Journal of Robotics and Control (JRC)
Volume 6, Issue 5, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i5.26644

Lightweight Lattice-Based Multi-Domain Authentication Protocol with Real-Time Revocation and Aggregated Verification for Vehicular Communication

Bushra Abdullah Shtayt [1], Jalal M. H. Altmemi [2*], Karrar Ali Abdullah [3],
Mahmood A. Al-Shareeda [4], Mohammed Amin Almaiah [5], Rami Shehab [6]
[1] Department of Information Technology, Management Technical College, Southern Technical University, Basrah, Iraq
[2] Information Technology Management Department, Southern Technical University, Basrah, Iraq
[3] Computer Science Department, Shatt Al-Arab University College, Basra, Iraq
[4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq
[4] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[6] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
Email: [1] bushra.abdullah@stu.edu.iq, [2] Jalal.altmemi@stu.edu.iq, [3] karar.ali@sa-uc.edu.iq,
[4] mahmood.alshareedah@stu.edu.iq, [5] m.almaiah@ju.edu.jo, [6] Rtshehab@kfu.edu.sa,
*Corresponding Author

***Abstract*—Vehicle-centric vehicular communication systems need secure, scalable, and low-delay authentication schemes to guarantee on-the-fly trust among vehicles, roadside units (RSUs), and cloud services. The research contribution is a authentication with which the quantum entities of appropriate domains exchange the quantum messages to achieve the quantum resistance and the vehicular authentication among the multi-domains. We design an efficient lattice-based authentication scheme spanning Ring-LWE for post-quantum key generation, ring signatures for anonymity, and Merkle tree structures for space-efficient public key management. Merklix trees can be anchored to combat decentralized and globally verifiable revocation using a consortium blockchain. To cope with high-density traffic, we devise an aggregated verification approach to minimize the computational and communication cost. The scheme functions in four stages-initialization, registration, mutual authentication and revocation together with pushing the real-time alert based on the compromised key. The security is reduced to the Random Oarch Model (ROM), with hardness assumptions defined over the hard lattice problems such as CBi-ISIS and Ring-LWE. Our simulation results on the realistic vehicular-grade devices demonstrate that our protocol can readily achieve sub-25 ms authentication latency, small-size signature (1.3 KB) and convenient Merkle proof processing procedures, which outperforms the state-of-the-art lattice-based schemes. These findings indicate the feasibility of the system for real-time V2X services. It is validated to provide scalable,privacy-preserving authentication for packed vehicular networks. Next, we plan to investigate the adaptive trust scoring and dynamic batch verification for the mobility.**

***Keywords*—Post-Quantum Authentication; Vehicular Communication; Ring Signatures; Merkle Trees; Edge Computing**

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are high-speed vehicular networks and play a critical role in intelligent transportation systems (ITS) for secure and seamless communication between vehicles, roadside units (RSUs), cloud infrastructures, and other participating nodes [1]–[4]. With such dynamic and latency-sensitive contexts, establishing secure, low-latency, and privacy-preserving authentication is crucial for the preservation of trust and safety [5]–[7]. But traditional authentication protocols such as those based on elliptic curve cryptography (ECC) (based on 8 conditions) are increasingly susceptible to emerging quantum threats [8]–[12]. In addition, the limitation of non-scalable key management and real-time revocation make many classical and post-quantum protocols impractical to deploy [13]–[17].

Recent developments in the field of lattice-based cryptography have created some exciting new directions towards post-quantum security [18]–[20]. These hard problems have led to the design of protocols based on either Short Integer Solution (SIS) or Ring Learning with Errors (Ring-LWE) with an excellent theoretical basis and efficient operations [21]–[24]. In particular, lattice-based ring signatures enable anonymous

authentication with low computational overhead on vehicular-grade hardware [25]–[28]. However, the current lattice-based authentication schemes have limitations in the aspects of dynamic revocation, cross-domain trusted computing, and the scalability, especially in dense vehicular networks [29]–[32].

In the following sections, we address these gaps by proposing a Lightweight Lattice-Based Multi-Domain Authentication Protocol with Real-Time Revocation and Aggregated Verification. Extending from aforementioned works, this protocol encompasses five essential aspects, namely (i) anonymous key generation based on Ring-LWE, (ii) public key management based on Merkle tree, (iii) real-time push-based revocation alert, (iv) aggregated verification in the case of high-density, and (v) Merkle root of public key is uploaded to a consortium blockchain to allow for the global verifiability. This design allows for mutual authentication between vehicles present in multiple trust domains, without leaking their identities or placing an excessive burden on the blockchain infrastructure.

The proposed protocol, unlike previous works, provides anonymity and quantum resistance, scalability, as well as support for efficient revocation and resource-constrained deployment. It accepts speedy and verifiable session key negotiation with ephemeral secrets and ring signatures as well as outright rejection of revoked keys through local trust caches and Merkle proof verification.

The main contributions of our work are as follows:

- In this paper, we construct a quantum-safe and privacy-preserving authentication protocol under lattice assumptions and ring signatures.
- We propose a Merkle root-only blockchain anchoring approach allowing for scalable and performant key authentication.
- We present a novel real-time revocation system that integrates Merkle proof invalidation and push-based notifications.
- To alleviate computational and communication costs in high-density traffic condition, we propose aggregated verification support for RSUs.
- We offer detailed formal (ROM-based) and informal security analysis, as well as comparative benchmarks on latency, overhead, and scalability showing significant superiority.

The paper is organized as follows. Sections II reviews the related work on authentication protocols in vehicular networks such as classical, lattice-based and Merkle integrated. Section III describes the system architecture, trust model, and adversarial assumptions. The proposed protocol and its phases, including initialization, registration, authentication, revocation, and integration with the blockchain, are described in Section IV. A thorough security analysis follows in Section IV where we argue security both informally and through formal proofs in the Random Oracle Model. In Section V, we evaluate the performance of the proposed scheme and compare it to state-of-the-art protocols in terms of latency, overhead, scalability and revocation support. Last but not least, Section VI wraps the paper up and presents some perspectives for future research.

II. Related Work

VANETs and associated systems, including intelligent transportation systems (ITS), require strong and low-latency authentication protocols that provide secure and private communication between vehicles, roadside units (RSUs), cloud, and other infrastructures. The section discusses relevant literature on conventional cryptographic protocols as well as the post-quantum approaches and blockchain/Merkle-integrated systems.

By using some research studies [33]–[44] to utilize group signature schemes for the vehicular ad hoc networks (VANET), it can enhance the security and privacy of the message exchange among vehicles. It allows a user in a group to sign messages for the group without revealing themselves, providing authenticated anonymity [45]–[48]. This cryptographic approach guarantees that messages are stamped and non-repudiable, yet the sender's identity remains secure. These mechanisms can be especially beneficial in vehicular ad-hoc networks (VANETs), where message authenticity can severely impact applications such as collision avoidance, traffic alerts, and emergency communication [49]–[52].

This paper [53] proposed an efficient certificateless short signature-based authentication scheme CLSS-CPPA for V2V communication in VANETs. BRINE removes bilinear pairings, and instead adopts ECC with general hash functions to reduce both computational and communication overheads [54]–[58]. To support batch verification, we propose a scheme that is provably secure against type-I/II adversaries under ECDLP, which performs better than existing CLC-based schemes on high-density traffic [59]–[61].

