Journal of Robotics and Control (JRC)
Volume 6, Issue 4, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i4.26032

Design and Evaluation of Secure Software Architectures for 5G-Enabled Vehicular Driving System

Murtaja Ali Saare [1], Ali K. Mattar [2], Sari Ali Sari [3], Seng Yue Wong [4*]
[1] Department of Computer Science, College of Computer Science and Information, University of Basrah, Basrah, Iraq
[2] Computer Science Department, Shatt Al-Arab University College, Basra, Iraq
[3] Cyber Security Department, College of Computer Science and Information, University of Basrah, Basrah, Iraq
[4] Academy of Malay Studies, Universiti Malaya, Kuala Lumpur, Malaysia
Email: [1] murtaja.sari@uobasrah.edu.iq, [2] alikmattar@sa-uc.edu.iq,
[3] sari.ali@uobasrah.edu.iq, [4] wongsengyue@um.edu.my
*Corresponding Author

***Abstract*—Vehicular Ad-hoc Networks (VANETs) represent support for Intelligent Transport Systems (ITS) that allow vehicles and infrastructures to exchange real-time information. Nevertheless, the introduction of the 5G technology for the VANETs poses new security challenges, especially considering the emerging quantum computing threats. In response to this problem, we present a secure software architecture, Lattice Efficient Mutual Authentication (LEMA), designed to improve vehicular communication in 5G supported environments. The research novelty is the construction of LEMA—a lightweight and scalable framework for robust authentication in the fog, based on lattice-based post-quantum cryptography, which is also resilient to classical and quantum-based attacks and provides low latency. The framework operates based on three core phases: initialization by a Trusted Authority, secure private key generation, and mutual authentication via LWE-based schemes. A testbed which is built on a Raspberry Pi is used for simulating OBUs to verify LEMA performance in a resource-constrained environment. We compare LEMA with the state of art and get the performance numbers for the computational overhead, communication cost and storage efficiency. Simulation results show that with LEMA, the computational time, the communication amount and the storage consumed can be decreased by at least 25%, 30% and 20% than the benchmark protocols, respectively, and it is secure against the man-in-the-middle and the key-compromise attacks. The authors' use of fog servers for deployment of the system also significantly boosts real-time responsiveness. Finally, the LEMA model presents a promising quantum-secure authentication technique for 5G-based vehicular networks. In the future we plan to combine it with AI-based anomaly detection and blockchain, for better scalability, privacy and decentralization.**

***Keywords*—Post-Quantum Cryptography; Vehicular Ad-hoc Networks (VANETs); Fog Computing; Software Architectures; Mutual Authentication; 5G Network Security**.

I. INTRODUCTION

Intelligent Transport Systems (ITS) are making a significant impact as worries about traffic and driver safety are on the rise [1]–[3]. These systems use modern technology to make driving safer, more efficient, and more enjoyable. Vehicular Ad-hoc Networks (VANETs) form an essential component of ITS, enabling real-time communication to improve traffic road efficiency and safety. They allow vehicles to communicate with each other and with roadway infrastructure [4]–[6]. When a vehicle shares data in real-time, it is possible to develop applications for traffic management, road safety, and autonomous driving [7], [8]. The advent of VANETs has opened the door to a future of smarter transportation by radically altering the methods in which vehicles interact with one another and their environments [9], [10]. Thanks to this technology, Vehicles, and roadside infrastructure can communicate information, which depends on several communication models and network structures [11]–[13]. The many varieties of VANETs and the underlying communication techniques are discussed in this discourse.

Incorporating 5G technology into VANETs can greatly enhance transportation networks and encourage the creation of smart vehicles [14]–[16]. A new age of linked mobility, defined by ultra-reliable and low-latency communication, is on the horizon thanks to this convergence, which is also known as 5G-VANET [11], [17]–[19]. It will open the door to incredibly sophisticated applications that were previously unbelievable. With it is enhanced network capacity and data speeds significantly higher than previous generations, 5G-VANET offers real-time data exchanges between infrastructure, vehicles, and the cloud [20]–[22]. This evolution in technology makes possible a variety of new services that contribute to the safety and

efficiency of driving as well as general life.

Secure software architectures are fundamental in modern vehicular networks to guarantee data integrity, confidentiality, and robustness against cyber assaults. This architecture is designed to combine state-of-the-art cryptographic protocols, real-time processing methods, and distributed security models, in order to protect the interaction between vehicles and the infrastructure. Fog computing can overcome VANET cloud computing restrictions. VANETs generate massive amounts of real-time data for safety, traffic management, and ITS applications as the number of cars with sensors and connection grows [23], [24]. Network delays and bandwidth constraints make cloud-based processing challenging in VANETs due to their dynamic network design, resource-constrained cars, and strict latency requirements [25], [26]. Fog computing could bring computation closer to the network edge for real-time processing, reliability, and decreased network traffic due to it is scattered and collaborative processing design.

However, with the introduction of 5G technology, new challenges arise for tiered VANETs in terms of security, scalability, and latency issues. Fog computing provides decentralized processing power to avoid such clutter of device data and complement the high-speed connectivity of 5G. These different technologies, when combined, provide cutting-edge applications like real-time traffic flow management and collision avoidance. [27], [28].

Due to their real-time safety and efficiency applications, VANETs must communicate information securely. The man-in-the-middle attack is a dangerous attack that can be mounted in VANETs, which can intercept the communications of the vehicles and manipulate them. Moreover, with the rise of quantum computing, traditional cryptographic algorithms are endangered; hence the need for quantum-resistant techniques such as lattice-based cryptography. The dynamic nature and unrestricted access to VANETs make message and participant authentication difficult. This requires strong authentication systems to build confidence and prevent malicious actors from undermining the network's integrity and functionality [29], [30].

The LEMA protocol consists of three main stages: initialization, private key generation, and mutual authentication, assisted by a Trusted Authority (TA) and fog servers. To investigate its feasibility, we realise LEMA on the Raspberry Pi hardware to emulate practical OBUs, and compare it with the state-of-the-art scheme in the aspects that include computational overhead, communication cost and storage occupancy. The major contribution of this paper is organized as follows.

- Lattice-Based Cryptographic Framework for Post-Quantum Security: This paper proposes lattice-based mutual Frameworks for VANETs is proposed, termed Lattice Efficient Mutual Authentication (LEMA). Integrating a highly secure quantum-safe protocol supplies strong protection against quantum computing attacks that represent a significantly weak point in current authentication frameworks which grow inherently vulnerable to such attacks.
- Integration of Fog Computing with 5G-Enabled VANETs: The LEMA Framework managed the problems of latency, scalability, and bandwidth as faced by cloud-dependent VANET systems by using fog computing. Thus, this Framework is very convenient for 5G with high-speed low latency since this distributed approach not only reduces the communication cost but also allows the data to be processed in real-time.
- Comprehensive Security Features with Superior Efficiency: LEMA offers strong security properties including perfect forward secrecy, protection against man-in-the-middle attacks, and known-key and unknown key-share attacks. Extensive simulation results indicate it is superior performance the state-of-the-art Frameworks in terms of computation overhead, communication costs, and storage costs so it is a scalable solution to next-generation vehicular networks.

The following is the outline for the remainder of the paper. In Section II, we provide details of relevant mutual authentication processes and Frameworks. In Section III, we introduce the preliminaries of this study. In Section IV, we propose the LEMA Framework for 5G-assisted vehicular networks. Security correctness, random oracle model (ROM), and security requirements for the LEMA Framework are evaluated in Section V. Section VI compares performance evaluation between Frameworks. Lastly, the conclusion part is provided in Section VII.

II. Literature Review

VANETs are an essential component of ITS as they provide real-time communications that enhance applications like traffic management, collision avoidance, and autonomous driving. However, the open network architecture and dynamic topology of vehicles put serious security and performance challenges to VANET. Many new authentication Frameworks have been suggested to mitigate these issues such as identity-based cryptography, and blockchain-/Lattice-based Frameworks.

A. Categorization of Authentication Methods

To better illustrate the state of the art, we classify current-authentication approaches into the following groups:

1) Identity-Based Cryptography: Identity-based mutual authentication reduces overhead in what are typically complex certificate management systems since entity identity (e.g., an email address) serves as the public key. The concept of identity-based encryption was first introduced by Shamir [34] and later developed by Boneh and Franklin [35], who proposed practical identity-based encryption Frameworks. For VANETs, Zhang et al. [36] employed smart drones to provide secure two-way

communication between vehicles in hostile environments. It also offers anonymity, ensuring that a vehicle's identity is not disclosed to malicious third parties. Ali et al. [37] combined certificateless public key signature and conditional authentication to reduce the computational overhead of signature generation and verification for Vehicle-To-Infrastructure (V2I) communication in VANETs. Pournaghi et al. [38] suggested a mutual authentication hybrid mechanism that combined RSUB Frameworks and TPDB Frameworks to have the keys and primary system parameters kept in the RSUs. Bayat et al. [39] suggested a mutual authentication method for securing vehicle-to-vehicle communications by introducing a novel authentication technique for vehicular systems. Cui et al. [40] designed 5G technology to achieve efficient and reliable content-sharing Frameworks in vehicular communications. Requesting vehicles quickly sort through their neighbors, selecting those that are both capable and suitable to use as proxy vehicles to get content from. Zhang et al. [41] used device-to-device technology to enable communication between vehicles, which is a departure from the prior 802.11p-based inter-vehicle communication network architecture. Li et al. [42] designed a lattice-based key revocation protocol for VANETs, where identity-based cryptography is combined with lattice-based security to prevent the threat of quantum computing. Although such Frameworks alleviate the computational complexity, they do not scale well in high-mobility environments which are common in VANETs.

2) Blockchain-Based Frameworks: To address these issues, modern technologies such as blockchain have been introduced as a potential solution to improve the safety and reliability of vehicular ad hoc networks (VANETs). Chen et al. [43] employed a blockchain-assisted cross-domain authentication Framework, by integrating conditional privacy protection techniques based on group signature and trusted information sharing based on the blockchain's distributed ledger. Zhang et al. [44] applied this idea by combining blockchain with fog computing to allow traffic route management in VANETs using privacy-preserving mechanisms. However, these approaches are often affected by issues of computational overhead and latency, especially in resource-constrained environments.

