International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 4000-4011

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

CSAS-V: Certificateless Schnorr Aggregate Signature for VANETs

May Adnan Faleh[1], Mohammed Yousif[2], Mahmood A. Al-Shareeda[1,3*], Mohammed Amin Almaiah[4], Mansour Obaidat[5]

[1]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.*
[2]*Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, Iraq.*
[3]*Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq.*
[4]*King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.*
[5]*Applied College, King Faisal University, Al-Ahsa, Saudi Arabia.*

Corresponding author: Mahmood A. Al-Shareeda (*Email: mahmood.alshareedah@stu.edu.iq*)

Abstract

Efficient message authentication mechanisms for securing vehicular message exchange in VANETs are essential for meeting the diverse needs of real-time communication, driver safety, and data integrity. As such, certificateless aggregate signature (CLAS) schemes are widely used in this area, since they can significantly lower the communication and verification costs and overcome certificate management as well as key escrow issues that existing cryptography systems have. Nonetheless, bilinear pairings are still widely used in existing CLAS schemes, imposing a heavy computational burden and limiting scalability in high-density vehicular scenarios. In this paper, we develop CSAS-V, a novel Certificateless Schnorr Aggregate Signature scheme for VANETs. CSAS-V also utilizes the lightweight and pairing-free property of Schnorr signatures on a certificateless model to enable rapid, secure, and scalable message authentication. Our scheme achieves conditional privacy with pseudonyms, traceability with respect to a trusted authority, and strong security guarantees against both Type I and Type II adversaries under the assumption of the Discrete Logarithm Problem (DLP) in the random oracle model. Hence, we provide a thorough security analysis and show the performance of CSAS-V in terms of computational cost, communication cost, and scalability compared to recent CLAS schemes. To this end, the results show that CSAS-V provides a significant saving in the signing and verification time compared with existing signatures, without loss of security and privacy, and is particularly suitable for real-time applications in future intelligent transportation systems.

Keywords: Aggregate signature, Certificateless cryptography, Hoc networks (VANETs), Lightweight cryptographic protocol, Schnorr signature, Vehicular ad.

DOI: 10.53894/ijirss.v8i2.6200
Funding: This study received no specific financial support.
History: Received: 3 March 2025 / **Revised:** 4 April 2025 / **Accepted:** 7 April 2025 / **Published:** 14 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Acknowledgment: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant Number: KFU251391).
Publisher: Innovative Research Publishing

1. Introduction

VANETs are an enabler for intelligent transportation systems that allow secure, low-latency communication between vehicles and roadside units [1-3]. VANETs are used to improve vehicular safety, collision avoidance, and optimize traffic flow by periodically broadcasting messages such as Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) [4-6]. Nevertheless, the open and distributed characteristic of VANETs renders them vulnerable to many security and privacy attacks such as message forgery, replay attacks, impersonation, and vehicle tracking [7-9].

Digital signature schemes are one of the basic types of cryptographic mechanisms that can guarantee message authenticity and integrity in VANETs [10-12]. Traditional PKI solutions have been used, but they have too much certificate management overhead and scalability problems. IBC (Identity-Based Cryptography) provides a certificateless account system, but the KGC (Key Generation Center) can impersonate any user (key escrow problem) [13-15]. To address this issue, the Certificateless Public Key Cryptography (CL-PKC) approach has been proposed as a viable alternative capable of omitting certificates without giving the KGC full control over the keys [16-19].

Certificateless aggregate signature (CLAS) schemes have been proposed in order to effectively reduce bandwidth consumption and computational costs in high-density vehicular environments. Such schemes enable the aggregation of multiple signatures into one compact form, which drastically reduces communication overhead and allows for batch verification. Yet, existing CLAS schemes, mainly based on bilinear pairings, incur heavy computational overhead, which is not suitable for resource-efficient onboard units or real-time processing requirements.

In this work, we present a certificateless Schnorr aggregate signature (CSAS-V) for VANETs. CSAS-V builds a Schnorr signature framework that completely avoids bilinear pairings, bringing the real computation time of signing and verifying results to a lower level. Our scheme retains fundamental security properties—resilience against Type I and Type II adversaries, prevention of public key replacement, and protection against attacks from a malicious KGC—while allowing for conditional anonymity using pseudonyms and the ability to trace through a trusted authority.

In the random oracle model, we provide a formal proof of the security for CSAS-V under the Discrete Logarithm Problem (DLP) assumption. The results of the performance evaluations illustrate that CSAS-V offers significantly greater signing and verification efficiency compared to other existing pairing-based schemes while preserving full message authenticity and user privacy. Due to its lightweight construction and strong security guarantees, CSAS-V is best suited for real-time VANET applications that rely on scalable and privacy-preserving authentication methods. The contributions of this paper can be summarized as follows:

- Low Overhead: We propose a Schnorr signatures-based certificateless aggregate signature scheme without bilinear pairings, to mitigate their overhead in computation and communication.
- Improved security: CSAS-V is provably secure against Type I and Type II adversaries for public key replacement and malicious KGC attacks under the DLP assumption.
- Open Access and Traceability: The scheme provides a conditional anonymity with pseudonyms and allows a trusted authority to trace the identity of legitimate users. • Efficient Aggregation and Verification: CSAS-V offers compact signature aggregation and scalable batch verification, which is advisable for dense VANET deployment.
- Extensive Evaluation: Theoretical analysis and empirical comparison to existing CLAS schemes show that CSAS-V is both more efficient and scalable than prior solutions.

2. Related Work

Secure and efficient message authentication is essential in Vehicular Ad Hoc Networks (VANETs), which are critical for road safety, data integrity, and user privacy. Many digital signature schemes have been proposed for these needs over the last decade. Certificateless aggregate signature (CLAS) schemes are one of the most promising alternatives, as they provide communication overhead reduction and avoid the burden of certificate management and key escrow.

Traditional Public Key Infrastructure (PKI) underpins the security of various digital communications, providing entities with a way to authenticate and securely share information using digital certificates and trusted Certificate Authorities (CAs) to issue those certificates [20-24]. In contrast, conventional PKI has several limitations when it comes to its application to VANETs. Conventional PKI systems may not be scalable or latency-efficient within the VANET environments due to the high mobility, frequent topology changes, and real-time decision-making. The process of verifying the certificate, revocation, and distribution of Certificate Revocation Lists (CRLs) will take considerable time and will not be appropriate for real-time vehicular applications such as collision avoidance and emergency notifications [25-27]. Furthermore, the inherent centralized structure of PKI creates single points of failure and trust bottlenecks that hinder its resilience in highly dynamic, decentralized vehicular networks. There is also the issue of privacy preservation, because static certificates can be used to track the identities and movements of vehicles, which leads to violating user anonymity. Under these limitations, lightweight, decentralized, and privacy-aware authentication mechanisms tailored for VANETs is a necessity.

