# Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles

Daya Sagar Gupta, Arijit Karati, *Senior Member, IEEE*, Walid Saad *Fellow, IEEE*, and Daniel Benevides da Costa *Senior Member, IEEE*

***Abstract*—The so-called Internet of Vehicle (IoV) systems will interconnect numerous vehicles to communicate significant information through an Internet of Things (IoT) enabled network. It has emerged as a promising system wherein various data authentication techniques have been introduced using clumsy certificate management and Diffie-Hellman (DH) assumption. However, in the presence of quantum cryptanalysis, DH-type problems could be solved in polynomial-time. In this paper, a novel certificateless data authentication protocol is designed, enabling security features in open wireless communication in the IoV. The proposed protocol resists a quantum attack using lattice cryptography. Further, a reliable blockchain mechanism is shown to provide vehicles' trustworthiness in batch data verification. Rigorous formal analysis shows the ability of the proposed algorithm to resist existential unforgeability against the chosen-message attack. Nonetheless, the developed protocol supports other essential security functionalities, including unlikability, conditional-traceability, anti-replay, and data authenticity. Performance analysis exhibits the simulation orchestration and shows the way the proposed protocol outperforms other related techniques in energy consumption, data computation, communication, and cryptographic key storage overheads.**

***Index Terms*—Security; Privacy; Authentication; Internet of Vehicles; Blockchain; Lattice-based cryptography.**

## I. Introduction

TRANSPORTATION systems in many nations are becoming increasingly expanded to their limits as the number of users continues growing [1]. Recent advances in computer and networking technology led to the emergence of a diverse range of smart devices used in an Internet of Vehicle (IoV) [2] system. The IoV creates a more dependable and favorable environment through device connectivity and interoperability. It unites two technological insights [3]: a) vehicle's intelligent networking and b) secure communication, and focuses on the integration of objects (such as humans, vehicles, things, networks, and surroundings) to create an intelligent network that supports computing and communication capabilities. Besides, the IoV network provides services (such as global traffic competence and administration support depending on corruption levels, highway conditions, traffic congestion, or vehicle protection services) for major cities or even an entire country.

Fig. 1 depicts a range of communication links in a typical IoV environment. Here, "intelligent" vehicles, outfitted with embedded processors and wireless transmission technologies in onboard units (OBUs), interact with each other through specific communication links in a vehicle-to-everything (V2X) environment in which a vehicle could be connected to another vehicle, roadside unit, infrastructure, pedestrian, or network infrastructure. A vehicle toiled as an information receiver alerts others of what it observes to assist vehicles dynamically to renew certain critical information. Such pieces of information are driving direction (fuel preservation), obstruction, or collision evasion (traffic monitoring and safety), a post-crash notification (reliable feedback). Due to extensive data exchange, it is necessary to boost the roadside unit's (RSU's) processing speed and ensure the validity and authenticity of data transmitted through public channels. Alternatively, during interaction with another node using V2X links, sensitive data could be breached due to a range of public communication. Therefore, certain data security vulnerabilities, e.g., replay attack, identity tracing attack, denial of service attack, etc., in the IoV, may be introduced due to attackers' distinct capabilities. We group such attackers into malicious and semi-trusted. A *malicious attacker* is fully vulnerable while a *semi-trusted attacker* is partially-trusted, always curious about the actual content but never directly attacking the system. In the presence of such attackers, data in the IoV must be unbreachable, reliable, and truthful, as lives and essential judgments may rely on it. In this respect, several batch verification procedures have been proposed [4]–[6]. One verification approach is ID-based batch verification, which eliminates the need for cumbersome certificate management. However, this type of batch verification cannot withstand some recent attacks, including data modification, vehicle impersonation, and futuristic quantum attack due to the *key-escrow* problem and security under the Diffie-Hellman (DH)-type assumption. Moreover, its performance degrades due to inadequate usage of time-consuming bilinear pairing operations. Besides, it is not a



Manuscript received XXXXXXXXXXXXXXX; revised XXXXXXXXXX XXXXXXXXXX; accepted XXXXXXXXXXXXXXX. This work was supported in part by the Taiwan Ministry of Science and Technology under Grant MOST 110-2222-E-110-006- and administered by CANSEC-LAB@NSYSU in Taiwan. It is supported in part by the Indian Rajiv Gandhi Institute of Petroleum Technology under Grant P-2106. (Corresponding author: Arijit Karati.)

A. Karati is with Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan (e-mail: arijit.karati@mail.cse.nsysu.edu.tw).

D. S. Gupta is with the Department of Computer Science and Engineering, Rajiv Gandhi Institute of Petroleum Technology Jais, Amethi, 229304, India (e-mail: dayasagar.ism@gmail.com, dsgupta@rgipt.ac.in)

W. Saad is with Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech, Arlington, VA, USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, South Korea (e-mail: walids@vt.edu).

D. B. da Costa is with the Intelligent Wireless Communications (IWiCom) Research Group, Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan, and also with the Department of Computer Engineering, Federal University of Ceará, Sobral-CE 62010-560, Brazil (e-mail: danielbcosta@ieee.org).

This article has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the author.
Digital Object Identifier XX.XXXX/TVT.2022.XXXXXXX

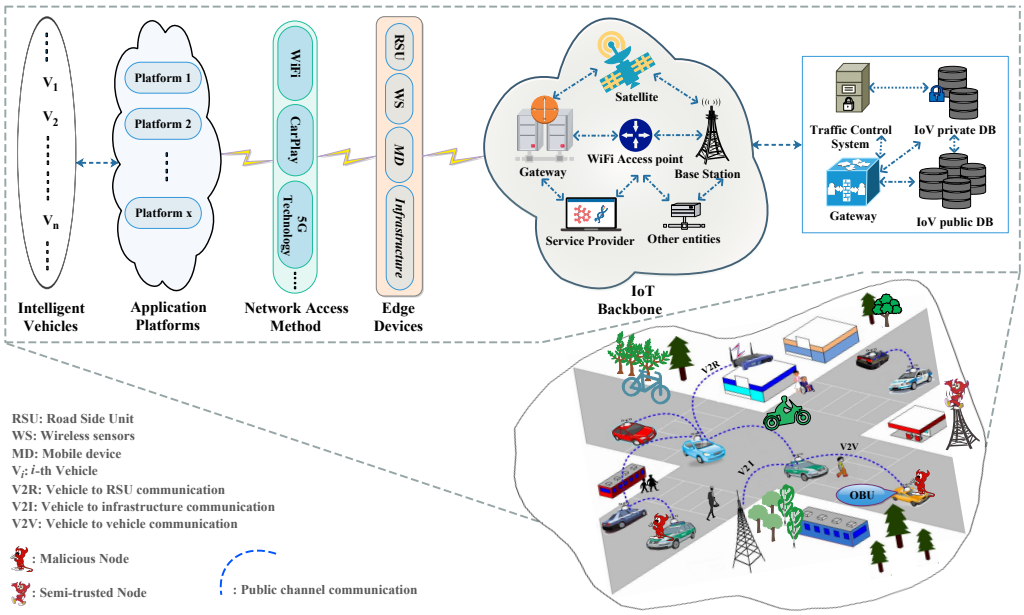



Fig. 1: A typical overview of the Internet of Vehicles

suitable technique to realize data security and privacy in IoV. The advent of quantum computing addresses many classical cryptographic techniques, leading to public-key cryptography innovations, vulnerable in the realization of modern technology [7]. Lattice-based cryptography is a potential post-quantum approach in its application to conventional and upcoming security challenges such as key exchange, encryption, and digital signature. Because of their inherent characteristics, lattice-based cryptographic techniques provide advanced security features against quantum cryptanalysis while being easy to implement.

Another kind of data verification is certificate-based batch verification, which checks the vehicle's authenticity using a public key (pseudonymous) certificate provided by trustworthy certificate authorities. However, this type of trust management necessitates a substantial amount of certificate storage and administration overhead when communicating with RSUs and other organizations. To overcome such a barrier, we can utilize blockchains as a possible way to introduce "trust" and "autocheck" nodes into the IoV [8]. A blockchain policy is an append-only database managed by peer-to-peer network nodes. The overhead associated with blockchain-based trust management is significantly lower than that associated with certificate-based trust management. Each node in a blockchain associated with the network's routing rule maintains the connections to adjacent peers, delivers and validates signed messages, and synchronizes data blocks. Therefore, a blockchain's topology ensures network users immutable, decentralized, autonomous and contractual "benefits". By integrating auto-trust into the IoV, a blockchain can be seen as a robust and scalable mechanism that automatically monitors message trustworthiness, vehicle performance, and further traces regular communication reports [9]. In the proposed protocol, we leverage lattice-based operations to ensure data dependability in the IoV, while a blockchain is considered to assure vehicle validity. Now, we mention several key security requirements that the proposed protocol fulfills.

### A. IoV Security Requirements

If an intruder logs false information about a vehicle's position or traffic status, it may face negative repercussions, such as traffic congestion and road accidents [10]. Given security and privacy concerns, the following requirements must be satisfied:

- *Message authentication:* The validity and integrity of messages sent by a node can be verified efficiently.
- *Conditional anonymity*: The vehicle's real identity (e.g., visible serial number) should only be intimated to authorized registration authority (RA). No third party onlooker can disrupt driver privacy during communication.
- *Traceability*: A RA can trace the real identity of any vehicle, i.e., identification of a malicious node through the examination of transmitted messages. This characteristic indicates both privacy and accountability when bogus messages appear in violations or accidents.
- *Un-linkability:* No malicious entity can link a vehicle's activities to its transmitted messages, i.e., no relationship among messages sent by a vehicle from its activities.
- *Resistance of quantum attack:* Security of an IoV application must remain against quantum attacks, i.e., the protocol must resist a cryptanalytic attack by quantum computers.
- In addition to the above requirements, the protocol resists other cybertreats such as *modification*, *man-in-the-middle*, *impersonation*, *stolen verifier table*, and *replay* attacks.

