Revocable and Conditionally Anonymous Certificateless Authentication for VANETs

Peiyong Sun[1], Yangfan Liang[2], Mingrong Xiang[3], Yining Liu[3]*

[1] School of Computer Science, Henan Institute of Information Science and Technology, China
[2] College of Information Science and Engineering, Jiaxing University, China
[3] School of Data Science and Artificial Intelligence, Wenzhou University of Technology, China
754630794@qq.com, afarloeng@zjxu.edu.cn, mingrong.xiang@hotmail.com, 20240035@wzut.edu.cn

Abstract

Vehicular Ad-hoc Networks (VANETs) serve as the cornerstone of Intelligent Transportation Systems (ITS), facilitating real-time communication between vehicles and infrastructure to enhance road safety and traffic efficiency. However, authentication schemes in VANETs still face several issues, such as high computational overhead, neglect of conditional privacy, lack of revocation mechanisms, and disregard for physical security. To address these challenges, we propose a Revocable and Conditionally Anonymous Certificateless Authentication Scheme with Anti-Physical Theft Protection. First, this scheme employs a pairing-free certificateless aggregate signature to significantly improve computational efficiency. Second, we design a conditional anonymity mechanism that dynamically assigns pseudonyms to conceal a vehicle's real identity while allowing a trusted authority (TA) to recover the true identity when necessary. Moreover, this scheme adopts a Dynamic Sparse Merkle Tree (DSMT) to achieve efficient pseudonym revocation, enabling real-time identity management without incurring excessive communication overhead. Meanwhile, recognizing the threat of physical attacks, the scheme enhances security by integrating Physical Unclonable Functions (PUFs) and fuzzy extractors, which bind cryptographic keys to unique hardware characteristics to resist physical extraction attacks. Finally, rigorous security analysis and performance evaluations confirm that the proposed scheme outperforms existing approaches in both reliability and efficiency.

Keywords: VANETs, Authentication, Conditional anonymity, Dynamic Sparse Merkle Tree, Physical Unclonable Functions

1 Introduction

Vehicular Ad-hoc Networks (VANETs), a key component of Intelligent Transportation Systems (ITS), enable real-time communication among vehicles and roadside infrastructure, supporting applications such as collision warning and traffic scheduling while improving road safety and efficiency. Hence, secure authentication is essential to prevent message tampering, identity forgery, and malicious attacks [1].

In recent years, certificateless aggregate signature (CLAS) schemes have been widely studied for VANETs [2-4], improving authentication efficiency in V2V and V2I communications through batch verification. However, most existing schemes rely on bilinear pairing operations [5], whose high computational complexity limits their applicability in latency-sensitive scenarios. To address this, pairing-free ECC-based schemes have been explored to reduce overhead.

Anonymity is critical for privacy protection, but excessive anonymity may hinder traceability, increasing the risk of malicious misuse. Therefore, conditional anonymity has emerged as an effective solution to balance privacy and accountability [6].

Beyond efficiency and privacy, revocation is essential for system security [7], allowing compromised nodes to be promptly excluded. Additionally, with increasing hardware integration in vehicles, VANETs face growing physical-layer threats [8], making lightweight hardware-assisted security mechanisms necessary to protect sensitive credentials.

1.1 Motivation and Contributions

Balancing authentication and privacy in VANETs requires both efficiency and strong security, yet existing schemes still face several limitations:

1) Inefficient Authentication: Many schemes rely on bilinear pairing [9-12], leading to high computational cost and latency.

2) Lack of Traceability: Overemphasis on anonymity often neglects traceability, making malicious behavior unidentifiable [13-16].

3) No Effective Revocation: Existing protocols often lack efficient revocation, allowing compromised vehicles to continue participating [3, 5, 13, 17-19].

4) Weak Physical Security: Many schemes ignore hardware-level protection, exposing keys to physical attacks [14, 19-24].

To address these issues, we propose a certificateless authentication scheme for VANETs with the following contributions:

1) Efficient Authentication: We design a pairing-free certificateless aggregate signature scheme based on

*Corresponding Author: Mingrong Xiang; Email: mingrong.xiang@hotmail.com
DOI: https://doi.org/10.70003/160792642026092705014

ECC, enabling RSUs to perform batch verification in O(n) time. Compared with bilinear pairing-based schemes [9-12], our approach eliminates expensive pairing operations, significantly reducing computational overhead and verification latency (see Section VII).

2) Conditional Anonymity: To balance anonymity and traceability [13-16], we adopt a pseudonym-based mechanism where vehicles communicate using TA-issued pseudonyms. While identities remain hidden under normal conditions, the TA can recover real identities when necessary, ensuring accountability (see Section VI.C).

3) Efficient Revocation: Addressing the lack of revocation in existing works [3, 5, 13, 17-19], we introduce a Dynamic Sparse Merkle Tree (DSMT) to support efficient pseudonym revocation. Revoked pseudonyms are updated via Merkle root recomputation without key reissuance, enabling fast verification (see Section VI.C).

4) Anti-Physical Theft: We enhance physical security by integrating PUFs and fuzzy extractors to bind private keys to hardware-specific CRPs, preventing key extraction. This approach improves resistance to physical attacks compared with [14, 19-24] (see Section VI.C).

1.2 Paper Structure Overview

Section II surveys related work in vehicular authentication. Section III covers essential preliminaries. Section IV presents the system model and security objectives. Section V details the RCACAS algorithms. Section VI offers formal security proofs. Section VII evaluates performance against existing schemes. Section VIII concludes and outlines future work.

2 Related Work

To address the challenges of user privacy and data security in VANETs, the academic community has proposed various authentication schemes. Early public key infrastructure (PKI) based approaches [11] bind public keys to user identities through a certificate authority (CA), yet incur high certificate management overhead. While Shamir's identity-based cryptography (IBC) [25] eliminates certificate requirements, it introduces security risks due to key escrow issues. Al-Riyami and Paterson [26] subsequently proposed certificateless cryptography (CL-PKC), which mitigates both certificate management and key escrow problems, laying the foundation for certificateless aggregate signature (CLAS) schemes.

For efficiency optimization, Boneh *et al.* [27] pioneered aggregate signature (AS) technology to streamline verification in multi-signature scenarios. Castro and Dahab [28] first integrated AS with CL-PKC, but their bilinear pairing-dependent design struggled to meet VANETs' scalability demands. Subsequent bilinear pairing-based certificateless aggregate authentication protocols [9-12] were proposed, yet their high computational complexity still caused verification delays in large-scale vehicular networks.

To reduce pairing computation overhead, pairing-free certificateless aggregate authentication protocols [5, 13-16] have emerged as a research focus. For instance, Yang *et al.* [5] designed a CLAS scheme based on the elliptic curve discrete logarithm problem (ECDLP), though such schemes generally lack support for conditional anonymity.

As a critical balance between privacy preservation and security accountability, conditional anonymity enables anonymous communication while permitting authorized entities to reveal user identities when necessary. Addressing this requirement, Wu *et al.* [18] implemented conditional anonymity through dynamic pseudonym generation and trusted third-party key management, with similar mechanisms proposed in [5, 17-19]. However, these protocols fail to incorporate revocation mechanisms for traced malicious entities, leaving systems persistently vulnerable to unauthorized access risks.

Furthermore, PUFs offer novel hardware security solutions for VANETs, yet existing studies [14, 19-24] predominantly neglect physical-layer protection, rendering systems susceptible to hardware side-channel attacks and key extraction threats.

In summary, although pairing-free ECC-based CLAS schemes for VANETs enhance efficiency and basic security, they often lack conditional anonymity, expose private keys, and suffer delayed revocation. Building an integrated framework with anonymity, PUF-based hardware protection, and scalable revocation remains challenging. We address this by co-designing a certificateless protocol that integrates dynamic pseudonyms, PUF-key binding, and dynamic sparse Merkle trees to satisfy privacy and large-scale security requirements.

3 Preliminaries

This section introduces essential concepts and methodologies that form the foundation of our research.

3.1 Elliptic Curve Cryptography (ECC)}

ECC utilizes elliptic curves over finite fields $\mathbb{F}_p$ defined by $y^2 = x^3 + ax + b$ with $4a^3 + 27b^2 \neq 0$. Its points and a point-at-infinity form an abelian group under addition. ECC provides security equivalent to traditional public-key systems with shorter keys, ideal for resource-constrained environments. Security relies on the intractability of the Elliptic Curve Discrete Logarithm Problem: computing k from $Q = kP$ is infeasible, even though Q can be efficiently derived.

3.2 Collision-Resistant Hash Functions

A hash function H is collision-resistant if it is computationally infeasible to find two distinct inputs x_1 and x_2 such that $H(x_1) = H(x_2)$. This property is crucial for ensuring the integrity of data in cryptographic protocols. Formally, a hash function H is collision-resistant if for any probabilistic polynomial-time (PPT) algorithm A, the probability of finding a collision is negligible.

