Graph Based Multipartite Secret Sharing on Enterprise Systems

Farhan Nafis Rayhan
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13522037@std.stei.itb.ac.id farhannafis281004@gmail.com

***Abstract*—Enterprise cloud environments rely on Relationship-Based Access Control (ReBAC) systems and graph databases to manage authorization at scale, solving the role-explosion and complexity challenges of traditional RBAC and ABAC. However, cryptographic key management for sensitive resources continues to use generic threshold schemes that ignore organizational structure—allowing any k of n custodians to reconstruct encryption keys regardless of role or department. This paper proposes encoding an enterprise's role/relationship graph directly into the access structure of a linear secret sharing scheme (LSSS) using multipartite secret sharing. We demonstrate that complete multipartite graphs model organizational governance constraints, where participants are partitioned into units (Engineering, Legal, Finance/Operations, Security/Audit) and authorized coalitions must contain at least one representative from each unit. We evaluate our approach on a concrete TechCorp scenario ($K_{3,2,2,2}$ access structure with 9 custodians) and demonstrate that cross-functional constraints can be cryptographically enforced without compromising storage efficiency. This work bridges multipartite secret sharing theory with practical enterprise key governance, enabling fine-grained, role-aware cryptographic control in multi-cloud environments.**

***Index Terms*—Access Control, Enterprise Security, Multipartite Secret Sharing, Linear Secret Sharing Schemes (LSSS), Graph-Based Security Models, Relationship-Based Access Control (ReBAC), Cryptographic Key Management, Enterprise Key Governance, Role-Aware Cryptography**

I. Introduction

A. Motivation: The Organizational Governance Gap

Modern cloud platforms and enterprises have adopted Relationship-Based Access Control (ReBAC) systems that represent users, roles, and resources as nodes in a knowledge graph, where authorization edges encode access relationships. AWS's graph-powered authorization, built on Amazon Neptune, exemplifies this architectural shift: by modeling authorization as a graph, enterprises can solve the "role explosion" problem inherent to RBAC (where the number of roles grows combinatorially with organizational structure) and the complexity of ABAC policies. ReBAC systems scale to billions of relationships and can process millions of authorization decisions per second.

However, a critical asymmetry exists in how organizations protect high-value encryption keys:

- **Authorization Layer (Logical):** ReBAC systems enforce fine-grained, role-based access policies through graph traversal and relationship validation. A key access request is checked against the authorization graph: "Does this user have the required role or relationship to use this key?"
- **Cryptographic Layer (Mathematical):** Key protection relies on threshold schemes, typically variants of Shamir's (t, n) threshold cryptography. In these schemes, any k of n custodians holding key shares can reconstruct the encryption key, regardless of their roles, departments, or organizational relationships.

Currently the gap of this topic is the authorization graph and the cryptographic access structure are decoupled. An insider with a key share has absolute cryptographic power over reconstruction, no amount of role-based authorization logic can prevent them from combining their share with any $k-1$ other shares to access the key, even if the organization's governance model forbids such a cross-role coalition.

B. Alignment Change

Enterprise key management best practices (DoD CSI guidance, NIST recommendations, WWPass distributed key management) emphasize:

- **Separation of duties:** No single individual or unit should hold complete key control.
- **Multi-level access control:** Access policies should enforce hierarchical or compartmented structures.
- **Split custody and quorum approvals:** High-risk operations require coordinated approvals from multiple, independent parties.
- **Flow control and data secrecy:** Information flow between units should be restricted by design.

Yet standard threshold schemes cannot express these organizational constraints cryptographically. A $(4, 9)$ Shamir scheme protects the key through quantitative threshold, but it cannot enforce the qualitative requirement that reconstruction coalitions must be cross-functional.

C. Novel Contributions

This paper propose to encode the enterprise's organizational structure directly into the mathematical access structure of a secret sharing scheme. Specifically:

- **Multi-partite Modeling:** Participants are partitioned into organizational units (C_1, C_2, C_3, C_4), represented as a complete multipartite graph $K_{n_1,n_2,\ldots,n_k}$.