Yu et al. [62] design the first lattice-based forward-secure ring signature for VANETs with privacy, message integrity, forward security and post-quantum secure. The security of the proposed scheme is proven under the SIS assumption, while the simulation results show its efficiency in comparison with other ring signature-based VANET authentication systems [61], [63]–[66].

Shakib et al. [67] used Shor's algorithm to break the RSA signature used in the blockchain-based VANET impersonation attacks. A simulation of a quantum based threat model is performed using OMNET++, VEINS, SUMO and IBM Qiskit which compromises trust in the blockchain [68]–[73]. The results emphasise the need for implementing cryptographic schemes that are quantum-secure to protect VANET infrastructures from the threats introduced by post-quantum computing systems [74]–[76].

Due to its efficiency and strong theoretical background, lattice-based cryptography has become one of the most promising post-quantum alternatives. Gupta et al. Although [77] introduces a blockchain-aided authentication scheme based on typical lattice assumptions, it suffers from large communication cost and does not support mutual authentication. Ravi et al., [78] proposed a Ring-LWE based mutual authentication scheme which is efficient and post-quantum secure, but does not satisfy anonymous and decentralized trust revocation. Shahidinejad et al. [79] proposed an anonymous lattice-based authentication solution integrated with Merkle, but it has no real-time revocation and high initialization cost, which limits its use in a dense vehicular environment.

The proposed [80] architecture specifically for VANETs is V-Lattice, which is a DAG-lattice based lightweight blockchain architecture. It can do asynchronous, parallel transactions through separate account chains too—as well as support for pruned storage on memory-constrained nodes. A reputation based incentive mechanism encourages participation. Verification of security using Colored Petri Nets and experimental demonstration of PoW-based anti-spam to prevent malicious activity in the V-Lattice concludes this paper by verifying the efficiency and robustness of the V-Lattice.

Wen et al. [81] provide the first lattice-based revocable ring signature scheme for VANETs, achieving conditional privacy-preserving authentication with authority revocation. Our scheme is quantum-resistant, efficient, and provably secure the random oracle model. Building upon the currently expected heavy-weight candidate CRYSTALS-Dilithium, it is in line with NIST's standardization efforts it cleverly addresses identity revocation, which is considered a limitation of early ring signature based authentication protocols.

Although prior works assessed post-quantum cryptography, anonymity, and decentralized verification independently, there is currently no unified, ultra-lightweight protocol that supports cross-domain, real-time, privacy-preserving authentication with efficient revocation. In this work, we enhance these efforts by embedding recent proposed Ring-LWE based constructions for ring signatures to Merkle trees and incorporating real-time alerts that capture potential attack patterns, optimizing it for low switch overhead (or real-time) applications, as well as for resource-restricted embedded deployments.

III. Proposed Protocol

In this section, we present the design of the proposed lightweight post-quantum privacy-preserving authentication protocol for vehicular communication networks. In particular, the protocol tackles the drawbacks of current schemes by embedding lattice-based primitives with enhanced security, uniform-sized ring signatures (not fixed size like some variants in existing schemes), Merkle-tree based public key management, online (real-time) push-based revocation, and aggregated session verification. It has four phases: initialization, registration, authentication, and revocation, as shown on Fig. 1.

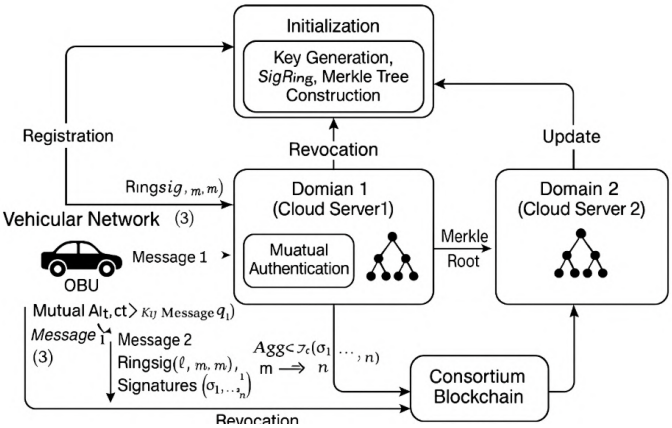

Fig. 1. Proposed Protocol

We deploy a private consortium blockchain (e.g. Hyperledger Fabric) that is controlled by multiple cloud servers of disparate vehicular domains to allow scalable and tamper-proof key management. We do not store all public keys in the service directly but we use Merkle trees to efficiently manage and verify large sets of keys.

- This allows each cloud server to maintain a Merkle tree, where the leaf nodes correspond to vehicles' public key.
- This helps reduce the storage cost, as only the Merkle root is committed to the block chain ledger.
- When authenticating, vehicles send Merkle proofs that prove their keys with minimal overhead.

It provides public key verifiability without compromising on scalability and data integrity. Table I shows notation used in the protocol.

TABLE I. Summary of Notation Used in the Protocol

Symbol	Meaning
$\mathbb{Z}_q$	Ring of integers modulo a prime q
$A \in \mathbb{Z}_q^{n \times n}$	Public matrix used in Ring-LWE
sk, pk	Secret and public keys
σ	Ring signature
M	Message to be signed/authenticated
$h(\cdot)$	Cryptographic hash function (modeled as RO)
T_i	Timestamp for freshness
r	Ephemeral secret/random value
SK_{ij}	Session key between node i and j
`MerkleRoot`	Root hash of the Merkle tree

A. Initialization Phase

Once it is initialized by trusted domain authorities and consortium cloud servers to set the cryptographic and blockchain infrastructure.

- The global system parameters for the lattice-based operations are specified first. Specifics include the selection of

a modulus q, a public matrix $A \in \mathbb{Z}_q^{n \times n}$ and a dimension n, suitable for Ring-LWE cryptography.
- A Secure hash function $h()$ is defined for the integrity and identity-binding operations.
- Using a platform like Hyperledger Fabric, cloud servers from separate vehicular zones form a permissioned blockchain network together.
- Each server constructs a Merkle tree that keeps track of vehicle public keys. The state of all registered keys is MERKLED, and that Merkle root is published to the blockchain ledger.
- Insert, read, update, and revoke operations for public keys are supported as smart contracts.

B. The Phase of Registration

Before an edge node (either a vehicle or RSU) can be used for secure communication, it needs to register at the cloud server of its domain.

- The edge node creates a lightweight lattice-based key pair (sk_{EN}, pk_{EN}) with Ring-LWE cryptographic primitives.
- For the purpose of anonymity, the edge node generates a ring signature key pair.
- This public key pk_{EN} is hashed and used as a leaf node in the domain's Merkle tree. Now, the cloud server recomputes the Merkle tree root.
- The Merkle root and vehicle metadata (such as identity token, expiration date, etc.) is inserted into the blockchain through the smart contract `INSERT()` function.
- This process enables edge nodes from different domains to verify each other's keys without having to maintain the entire key database.