3.3 Physical Unclonable Functions (PUFs)

PUFs are hardware-based security primitives that leverage inherent manufacturing variations to produce unique responses. For a challenge ch, the response $res = PUF(ch)$ forms an unclonable Challenge-Response Pair (CRP), providing tamper-resistant assurance for cryptographic key generation.

3.4 Fuzzy Extractor

A fuzzy extractor generates stable cryptographic keys from noisy inputs (e.g., PUF responses). It tolerates minor variations via two algorithms:

1) Gen: Extracts key R and helper data P from input w;

2) Rep: Recovers R from noisy w' and P, despite environmental/hardware variations.

3.5 Merkle Tree

A Merkle tree is a hierarchical structure that verifies data integrity efficiently. Leaf nodes store hashes of raw data, while non-leaf nodes contain hashes of their children. The root hash (Merkle root) acts as a compact digest of the entire dataset. Any modification to a leaf propagates upward, altering the root and enabling tamper detection in $O(\log n)$ time.

3.6 Notation Table

This subsection presents Table 1, which consolidates the notations and their corresponding definitions used throughout the paper.

Table 1. Notations and descriptions

Symbol	Description
G	Elliptic curve additive cyclic group
P	Generator of G
p	Prime order of the finite field F_p
s	Master private key of KGC
P_{pub}	Master public key: $P_{pub} = sP$
H_0, H_1, H_2, H_3	Collision-resistant hash functions
ID_i	Real identity of vehicle V_i
PID_i	Pseudonym of V_i
(a_i, A_i)	Secret value pair: $A_i = a_iP$
(c_i, R_{1i})	Partial private key from KGC
(SK_i, Q_i)	Full private-public key pair: $SK_i = (a_i, c_i, q_i)$, $Q_i = q_iP$
$\sigma_i = (R_i, z_i)$	Individual signature for message M_i
$\sigma_{agg} = (R, z)$	Aggregate signature
t_i	Timestamp for freshness
Δt	Maximum allowable time delay

4 System Model

As shown in Figure 1, this section presents the system architecture, threat model, and design goals of RCACAS, aiming to ensure secure, efficient, and privacy-preserving communication in VANETs.

4.1 System Architecture

The proposed system architecture consists of five entities:

1) Key Generation Center (KGC): Generates system parameters and partial private keys without accessing full private keys, avoiding key escrow.

2) Trusted Authority (TA): Issues pseudonyms for anonymity, supports identity tracing, and revokes malicious vehicles.

3) Vehicles: Generate full private keys by combining secret values with KGC-issued partial keys and use pseudonyms for secure communication.

4) Roadside Units (RSUs): Verify and aggregate vehicle signatures, forwarding authenticated data to the TMC.

5) Traffic Management Center (TMC): Performs aggregate verification, coordinates with TA for tracing, and manages traffic operations.

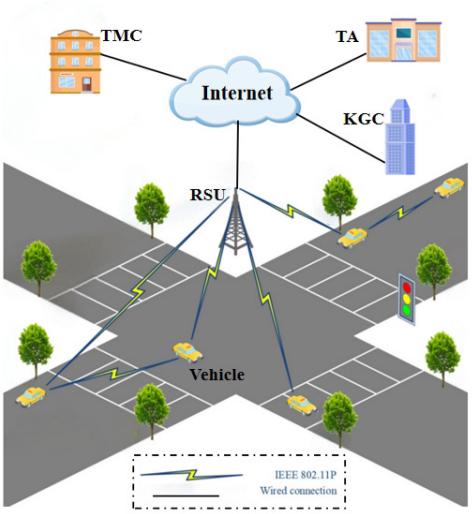

Figure 1. System model

4.2 Security Model

Our scheme resists three adversary types under certificateless cryptography:

Type-I $\mathcal{A}_1$: External attackers replacing public keys without KGC's master key.

Type-II $\mathcal{A}_2$: Malicious KGC holding msk but unable to replace public keys.

Type-III $\mathcal{A}_3$: Colluding users forging aggregate signatures with invalid components.

4.3 Design Objectives

Our scheme fulfills seven core security requirements:

1) Authentication: Ensure only authorized vehicles/RSUs generate valid signatures, preventing impersonation and forgery.

2) Integrity: Detect message tampering through cryptographic verification mechanisms.

3) Conditional Anonymity: Protect vehicle identities using pseudonyms while enabling TA-authorized tracing.

4) Unlinkability: Prevent message correlation to thwart vehicle tracking attempts.

5) Replay Resistance: Implement freshness guarantees via timestamp/nonce validation.

6) Physical Attack Resistance: Secure storage for

private keys and pseudonyms in OBUs/RSUs.

7) Revocability: Immediate credential revocation for compromised entities.

5 Our RCACAS Scheme

This section describes the algorithms and applications of RCACAS.

5.1 Algorithm Definition

The RCACAS scheme contains nine key algorithms.

Algorithm 1. System Setup (SS)
Input: Security parameter λ
Output: System parameters *params*, master secret s
1. Select elliptic curve group $\mathbb{G}$ with generator P of prime order p;
2. Generate master private key $s \xleftarrow{\$} \mathbb{Z}_p^*$;
3. Compute master public key $P_{\text{pub}} \leftarrow sP$;
4. Choose hash functions: H_0, H_1, H_2, H_3;
5. Define *params* $\leftarrow \langle \mathbb{G}, P, P_{\text{pub}}, H_0, H_1, H_2, H_3 \rangle$;
6. **Return** (*params*, *s*);

Algorithm 2. Partial Private Key Generation (PPKG)
Input: Master secret s, pseudonym PID_i
Output: Partial private key (c_i, R_{1i})
1. Select random $r_{1i} \xleftarrow{\$} \mathbb{Z}_p^*$;
2. Compute $R_{1i} \leftarrow r_{1i}P$;
3. Calculate $c_i \leftarrow r_{1i} + s \cdot H_1(PID_i \| R_{1i}) \bmod p$;
4. **Return** (c_i, R_{1i});

Algorithm 3. Secret Value Setup (SVS)
Input: Security parameter λ
Output: Secret pair (a_i, A_i)
1. Vehicle V_i selects $a_i \xleftarrow{\$} \mathbb{Z}_p^*$;
2. Compute public component $A_i \leftarrow a_iP$;
3. Register (ID_i, A_i) with Trusted Authority (TA);
4. **Return** (a_i, A_i);

Algorithm 4. Pseudonym Generation (PG)
Input: Real identity ID_i, public key A_i
Output: Pseudonym (PID_i, TP_i)
1. TA selects ephemeral key $k \xleftarrow{\$} \mathbb{Z}_p^*$;
2. Generate timestamp TP_i;
3. Compute $PID_i \leftarrow ID_i \oplus H_0(TP_i, P_{\text{pub}}, kA_i)$;
4. Update DSMT with $H_2(PID_i)$;
5. **Return** (PID_i, TP_i);

Algorithm 5. Private Key Generation (PKG)
Input: Partial private key c_i, secret value a_i
Output: Full key pair (Sk_i, Q_i)
1. Select random $q_i \xleftarrow{\$} \mathbb{Z}_p^*$;
2. Compute public component $Q_i \leftarrow q_iP$;
3. Embed PUF module for SK_i protection;
4. Set $Sk_i \leftarrow (a_i, c_i, q_i)$;
5. **Return** (Sk_i, Q_i);

Algorithm 6. Signature Generation (SG)
Input: Message M_i, timestamp t_i, private key SK_i
Output: Signature $Sig_i = (R_i, z_i)$
1. Select random $r_{2i} \xleftarrow{\$} \mathbb{Z}_p^*$;
2. Compute $R_{2i} \leftarrow r_{2i}P$;
3. Calculate $v_i \leftarrow H_3(M_i \| t_i \| PID_i \| R_{2i} \| Q_i)$;
4. Compute $z_i \leftarrow r_{2i} + c_i + q_i \cdot v_i \bmod p$;
5. Set $R_i \leftarrow R_{1i} + R_{2i}$;
6. **Return** (R_i, z_i);

Algorithm 7. Signature Verification (SV)
Input: Signature Sig_i, message M_i, public key Q_i
Output: Validation result
1. Verify $z_iP \stackrel{?}{=} R_i + P_{\text{pub}} \cdot H_1(PID_i \| R_{1i}) + Q_i \cdot v_i$;
2. Check timestamp freshness $|t_{\text{current}} - t_i| \le \Delta t$;
3. **Return** *Valid if both conditions hold, else Invalid*;

Algorithm 8. Signature Aggregation (SA)
Input: Signatures $\{Sig_1, \ldots, Sig_n\}$
Output: Aggregate signature $Sig_{\text{agg}} = (R, z)$
1. Compute $R \leftarrow \sum_{i=1}^{n} R_i$;
2. Compute $z \leftarrow \sum_{i=1}^{n} z_i$;
3. **Return** (R, z);

Algorithm 9. Aggregate Verification (AV)
Input: Aggregate signature Sig_{agg}, messages $\{M_i\}$, public keys $\{Q_i\}$ (for $1 \le i \le n$)
Output: Batch validation result
1. Verify $zP \stackrel{?}{=} R + P_{\text{pub}} \cdot \sum_{i=1}^{n} H_1(PID_i \| R_{1i}) + v_i \cdot \sum_{i=1}^{n} Q_i$;
2. Check freshness of all timestamps $\{t_i\}$;
3. **Return** *Valid if all conditions hold, else Invalid*;

5.2 Scheme Application

The proposed RCACAS scheme operates through four coordinated phases: system initialization, vehicle registration, secure data exchange, and revocation/tracing.