- **Monotone Access Structure:** Authorized coalitions are characterized by the property that they must contain at least one representative from each unit:

$$A \in \Gamma \iff \bigwedge_{i=1}^{4} |A \cap C_i| \geq 1$$

- **Linear Secret Sharing Realization:** We construct an LSSS over a finite field such that any authorized coalition (with representatives from each unit) can reconstruct the key through linear algebra, while on the other hand any unauthorized coalition (missing any unit) learns no information about the key.
- **Ideal Schemes with Information Rate of 1:** Leveraging recent results from multipartite secret sharing theory, we show that complete multipartite graphs admit ideal linear schemes, where share size equals secret size. This matches Shamir's storage efficiency while enforcing much richer policies.

II. Background

A. Linear Secret Sharing Schemes (LSSS)

A linear secret sharing scheme (LSSS) is defined over a finite field $\mathbb{F}_q$ as follows.

Let $P = \{P_1, \ldots, P_n\}$ be a set of participants, and let $\Gamma \subseteq 2^P$ be a monotone access structure (i.e., upward-closed: if $A \in \Gamma$ and $A \subseteq B \subseteq P$, then $B \in \Gamma$). An LSSS realization of Γ consists of an $n \times d$ sharing matrix M over $\mathbb{F}_q$ satisfying the following properties.

a) Share Generation.: The dealer samples a secret $s \in \mathbb{F}_q$ and random masks $r_2, \ldots, r_d \in \mathbb{F}_q$, and forms the secret vector

$$\mathbf{v} = (s, r_2, \ldots, r_d)^{\mathsf{T}} \in \mathbb{F}_q^d.$$

Each participant P_i receives a share

$$\sigma_i = M_i \cdot \mathbf{v},$$

where M_i denotes the i-th row of the matrix M.

b) Authorized Reconstruction.: For any authorized set $A \in \Gamma$, there exist reconstruction coefficients $\boldsymbol{\lambda} = (\lambda_i)_{i \in A}$ such that

$$\boxed{\sum_{i \in A} \lambda_i \, M_i = (1, 0, 0, \ldots, 0) \; [Secret\,Select\,Vector]}$$

Consequently, the secret can be reconstructed as

$$s = \sum_{i \in A} \lambda_i \, \sigma_i.$$

c) Unauthorized Privacy.: For any unauthorized set $B \notin \Gamma$, no such reconstruction coefficients exist. The shares held by participants in B are statistically independent of the secret s, guaranteeing perfect secrecy.

The key property is linearity, where reconstruction is linear, enabling homomorphic properties useful for secure computation and threshold cryptography.

B. Multipartite Access Structures

A multipartite access structure partitions the set of participants into k disjoint parts $C_1, \ldots, C_k$, where participants within the same part play equivalent roles. Such a structure can be represented geometrically by a complete multipartite graph $K_{n_1,\ldots,n_k}$ [1], [2], defined as follows.

- **Vertices:** The vertex set is the union of the k parts, $\bigcup_{i=1}^{k} C_i$, with $|C_i| = n_i$ for each i.
- **Edges:** All possible edges between vertices belonging to different parts are present (complete bipartite connections), while no edges exist between vertices within the same part.
- **Authorized Sets:** The minimal authorized sets correspond to independent sets that intersect every part, i.e., sets containing exactly one participant from each C_i.

For the TechCorp example represented by the complete multipartite graph $K_{3,2,2,2}$, the minimal authorized sets are 4-tuples

$$\{p_1, p_2, p_3, p_4\} \quad \text{with} \quad p_i \in C_i.$$

Any superset of a minimal authorized set is also authorized, reflecting the monotone property of the access structure.

C. Information Rate and Efficiency

The information rate ρ of a secret sharing scheme quantifies its storage efficiency and is defined as

$$\boxed{\rho = \frac{\text{number of bits in the secret}}{\max_i\big(\text{number of bits in share}_i\big)}.}$$

For Shamir's (t, n) threshold scheme, the information rate satisfies $\rho = 1$: the secret is an element of $\mathbb{F}_q$, and each share is also a single element of $\mathbb{F}_q$, hence all shares have the same size as the secret.

[3] and subsequent work showed that for general access structures, the information rate can be strictly less than 1. In particular, there exist access structures on four participants that require shares at least 50% larger than the secret [4]. The best general lower bound obtainable via information-theoretic methods guarantees

$$\rho \geq \frac{1}{n},$$

for an access structure with n participants; however, the gap between this lower bound and achievable rates can be exponential.

