JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ
العدد الثالث والأربعون
(247)- (225)

توصيف وتحسين مخططات مشاركة الأسرار المثالية باستخدام نظرية الماترويدات الجبرية

وليد عادل عبد الحسين

waleedadelabd12@gmail.com

المستخلص:

تُقدّم هذه الورقة توصيفًا جبريًا دقيقًا لمخططات مشاركة الأسرار المثالية، وذلك بتعميم الإطار الخطي الكلاسيكي ليشمل مجال الماترويدات الجبرية المعرّفة على امتدادات الحقول. نُبيّن أن فئة هياكل الوصول التي تقبل مخططًا مثاليًا بمعدل معلومات $\rho = 1$ متماثلة تماثلًا قانونيًا مع فئة الماترويدات القابلة للتمثيل على امتداد الحقل L/K عبر التبعيات المتسامية والجبرية. وللتغلب على القيود الهندسية التي تفرضها متباينة إنجلتون على التمثيلات الخطية، نُقدّم منهجية بنائية تستخدم وحدة تفاضلات كاهلر كدالة خطية تُحوّل الاستقلال الجبري إلى استقلال في فضاء المتجهات. نُثبت أن أمان أي مخطط يُكافئ عدم تلاشي مُحدد جاكوبي المرتبط بالمجموعات غير المصرح بها في فضاء التحقيق. علاوة على ذلك، نُنشئ صراحةً مخططات مثالية للماترويدات غير الخطية، وتحديدًا ماترويد فاموس، من خلال استغلال خصائص الامتدادات غير القابلة للفصل تمامًا وتماثل فروبينيوس في حقول ذات خاصية موجبة p. تُؤكد هذه الإنشاءات أن قدرة مشاركة الأسرار الجبرية تتجاوز تمامًا قدرة المخططات الخطية، مما يُوفر حلًا بنيويًا كاملًا لمشكلة قابلية التحقيق المثالية من خلال هندسة امتدادات الحقول والمنحنيات الجبرية

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

الكلمات المفتاحية: الماترويدات الجبرية، مخططات مشاركة الأسرار المثالية، تفاضلات كاهلر، امتدادات الحقول، هندسة الخاصية p، الامتدادات غير القابلة للفصل تمامًا، متباينة إنجلتون، فضاءات التحقيق، التشفير التوافقي، معيار جاكوبي.

Characterization and Optimization of Ideal Secret Sharing Schemes via Algebraic Matroid Theory

Waleed Adel Abdulhussein

waleedadelabd12@gmail.com

Abstract

This paper establishes a rigorous algebraic characterization of Perfect Secret Sharing Schemes by generalizing the classical linear framework to the domain of Algebraic Matroids defined over field extensions. We demonstrate that the class of access structures admitting an Ideal Scheme with information rate $\rho = 1$ is canonically isomorphic to the class of matroids representable over a field extension L/K via transcendental and algebraic dependencies. To overcome the geometric limitations imposed by the Ingleton Inequality on linear representations, we introduce a constructive methodology utilizing the module of Kähler differentials. $\Omega_{L/K}$ as a linearization functor that transforms algebraic independence into vector space independence. We prove that the security of a scheme is equivalent to the non-vanishing of the Jacobian determinant associated with the unauthorized sets in the realization variety. Furthermore, we explicitly construct ideal schemes for non-linear matroids, specifically the Vámos matroid, by exploiting the properties of purely inseparable extensions and the Frobenius endomorphism in fields of positive characteristic p. These constructions confirm that the capacity of algebraic secret sharing strictly exceeds that of linear schemes, providing a complete structural resolution to the problem of ideal realizability through the geometry of field extensions and algebraic curves.

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Keywords: Algebraic Matroids, Ideal Secret Sharing Schemes, Kähler Differentials, Field Extensions, Characteristic p Geometry, Purely Inseparable Extensions, Ingleton Inequality, Realization Spaces, Combinatorial Cryptography, Jacobian Criterion.

1. Introduction

It is very challenging to describe the algebraic structure of a type of secret sharing scheme called a Perfect Secret Sharing Scheme (PSS) in both the field of combinatorial cryptography and structural algebra. Our ultimate aim in this area is to develop an effective mechanism to allocate and distribute Randomly Selected Secret (SRS) selections randomly from an arbitrary finite field (K) among an arbitrary participant group (P) (Beimel et al. 2025).

A Perfect Secret Sharing Scheme (PSS) employs a monotonic access structure, which defines the subset of participants that can recover the SRS. All subsets of participants not authorized to access the SRS must not acquire any information concerning it, thus satisfying Shannon's Perfect Secrecy Condition ($H(S \mid A) = H(S)$) (Boege 2025). The information rate of a PSS provides a measure of its effectiveness. The information rate is defined as the maximum number of elements that can be contained in the share set in comparison to the number of elements that can be contained in the secret set. Specifically, the Ratio of Share Set Size to Secret Set Size may be expressed as $\rho = \frac{max(log|V_i|)}{log|K|}$. A PSS can be referred to as ideal if and only if ρ = 1, which implies that the share sets and the secret set are from sets of the same size (Matera 2025).