1) System Initialization Phase

This phase establishes foundational cryptographic

parameters and authority roles.

Step 1 (KGC Setup): The Key Generation Center (KGC) executes System Setup (Algorithm 1):

- Generates elliptic curve group G with generator P.
- Selects master private key $s \in \mathbb{Z}^*_p$ and computes $P_{\text{pub}} = sP$.
- Publishes system parameters params = $\langle G, P, P_{\text{pub}}, H_0, H_1, H_2, H_3 \rangle$.

Step 2 (TA Initialization): The Trusted Authority (TA):

- Prepares Dynamic Sparse Merkle Tree (DSMT) for pseudonym management.
- Generates a secret tracing key $k \in \mathbb{Z}^*_p$ for identity recovery.

2) Vehicle Registration Phase

Vehicles acquire cryptographic credentials while preserving anonymity.

Step 1 (Secret Value Generation): Vehicle V_i runs Secret Value Setup (Algorithm 3):

- Selects secret $a_i \in \mathbb{Z}^*_p$, computes $A_i = a_i P$.
- Registers (ID_i, A_i) with TA via secure channel.

Step 2 (Pseudonym Assignment): TA executes Pseudonym Generation (Algorithm 4):

- Generates timestamped pseudonym $PID_i = ID_i \oplus H_0(TP_i, P_{\text{pub}}, kA_i)$.
- Updates DSMT with $H_2(PID_i)$ as leaf node.
- Distributes (PID_i, TP_i) to V_i .

Step 3 (Key Generation): KGC and V_i collaborate:

KGC runs *Partial Private Key Generation (Algorithm 2)* to produce (c_i, R_{1i}).

V_i executes *Private Key Generation (Algorithm 5)* by first generating the full private key $SK_i = (a_i, c_i, q_i)$ and corresponding public key $Q_i = q_i P$. To enhance physical security through PUF integration, the vehicle then: (1) generating challenge-response pairs (ch_i, res_i) where $res_i = PUF(ch_i)$; (2) deriving secure key material (w_i, hd_i) ← FuzzyExtractor.Gen(res_i); (3) computing the verification value $Ver_i = H_2(a_i, c_i, q_i, ID_i, PID_i, ch_i, w_i, hd_i)$; (4) and finally storing (ch_i, Ver_i) in tamper-proof storage.

3) Secure Data Exchange Phase

Vehicles authenticate messages and RSUs perform efficient verification.

Step 1 (PUF-Based Integrity Check): Before signing, V_i verifies hardware integrity:

- Recomputes $res'_i = PUF(ch_i)$.
- Regenerates $w'_i = FuzzyExtractor.Rep(res'_i, hd_i)$.
- Validates $Ver'_i = H_2(a_i, c_i, q_i, ID_i, PID_i, ch_i, w'_i, hd_i)$.
- Proceeds only if $Ver'_i = Ver_i$; otherwise, aborts.

Step 2 (Message Signing): V_i runs *Signature Generation (Algorithm 6)* for message M_i :

- Selects $r_{2i} \in \mathbb{Z}^*_p$, computes $R_{2i} = r_{2i} P$.
- Generates signature $\sigma_i = (R_i, z_i)$ where $R_i = R_{1i} + R_{2i}$ and $z_i = r_{2i} + c_i + q_i H_3(M_i \| t_i \| PID_i \| R_{2i} \| Q_i)$.
- .roadcasts $\{M_i, t_i, R_{2i}, PID_i, \sigma_i\}$.

Step 3 (Single Signature Verification): RSU verifies via *Signature Verification (Algorithm 7)*:

- Checks freshness: $|t_{\text{current}} - t_i| \le \Delta t$.
- Validates

$$z_i P \stackrel{?}{=} R_i + P_{\text{pub}} H_1(\text{PID}_i \| R_{1i}) + Q_i H_3(M_i \| \text{PID}_i \| R_{2i} \| Q_i)$$

Step 4 (Signature Aggregation): RSU executes *Signature Aggregation (Algorithm 8)* for n messages:

- Computes $R = \sum_{i=1}^{n} R_i$, $z = \sum_{i=1}^{n} z_i$.
- Transmits aggregate signature $\sigma_{\text{agg}} = (R, z)$ and message set to TMC.

Step 5 (Batch Verification): TMC performs *Aggregate Verification (Algorithm 9)*:

$$zP \stackrel{?}{=} R + P_{\text{pub}} \sum_{i=1}^{n} H_1(PID_i \| R_{1i}) + \sum_{i=1}^{n} Q_i H_3(M_i \| PID_i \| R_{2i} \| Q_i)$$

4) Revocation and Tracing Phase

Malicious vehicles are revoked while preserving system integrity.

Step 1 (Identity Tracing): TA recovers real identity from pseudonym:

- Computes $ID_i = PID_i \oplus H_0(TP_i, P_{\text{pub}}, kA_i)$.

Step 2 (Pseudonym Revocation): TA updates DSMT:

- Replaces $H_2(PID_i)$ with $H_2(0)$ in Merkle tree.
- Recomputes and broadcasts updated Merkle root.

Step 3 (System Synchronization): All entities verify revocation status using latest Merkle root, rejecting messages from revoked PID_i.

This structured implementation ensures computational efficiency through elliptic curve operations and pairing-free design, while the DSMT-based revocation mechanism provides real-time responsiveness to security threats. The PUF integration strengthens resistance against physical attacks, aligning with the security objectives outlined in Section IV.D.

6 Security Analysis

In this section, we provide a correctness proof and a security proof for our proposed RCACAS scheme.

6.1 Proof of Correctness

1) Signature Generation and Verification

Signature Generation Phase:

Each vehicle V_i generates a signature $Sig_i = (R_i, z_i)$ as follows:

- Compute $R_{2i} = r_{2i} P$
- Compute $V_i = H_3(M_i \| t_i \| PID_i \| R_{2i} \| Q_i)$
- Compute $z_i = r_{2i} + c_i + q_i v_i$

Verification Phase:

The RSU verifies the signature by checking:

$$z_i P = R_i + P_{pub} H_1(PID_i \| R_{1i}) + Q_i H_3(M_i \| PID_i \| R_{2i} \| Q_i)$$

Proof:

$$\begin{aligned} z_i P &= (r_{2i} + c_i + q_i v_i) P \\ &= r_{2i} P + c_i P + q_i v_i P \\ &= R_{2i} + \underbrace{c_i P}_{R_{1i} + sH_1(\cdot)P} + q_i H_3(\cdot) P \end{aligned}$$

$$= R_{2i} + R_{1i} + sH_1(PID_i \| R_{1i})P + q_iH_3(M_i \| t_i \| PID_i \| R_{2i} \| Q_i)P$$
$$= \underbrace{R_{2i} + R_{1i}}_{R_i} + P_{pub}H_1(\cdot) + Q_iH_3(\cdot)$$

2) Aggregation and Verification

Aggregation Phase:

The RSU aggregates signatures as:

$$R = \sum_{i=1}^{n} R_i,$$

$$z = \sum_{i=1}^{n} z_i$$

Verification Phase:

The TMC verifies the aggregate signature by checking:

$$zP = R + P_{pub}\sum_{i=1}^{n} H_1(PID_i \| R_{1i}) + \sum_{i=1}^{n} Q_iH_3(M_i \| PID_i \| R_{2i} \| Q_i)$$

Proof:

$$zP = \left(\sum_{i=1}^{n} z_i\right)P$$
$$= \sum_{i=1}^{n}\left[R_i + P_{pub}H_1(\cdot) + Q_iH_3(\cdot)\right]$$
$$= \underbrace{\sum_{i=1}^{n} R_i}_{R} + P_{pub}\sum_{i=1}^{n} H_1(\cdot)$$
$$+\sum_{i=1}^{n} Q_iH_3(M_i \| PID_i \| R_{2i} \| Q_i)$$

6.2 Formal Proof

This subsection provides a rigorous formal analysis of the RCACAS scheme under the random oracle model (ROM), addressing existential unforgeability, conditional anonymity, and aggregate unforgeability. Each proof is structured to align with the security model (Section V) and design objectives (Section IV.D).

