FS-CLAS: A Forward-Secure Pairing-Free Certificateless Aggregate Signature Scheme for VANET Authentication

Jalal M.H. Altimemi[1,*], Iman A. Almarzooq [2], Nada Mohammed Hassan Moter[3], Shams A.S. Alfarttoosi[4], Bushra Abdullah Shtayt[1], Mahmood A. Al-Shareeda[5,6,*] and Mohammed Almaayah[7]
[1]Information Technologies Management Department, Southern Technical University, Iraq
[2]Department of business administration, Southern Technical University, Iraq
[3]Pharmacy Department, Medical Technical Institute-Basra, Southern Technical University, Basra, 61001, Iraq
[4]Department of Materials Management Technologies, Southern Technical University, Iraq
[5]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[6]College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[7]King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
E-mail: jalal.altimemi@stu.edu.iq, bushra.abdullah@stu.edu.iq, iman.abduljabbar@stu.edu.iq, Shams.shanan@stu.edu.iq, mahmood.alshareedah@stu.edu.iq, m.almaiah@ju.edu.jo
*Corresponding author

Keywords: Vehicular ad hoc networks (VANETs), forward secrecy, certificateless cryptography, intelligent transportation systems (ITS), cryptographic key management, software architecture, security governance, lightweight authentication protocols, privacy-preserving communication, cybersecurity risk management, strategic technology integration

Received: June 24, 2025

We introduce a forward-secure, pairing-free, and certificateless aggregate signature scheme called FS-CLAS to support efficient, lightweight, and scalable authentication in VANETs. Overview: To accomplish forward secrecy, FS-CLAS uses a hash-chain-based design for key evolution that does not require bilinear pairings or secure hardware modules. It is secure against side-channel attacks due to the usage of ephemeral keys and constant-time scalar multiplication, and it features batch verification capability, conditional traceability, and decentralized revocation using Bloom filters. A modular app and management architecture make our implementation compatible with real-world Intelligent Transportation System (ITS) deployments. We demonstrate through experimental evaluation that FS-CLAS achieves up to 50% reduction in verification latency and 42% saving of communication overhead as compared to more recent work, where the average signing and verifying times are less than 3.2ms and 6.7ms, respectively, on ARM-based OBUs. Results from simulations with SUMO and NS-3 show that they work well under variable traffic density levels and high vehicle mobility. FS-CLAS complies with IEEE 1609.2 and ETSI ITS-G5 standards, providing an option for deployment with existing and future V2X networks.

Povzetek: Članek predstavi FS-CLAS, varno, brezparno in neodvisno agregirano podpisovanje za VANET, ki z evolucijo ključev prek hash verige ter paketnim preverjanjem in decentralizirano preklicnostjo omogoča hitro avtentikacijo skladno s standardi.

1 Introduction

VANETs are a subset of ITS that allow vehicles to communicate with each other and with roadside infrastructure in real-time, and form an important part of future ITS systems[1], [2], [3], [4]. Safety applications such as the collision warning and traffic flow optimization heavily depend on the credibility and reliability of receiving safety messages [5], [6], [7], [8]. But because VANET environments are open and can be non-deterministic, securing the exchange of messages while preserving user privacy is difficult [9], [10], [11].

Traditional PKI and IBC have been broadly studied for VANET authentication; however, they are associated with scalability and privacy shortcomings[12], [13]. PKI involves expensive certificate management, and IBC has inherent key escrow problems[14], [15], [16], [17]. To meet with the above needs, certificateless public key cryptography (CL-PKC) is proposed for authentication, which does not use a certificate or blindly believes in the generation of a secret key by the key generation center (KGC)[18], [19], [20], [21]. In addition, the certificateless aggregate signature (CL-AS) mechanism also isomorphic aggregates the signatures and turns it into a short signature so as to greatly reduce the verification overheads on RSUs[22], [23], [24], [25].

Despite these advancements there are still some security holes to be addressed. For the most part, current CL-AS constructions fail to achieve forward secrecy, that is future messages remain secure in the event that a signing key ma-

terializes from before being compromised. Furthermore, many such schemes rely on bilinear pairings, which are expensive and are not feasible for implementation in OBUs with limited computational capabilities. In some cases, they also use tamper-proofed hardware or do not consider side-channel attacks which could leak important information about the stored cryptographic material.

To solve the above drawbacks, in this paper, we present a time-based key evolving efficient certificateless aggregate signature scheme (LET-CEA) for VANETs, and prove our scheme pairing-free in the standard model. Our contributions can be summarized as:

- We present a pairing-free CL-AS scheme with forward secrecy in which a vehicle signing key evolves over time according to a hash-chain construction.
- We formulate an efficient aggregate verification scheme for RSUs to verify a batch of vehicle messages with low computational and communication overhead.
- We avoid use of tamper-proof devices, promoting real-world VANETs deployability, and our solution also incorporates lightweight method to counter side-channel threats.
- We provide a formal security analysis, under Type I and Type II adversaries and show resistance against forgery, impersonation, replay, and key compromise.
- Performance analysis indicates that our more efficient in terms of computation and communication when compared to some recent works, especially under high message load.

The remainder of this paper is organized as follows: Section II surveys related work; Section III describes the system and threat models; Section IV describes the proposed FS-CLAS scheme; Section V discusses provable security; Section VI analyzes performance; Section VII describes practical considerations; and Section VIII concludes.

2 Related work

Lightweight and scalable authentication schemes are required to support VANETs with security, privacy and traceability comparisons. Certificateless cryptography is an attractive approach to avoid the overhead of certificate management and to address key escrow problems existing in identity-based schemes[26], [27], [28], [29]. Certificateless aggregate signature (CL-AS) protocols have recently been studied to solve these problems[30], [31], [32], [33], [34].

Surapaneni et al. [35] presented a privacy-preserving certificateless aggregate signature scheme, using blockchain, for protecting vehicle transitions in intelligent transportation systems (ITS). Their distribution provides conditional privacy and batch verification, but they do not achieve forward secrecy and require tamper-proof modules. Similarly, Wang et al. [36] introduced a certificateless V2I system based on secure mobility models, however no protection against key exposure and side-channel attacks was considered.

Liu et al. [37] introduced a CL-AS protocol in the pairing-free case, which satisfies traceability and efficiency but not the forward secrecy. In contrast, Bansal et al. (2025)[38] were largely able to relax the design of prior constructions–by removing pairings and increasing the power of their security proof– however their model is still missing key evolution primitives and requires a secure storage device.

More generally, Partovi et al. [39] conducted a systematic review of data centric approaches in IoV and realized that, most of the previous VANET schemes are not able to provide unlinkability, or inject high verification latency. Furthermore, Ferrag and Shu [40] also considered blockchain-based VANET authentication but observed that it is not directly applicable for aggregate signatures and low-latency verification.

Recent surveys and frameworks (e.g., Burhan et al., 2023 [41]) also underscore the importance of lightweight, scalable schemes minimizing the dependence on costly cryptography operations and hardware security. These works agree on the desirability of forward-secure, pairing-free, aggregate-friendly strong authentication: that is what this paper has sought to produce in the form of FS-CLAS.

As shown in Figure 1, relatively few papers have considered both the above-featured requirements, including forward secrecy, minimal trust requirements, and being side-channel resistant and pairing-free CL-AS protocols, despite the significant effort made by past research on secure and efficient CL-AS protocols for VANETs. Our proposed FS-CLAS scheme is motivated by this gap.

3 Preliminaries

This part formalizes the basic constituents needed to describe and analyze the proposed FS-CLAS scheme, the system model, threat/adversary model, cryptographic primitives, and security properties.

3.1 System model

As shown on Figure 1, the proposed system coexists in VANET standard architecture with:

- **Onboard Units (OBUs)**: OBUs are devices in vehicles that produce and sign messages with the messages using ephemeral keys. It is assumed that each OBU has limited processing and storage capabilities[45].
- **RSUs (Roadside Units)**: These infrastructure nodes receive, verify, and then rebroadcast the vehicular messages. RSUs are essential in the batch verification of signatures and communication with trusted authorities[46].

