Moroccan Journal of Algebra and Geometry with Applications
x (xx) (2026), 1–11
Supported by Sidi Mohamed Ben Abdellah University, Fez, Morocco **ISSN: 2820-7114**

Secret Sharing Scheme via Free Bivariate Skew Polynomial

Muhammad Sairozi[1] and Intan Muchtadi-Alamsyah[2]

[1]*Master's Program in Mathematics, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha No. 10, 40132, Bandung, Indonesia*
e-mail: muhammadsairozi00@gmail.com
[2]*Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha No. 10, 40132, Bandung, Indonesia*
e-mail: ntan@itb.ac.id

Communicated by Abderrahmane Nitaj
(Received 20 November 2025, Revised 19 February 2026, Accepted 24 February 2026)

Abstract. A secret sharing scheme is a method for securing confidential data by distributing it among a group of participants in the form of several shares. This study examines the construction of a secret sharing scheme based on free bivariate skew polynomials, which offers flexibility in determining the threshold for reconstructing the secret data. Compared to the scheme based on regular bivariate polynomials, the proposed approach provides a more efficient secret reconstruction process, although the share generation requires more complex computational steps.

Key Words: Free Bivariate Skew Polynomial, Secret Sharing Scheme, Skew Polynomial.
2020 MSC: Primary 94A60.

1 Introduction

A secret sharing scheme is a method for securing confidential data among a group of participants by dividing it into several pieces of data called shares. The secret data can be reconstructed only when a certain number of participants, satisfying specific criteria, combine their shares. Secret sharing plays an important role in various cryptographic applications, including secure data storage, distributed systems, and secure multiparty computation.

The first and most influential secret sharing scheme was introduced by Shamir in 1979, known as the (k, n) threshold scheme [16]. This scheme is based on the concept of univariate polynomial interpolation over a finite field. In this scheme, the secret s is represented as the constant term of a random polynomial $f(x)$ of degree $k-1$. Each share s_i is constructed by selecting distinct b_i and evaluating $f(x)$ at b_i, so that s_i takes the form $(b_i, f(b_i))$. The secret s is then recovered by interpolating to obtain the polynomial $f(x)$ and evaluating $f(0) = s$. In the same year, Blakley proposed an alternative secret sharing scheme based on geometric principles, where the secret is recovered as the intersection point of hyperplanes in multidimensional space [4].

Following these seminal works, several secret sharing schemes based on different algebraic frameworks have been proposed. Brickell developed ideal secret sharing schemes using linear algebraic constructions [5]. Later, Massey established a close connection between secret sharing and linear codes, leading to code-based secret sharing schemes whose reconstruction relies on linear algebra over finite fields [11]. These linear secret sharing schemes subsequently became fundamental tools in secure multiparty computation, as shown by Cramer et al. [6].

This research is supported by the PPMI Institut Teknologi Bandung grant FMIPA.PPMI-KK-PN-07-2025, contract number 1G/IT1.CO2/KU/2025.

In parallel with the development of secret sharing schemes, non-commutative algebraic structures have attracted increasing attention in cryptography. A fundamental concept in this area is the theory of skew polynomial rings introduced by Ore [14], where polynomial multiplication is twisted by an automorphism. Skew polynomials play a central role in modern coding theory, particularly in the construction of rank-metric codes such as Gabidulin codes and their generalizations [8]. These codes are based on linearized or skew polynomials and have found important applications in code-based cryptography and post-quantum cryptographic constructions [13].

Beyond coding-theoretic applications, non-commutative polynomial rings have also been studied extensively from an algebraic persepective. Recent work has invertigated fundamental properties of polynomial rings over finite fields, including finiteness conditions for non-commutative Gröbner bases, as studied by Diop and Mesmoudi [7]. Related structural aspects of ring-theoretic properties have also been explored, such as conditions under which generalized notions of primeness coincide with classical prime ideals [3], as well as investigations into algebraic decompositions and nilpotent behaviors in commutative and non-commutative ring settings [2]. These results provide important algebraic foundations supporting the study of skew polynomial constructions.

Non-commutative algebraic techniques have also been explored in other cryptographic domains. For instance, the learning with errors (LWE) problem introduced by Regev [15] forms the basis of lattice-based cryptography. In symmetric cryptography and authentication, non-commutative algebraic constructions have also been proposed to enhance security by increasing algebraic complexity and resistance to certain classes of attacks [9].

Within the context of non-commutative polynomial structures, Zhang designed a secret sharing scheme using a skew polynomial ring [17]. The non-commutative nature of the polynomial multiplication introduces additional complexity due to the involvement of an automorphism σ. Furthermore, specific definitions for evaluation and interpolation are required, which increase computational complexity. Martínez-Peñas and Kschischang further extended the concept of evaluation and interpolation from univariate to multivariate cases [12].