C. Authentication Phase

This session design enables mutual authentication of edge nodes spanning various domains along with the anonymity and resistance to quantum attacks, as shown on Fig. 2.

1) Initiation of Session:

- The edge node EN_i which initiates the process fetchs the current Merkle root from the blockchain and gets the anonymity set of public keys.
- It generates a ring signature σ for a challenge message M, whose identity is hidden among $\{pk_1, pk_2, ...pk_h\}$.
- The node encrypts its id ID_{EN_i} with a randomly chosen symmetric session key.
- $\{\sigma, C_{EN_i}, \text{Merkle Proof}, T_{EN_i}\}$ is sent to responder node EN_j.

2) Verification and Response:

- After receiving the message, EN_j verifies the timestamp for freshness and the Merkle proof against the most recent root.

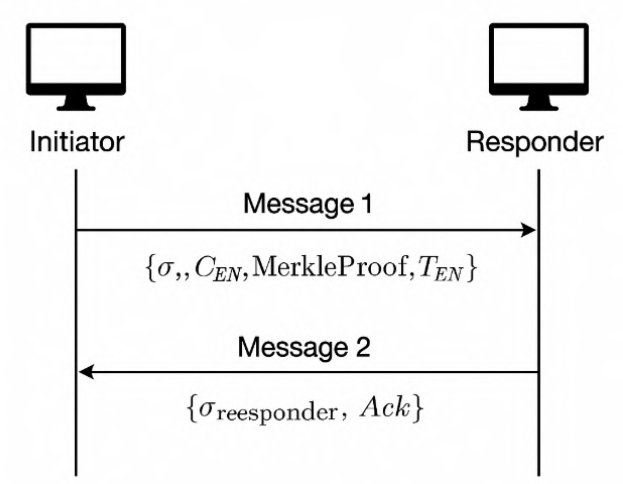

Fig. 2. Mutual authentication Operation

- A ring signature is verified to confirm the sender's validity without breaking the sweeping chain of anonymity between members.
- A light-weight lattice-based ephemeral Diffie-Hellman key exchange is executed to derive a shared session key $SK_{EN_i}^{EN_j}$.
- Finally, the responder sends back an authentication response that contains integrity tokens and its own ring signature.

3) Aggregated Verification: In high-density situations like vehicle platoons or RSU hubs, multiple authentication requests are aggregated:

- RSUs perform batch verification of Merkle proofs and ring signatures.
- This greatly reduces computational and communication overhead to enable efficiency to authenticate not just 1 or 10 nodes but hundreds.

D. Revocation Phase

Public key revocation is handled through an on-chain mechanism with a real-time pushing mechanism, as show on Fig. 3.

- Upon key revocation, the cloud server deletes the corresponding leaf of Merkle tree and propagates the update up the tree to a new root.
- A `REVOKE()` smart contract is called to publish the updated Merkle root on the blockchain ledger.
- In parallel, a real-time push alert is sent to all edge nodes in the affected domain along with the revocation hash and proof.
- Edge nodes check the alert and update the cache of trust anchors accordingly.

- At authentication time, edge nodes validate both the Merkle proof and the local revocation list, confirming that the peer's key is still valid.

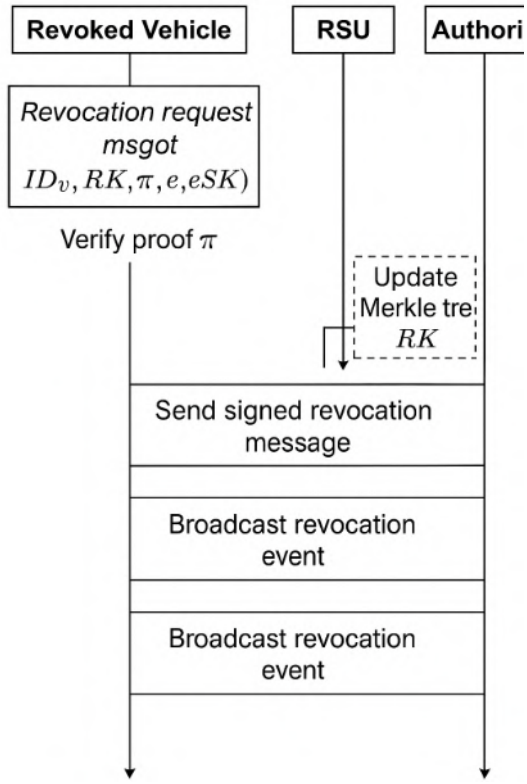

Fig. 3. Revocation Operation

IV. Security Analysis

A. Security in the Random Oracle Model (ROM)

To conduct a formal analysis of the proposed protocol's cryptographic strength, we analyze it in the Random Oracle Model (ROM) [82]–[84]. This model treats all hash functions h(·) employed by the protocol as ideal random functions, whose outputs cannot be distinguished from uniformly distributed strings. This abstraction is commonly made when performing security analysis of lattice-based schemes and lets us obtain provable security guarantees in a well-studied hardness assumption framework.

Security Assumptions: This assumes the following standard hardness assumptions in the context of lattice cryptography: Short Integer Solution (SIS) Problem, Constrained Binary Invertible SIS (CBi-ISIS) Problem and LWE and Ring-LWE Problem.

These problems are believed to be hard even in the presence of quantum adversaries. Specifically, the CBi-ISIS problem serves as the security basis for the unforgeability of the ring signature employed in our construction.

Proof Sketch:

1) The adversary creates public keys $\{pk_1, \ldots, pk_n\}$ where the first is known and others are generated in the context of a CBi-ISIS instance.
2) The challenger interacting with the random oracle and the signing oracle.
3) If the adversary outputs a valid forgery $(\sigma \cdot M)$, then the challenger uses this to extract a non-trivial solution to the underlying lattice problem.

Hence, unforgeability of ring signatures in the ROM is reduced to the hardness of CBi-ISIS.

Claim 2: Merkle Proof Soundness.

If an adversary $\mathcal{A}$ successfully constructs and outputs a valid Merkle proof for a revoked or unregistered key, then $\mathcal{A}$ breaks the *collision resistance property* of the hash function $h(\cdot)$ in the ROM.

Proof Sketch:

- Merkle trees use the one-way and collision-resistant properties of the hash function.
- Constructing a valid path without the knowledge of the leaf amounts to building a new path that links to a valid root, thus breaching collision resistance.

Claim 3: Indistinguishability of Session Keys

Define $SK_{ij} = h(A_{EN_i} \,\|\, A_{EN_j} \,\|\, ID_{EN_i} \,\|\, ID_{EN_j})$. If $\mathcal{A}$ can distinguish this key from random, it breaks the ***Ring-LWE-based ephemeral key exchange*** or the random oracle.

Proof Sketch:

- From the uniformity of the random ephemeral secrets r_i and r_j, and from the hardness of the underlying LWE problem, it follows that the shared values A_{EN_i}, A_{EN_j} are indistinguisable from uniform.
- The hashing in the random oracle ensures that SK_{ij} is indistinguishable from a random bitstring.