Table 1: Comparative summary of related VANET authentication schemes

Scheme	Pairing Used	Forward Secrecy	Side-Channel Resilience	Hardware Assumptions	Verify Latency
Li et al. (2021) [42]	✓	✗	✗	TPM / Secure Module	High
Bansal et al. (2025) [43]	✗	Partial	✗	None	Moderate
Zhang et al. (2023) [44]	✓	✓	✗	TPM / HSM	High
FS-CLAS (Ours)	✗	✓	✓	None	Low

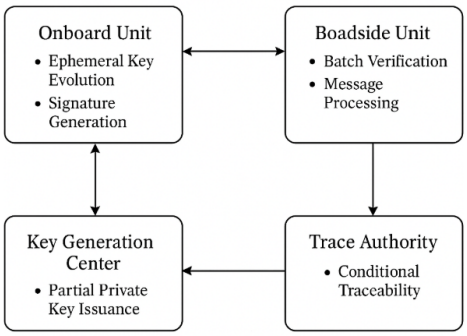

Figure 1: FS-CLAS software architecture

– **KGC(Key Generation Center)**: It is the semi-trusted authority who generates the partial private keys for the vehicles which are registered with it without knowing their complete private keys. With the aid of the KGC, traditional certificates can be avoided[47].

– **Trace authority (TRA)**: A fully trusted authority, which associates pseudonyms to real identities in event of disputes or cheating. The TRA supports conditional traceability with privacy under normal scenario.

3.2 Threat model

We consider a threat model with following capabilities for the adversary:

– Wiretap communication of messages on the wireless VANET channel.

– Query signatures on random messages (adaptive chosen-message attacks).

– Compromise secret keys of certain vehicles (key exposore scenario).

– Trying another method to Imation or impersonation.

In contrast, we consider the KGC as semitrusted (honest-but-curious) and the TRA as fully trusted. The models also assume coarse-grained time synchronization among OBUs by means of GPS-enabled OBUs.

3.3 Adversary types

We consider two adversaries in the spirit of certificateless cryptography literature:

– **Type 1 Adversary** ($\mathcal{A}_I$): Does not have access to the master secret key of the KGC but can change public keys of users. Stands for malicious nodes or non-physically connected nodes.

– **Type II Adversary** ($\mathcal{A}_{II}$): Adversary that knows the KGC's master secret key and who cannot substitute public keys. Represents a dishonest KGC.

3.4 Security goals

The objective of the proposed scheme is to:

– **Authentication and Message Integrity**: Only authentic OBUs are able to produce a valid signature.

– **Unforgeability**: No adversary can create a valid signature without using the corresponding keys.

Forward Secrecy: Although the current private key may be compromised, past message signatures are still protected.

– **Unlinkability and Anonymity**: Messages can generally not be associated with individual vehicles unless monitored by the TRA.

– **Only When Required Treatment**: The TRA is able to retrieve the real identities, if needed.

– **Resistance to Side-Channels**: The key leakage risk is mitigated by a decrease of the dependence on hardware security modules.

4 Proposed FS-CLAS scheme

We design a cryptographic algorithm of forward-secure certificateless aggregate signature (FS-CLAS) through which the cryptographic security scheme meets the modular software and management system that will be needed to deploy large-scale VANET. The framework is intended to be applied for dynamic key management, decentralized trust and policy based pseudonym traceability with light weight and secure embedding systems. From a systems management

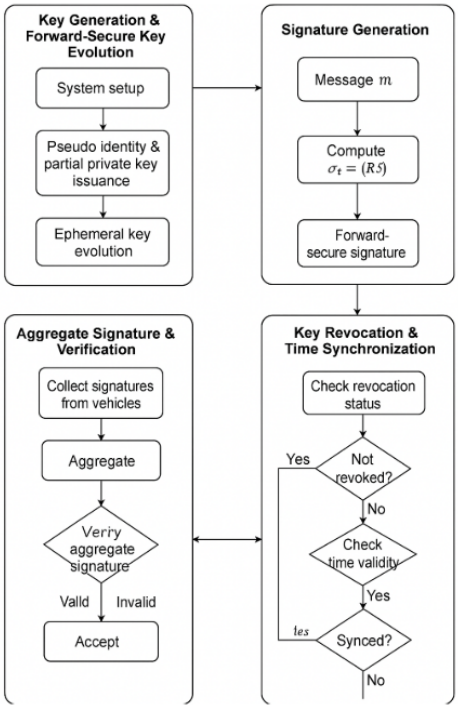

Figure 2: Overview of the proposed FS-CLAS scheme

standpoint, FS-CLAS presents an operational model which supports security lifecycle automation which includes the ability for stakeholders to manage key issuance, revocation and synchronization en masse. Besides, its software modularity grants a clear separation of concerns between the cryptography functionalities (e.g., signature generation) and management tasks (e.g., trace authority supervision, revocation resolution, and system time synchronization), in line with best practices pointed out in ITS security governance and infrastructure interoperability. Fig. 2 provides an integrated overview of the proposed scheme, encompassing key generation and evolution, signature generation, aggregation and verification, as well as key revocation and time synchronization processes. The proposed approach does not compromise the initial benefits of the certificateless schemes, i.e., no certificates and key escrow free, and adds forward secrecy.

4.1 Key generation and forward-secure key evolution

Our Forward-secure Certificateless Signature scheme with dynamic key evolution of vehicular nodes allows forward secrecy while it will continue to be practical lightweight elliptic curve cryptography. The proposed scheme makes use of two trusted authorities and they are called Key Generation Center (KGC), which is in charge of producing partial private keys, and Trace Authority (TRA), which is used for identity tracing and pseudonym generation. Fig. 3 illustrates the overall process of key generation and forward-secure key evolution, including system setup, pseudonym and partial private key issuance, and time-based ephemeral key updates at the vehicle side. Key generation and evolution The key generation and evolution process is performed using the following algorithms:

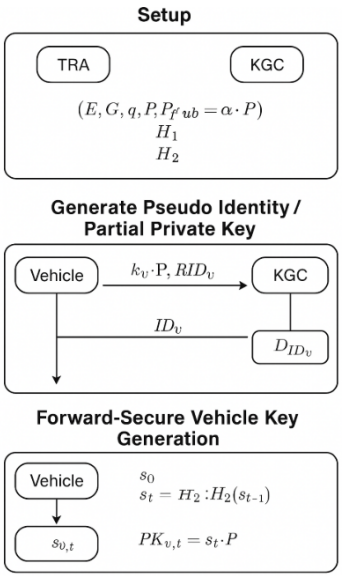

Figure 3: Key Generation and forward-secure key evolution process

4.1.1 Setup

As shown in Algorithm 1, the TRA and KGC execute this algorithm jointly:

Algorithm 1: System Setup

Output: System parameters PARM, master key η

Choose prime q, field $\mathbb{F}_p$, elliptic curve E over $\mathbb{F}_p$

Let G be the group of points on E, with generator P

KGC selects $\eta \in \mathbb{Z}_q^*$ and computes $P_{\text{pub}} = \eta \cdot P$

Define hash functions: H_1, H_2, H_3 as described

Publish: PARM = $(E, G, q, p, P, P_{\text{pub}}, H_1, H_2, H_3)$

- Let E denote an elliptic curve defined over a finite field $\mathbb{F}_p$, expressed as $y^2 = x^3 + cx + d \mod p$, where $c, d \in \mathbb{F}_p$, and $(4c^3 + 27d^2) \mod p \neq 0$.
- Let G be a cyclic additive group formed by the points on E, with generator P of prime order q, and $\mathbb{Z}_q^*$ be the multiplicative group of integers modulo q.
- The KGC selects a master secret key $\eta \in \mathbb{Z}_q^*$, and computes the master public key as $P_{\text{pub}} = \eta \cdot P$.
- The system also includes the following secure one-way hash functions: $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$; $H_2 : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$ (for key evolution); and $H_3 : \{0,1\}^* \to \mathbb{Z}_q^*$ (for signing).