Theorem 1 (Unforgeability)

The RCACAS scheme is existentially unforgeable against adaptive chosen-message attacks (EUF-CMA) under the ECDL and CDH assumptions, resisting all three adversary types (Type-I, II, III).

Proof Structure:

The proof is divided into three lemmas, each addressing a specific adversary type.

Lemma 1 (Resistance to Type-I Adversary)

Let $\mathcal{A}_1$ be a Type-I adversary (public-key replacement attacker) making q_{H_i} hash queries (i = 0, 1, 2, 3), q_{PPK} partial-private-key queries and q_{SV} secret value queries. If $\mathcal{A}_1$ forges a signature with non-negligible advantage ε, the ECDL problem can be solved with probability:

$$Adv_{\mathcal{C}}^{\text{ECDL}} \geq \varepsilon\left(1-\frac{1}{q_{H_1}}\right)^{q_{PPK}}\left(1-\frac{q_{SV}}{2^{\lambda}}\right)\frac{1}{q_{H_1}q_{H_3}}.$$

Proof:

Setup Phase:

Input: Challenger $\mathcal{C}$ receives an ECDL instance (P, $Q = vP$).

System Initialization:

- $\mathcal{C}$ sets $P_{\text{pub}} = sP$, where $s \xleftarrow{\$} \mathbb{Z}_p^*$.
- $\mathcal{C}$ publishes system parameters params = $\langle G, P, P_{\text{pub}}, H_0, H_1, H_2, H_3\rangle$.

Target Identity Setup:

- $\mathcal{C}$ selects a target identity ID_I and embeds $Q = vP$ into its pseudonym PID_I by setting $A_I = Q$.
- The pseudonym is computed as $PID_I = ID_I \oplus H_0(TP_I, P_{\text{pub}}, kQ)$, where $k \xleftarrow{\$} \mathbb{Z}_p^*$ is the TA's secret.

Query Phase:

User-Creation Query:

- For $ID_i \neq ID_I$, $\mathcal{C}$ generates (a_i, A_i) normall: $a_i \xleftarrow{\$} \mathbb{Z}_p^*$, $A_i = a_iP$.
- For ID_I, *mathcalC* sets $A_I = Q$ and simulates PID_I without knowing v.

Partial-Private-Key Query:

- If $\mathcal{A}_1$ queries PID_I, $\mathcal{C}$ aborts.
- For other identities, $\mathcal{C}$ returns $c_i = r_{1i} + s \cdot H_1(PID_i \| R_{1i})$, where $r_{1i} \xleftarrow{\$} \mathbb{Z}_p^*$ and $R_{1i} = r_{1i}P$.

Public-Key-Replacement Query:

- $\mathcal{C}$ records replaced public keys but blocks replacements for PID_I.

H_3 Query Simulation:

- $\mathcal{C}$ maintains a list L_{H_3} of tuples (M_i, PID_i, R_{2i}, Q_i, v_i).
- For each query, $\mathcal{C}$ randomly selects $v_i \xleftarrow{\$} \mathbb{Z}_p^*$, stores the tuple, and returns v_i.

Signing Query:

- For $PID_i \neq ID_I$, $\mathcal{C}$ generates valid signatures using $z_i = r_{2i} + c_i + q_iv_i$.
- For PID_I, $\mathcal{C}$ simulates $z_I = r_{2i} + c_i + q_iv_i$ by programming $H_3(M_i \| PID_I \| R_{2i} \| Q) = v_i$.

Forgery Phase:

Forgery Output: $\mathcal{A}_1$ outputs a forgery $\sigma^* = (R^*, z^*)$ for (PID^*, M^*).

Abort Condition: If $PID^* \neq PID_I$, $\mathcal{C}$ aborts.

Forking Lemma Application:

$\mathcal{C}$ rewinds $\mathcal{A}_1$ with the same randomness but different H_3 outputs to obtain two forgeries (z^*, v^*) and ($z^{*'}$, $v^{*'}$).

From the two equations: $z^* = r_2^* + c^* + q^*v^*$, $z^{*'} = r_2^* + c^* + q^*v^{*'}$,

$\mathcal{C}$ solves for v:

$$v = \frac{z^* - z^{*'}}{v^* - v^{*'}} \mod p.$$

Probability Analysis:

Event E_1: $\mathcal{C}$ does not abort during partial-private-key queries.

$$\Pr[E_1] \geq \left(1-\frac{1}{q_{H_1}}\right)^{q_{PPK}}.$$

Event E_2: $\mathcal{A}_1$ selects PID_I as the target.

$$\Pr[E_2 \mid E_1] = \frac{1}{q_{H_1}}.$$

Event E_3: $\mathcal{A}_1$ queries H_3 o PID_I.

$$\Pr[E_3 \mid E_1 \wedge E_2] = \frac{1}{q_{H_3}}.$$

Total Success Probability:

$$Adv_{\mathcal{C}}^{\text{ECDL}} \geq \varepsilon \cdot \Pr[E_1] \cdot \Pr[E_2 \mid E_1] \cdot \Pr[E_3 \mid E_1 \wedge E_2] \cdot \left(1 - \frac{q_{SV}}{2^{\lambda}}\right).$$

Lemma 2 (Resistance to Type-II Adversary)

Let $\mathcal{A}_2$ (malicious KGC) make qH_i hash queries and q_{SV} secret-value queries. If $\mathcal{A}_2$ forges a signature with advantage ε, the ECDL problem is solvable with probability:

$$\text{Adv}_{\mathcal{C}}^{\text{ECDL}} \geq \varepsilon \left(1 - \frac{1}{q_{H_1}}\right)^{q_{SV}} \frac{1}{q_{H_3}}$$

Proof:

Setup Phase:

- $\mathcal{C}$ provides the master key s to $\mathcal{A}_2$ but embeds an ECDL instance $Q = vP$ into a user's public key $A_I = Q$.

Query Handling:

Secret-Value Extraction:

- If $\mathcal{A}_2$ queries a_I, $\mathcal{C}$ aborts.
- For other identities, $\mathcal{C}$ returns a_i.

Signing Queries:

- For PID_I, $\mathcal{C}$ programs $H_3(M_i \| PID_I \| R_{2i} \| Q) = v_i$.
- $\mathcal{C}$ computes $z_i = r_{2i} + c_i + q_i v_i$ using simulated $c_i = r_{1i} + s \cdot H_1(PID_I \| R_{1i})$.

Forgery Extraction:

- $\mathcal{A}_2$ outputs a forgery $\sigma^* = (R^*, z^*)$.
- Using the Forking Lemma, $\mathcal{C}$ extracts:

$$v = \frac{z^* - c_i - r_{2i}}{v_i} \mod p.$$

Probability Analysis:

- Event E_1: $\mathcal{C}$ does not abort during secret-value queries.

$$\Pr[E_1] \geq \left(1 - \frac{1}{q_{H_1}}\right)^{q_{SV}}.$$

- Event E_2: $\mathcal{A}_2$ queries H_3 on PID_I.

$$Pr[E_2 \mid E_1] = \frac{1}{q_{H_3}}.$$

Total Advantage:

$$\text{Adv}_{\mathcal{C}}^{\text{ECDL}} \geq \varepsilon \cdot \Pr[E_1] \cdot \Pr[E_2 \mid E_1].$$

Lemma 3 (Resistance to Type-III Adversary)

Let $\mathcal{A}_3$ (colluding users) make q_{H_i} hash queries and q_{PK} private-key queries. If $\mathcal{A}_3$ forges an aggregate signature with advantage ε, the CDH problem can be solved with probability:

$$\text{Adv}_{\mathcal{C}}^{\text{CDH}} \geq \varepsilon \left(1 - \frac{1}{q_{H_2}}\right)^{q_{PK}} \frac{1}{q_{H_3}}.$$

Proof:

Setup Phase:

- $\mathcal{C}$ receives a CDH instance (P, aP, bP) and embeds \$aP\$ into $Q_j = aP$ and bP into $R_{2j}^* = bP$.

Query Handling:

Private-Key Extraction:

$\mathcal{C}$ aborts if $\mathcal{A}_3$ queries a or b.

Aggregate Signing Queries:

- For non-target users, $\mathcal{C}$ generates valid signatures.
- For the target user PID_j^*, $\mathcal{C}$ programs H_3 ($M_j^* \| PID_j^* \| R_{2j}^* \| Q_j$) = v_j and computes $z_j = r_{2j} + c_j + q_j v_j$.