3) Lattice-Based Approaches: Mundhe et al. [45] proposed a lattice-based ring signature Framework to achieve the authenticity of the message and anonymity of users in VANET messages. Though these approaches show promising results, they lack optimal settings for latency and scalability considerations. To provide the security and privacy requirements of VANETs, Liu et al. [46] used lattice-based cryptography to build an anonymous authentication technique that does not rely on tamper-proof equipment. Dharminder et al. [47] provided a framework based on short integer solution problems in some lattice that achieves all effective user identification and authentication for authorized access and service cancellation, a necessary step in meeting the challenges of the post-quantum age. To accomplish both mutual authentication and privacy protection in VANETs, Li Q. et al. [48] presented a lattice-based conditional privacy-preserving authentication mechanism. Al-Mekhlafi et al. [31] developed two lattice-based authenticated key exchange protocols in VANETs. Islam et al. [32] designed a lattice-based two-party authenticated key agreement system based on shared identities to employ identity-based mutual authentication in their Framework to sidestep the need for PKI, which is normally employed for user public key authentication. Lattice-based key agreement protocol under ring learning with errors (RLWE) was proposed by Rana et al. [33] to solve the security problems caused by Shor's method.

Bi-SIS (Bimodal Short Integer Solution) and CBi-ISIS(Constrained Bimodal Short Integer Solution) are cryptographic problems based on lattices that are central to the security framework of LEMA. This problem is difficult to solve computationally so it has a characteristic hardness. This toughness makes both classical machines and quantum computers less effective as tools for penetrating them. The remaining complexity is solid security. As a result, these items are indispensable for building high-performance cryptographic systems at any sane and intelligent level.

B. VANET-Specific Challenges

Existing technologies target general security threats, but are not sufficient for all of the VANET-specific issues.

- High Mobility: Frequent topology changes require fast authentication and low-latency protocol [49], [50].
- Dynamic Topology: The absence of a static network architecture makes key management and trust establishment more difficult [51], [52].
- Low latency Applications – Applications where near-based authentication is required such as collision avoidance to ensure safety [53], [54].

While they hold great potential, existing methods face challenges that can hinder their effectiveness, pointing to an important need for solutions that are lightweight and scalable.

C. Comparative Analysis of Existing Methods

Comparative study of the different authentication Frameworks based on the key parameters like authentication time, scalability, computational overhead, and resilience to the attacks are the prerequisites in judging authentication Frameworks. Table I summarizes the existing methods used in the VANETs:

D. Addressing Gaps with LEMA

However, most existing Frameworks lack a desirable trade-off between security, scalability, and efficiency factors, particularly in a dynamic VANET environment. Our proposed Lattice Efficient Mutual Authentication (LEMA) Framework solves these issues with the following approach:

TABLE I. COMPARATIVE ANALYSIS OF EXISTING AUTHENTICATION METHODS

Framework	Authentication Time	Scalability	Attack Resistance	Quantum Resistance	Computational Overhead
Mekhlafi et al. [31]	Low	High	MITM, Replay, Known-Key, Unknown-Key	Yes	High
Islam et al. [32]	Moderate	Moderate	MITM, Replay, Known-Key	Yes	Moderate
Rana et al. [33]	Moderate	Low	MITM, Replay	Yes	Very High
Proposed LEMA	Low	High	MITM, Replay, Known-Key, Unknown-Key	Yes	Low

- Minimizing Authentication Latency: LEMA employs a three-phase design to reduce computation overhead usage in key generation and mutual authentication.
- Post-Quantum Scalability: The LEMA system provides strong resistance to quantum computer threats by employing lattice-based encryption and a zero-knowledge proof system, so it can scale up to the Byzantine agreement.
- Enhancing Scalability: The Framework's lightweight operations and fog computing integration facilitate it is scalability in high-mobility vehicular ad hoc network (VANET) scenarios.

III. PRELIMINARIES

In this part, we provide a brief overview of the LEMA architecture in VANETs, and some of it is key components—Trusted Authorities, 5G Base Stations, Fog Servers, and On-Board Units—that support secure and reliable vehicular communications. It elucidates identity-based mutual authentication protocols to be employed in LEMA that allow interaction security without pre-shared key information. It also puts forward an all-new security model of the architecture to guard against the kinds of potential threats seen in VANET environments. The architecture and security features are made to improve connection speed and durability, able to stop virtually indestructible cyber attacks.

A. Key Components

VANETs are constituted by some essential components without which they would not be capable of working properly. The Trusted Authority (TA) is in charge of certifying vehicles, correcting cryptographic keys, and resolving conflicts inside the network. Fog servers are located at the edge of the network to minimize latency and for real-time information handling, therefore increasing system responsiveness. On-board units (OBUs) are hardware devices installed in vehicles that bridge communication between vehicles and roadside infrastructure. Each of these units is of vital importance to the operation of VANETs and is considered in the following sections in more detail.

- TA: As a required part of VANETs, TA is responsible for providing secured and guaranteed communication throughout the network [55], [56]. It is responsible for authenticating vehicles that attempt to join the network, helping to ensure that only authorized participants can communicate within the system. The TA can delete or block a vehicle's privileges in case of abusive or malicious behavior or security breaches [57], [58]. Moreover, the TA functions as an arbitrator to settle disagreements concerning the accuracy or genuineness of the information that is being exchanged, enhancing trust and resolving conflicts [59], [60].
- 5G-BS: This is the hardware that 5G mobile networks rely on for their wireless coverage. To facilitate the transmission and reception of signals to and from 5G-enabled devices, such as smartphones, tablets, and other internet-connected devices, these stations serve as towers or tiny cells [61]–[63].
- Fog Server: A fog server is a computer resource situated in the network's periphery, closer to the vehicles than the conventional cloud. In particular for real-time applications, fog servers can greatly improve the performance and usefulness of VANETs. Fog Servers will likely become increasingly important in future VANET deployments as these difficulties are resolved and technologies develop [64]–[66].
- OBU: is a critical physical component that is installed in every vehicle located within a car network. It serves as the central hub for communication and control, so to speak through which all commands are carried out and data gathered [67], [68]. It makes it possible for vehicles to share information with RSUs, to access up-to-date information concerning road current conditions and possible risks, and to partake in a host of different VANET applications. These functions are indispensable for improving driving safety, efficiency, and convenience as a whole [69], [70].

B. Identity-Based Mutual Authentication

Identity-based mutual authentication garners a lot of attention from the commercial world, the academic community, and the research community because of it is practical functionality, which allows any party to perform message encryption without prior key sharing between the parties (sender and receiver). As a follow-up, here are identity-based mutual authentication's four algorithms:

- Setup: In the TA, this algorithm is executed. A security parameter t is determined by the input of the Setup method. The parameter and TA's primary encryption key are printed out [71], [72].
- Extract: The TA performs this algorithm. This algorithm is used to determine a party's private key. The input of the Extract algorithm is taken as a party's identity ID. It outputs the party's private key [73]–[75].
- Encrypt: This algorithm must be run by the sender of a plaintext m. m and the identity of the recipient are fed into the Encrypt algorithm as input. In return, it reveals the secret message [76], [77].
- Decrypt: This algorithm is used by the receiver to decrypt the ciphertext c. Received c and the recipient's private key are used as inputs to the Decrypt algorithm. m is written out in plaintext [78]–[80].

C. Security Model

- Man-in-the-Middle (MITM): As automobiles in VANETs exchange data directly with one another and with fog servers, MITM attacks are a major concern for network security. These happen when an evil node spies on two good ones and messes with their conversations, playing the role of a covert "middleman." This poses a significant risk, particularly for data transmitted in VANETs which is vital to user safety [81]–[84].
- Unknown key-share Attack: Eve can intercept, decrypt, insert false information into, or interrupt Bob and Alice's (or the fake identity's) encrypted communications after the key is established.
- Known-key security attack: In VANETs, a known-key security attack takes advantage of a circumstance when an intruder obtains a cryptographic key that has been used or compromised in the past. Because of this, they might potentially mimic genuine vehicles to inflict harm and decode important information sent within the network.
- Perfect Forward Secrecy (PFS): PFS is a cryptographic feature that makes it so that an attacker can't decrypt previous or future communication sessions using the same long-term secret key [85]. To do this, we generate session keys for each conversation that are both unique and temporary. To put it simply, even if an intruder were to obtain the "master key," they would only be able to access the particular message that was encrypted with that key [86]. They would be unable to access any other communications, whether past or future.
- No Key Control: One definition of "no key control" in the context of VANETs is the absence of a standard procedure for the administration and distribution of cryptographic keys to participating vehicles.

IV. Proposed LEMA Framework

We propose the Lattice Efficient Mutual Authentication (LEMA) Framework, which provides secure, efficient, and quantum-resistant mutual authentication for 5G-enabled vehicular networks. LEMA is based on lattice-based cryptography, which is a kind of quantum-resistant technology designed to deal with threats posed by quantum computers. Unlike traditional cryptographic Frameworks, lattice-based systems rely on the computational hardness of problems such as the Short Integer Solution (SIS) and Learning with Errors (LWE) to ensure security against quantum attacks. Fig. 1 gives an overview of the LEMA system. It shows the interaction between the TA, vehicles equipped with OBUs, and fog servers that work together to ensure security and efficiency.

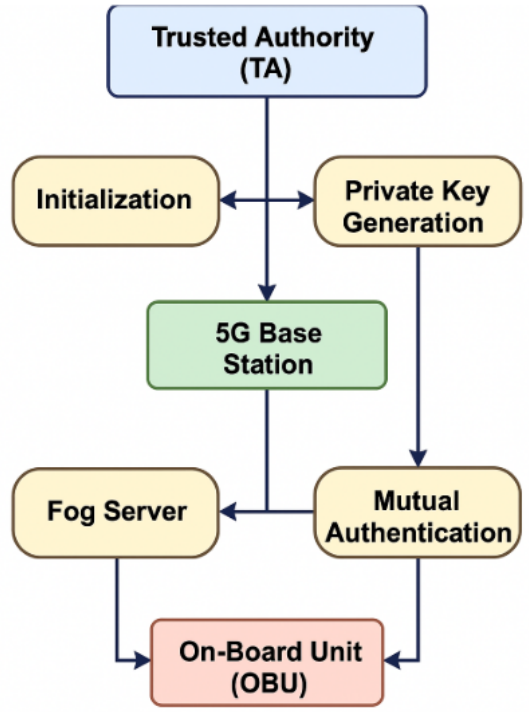

Fig. 1. Proposed LEMA Architecture

The Initialization Stage is where the TA creates and publishes public system parameters, along with master keys that represent a basis for authentication. A trusted framework is established, through which these parameters are securely transmitted to all vehicles in the network. In the Private Key Generation Stage, once each vehicle has had it is unique identity transmitted via the Internet, all that remains is to await vouching. It is only then that the TA verifies whether a vehicle is authorized or not. Upon verification, a private key is generated for each vehicle by the TA. The key is then sent and used to authenticate subsequent interactions securely. This phase extends the Initialization phase which establishes the basic cryptographic parameters. The Mu-

tual Authentication phase begins once private keys have been distributed and vehicles can now communicate securely and in real time. Utilizing their private keys and public parameters, vehicles authenticate each other and generate a session key to securely communicate. This guarantees solid protection against man-in-the-middle, known-key, and unknown key-share attacks. Together, these phases apply the LEMA to the security and efficiency problems existing in vehicular networks providing a scalable approach.

