Poster: Efficient and Dynamic Witness-Free Certificate Revocation Using And-Tree Accumulator

Jheng-Jia Huang[1], Guan-Yu Chen[1*], Daisuke Inoue[2], Nai-Wei Lo[1], Yi-Fan Tseng[3], and Yu-Hung Wang[1]
[1]National Taiwan University of Science and Technology, Department of Information Management, Taipei, Taiwan
[2]National Institute of Information and Communications Technology, Tokyo, Japan
[3]National Chengchi University, Department of Computer Science, Taipei, Taiwan
{$*$ = The corresponding author: d11209103@mail.ntust.edu.tw}

***Abstract*—In large-scale vehicular networks, the Security Credential Management System (SCMS) ensures identity anonymity through numerous short-term pseudonym certificates. However, its Certificate Revocation List (CRL)-based revocation mechanism grows continuously over time, leading to significant transmission and verification overhead. To address this issue, this work proposes an efficient revocation architecture that integrates a bitwise AND-based accumulator with an And-Tree structure. The proposed design provides a scalable and efficient framework, enables lightweight witness-free verification, and supports dynamic revocation with low latency and high adaptability in large-scale SCMS environments.**

I. Introduction

With the rapid growth of Vehicle-to-Everything (V2X), ensuring secure and privacy-preserving vehicular communication has become a critical challenge. To address authentication and privacy issues, the U.S. Department of Transportation proposed the SCMS [1], which issues short-term pseudonym certificates to vehicles, enabling anonymous yet verifiable communication while preserving untraceability.

As illustrated in Fig. 1, the SCMS consists of two main processes: certificate issuance and revocation. In the issuance phase, the Linkage Authority (LA) generates pre-linkage values from an initial seed and sends them to the Registration Authority (RA), which forwards them to the Authorization Certificate Authority (ACA) to compute and embed linkage values into pseudonym certificates. This linkage values allows the system to revoke all certificates associated with the same vehicle while preserving anonymity.

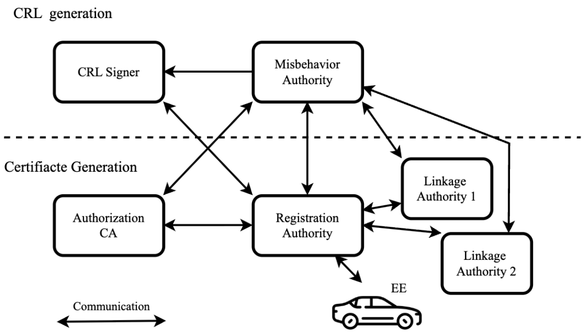

Fig. 1. Certificate Issuance and CRL Generation Architecture in SCMS

In the revocation phase, when the Misbehavior Authority (MA) identifies a malicious vehicle, it provides related data to the CRL Signer, which generates an updated CRL and forwards it to the Registration Authority (RA) for distribution to vehicles. Vehicles then derive possible linkage values from CRL seeds and compare them with those in their certificates. As revoked entries grow, the CRL size increases rapidly, causing significant transmission and verification overhead.

A. Challenges in Certificate Revocation

While the CRL-based mechanism guarantees verification correctness, it faces scalability and efficiency issues as the revocation list expands over time, causing high transmission and verification overhead. Cryptographic accumulators have been proposed to compress revocation data, but existing schemes still face key challenges:

- **High update cost:** Frequent revocations require recomputation of accumulators and witnesses.
- **Heavy computation:** RSA- and pairing-based accumulators are unsuitable for real-time vehicular environments.
- **Poor dynamic support:** Frequent synchronization accumulators and witnesses may cause version inconsistency.

B. Contributions

To overcome these challenges, we propose a lightweight and dynamically updatable revocation verification framework that integrates a *bitwise AND-based accumulator* with a hierarchical *And-Tree structure*. The design replaces traditional CRL comparisons with efficient bitwise operations, achieving data compression, rapid verification, and fast recomputation. Moreover, the *witness-free* architecture enables direct linkage-value verification without maintaining or synchronizing witnesses, significantly reducing computational and communication overhead. The main contributions are summarized as follows:

- **Scalable and efficient architecture:** Uses an *And-Tree* structure for hierarchical accumulation and localized updates, enhancing scalability and reducing recomputation.
- **Lightweight verification:** Utilizes *bitwise AND-based accumulator* to achieve data compression and enables witness-free verification with low computation cost.
- **Dynamic revocation support:** Enables real-time and adaptive verification as revocation lists evolve in large-scale SCMS environments.