### B. Prior works with their limitations

In recent years, vehicular communication has received much attention from researchers in industry and academia. The authors in [11] presented an extensive survey regarding the uses of blockchain in an IoV. They explored IoV scenarios in which advanced blockchain can be used. The authors in [12] proposed a blockchain-based IoV trust management system focused on reputation values. The work in [13] used a smart contract-based blockchain for building a trust management mechanism for the IoV. The authors in [14] provide an IoV authentication scheme

using a blockchain consensus algorithm. Furthermore, many certificate-based batch verification techniques in [15]–[17] were designed to deal with vehicles' real identities privacy, unlinkability, data injection attack. However, most of these schemes are not suitable for the IoV due to the need for cumbersome certificates, high storage burden of cryptographic keys, and time-consuming operations during rapid data communication between vehicles and RSU. One may note that for heterogeneous devices, such as lightweight OBU, computation and storage overheads are important. Moreover, public key infrastructure (PKI)-based authentication exhibits key weaknesses, such as a) maintaining a decent number of certificates and secret keys to preserve vehicles' privacy, b) managing ample space to save all the certificates, and c) practicing high computation and communication burdens to manage certificates (e.g., query, issue, or revocation). To mitigate the burden of certificate management, the authors in [18] employed the concept of ID-based cryptography (IBC) to design a new privacy preservation technique. Trust management was provided by considering the vehicle's publicly verified identity as a public key. Since then, several ID-based techniques have been introduced for vehicular networks. For instance, the work in [19] proposed an approach to enhance the vehicle privacy of [18], but it was found to be vulnerable to impersonation attack by the authors in [20]. Subsequently, the authors proposed two ID-based privacy preservation authentications without bilinear pairings in [21] and [22]. Although the performance was enhanced, the works were vulnerable under *key-escrow* in vehicular communication. Recently, the authors in [23] designed a ciphertext-policy attribute-based encryption for certifying vehicles while supporting data revocation for the vehicles that no longer share data. The work in [24] introduced a mutual authentication with decentralized key management for vehicular ad-hoc network (VANET) with blockchain. Most of the works in [18]–[20] that look at certificate-based and ID/attribute-based batch verification methods are still vulnerable to quantum attacks. This is because the security of such systems depend on the hardness of the DH-type assumption. Lattice-based encryption was recently proposed as an alternate approach to resisting such quantum attacks as described in [25] and [26].

To address the issues raised above, the authors of [27] presented a practical lattice-based signature for embedded systems. Meanwhile, the authors of [28] presented a lightweight lattice-based homomorphic privacy-preservation scheme for home area networks that ensures message integrity and client privacy. Both systems are, however, incompatible with vehicle communication. The work in [29] developed lattice-based anonymous authentication without tamper-proof devices, achieving the necessary security and privacy on VANETs. However, the solution of [29] results in a high computation cost during data transfer. The work in [30] proposed the first lattice-based double-authentication-preventing ring signature. It was used to develop a novel privacy-preserving authentication for VANETs, offering the potential for security against a quantum attack. This approach, however, necessitates a considerable amount of energy and storage in VANET nodes and fails to meet security criteria such as un-linkability, replay attack, and stolen verifier assault. The authors of [31] devised a conditional privacy-preserving authentication scheme that was resistant to quantum attacks in the random oracle model. However, the solution [31] is not energy-efficient and hence unsuitable for lightweight IoV devices. The developers of [32] have created a lattice-based ring signature on VANETs. The method enables unconditional identity privacy preservation, message authentication, and vehicle location privacy; nevertheless, it lacks key tracing properties. The developers of [33] created a lattice-based signcryption for electric vehicles. However, due to the expensive encryption overhead and substantial storage expense, the scheme cannot be applied in actual IoV applications. Furthermore, this approach is subject to assaults on traceability, identity breach, and replay.

### C. Motivations and Salient Features

Due to the open nature of wireless links, malicious nodes may intercept, replay, and even tamper with the transmitted data. According to Section I-B, most earlier works [15]–[17] consider a certificate-based method, which is inefficient for the IoV context owing to the cost of certificate administration. Some techniques, such as [19]–[22], provided an ID-based data verification solution that necessitates time-consuming bilinear pairing procedures and cannot overcome the *key escro*w problem. Further, these approaches prove the security resistance under DH-type assumptions. It is known that the DH-type assumptions-based schemes are vulnerable against the evolving quantum attack. Lattice-based operations are robust to the quantum attack and are efficiently implementable. Aside from that, protecting vehicle privacy is a strict obligation in the IoV. Blockchain technology has the potential to handle trust management concerns, provide an automatic monitor of vehicle integrity, and provide traceable dependable communication. Motivated by the IoV's security and privacy concerns, we pose the following question: "Could we develop a quantum-resistant authentication system for the IoV that maintains vehicle privacy through blockchain?"

The major contribution of this paper is, thus, a novel quantum -defended blockchain-assisted conditional privacy-preserving data authentication (QBCPDA) technique for the IoV that provides secure and authentic batch verification. Within the context of this new framework, we make the following contributions:

- The QBCPDA protocol incorporates lattice cryptography capabilities to protect against data forgery and quantum assaults. It enables authentic batch verification in addition to data sharing, security, and credibility. Moreover, the vehicles' public information is protected using the blockchain approach to guarantee the vehicles' privacy quickly.
- Considering different adversaries and their attacks in the IoV, a formal security model is given and further adopted to show the semantic security of the proposed protocol.
- The QBCPDA satisfies the unlinkability, traceability, and message authentication. Besides, it can thwart man-in-the-middle, replay, node impersonation, and quantum attacks.
- The QBCPDA under a suitable environment is shown to outperform other related techniques in incurred computation, communication storage, and energy overheads.

The rest of this paper is arranged as follows. Section II gives some preliminaries, and Section III presents the QBCPDA protocol in detail. Section IV analyzes the security of the QBCPDA. Section V provides performance analysis and comparison to other protocols. Finally, conclusions are drawn in Section VI.

## II. Technical Background

Some useful preliminaries for the proposed protocol are discussed in this section. Table I lists various symbols.

### A. Notion of Lattice

Let $\boldsymbol{x} = \{\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n\}$ be a set of linearly independent vectors in *m*-dimensional Euclidean space $\mathcal{R}^m$ that generates a lattice $\mathcal{X}(\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n) = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i : \alpha_{i\in[1,n]} \in Z$ where $\boldsymbol{x}_{i\in[1,n]} \in \mathcal{R}^m$ are basis vectors, and *m* and *n* are the dimension and rank of $\mathcal{X}$, respectively [34]. The minimum distance of $\mathcal{X}$ is $d_{\min}(\mathcal{X}) = \min_{\boldsymbol{x}\in\mathcal{X}\setminus\{0\}} \parallel \boldsymbol{x} \parallel$. Further, a set of linearly independent vectors which generates $\mathcal{X}$ is known as basis of $\mathcal{X}$. The properties of basis vectors are

- Every $\mathcal{X}$ must have at least one basis.
- Basis of $\mathcal{X}$ is not unique.

**Definition 1.** Let $\boldsymbol{X} = [\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n] \in Z^{m\times n}$ be a basis of a lattice, where basis vectors are the columns of $\boldsymbol{X}$. Lattice $\mathcal{X}$ in a $m$-dimensional Euclidean space $\mathcal{R}^m$ is denoted as $\mathcal{X}(\boldsymbol{X}) = [\boldsymbol{X}\boldsymbol{t} : \boldsymbol{t} \in Z^n]$ where $\boldsymbol{X}\boldsymbol{t}$ refers a matrix-vector multiplication.

**Definition 2** (Shortest Vector Problem (SVP))**.** Given lattice $\mathcal{X}$ and its basis $\boldsymbol{X} \in Z^{m\times n}$, finding a non-zero vector $\boldsymbol{t} \in \mathcal{X}$ such that $\parallel \boldsymbol{t} \parallel = d_{min}(\mathcal{X})$ is computationally infeasible.

**Definition 3** (Closest Vector Problem (CVP))**.** Given lattice $\mathcal{X}$, basis $\boldsymbol{X} \in Z^{m\times n}$ and vector $\boldsymbol{u}(\notin \mathcal{X})$, finding a non-zero vector $\boldsymbol{t} \in \mathcal{X}$ where $\parallel \boldsymbol{u}-\boldsymbol{t} \parallel = d_{min}(\mathcal{X})$ is computationally infeasible.

### B. Properties of q-ary Lattice

A lattice $\mathcal{X}$ $(Z_q^n \subseteq \mathcal{X} \subseteq Z^n)$ supporting modular arithmetic is called *q-ary* lattice for an integer $q$.

**Definition 4.** For a matrix $\boldsymbol{X} \in Z_q^{m\times n}$ under modulo $q$, two different *q-ary* lattices $\mathcal{X}_q^{\perp}$ and $\mathcal{X}_q$ can be mentioned as:

$$\mathcal{X}_q^{\perp} = \{\boldsymbol{t} \in Z^n : \boldsymbol{X}\boldsymbol{t} = \boldsymbol{0} \bmod q\}$$
$$\mathcal{X}_q = \{\boldsymbol{t} \in Z^n \text{ and } \boldsymbol{u} \in Z^m : \boldsymbol{t} = \boldsymbol{X}^T\boldsymbol{u} \bmod q\}$$

The QBCPDA employs the notion of *q-ary* lattices, where the security analysis is under the hard problems as defined below.

**Definition 5** (Small Integer Solution (SIS) [34])**.** Given integral modular matrix $\boldsymbol{X} \in Z_q^{m\times n}$ and an integer constant $\alpha$, finding a vector $\boldsymbol{t} \in Z^n\setminus\{0\}$ where $\parallel \boldsymbol{t} \parallel < \alpha$ and $\boldsymbol{X}\boldsymbol{t} = \boldsymbol{0} \bmod q$ is computationally infeasible.

**Definition 6** (Inhomogeneous Small Integer Solution (ISIS) [34])**.** Given integral modular matrix $\boldsymbol{X} \in Z_q^{m\times n}$, an integer constant $\alpha$ and a random vector $\boldsymbol{u} \in Z_q^m$, finding a vector $\boldsymbol{t} \in Z^n\setminus\{0\}$ where $\parallel \boldsymbol{t} \parallel < \alpha$ and $\boldsymbol{X}\boldsymbol{t} = \boldsymbol{u} \bmod q$ is infeasible.

**Definition 7** (Negligible Function [35])**.** Function $\varepsilon(k)$ is negligible if $\forall\ \mu > 0\ \exists k_0$ s. t. $\varepsilon(k) \leq \frac{1}{k^{\mu}}$ holds for any $k \geq k_0$.

The QBCPDA resists quantum attack based on three traits [34]:

- Closure: For valid vehicle $V_i$, $\boldsymbol{P}_i = \boldsymbol{x}_i^T\boldsymbol{X} \in Z_q^{1\times n}$ and $\boldsymbol{S}_i = \boldsymbol{r}_i^T\boldsymbol{X} \in Z_q^{1\times n}$ satisfies $\forall \boldsymbol{X} \in Z_q^{m\times n}$, $\boldsymbol{x}_i, \boldsymbol{r}_i \in Z_q^m$.
- Collision Resistance [31]: The function family $\{\mathbf{(X)} : Z_q^n \to \mathcal{R}^m | (\boldsymbol{X}) \in Z_q^{m\times n}\}$ is Collision Resistant.
- $(\varphi, \vartheta)-$Hiding: For $\boldsymbol{X} \in Z_q^{m\times n}$, $\boldsymbol{x}_i \in Z_q^m$ and $\boldsymbol{r}_i \in Z_q^m$,

$$\Gamma(\boldsymbol{x}_i, m_i) = \{(\boldsymbol{x'}_i, \boldsymbol{r'}_i) : \boldsymbol{x}_i^T\boldsymbol{X} = \boldsymbol{x'}_i^T\boldsymbol{X} \wedge \boldsymbol{r}_i^T\boldsymbol{X} = \boldsymbol{r'}_i^T\boldsymbol{X} \wedge\ (\boldsymbol{r}_i - k_i \cdot \boldsymbol{x}_i) = (\boldsymbol{r'}_i - k_i \cdot \boldsymbol{x'}_i)\}$$

be a set of secrets precise with $\boldsymbol{x}_i^T\boldsymbol{X}$, $\boldsymbol{r}_i^T\boldsymbol{X}$ and $(\boldsymbol{r_i} - k_i\boldsymbol{x_i})$.