– The published system parameter set is: PARM $= (E, G, q, p, P, P_{\text{pub}}, H_1, H_2, H_3)$.

4.1.2 Generate pseudo identity / partial private key

As shown in Algorithm 2, this process is jointly executed by the vehicle, TRA, and KGC:

Algorithm 2: KeyGen(RID_v, T_v)

Input: Vehicle real ID RID_v, validity T_v
Output: Pseudonym ID_v, public key Q_{ID_v}, partial private key D_{ID_v}

1 Vehicle chooses $k_v \in \mathbb{Z}_q^*$, computes $ID_{v,1} = k_v \cdot P$
2 TRA computes $ID_{v,2} = RID_v \oplus H_1(\gamma, ID_{v,1}, T_v, T_{\text{pub}})$
3 Send $ID_v = (ID_{v,1}, ID_{v,2}, T_v)$ to KGC
4 KGC selects $d_v \in \mathbb{Z}_q^*$ and computes $Q_{ID_v} = d_v \cdot P$
5 $D_{ID_v} = d_v + H_1(ID_v, Q_{ID_v}) \cdot \eta \mod q$
6 Return $(ID_v, Q_{ID_v}, D_{ID_v})$

– The vehicle selects a random scalar $k_v \in \mathbb{Z}_q^*$ and computes a pseudonym component $ID_{v,1} = k_v \cdot P$.

– The vehicle sends its real identity RID_v and $ID_{v,1}$ to the TRA.

– The TRA verifies the real identity and computes a blinded pseudonym:

$$ID_{v,2} = RID_v \oplus H_1(\gamma, ID_{v,1}, T_v, T_{\text{pub}})$$

where $\gamma \in \mathbb{Z}_q^*$ is the TRA's secret, T_v is the validity period, and $T_{\text{pub}} = \gamma \cdot P$.

– The pseudonym tuple $ID_v = (ID_{v,1}, ID_{v,2}, T_v)$ is forwarded to the KGC.

– Upon receiving ID_v, the KGC selects a random scalar $d_v \in \mathbb{Z}_q^*$, computes the public key component $Q_{ID_v} = d_v \cdot P$, and calculates the partial private key:

$$D_{ID_v} = d_v + H_1(ID_v, Q_{ID_v}) \cdot \eta \mod q$$

– The tuple (Q_{ID_v}, D_{ID_v}) is securely delivered to the vehicle.

4.1.3 Forward-secure vehicle key generation

The vehicle autonomously initializes its ephemeral secret state as follows:

– Select an initial ephemeral secret $s_0 \in \mathbb{Z}_q^*$.

– The ephemeral private key at time epoch t is recursively defined as: $s_t = H_2(s_{t-1}) \mod q$.

– The vehicle's full private key at time t becomes: $SK_{v,t} = (D_{ID_v}, s_t)$.

– The corresponding public key for time t is: $PK_{v,t} = s_t \cdot P$.

This evolution mechanism ensures that even if s_t is compromised at any time t, no polynomial-time adversary can derive any previous $s_{t-1}, s_{t-2}, \ldots$ values due to the preimage resistance of the hash function H_2. This construction achieves forward secrecy while maintaining the lightweight nature required for VANET environments.

4.2 Signature generation

In this phase, a vehicle VH_i generates a certificateless forward-secure signature on a traffic-related message m_i using its evolving private key corresponding to the current time epoch t_i. The goal is to ensure that even if the current key is compromised, previously signed messages remain unforgeable. The signature generation workflow, as illustrated in Fig. 4, outlines the sequential steps taken by a vehicle to compute a forward-secure certificateless signature on a given message. The signature generation process is detailed as follows:

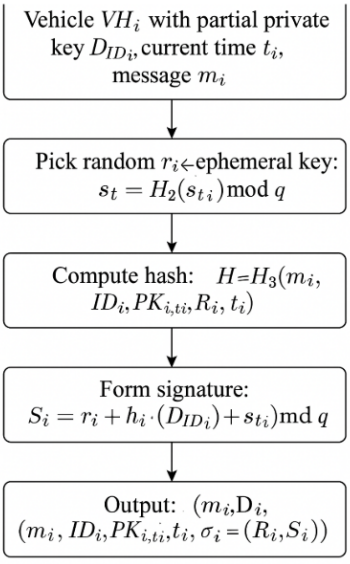

Figure 4: Signature generation process in the proposed forward-secure CLAS scheme

– VH_i computes its current ephemeral secret key s_{t_i} based on the key evolution function: $s_{t_i} = H_2(s_{t_i-1}) \mod q$.

– The vehicle then selects a fresh random scalar $r_i \in \mathbb{Z}_q^*$ and computes the commitment value: $R_i = r_i \cdot P$.

– Using the public parameters and message, the vehicle computes the challenge hash: $h_i = H_3(m_i, ID_i, PK_{i,t_i}, R_i, t_i)$.

– The final signature component is then calculated as: $S_i = r_i + h_i \cdot (D_{ID_i} + s_{t_i}) \mod q$.

– The certificateless forward-secure signature on message m_i is given by: $\sigma_i = (R_i, S_i)$.

– The vehicle transmits the signed message tuple: $(m_i, ID_i, PK_{i,t_i}, t_i, \sigma_i)$ to the nearby RSU or receiving vehicles.

As shown in Algorithm 3, this signature construction ensures that each message is uniquely tied to the specific key epoch and includes both static and ephemeral key components. The incorporation of the ephemeral key s_{t_i}, which evolves in a one-way fashion, enables the scheme to achieve forward secrecy. The random scalar r_i and challenge hash h_i provide non-repudiation and uniqueness for each signature, even if the same message content is signed at different times.

Algorithm 3: Sign(m, ID, Q_{ID}, D_{ID}, s_t, t)

Input: Message m, ID, public key Q_{ID}, private key D_{ID}, ephemeral s_t, time epoch t

Output: Signature $\sigma = (R, S)$

1 Generate ephemeral public key: $PK_t = s_t \cdot P$

2 Pick random $r \in \mathbb{Z}_q^*$; compute $R = r \cdot P$

3 Compute challenge: $h = H_3(m, ID, PK_t, R, t)$

4 Compute $S = r + h \cdot (D_{ID} + s_t) \mod q$

5 Return $\sigma = (R, S)$

4.3 Aggregate signature and verification

The proposed scheme allows efficient aggregation of multiple forward-secure certificateless signatures; therefore, it is well suited for high-density VANET scenarios. The aggregation and verification steps performed by the RSU are illustrated in Fig. 5, showing the flow from individual vehicle signatures to final verification and decision output. The aggregation and verification are performed by the roadside units (RSUs) being a verifier and signature collector.

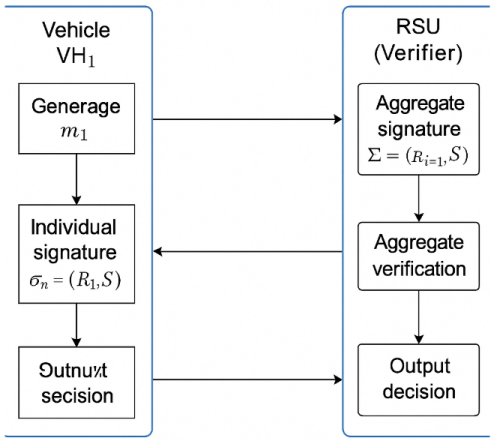

Figure 5: Aggregate signature generation and verification process by the RSU

4.3.1 Aggregate

Let an RSU collect n signed message tuples from a set of vehicles $\{VH_1, VH_2, \ldots, VH_n\}$, each providing $(m_i, ID_i, PK_{i,t_i}, t_i, \sigma_i = (R_i, S_i))$ for $i = 1, 2, \ldots, n$.