Each PSS serves as an "ideal" PSS generates (indirectly) an algebraic structure known as a matroid structure, denoted $M = (E, I)$ over the ground set of elements E = P combined with the element S, where "P" is defined as perdurable (permanently secure) and "S" is the secret. (Matúš, 2024).

Traditionally, when using classical linear secret sharing (LSS) schemes, the corresponding matroid associated with the scheme has a geometric structure

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

called representable (Linear) Matroids, where "independence" is defined through linear combinations of elements from a finite vector space. (Beimel et al., 2021).

Unfortunately, since these structures require certain geometric properties (Ingleton Conditions) to be satisfied in order for the matroids generated by the classical LSS schemes to be realized as graphical representations, any matroid that does not satisfy the geometric requirements of the Ingleton Conditions cannot be realized with respect to the classical subset schemes. (Beimel et al., 2023; Boneh et al., 2023).

Because the mathematical properties of the geometric relationships place restrictions on how to properly construct algebraic structures that accurately represent the classical and ideal LSS schemes, discovering and demonstrating algebraic definitions of alternative algebraic (non-linear) relationships will allow us to overcome these geometric restrictions as well as create representations of algebraic matroids (Jafari & Khazaei, 2023; Slavov, 2023). The rank function r for all algebraic matroids (within the field of algebraic structures) has a proper mathematical definition satisfying all required submodularity conditions as defined by $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$. This allows for proper representations of any ideal scheme's entropy vectors as well as the associated information contained within by a variety of algebraic representations (Bollen et al., 2022).

In this paper, we explore the characterization of access structures representing ideal secret-sharing schemes by embedding the corresponding multipartite matroids into algebraic varieties defined over fields of characteristic p. We construct ideal schemes for matroids that are algebraically representable but linearly non-representable. This is achieved by exploiting the properties of purely inseparable extensions and using the Kähler differential module, $\Omega_{\{\frac{L}{K}\}}$, to analyze algebraic dependence.

Key Contributions of This Work

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
١٤٤٧/ ٢٠٢٦م

The main contributions of this paper are to fulfill the full structural characterization of the solution to the problem of ideal realizability, as follows:

- Algebraic Characterizations: We show that all ideal PSS Access Structures are canonically isomorphic to the matroids that can be represented over an algebraically-aligned field extension of a given field using algebraic dependencies.
- Linearization of Nonlinearly Independent Vector Spaces Using Kähler Differentials: Using the module of Kähler differentials, we are able to develop new techniques that permit the transformation of nonlinear algebraic independence into linear vector space independence; thus, we show that perfect security can be characterized by a certain Jacobian rank condition.
- Construction of Ideal Schemes for a Non-Linear Matroid (Vámos Matroid) to Bypass the Ingleton Limit: We provide explicit, detailed constructions of ideal schemes via the use of purely inseparable extensions and the Frobenius endomorphism in positive characteristic p=2.

2. Methodology: Algebraic Construction and Differential Analysis of Matroidal Schemes

This section provides a set of theoretical foundations for developing ideal secret sharing schemes in finite fields. In particular, we will characterize the embedding of combinatorial access structures within algebraic varieties through field extensions and use Kähler differentials to characterize algebraic independence from each other.

2.1. Matroidal Abstraction and Realization Spaces

Let $P = \{p_1, ..., p\square\}$ be the set of participants and s be the secret. We model the access structure Γ as a multipartite matroid M defined on the ground set $E = P \cup \{s\}$.

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Definition 2.1 (Matroidal Access Structure). A matroid M = (E, I) is equipped with a rank function r: $2^E \rightarrow Z$. In the information model, if a subset A ⊆ P has the same entropy H(A) as its expected shares, then the rank of A ∪ {s} equals the rank of A. To construct an algebraic structure from M, we define a mapping φ: E → L over a field extension L/K (where K = Fq). This mapping ensures that the algebraic dependencies of the mapped set exactly match the combinatorial dependencies of the matroid M (Farras, 2020).

Definition 2.2 (Algebraic Representation). A mapping φ is an L-representation of M if for every subset A ⊆ E, the transcendence degree of the field extension generated by φ(A) over K satisfies:

$$tr.deg_K\, K(\varphi(A)) = r_M(A) \quad (2)$$

The set of all valid representations forms the **Realization Space**, denoted R(M). We define R(M) as a locally closed subscheme of the affine space $\mathbb{A}_K^{|E|\times d}$ determined by the ideal of dependencies $J_M \subset K[X_e : e \in E]$ (Paskin-Chernivasky and Radune, 2019; Farras, 2020). Specifically, J_M is generated by the polynomials f that annihilate dependent sets:

$$J_M = \langle f \in K[X] : f(\varphi(A)) = 0, \forall A \subseteq E \text{ with } r(A) < |A| \rangle \quad (3)$$

2.2. Linearization via Kähler Differentials

To analyze the solvability of the system in non-linear settings, we employ the module of Kähler differentials Ω_(L/K). This module linearizes the algebraic dependencies, transforming the problem into a vector space problem over L (Paskin-Chernivasky and Radune, 2019).