In the commutative polynomial structure, Hartanto and Sutjijana developed a secret sharing scheme using multivariate polynomials, which generalizes Shamir's scheme [10]. This scheme, however, has a limitation in terms of threshold flexibility, where the threshold k depends on the number of variables m and the total degree n, given by $k = \binom{n+m}{n}$.

Based on the above studies, we propose a secret sharing scheme that utilizes free bivariate skew polynomials (two variables). This scheme combines the advantages of the non-commutative bivariate polynomial structure following the evaluation and interpolation framework of Martínez-Peñas and Kschischang, while maintaining the threshold flexibility k as in the design of Hartanto and Sutjijana.

The remainder of this paper is organized as follows. Section 2 introduces free bivariate skew polynomials as defined by Martínez-Peñas and Kschischang. Section 3 presents the main results of this work. Section 4 presents a security analysis of the proposed scheme and a comparison of its computational complexity with the bivariate scheme of Hartanto and Sutjijana. Finally, Section 5 concludes the paper.

2 Free Bivariate Skew Polynomials and Vandermonde Interpolation

In this section, we present the related definitions and theories of free bivariate skew polynomials based on previous studies. The term free in the polynomials used here refers to their construction from a free monoid.

Let x, y be distinct characters and let $\mathcal{M}$ be the set of all finite strings composed of x and y, including the empty string (without characters), denoted by 1. The set $\mathcal{M}$ forms a free monoid on $\{x, y\}$ under concatenation with identity 1. Each element $m \in \mathcal{M}$ is called a monomial, and the degree of m, denoted by $\deg(m)$, represents its length.

Let $\mathcal{R}$ be a left vector space over a division ring $\mathbb{F}$ with basis $\mathcal{M}$. Each $f \in \mathcal{R}$ can be written as a unique linear combination

$$f = \sum_{m \in \mathcal{M}} c_m m,$$

with $c_m \in \mathbb{F}$ and $c_m = 0$ except for finitely many monomials. Each element $f \in \mathcal{R}$ is called a bivariate polynomial, and the degree of f, denoted by $\deg(f)$, is the maximum degree of the monomials $m \in \mathcal{M}$ with $c_m \neq 0$, if $f \neq 0$. We define $\deg(f) = \infty$ if $f = 0$.

Let $\sigma_1, \sigma_2 : \mathbb{F} \to \mathbb{F}$ be automorphisms and define a map $\sigma : \mathbb{F} \to \mathbb{F}^{2\times 2}$ over $\mathbb{F}$. Each form

$$\sigma(a) = \begin{pmatrix} \sigma_1(a) & 0 \\ 0 & \sigma_2(a) \end{pmatrix}$$

is called a morphism matrix, and denote the following two-dimensional column vector as follows:

$$\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{F}^2.$$

Definition 2.1. [12] **(Free Bivariate Skew Polynomial Ring)** Let $\mathbb{F}$ be a division ring with morphism matrix σ over $\mathbb{F}$. $\mathbb{F}[\mathbf{x};\sigma]$ is the free bivariate skew polynomial ring with ordinary vector addition and left scalar multiplication. For the right multiplication:

$$\mathbf{x} \cdot a = \sigma(a) \cdot \mathbf{x}, \text{ for all } a \in \mathbb{F}.$$

Let $f(x,y) = \sum_{m \in \mathcal{M}} c_m m$ be a polynomial in $\mathbb{F}[\mathbf{x};\sigma]$. The σ-evaluation of $f(x,y)$ at a vector $\mathbf{a} = (x,y) \in \mathbb{F}^2$ is defined as

$$f(\mathbf{a}) = E^{\sigma}_{\mathbf{a}}(f) = \sum_{m \in \mathcal{M}} c_m N^{\sigma}_m(\mathbf{a}),$$

where N^{σ}_m is called a fundamental function and is computed recursively in the following theorem.

Theorem 2.2. [12] **(Monomial Evaluation on the Free Bivariate Skew Polynomial Ring)** The σ-evaluation fundamental functions are defined as

$$N^{\sigma}_m = N_m : \mathbb{F}^2 \longrightarrow \mathbb{F}, \text{ for all } m \in \mathcal{M}.$$

These fundamental functions are given recursively as follows:

$$N_1(\mathbf{a}) = 1$$

and

$$\begin{pmatrix} N_{xm}(\mathbf{a}) \\ N_{ym}(\mathbf{a}) \end{pmatrix} = \sigma(N_m(\mathbf{a})) \cdot \mathbf{a}$$

for all $\mathbf{a} \in \mathbb{F}^2$.