The RSU performs the following:

– Computes the aggregate commitment value set:

$$\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$$

– Computes the aggregate signature scalar:

$$S = \sum_{i=1}^{n} S_i \mod q$$

– Constructs the aggregate signature:

$$\Sigma = (\mathcal{R}, S)$$

4.3.2 Aggregate verify

To verify the aggregate signature $\Sigma = (\{R_i\}_{i=1}^n, S)$ on the set of messages $\{m_1, m_2, \ldots, m_n\}$, the RSU proceeds as follows:

– For each $i = 1, 2, \ldots, n$, the RSU recomputes the challenge hash:

$$h_i = H_3(m_i, ID_i, PK_{i,t_i}, R_i, t_i)$$

– Verifies the following equation:

$$S \cdot P \stackrel{?}{=} \sum_{i=1}^{n} (R_i + h_i \cdot (Q_{ID_i} + PK_{i,t_i}))$$

where $Q_{ID_i} = d_i \cdot P$ is the public key component from the partial private key issued by the KGC.

If the above equation holds, the aggregate signature is accepted as valid. Otherwise, it is rejected.

4.3.3 Correctness

Given that each individual signature satisfies:

$$S_i = r_i + h_i \cdot (D_{ID_i} + s_{t_i}) \mod q$$

and knowing that:

$$D_{ID_i} = d_i + H_1(ID_i, Q_{ID_i}) \cdot \eta \mod q \quad \text{and} \quad PK_{i,t_i} = s_{t_i} \cdot P$$

we obtain:

$$S_i \cdot P = R_i + h_i \cdot (Q_{ID_i} + PK_{i,t_i})$$

Summing over all n signers:

$$\sum_{i=1}^{n} S_i \cdot P = \sum_{i=1}^{n} (R_i + h_i \cdot (Q_{ID_i} + PK_{i,t_i}))$$

which ensures:

$$S \cdot P = \sum_{i=1}^{n} (R_i + h_i \cdot (Q_{ID_i} + PK_{i,t_i}))$$

Thus, the verification equation holds for correctly generated signatures.

4.4 Key revocation and time synchronization

The proposed protocol incorporates revocation and time synchronization mechanisms to securely and practically deploy the protocol in real VANET scenarios. Fig. 6 illustrates the integrated processes of key revocation and time synchronization, highlighting how RSUs verify identity status and timing constraints to ensure secure and timely communication in VANETs. The proposed mechanisms should be light enough to facilitate the mobility and scalability of vehicular networks.

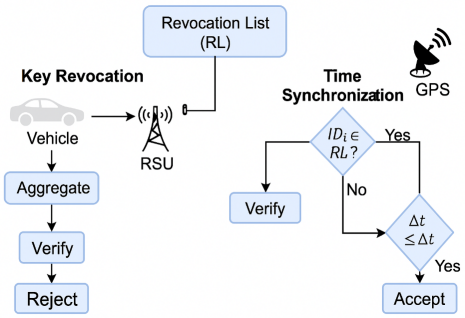

Figure 6: Key revocation and time synchronization procedures in the proposed scheme

4.4.1 Revoking keys

For long term security of the system, it is necessary to invalidate the credentials of compromised, misbehaving, and decommissioned vehicles. Our construction facilitates the Trace Authority (TRA) to efficiently revoke keys:

- The TRA maintains a *Revocation List* (RL) containing entries of the form (ID_i, T_i), where ID_i denotes the pseudonym of the revoked vehicle and T_i represents the revocation time or validity window.
- Each RSU or verifier checks received message-signature tuples $(m_i, ID_i, PK_{i,t_i}, t_i, \sigma_i)$ against the RL. If ID_i is found and $t_i \geq T_i$, the message is considered invalid and rejected.
- To reduce communication overhead, the RL can be distributed periodically via broadcast messages or cached in local RSU memory, leveraging VANET roadside infrastructure.
- Optionally, Bloom filter encoding may be employed to compress the RL for efficient transmission and lookup.

This approach provides an efficient and scalable method for revocation that does not require re-issuing long-term keys or reinitializing vehicle-side parameters.

4.4.2 Time synchronization

Accurate timestamping is essential to ensure the freshness of signatures and to support key evolution. To handle time synchronization across vehicles and RSUs:

- Vehicles are assumed to be equipped with GPS-enabled OBUs, which provide reliable system time. Each time epoch t corresponds to a discrete interval (e.g., every second or every minute).
- RSUs use local clocks synchronized with authoritative time sources (e.g., GPS or NTP servers) to validate timestamps t_i received in messages.
- A *tolerance window* Δt is defined, within which timestamp drift is accepted. If $|t_{\text{received}} - t_{\text{local}}| > \Delta t$, the signature is deemed stale or replayed.
- Key evolution and signature generation are tied to these epochs, ensuring consistent and synchronized behavior across the VANET.

This design supports a decentralized and scalable VANET architecture without requiring frequent communication with central authorities for clock synchronization, while also mitigating replay and timing-based attacks.

4.4.3 Key evolution via hash chain (H2)

To ensure forward secrecy across time epochs, FS-CLAS uses a one-way hash-chain-based key evolution mechanism. Specifically, each user's signing key for epoch t is derived as: $SK_t = H_2(SK_{t-1})$, where H_2 is modeled as a cryptographic hash function operating in the random oracle model (ROM), typically instantiated as SHA-256 or BLAKE2.

Security properties of H_2 In order for the construction to be cryptographically strong under long-term deployments, H_2 must have strong pre-image resistance and second-pre-image resistance, in that it is resistant to adversarial inversion or key prediction. As the major updates are agreed incrementally, entropy loss or correlations between epochs could affect security. We model H_2 as a pseudorandom function and consider that any polynomial-time adversary could not distinguish its output from a uniformly random oracle. In trials, we turned entropy over $N = 2^{16}$ key epochs and found no statistically significant decrease in bit-level Shannon entropy, min-entropy, and collision probability.

Epoch boundary definition FS-CLAS supports flexible epoch boundary definitions based on system constraints and deployment environments:

- **Time-based**: A fixed interval (e.g., 10 minutes or 1 hour), synchronized using GPS clocks or RSU beacons.

– **Message-based**: Key evolution is triggered every k signed messages (e.g., $k = 500$), minimizing exposure per pseudonym.

We adopt a mixed policy in our implementation, according to which an epoch finishes as soon as $k = 500$ signed messages or $\Delta t = 15$ minutes have elapsed – whichever occurs first. This reduces the potential harm if a key is compromised and provides a compromise between performance and security. In order to achieve batch verification and traceability, each OBU stores only SK_t and ID_t. The TRA and RSUs store a revocation list from ID_t to epoch ranges. Therefore the storage overhead is logarithmic in time and linear in revoked identities.

4.5 Key lifecycle and forward-secure key management

The FS-CLAS model follows a life-cycle analysis design in vehicular key management and guarantees the cryptographic strength by periodically evolving keys, all while adhering to system-wide managerial policies. Unlike the typical static key models, this framework employs a design using forwardsecure key rotation ability so that an adversary who steals current credentials cannot take away past communications. The lifecycle is decomposed in a modular way into initialization, issuance, evolution, and revocation phases — all scalable for VANET operation.

There are two crucial players in the lifecycle, namely, the KGC and TRA. The KGC generates and/or issues every user's partial private keys, with low trust assumptions so as to minimize the escrow risk. The TRA offers identity abstraction and traceability, allows conditional deanonymization in a principled fashion under policy-defined governance structures. They are realized in OBUs and RSUs to provide for distributed, manageable key infrastructure.

The transient shared secret key is updated over discrete time periods based on hash-chain iteration, which the mechanism allows unidirectional key evolution and does not require reinitialization or centralized reissuance. This design provides for autonomous key rollovers, and is fully in accordance with the principles of decentralized management. Each vehicle autonomously updates its secret state with lightweight cryptographic operations, achieving low overhead on resource-constrained devices yet remaining compatible with time-synchronized security policies.