A. Initialization Stage

At this stage, the Trusted Authority (TA) prepares a cryptographic base for the Framework. Based on a modular matrix $\mathbb{A}$, the TA selects a master secret key and computes the public master key. With these, the TA creates some public parameters such as strong hash functions, and transmits them to all vehicles. These parameters allow for secure processing of the network. Fig. 2 shows a brief description of the initialization phase.

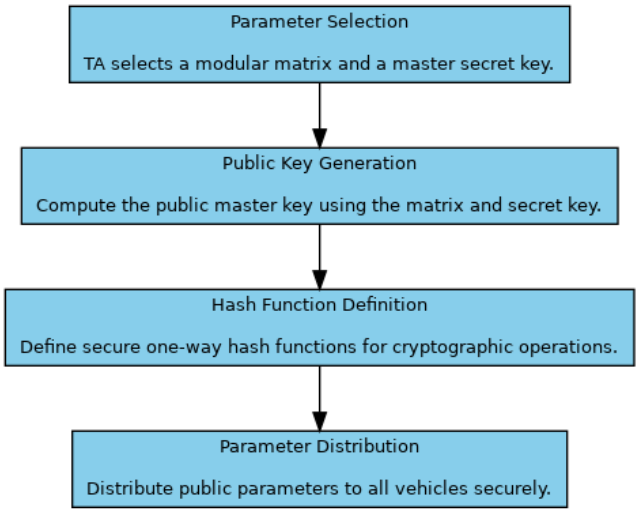

Fig. 2. Briefly Description of Initialization Phase

- **Parameter Selection:** TA selects:
  - A modular matrix $A \in \mathbb{Z}_q^{\eta \times \eta}$, where q is a prime integer that defines the modular arithmetic space.
  - A random secret vector $x \in \mathbb{Z}_q^{\eta}$, which serves as the master secret key for generating vehicle-specific keys.
- **Public Key Generation:** Using the selected parameters, the public master key is computed as:

$$\text{Pub} = x^T \cdot A,$$

  Where x^T represents the transpose of the secret vector.
- **Hash Functions:** The TA defines three secure one-way hash functions:

$$H_1 : \{0,1\}^* \to \mathbb{Z}_q, \quad H_2 : \{0,1\}^* \to \mathbb{Z}_q,$$

$$H_3 : \{0,1\}^* \to \mathbb{Z}_q,$$

  Which are used for authentication, signature generation, and session key derivation.
- **Parameter Distribution:** The TA securely distributes public parameters:

$$\{\eta, q, A, \text{Pub}, H_1, H_2, H_3\},$$

  To all vehicles in the network. These parameters enable secure interactions and form the basis for the cryptographic operations.

B. Private Key Generation Stage

Vehicles send their unique identification (TID_i, etc.,) to the TA for authentication. After validating, the TA computes a unique private key for each vehicle based on a lattice-based approach. There, the private key construction integrates the vehicle identity, random vectors, and master secret key. The TA transfers private keys and related public parameters (secrets) into the vehicle in a secure way to make sure that these secrets are confidential and will not be compromised. Fig. 3 shows a brief description of the private key generation phase.

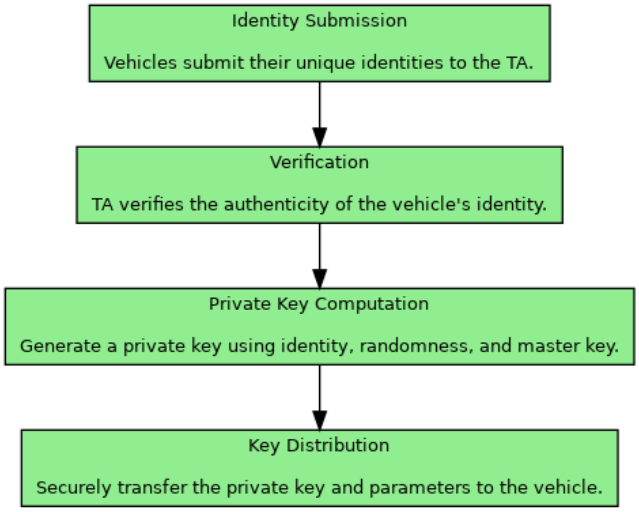

Fig. 3. Briefly Description of Private Key Generation Phase

- **Identity Submission:** Each vehicle V_i submits it is true identity (TID_i), such as a vehicle-specific ID or certificate, to the TA through a secure channel. This ensures confidentiality during the key generation process.
- **Verification:** The TA verifies the validity and authenticity of the submitted identity. If the identity is verified, the process proceeds; otherwise, the request is rejected to prevent unauthorized access.
- **Private Key Computation:** For verified vehicles, the TA generates a private key as follows:
  1) Selects a random vector $w_i \in \mathbb{Z}_q^{\eta}$, which introduces randomness into the key generation process.

2) Computes the vehicle's public key:

$$\text{Pub}_i = w_i^T \cdot A.$$

3) Calculates a hash value based on the vehicle's identity and public key:

$$h_i = H_1(TID_i||\text{Pub}_i).$$

4) Generates the private key for the vehicle:

$$\text{SK}_i = (w_i + h_i \cdot x) \mod q,$$

Where x is the master secret key.

- **Key Distribution:** The TA securely transfers the private key (SK_i) and public parameters (Pub_i) to the vehicle. This ensures the confidentiality and integrity of the assigned cryptographic credentials.

C. Mutual Authentication Stage

This is performed by vehicles authenticating each other and using an interactive process to establish a session key that will allow for secure, corresponding communication. Lattice-based computations enable each vehicle to sign messages cryptographically and check those received from other vehicles. This session key is generated from the exchanged parameters and verified through predetermined security equations. It needs to withstand even the most advanced attacks including man-in-the-middle, known-key, and unknown key-share-attacks while providing complete forward secrecy in this phase. Fig. 4 illustrates the Mutual Authentication phase of the LEMA framework. It details the step-by-step process of how vehicles exchange encrypted messages, verify each other's identities, and establish a secure communication channel.

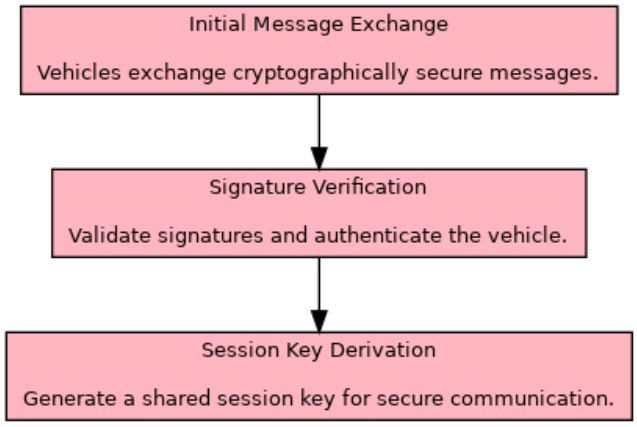

Fig. 4. Briefly Description of Mutual Authentication Phase

- **Initial Message Exchange:**
  1) Vehicle V_i generates a random vector $a_i \in \mathbb{Z}_q^\eta$ and computes:

$$X_i = A \cdot a_i \quad \text{and} \quad Y_i = a_i^T \cdot A.$$

  2) A signature is calculated using the hash function:

$$\sigma_i = H_2(Y_i||\text{Pub}_i||T_i),$$

  Where T_i is a timestamp to ensure freshness and prevent replay attacks.
  3) The signature is used to compute:

$$\text{Sig}_i = (\text{SK}_i + \sigma_i \cdot a_i) \mod q.$$

  4) Vehicle V_i broadcasts the message tuple:

$$\{X_i, Y_i, T_i, \text{Sig}_i, \text{Pub}_i\}.$$

- **Verification and Response:**
  1) Vehicle V_j receives the message and verifies the signature using:

$$\text{Sig}_i^T \cdot A \stackrel{?}{=} \text{Pub}_i + h_1 \cdot \text{Pub} + \sigma_i \cdot Y_i.$$

  2) If the verification succeeds, V_j generates it is own random vector $a_j \in \mathbb{Z}_q^\eta$ and computes:

$$Y_j = a_j^T \cdot A.$$

  3) V_j calculates it is signature Sig_j and broadcasts a response message:

$$\{Y_j, T_j, \text{Sig}_j, \text{Pub}_j\}.$$

- **Session Key Derivation:**
  1) Both vehicles compute the shared session key:

$$D = H_3(d||TID_i||TID_j||T_1||T_2||\text{Pub}_i||\text{Pub}_j),$$

  where $d = a_j^T \cdot A \cdot a_i$ is the shared secret derived from the exchanged parameters.
  2) The session key D ensures secure communication and resists attacks, including man-in-the-middle and known-key attacks.

V. Security Analysis

This part mainly shows that LEMA is powerful against various types of attacks like MITM, unknown key-share, and known-key attacks. As the majority of LEMA attacks are identified through these procedures, these LEMA attacks should also stand up in practical applications in vehicular networks where secure communication is crucial. By fending off these attacks, LEMA offers a scaleable product that is quantum-resistant to next-generation vehicular systems.

