Fortifying V2RSU Communication with Post Quantum Security in the Green Internet of Vehicles

Basudeb Bera *, Sourav Saha †, Ashok Kumar Das ‡, *Senior Member, IEEE*,
Joel J. P. C. Rodrigues §, *Fellow, IEEE*, and Biplab Sikdar ¶, *Fellow, IEEE*
*¶ Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583
E-mail: b.bera26@nus.edu.sg; bsikdar@nus.edu.sg
† School of Electrical Engineering and Computer Science,
KTH Royal Institute of Technology, Stockholm 11428, Sweden
E-mail: sous@kth.se
‡ Center for Security, Theory and Algorithmic Research,
International Institute of Information Technology, Hyderabad 500 032, India
E-mail: iitkgp.akdas@gmail.com; ashok.das@iiit.ac.in
§ Federal University of Piauí (UFPI), Teresina - PI, Brazil
E-mail: joeljr@ieee.org

***Abstract*—Communication in the green Internet of Vehicles (IoV) demands significant energy, encompassing both communication and computation costs, along with fuel and electricity for vehicle operation. The rise of quantum computing threatens the security of existing IoV frameworks, particularly those relying on conventional public-key cryptosystems (PKC) like integer factorization and elliptic curve cryptography, which are vulnerable to quantum attacks. This paper proposes a lightweight, post-quantum security protocol for electric vehicles (EVs) in IoV, aimed at reducing computation and communication costs while enhancing energy efficiency. We conduct a comprehensive security analysis and compare our protocol with existing solutions, demonstrating its superior security, scalability, and practical effectiveness. Network simulations using NS3 further validate the robustness and efficiency of the proposed scheme for green IoV applications.**

***Index Terms*—Security, communication, IoV, post-quantum, RLWE.**

I. Introduction

In green Vehicular Communication (VC) systems, electric vehicles are interconnected and communicate wirelessly. This type of communication plays a crucial role in the development of "Intelligent Transportation Systems (ITS)", enabling electric vehicles equipped with "Onboard Units (OBUs)" to interact with connected "Roadside Units (RSUs)". These interactions improve traffic efficiency, enhance driver safety, aid in collision avoidance, provide traffic congestion warnings, and issue alerts for emergency vehicles, among other benefits. Despite advancements in ITS and the implementation of safety features in vehicles, such as Anti-lock Brake Systems (ABS), airbags, and rear-view cameras, a significant number of individuals still lose their lives in traffic accidents each year [1]. In situations involving congestion, accidents, or other road hazards, vehicles must communicate with one another in real time to reroute or avoid dangerous areas. They need to share critical information, including visibility, current locations, speeds, maneuver coordination, meteorological data, and other vital statistics. To reduce vehicle accidents and maintain transportation safety, VC networks must securely exchange data between OBUs and RSUs. The transmission of "Cooperative Awareness Messages (CAMs)" and "Decentralized Environmental Notification Messages (DENMs)" in vehicle-to-vehicle (V2V) communications presents various challenges. Since these messages are transmitted over public channels, ensuring secure communication is essential, as attackers may intercept crucial messages and conduct various attacks. Implementing robust security and privacy mechanisms within VC systems is vital to prevent malicious behavior and further enhance transportation safety and efficiency. Authentication protocols are particularly important for ensuring the privacy and security of vehicular communications. These schemes are designed to protect user privacy while fulfilling key security requirements, such as authentication, integrity, and resistance to various active and passive attacks, thereby ensuring accountability [2].

The emergence of quantum computers poses a significant security threat to traditional public-key cryptosystems (PKC), which are currently used to secure conventional systems. With the rapid advancements in quantum computing, it is essential for these traditional systems to be equipped to handle quantum attacks using existing hardware. However, traditional elliptic curve cryptography (ECC)-based security schemes are vulnerable to various attacks, such as "man-in-the-middle attacks, replay attacks, impersonation attacks" and others, presenting considerable risks to VC. Recently, lattice-based cryptography (LBC) has gained considerable attention for its ability to resist attacks from quantum threats while ensuring integrity and confidentiality. In the quantum era, it is crucial to design and implement efficient authentication mechanisms between vehicles and RSUs that incorporate post-quantum security within the green IoV system. In addition, the design protocols must be lightweight. This is important because green IoV devices, especially in EVs, often have limited processing power and battery life; a lightweight protocol minimizes en-

ergy consumption while ensuring efficient operation [3]. Moreover, lightweight protocols facilitate real-time communication, reducing latency and enabling timely responses to critical situations. As a result, we proposes a lightweight security protocol for EVs which will effectively address the security challenges posed by post-quantum attacks while promoting green communication practices in IoV systems.