Definition 2.3. [12] **(Zeros Set of Skew Polynomials)** Let $A \subseteq \mathbb{F}[\mathbf{x};\sigma]$, the zeros set of A is defined as

$$Z(A) = \{\mathbf{a} \in \mathbb{F}^2 | f(\mathbf{a}) = 0, \forall f \in A)\}.$$

Let $\Omega \subseteq \mathbb{F}^2$, the ideal associated with Ω is defined as

$$I(\Omega) = \{f \in \mathbb{F}[\mathbf{x};\sigma] | f(\mathbf{a}) = 0, \forall \mathbf{a} \in \Omega\}.$$

Definition 2.4. [12] **(P-closed)** Let $\Omega \subseteq \mathbb{F}^2$, the P-closure is defined as

$$\overline{\Omega} = Z(I(\Omega))$$

and Ω is called P-closed if $\overline{\Omega} = \Omega$.

Definition 2.5. [12] **(P-generator)** Let $\Omega \subseteq \mathbb{F}^2$ be a P-closed set. A subset $G \subseteq \Omega$ generates Ω if $\overline{G} = \Omega$. In this case, G is called a P-generator of Ω. Moreover, Ω is said to be finitely generated if it has a finite P-generator.

Definition 2.6. [12] **(P-independence)** A vector $\mathbf{a} \in \mathbb{F}^2$ is P-independence from $\Omega \subseteq \mathbb{F}^2$ if $\mathbf{a} \notin \overline{\Omega}$. A set $\Omega \subseteq \mathbb{F}^2$ is called P-independence if each $\mathbf{a} \in \Omega$ is P-independence from $\Omega \setminus \{a\}$ or $\mathbf{a} \notin \overline{\Omega \setminus \{a\}}$.

Definition 2.7. [12] **(P-basis)** Let $\Omega \subseteq \mathbb{F}^2$ be a P-closed set, and let $B \subseteq \Omega$ be called a P-basis if B is P-independence and P-generator.

Definition 2.8. [1] **(Degree Lexicographical Order)** Let $\mathcal{M}$ be the set of monomials with basis x and y.
The degree lexicographical order or deglex on $\mathcal{M}$ with $x \prec_{deglex} y$ is defined as follows.
For each $m, m' \in \mathcal{M}$ define

$$m \prec_{deglex} m' \iff \begin{cases} deg(m) < deg(m'), \\ \text{or} \\ deg(m) = deg(m') \text{ and there exists a leftmost differing basis} \\ \text{at the same position, where } m_1 \text{ in } m \text{ and } m_1' \text{ in } m' \text{ satisfy } m_1 \prec_{deglex} m_1'. \end{cases}$$

The following theorem ensures the existence of an interpolation polynomial for any set of vectors forming a P-basis.

Theorem 2.9. [12] Let $\Omega \subseteq \mathbb{F}^2$ be a finitely generated P-closed set with a finite P-basis $B = \{\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_M}\}$. The following statements hold:

1. If $E_B^\sigma(f) = E_B^\sigma(g)$, then $E_\Omega^\sigma(f) = E_\Omega^\sigma(g)$, for all $f, g \in \mathbb{F}[\mathbf{x}; \sigma]$. That is, the values of a skew polynomial function $f : \Omega \longrightarrow \mathbb{F}$ are uniquely determined by $f(\mathbf{b_1}), f(\mathbf{b_2}), ..., f(\mathbf{b_M})$.
2. For any $a_1, a_2, ..., a_M \in \mathbb{F}$. There exists $f \in \mathbb{F}[\mathbf{x}; \sigma]$ such that $\deg(f) < M$ and $f(\mathbf{b_i}) = a_i$, for $i = 1, 2, ..., M$.

Definition 2.10. [12] **(Skew Vandermonde Matrix)** Let $\mathcal{N} \subseteq \mathcal{M}$ be a finite set of monomials and let $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_M}\} \subseteq \mathbb{F}^2$. The σ-Vandermonde matrix, $V_\mathcal{N}^\sigma(B)$, is a $|\mathcal{N}| \times M$ matrix over $\mathbb{F}$ whose rows are given by

$$(N_m(\mathbf{b_1}), N_m(\mathbf{b_2}), ..., N_m(\mathbf{b_M})) \in \mathbb{F}^M,$$

for all $m \in \mathcal{N}$ (with an ordering in $\mathcal{M}$).

As a consequence of Theorem 2.9, the interpolation problem can be formulated as a linear system based on a Vandermonde matrix.

Corollary 2.11. *[12] Let $\Omega \subseteq \mathbb{F}^2$ be finitely generated with a P-basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_M}\}$. Then there exists a solution to the linear system*

$$(c_m)_{m \in \mathcal{M}_M} \cdot V_M^\sigma(B) = (a_1, a_2, \cdots, a_M),$$

for any $a_1, a_2, \cdots, a_M \in \mathbb{F}$ (V_M^σ is left-invertible). For any solution, the corresponding skew polynomial f satisfies $f(\mathbf{b_i}) = a_i$ for each $i = 1, 2, ..., M$ and $deg(f) < M$.

