Poster: GSIT: A Geometric Space-based Information Tree for Hierarchical Certificate Management in Vehicular Networks

Jheng-Jia Huang, Wei-Hsueh Wang, Guan-Yu Chen*, and Nai-Wei Lo
National Taiwan University of
Science and Technology,
Department of Information Management,
Taipei, Taiwan
{* = The corresponding author: d11209103@mail.ntust.edu.tw}

***Abstract*—This work introduces the Geometric Space Information Tree (GSIT), a novel framework that constructs hierarchical relationships by assigning hyperplanes to entities and reducing the dimensionality of subordinate nodes. Members within the framework are verified through inner product calculations, streamlining execution steps while enabling authentication across hierarchical structures of varying depths. GSIT leverages the geometric properties of hyperplanes to efficiently encode and manage hierarchical information. It is applied to vehicular network Public Key Infrastructure (PKI), enhancing privacy protection, pseudonymous certificate management, and multi-level traceability. This approach offers a scalable and flexible solution for managing complex hierarchies in secure communication systems.**

I. Introduction

In many applications, hash chains are commonly used to manage relationships between multiple nodes under a single entity. Due to the one-way property of hash functions, it is computationally infeasible to reverse-engineer the input value from its hash value. This characteristic helps protect user privacy. However, hash chains have limitations in expressing complex hierarchical relationships.

This paper presents a novel approach using geometric space to construct a multi-layered structural tree. The method designates a hyperplane space for different entities, and when subordinate nodes need to be added, the entity reduces the hyperplane by one dimension and assigns it to the node. To verify whether a node belongs to a specific entity, we compute the inner product between the normal vector and any vector on the plane - if the inner product equals zero, it confirms the node's affiliation. We will apply this Geometric Space-based Information Tree (GSIT) to vehicular network Public Key Infrastructure (PKI).

A. Vehicular Network Public Key Infrastructure

The Security Credential Management System (SCMS) [1], [2] implements two primary categories of certificates: enrollment certificates, which prove vehicles' legitimacy in Intelligent Transportation Systems (ITS) communications, and authorization certificates, which are divided into identity and pseudonym certificates. These enable vehicles to access ITS messages or applications, with the specific type depending on the accessed message or application. This paper focuses on the mechanisms related to pseudonym certificates.

Pseudonym certificates in SCMS protect vehicle privacy through pseudonymization and untraceability. A vehicle simultaneously holds multiple valid certificates with different pseudonyms and can use different pseudonym certificates at various times and locations, preventing eavesdroppers from tracking vehicle movements. This mechanism requires innovative methods for system management to trace certificate-holding vehicles. IEEE 1609.2 [3] defines a linking value technique that effectively identifies misbehaving vehicles for revoking their pseudonym certificates.

The linking value technique uses hash chains to connect pseudonym certificates belonging to the same vehicle. However, this association is limited to a single-layer relationship between vehicles and their pseudonym certificates. We explore incorporating multi-layer relationship structures into the pseudonym certificate mechanism. For example, consider a scenario where an individual owns multiple vehicles, each with multiple pseudonym certificates - can we establish associations between pseudonym certificates and specific identities?

Our paper proposes the GSIT method, utilizing the relationship between parent spaces and subspaces, and employing inner products to verify multi-layer structural relationships (such as the affiliation between pseudonym certificates and specific individuals). We introduce the GSIT method in Section II and present its application to vehicular networks in Section III.

II. Geometric Space-based Information Tree (GSIT)

In this section, we provide a concise introduction to constructing GSIT. Our primary goal is to build a hierarchical membership structure. As illustrated in Figure 1, Depth_1 consists of $i+1$ nodes, where each node may have a different number of child nodes. For instance, Depth 1 node_0 has $j+1$ child nodes, ranging from $\text{node}_{0,0}$ to $\text{node}_{0,j}$. Similarly,

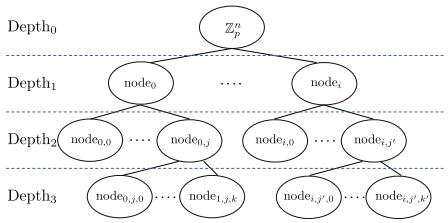

Fig. 1. Information Tree

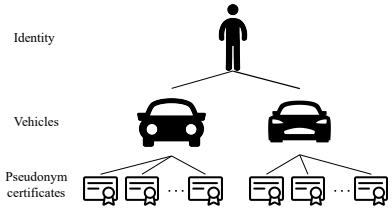

Fig. 2. GSIT in Vehicular Network PKI

Depth$_2$ node$_{0,j}$ may have $k+1$ child nodes, ranging from node$_{0,j,0}$ to node$_{0,j,k}$.

Within this information tree, two key security properties are defined:

- Collision resistance: The probability of elements in different nodes being equal is negligible.
- Unforgeability: This includes both external and inter-depth unforgeability. External unforgeability ensures that nodes outside the information tree cannot forge as nodes within the tree. Inter-depth unforgeability ensures that child nodes cannot forge parent nodes.