A. Related Works

Wang et al. [4] proposed an "authentication scheme for V2V communication" that utilizes bilinear pairing, ECC, and hash functions. However, this scheme requires significant computational resources, making it impractical for real-world applications, and it is also vulnerable to quantum attacks. Nath et al. [5] proposed an "authentication scheme for group communication in a vehicular ad hoc network (VANET)". This scheme employs batch authentication, allowing messages from multiple vehicles to be easily authenticated by the RSU. However, it is vulnerable to ESL and quantum attacks. Zhang et al. [6] designed an "authentication scheme for VANET that utilizes a hash function and a symmetric encryption/decryption algorithm". However, this scheme is vulnerable to replay attacks and does not provide support for anonymity or untraceability. In 2023, Wang et al. [7] developed an authentication and key agreement scheme for cloud-assisted IoT applications. In their model, IoT devices, users, gateway nodes, and cloud centers mutually authenticate before establishing a session key, which is created using a hash function and ECC along with random numbers and public parameters. However, this approach is vulnerable to ESL attacks under the "Canetti and Krawczyk adversary (CK-adversary) model" [8] and cannot defend against replay attacks. Mishra et al. [9] proposed a communication mechanism for the Internet of Drones (IoD) in the context of scalable quantum computers. However, their scheme reveals the true identities of communicating parties over public channels, raising concerns about anonymity and traceability. Similarly, in 2023, Rewal et al. [10] developed an authentication scheme based on the lattice assumption for mobile communication in post-quantum environments. Their approach also exposes the real identities of mobile users, lacking anonymity and traceability. Furthermore, their scheme does not accommodate the dynamic addition of drones or devices, limiting its scalability. Vasudev et al. [11] developed an authentication mechanism for V2V communication in the IoV network using a hash function. Their scheme employs random numbers and public information to construct a session key, making it vulnerable to ESL attacks under the CK-adversary model. Furthermore, their scheme does not protect against quantum attacks, as well as anonymity and traceability attacks. Xie et al. [12] suggested an authentication mechanism for vehicles and transportation infrastructure (V2I) and V2V communication in VANETs, utilizing ECC and hash functions. However, their protocol reveals the real identities of network entities, making it susceptible to anonymity and untraceability attacks. Additionally, their scheme is vulnerable to quantum attacks and ESL attacks under the CK-adversary model.

B. Research Gap and Motivation

Current authentication protocols in IoV applications rely on integer factorization problem (IFP) based PKC or similar ECC-based security schemes. However, advancements in quantum computing and algorithms like Shor's algorithm [13] present significant threats to the security of these applications. Existing schemes, such as [4], [5], [6], [7], [12], among others, which are based on ECC, are particularly vulnerable to various attacks in the post-quantum era. To tackle these security issues, we propose a quantum-secure protocol for V2RSU communication in IoV applications, leveraging the complexity of the "Ring Learning With Errors (RLWE)" lattice problem.

C. Research Contributions

The key contributions of this paper are outlined as follows:

- This paper presents a lightweight security protocol aimed at safeguarding post-quantum communications in V2RSU interactions, offering protection against quantum attacks.
- A comprehensive security analysis demonstrates the protocol's robustness against various active and passive attacks in both classical and quantum environments.
- A real-time experimental setup using Raspberry Pi 4 devices is conducted to evaluate the computational overhead associated with different cryptographic primitives.
- A thorough comparative assessment with existing related schemes highlights the scalability and efficiency of the proposed solution in practical applications.
- A detailed network simulation using NS3 illustrates the performance of the proposed scheme, enhancing its reliability and effectiveness in IoV applications.

II. System Model

In this section, we present the network and threat models as part of the system model to visualize the network components and address security considerations during open channel communication.

1) Network Model: The system model comprises of three principal entities: the Trusted Registration Authority (TRA), Roadside Units (RSU)s, and electric vehicles equipped with OBUs. The architecture of this system model, referred to as V2RSU-PQS, is depicted in Fig. 1. Both the RSU and the OBU must register with the TRA to obtain the necessary authentication credentials and parameters. After exchanging the required information, the RSU and OBU will initiate the Authentication and Key Agreement (AKA) phase to establish secure communications.

2) Threat Model: In our proposed scheme, an EV with an OBU communicates with a RSU over an insecure public channel, which makes it vulnerable to information leakage. In this scenario, an unauthorized person could easily access the transmitted information by eavesdropping or launching active or passive attacks. Therefore, we adopted two well-recognized security threat models: 1) "Dolev-Yao (DY) model" [14] and 2) "Canetti and Krawczyk adversary (CK-adversary) model" [8]. According to the DY threat model, the adversary $\mathcal{Y}$ is

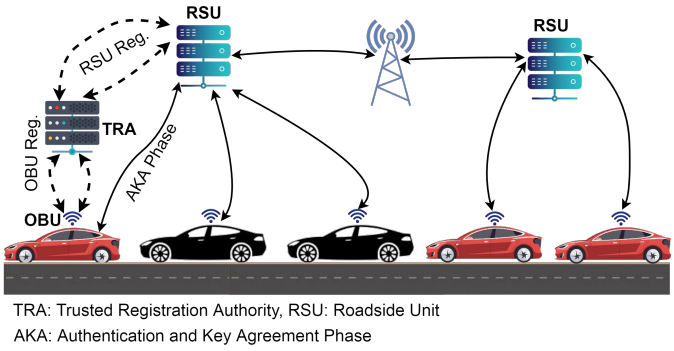

Fig. 1. Network model for V2RSU communication.

capable not only of intercepting communicated messages but also of manipulating them by modifying, inserting, or injecting information as they are transmitted between various entities within the network. In contrast, the CK-adversary model encompasses all the capabilities of $\mathcal{Y}$ described in the DY model, while additionally enabling $\mathcal{Y}$ to compromise "secret keys, credentials, and session states through session hijacking attacks during the session key establishment process". Furthermore, $\mathcal{Y}$ can launch power analysis attacks [15] on a physically compromised OBU to extract sensitive information from its insecure memory. In addition, $\mathcal{Y}$ has access to a quantum computer in a post-quantum scenario and can launch quantum attacks, such as lattice reduction attacks on the communication channels.