TABLE I: Various notations and their meanings

| Notation | Description |
|---|---|
| $q$ | A sufficiently large prime number |
| $m, n$ | Two positive integers |
| $\boldsymbol{X}$ | A public matrix $\boldsymbol{X}$ generated from $Z_q^{m\times n}$ |
| $(\boldsymbol{x}_i, \boldsymbol{P}_i)$ | Private and public key pair of vehicle $V_i$ |
| $h_1(.), h_2(.)$ | Two cryptographic hash function |
| $Rid_i, Pw_i$ | Real identity and password of vehicle $V_i$ |
| $m_i$ | Traffic related message from vehicle $V_i$ |
| $t_i$ | Timestamp generated during $i$-th communication |
| $\sigma_i$ | Signature of Vehicle $V_i$ on message $m_i$ |
| $\epsilon$ | A negligible function |
| $A \parallel B$ | Concatenation of $A$ and $B$ |

**Definition 8.** The QBCPDA is $(\varphi, \vartheta)$-*Hiding* if we have

$$\Pr_{\boldsymbol{x}_i\in Z_q^m}[\forall\ m_i \neq m_i' | \Gamma(\boldsymbol{x}_i, m_i) \cap \Gamma(\boldsymbol{x}_i, m_i')| \leq \varphi|\Gamma(\boldsymbol{x}_i, m_i)|] \geq \vartheta.$$

### C. Formal security model

This formal security model for the QBCPDA follows a game played between a challenger $\mathcal{C}$ and a probabilistic polynomial-time adversary $\mathcal{A}$. In this game, $\mathcal{A}$ wishes to breach the security, and $\mathcal{C}$ assists $\mathcal{A}$ to do so. The game between $\mathcal{C}$ and $\mathcal{A}$ is as below:

- *Initialization*: $\mathcal{C}$ runs *Setup* for a security input $k$. Then, $\mathcal{C}$ outputs public parameters $param$ to $\mathcal{A}$.
- *Training:* $\mathcal{A}$ asks the following queries (in adaptive manner) and receives replies from $\mathcal{C}$ as follows:
  - $h_1$*-Oracle:* In this query, a random number $r \in Z_q^*$ is selected by $\mathcal{C}$. $\mathcal{C}$ inserts a tuple $(msg, r)$ into a hash list $L_{h_1}$ and returns $r$ to $\mathcal{A}$.
  - $h_2$*-Oracle:* In this query, a random number $r \in Z_q^*$ is selected by $\mathcal{C}$. $\mathcal{C}$ inserts a tuple $(msg, r)$ into a hash list $L_{h_1}$ and returns $r$ to $\mathcal{A}$.
  - *Registration-Query ($V_i$):* $\mathcal{C}$ performs the registration of a vehicle node $V_i$ as $\mathcal{A}$ asks for it.
  - *Sign-Query ($V_i, m_i$):* $\mathcal{A}$ asks this query with a message $m_i$. In response, $\mathcal{C}$ outputs the signed message tuple $\langle m_i, t_i, \sigma_i, Tid_i\rangle$ to the adversary.
- *Output:* $\mathcal{A}$ submits $\langle m^*, t^*, \sigma^*, Tid^*\rangle$ for a vehicle $V_i$. It wins if the two essential conditions are fulfilled
  - *Registration-Query ($V_i$)* and *Sign-Query ($V_i, m^*$)* have not been asked so far.
  - Verification of $\langle m^*, t^*, \sigma^*, Tid^*\rangle$ does not abort.

Advantage in performing existential unforgeability under chosen-message attack (EUF-CMA) by $\mathcal{A}$ is mentioned as $\epsilon_0 = Adv_{\mathcal{A},\ \text{EUF-CMA}}^{\text{QBCPDA}}(k) = |\Pr[\mathcal{A} \text{ wins}]|$.

**Definition 9.** The QBCPDA resists EUF-CMA if an adversary $\mathcal{A}$ gains negligible advantage $\epsilon$ where $\epsilon_0 \leq \epsilon$.

Now, we present the proposed QBCPDA to answer the question, "Could we design a quantum-resistant authentication system for the IoV that maintains vehicle privacy through blockchain?" The QBCPDA eases certificate management hassle. Besides, it meets a wide range of security needs, including anonymity, authentication, traceability, anti-replay, and MITM.

## III. Proposed QBCPDA Protocol for the IoV

The QBCPDA protocol is built with lattice-based cryptography and has been proved to be resistant to both exiting and quantum assaults. Before delving into our protocol, we mention the network model, the threat model, and some key assumptions.

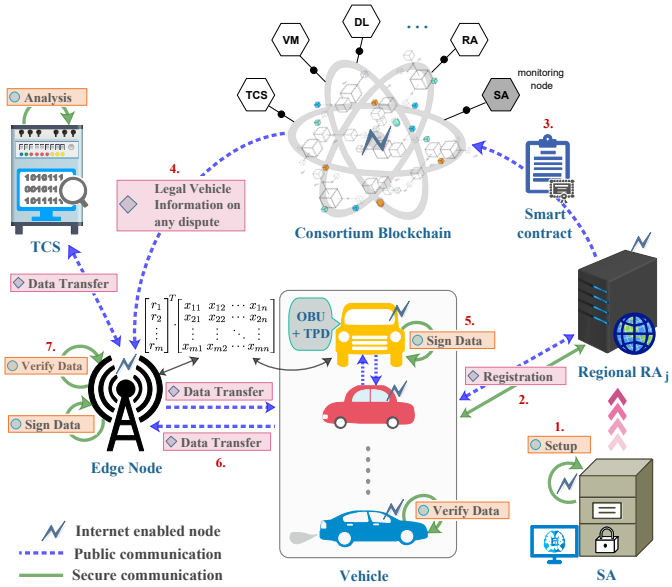



Fig. 2: System model of the QBCPDA protocol

### A. Network Model

The QBCPDA involves five entities that communicate with each other over the Internet: traffic control system (TCS), system administrator (SA), registration authority (RA), edge device, and vehicle. The operations of such entities are described below.

- *Traffic control system (TCS)*: The secure server with analytical capabilities. This entity receives driving information of vehicles from the edge node. It performs the optimal traffic signal control according to the constantly changing road traffic situation and provides useful traffic information to drivers based on the data collected.
- *Edge device (ED)*: An ED mounted in the network bridges the communication between the vehicles and the TCS, as illustrated in Fig. 1.
- *System administrator (SA)*: The SA is a trust manager who is in charge of defining the system's principles and policies. The global parameters must be generated and published. The SA offers technical assistance to edge devices and manages traffic safety with the help of TCS.
- *Registration Authority (RA)*: A RA is a semi-trusted third party that participates in the blockchain as a node. This RA registers a vehicle in its local domain using advanced computing skills. It is important to note that there are multiple RAs for different domains, and the vehicle in a certain domain must register with its local RA.
- *Vehicle*: It is responsible for data transfer and is equipped with an OBU and a tamper-proof device (TPD). The former facilitates communication while the latter saves vital data.

Fig. 2 illustrates a network model in which the SA begins the communication within the IoV system. Upon receiving a proper registration request from a vehicle, the local RA performs certain computations and sends the secret token to the vehicle. Subsequently, the RA uploads the vehicle's information $dig_i$ through a smart contract in the consortium blockchain of several block nodes, including vehicle manufacturers (VM), license authorities (DL), RAs, TCS, etc[1]. In this way, all valid vehicles' information are listed in the blockchain, which later helps authenticate individual vehicles adequately on the occurrence of any disputes. This strategy resists outsider attacks. A vehicle $V_i$, equipped with OBU and TPD, signs traffic/driving data and sends it to the edge nodes or nearby vehicles. Upon receiving such data, the receiver can check the authenticity of traffic data and send it to the TCS after successful verification. Based on the analysis, the TCS returns valuable information to the edge node over the public channel. We assume that the information provided by the TCS is encrypted using symmetric encryption, where the respective key is known to the edge node. Here, we mainly show how a mobile node can authentically send valuable data. An overview of the vehicle registration and data authentication between $V_i$ and edge node are shown in Fig. 2 with an order of task execution.

### B. Data Security Threat Model and Assumptions

The IoV data is typically transmitted over a public communication channel. There are two types of adversaries: a) *insider attacker* who has authorized data access but is challenging to identify their illegal practice, and b) *outsider attacker* whose risks are only slightly less severe. Both of these attackers are targeted by the QBCPDA protocol. In an authentication protocol, the adversary launches a chosen message attack (CMA), which allows it to obtain signatures for multiple messages from signatory TPD. The EUF-CMA ensures that no adversary impersonates a genuine TPD to generate a valid signature without knowledge of the TPD's private key. Under the following assumptions, the QBCPDA meets all of the security requirements of Section I-A:

- The design and algorithms of our protocol are public. Thus, the individual values/parameters could be extracted if the adversary is able to obtain all necessary credentials.
- In the IoV, among two kinds of communication (public and private communications), the adversary cannot breach data transmitted over the private channel. However, the adversary accesses data (deletion, re-transmission, interception, modification) sent over a public channel.
- During the protocol execution, only the RA is allowed to detect the real identity of a vehicle.
- A TPD ensures that the stored data is never compromised as a result of any calculation feasibility effects [21].
- Suppose one of two authorized users engages in illegal behavior by violating the second user's OBU credentials or public parameters. In that case, the former is considered a formidable opponent for the latter because it is playing two roles (legitimate user and attacker) [2].
- All the standard cryptographic primitives are considered secure, i.e., no attacker can achieve a non-negligible advantage over such well-known operations.

[1]It is worth noting that the SA is the administrator of this consortium blockchain and does not participate in reaching the consensus [23].

### C. Protocol Description

We consider a set of vehicles $\mathcal{V}$ belonging to various administrative areas, each controlled by one $RA_j$. The SA establishes the system's rules and publishes the global parameters. The QBCPDA consists of five phases as mentioned below.

*1) Setup:* For a security parameter $k$ as input, the SA chooses $m$ and $n$, and $q$ as a prime number. It selects $\boldsymbol{X} \in Z_q^{m\times n}$ where all operations are done under modulo $q$. Besides, it chooses two cryptographic hash functions defined as $h_1 : Z_q^{1\times n} \times \{0,1\}^* \to Z_q^*$ and $h_2 : \{0,1\}^* \to Z_q^*$. Finally, it publishes public parameter $param = \{m, n, q, \boldsymbol{X}, h_1(\cdot), h_2(\cdot)\}$.

