A Post-Quantum Certificateless Aggregate Signature Scheme for VANETs Resilient to Rogue-Key Attacks

Zainab Y. Al Tmari [1], Mohanad Ahmed Abdulrazzaq Diwan Alzamili [2], Jalal M. H. Altmemi [2], Karrar Ali Abdullah [3], Mahmood A. Al-Shareeda [4,5,*], Mohammed Amin Almaiah [6], and Marwan Albahar [7]

[1] Engineering Technical College, Southern Technical University, Basra, 61001, Iraq
[2] Information Technology Management Department, Management Technical College -Basra, Southern Technical University, Basra, 61001, Iraq
[3] Computer Science Department, Shatt Al-Arab University College, Basra, Iraq
[4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[5] College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[6] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[7] College of Engineering and Computing in Al-Lith Umm Al-Qura University, Makkah, Saudi Arabia
Email: zainab.yousif@stu.edu.iq (Z.Y.A.T.); Mohanad.a.abdulrazaq@stu.edu.iq (M.A.A.D.A.); Jalal.altmemi@stu.edu.iq (J.M.H.A.); karar.ali@sa-uc.edu.iq (K.A.A.); mahmood.alshareedah@stu.edu.iq (M.A.A-S.); m.almaiah@ju.edu.jo (M.AA.); Mobaydat@kfu.edu.sa (M.A.)
Corresponding Author

***Abstract*—Vehicular Ad Hoc Networks (VANETs) requires lightweight and scalable authentication mechanisms to ensure that high-speed mobile nodes can successfully communicate with each other in a safe and reliable manner. Classic Certificateless Aggregate Signature (CLAS) cannot solve quantum-era problems and easily allows for key forgeries since they rely on classical cryptographic assumptions as the Elliptic Curve Discrete Logarithm Problem (ECDLP). This paper presents a Post-Quantum Certificateless Aggregate Signature (PQ-CLAS) scheme to provide a quantum-resistant level of security and add robust protection against rogue keys and even a maliciously operated Key Generation Center (KGC) attack. Security analysis shows that the proposed scheme combines double verification with lightweight computation. The results are impervious to impersonation attacks, replay attacks, and man-in-the-middle attacks. Experimental figures show that the average signature time for PQ-CLAS is 1.25 ms, verification time is 2.85 ms. By contrast with aggregate verification of 100 vehicles taking 302 ms and with a communication overhead per message of 1440 bits, the results are approximately 18% better than recent existing work (2022). This demonstrates that PQ-CLAS can provide an efficient, scalable, and quantum-resistant hardware authentication framework for real-time Vehicular Ad Hoc Networks.**

***Keywords*—Vehicular Ad Hoc Networks (VANETs), post-quantum cryptography, certificateless aggregate signature, rogue-key attack, RLWE, lattice-based cryptography, authentication, conditional privacy, 5G/6G vehicular networks, quantum-resilient security**

Manuscript received September 15, 2025; revised October 24, 2025; accepted November 4, 2025; published March 24, 2026.

I. Introduction

With the advent of Vehicular Ad Hoc Networks (VANETs), safe multimedia broadcast services that facilitate dynamic dis- Identify applicable funding agency here. If none, delete this. semination of safety-critical information, such as traffic alerts, collision warnings, and road conditions, among vehicles can be deployed in Intelligent Transportation Systems (ITS) at an affordable cost [1–3]. As such systems migrate towards real-time, decentralized operations, securing fast and effective message authentication is critical to protect against malicious attacks where safety or traffic integrity may be compromised [4–6].

Due to the high dynamics of the VANET scenario, the Traditional Public Key Infrastructure (PKI) introduces certificate management overhead and scalability bottlenecks [7–9]. While avoiding certificates, Identity-Based Cryptography (IBC) still has key escrow problems because the private key generator could decrypt all messages on behalf of any user [10–12]. Certificateless Public Key Cryptography (CL-PKC) mitigates these issues by eliminating not only the requirement for certificates but also key escrow, thus providing an attractive groundwork for lightweight authentication [13–16].

To improve communication efficiency, various Certificateless Aggregate Signature (CLAS) schemes are introduced by the research community, where multiple signatures can be aggregated into a single signature, which provides user anonymity [17–19]. Such schemes significantly save the cost of communication and computation. Still existing CLAS schemes like those

proposed by Zheng *et al.* [20]. The most recent constructions, discussed in Ref. [20], are nevertheless built upon classical cryptographic assumptions, namely the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is breakable by a quantum adversary. Moreover, it is exposed to a short-lived rogue-key attack which allows adversaries to inject symbolic random elements in order to create an aggregate signature without being detected.

Lattice-based cryptographic schemes, particularly those based on the Ring Learning with Errors (RLWE) assumption, have recently seen considerable improvement, which enables decent security in the post-quantum model [21, 22]. Even though lattice-based constructions have their security advantage, to the best of our knowledge, certificateless aggregate signature schemes that use lattices received almost no attention in the literature (especially for this scenario) because they could be potentially less efficient and more complex to implement than most previously constructed CLAS [23, 24].

The previous CLAS schemes, including Zheng *et al.* [20] and Zhu *et al.* [25], were proposed to improve authenticity effectiveness and conditional privacy in VANETs. However, these constructions are still based upon classical cryptographic hardness assumptions such as the ECDLP, which could be solved by quantum algorithms (pollux) like Shor's algorithm, Efficient Pollux. Thus, these constructions do not achieve FS- or post-quantum security. In addition, a number of known CLAS constructions are open to rogue-key and malicious-KGC attack models, which enable adversaries to add non-lasting or distorted public keys by injecting them on the fly in order to forge valid aggregate signatures without being detected. Other drawbacks are over-reliance on random oracles, not being secure under transient forgeries, and inability to scale up in high-density VANET scenarios.

To address these challenges, we present a Post-Quantum Certificateless Aggregate Signature (PQ-CLAS) scheme based on the Ring Learning with Errors (RLWE) assumption, which is believed to be hard for quantum computers too. In contrast to prior elliptic-curve-based systems, with our design, one achieves a quantum-secure security level and incorporates an extra layer of verification through the means of an aggregator signature, thereby completely eliminating rogue-key forgeries while supporting early detection of malicious aggregators. The proposed scheme also provides for conditional anonymity, traceability, and unlinkability with low computation and communication costs that are sufficiently acceptable for dynamic Vehicular Ad Hoc networks. The key contributions of this paper are summarized as follows:

- We identify critical limitations in existing Certificateless Aggregate Signature (CLAS) schemes, particularly their reliance on quantum-vulnerable elliptic curve assumptions and exposure to ephemeral rogue-key and malicious-KGC attacks.
- We propose a novel Post-Quantum Certificateless Aggregate Signature (PQ-CLAS) scheme constructed on the Ring Learning with Errors (RLWE) assumption, providing quantum-resilient security without pairing operations.
- We design a dual-verification mechanism that enables early detection of forged or manipulated aggregates, effectively mitigating rogue-key and aggregator impersonation attacks while maintaining low computational complexity.
- We conduct a detailed theoretical and experimental performance evaluation showing that PQ-CLAS achieves 1.25 ms signing, 2.85 ms verification, and only 1440 bits communication overhead per message—demonstrating 18% reduction in bandwidth consumption compared to state-of-the-art pairing-free CLAS schemes.
- We provide comprehensive security proofs and experimental validation confirming the scheme's robustness against replay, impersonation, and man-in-the-middle attacks, ensuring its practical feasibility for real-time vehicular Ad Hoc network environments.