III. The Proposed Framework

In this section, we introduce our proposed model, V2RSU-PQS, aimed at enhancing V2RSU communication with post-quantum security in the IoV. The model consists of several phases, which are detailed below.

1) Initial Setup Phase: The initial setup phase is carried out by the RA, a "trusted registration authority", which determines the system parameters as follows.

• The RA selects a security parameter $n \in \mathbf{Z}$ that is power of 2 and a large prime number $q \in \mathbf{Z}$, where $\mathbf{Z}$ is a set of integers. The RA selects $\mathbf{Z}[x]$ and $\mathbf{Z}_q[x]$, representing the ring of polynomials over $\mathbf{Z}$ and $\mathbf{Z}_q$, respectively. In $\mathbf{Z}_q[x]$, the coefficients of all polynomials are reduced modulo q.

• The RA picks an irreducible $2n$-th cyclotomic polynomial over $\mathbf{Z}$ as $x^n + 1$ and defines a polynomial ring $\mathbf{R}$ as $\mathbf{R} = \frac{\mathbf{Z}[x]}{x^n+1}$. Additionally, it defines a quotient polynomial ring $\mathbf{R}_q$ as $\mathbf{R}_q = \frac{\mathbf{Z}_q[x]}{x^n+1}$, where the coefficients of the polynomials are reduced modulo q.

• The RA then generates a discrete Gaussian distribution χ_γ over $\mathbf{R}_q$, where $\gamma > 0$ is a real number and denoted as the standard deviation of the distribution [16].

• The SP selects a post quantum secure hash function $h(\cdot)$ as SHA-256, generates secret key $s \in \mathbf{R}_q$, and samples an unique polynomial $\alpha \in \mathbf{R}_q$ for each RSU_j.

• Finally, the RA broadcasts initial parameters $\{n, q, \alpha, \chi_\gamma, h(\cdot)\}$ and stores the s as a secret key into its memory.

2) OBU Registration Phase: The RA registers all OBU_is with their respective users by the following steps.

• The RA selects an unique identity id_i and temporary identity Tid_i for each OBU_i.

• The RA then calculates $h(id_i \,||s)$ and sends the registration credentials $\{id_i, Tid_i, h(id_i \,||s)\}$ to OBU_i.

• User picks a password pw_i, calculates $a_o = h(id_i \,||s) \oplus h(pw_i \,||id_i)$ and $b_o = h(id_i \,||pw_i \,||a_o)$.

• User then stores the registration credentials $\{id_i, Tid_i, a_o, b_o, h(\cdot)\}$ into its OBU_i's memory.

• The RA then loads the credentials $\{Tid_i, h(id_i \,||s)\}$ into associated RSU_j. After that, RA deletes $h(id_i \,||s)$ from its memory for resisting insider attacks.

3) Authentication and Key Agreement (AKA) Phase: In this phase, an OBU_i establishes a session key SK_{ij} $(= SK_{ji})$ with RSU_j using the following steps.

• An OBU_i selects a random nonce and error vector as $r_i, f_i \leftarrow \chi_\gamma$, a fresh timestamp TS_1, and then computes $a_i = \alpha.r_i + 2.f_i \in \mathbf{R}_q$, $b_i = h(Tid_i \,||h(id_i, s) \,||TS_1 \,||a_i)$. Next, OBU_i sends a request messages Msg_1 with $\{Tid_i, TS_1, a_i, b_i\}$ to the RSU_j via public channel.

• Upon receiving the message Msg_1 at a timestamp TS_1^*, RSU_j checks its freshness as $|TS_1^* - TS_1| < \Delta T$, where ΔT is the maximum message transmission delay. If it is valid, RSU_j then fetchs $h(id_i, s)$ corresponding to Tid_i from its database, and then computes $b_i' = h(Tid_i \,||h(id_i, s) \,||TS_1 \,||a_i)$, and verifies $b_i' = b_i$. If it is verified, RSU_j confirms Msg_1 is valid, picks $r_j,\ f_j \leftarrow \chi_\gamma$, and a fresh timestamp TS_2. Next, RSU_j computes $c_j = \alpha.r_j + 2.f_j \in \mathbf{R}_q$, $d_j = a_i.r_j$, $u_j = Cha(d_j)$, $w_j = Mod_2(d_j, u_j)$, and a session key SK_{ji} as $SK_{ji} = h(h(id_i, s) \,||w_j \,||c_j \,||a_i \,||Tid_i \,||TS_1 \,||TS_2)$. After that, RSU_j picks a new temporary identity Tid_i^n and encrypts it as $e_j = E_{SK_{ji}}(Tid_i^n \,||TS_2)$ with AES-CBC mode. Next, RSU_j computes a session key verifier as $SKV_{ji} = h(c_j \,||SK_{ji} \,||u_j \,||TS_1 \,||TS_2 \,||e_j)$, and sends a reply message Msg_2 as $\{SKV_{ji}, c_j, u_j, e_j, TS_2\}$ to OBU_i via public channel.

