QSVP: A Quantum Safe Mutual Authentication Protocol for Vehicular Platoon Communications

Rohini Poolat Parameswarath, *Senior Member, IEEE,* Chao Wang, and Biplab Sikdar, *Fellow, IEEE*

***Abstract*—Vehicular platoons can transform the way we travel and have the potential to shape the future of mobility. To realize the full potential of vehicular platoons, vehicular platoon communication should be resilient to cyber-attacks including conventional and future quantum-computer-enabled attacks. In this paper, we propose a quantum-safe mutual authentication protocol for vehicular platoon communications, QSVP, leveraging the concepts of Quantum Key Distribution (QKD) and Post-Quantum Key Encapsulation Mechanism (PQKEM). The PQKEM used in QSVP is CRYSTALS-Kyber, a lattice-based PQKEM, selected by the National Institute of Standards and Technology (NIST) in round 3 of the post-quantum standardization process. Using the Real-or-Random (RoR) model, we demonstrate that QSVP offers provable security. Further, we evaluate the performance of QSVP using simulations carried out with the NS3 simulator. A performance analysis of QSVP demonstrates its superior security features and scalability compared to other similar schemes.**

***Index Terms*—CRYSTALS-Kyber, post-quantum key encapsulation mechanism (PQKEM), quantum key distribution (QKD), vehicular platoon.**

I. Introduction

A VEHICULAR platoon or convoy refers to a group of vehicles moving together, following one another, with coordinated driving [1], [2]. The vehicle positioned at the front of the platoon is known as the leader vehicle and the rest of the vehicles in the platoon are called followers. All the follower vehicles strictly follow the one in front of them and maintain a constant safe distance. Since the vehicles in a platoon are closer to each other, they occupy less space on the road. Thus, platooning helps to increase road capacity and reduce traffic congestion [3], [4]. Further, platooning reduces fuel consumption and carbon dioxide emissions [4]. Hence, we can expect widespread adoption of platooning technologies soon as they promise more efficient transportation systems.

A human driver always drives the leader vehicle in the platoon, and the leader vehicle's actions are subsequently broadcast to all followers [5]. The followers act according to the information they receive such as speed, location, change in speed, and direction [5]. Also, the leader communicates with the Road Side Unit (RSU) and the RSU sends data to the cloud server which is in charge of providing the platoon services. Technologies such as the Cooperative Adaptive Cruise Control (CACC) and Vehicle-to-Everything (V2X) communication protocol are used for communication and controlling the vehicles in a platoon ensuring that all vehicles in the platoon move at a given velocity while maintaining a fixed inter-vehicle distance [6], [7], [8], [9], [10].

Though platoons are promising and efficient transportation systems, vehicular platoon communications face several security and privacy challenges [11]. Attackers can launch several attacks to compromise sensor measurements and control command data in a platoon exploiting the openness of the wireless communication [8]. As an example, if an adversary gains control of the communication channels used for message exchange between vehicles in a platoon and modifies the transmitted messages with the intention of misleading vehicles, it can compromise the integrity and reliability of the system [6], [12]. If information related to a particular vehicle's location is modified maliciously, it can result in unwanted effects, including collisions among vehicles [11]. Another example is an adversary impersonating a legitimate vehicle and sending fake messages, such as hazard warnings to vehicles in the platoon [6]. Further, the adversary may eavesdrop on the exchanged messages to gather sensitive information, such as the location information of vehicles and identity details of the users [13], [14]. Hence, ensuring robust cybersecurity measures is crucial to protect against malicious interference with vehicular platoon communications and to protect the privacy of users.

