Palestine Journal of Mathematics

Vol 15(1)(2026) , 723–737

A Secret Sharing Scheme Constructed from LCD Codes over the Ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$

Ouarda Haddouche, Karima Chatouh and Sassia Makhlouf

Communicated by: Manoj Patel

MSC 2010 Classifications: Primary 11TXX; Secondary 11T71, 14G50.

Keywords and phrases: LCD Codes over the Ring, Secret sharing scheme, Multi-secret sharing scheme, Participants, Hash function

The author expresses appreciation to the reviewers and editor for their insightful feedback and valuable suggestions, which contributed to improving the quality of the paper.

Corresponding Author: Karima Chatouh

Abstract Data privacy is a vital issue in today's digital communication landscape, playing a key role in areas such as secure messaging and cloud storage. Secret sharing plays a fundamental role in this context by dividing a confidential secret into multiple *shares*, such that only authorized subsets of participants defined by an access structure can reconstruct the secret. In a typical (k, n)-threshold scheme, at least k out of n shares are required for recovery, ensuring confidentiality against smaller coalitions. Coding-theoretic approaches, particularly those based on *linear codes*, offer efficient constructions for such schemes. However, identifying minimal codewords remains a computational challenge. To address this, we propose a perfect secret-sharing scheme based on *linear complementary dual (LCD) codes*, which feature disjoint intersections with their duals, simplifying decoding and enhancing security. Additionally, we incorporate a cryptographic one-way hash function to authenticate participants during the reconstruction phase, facilitating cheater detection and ensuring data integrity. Our analysis shows that the scheme balances efficiency and robustness, making it suitable for secure, scalable, and practical implementations.

1 Introduction

Over the past few decades, coding theory has played a pivotal role in various areas of modern cryptography, particularly in public-key cryptosystems and a wide range of applications such as e-cash systems, electronic voting, distributed authentication, and secure cloud storage. One of the persistent challenges in public-key infrastructure is efficient and secure key management. Verifying that private keys are safely shared and stored is key to keeping these systems secure and trustworthy.

Secret Sharing Schemes (SSSs) were developed as cryptographic methods that allow a dealer to split a secret s into multiple pieces, known as *shares*, and distribute them among a set of participants $P = \{P_1, P_2, \ldots, P_n\}$. The central idea is that only specific, authorized groups of participants-referred to as *access structures*-can come together to reconstruct the original secret. Unauthorized groups, on the other hand, gain no information about it.

In 1979, two pioneering secret-sharing methods were introduced separately by Blakley [7] and Shamir [33]. Shamir's scheme is based on algebra, using Lagrange interpolation over finite fields, while Blakley's method takes a geometric approach involving hyperplane intersections. Both are classified as *perfect* schemes because they ensure complete secrecy from any unauthorized subset.

Secret sharing has since found applications in diverse domains, including secure multiparty

computation, protection of cryptographic keys in ad hoc networks, control over access to financial and military systems, and fault-tolerant data recovery. The classical (k, n)-threshold scheme is a specific type of SSS where the secret is distributed among n participants in such a way that any subset of size at least k can recover the secret, a subset of fewer than k participants cannot.

In practical situations, it is commonly necessary to distribute several secrets at once rather than just one. Need led to the development of Multi-Secret Sharing Schemes (MSSSs), where several secrets are shared among the same group of participants. A robust MSSS ensures that an authorized subset can recover all or some of the secrets while maintaining the privacy of the missing ones. Various MSSSs have been presented over the years [2, 3, 5, 9, 10, 11, 12, 13, 14, 15, 16, 17, 34], offering improved efficiency, enhanced security, and support for general access structures.

In 1993, Massey [27, 28] pioneered the application of linear codes to the construction of secret-sharing schemes by linking minimal codewords of a linear code to the access structures of such schemes. Later, Massey [29] expanded this approach by exploring the application of dual codes in cryptography. Building on this, Ding et al. [22, 23] introduced sufficient conditions to identify minimal codewords of specific linear codes, which are crucial in defining the authorized access sets.

Subsequent research brought several innovations: Dougherty et al. [25] used self-dual codes and combinatorial techniques to explore access structures. Bai [5, 6] designed a threshold MSSS based on matrix projection techniques. Das and Adhikari [21] employed one-way hash functions to construct multi-secret sharing schemes (MSSSs) with general access structures, facilitating verification by participants and the combiner. Chum and Zhang [20] presented an ideal and perfect threshold scheme incorporating cryptographic hash functions and herding techniques.

Later, Çalkavur and Solé [8] introduced an MSSS based on error-correcting codes, where secret reconstruction relied on bounded distance decoding. Pilaram and Eghlidos [31] proposed a lattice-based MSSS built on lattice problems, enabling selective recovery of secrets across multiple stages. Ding et al. [24] leveraged dual Golay codes and design theory to develop an MSSS with explicitly determined minimal access structures.

These works highlight the critical role of coding theory in enhancing the security and functionality of secret-sharing schemes. In particular, linear codes offer error detection and correction capabilities, which can be put to improve robustness against cheating and ensure secure reconstruction.

Motivated by these advancements, this article introduces a novel (k, n)-threshold MSSS constructed using Linear Complementary Dual (LCD) codes over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, and enhanced by the incorporation of a cryptographic one-way hash function. The LCD codes ensure structural properties conducive to efficient error detection and low-complexity implementation, making the scheme suitable for resource-constrained environments such as embedded systems.

An aspect of the proposed scheme is its inherent cheater detection mechanism, made possible by the collision-resistant nature of the hash function. Only authorized participants can effectively contribute to the secret reconstruction, while any dishonest behavior is readily detected by the dealer.

The rest of this article is structured as follows: Section 2 and 3 provides necessary preliminaries on hash functions, linear codes, LCD codes, and the general of secret sharing. In Section 4, we detail the construction of the proposed scheme and provide a concrete example. Section 5 presents a thorough security and performance analysis. Finally, we conclude our work and outline future directions in Section 6.

2 Preliminaries

Let $\mathbb{F}_p$ be a finite field with p elements, where p is a prime number. Define the indeterminate u such that $u^5 = 0$. The ring $\mathcal{R}$ is then defined as: $\mathcal{R} = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p + u^4\mathbb{F}_p = \sum_{i=0}^{4} u^i \mathbb{F}_p$, where addition and multiplication are carried out modulo $u^5 = 0$.