Recent work [2] demonstrates that many multipartite access structures, including those corresponding to complete multipartite graphs, admit ideal LSSS realizations with information rate $\rho = 1$. These constructions rely on polymatroid characterizations of access structures and their connections to integer polymatroids.

D. Information Rate and Efficiency

A secret sharing scheme is perfect if any unauthorized set's shares are statistically independent of the secret:

For all unauthorized sets $B \notin \Gamma$, the secret remains perfectly private:

$$H(s \mid \text{shares}_B) = H(s),$$

i.e., observing the shares held by B does not reduce the entropy of the secret.

LSSS schemes over finite fields achieve perfect secrecy when constructed properly: if no linear combination of rows corresponding to an unauthorized set B spans the secret selector vector $(1, 0, \ldots, 0)$, then the system of equations $\sigma_B = M_B v$ has uniform solution space independent of s.

III. Related Work

IV. Methodology

A. Organization as a Complete Multipartite Graph

The core insight is to model the enterprise's organizational structure as a complete multipartite graph, defined as follows.

a) Participants (Vertices).: Let the set of participants be

$$P = \{P_1, \ldots, P_9\}.$$

These participants are partitioned into four disjoint divisions:

- C_1 (**Engineering**):

  $$C_1 = \{P_1, P_2, P_3\}$$

  (IP Protection Officer, two Principal Engineers).
- C_2 (**Legal**):

  $$C_2 = \{P_4, P_5\}$$

  (General Counsel, Contracts Attorney).
- C_3 (**Finance/Operations**):

  $$C_3 = \{P_6, P_7\}$$

  (CFO, COO).
- C_4 (**Security/Audit**):

  $$C_4 = \{P_8, P_9\}$$

  (CISO, Internal Auditor).

b) Graph Structure.: This partition induces a complete multipartite graph

$$K_{3,2,2,2},$$

where edges exist between vertices belonging to different parts, representing potential participation in authorized coalitions. No edges exist within the same part, reflecting that internal collusion alone does not form an authorized coalition.

c) Authorized Coalition Property.: A coalition $A \subseteq P$ is authorized if and only if it spans all four parts:

$$\boxed{A \in \Gamma \iff \forall i \in \{1, \ldots, 4\},\ A \cap C_i \neq \varnothing.}$$

B. Monotone Access Structure Formalization

The access structure Γ is a monotone family of subsets where based on [6] it's defined:

$$\boxed{\Gamma \text{ is monotone if whenever } A \in \Gamma \text{ and } A \subseteq B \text{ then } B \in \Gamma}$$

For the complete multipartite graph $K_{3,2,2,2}$, all minimal authorized sets have size 4 and consist of exactly one participant from each part:

$$\{p_i, p_j, p_k, p_\ell\} \quad \text{where} \quad p_i \in C_1,\ p_j \in C_2,\ p_k \in C_3,\ p_\ell \in C_4.$$

The total number of minimal authorized sets is therefore

$$|C_1| \cdot |C_2| \cdot |C_3| \cdot |C_4| = 3 \times 2 \times 2 \times 2 = 24.$$

Consider a few examples of sets authorization:

- $\{P_1, P_2, P_3\}$ (all engineers): missing representatives from C_2, C_3, and C_4; hence unauthorized.
- $\{P_1, P_4, P_6\}$ (engineering, legal, finance): missing a representative from C_4 (security); hence unauthorized.
- $\{P_1, P_4, P_6, P_8\}$ (one participant from each part): authorized.
- $\{P_1, P_2, P_4, P_6, P_8\}$ (two engineers and one from each other unit): authorized, by monotonicity.

C. LSSS Construction for $K_{3,2,2,2}$

Following LSSS from [5], We construct the scheme for our multipartite graph. All operations are performed over a finite field $\mathbb{F}_q$, where q is a large prime (e.g., $q = 2^{127} - 1$), sufficient to support 128-bit secrets.