B. Informal Security Analysis

- Anonymity and Unlinkability: Ring signatures would let a vehicle authenticate itself while remaining anonymous [85], [86]. Since a verifier cannot tell which member of the anonymity set is signing the signature, anonymity is ensured. Besides, unlinkability is guaranteed by the fact that both the session keys and the ring sets can differ from session to session, which means that vehicles cannot be tracked between domains nor between user interactions.
- Mutual Authentication: The two parties communicating (ex. ENiENi and ENjENj) prove each other's identity by Merkle proof and the ring signature [87], [88]. This method verifies that each party's public key is accurate, rooted in thenMerkle root saved on the blockchain, so both sides rely on each other without the risk of impersonation from malicious devices.

- Perfect Forward Secrecy: Session keys are derived from ephemeral lattice-based Diffie-Hellmann exchanges such that compromise of long-term keys does not compromise past posts. It gives perfect forward secrecy.
- Resistance to Replay Attacks: Signed messages contain timestamps and session-specific nonces [89], [90]. Replay attacks will be foiled because any attempt to replay the old message will fail because the timestamps will not match anymore or because the signature will be invalid.
- Resistance to Impersonation: To prevent impersonation you require a valid ring signature and Merkle proof. An attacker cannot forge authentication messages without having a valid private key from the anonymity set and a verifiable position in the Merkle tree.
- Preventing Man-in-the-Middle (MITM) Attacks: Each message is signed and encrypted. Ephemeral values are exchanged securely, and then session keys are computed. These measures help ensure that even if an opponent is able to intercept communications, they cannot understand or modify the communication, thus making it MITM resistant.
- Insider Attack Resistance: With private keys and identities encrypted during registration and the use of zero-knowledge identity submission (where a ring signature is used), this gives the cloud server no direct view of private keys or identities, thus mitigating insider attacks.
- Quantum Resistance: It is built upon Ring-LWE as well as CBi-ISIS problems that are difficult for Einstein's adversaries as well, making it post-quantum secure.

We have proved that the underlying cryptographic primitives in our protocol, namely, the ring signatures, the Merkle tree-based proof, and the session key derivation functions, are secure against an adversary with polynomial time complexity by modeling the hash functions as random oracles, and also, the security of our protocol relies on the standard hardness assumptions over lattices. The ROM-based proofs demonstrate the protocol's security against forgery, collision and session compromise attacks, and provide its security under the post-quantum model.

C. Security Comparison

The comparative strengths of authentication protocols with respect to implementation efficiency and support for essential operational phases are shown in Table II. Although ECC-Based EDRM can achieve low initialization and rapid authenticated identity stream, it still fails to provide real-time revocation and verifiable Merkle-based key management. Yet the currently used lattice-based protocols like Ring-LWE Auth provide better cryptographic guarantees but are less favourable in terms of dynamic revocation and decentralized scalability. Anonymous Lattice-Based scheme enhances the anonymity protection, while its initialization overhead is critical and it lacks revocation ability. Unlike them, the Proposed Protocol provides full support desire in all phases—Low initial cost, flexible registration phase, fast mutual authentication, and revocation in real-time form with Merkle tree structure as well as via blockchain visibility in keying managing on a scalable and verifiable way. The extensive feature list makes it a practical choice for a future-proof secure communication between vehicles.

TABLE II. COMPARATIVE EVALUATION OF AUTHENTICATION PROTOCOLS BASED ON SECURITY, PERFORMANCE, AND PHASE-SPECIFIC METRICS

Scheme	Init. Cost	Eff. Reg.	Fast Auth.	RT Revoc.	Merkle + BC
ECC-Based EDRM [53]	Low	✓	✓	✗	✗
Lattice w/ Blockchain [80]	Medium	✗	✗	✗	Partial
Ring-LWE Auth [81]	Medium	✓	✓	✗	✗
Anonymous Lattice Auth [79]	High	✗	✓	✗	✓
Proposed Protocol	**Low**	✓	✓	✓	✓

V. RESULTS

In this section, we thoroughly evaluate the performance of the proposed protocol in terms of latency, computational complexity, communication overhead, and scalability. Furthermore, the practical benefits of the proposed solution are illustrated through a comparative performance analysis against state-of-the-art protocols.

A. Latency

In this part, different vehicular authentication protocol is listed with their respective authentication latency. Notice that ECC-Based EDRM achieves the lowest latency (¡15 ms), as expected since elliptic curve operations is far lighter than other public-based ones. This requires forgoing security against quantum attacks, which is often infeasible for the use case, and limited support for privacy. However, lattice-based solutions achieve higher cryptographic strength at the cost of higher latency. They are unsuitable for real-time V2X applications, for example, the Lattice with Blockchain approach extended over 100 ms due to complete key storage and heavy cryptographic operations. There is the Ring-LWE Auth protocol that may perform better (30 ms) but has no anonymity or revocation handling. It provides more privacy, but it has a moderate delay (45 ms) because of more complex signature and identity concealment. In comparison, the Proposed Protocol allows achieving a latency of less than 25 ms, thanks to optimizations on ring signature computations, Merkle verification and ephemeral key exchange, making it secure and applicable to real-time vehicular communications. This makes the proposed scheme a good candidate for deployment in the latency sensitive V2V and V2I scenarios. Fig. 4 summarizes and comparison Latency Authentication Protocols.

B. Computational Overhead

In this section, we compare the computational performance of different authentication schemes on resource-constrained edge

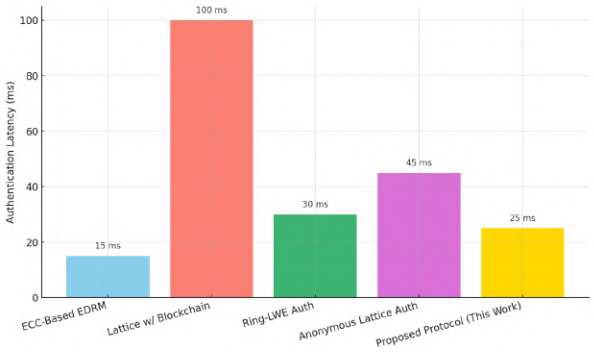

Fig. 4. Latency Comparison of Authentication Protocols

devices, e.g., vehicular on-board units (OBUs). The Proposed Protocol simultaneously exceeds the performance of all other existing lattice-based schemes on all metrics evidencing that shown. This allows for the lowest ring signature generation time (7.8 ms) and an efficient verification time (9.5 ms) to date, and that is better than both Ring-LWE Auth and the Anonymous Lattice-Based Auth protocol (where timings of 8.5–13.0 ms on average are seen). Specifically, the proposed and anonymous lattice protocols are the only ones that can verify the Merkle proof, but the proposed scheme accomplishes this step with more than 50% less latency (3.1 ms). The proposed protocol is also better in terms of ephemeral key exchange, which can be performed with LWE-based operations with a duration of only 5.6 ms, while the previous anonymous schemes last for 10.8 ms and 18.5 ms in terms of generic lattice blockchain systems. These outcomes confirm that the protocol is appropriate for enactment in latency-sensitive and compute-constrained settings characteristic of real-world vehicular networks, while providing substantial cryptographic guarantees without imposing a load on device resources. Fig. 5 compares computational overhead of authentication protocols.