Each element $r \in \mathcal{R}$ can be uniquely written as:

$$r = a_0 + a_1 u + a_2 u^2 + a_3 u^3 + a_4 u^4, \quad \text{where } a_i \in \mathbb{F}_p. \tag{2.1}$$

This ring $\mathcal{R}$ is a finite commutative local ring with unity. It is a **finite chain ring**, meaning that its ideals are linearly ordered by inclusion. The maximal ideal is generated by the nilpotent element u, and we have the following chain of ideals:

$$\mathcal{R} \supset u\mathcal{R} \supset u^2\mathcal{R} \supset u^3\mathcal{R} \supset u^4\mathcal{R} \supset \{0\}. \tag{2.2}$$

The cardinality of $\mathcal{R}$ is:

$$|\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p| = p^5. \tag{2.3}$$

This ring is widely used in coding theory due to its rich algebraic structure, particularly for constructing linear codes with desirable properties such as LCD (linear complementary dual) codes and self-dual codes.

Let $\mathbb{F}_p$ be a finite field with p elements, and define the finite commutative chain ring $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$, where $u^5 = 0$ and u is an indeterminate. Each element $r \in \mathcal{R}$ can be uniquely expressed as:

$$r = a_0 + a_1u + a_2u^2 + a_3u^3 + a_4u^4, \quad \text{where } a_i \in \mathbb{F}_p.$$

2.1 Gray Map over $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$

The **Gray map** is a linear and distance-preserving map from $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$ to $\mathbb{F}_p^5$ defined component-wise. Specifically, the Gray map $\Phi : \mathcal{R} \to \mathbb{F}_p^5$ is given by:

$$\Phi(r) = \Phi(a_0 + a_1u + a_2u^2 + a_3u^3 + a_4u^4) = (a_0, a_1, a_2, a_3, a_4). \tag{2.4}$$

This map can be extended naturally to vectors in $\mathcal{R}^n$ by applying Φ component-wise:

$$\Phi : \mathcal{R}^n \to \mathbb{F}_p^{5n}, \quad \Phi((r_1, r_2, \ldots, r_n)) = (\Phi(r_1), \Phi(r_2), \ldots, \Phi(r_n)). \tag{2.5}$$

2.2 Gray Images of Codes over $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$

Let C be a linear code of length n over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$. The **Gray image** of C, denoted $\Phi(C)$, is the image of C under the Gray map:

$$\Phi(C) = \{\Phi(c) \mid c \in C\} \subseteq \mathbb{F}_p^{5n}.$$

The Gray image $\Phi(C)$ is a linear code over $\mathbb{F}_p$ of length $5n$, and it preserves many structural properties of the original code C, including its Hamming distance. In particular, if C is an LCD code over $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$, then $\Phi(C)$ inherits useful properties that can be exploited in cryptographic applications such as secret sharing and authentication.

Remark 2.1. The Gray map is especially useful in transforming ring-based constructions into field-based counterparts, enabling the application of classical linear code theory over finite fields.

3 Codes over the Ring $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$ and Their Role in Secret Sharing

Let $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$ be a finite commutative chain ring with unity, where $u^5 = 0$ and $\mathbb{F}_p$ is a finite field with p elements, for a prime p. The ring $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$ is a local principal ideal ring of characteristic p, with maximal ideal $\langle u\rangle$ and residue field $\mathcal{R}/\langle u\rangle \cong \mathbb{F}_p$. Let n be a positive integer. An $\mathcal{R}$-linear code C of length n is defined as a submodule of the free $\mathcal{R}$-module $\mathcal{R}^n$. That is, $C \subseteq \mathcal{R}^n$ such that C is an $\mathcal{R}$-submodule. The code C is called an $[n, k, d]$-*linear code* over $\mathcal{R} = \sum_{i=0}^{4} u^i\mathbb{F}_p$ if the rank of C as an $\mathcal{R}$-module is k, and d denotes the minimum Hamming

distance between any two distinct codewords in C. The Hamming weight of a codeword $c = (c_1, c_2, \ldots, c_n) \in C$, denoted by $\mathrm{wt}(c)$, is defined as the number of non-zero coordinates in c, i.e.,

$$\mathrm{wt}(c) = |\{i \in \{1, 2, \ldots, n\} \mid c_i \neq 0\}|. \tag{3.1}$$

Let A_i denote the number of codewords in C having Hamming weight exactly i. Then the vector $A = (A_0, A_1, \ldots, A_n)$ is referred to as the *weight distribution* of C, and the set of non-zero indices is defined as:

$$S = \{i \in \{0, 1, \ldots, n\} \mid A_i \neq 0\}. \tag{3.2}$$

The *dual code* $C^\perp$ of C is defined with respect to the standard inner product on $\mathcal{R}^n$: $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i, \quad$ for $x, y \in \mathcal{R}^n$. Then

$$C^\perp = \{x \in \mathcal{R}^n \mid \langle x, y\rangle = 0 \text{ for all } y \in C\}. \tag{3.3}$$

The dual $C^\perp$ is also an $\mathcal{R}$-linear code of length n.

A code C is said to be a *Linear Complementary Dual (LCD)* code over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ if: $C \cap C^\perp = \{0\}$. This condition implies that the code and its dual share only the trivial codeword. LCD codes offer resistance to certain types of attacks in secure communication systems and are suitable for constructing cryptographically secure protocols. Let G be a generator matrix for C of size $k \times n$, and let H be a generator matrix of $C^\perp$ of size $(n-k) \times n$. Then, the orthogonality conditions imply: $GH^T = 0 \quad$ and $\quad HG^T = 0$, where G^T and H^T denote the transposes of G and H, respectively. A necessary and sufficient condition for a linear code C over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ to be LCD is that the matrix GG^T is invertible over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ [27, 32]. Moreover, the block matrix

$$\mathcal{D} = \begin{pmatrix} G \\ H \end{pmatrix} \tag{3.4}$$

is invertible if and only if C is LCD. These algebraic properties of LCD codes are crucial in designing efficient and secure secret sharing schemes.