Wang et al. [28] presents a new conditional privacy-preserving certificateless aggregate signature (CLAS) scheme for VANETs, overcoming major shortcomings of existing schemes including susceptibility to passive attacks and inefficiency. Utilizing standard model proofs, full aggregation, and pseudonym techniques, it secures and accelerates communication between vehicles while keeping privacy in consideration in intelligent vehicular networks. The rapid development of Internet of Vehicles (IoV) has been proposed by Dong et al. [29] as a new paradigm for secure and reliable data communication. This proposes a new CLAS scheme with security proven in the standard model, which guarantees to be stronger in protecting realistic implementations. The efficiency and robustness of the scheme make it more suitable for use in the IoV environment.

Shim [30] studied the weaknesses of compact CLAS schemes in IoT, and we show that two schemes are vulnerable to universal forgery and type I attacks. The authors demonstrate flaws and mitigation options despite prior security claims. Clustering analysis ·enforces the importance of secure design in any CLAS schemes, as they should provide strong security but with lightweight components specific to the overall IoT context. Xu et al. [31] propose a pairing-free certificateless aggregate signature (CLAS) scheme that is secure and efficient for message authentication in IoT-based smart home environments. It improves verification speed and protects data integrity, while its security is based on elliptic curve cryptography. Performance evaluations demonstrate that it outperforms current CLAS approaches in terms of efficiency and security under the random oracle model. Wu and Ye [32] discovered that the PCAS certificateless aggregate signature scheme for VANETs does not guarantee unlinkability and is vulnerable to Type-I adversary attacks. We propose IPCAS, a secure and efficient alternative that is resilient against chosen message attacks while providing better performance. To enhance the applicability of IPCAS to realistic vehicular networks, IPCAS reduces both computational and communication overhead. Xu et al. [33] propose the lattice-based certificateless aggregate signature (LB-CLAS) scheme for vehicular ad hoc networks (VANETs) that achieves both strong security and high privacy in a post-quantum environment. Specifically, LB-CLAS greatly reduces the size of the signature, computation cost, and verification overhead by utilizing the hard problems of MSIS and MLWE and optimizing modes of V2V and V2I. Based on Dilithium, its design increases scalability, further reducing batch certification time by more than 90% with the squad vehicle count increase.

In 2025, certificateless aggregate signatures allow many users' signatures to be aggregated into one smaller signature, saving communication and achieving fast batch verification. Li et al. [34] designed a certificateless aggregate signature scheme for vehicular ad hoc networks (VANETs) that provides confidential privacy and is resilient to various known attacks. Nonetheless, their approach is based on bilinear pairings and incurs significant computational overhead, especially in the verification step. Although there is progress in CLAS designs for VANETs, most of the existing schemes either have high verification latency (due to pairing operations) or increase the message size. To overcome these shortcomings, we propose a new scheme called CSAS-V, which employs Schnorr signatures in a certificateless setting, thus eliminating the necessity for pairings entirely while also decreasing the computation and communication cost. This approach is not only optimizing the trade-off between security, privacy, and performance without sacrificing either of them, making CSAS-V the best choice for high-density, real-time vehicular context, unlike the previous works.

3. Preliminaries

3.1. System Model

We propose a scheme, CSAS-V, specifically suited for the VANET environment, which is composed of five entities: the TA, KGC, vehicles (OBUs), RSUs, and the AS. The roles of the system entities are particular to their purposes in the authentication, communication, and security processes.

- Trusted Authority (TA): The TA is a trusted entity that manages the vehicle registrations as well as the pseudonyms. It securely associates real vehicle identities with temporary pseudonyms, allowing conditional privacy. In cases of disputes or malice, the TA can do identity tracing to expose the true sender of a message [35-37].
- Key Generation Center (KGC): The KGC initializes the system-wide parameters and generates a partial private key for each registered vehicle. It relates to key distribution but does not construct the full private key through the certificateless design. This avoids key escrow but without the KGC itself being able to create valid signatures [38, 39].
- Vehicles (OBUs): Every vehicle is considered to have an On-Board Unit (OBU), which contains a Tamper-Proof Device (TPD) for safe keeper cryptographic keys, as well as carrying out specific operations. Each vehicle part of its private keys are generated independently, and the messages are signed with pseudo names. They relay authenticated safety and status messages to proximal vehicles and RSUs in real-time [40-42].
- Roadside Units (RSUs): At fixed locations across the transportation network are RSUs, or infrastructure nodes. They collect signed messages from surrounding vehicles, validate them against timestamps, and consolidate multiple signatures into a compact representation. Such batching has the advantage of minimizing the amount of verification bandwidth and computational workload [43, 44].
- Authority Server (AS): AS on the backend is a verifier and processor. It gets aggregated batches of messages from RSUs and verifies signatures for batches. The AS can request for identity resolution from the TA in case of a signature dispute or suspected forgery, a way to balance out privacy and accountability.

3.2. Security Assumptions

The security of the proposed CSAS-V scheme is based on standard cryptographic assumptions as follows:

3.3. Discrete Logarithm problem (DLP)

Let G be a group of prime order q, $P \in G$ a generator, and $A = xP$, it is computationally infeasible to find $x \in \mathbb{Z}_q^*$. The security of Schnorr signatures and our aggregate scheme rests on the hardness of this problem [45-47].

3.4. Random Oracle Model

We model the hash function H: $\{0,1\}^* \rightarrow Zq$ as a random oracle. Because of this, we can treat the hash more or less as a truly random function with security guarantees through standard proof techniques (the most prominent one being the forking lemma) [48, 49].

3.5. Adversary Models

This security model is studied concerning two classes of adversaries in the certificateless cryptographic setting. Each of those adversaries captures a different threat model, depending on capability and access to cryptographic material. The signature scheme must be capable of resisting both types of adversaries under an adaptive chosen-message attack.