Based on these principles, we propose the GSIT method, which utilizes the membership relationship between parent and child spaces to construct the information tree. Specifically, we define one of the Depth$_1$ node as a polynomial hyperplane

$$\{(x_1, ..., x_n) \in \mathbb{Z}_p^n | b_1x_1 + ... + b_{n-1}x_{n-1} + b_nx_n = 0\}.$$

This set can be regarded as the inner product of two vectors, $(x_1, ..., x_n)\cdot(b_1, ..., b_n)$, where $(b_1, ..., b_n)$ serves as the normal vector of the space. If the node has a subordinate node, the corresponding hyperplane will reduce its dimensionality. For example:

$$\{(x_2, ..., x_n) \in \mathbb{Z}_p^n | b_2x_2 + ... + b_{n-1}x_{n-1} + b_nx_n = 0\}$$

To verify whether a given plane belongs to a parent plane, simply take one vector from the sub-plane and calculate its inner product with the normal vector of the parent plane. If the result is 0, it confirms the membership relationship. For example, to test whether a sub-plane belongs to a Depth$_1$ node, you can verify it by computing the inner product with the normal vector $(b_1, ..., b_n)$.

III. GSIT in Vehicular Network Public Key Infrastructure

In IEEE 1609.2 [3], the architecture of the SCMS is defined, which places greater emphasis on vehicle privacy compared to traditional PKI architectures. To protect vehicle privacy, SCMS introduces a series of techniques for pseudonymous certificates. These techniques allow a vehicle to possess multiple valid pseudonymous certificates simultaneously. This work focuses on the management issues arising from pseudonymous certificates, specifically addressing how to revoke certificates when needed and even identifying the vehicle's user if necessary.

Our proposed GSIT can be applied to such scenarios. In Figure 2, the identity in the figure is assigned a set of hyperplanes. Let $\mathbf{b} = (b_1, \ldots, b_n)$ be a vector in $\mathbb{Z}_p^n$. The hyperplanes for an identity are defined as the set of all points $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{Z}_p^n$ such that their inner product with $\mathbf{b}$ equals zero. Next, by reducing the dimensionality, we can assign the resulting hyperplane to a vehicle. This hyperplane consists of all points $(x_2, \ldots, x_n)$ in $\mathbb{Z}_p^{n-1}$ such that their inner product with $(b_2, \ldots, b_n)$ equals zero.

Finally, vectors from the vehicle's hyperplane are used during the pseudonymous certificate issuance process, where the certificate authority embeds these as linkage values into the pseudonymous certificates. In this way, to determine whether a certificate belongs to a specific identity or vehicle, it suffices to compute the inner product between the linkage value in the certificate and the vector from the hyperplane held by the verifier. This computation reveals whether there is an affiliation.

IV. Conclusion and Future Work

This work presents the GSIT methodology and illustrates its effectiveness through a practical implementation in vehicular network PKI. Our future research directions will concentrate on analyzing and enhancing security properties within various application contexts, with particular emphasis on collision resistance and unforgeability guarantees. Additionally, we plan to investigate the potential applications of GSIT in different domains, exploring new opportunities for integration and adaptation of this framework.

Acknowledgment

This work was partially supported by the National Science and Technology Council of Taiwan, under grants NSTC 112-2221-E-011 -094 -MY2, NSTC 112-2221-E-011 -092 -MY2, and NSTC 113-2634-F-011 -002 -MBK.

References

[1] R. D. Mushrall, M. D. Furtado, and H. Liu, "Emulab of security credential management system (scms) for vehicular communications," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, pp. 1–5.

[2] M. D. Furtado, R. D. Mushrall, and H. Liu, "Threat analysis of the security credential management system for vehicular communications," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2018, pp. 1–5.

[3] "Ieee standard for wireless access in vehicular environments (wave)–certificate management interfaces for end entities," *IEEE Std 1609.2.1-2020*, pp. 1–287, 2020.

Poster: GSIT: A Geometric Space-based Information Tree for Hierarchical Certificate Management in Vehicular Networks

Authors: Jheng-Jia Huang, Wei-Hsueh Wang, Guan-Yu Chen, and Nai-Wei Lo

National Taiwan University of Science and Technology, Department of Information Management, Taipei, Taiwan

Abstract

This work introduces the Geometric Space Information Tree (GSIT), a novel framework that constructs hierarchical relationships by assigning hyperplanes to entities and reducing the dimensionality of subordinate nodes. Members within the framework are verified through inner product calculations, streamlining execution steps while enabling authentication across hierarchical structures of varying depths. GSIT leverages the geometric properties of hyperplanes to efficiently encode and manage hierarchical information. It is applied to vehicular network Public Key Infrastructure (PKI), enhancing privacy protection, pseudonymous certificate management, and multi-level traceability. This approach offers a scalable and flexible solution for managing complex hierarchies in secure communication systems.