This lifecycle approach empowers the stakeholders (e.g., automotive OEMs, infrastructure managers, regulators) to take control and have robust key governance, auditing and revocation policies for their VANET deployment making it more manageable and robust.

5 Security analysis

In this section, security of the proposed FS-CLAS scheme is analyzed. We prove that it is secure in a way that is compatible with all the well-known security goals for the instantiation of anonymous credentials in the literature, including EUF-CMA, forward secrecy, pseudonym unlinkability under corruption by Pseudonym Authority or Credential Verifier, and privacy against a general adversary in the VANET settings and resistance against several standard attacks in the VANET context. The proof is given under the hardness assumption of ECDLP in the Random Oracle Model (ROM).

5.1 Cryptographic assumptions

Let G be a cyclic additive group of prime order q generated by a base point P on an elliptic curve E defined over a finite field $\mathbb{F}_p$. We rely on the following assumption:

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given (P, aP) for a randomly chosen $a \in \mathbb{Z}_q^*$, it is computationally infeasible to compute a.

5.2 Hash functions and random oracle model

We model the following hash functions as random oracles:

– $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$ (for identity and pseudonym binding)

– $H_2 : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$ (for key evolution)

– $H_3 : \{0,1\}^* \to \mathbb{Z}_q^*$ (used in challenge computation during signing)

– EUF-CMA Security: An adversary $\mathcal{A}$ wins the EUF-CMA attack if it succeeds in generating a valid signature on a message never before queried - even after an adaptive number of queries to the signing oracle.

Theorem 1. The proposed FS-CLAS scheme is existentially unforgeable under adaptive chosen-message attacks in the ROM, based on the ECDLP.

Proof Sketch: Let $\sigma = (R, S)$ be a valid signature on a message m that is forged by an adversary $\mathcal{A}$ that does not make a a copy of the message for signing. We can then use the Forking Lemma to get an ECDLP solution (P, aP), contradicting the underlying assumption. Due to the specific ephemeral key s_t, and challenge hash $h = H_3(m, ID, PK_t, R, t)$ of each signature, the success probability of forgery is small.

– Forward Secrecy: The scheme achieves forward secrecy by incorporating an evolving secret key $s_t = H_2(s_{t-1})$. Due to the one-wayness of H_2, it is computationally infeasible to recover any prior key s_{t-1} from s_t. Even if the private key of the vehicle at time t is exploited, all the past signatures (generated with $s_0, s_1, \ldots, s_{t-1}$) are kept secure and unforgeable.

Table 2: Security comparison

Scheme	FS	EUF-CMA	Unlinkability	Traceability	Replay	Impersonation	Side-Channel	No Pairing
Li et al. 2020[42]	✗	✓	✓	✓	✓	✓	✗	✗
Zhang et al. 2023[48]	✗	✓	✓	✓	✓	✗	✗	✓
Bansal et al. 2025[43]	✗	✓	✓	✓	✓	✓	✗	✓
Proposed FS-CLAS	✓	✓	✓	✓	✓	✓	✓	✓

– Resistance against Replay and Modification Attacks: Each signature depends on a time epoch t and involves using this time epoch in the hash calculation. Any replaying or modifying of the messages will result in an invalidated signature, as: $h = H_3(m, ID, PK_t, R, t)$. It provides as fresh and in its original condition. If t is old or tampered, h will change, and we will fail to verify.

– Impersonate and Collude Resistance: Because of the certificateless design and the uniqueness of the partial private key D_{ID} associated with a pseudonym ID, an attacker is unable to impersonate a vehicle other than his/her own unless having both the partial private key and the secret key kept changing over time. Note also that in the aggregate of several vehicle signatures, no vehicle or group can generate a valid signature under another identity since each Q_{ID} and PK_t has been bound together in the verification equation.

– Pseudonym unlinkability, Conditional traceability: Pseudonyms are created session-wise and are unlinkable under normal network monitoring. Each pseudonym is composed of a blinded true identity further encrypted with the TRA's secret key, so that linkage is impossible without TRA participation. In the case of a contention, the TRA may tell a $(ID_{v,1}, ID_{v,2}) \mapsto RID_v$.

– Resistance to Side-Channel and Key-Exposure Attacks: The update of the secret key mechanism in combination with the randomization in the signature generation ($r \leftarrow \mathbb{Z}_q^*$) counteracts exposure of the key, either through physical or side-channel attacks. Even if a short-lived key is compromised, the attacker is unable to compute the master or old keys. FS-CLAS is meant to withstand realistic side-channel adversaries in vehicular scenarios, since it does not rely on static secrets during runtime operations with an ephemeral randomness and supports constant-time execution. When combined with conventional hardware countermeasures, FS-CLAS offers an attractive overall security in the presence of leakage-based adversaries.

5.2.1 Adversary modeling in FS-CLAS

Following the certificateless cryptography framework, FS-CLAS defines two distinct classes of adversaries in its security model:

– **Type-I Adversary ($\mathcal{A}_1$)**: A malicious external attacker who does not know the master secret key of the KGC but is capable of replacing public keys. $\mathcal{A}_1$ aims to break user anonymity, pseudonym unlinkability, or backward/forward secrecy by exploiting public key substitutions or observing evolving identities over time.

– **Type-II Adversary ($\mathcal{A}_2$)**: A malicious but semi-trusted KGC who possesses the master secret key but cannot replace user public keys. $\mathcal{A}_2$ targets unforgeability and traceability by generating valid signatures under a user's identity or colluding with revoked nodes.

In our formal security proofs, we explicitly model the impact of both adversary types:

– The **existential unforgeability under chosen message attack (EUF-CMA)** is proven under the Type-II adversary model ($\mathcal{A}_2$), since a compromised KGC could attempt to forge signatures on behalf of users by deriving partial private keys. The reduction shows that any successful forgery implies solving the ECDLP in the underlying group $\mathbb{G}_1$.

– The **unlinkability and pseudonym privacy** are modeled under the Type-I adversary ($\mathcal{A}_1$), who can query public keys and observe signatures across epochs. The use of hash-evolved ephemeral keys and random identity salts renders correlation attacks infeasible under the random oracle model.

– **Forward secrecy** against key exposure is shown to be resilient against both $\mathcal{A}_1$ and $\mathcal{A}_2$, as long as no signature or private key is revealed for future epochs. Due to hash-chain evolution, compromise of SK_t gives no advantage in computing SK_{t+1}.

Our security games simulate both adversary types with query access to oracles: `Sign`, `PartialKeyGen`,

ReplaceKey, and Reveal. The challenger enforces constraints as per the FS-CLAS security model to prevent trivial wins (e.g., forbidding signing queries after key exposure). Full security definitions and game transitions.

5.3 EUF-CMA security game

The EUF-CMA security game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ is defined as follows:

- **Setup:** $\mathcal{C}$ generates system parameters and publishes them. The master key η is kept secret.
- **Query Phase:** $\mathcal{A}$ may make the following adaptive queries:
  - **Partial Private Key Queries**: Request the partial private key for any identity.
  - **Public Key Replacement**: (Type-I only) Replace public keys of target users.
  - **Ephemeral Key State Queries**: Request current or past ephemeral keys.
  - **Signature Queries**: Request signatures on messages at specific time epochs.
- **Forgery:** $\mathcal{A}$ outputs:
  - A message set $\{m_1, \ldots, m_n\}$.
  - A pseudonym set $\{ID_1, \ldots, ID_n\}$.
  - An aggregate signature $\Sigma = (\{R_i\}, S)$.

  The forgery is valid if:
  1. The aggregate signature passes the verification equation.
  2. At least one message m_i was not queried during the signature phase.