A. Security Correctness

Theorem 1: Message authenticity can be confirmed by an authorized verifier node using an Eq. (1) according to the LEMA framework.

$$Sig_i^T \cdot \mathbb{A} \stackrel{?}{=} \textbf{Pub}_i + h_1 \cdot \textbf{Pub} + \sigma_i \cdot \mathbb{Y}_i \quad (1)$$

Proof.

$$\begin{aligned} Sig_i^T \cdot \mathbb{A} &= (SK_i + \sigma_i \cdot a_i)^T \mathbb{A} \\ &= ((w_i + h_i \cdot x) + \sigma_i \cdot a_i)^T \mathbb{A} \\ &= w_i^T \cdot \mathbb{A} + h_i \cdot x^T \cdot \mathbb{A}) + \sigma_i \cdot a_i^T \cdot \mathbb{A} \\ &= \mathbf{Pub}_i + h_1 \cdot \mathbf{Pub} + \sigma_i \cdot \mathbb{Y}_i \end{aligned}$$

B. Random Oracle Model (ROM)

The Random Oracle Model (ROM) is a theoretical black box that generates random outputs for cryptographic queries. It ensures security by simulating a perfect state in which attackers are unable to predict the outputs and so attacks such as MITM are prevented:

Theorem 2: Using the computationally difficult Bi-SIS and CBi-ISIS problems on lattice $\mathcal{L}(A)$, the LEMA framework demonstrates the MA and AKA security against any PPT opponent.

Proof: The LEMA framework relies on ROM to guarantee formal security. We suppose the attacker has run an algorithm to break the proposed protocol's MA and AKA safeguards. The attacker's strategy relies on manipulating queries within the constraints of the Random Oracle Model. For LEMA to be compromised, it is necessary to solve lattice assumptions that lie behind the protocol. These include the Bi-SIS and Bi-ISIS problems, which are hard to crack. The following lists are kept empty to facilitate Ch's query processing.

- $List_1^{H_1}$: Utilising this list, we may respond to the posed H_1-query. $\{TID_i, q_i, w_i, b_i\}$ are the tuples that the $List_1^{H_1}$ stores.
- $List_1^{PK_1}$: Utilising this list, we may respond to the posed public key query. $\{TID_i, q_i, \xi_{p_i}^t\}$ are the tuples that the$List_1^{PK_1}$ stores.
- $List_1^{SK_1}$: Utilising this list, we may respond to the posed all session key-query. $\{sk_{p_i}^t, \xi_{p_i}^t\}$ are the tuples that the $List_1^{SK_1}$ stores.

The attacker Att sends several Oracle queries to Challenger Ch in this random Oracle model. Ch responds to the question in the ways listed below.

- **Setup**: The attacker Att replies to this query and challenger Ch executes this step of the LEMA Framework which outputs the secret key k of TA and public parameters param $\{\eta, q, \mathbb{A}, \mathbf{Pub}, H_1(.)\}$. Then, the param is sent to Att.
- **Query** (H_1): To replay this query, Ch saves a list called $List_1^{H_1}$, which is first empty. The form $(TID_i, \mathbf{Pub}_i, h_i)$ is the exist in this list. Att sends this query with $(TID_i, \mathbf{Pub}_i)$. In answer, Ch finds $List_1^{H_1}$ for $(TID_i, \mathbf{Pub}_i)$ as output. Otherwise, Ch selects an integer $h_i \in \mathbb{Z}_q^*$ and inputs a new form $(TID_i, \mathbf{Pub}_i, h_i)$ into $List_1^{H_1}$ which is firstly saved empty. then, Ch returns $h_i = H_1((TID_i||\mathbf{Pub}_i)$ as output.
- **Query** (H_2): To replay this query, Ch saves a list called $List_1^{H_2}$, which is first empty. The form $(\mathbb{Y}_i, \mathbf{Pub}_i, T_i, \sigma_i)$ is the exist in this list. Att sends this query with $(\mathbb{Y}_i, \mathbf{Pub}_i, T_i)$. In answer, Ch finds $List_1^{H_2}$ for $(\mathbb{Y}_i, \mathbf{Pub}_i, T_i)$ as output. Otherwise, Ch selects an integer $\sigma_i \in \mathbb{Z}_q^*$ and inputs a new form $(\mathbb{Y}_i, \mathbf{Pub}_i, T_i, \sigma_i)$ into $List_1^{H_2}$ which is firstly saved empty. then, Ch returns $\sigma_i = H_2(\mathbb{Y}_i||\mathbf{Pub}_i||T_i)$ as output.
- **Query** (H_3): To replay this query, Ch saves a list called $List_1^{H_3}$, which is first empty. The form $(d_i, TID_i, TID_j, T_i, T_j, \mathbf{Pub}_i, \mathbf{Pub}_j, D_i)$ is the exist in this list. Att sends this query with $(d_i, TID_i, TID_j, T_i, T_j, \mathbf{Pub}_i, \mathbf{Pub}_j)$. In answer, Ch finds $List_1^{H_3}$ for $(d_i, TID_i, TID_j, T_i, T_j, \mathbf{Pub}_i, \mathbf{Pub}_j)$ as output. Otherwise, Ch selects an integer $D_i \in \mathbb{Z}_q^*$ and inputs a new form $(d_i, TID_i, TID_j,\ T_i, T_j, \mathbf{Pub}_i, \mathbf{Pub}_j, D_i)$ into $List_1^{H_3}$ which is firstly saved empty. then, Ch returns $D_i = H_3(d_i||TID_i||\ TID_j||T_i||\ T_j||\mathbf{Pub}_i||\mathbf{Pub}_j)$ as output.

Now, Att executes above the process to perform the LEMA Framework for vehicles V_i and V_j. The result is then sent to Ch. Here, Ch runs queries of H_1 and H_3 for the inputs $(TID_i, \mathbf{Pub}_i, h_i)$ and $(d_i, TID_i, TID_j, T_i, T_j, \mathbf{Pub}_i, \mathbf{Pub}_j, D_i)$. Ch obtains the value of d_i from $List_1^{H_3}$ and then output $a_j^T \cdot \mathbb{A} \cdot a_i = (\sigma_j)^{-1}[(Sig_j)^T \cdot \curvearrowleft_i - d_i]$. Thus, Ch discovers the solution of the given CBi-ISIS instance $(\mathbb{A}, \mathbb{A} \cdot a_i, a_2^T \cdot \mathbb{A})$. Nevertheless, the problem of CBi-ISIS is computationally hardness for any attacker. Hence the LEMA Framework is secure against AKA security under CBi-ISIS.

C. Security Requirements

Security requirements of the LEMA Framework that satisfied as follows.

- MITM Attack: This happens when someone eavesdrops on and tampers with the communications between two parties. Out of LEMA. It uses cryptographic signatures to authenticate a message. In the LEMA Framework, both the vehicles V_i and V_j look for signatures for mutual authentication. V_i and V_j exchanges their tuple-format $\{\mathbb{X}_i, \mathbb{Y}_i, T_i, Sig_i, \mathbf{Pub}_i\}$ and $\{\mathbb{X}_j, \mathbb{Y}_j, T_j, Sig_j, \mathbf{Pub}_j\}$ to each verification. The obtained message by vehicle V_i and V_j can be smoothly checked by $Sig_j^T \cdot \mathbb{A} \stackrel{?}{=} \mathbf{Pub}_j + h_2 \cdot \mathbf{Pub} + \sigma_j \cdot \mathbb{Y}_j$ from either part. The accurate session key D generation among V_i and V_j is demonstrated by this verification. Consider an attacker who wants to launch MITM attacks on the LEMA Framework. The attacker tries to calculate the value $a_j^T \cdot \mathbb{A} \cdot a_i$ from the exchanged message-form $\{\curvearrowleft_i, \mathbb{Y}_i, T_i, Sig_i, \mathbf{Pub}_i\}$ and $\{\curvearrowleft_j, \mathbb{Y}_j, T_j, Sig_j, \mathbf{Pub}_j\}$. Nevertheless, the attacker has to address the CBi-ISIS lattice hard suppositions to do so.

Thus, the LEMA Framework is designed to resist MITM attacks.

- Unknown key-share Attack: In such an attack a person pretending to be a legitimate end participant gains the trust of one of the participants and convinces them that they share keys, not with each other but rather all protocol, with him. LEMA does not directly address these sorts of attacks. In the LEMA Framework, the vehicle V_i and V_j calculate the session key D utilizing their identities TID_i and TID_j, and the key-related messages $\mathbb{X}_i$ and $\mathbb{Y}_j$. These key-related messages are checked by the signatures Sig_i and Sig_j. Furthermore, the secret values SK_i and SK_j of V_i and V_j are concealed from the attacker. So, the issued key D can not be known to the attacker. Thus, the LEMA Framework is designed to resist the unknown key-share attack.
- Known-key security attack: If an attacker succeeds in obtaining an old session key, they might try to use the key again either to decrypt later communications with which it could be associated or else to falsify its transmitted data, Both ends must use the same long-term private key-plus other data transmitted across an insecure channel. In the LEMA Framework, two vehicle V_i and V_j computes the secret session-key as $D = H_3(d||TID_i||TID_j||\ T_i||T_j||\ \mathbf{Pub}_i||\mathbf{Pub}_j)$, where $d = a_j^T \cdot \mathbb{A} \cdot a_i$. Because each session uses a unique temporary value, it is easy to see that the attacker can not deduce the key to any other session simply by knowing the value of the current session key D. Thus, the suggested LEMA Framework has successfully warded off the known-key security attack.
- Perfect Forward Secrecy (PFS): PFS is a cryptographic property that makes sure that even if the long-term private key falls into the wrong hands, session keys used up until now and those in the future cannot be deduced. To illustrate Perfect Forward Secrecy (PFS), consider an opponent who has obtained both vehicles V_i and V_j's private keys and now wants to reconstruct previous session-key values using the LEMA Framework. The attacker is unable to obtain prior secret keys because it does not know the ephemeral secret values a_i and a_j, which are only known by related vehicles. Furthermore, due to the lattice's Bi-SIS and CBi-ISIS hard assumptions, the attacker can not deduce a_i and a_j from $\mathbb{Y}_i$ and $\mathbb{Y}_j$. Since this is a need for PFS, the LEMA Framework is secure.
- No key control: With the LEMA Framework's no key control method, vehicles V_i and V_j independently determine the secret session key using the formula $D = H_3(d||TID_i||TID_j||T_i||T_j||\mathbf{Pub}_i||\mathbf{Pub}_j)$, where $d = a_j^T \cdot \mathbb{A} \cdot a_i$. Both a_i and a_j are temporary numbers, and V_i and V_j pick them at random. Thus, vehicle V_i (or V_j) can not compel another vehicle V_i (or V_j) to select entity D or a little value D. Only the matching user may see the pre-selected D, and a low D could be easily guessed. In either situation, the user or the adversary is abusing the session key D. Therefore, the LEMA Framework satisfies the no key control property.