3 Secret Sharing Scheme via Free Bivariate Skew Polynomial

In the proposed scheme, we work on a vector set that forms a P-basis. This set of vectors will be used to interpolate the polynomial, since the existence of a solution has been guaranteed by Corollary 2.11. In the share generation process, several secret sharing schemes generally construct the polynomial first, then select a certain number (a vector in this scheme) with specific criteria that will serve as a candidate for the share components. However, in this scheme, we reverse the process: the points are chosen first, and then the polynomial is constructed. The reason is that if we follow the first process, the interpolation is not guaranteed to succeed. Moreover, since we work with non-commutative polynomials, the evaluation of a vector at monomials xy and yx may not yield the same result, so we have many monomial candidates available as the polynomial basis generated by the threshold number. Therefore, we propose the following algorithm to select the appropriate monomial and ensure that any subset of the shares set can be successfully interpolated.

Algorithm 1 Basis Selection on $\mathcal{M}$

Input: $\Omega = \{b_1, ..., b_n\} \subseteq \mathbb{F}^2$, a positive integer k, with $1 < k \leq n$.
Output: A set of monomials with maximum degree $k-1$.
Initialization:

- $\mathcal{M}$ is the set of monomials of degree at most $k-1$, ordered by deglex.
- $\mathcal{N} = \{1\}$.
- Matrix $V_{\mathcal{N}} = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}$ of size $1 \times n$.

for monomial m in $\mathcal{M} \setminus \{1\}$ **do**
  $V_m = \begin{bmatrix} N_m(b_1) & N_m(b_2) & \cdots & N_m(b_n) \end{bmatrix}$
  if V_m is linearly independent from the rows of $V_{\mathcal{N}}$ **then**
    Add V_m as a new row to $V_{\mathcal{N}}$
    if the rank of any submatrix of size $(|\mathcal{N}|+1) \times (|\mathcal{N}|+1)$ of $V_{\mathcal{N}}$ is full **then**
      $\mathcal{N} = \mathcal{N} \cup \{m\}$
    else
      Remove V_m from the rows of $V_{\mathcal{N}}$
    end if
  end if
  if $|\mathcal{N}| = k$ **then**
    break
  end if
end for
Return $\mathcal{N}$

The proposed secret sharing scheme consists of three phases: the initialization phase, the share generation phase, and the secret reconstruction phase.

3.1 Initialization Phase

In this phase, the dealer determines the number of participants denoted by n, the threshold for reconstructing the secret denoted by k, the polynomial structure $\mathbb{F}[\mathbf{x}, \sigma]$, and the secret $s \in \mathbb{F}$.

3.2 Share Generation Phase

1. The dealer selects $\mathbf{b_i} = (x_i, y_i) \in \mathbb{F}^2$ such that $\{\mathbf{b_i}\}$ forms a P-basis, for each $i = 1, ..., n$.
2. Using k and $\{\mathbf{b_i}\}$, based on Algorithm 1, the dealer constructs a polynomial of degree less than k
$$f(x, y) = c_0 + \sum_{j=1}^{k-1} c_j m_j$$
where $c_0, ..., c_{k-1} \in \mathbb{F}$ and $m_j \in \mathcal{M}$ are the corresponding ordered monomials. Then set $c_0 = s$ and randomly choose $c_1, ..., c_{k-1} \in \mathbb{F}$.
3. The dealer computes $d_i = f(\mathbf{b_i})$.
4. The dealer defines the shares $s_i = (x_i, y_i, d_i)$ and distributes them privately to each P_i.

3.3 Secret Reconstruction Phase

1. At least k participants who hold shares gather together.
2. The participants collect their shares s_i.
3. The participants perform interpolation using the Vandermonde interpolation.
4. The participants evaluate $f((0, 0)) = s$ to obtain the secret.

3.4 Example

Suppose D is the dealer and $\{p_1, p_2, p_3, p_4, p_5\}$ are the set of participants with $n = 5$. D sets the threshold $k = 4$ and defines the free bivariate skew polynomial $\mathbb{C}[\mathbf{x}; \sigma]$ as

$$\sigma(a) = \begin{pmatrix} \overline{a} & 0 \\ 0 & a \end{pmatrix}, \quad \forall a \in \mathbb{C},$$

and sets the secret information $s = 10 + i$. D selects five vectors, $\mathbf{b_1} = (i, -5), \mathbf{b_2} = (i, -i), \mathbf{b_3} = (i, i), \mathbf{b_4} = (i, -2), \mathbf{b_5} = (i, 2)$, and based on Algorithm 1, constructs the polynomial