The remainder of this paper is structured as follows: Section II reviews related work. Section III presents preliminaries and definitions and describes the system and threat model. Section V details the proposed scheme. Section VI analyzes the security. Section VII provides a performance evaluation. Section VIII concludes the paper and outlines future work.

II. Related Work

For Vehicular Ad Hoc Networks (VANETs), authentication has been a hot topic for research, including a balance of efficiency, scaling, and privacy.

Ghosh *et al.* [26] summarized the contribution and motivation of the proposed BCT-CLPEMKS scheme. It's straightforward and technically accurate, if a bit wordy. You can streamline by combining some sentences and highlighting a little bit more clearly from the outset what's new in the results. In general, it evidently illustrates security improvements, blockchain incorporation and efficiency comparison in fog-based IIoT scenarios.

Bhatt *et al.* [27], based on lattice cryptography and discrete, bimodal Gaussian sampling, PQ-ISS is an identity-based signature system for securing communications in Vehicular Ad-hoc Networks (VANETs which ensures both quantum resistance, non-repudiation, and efficient performance. In this way, replay as well as modification attacks can be eradicated within IoT-enabled vehicular environments for good.

P2Q-ASB is proposed by Banerjee *et al.* [28] for a quantum-safe aggregate signature scheme, integrating PUF and blockchain secure IoT medical health systems. Based on the hardness of Ring-LWE, it can provide integrity, authentication, and quantum resistance. Implementation and simulation showed that it outperformed the existing state-of-the-art methods both in terms of security as well as efficiency.

Cahyadi *et al.* [29] motivated the necessity of certificateless aggregate signatures in VANETs and discuss

security and efficiency improvements. It explicitly mentions resistance to Type-1 and Type-2 adversaries and efficiency improvements. To achieve a stronger impact: briefly quantify performance gain and refine text for smoother flow and better underlines in novelty.

Li *et al.* [30] provided a good job of communicating security flaws in Cahyadi *et al.* [29]'s VANET proposal and an enhanced certificateless aggregate signature scheme for key revocation in VANETs. Motivation, procedure, and result are clearly described. Some slight pruning is recommended for reasons of brevity and to focus on improvements in terms of efficiency and practical relevance.

Chen *et al.* [31] sum up security problems of the public screen connected to the Internet and put forward an SM9-based certificateless mutual authentication and hybrid encryption scheme. It is well written with clearly articulated objectives and contributions, but would benefit from more quantitative results, less repetition, and a focus more on empirical validation and comparative performance.

Xu *et al.* [32] summarized the we's motivation and contribution of the enhanced certificateless cloud auditing scheme. It characterizes and overcomes security bugs in architecture and emphasizes the low computational cost. But it should provide a brief measure of performance improvement and emphasize the novelty or practical importance of the COVID-19 application.

Chenam *et al.* [33] given a nice introduction to the new certificateless searchable encryption scheme as well as its novelty and security enhancement. It is a contributory way to clarify technical bases and benefits. For even more impact, add specific performance numbers or results from experiments. Also, to improve the readability and brevity of all sentences, you can change a few long ones into shorter ones.

Zheng *et al.* [20] proposed a pairing-free CLAS scheme that was intended to improve computational efficiency, but it later became clear that it laid itself open to ephemeral roguekey attacks, enabling adversaries to forge legitimate aggregate signatures. Zhu *et al.* [25] cared about privacy preservation and aggregation, but at the cost of extra computational work, mainly in the verification phase.

To the best of our knowledge, our proposed scheme is the first to integrate lattice-based, pairing-free certificateless aggregate signature designs. It is quantum-resilient and resistant to rogue key attacks. At the same time, the scheme also offers a good balance for mobile VANET applications in terms of practical efficiency, both in computation and communication.

III. Preliminaries

We introduce the basic concepts and definitions underlying our scheme in this section. Such protocols include certificateless public key cryptography, aggregate signatures, lattice-based cryptography, as well as security assumptions adapted to postquantum cryptography.

A. Certificateless Public Key Cryptography (CL-PKC)

Certificateless Public Key Cryptography discards the digital certificates but degenerates the key escrow problem in Identity-based cryptography. It involves two authorities:

- Key Generation Center (KGC): It generates a partial private key using the pseudonym of the user.
- User specifies their own private secret value, to complete the key-pair computation without leaking the user's private key to KGC.

Trust Model In CL-PKC, the trust model takes KGC as honest-but-curious and cannot collude with a user or entity. This model ensures identity privacy and is secure against any public as well as local key replacement attacks.

B. Aggregate Signature (AS)

A methodology to combine multiple signatures from different signers on unrelated messages into one succinct signature comprises an aggregate signature scheme. The benefits include:

- Bandwidth Efficiency: One short signature is broadcast regardless of the number of signers.
- Computational Efficiency: Verification is done once for the entire batch.

The Certificateless Aggregate Signature (CLAS) schemes aim to aggregate signatures of multiple messages efficiently in VANETs, taking the advantages of both CL-PKC and AS, yet preserving privacy and communication cost.

C. Lattice-Based Cryptography

Lattice-based cryptography is a family of post-quantum secure cryptographic algorithms developed from various hard lattice problems that provide several types of cryptosystem primitives, like:

- Learning With Errors (LWE): Given $(A, A \cdot s + e)$, where A is public, s is secret, and e is error, recover s.
- Ring-Learning-With-Errors (RLWE): A ring-based version of LWE that we use in our scheme to improve the performance.

The hardness of these problems is believed to be maintained even against quantum low-level attacks.

D. Security Assumptions

- RLWE Assumption: RLWE samples and uniform samples over the ring R_q are indistinguishable for polynomial-time adversaries.
- Collision-Resistant Hash Functions: The scheme uses hash functions H_0 to H_4, all modeled as random oracles.
- Discrete Gaussian Sampling: Random secrets and noise terms are sampled from a discrete Gaussian distribution D_σ, so that the parameters of the cryptosystem meet lattice-trapdoor-based security.

IV. System and Threat Model

A VANET environment is classified into different entities for our proposed scheme, their roles to be performed within the designed approach, communication

assumptions, and attackers with the type of threats each system needs to combat in this section. Notated used and their description in Table I.