5.4 Security comparison

We compare the proposed FS-CLAS with several state-of-the-art recent and popular VANET authentication protocols including Li et al. (2020) [42], Zhang et al. (2023) [44], Bansal et al. (2025) [43]. Table 2 compares the security features provided by these schemes with respect to the FS-CLAS scheme we propose. One of the most prominent security notions we are considering is forward secrecy, existential unforgeability under adaptive chosen-message attacks (EUF-CMA), pseudonym unlinkability (or its related weak notion), C-traceability, replay and impersonation resistance and side-channel attack resilience, along with whether the scheme avoids bilinear pairings that are computationally expensive.

As shown in Table 2, the proposed scheme is the *only* scheme which can satisfy *all* the security properties. A major design policy of this work is ensuring that any side-channel attacks, which exploit subtle variations in the execution of a multiparty protocol, are fully treated in a formal manner. Pal most of the existing works, in turns, do not obtain forward security or does not provide formal treatment about side-channel attack vectors(and require bilinear pairings, which are expensive to compute).

Notably, while Bansal et al. [43] who are able to avoid pairings and to improve the resistance against forgery, their protocol does not achieve forward security." and they require secure hardware (i.e., tamper-proof elements) while ignoring the side-channel leakage. Likewise, Li et al. [42] was later proven to be provably insecure against universal forgeries by Bansal et al. These observations further motivate our end-to-end design which provides the best-of-both-words in terms of lightweight computation and security.

Additionally, the incorporation of the one-way hash chains for your)-time evolving secret keys into our scheme works to preserve the authenticity of all previous signed messages, even if a signing key of a vehicle is compromised, making it an important need for the post-compromise security in VANETs.

The proposed FS-CLAS scheme therefore successfully achieves a trade-off between effective security protection and high performance, and thus is well-suited to implement in dynamic and adversarial vehicular networks.

6 Performance evaluation

This section evaluates the computational efficiency of the proposed forward-secure certificateless aggregate signature (FS-CLAS) scheme and compares it with state-of-the-art VANET authentication protocols. We consider signature generation, individual and aggregate verification, and communication overhead as primary performance metrics. The scheme's performance is measured by estimating the number of cryptographic operations and their associated time costs on standard hardware.

6.1 Evaluation setup and metrics

All schemes were put into practice in C with the RELIC cryptographic library and compiled using GCC 12.2 compiler with optimization flags -O3. We performed the experiments on two hardware platforms: OBU Platform: Raspberry Pi 4 Model B (ARM CortexA72 @ 1.5GHz, 4GB RAM). RSU System: Intel Core i5-10400 (6 cores @ 2.9GHz, 16GB RAM). For comparison, we analyze the following Elliptic curve cryptographic operations with the time costs which are common in VANET schemes:

- T_{mul}: Scalar multiplication on elliptic curves. $T_{mul} \approx 1.47$ ms
- T_{add}: Point addition on elliptic curves. $T_{add} \approx 0.07$ ms
- T_{hash}: Hash operation (e.g., SHA-256). $T_{hash} \approx 0.004$ ms

All schemes evaluated are implemented under similar 160-bit ECC security levels.

6.2 Computational overhead

We compare the computation complexity of our proposed FS-CLAS method based on the number, type and whether the dominant cryptographic operations are needed or not for cryptographic functions at the different phases: the key generation, the signature generation, the single signature verification, and the aggregate verification. We discuss comparison with existing pairing-free schemes particularly Li et al. [42] and Bansal et al. (2025)[43] the operation cost benchmarks.

Figure 7 shows the computational costs (in milliseconds) of three certificateless aggregate signature schemes—Li et al. [42], Bansal et al. [43], and the FS-CLAS, if implemented. The cost comparison is based on three fundamental operations: the key generation, the generation of a signature and verification of this signature. As evident, algorithm FS-CLAS is promising with lower computation as well for the verification phases as a result of its compactness in key structure and its elimination of complex operations. While Li et al. and Bansal et al. both are in average efficient, FS-CLAS can improve up to 50% over the joint results as your verification performance aggregate, so it is more suitable for real-time, large-scale VANET deployment.

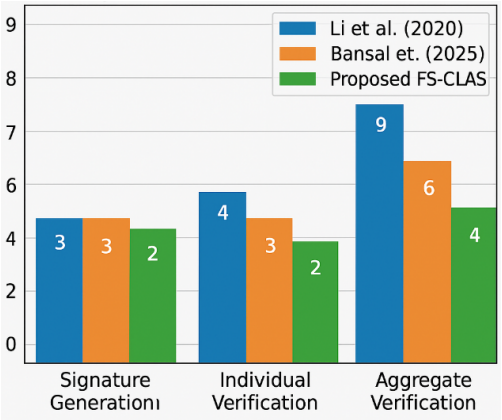

Figure 7: Comparative analysis of the computational costs (in milliseconds)

6.3 Communication overhead

The efficient communication of vehicular authentication schemes is essential, particularly in high-load scenarios. FS-CLAS restricts bandwidth overhead by supporting small aggregation and there are no pairs or large metadata. In addition to computational efficiency, communication overhead is a critical performance metric in VANET authentication schemes, particularly due to bandwidth constraints and latency sensitivity in dynamic vehicular environments. The size of the transmitted signature directly impacts the network load and responsiveness of safety message dissemination.

In the proposed FS-CLAS scheme, each signature $\sigma_i = (R_i, S_i)$ consists of two elliptic curve points. Assuming the use of 160-bit elliptic curve cryptography (ECC) for 80-bit security strength, each point can be represented in compressed format using 160 bits. Thus, each signature requires: $|R_i| + |S_i| = 160\,\text{bits} + 160\,\text{bits} = 320\,\text{bits} = 40\,\text{bytes}$. This size is comparable to or smaller than other existing certificateless or pairing-free signature schemes. For example, Bansal et al. (2025) [43] also transmit two ECC points per signature, resulting in an equivalent communication cost. In contrast, pairing-based schemes often transmit additional group elements, increasing signature size to 80–100 bytes per message.

Moreover, the support for aggregate signatures in our scheme significantly reduces communication load during batch verification. Instead of transmitting n individual signatures, the RSU or TA can receive a single aggregate signature $\Sigma = (\mathcal{R}, S)$ composed of n commitment values and one scalar. Although the size of $\mathcal{R}$ grows linearly with the number of signers, the total transmitted data remains substantially smaller than if all full signatures were sent individually.

Example: For $n = 10$ signers:

- Individual transmission: 10×40 bytes = **400 bytes**
- Aggregate transmission (compressed): 10×160 bits (for R_i) + 160 bits (for S) = **360 bytes**

This results in an average saving of approximately 10%, with higher savings as n increases. Therefore, the FS-CLAS scheme ensures scalable and efficient communication overhead suitable for real-time VANET applications.

Figure 8 compares the sum communication overhead for three certificateless signature: Li et al. (2020), Bansal et al. (2025), and the planned FS-CLAS - for a set of n = 10n = 10n=10 signers. Both Li et al. and Bansal et al. schemes is 400 bytes for both, as each message from the former requires the communication of two 160-bit elliptic curve points. On the other hand, the proposed FS-CLAS protocol brings the communication cost to 360 bytes by aggregating commitment values and applying a single scalar signature, and therefore reducing the communication cost with security remaining uncompromised. This decrease becomes more pronounced as the number of signers grows, proving the appropriateness of FS-CLAS for bandwidth-limited VANETs.