• After receiving Msg_2 from the RSU_j at a timestamp TS_2^*, OBU_i checks its freshness as $|TS_2^* - TS_2| < \Delta T$. If it is valid, OBU_i proceeds to compute $y_i = c_j.r_i$, $z_i = Mod_2(y_i, u_j)$, and a session key $SK_{ij} = h(h(id_i, s) \,||z_i \,||c_j \,||a_i \,||Tid_i \,||TS_1 \,||TS_2)$. Next, OBU_i decrypts e_j as $(Tid_i^n \,||TS_2) = D_{SK_{ij}}(e_j)$, and computes the session key verifier $SKV_{ij} = h(c_j \,||SK_{ij} \,||u_j \,||TS_1 \,||TS_2 \,||e_j)$. Next, OBU_i verifies it with the received one as $SKV_{ij} = SKV_{ji}$, and if it is verified, OBU_i updates Tid_i with new Tid_i^n. Next, OBU_i picks a new timestamp TS_3, and computes an acknowledgment $Ack = h(SK_{ij} || TS_3 || Tid_i^n || TS_2)$. Finally, OBU_i sends acknowledgment message Msg_3 with $\{Ack, TS_3\}$ to RSU_j via public channel.

• Once RSU_j receives Msg_3 at TS_3^*, verifies its freshness by the condition $|TS_3^* - TS_3| < \Delta T$. If it is valid, then RSU_j computes $Ack' = h(SK_{ji} || TS_3 || Tid_i^n || TS_2)$ and checks $Ack' = Ack$. If it verified, then RSU_j update new Tid_i^n. A detail summary of this phase is shown in Fig. 2.

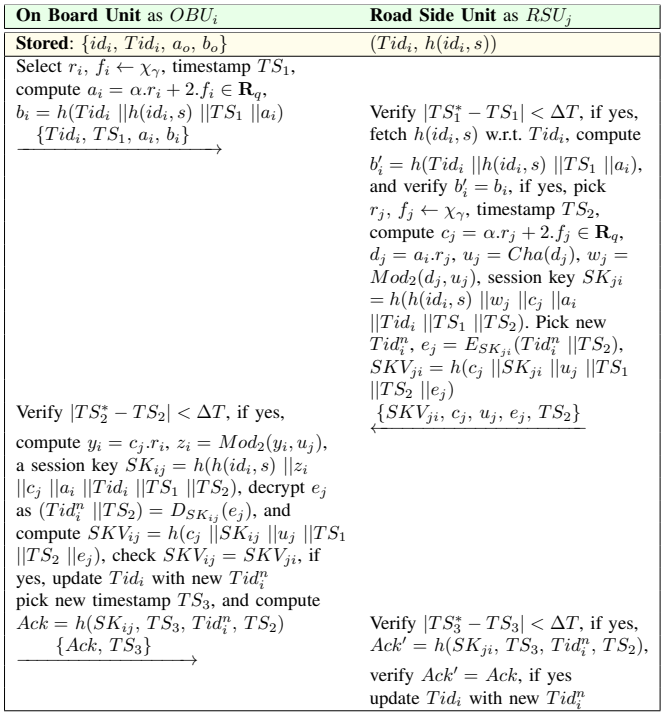

Fig. 2. Summary of AKA phase.

4) Dynamic OBU Addition Phase: A new electric vehicle with an onboard unit, say OBU_n, can be dynamically added to the network by the following registration process.

• The RA picks an unique identity id_n and temporary identity Tid_n for OBU_n. Next, the RA computes $h(id_n \,||s)$ and loads registration credentials $\{id_n, Tid_n, h(id_n \,||s)\}$ to the new OBU_n's memory.

• OBU_n chooses a password pw_n, calculates $a_n = h(id_n \,||s) \oplus h(pw_n \,||id_n)$, and $b_n = h(id_n \,||pw_n \,||a_n)$. OBU_n stores the credentials $\{id_n, Tid_n, a_n, b_n, h(\cdot)\}$ into its memory.

• Finally, the RA sends the credentials $\{Tid_n, h(id_n \,||s)\}$ into associated RSU_j via secure channel. After that, RA deletes $h(id_n \,||s)$ from its memory for resisting insider attacks.

IV. Informal Security Analysis

1) Replay Attack: During communication between the electric vehicle and the RSU, an attacker $\mathcal{Y}$ attempts to capture the messages $\{Tid_i, TS_1, a_i, b_i\}$, $\{SKV_{ji}, c_j, u_j, e_j, TS_2\}$, and $\{Ack, TS_3\}$, and then tries to re-transmit the older messages. However, the proposed scheme ensures the freshness of the messages by incorporating fresh timestamps and random nonces, which the receiver uses to verify the freshness of the received timestamps. If the timestamp is not fresh, the receiver discards the messages. Thus, the proposed scheme effectively resists replay attacks.