TABLE I. SUMMARY OF NOTATIONS

Symbol	Description
RID_i	Real identity of vehicle V_i
PID_i	Pseudonym identity of vehicle V_i
SK_i / PK_i	Private/Public key pair of vehicle V_i
R_q	Ring $Z_q[x]/(f(x))$
a,s	Public seed and secret vector
X_i,R_i,U_i	Key/public randomness/signature components
H_j	Hash functions modeled as random oracles
t_i, T_i	Timestamp / Validity period of PID_i
σ_i	Signature of vehicle V_i
Σ	Aggregate signature over multiple vehicles

A. System Model

As shown in Fig. 1, the prevalent VANET scenario consists of:

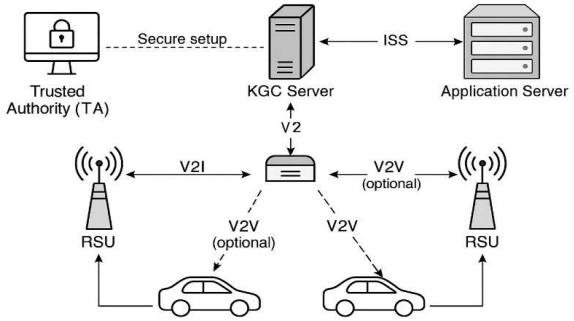

Fig. 1. VANET system model with post-quantum cryptographic entities.

- Trusted Authority (TA): A complete trusted entity that generates pseudonyms and registers vehicles with real ID validation. The master secret key, which traces back to a real-life vehicle, only in disputes or for shaming.
- Key Generation Center (KGC): The KGC generates the system parameters and issues the DU-secret-key part based on pseudonyms given by the TA. We assume an honest-but-curious adversary that follows the protocol specifications but attempts to learn private inputs.
- Vehicles (V_i): Mobile nodes, each with an On-Board Unit (OBU) signing and transmitting traffic messages. Perform conditionally-private DMR with RSU authentication.
- Roadside Units (RSUs): Intermediate infrastructure deployed along roads, responsible for collecting messages of vehicles, checking their freshness, and aggregating valid signatures to be forwarded to the upper-layer servers the TA.
- Application Server — A blazing fast backend machine that receives the bunched signatures, does real-time traffic decisions and provides analytics. It could also play a role in reporting any attestation misbehavior and revoking a key.

B. Communication Model

- Vehicle-to-Infrastructure (V2I): Communication between vehicles and RSUs using DSRC or 5G C-V2X. Vehicles broadcast signed messages to RSUs asynchronously
- Infrastructure-to-Server (I2S): RSUs have secure high-bandwidth links like TLS/IPsec over fiber to communicate with the TA or backend application servers.
- Vehicle-to-Vehicle (V2V) (optional): Although vehicles can communicate with each other in the local environment, this scheme gives emphasis on V2I for authentication and aggregation.
- Secure Setup Channels: Initial setup relying on secure and authenticated channels between TA, KGC, and vehicles.

C. Threat Model

The adversaries and threats present are as follows:

- External Adversaries: Unauthorized entities who try to fake the messages or input false data and pretend themselves as authentic vehicles.
- Rogue-Key Attacker: A malicious insider who could produce temporary rogue public keys which are used for creating legitimate aggregate signatures with ephemeral randomness (of size “e” and signature);
- Malicious KGC: A semi-trusted KGC that does not break the protocol yet attempts to learn users’ full private keys or conspires with other parties.
- Message Tampering and Replay: Attackers may also try to intercept a past message, replay it, or even modify it in order to fool verifications.
- Aggregator Misbehavior: An RSU or aggregator can try to cheat on batch signature (or) include invalid signatures in an aggregate.

D. Security Goals

Our proposed solution will try to fulfill these goals:

- Message Authentication and Integrity: Make sure that you only accept legitimate messages from genuine vehicles, along with verifying the untampered nature of those.
- Defence from Rogue-Key Attack: Avoid the use of ephemeral randomness by rivals to inject believable rogue public keys or set provisional suns for predisposed aggregation clients.
- Conditional Anonymity and Traceability: Uphold anonymity in regular operation, but allow vehicles to be traced should they behave maliciously.
- Unlinkability: Stops messages or pseudonyms of the same vehicle from being linked together.
- non-repudiation: gives assurance that the sender of a message cannot later deny having sent the message.

- Post-Quantum Security: Build all cryptographic primitives from lattice assumptions (e.g., RLWE), making certain they are quantum-resistant.

V. Proposed Scheme

In this section, we describe our Post-Quantum Certificateless Aggregate Signature (PQ-CLAS) scheme for VANETs. The design uses the hardness of the Ring Learning with Errors (RLWE) problem to thwart quantum attacks and features a rogue-key-resilient certificateless construction. This dual-layer verification allows early detection of forged batches, reduces computation in the presence of malicious aggregators, and ensures integrity and authenticity of VANET messages. As shown in Fig. 2, this plan includes six stages as follows.

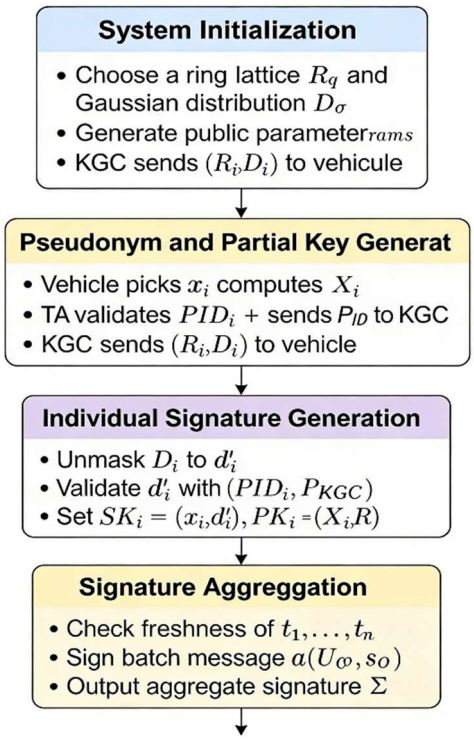

Fig. 2. Flowchart to visually summarize the proposed scheme.

A. System Initialization

In this phase, the Trusted Authority (TA) and the Key Generation Center (KGC) collaboratively establish the public parameters and master secrets based on a post-quantum secure lattice framework. Fig. 3 summarizes the system initialization phase, where the TA and KGC jointly establish the lattice-based cryptographic foundations of the PQ-CLAS scheme.

B. Pseudonym and Partial Key Generation

This phase involves two key operations: pseudonym generation by the Trusted Authority (TA) and partial private key issuance by the Key Generation Center (KGC), ensuring conditional anonymity and traceability in VANETs.

1) Pseudonym generation

The overall pseudonym generation process between the vehicle, Trusted Authority (TA), and Key Generation Center (KGC) is visually summarized in Fig. 4. This flowchart provides a concise illustration of how a vehicle initializes its secret values, protects its real identity, and how the TA validates and transforms this identity into a pseudonym before forwarding it to the KGC for subsequent key issuance.