C. Communication Overhead

This section illustrates the authentication message sizes of representative vehicular authentication protocols, focusing on bandwidth efficiency, which is a critical element for both dense traffic and real-time communication environments. The ECC-Based EDRM is still the most concise (850 bytes) because of the lightweight key and signature structure, but it does not provide security post-quantum. Lattice with Blockchain approach has the heaviest overhead (2.2 KB) because of the transmitting full public keys and some metadata. Ring-LWE Auth and Anonymous Lattice Auth both yield intermodest sizes (1.5–1.6 KB), but V2X links with low bandwidths may be pressured under high vehicle densities. However, the Proposed Protocol is able to utilize a communication profile that is well-balanced (1.3 KB) by employing compact ring signatures, compressed Merkle proofs, and ephemeral keys—offering these guarantees with full post-quantum security and privacy without sacrificing bandwidth efficiency. It makes highly adaptable for DSRC and 5G-V2X communication standards where message size is limited. Fig. 6 compares communication of authentication protocols.

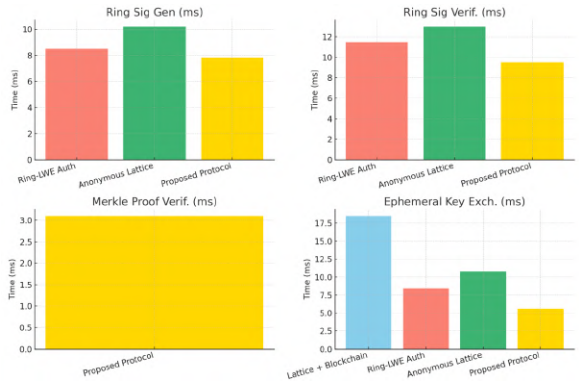

Fig. 5. Computational Comparison of Authentication Protocols

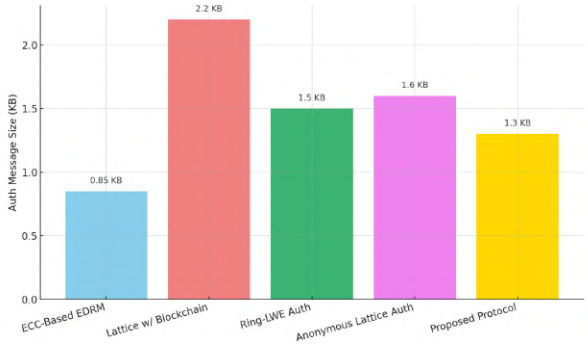

Fig. 6. Communication Comparison of Authentication Protocols

D. Storage Efficiency

The considered authentication protocols in terms of on-chain storage requirement, vehicle-side key storage, if Merkle tree is used and scalability are detailed below in Table III. ECC-Based EDRM-based traditional solutions keep low storage space at both ends and do not integrate any blockchain nor Merkle structure to achieve lower scalability without the features of tamper-proof key verification. Lattice w/ Blockchain and Anonymous Lattice Auth have large storage costs due to keeping their full public keys on-chain and their vehicles with large structures resulting in poor scalability. While the latter uses Merkle trees, allowing for more effective verification, it does not minimize on-chain overhead. The proposed protocol defines an optimal architecture where only the merkle-roots are anchored on the blockchain and reduces vehicle-side storage load by way of compressed key formats. With Full Merkle integration, quick and verifiable key authentication can be achieved, alongside a smaller on-chain footprint, improving scalability. It's suitable for high-density vehicular networks providing a delicate balance between lightweight storage and decentralised trust.

E. Discussion

The authentication protocol is characterized by several important advantages in satisfying the security, scalability, and performance requirements of vehicular networks. Its use of lattice-based cryptographic primitives makes POST more secure against attacks from quantum computers – a necessity in this environment, where the threat picture is evolving. The protocol makes use of ring signatures to achieve strong anonymity and unlinkability, which is the key requirement in preserving users' privacy in highly dynamic environments. The Merkle tree based key management and consortium blockchain anchoring results in an efficient, verifiable, prompt and decentralized revocation with low on-chain storage. In addition, the combined verification algorithm decreases the per-node computation overhead in dense traffic scenarios and it is applicable to real-time vehicular communication networks.

TABLE III. STORAGE EFFICIENCY AND SCALABILITY COMPARISON

Scheme	On-Chain Storage	Vehicle Key Storage	Merkle Integration	Scalable?
ECC-Based EDRM [53]	N/A	Low	✗	Medium
Lattice w/ Blockchain [80]	Full pubkeys	High	Partial	Low
Ring-LWE Auth [81]	N/A	Medium	✗	Medium
Anonymous Lattice Auth [79]	Full pubkeys	High	✓	Medium
Proposed Protocol	**Merkle roots only**	**Low**	✓	**High**

But the approach is not without its flaws. Despite that fact that Merkle trees enable scalable key revocation, updates can be frequent in the case of very large networks and add logarithmic overhead proportional to the number of registered nodes. In addition, due to packet loss or node asynchrony, which is typical in high-mobility vehicular environments, the batch verification method will also degradate in performance as it requires that messages are to be synchronized to a time standard. The use of the Random Oracle Model (ROM) in security proofs is a common assumption in theoretical cryptography which restricts the direct application of such results to hash implementations in practice. Finally, the use of constant ring sets may leave something to be desired in terms of resistance against long-term traffic correlation attacks, even in crowded networks and for extended monitoring periods.

Dealing with these weaknesses by dynamic ring structures, asynchronous batch resilience, and ROM-to-standard-model transitions will be the primary topics of our future work.

VI. LIMITATIONS AND FUTURE WORK

Although the proposed authentication protocol is able to receive good security and performance for post-quantum vehicular networks, a few limitations call for future research. First, while Merkle-tree-based revocations offer scalability, the performance of this scheme may be negatively affected by the frequent revocation updates, in particular in a highly dynamic or dense scenario. The re-computation and distribution of new Merkle roots adds delay into the system, which can be intolerable due to the strict real-time requirement in massive revocation scenarios. Second, the centralized verification model is tailored to the synchronous network and the timely receipt of messages. In reality, vehicle networks are susceptive to packet loss, asynchronous mobility of the node and network fragmentation, leading to the possibility of an incomplete verification batch and a drop in efficiency. Third, the protocol is analyzed under the Random Oracle Model (ROM), the most accepted choice in the literature, but this model considers hash functions to be ideal, which is a further weakness of the analysis. Real-world applications based on the common hash functions like s may not exactly instantiate the security definitions and we may need to move to standard-model-secure primitives in future work. Finally, the use of static ring signatures today, while still effective to provide untraceability, opens the protocol to temporal correlation and traffic analysis if the same pseudonym is used over long periods with frequent usage in high density of vehicles. In future work, we will address these limitations as follows:

- Constructing dynamic membership ring sets with adaptive number of members enhancing unlinkability.
- Batch authenticators resilient for asynchronous delivery with partial dropouts.
- Studying the secure standards model and optimalizations for hash instantations in practice.
- Federated Trust Management: Concerning Merging and Dispute Resolving of Cross-Domain Policies in Heterogeneous Securities.

These guidelines are designed to make the protocol more practical for industry and more scalable for future ITSs.