II. Preliminaries

Fast Accumulated Hashing: Fast Accumulated Hashing, proposed by Nyberg [2], is a lightweight cryptographic accumulation method that compresses large data sets into short bit strings using bitwise operations.

Each element is hashed into a fixed-length binary string, divided into equal-sized blocks, and each block is mapped to 1 if nonzero or 0 otherwise, forming a binary vector. The vectors of all elements are then combined bit by bit using the AND operation to produce a compact accumulated value representing the entire set.

For verification, a queried element is transformed into its binary vector and compared with the accumulated value. If all zero bits in the query align with zeros in the accumulated value, the element is considered included.

III. Proposed Dynamic And-Tree Revocation Construction

To enhance the dynamic capability and scalability of the certificate revocation mechanism, this study proposes a hierarchical accumulation architecture based on an *And-Tree*, designed for efficient computation and recompute of certificate verification values (accumulated root values).

The And-Tree adopts a binary tree structure, where each leaf node corresponds to a revoked vehicle i ($i = 1, 2, \ldots, |CRL|$) in the CRL. For each revoked vehicle i, let $\{lv_{i1}, lv_{i2}, \ldots, lv_{im_i}\}$ denote its set of revoked linkage values. Each linkage value lv_{ij} is first hashed and mapped into a binary vector using the *Fast Accumulated Hashing* transformation:

$$h_{ij} = H(lv_{ij}) \Rightarrow (h_{ij1}, h_{ij2}, \ldots, h_{ijr}),$$

$$b_{ijk} = \begin{cases} 1, & \text{if } h_{ijk} \neq 0, \\ 0, & \text{otherwise,} \end{cases} \qquad b_{ij} = (b_{ij1}, b_{ij2}, \ldots, b_{ijr}),$$

where $H(\cdot)$ is a one-way hash function and r is the number of bit blocks.

The accumulated value of each revoked vehicle i is then computed by combining all its corresponding vectors via bitwise AND:

$$av_i = b_{i1} \wedge b_{i2} \wedge \cdots \wedge b_{im_i},$$

where $\wedge$ denotes the bitwise AND operation.

Each leaf node in the And-Tree stores the corresponding av_i. For higher levels, every parent node $p_{x,y}$ is derived by performing a bitwise AND operation on its two child nodes $c_{x+1,2y-1}$ and $c_{x+1,2y}$ as:

$$p_{x,y} = c_{x+1,2y-1} \wedge c_{x+1,2y}.$$

This process is recursively performed from the bottom up until the root node is obtained, which represents the accumulated root value.

Unlike static accumulation structures, the proposed And-Tree supports **modification**, **insertion**, and **deletion** operations, enabling localized updates when revocation data changes. Only affected branches are recomputed, significantly reducing reconstruction costs.

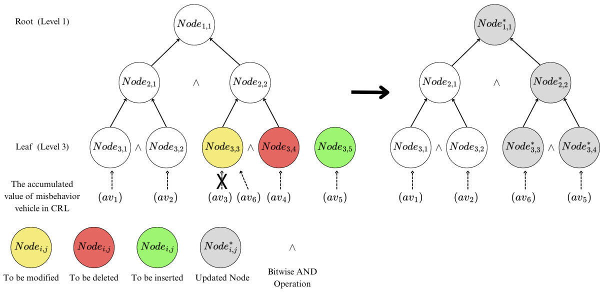

Fig. 2. Dynamic And-Tree Construction

As illustrated in Fig. 2, suppose node $node_{3,3}$ (yellow) is updated from av_3 to av_6, node $node_{3,4}$ (red) is deleted, and a new leaf $node_{3,5}$ (green) with value av_5 is inserted. In this case, only the right-side sub-branches are recalculated, and a new root node $node^*_{1,1}$ is produced, demonstrating the efficiency of dynamic updates.