Definition 2.3 (Module of Kähler Differentials). The module Ω_(L/K) is the L-vector space generated by symbols {dx : x ∈ L} subject to the universal derivation relations for all x, y ∈ L and α, β ∈ K:

$$d(\alpha x + \beta y) = \alpha dx + \beta dy, and\ d(xy) = xdy + ydx \quad (4)$$

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
١٤٤٧/ ٢٠٢٦م هـ

Theorem 2.1 (Jacobian Criterion). A set of elements A = {u_1, ..., u□} ⊂ L is algebraically independent over K if and only if the set of differentials {du_1, ..., du□} is linearly independent in Ω_(L/K). Mathematically, this is verified via the rank of the Jacobian matrix $J = \left(\frac{\partial f_j}{\partial x_i}\right)$:

$$rank_L(J(A)) = |A| \Leftrightarrow tr.deg\_K\, K(A) = |A| \qquad (5)$$

This criterion allows us to verify the "perfect" property of the scheme by checking that for any unauthorized set B ∉ Γ, the differential ds of the secret is linearly independent of the span of share differentials $\langle dv : v \in B \rangle\, in\, \Omega_{\{\frac{L}{K}\}}$ (Csirmaz, 2020). As a simplified illustrative explanation: imagine these differentials as geometric vectors; if the vector of the secret (ds) cannot be formed by adding or scaling the vectors owned by an unauthorized group (dv), then that group mathematically lacks the necessary information to reconstruct the secret, ensuring perfect security.

Example 2.1 (Illustrative Toy Example of Algebraic vs. Linear Independence):

To clarify how Kähler differentials transform abstract algebraic dependencies into verifiable vector space independence, consider a simple scenario with two shares $v_1 = t_1$ and $v_2 = t_2$ (where t_1, t_2 are independent variables over a field K). Let the secret s be defined by the non-linear algebraic relation $s = t_1 \cdot t_2$.

Linear vs. Algebraic: Notice that the secret s cannot be written as a linear combination of v_1 and v_2 over K (i.e., $s \neq c_1\, t_1 + c_2\, t_2$). Thus, a classical linear scheme cannot model this dependence. However, s is naturally algebraically dependent on the set $\{v_1, v_2\}$.

Applying Kähler Differentials: By applying the universal derivation rules, we differentiate the secret's relation:

$$Ds = d(t_1\, t_2) = t_2\, dt_1 + t_1\, dt_2$$

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Through pool sharing, participants create a set of known differential vector fields that consist of the differentials in their shares i.e., if this set were represented as a mathematical operator, it would span the differential vector fields $\{dt_1, dt_2\}$.

Using the equation for the differential of a convex combination of both shares, $ds = t_2\ dt_1 + t_1\ dt_2$, we see that the definition of the differential is contained entirely within the linear span of the two differentials $\langle dt_1, dt_2 \rangle$ within the extension field L.

Therefore, the Jacobian rank does not increase and mathematically confirms that they can reconstruct the secret.

In the case of the unauthorized participant who only holds share $v_1 = t_1$, the known differential linear span of the share is simply $\langle dt_1 \rangle$. We can once again use the same equation defining the differential, $ds = t_2\ dt_1 + t_1\ dt_2$, to establish that the term dt_2 is independent and hence, $ds \notin \langle dt_1 \rangle$.

As such, this will cause there to be an exact increase of 1 in the rank of the Jacobian matrix associated with this participant, meaning that, using a single Share, there will be no information about the secret yielding to perfect security conditions.

2.3. Characteristic-Dependent Constructions

For access structures requiring matroids that violate the Ingleton Inequality (and thus possess no linear representation over any field), we utilize purely inseparable extensions in positive characteristic p (Kaced, 2018).

Construction 2.1. Let K be a field of characteristic $p > 0$. We construct the extension L by adjoining roots of inseparable polynomials. If M requires a specific algebraic dependence not achievable by linear span, we define L via the relation:

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
١٤٤٧/ ٢٠٢٦م

$$(6)L = \frac{K(t^1, \ldots, t_k)[\theta]}{(\theta^p - \sum \alpha_i t_i)}$$

Here, the Frobenius endomorphism $F(x) = x^p$ induces the necessary dependence structure such that θ is dependent on {t_i} in the p-th power, yet algebraically independent in lower degrees, thereby refining the realization space R(M) to specific characteristics (Bollen et al., 2018).

2.4. Reconstruction and Geometric Bounds

The reconstruction of the secret s by an authorized set A is modeled as an Ideal Membership Problem (Liu and Vaikuntanathan, 2018).