- Type I Adversary (AIA_IAI): A Type I adversary simulates an external attacker who never gets access to the KGC's (Key Generation Center's) master secret key. However, here the adversary is allowed to substitute the public key of any honest user with a value of its choosing. AIA_IAI aims to create a valid signature with a modified public key to impersonate a genuine vehicle. As a result, Type I attacks are resisted, and it is impossible to create valid signatures without knowledge of the private key, with malicious alteration of public keys.
- Type II Adversary ($AIIA_{II}AII$): A Type II adversary is an adversary who can take over a potentially malicious or compromised KGC who have the master secret key. Although $AIIA_{II}AII$, as an instance of the adversary, cannot replace a user's public key, it can create a valid partial private key for any identity. The challenge on the signature scheme is to ensure that despite possessing such a strong capability, the adversary cannot forge up a signature in case the user is equipped with a secret user value, known only to KGC. Type II attacks are definitively impossible because resistance to this type of attack avoids key escrow and prevents the authority from forging signatures.

Since it takes both adversary models into account, the CSAS-V scheme proposed herein provides a high level of security regarding unforgeability, even under these extreme conditions involving compromised infrastructure or the presence of malicious external actors.

4. Proposed CSAS-V Scheme

This section details the design of CSAS-V, a certificateless Schnorr aggregate signature for secure and efficient message authentication in VANETs. This eliminates the utilization of bilinear pairings, resulting in a significant performance improvement for time-sensitive and resource-constrained vehicular networks. Our proposal contains seven polynomial-time algorithms: Setup, UserKeyGen, PartialPrivateKeyGen, FullKeyGen, Sign, Verify, Aggregate, and Aggregate-Verify. A Tamper-Proof Device (TPD) is embedded into each vehicle, safeguarding cryptographic keys. The commonly used symbols and functions in the CSAS-V scheme are defined in Table 1.

Table 1.
Symbol definitions used in the proposed scheme.

Symbol	Description
G	A cyclic additive group of prime order q
P	A generator of group G
q	A large prime order of the group G
Zq	A finite field with integers modulo q
s	The KGC's master secret key
Ppub	Public system key: $P_{pub} = sP$
x_i	Secret value of vehicle V_i (user-generated)
Px_i	Public key: $P_{xi} = x_iP$
ID_i	Real identity of vehicle V_i
QID_i	Hashed identity point: $Q_{IDi} = H(ID_i)P$
D_i	Partial private key: $D_i = sQ_{IDi}$
PID_i	Pseudonym assigned to vehicle V_i
$H(\cdot)$	Cryptographic hash function modeled as a random oracle
Ri,zi	Schnorr signature components
σ_i	Signature tuple: $\sigma_i = (R_i,z_i)$
e_i	Hash challenge: $e_i = H(\cdot)$

4.1. Setup

The TA and KGC execute the Setup algorithm together to produce initial system parameters for the certificateless Schnorr aggregate signature scheme in the VANET environment.

- The KGC picks a cyclic additive group G of a large prime order q, and a generator point $P \in G$.
- It selects the system master secret key $s \in \mathbb{Z}_q^*$, and computes the system public key accordingly: $P_{pub} = sP$.
- A secure cryptographic hash function is chosen: H: $\{0,1\}^* \rightarrow Zq$. In the security analysis, this function is treated as a random oracle.
- The parameters of the system are defined as: $params = q,G,P,Ppub,H$. These parameters are assumed to be preloaded into each vehicle's Tamper-Proof Devices (TPDs). The master secret s key is only known by the KGC and is never revealed in the course of the operation of the protocol. Each definition of Roadside Unit (RSU) is assumed to receive *parameters* in a secure way and will play a role in verifying and aggregating messages as part of VANET operation.
- The TA also opens the secure registration channel with each vehicle to issue (and revoke) random pseudonyms and track real identities should malicious behaviors occur during the process or to resolve disputed claims.

In the setup procedure, we ensure that every entity that participates in the VANET can access the cryptographic settings to produce, validate, and aggregate a signature, with minimal dependence on certification organizations.

4.2. UserKeyGen Algorithm

The UserKeyGen algorithm is individually executed by each vehicle in the VANET to produce a device-specific user-controlled key pair. This performing operation is done locally at the vehicle's Tamper-Proof Device (TPD), where the KGC is not required, which means the KGC never knows the whole private key of the user.

- The vehicle randomly chooses a secret value $x_i \in \mathbb{Z}_q^*$ as its private secret component.
- Then it computes the corresponding public key component as: $P_{xi} = x_i P$.
- Consequently, this procedure results in the user's locally generated key pair: (x_i, P_{xi}), where x_i is private and kept at TPD, and P_{xi} can be published or sent to the Trusted Authority (TA) to get a pseudonym.
- This step guarantees that the private key is still partially controlled by the user and is not derivable by KGC, thus achieving the certificateless property and avoiding risks in key escrow.

The UserKeyGen phase decentralized key generation responsibilities and provides a strong guarantee that even a malicious KGC cannot reconstruct the full private key unless the user cooperates.

4.3. Partial Private Key Generation Algorithm

The Key Generation Center (KGC) executes the PartialPrivateKeyGen algorithm when it receives a request for identity from a vehicle. In this way, the KGC constructs one part of the private key, which, upon combining with the vehicle's own secret key part, forms the complete private key for use in the CSAS-V signature scheme.

- The vehicle registers with the KGC and submits its real identity ID_i in a secure and authenticated manner
- The KGC generates a hashed identity point: $Q_{IDi} = H(ID_i)P$, where $H : \{0,1\}^* \rightarrow Zq$ is the hash function established in setup. This step assigns the vehicle's identity to some group element in G, guaranteeing uniqueness and non-repudiation.
- The KGC then generates the partial private key as follows using its master secret key $s \in \mathbb{Z}_q^*$ as: $D_i = s \cdot Q_{ID_i}$.
- The value $D_i \in G$ is cryptographically sent back to the vehicle. The KGC cannot ascertain the vehicle's full private key since it has no knowledge of the vehicle's self-generated secret value x_i.
- The vehicle saves D_i in its Tamper-Proof Device (TPD) for signing operations.

This guarantees that signature generation can only be done by the real vehicle with access to both x_i and D_i thus the KGC cannot alone impersonate the user. In addition, it maintains the certificateless security model by eliminating the requirement of digital certificates and being resistant to key escrow.

4.4. FullKeyGen Algorithm

The FullKeyGen algorithm is run by the vehicle, which uses the information generated locally in the forth phase through the UserKeyGen and the partial private key received from KGC in the third phase through PartialPrivateKeyGen to construct its complete private and public key: FullKeyGen.