3.1 Secret Sharing Concepts over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$

Secret sharing is a cryptographic protocol in which a secret is divided into multiple shares and distributed among participants. The scheme ensures that only authorized subsets of participants can collaboratively reconstruct the secret, while unauthorized subsets gain no information about it. Such schemes are defined by a triplet (P, Γ, S), where P denotes the set of participants, Γ represents the access structure, and S is the secret. The fundamental components of a secret sharing scheme include the following: **Shares**, which are elements of $\mathcal{R}^t$ (typically with $t \geq 1$) distributed to participants by the Dealer based on a specific coding method; the **Dealer**, who is a trusted entity responsible for generating the secret and assigning shares by the access structure; and the **Access Structure** Γ, which consists of all qualified subsets of participants that can jointly reconstruct the secret. A subset is called a *minimal access set* if any participant from it results in an unauthorized set. The **Information Rate** of a scheme, defined as $\rho = \dfrac{\text{length of the secret}}{\text{length of the share}}$, quantifies its efficiency-higher values indicate more storage-efficient schemes. A **Perfect Secret Sharing Scheme** ensures that every unauthorized subset of participants has zero mutual information with the secret, meaning they have no probabilistic advantage in guessing it. Furthermore, a **Perfect Scheme** is said to be **Ideal** if its information rate is $\rho = 1$, i.e., each share is the same size as the secret.

3.2 Hash Functions and Their Role

To verify the authenticity of shares during the secret reconstruction phase, a cryptographic hash function $H : \{0,1\}^* \to \{0,1\}^\xi$ is in the scheme. The function H satisfies the following security

properties:

1. **Preimage Resistance:** Given a hash output h, it is computationally infeasible to find an input x such that $H(x) = h$.
2. **Second Preimage Resistance:** Given an input x, it is hard to find a distinct input $x' \neq x$ such that $H(x') = H(x)$.
3. **Collision Resistance:** It is computationally infeasible to find two distinct inputs $x \neq x'$ such that $H(x) = H(x')$.

Example 3.1. Suppose a dealer wants to distribute a secret using a secret-sharing scheme and ensure that the shares received by participants are authentic. Let s be the secret and let $s_1, s_2, \ldots, s_n$ be the shares given to participants $P_1, P_2, \ldots, P_n$. For each share s_i, the dealer computes a hash value $h_i = H(s_i)$ and publicly publishes the tuple (P_i, h_i). During the reconstruction phase, each participant submits their share s_i'. The dealer (or any verifier) checks the validity of each submitted share by computing $H(s_i')$ and verifying whether it matches the corresponding published hash value h_i. If $H(s_i') = h_i$, the share is considered authentic; otherwise, it is rejected as tampered or invalid. This mechanism allows the detection of incorrect or maliciously modified shares without revealing any information about the secret itself, leveraging the cryptographic strength of the hash function H. These properties ensure the integrity and authenticity of the shares and play a pivotal role in detecting malicious behavior during the reconstruction phase of the secret sharing protocol.

4 Construction of the Proposed Secret Sharing Scheme over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$

In this section, we present a novel multi-secret sharing scheme utilizing the algebraic structure of linear complementary dual (LCD) codes defined over a finite commutative chain ring. Specifically, we consider the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p, \quad \text{with } u^5 = 0$, which is a local principal ideal ring of characteristic p and nilpotency index 5. This ring is well-suited for constructing robust codes and cryptographic primitives, particularly in secret-sharing schemes with enhanced structural and combinatorial properties.

Let C be an $[n, k, d]$ linear code over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ that is LCD, meaning $C \cap C^{\perp} = \{0\}$, where $C^{\perp}$ denotes the dual code of C under the standard inner product over $\mathcal{R}^n$.

Assume that $G \in \mathcal{R}^{k \times n}$ is a generator matrix of C, and let the code parameters satisfy the inequality $n > 2k - 3$, which ensures sufficient redundancy to enable accurate secret reconstruction and integrity verification. A property of LCD codes used here is that the matrix product GG^T is invertible over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, which guarantees both the security and correctness of the scheme [1, 26].

Define the transpose of the generator matrix as:

$$\mathcal{T} = G^T \in \mathcal{R}^{n \times k}. \tag{4.1}$$

Since G has full row rank k, the matrix $\mathcal{T}$ also has full column rank k. This allows the computation of a projection matrix $\mathcal{T}^*$ associated with the column space of $\mathcal{T}$, which is defined as:

$$\mathcal{T}^* = \mathcal{T}(\mathcal{T}^T\mathcal{T})^{-1}\mathcal{T}^T. \tag{4.2}$$

Projection matrices play a central role in our construction by facilitating linear transformations that preserve algebraic structures, and they are highly advantageous in designing secure linear operations in cryptographic protocols [5].

Let $s \in \mathcal{R}^k$ be the secret vector that needs to be securely distributed among the participants. The dealer encodes this secret as a codeword of C by computing:

$$x = sG \in \mathcal{R}^n. \tag{4.3}$$

This codeword x embeds the secret in a linear transformation that benefits from the error-detecting capabilities of the code C.

Next, the dealer constructs a square matrix $\mathcal{M} \in \mathcal{R}^{n\times n}$ whose purpose is to blend the secret and a set of orthogonal redundancy vectors to form a recoverable structure:

(i) The first row of $\mathcal{M}$ is the encoded secret $x = sG$.

(ii) The remaining $n-1$ rows are selected as codewords $c_1, c_2, \ldots, c_{n-1} \in C^{\perp}$.

Since $C^{\perp}$ is orthogonal to C under the inner product, each codeword $c_i \in C^{\perp}$ satisfies:

$$c_i G^T = 0, \quad \text{for all } 1 \leq i \leq n-1. \tag{4.4}$$

This orthogonality ensures that these vectors do not interfere with the embedded secret and that their inclusion serves a purely protective function.

To prepare for secret reconstruction and future verification, the dealer computes the difference between the matrix $\mathcal{M}$ and the projection matrix $\mathcal{T}^*$:

$$\mathcal{N} = \mathcal{M} - \mathcal{T}^*. \tag{4.5}$$

The matrix $\mathcal{N}$ is securely stored and used during the reconstruction phase to recover the original matrix $\mathcal{M}$ through a re-computation of the projection matrix from authenticated shares.