The dealer constructs the secret vector

$$\mathbf{v} = (s, r_2, r_3, r_4)^{\mathsf{T}},$$

where

- $s \in \mathbb{F}_q$ is the secret (e.g., an AES master key),
- $r_2, r_3, r_4 \in \mathbb{F}_q$ are random masks, sampled uniformly and independently.

a) Sharing Matrix.: Let $M \in \mathbb{F}_q^{9 \times 4}$ be the sharing matrix, with one row per participant and one column per coordinate of $\mathbf{v}$. The matrix M is constructed to satisfy the following properties:

- For every minimal authorized set

  $$A = \{p_i, p_j, p_k, p_\ell\} \quad \text{with } p_i \in C_1,\ p_j \in C_2,\ p_k \in C_3,\ p_\ell \in C_4,$$

  the corresponding rows $M_{p_i}, M_{p_j}, M_{p_k}, M_{p_\ell}$ are linearly independent and span the vector $(1, 0, 0, 0)$.
- For any unauthorized set $B \notin \Gamma$ (i.e., missing at least one part), the rows M_B do not span $(1, 0, 0, 0)$.

One systematic construction of such a matrix M uses a characteristic matrix approach (see Section 3.4 for details).

b) Share Distribution.: Each participant P_i receives a single share

$$\sigma_i = M_i \cdot \mathbf{v} \in \mathbb{F}_q,$$

where M_i denotes the i-th row of M.

D. Reconstruction Protocol

Suppose we have an authorized coalition A defined as P_1, P_4, P_6, P_8, consisting of one engineer, lawyer, finance officer, security officer, wish to reconstruct s. Notice that the reconstruction coefficients $\boldsymbol{\lambda} = (\lambda_1, \lambda_4, \lambda_6, \lambda_8)$ are obtained by solving the linear system over $\mathbb{F}_q$:

$$\lambda_1 M_1 + \lambda_4 M_4 + \lambda_6 M_6 + \lambda_8 M_8 = (1, 0, 0, 0).$$

Such a solution exists because A is authorized and the corresponding rows span the secret selector vector. Thus, the secret could be recovered by linearly combining the shares:

$$\begin{aligned} s &= \lambda_1 \sigma_1 + \lambda_4 \sigma_4 + \lambda_6 \sigma_6 + \lambda_8 \sigma_8 \\ &= \big(\lambda_1 M_1 + \lambda_4 M_4 + \lambda_6 M_6 + \lambda_8 M_8\big) \cdot \mathbf{v} \\ &= (1, 0, 0, 0) \cdot (s, r_2, r_3, r_4)^\mathsf{T} \\ &= s. \end{aligned}$$

V. Information Rate and Efficiency Analysis

VI. Experimental Results

VII. Enterprise Application Scenarios

VIII. Threat Model and Security Considerations

IX. Conclusion

Acknowledgment

The writer would like to thank first of all, to God for giving me all ability and chance to finish this paper. Gratitude also extends to the IF4020 Cryptography lecturer, Dr. Ir. Rinaldi Munir, M.T., for teaching and supporting students in making contributions through innovative papers. The writer has gained a much deeper understanding of cryptography and its application in the real world through the materials and lectures from the course. Lastly, writter thanks family, friends, and everyone providing support while writing this paper.

References

[1] M. Akdim and A. Drissi, “A comprehensive review of graph theory applications in secret sharing schemes,” J. Combinatorial Math. Combinatorial Computing, vol. 123, pp. 60–89, 2025. https://doi.org/10.6028/NIST.SP.800-133r2

[2] O. Farràs and C. Padrò, “Ideal secret sharing schemes for useful multipartite access structures,” in Advances in Secret Sharing and Key Management. Cham, Switzerland: Springer, 2024.

[3] L. Csirmaz, “On the information rate of perfect secret sharing schemes,” J. Cryptology, vol. 10, no. 3, pp. 223–231, 1995.

[4] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, “On the size of shares for secret sharing schemes,” J. Cryptology, vol. 6, no. 3, pp. 157–167, 1993.

[5] COSIC Research Group, “Linear secret sharing schemes (LSSS),” KU Leuven, 2024. [Online]. Available: https://www.esat.kuleuven.be/cosic/blog/lsss/

[6] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 72(9):56-64, 1989.

Statement

I, the individual signing below, affirm that the content presented in this document is an original creation authored by me. It is not a derivative work, translation of another document, or a product of plagiarism.

Bandung, 26th December 2025,

Farhan Nafis Rayhan, 13522037