$$f(x, y) = (10 + i) + 3y + (5 - i)yy + xyx.$$

D computes $f(\mathbf{b_i})$ for $i = 1, ..., 5$, obtaining

$$\begin{aligned}
f((i, -5)) &= (10 + i) + 3(-5) + (5 - i)(25) - 5 = 115 - 24i, \\
f((i, -i)) &= (10 + i) + 3(-i) + (5 - i)(-1) + i = 5, \\
f((i, i)) &= (10 + i) + 3(i) + (5 - i)(-1) - i = 5 + 4i, \\
f((i, -2)) &= (10 + i) + 3(-2) + (5 - i)(4) - 2 = 22 - 3i, \\
f((i, 2)) &= (10 + i) + 3(2) + (5 - i)(4) + 2 = 38 - 3i.
\end{aligned}$$

D distributes the shares to each participant as follows:

$$\begin{aligned}
P_1 &: s_1 = (i, -5, 115 - 24i), \\
P_2 &: s_2 = (i, -i, 5), \\
P_3 &: s_3 = (i, i, 5 + 4i), \\
P_4 &: s_4 = (i, -2, 22 - 3i), \\
P_5 &: s_5 = (i, 2, 38 - 3i).
\end{aligned}$$

Suppose four participants P_1, P_3, P_4, and P_5 gather. From the general form $f(x,y) = c_0 + c_1 y + c_2 yy + c_3 xyx$, we want to find the values of c_0, c_1, c_2, and c_3. Using Vandermonde interpolation, we obtain

$$\begin{pmatrix} f((i,-5)) & f((i,i)) & f((i,-2)) & f((i,2)) \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ N_y((i,-5)) & N_y((i,i)) & N_y((i,-2)) & N_y((i,2)) \\ N_{yy}((i,-5)) & N_{yy}((i,i)) & N_{yy}((i,-2)) & N_{yy}((i,2)) \\ N_{xyx}((i,-5)) & N_{xyx}((i,i)) & N_{xyx}((i,-2)) & N_{xyx}((i,2)) \end{pmatrix}$$

$$\begin{pmatrix} 115-24i & 5+4i & 22-3i & 38-3i \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ -5 & i & -2 & 2 \\ 25 & -1 & 4 & 4 \\ -5 & -i & -2 & 2 \end{pmatrix}$$

then we get

$$\begin{aligned} \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \end{pmatrix} &= \begin{pmatrix} 115-24i & 5+4i & 22-3i & 38-3i \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ -5 & i & -2 & 2 \\ 25 & -1 & 4 & 4 \\ -5 & -i & -2 & 2 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 115-24i & 5+4i & 22-3i & 38-3i \end{pmatrix} \cdot \begin{pmatrix} -4/21 & -5i/42 & 1/21 & 5/42 \\ 0 & -i/2 & 0 & i/2 \\ 5/6 & -1/8+11i/24 & -1/12 & -1/8-11i/24 \\ 5/14 & 1/8+9i/56 & 1/28 & 1/8-9i/56 \end{pmatrix} \\ &= \begin{pmatrix} 10+i & 3 & 5-i & 1 \end{pmatrix} \end{aligned}$$

Hence, the original polynomial is $f(x,y) = (10+i) + 3y + (5-i)yy + xyx$. By evaluating $f(x,y)$ at $(0,0)$, we obtain $f((0,0)) = 10+i$, which is the secret.

4 Scheme Analysis

4.1 Security Analysis

In this subsection, we analyze the security properties of the proposed scheme, including its correctness and threshold security.

Theorem 4.1. Given any set S of shares containing k or more members, the secret s can be reconstructed from S.

Proof. Let $s_{i_1} = (x_{i_1}, y_{i_1}, d_{i_1}), s_{i_2} = (x_{i_2}, y_{i_2}, d_{i_2}), \cdots, s_{i_k} = (x_{i_k}, y_{i_k}, d_{i_k})$ be shares where $b_{i_j} = (x_{i_j}, y_{i_j})$, for $j = 1, ..., k$ forming a P-basis in Ω. According to Theorem 2.9 (2), there exists $g \in \mathbb{F}[\mathbf{x}, \sigma]$ with $\deg(g) < k$ and $g(b_{i_j}) = d_{i_j}$. Since $f(b_{i_j}) = d_{i_j}$ as well, then $E^{\sigma}_{\Omega}(f) = E^{\sigma}_{\Omega}(g)$. Define $h(x,y) = f(x,y) - g(x,y)$. We claim that the polynomial $h(x,y)$ is a zero polynomial. Suppose $h(x,y)$ is not a zero polynomial, then $\deg(h)$ can be determined. Because $\deg(f)$,$\deg(g) < k$, we have $\deg(h) < k$. Note that since $E^{\sigma}_{\Omega}(f) = E^{\sigma}_{\Omega}(g)$, then $h(b_i) = 0$ for every $b_i \in \Omega$. Consequently, $h(x,y) \in I(\Omega)$. Because $I(\Omega)$ is the set of skew polynomials that evaluate to zero at Ω and $|\Omega| = k$, we have $\deg(h) \geq k$ (contradiction). Thus, the claim is proven. Since $h(x,y)$ is a zero polynomial, it follows that $f(x,y) = g(x,y)$. Therefore, $f((0,0)) = g((0,0)) = s$. Hence, s can be reconstructed from S. □