This construction not only integrates the LCD structure of the code but also utilizes projection theory and hash-based verification (as detailed in the next section) to provide confidentiality, integrity, and participant authentication. It lays the foundation for a robust multi-secret sharing scheme that can resist cheating and information leakage even when implemented over a ring with a nontrivial nilpotent structure.

4.1 Secret Distribution Phase

In this phase, the dealer prepares and distributes the secret shares to the participants in such a way that only authorized subsets will be able to reconstruct the original secret, while any unauthorized subset obtains no information. The scheme leverages the algebraic structure of the LCD code over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ and the security properties of cryptographic hash functions.

To initiate the distribution process, the dealer randomly selects n distinct column vectors:

$$x_i \in \mathcal{R}^{k\times 1}, \quad \text{for } 1 \leq i \leq n, \tag{4.6}$$

such that any k of them form a linearly independent set over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$. This condition ensures that, later, a projection matrix constructed from any k of these vectors will be of full rank, which is critical for successful secret reconstruction. The selection of such vectors relies on techniques from module theory over local rings [16] and requires a source of cryptographic randomness [17].

For each x_i, the dealer computes a corresponding share vector using the previously defined transpose of the generator matrix:

$$v_i = \mathcal{T} x_i \in \mathcal{R}^n, \tag{4.7}$$

where $\mathcal{T} = G^T$ and G is the generator matrix of the LCD code C. These vectors v_i constitute the actual shares to be distributed to the participants. Each v_i encodes linear information derived from the code structure and contributes to the eventual reassembly of the projection matrix in the reconstruction phase.

To ensure the authenticity and verifiability of each share, the dealer employs a cryptographic hash function $H(\cdot)$ that satisfies standard properties such as preimage resistance, second preimage resistance, and collision resistance. For each computed share v_i, the dealer computes a corresponding hash function:

$$h_i = H(v_i). \tag{4.8}$$

Finally, the dealer securely transmits to each participant P_i the ordered pair:

$$(v_i, h_i), \tag{4.9}$$

where v_i is the participant's private share, and h_i is a public digest used later for verification during the secret reconstruction process.

This combination of algebraic encoding with cryptographic hashing provides structural soundness and protection against dishonest participants for submitting forged or modified shares. It also allows the dealer (or verifier) to detect such tampering efficiently without requiring storage of the original shares.

4.2 Secret Reconstruction Phase

This phase involves the recovery of the original secret by an eligible subset of participants. A set of at least k participants say $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$, must collaboratively submit their shares to recover the secret. The security and correctness of this process are grounded in the algebraic properties of the LCD code over $\mathcal{R}$ and the integrity guarantees of the cryptographic hash function.

Let the submitted shares be denoted by $v_{i_1}, v_{i_2}, \ldots, v_{i_k} \in \mathcal{R}^n$.

1. **Linearly Independent Shares Verification:** The dealer begins by verifying that the collection $\{v_{i_1}, v_{i_2}, \ldots, v_{i_k}\}$ forms a linearly independent set over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$. This condition ensures that the column space of the matrix formed from these vectors spans a k-dimensional submodule of $\mathcal{R}^n$, which is necessary for computing a valid projection matrix. Techniques from module theory over chain rings can efficiently check linear independence in this context.

2. **Weight Validation:** For each share v_{i_j}, the dealer checks whether its Hamming weight $\mathrm{wt}(v_{i_j})$ lies within the support set S of the LCD code C, which is determined from the code's weight distribution:

$$S = \{i \in \{0, 1, \ldots, n\} \mid A_i \neq 0\}. \tag{4.10}$$

   This verification step ensures that each submitted share corresponds to a valid codeword structure.

3. **Authentication Using Hash Values:** The dealer computes the hash of each submitted share and compares it with the previously stored hash values:

$$H(v_{i_j}) \stackrel{?}{=} h_{i_j}, \quad \text{for } j = 1, 2, \ldots, k. \tag{4.11}$$

   The share is considered authentic if the weight check and hash match pass successfully. This step helps detect cheating or tampering by malicious participants, relying on the cryptographic properties of the hash function.

4. **Matrix Construction and Projection:** The dealer constructs the matrix

$$\mathcal{Q} = [v_{i_1}\ v_{i_2}\ \cdots\ v_{i_k}] \in \mathcal{R}^{n \times k}, \tag{4.12}$$

   and computes its associated projection matrix:

$$\mathcal{Q}^* = \mathcal{Q}(\mathcal{Q}^T \mathcal{Q})^{-1} \mathcal{Q}^T. \tag{4.13}$$

   This matrix projects any vector in $\mathcal{R}^n$ onto the column space of $\mathcal{Q}$, which, due to the linear independence of the v_{i_j}, has full rank k.

5. **Invariance Property:** By the invariance theorem of projection matrices [6], which states that if two projection matrices project onto the same submodule, then they are equal, we conclude:

$$\mathcal{Q}^* = \mathcal{T}^*, \tag{4.14}$$

   since $\mathcal{Q}$ and $\mathcal{T}$ span the same k-dimensional subspace of $\mathcal{R}^n$.

6. **Matrix Reconstruction:** The dealer then reconstructs the original matrix $\mathcal{M}$ using:
$$\mathcal{M} = \mathcal{N} + \mathcal{Q}^* = \mathcal{N} + \mathcal{T}^*, \tag{4.15}$$
where $\mathcal{N}$ was previously stored in the setup phase.
7. **Retrieving the Codeword:** The first row of the reconstructed matrix $\mathcal{M}$ corresponds to the codeword $p_1 \in C$ that originally encoded the secret:
$$p_1 = sG. \tag{4.16}$$
8. **Recovering the Secret Vector:** Assuming $p_1 = s'G$ for some $s' \in \mathcal{R}^k$, the dealer recovers the secret by solving:
$$s' = (p_1 G^T)(GG^T)^{-1}. \tag{4.17}$$
Since GG^T is invertible over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$ by construction, this computation yields a unique solution for s'.
9. **Correctness:** Given that $x = sG = s'G$ and that G has full row rank, it follows that:
$$s = s', \tag{4.18}$$
confirming the correctness and integrity of the reconstructed secret.

