Kreb algebra framework facilitates the analysis of algebraic invariants and internal state transformations of protocol states. Nonetheless, to fully conform to the Dolev–Yao threat model, explicit adversarial behaviors and attack rules must be formally embedded within the algebraic structure.

7.2. BAN logic

BAN logic is a belief-based formal logic designed to reason about authentication properties of cryptographic protocols. It models how the beliefs of protocol participants evolve after each message exchange, using modal operators to represent trust, freshness, and key ownership.

In contrast to BAN logic, which is primarily concerned with epistemic reasoning, the Kreb algebra–based framework focuses on algebraic relations and operational semantics of protocol components. Consequently, the proposed approach is better suited to capturing algebraic dependencies and structural properties, whereas BAN logic excels at expressing and verifying belief-driven authentication goals. The two approaches are therefore orthogonal and potentially complementary.

7.3. ProVerif and Tamarin prover

ProVerif and the Tamarin prover are widely adopted automated tools for the formal verification of security protocols under the symbolic model. ProVerif relies on Horn clause resolution and supports unbounded session analysis, while Tamarin provides rule-based protocol modeling with support for rich equational theories and interactive, human guided proofs.

The Kreb algebra framework, in contrast is primarily theoretical and algebraic in nature, offering strong mathematical rigor and structural insight but currently lagging direct automation support. Nevertheless, the algebraic rules, identities, and derivation operators of Kreb algebras could potentially be encoded as equational theories or rewrite rules within tools such as Tamarin, thereby bridging the gap between abstract combining algebraic expressiveness and practical automated verification capabilities.

7.4. Summary of comparison

Table 8 summarizes the key differences between the proposed Kreb algebra–based approach and existing formal methods.

Table 8. Comparison of formal methods for security protocol analysis.

Aspect	Dolev–Yao	BAN logic	ProVerif/ Tamarin	Kreb algebra
Modeling style	Symbolic terms	Belief logic	Symbolic + equational	Algebraic relations
Adversary model	Explicit, strong	Implicit	Explicit, strong	Model-dependent
Automation	Limited	None	High	Limited
Primary focus	Attacks and secrecy	Authentication beliefs	Automated verification	Structural invariants
Main strength	Clear attacker model	Epistemic reasoning	Scalability and tools	Algebraic expressiveness
Main limitation	Limited algebraic depth	Misses algebraic flaws	Complex modeling	Lack of automation

Therefore, the proposed Kreb algebra–based framework complements established security protocol analysis methods, such as the Dolev–Yao model, BAN logic, and ProVerif/Tamarin, by providing a rigorous algebraic characterization of protocol structures and state transformations.

7.5. Limitations of the proposed framework

Although the differential Kreb algebra framework provides a rigorous algebraic foundation for security protocol analysis, it exhibits certain inherent limitations.

- **Side-channel attacks:** The proposed model is symbolic and algebraic in nature and does not account for implementation-level side-channel attacks such as timing analysis, power consumption, or electromagnetic leakage.
- **Probabilistic behavior:** The framework is primarily deterministic and therefore cannot effectively model probabilistic aspects of protocols, including randomized encryption, nonce generation, or stochastic adversarial behavior.
- **Adversary modeling:** The approach does not explicitly incorporate a strong adversary model, such as the Dolev–Yao adversary with full control over the communication network, which may limit its applicability in highly adversarial environments.
- **Lack of automation:** Unlike established verification tools such as ProVerif or the Tamarin prover, the proposed framework does not currently provide automated verification or counterexample generation.
- **Scalability and practical complexity:** The framework is better suited for theoretical analysis and may face challenges when applied to large-scale, real-world protocols involving concurrency,

multiple sessions, or complex message structures.

8. Conclusions

This paper has established the foundational framework of differential Kreb algebras by introducing higher-order derivations and analyzing their behavior through a range of algebraic constructions. We defined a generalized derivative operator $\mathcal{D}^{\gamma,\delta}(\varpi,\zeta)$ and derived key results on symmetry, recurrence relations, and derivation identities. We systematically investigated homomorphisms, isomorphisms, and automorphisms of differential Kreb algebras, demonstrating that these morphisms preserve differential identities and form well-structured algebraic systems. These results contribute to a deeper theoretical understanding of algebraic transformations within non-classical logical frameworks.

From an applied perspective, differential Kreb algebras were shown efficiently model security protocol behaviors, including recursive permission structures, policy symmetry, and trust-validation chains. Illustrative numerical examples demonstrated how access-control decisions—both blocked and successful—can be derived algebraically, and a simulation framework was outlined for potential dynamic implementations.

The proposed Kreb algebra complements existing security-protocol analysis techniques, such as the Dolev–Yao model, BAN logic, and ProVerif/Tamarin by providing a rigorous algebraic interpretation of protocol structure and state transformations. While existing approaches primarily emphasize adversary modeling or automated verification, Kreb algebras offer deeper structural insight and can be naturally integrated with automated analysis tools in future work. Finally, the notion of differential operators introduced here can be extended to other non-classical algebraic structures, such as BCI-algebras, BCK-algebras, KU-algebras, BE-algebras, and d-algebras.

Author contributions

Ghulam Muhiuddin: Conceptualization, methodology, writing–original draft preparation and supervision. Nabilah Abughazalah: Conceptualization, methodology, writing–review suggestions and editing. Manivannan Balamurugan: Conceptualization, methodology, writing–original draft preparation. All authors have read and agreed to the published version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Funding

The authors extend their appreciation to Princess Nourah Bint Abdulrahman University Researchers Supporting Project Number (PNURSP2026R87), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflict of interest

We declare that we have no conflicts of interest.