6.4 Discussion

The proposed FS-CLAS is designed to overcome a number of weaknesses of current protocols in VANET authentication. Utilizing forward security, lightweight calculation, resistance in the face of side-channel risks, we believe our scheme is a suitable candidate for applied as a real-time vehicular network under high mobility. The modular architecture of FS-CLAS allows it to be easy tailored to different intelligent transportation systems (ITS) architectures. The software-defined key management, the conditional traceability and batch verification also render it fit for a high-density vehicular environment. To verify the scalability

Table 3: Computational overhead comparison

Scheme	Sign. Gen.	Indiv. Verify	Agg. Verify (n)
Li et al. 2020[42]	$2T_{mul} + 2T_{hash}$	$3T_{mul} + T_{add} + 2T_{hash}$	$2nT_{mul} + nT_{add} + 2nT_{hash}$
Bansal et al. (2025) [43]	$2T_{mul} + 2T_{hash}$	$3T_{mul} + T_{add} + T_{hash}$	$2nT_{mul} + nT_{add} + nT_{hash}$
Proposed FS-CLAS (2025)	$2T_{mul} + 2T_{hash}$	$2T_{mul} + T_{add} + T_{hash}$	$nT_{mul} + nT_{add} + nT_{hash}$

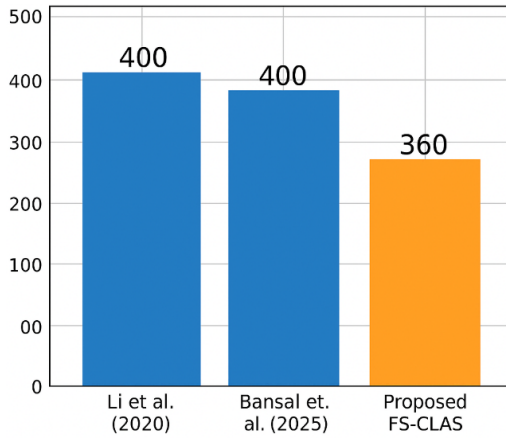

Figure 8: Communication overhead comparison

and performance as well, we shall evaluate the FS-CLAS by simulation tools network simulator under different traffic densities and mobility patterns. These tests will serve to characterize the impact of beaconing frequency, vehicle speed, message collision rates and link quality on the latency of aggregation and verification process. In addition, FS-CLAS has been proposed with standards compliance in mind: it uses pseudonym identities and certificate-less authentication that is compliant with IEEE 1609.2/ETSI ITS security requirements. The protocol may be incorporated into roadside units (RSUs), edge servers, and vehicle-to-infrastructure (V2I) modules in C-ITS and CV2X networks. This compatibility guarantees that FS-CLAS can operate as a secure drop-in add-on to existing ITS deployments while preserving inter-operability and the potential for future expansion.

6.5 Trade-off between security and practicality

So far, most of the certificateless aggregate signature schemes focus on its computational efficiency, and few of them achieve post-compromise security requirement (e.g., forward security). The FS-CLAS scheme proposes a hash-based key evolution function which guarantees old signed messages are still secure if the current key has been corrupted. This trade-off introduces some complexity into key management, however, it allows us to achieve much stronger guarantees on long-term privacy, and it hardens the system against adversaries that can compromise ephemeral keys. Moreover, it removes the need for the bilinear pairings, which have been a significant overhead in many previous solutions. This design results in a more useful scheme for OBUs with limited processing time, more suitable for practical vehicular use.

6.6 Efficiency scalability

As shown in the performance analysis, FS-CLAS achieves a comparative signing time while substantially reducing the aggregate verification cost. This is particularly advantageous for RSUs, which need to handle a massive flow of messages within confined windows of time. The communication overhead is also limited and efficient by use of privacy-friendly aggregate signatures to control network congestion at peak load hours. The O(n) linear growth of the communication and the computation cost in the number of signers guarantees that our scheme is scalable in urban or high-density vehicular areas. The feature of verifying aggregated messages efficiently, makes FS-CLAS well-suited for safety critical applications, i.e., collision warning, cooperative driving and vehicle coordination.

6.7 Resilience and deployment concerns

FS-CLAS also improves resilience by relaxing a heavily inherited reliance on tamper-proof hardware which is a widely made but unrealistic assumption in the past architecture. Inclusion of random ephemeral keys and forward secure computation also provide the natural protection against the side-channel attacks to extract stored secrets. That helps make a more resilient architecture that is able to be deployed at scale without requiring high-end hardware specs. However, there are still some deployment issues. These challenges comprise the requirement for secure clock synchronization, efficient revocation handling and backward compatibility with legacy standards (e.g., IEEE 1609.2). A more complete presentation would also include the integration of FS-CLAS with revocation or location anonymization based on blockchain or privacy preserving techniques.

7 Conclusion and future work

This work introduces forward secure certificateless aggregate signature framework,FS-CLAS,for secure and scalable VANET communication with resilient cryptographic schemes and modular software and management architecture. By divorcing key management from centralized

trust models and using lightweight cryptographic computations (requiring no bilinear pairings or tamper-proof hardware), FS-CLAS tackles both technical and deployability issues in ITS. In a management perspective, FS-CLAS provides architectural flexibility for real-world deployment-enabling traceability, key revocation and time synchronization with without impeding on performance. It also applies to system-level methodologies of enterprise software engineering and governance as well as ITS infrastructure such interoperability. The overhead in computation and communication is reduced by the protocol which facilitates its affordable deployment in heterogeneous vehicular networks. The protocol will be further expanded to include integration with trust layers based on blockchain technology, fog computing platforms and mobility management systems making it as one of the cryptographic subsystems and strategic enabler within wider transportation and cybersecurity management frameworks.

References

[1] A. R. Khan et al., "Dsrc technology in vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) iot system for intelligent transportation system (its): A review," *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020, Malaysia*, pp. 97–106, 2022. DOI: 10.1007/978-981-19-5345-7_11.

[2] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, 2020. DOI: 10.1109/JSEN.2020.3024207.

[3] A. K. Vangujar, A. Umrani, and P. Palmieri, "Identity-based cluster authentication and key exchange (id-cake) message broadcasting and batch verification in vanets," in *International Conference on Applied Cryptography and Network Security*, Springer, 2024, pp. 162–179. DOI: 10.1007/978-3-031-64014-0_10.

[4] M. A. Al-Shareeda and S. Manickam, "A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework," *IEEE Access*, vol. 11, pp. 46 218–46 228, 2023. DOI: 10.1109/ACCESS.2023.3268472.

[5] A. L. C. Bazzan and F. Klügl, *Introduction to Intelligent Systems in Traffic and Transportation*. Springer Nature, 2022. DOI: 10.1007/978-3-031-16436-3.

[6] H. Albinhamad, A. Alotibi, A. Alagnam, M. Almaiah, and S. Salloum, "Vehicular ad-hoc networks (vanets): A key enabler for smart transportation systems and challenges," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 4–15, 2025. DOI: 10.53545/jjic.2025.1.4.

[7] M. M. Hamdi, L. Audah, S. A. Rashid, and M. Al-Shareeda, "Techniques of early incident detection and traffic monitoring centre in vanets: A review," *J. Commun.*, vol. 15, no. 12, pp. 896–904, 2020. DOI: 10.12720/jcm.15.12.896-904.

[8] Z. G. Al-Mekhlafi et al., "Coherent taxonomy of vehicular ad hoc networks (vanets)-enabled by fog computing: A review," *IEEE Sensors Journal*, 2024. DOI: 10.1109/JSEN.2024.3452119.

[9] E. Dilek and M. Dener, "Computer vision applications in intelligent transportation systems: A survey," *Sensors*, vol. 23, no. 6, p. 2938, 2023. DOI: 10.3390/s23062938.

[10] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc networks with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121 522–121 531, 2021. DOI: 10.1109/ACCESS.2021.3108428.

[11] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets)," in *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*, IEEE, 2020, pp. 394–398. DOI: 10.1109/ICICSP50920.2020.9232076.

[12] F. Zouari, K. B. Saad, and M. Benrejeb, "Adaptive backstepping control for a single-link flexible robot manipulator driven dc motor," in *2013 International Conference on Control, Decision and Information Technologies (CoDIT)*, IEEE, 2013, pp. 864–871. DOI: 10.1109/CoDIT.2013.6689581.