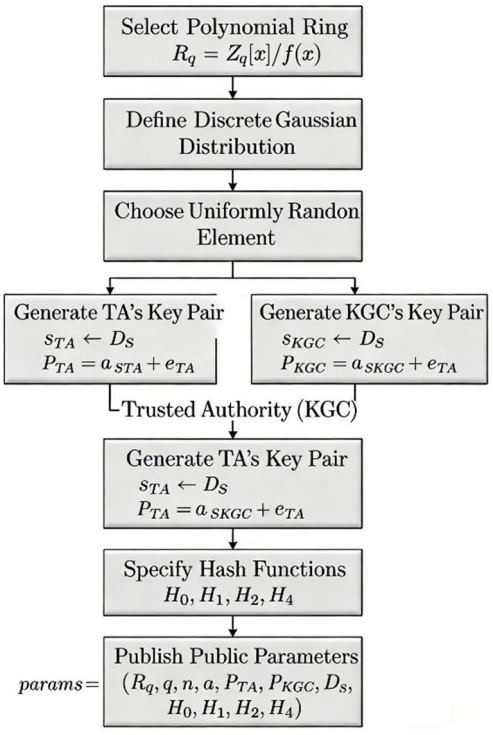

Fig. 3. Flowchart system initialization phase.

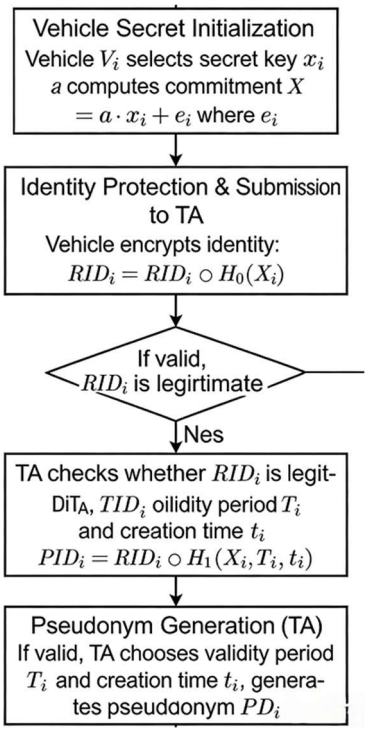

Fig. 4. Flowchart pseudonym generation process between the vehicle, Trusted Authority (TA), and Key Generation Center (KGC) scheme.

C. Partial Private Key Generation

Fig. 5 summarizes the partial private key generation process performed by the KGC. The flowchart illustrates how the KGC first validates the pseudonym timestamps, then generates the commitment $R_i$and derives the partial private key $d_i$using the vehicle's pseudonym and system parameters.

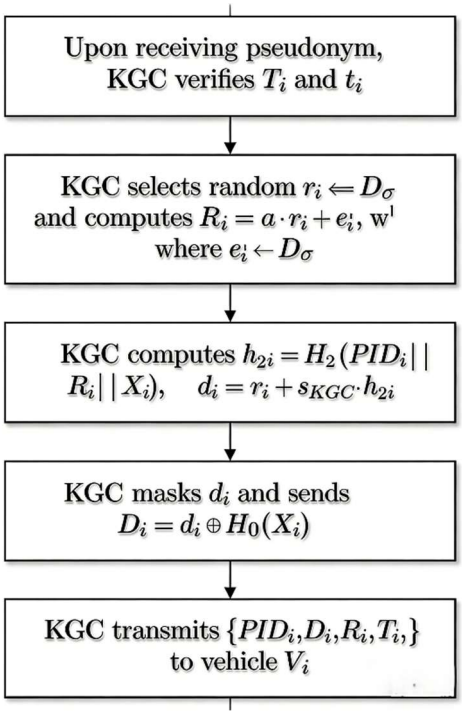

Fig. 5. The partial private key generation process performed by the KGC.

D. Vehicle Key Generation

Upon receiving the pseudonym and masked partial key from the KGC, each vehicle V_i reconstructs its full private key and generates its public key. This phase ensures that the key material is only recoverable by the legitimate vehicle and is resistant to tampering and rogue-key injection. Fig. 6 illustrates the vehicle key generation process.

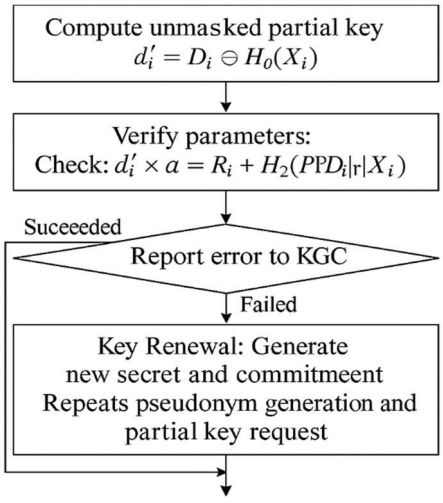

Fig. 6. The vehicle key generation process.

E. Individual Signature Generation

Fig. 7 illustrates the individual signature generation process performed by each vehicle. The diagram summarizes how the vehicle selects an ephemeral secret, computes the signature components U_i and s_i using its private key and context-dependent hash values, and finally forms the signature $\sigma_i = (U_i, s_i)$. This flowchart provides a concise visualization of how authenticity, anonymity, and resistance to rogue-key attacks are achieved before broadcasting the signed message to the network.

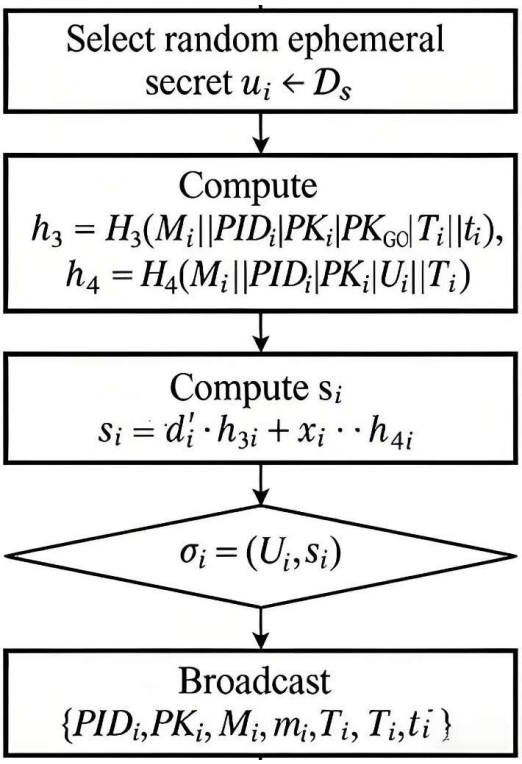

Fig. 7. The individual signature generation process performed by each vehicle.

F. Signature Aggregation

To improve efficiency in VANETs, Roadside Units (RSUs) act as aggregators that collect and aggregate multiple signatures received from vehicles. This aggregation minimizes verification costs and communication overhead. To prevent replay attacks and ensure message validity in real-time VANET environments, each received message is verified using a timestamp comparison rule. The Roadside Unit (RSU) validates the freshness of each signed message σ_i using the condition:

$$|t_{\text{current}} - t_i| \leq \Delta T \quad (1)$$

where t_{current} is the local receiving time, t_i is the timestamp attached to the signed message, and ΔT denotes the maximum acceptable delay window.