In addition to the classical cyber-attacks against vehicular platoon communications, there is a new threat: cyber-attacks enabled by quantum computers. Symmetric and asymmetric cryptographic techniques are widely used to build authentication protocols to ensure the security of vehicular platoon communications. The security offered by asymmetric cryptographic approaches such as Elliptic-Curve Cryptography (ECC) and Rivest–Shamir–Adleman (RSA) comes from the hardness of solving the underlying mathematical problems, e.g., the discrete logarithm problem or the integer factorization problem. Shor's quantum algorithm [15] is a quantum cryptanalysis algorithm for factoring that can solve such problems quickly. Grover's quantum search [16] is a key search algorithm that can speed up searches [17]. The security level offered by the symmetric cryptographic key schemes reduces by half when an adversary applies Grover's search [18]. A quantum computer leverages quantum mechanical properties

Received 3 April 2025; revised 4 December 2025; accepted 14 January 2026. Date of publication 20 January 2026; date of current version 3 February 2026. This work was supported in part by Advanced Research and Technology Innovation Centre and in part by the National University of Singapore under Grant AFP-RP2. Recommended for acceptance by Dr. Hoang Thai Dinh. *(Corresponding author: Rohini Poolat Parameswarath.)*

The authors are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: rohini.p@nus.edu.sg; wang.chao@nus.edu.sg; bsikdar@nus.edu.sg).

and can perform these operations exponentially faster than conventional computers. Thus, the security offered by existing security solutions for vehicular platoon communications can be weakened by an adversary armed with quantum computers and advanced algorithms such as Shor's algorithm. Hence, any authentication protocol for vehicular platoon communications must be resilient to future quantum computer-enabled attacks as well, in addition to the classical attacks.

As discussed above, techniques that can make systems quantum-safe must be employed in authentication protocols. The National Institute of Standards and Technology (NIST) [19] initiated the Post-Quantum Cryptography (PQC) standardization process [20] in 2016. CRYSTALS-Kyber [21] has been selected as a quantum-safe Key Encapsulation Mechanism (KEM) after three rounds of evaluation as part of this PQC standardization process. CRYSTALS-Kyber derives its security from the hardness of solving the Learning-With-Errors (LWE) problem over module lattices [22]. Key length and computation costs of CRYSTALS-Kyber are reasonable [23]. Quantum Key Distribution (QKD) techniques can also be employed to make systems quantum-safe. A QKD scheme helps two entities establish a common secret key by leveraging the laws of quantum mechanics. We propose a hybrid solution that employs a combination of QKD and PQKEM. The proposed authentication protocol, QSVP, is based on the Bennett-Brassard 1984 (BB84) protocol [24], which is one of the most widely commercially adopted QKD protocols, and CRYSTALS-Kyber KEM. Hence, QSVP is secure against attacks by both classical and quantum computers.

Design Choice of QKD - Kyber Split: Kyber is a software-based algorithm with consistent and low latency, and high availability. QKD latency and availability can vary depending on the distance and conditions. The key budget in the QKD network could be affected by the physical constraints of QKD systems. Also, PQKEM does not require any additional hardware. On the other hand, QKD needs dedicated hardware and optical alignment. However, as the computational power of quantum computers increases, the security offered by PQC may also be at stake as it is mathematically based [25]. In contrast, QKD is not based on mathematical assumptions and gives information-theoretic security. As a result, a hybrid solution where PQC is used in customers' devices and QKD in servers is a recommended approach [25].

Since QKD gives information-theoretic security, it is suitable for the RSU - Server link. The RSU - Server link carries aggregated traffic and edge decisions. If an attacker compromises this link, the compromised link can affect the entire region. The RSU-Server link is stationary. Hence, using QKD in the RSU - Server link gives the highest security where it is most needed and sustainable, leveraging the full strength of quantum-derived keys for the core link. In contrast, more channel-flexible technologies, such as PQKEM, are better suited for the mobile and dynamic environments of Vehicle-to-RSU and Vehicle-to-Vehicle communication, as they require no additional hardware and can adapt to varying channel conditions. Hence, using PQKEM on mobile Vehicle-to-RSU or Vehicle-to-Vehicle links helps with practicality and scalability.

Thus, the design choice of using QKD only for the RSU–Server link and PQKEM for the rest is chosen considering the aspects of practicality, security, scalability, and cost-effectiveness.