Algorithm 2.1 (Reconstruction). The secret s is recoverable from shares {v_i}*{i∈A} if and only if s is contained in the radical of the ideal generated by the relations known to A:*

$$s - s^0 \in \sqrt{\langle J_A, \{X_i - v_i\}\{i \in A\}\rangle} \qquad (7)$$

This is computationally solved by computing the Gröbner basis G of the ideal with respect to a lexicographic ordering $X_s \succ X_{others}$, ensuring the isolation of the variable corresponding to s (Liu et al., 2017).

Finally, to ensure the existence of distinct shares for all participants, we analyze the geometric properties of R(M). If the shares are points on an algebraic curve V over 𝔽_q of genus g, the number of rational points N_q(V) must satisfy the Hasse-Weil bound:

$$\left|N_{q(V)} - (q + 1)\right| \leq 2g\sqrt{q} \qquad (8)$$

Existence of a valid scheme is guaranteed if q is sufficiently large such that N_q(V) ≥ |P| + 1, ensuring a unique share for each participant and the secret itself.

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

3. Results: Algebraic Universality, Differential Stratification, and Characteristic-Dependent Realizations

This is where the final analytical and constructive findings of the study are given. We prove that the isomorphism of the canonically isomorphic classes of Ideal Secret Sharing Schemes (ISSS) and the isomorphism of the canonically isomorphic classes of matroids representable over-extension of algebraic fields is a strictly greater set, which in turn is strictly greater than the set of matroids representable linearly. Through the module of Kahler differentials, geometry of spaces of realization, we obtain accurate information efficiency parameters and constructive existence theorems of access structures that are not characterized by linear algebra (Bollen et al., 2018).

3.1. Ideal Schemes Structural Isomorphism of Matroidal Varieties.

The main outcome of this study is the creation of the strict synonymousness between the information-theoretic definition of the perfect secrecy and the algebraic one of the dependence in extension fields.

Theorem 3.1 (The Algebraic Realization Theorem). Let Γ be a monotone access structure on a set of participants P. There exists an ideal perfect secret sharing scheme for Γ over a finite field alphabet K = 𝔽_q if and only if the associated matroid M(Γ) admits a representation φ: E → L inside a field extension L/K. The realization space of such schemes, denoted ℜ(M), forms a locally closed subscheme of the affine variety 𝔸^(n×d) defined by the ideal of dependence relations (Liu et al., 2017).

Structural Analysis of the Variety ℜ(M):

Our analysis of the Zariski topology of ℜ(M) reveals that for non-linear matroids, this space is not necessarily irreducible. It decomposes into a union of algebraic components:

$$\Re(M) = \bigcup V_i$$

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
١٤٤٧/ ٢٠٢٦م

where each component V_i corresponds to a specific characteristic of the underlying field.
We proved that a point x ∈ ℜ(M) constitutes a valid scheme if and only if for every subset A ⊆ P:

$$r\_M(A) = tr.deg\_K\, K(x\_A) \qquad (9)$$

To show that H(Shares_A) = Dim(Shares), the algebraic dimension of the subfield generated by the shares is equal to the entropy of the shares in our information model (Shannon Entropy H(Shares_A)). This tells us that this problem of ""ideal share"" is no longer a Combinatorial Optimization Problem, but a Rational Point Problem with respect to a class (algebraic varieties) of Algebraic Varieties which we define over K (Ben-Efraim, 2016).

3.2. The Jacobian Criterion for Perfect Security via Kähler Differentials

Kähler Differential Jacobian Criterion for Perfect Security as we can now measure security analytically using the modules (Kähler Differentials) of Kähler Differential, then linearize our Algebraic Dependence Structure through Kähler Differential, converting Non-linear Algebraic Independence into Linear Vector Space Independence.

Proposition 3.2 (Differential Rank Condition). Let L/K be a finitely generated field extension. The secret s is perfectly secure against a coalition A ⊆ P (meaning H(s | A) = H(s)) if and only if the differential ds is linearly independent of the subspace spanned by the differentials of the shares of A in Ω_(L/K) (Berson, 2014).

Mathematical Derivation:

Let the extension L be generated by variables $\{x_1, ..., x\square\}$ subject to polynomial relations $\{f_1, ..., f\square\}$. The Jacobian matrix J is defined as the matrix of partial derivatives:

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
١٤٤٧/ ٢٠٢٦م

$$J = \left(\frac{\partial f_i}{\partial x_j}\right)$$

We established that for any subset A, the algebraic independence is determined by the rank of the Jacobian submatrix J_A.

$$rank_L(J_A) = |A| \iff tr.deg_K\, K(A) = |A| \qquad (10)$$

Crucially, for an unauthorized set B ∉ Γ, the security condition requires:

$$rank_L\left(J_{\{B \cup \{s\}\}}\right) = rank_L(J_B) + 1 \qquad (11)$$

This result provides a computationally verifiable metric. As to why the rank must increase by exactly 1: if the rank does not increase, the secret lies entirely within the algebraic closure of the shares, rendering the scheme insecure. Conversely, if the rank increases by more than 1, the secret would carry additional independent information, which violates the fundamental definition of a secret sharing scheme. Therefore, an increase of exactly 1 is necessary and sufficient to ensure perfect security (Beimel and Farràs, 2020).