As a result, any authorized subset of k participants is qualified to reconstruct the secret uniquely and successfully. Unauthorized subsets, lacking sufficient linearly independent shares, cannot form a valid projection matrix and cannot recover the secret.

Example 4.1. Let $p = 2$ and consider the ring $\mathcal{R} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2$ where $u^5 = 0$. Let C be an $[5, 3, 3]$ LCD code over $\mathcal{R}$ with generator matrix:
$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & u \\ 0 & 1 & 0 & u^2 & 1 \\ 0 & 0 & 1 & u & u \end{pmatrix}$$
and parity-check matrix:
$$H = \begin{pmatrix} 1 & u^2 & u & 1 & 0 \\ u^2 & 1 & u & 0 & 1 \end{pmatrix}.$$
The index set of the weight distribution is $S = \{3, 4, 5\}$. Let $\mathcal{T} = G^T$. Then the projection matrix is:
$$\mathcal{T}^* = \mathcal{T}(\mathcal{T}^T\mathcal{T})^{-1}\mathcal{T}^T = \begin{pmatrix} 0 & u^2 & u & 1 & 0 \\ u^2 & 0 & u & 0 & 1 \\ u & u & 1 & 1 & 1 \\ 1 & 0 & 1 & u^2 & 1 \\ 0 & 1 & 1 & 1 & u^2 \end{pmatrix}.$$
Let the secret be $s = (1, 0, u) \in \mathcal{R}^3$. Then the encoded secret is:
$$x = sG = (1, 0, u, u, 0) \in C.$$
Construct the matrix $\mathcal{M}$ as:
$$\mathcal{M} = \begin{pmatrix} 1 & 0 & u & u & 0 \\ 1 & 0 & 1 & u & 1 \\ u & 0 & u & u^2 & u \\ u^2 & 0 & u^2 & 1 & u^2 \\ 0 & 1 & 1 & 1 & u \end{pmatrix}.$$

Then compute:

$$\mathcal{N} = \mathcal{M} - \mathcal{T}^* = \begin{pmatrix} 1 & u^2 & 0 & u^2 & 0 \\ u & 0 & u^2 & u & 0 \\ 0 & u & u^2 & u & u^2 \\ u & 0 & u & u & u \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now, the dealer selects five distinct random vectors:

$$x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 \\ u \\ 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 \\ 0 \\ u^2 \end{pmatrix}, \quad x_4 = \begin{pmatrix} 1 \\ 1 \\ u \end{pmatrix}, \quad x_5 = \begin{pmatrix} 1 \\ u \\ u^2 \end{pmatrix}.$$

The dealer computes $v_i = \mathcal{T} x_i$ as follows:

$$\begin{aligned} v_1 &= (1, 0, 0, 1, u^2)^T, \\ v_2 &= (0, u, 0, 1, u)^T, \\ v_3 &= (0, 0, u^2, 1, 1)^T, \\ v_4 &= (1, 1, u, 1, 1)^T, \\ v_5 &= (1, u, u^2, 1, 0)^T. \end{aligned}$$

The dealer uses a one-way hash function $H(\cdot)$ to compute:

$$h_i = H(v_i), \quad \text{for } 1 \le i \le 5,$$

and sends the pair (v_i, h_i) to each participant P_i.

Reconstruction phase. Assume participants P_1, P_2, and P_4 collaborate. Their shares are v_1, v_2, and v_4. Compute:

$$\mathrm{wt}(v_1) = 3, \quad \mathrm{wt}(v_2) = 3, \quad \mathrm{wt}(v_4) = 5 \in S.$$

Verify hash values:

$$H(v_j) = h_j \quad \text{for } j = 1, 2, 4.$$

Form the matrix:

$$\mathcal{Q} = [v_1 \; v_2 \; v_4] \in \mathcal{R}^{5\times 3}.$$

Compute the projection matrix:

$$\mathcal{Q}^* = \mathcal{Q}(\mathcal{Q}^T\mathcal{Q})^{-1}\mathcal{Q}^T.$$

By the invariance theorem of projection matrices, we have $\mathcal{Q}^* = \mathcal{T}^*$. Then reconstruct:

$$\overline{\mathcal{M}} = \mathcal{N} + \mathcal{Q}^* = \mathcal{N} + \mathcal{T}^* = \mathcal{M}.$$

Compute:

$$\overline{\mathcal{M}} G^T = \begin{pmatrix} u^2 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Thus, the first row of $\overline{\mathcal{M}}$ is $p_1 = (1, 0, u, u, 0) \in C$. Since $p_1 = \alpha G$ for some $\alpha \in \mathcal{R}^3$, recover:

$$\alpha = p_1 G^T (GG^T)^{-1} = (1, 0, u).$$

Hence, the secret is recovered correctly as $s = (1, 0, u)$.

Example 4.2. Let $\mathcal{R} = \mathbb{F}_8 + u\mathbb{F}_8 + u^2\mathbb{F}_8 + u^3\mathbb{F}_8 + u^4\mathbb{F}_8$ be a finite chain ring where $u^5 = 0$, and let $\mathbb{F}_8$ be the field with 8 elements defined by the irreducible polynomial $\alpha^3 + \alpha + 1 = 0$.

Let C be a linear complementary dual (LCD) code of parameters $[9, 4, 5]$ over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_8$ with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \alpha & \alpha^2 & 0 & 1 & \alpha^3 \\ 0 & 1 & 0 & 0 & \alpha^2 & 1 & \alpha^3 & 0 & \alpha \\ 0 & 0 & 1 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & 1 \\ 0 & 0 & 0 & 1 & \alpha^3 & \alpha & 1 & \alpha^2 & 0 \end{pmatrix}$$