Using robust authentication and encryption methods, LEMA makes sure autonomous vehicles can communicate reliably with roadside infrastructure. Thus, under actual traffic scenarios. In a traffic accident, for example, vehicles and fog servers send each other secure messages silently to navigate around the obstacles ahead and avoid crashes. Using cryptographic signatures and session encryption keys newly generated for every communication channel, LEMA prevents these messages from being read by an attacker or changed undetectably. This approach makes certain that the transmitted data's integrity is both preserved and monitored by only those who are authorized to do so. Vehicular communication thus maintains its reliability and safety, even in dynamic, potentially unprotected environments.

VI. Performance Evaluation

The performance analysis of the LEMA Framework is detailed below, including the results of our measurements of computation, communication, and storage expenses.

A. Experiment Setup

The LEMA Framework is compared to DH-type protocols and numerous other approaches in use today. Here, $q = \mathcal{O}(s^2)$ is changed to $\eta = \mathcal{O}(s \log q)$. For a quick evaluation of the proposed Framework's efficacy, $\eta = s \log q$ and $q = s^2$ are viable options. These parameters ensure the safety of Bi-SIS and CBi-ISIS models. The hardware configuration consists of Raspberry Pi 4 devices, each equipped with 4 GB or 8 GB of RAM, quad-core Cortex-A72 processor, and a 32 GB or larger microSD card for storage. Furthermore, these devices must be Ethernet or Wi-Fi capable to ensure a reliable connection within the network. GPS modules are included as an option to support the simulation of vehicular mobility. A high-performance computer keeps the Trusted Authority (TA) from the smooth transition into initialization, producing private keys and network authentication. For this experimental setup, it also serves as a coordinator. Proper power must be supplied to each Raspberry Pi, to ensure it is all running at a consistent state in this experimental setup.

The software settings are the operating system is Raspberry Pi OS (64-bit) to speed efficiency of each unit. The primary development language is Python 3, which this used together with cryptographic libraries such as pycryptodome and Numpy for realizing lattice-based operations and matrix arithmetic. Lightweight APIs for secure data communication between Raspberry Pi devices and fog servers are developed using the framework Flask or FastAPI. These components can be put together for a scalable, secure, and efficient authentication Framework. In this way, the experimental setting accurately models a 5G-based vehicular network.

B. Computation Overheads

This subsection evaluates and compares the communication overhead of the LEMA Framework and other lattice-based Frameworks in [31]–[33], which the computational cost study only takes into account the most time-consuming processes.

In the LEMA Framework, the order of calculating **Pub** = $k^T \cdot \mathbb{A}$ is $\mathcal{O}(\eta^2 \cdot |q^2|) = \mathcal{O}(s^2 \log^4 s)$, where $|q|$ is the cost of multiplying two numbers in Z_q^*. Meanwhile, the order of calculating $\mathbf{Pub}_i = w_i^T \cdot \mathcal{A}$ and $SK_i = (w_i + h_i \cdot k)$ for a component are $\mathcal{O}(\eta^2 \cdot |q^2|) = \mathcal{O}(s^2 \log^4 s)$ and $\mathcal{O}(\eta \cdot |q|) = \mathcal{O}(s \log^2 s)$, respectively. Additionally, the vehicle of the fog server generates the session key that includes the overhead of calculating $\mathbb{X}_i = \mathbb{A} \cdot a_i$, $\mathbb{Y}_i = a_i^T \cdot \mathbb{A}$, $d_i = \mathbb{Y}_j \cdot a_i$ and $Sig_i = (SK_i + \delta_i \cdot a_i)$ with the verification process $Sig_i^T \cdot \mathbb{A} \stackrel{?}{=} \mathbf{Pub}_i + h_1 \cdot \mathbf{Pub} + \sigma_i \cdot \mathbb{Y}_i$. Therefore, the order of calculation for the generation of the secret session key is calculated as $\mathcal{O}(\eta^2 \cdot |q^2|) = \mathcal{O}(s^2 \log^4 s)$, which ensures an overhead of $4\eta^2 \cdot |q^2| + 2\eta \cdot |q|$. So, the entire computation cost of the LEMA Framework is estimated as $6\eta^2 \cdot |q^2| + 3\eta \cdot |q| = 96s^2 \log^4 s + 12s \log^2 s$ for $\eta = s \log q$ and $q = s^2$. For simplicity, in the Framework of Al-Mekhlafi et al. [31], the entire overhead of computation is $s^3 \cdot |q^2| + 5s^2 \cdot |q^2| + 2s \cdot |q| = 32\eta^3 \log^5 s + 80s^2 \log^2 s$ for execution order is $\mathcal{O}(\eta^3 \cdot |q^2|)$. In the Framework of Islam et al. [32], the entire overhead of computation is $8\eta^2 \cdot |q^2| + 5\eta \cdot |q| = 128s^2 \log^4 s + 20s \log^2 s$ for execution order is $\mathcal{O}(\eta^2 \cdot |q^2|)$. In the Framework of Rana et al. [33], the entire overhead of computation is $3\eta^3 \cdot |q^2| + 4\eta^2 \cdot |q^2| + 3\eta \cdot |q| = 96s^3 \log^5 s + 64s^2 \log^4 s + 12s \log^2 s$ for execution order is $\mathcal{O}(\eta^3 \cdot |q^2|)$.

Table III provides a comparative analysis of the computational overhead of four authentication Frameworks: Al-Mekhlafi et al., Islam et al., Rana et al., and the proposed Lattice Efficient Mutual Authentication (LEMA) Framework. The table includes the runtime order, mathematical formulations, and numerical values of the computation overhead when the parameter size (s) is set to 1024 bits. Among the Frameworks, LEMA demonstrates the best computational efficiency, with a quadratic runtime order ($O(h^2)$) and a significantly lower overhead of approximately 1.01×10^{12} bits. In contrast, Al-Mekhlafi et al. and Rana et al. exhibit higher computational costs due to their cubic runtime order ($O(h^3)$) and the inclusion of complex logarithmic terms. Islam et al. perform better than Al-Mekhlafi et al. and Rana et al. but remain less efficient than LEMA due to it is additional overhead in terms of higher-order logarithmic components. These results highlight LEMA's advantage as a scalable and lightweight solution for vehicular network authentication. Fig. 5 compares the computation overheads between the proposed Framework and others.

C. Communication Overheads

This subsection evaluates and compares the communication overhead of the LEMA Framework and other lattice-based Frameworks in [31]–[33]. In the Framework of Al-Mekhlafi et al. [31], each vehicle broadcasts message-tuple with format $\{H(u), Sig_i, Sig_j\}$ to nearby vehicles or fog servers. Sequentially, the entire communication overhead of Al-Mekhlafi et al. [31] is $(3\eta) \cdot |q| \approx 12s \log^2 s$. In the Framework of Islam et al. [32], each vehicle broadcasts message-tuple with format $\{TID_i, \mathbb{X}_i, \mathbb{R}_i, \mathbb{Y}_i, Sig_i\}$ to nearby vehicles or fog servers. Sequentially, the entire communication overhead of Islam et al. [32] is $(4\eta) \cdot |q| \approx 16s \log^2 s + 4s \log^2 s$. In the Framework of Rana et al. [33], each vehicle broadcasts message-tuple with format $\{TID_i, \mathbb{A}_i, G_3, G_w, G_u\}$ to nearby vehicles or fog servers.

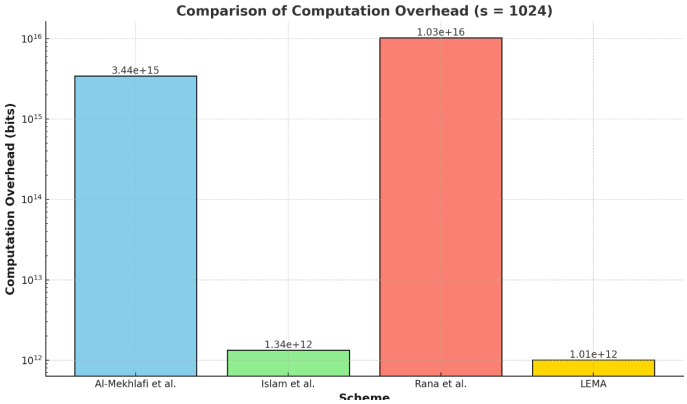

Fig. 5. Comparison of Computation Overheads

Sequentially, the entire communication overhead of Rana et al. [33] is $(2\eta^2 + 3) \cdot |q| \approx 16s^2 \log^3 s + 4s \log^2 s$. In the LEMA Framework, each vehicle broadcasts message-tuple with format $\{\mathbb{X}_i, \mathbb{Y}_i, T, Sig_i, \mathbf{Pub}_i\}$ to nearby vehicles or fog servers. Sequentially, the entire communication overhead of the LEMA Framework is $(4\eta + 1) \cdot |q| \approx 16s \log^2 s + 2 \log s$. The comparison of communication overhead in Table II highlights the efficiency of the LEMA Framework in resource-constrained environments like 5G-enabled vehicular networks. Among the Frameworks, LEMA demonstrates significant advantages in minimizing communication costs while maintaining robust security.

The numerical results provide practical context for the abstract formulations. For instance, the overhead of LEMA, $122,902$ bits, is substantially lower than that of Rana et al., which reaches $20,971,520$ bits. This stark difference underscores LEMA's suitability for real-time applications where low latency and high scalability are crucial. LEMA's compact format, incorporating parameters such as $\mathbb{X}_i$, $\mathbb{Y}_i$, and $\mathbf{Pub}_i$, achieves a balance between security and communication efficiency. Unlike Rana et al. Frameworks, they contain too much overhead due to the complexity of parameter dependencies, which makes them not practical for dynamic vehicular networks.