Forgery Extraction:

- $\mathcal{A}_3$ outputs a forged aggregate signature $\sigma_{\text{agg}}^* = (R^*, z^*)$.
- From the target component $z_j^* = r_{2j}^* + c_j^* + q_j^* v_j^*$, $\mathcal{C}$ solves: $abP = (z_j^* - c_j^* - r_{2j}^*)P$.

Probability Analysis:

- Event E_1: $\mathcal{C}$ does not abort during private-key queries.

$$\Pr[E_1] \geq \left(1 - \frac{1}{q_{H_2}}\right)^{q_{PK}}.$$

- Event E_2: $\mathcal{A}_3$ queries H_3 on the forged component.

$$\Pr[E_2 \mid E_1] = \frac{1}{q_{H_3}}.$$

Total Advantage:

$$\text{Adv}_{\mathcal{C}}^{\text{CDH}} \geq \varepsilon \cdot \Pr[E_1] \cdot \Pr[E_2 \mid E_1].$$

Theorem 2 (Conditional Anonymity)

RCACAS provides conditional anonymity: No PPT adversary can link a pseudonym PID_i to its real identity ID_i without the TA's trapdoor k, under the CDH assumption.

Proof:

Adversarial Game:

- Challenge $\mathcal{C}$: Generates two pseudonyms $PID_0 = ID_0 \oplus H_0$ (TP_0, P_{pub}, kA_0) and $PID_1 = ID_1 \oplus H_0$ (TP_1, P_{pub}, kA_1).
- Adversary $\mathcal{A}$: Adaptively queries pseudonyms, partial keys, and signatures, then attempts to distinguish PID_0 from PID_1.

Reduction to CDH:

- Key Insight: To distinguish PID_0 and PID_1, $\mathcal{A}$ must compute kA_0 or kA_1.
- Given $A_b = a_bP$ and kP, solving $kA_b = ka_bP$ is equivalent to solving CDH.

Simulation Steps:

- Setup: $\mathcal{C}$ embeds a CDH instance (aP, kP) into $A_b = aP$ and the TA's public parameter kP.
- Pseudonym Generation: $PID_b = ID_b \oplus H_0(TP_b, P_{\text{pub}}, kA_b)$.

- Adversarial Queries: $\mathcal{C}$ answers all queries except partial-private-key extraction for PID_0 and PID_1.
- Challenge Phase: $\mathcal{C}$ returns σ_b^* for a random $b \xleftarrow{\$} \{0,1\}$.

Probability Analysis:

- If $\mathcal{A}$ guesses b with advantage ε, $\mathcal{C}$ solves CDH with probability:

$$\mathrm{Adv}_{\mathcal{C}}^{\mathrm{CDH}} \geq \varepsilon \cdot \frac{1}{q_{H_0}} \cdot \frac{1}{2}.$$

Theorem 3 (Aggregate Unforgeability)

RCACAS resists existential forgery on aggregate signatures under the CDH assumption. Even if an adversary forges an aggregate signature containing n components, at least one must be a valid forgery.

Proof:

Adversarial Model:

- $\mathcal{A}$ outputs a forged aggregate signature $\sigma_{\mathrm{agg}}^* = (R^*, z^*)$ for messages $\{M_1^*, \ldots, M_n^*\}$ and pseudonyms $\{PID_1^*, \ldots, PID_n^*\}$, where at least one PID_j^* was never queried.

Reduction to CDH:

Setup: $\mathcal{C}$ embeds a CDH instance (aP, bP) into $Q_j = aP$ and $R_{2j}^* = bP$.

Forgery Extraction:

- $\mathcal{A}_3$ outputs a forged aggregate signature $\sigma_{\mathrm{agg}}^* = (R^*, z^*)$.
- From the target component $z_j^* = r_{2j}^* + c_j^* + q_j^* V_j^*$, $\mathcal{C}$ solves: $abP = (z_j^* - c_j^* - r_{2j}^*)P$.

Probability Analysis:

- Event E_1: $\mathcal{A}$ does not query the private key for PID_j^*.

$$\Pr[E_1] \geq \left(1 - \frac{1}{q_{H_2}}\right)^{q_{PK}}.$$

- Event E_2: $\mathcal{A}$ queries H_3 on the forged component.

$$\Pr[E_2 \mid E_1] = \frac{1}{q_{H_3}}$$

- Total Advantage: $\mathrm{Adv}_{\mathcal{C}}^{\mathrm{CDH}} \geq \varepsilon \cdot \Pr[E_1] \cdot \Pr[E_2 \mid E_1]$.

6.3 Informal Security Analysis

The RCACAS scheme attains robust security through ECC, collision-resistant hashing, PUF integration, and formal proofs. Below we summarize its informal analysis.

1) Authentication

As shown in Theorem 1, RCACAS is EUF-CMA secure under the ECDLP and CDH assumptions, thwarting:

Type-I (public-key replacement) attackers lacking partial or user secrets;

Type-II (malicious KGC) with the master key but no user-generated secret;

Type-III collusion forging aggregate signatures (Lemma 3).

2) Integrity

Using $H_0 - H_3$ and certificateless aggregate signatures, any alteration of message M_i or signature (R_i, z_i) breaks $z_i P = R_i + P_{\mathrm{pub}} H_1(\ldots) + Q_i H_3(\ldots)$, which implies solving the ECDLP.

3) Conditional Anonymity

Vehicles hide ID_i in pseudonym $PID_i = ID_i \oplus H_0(TP_i, P_{\mathrm{pub}}, kA_i)$, and only the TA, holding trapdoor k, can recover or revoke identities via DSMT.

4) Unlinkability

Fresh r_{2i}, timestamps t_i, and one-time PID_i ensure signatures cannot be correlated across sessions without the TA.

5) Resistance to Physical Attacks

Keys $SK_i = (a_i, c_i, q_i)$ are bound to PUF challenge–response pairs and fuzzy-extractor outputs (w_i, h_i) so that any tampering invalidates $Ver_i = H_2(a_i, c_i, q_i, ID_i, PID_i, CRP, w_i, h_i)$.

6) Resistance to Replay Attacks

Verifiers reject messages when $|t_{\mathrm{current}} - t_i| > \Delta t$, preventing stale or replayed signatures.

7) Revocability

The TA replaces $H_2(PID_i)$ with $H_2(0)$ in the DSMT, recomputes the Merkle root in $O(\log n)$, and broadcasts updates. Combined with timestamp validation, revoked pseudonyms are rejected network-wide in real time, preventing evasion.

6.4 Security Comparison

To comprehensively evaluate the security properties of our proposed scheme, we conduct a comparative analysis with seven existing schemes ([3, 29-34]) across six critical security attributes: authentication, integrity, conditional anonymity, unlinkability, resistance to replay attacks (RT), and resistance to physical attacks. The comparative results are systematically presented in Table 2, revealing distinct security advantages of our scheme.

Table 2. Security attribute comparison of different schemes

Scheme	Authentication	Integrity	Conditional Anonymity	Unlinkability	Replay Attacks	Physical Attacks	Revocability
[29]	√	×	×	×	×	×	×
[30]	√	×	×	×	×	×	×
[31]	√	×	×	×	×	×	×
[32]	√	√	×	×	×	×	×
[33]	√	√	√	×	×	×	×
[34]	√	√	√	√	√	×	×
[3]	√	√	√	√	√	×	×
Ours	√	√	√	√	√	√	√

Existing schemes exhibit limitations to varying degrees, such as [29-31] lacking conditional anonymity, [32] neglecting unlinkability (which enables user behavior tracking), and [34] and [3] failing to resist physical attacks, but our solution successfully integrates all six evaluated security characteristics. This holistic security framework particularly addresses the growing threat landscape where advanced adversaries combine multiple attack vectors, including physical device tampering and protocol-level replay attacks.

7 Performance Evaluation

We evaluate our scheme's computational and communication overhead against six ECC-based, pairing-free CLAS protocols [19, 35-39].

7.1 Computational Overhead

All experiments run on a 3.00GHz Intel Core i5-12500 with 16GB RAM under Linux, implemented in Python using Charm Crypto, pypuf and python-fuzzy-extractor. We adopt the secp192v1 curve ($y^2 = x^3 + ax + b \pmod p$), $|p| = 192$ bits), measure 1,000 iterations of core elliptic-curve operations, and report the averages in Table 3.

Building on these baselines, we compare our RCACAS scheme's single-signature generation, single-signature verification, and n aggregate verification times to those of existing schemes; the results are summarized in Table 4.