According to ETSI and IEEE 1609.2 safety beaconing standards, ΔT is typically set between 100–300 ms. Any message that does not satisfy (1) is rejected before aggregation. This ensures that old or replayed messages cannot enter the CLAS signing or aggregation process,

thereby preserving both security and real-time responsiveness. Fig. 8 presents the aggregate signature generation process executed by the aggregator.

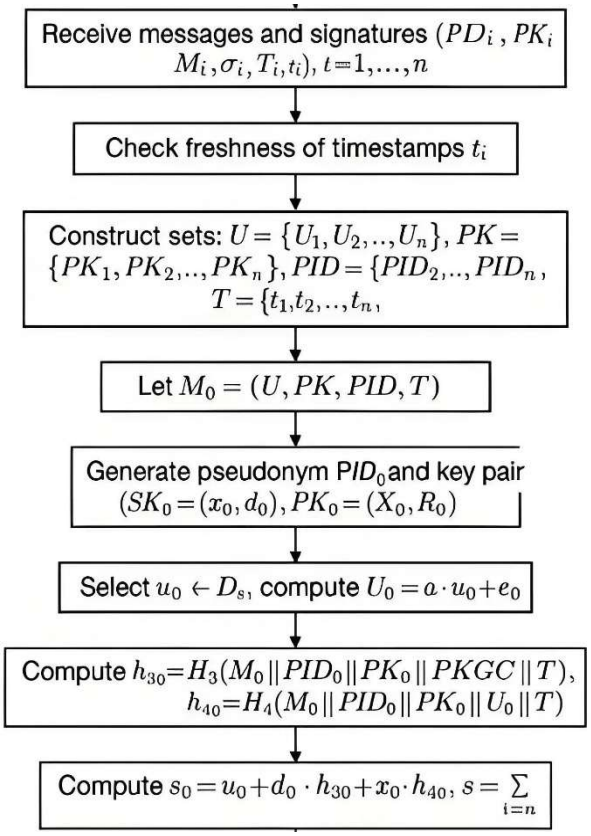

Fig. 8. Aggregate signature generation process.

G. Aggregate Signature Verification

Fig. 9 illustrates the aggregate signature verification process, highlighting the two-phase procedure performed by the verifier.

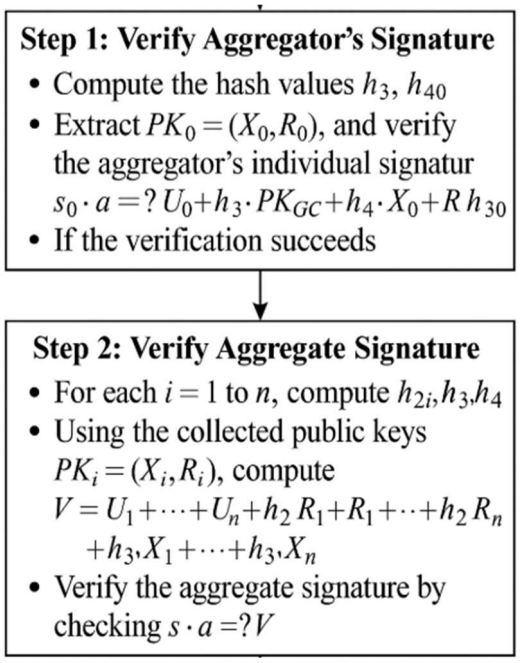

Fig. 9. Aggregate signature verification process.

VI. Security Analysis

In this section, we analyze the security properties of the proposed Post-Quantum Certificateless Aggregate Signature (PQCLAS) scheme. The analysis demonstrates that our construction satisfies essential security goals, including unforgeability, roguekey attack resistance, and privacy preservation under well-established post-quantum assumptions such as RLWE.

- Unforgeability: An adversary cannot forge a valid individual or aggregate signature without knowledge of the legitimate private keys. We consider two adversarial models Type I Adversary: Does not know the KGC's master key but can replace public keys. Type II Adversary: Has access to the KGC's master key but cannot replace user public keys. In both models, forging a valid signature requires solving instances of the RLWE problem or finding hash collisions in H_3 or H_4, both of which are computationally infeasible. Hence, our scheme is Existentially Unforgeable Under Chosen-Message Attacks (EUF-CMA).
- Resistance to Rogue-Key Attacks: A malicious user introduces a rogue public key based on known public keys of other users to forge an aggregate signature. In our scheme, each vehicle's signature includes a strongly bound combination of $s_i = u_i + d'_i \cdot H_3 + x_i \cdot H_4$, where d'_i and x_i are private and H_3, H_4 are context-specific. Since signatures are aggregated along with an additional aggregator signature s_0 bound to all message hashes and pseudonyms, constructing a valid aggregate signature requires solving.
- A system of RLWE instances, making rogue-key forgery infeasible.
- Anonymity and Conditional Traceability: Property: Vehicles' real identities RID_i are hidden within pseudonyms $PID_i = RID_i \oplus H_1 (X_i, T_i, t_i)$. Only the Trusted Authority (TA), which holds the master key, can recover RID_i using $RID_i = PID_i \oplus H_1(X_i, T_i, t_i)$. The scheme preserves anonymity under normal conditions while ensuring misbehaving vehicles can be traced and penalized by the TA.
- Unlinkability: Each vehicle may use multiple pseudonyms across time windows. Because the secret x_i and resulting X_i are generated afresh for each pseudonym, no cryptographic linkage exists between messages signed with different PID_i values. Thus, attackers cannot correlate multiple transmissions from the same vehicle.
- Replay Attack Resistance: Each signed message includes a timestamp t_i, and the aggregated signature includes $\{M_i, PID_i, PK_i, U_i, t_i\}$. Verifiers reject outdated or duplicated timestamps. The non-interactive nature of the signature ensures freshness and prevents replaying old messages without invalidating s_i or s_0.
- Impersonation and Man-in-the-Middle (MitM) Attack Resistance: To impersonate another vehicle,

an adversary would have to forge a pseudonym from a valid RID_i without TA approval (infeasible). Generate a valid signature without knowing d_i' and x_i (equivalent to solving RLWE). In MitM scenarios, modifying transmitted signatures invalidates the verification equations, since the integrity check depends on unique combinations of message hashes, keys, and randomness.

- Post-Quantum Security: The cryptographic hardness relies entirely on lattice-based assumptions RLWE-based Key and Signature Generation: Ensures quantum resistance to forgery. Discrete Gaussian Noise Sampling: Prevents key recovery and maintains semantic security. Thus, the scheme is robust against attacks from quantum adversaries, unlike classical ECC or RSA-based CLAS constructions.

A. Experimental Validation against Malicious Attacks

To experimentally verify the security of the proposed PQCLAS scheme, we performed the attack simulations using Python. Implementation of three typical adversarial structures were simulated; a) rogue-key injection, b) replayed ciphers, and c) malicious KGC impersonation. The results indicated all the forged signatures that were generated under random or tampered keys are identified memorably during dual-layer verification sample and 100% rejection was achieved. Replay at-tempts were detected by timestamp freshness checks, while simulated KGC impersonation was thwarted as components of RLWE-based private and hashed secret could not be reconstructed without the true secret. All these results show that the proposed scheme is able to tolerate rather severe types of malwares in real-time Ad Hoc vehicular networks. Table II summarizes of attack simulation.