*2) Vehicle Registration:* Upon receiving vehicle details such as real identity and other necessary proofs, $RA_j$ installs a key $K_i = H(Rid_i||R_i)$ into the TPD of vehicle $V_i$ via secure link where $R_i$ is the secret key of $RA_j$. The $TPD_i$ chooses a random vector $\boldsymbol{x}_i \in Z_q^m$ and computes $\boldsymbol{P}_i = \boldsymbol{x}_i^T\boldsymbol{X} \in Z_q^{1\times n}$ as its private key and public key, respectively. Besides, it selects a password $Pw_i$ based on its real identity $Rid_i$. It computes $Tid_i = Rid_i \oplus h_2(K_i)$ and $dig_i = h_1(\boldsymbol{P}_i, Rid_i)$. Now, it encrypts $(\boldsymbol{P}_i, dig_i)$ using the symmetric key $K_i$, and sends ciphertext to $RA_j$ over public channel. Then, $TPD_i$ saves $\langle H(H(Pw_i)), Rid_i \oplus H(Pw_i), Tid_i, (\boldsymbol{x}_i||\delta_i) \oplus H(Pw_i)\rangle$. Note that $Tid_i$ is used to trace vehicle's real identity by $RA_j$ knowing $K_i$. Finally, $RA_j$ adds public information in the blockchain.

*Key to Blockchain:* To manage the trustworthiness of vehicles, a consortium blockchain is considered. The $RA_j$ performs a transaction with digest $dig_i$ of vehicle $V_i$ to invoke a smart contract that will be deployed into the blockchain. This smart contract, as auto-trust, is used to save and modify the public information of a vehicle. The $RA_j$ utilizes a Byzantine-fault tolerance (BFT) consensus to add a new node in the blockchain. If $RA_j$ succeeds in transmitting the digest $dig_i$ to the on-chain, then the smart contract receives its unique addresses. Thus, vehicle $V_i$ is announced as an authentic node in IoV[2], and the respective smart contract can be traced using transactions with convenient access permissions.

*3) Signature generation:* Vehicle $V_i$ with $TPD_i$ signs traffic data $m_i$. To do this, password $Pw_i$ is supplied. On successful verification, $TPD_i$ selects a random $\boldsymbol{r}_i \in Z_q^m$, calculates $k_i = [h_2(m_i||t_i) + \prod_{j=1}^n (\boldsymbol{S}_i)_j] \bmod q$ where $t_i$ is timestamp and

$$\boldsymbol{S}_i = \boldsymbol{r}_i^T\boldsymbol{X} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix}^T \cdot \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix}$$

and $\prod_{j=1}^n (\boldsymbol{S}_i)_j$ denotes the product of elements of vector $\boldsymbol{S}_i$ modulo $q$. Then, $TPD_i$ computes $\boldsymbol{s}_i = \boldsymbol{r}_i - k_i \cdot \boldsymbol{x}_i$. Finally, it sends $\langle m_i, t_i, \sigma_i, Tid_i\rangle$ to other nodes where $\sigma_i = (\boldsymbol{S}_i, \boldsymbol{s}_i)$.

*4) Verification:* Vehicle $V_j$ (or an edge node) verifies traffic data in two ways: *a) single verification:* a single message from a particular node at a time, and *b) batch verification:* multiple messages coming from different sources simultaneously[3]. The verifier executes either of the following methods.

- *Single verification*: On intended message $\langle m_i, t_i, \sigma_i, Tid_i\rangle$ received, the verifier checks timestamp $t_i$ for its freshness. If it succeeds, then it calculates $y_i = h_2(m_i||t_i) \bmod q$ and $z_i = y_i + \prod_{j=1}^n (\boldsymbol{S}_i)_j \bmod q$. If $\boldsymbol{S}_i = \boldsymbol{s}_i^T\boldsymbol{X} + z_i\boldsymbol{P}_i$ holds, then the verifier declares signature $\sigma_i$ is valid.
- *Batch verification*: On receiving $p \in Z^+$ messages $\langle m_1, t_1, \sigma_1, Tid_1\rangle, \cdots, \langle m_p, t_p, \sigma_p, Tid_p\rangle$ from different nodes in IoV, the verifier checks these messages through batch verification. It verifies the timestamps $t_i$ for its freshness. On successful check, the verifier chooses a vector $\boldsymbol{l} = \{l_1, \cdots, l_p\}$ at random where $l_i$ is a small positive number. If $\sum_{i=1}^p l_i\boldsymbol{S}_i = \left(\sum_{i=1}^p l_i\boldsymbol{s}_i^T\right)\boldsymbol{X} + \sum_{i=1}^p l_i z_i\boldsymbol{P}_i$, then the batched data is treated as valid.

The QBCPDA is consistent, i.e., a designated verifier can check the authenticity of messages. For single message verification,

$$\begin{aligned} \boldsymbol{s}_i^T\boldsymbol{X} \quad + \quad z_i\boldsymbol{P}_i \quad &= \quad (\boldsymbol{r}_i - k_i\cdot\boldsymbol{x}_i)^T\boldsymbol{X} + [y_i + \textstyle\prod_{j=1}^n (\boldsymbol{S}_i)_j]\boldsymbol{P}_i \\ &= \quad \boldsymbol{r}_i^T\boldsymbol{X} - (k_i\cdot\boldsymbol{x}_i^T)\boldsymbol{X} + [h_2(m_i||t_i) + \textstyle\prod_{j=1}^n (\boldsymbol{S}_i)_j]\boldsymbol{P}_i \\ &= \quad \boldsymbol{S}_i - k_i\boldsymbol{P}_i + k_i\boldsymbol{P}_i = \boldsymbol{S}_i. \end{aligned}$$

For batch verification, we get

$$\begin{aligned} &\left(\textstyle\sum_{i=1}^p l_i\cdot\boldsymbol{s}_i^T\right)\boldsymbol{X} + \sum_{i=1}^p l_i z_i\boldsymbol{P}_i \\ &= \quad \left(\textstyle\sum_{i=1}^p l_i(\boldsymbol{r}_i - k_i\cdot\boldsymbol{x}_i)^T\right)\boldsymbol{X} + \sum_{i=1}^p l_i[y_i + \textstyle\prod_{j=1}^n (\boldsymbol{S}_i)_j]\boldsymbol{P}_i \\ &= \quad \textstyle\sum_{i=1}^p l_i\boldsymbol{S}_i - \sum_{i=1}^p l_i k_i\boldsymbol{P}_i + \sum_{i=1}^p l_i k_i\boldsymbol{P}_i = \sum_{i=1}^p l_i\boldsymbol{S}_i. \end{aligned}$$

## IV. Security Analysis

The QBCPDA is secure even if an adversary is capable of quantum analysis. Thus, a hostile vehicle cannot impersonate any network communication. Further, the QBCPDA fulfills various essential security criteria, and a comparison with other comparable methods is presented in Table II.

### A. Provable Security Proofs

The proposed protocol is shown next to be quantum secure and existential unforgeable.

**Theorem 1** (Quantum resistance)**.** If adversary $\mathcal{A}$ breaks the $(\zeta, t)-$QBCPDA, then the characteristic of *Collision Resistance* violates under a quantum environment for polynomial time $t'$ with a non-negligible advantage $\zeta'$ for $\vartheta \approx 1$ and $\varphi < 1$, where

$$\zeta' \geq (\zeta + \vartheta - 1)\cdot\frac{(1-\varphi)}{(2-\varphi)} \quad \text{and} \quad t' = t + O(T_{\boldsymbol{x}\cdot\boldsymbol{X}})$$

and $T_{\boldsymbol{x}\cdot\boldsymbol{X}}$ is the multiplication cost of $\boldsymbol{x} \in \mathbb{Z}_q^m$ with $\boldsymbol{X} \in \mathbb{Z}_q^{m\times n}$.

*Proof.* Assume the QBCPDA holds the $(\varphi, \vartheta)-$*Hiding* and *Closure* properties. Let forger $\mathcal{A}$ gains advantage $\zeta$ in breaching the security of the QBCPDA. Then, the challenger $\mathcal{C}$ executes $\mathcal{A}$ to breach the *Collision Resistance* property as follows:

- Given $\boldsymbol{X} \in Z_q^{m\times n}$, $\mathcal{C}$ select a key $\boldsymbol{x}_i \in Z_q^m$ at random.
- $\mathcal{C}$ returns the public values $(\boldsymbol{X}, \boldsymbol{x}_i^T\boldsymbol{X})$ to $\mathcal{A}$.

[2]The RSU, being an edge node, does not actively participate in registering a new vehicle. Although the public values $(P_i, \text{dig}_i)$ of vehicle $V_i$ is freely accessible to edge nodes, the vehicle's real identity $\text{Rid}_i$ cannot be revealed in an unauthentic way from the consortium blockchain.

[3]A verifier may not always need to authenticate the validity of a vehicle's public key through blockchain when receiving several messages from the same vehicle. This event is occurred in contrast to analogous cases when certificate verification is needed. Thus, the QBCPDA eliminates central dependency and certificate administration overheads and is suitable for scalable communication.

- $\mathcal{C}$ acquires query message $m_i \leftarrow \mathcal{A}(\boldsymbol{X}, \boldsymbol{x}_i^T \boldsymbol{X})$.
- $\mathcal{C}$ verifies the validity of $m_i$ and sends the signature $\sigma_i = (\boldsymbol{S}_i, \boldsymbol{s}_i)$ to $\mathcal{A}$, where $\boldsymbol{S}_i = \boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{s}_i = \boldsymbol{r}_i - k_i.\boldsymbol{x}_i$.
- $\mathcal{C}$ acquires a forgery tuple $(m_i', \sigma_i') \leftarrow \mathcal{A}(\boldsymbol{X}, \boldsymbol{x}_i^T \boldsymbol{X}, \sigma_i)$.
- Finally, $\mathcal{C}$ outputs $(\boldsymbol{r}_i^T \boldsymbol{X}, \boldsymbol{r}_i - k_i'.\boldsymbol{x}_i, \boldsymbol{S'}_i, \boldsymbol{s'}_i)$ as a collision to $\boldsymbol{X}$ where $k_i' = h_2(m_i' || t_i) + \prod_{j=1}^{n} (\boldsymbol{S}_i)_j$ for message $m_i'$.