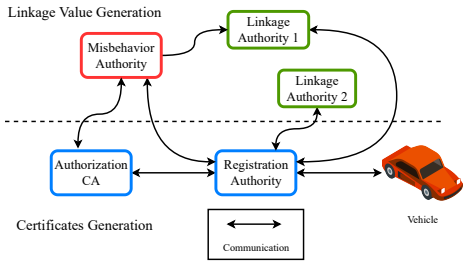

Figure 1. Communication Flow of Pseudonym Certificate in SCMS.

Introduction

- **Current Limitations:** SCMS relies on hash chain techniques for managing relationships between vehicles and their certificates. While these hash functions provide privacy through their one-way property, they are fundamentally limited to single-layer relationships, making it challenging to manage complex hierarchies where individuals own multiple vehicles with multiple pseudonym certificates.
- **GSIT Framework:** Our proposed Geometric Space-based Information Tree uses geometric spaces to construct multi-layered relationships. The framework assigns hyperplanes to entities and reduces dimensionality for subordinate nodes, enabling flexible certificate management while maintaining robust privacy protection through mathematical properties.
- **Key Contributions:** GSIT significantly enhances SCMS capabilities by supporting complex hierarchical relationships through efficient inner product calculations. This advancement enables verification across multiple layers while preserving privacy benefits, offering a comprehensive and scalable solution for modern vehicular networks.

Geometric Space-based Information Tree (GSIT)

The GSIT framework constructs a hierarchical tree structure with multiple depth levels. As shown in Figure 1, Depth_1 contains nodes (node_0 to node_i), where each node has multiple child nodes. For instance, node_0 at Depth_1 connects to $\text{node}_{0,0}$ through $\text{node}_{0,j}$ at Depth_2.

Security Properties

- **Collision Resistance:** Ensures negligible probability of node element duplication
- **Unforgeability:** Provides two-level protection:
  - External: Prevents outside nodes from forging as internal nodes
  - Inter-depth: Prevents child nodes from forging parent nodes

Membership Verification

GSIT enables efficient verification through parent-child space relationships, ensuring:

- Simple verification process
- Maintenance of hierarchical structure
- Support for multiple depth levels
- Flexible node management

The figure shows how GSIT manages complex hierarchical relationships while maintaining security at each level, providing a foundation for secure certificate management in vehicular networks.

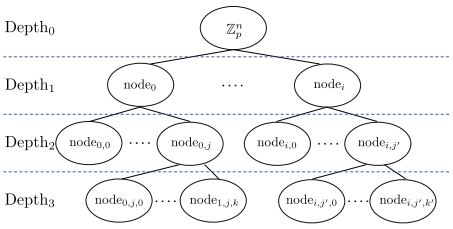

Figure 2. Information Tree

GSIT in Vehicular Network Public Key Infrastructure

The Security Credential Management System (SCMS) in vehicular networks prioritizes privacy protection through pseudonymous certificates. Our GSIT framework enhances this system by introducing a hierarchical geometric approach.

Key Implementation
Identity Level:

- Assigns hyperplane space defined as:

$$\{(x_1, \ldots, x_n) \in \mathbb{Z}_p^n \mid b_1x_1 + \ldots + b_{n-1}x_{n-1} + b_nx_n = 0\}$$

- Serves as the root level for certificate management

Vehicle Level:

- Utilizes reduced dimensional hyperplane:

$$\{(x_2, \ldots, x_n) \in \mathbb{Z}_p^n \mid b_2x_2 + \ldots + b_{n-1}x_{n-1} + b_nx_n = 0\}$$

- Maintains connection to parent identity while preserving privacy

Certificate Management:

- Embeds vectors from vehicle's hyperplane as linkage values
- Enables efficient verification through inner product calculations
- Maintains pseudonymity while supporting traceability when needed

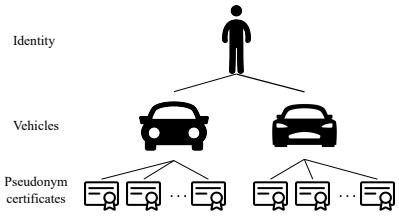

Figure 3. GSIT in Vehicular Network PKI

Conclusion

This work presents the GSIT methodology and illustrates its effectiveness through a practical implementation in vehicular network PKI. Our future research directions will concentrate on:

- Analyzing and enhancing security properties within various application contexts:
  - Collision resistance guarantees
  - Unforgeability guarantees
- Investigating potential applications of GSIT in different domains
- Exploring new opportunities for integration and adaptation

Acknowledgment

This work was partially supported by the National Science and Technology Council of Taiwan, under grants NSTC 112-2221-E-011 -094 -MY2, NSTC 112-2221-E-011 -092 -MY2, and NSTC 113-2634-F-011 -002 -MBK.