2) Man-in-the-Middle (MiTM) Attack: Employing the DY threat model, $\mathcal{Y}$ eavesdrops on the communicated messages and attempts to reconstruct a similar message on the fly, denoted as $Msg_1' = \{Tid_i', TS_1', a_i', b_i'\}$. To achieve this, $\mathcal{Y}$ selects a temporary identity Tid_i', generates a fresh timestamp TS_1', r_i', $f_i' \leftarrow \chi_\gamma$, and calculates $a_i' = \alpha.r_i' + 2.f_i'$. Next, $\mathcal{Y}$ tries to generate $b_i' = h(Tid_i' \,||h(id_i, s)\, ||TS_1' \,||a_i')$, but this is impossible without the secret value $h(id_i, s)$. Consequently, without this value, $\mathcal{Y}$ cannot successfully generate another valid message Msg_1. Similarly, $\mathcal{Y}$ cannot proceed with the other messages Msg_2 and Msg_3. Therefore, $\mathcal{Y}$ is incapable of launching a MiTM attack, demonstrating that the proposed scheme is secure against such attacks.

3) OBU Impersonation Attack: In this attack, on behalf of a legitimately registered OBU, $\mathcal{Y}$ pretends to be an authentic communicating party and tries to provide a legitimate request message in real-time, $Msg_1' = \{Tid_i', TS_1', a_i', b_i'\}$. To achieve this offline, $\mathcal{Y}$ selects a temporary identity Tid_i', generates a fresh timestamp TS_1', r_i', $f_i' \leftarrow \chi_\gamma$, and calculates $a_i' = \alpha.r_i' + 2.f_i'$. After that, $\mathcal{Y}$ tries to generate $b_i' = h(Tid_i' \,||h(id_i, s)\, ||TS_1' \,||a_i')$. It is noted that, the secret values $\{s, id_i\}$ are hidden with one-way hash function $h(\cdot)$. Therefore, finding the value of $h(id_i, s)$ is infeasible. Thus, $\mathcal{Y}$ will not progress without access to these values and the proposed scheme is safe from OBU impersonation attack.

4) Privileged-Insider Attack: During the device registration process, the trusted registration authority RA does not receive any sensitive information related to the OBU. Instead, the RA creates secrets for the OBU and uploads these credentials either over a secure channel or in offline mode to the OBU's memory. After receiving this information from the RA, OBU generates a password to securely store these credentials in its memory. Furthermore, after forwarding the registration details to both OBU and RSU, the RA removes the records of these entities from its own memory. As a result, an insider attacker cannot gain knowledge of the registration secrets and cannot be granted any privileges. Therefore, the proposed scheme is not vulnerable to such attacks.

5) Physical OBU Capture Attack: In this scheme, OBUs operate in geographically diverse areas where the physical security of electric vehicles may be compromised. In such hostile environments, $\mathcal{Y}$ could potentially capture the OBUs. Subsequently, $\mathcal{Y}$ could launch side-channel attacks, utilizing quantum computing capabilities, such as power analysis attacks [15], to extract stored data from the compromised OBUs. It is important to note that each OBU has a unique set of stored credentials. Therefore, if $\mathcal{Y}$ captures one OBU, it will not expose any secret credentials related to other non-compromised OBUs. Consequently, the proposed scheme remains resilient against such attack.

6) Ephemeral Secret Leakage (ESL) Attack: In this proposed scheme, the RSU_j constructs a session key SK_{ji} as $SK_{ji} = h(h(id_i, s)\, ||w_j \,||c_j \,||a_i \,||Tid_i \,||TS_1 \,||TS_2)$, where $c_j = \alpha.r_j + 2.f_j \in \mathbf{R}_q$, $d_j = a_i.r_j$, $u_j = Cha(d_j)$, and $w_j = Mod_2(d_j, u_j)$. This SK_{ji} is generated with short-term (ephemeral) secrets $\{r_j, f_j, r_i, f_i\}$ and long-term secrets $\{id_i, s\}$. Therefore, generating a session key requires both short-term and long-term secrets. If $\mathcal{Y}$ can reveal these credential secrets, then they would be able to generate the correct session key. According to the CK-adversary model, even if $\mathcal{Y}$ compromises a session key by gaining access to a session

state, this will not affect previous or subsequent sessions. This is because the randomness of timestamps and random secrets ensures that session keys remain intrinsically distinct across different sessions. Similarly, $\mathcal{Y}$ cannot generate a valid session key SK_{ij}. Thus, the proposed scheme is secure against such attacks under the CK-adversary model.

7) Anonymity and Untraceability: The true identities of the communicating parties remain hidden over the public channel within the messages $\{Msg_1, Msg_2, Msg_3\}$ in the proposed scheme. These identities, essential for constructing the session key, are obscured by utilizing one-way hash function $h(\cdot)$. As a result, $h(\cdot)$ prevents the recovery of the actual identities from these messages, thereby maintaining the anonymity of OBUs in the scheme. Furthermore, since the transmitted messages are generated with random nonces and fresh timestamps, they exhibit dynamic characteristics in each session. The temporal identity also changes with each session, ensuring that the messages possess distinct and unique features for different interactions. Therefore, $\mathcal{Y}$ is unable to trace the recipients of the messages. Thus, the proposed scheme ensures the property of untraceability.