By the *Closure* property, it is considered that $\boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{r}_i - k_i'.\boldsymbol{x}_i$ are valid. For the rest of the proof, we assume that $\mathcal{A}$ always returns correct traffic data $(m_i, m_i')$ and true signature pair $(\boldsymbol{S'}_i, \boldsymbol{s'}_i)$. Hence, $\mathcal{C}$ always produces a valid collision and it is successful if and only if the collision is non-trivial, *i.e.,* $\boldsymbol{r}_i^T \boldsymbol{X} \neq \boldsymbol{S'}_i$ and $\boldsymbol{r}_i - k_i'.\boldsymbol{x}_i \neq \boldsymbol{s'}_i$. Similarly, $\mathcal{A}$ generates a valid message-signature pair $(m_i', \sigma_i')$ when the pair is non-trivial, i.e., $(m_i', \sigma_i') \neq (m_i, \sigma_i)$. By the assumption, $\mathbf{Pr}[(m_i', \sigma_i') \neq (m_i, \sigma_i)] = \zeta$. Now $\mathcal{C}$ picks a bit $b \leftarrow \{0, 1\}$ such that $\mathbf{Pr}[b = 0] = (1 - \varphi)/(2 - \varphi)$ and $\mathbf{Pr}[b = 1] = 1/(2 - \varphi)$. if $b = 0$, set $\boldsymbol{x'}_i = \boldsymbol{x}_i$ and $\boldsymbol{r'}_i = \boldsymbol{r}_i$. otherwise $\boldsymbol{x'}_i$ and $\boldsymbol{r'}_i$ are chosen uniformly at random from $\Gamma(\boldsymbol{x}_i, m_i)$. Now the output of this modified algorithm is $(\boldsymbol{r'}_i^T \boldsymbol{X}, \boldsymbol{r'}_i - k_i'.\boldsymbol{x'}_i, \boldsymbol{S'}_i, \boldsymbol{s'}_i)$. As the outputs of $\mathcal{A}$ depends on $(\boldsymbol{X}, \boldsymbol{x}_i^T \boldsymbol{X}, \boldsymbol{r}_i^T \boldsymbol{X}, \boldsymbol{r}_i - k_i.\boldsymbol{x}_i)$, value of $b$ and uniform distribution of private values on $\Gamma(\boldsymbol{x}_i, m_i)$. Thus, $(\boldsymbol{r'}_i^T \boldsymbol{X}, \boldsymbol{r'}_i - k_i'.\boldsymbol{x'}_i, \boldsymbol{S'}_i, \boldsymbol{s'}_i)$ is distributed identical as the output of original collision finding algorithm, and modified algorithm exhibits equal advantage for finding a collision. Thus, the advantage of the new algorithm that finds a collision *i.e.*,

$$Ev_0 : \boldsymbol{r'}_i^T \boldsymbol{X} \neq \boldsymbol{S'}_i \wedge \boldsymbol{r'}_i - k_i'.\boldsymbol{x'}_i \neq \boldsymbol{s'}_i$$

Following two events are used for event $Ev_0$.

$$Ev_1 : \boldsymbol{S'}_i \neq \boldsymbol{r}_i^T \boldsymbol{X} \wedge \boldsymbol{s'}_i \neq \boldsymbol{r}_i - k_i'.\boldsymbol{x}_i$$
$$Ev_2 : \boldsymbol{S'}_i = \boldsymbol{r}_i^T \boldsymbol{X} \wedge \boldsymbol{s'}_i = \boldsymbol{r}_i - k_i'.\boldsymbol{x}_i$$

Therefore, the probability of event $Ev_0$ is

$$\begin{aligned}\mathbf{Pr}[Ev_0] = \mathbf{Pr}[Ev_0 \wedge m_i = m_i'] + \mathbf{Pr}[Ev_0 \wedge m_i \neq m_i' \wedge Ev_1] \\ + \mathbf{Pr}[Ev_0 \wedge m_i \neq m_i' \wedge Ev_2]\end{aligned}$$

Consider the case where $m_i = m_i'$, then $Ev_0 \wedge m_i = m_i'$ holds if $(m_i', \sigma_i') \neq (m_i, \sigma_i) \wedge m_i = m_i'$ is satisfied. Thus, we have

$$\begin{aligned}\mathbf{Pr}[Ev_0 \wedge m_i = m_i'] &\geq \mathbf{Pr}[(m_i', \sigma_i') \neq (m_i, \sigma_i) \wedge m_i = m_i'] \\ &\geq \mathbf{Pr}[(m_i', \sigma_i') \neq (m_i, \sigma_i) \wedge m_i = m_i'] \cdot \frac{1 - \varphi}{2 - \varphi}\end{aligned}$$

Suppose, $m_i = m_i' \wedge Ev_1$. If $m_i \neq m_i' \wedge \ Ev_1 \wedge \ b = 0$, then $\boldsymbol{x}_i' = \boldsymbol{x}_i$ and $\boldsymbol{r'}_i = \boldsymbol{r}_i$ and $Ev_0$ holds true. Hence,

$$\begin{aligned}\mathbf{Pr}[Ev_0 \wedge m_i \neq m_i' \wedge Ev_1] &\geq \mathbf{Pr}[m_i \neq m_i' \wedge Ev_1 \wedge b = 0] \\ &= \mathbf{Pr}[b = 0].\mathbf{Pr}[m_i \neq m_i' \wedge Ev_1] \\ &= \frac{1 - \varphi}{2 - \varphi}.\mathbf{Pr}[((m_i', \sigma_i') \neq (m_i, \sigma_i)) \wedge m_i \neq m_i' \wedge Ev_1]\end{aligned}$$

where in last equality, $m_i \neq m_i'$, implies $(m_i', \sigma_i') \neq (m_i, \sigma_i)$.

We observe that $\boldsymbol{S'}_i = \boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{s'}_i = \boldsymbol{r}_i - k_i'.\boldsymbol{x}_i$. Then the event $Ev_0$ is equivalent to the situation when $\boldsymbol{r'}_i^T \boldsymbol{X} \neq \boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{r'}_i - k_i'.\boldsymbol{x'}_i \neq \boldsymbol{r}_i - k_i'.\boldsymbol{x}_i$. Thus, for all $\boldsymbol{x'}_i$ where $\boldsymbol{x'}_i^T \boldsymbol{X} = \boldsymbol{x}_i^T \boldsymbol{X}$, $Ev_0$ satisfies if $\boldsymbol{x'}_i \notin \Gamma(\boldsymbol{x}_i, m_i')$. Let $\mathbb{X} \subseteq Z_q^m$ and $\mathbb{R} \subseteq Z_q^m$ be the sets of secrets $\boldsymbol{x}_i$ and $\boldsymbol{r}_i$ respectively such that,

$$\forall \ m_i \neq m_i'.|\Gamma(\boldsymbol{x}_i, m_i) \cap \Gamma(\boldsymbol{x}_i, m_i')| \leq \theta |\Gamma(\boldsymbol{x}_i, m_i)|$$

According to $(\varphi, \vartheta)$-Hiding property, $\mathbf{Pr}[\boldsymbol{x}_i \in \mathbb{X}, \boldsymbol{r}_i \in \mathbb{R}] \geq \vartheta$. By a union bound and independence of $b$, the probability of event $Ev_3 : m_i \neq m_i' \wedge Ev_2 \wedge \boldsymbol{x}_i \in \mathbb{X} \wedge \boldsymbol{r}_i \in \mathbb{R} \wedge (b = 1)$ is

$$\begin{aligned}\mathbf{Pr}[Ev_3] &= \mathbf{Pr}[b = 1].\mathbf{Pr}[m_i \neq m_i' \wedge Ev_2 \wedge \boldsymbol{x}_i \in \mathbb{X} \wedge \boldsymbol{r}_i \in \mathbb{R}] \\ &\geq \frac{\mathbf{Pr}[m_i \neq m_i' \wedge Ev_2] - \mathbf{Pr}[\boldsymbol{x}_i \notin \mathbb{X} \wedge \boldsymbol{r}_i \notin \mathbb{R}]}{2 - \varphi} \\ &\geq \frac{\mathbf{Pr}[((m_i', \sigma_i') \neq (m_i, \sigma_i)) \wedge m_i \neq m_i' \wedge Ev_2] - 1 + \vartheta}{2 - \varphi}\end{aligned}$$

Besides, we have $\mathbf{Pr}[Ev_0 | Ev_3] = \mathbf{Pr}[\boldsymbol{x'}_i \notin \Gamma(\boldsymbol{x}_i, m_i') | Ev_3] = 1 - \mathbf{Pr}[\boldsymbol{x'}_i \in \Gamma(\boldsymbol{x}_i, m_i') | Ev_3]$

$$\Pr[Ev_0 | Ev_3] \geq 1 - \max_{\boldsymbol{X}, \boldsymbol{x}_i \in \mathbb{X}, \boldsymbol{r}_i \in \mathbb{R}, m_i \neq m_i'} \frac{|\Gamma(\boldsymbol{x}_i, m_i) \cap \Gamma(\boldsymbol{x}_i, m_i')|}{|\Gamma(\boldsymbol{x}_i, m_i)|} \geq 1 - \varphi$$

Therefore, $\mathbf{Pr}[Ev_0 \wedge m_i \neq m_i \wedge Ev_2] \geq \mathbf{Pr}[Ev_0 \wedge Ev_3]$ where

$$\mathbf{Pr}[Ev_3].\mathbf{Pr}[Ev_0 | Ev_3] \geq \tfrac{(1-\varphi)}{(2-\varphi)} \cdot \mathbf{Pr}\begin{bmatrix}(m_i', \sigma_i') \neq (m_i, \sigma_i) \\ \wedge \ m_i \neq m_i' \wedge Ev_2\end{bmatrix} - 1 + \vartheta$$

Now uniting three bounds, we get

$$\begin{aligned}\mathbf{Pr}[Ev_0] &\geq (\mathbf{Pr}[((m_i', \sigma_i') \neq (m_i, \sigma_i))] - 1l + \vartheta) \ \frac{1 - \varphi}{2 - \varphi} \\ &= (\zeta - 1 + \vartheta) \cdot \frac{1 - \varphi}{2 - \varphi}\end{aligned}$$

We note that if $\vartheta$ closes to 1 and $\varphi$ is less than 1, then $\mathbf{Pr}[Ev_0]$ and $\zeta$ are negligible. To achieve the said advantage, one should avail additional $O(T_{\boldsymbol{x} \cdot \boldsymbol{X}})$ computation time where $T_{\boldsymbol{x} \cdot \boldsymbol{X}}$ is the time to multiply $\boldsymbol{x} \in Z_q^m$ with $\boldsymbol{X} \in Z_q^{m \times n}$. Thus, the QBCPDA resists $\mathcal{A}$ under quantum environment provided the *Closure*, *Collision Resistance* and $(\varphi, \vartheta) - Hiding$ properties hold. ■

**Theorem 2** (Unforgeability)**.** The QBCPDA is $(\epsilon, t)-$EUF-CMA secure; else, a solver $C$ breaks the SIS/ISIS problem for a lattice $\mathcal{X}$ with a non-negligible advantage $\epsilon'$ in time $t'$ where

$$\epsilon' \geq \epsilon \cdot \left(q_h / 2^k\right) \quad \text{and} \quad t' = t + O(q_s T_{\boldsymbol{x} \cdot \boldsymbol{X}})$$

$q_h$, $q_s$ and $T_{\boldsymbol{x} \cdot \boldsymbol{X}}$ denote the number of hash, signature queries and multiplication cost of $\boldsymbol{x}$ with $\boldsymbol{X}$, respectively.

*Proof.* Due to space limitations, the formal proof is given in the appendix of a supplementary file. ■

### *B. Informal Security Discussions*

Besides, the quantum attack and EUF-CMA resistance, the QBCPDA meets the requirements of *un-linkability*, *identity privacy*, *traceability* and *message authentication*, and it withstands the *data modification*, *man-in-the-middle*, *impersonation*, *stolen table verifier* and *replay* attacks.