A. Related Work

We divide this subsection into three parts to provide a comprehensive literature review that will equip the readers with the knowledge of research advancements and limitations in platoon communications. In the first part of this subsection, we summarize the existing works on platoon leader selection. In the second part, we discuss the existing works on securing platoon communications. To highlight the strengths and research gaps in the existing works on securing platoon communications, we have provided a table (Table I) with related works on securing platoon communications listing the primitives used, strengths, and limitations. In the third part of this subsection, we provide a discussion on related works on QKD applied in real-world scenarios to demonstrate that QKD has matured enough to be deployed outside the labs and has practical applications.

1) Platoon Leader Selection: Some platoon leaders may provide low-quality services that can result in security threats to platoon communication [26]. Hence, it is important to select a trusted platoon leader [27]. Selecting a trusted platoon leader is a well-explored research problem. The reputation of a vehicle is key parameter in selecting it as the platoon leader to have a trusted platoon leader. Hence, several research works have been proposed on evaluating the reputation score of the platoon leader. A privacy-preserving platoon communication scheme was proposed in [26]. For the cloud-assisted platoon formation proposed in this scheme, the vehicle with the maximum reputation value based on the reputation value ciphertext comparison protocol is selected as the platoon leader. The protocol employs the Paillier algorithm to encrypt reputation values, which results in significant computation cost.

Zhang et al. proposed a trust-based and privacy-preserving platoon recommendation scheme, TPPR, in [27]. TPPR employed pseudonyms, bilinear pairing, and Paillier algorithm. In TPPR, each vehicle holds a trust value, and the reputation value of the leader is calculated through a truth discovery process. Though TPPR ensures identity privacy and reliability of the platoon leader, it does not preserve the privacy of the reputation value [26], [28]. Li et al. proposed another reputation-based platoon management scheme, RPPM, in [28]. RPPM employed a secure comparison protocol to select the leader, which preserves the reputation values of vehicles. Similarly, Cheng et al. proposed a platoon recommendation scheme, PPRT, based on ECC, Paillier algorithm, and truth discovery techniques [29]. The scheme in [29] calculates the reputation score of the platoon leader based on the feedback provided by the platoon members, maintaining the privacy of vehicles. A reputation updating scheme for cloud-assisted vehicular networks was proposed in [30]. This scheme, based on the ECC and Paillier algorithms, ensures privacy preservation, robust security, and efficient reputation management. In this scheme, the reputation feedbacks are collected and preprocessed by the Cloud Service Provider, reducing computation and communication overheads

TABLE I
A BRIEF SUMMARY OF RELATED SCHEMES

Scheme	Brief Description	Primitives Used	Quantum Security	Replay Attack Protection	Privacy	Unlinkability	Low Computation Cost
Han et al. [1]	Secure admission of vehicles into a platoon	Context-based authentication	×	×	✓	✓	✓
Khan et al. [14]	Secure and privacy-preserving platoon formation	Blockchain and ZKP	×	✓	✓	✓	✓
Dickey et al. [32]	Secure admission of vehicles into a platoon	Context-based authentication	×	✓	×	✓	✓
Junaidi et al. [35]	Secure platoon management	ECC	×	✓	×	×	×
Gonçalves et al. [36]	Secure communication between platoon members	Public key infrastructure and attribute-based encryption	×	✓	✓	✓	×
Lai et al. [[37]	Authentication of platoon members	Attribute-based encryption and contributory key agreement	×	✓	×	×	✓
Basiri et al. [38]	Analyzes the security of vehicular platoons	Game-theoretic approach	×	✓	✓	✓	✓
Xie et al. [39]	V2I and V2V authentication	ECC	×	✓	✓	✓	✓
Wang and Liu [40]	Mutual authentication between vehicles and RSU	Bilinear pairing, RSA, Diffie-Hellman problem	×	✓	✓	✓	✓
Son et al. [41]	V2I handover authentication	Blockchain	×	✓	✓	✓	✓
Bagga et al. [42]	Mutual authentication and key agreement in ITS	Blockchain	×	✓	×	×	✓
Lai et al. [43]	Secure and privacy-preserving platoon communication	Private set intersection, bilinear pairing, certificateless ring signcyption	×	✓	✓	✓	✓
Parameswarath and Sikdar [44]	Secure admittance of vehicles into a platoon	DID, VC, blockchain	×	✓	✓	✓	✓
Li et al. [45]	Authentication through identity verification	ZKP, blockchain	×	✓	✓	✓	×
Yan et al. [46]	Authentication of a platoon when it moves from one base station to another	Certificateless public key cryptography, certificateless aggregate signature	×	✓	✓	✓	✓
Zhao et al. [47]	Secure transmission of messages in a platoon	Bilinear maps, Identity-based signcryption	×	✓	✓	✓	✓
Zhao et al. [48]	Secure transmission of messages between platoons	Bilinear maps	×	✓	✓	✓	✓
Abulkasim et al. [49]	Secure transmission of messages for IoD	ECC and Lattice-based KEM	✓	✓	✓	✓	×
Mishra et al. [50]	Secure authentication for IoD	Lattice-based KEM	✓	✓	×	×	✓
QSVP	Quantum-secure transmission of messages in a platoon	QKD, PQKEM	✓	✓	✓	✓	✓