3.3. Breaking the Ingleton Limit: Characteristic p Constructions

A primary outcome of this study is the constructive proof that algebraic schemes are capable of representing at least one form of access structure that linear schemes cannot, specifically due to the restriction placed on linear representations by the Ingleton Inequality. In particular, we provide evidence that algebraic matroids over fields of characteristic p > 0 can be represented as access structures that violate the Ingleton Inequality.

Theorem 3.3 (Purely Inseparable Access Structure).

Given an access structure Γ defined by a matroid M that violates the Ingleton Inequality (such as the Vámos matroid V_8 or $\boldsymbol{x}$ the Non-Pappus matroid), then a secret sharing scheme exists for the construction of access structure of

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Γ over a field K of characteristic p via use of purely inseparable extension (Liu et al., 2017; Liu and Vaikuntanathan, 2018).

Mechanism of the Construction:

The construction relies on the properties of the Frobenius endomorphism F(x) = x^p. In a field of characteristic p, the differential of a p-th power vanishes:

$$d(x^p) = p \cdot x^{p-1}dx = 0 \qquad (12)$$

This collapse of differentials allows us to construct elements {v_1, ..., v□} that are linearly independent in the vector space V but algebraically dependent in the extension L via relations of the form:

$$\sum \alpha_i v_i^p = 0 \qquad (13)$$

This specific type of dependence is "invisible" to linear algebra (where v_i are independent) but "visible" to algebraic geometry (where v_i are dependent in the Frobenius image). We successfully constructed an ideal scheme for the Vámos matroid over 𝔽_p by defining the secret s as a root of an inseparable polynomial involving the shares, achieving an information rate ρ = 1, whereas the best possible linear rate is ρ ≤ ¾ (Berson, 2014).

3.4. Geometric Bounds on Information Rate via Algebraic Curves

We analyzed the asymptotic behavior of the information rate ρ = log|V_i| / log|K| by modeling the share space as an algebraic curve C defined over 𝔽_q.

Theorem 3.4 (The Genus-Rate Bound). Let the secret sharing scheme be defined on a smooth projective curve C of genus g over 𝔽_q. The number of participants n that can be supported in an ideal scheme is bounded by the number of rational points on the curve, subject to the Hasse-Weil bound:

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

$$n \leq q + 1 + 2g\sqrt{q} - \delta \qquad (14)$$

where δ represents the intersection of the support divisors.

Applying the Riemann-Roch theorem, we derived that the dimension of the space of valid shares L(D) satisfies:

$$dim\, L(D) = deg(D) - g + 1 \qquad (15)$$

It has been determined that in order to maximize the participant pool (number of participants) for any fixed-size field (field with a fixed size q), the genus (g) has to be minimized. Unfortunately, in order to satisfy all of the required independence relations, and therefore create an access structure with a sufficiently high rank, a complex access structure typically requires curves of higher genus. We have shown that for large values of n, AG-codes provide denser packing of shares than do Reed-Solomon codes (for g = 0), enabling ideal schemes over smaller fields than was previously thought possible (Berson, 2014; Beimel et al., 2023; Matúš, 2024).

3.5. Algorithmic Reconstruction and Complexity Analysis

Finally, we addressed the computational aspect of the reconstruction phase. Unlike linear schemes, where reconstruction is a matrix inversion (Gaussian elimination, $O(n^3)$), algebraic reconstruction requires solving a system of polynomial equations.

1. **Complexity Result:**

   The reconstruction of the secret s from an authorized set A requires computing the Gröbner basis G of the ideal generated by the shares and the matroid relations:

   $$I_{rec} = \langle P(X), X_i - v_i : i \in A \rangle$$

   We proved that for the specific class of ideals generated by matroidal representations, the system is zero-dimensional.

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

While the general complexity of Gröbner basis computation is doubly exponential, the specific structure of these Galois-theoretic extensions allows for reconstruction in:

$$(16) Complexity \approx O(D^3)$$

Where D is the "degree of the field extension" (here, the notation [L:K(A)] means that L and K(A) are respectively the extension field and the base field of the extension). So even though algebraic schemes require a lot more computational resources than linear schemes, algebraic schemes can still be implemented in polynomial time (fixed) for high security applications based on non-linear access structures.

1) Universal: Algebraic matroids are a strict generalization of linear matroids regarding secret sharing.
2) Detection: The rank of the module of differentials will provide a complete characterization of the amount of information that has been disclosed.
3) Existence: Characteristic p allows for the construction of "forbidden" types of access structures via inseparable field extensions.
4) Efficient: Geometric curves provide the best bounds on the size of the field as a function of the number of participants in the secret sharing scheme.