- The vehicle generates its private key component $x_i \in Zq^*$ and public key component $Px_i = x_i P$, which came from the KGC secured path, as the vehicle, combined it with the partial private key $D_i \in G$.
- The vehicle's entire private key is then generated as: $sk_i = (x_i, D_i)$, where x_i is a user-generated secret of the vehicle and D_i is the partial private key corresponding to the vehicle identity.
- The full vehicle public key is given by: $pk_i = (P_{xi}, Q_{IDi})$, where $Q_{IDi} = H(ID_i)P$ is the hashed identity point employed to compute the corresponding partial key.
- A public key pk_i can be utilized by RSUs or AS to validate signatures and authenticate messages, in a conditionally anonymous manner through pseudonymization.

In this way, both the user (through x_i) and the KGC (through D_i) play a role in generating the key pair. Nonetheless, no party alone can produce a valid signature, thus protecting against malicious impersonation and ensuring the security guarantees of the certificateless signature model.

4.5. Sign

A vehicle executes the Sign algorithm to compute a certificateless Schnorr signature on a message M_i using its full private key $sk_i = (x_i, D_i)$ and a temporary pseudonym PID_i. This makes the signature lightweight and unlinkable, which means it also meets VANET privacy and performance objectives.

- The vehicle chooses a nonce at random $r_i \in \mathbb{Z}_q^*$.
- It computes the ephemeral commitment value as: $R_i = r_i P$, where $R_i \in G$ is a temporary group element involved in the challenge-response form of the Schnorr signature.
- The vehicle computes the challenge hash from all data relevant for the context: $e_i = H(M_i || t_i || PID_i || P_{xi} || Q_{IDi} || R_i)$, here, t_i is the timestamp of the message, PID_i is the pseudonym used to sign, and H: $\{0,1\}^* \rightarrow Zq$ is the hash function defined in setup.
- Set $D_i = d_i P$, where the two partial private keys are represented as scalars as $d_i \in Zq$. The vehicle determines the response as follows: $z_i = (r_i + e_i(x_i + d_i))(mod q)$ • The last signature is the tuple: $\sigma_i = (R_i, z_i)$
- The vehicle then broadcasts the signed message packet: $[M_i, PID_i, P_{xi}, Q_{IDi}, \sigma_i, t_i]$ to the nearest RSU or recipient vehicles.

This Schnorr-like signing algorithm is very efficient and does not rely on pairings, as it only doubles lgk scalar multiplications. Moreover, message authenticity is somehow managed while at the same time, sender conditional anonymity is preserved due to the pseudonyms used.

4.6. Verify

Inspecting a Schnorr-based certificateless signature $\sigma_i = (R_i, z_i)$ attached to an incoming message, a Roadside Unit (RSU) or any receiving vehicle runs the *Verify* algorithm to confirm its validity. Thus, the verification process allows confirming the authenticity and integrity of the message without revealing the identity of the signer.

- On receiving the signed message tuple $(M_i, PID_i, P_{xi}, Q_{IDi}, \sigma_i, t_i)$, the verifier first determines if the timestamp t_i is within an acceptable time window. In other cases, the original message is discarded to avoid replay attacks.
- Incase t_i is valid, the verifier reconstructs the challenge hash: $e_i = H(M_i||t_i||PID_i||P_{xi}||Q_{IDi}||R_i)$.
- Using the signature component z_i, the verifier computes the expected commitment point: $R0 = i = z_iP - e_i(P_{xi} + Q_{IDi}P_{pub})$
- The verifier then verifies if: $R_i' =^? R_i$, if that equality holds, then the signature σ_i is valid, and the message is accepted. If not, it rejects the signature.

This verification algorithm simply requires a few scalar multiplications and dispenses with costly bilinear pairings. Hence, it is ideal for resource-limited settings like VANETs that require real-time message authentication.

4.7. Aggregate

Upon receiving multiple signed message tuples from a group of nearby vehicles, a Roadside Unit (RSU) executes the Aggregate algorithm. Once this is done, multiple independent Schnorr signatures can be aggregated into a single Schnorr signature, combining them all, which is easier for communication but also simpler for validation keeping security intact.

- Suppose the RSU has n signed messages from different vehicles: $\{(M_i, PID_i, P_{xi}, Q_{IDi}, \sigma_i, t_i) \mid 1 \leq i \leq n\}$ with each $\sigma_i = (R_i, z_i)$ being a Schnorr signature made by vehicle V_i.
- The RSU calculates the aggregate signature as follows: $\sigma_{agg} = (Ragg, zagg)$ where: $R_{agg} = \sum_{i=1}^{n} R_i$ and $z_{agg} = \sum_{i=1}^{n} z_i \mod q$.
- The RSU sends the next packet to the Authority Server (AS) or the next hop, $(M_1,...,M_n, PID_1,...,PID_n, P_{x1},...,P_{xn}, Q_{ID1},...,Q_{IDn}, \sigma_{agg}, t_1,...,t_n)$

Hence, the proposed aggregation mechanism enhances the overall bandwidth and computational requirements during the verification phase and is promising for high-density vehicular networks.

4.8. Aggregate-Verify

The Aggregate-Verify algorithm is performed by the Authority Server (AS) or an appointed verifier to verify that an aggregated Schnorr signature $\sigma_{agg} = (R_{agg}, z_{agg})$ belongs to a combination of messages. This step prevents compromises to each individual message and makes sure that the efficiency benefits from aggregation are not lost.

- When receiving the aggregate signature packet: $(M_1,...,M_n, PID_1,...,PID_n, P_{x1},...,P_{xn}, Q_{ID1},...,Q_{IDn}, \sigma_{agg}, t_1,...,t_n)$, the verifier computes the challenge hashes for each $i \in \{1,2,...,n\}$: $e_i = H(M_i||t_i||PID_i||P_{xi}||Q_{IDi}||R_i)$. Here, R_i is the original commitment value from the signature of each vehicle.
- The verifier then calculates the aggregate challenge sum: $V = i = 1 \sum_{e_i}^{n} (Pxi + QIDiPpub) \in G$, using the aggregate response $z_{agg} \in Zq$ and aggregate commitment $R_{agg} \in G$, the verifier computes: $R' = z_{agg}P - V$.
- If an aggregate signature is accepted, it does the following: $R' =^? R_{agg}$
- If this holds, all signatures are valid. If not, the aggregate signature will be rejected as at least one signature in the batch is deemed invalid.

This verification methodology exploits the linear properties of Schnorr signatures to obtain an overhead independent of the number of signatures in the verification process, ensuring excellent scalability in VANET scenarios. It is essentially enabled to substantially fewer number of group operations and supports speedy batch authentication with little cost of security.