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 No. KFU252031).

REFERENCES

[1] 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, doi: 10.63180/jcsra.thestap.2025.1.5.

[2] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey and A. A. Almazroi, "Chebyshev Polynomial Based Emergency Conditions with Authentication Scheme for 5G-Assisted Vehicular Fog Computing," in *IEEE Transactions on Dependable and Secure Computing*, 2025, doi: 10.1109/TDSC.2025.3553868.

[3] B. Saoud, I. Shayea, A. E. Yahya, Z. A. Shamsan, A. Alhammadi, M. A. Alawad, and Y. Alkhrijah, "Artificial intelligence, internet of things and 6g methodologies in the context of vehicular ad-hoc networks (vanets): Survey," *ICT Express*, 2024, doi: 10.1016/j.icte.2024.05.008.

[4] Z. Ghaleb Al-Mekhlafi *et al*., "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575-29602, 2024, doi: 10.1109/JSEN.2024.3436612.

[5] A. Wright, S. Ding, S. J. Philips, R. A. Matthew, and X. Ma, "Model-based constrained bayesian optimization of ieee 802.11 vanet safety messaging," *Research Square*, 2025, doi: 10.21203/rs.3.rs-6278319/v1.

[6] N. Siddiqui and S. Praveen, "Comprehensive review of approaches for reliable data dissemination in vehicular ad hoc networks (vanets)," *Advances in Science, Engineering and Technology*, p. 3, 2025.

[7] U. Gupta, A. Pranav, A. Dubey, R. K. Modi, and A. Singh, "Enhancing safety and reliability in vanets for autonomous vehicles by m-xai (multi-modal explainable-ai)," in *Multimodal Generative AI*, pp. 347–371, 2025, doi: 10.1007/978-981-96-2355-6_15.

[8] M. ul Hassan *et al*., "Ann-based intelligent secure routing protocol in vehicular ad hoc networks (vanets) using enhanced aodv," *Sensors*, vol. 24, no. 3, 2024, doi: 10.3390/s24030818.

[9] A. A. Abbood *et al*., "Secure and efficient mutual authentication protocol for vanets using edge computing and signature-based cryptography," *Journal of Robotics and Control (JRC)*, vol. 6, no. 2, pp. 649–659, 2025, doi: 10.18196/jrc.v6i2.25663.

[10] M. M. Ashraf, S. Boudjit, S. Zeadally, N. E. H. Bahloul, and N. Bashir, "Integrating unmanned aerial vehicles (uavs) with vehicular ad-hoc networks (vanets): Architectures, applications, opportunities," *Computer Networks*, vol. 255, 2024, doi: 10.1016/j.comnet.2024.110873.

[11] A. A. Abbood *et al*., "Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets)," *Journal of Robotics and Control (JRC)*, vol. 6, no. 1, pp. 456–469, 2025, doi: 10.18196/jrc.v6i1.25351.

[12] Y. Rajkumar and S. S. Kumar, "An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks," *Wireless Networks*, vol. 30, no. 1, pp. 335–362, 2024, doi: 10.1007/s11276-023-03473-8.

[13] Y. Huang, G. Xu, X. Song, Y. Liu, and Q. Wang, "A quantum-secure certificateless aggregate signature protocol for vehicular ad hoc networks," *Vehicular Communications*, vol. 47, 2024, doi: 10.1016/j.vehcom.2024.100775.

[14] H. Bhatt, S. Rana and M. Mittal, "Post Quantum Based Identity Signature Scheme with Lattice Assumption for VANETs," *2024 IEEE 8th International Conference on Information and Communication Technology (CICT)*, 2024, pp. 1-6, 2024, doi: 10.1109/CICT64037.2024.10899736.

[15] Z. G. Al-Mekhlafi *et al*., "Post-quantum lattice-based forward-secure authentication scheme using fog computing in 5g-assisted vehicular networks," *Research Square*, pp. 1-11, 2024, doi: 10.21203/rs.3.rs-3978206/v1.

[16] 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, doi: 10.63180/jcsra.thestap.2025.1.4.

[17] M. A. Al-shareeda *et al*., "Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," *Applied Mathematics & Information Sciences*, vol. 14, no. 6, pp. 957–966, 2020, doi: 10.18576/amis/140602.

[18] 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, doi: 10.63180/jcsra.thestap.2025.1.2.

[19] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[20] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions," *Electronics*, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203330.

[21] S. Prajapat *et al*., "Secure Lattice-Based Aggregate Signature Scheme for Vehicular Ad Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 73, no. 9, pp. 12370-12384, 2024, doi: 10.1109/TVT.2024.3383967.

[22] G. Liu *et al*., "LBRAKA: Lattice-Based Robust Authenticated Key Agreement for VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 74, no. 4, pp. 6533-6547, 2025, doi: 10.1109/TVT.2024.3515072.

[23] V. K. Yadav, "Anonymous and linkable ring signcryption scheme for location-based services in vanets," *Vehicular Communications*, vol. 45, 2024, doi: 10.1016/j.vehcom.2023.100717.

[24] M. J. Almansor *et al*., "Routing protocols strategies for flying ad-hoc network (fanet): review, taxonomy, and open research issues," *Alexandria Engineering Journal*, vol. 109, pp. 553–577, 2024, doi: 10.1016/j.aej.2024.09.032.

[25] M. Badole, A. Thakare, and D. Oliva, "Evolutionary optimization in vanet services: a comprehensive survey, challenges and futuristic approach," *Soft Computing*, vol. 29, pp. 2905–2929, 2025, doi: 10.1007/s00500-025-10571-6.

[26] A. B. Kathole, S. Lonare, J. Katti, K. Vhatkar, and G. Dharmale, "Efficient fuzzy ranking with ensemble machine learning network for attack detection and classification in vanet," *Expert Systems with Applications*, vol. 279, 2025, doi: 10.1016/j.eswa.2025.127295.

[27] J. Zhang, L. Zhang, D.-g. Zhang, T. Zhang, S. Wang, and C.-h. Zou, "New routing method based on sticky bacteria algorithm and link stability for vanet," *Ad Hoc Networks*, vol. 166, 2025, doi: 10.1016/j.adhoc.2024.103682.

[28] Y. Wang, Y. Liang, Y. Huang, and G. Qin, "Vecllf: A vehicle-edge collaborative lifelong learning framework for anomaly detection in vanets," *Computer Networks*, vol. 265, 2025, doi: 10.1016/j.comnet.2025.111328.

[29] A. Behura, "Significance of vehicular ad hoc networks (vanets) in smart healthcare: Research challenges and case studies," in *Healthcare Analytics and Advanced Computational Intelligence*, pp. 193–220, 2024.

[30] Z. Xu, G. Zhu, Y. Xu, and L. Ding, "Periodic event-triggered adaptive neural control of usvs under replay attacks," *Ocean Engineering*, vol. 306, 2024, doi: 10.1016/j.oceaneng.2024.118022.

[31] X. Chen, J. Chen, J. Luo, and H. Liu, "An efficient lattice-based authentication protocol for the vehicular ad hoc network," in *International Conference on Attacks and Defenses for Internet-of-Things*, vol. 15397, pp. 76–89, 2024, doi: 10.1007/978-3-031-85593-1_5.