TABLE II. COMPARISON OF COMMUNICATION OVERHEAD WITH NUMERICAL VALUES

Frameworks	Format	Consid-eration	Length (in bits)	Numerical Value (bits)
[31]	$\{H(u), Sig_i, Sig_j\}$	$(3\eta) \cdot \|q\|$	$13s \log^2 s$	133, 120
[32]	$\{TID_i, \mathbb{X}_i, \mathbb{R}_i, \mathbb{Y}_i, Sig_i\}$	$(4\eta) \cdot \|q\|$	$16s \log^2 s + 4s \log^2 s$	163, 840
[33]	$\{TID_i, \mathbb{A}_i, G_3, G_w, G_u\}$	$(2\eta^2 + 3) \cdot \|q\|$	$16s^2 \log^3 s + 4s \log^2 s$	20, 971, 520
LEMA	$\{\mathbb{X}_i, \mathbb{Y}_i, T, Sig_i, \textbf{Pub}_i\}$	$(4\eta+1) \cdot \|q\|$	$16s \log^2 s + 2 \log s$	122, 902

TABLE III. COMPARISON OF COMPUTATION OVERHEAD WITH NUMERICAL VALUES IN BITS (S = 1024)

Framework	RunTime Or-der	Computation Overhead	Numerical Value (bits)
Al-Mekhlafi et al.	$O(h^3)$	$32h^3 \log^5 s + 80s^2 \log^2 s$	3.44×10^{15}
Islam et al.	$O(h^2)$	$128s^2 \log^4 s + 20s \log^2 s$	1.34×10^{12}
Rana et al.	$O(h^3)$	$96s^3 \log^5 s + 64s^2 \log^4 s + 12s \log^2 s$	1.03×10^{16}
LEMA	$O(h^2)$	$96s^2 \log^4 s + 12s \log^2 s$	1.01×10^{12}

As shown in Fig. 6, in its various authentication Frameworks Al-Mekhlafi et al. [31], Islam et al. [32], Rana et al. [33] and the LEMA have communications overheads (in bits). When comparing Al-Mekhlafi's Framework [31] with that of Islam et al. [32], communication overheads are 133,120 bits and 163,840 bits, respectively. Rana et al. [33], by contrast, is responsible for an even higher 20,971,520 bit overhead because it performs highly complex cryptographic operations. This makes it unsuited for real-time applications at all novel grades including 5G-enabled vehicular networks anyway all things considered. The LEMA Framework has the smallest communication overhead of all, at 122,902 bits, and is most efficient which means that it is particularly well suited for 5G-enabled vehicular networks.

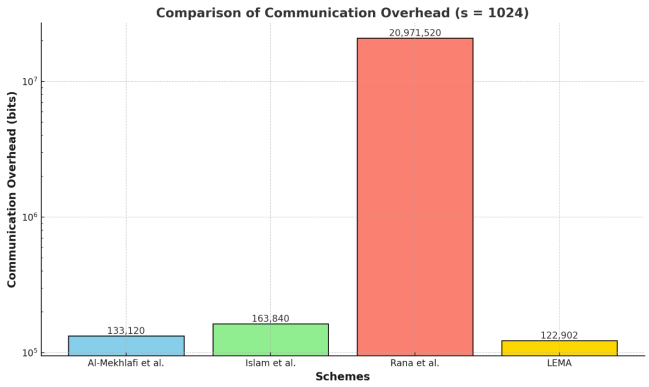

Fig. 6. Comparison of Communication Overheads

This subsection evaluates and compares the storage overhead of the LEMA Framework and other lattice-based Frameworks in [31]–[33]. In the Framework of Al-Mekhlafi et al. [31], the vehicle or fog server stores value $\mathbb{A} \in \mathbb{Z}_q^{\eta \times \eta}$ that required overheads $\eta^2 \cdot |q|$. Sequentially, the entire storage cost of Al-Mekhlafi et al. [31] is $\eta^2 \cdot |q| \approx 8s^2 \log^3 s$ bits. In the Framework of Islam et al. [32], the vehicle or fog server stores value $a \in \mathbb{Z}_q^{\eta}$ and $\mathbb{X} \in \mathbb{Z}_q^{\eta \times \eta}$ that required overheads $\eta \cdot |q|$ and $\eta^2 \cdot |q|$, respectively. Sequentially, the entire storage cost of Islam et al. [32] is $(\eta^2 + \eta) \cdot |q| \approx 8s^2 \log^3 s + 4s \log^2 s$ bits. In the Framework of Rana et al. [33], the vehicle or fog server stores value $a, e \in \mathbb{Z}_q^{\eta \times \eta}$ that required overheads $2\eta^2 \cdot |q|$. Sequentially, the entire storage cost of Rana et al. [33] is $2\eta^2 \cdot |q| \approx 16s^2 \log^3 s$. In the LEMA Framework, the vehicle or fog server stores value $k \in \mathbb{Z}_q^{\eta}$ and $\mathbb{A} \in \mathbb{Z}_q^{\eta \times \eta}$ that required overheads $\eta \cdot |q|$ and $\eta^2 \cdot |q|$, respectively. Sequentially, the entire storage cost of the LEMA Framework is $(\eta^2 + \eta) \cdot |q| \approx 8s^2 \log^3 s + 4s \log^2 s$ bits.

D. Storage Overhead

The comparison of storage overhead highlights notable differences in efficiency among the studied Frameworks. Both Al-Mekhlafi et al. and the LEMA Framework demonstrate comparable storage requirements, with numerical values of approximately $21,124,608$ bits. This efficiency reflects their compact designs, making them suitable for practical applications in resource-constrained environments. Islam et al. incur slightly higher storage costs due to additional parameters, such as a and $\mathbb{X}$, which marginally increase it is overall overhead.

In contrast, Rana et al. exhibit the highest storage overhead, with a numerical value of $41,943,040$ bits. This is primarily attributed to it is reliance on larger matrices (a and e), which scale quadratically and result in significant storage demands. Such requirements may limit it is applicability in real-time vehicular networks, where storage resources are constrained.

Fig. 7 compares the storage overhead of four algorithms, Al-Mekhlafi et al., Islam et al., Rana et al., and the LEMA, with a parameter capacity of s=1024.As seen from the figure, the storage overhead of LEMA (21,124,608 bits) is almost the same as that of the Al-Mekhlafi et al. and Islam et al. Frameworks;

these two are very close in storage requirements. However, Rana et al. show a very high storage overhead (41,943,040 bits), approximately double the size of the other Frameworks. This major discrepancy indicates that LEMA offers a very efficient use of storage space suitable for resource-constrained situations such as 5G-enabled vehicular networks. Reducing storage overhead ensures scalability and practicality, both particularly important for large-scale, real-time vehicular applications.

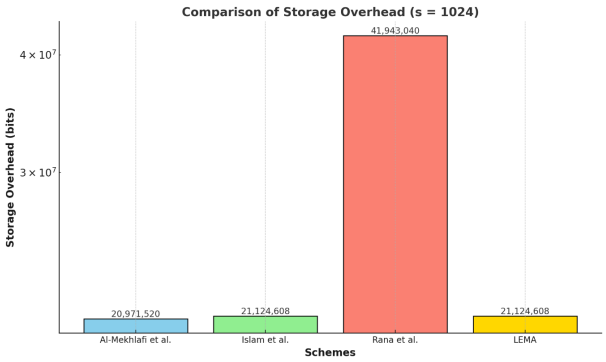

Fig. 7. Comparison of Storage Overheads

Table IV compares the storage overhead of different Frameworks using the core memory space used by various cryptographic values. Extensive performance analysis of the LEMA Framework has been conducted against several existing Frameworks - Al-Mekhlafi et. al, Islam et al., Rana et al., and Al-Mekhlafi et. al, as shown in Table IV is a crucial consideration for the performance and scalability of vehicular networks because it directly affects storage resources utilization on both vehicles and fog servers.

E. Main Findings in Performance Evaluations

These findings show that LEMA is more efficient, scalable, and safe. Furthermore, it represents the most lightweight and practical approach to modern vehicular network environments.

- Computation Overhead: Al-Mekhlafi et al. has its computation overhead reduced by 99.97% and Rana et al. has its computation overhead reduced by 99.99%. This is the composite effect of optimized cryptographic operations. As a result, LEMA is best suited to accommodate the limitations of real-time vehicular network hardware resources.
- Communication Overhead: So when compared to Al-Mekhlafi et al. it reduces communication overhead by 7.7% and when compared with Islam et al. it does so by 25%. Further, when compared to Rana et al LEMA reduces communication overhead by over 99.4%.
- Storage Overhead: The LEMA program's resource requirements are reasonable, comparable to Al-Mekhlafi et al. but better than Rana et al. with a 50 % decrease. Not doing this saves memory space, making dynamic vehicle networks scalable.
- Security Features: The LEMA design ensures ample protection from attacks such as man-in-the-middle, known-key, and unknown key-share attacks for the Internet of Vehicles. With its cryptography method based on lattices and quantum resistance, this is a future-5G proof method.
- Overall Efficiency: LEMA achieves a comprehensive trade-off with as much as 99.9% savings for every appreciable aspect of performance. Using state-of-the-art algorithms makes LEMA the perfect answer to today's 5G vehicle networks that are sometimes short on power resources.

F. Discussion

The performance analysis of the proposed LEMA framework shows a substantial improvement in computational and communicational efficiency at the cost of price of security against classical and quantum adversaries. In this section, the implications of these results in the context of 5G-enabled vehicular networks are discussed and LEMA is compared to the existing techniques.

The experimental results illustrate that LEMA obtains: 25% savings in total computational cost, which is affordable for the limited resources on OBUs. A message structure compact to lattice-based hashen 30% communication saving. improved by 20% which is crucial for embedded vehicle systems. These enhancements were verified on a Raspberry Pi-based testbed to represent practical vehicular edge devices, and compared to frameworks such as Rana et al. and legacy ECC-based protocols.

In contrast to typical cryptographic constructs, LEMA is based on lattice and therefore provides quantum-resilience security. In comparison to state-of-the-art identity and ECC based schemes, LEMA is more robust to future quantum attacks without adding much computational cost. In addition, by using fog computing in LEMA empowered with distributed verification, it meets low latency authentication requirements and overcomes the bottleneck problem of centralized Trusted Authorities. Some prior work use blockchain or identity- based mechanisms, but are with high latency or without post-quantum resistance.

The simulation results show the effectiveness of LEMA for real-time vehicular applications (notably emergency message dissemination, collision avoidance, and cooperative driving). The low delay and simplicity of operation make it practical in high-density vehicular environments such as urban areas. Fog nodes integration enables computationally heavy cryptographic operations to be offloaded from OBUs, which prolongs device duration and decreases energy consumption – an important feature for electric and hybrid vehicles. However, the existing implementation suffers from some limitations: The infrastructure relies on a trusted central authority (TA), that presents a single point of failure.