**Theorem 3.** QBCPDA supports un-linkability property.

*Proof.* The $TPD_i$ of a vehicle $V_i$ selects a random vector $\boldsymbol{r_i} \in Z_q^m$ to generate a signature $\sigma_i = (\boldsymbol{S}_i, \boldsymbol{s}_i)$ where $\boldsymbol{S}_i = \boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{s}_i = \boldsymbol{r}_i - k_i \boldsymbol{x}_i$. Note, $k_i$ includes $\langle m_i, t_i, \boldsymbol{S}_i \rangle$. Thus, no adversary $\mathcal{A}$ is able to link two different signatures $\sigma_i$ and $\sigma_i'$ of $V_i$ because of randomness of $\boldsymbol{r}_i$ and inclusion of $\boldsymbol{S}_i$ in $k_i$. Hence, the QBCPDA supports un-linkability. ■

**Theorem 4.** QBCPDA maintains identity privacy.

*Proof.* Vehicle's real identity $Rid_i$ is hidden in $Tid_i = Rid_i \oplus h_2(K_i)$ and $dig_i = h_2(\boldsymbol{P}_i, Rid_i)$. Only the $RA_j$ as third-party

TABLE II: Security requirements comparisons of related protocols

| Protocol | Various security attacks | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **SA1** | **SA2** | **SA3** | **SA4** | **SA5** | **SA6** | **SA7** | **SA8** | **SA9** | **SA10** |
| Liu et al. [29] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Liu et al. [30] | √ | × | ⊡ | √ | √ | √ | × | √ | × | √ |
| Mukherjee et al. [31] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Mundhe et al. [32] | √ | ⊡ | × | √ | √ | √ | √ | √ | ⊡ | √ |
| Kumar et al. [33] | √ | ⊡ | × | × | √ | √ | × | √ | ⊡ | √ |
| QBCPDA | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |

SA1: *Modification*; SA2: *Un-linkability*; SA3: *Traceability*; SA4: *Identity privacy*; SA5: *Message authentication*; SA6: *Man-in-the-middle*; SA7: *Replay*; SA8: *Impersonation*; SA9: *Stolen verifier table*; SA10: *Quantum*. √: *Secure*; ×: *Insecure*; ⊡: *Unavailable*.

is allowed to access $Rid_i$ through secret $K_i$. Revealing $Rid_i$ is computationally infeasible for other entities due to the unavailability of high entropy $K_i$ or password $Pw_i$. Further, computing $Rid_i$ from $dig_i$ is hard due to the collision resistance property of $h_2$. Thus, an adversary cannot reveal real identities of vehicles. Hence, QBCPDA enables identity privacy preservation. ■

**Theorem 5.** QBCPDA supports traceability property.

*Proof.* Only $RA_j$ can trace the real identity $Rid_i$ of a node on any dispute. The vehicle's $Rid_i$ is masked in $Tid_i$ and it is sent to edge node with the signature. As $Tid_i = Rid_i \oplus h_2(K_i)$, $RA_j$ could use the same secret $K_i$ to unwrap $Rid_i = Tid_i \oplus h_2(K_i)$ from $Tid_i$. Thus, the QBCPDA provides traceability. ■

**Theorem 6.** QBCPDA supports message authentication under the ISIS assumption.

*Proof.* According to Theorem 2, an adversary cannot alter a tuple $T = \langle m_i, t_i, \sigma_i, Tid_i \rangle$ sent through an insecure channel due to the hardness of ISIS assumption. Besides, the integrity of $T$ is preserved by the sender's signature. Any alteration in the transmitted message can be easily detected by an edge node through $\boldsymbol{S}_i = \boldsymbol{s}_i^T \boldsymbol{X} + z_i.\boldsymbol{P}_i$. Hence, the QBCPDA meets message authentication. ■

**Theorem 7.** QBCPDA withstands modification, man-in-the-middle, impersonation, stolen verifier table and replay attacks.

*Proof.* Our protocol resists the following attacks:

- *Modification attack*: Any alteration in $\langle m_i, t_i, \sigma_i, Tid_i \rangle$ can be detected by verifying the correctness of $\boldsymbol{S}_i = \boldsymbol{s}_i^T \boldsymbol{X} + z_i.\boldsymbol{P}_i$. From Theorem 2, it is clear that no adversary $\mathcal{A}$ can forge the message tuple $\langle m_i, t_i, \sigma_i, Tid_i \rangle$ successfully. Thus, the QBCPDA withstands modification attack.
- *Man-in-the-middle (MITM) attack*: In the QBCPDA protocol, it is difficult for an adversary $\mathcal{A}$ to impersonate an authentic node in IoV because it does not have any access to either private key $\boldsymbol{x_i}$ or ephemeral key $\boldsymbol{r_i}$ of a particular vehicle ($V_i$). Hence, $\mathcal{A}$ is unable to generate valid signature $\sigma_i = (\boldsymbol{S}_i, \boldsymbol{s}_i)$ for impersonating $V_i$ as the calculation of $\boldsymbol{S}_i = \boldsymbol{r}_i^T \boldsymbol{X}$ and $\boldsymbol{s}_i = \boldsymbol{r}_i - k_i.\boldsymbol{x}_i$ require $\boldsymbol{x}_i$ and $\boldsymbol{r}_i$. Thus, the QBCPDA is invulnerable to MITM attack.
- *Impersonation attack*: According to the Theorem 2, all adversary has a negligible probability to generate a valid signature $\sigma_i$ for an authentic node in IoV. For impersonating any node, $\mathcal{A}$ must generate a valid tuple $\langle m_i, t_i, \sigma_i, Tid_i \rangle$ such that $\boldsymbol{S}_i = \boldsymbol{s}_i^T \boldsymbol{X} + z_i.\boldsymbol{P}_i$. However, no such adversary can generate such tuple due to unavailability of $\boldsymbol{x_i}$. Besides, $\boldsymbol{x}_i$ can not be extracted from $\boldsymbol{P}_i = \boldsymbol{x}_i^T \boldsymbol{X}$ as ISIS problem is hard in a lattice family. On the other hand, only the data by edge node or other trusted vehicles are accepted as valid. Thus, the QBCPDA withholds impersonation attack.
- *Stolen verifier table attack*: No verifier table is created for data authentication. The private values of a node or RSUs are kept with them secretly in TPD. Thus, an adversary is unable to get any such table that might be helpful. Hence, the QBCPDA resists stolen verifier table attack.
- *Replay attack*: A vehicle $V_i$ sends $\langle m_i, t_i, \sigma_i, Tid_i \rangle$ where timestamp $t_i$ is included in $\sigma_i = (\boldsymbol{S}_i, \boldsymbol{s}_i)$ as $k_i = [h_2(m_i || t_i) + \prod_{j=1}^{n} (\boldsymbol{S}_i)_j] \bmod q$ to calculate $\boldsymbol{s}_i$. The replay attack can be resisted with the freshness of $t_i$. Hence, the QBCPDA in not vulnerable to replay attack. ■

## V. Performance Evaluation

We evaluate the performance of QBCPDA by measuring computational, communication, storage, and energy costs. Subsequently, a comparative analysis of the QBCPDA protocol is also provided to benchmark our results with various existing competing techniques. For $q = O(k^2)$, we select security parameter $m = n = O(k \log q)$. Note that these choices are sufficient to provide the security of the ISIS assumption. For the purpose of comparison, we set $q = k^2$ and $m = n = k \log q$.

### A. Computation cost

Because the overhead is focused on time-consuming processes, lightweight cryptographic operations are not considered. $\boldsymbol{P} = \boldsymbol{x}^{\boldsymbol{T}} \cdot \boldsymbol{X}$ is computed with $O(mn \cdot |q^2|) = O(k^2 \log^4 k)$ where $|q^2|$ is the cost of multiplying two numbers in $Z_q^*$. Further, $\boldsymbol{S} = \boldsymbol{r}^{\boldsymbol{T}} \cdot \boldsymbol{X}$ and $\boldsymbol{s} = \boldsymbol{r} - k\boldsymbol{x}$ for a participant are computed with $O(mn \cdot |q^2|) = O(k^2 \log^4 k)$ and $O(m \cdot |q|) = O(k \log^2 k)$, respectively. Moreover, the computational order for verifying an intended message considers the overhead of checking $\boldsymbol{S} = \boldsymbol{s}^{\boldsymbol{T}}.\boldsymbol{X} + z.\boldsymbol{P}$ is noted as $O(mn \cdot |q^2|) = O(k^2 \log^4 k)$ which incurs a cost of $mn \cdot |q^2| + n \cdot |q|$. Thus, the total computation overhead of the QBCPDA is estimated as $3mn \cdot |q^2| + (m+n) \cdot |q|$.

### B. Communication and storage costs

The transmission overhead of a message-signature tuple $\langle m, t, \sigma, Tid \rangle$ requires $(m + n + 3) \cdot |q| = (2k \log q + 3) \cdot \log q$. Moreover, the overhead of storing secret value $\boldsymbol{x}$ considers $m \cdot |q|$, $\boldsymbol{X}$ requires $mn \cdot |q|$ and $\langle Rid, Pass, Tid, K \rangle$ takes $4|q|$. Thus, the total storage cost incurred in the QBCPDA protocol is considered as $(mn + m + 4) \cdot |q| = ((k \log q)^2 + k \log q + 4) \cdot \log q$ where $|q| = \log q$. The complexity of DH-type protocols depend

TABLE III: Computation costs of related protocols (based on lattice operations only)

| Protocol | Order of execution | Total cost |
|---|---|---|
| Liu et al. [29] | $O(mn \cdot \|q^2\|)$ | $4mn \cdot \|q^2\| + m \cdot \|q\| + n \cdot \|q\| = 64k^2 \log^4 k + 8k \log^2 k$ |
| Liu et al. [30] | $O(mn \cdot \|q^2\|)$ | $7mn \cdot \|q^2\| + 2m \cdot \|q\| + 2n \cdot \|q\| = 112k^2 \log^4 k + 16k \log^2 k$ |
| Mukherjee et al. [31] | $O(mn \cdot \|q^2\|)$ | $4mn \cdot \|q^2\| + 2m \cdot \|q\| + 2n \cdot \|q\| = 64k^2 \log^4 k + 16k \log^2 k$ |
| Mundhe etal. [32] | $O(mn \cdot \|q^2\|)$ | $4mn \cdot \|q^2\| + 3m \cdot \|q\| = 64k^2 \log^4 k + 12k \log^2 k$ |
| Kumar etal. [33] | $O(mn \cdot \|q^2\|)$ | $6mn \cdot \|q^2\| + 2m \cdot \|q\| + 7T_{pt} = 96k^2 \log^4 k + 8k \log^2 k + 7T_{pt}$ |
| QBCPDA | $O(mn \cdot \|q^2\|)$ | $3mn \cdot \|q^2\| + m \cdot \|q\| + n \cdot \|q\| = \mathbf{48k^2 \log^4 k + 8k \log^2 k}$ |