8) Quantum Attack: The security of the proposed scheme relies on the difficulty of the RLWE lattice problem. This problem asserts that, given a polynomial and a collection of polynomial pairs in the form $(x, y = x.f + 2.e) \in \mathbf{R}_q \times \mathbf{R}_q$, it is challenging to identify the unknown polynomials f and e drawn from a discrete Gaussian distribution, that is, $f, e \in \chi_\gamma$. Thus, determining the small error vector e in the noisy polynomial equation within the polynomial ring $\mathbf{R}_q$ constitutes a hard problem, making it difficult for both classical and quantum algorithms to solve in polynomial time. In our proposed scheme, we ensure that the vectors $\{r_i, f_i, r_j, f_j\}$ are sufficiently large so that $\mathcal{Y}$ cannot discover these vectors through lattice reduction attacks within polynomial time. For practical implementation, larger parameters can be chosen, similar to the methodology employed by Gao et al. [17], to establish lattice-based parameters that provide 200-bit classical and 80-bit quantum security. This approach utilizes a discrete Gaussian distribution χ_γ with a standard deviation of $\gamma = 3.192$, a polynomial degree of $n = 1024$, and a large prime modulus of $q = 1073479681$ (30 bits). To ensure both high statistical quality and security, the statistical distance between the sampled distribution and the discrete Gaussian distribution is maintained at 2^{-128}. To achieve 256-bit security against quantum threats, one should consider increasing n to at least 2048 and q to a larger value, such as 2^{64} or beyond. Depending on the specific security requirements and trade-offs of the application, one can choose the security parameters accordingly.

V. Comparative Analysis

In this section, we systematically evaluate and juxtapose the efficacy of the proposed framework against other pertinent competing frameworks, including those by Vasudev et al. [11], Xie et al. [12], Wang et al. [7], Mishra et al. [9], and Rewal et al. [10].

A. Communication Costs Analysis

The following assumptions about the sizes of different data components are made in order to calculate the communication cost: 160 bits, 32 bits, 160 bits, 256 bits, and 320 bits, for identity or temporal-identity, timestamp, random nonce, hash digest (using the SHA-256 hashing technique), and elliptic curve points, respectively. Additionally, we consider the polynomials in $\mathbf{R}_q$ to be 4096 bits and $Cha(\cdot)$ and $Mod_2(\cdot, \cdot) \in \{0, 1\}$. Three messages are sent over the open channel in the proposed scheme: $M_1 = \{Tid_i, TS_1, a_i, b_i\}$, $M_2 = \{SKV_{ji}, c_j, u_j, e_j, TS_2\}$, and $M_3 = \{Ack, TS_3\}$. For a total of 9473 bits, these messages require (160 + 32 + 4096 + 256) = 4544 bits, (256 + 4096 + 1 + 256 + 32) = 4641 bits, and (256 + 32) = 288 bits, respectively. Table I shows that the proposed scheme incurs lower communication costs compared to the schemes in [9] and [10]. Although the proposed scheme has higher costs compared to [7], [11], and [12], these schemes do not meet all necessary security requirements, as discussed in Section V-C.

TABLE I
COMPARATIVE ANALYSIS ON COMMUNICATION COSTS

Scheme	No. of messages	Total cost (in bits)
Wang et al. [7]	6	4800
Mishra et al. [9]	3	14018
Rewal et al. [10]	4	18626
Vasudev et al. [11]	4	2560
Xie et al. [12]	3	3360
Proposed scheme	3	9473

TABLE II
COMPARATIVE ANALYSIS ON COMPUTATION COSTS

Scheme	OBU_i/smart device	RSU_j/Server
Wang et al. [7]	$9T_h + 5T_{ecm}$ ≈ 8.2243 ms	$18T_h + T_{ecm}$ ≈ 0.9222 ms
Mishra et al. [9]	$8T_h + 4T_{gs} + 2T_{sm} +$ $3T_{pm} + 2T_{ma} + 2T_{cha}$ ≈ 2.553 ms	$6T_h + T_pm$ ≈ 0.255 ms
Rewal et al. [10]	$8T_h + 4T_{gs} + 2T_{sm} +$ $2T_{pm} + 2T_{ma} + T_{cha}$ ≈ 2.552 ms	$6T_h$ ≈ 0.254 ms
Vasudev et al. [11]	$6T_h \approx 1.9122$ ms	$11T_h \approx 0.4664$ ms
Xie et al. [12]	$6T_h + 5T_{ecm} + T_{eca}$ ≈ 7.4149 ms	$5T_h + 5T_{ecm} + 2T_{eca}$ ≈ 1.0528 ms
Proposed scheme	$4T_h + T_{sdec} + 2T_g +$ $T_{sm} + T_m + T_{ma}$ ≈ 1.368 ms	$4T_h + T_{senc} + 2T_g$ $+T_m + T_{ma} + T_{sm}$ $+T_{cha} \approx 0.187$ ms

B. Computation Costs Analysis in Milliseconds (ms)

Let T_h represent the time needed to execute a one-way hash function, T_{senc}/T_{sdec} the time needed to encrypt and decrypt data using AES, and T_{eca}/T_{ecm} the time needed to add and multiply elliptic curve points, respectively. Furthermore, let T_g, T_{sm}, T_m, T_{ma}, and T_{cha} represent the sampling time from χ_γ, one component-wise multiplication in $\mathbf{R}_q$, one component-wise multiplication in $\mathbf{R}_q$, one component-wise multiplication and addition operation in $\mathbf{R}_q$, and the characteristic function in $\mathbf{R}_q$, respectively.