on the Trusted Authority. It can be noted that none of the works mentioned above [26], [27], [28], [29], [30] are quantum-secure.

2) Secure Platoon Communications: Several attacks against vehicular platoons have been reported in literature [12]. Though selecting a trusted platoon leader is important in a platoon, it alone does not eliminate all security threats in a platoon. As an example, an attacker may capture control messages from the platoon leader, such as the instructions to change speed or lanes, and reply those messages later. This can result in the deviation of vehicles from the platoon, leading to platoon disruption [31]. Such a platoon deviation attack was simulated in [31]. We discuss the existing works on securing platoon communications next.

Researchers have applied various approaches to secure platoon communications. Context-based authentication and cryptography are some of the widely used approaches to secure communication in platoon systems. Han et al. proposed a scheme that verifies the physical context of vehicles before giving admission into a platoon in [1]. They leveraged the fact that the unique attributes of road surfaces will be the same for two adjacent vehicles. However, this protocol is vulnerable to record and replay attacks [32]. A scheme based on a challenge-response verification mechanism for platoon verification was proposed in [32]. However, the scheme in [32] did not address the anonymity and privacy of vehicles. Vaas et al. used trajectories of two vehicles to verify their presence and to form a platoon in [33]. A protocol for platoon verification based on Optical Camera Communications (OCC) was proposed in [34]. The above works [1], [32], and [34] are based on context-based authentication.

A platoon management scheme that is secure against several attacks was proposed in [35]. The scheme in [35] is based on ECC and has a high processing delay. Hence, there will be scalability issues when the number of vehicles increases. Further, the scheme in [35] reuses some parameters in every session. Hence, an adversary can link two sessions of the same vehicle. The Vehicular Ad hoc Network Public Key Infrastructure and Attribute-Based Encryption with Identity Manager Hybrid (VPKIbrID) model was proposed to protect communication between platoon members in [36]. Though VPKIbrID offers security and privacy, its computational complexity is high [51]. Lai et al. [37] proposed a protocol to authenticate vehicles in a platoon. It is based on attribute-based encryption and contributory key agreement. This scheme does not preserve the unlinkability of vehicles. A ciphertext policy attribute-based encryption scheme to secure platoon communication was proposed in [52]. A collaborative control strategy to secure vehicular platoons was proposed in [53]. The security of vehicular platoons was analyzed using a game-theoretic approach in [38]. An authentication protocol for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) with batch verification based on ECC was proposed in [39]. An authentication protocol that achieves mutual authentication between vehicles and RSUs was proposed in [40].