TABLE IV: Storage and communication comparisons of the competitive protocols

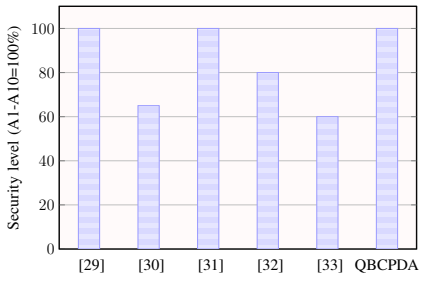
| Protocol | **Type** and **Primitive** | **Length (in bits)** |
|---|---|---|
| Liu et al. [29] | Storage: $\langle \boldsymbol{A}, \boldsymbol{B} \rangle \in Z_q^{m \times n}$, $\langle \boldsymbol{e}, \boldsymbol{x}, \boldsymbol{u} \rangle \in Z_q^m$, $RID$, $k$ | $(2mn + 3m + 2) \cdot \|q\| \approx 16k^2 \log^3 k + 12k \log^2 k + 4 \log k$ |
| | Communication: $\langle m, \sigma, T \rangle$ | $(m + n + 4) \cdot \|q\| \approx 8k \log^2 k + 8 \log k$ |
| Liu et al. [30] | Storage: $\langle \hat{s}_{RA}, \hat{s}, \hat{b}, Cert \rangle \in Z_q^{m*n}$, $RID$ | $(4mn + 1) \cdot \|q\| \approx 32k^2 \log^3 k + 2 \log k$ |
| | Communication: $\langle m, R, \sigma \rangle$, $\langle \hat{b}, RID, S, \hat{c} \rangle$ | $(7mn + 2) \cdot \|q\| \approx 56k^2 \log^3 k + 4 \log k$ |
| Mukherjee et al. [31] | Storage: $\boldsymbol{d} \in Z_q^m$, $\boldsymbol{A} \in Z_q^{m \times n}$, $Real$, $Pass$, $\langle ANS, \gamma, \boldsymbol{sk} \rangle$ | $(mn + 3m + 4) \cdot \|q\| \approx 8k^2 \log^3 k + 12k \log^2 k + 8 \log k$ |
| | Communication: $\langle M, ANS, T, \boldsymbol{R}, \boldsymbol{S} \rangle$ | $(m + 2n + 3) \cdot \|q\| \approx 12k \log^2 k + 6 \log k$ |
| Mundhe et al. [32] | Storage: $\langle R, R_q^n, R_q^k, R_{q[B]}^n \rangle \in Z_q^{m*n}$, $\langle D_\varphi^n, a_i, sk_i \rangle \in Z_q^n$ | $(4mn + 3m) \cdot \|q\| \approx 32k^2 \log^3 k + 12k \log^2 k$ |
| | Communication: $\langle z_1, z_2 \cdots z_3, c', \rangle$ | $(3mn + 1) \cdot \|q\| \approx 12k^2 \log^3 k + 2 \log k$ |
| Kumar et al. [33] | Storage: $\langle R_q, \mathcal{N}_{ag} \rangle \in Z_q^{m \times n}$, $\langle s, e_1, e_2 \rangle \in Z_q^n$, $ID, K_{op-}, K_{ev-} \in Z_q^*$, $G, K_{opagg-} \in F_{q_1}$ | $(2mn+3m+3) \cdot \|q\|+2\|q_1\| \approx 16k^2 \log^3 k+12k \log^2 k+12 \log k+2 \log q_1$ |
| | Communication: $\langle R, s, c \rangle$ | $(mn + 2) \cdot \|q\| \approx 8k^2 \log^3 k + 4 \log k$ |
| QBCPDA | Storage: $\boldsymbol{d} \in Z_q^m$, $\boldsymbol{X} \in Z_q^{m \times n}$, $\langle Rid, Pass, Tid, K \rangle \in Z_q^*$ | $(mn + m + 4) \cdot \|q\| \approx \mathbf{8k^2 \log^3 k + 4k \log^2 k + 8 \log k}$ |
| | Communication: $\langle m, t, \sigma, Tid \rangle$ | $(m + n + 3) \cdot \|q\| \approx \mathbf{8k \log^2 k + 6 \log k}$ |

on the modulus $q_1 \approx 2^{k_1}$ for security parameter $k_1 > k$. Considering $q = k^2$ and $m = n = k \log q$, the storage, computation and communication overheads of lattice operations in the QBCPDA are $8k^2 + \log^3 k + 4k \log^2 k + 8 \log k$, $48k^2 \log^4 k + 8k \log^2 k$ and $8k \log^2 k + 6 \log k$, respectively. Most previous works [11]–[24] in IoV primarily provide vehicle authenticity and identity shield via blockchain, PKI, and IBC, however such approaches cannot protect vehicle privacy or withstand quantum attacks. Thus, the quantum-safe state-of-the-art [29]–[33] are used for performance analysis. Tables III and IV offer thorough comparisons with related schemes, and the results indicate that the QBCPDA outperforms others [29]–[33].

### C. Experimental Setup and Result Discussion

We now explain our simulation setup. We consider that $RA_j$ is a semi-honest third-party. Upon successful login, a vehicle ($V_i$) with an OBU can exchange sensitive data. Here, the tasks of the $RA_j$ are executed on a potent device with Intel(R) CoreTM i7-8700 CPU@3.20GHz with RAM 8 GB, OS Ubuntu-18. In contrast, to realize the OBU and TPD's functionalities, all the vehicles' ($V_i$) tasks are executed on the IoT device Raspberry-Pi with ARM Cortex-A53CPU@1.4 GHz with RAM 1GB, OS Kali Linux. Furthermore, the tasks of the RSU are performed on a device with Intel(R) CoreTM i3-2310M CPU@2.10 GHz with RAM 6GB, OS Ubuntu-18. All the necessary cryptographic tasks are completed through Multiprecision Integer and Rational Arithmetic C Library (MIRACL) [36], and the individual costs are mentioned in Fig. 3b. MIRACL Crypto SDK is a C-based library universally approved by developers as the 'golden standard open-source SDK' for several advanced cryptosystems. For estimation purposes, the run-time complexity of various cryptographic action is considered as the mean of thirty runs for $m = n = 64$. Interestingly, $RA_j$ requires 145 ms to set up. Successful registration requires to perform various cryptographic tasks for 233 ms. The computational overhead of a signature generation phase is 9679 ms for a 1024-bit message. Meanwhile, the RSU verifies a single signature in 558 ms while requires 3962 ms for batch verification. The communication overheads is estimated based on the volume of different parameters, such as $|h| = 64$ bytes, $|Z_q^*| = 20$ bytes, $|ID| = 16$ bytes, $|T_i| = 4$ bytes. To ensure authenticity of the sensitive data, the QBCPDA stores 195 Kilobytes (KB) cryptographic keys in the OBU.

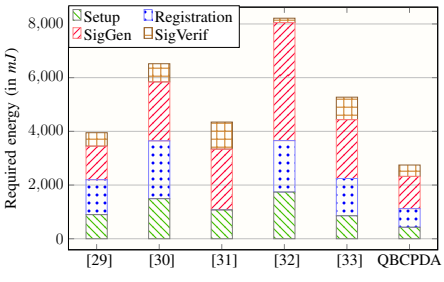
The overhead of privacy-preserving communication is 2.69 KB. Fig. 3 shows performance comparisons of the QBCPDA with the related protocols in its achieved security level along with incurred computation, communication, storage, and energy overheads. The estimated energy consumption is $E = P \times T$, where the units of energy $E$, power $P$, and time $T$ are millijoule (mJ), watt (W), and millisecond (ms), respectively. The powers of RA, ED, OBU are set approximately to 300 W, 75 W, and 12.5 W, respectively. Upon successfully executing specific tasks on the listed devices, the QBCPDA protocol consumes nearly 429 mJ to boot the IoV system and 693 mJ for the vehicle registration. The OBU requires 1210 mJ to generate a signature, while ED verifies the signature with energy 424 mJ. Further, a comparison in terms of energy consumption is shown in Fig. 3c. According to Fig. 3d, the computational overhead of the QBCPDA is nearly 75% of the scheme in [29], 43% of scheme in [30], 74% of scheme in [31], 75% of scheme in [32], and 50% of scheme in [33]. The QBCPDA is designed to allow the RSU to execute a more significant number of time-consuming operations compared to the lightweight OBU. As such, a proper load balance is achieved in the network. However, some of the baseline schemes do not follow this concept. Moreover, the signature generation overhead of the OBU is much higher than the signature verification by the RSU. This is the reason why QBCPDA has a smaller computation overhead. Fig. 3e shows the communication overhead is significantly lesser than the schemes [30], [32], [33]. Besides, Fig. 3f show that the QBCPDA stores minimal data with a overhead nearly 48% of



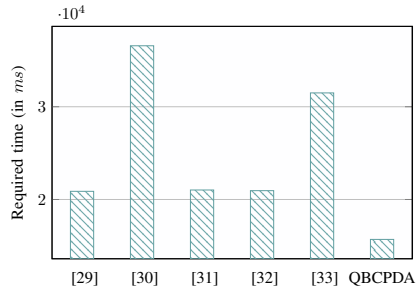

(a)

| Operation | RA | ED | OBU |
|---|---|---|---|
| $T_h$ | 0.95 | 1.35 | 36.25 |
| $T_r$ | 0.27 | 0.41 | 13.45 |
| $T_{\boldsymbol{X}}$ | 143.17 | 282.91 | 5829.06 |
| $T_{\boldsymbol{x}}$ | 3.79 | 8.15 | 160.30 |
| $T_{\boldsymbol{xX}}$ | 211.71 | 441.65 | 8726.81 |
| $T_{\boldsymbol{xx'}^T}$ | 2.29 | 4.72 | 80.33 |
| $T_{\boldsymbol{x}^T}$ | 0.01 | 0.02 | 0.11 |
| $T_{\boldsymbol{X}^T}$ | 0.29 | 0.63 | 7.54 |

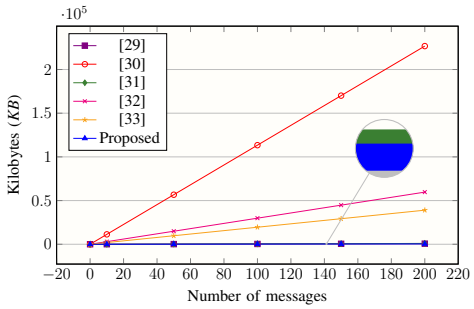
(b)



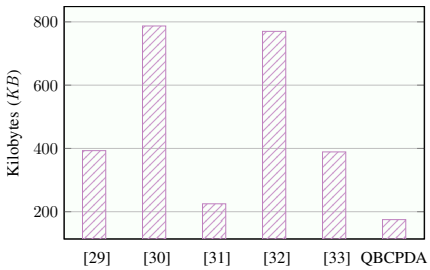

(c)




(d)




(e)




(f)

Note: $T_h$: hash digest; $T_r$: random element; $T_{\boldsymbol{X}}$: matrix in $Z^{m\times n}$; $T_{\boldsymbol{x}}$: vector in $Z^m$; $T_{\boldsymbol{xX}}$: product of $\boldsymbol{x}$ and $\boldsymbol{X}$; $T_{\boldsymbol{xx'}^T}$: product of $\boldsymbol{x}$ and $\boldsymbol{x'}^T$; $T_{\boldsymbol{x}^T}$: transpose of $\boldsymbol{x}$; $T_{\boldsymbol{X}^T}$: transpose of $\boldsymbol{X}$.