In our experimental setup, the execution times for traditional cryptographic primitives are as follows: T_h is 0.0424 ms and 0.3187 ms, T_{senc} is 0.0173 ms and 0.0926 ms, T_{sdec} is 0.0163 ms and 0.0945 ms, T_{eca} is 0.0229 ms and 0.1509 ms, and T_{ecm} is 0.1590 ms and 1.0712 ms, for the RSU_j (configured with "Ubuntu 22.04 LTS, 16 GB of memory, Intel® Core™ i7-9750H CPU @ 2.60GHz with 6 cores and 12 threads, 64-bit OS, and a 256 GB SSD") and OBU_i (using a "Raspberry Pi 4 Model B with a 64-bit CPU, 1.4 GHz Quad-core processor, 4 cores, 1 GB RAM, and Ubuntu 20.04 LTS 64-bit OS") environments, respectively. For lattice-based primitives, execution times were sourced from Feng et al. [18]. To assess the computational cost, we focus on the AKA phase, where an OBU_i has a computational cost of approximately $4T_h + T_{sdec} + 2T_g + T_{sm} + T_m + T_{ma} \approx 1.368$ ms, while an RSU_j has a computational cost of approximately $4T_h + T_{sdec} + 2T_g + T_{sm} + T_m + T_{ma} + T_{cha} \approx 0.187$ ms. Table II provides a computational cost comparison of the proposed scheme with other current schemes, showing that our scheme has lower communication costs for OBU_i than other existing schemes.

TABLE III
COMPARATIVE ANALYSIS ON VARIOUS FS ATTRIBUTES

Attribute (FS)	[7]	[9]	[10]	[11]	[12]	Proposed scheme
FS_1	×	✓	✓	✓	✓	✓
FS_2	✓	✓	✓	✓	✓	✓
FS_3	✓	✓	✓	✓	✓	✓
FS_4	✓	✓	✓	✓	✓	✓
FS_5	✓	✓	✓	✓	✓	✓
FS_6	✓	✓	✓	✓	✓	✓
FS_7	×	✓	✓	×	×	✓
FS_8	✓	×	×	×	×	✓
FS_9	✓	✓	✓	✓	✓	✓
FS_{10}	✓	×	×	×	×	✓
FS_{11}	×	✓	✓	×	×	✓

FS_1: Replay attack; FS_2: MITM attack; FS_3: Mutual authentication; FS_4: Key Agreement; FS_5: Device impersonation attack; FS_6: "Device physical capture attack"; FS_7: "ESL attack under the CK-adversary model"; FS_8: Anonymity and untraceability; FS_9: Privileged-insider attack; FS_{10}: Node addition phase; FS_{11}: Quantum attack
✓: "a scheme is secure or it supports an attribute"; ×: "a scheme is insecure or it does not support an attribute; N/A: means Not applicable in a scheme".

C. Functionality and Security (FS) Attributes

The proposed method satisfies all the functional and security requirements, as shown in Table III, offering a strong security solution for post-quantum communication in IoV. On the other hand, existing related scheme that are currently in use fall short of the required level of security.

D. Network Simulation using NS3

In this section, we measure the network performance of the proposed scheme compared to competitive schemes in terms of "throughput", "packet delivery ratio (PDR)", and "end-to-end (E2E) delay" using Network Simulator 3 (NS3). These performance metrics are evaluated based on the communication messages involved in the authentication and key agreement processes of the schemes. The following environmental setup was used for this simulation: the operating system is Ubuntu 20.04.6 LTS, 64-bit, with a simulation time of 1300 seconds. The network coverage area measures 100 m x 100 m, and there is 10 electric vehicles and one RSU. The routing protocol employed is OLSR, while the MAC protocol is IEEE 802.11b. The distance between the electric vehicle and the RSU ranges from 10 m to 50 m, and the mobility model utilized is the RandomDirection2dMobilityModel (for more details, please see ns-3 Manual Release ns-3-dev).

1) Effect on Throughput: Throughput (T_p) is typically calculated using: $T_p = \frac{T_r}{T_{sm}}$, where T_r is the "total number of received packets" and T_{sm} is the "simulation time". Figure 3 (A) shows a comparison of the throughput of the proposed scheme with related schemes, indicating that the proposed scheme achieves the highest throughput compared to those of Vasudev et al. [11], Xie et al. [12], and Wang et al. [7]. On the other hand, the proposed scheme achieves lower throughput compared to the schemes of Mishra et al. and Rewal et al., as these schemes require larger message sizes.

2) Effect on Packet Delivery Ratio (PDR): Monitoring the effect on PDR is essential for evaluating and enhancing network performance (to track network congestion), ensuring reliable communication, and providing a satisfactory user experience. It is the "ratio of the total number of received packets and total number of sent packets". Figure 3 (B) shows that the proposed schemes have PDR values of $\approx 78.87\%$, while the PDR values from [7], [9], [10], and [11] are higher. In contrast, the proposed scheme has a lower PDR value of [12] which have PDR value as $\approx 81.23\%$

3) Effect on E2E Delay: It is calculated as the "total time taken for a packet to travel from the source to the destination". In our measurements, the proposed scheme has an E2E delay of ≈ 0.0429212 seconds, which is lower than that of the schemes by [9] and [10]. This is reflected in Fig. 3 (C).