5. Security Analysis

The security properties of the proposed CSAS-V scheme are analyzed in this section. We prove that CSAS-V achieves existential unforgeability under adaptive chosen-message attacks in the random oracle model and fulfills essential privacy and authentication properties in the VANET context. The proposed scheme is analyzed in the context of the widely acknowledged adversarial models for certificateless public key cryptography, namely Type I adversaries and Type II adversaries.

5.1. Security Models

Type I Adversary: Type I adversary A_I, whom does not have access to the KGC's master secret key, replaces public keys of any user. This simulates an external attacker trying to masquerade a legitimate car or generate a correct signature.

Type II Adversary: The Type II adversary A_{II} has access to the master key of the KGC and is capable of generating partial private keys. But it does not, it cannot take the place of user public keys. This simulates an immoral KGC or compromised KGC trying to produce signatures or deanonymize users.

5.1.1. Unforgeability Under Chosen Message Attack

Theorem 1: Assuming the DLP holds in the group G, the CSAS-V scheme is existentially unforgeable against Type I and Type II adversaries in the random oracle model.

Proof Sketch: We provide a reduction from a successful forger A to solving the DLP. Assume A is able to produce a valid signature $\sigma = (R,z)$ for a message M under public key (P_x,Q_{ID}). Using the algorithm A we build an algorithm B that solves for x in the problem $P_x = xP$, contradicting the statement that DLP is hard.

In the simulation, B acts as the hash oracle and processes signature queries for A, using the random oracle to program in challenge values. Upon successful forgery by A, B uses the forking lemma to obtain two valid signatures with the same message but different challenges and uses this to compute x. This means that it is computationally infeasible in DLP to forge a signature in CSAS-V.

5.1.2. Vulnerability to Public Key Replacement Attack

Although a Type I adversary replaces a user i's public key P_{xi}, the signature of user i in CSAS-V cannot be forged unless the adversary knows the private secret x_i and partial key scalar d_i. As both are necessary in helping to compute the valid response $z_i = r_i + e_i(x_i + d_i)$ and neither is available to the adversary alone, public key replacement results in an invalid forgery.

5.1.3. Resistance to Malicious KGC Attack

For a Type II adversary (malicious KGC), CSAS-V is still secure, because of the user-generated secret key component x_i is independent of KGC. Thus KGC is able to compute $D_i = sQ_{IDi}$ but not to produce valid signatures without knowledge of x_i, which is never revealed. Splitting the key material makes it impossible for the KGC to forge a signature.

5.1.4. Message Integrity & Authentication

Every signature consists of a hash of message content, timestamp, and pseudonym: $e_i = H(M_i||t_i||PID_i||P_{xi}||Q_{IDi}||R_i)$.

This associates the signature with the unique message and context, stopping tampering and replay attacks. Using fresh nonces and timestamps ensures that all signatures are unique and cannot be replayed.

5.1.5. Privacy and Anonymity

In each message, real identities are replaced by pseudonyms PID_i the pseudonyms are periodically changed, and they're unlinkable across sessions. This keeps anonymity since the challenge hash e_i has PID_i but not ID_i. In disputes, only the Trusted Authority (TA) can map a pseudonym to an identity, allowing conditional traceability.

5.1.6. Non-repudiation & Traceability

In the event of a dispute, the TA can refer to its pseudonym resolution mechanism to match PID_i with ID_i and check the signature with the corresponding public key. Consequently, CSAS-V provides non-repudiation while ensuring privacy under normal operation.

5.2. Security Comparison

As shown in Table 2, we also compare the proposed CSAS-V scheme with the certificateless aggregate signature scheme proposed by Li et al. [34]. Both schemes possess powerful security requirements against Type I and Type II adversaries, resistance against public key replacement and malicious KGC attacks, and employ pseudonym-based authentication to achieve conditional privacy. However, a significant difference lies in the underlying cryptographic model and asyncio performance. While Li et al. [34] have a scheme based on bilinear pairings and the Computational Diffie-Hellman (CDH) assumption, CSAS-V is based on Schnorr signatures and the Discrete Logarithm Problem (DLP), thus completely eliminating bilinear pairing.

Table 2.
Security comparison between CSAS-V and.

Security Property	Li et al. [34]	**CSAS-V (This Work)**
Unforgeability (ROM + CDH/DLP)	✓(CDH)	✓(DLP)
Resistance to Type I Adversary	✓	✓
Resistance to Type II Adversary	✓	✓
Public Key Replacement Attack	✓	✓
Malicious KGC Resistance	✓	✓
Bilinear Pairing-Free	×	✓
Efficient Signature Generation	Moderate	High (Faster)
Efficient Verification	Moderate	High (Faster)
Conditional Privacy (Pseudonym)	✓	✓
Replay Attack Resistance	✓	✓
Traceability via TA	✓	✓
Signature Aggregation	✓	✓
Aggregate Verification	✓	✓

This leads to a substantially lower computational cost for CSAS-V. Signed triples are generated in much less time, and also verified faster, since expensive operations are minimized in both signing and verification phases; thus, both phase run much faster - it is also best suited for high-density VANET environments. However, CSASV does not lose any of the functionality offered by the previous eco schemes, such as signatures in aggregate form, replay attack protection or being able to trace directly from a known source, being just a more scalable version than the previous pairing-based schemes. Such an enhancement ideally renders CSAS-V a formidable candidate for vehicular communications in real-time, where latency and resource constraints are of critical importance.

6. Performance Evaluation

In this section, we analyze the computational efficiency of the proposed CSAS-V scheme and compare it with the certificateless aggregate signature scheme of Li et al. [34] and other recent CLAS-based methods. We measure two important metrics, computational efficiency (signing and verification time) and aggregate signature scalability, as both of which play a significant role in ensuring the timely and secure obtainability of VANET.

6.1. Computational Efficiency

CSAS-V removes bilinear pairings and leverages pure scalar multiplications over elliptic curves to minimize cryptographic overhead. Signature generation for CSAS-V needs only two scalar multiplications and one hash computation, and three scalar multiplications and no pairing are required for signature verification. In contrast, Li et al. [34] need few bilinear pairings, but these bilinear pairings are practically at least an order of magnitude more expensive than scalar multiplications.

Standard benchmarks on elliptic curve operations with a 256-bit prime-order curve yield the estimated computational costs shown in Figure 1. These values are taken from previous implementations using a 3.4 GHz Intel Core i7 CPU with OpenSSL or RELIC cryptographic libraries.