Fig. 3: Performance comparisons of related quantum-resistant authentication protocols in vehicular communication. (a) achieved security (↑ *is desirable*). (b) execution costs ($\times 10^{-2}$ ms) of various entities. (c) average consumption (↓ *is desirable*). (d) computation cost (↓ *is desirable*). (e) communication cost (↓ *is desirable*). (f) required storage space (↓ *is desirable*).

the schemes in [29], [33], 24% of the scheme in [30], 92% of the scheme in [31], and 24% of the scheme in [32].

In terms of computation, communication, storage, and energy costs, the QBCPDA is efficient than [30], [32] and [33]. Although it is nearly equal to [29] and [31] in communication, such systems require more processing, storage, and energy. Despite this, the QBCPDA obtains higher security, as shown in Fig. 3a.

## VI. Conclusion

In this paper, we have proposed a lattice-based conditional privacy-preserving authentication to avoid the possibility of a quantum attack in IoV. We have then demonstrated that the proposed protocol is provably secure under the random oracle model based on the infeasibility of standard ISIS assumption. Further, each vehicle's anonymity is preserved through a consortium blockchain mechanism. Our findings demonstrate that the proposed protocol is resistant to security flaws such as unlinkability, identity disclosure, traceability, message authentication, replay, and quantum attacks. Nonetheless, the proposed protocol eliminates the need for certificate administration. Under a suitable scenario, performance evaluation reveals that our protocol is at least 43% more energy-efficient and uses 25% less storage space than other competitive approaches that are acceptable for the lightweight devices utilized in IoV. In the near future, we plan to improve the proposed protocol by incorporating edge caching and a blockchain incentive system.

## References

[1] I. Wagner, "Estimated worldwide automobile production from 2000 to 2019," Available: https://www.statista.com/statistics/262747/worldwide-automobile-production-since-2000/, Apr 2020.

[2] T. Limbasiya and D. Das, "Iovcom: Reliable comprehensive communication system for internet of vehicles," *IEEE Trans. Dependable Secure Comput.*, Dec 2019.

[3] A. Ferdowsi, U. Challita, and W. Saad, "Deep learning for reliable mobile edge analytics in intelligent transportation systems: An overview," *IEEE vehicular technology magazine*, vol. 14, no. 1, pp. 62–70, Jan.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, Jan 2007.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. of the 27th IEEE Conf. on Comp. Commun.*, Phoenix, AZ, USA, Apr 2008, pp. 1229–1237.

[6] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam, "Cyber-physical security and safety of autonomous connected vehicles: Optimal control meets multi-armed bandit learning," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7228–7244, Jul 2019.

[7] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-quantum Cryptography*. Springer, 2009, pp. 1–14.

[8] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol*, vol. 68, no. 3, pp. 2906–2920, Jan 2019.

[9] Q. Feng, D. He, S. Zeadally, and K. Liang, "Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Oct 2019.

[10] S. Su, Z. Tian, S. Liang, S. Li, S. Du, and N. Guizani, "A reputation management scheme for efficient malicious vehicle identification over 5g networks," *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 46–52, 2020.

[11] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, 2020.

[12] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for internet of vehicles," *IEEE Trans. Emerg. Topics Comput.*, 2020.

[13] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, 2020.

[14] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE access*, vol. 7, pp. 45 061–45 072, 2019.

[15] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Commun.*, vol. 4, no. 7, pp. 894–903, Apr 2010.

[16] M. Khodaei and P. Papadimitratos, "Scalable & resilient vehicle-centric certificate revocation list distribution in vehicular communication systems," *IEEE Trans. Mobile Comput.*, 2020.

[17] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *Proc. of IEEE Int. Conf. on Comm.*, Beijing, China, May 2008, pp. 1451–1457.

[18] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. of the 27th IEEE Conf. on Comp. Commun.*, Phoenix, USA, Apr 2008, pp. 246–250.

[19] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Specs: Secure and privacy enhancing communications schemes for vanets," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, Mar 2011.

[20] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct 2015.

[21] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2681–2691, Aug 2015.

[22] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, Dec 2016.

[23] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol*, Jan 2020.

[24] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for vanet with blockchain," *IEEE Trans. Veh. Technol*, Feb 2020.

[25] E. Alkim, N. Bindel, J. A. Buchmann, Ö. Dagdelen, and P. Schwabe, "Tesla: Tightly-secure efficient signatures from standard lattices." *IACR Cryptology ePrint Archive*, vol. 2015, p. 755, Oct 2015.

[26] D. S. Gupta, G. Biswas, and R. Nandan, "Security weakness of a lattice-based key exchange protocol," in *Proc. of 4th IEEE Int. Conf. on Recent Advances in Information Technology*, Dhanbad, India, Mar 2018, pp. 1–5.

[27] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," in *Proc. of 14th Int. Workshop on Cryptographic Hardware and Embedded Systems*. Leuven, Belgium: Springer, Sep 2012, pp. 530–547.

[28] A. R. Abdallah and X. S. Shen, "Lightweight lattice-based homomorphic privacy-preserving aggregation scheme for home area networks," in *Proceedings of 6th IEEE International Conference on Wireless Communications and Signal Processing*, Hefei, China, Oct 2014, pp. 1–6.

[29] 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, Jan 2019.

[30] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, and H. Zhang, "Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks," *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 575–584, Apr 2019.

[31] S. Mukherjee, D. S. Gupta, and G. Biswas, "An efficient and batch verifiable conditional privacy-preserving authentication scheme for vanets using lattice," *Computing*, vol. 101, no. 12, pp. 1763–1788, Dec 2019.

[32] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan, "Efficient lattice-based ring signature for message authentication in vanets," *IEEE Systems Journal*, 2020.

[33] G. Kumar, M. Rai, R. Saha, W. J. Buchanan, R. Thomas, G. Geetha, T.-H. Kim, and J. Rodrigues, "A privacy-preserving secure framework for electric vehicles in iot using matching market and signcryption," *IEEE Trans. Veh. Technol*, Apr 2020.

[34] V. Lyubashevsky and D. Micciancio, "Asymptotically efficient lattice-based digital signatures," *Journal of Cryptology*, vol. 31, no. 3, pp. 774–797, Jul 2018.

[35] A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for iiot environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, 2018.

[36] Miracl, "miracl/miracl," Aug 2019. [Online]. Available: https://github.com/miracl/MIRACL


**Daya Sagar Gupta** received the B. Tech. degree in Computer Science and Engineering from UPTU Lucknow, UP, India. He received the M. Tech. and Ph.D. degrees in Computer Science and Engineering (CSE) from Indian Institute of Technology (IIT) Dhanbad, India. Presently, he is working as an Assistant Professor in the Department of CSE, Rajiv Gandhi Institute of Petroleum Technology Jais, Amethi, India. His research interests include information security, lattice-based cryptography and IoT security.

**Arijit Karati** (Senior Member, IEEE) received the M.Sc. degree in Computer Science from Pondicherry University, Puducherry, India in 2013. He received the Ph.D. degree from Indian Institute of Technology (IIT) Dhanbad, India in 2018. He was a Postdoctoral Fellow in the Department of Computer Science and Engineering (CSE), National Sun Yat-Sen University (NSYSU), Kaohsiung, Taiwan. Presently, he is working as an Assistant Professor in the Department of CSE, NSYSU where he leads the cryptology and network security (CANSEC) laboratory. He was a recipient of 108th Postdoctoral Researcher Academic Research Award from the Taiwan Ministry of Science and Technology in 2020. His research interests include applied cryptology, automotive security, and decentralized data privacy.

**Walid Saad** (Fellow, IEEE) received his Ph.D. degree from the University of Oslo in 2010. He is currently a Professor at the Department of Electrical and Computer Engineering at Virginia Tech, where he leads the Network sciEnce, Wireless, and Security (NEWS) laboratory. His research interests include wireless networks, machine learning, game theory, security, unmanned aerial vehicles, cyber-physical systems, and network science. He is an IEEE Distinguished Lecturer. He was also the recipient of the NSF CAREER award in 2013, the AFOSR summer faculty fellowship in 2014, and the Young Investigator Award from the Office of Naval Research in 2015. He was a recipient of the best paper awards at WiOpt 2009, ICIMP 2010, IEEE WCNC 2012, IEEE PIMRC 2015, IEEE SmartGridComm 2015, EuCNC 2017, IEEE GLOBECOM 2018 and 2020, IFIP NTMS 2019, IEEE ICC 2020. He is the recipient of the 2015 Fred W. Ellersick Prize from the IEEE ComSoc, the 2017 IEEE ComSoc Best Young Professional in Academia award, the 2018 IEEE ComSoc Radio Communications Committee Early Achievement Award, and the 2019 IEEE ComSoc Communication Theory Technical Committee. He was a co-author of the IEEE ComSoc Young Author Best Paper in 2019 and 2021. From 2015 to 2017, he was the Stephen O. Lane Junior Faculty Fellow at Virginia Tech, and in 2017, he was the College of Engineering Faculty Fellow. In 2019, he was honoured by Virginia Tech with the Dean's Award for Research Excellence. He is the Editor of several prestigious IEEE journals.

**Daniel B. da Costa** (Senior Member, IEEE) was born in Fortaleza, Ceará, Brazil, in 1981. He received the B.Sc. degree in Telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and the M.Sc. and Ph.D. degrees in Electrical Engineering, Area: Telecommunications, from the University of Campinas, SP, Brazil, in 2006 and 2008, respectively. His Ph.D. thesis was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. From 2008 to 2009, he was a Postdoctoral Fellow with INRS-EMT, University of Quebec, Montreal, Canada. Since 2010, he has been with the Federal University of Ceará, where he is currently an Associate Professor. From January 2019 to April 2019, he was Visiting Professor at Lappeenranta University of Technology (LUT), Finland, with financial support from Nokia Foundation. He was awarded the prestigious Nokia Visiting Professor Grant. From May 2019 to August 2019, he was with King Abdullah University of Science and Technology (KAUST), Saudi Arabia, as a Visiting Faculty, and from September 2019 to November 2019, he was a Visiting Researcher at Istanbul Medipol University, Turkey. In 2021, he joined as Full Professor at the National Yunlin University of Science and Technology (YunTech), Taiwan. He is the Founder and the Head of the Intelligent Wireless Communications (IWiCom) Research Group, the first research group created under the umbrella of the Future Technology Research Center (a new landmark at the YunTech Campus since 2020). He is Editor of several IEEE journals and has acted as Symposium/Track Co-Chair in various IEEE flagship conferences.