A V2I handover authentication protocol based on blockchain was proposed in [41]. Bagga et al. proposed a mutual authentication and key agreement protocol for Intelligent Transportation System (ITS) in [42]. However, the protocol in [42] does not provide unlinkability [54]. A secure and privacy-preserving platoon setup and communication scheme was proposed in [43] employing the concepts of private set intersection, bilinear pairing, and certificateless ring signcyption. Khan et al. [14] proposed a secure and privacy-preserving platoon formation scheme based on blockchain and Zero Knowledge Proof (ZKP). If an adversary gains admission into a platoon, the adversary will have access to the control commands of the platoon and may modify the control messages, posing a threat to the safety of people. To avoid this scenario, an authentication protocol was proposed in [44] to ensure that only legitimate vehicles are admitted into a platoon. The protocol in [44] leveraged the concepts of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Li et al. proposed an aggregated ZKP and blockchain-based authentication protocol for platooning in [45]. It ensures privacy-preserving identity verification. However, since the protocol in [45] aggregates all the proofs generated by platoon members and proof generation requires access to the blockchain, the process is time-consuming [14]. A protocol for secure authentication of a platoon when it moves from one base station to another base station was proposed in [46]. Certificateless public key cryptography and certificateless aggregate signature schemes were employed in designing the protocol in [46]. An identity-based signcryption scheme to secure platoon communication was proposed in [47]. In this scheme, the platoon leader generates a verifiable ciphertext and broadcasts it to the followers. This scheme employing bilinear maps ensures security of transmitted commands in the platoon as unauthorized vehicles cannot access the commands. Zhao et al. also applied signcryption technique and proposed a data authorization scheme for secure information sharing between platoons in [48]. This scheme also leveraged bilinear maps.

It can be summarized that the schemes mentioned above for vehicular platoon security have limitations such as being vulnerable to certain attacks, not providing all required security features, or having high computation costs. Another significant factor that the above protocols overlooked is the imminent threat of quantum computer-enabled attacks. None of the schemes discussed above addressed the quantum computer-enabled attacks.

Various authentication protocols with resistance to quantum adversaries have been introduced in recent research, such as [49], [50], [55], [56]. Abulkasim et al. proposed a quantum-secure communication scheme for Internet-of-Drones (IoD) by combining the ECC and lattice-based key exchange mechanism in [49]. Although the scheme in [49] offers quantum resistance, the protocol has a very high computational cost. Gupta et al. [55] proposed a lattice-based quantum-secure authentication scheme designed for IoT environments. However, this scheme is susceptible to desynchronization and impersonation attacks. A lattice-based quantum-secure authentication scheme for the IoD was introduced in [50]. Though this scheme is quantum-secure, it lacks strong anonymity and unlinkability. Hence, it fails to protect the privacy of participants. Chaudhary et al. introduced a three-party key agreement scheme in [56], which is quantum-secure. However, the scheme is vulnerable to replay attacks and lacks perfect forward secrecy. Additionally, its high computational cost significantly limits its scalability.

Table I provides a summary of the related schemes mentioning the primitives used, the security properties, and the performance properties. This table highlights the novelty of the proposed protocol.

3) Quantum Key Distribution: QKD technique helps to distribute cryptographic keys securely among parties across untrusted networks [57], [58], [59]. Unlike conventional key distribution methods that rely on the computational complexity of certain mathematical problems, QKD's security is grounded in the fundamental laws of quantum physics. This profound distinction offers provably secure communication, resilient to future hardware or algorithmic advancements, including the impending threat posed by quantum computers.

QKD has undergone remarkable progress since its inception, emerging as the most mature quantum information technology. Metropolitan QKD networks are being developed globally [60], [61], [62], [63], experimental demonstrations pushing transmission distances over thousands of kilometres [64], [65], [66], and portable QKD systems enabling secure key exchange over short-range free-space channels, on platforms such as handheld devices [67], [68] and automobiles [69]. These research advancements demonstrate that QKD is a practical choice to ensure quantum security.