Let $\mathcal{T} = G^T \in \mathcal{R}^{9\times 4}$ and define the projection matrix:

$$\mathcal{T}^* = \mathcal{T}(\mathcal{T}^T\mathcal{T})^{-1}\mathcal{T}^T.$$

Let the secret vector be $s = (1, \alpha^2, 0, \alpha^3) \in \mathcal{R}^4$. The dealer encodes the secret as:

$$x = sG \in C.$$

Suppose the codeword is:

$$x = (1, \alpha^2, 0, \alpha^3, \alpha, 1, \alpha^2, \alpha^3, 0).$$

The dealer constructs the matrix $\mathcal{M} \in \mathcal{R}^{9\times 9}$ such that the first row is x, and the remaining 8 rows are selected from $C^\perp$ (satisfying $c_i G^T = 0$). The matrix $\mathcal{N}$ is computed as:

$$\mathcal{N} = \mathcal{M} - \mathcal{T}^*.$$

Next, the dealer selects 9 random vectors in $\mathcal{R}^5$:

$$\begin{aligned} x_1 &= (1,0,0,0)^T, & x_2 &= (0,\alpha,0,0)^T, \\ x_3 &= (0,0,\alpha^2,0)^T, & x_4 &= (0,0,0,1)^T, \\ x_5 &= (1,\alpha^3,0,0)^T, & x_6 &= (\alpha,0,\alpha^2,0)^T, \\ x_7 &= (1,1,1,1)^T, & x_8 &= (0,\alpha^2,1,1)^T, \\ x_9 &= (\alpha,1,\alpha^2,\alpha^3)^T. \end{aligned}$$

Then, the dealer computes:

$$v_i = \mathcal{T}x_i \in \mathcal{R}^9, \quad h_i = H(v_i),$$

and sends the pair (v_i, h_i) to participant P_i for $i = 1$ to 9.

Reconstruction Phase: Suppose participants P_1, P_2, P_5, and P_9 collaborate. They send their shares v_1, v_2, v_5, v_9 to the dealer.

- The dealer verifies that $\{v_1, v_2, v_5, v_9\}$ are linearly independent over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_8$.
- Confirms that $\mathrm{wt}(v_j) \in S$ for all $j \in \{1, 2, 5, 9\}$.
- Verifies hash matches: $H(v_j) = h_j$ for all j.

Then constructs:

$$\mathcal{Q} = [v_1\ v_2\ v_5\ v_9] \in \mathcal{R}^{9\times 4}, \quad \mathcal{Q}^* = \mathcal{Q}(\mathcal{Q}^T\mathcal{Q})^{-1}\mathcal{Q}^T.$$

Using the invariance property:

$$\mathcal{Q}^* = \mathcal{T}^*, \quad \overline{\mathcal{M}} = \mathcal{N} + \mathcal{Q}^*.$$

Now,

$$\overline{\mathcal{M}}G^T = \begin{pmatrix} \star & \star & \star & \star \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The first row of $\overline{\mathcal{M}}$ corresponds to $p_1 = x = sG$, and since G has full row rank, the secret is recovered as:

$$s = p_1 G^T (GG^T)^{-1} = (1, \alpha^2, 0, \alpha^3).$$

Thus, the original secret is correctly reconstructed.

Example 4.3.

5 Assessment of Scheme Security and Operational Performance

5.1 Examination of Scheme Security

This subsection evaluates the security properties of the proposed (k, n) multi-secret sharing scheme (MSSS), which is constructed using linear complementary dual (LCD) codes over the finite commutative chain ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, with the nilpotent condition $u^5 = 0$.

Theorem 5.1. *The proposed construction realizes a valid (k, n)-threshold multi-secret sharing scheme.*

Proof. The scheme allows the dealer to generate and distribute n distinct share vectors from $\mathcal{R}^n$ using a carefully selected rank-k generator matrix derived from an LCD code. These shares are linear combinations of the secret, designed so that any group of at least k participants can collaboratively reconstruct the secret.

More formally, for any authorized set of k participants, the corresponding share vectors span a full-rank matrix $\mathcal{Q} \in \mathcal{R}^{k\times n}$, ensuring that the secret can be recovered using a decoding algorithm or by computing an appropriate projection matrix $\mathcal{Q}^*$. Conversely, any subset of fewer than k participants results in a rank matrix strictly less than k, rendering the projection and the reconstruction of the secret infeasible. This is any partial information about the secret from being inferred when the shares are insufficient. Therefore, the scheme satisfies the threshold condition and qualifies as a valid (k, n)-threshold MSSS. □

Theorem 5.2. *The proposed MSSS is a perfect and asymptotically ideal scheme.*

Proof. A multi-secret sharing scheme is said to be *perfect* if every authorized subset of participants can reconstruct the secret without error while every unauthorized subset gains no information about the secret. This condition is firmly upheld in our construction by two integrated mechanisms: linear algebraic constraints and cryptographic authentication.

During the reconstruction phase, each participant submits a shared vector $v_i \in \mathcal{R}^n$ accompanied by a corresponding hash value $h_i = H(v_i)$, where $H : \{0,1\}^* \to \{0,1\}^\xi$ is a secure

cryptographic hash function. The dealer performs two verification steps: first, a *weight test*, where the Hamming weight of each share is checked against a predefined index set S associated with the weight distribution of the LCD code; and second, a *hash check*, ensuring that $H(v_i) = h_i$ holds for each submitted share.

Due to the preimage resistance and collision resistance, it is computationally infeasible for an adversary to forge a valid share or manipulate existing ones without detection. Consequently, unauthorized subsets cannot bypass the verification phase, ensuring the scheme maintains perfect secrecy.

From a performance standpoint, the *information rate* ρ-which measures the efficiency of the scheme-is defined as: $\rho = \dfrac{\text{length of the secret}}{\text{length of the share}}$. Assume the secret has length n, and each hash output has a fixed length ξ. Each participant's share the pair (v_i, h_i), with total length $n + \xi$. Therefore, the information rate becomes:

$$\rho = \frac{n}{n+\xi}. \tag{5.1}$$

As n grows (i.e., in systems with many participants or secrets), the denominator becomes increasingly dominated by n, and the information rate approaches 1. This shows that the scheme is *asymptotically ideal*-it achieves near-optimal efficiency while preserving robust security guarantees.

The proposed scheme satisfies the dual goals of perfect secrecy and high efficiency, making it secure and practical for real-world applications involving multiple secrets. □

5.2 Detection and Identification of Malicious Participants

A significant advantage of utilizing linear codes over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, where $u^5 = 0$, is the built-in capability for detecting dishonest behavior during the reconstruction phase of the secret sharing process. In the proposed scheme, each participant's share is a valid codeword from a carefully selected LCD code over $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, which enables structural consistency checks.