Table 3. Execution time of basic operations

Operation	Description	Time (ms)
T_{pa}	Elliptic curve point addition P + Q	0.0011
T_{sm}	Elliptic curve scalar multiplication	0.1747
T_h	sP SHA-256 hash function	0.0005
$T_{p,128}$	PUF response generation (128-bit)	0.0007
$T_{g,128}$	Fuzzy extractor: Gen (128-bit input)	1.2644
$T_{r,128}$	Fuzzy extractor: Rep (128-bit recovery)	0.2412

1) Single Signature Generation Time

The single signature generation time reflects the computational cost incurred by a vehicle when generating a digital signature for a message. In our scheme, the single signature time is calculated as $1T_h + T_{sm} + 1T_{pa} = 0.1763$ ms, reflecting a well-considered balance between security and efficiency.

Specifically, our scheme combines three operations: hash function computation T_h, scalar multiplication T_{sm}, and point addition T_{pa}. The hash function ensures data integrity, scalar multiplication is central to elliptic curve cryptography for security, and point addition enhances complexity against attacks.

Comparatively, schemes [35] and [38] at $1T_{sm} + 1T_h = 0.1752$ milliseconds is slightly faster but lacks point addition, potentially making it less secure against certain attacks. Schemes [36, 19, 37] and [39], all at $1T_{sm} + 2T_h = 0.1757$ milliseconds, have more hash computations but no point addition, leading to efficiency close to ours but possibly with security trade-offs. In large-scale VANETs, minor millisecond-level delays have negligible system impact. Our scheme strategically incorporates point addition operations to enhance physical attack resistance and conditional anonymity critical security requirements for VANETs. While RCACAS exhibits marginally longer single-signature generation times, its optimized operation portfolio effectively balances cryptographic robustness with computational practicality for high-security deployments.

2) **Single Signature Verification Time**

The single signature verification time indicates the computational effort required by an RSU to verify the validity of a signature received from a vehicle. For our scheme, this time is $3T_{sm} + 2T_{pa} + 2T_h = 0.1779$ ms. This involves elliptic curve scalar multiplication, multiple point additions, and hash function evaluations.

- The schemes from [36, 19, 37, 39] require $3T_{pa} + 4T_{sm} + 3T_h = 0.7071$ ms for single signature verification, which is significantly higher than our scheme. This suggests that while these schemes may be efficient in signature generation, their verification process is more computationally intensive.
- The scheme from [35] has a verification time of $1T_{pa} + 2T_{sm} + 1T_h = 0.3510$ ms, which is intermediate between our scheme and the group with the highest verification time.
- The scheme from [38] requires $2T_{pa} + 3T_{sm} + 2T_h = 0.5273$ ms for verification, which is the same as our proposed scheme. However, it relies on static pseudonym binding mechanisms, thus exposing itself to long-term correlation attacks. Moreover, the lack of Physical Unclonable Function (PUF) protection makes it vulnerable to hardware side-channel attacks.

Our scheme strikes a balance between security and efficiency in the verification process, ensuring that RSUs can perform verifications relatively quickly while still maintaining the necessary security guarantees.

3) n-Aggregate Verification Time

The n-aggregate verification time is crucial for assessing the efficiency of batch verification processes, where multiple signatures are verified simultaneously. In our scheme, this time is given by $(n+1)T_{pa} + (n+2)T_{sm} + 2nT_h = 0.1768n + 0.3505$ ms. This linear relationship with the number of signatures n indicates that our scheme scales efficiently for aggregate verification.

- The schemes from [36, 19, 37, 39] have an n-aggregate verification time of $3nT_{pa} + (2n+2)T_{sm} + 3nT_h = 0.3554n + 0.3494$ ms (or similar expressions with slight variations). These schemes exhibit a higher computational overhead for aggregate verification, especially as the number of signatures increases.
- The scheme from [35] shows an n-aggregate verification time of $(3n-1)T_{pa} + (3n+3)T_{sm} + (n+1)T_h = 0.5279n + 0.5235$ ms, which grows more

rapidly with n compared to our scheme.

- The scheme from [38] has an n-aggregate verification time of $2nT_{pa} + (2n+1)T_{sm} + 2nT_h$ = $0.3554n + 0.1747$ ms, which is more efficient than some but still less efficient than our proposed scheme for larger n.

OUR Scheme achieves the lowest linear coefficient 0.1768, reducing verification time by 50% compared to [19, 36-38] and 67% compared to [35].

The linear scaling of our scheme's aggregate verification time makes it particularly suitable for scenarios where a large number of signatures need to be verified simultaneously, ensuring that the computational overhead remains manageable even as the network scales.

To more intuitively demonstrate the computational overhead advantages of our scheme, we compare seven schemes' computational overhead in resource-constrained environments using Table 4 data in Figure 2, while simultaneously evaluating their n-aggregate-verification computational overhead (n = 1000). The comparative results are shown in Figure 3.

Figure 4 systematically evaluates and compares the computational overhead of n aggregate-verification for different certificateless authentication schemes when $n \in \{100, 200, 300, 400, 500\}$.

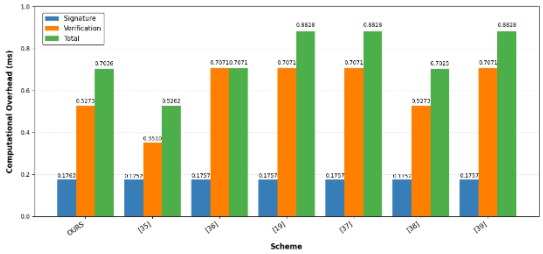

Figure 2. Computational overhead for a single operation

Table 4. Comparison of computational overhead

Scheme	Single signature (ms)	Single verification (ms)	n-aggregate verification (ms)
Ours	$1T_h+1T_{sm}+1T_{pa}=0.1763$	$3T_{sm}+2T_{pa}+2T_h=0.5273$	$(n+1)T_{pa}+(n+2)T_{sm}+2nT_h=0.1768n+0.3505$
[35]	$1T_{sm}+1T_h=0.1752$	$1T_{pa}+2T_{sm}+1T_h=0.3510$	$(3n-1)T_{pa}+(3n+3)T_{sm}+(n+1)T_h=0.5279n+0.52353$
[36]	$1T_{sm}+2T_h=0.1757$	$3T_{pa}+4T_{sm}+3T_h=0.7071$	$nT_{pa}+(2n+2)T_{sm}+3nT_h=0.3554n+0.3494$
[19]	$1T_{sm}+2T_h=0.1757$	$3T_{pa}+4T_{sm}+3T_h=0.7071$	$(3n+1)T_{pa}+(2n+3)T_{sm}+3nT_h=0.3554n+0.5300$
[37]	$1T_{sm}+2T_h=0.1757$	$3T_{pa}+4T_{sm}+3T_h=0.7071$	$3nT_{pa}+(2n+2)T_{sm}+3nT_h=0.3554n+0.3494$
[38]	$1T_{sm}+1T_h=0.1752$	$2T_{pa}+3T_{sm}+2T_h=0.5300$	$2nT_{pa}+(2n+1)T_{sm}+2nT_h=0.3554n+0.1747$
[39]	$1T_{sm}+2T_h=0.1757$	$3T_{pa}+4T_{sm}+3T_h=0.7071$	$(4n-1)T_{pa}+(3n+1)T_{sm}+3nT_h=0.5316n+0.1706$

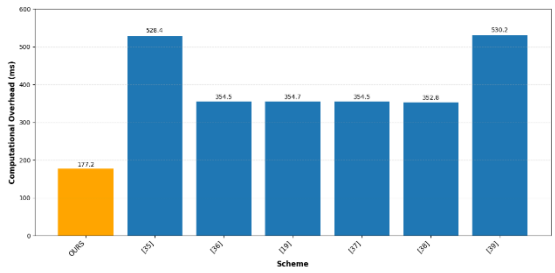

Figure 3. Computational overhead for 1000-aggregate verification

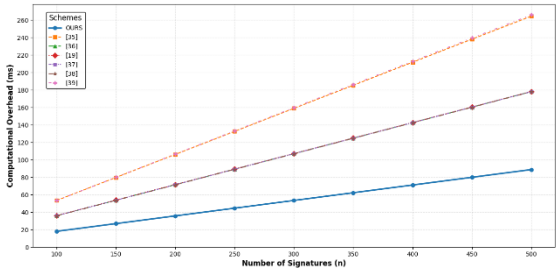

Figure 4. Computational overhead of n-aggregate-verification

In summary, RCACAS trades a modest increase in signature-generation time for markedly faster (especially aggregate) verification, striking an ideal balance for VANETs' security and scalability needs. The small extra cost enables physical attack resistance, conditional anonymity, and efficient revocation delivering a practical, robust authentication solution for dynamic, adversarial vehicular networks.