During verification, the verifier computes the binary vector b_y from the linkage value in vehicle y's certificate and compares it with the accumulated root value r. If all zero bits in b_y align with zeros in r, the certificate is considered revoked; otherwise, it remains valid:

$$b_y \wedge r = b_y \;\Rightarrow\; \text{revoked.}$$

This design enables partial node updates and allows for rapid recomputation of the root node. By integrating a *bitwise and operations* for efficient computation and verification, the proposed *And-Tree* module achieves fast, lightweight, and scalable revocation verification.

IV. Conclusion

This work proposes an efficient certificate revocation verification framework that combines a *bitwise AND-based accumulator* with an *And-Tree structure* to reduce the transmission and verification costs of traditional CRLs in SCMS. The accumulator compresses CRL and enables verification without witnesses, while the And-Tree structure supports incremental updates and fast root recomputation. Overall, the framework provides a low-latency, scalable, and lightweight revocation mechanism for large-scale SCMS deployments.

Acknowledgment

This work was partially supported by the National Science and Technology Council of Taiwan, under grants NSTC 114-2221-E-011 -122 -, NSTC 114-2634-F-011 -002 -MBK, NSTC 114-2221-E-011 -115 - and NSTC 114-2634-F-004 -002 -MBK.

References

[1] *IEEE Std 1609.2.1-2022, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Certificate Management Interfaces for End Entities*, IEEE, 2022.

[2] K. Nyberg, "Fast accumulated hashing," in *Proceedings of the Third International Workshop on Fast Software Encryption*, Springer-Verlag, 1996, pp. 83–87.

Poster: Efficient and Dynamic Witness-Free Certificate Revocation Using And-Tree Accumulator

Authors: Jheng-Jia Huang[1], Guan-Yu Chen[1*], Daisuke Inoue[2], Nai-Wei Lo[1], Yi-Fan Tseng[3], and Yu-Hung Wang[1]

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

[2] National Institute of Information and Communications Technology, Tokyo, Japan

[3] National Chengchi University, Department of Computer Science, Taipei, Taiwan

{⋆ = The corresponding author: d11209103@mail.ntust.edu.tw}

Abstract

In large-scale vehicular networks, the Security Credential Management System (SCMS) preserves identity privacy through short-term pseudonym certificates; however, its CRL-based revocation mechanism grows continuously, resulting in substantial communication and verification overhead. In dense traffic scenarios, large CRLs may delay message verification, potentially impacting time-critical vehicular safety applications. This work proposes an efficient revocation architecture that combines a bitwise AND-based accumulator with a hierarchical And-Tree structure. The proposed framework enhances scalability, enables lightweight witness-free verification, and supports low-latency dynamic revocation in large-scale SCMS environments.

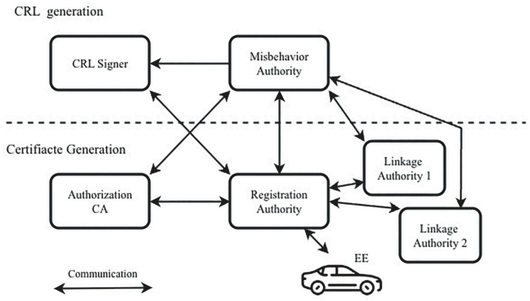

Figure 1. Certificate Issuance and CRL Generation Architecture in SCMS

Introduction

Background:

The SCMS enables secure and privacy-preserving vehicular communication through short-term pseudonym certificates. However, as revoked vehicles increase, CRL sizes grow rapidly, leading to significant communication and verification overhead.

Limitations of Existing Approaches:

CRL-based revocation guarantees correctness but **scales poorly**. While cryptographic accumulators reduce revocation data size, existing schemes suffer from **high update costs**, **heavy cryptographic computation**, and **limited support for dynamic revocation**.

Key Contributions:

- **Scalable architecture:** The And-Tree enables hierarchical accumulation and localized updates for efficient recomputation.
- **Lightweight verification:** A bitwise AND-based accumulator achieves compact data representation and witness-free verification.
- **Dynamic Revocation:** Supports real-time updates for evolving CRLs in SCMS.