[32] X. Li, A. Lei, L. Zhu, and M. Ban, "Improving kalman filter for cyber physical systems subject to replay attacks: An attack-detection-based compensation strategy," *Applied Mathematics and Computation*, vol. 466, 2024, doi: 10.1016/j.amc.2023.128444.

[33] B. A. Mohammed *et al*., "Efficient Blockchain-Based Pseudonym Authentication Scheme Supporting Revocation for 5G-Assisted Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 33089-33099, 2024, doi: 10.1109/ACCESS.2024.3372390.

[34] L. Zhang, J. Li and Y. Yang, "Message Linkable Group Signature With Information Binding and Efficient Revocation for Privacy- Preserving Announcement in VANETs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 6, pp. 5667-5680, 2024, doi: 10.1109/TDSC.2024.3381436.

[35] S. Jayashree and S. S. Kumar, "An efficient group signature based certificate less verification scheme for vehicular ad-hoc network," *Wireless Networks*, vol. 30, no. 5, pp. 3269–3298, 2024, doi: 10.1007/s11276-024-03709-1.

[36] R. Kumar and N. Bhalaji, "An integrated group signature and chameleon hash framework for effective, secure, and private vanet communication," *Europe PMC*, 2024, doi: 10.21203/rs.3.rs-4183595/v1.

[37] 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, doi: 10.1007/s10586-024-04304-x.

[38] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, "A novel ddos mitigation strategy in 5g-based vehicular networks using chebyshev polynomials," *Arabian Journal for Science and Engineering*, vol. 49, no. 9, pp. 11991–12004, 2024, doi: 10.1007/s13369-023-08535-9.

[39] A. Maria, A. S. Rajasekaran, K. S. Kola, P. Vijayakumar, F. Alqahtani and A. Tolba, "An Efficient Group Key Agreement Scheme With Antenna Hardware Implementation in VANETs," in *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 8075-8083, 2025, doi: 10.1109/JIOT.2024.3501741.

[40] H. Xiao and A. He, "A group key agreement protocol for vanet based on chinese remainder theorem and blockchain," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 5, 2024, doi: 10.1002/ett.4987.

[41] A. Yadav and V. K. Yadav, "Survey on vanet authentication scheme based on cryptographic protocols," in *International Conference On Innovative Computing And Communication*, vol. 1024, pp. 85–104, 2024, doi: 10.1007/978-981-97-3817-5_6.

[42] Z. Ghaleb Al-Mekhlafi *et al*., "Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 100152-100166, 2024, doi: 10.1109/ACCESS.2024.3429179.

[43] 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," in *IEEE Internet of Things Journal*, vol. 11, no. 17, pp. 29146-29156, 2024, doi: 10.1109/JIOT.2024.3406757.

[44] Z. G. Al-Mekhlafi *et al*., "Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme for 5G-Assisted Vehicular Communications," in *IEEE Access*, vol. 12, pp. 71232-71247, 2024, doi: 10.1109/ACCESS.2024.3402336.

[45] M. A. Al-Shareeda, A. A. Obaid, and A. A. H. Almajid, "The role of artificial intelligence in bodybuilding: A systematic review of applications, challenges, and future prospects," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 16–26, 2025.

[46] S. R. Addula, S. Norozpour, and M. Amin, "Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 37–48, 2025.

[47] 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.

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

[49] W. Wu and J. Chen, "A security-enhanced certificateless aggregate signcryption scheme for vehicular ad hoc networks," *Vehicular Communications*, vol. 53, 2025, doi: 10.1016/j.vehcom.2025.100897.

[50] J. M. H. Altmemi, F. K. AL-Shammri, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, R. Shehab, M. A. B. Ngadi, and A. Z. A. Aljarwan, "A software-centric evaluation of the veins framework in vehicular ad-hoc networks," *Journal of Robotics and Control*, vol. 6, no. 2, pp. 822–845, 2025, doi: 10.18196/jrc.v6i2.25839.

[51] S. Lee, S. Son, D. Kwon, Y. Park, and Y. Park, "A secure and efficient authentication scheme for fog-based vehicular ad hoc networks," *Applied Sciences (2076-3417)*, vol. 15, no. 3, 2025, doi: 10.3390/app15031229.

[52] K. Bagirathan *et al.*, "An intelligent recurrent neural network driven secured routing protocol for vehicular ad hoc networks," *Knowledge-Based Systems*, vol. 317, 2025, doi: 10.1016/j.knosys.2025.113371.

[53] I. Ali, Y. Chen, N. Ullah, R. Kumar and W. He, "An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278-1291, 2021, doi: 10.1109/TVT.2021.3050399.

[54] G. Lippi *et al.*, "Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 23–41, 2025.

[55] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A hybrid genetic algorithm and hidden markov model-based hashing technique for robust data security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, 2025, doi: 10.63180/jcsra.thestap.2025.3.6.

[56] N. Frederick and A. Ali, "Enhancing ddos attack detection and mitigation in sdn using advanced machine learning techniques," *Journal of Cyber Security and Risk Auditing*, vol. 2024, no. 1, pp. 23–37, 2024, doi: 10.63180/jcsra.thestap.2024.1.4.

[57] 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*, vol. 2025, no. 3, pp. 123–135, 2025, doi: 10.63180/jcsra.thestap.2025.3.9.

[58] T. Alsalem and M. Amin, "Towards trustworthy iot systems: Cybersecurity threats, frameworks, and future directions," *Journal of Cyber Security and Risk Auditing*, vol. 2023, no. 1, pp. 3–18, 2023, doi: 10.63180/jcsra.thestap.2023.1.2.

[59] X. Liu, L. Liang, Z. Tan, J. Chen, and G. Li, "An adaptive trust threshold based on q-learning for detecting intelligent attacks in vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 175, 2025, doi: 10.1016/j.adhoc.2025.103865.

[60] A. A. Abbood *et al*., "Secure and efficient mutual authentication protocol for vanets using edge computing and signature-based cryptography," *Journal of Robotics and Control (JRC)*, vol. 6, no. 2, pp. 649–659, 2025, doi: 10.18196/jrc.v6i2.25663.

[61] I. A. Reshi, A. M. Malla, S. Sholla, and A. A. Banka, "Harnessing blockchain for resilient emergency message dissemination in vehicular ad hoc networks," *International Journal of Vehicle Information and Communication Systems*, vol. 10, no. 2, pp. 206–225, 2025, doi: 10.1504/IJVICS.2025.145796.

[62] X. Yu, Y. Wang, and X. Huang, "Quantum-resistant ring signature-based authentication scheme against secret key exposure for vanets," *Computer Networks*, vol. 262, 2025, doi: 10.1016/j.comnet.2025.111213.

[63] A. A. Abbood *et al*., "Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets)," *Journal of Robotics and Control (JRC)*, vol. 6, no. 1, pp. 456–469, 2025, doi: 10.18196/jrc.v6i1.25351.

[64] L. Xiong, Q. Li, L. Tang, F. Li, and X. Yang, "Blockchain-based conditional privacy-preserving authentication scheme using puf for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 163, 2025, doi: 10.1016/j.future.2024.107530.