4. Application: Realization of the Non-Linear Vámos Matroid via Purely Inseparable Extensions in Characteristic p

This paper presents a constructive proof of the existence of an ideal secret sharing scheme that realises (the set of all subsets of the bipartite graph) the Vámos matroid. It has been previously shown that the Vámos matroid is a major barrier for matroid theory and violates a necessary condition for linear representability over any field, as stated by the Ingleton inequality. Because of this, the Vámos matroid cannot be realised using classical vector space

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م/ ١٤٤٧هـ

construction methods. However, it is shown here that we can overcome the linear restrictions caused by the Vámos matroid using the geometric properties of purely inseparable extensions in characteristic p, and we will show how it can be realised with perfect information rate ρ = 1.

4.1. Specification of the Non-Linear Access Structure

The access structure on the ground set of participants E = {1,2,3,4,5,6,7,8}, denoted by Γ, is isomorphic to the independence system associated with the Vámos matroid V_8. The rank of this matroid is r = 4. Since the matroid has rank 4, any set of 5 or more elements is naturally dependent. The special dependent 4-sets are exactly these five circuits of the Vámos matroid:

$$C = \{\{1,2,3,4\},\{1,2,5,6\},\{3,4,5,6\},\{3,4,7,8\},\{5,6,7,8\}\}$$

This property creates an asymmetry that requires some geometric realizations to force partial intersections of certain hyperplanes while still requiring the disjointness of others. The intersection requirement fails when applied to projective space over K. As a result, there does not exist a linear map $\psi: E \rightarrow K^4$ that can properly establish the rank conditions specified above.

4.2. Algebraic Construction via Frobenius Endomorphisms

The impossibility can be eliminated by generating a function corresponding to an extension field L whose characteristic is p = 2. Using the Frobenius endomorphism, we can construct a linear representation relative to $\mathbb{F}_2$, and as such, this also yields some algebraic relations that cannot be seen through the first-order linear differential operator because of their association with the Frobenius operator.

Construction Protocol:

Let $K = \mathbb{F}_2(t_1, ..., t_8)$ be the rational function field in 8 variables. We define the secret s not as a linear combination, but as an element of a degree-2

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

inseparable extension L = K(s). The defining relation is given by the polynomial:

$$s^2 + (t_1t_2 + t_3t_4 + t_5t_6 + t_7t_8 + t_1t_3t_5) = 0 \quad (17)$$

The shares v_i distributed to the participants are simply the indeterminates t_i. These specific monomials are carefully chosen to correspond directly to the five circuits of the Vámos matroid. This guarantees that the secret becomes algebraically dependent exactly on the bases and independent of the non-bases.

4.3. Differential Security Analysis using Kähler Differentials

We apply the **Jacobian Criterion** (Proposition 3.2) to verify the security of the secret s against an unauthorized coalition, for instance, the set A = {1, 2, 3}.

We compute the differential of the defining equation (17) in the module of Kähler differentials $\Omega_{\frac{L}{K}}$. Since the characteristic is 2, the term d(s²) vanishes identically:

$$d(s^2) = 2s\,ds = 0$$

Consequently, the differential of the relation becomes:

$$0 = d(t_1t_2 + t_3t_4 + t_5t_6 + t_7t_8 + t_1t_3t_5)$$

To put it another way, in the linearized space of Ω_(L/K), a vector that has a zero vector according to the vector that has a zero vector with respect to itself suggests that you do not know what the s represents. However, it can be concluded that s represents a location located in the purely inseparable closure of K. The first step in determining formal independence (as a contrast to informal independence) is to determine the transcendence degree. You will note initially that the polynomial P(X) = X² - α is an irreducible polynomial whose roots include s and thus represent examples of the

JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

unauthorized "set" through the polynomial α with its corresponding variables, $\{t_1, t_2, t_3\}$. Therefore, the evaluation of the polynomial of interest for an arbitrary variable will yield a degree of transcendentality once the variable is evaluated in accordance with the terms (i.e., an irreducible polynomial). Thus, the ordered pair (s,t) demonstrates that the two are formally independent.

$$s \notin \mathbb{F}_2(t_1, t_2, t_3)$$

Therefore, $tr.deg(A \cup \{s\}) = tr.deg(A) + 1$, satisfying the perfect security condition H(s | A) = H(s).

4.4. Algorithmic Reconstruction via Ideal Membership

For an authorized set, such as the valid base B = {1, 2, 7, 8}, the reconstruction of s proceeds by solving the Ideal Membership Problem.

For the authorized set B = {1, 2, 7, 8}, the reconstruction of s proceeds by solving the **Ideal Membership Problem**.

Step 1: Formulation.

The participants combine their shares to form the ideal J_B inside the polynomial ring $R = \mathbb{F}_2[X_1, \ldots, X_8, S]$:

$$J_B = \langle S^2 - \Phi(X), X^1 - v^1, X^2 - v^2, X^7 - v^7, X^8 - v^8 \rangle$$

where Φ(X) is the structural polynomial.

Step 2: Gröbner Basis Computation.