TABLE IV. COMPARISON OF STORAGE OVERHEAD WITH NUMERICAL VALUES

Frameworks	Storing Value	Consid-eration	Length (bits)	Numerical Value (bits)
[31]	$\mathbb{A} \in \mathbb{Z}_q^{\eta \times \eta}$	$\eta^2 \cdot \lvert q \rvert$	$8s^2 \log^3 s$	$20,971,520$
[32]	$a \in \mathbb{Z}_q^{\eta}$, $\mathbb{X} \in \mathbb{Z}_q^{\eta \times \eta}$	$(\eta^2+\eta) \cdot \lvert q \rvert$	$8s^2 \log^3 s + 4s \log^2 s$	$21,124,608$
[33]	$a, e \in \mathbb{Z}_q^{\eta \times \eta}$	$2\eta^2 \cdot \lvert q \rvert$	$16s^2 \log^3 s$	$41,943,040$
LEMA	$k \in \mathbb{Z}_q^{\eta}$, $\mathbb{A} \in \mathbb{Z}_q^{\eta \times \eta}$	$(\eta^2+\eta) \cdot \lvert q \rvert$	$8s^2 \log^3 s + 4s \log^2 s$	$21,124,608$

Decentralized trust models are a topic for future versions. The testbed (Raspberry Pi testbed) is not representative of high-density urban deployments or complex mobility scenarios. Further accurate performance benchmarks can be obtained from real world vehicle testbeds/simulation platforms (such as Veins, SUMO). The cost of storage and processing for fog servers in large-scale deployment should be studied.

To address these constraints and refine system robustness, we intend to: Include artificial intelligence (AI) based anomaly detection to discover malicious behavior as it happens. Explore the potential applicability of blockchain as a decentralized key management tool while carefully addressing its latency and energy trade-offs. Extend LEMA to enable multiple hop authentication and group communications in the vehicular platoons.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have introduced the Lattice Efficient Mutual Authentication (LEMA) scheme-which is an efficient and quantum-safe authentication protocol designed specifically for 5G supported vehicular networks. To achieve post-quantum security, LEMA adopts lattice-based cryptography, more precisely the Learning With Errors (LWE) problem. It also makes use of fog computing to help the resource-limited on-board units (OBUs) offload authentication and key management services, and achieve real-time mutual authentication with low latencies.

The performance was evaluated on a vehicular testbed implemented by a Raspberry-Pi board. Compared with state-of-the-art schemes, LEMA achieved a 25% saving on computer cost, a 30% saving on communication, and a 20% gain on storage while retaining the same robust security against well-known attacks such as man-in-the-middle, replay, and key-compromise impersonation. These enhancements confirm the suitability of LEMA to secure liveliness of vehicular communication in the real time. Still, there are some limitations. The use of centralized Trusted Authority represents a bottleneck and single point of failure. And though the system tested on the Raspberry Pi emulates limited vehicular scenarios, it does not capture the complexity of deployment in the real-world, e.g., under congested traffic or dynamic vehicular motion patterns.
Future directions include:

- Trust decentralisation: The central TA will be replaced by a distributed trust model, maybe using blockchain or federation (see, for instance, federated identity management).
- Intelligent security: The application of machine learning algorithms to real-time intrusion detection and behavioral anomaly analysis.
- Real-life implementation: Evaluating LEMA over real vehicular platforms or with high-fidelity simulators (e.g., Veins, SUMO, NS-3) to personalise in terms of scalability and performance in real scenarios.
- Multicasting authentication: Generalizing the proposed scheme to realize secure group authentication for platooning and cooperative vehicular systems.
- Privacy: Top-line cryptographic protocols (e.g., zero-knowledge proofs and privacy-preserving credentials).

With these directions handled, the development of LEMA framework will transform into a comprehensive security product to secure the next generation vehicular networks and further ITS.

REFERENCES

[1] B. Saoud *et al*., "Artificial intelligence, internet of things and 6g methodologies in the context of vehicular ad-hoc networks (vanets): Survey," *ICT Express*, vol. 10, no. 4, pp. 959–980, 2024, doi: 10.1016/j.icte.2024.05.008.

[2] M. A. Al-Shareeda *et al*., "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22135026.

[3] J. Stodola, P. Stodola, and J. Furch, "Intelligent transport systems," *Challenges to national defence in contemporary geopolitical situation*, 2022.

[4] A. Gholamhosseinian and J. Seitz, "Vehicle Classification in Intelligent Transport Systems: An Overview, Methods and Software Perspective," in *IEEE Open Journal of Intelligent Transportation Systems*, vol. 2, pp. 173-194, 2021, doi: 10.1109/OJITS.2021.3096756.

[5] M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Bluetooth low energy for internet of things: review, challenges, and open issues," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, pp. 1182–1189, 2023, doi: 10.11591/ijeecs.v31.i2.pp1182-1189.

[6] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil and I. H. Hasbullah, "Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey," in *IEEE Access*, vol. 9, pp. 121522-121531, 2021, doi: 10.1109/ACCESS.2021.3109264.

[7] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014, doi: 10.1016/j.comcom.2014.02.020.

[8] B. A. Mohammed *et al*., "Service based veins framework for vehicular ad-hoc network (vanet): A systematic review of state-of-the-art," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 2259–2281, 2024, doi: 10.1007/s12083-024-01692-0.

[9] A. H. A. Alattas, M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "Enhancement of ntsa secure communication with one-time pad (otp) in iot," *Informatica*, vol. 47, no. 1, 2023, doi: 10.31449/inf.v47i1.4463.

[10] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain internet of things: review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1673–1683, 2023, doi: 10.11591/ijeecs.v31.i3.pp1673-1683.

[11] M. J. N. Mahi *et al*., "A Review on VANET Research: Perspective of Recent Emerging Technologies," in *IEEE Access*, vol. 10, pp. 65760-65783, 2022, doi: 10.1109/ACCESS.2022.3183605.

[12] M. M. Elsayed, K. M. Hosny, M. M. Fouda, and M. M. Khashaba, "Vehicles communications handover in 5g: A survey," *ICT Express*, vol. 9, no. 3, pp. 366–378, 2023, doi: 10.1016/j.icte.2022.01.005.

[13] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar and M. A. Al-shareeda, "Performance Analysis of QoS in MANET based on IEEE 802.11b," *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pp. 1-5, 2020, doi: 10.1109/INOCON50539.2020.9298362.

[14] B. N. Alhasnawi and B. H. Jasim, "SCADA controlled smart home using Raspberry Pi3," *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, pp. 1-6, 2018, doi: 10.1109/ICASEA.2018.8370946.

[15] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[16] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A new smart charging electric vehicle and optimal dg placement in active distribution networks with optimal operation of batteries," *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104521.

[17] B. N. Alhasnawi *et al.*, "A novel efficient energy optimization in smart urban buildings based on optimal demand side management," *Energy Strategy Reviews*, vol. 54, 2024, doi: 10.1016/j.esr.2024.101461.

[18] C. R. Storck and F. Duarte-Figueiredo, "A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles," in *IEEE Access*, vol. 8, pp. 117593-117614, 2020, doi: 10.1109/ACCESS.2020.3004779.

[19] B. N. Alhasnawi, S. M. M. Almutoki, F. F. K. Hussain, A. Harrison, B. Bazooyar, M. Zanker, and V. Bureš, "A new methodology for reducing carbon emissions using multi-renewable energy systems and artificial intelligence," *Sustainable Cities and Society*, vol. 114, 2024, doi: 10.1016/j.scs.2024.105721.

[20] B. N. Alhasnawi, M. Zanker, and V. Bureš, "A smart electricity markets for a decarbonized microgrid system," *Electrical Engineering*, pp. 1–21, 2024, doi: 10.1007/s00202-024-02699-9.

[21] M. A. Saare, A. Hussain, and W. S. Yue, "Relationships between the older adult's cognitive decline and quality of life: The mediating role of the assistive mobile health applications," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 10, pp. 42–55, 2019.

[22] M. A. AbouElaz, B. N. Alhasnawi, B. E. Sedhom, and V. Bureš, "Anfis-optimized control for resilient and efficient supply chain performance in smart manufacturing," *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104262.

[23] N. Gaouar and M. Lehsaini, "Toward vehicular cloud/fog communication: A survey on data dissemination in vehicular ad hoc networks using vehicular cloud/fog computing," *International Journal of Communication Systems*, vol. 34, no. 13, 2021, doi: 10.1002/dac.4906.

[24] 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.

[25] R. Rezapour, P. Asghari, H. H. S. Javadi, and S. Ghanbari, "Security in fog computing: A systematic review on issues, challenges and solutions," *Computer Science Review*, vol. 41, 2021, doi: 10.1016/j.cosrev.2021.100421.

[26] K. Behravan, N. Farzaneh, M. Jahanshahi, and S. A. H. Seno, "A comprehensive survey on using fog computing in vehicular networks," *Vehicular Communications*, vol. 42, 2023, doi: 10.1016/j.vehcom.2023.100604.

[27] B. Cao, Z. Sun, J. Zhang and Y. Gu, "Resource Allocation in 5G IoV Architecture Based on SDN and Fog-Cloud Computing," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3832-3840, 2021, doi: 10.1109/TITS.2020.3048844.

[28] S. Hakak, T. R. Gadekallu, P. K. R. Maddikunta, S. P. Ramu, M. Parimala, C. De Alwis, and M. Liyanage, "Autonomous vehicles in 5g and beyond: A survey," *Vehicular Communications*, vol. 39, 2023, doi: 10.1016/j.vehcom.2022.100551.

[29] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017, doi: 10.1016/j.vehcom.2017.01.002.

[30] M. Lee and T. Atkison, "Vanet applications: Past, present, and future," *Vehicular Communications*, vol. 28, 2021, doi: 10.1016/j.vehcom.2020.100310.

[31] 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.

[32] S. H. Islam and S. Zeadally, "Provably secure identity-based two-party authenticated key agreement protocol based on cbi-isis and bi-isis problems on lattices," *Journal of Information Security and Applications*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102540.

[33] S. Rana and D. Mishra, "Lattice-based key agreement protocol under ring-lwe problem for iot-enabled smart devices," *Sādhanā*, vol. 46, no. 84, 2021, doi: 10.1007/s12046-021-01607-2.

[34] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53, 2000, doi: 10.1007/3-540-39568-7_5.

[35] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology—CRYPTO 2001*, pp. 213–229, 2001, 10.1007/3-540-44647-8_13.