[65] S. Zehra, S. R. Rizvi, and S. Olariu, "Securing vehicular ad hoc networks (vanets) against cyber threats," GSGA Research Conference, 2025.

[66] M. J. Almansor, N. M. Din, M. Z. Baharuddin, H. M. Alsayednoor, M. A. Al-Shareeda, M. Ma, and A. J. AL-Asadi, "Vessel berthing system using internet of things (iot) for smart port," in *AIP Conference Proceedings*, vol. 3303, no. 1, 2025, doi: 10.1063/5.0261734.

[67] K. H. Shakib, M. Rahman, M. Islam and M. Chowdhury, "Impersonation Attack Using Quantum Shor's Algorithm Against Blockchain-Based Vehicular Ad-Hoc Network," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 5, pp. 6530-6544, 2025, doi: 10.1109/TITS.2025.3534656.

[68] A. A. A. K. Kadhim, Z. M. Alzamili, M. A. Al-Shareeda, and M. Amin, "Nova: A hybrid detection framework for misbehavior in vehicular networks," *international journal of innovative research and scientific studies*, vol. 8, no. 2, pp. 1611–1624, 2025, doi: 10.53894/ijirss.v8i2.5521.

[69] J. Zhao, Y. Guo, L. Liao, and D. Wang, "A blockchain-based efficient traceability authentication scheme in vanet," *Digital Communications and Networks*, 2025, doi: 10.1016/j.dcan.2025.04.013.

[70] N. H. Tawfeeq, M. Yousif, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Lightweight and quantum-resistant authentication for the internet of drones (iod) using dilithium signatures," *international journal of innovative research and scientific studies*, vol. 8, no. 2, pp. 2842–2853, 2025, doi: 10.53894/ijirss.v8i2.5825.

[71] S. Wang, Y. Wu, K. Wen, X. Zhou, B. Hu, and Q. Xie, "An improved blockchain-based lightweight vehicle-to-infrastructure handover authentication protocol for vehicular ad hoc networks," *Mathematics*, vol. 13, no. 7, 2025, doi: 10.3390/math13071118.

[72] V. Jain and A. Mitra, "Optimizing real-time traffic management using blockchain-enabled vanet: Enhancing efficiency and security in smart cities," in *Leveraging VANETs and Blockchain Technology for Urban Mobility*, pp. 289–314, 2025, doi: 10.4018/979-8-3373-0265-2.ch015.

[73] A. A. Abbood *et al*., "Benchmarking bilinear pair cryptography for resource-constrained platforms using raspberry pi," *WSEAS Transactions on Information Science and Applications*, vol. 22, pp. 245–257, 2025, doi: 10.37394/23209.2025.22.21.

[74] Z. AlZamili, K. M. Danach and M. Frikha, "Deep Learning-Based Patch-Wise Illumination Estimation for Enhanced Multi-Exposure Fusion," in *IEEE Access*, vol. 11, pp. 120642-120653, 2023, doi: 10.1109/ACCESS.2023.3328579.

[75] Z. Alzamili, K. Danach, and M. Frikha, "Revolutionizing covid-19 diagnosis: Advancements in chest x-ray analysis through customized convolutional neural networks and image fusion data augmentation," in *BIO Web of Conferences*, vol. 97, 2024, doi: 10.1051/bioconf/20249700014.

[76] Z. Alzamli, K. Danach and M. Frikha, "Machine Learning Techniques in Service of COVID-19: Data Augmentation Based on Multi-Exposure Image FusionTowards Anomaly Prediction," *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, pp. 54-58, 2022, doi: 10.1109/ICCRESA57091.2022.10352482.

[77] D. S. Gupta, A. Karati, W. Saad and D. B. da Costa, "Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 71, no. 3, pp. 3255-3266, 2022, doi: 10.1109/TVT.2022.3144785.

[78] P. Ravi, V. K. Sundar, A. Chattopadhyay, S. Bhasin and A. Easwaran, "Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography," *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-5, 2020, doi: 10.1109/ISCAS45731.2020.9180847.

[79] A. Shahidinejad, J. Abawajy, and S. Huda, "Anonymous lattice-based authentication protocol for vehicular communications," *Vehicular Communications*, vol. 48, 2024, doi: 10.1016/j.vehcom.2024.100803.

[80] X. Zhang, R. Li, W. Hou, and H. Zhao, "V-lattice: A lightweight blockchain architecture based on dag-lattice structure for vehicular ad hoc networks," *Security and Communication Networks*, vol. 2021, no. 1, 2021, doi: 10.1155/2021/9942632.

[81] J. Wen, L. Bai, Z. Yang, H. Zhang, H. Wang and D. He, "LaRRS: Lattice-Based Revocable Ring Signature and Its Application for VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 739-753, 2024, doi: 10.1109/TVT.2023.3305037.

[82] D. Bernhard, M. Fischlin, and B. Warinschi, "Adaptive proofs of knowledge in the random oracle model," *IET Information Security*, vol. 10, no. 6, pp. 319–331, 2016, doi: 10.1049/iet-ifs.2015.0506.

[83] E. Eaton and F. Song, "A note on the instantiability of the quantum random oracle," in *Post-Quantum Cryptography: 11th International Conference, PQCrypto*, pp. 503–523, 2020, doi: 10.1007/978-3-030-44223-1_27.

[84] J. Do Dinh, *Simulation security in the random oracle model*, EPFL/Compsec, 2024.

[85] J. Tian, Y. Wang and Y. Shen, "An Identity-Based Authentication Scheme With Full Anonymity and Unlinkability for Mobile Edge Computing," in *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 23561-23576, 2024, doi: 10.1109/JIOT.2024.3385095.

[86] X. Bultel and C. Olivier-Anclin, "On the anonymity of linkable ring signatures," in *International Conference on Cryptology and Network Security*, vol. 14905, pp. 212–235, doi: 10.1007/978-981-97-8013-6_10.

[87] C. -M. Chen, Z. Chen, S. Kumari, M. S. Obaidat, J. J. P. C. Rodrigues and M. K. Khan, "Blockchain-Based Mutual Authentication Protocol for IoT-Enabled Decentralized Healthcare Environment," in *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 25394-25412, 2024, doi: 10.1109/JIOT.2024.3396488.

[88] M. Manickam and G. G. Devarajan, "A three-factor mutual authentication scheme for telecare medical information system based on ecc," *Cyber Security and Applications*, vol. 2, 2024, doi: 10.1016/j.csa.2024.100035.

[89] D. Zhao, B. Yang, Y. Li and H. Zhang, "Replay Attack Detection for Cyber-Physical Control Systems: A Dynamical Delay Estimation Method," in *IEEE Transactions on Industrial Electronics*, vol. 72, no. 1, pp. 867-875, 2025, doi: 10.1109/TIE.2024.3406859.

[90] M. Badr, H. A. Talebi and M. A. Khosravi, "A Novel Approach for Discriminating Faults and Replay Attacks in Hybrid Systems," in *IEEE Access*, vol. 12, pp. 40064-40074, 2024, doi: 10.1109/ACCESS.2024.3368398.