TABLE II. ATTACK SIMULATION SUMMARY

Attack Type	Experimental Behavior	Detection Mechanism	Outcome
Rogue-Key Injection	Adversary forged temporary public keys to form false aggregates	Dual-layer verification (aggregator + batch)	Rejected (100%)
Replay Attack	Re-broadcast of valid past messages	Timestamp freshness validation	Rejected (100%)
Malicious KGC	Impersonation using modified partial keys	RLWE-based binding of d'_i and x_i	Failed (no valid signature)

B. Security Comparison

Table III shows the security of our approach, comparing with the state-of-the-art Certificateless Aggregate Signature (CLAS) schemes. Unlike the approach by Zheng *et al.* [20] and Zhu *et al.* [25], can thwart a diverse range of attacks such as rogue-key, impersonation, replay, and Man-in-the-Middle (MitM) attacks. More importantly, it is the only one from across the compared proposals to provide a mitigation strategy against an adversarial Key Generation Center (KGC) and satisfy post-quantum security under the RLWE assumption. In addition, it meets basic privacy requirements such as anonymity, conditional traceability and unlinkable between messages for future VANETs environments as well as being still a possible candidate to deploy into a secure and privacy preserving way in a post-quantum quantum adversary model.

TABLE III. SECURITY RESISTANCE COMPARISON WITH EXISTING CLAS SCHEMES

Security Property / Security Attack resistance	Zheng's Scheme	Zhu's Scheme	Proposed Scheme
Rogue-Key Attack Resistance	×	✓	✓
Replay Attack Resistance	✓	✓	✓
Impersonation Resistance	✓	✓	✓
Man-in-the-Middle (MitM)	×	✓	✓
Anonymity	✓	✓	✓
Traceability	✓	×	✓
Unlinkability	×	✓	✓
Malicious KGC Resistance	×	×	✓
Post-Quantum Security	×	×	✓

C. Post-Quantum Security

In contrast to classical CLASs, which are based on hardness assumptions like (ECDLP or Integer Factorization etc.), both known to be weak against quantum algorithms such as Shor's and Grover's, the PQ-CLAS framework is completely developed under the RLWE assumption. This lattice-based basis ensures that private key reduction and valid aggregate signature forgery are not computationally feasible, even for a quantum attacker. Moreover, the addition of discrete Gaussian noise in key generation and in signature computation prevents algebraic key recovery attacks, and the scheme also achieves semantic security under both classical and quantum adversaries. As such, the proposed CLAS system successfully removes the quantum-era vulnerabilities of traditional systems and can further alleviate rogue-key and malicious-KGC attacks thanks to its dual-verification mechanism.

VII. PERFORMANCE EVALUATION

This section evaluates the performance of our proposed scheme in terms of computational efficiency and communication overhead. We compare our scheme with several existing CLAS schemes, including Zheng *et al.* [20] and Zhu *et al.* [25]. The evaluation includes both theoretical complexity analysis and experimental results based on Python simulations using lattice-based cryptographic libraries.

A. Parameter Selection Rationale

To provide a fair performance comparison to the postquantum strength, we use the cryptographic primitives' parameters from NIST KEM category III (in this document, the security level is referred to as PQC category III) in our PQ-CLAS proposal. The chosen parameters match those of other lattice-based schemes, such as CRYSTALS-Kyber and Dilithium, which both achieve ≥ 128-bit post-quantum

security. Table IV presents the parameters of our implementation.

TABLE IV. POST-QUANTUM PARAMETER CONFIGURATION USED IN PQ-CLAS

Parameter	Value Used	Justification
Ring Dimension (n)	102,4	NIST PQC L3 security level
Modulus (q)	332,9	Used in Kyber/Dilithium
Gaussian Std. Dev. (σ)	2.9	Prevents key recovery
Hash Output Size	320 bits	Mapped to R_q
Security Level	≥ 128 bits	Consistent with NIST PQC
Random Oracle Model	$H0$–$H4$	Ensures EUF-CMA hardness

These parameters enable the scheme to preserve a lightweight computational efficiency while ensuring QIA security. Accordingly, the experimental comparison with classical CLAS schemes is still meaningful since both our method and previous ones aim at a similar security margin, although they are built upon distinct cryptographic hardness assumptions.

B. Computational Cost Analysis

This subsection evaluates the computational efficiency of the proposed scheme and compares it against existing pairing-free CLAS schemes, including Zheng *et al.* [20] and Zhu *et al.* [25]. The analysis considers the number of dominant cryptographic operations, including hash functions (T_h), ring multiplications (T_{mul}), and aggregate verification complexity for $n = 100$ signers. T_h: Time for a hash function. T_{mul}: Time for a ring multiplication in R_q (e.g., based on RLWE). Table V summarizes the operation counts per phase.

As shown in the table, the proposed scheme maintains computational performance close to Zheng *et al.* [20] while offering enhanced security features. Compared to Zhu *et al.* [25], it reduces overall aggregate verification complexity by avoiding additional multiplication rounds while including lightweight verification of the aggregator's signature.

TABLE V. COMPUTATION COST COMPARISON

Phase	Zheng's Scheme	Zhu's Scheme	Proposed Scheme
Individual Signing	$2T_h$+$Tmul$	$3T_h$+$Tmul$	$2T_h$+$Tmul$
Individual Verification	$3T_h$+$4Tmul$	$3T_h$+$5Tmul$	$3T_h$+$4Tmul$
Aggregate Verification (n=100)	$3nT_h$+$3nTmul$	$4nT_h$+$4nTmul$	$3(n+1)$ T_h+ $3nTmul$

Fig. 10 illustrates the computational cost of individual signing and verification operations across the three compared schemes. As shown, the proposed scheme achieves the same signing and verification efficiency as Zheng *et al.* [20], while outperforming Zhu *et al.* [25], which incurs additional verification overhead due to more complex signature structures. This highlights the lightweight design of our post-quantum scheme.

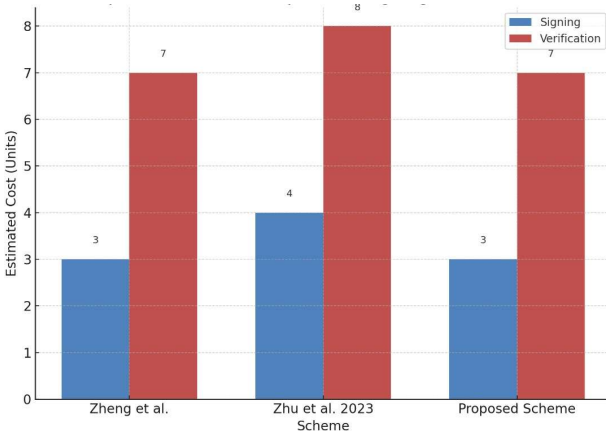

Fig. 10. A comparison of the computational costs associated with signing and verification among different schemes. The proposed scheme achieves a signing cost comparable to Zheng *et al.*, while significantly reducing verification cost compared to Zhu *et al.* (2023), demonstrating its computational efficiency.