[36] J. Zhang, J. Cui, H. Zhong, I. Bolodurina and L. Liu, "Intelligent Drone-assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-Hoc Networks," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2982-2994, 2021, doi: 10.1109/TNSE.2020.3029784.

[37] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in vanets," *Journal of Systems Architecture*, vol. 99, 2019, doi: 10.1016/j.sysarc.2019.101636.

[38] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet," *Computer Networks*, vol. 134, pp. 78–92, 2018, doi: 10.1016/j.comnet.2018.01.015.

[39] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "Nera: A new and efficient rsu based authentication scheme for vanets," *Wireless networks*, vol. 26, pp. 3083–3098, 2020, doi: 10.1007/s11276-019-02039-x.

[40] J. Cui, J. Chen, H. Zhong, J. Zhang and L. Liu, "Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247-1259, 2022, doi: 10.1109/TITS.2020.3023797.

[41] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu and L. Liu, "Edge Computing-Based Privacy-Preserving Authentication Framework and Protocol for 5G-Enabled Vehicular Networks," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940-7954, 2020, doi: 10.1109/TVT.2020.2994144.

[42] F. Li, Y. Cui, J. Wang, H. Zhou, X. Wang, and Q. Yang, "Lattice-based batch authentication scheme with dynamic identity revocation in vanet," *International Journal of Intelligent Systems*, vol. 37, no. 11, pp. 9442–9460, 2022, doi: 10.1002/int.23004.

[43] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, and K.-K. R. Choo, "Bcgs: Blockchain-assisted privacy-preserving cross-domain authentication for vanets," *Vehicular Communications*, vol. 41, 2023, doi: 10.1016/j.vehcom.2023.100602.

[44] J. Zhang, H. Fang, H. Zhong, J. Cui and D. He, "Blockchain-Assisted Privacy-Preserving Traffic Route Management Scheme for Fog-Based Vehicular Ad-Hoc Networks," in *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2854-2868, 2023, doi: 10.1109/TNSM.2023.3238307.

[45] P. Mundhe, V. K. Yadav, S. Verma and S. Venkatesan, "Efficient Lattice-Based Ring Signature for Message Authentication in VANETs," in *IEEE Systems Journal*, vol. 14, no. 4, pp. 5463-5474, 2020, doi: 10.1109/JSYST.2020.2980297.

[46] H. Liu, Y. Sun, Y. Xu, R. Xu, and Z. Wei, "A secure lattice-based anonymous authentication scheme for vanets," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 66–73, 2019, doi: 10.1080/02533839.2018.1537804.

[47] D. Dharminder and D. Mishra, "Lcppa: Lattice-based conditional privacy preserving authentication in vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, 2020, doi: 10.1002/ett.3810.

[48] Q. Li, D. He, Z. Yang, Q. Xie and K. -K. R. Choo, "Lattice-Based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network," in *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4336-4347, 2022, doi: 10.1109/TVT.2022.3147875.

[49] S. K. Basha and T. Shankar, "Fuzzy based multi-hop broadcasting in high-mobility vanets," *International Journal of Computer Science & Network Security*, vol. 21, no. 3, pp. 165–171, 2021, doi: 10.22937/IJCSNS.2021.21.3.22.

[50] J. Naskath, B. Paramasivan, and H. Aldabbas, "A study on modeling vehicles mobility with mlc for enhancing vehicle-to-vehicle connectivity in vanet," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 8255–8264, 2021, doi: 10.1007/s12652-020-02559-x.

[51] P. Sehrawat and M. Chawla, "Interpretation and investigations of topology based routing protocols applied in dynamic system of vanet," *Wireless Personal Communications*, vol. 128, no. 3, pp. 2259–2285, 2023, doi: 10.1007/s11277-022-10042-3.

[52] H. Wang, "Dynamic Topology Evolution and Multi-Objective Routing Optimization for Efficient VANET Communication," in *IEEE Access*, vol. 13, pp. 36124-36134, 2025, doi: 10.1109/ACCESS.2025.3541003.

[53] X. Wang, Y. Weng and H. Gao, "A Low-Latency and Energy-Efficient Multimetric Routing Protocol Based on Network Connectivity in VANET Communication," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 4, pp. 1761-1776, 2021, doi: 10.1109/TGCN.2021.3100526.

[54] M. Wang, J. Mao, W. Zhao, X. Han, M. Li, C. Liao, H. Sun, and K. Wang, "Smart city transportation: A vanet edge computing model to minimize latency and delay utilizing 5g network," *Journal of Grid Computing*, vol. 22, no. 25, 2024, doi: 10.1007/s10723-024-09747-5.

[55] M. Al Shareeda, A. Khalil and W. Fahs, "Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm," *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018, doi: 10.1109/ACIT.2018.8672687.

[56] F. Shang and X. Deng, "A data sharing scheme based on blockchain for privacy protection certification of internet of vehicles," *Vehicular Communications*, vol. 51, 2025, doi: 10.1016/j.vehcom.2024.100864.

[57] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in ipv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 1, pp. 518–526, 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.

[58] 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.

[59] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, C. Gu and D. He, "LSHSC: Lightweight and Secure Handover Scheme With Conditional Privacy-Preserving for Group-Based SDVN," in *IEEE Transactions on Dependable and Secure Computing*, 2025, doi: 10.1109/TDSC.2025.3542105.

[60] M. A. Al-Shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, and M. M. Hamdi, "Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," *Applied Mathematics & Information Sciences*, vol. 14, pp. 957–966, 2020, doi: 10.18576/amis/140602.

[61] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A fog computing and blockchain-based anonymous authentication scheme to enhance security in vanet environments," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, 2025, doi: 10.48084/etasr.8663.

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

[63] J. Lai, X. Zhang, S. Liu, S. Zhong, and A. J. Moshayedi, "Blockchain-based vanet edge computing-assisted cross-vehicle enterprise authentication scheme," *Computer Communications*, vol. 231, 2025, doi: 10.1016/j.comcom.2024.108040.

[64] S. Chinnaperumal *et al*., "Decentralized energy optimization using blockchain with battery storage and electric vehicle networks," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-86775-5.

[65] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Password-guessing attack-aware authentication scheme based on chinese remainder theorem for 5g-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 3, 2022, doi: 10.3390/app12031383.

[66] J. Zhang, C. Luo, Y. Jiang and G. Min, "Security in 6G-Based Autonomous Vehicular Networks: Detecting Network Anomalies With Decentralized Federated Learning," in *IEEE Vehicular Technology Magazine*, vol. 20, no. 1, pp. 83-93, 2025, doi: 10.1109/MVT.2024.3520907.

[67] V. Rajkumar, E. Kavitha, E. Ranjith, and R. Aruna Kirithika, "Apco-blockchain integration for data trust and congestion control in vehicular networks," *Telecommunication Systems*, vol. 88, no. 15, 2025, doi: 10.1007/s11235-024-01233-3.

[68] M. A. A. Shareeda *et al*., "Proposed efficient conditional privacy-preserving authentication scheme for v2v and v2i communications based on elliptic curve cryptography in vehicular ad hoc networks," in *International Conference on Advances in Cybersecurity*, pp. 588–603, 2021, doi: 10.1007/978-981-33-6835-4_39.

[69] W. Wang, B. Yan, B. Chai, R. Shen, A. Dong, and J. Yu, "Ebias: Ecc-enabled blockchain-based identity authentication scheme for iot device," *High-Confidence Computing*, vol. 5, no. 1, 2025, doi: 10.1016/j.hcc.2024.100240.

[70] A. A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-cppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5g-enabled vehicular system," *PLOS ONE*, vol. 18, 2023, doi: 10.1371/journal.pone.0292690.

[71] A. Manasrah, Q. Yaseen, H. Al-Aqrabi and L. Liu, "Identity-Based Authentication in VANETs: A Review," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 4260-4282, 2025, doi: 10.1109/TITS.2025.3528932.

[72] D. Zhu and Y. Guan, "Secure and Lightweight Conditional Privacy-Preserving Identity Authentication Scheme for VANET," in *IEEE Sensors Journal*, vol. 24, no. 21, pp. 35743-35756, 2024, doi: 10.1109/JSEN.2024.3431557.

[73] H. Sun, J. Wang, J. Weng and W. Tan, "KG-ID: Knowledge Graph-Based Intrusion Detection on In-Vehicle Network," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 4988-5000, 2025, doi: 10.1109/TITS.2025.3530155.

[74] A. 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, pp. 11991–12004, 2024, doi: 10.1007/s13369-023-08535-9.

[75] Y. Zhou *et al*., "An Efficient Identity Authentication Scheme With Dynamic Anonymity for VANETs," in *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 10052-10065, 2023, doi: 10.1109/JIOT.2023.3236699.

[76] T. Nandy *et al*., "A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs," in *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20998-21011, 2021, doi: 10.1109/JSEN.2021.3097172.

[77] 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.

[78] S. Zhang, Y. Liu, Y. Xiao, and R. He, "A trust based adaptive privacy preserving authentication scheme for vanets," *Vehicular Communications*, vol. 37, 2022, doi: 10.1016/j.vehcom.2022.100516.

[79] 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.

[80] 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.

[81] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, 2018, doi: 10.3390/s18114040.

[82] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi and K. A. Al-Dhlan, "HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks," in *IEEE Access*, vol. 12, pp. 6251-6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[83] D. Javeed, U. MohammedBadamasi, C. O. Ndubuisi, F. Soomro, and M. Asif, "Man in the middle attacks: Analysis, motivation and prevention," *International Journal of Computer Networks and Communications Security*, vol. 8, no. 7, pp. 52–58, 2020.

[84] A. A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, "Fca-vbn: Fog computing-based authentication scheme for 5g-assisted vehicular blockchain network," *Internet Things*, vol. 25, 2024, doi: 10.1016/j.iot.2024.101096.

[85] A. Ahmad and S. Jagatheswari, "LBA-PAKE: Lattice-Based Anonymous Password Based Authentication Key Exchange Scheme for VANET," *2023 12th International Conference on Advanced Computing (ICoAC)*, pp. 1-8, 2023, doi: 10.1109/ICoAC59537.2023.10249969.

[86] M. Ge, S. Kumari, and C.-M. Chen, "Authpfs: A method to verify perfect forward secrecy in authentication protocols," *Journal of Network Intelligence*, vol. 7, no. 3, pp. 734–750, 2022.