Theorem 4.2. Let Λ be any set of shares containing fewer than k members. Then Λ provides no information about s.

Proof. Suppose $|\Lambda| < k$ with the assumption that Λ does not contain the share $(0,0,s)$. Choose $s' \in \mathbb{F}$ as a candidate for the secret s. Form $\Lambda' = \Lambda \cup \{(0,0,s')\}$. Let $g_1(x,y)$ be the polynomial that interpolates the points in Λ'. We obtain $\deg(g_1(x,y)) < k$ and $g_1((0,0)) = s'$. However, note that if we choose another point $s'' \in \mathbb{F}$ as another candidate for s and form $\Lambda'' = \Lambda \cup \{(0,0,s'')\}$, then $g_2(x,y)$ is the polynomial that interpolates Λ'' with $\deg(g_2(x,y)) < k$ and $g_2((0,0)) = s''$. Consequently, any choice of s' or s'' is equally possible as the original secret information s. Therefore, the set Λ with $|\Lambda| < k$ provides no information about s. □

Theorems 4.1 and 4.2 show that the proposed scheme satisfies the fundamental security requirements of a threshold secret sharing scheme. In particular, the secret can be uniquely reconstructed from any set of at least k valid shares, while any set of fewer than k shares reveals no information about the secret.

Known attacks on secret sharing schemes based on bivariate polynomial arithmetic generally aim to recover the underlying polynomial through interpolation techniques. In the proposed scheme, the use of skew polynomial arithmetic increases the complexity of the interpolation problem. As a result, attacks designed for secret sharing schemes based on commutative bivariate polynomials cannot be directly applied to the proposed construction.

4.2 Complexity Comparison

In this subsection, we compare the algorithmic complexity between the secret sharing scheme using a regular bivariate polynomial and the one using a free bivariate skew polynomial. The regular polynomial based scheme is taken from [10] for the bivariate case.

There are design differences between the scheme in [10] and the one we propose. These differences lie in the threshold flexibility and the polynomial generation process used. In [10], the threshold depends on the number of variables and the degree of the polynomial used. Meanwhile, in the proposed scheme, the threshold is given as an input value. Then, in the polynomial generation process, [10] uses all available monomials as the polynomial basis, while in our scheme, only a subset of available monomials is used, selected based on Algorithm 1.

From the above discussion, the following components are considered to determine the complexity. Share generation phase:

1. Determining the threshold.
2. Constructing the polynomial $f(x,y)$.
3. Evaluating $f(\mathbf{b_i})$ for each participant i.

Secret reconstruction phase: interpolating the polynomial $f(x,y)$.

4.2.1 Secret Sharing Scheme via Regular Bivariate Polynomial

Suppose we use a (ρ, n) scheme and the polynomial used has degree k. In the share generation phase, the threshold is determined by $\rho = \binom{k+2}{2} = \frac{k^2+3k+2}{2}$. This determination has a complexity of $O(1)$.

For constructing the polynomial $f(x,y)$, the considered components are the selection of polynomial basis candidates and the selection of $k-1$ coefficients from that basis. The number of ways to choose the basis is $\binom{\rho}{\rho} = 1$. If the cost of selecting one coefficient is considered constant or $O(1)$, then the complexity of selecting $k-1$ coefficients is $(\rho-1)\times O(1) = O(\rho) = O(k^2)$. Thus, the total complexity of constructing the polynomial is $O(1) + O(k^2) = O(k^2)$.

To evaluate $f(\mathbf{b_i})$, the number of arithmetic operations is

$$\begin{aligned} T(n,k) &= n \times ((1\cdot 0 + 2\cdot 1 + \cdots + (k+1)\cdot k + \left(\frac{k^2+3k+2}{2} - 1\right)\Bigg) \\ &= n \times \left(\left(\sum_{j=1}^{k} j\cdot(j+1)\right) + \frac{k^2+3k}{2}\right) = n \times \left(\sum_{j=1}^{k} j^2 + \sum_{j=1}^{k} j + \frac{k^2+3k}{2}\right) \\ &= n \times \left(\frac{k(k+1)(2k+1)}{6} + \frac{k(k+1)}{2} + \frac{k^2+3k}{2}\right) = \frac{2nk^3+9nk^2+13nk}{6}, \end{aligned}$$