To improve this integrity check, the scheme incorporates a cryptographic one-way hash function $H : \{0,1\}^* \to \{0,1\}^{\xi}$, which plays a critical role in verifying the authenticity of the submitted shares. During reconstruction, each participant submits a codeword $v_i \in \mathcal{R}^n$ along with its corresponding hash value $h_i = H(v_i)$, which was precomputed during the distribution phase by the trusted dealer.

Suppose an adversarial participant (a cheater) submits a forged share v_c such that its Hamming weight satisfies $\text{wt}(v_c) \in S$ (where S is the allowed weight set determined by the LCD code). Even if v_c structurally appears legitimate, the dealer performs an authentication check by computing $H(v_c)$ and verifying whether it matches any previously distributed hash value h_i for $1 \leq i \leq n$. Due to the preimage resistance and collision resistance of the hash function, it is computationally infeasible for the cheater to construct a codeword v_c such that $H(v_c) = h_i$ for some legitimate i unless v_c is the same as the original v_i.

Hence, if the computed hash $H(v_c)$ does not match any known value in the dealer's hash registry, the dealer can confidently reject the forged share and identify the cheater. This verification process improves the scheme's robustness and safeguards the integrity of secret reconstruction, even against malicious participants.

Table 1. Assessment of Existing Multi-Secret Sharing Approaches

Scheme	Participants	Secret Size	Information Rate (ρ)	Perfect
Çalkavur and Solé [8]	n	q^k	1	Yes
Ding et al. [22]	n	q^k	$\frac{n}{n-1}$	Yes
Massey [28]	$n-1$	q	1	Yes
Pang and Wang [30]	n	q	$\frac{n}{n-p-t+1}$	No
Yang et al. [19]	n	q^{k-1}	$\frac{k-1}{n}$	Yes
Proposed Scheme	n	p^k	$\frac{\eta}{n+\xi}$	Yes

5.3 Analysis of Computational Efficiency

The security of the proposed scheme relies on the use of an LCD code over the ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, where the security parameters such as p, n, and k play a crucial role in determining the overall strength and flexibility of the scheme. With sufficiently large values of n and p, there are numerous possibilities for selecting the generator matrix G and the parity-check matrix H that satisfy the LCD property, allowing for a wide range of code configurations. This flexibility is beneficial for adapting the scheme to different use cases and security requirements. Moreover, the scheme is suitable for deployment in embedded systems, enabling highly efficient execution of arithmetic operations over finite fields. As a result, the computational cost of the proposed scheme is lower compared to alternative schemes that rely on interpolation techniques, making it more efficient in terms of both time and resource usage. The operations required during the setup and the secret reconstruction phases are optimized for efficiency, ensuring the scheme is practical and scalable for real-world applications. The system's overall complexity is primarily controlled by the properties of the cryptographic hash function used and the error-detection features of the underlying code C. Table 1 provides a comparative analysis with existing threshold schemes, underscoring the relative benefits of our approach. Notably, our scheme allows the dealer to verify the validity of authorized participants during the secret reconstruction phase, ensuring that only legitimate participants contribute to the reconstruction process. Additionally, the cryptographic properties of the hash function enable the detection of dishonest or cheating participants, providing a robust mechanism for maintaining security. Furthermore, the proposed scheme stands out for its dual capability to function as both a multi-secret sharing scheme (MSSS) and a perfect scheme, combining strong security guarantees with high efficiency, making it an attractive solution for practical applications.

6 Conclusion

In this work, we have presented a novel construction of a (k, n)-threshold multi-secret sharing scheme (MSSS) based on linear complementary dual (LCD) codes defined over the finite commutative chain ring $\mathcal{R} = \sum_{i=0}^{4} u^i \mathbb{F}_p$, with the integration of a cryptographic hash function. The scheme is designed to securely distribute multiple secrets among n participants such that only qualified subsets of size at least k can recover the original secrets, while unauthorized subsets gain no information. A detailed security analysis has been conducted, showing that the security of the proposed scheme relies fundamentally on the selection of parameters n and p, as well as the robustness of the employed hash function. While larger values of n and p enhance security and resistance to attacks, they may also incur increased computational costs during arithmetic operations. However, since all operations are over finite fields and rings, efficient implementation techniques can be harnessed-especially in hardware-oriented or embedded systems. Additionally, we have demonstrated the scheme's ability to detect and identify dishonest participants during the secret reconstruction phase, thanks to the cryptographic properties of the one-way hash

function. Each participant's share is verifiable, ensuring the integrity of the reconstruction process. To assess the practical effectiveness, we conducted a comparison between our scheme and existing linear code-based secret-sharing schemes. The results show that our approach achieves an information rate close to Table 1, indicating minimal redundancy and high efficiency. As a result, the scheme qualifies as a *perfect*-since unauthorized participants learn nothing *ideal*-since the share sizes match the secret size (or nearly so). Therefore, the proposed scheme offers a secure, efficient, and scalable solution for multi-secret sharing applications, making it suitable for secure communications, distributed systems, and cryptographic protocols requiring secrecy and integrity.

References

[1] A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, H. Shoaib, and P. Solé, A multisecret-sharing scheme based on LCD codes, *Mathematics*, **8**(2), 2020, 272.

[2] M. M. AL-Ashker and A. Q. Mahmoud Abu-Jazar, Skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, Palestine Journal of Mathematics **5(2)**, 96-103, (2016).

[3] M. M. Al-Ashker and K. Chatouh, Exploring simplex codes and their applications over $\mathbb{Z}_3\mathbb{Z}_6$, Filomat **39**(11), 3609–3622, (2025).

[4] R. AL-Shorbassi and M. M. Al-Ashker, Skew $(\mu_1 + u\mu_2 + v\mu_3 + w\mu_4 + uv\mu_5 + vw\mu_6 + uw\mu_7 + uvw\mu_8)$ Constacyclic Codes over $F_q\left[u,v,w\right] \diagup \left\langle u^2-1, v^2-1, w^2-1, uv-vu, vw-wv, uw-wu\right\rangle$, Palestine Journal of Mathematics, **12(4)**, 331-339, (2023).

[5] L. Bai and X. Zou, A proactive secret sharing scheme in matrix projection method, *International Journal of Security and Networks*, **4**, 2009, In Press.