B. Motivation

Platoon communications involve the exchange of sensitive data, including location, speed, and direction, between vehicles, RSUs, and servers. Protecting this data is critical,

as any compromise can directly affect the safety of the platoon. Existing authentication and key-agreement protocols rely on asymmetric cryptography, whose security is threatened by quantum-computer-enabled attacks. Although several quantum-safe schemes exist, they suffer from issues such as susceptibility to specific attacks, inadequate privacy protection, high computational cost, and poor scalability, as discussed in Section I.A. These limitations highlight the need for a quantum-safe mutual authentication protocol for vehicular platoon communications that secures all communication links with low computational overhead and high scalability.

C. Contributions

The main contributions of this paper are listed below:

- *A quantum-safe mutual authentication protocol for vehicular platoon communications based on QKD and PQKEM:* The core contribution of our work lies in addressing limitations of existing protocols by proposing a hybrid framework that combines QKD with PQKEM and lightweight operations such as XOR to enable quantum-secure, lightweight, and scalable authentication. The specific integration offers a new direction for deployable hybrid authentication in realistic platoon environments. This is the first authentication protocol for platoon communications that employs QKD and CRYSTALS-Kyber as building blocks, together with lightweight cryptographic operations. Kyber has medium-sized keys and offers the best overall performance compared to other KEM schemes [70], [71]. QSVP leverages QKD and Kyber to derive unique, quantum-secure session keys for each session. Thus, the proposed protocol's design ensures that it is lightweight and offers protection against quantum attacks.
- *Protection from conventional and future quantum computer-enabled attacks:* QSVP employs QKD and PQKEM CRYSTALS-Kyber. It does not depend on the complexity of underlying mathematical problems as in public key cryptography, to secure communication. Hence, QSVP offers protection even from attacks by an adversary with quantum computing capabilities. In addition to ensuring post-quantum security, QSVP provides robust security features, including session key security, mutual authentication, strong anonymity, perfect forward secrecy, unlinkability, as well as resistance to attacks such as eavesdropping, impersonation, replay, and Ephemeral Secret Leakage (ESL). Thus, compared with the existing literature, QSVP is lightweight and offers superior security features by protecting against conventional and quantum attacks.
- *Performance analysis:* We use liboqs [72] which is an open-source C library for quantum-safe KEM under the MIT license and the C/C++-based Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) [73] for the calculation of computation cost. We compare QSVP with other similar schemes based on computation cost, communication cost, and security properties.
- *Simulation of QKD System:* We simulate the use of QKD systems in QSVP using realistic experimental parameters to demonstrate the feasibility of QSVP.

D. Paper Organization

The rest of this paper is organized as follows. In Section II, we discuss the preliminaries required for QSVP. The system and adversary models are given in Section III. We present QSVP in Section IV. In Section V, we provide formal and informal security proofs for QSVP. Section VI presents a performance analysis of QSVP. The results of performance analysis using the NS3 simulator are given in Section VII. We conclude this paper in Section VIII.

II. Preliminaries

In this section, we provide a quick overview of the fundamentals of quantum key distribution and key encapsulation mechanism.

A. Quantum Key Distribution

In this work, we adopt the BB84 protocol [24] to showcase QSVP based on QKD. In the BB84 protocol, the authenticated users, named Alice and Bob, repeat the following steps to obtain the final secure keys.

Quantum State Preparation: Alice randomly chooses a basis $a_i \in \{\mathbb{X}, \mathbb{Z}\}$, and a uniformly random bit $y_i \in \{0, 1\}$. Given the basis information a_i and random bit y_i, Alice prepares the corresponding quantum state from the set $\{|0\rangle, |1\rangle, |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$.

Quantum State Transmission: Alice sends the prepared quantum state to Bob via an untrusted quantum channel.

Quantum State Measurement: Bob measures the received quantum state based on a randomly selected measurement basis $b_i \in \{\mathbb{X}, \mathbb{Z}\}$ and stores the outcome in $y' \in \{0, 1, \emptyset\}$.