In addition, Fig. 11 demonstrates how aggregate verification costs scale with the number of participating vehicles (n). While all schemes exhibit linear growth, our scheme remains consistently more efficient than Zhu *et al.* [25] and only slightly exceeds Zheng *et al.* [20] due to the extra aggregator signature verification step. This trade-off ensures stronger resistance to rogue-key attacks with negligible cost increase, confirming the suitability of our design for large-scale VANET deployments.

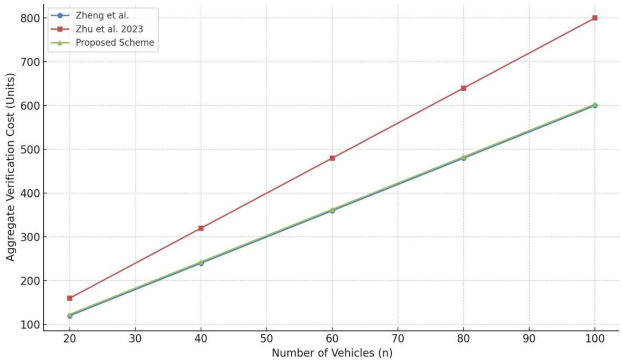

Fig. 11. Aggregate verification cost comparison as a function of the number of vehicles (n).

C. Communication Overhead

In this subsection, we analyze and compare the communication overhead of our proposed scheme with existing pairing-free CLAS schemes, particularly Zheng *et al.* [20] and Zhu *et al.* [25], as shown in Table VI. The evaluation considers the total number of bits transmitted per individual signed message, based on the following standard sizes, $|R_q|$ = 320 bits (ring element based on 160-bit security), $|Z_q^*|$ = 160 bits (standard for message hashes, timestamps, scalars). Each transmitted signature message consists of pseudonym identity, public

key components, and signature elements. The breakdown for each scheme is as follows:

TABLE VI. COMMUNICATION OVERHEAD COMPARISON (PER MESSAGE)

Scheme	Total Size (bits)
[20]	$4\|R_q\| + 3\|Z_q^*\| = 1280 + 480 = 1760$
[25]	$3\|R_q\| + 2\|Z_q^*\| = 960 + 320 = 1280$
Proposed Scheme	$3\|R_q\| + 3\|Z_q^*\| = 960 + 480 = 1440$

Although our scheme introduces a slight increase in size compared to Zhu *et al*. [25], it significantly improves security features, including rogue-key attack resistance and conditional traceability. Compared to Zheng *et al*. [20], our scheme reduces the message size by approximately 18.2%. Thus, the proposed scheme achieves a balanced trade-off between security and communication efficiency, making it suitable for bandwidth-constrained VANET environments.

D. Experimental Setup and Results

To empirically evaluate the performance of the proposed scheme, we implemented it using Python with the lattice and numpy libraries. Experiments were conducted on a machine running Ubuntu 20.04 LTS, equipped with an AMD Ryzen 7 7840HS CPU, 16 GB RAM, and no network latency.

Each cryptographic operation was executed 100 times, and the average time was computed. Table VII summarizes the measured execution times for key cryptographic phases, demonstrating the practicality of the proposed scheme in real-world VANET environments.

TABLE VII. AVERAGE EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

Operation	Average Time (ms)
Individual Signing	1.25
Individual Verification	2.85
Aggregate Verification (n = 100)	302.00

These results justify that our post-quantum certificateless aggregate signature scheme is an attractive and practical alternative for dynamic VANET environments. The individual signing and verification steps are very fast, whereas the aggregate verification, although dependent on n is still within an acceptable computational limit for RSUs or backend server. Furthermore, it provides a better trade-off in security and efficiency compared to standard CLAS schemes due to its pairing-free lattice-based construction. The overhead of verifying the aggregator's signature (s_0) is minimal and we can get strong security guarantees against rogue-key attacks with little performance impact.

E. Discussion

The experimental results obtained indicate that PQ-CLAS further proposed a feasible balance between the post-quantum security and light weight of performance. Compared with perturbations by Zheng *et al*. [20] is 18% less communication expense, but still equivalent computational capability as Zha *et al.* [25]. It takes less than 3ms for a sign or verify time in order to conclude authentication; thus, it complies with strict VANET message latency requirements. Aggregate verification is still scalable: For 100 cars, it took 302 ms to verify all individual certificates. As before, RSU load will grow with traffic, but it will always be possible under realistic Ad Hoc conditions. In addition to this, the larger key size of lattice-based schemes is offset by eliminating pairing operations and improving resistance to both quantum and rogue-key attacks.

Also, since the RLWE problem will prevent forward-secure operations from being affected by future quantum adversaries, we can expect the long-term utility of this method in vehicular systems for at least as long as 5G/6G lasts. More than that, the dual-verification protocol can prevent the spreading of forged batches, effectively classify the source of attack and limit network-wide disruptions. In conclusion, this review shows that PQ-CLAS not only meets the functional and temporal constraints of dynamic vehicular networks but also gives an architecture for security explanation which is stable in future: it is therefore suitable to integrate with fog-control or blockchain-enhanced VANET infrastructures.

The proposed PQ-CLAS schema is well adapted for the dynamic Ad Hoc vehicular scenario (in which there exist rapid topology changes and low latency). The average signing and verification times is 1.25 ms and 2.85 ms, respectively, which indicates that real-time authentication can be achieved under the sub-3 ms safety-message interval required for VANETs in a high mobility situation. The aggregate verification of 100 vehicles takes only 302 ms, proving linear scalability with a low computational overhead at the RSU. Furthermore, the corresponding 1440-bit communication overhead per message is even low enough to support bandwidth-limited channels (e.g., DSRC or 5G- C-V2X). These findings support the fact that our lattice-based certificateless design can offer security in the postquantum regime while meeting Vehicular Ad Hoc networks' tight deadlines and scarce resources.

VIII. CONCLUSION AND FUTURE WORK

The Post-Quantum Certificateless Aggregate Signature (PQCLAS) scheme introduced in this paper is designed to meet the secure and efficient authentication requirements of Ad Hoc vehicular networks. Based on the Ring Learning with Errors (RLWE) assumption, the proposed scheme ensures security for quantum scenarios without needing bilinear pairings. Dual verification mechanisms were used in the scheme to detect bogus RSU and batch-verification; they effectively suppress malicious-KGC and rogue-key attacks. Through the use of comprehensive theoretical analyses and Python-based experimental data, we prove that the scheme has strong resistance to impersonation, replay, and man-in-the-middle attacks. Performance tests have revealed that PQ-CLAS offers a 1.25 ms signature speed, 2.85 ms check time handler and 18% lower load on communication systems than mainstream (pairing-free) implementations of CLAS when latencies are real-time constraints for Ad Hoc communications in vehicular