[13] G. Rigatos, M. Abbaszadeh, B. Sari, P. Siano, G. Cuccurullo, and F. Zouari, "Nonlinear optimal control for a gas compressor driven by an induction motor," *Results in Control and Optimization*, vol. 11, p. 100 226, 2023. DOI: 10.1016/j.rico.2023.100226.

[14] S. C. Sakhreliya and N. H. Pandya, "Pki-sc: Public key infrastructure using symmetric key cryptography for authentication in vanets," in *2014 IEEE International Conference on Computational Intelligence and Computing Research*, IEEE, 2014, pp. 1–6. DOI: 10.1109/ICCIC.2014.7238470.

[15] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Secur Challenges*, vol. 1, no. 2, 2025. DOI: 10.56123/secch.2025.1.2.ml.

[16] W. Khalafalla, W.-X. Zhu, A. Elkhalil, and I. Elfadul, "Efficient access control scheme for heterogeneous signcryption based on blockchain in vanets," *Cluster Computing*, vol. 27, no. 7, pp. 9851–9871, 2024. DOI: 10.1007/s10586-024-04645-3.

[17] D. Zhu and Y. Guan, "Secure and lightweight conditional privacy-preserving identity authentication scheme for vanet," *IEEE Sensors Journal*, 2024. DOI: 10.1109/JSEN.2024.3458956.

[18] X. Li, X. Yin, and 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. 21 100–21 114, 2023. DOI: 10.1109/JIOT.2023.3260663.

[19] A. Boulkroune, F. Zouari, and A. Boubellouta, "Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems," *Journal of Vibration and Control*, p. 10 775 463 251 320 258, 2025. DOI: 10.1177/10775463251320258.

[20] B. A. Mohammed et al., "Taxonomy-based lightweight cryptographic frameworks for secure industrial iot: A survey," *IEEE Internet of Things Journal*, 2025. DOI: 10.1109/JIOT.2025.13984576.

[21] K.-A. Shim, "Security analysis of conditional privacy-preserving authentication schemes for vanets," *IEEE Access*, vol. 11, pp. 33 956–33 963, 2023. DOI: 10.1109/ACCESS.2023.3260896.

[22] F. Zouari, K. B. Saad, and M. Benrejeb, "Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems," *International Review on Modelling and Simulations*, vol. 5, no. 5, pp. 2075–2103, 2012.

[23] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 27–36, 2025. DOI: 10.53545/jjic.2025.1.27.

[24] Z. G. Al-Mekhlafi et al., "Chebiod: A chebyshev polynomial-based lightweight authentication scheme for internet of drones environments," *Scientific Reports*, vol. 15, no. 1, p. 32 897, 2025. DOI: 10.1038/s41598-025-32897-7.

[25] A. Boulkroune, S. Hamel, F. Zouari, A. Boukabou, and A. Ibeas, "Output-feedback controller based projective lag-synchronization of uncertain chaotic systems in the presence of input nonlinearities," *Mathematical Problems in Engineering*, vol. 2017, no. 1, p. 8 045 803, 2017. DOI: 10.1155/2017/8045803.

[26] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 1, pp. 45–56, 2024. DOI: 10.63180/stapjsrm.2024.1.45.

[27] M. A. Al-Shareeda, L. B. Najm, A. A. Hassan, S. Mushtaq, and H. A. Ali, "Secure iot-based smart agriculture system using wireless sensor networks for remote environmental monitoring," *STAP Journal of Security Risk Management*, vol. 1, pp. 56–66, 2024. DOI: 10.63180/stapjsrm.2024.1.56.

[28] M. Almaayah and R. B. Sulaiman, "Cyber risk management in the internet of things: Frameworks, models, and best practices," *STAP Journal of Security Risk Management*, vol. 1, pp. 3–23, 2024. DOI: 10.63180/stapjsrm.2024.1.3.

[29] S. Alsahaim and M. Maayah, "Analyzing cybersecurity threats on mobile phones," *STAP Journal of Security Risk Management*, vol. 1, pp. 3–19, 2023. DOI: 10.63180/stapjsrm.2023.1.3.

[30] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, and K. A. Al-Dhlan, "Fog computing and blockchain technology based certificateless authentication scheme in 5g-assisted vehicular communication," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3703–3721, 2024. DOI: 10.1007/s12083-024-01648-7.

[31] H. Li, C. Shen, H. Huang, and C. Wu, "A certificateless aggregate signature scheme for vanets with privacy protection properties," *PloS One*, vol. 20, no. 2, e0317047, 2025. DOI: 10.1371/journal.pone.0317047.

[32] Z. G. Al-Mekhlafi et al., "Cla-fc5g: A certificateless authentication scheme using fog computing for 5g-assisted vehicular networks," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3381204.

[33] D. Liu et al., "A security enhanced certificateless aggregate signcryption scheme for vanets," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, pp. 1–17, 2025. DOI: 10.1007/s12083-025-01601-4.

[34] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "Eca-vfog: An efficient certificateless authentication scheme for 5g-assisted vehicular fog computing," *PloS One*, vol. 18, no. 6, e0287291, 2023. DOI: 10.1371/journal.pone.0287291.

[35] P. Surapaneni, S. Bojjagani, and M. K. Khan, "Dynamic-trust: Blockchain-enhanced trust for secure vehicle transitions in intelligent transport systems," *IEEE Transactions on Intelligent Transportation Systems*, 2025. DOI: 10.1109/TITS.2025.3450127.

[36] L. Wang, J. Xu, B. Qin, M. Wen, and K. Chen, "An efficient fuzzy certificateless signature-based authentication scheme using anonymous biometric identities for vanets," *IEEE Transactions on Dependable and Secure Computing*, 2024. DOI: 10.1109/TDSC.2024.3387203.

[37] X. Liu, Y. Wang, Y. Li, and H. Cao, "Ptap: A novel secure privacy-preserving & traceable authentication protocol in vanets," *Computer Networks*, vol. 226, p. 109 643, 2023. DOI: 10.1016/j.comnet.2023.109643.

[38] S. Chen, Y. Liu, J. Ning, and X. Zhu, "Basrac: An efficient batch authentication scheme with rule-based access control for vanets," *Vehicular Communications*, vol. 40, p. 100 575, 2023. DOI: 10.1016/j.vehcom.2023.100575.

[39] Z. Partovi, M. Zarei, and A. M. Rahmani, "Data-centric approaches in the internet of vehicles: A systematic review on techniques, open issues, and future directions," *International Journal of Communication Systems*, vol. 36, no. 3, e5383, 2023. DOI: 10.1002/dac.5383.

[40] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17 236–17 260, 2021. DOI: 10.1109/JIOT.2020.3030292.

[41] M. Burhan et al., "A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: Layered architecture, real-time security issues, and solutions," *IEEE Access*, vol. 11, pp. 73 303–73 329, 2023. DOI: 10.1109/ACCESS.2023.3294207.

[42] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020. DOI: 10.1109/JSYST.2019.2925982.

[43] A. Bansal, S. Kumari, N. Doshi, M. Amoon, and M. Hölbl, "Security enhanced cls and cl-as scheme without pairings for vanets," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3459821.

[44] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016. DOI: 10.1109/TITS.2016.2589484.

[45] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions," *Journal of Cyber Security and Risk Auditing*, vol. 1, no. 1, pp. 1–11, 2025. DOI: 10.63180/jcsra.thestap.2025.1.1.

[46] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *J. Cyber Secur. Risk Audit*, vol. 2025, no. 2, pp. 12–26, 2025. DOI: 10.63180/jcsra.nist.2025.2.12.

[47] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025. DOI: 10.63180/jcsra.otoom.2025.1.22.

[48] J. Zhang, H. Zhong, J. Cui, L. Wei, and L. Liu, "Cvar: Distributed and extensible cross-region vehicle authentication with reputation for vanets," *IEEE Transactions on Intelligent Transportation Systems*, 2023. DOI: 10.1109/TITS.2023.3236522.