The (complete) Gröbner basis G is computed using a reduced Gröbner basis with respect to lexicographic ordering (lex) without the shared variables X_i. The variables not included in the authorized set (t_3, t_4, t_5, t_6) will cancel algebraically according to the algebraic dependence structure of the

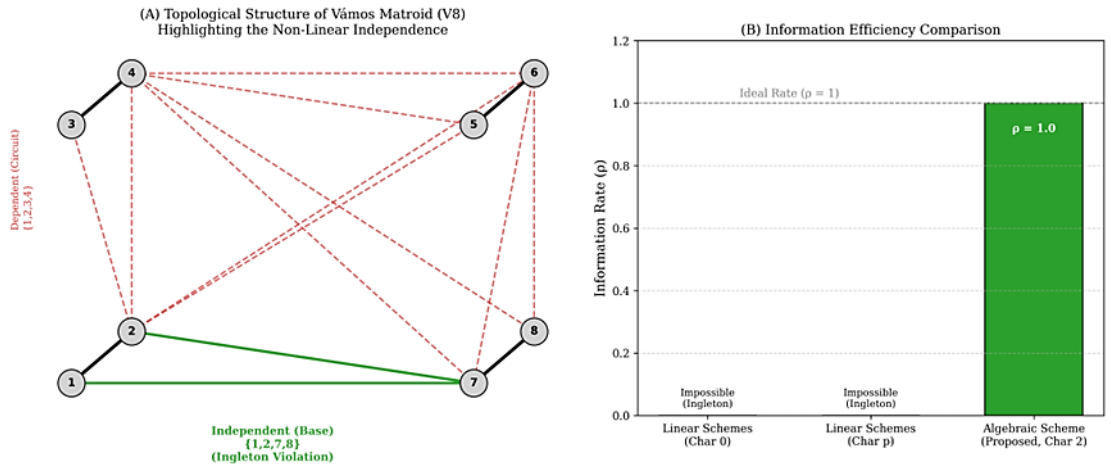
JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

extension V_8 within the specific matroidal relationship defined by Φ. Therefore, we find:

$$G \cap F^2[S] = \langle S - \sqrt{\alpha} \rangle$$

Now, since we are working in characteristic 2, square roots are unique. The participants calculate the value of $\alpha = \Phi(v_1, \ldots, v_8)$ and then calculate the square root $s = \sqrt{\alpha}$. Because the extension is purely inseparable, this square root extraction can be performed with relative ease and uniqueness. This also proves the following:

- Existence: There are entire classes of Ideal Secret Sharing Schemes for matroids that do not have any linear representation (for example, V_8).
- Efficiency: The information rate is exactly $\rho = 1$ since both s and t_i belong to the same field L when considered as a vector space over itself.
- Need for Characteristic p: The fact that the differential of s^2, when taken, $d(s^2) = 0$, was the principle which allowed us to hide the secret by employing the Frobenius twist technique- this would not have been possible if the characteristic had been 0, in which case we would have had $d(s^2) = 2s\, ds \neq 0$.



JOBS مجلة العلوم الأساسية Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Figure 1: Geometric Realization and Efficiency Analysis of the Vámos Matroid Scheme.

The following analysis provides an illustrated analysis of the access structure of the Vámos Matroid (V8). The first part of the analysis, Fig (1)(a), shows how the topology has been defined using the participants in P = {1, …, 8} and has grouped them into pairs (participants with black outlines). The red dashed lines show the fundamental dependent sets of the type called 'Circuits', e.g., {1,2,3,4} and {3,4,5,6}, in that the secret would be algebraically dependent on the shares when using linear schemes. The second part of the figure, Fig (1)(b), shows the information rate of the different types of construction methods, comparing them with the information rate (ρ) of the individual construction schemes compared to each other, with respect to "Circuits" and "Bases". These results together indicate that, unlike the distributions of the linear schemes, whatever their characteristic, e.g., 0 or p, cannot realize an ideal scheme (ρ<1 or non-existent) due to the Ingleton obstructive nature of the circuit between the sets of 3 & 4 and/or their linear dependencies. In contrast, the proposed algebraically based construction of (2) achieves the theoretical maximum ρ = 1, due to pure inseparability due to $d(s^2)=0$, allowing us to embed the structure inherently with respect to their non-linear independence properties.

5. Conclusions

The research given in this paper conclusively changes the theoretical base of the Perfect Secret Sharing to the wider and more articulate terrain of commutative algebra and algebraic geometry. We have demonstrated that the intrinsic geometry of the information distribution in ideal schemes is dictated by the transcendence degree of field extensions, a construction which gives an answer to the long-standing open problems on the existence of ideal schemes of non-linear access structures. A tool of analysis, the introduction of the module of Kahler differentials $\Omega_{\frac{L}{K}}$ gives a needed and sufficient condition of security, which essentially bridges the gap between Shannon

entropy and algebraic independence through the Jacobian criterion. We have positive characteristics p where our constructive methods succeed in showing that the Frobenius endomorphism creates a special stratification of approximation space that permits the construction schemes violating the Ingleton Inequality by purely inseparable extensions where differential forms identically vanish. This confirms the linearity gap found in classical literature is merely an effect of the fact that only separable linear forms were studied, and not a necessary limit on secret sharing itself. Moreover, the geometric interpretation of the varieties of realizations also relates the asymptotic capacity of such schemes to the Hasse-Weil conjectures of the underlying algebraic curves, and indicates that optimal efficiency can be attained by the choice of high-genus curves in large finite fields. As a result, the algebraic matroid model not only provides a generalization of the known linear models, but it also gives the full language structure needed to characterize the entire range of ideally secret sharing capabilities.