7.2 Communication Overhead

In VANETs, minimizing communication overhead is critical to ensure real-time responses and efficient bandwidth utilization. To evaluate the practicality of RCACAS, we compare its communication overhead with six state-of-the-art schemes [19, 35-39]. The size of cryptographic elements used in this analysis is defined in Table 5, where a group element G occupies 48 bytes, a finite field element $\mathbb{Z}_q^*$ requires 24 bytes, a timestamp T consumes 8 bytes, and a small integer B takes 4 bytes.

Table 5. Size of each element

Type	Description	Size (bytes)
G	A group G element	48
Z_q^*	A finite field Z_q^*	24
T	element A timestamp	8
B	A small integer	4

As illustrated in Table 5, RCACAS achieves superior efficiency in both single-message and aggregated-message scenarios. As depicted in Figure 5, for a single authentication message, our scheme incurs $2|G| + 2|\mathbb{Z}_q^*| + |T| = 176$ bytes, which is 31.25% lower than the 256 byte overhead of [35, 19, 37, 39]. This reduction stems from our optimized certificateless design that eliminates redundant group operations while ensuring conditional anonymity.

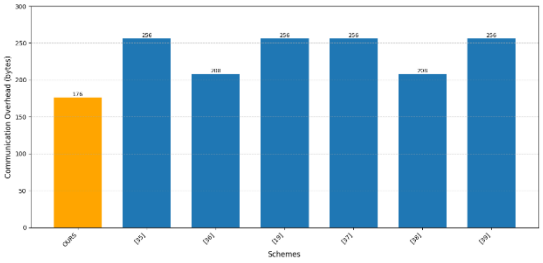

Figure 5. Communication overhead for a single message

As illustrated in Figure 6, for aggregated messages from n vehicles, RCACAS further demonstrates scalability. The total overhead is calculated as $80n + 72$ bytes, significantly outperforming existing schemes. For instance, when $n = 10$, our scheme requires only 872 bytes, whereas [35] and [36] demand 2,368 bytes and 1,864 bytes, respectively. This improvement (up to 63% savings) arises from our lightweight aggregation mechanism that avoids repetitive transmission of timestamp and group elements.

The results confirm that RCACAS strikes an optimal balance between security and efficiency, making it highly suitable for bandwidth constrained VANET environments. Detailed comparisons are provided in Table 6, with supporting element size definitions in Table 5.

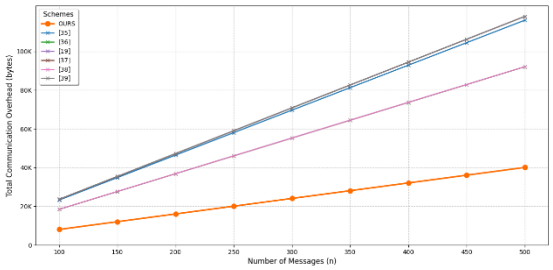

Figure 6. Communication overhead for n message

Table 6. Comparison of communication overhead

Paper	Single message (bytes)	n aggregate messages (bytes)
Ours	$2\|G\| + 2\|Z_q^*\| + \|T\| = 176$	$n(\|T\| + \|Z_q^*M\| + \|G\| + \|Z_q^*M\| + \|G\| + \|Z_q^*M\| = 80n + 72$
[35]	$4\|G\| + 2\|Z_q^*M\| + 2\|T\| = 256$	$4n\|G\| + (n+2)\|Z_q^*\| + 2n\|T\| = 232n + 48$
[36]	$3\|G\| + 2\|Z_q^*M\| + 2\|T\| = 208$	$3n\|G\| + (n+1)\|Z_q^*M\| + 2n\|T\| = 184n + 24$
[19]	$4\|G\| + 2\|Z_q^*M + 1\| = 256$	$4n\|G\| + (n+1)\|Z_q^*M\| + (n-1) = 236n + 20$
[37]	$4\|G\| + 2\|Z_q^*M + 1\| = 256$	$4n\|G\| + (n+1)\|Z_q^*M + 1\| + (n-1) = 236n + 20$
[38]	$3\|G\| + 2\|Z_q^*M + 1\| = 208$	$(3n+1)\|G\| + (n+1)\|Z_q^*\| + 2n\|T\| = 184n + 72$
[39]	$4\|G\| + 2\|Z_q^*M + 1\| + 2\|T\| = 256$	$4n\|G\| + (n+1)\|Z_q^*M + 1\| + 2n\|T\| + (n-1) = 236n + 20$

8 Conclusion

In this paper, we introduced RCACAS, a pairing-free certificateless authentication scheme for VANETs that unifies conditional anonymity, DSMT-based revocation, and PUF-protected keys to resist physical attacks and reduce communication overhead. Under the Random Oracle Model, we proved security against Type-I/II/III adversaries. Performance evaluations demonstrate lower computational and bandwidth costs than existing approaches, achieving a robust balance of security, efficiency, and scalability. Future work may explore the integration of blockchain-based distributed trust management to further enhance security and decentralization. Additionally, optimizing the PUF response stabilization mechanisms could improve reliability in real-world deployments.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 62072133), Wenzhou Major Scientific and Technological Innovation Projects (No. ZG2023028).

References

[1] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, D. Wu, Trove: A context-awareness trust model for vanets using reinforcement learning, *IEEE Internet of Things Journal*, Vol. 7, No. 7, pp. 6647–6662, July, 2020. https://doi.org/10.1109/JIOT.2020.2975084

[2] W. Yang, P. Cao, F. Zhang, Z. Liu, Secure pairing-free certificate-based online/offline signcryption scheme with conditional privacy preserving for vanets, *IEEE Internet of Things Journal*, Vol. 12, No. 4, pp. 4435–4447, February,

2025.
https://doi.org/10.1109/JIOT.2024.3485654

[3] Q. Zhang, Y. Sun, Y. Lu, N. Xia, G. Wu, Efficient certificateless aggregate designated verifier signature with conditional privacy preserving in vanets, *IEEE Internet of Things Journal*, Vol. 11, No. 15, pp. 26191–26202, August, 2024.
https://doi.org/10.1109/JIOT.2024.3393000

[4] Q. Wu, L. Zhang, Y. Yang, K.-K. R. Choo, Certificateless signature scheme with batch verification for secure and privacy-preserving v2v communications in vanets, *IEEE Transactions on Dependable and Secure Computing*, Vol. 22, No. 2, pp. 1448–1459, March-April, 2025.
https://doi.org/10.1109/TDSC.2024.3445164

[5] X. Yang, S. Li, L. Yang, X. Du, C. Wang, Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for vanets, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 9, pp. 12256–12268, September, 2024.
https://doi.org/10.1109/TITS.2024.3367925

[6] Y. Liang, H. Yan, Y. Liu, Unlinkable signcryption scheme for multi-receiver in vanets, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 9, pp. 10138–10154, September, 2023.
https://doi.org/10.1109/TITS.2023.3271110

[7] Y. Wang, X. Wang, H. N. Dai, X. Zhang, M. Imran, A data reporting protocol with revocable anonymous authentication for edge-assisted intelligent transport systems, *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 6, pp. 7835–7847, June. 2023.
https://doi.org/10.1109/TII.2022.3226244

[8] Y. Liang, Y. Liu, X. Zhang, G. Liu, Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 11, pp. 18831–18846, November, 2024.
https://doi.org/10.1109/TITS.2024.3443171

[9] Y. Yang, L. Zhang, Y. Zhao, K. R. Choo, Y. Zhang, Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 317–331, 2022.
https://doi.org/10.1109/TIFS.2022.3140657

[10] C. Yan, H. Wang, S. Yan, An identity-based message authentication scheme for internet of vehicles, *Proceedings of the IEEE 8th International Conference on Big Data Security, Cloud (BigDataSecurity), International Conference on High Performance Smart Computing (HPSC), IEEE International Conference on Intelligent Data Security (IDS)*, Jinan, China, 2022, pp. 154–156.
https://doi.org/10.1109/BigDataSecurityHPSCI DS54978.2022.00037

[11] B. B. Gupta, A. Gaurav, C.-H. Hsu, B. Jiao, Identity-based authentication mechanism for secure information sharing in the maritime transport system, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 2, pp. 2422–2430, February, 2023.
https://doi.org/10.1109/TITS.2021.3125402

[12] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, M. Guizani, Blockchain-assisted secure device authentication for cross-domain industrial iot, *IEEE Journal on Selected Areas in Communications*, Vol. 38, No. 5, pp. 942–954, May, 2020.
https://doi.org/10.1109/JSAC.2020.2980916

[13] Z. Xie, Y. Chen, I. Ali, C. Pan, F. Li, W. He, Efficient and secure certificateless signcryption without pairing for edge computing-based internet of vehicles, *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 5, pp. 5642–5653, May, 2023.
https://doi.org/10.1109/TVT.2022.3230442