so the evaluation complexity of $f(\mathbf{b_i})$ is $O(nk^3)$. Thus, the complexity of the share generation phase is

$$O(1) + O(k^2) + O(nk^3) = O(nk^3).$$

For the secret reconstruction phase, the most expensive step in interpolating the polynomial $f(x,y)$ is finding the inverse of the Vandermonde matrix of size $\rho \times \rho$. The inverse is found using Gaussian–Jordan elimination with the number of arithmetic operations

$$\begin{aligned} T(\rho) &= 2 \times (2 \times (((\rho-1)\cdot\rho + (\rho-2)\cdot\rho + \cdots + 1\cdot\rho)\cdot 3) + \rho^2) \\ &= 2 \times \left(2 \times \left(\frac{3\rho^3 - 3\rho^2}{2}\right) + \rho^2\right) = 6\rho^3 - 4\rho^2. \end{aligned}$$

Thus, the complexity of the secret reconstruction phase is

$$O(\rho^3) = O\left(\left(\frac{k^2+3k+2}{2}\right)^3\right) = O(k^6).$$

4.2.2 Secret Sharing Scheme via Free Bivariate Skew Polynomial

Suppose we use a (k,n) scheme. In the share generation phase, the threshold is given as an input value, which has a complexity of $O(1)$.

For constructing the polynomial $f(x,y)$, the most expensive step is selecting the polynomial basis performed using Algorithm 1. In this algorithm, there are at most $|M - \{1\}| = 2^{k+1} - 2$ iterations, where in each iteration the computed components are the formation of row V_m, checking the linear independence of the rows of V_m, and checking the rank of any submatrix of size $(|\mathcal{N}|+1) \times (|\mathcal{N}|+1)$ of V_m.

Formation of row V_m :
the number of arithmetic operations is $T(n,k) = 6nk$, so the complexity is $O(nk)$.

Checking the linear independence of rows of V_m :
The linear independence check is performed by computing the rank of matrix V_m, i.e., by reducing V_m to row echelon form. The number of arithmetic operations is

$$T(n,k) = ((k-1)\cdot n + (k-2)\cdot n + \cdots + 1\cdot n)\cdot 3 = \frac{3nk^2 - 3nk}{2}.$$

Hence, the complexity is $O(nk^2)$.

Checking the rank of any submatrix of size $(|\mathcal{N}|+1) \times (|\mathcal{N}|+1)$ of V_m :

Let $|\mathcal{N}| = s$, for some s, $1 \leq s \leq k-1$. To form a square submatrix $(s+1)\times(s+1)$, we choose $s+1$ columns from the n available columns. The number of ways to choose $s+1$ is

$$\binom{n}{s+1} = \frac{n!}{(n-s-1)!(s+1)!}.$$

Then, similarly to the linear independence check, the complexity of checking the rank of that square matrix is $O\left((s+1)^3\right)$. Suppose the most expensive step occurs when $s = k-1$, then the total complexity is

$$\binom{n}{s+1}\cdot O((s+1)^3) = \binom{n}{k}\cdot O(k^3) = O\left(\binom{n}{k}k^3\right).$$

Therefore, the complexity of constructing the polynomial $f(x,y)$ is

$$(2^{k+1}-2)\times\left(O(nk)+O(k^2n)+O\left(\binom{n}{k}k^3\right)\right) = O\left(2^{k+1}\binom{n}{k}k^3\right) = O\left(\binom{n}{k}2^k k^3\right).$$

To evaluate $f(\mathbf{b_i})$, consider the polynomial $f(x,y)$ with monomials selected according to Algorithm 1. In this analysis, we consider the worst-case scenario, in which the selected monomials consist of one monomial from each degree level ranging from 0 to $k-1$. Since the evaluation process is performed recursively, the cost of evaluating each selected monomial at $\mathbf{b_i}$ is proportional to the degree of that monomial. Each recursive step involves six arithmetic operations. Therefore, to evaluate n vectors, the total number of arithmetic operations is

$$T(n,k) = n\times((0+1+2+\cdots+(k-1)\cdot 6)+k+(k-1)) = 3nk^2-nk-n,$$

so the complexity is $O(nk^2)$. Thus, the complexity of the share generation phase is

$$O(1)+O\left(\binom{n}{k}2^k k^3\right)+O(nk^2) = O\left(\binom{n}{k}2^k k^3\right).$$

For the secret reconstruction phase, the most expensive step in interpolating the polynomial $f(x,y)$ is finding the inverse of the Vandermonde matrix of size $k\times k$. The inverse is found using Gaussian–Jordan elimination with the number of arithmetic operations

$$\begin{aligned} T(k) &= 2\times(2\times(((k-1)\cdot k+(k-2)\cdot k+\cdots+1\cdot k)\cdot 3)+k^2) \\ &= 2\times\left(2\times\left(\frac{3k^3-3k^2}{2}\right)+k^2\right) = 6k^3-4k^2. \end{aligned}$$

Thus, the complexity of the secret reconstruction phase is $O(k^3)$.