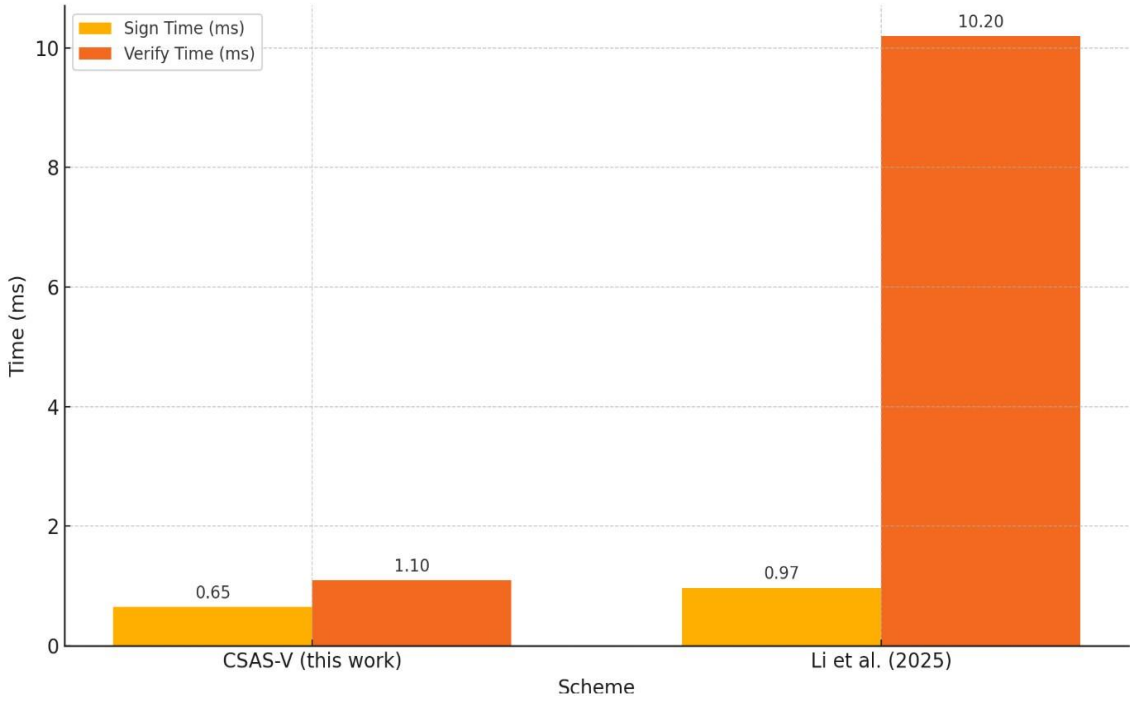

Figure 1.
Sign and Verify Time Comparison

The comparison of computational cost between CSAS-V (this work) and the scheme in Li et al. [34] observes that CSAS-V has remarkable benefits in vehicular networks. On average, CSAS-V shows a sign time about 0.65 ms and verify time of 1.10 ms, which is much better than the Li et al. [34] 's scheme has a sign time of 0.97 ms and a much higher verify time of 10.20 ms, while a major contributor to this performance gap is the absence of pairing operations in the CSAS-V, while that of Li et al. requires 2–3 (computationally intensive) pairings. CSAS-V also attains an "Excellent" score for scalability, making it viable for large-scale VANET deployments, whereas Li et al. 's plan in this regard is only "Moderate." Likewise, as a light-weight design, CSAS-V is also rated as a "High" efficiency, whereas Li et al. (ptfp) offers but modest efficiency. The enhancements provided by CSAS-V render it an excellent candidate for all scenarios in which time and scalability constraints play an important role, such as in real-time, resource-constrained vehicular communication systems.

6.2. Signature Aggregation and Verification

CSAS-V allows an RSU to aggregate multiple Schnorr signatures into a single concise form, facilitating batch aggregation. Aggregated signature verification with FOR is pairing-free, and in fact, very lightweight; it only takes n+1 scalar multiplications for n messages. This significantly reduces verification time in comparison to pairing-based schemes and makes CSAS-V a better candidate to fit dense vehicular networks, where hundreds of messages may be processed in P a second. Figure 2 shows the signature aggregation and verification.

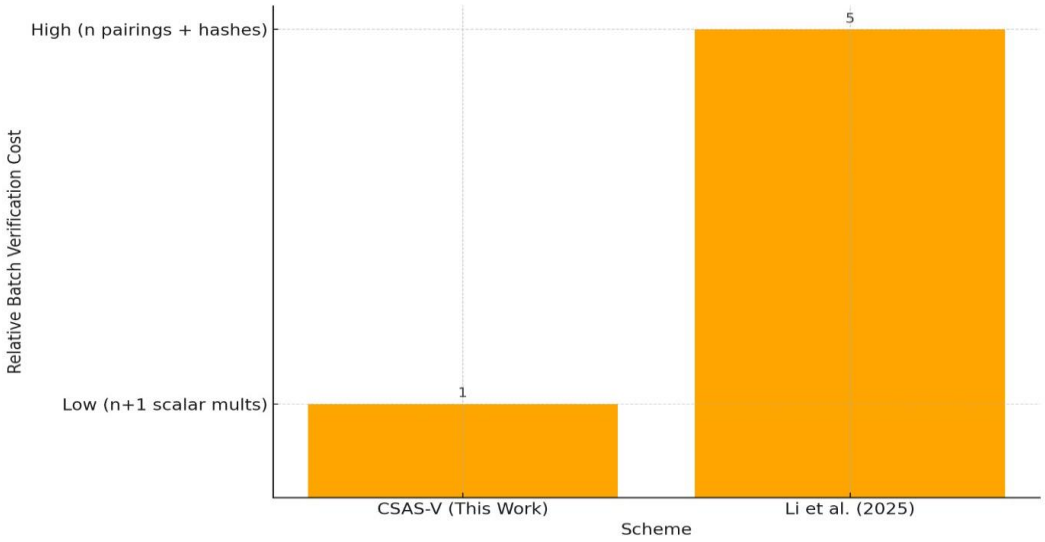

Figure 2.
Signature Aggregation and Verification

CSAS-V achieves an almost linear growth of verification time with a small overhead as shown via experiments with the simulated message sets (from 10 to 1000 vehicles), which significantly outperforms the pairing-based schemes with an exponential slowdown caused by the cost of bilinear map evaluations. Signature aggregation and batch verification between CSAS-V and Li et al. [34] were found to have additional performance benefits of the CSAS-V scheme, especially in resource-aware and high mobility situations such as virtual area networks (VANETs). They both also support signature aggregation, which allows multiple signatures to be aggregated and verified together. However, the batch verification cost in CSAS-V is much lower, needing n + 1 scalar multiplications, while Li et al. 's scheme requires n pairing operations and hashing, which are both more computationally expensive. In addition, CSAS-V does not rely on the expensive pairing operation at all, while Li et al. [34] overhead due to pairing operations per signature, making it linear among users and inversely proportional to efficiency. Although Li et al. [34] stay moderate in that department. CSAS-V has an aggregate efficiency rating of "Very High," which greatly contributes to its implementation for real-time, large-scale vehicular networks. These improvements allow CSAS-V to be used to accelerate applications that need message authentication that is fast, secure, and compact.