[6] L. Bai, A strong ramp secret sharing scheme using matrix projection, In *Proc. 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)*, IEEE, 2006, 652–656.

[7] G. R. Blakley, Safeguarding cryptographic keys, In *Proceedings of the National Computer Conference*, AFIPS Press, 313–317, (1979).

[8] S. Çalkavur and P. Solé, Multisecret-sharing schemes and bounded distance decoding of linear codes, *International Journal of Computer Mathematics*, **94**(1), 107–114, (2017).

[9] K. Chatouh K. Guenda, T. A. Gulliver and L. Noui, Simplex and MacDonald codes over R_q, J. Appl. Math. Comput, **55(1-2)**, 455-478, (2017).

[10] K. Chatouh, Linear codes over $R = \mathbb{Z}_7(\mathbb{Z}_7 + u\mathbb{Z}_7)(\mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7)$, Palestine Journal of Mathematics, **13**(Special Issue III), 55-62, (2024).

[11] K. Chatouh K. Guenda and T. A. Gulliver, New Classes of Codes Over $R_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\left\langle u_i^2 = 0, u_iu_j = u_ju_i\right\rangle$ and Their Applications. Computational and Applied Mathematics, **39(3)**, 1-39, (2020).

[12] K. Chatouh, Some codes over $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$ and their applications in secret sharing schemes. Afr. Mat. **35**, 1 (2024).

[13] K. Chatouh, Linear Codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ and their Applications, Matematychni Studii, **62**(1), 3–10, (2024).

[14] K. Chatouh, K. Guenda, T. A. Gulliver, and L. Noui, On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii, J. Appl. Math., **53**, 201-222 , (2017).

[15] K. Chatouh, Linear skew cyclic codes over the ring $\mathcal{R} = \mathcal{B}[v_1, v_2, v_3] + \vartheta\mathcal{B}[v_1, v_2, v_3] + \vartheta^2\mathcal{B}[v_1, v_2, v_3] + \vartheta^3\mathcal{B}[v_1, v_2, v_3]$, Palestine Journal of Mathematics, **13(4)**, 1213-1226, (2024).

[16] K. Chatouh, *Skew-cyclic linear codes over the finite ring* $\mathbb{R}_p = \mathbb{F}_p[v_1, v_2, \ldots, v_\tau]/\langle v_i^2 = 1, v_iv_j - v_jv_i\rangle$*: an in-depth exploration*, TWMS J. Appl. Eng. Math., **15(3)**, 511-525, (2025).

[17] K. Chatouh, D. Mokhtari, and K. Guenda, *Application of multi-secret sharing schemes using LCD codes over* $\mathcal{R} = R[w]$, Comput. Appl. Math., **44**(1), 123, (2025).

[18] H. K. Chien, J. K. Jan, and Y. M. Tseng, A practical (t, n) multi-secret sharing scheme, IEICE Transactions on Fundamentals, **83**, 2762–2765, (2000).

[19] Y. Chou-Chen, T. Yi Chang, and M. Shiang Hwang, A (t, n) multi-secret sharing scheme, Applied Mathematics and Computation **151**(2), 483-490, (2004).

[20] C. S. Chum and X. Zhang, Hash function-based secret sharing scheme designs, *Security and Communication Networks*, **6**(5), 584–592, (2013).

[21] A. Das and A. Adhikari, An efficient multi-use multi-secret sharing scheme based on hash function, *Applied Mathematics Letters*, **23**(9), 993–996, (2010).

[22] C. Ding, T. Laihonen, and A. Renvall, Linear multisecret-sharing schemes and error correcting codes, *Journal of Computer Science*, **3**, 1023–1036, (1997).

[23] C. Ding, J. Yuan, C. S. Calude, M. J. Dinneen, and V. Vajnovszki, Covering and secret sharing with linear codes, *Lecture Notes in Computer Science*, **2731**, Springer, Berlin, (2003).

[24] J. Ding, C. Lin, and S. Mesnager, Secret sharing schemes based on the dual of Golay codes, *Cryptography and Communications*, **13**, 1025–1041, (2021).

[25] S. T. Dougherty, S. Mesnager, and P. Solé, Secret-sharing schemes based on self-dual codes, In *2008 IEEE Information Theory Workshop*, IEEE, 338–342, (2008).

[26] G. Haradhan, P. Kumar Maurya, and S. Bagchi, Secret Sharing Scheme: Based on LCD Code, International Interdisciplinary Conference on Mathematics, Engineering and Science (MESIICON). IEEE, 2022.

[27] J. L. Massey, Linear codes with complementary duals, *Discrete Mathematics*, **106/107**, 337–342, (1992).

[28] J. L. Massey, Minimal codewords and secret sharing, In *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, 276–279, (1993).

[29] J. L. Massey, Some applications of coding theory in cryptography, In: *Cryptography and Coding IV*, Formara Ltd, Esses England, 33–47, (1995).

[30] L. J. Pang and Y. M. Wong, A new (t, n) multisecret sharing scheme based on Shamir's secret sharing, *Applied Mathematics*, **167**, 840–848, (2005).

[31] H. Pilaram and T. Eghlidos, An efficient lattice based multi-stage secret sharing scheme, *IEEE Transactions on Dependable and Secure Computing*, **14**(1), 2–8, (2017).

[32] N. ur Rehman, M. Azmi and G. Mohammad, Reversible cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+\ldots+u^{k-1}\mathbb{F}_2$, Palestine Journal of Mathematics, **12(2)**, 395-407, (2023).

[33] A. Shamir, How to share a secret, *Communications of the ACM*, **22**(11), 612–613, (1979).

[34] Melakhessou, A., Chatouh, K. & Guenda, K. DNA multi-secret sharing schemes based on linear codes over $\mathbb{Z}_4 \times R$. J. Appl. Math. Comput. **69**, 4833-4853, (2023).

Author information

Ouarda Haddouche, Karima Chatouh and Sassia Makhlouf, LAMIE Laboratory, Faculty of Economic, Commercial, and Management Sciences Batna 1 University, Batna, Algeria.
E-mail: ouarda.hadouche@univ-batna.dz
karima.chatouh@univ-batna.dz
sassia.makhlouf@univ-batna.dz

Received: 2025-05-02
Accepted: 2025-12-20