Based on the analysis of algorithmic complexity in both schemes, it is found that in the share generation phase, the scheme based on regular bivariate polynomials is more efficient than the scheme based on free bivariate skew polynomials. The complexity of the regular bivariate polynomial scheme is polynomial, namely $O(nk^3)$, while the complexity of the free bivariate skew polynomial scheme grows exponentially, i.e., $O\left(\binom{n}{k}2^k k^3\right)$. This indicates that the share generation process in the proposed scheme still requires improvement in the algorithm design to achieve better computational efficiency. However, in the secret reconstruction phase, our scheme demonstrates better efficiency. The reconstruction phase complexity is $O(k^3)$, whereas the regular bivariate polynomial scheme reaches $O(k^6)$.

5 Conclusion

In this paper, we proposed a secret sharing scheme constructed using free bivariate skew polynomials. The scheme is developed by employing evaluation and interpolation techniques based on skew Vandermonde matrices, which allow the reconstruction of the secret from a sufficient number of valid shares.

Compared to secret sharing schemes based on regular bivariate polynomials, the proposed approach provides greater flexibility in determining the threshold parameter. This flexibility is achieved at the cost of higher computational complexity in the share generation phase. However, the reconstruction phase can be performed more efficiently than in schemes based on regular bivariate polynomials.

Furthermore, the proposed scheme satisfies the fundamental security properties of threshold secret sharing schemes. In particular, the secret can be uniquely reconstructed from any set of at least k valid shares, while any set of fewer than k shares reveals no information about the secret.

References

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, 1994.

[2] C. Bakkari, M. Es-Saidi, M. A. S. Moutui, *On 2-Nil-Clean Commutative Rings*, Moroccan Journal of Algebra and Geometry with Applications 4 (2025), 81–89.

[3] C. Bakkari, R. Hachache, *Rings in Which Every S-Prime Ideal Is Prime*, Moroccan Journal of Algebra and Geometry with Applications 4 (2025), 38–45.

[4] G. R. Blakley, *Safeguarding Cryptographic Keys*, Proceedings of the National Computer Conference (AFIPS) 48 (1979), 313–317.

[5] E. F. Brickell, *Some Ideal Secret Sharing Schemes*, Journal of Combinatorial Mathematics and Combinatorial Computing 9 (1989), 105–113.

[6] R. Cramer, I. Damgård, U. Maurer, *General Secure Multi-party Computation from Any Linear Secret Sharing Scheme*, Advances in Cryptology – EUROCRYPT 2000, Lecture Notes in Computer Science 1807, Springer, 2000, 316–334.

[7] Y. Diop, L. Mesmoudi, *On Finiteness of Some Noncommutative Gröbner Bases over Finite Fields*, Moroccan Journal of Algebra and Geometry with Applications 4 (2025), 74–80.

[8] E. M. Gabidulin, *Theory of Codes with Maximum Rank Distance*, Problems of Information Transmission 21 (1985), 1–12.

[9] D. Grigoriev, V. Shpilrain, *Authentication from Matrix Conjugation*, Groups, Complexity, Cryptology 2 (2010), 199–206.

[10] A. D. Hartanto, Sutjijana, *A Secret Sharing Scheme Based on Multivariate Polynomials*, Journal of Fundamental Mathematics and Applications 2 (2019), 81–92.

[11] J. L. Massey, *Minimal Codewords and Secret Sharing*, Proceedings of the 6th Joint Swedish–Russian Workshop on Information Theory (1993), 276–279.

[12] U. Martínez-Peñas, F. R. Kschischang, *Evaluation and Interpolation over Multivariate Skew Polynomial Rings*, Journal of Algebra 525 (2019), 111–139.

[13] U. Martínez-Peñas, F. R. Kschischang, *Skew and Linearized Reed–Solomon Codes and Maximum Sum-Rank Distance Codes*, IEEE Transactions on Information Theory 65 (2019), 3162–3184.

[14] O. Ore, *Theory of Non-Commutative Polynomials*, Annals of Mathematics 34 (1933), 480–508.

[15] O. Regev, *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*, Journal of the ACM 56 (2009), 1–40.

[16] A. Shamir, *How to Share a Secret*, Communications of the ACM 22 (1979), 612–613.

[17] Y. Zhang, *A Secret Sharing Scheme via Skew Polynomials*, 2010 International Conference on Computational Science and Its Applications (2010), 33–38.