6.3. Communication Overhead

As the message exchange rate is high and available wireless bandwidth is limited with strict latency restrictions, efficient communication is an essential demand in VANETs. We analyze the communication overhead incurred by CSAS-V here in comparison to Li et al. [34] and other certificateless one-montage signature methods.

In CSAS-V, for each signature, we have two values: $R_i \in G$ and $z_i \in Zq$. With a 256-bit elliptic curve, each component takes up 32 bytes, so the signature size is 64 bytes per message. Each car's public key consists of the parameters $Px_i \in G$ and $Q_{IDi} \in G$, setting a total of 64 bytes. The length of the pseudonym PID_i is commonly between 16 and 32 bytes, as shown in Figure 3.

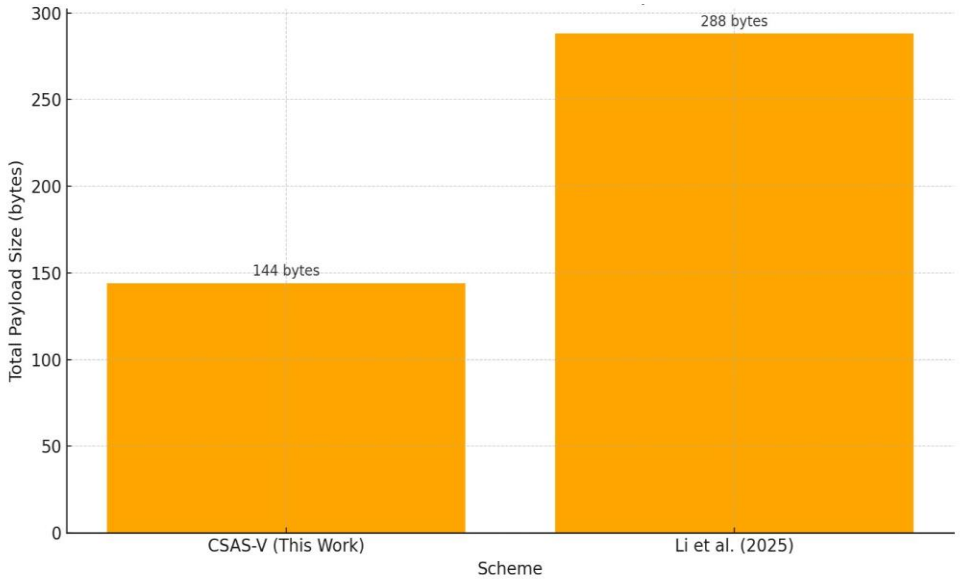

Figure 3.
Comparison of Communication Overhead.

In contrast, Li et al. [34] are based on bilinear pairing-based constructions that, in most cases, need several elements from pairing groups (e.g., G1, G2, and G*T*). Each signature of their scheme is made up of at least one pairing group element (which are usually 128 bytes or more in size) and two or more regular group elements, leading to a total signature size of about 128 to 160 bytes.

7. Conclusion and Future Work

Concretely, we have presented CSAS-V, a lightweight and efficient Certificateless Schnorr Aggregate Signature scheme adapted for the performance and security needs of Vehicle-to-One Access Networks (VANETs). CSAS-V introduces Schnorr signatures into a certificateless cryptographic structure, which eliminates the bilinear pairings and greatly reduces computation costs during both signature generation and batch verification. This scheme achieves strong security requirements such as public key replacement, protection against malicious KGC attacks, and adaptive chosen-message forgery security. It facilitates conditional privacy using pseudonyms and traceability under a trusted authority, achieving a balance between user anonymity and user accountability. The formal security analysis was provided in the random oracle model under the DLP (Discrete Logarithm Problem) assumption. We also provided performance comparisons with existing certificateless aggregate signature schemes, such as Li et al. [34], which show that the proposed CSAS-V scheme exhibits enhanced computational efficiency, a smaller signature size, and significant scalability in high-density vehicular scenarios. Designed not only to provide efficiency, security, and privacy-preserving properties, CSAS-V thus becomes applicable for real-time vehicle applications, including traffic safety messaging, cooperative awareness, and environmental notifications without a central authority in VANETs. Future work includes implementation in hardware on vehicular on-board units (OBUs), integration with fog computing architectures, and formal verification via symbolic tools.

References

[1] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1-39, 2024.

[2] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522-121531, 2021.

[3] A. Borah, A. Paranjothi, and J. P. Thomas, "A survey on distributed approaches for security enhancement in vehicular ad-hoc networks," *Computer Networks*, vol. 261, p. 111140, 2025. https://doi.org/10.1016/j.comnet.2025.111140

[4] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47-59, 2025.

[5] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indones. J. Electr. Eng. Comput. Sci*, vol. 29, pp. 518-526, 2023.

[6] 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.

[7] H. Batool, A. Anjum, A. Khan, S. Izzo, C. Mazzocca, and G. Jeon, "A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy," *Information Sciences*, vol. 652, p. 119717, 2024.

[8] H. Su, S. Dong, N. Wang, and T. Zhang, "An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs," *Vehicular Communications*, vol. 45, p. 100727, 2024.

[9] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 36-46, 2025.

[10] V. K. Yadav, Pushpa, K. Dabas, S. Khatri, and V. Sehrawat, "Circulation of legitimate information over VANETs using threshold signature scheme," *Cluster Computing*, vol. 27, no. 5, pp. 6205-6221, 2024.

[11] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of qos in manet based on ieee 802.11," presented at the In: 2020 IEEE International Conference for Innovation in Technology (INOCON), pp. 1–5 (2020). IEEE, 2020.

[12] S. Mazhar *et al.*, "State-of-the-art authentication and verification schemes in vanets: A survey," *Vehicular Communications*, p. 100804, 2024.

[13] M. Alhyan, M. Ouaissa, M. Ouaissa, Z. Nadifi, and A. Kartit, "A systematic review of cybersecurity in Internet of Vehicles," *Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications*, pp. 118-133, 2024.

[14] 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, p. e0287291, 2023.