[14] I. Dohare, K. Singh, A. Ahmadian, S. Mohan, P. K. R. M, Certificateless aggregated signcryption scheme (class) for cloud-fog centric industry 4.0, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 9, pp. 6349–6357, September, 2022.
https://doi.org/10.1109/TII.2022.3142306

[15] X. Liu, Y. Zhou, B. Yang, T. Zhu, M. Zhang, An efficient pairing-free certificateless signcryption scheme under the standard model for vanet, *IEEE Internet of Things Journal*, Vol. 12, No. 12, pp. 22142-22154, June, 2025.
https://doi.org/10.1109/JIOT.2025.3550660

[16] Y. Wang, C. Peng, X. Jia, J. Wen, Y. Zhang, Pairing-free blockchain-assisted certificateless aggregation signcryption scheme for vanets, *IEEE Internet of Things Journal*, Vol. 12, No. 11, pp. 15545-15557, June, 2025.
https://doi.org/10.1109/JIOT.2025.3528067

[17] C. Dai, Z. Xu, Pairing-free certificateless aggregate signcryption scheme for vehicular sensor networks, *IEEE Internet of Things Journal*, Vol. 10, No. 6, pp. 5063–5072, March, 2023.
https://doi.org/10.1109/JIOT.2022.3222237

[18] W. Wu, F. Ye, A secure and efficient certificateless aggregate signature authentication scheme with pseudonyms for vanets, *IEEE Internet of Things Journal*, Vol. 12, No. 1, pp. 124–139, January, 2025.
https://doi.org/10.1109/JIOT.2024.3459033

[19] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, F. Xu, A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 10, pp. 10456–10466, October, 2023.
https://doi.org/10.1109/TITS.2023.3275077

[20] X. Zhou, D. He, M. K. Khan, W. Wu, K.-K. R. Choo, An efficient blockchain-based conditional privacy-preserving authentication protocol for vanets, *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 1, pp. 81–92, January, 2023.
https://doi.org/10.1109/TVT.2022.3204582

[21] J. Xu, L. Wang, M. Wen, Y. Long, K. Chen, Dpb-ma: Low-latency message authentication scheme based on distributed verification and priority in vehicular ad hoc network, *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 4, pp. 5152–5166, April, 2023.
https://doi.org/10.1109/TVT.2022.3225204

[22] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, M. K. Khan, Efficient certificateless aggregate signature with conditional privacy preservation in iov, *IEEE Systems Journal*, Vol. 15, No. 1, pp. 245–256, March, 2021.
https://doi.org/10.1109/JSYST.2020.2966526

[23] W. Yang, J. Fan, K. Song, Y. Zheng, F. Zhang, An efficient and practical conditional privacy-preserving aggregate authentication for vehicular ad-hoc networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 12, pp. 20256–20267, December, 2024.
https://doi.org/10.1109/TITS.2024.3474210

[24] X. Meng, B. Liu, X. Meng, Y. Liang, H. Deng, A lightweight group authentication protocol for blockchain-based vehicular edge computing networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 8, pp. 8556–8567, August, 2024.

https://doi.org/10.1109/TITS.2024.3402432

[25] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology (CRYPTO)*, Santa Barbara, CA, USA, 1984, pp. 47–53. https://doi.org/10.1007/3-540-39568-7_5

[26] S. S. Al-Riyami, K. G. Paterson, Certificateless public key cryptography, *Advances in Cryptology–ASIACRYPT 2003*, Taipei, Taiwan, 2003, pp. 452–473. https://doi.org/10.1007/978-3-540-40061-5_29

[27] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Warsaw, Poland, 2003, pp. 416–432. https://doi.org/10.1007/3-540-39200-9_26

[28] R. Castro, R. Dahab, *Efficient certificateless signatures suitable for aggregation*, Technical Report 2007/454, Cryptology ePrint Archive, 2007.

[29] G. Wu, F. Zhang, L. Shen, F. Guo, W. Susilo, Certificateless aggregate signature scheme secure against fully chosen-key attacks, *Information Sciences*, Vol. 514, pp. 288–301, April, 2020. https://doi.org/10.1016/j.ins.2019.11.037

[30] L. Shen, J. Ma, Y. Miao, H. Liu, Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model, *IET Information Security*, Vol. 13, No. 3, pp. 167–173, May, 2019. https://doi.org/10.1049/iet-ifs.2018.5226

[31] T. Li, H. Wang, D. He, J. Yu, Designated-verifier aggregate signature scheme with sensitive data privacy protection for permissioned blockchain-assisted iiot, *IEEE Transactions on Information Forensics and Security*, Vol. 18, pp. 4640–4651, 2023. https://doi.org/10.1109/TIFS.2023.3297327

[32] F. Zhang, L. Shen, G. Wu, Notes on the security of certificateless aggregate signature schemes, *Information Sciences*, Vol. 287, pp. 32–37, December, 2014. https://doi.org/10.1016/j.ins.2014.07.019

[33] N. Zhao, G. Zhang, Privacy-protected certificateless aggregate signature scheme in vanet, *11th International Conference on Wireless Communications and Signal Processing (WCSP)*, Xi'an, China, 2019, pp. 1–6. https://doi.org/10.1109/WCSP.2019.8928040

[34] Y. Liang, Y. Liu, Analysis and improvement of an efficient certificateless aggregate signature with conditional privacy preservation in vanets, *IEEE Systems Journal*, Vol. 17, No. 1, pp. 664–672, March, 2023. https://doi.org/10.1109/JSYST.2022.3180221

[35] W. Xiong, R. Wang, Y. Wang, Y. Wei, F. Zhou, X. Luo, Improved certificateless aggregate signature scheme against collusion attacks for vanets, *IEEE Systems Journal*, Vol. 17, No. 1, pp. 1098–1109, March, 2023. https://doi.org/10.1109/JSYST.2022.3213245

[36] X. Li, X. Yin, J. Ning, Relclas: A reliable malicious kgc-resistant certificateless aggregate signature protocol for vehicular ad hoc networks, *IEEE Internet of Things Journal*, Vol. 10, No. 23, pp. 21100–21114, December, 2023. https://doi.org/10.1109/JIOT.2023.3285402

[37] Y. Zhou, Z. Wang, Z. Qiao, B. Yang, M. Zhang, An efficient and provably secure identity authentication scheme for vanet, *IEEE Internet of Things Journal*, Vol. 10, No. 19, pp. 17170–17183, October, 2023. https://doi.org/10.1109/JIOT.2023.3273234

[38] Y. L. Chen, J. H. Chen, Cpp-clas: Efficient and conditional privacy-preserving certificateless aggregate signature scheme for vanets, *IEEE Internet of Things Journal*, Vol. 9, No. 12, pp. 10354–10365, June, 2022. https://doi.org/10.1109/JIOT.2021.3121552

[39] H. Zheng, M. Luo, Y. Zhang, C. Peng, Q. Feng, A security-enhanced pairing-free certificateless aggregate signature for vehicular ad-hoc networks, *IEEE Systems Journal*, Vol. 17, No. 3, pp. 3822–3833, September, 2023. https://doi.org/10.1109/JSYST.2022.3220869

Biographies

Peiyong Sun received the M. S. degree in applied mathematics from Guilin University of Electronic Technology, Guilin, China, in 2012, and received the Ed.D. degree from Central China Normal University, Hubei, China, in 2023. He is currently working at School of Computer Science, Henan Institute of Information Science and Technology, China. His research interests include the secure authentication in VANETs, certificateless aggregate signature.

Yangfan Liang received the B. E. degree in Computer Science and Technology from Xihua University, Chengdu, Sichuan, China, in 2018. And he received the Ph. D. degree with the School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China, in 2023. He is currently a lecturer with the Institute of Information Network and Artificial Intelligence, and the Engineering Research Center of Intelligent Human Health Situation Awareness of Zhejiang Province, Jiaxing University, Jiaxing, China. His research fields include secure authentication in VANETs, key agreement.

Mingrong Xiang is currently the Deputy Director of the Department of Data Science and Big Data Technology at Wenzhou University of Technology, with a PhD in Computer Science from Deakin University, Australia, which he obtained in 2024. His research interests span deep learning, data mining, computer vision, and complex interaction network modelling, with extensive extensions to interdisciplinary fields such as cybersecurity and industrial intelligence.

Yining Liu received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, China, in 1995, the M. E. degree in computer software and theory from the Huazhong University of Science and Technology, Wuhan, China, in 2003,

and Ph. D. degree in mathematics from Hubei University, Wuhan, in 2007. He is currently a professor with school of data science and artificial intelligence, Wenzhou University of Technology, Wenzhou, China. His research interests include the information security protocol and data privacy.