Proposed Efficient Witness-Free Accumulator

Compute Accumulated Value of Vehicle:

- The *j*-th linkage value of vehicle *i* is hashed into a binary string and split into *r* segments.

$$h_{ij} = H(LV_{ij}) \Rightarrow (h_{ij1}, h_{ij2}, \ldots, h_{ijr})$$

- Each block h_{ijk} is mapped to 1 if its value is nonzero, otherwise 0, forming the binary vector b_{ij}.

$$b_{ijk} = \begin{cases} 1, & \text{if } h_{ijk} \neq 0, \\ 0, & \text{otherwise,} \end{cases} \quad b_{ij} = (b_{ij1}, b_{ij2}, \ldots, b_{ijr})$$

- All binary vectors of vehicle *i* are combined bit by bit using AND to generate one compact value av_i that represents the vehicle's revoked linkage values.

$$av_i = b_{i1} \wedge b_{i2} \wedge \cdots \wedge b_{im_i}$$

Compute Verification Value of All Vehicles :

- Bitwise AND all accumulated values from every vehicle.

$$r = av_1 \wedge av_2 \wedge \cdots \wedge av_i$$

Verify vehicle certificates :

- The bit vector b_y derived from the certificate's linkage value, is compared with *r*; if all zero bits match, the certificate is revoked.

$$b_y \wedge r = b_y \;\Rightarrow\; \text{revoked}$$

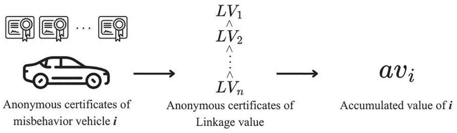
LV_1
$\wedge$
LV_2
$\wedge$
$\wedge$
LV_n
av_i
Anonymous certificates of misbehavior vehicle *i*
Anonymous certificates of Linkage value
Accumulated value of *i*

Figure 2. How to compute accumulate value of vehicle

Proposed Dynamic And-Tree Revocation Construction

We propose a **lightweight** and **dynamic** revocation framework that integrates a **bitwise AND-based accumulator** with a **hierarchical And-Tree** structure. This design achieves **efficient data compression**, **witness-free verification**, and **fast recomputation** through localized updates, significantly reducing CRL transmission and verification overhead.

Node Setting:

- Each leaf node represents the accumulated value (*av*) of a revoked vehicle in the CRL.
- Each parent node is derived by combining its two child nodes using

$$p_{x,y} = c_{x+1,2y-1} \wedge c_{x+1,2y}$$

Dynamic Update:

The And-Tree supports **modification, insertion, and deletion** of revoked entries, adapting as the CRL evolves. Only the affected leaf and ancestor nodes are recomputed to refresh the root, avoiding full reconstruction. This localized update achieves an efficient O(log n) cost, enabling real-time, low-latency, and scalable revocation management.

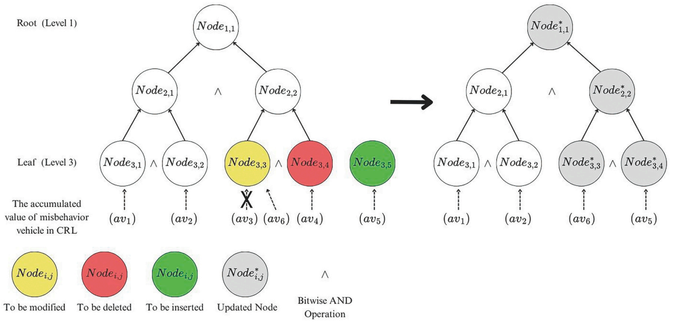

Figure 3. Dynamic And-Tree Construction

Conclusion

We propose a **scalable** and **lightweight** revocation framework for SCMS that supports **witness-free verification** and **efficient dynamic updates**. Future work will focus on real-world deployment and comprehensive security and performance evaluation.

Acknowledgment

This work was partially supported by the National Science and Technology Council of Taiwan, under grants NSTC 114-2221-E-011 -122 -, NSTC 114-2634-F-011 -002 -MBK, NSTC 114-2221-E-011 -115 - and NSTC 114-2634-F-004 -002 -MBK.