VI. CONCLUSION

In this article, the proposed scheme establishes a lightweight security protocol for V2RSU communication within the green IoV, specifically engineered to endure quantum attacks. This protocol exhibits strong resistance to various threats while ensuring efficiency in practical applications. Findings from real-time experiments and network simulations using NS3 validate its durability and scalability, positioning it as a valuable advancement in secure vehicular communications in the post-quantum era. Overall, this scheme plays a crucial role in improving the security of green vehicular communications in a post-quantum context, paving the way for safer and more resilient ITS.

ACKNOWLEDGMENTS

This research was supported by the National Research Foundation, Singapore and Infocomm Media Development Authority under its Future Communications Research Development Programme, under grant FCP-NUS-RG-2022-019. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and

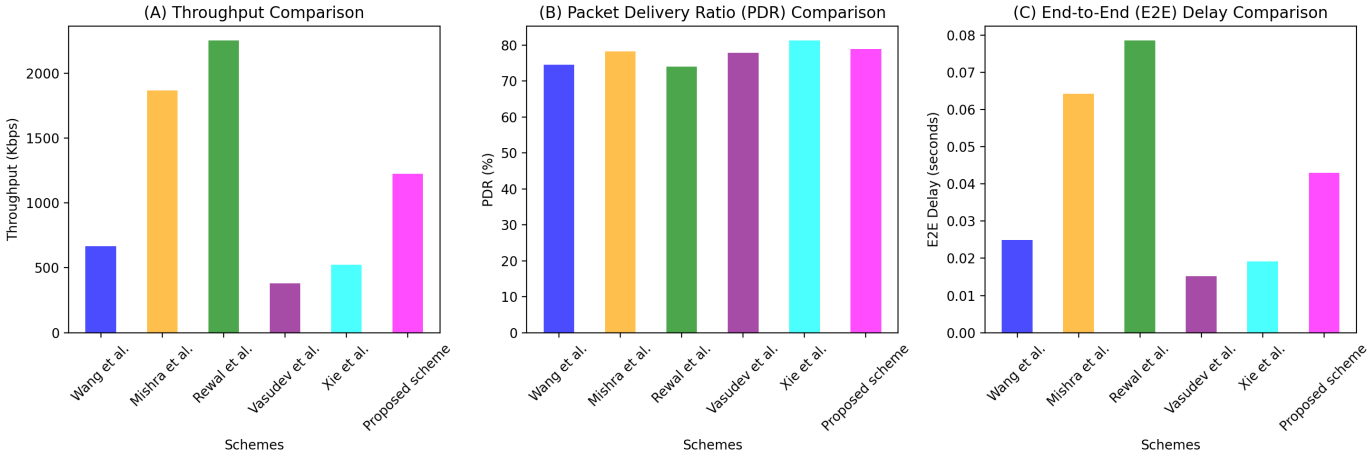

Fig. 3. Comparison of network performance using NS3.

do not reflect the views of National Research Foundation, Singapore and Infocomm Media Development Authority. This work was also partially funded by Brazilian National Council for Scientific and Technological Development - CNPq, via Grant No. 306607/2023-9.

REFERENCES

[1] J. Miao, Z. Wang, X. Ning, A. Shankar, C. Maple, and J. J. P. C. Rodrigues, "A UAV-Assisted Authentication Protocol for Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 8, pp. 10 286–10 297, 2024.

[2] Q. Xie, Z. Ding, and P. Zheng, "Provably secure and anonymous v2i and v2v authentication protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7318–7327, 2023.

[3] J. Wang, K. Zhu, and E. Hossain, "Green Internet of Vehicles (IoV) in the 6G Era: Toward Sustainable Vehicular Communications and Networking," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 391–423, 2022.

[4] Q. Wang, Y. Li, Z. Tan, N. Fan, and G. Yao, "Conditional privacy-preserving authentication scheme for V2V communication without pseudonyms," *Journal of Information Security and Applications*, vol. 78, p. 103616, 2023.

[5] H. J. Nath and H. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in VANET," *Computer Communications*, vol. 192, pp. 357–372, 2022.

[6] S. Zhang, Y. Liu, Y. Xiao, and R. He, "A trust based adaptive privacy preserving authentication scheme for VANETs," *Vehicular Communications*, vol. 37, p. 100516, 2022.

[7] C. Wang, D. Wang, Y. Duan, and X. Tao, "Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2961–2976, 2023.

[8] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[9] D. Mishra, M. Singh, P. Reval, K. Pursharthi, N. Kumar, A. Barnawi, and R. Rathore, "Quantum-safe Secure and Authorized Communication Protocol for Internet of Drones," *IEEE Transactions on Vehicular Technology*, pp. 1–10, 2023, doi: 10.1109/TVT.2023.3292169.

[10] P. Rewal, M. Singh, D. Mishra, K. Pursharthi, and A. Mishra, "Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices," *Journal of Information Security and Applications*, vol. 75, p. 103505, 2023.

[11] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709–6717, 2020.

[12] Q. Xie, Z. Ding, and P. Zheng, "Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7318–7327, 2023.

[13] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[14] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[15] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[16] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[17] X. Gao, J. Ding, L. Li, and J. Liu, "Practical Randomized RLWE-Based Key Exchange Against Signal Leakage Attack," *IEEE Transactions on Computers*, vol. 67, no. 11, pp. 1584–1593, 2018.

[18] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2775–2785, 2019.