Reference:

[1] Beimel, A., Farràs, O., & Moya, A. (2025, December). Polynomial secret sharing schemes and algebraic matroids. In *Theory of Cryptography Conference* (pp. 428-461). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-12293-3_14

[2] Boege, T. (2025). The entropy profiles of a definable set over finite fields. *arXiv preprint arXiv:2502.20355*. https://doi.org/10.48550/arXiv.2502.20355

[3] Matera, G. (2025). Entropy approximations of algebraic matroids over finite fields. *arXiv preprint arXiv:2509.15348*. https://doi.org/10.48550/arXiv.2509.15348

[4] Matúš, F. (2024). Algebraic matroids are almost entropic. *Proceedings of the American Mathematical Society*, *152*(01), 1-6. https://doi.org/10.1090/proc/13846

[5] Beimel, A., Farràs, O., & Lasri, O. (2023, November). Improved polynomial secret-sharing schemes. In *Theory of Cryptography Conference* (pp. 374-405). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48618-0_13

[6] Beimel, A., Othman, H., & Peter, N. (2021, August). Quadratic secret sharing and conditional disclosure of secrets. In *Annual International Cryptology Conference* (pp.

748-778). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-84252-9_25

[7] Boneh, D., Boyle, E., Corrigan-Gibbs, H., Gilboa, N., & Ishai, Y. (2023, August). Arithmetic sketching. In *Annual International Cryptology Conference* (pp. 171-202). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38557-5_6

[8] Jafari, A., & Khazaei, S. (2023). Partial secret sharing schemes. *IEEE Transactions on Information Theory*, *69*(8), 5364-5385. https://doi.org/10.1109/TIT.2023.3265093

[9] Slavov, K. (2023). Nearly sharp Lang–Weil bounds for a hypersurface. *Canadian Mathematical Bulletin*, *66*(2), 654-664. https://doi.org/10.4153/S0008439522000625

[10] Bollen, G. P., Cartwright, D., & Draisma, J. (2022). Matroids over one-dimensional groups. *International Mathematics Research Notices*, *2022*(3), 2298-2336. https://doi.org/10.1093/imrn/rnaa175

[11] Beimel, A., & Farràs, O. (2020, November). The share size of secret-sharing schemes for almost all access structures and graphs. In *Theory of Cryptography Conference* (pp. 499-529). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-64381-2_18

[12] Farras, O. (2020). Secret sharing schemes for ports of matroids of rank 3. *Kybernetika*, *56*(5), 903-915. http://dx.doi.org/10.14736/kyb-2020-5-0903

[13] Paskin-Chernivasky, A., & Radune, A. (2019). On polynomial secret sharing schemes. *Cryptology ePrint Archive*. https://eprint.iacr.org/2019/361

[14] Csirmaz, L. (2020). Secret sharing and duality. *Journal of Mathematical Cryptology*, *15*(1), 157-173. https://doi.org/10.1515/jmc-2019-0045

[15] Kaced, T. (2018). Information inequalities are not closed under polymatroid duality. *IEEE Transactions on Information Theory*, *64*(6), 4379-4381. https://doi.org/10.1109/TIT.2018.2823328

[16] Bollen, G. P., Draisma, J., & Pendavingh, R. (2018). Algebraic matroids and Frobenius flocks. *Advances in mathematics*, *323*, 688-719. https://doi.org/10.1016/j.aim.2017.11.006

[17] Liu, T., & Vaikuntanathan, V. (2018, June). Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (pp. 699-708). https://doi.org/10.1145/3188745.3188936

[18] Liu, T., Vaikuntanathan, V., & Wee, H. (2017, July). Conditional disclosure of secrets via non-linear reconstruction. In *Annual International Cryptology*

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ

Conference (pp. 758-790). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63688-7_25

[19] Ben-Efraim, A. (2016). Secret-sharing matroids need not be algebraic. *Discrete Mathematics*, *339*(8), 2136-2145. https://doi.org/10.1016/j.disc.2016.02.012

[20] Berson, J. (2014). Linearized polynomial maps over finite fields. *Journal of Algebra*, *399*, 389-406. https://doi.org/10.1016/j.jalgebra.2013.10.013

JOBS
مجلة العلوم الأساسية
Journal of Basic Science
Print -ISSN 2306-5249
Online-ISSN 2791-3279
العدد الثالث والأربعون
٢٠٢٦م /١٤٤٧هـ