Acknowledgments

The authors would like to express their sincere thanks to the anonymous referees for their valuable comments and suggestions, which improved the paper significantly. Moreover, the authors extend their appreciation to Princess Nourah Bint Abdulrahman University Researchers Supporting Project Number (PNURSP2026R87), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

References

1. Y. Imai, K. Iseki, On axiom system of propositional calculi, XIV, *Proc. Japan Acad.*, **42** (1966), 19–22. https://doi.org/10.3792/pja/1195522169
2. K. Iseki, An algebra related with propositional calculus, *Proc. Japan Acad.*, **42** (1966), 26–29. https://doi.org/10.3792/pja/1195522171
3. Q. P. Hu, X. Li, On BCH-algebras, *Math. Semin. Notes*, **11** (1983), 313–320.
4. J. Neggers, H. S. Kim, On d-algebras, *Math. Slovaca*, **49** (1999), 19–26.
5. H. S. Kim, Y. H. Kim, On BE-algebras, *Sci. Math. Jpn.*, **66** (2007), 113–116. https://doi.org/10.32219/isms.66.1_113
6. S. S. Ahn, K. S. So, On ideals and upper sets in BE-algebras, *Sci. Math. Jpn.*, **68** (2008), 351–357.
7. S. S. Ahn, K. S. So, On generalized upper sets in BE-algebras, *Bull. Korean Math. Soc.*, **46** (2009), 281–287. https://doi.org/10.4134/BKMS.2009.46.2.281
8. H. S. Kim, J. Neggers, S. S. Ahn, On pre-commutative algebras, *Mathematics*, **7** (2019), 336. https://doi.org/10.3390/math7040336
9. T. G. Jaiyeola, E. Ilojide, M. O. Olatinwo, F. Smarandache, On the classification of Bol-Moufang type of some varieties of quasi neutrosophic triplet loops (Fenyves BCI-algebras), *Symmetry*, **10** (2018), 427. https://doi.org/10.3390/sym10100427
10. T. G. Jaiyeola, E. Ilojide, A. J. Saka, K. G. Ilori, On the isotopy of some varieties of Fenyves quasi neutrosophic triplet loops (Fenyves BCI-algebras), *Neutrosophic Sets Syst.*, **31** (2020), 200–223.
11. E. Ilojide, T. G. Jaiyeola, M. O. Olatinwo, On holomorphy of Fenyves BCI-algebras, *J. Niger. Math. Soc.*, **38** (2019), 139–155.
12. E. Ilojide, On Obic algebras, *Int. J. Math. Combin.*, **4** (2019), 80–88.
13. E. Ilojide, A note on Torian algebras, *Int. J. Math. Combin.*, **2** (2020), 80–87.
14. E. Ilojide, On ideals of Torian algebras, *Int. J. Math. Combin.*, **2** (2020), 101–108.
15. E. Ilojide, On right distributive Torian algebras, *Int. J. Math. Combin.*, **4** (2020), 100–107.
16. E. Ilojide, On isomorphism theorems of Torian algebras, *Int. J. Math. Combin.*, **1** (2021), 56–61.
17. E. Ilojide, Monics and Krib maps in Nayo algebras, *J. Niger. Math. Soc.*, **40** (2021), 1–16.
18. M. Ebrahimi, A. Izadara, The ideal entropy of BCI-algebras and its application in binary linear codes, *Soft Comput.*, **23** (2019), 39–57. https://doi.org/10.1007/s00500-018-3620-0
19. J. Neggers, S. A. Sun, H. S. Kim, On Q-algebras, *Int. J. Math. Math. Sci.*, **27** (2001), 749–757. https://doi.org/10.1155/S0161171201006627

20. A. Rezaei, A. Borumand Saeid, Q. Zhan, Fuzzy congruence relations on pseudo BE-algebras, *J. Algebraic Hyperstruct. Log. Algebras*, **1** (2020), 31–43. https://doi.org/10.29252/HATEF.JAHLA.1.2.4

21. Y. B. Jun, Positive implicative BE-filters of BE-algebras based on Lukasiewicz fuzzy sets, *J. Algebraic Hyperstruct. Log. Algebras*, **4** (2023), 1–11. https://doi.org/10.61838/KMAN.JAHLA.4.1.1

22. B. Ganji Saffar, G. Muhiuddin, M. Aaly Kologani, R. A. Borzooei, Construction of (n-fold) EQ-algebras by using fuzzy n-fold filters, *New Math. Nat. Comput.*, **17** (2021), 827–851. https://doi.org/10.1142/S179300572150040X

23. Y. B. Jun, S. Z. Song, G. Muhiuddin, Filter theory in EQ-algebras based on soft sets, *Quasigroups Relat. Syst.*, **24** (2016), 25–32.

24. E. Ilojide, On Kreb algebras, *J. Algebraic Hyperstruct. Log. Algebras*, **5** (2024), 169–182. https://doi.org/10.61838/kman.jahla.5.2.14

25. E. Ilojide, Differential BCI algebras, *Int. J. Math. Anal. Model.*, **8** (2025), 14–21.

26. R. Needham, M. Schroeder, Using encryption for authentication in large networks of computers, *Commun. ACM*, **21** (1978), 993–999. https://doi.org/10.1145/359657.35965