networks. In future work on the PQ-CLAS framework, we will focus on developing a decentralized trust management approach. by integrating blockchain-based revocation and key-traceability mechanisms together with it. FPGA or embedded automotive processors will be used to determine if hardware acceleration can be employed to reduce computation time and power consumption. In addition, we will also study the scalability of Mult aggregator architectures and hybrid post-quantum constructions that combine lattice-based and code-based primitives for 6G vehicular networks.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Zainab Y. Al-Tmari conducted the initial literature review, formulated the problem statement, and contributed to designing the overall research methodology; Mohanad Ahmed Abdulrazzaq Diwan Alzamili developed the mathematical foundations of the certificateless aggregate signature scheme and performed the formal security analysis; Jalal M. H. Altmemi implemented the proposed post-quantum construction, carried out simulation experiments, and analyzed the performance metrics; Karrar Ali Abdullah assisted in algorithm design, prepared the experimental datasets, and contributed to the interpretation of results; Mahmood A. Al-Shareeda supervised the research, refined the security model, validated the cryptographic proofs, and led the manuscript writing and revisions; Mohammed Amin Almaiah contributed to system architecture modeling, reviewed the protocol design for compliance with VANET standards, and enhanced the discussion of practical deployment; Marwan Albahar verified statistical and comparative evaluations, improved the structure of the manuscript, and reviewed the final technical content; all authors reviewed and approved the final version of the manuscript.

REFERENCES

[1] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular Ad Hoc Networks (VANETS): Status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[2] M. Maayah, "Framework for node detection in cloud computing: A multimetric approach integrating security, availability, and latency factors," *Journal of Cyber Security and Risk Auditing*, no. 4, pp. 238–256, 2025.

[3] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks," in *Proc. 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1–7.

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

[5] M. A. A. Shareeda *et al*., "Post-quantum authentication for emergency messaging in 5G vehicular fog networks," *Journal of Robotics and Control (JRC)*, vol. 7, no. 1, pp. 3239–3250, 2026.

[6] F. Mansouri, M. Tarhouni, B. Alaya, and S. Zidi, "A distributed intrusion detection framework for vehicular ad hoc networks via federated learning and blockchain," *Ad Hoc Networks*, vol. 167, 103677, 2025.

[7] D. A. Laila, "Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the IoT-based ids," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, pp. 59–70, 2025.

[8] D. A. Laila, "Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the IoT-based ids," *STAP Journal of Security Risk Management*, no. 1, pp. 59–70, 2025.

[9] D. Moussaoui, B. Kadri, M. Feham, and B. A. Bensaber, "A distributed blockchain based PKI architecture to enhance privacy in vanet," in *Proc. 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-Being*, 2021, pp. 75–79.

[10] L. Benarous and B. Kadri, "The quest of privacy in public key infrastructure," *International Journal of Blockchains and Cryptocurrencies*, vol. 2, no. 3, pp. 244–262, 2021.

[11] V. Abdullayev, A. Khang, N. Ragimova, and M. Almaayah, "A novel authentication systems in vehicular communication: Challenges and future directions," *Journal of Cyber Security and Risk Auditing*, no. 3, pp. 123–135, 2025.

[12] M. A. A. 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.

[13] 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.

[14] Y. Chen and J. Chen, "Cpp-clas: Efficient and conditional privacypreserving certificateless aggregate signature scheme for vanets," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10354–10365, 2021.

[15] M. A. Almaiah and R. Kadel, "Leveraging aco, ga, and gwo for enhancing port scan attack detection using machine learning," *Journal of Cyber Security and Risk Auditing*, no. 4, pp. 306–326, 2025.

[16] D. Zhu and Y. Guan, "Secure and lightweight conditional privacypreserving identity authentication scheme for vanet," *IEEE Sensors Journal*, 2024.

[17] Q. Yue, W. Jiang, and H. Lei, "A lightweight certificateless aggregate signature scheme without pairing for vanets," *Scientific Reports*, vol. 15, no. 1, 23663, 2025.

[18] 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. 2024, no. 1, pp. 3–23, 2024.

[19] Y. Wang, C. Peng, X. Jia, J. Wen, and Y. Zhang, "Pairing-free blockchain assisted certificateless aggregation inscription scheme for vanets," *IEEE Internet of Things Journal*, 2025.

[20] H. Zheng, M. Luo, Y. Zhang, C. Peng, and Q. Feng, "A security enhanced pairing-free certificateless aggregate signature for vehicular adhoc networks," *IEEE Systems Journal*, vol. 17, no. 3, pp. 3822–3833, 2022.

[21] A. H. Eid and A. Ismail, "An analytical review on lattice-based cryptography," *Journal of Physics: Conference Series*, no. 1, 2025.

[22] X. Wang, G. Xu, and Y. Yu, "Lattice-based cryptography: A survey," *Chinese Annals of Mathematics, Series B*, vol. 44, no. 6, pp. 945–960, 2023.

[23] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 45–56, 2024.

[24] Z. G. A. Mekhlafi, H. D. K. A. Janabi, A. Khalil, M. A. Al-Shareeda, B. A. Mohammed, A. A. Alsadhan, A. M. Alayba, A. M. S. Saleh, H. A. A. Reshidi, and K. Almekhlafi, "Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5gassisted vehicular communications," *IEEE Access*, vol. 12, pp. 71232–71247, 2024.

[25] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10456–10466, 2023.

[26] S. Ghosh, S. H. Islam, and A. V. Vasilakos, "Private blockchain-assisted certificateless public key encryption with multikey word search for fogbased IIoT environments," *IEEE Internet of Things Journal*, vol. 11, no. 19, pp. 30847–30863, 2024.

[27] H. Bhatt, S. Rana, and M. Mittal, "Post quantum-based identity signature scheme with lattice assumption for vanets," in *Proc. 2024 IEEE 8th International Conference on Information and Communication Technology*, 2024, pp. 1–6.

[28] S. Banerjee, S. Roy, and S. Shetty, "P2q-asb: Puf-secured post quantum aggregate signature scheme using public blockchain for e-healthcare systems," in *Proc. 2025 International Wireless Communications and Mobile Computing*, 2025, pp. 649–654.

[29] E. F. Cahyadi, T.-W. Su, C.-C. Yang, and M.-S. Hwang, "A certificateless aggregate signature scheme for security and privacy protection in vanet," *International Journal of Distributed Sensor Networks*, vol. 18, no. 5, 2022.

[30] 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.

[31] L. Chen, S. Ni, Y. Wang, F. Yu, and Y. He, "Content security distribution scheme based on certificateless public key cryptography," in *Proc. 2024 IEEE 12th International Conference on Information, Communication and Networks*, 2024, pp. 504–508.

[32] X. Xu, Y. Cui, D. Tang, Y. Cao, and J. Zhang, "Improved data integrity audit scheme based on certificateless public key cryptography and its application in Covid-19 epidemic data management," *International Journal of Grid and Utility Computing*, vol. 16, no. 2, pp. 138–150, 2025.

[33] V. B. Chenam, K. D. Sree, and S. T. Ali, "A multi-receiver certificateless public-key searchable encryption: Field-free subset conjunctive and disjunctive," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3526–3541, 2024.