[15] A. Luthra and N. Chugh, "A review of traffic management: real-time monitoring and dynamic control," presented at the In 2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC) (pp. 1-9). IEEE, 2024.

[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.

[17] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12-21, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.2

[18] T. Liu, Z. Li, Y. Ji, and J. Chang, "Efficient key-escrow-free and vehicle-revocable data sharing protocol for vehicular ad hoc network," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11540-11553, 2023.

[19] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: A review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science* vol. 30, no. 2, pp. 778-786, 2023.

[20] P. K. Pandey, V. Kansal, and A. Swaroop, "PKI-SMR: PKI based secure multipath routing for unmanned military vehicles (UMV) in VANETs," *Wireless Networks*, vol. 30, no. 2, pp. 595-615, 2024.

[21] S. Jiang, X. Chen, Y. Cao, T. Xu, J. He, and Y. Cui, "Apki: An anonymous authentication scheme based on pki for vanet," presented at the In: 2022 7th International Conference on Computer and Communication Systems (ICCCS), pp. 530–536 (2022). IEEE, 2022.

[22] D. Moussaoui, B. Kadri, M. Feham, and B. A. Bensaber, "A distributed blockchain based pki (bcpki) architecture to enhance privacy in vanet," presented at the In: 2020 2nd International Workshop on Human-centric Smart Environments for Health and Well-being (IHSH), pp. 75–79 (2021). IEEE, 2021.

[23] A. Angelogianni, I. Krontiris, and T. Giannetsos, "Comparative evaluation of pki and daa-based architectures for v2x communication security," presented at the In 2023 IEEE Vehicular Networking Conference (VNC) (pp. 199-206). IEEE, 2023.

[24] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and PKI system," *High-Confidence Computing*, vol. 3, no. 1, p. 100096, 2023.

[25] Y. C. E. Adja and A. Serhrouchni, "Improved crl distribution point for cooperative intelligent transportation systems," presented at the In: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 322–330 (2021). IEEE, 2021.

[26] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient pki based authentication protocol for vanets," presented at the In: 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1–3 (2018). IEEE, 2018.

[27] M. Khodaei and P. Papadimitratos, "Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in vanets," in *In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 172–183*, 2018.

[28] H. Wang, L. Wang, K. Zhang, J. Li, and Y. Luo, "A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs," *IEEE Access*, vol. 10, pp. 15605-15618, 2022.

[29] S. Dong, Y. Yao, Y. Zhou, and Y. Yang, "A lattice-based unordered certificateless aggregate signature scheme for cloud medical health monitoring system," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 284-296, 2024. https://doi.org/10.1007/s12083-023-01588-5

[30] K.-A. Shim, "Cryptanalysis of compact certificateless aggregate signature schemes for hwmsns and vanets," *IEEE Access*, 2024.

[31] R. Xu *et al.*, "An efficient and secure certificateless aggregate signature scheme," *Journal of Systems Architecture*, vol. 147, p. 103030, 2024.

[32] W. Wu and F. Ye, "Ipcas: An improved conditional privacy-preserving certificateless aggregate signature scheme without bilinear pairing for vanets," *Journal of Systems Architecture*, vol. 152, p. 103175, 2024.

[33] S.-w. Xu, S.-h. Yu, Y.-J. Bai, Z.-Y. Yue, and Y.-L. Liu, "LB-CLAS: Lattice-based conditional privacy-preserving certificateless aggregate signature scheme for VANET," *Vehicular Communications*, vol. 50, p. 100843, 2024.

[34] 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, p. e0317047, 2025. https://doi.org/10.1371/journal.pone.0317047

[35] P. K. Roy, P. Kumar, and A. Bhattacharya, "ZeroVCS: An efficient authentication protocol without trusted authority for zero-trust vehicular communication systems," *Future Generation Computer Systems*, vol. 163, p. 107520, 2025.

[36] Y. Yang, W. Tan, Z. Li, Y. Chen, and C. Li, "Mutual Authentication Protocols Based on PUF and Multi Trusted Authority for Internet of Vehicle," *IEEE Internet of Things Journal*, 2024.

[37] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, "FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network," *Internet of Things*, vol. 25, p. 101096, 2024.

[38] X. Cao, L. Dang, K. Fan, X. Zhao, Y. Fu, and Y. Luan, "A dynamic and efficient self-certified authenticated group key agreement protocol for VANET," *IEEE Internet of Things Journal*, 2024.

[39] Y. Wang, X. Jia, Y. Bao, Y. Cao, and J. Wen, "Efficient and provably secure offline/online heterogeneous signcryption scheme for VANETs," *IEEE Internet of Things Journal*, 2024.

[40] S. Abbas, H. Song, and R. Khan, "An ML-based authentication for privacy-preservation in a distributed edge-enabled internet of Vehicles," *IEEE Internet of Things Journal*, 2024. https://doi.org/10.1109/JIOT.2024.3483275

[41] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251-6261, 2024.

[42] P. K. N. Kouonchie, V. Oduol, and G. N. Nyakoe, "Roadside units for vehicle-toinfrastructure communication: An overview," in *In: Proceedings of the Sustainable Research and Innovation Conference, pp. 69–72*, 202.

[43] A. Guerna, S. Bitam, and C. T. Calafate, "Roadside unit deployment in internet of vehicles systems: A survey," *Sensors*, vol. 22, no. 9, p. 3190, 2022.

[44] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the In: 2018 International Arab Conference on Information Technology (ACIT), pp. 1–5 (2018). IEEE, 2022.

[45] J. Zhang, Y. Yang, Y. Chen, and F. Chen, "A secure cloud storage system based on discrete logarithm problem," presented at the In: 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), pp. 1–10 (2017). IEEE, 2017.

[46] A. Sarkar, D. Guha Roy, and P. Datta, "An overview of the discrete logarithm problem in cryptography," presented at the In: International Conference on Advanced Computing and Applications, pp. 129–143 (2024). Springer, 2024.

[47] S. Tinani and J. Rosenthal, "A deterministic algorithm for the discrete logarithm problem in a semigroup," *Journal of Mathematical Cryptology*, vol. 16, no. 1, pp. 141-155, 2022.

[48] J. Don, S. Fehr, C. Majenz, and C. Schaffner, "Online-extractability in the quantum random-oracle model," presented at the In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 677–706 (2022). Springer, 2022.

[49] Y. Kondi and A. Shelat, "Improved straight-line extraction in the random oracle model with applications to signature aggregation," presented at the In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 279–309 (2022). Springer, 2022.