Sifting: Alice and Bob broadcast their basis choices, a_i and b_i, over a classical communication channel, and they preserve only those instances where the measurement outcome is valid and they used the same measurement basis ($a_i = b_i$). The above-mentioned steps are iteratively performed until a sufficiently large set of instances is acquired.

Parameter Estimation: Alice and Bob select a random subset from the sifted keys to obtain an estimation of system parameters, to evaluate the final secure key rate.

Error Correction: Alice and Bob execute an information reconciliation protocol to ensure their respective keys are identical.

Privacy Amplification: Alice and Bob apply a random universal$_2$ hash function to extract two shorter strings based on the estimated system parameters and the final secure key rate. This process removes any potential side information that an eavesdropper may possess. The extracted key strings form the final secure keys.

B. Key Encapsulation Mechanism

The KEM helps to exchange secure keys between two parties. The KEM functions [21], [74] are given below:

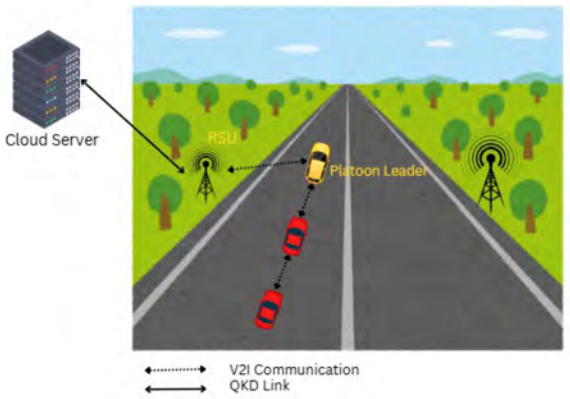


Fig. 1. System model.

Key Generation: Key Generation function does not take any inputs and generates a public key and a private key pair. The key generation function $KeyG()$ can be written as $(pu_x, pr_x) \leftarrow KeyG()$.

Encapsulation: The encapsulation function $Enc()$ uses the public key generated through $KeyG()$ to encapsulate a secret key k in a ciphertext c. Encapsulation can be written as $(c, k) \leftarrow Enc(pu_x)$.

Decapsulation: The decapsulation function $Dec()$ takes pr_x and c as inputs and outputs the secret key k. Decapsulation can be written as $k \leftarrow Dec(c, pr_x)$.

In QSVP, we use the CRYSTALS-Kyber KEM which has been selected by NIST for post-quantum cryptography standardization.

III. System and Adversary Models

A. System Model

The system model is illustrated in Fig. 1. We consider a platoon with a leader $\mathcal{L}$ and follower vehicles $\mathcal{F}_x$ for $x \in \{1, 2, \cdots n\}$. The followers relay their messages/data to the RSU, $\mathcal{R}$, through the leader. RSUs are installed on both sides of the road. RSUs act as contact points between platoons and cloud servers providing platoon services. The RSU aggregates information from several leaders and sends it to the cloud server $\mathcal{S}$. The RSUs have sufficient resources to do this computation. The leader, the follower vehicles, and the RSU are registered with the central cloud server. Several leader vehicles interact with an RSU, and several RSUs interact with the cloud server. There is a QKD link between the cloud server and the RSU. The existence of a classical authenticated channel is a prerequisite for the security of any QKD system. In practice, this authentication can be implemented using various well-established algorithms [63], [75], as it only requires short-term security rather than the long-term unconditional security demanded by the quantum key itself. For this reason, we do not emphasize the specific implementation of the classical authenticated channel in our system model, since it can be realized using standard and widely adopted authentication techniques without affecting the generality of our proposed scheme.

B. Adversary Model

We consider the Dolev-Yao (DY) model [76] where an adversary can listen to, edit, or delete the exchanged messages, and the Canetti-Krawczyk (CK) adversary model [77] where the adversary can capture long-term secrets or short-term keys as well. Under the DY model, some of the possible attacks are impersonation, eavesdropping, and replay attacks. Under the CK model, long-term and ephemeral secret leakage attacks are also possible [78]. To be CK-secure, the protocol must have perfect forward secrecy and ephemeral secret leakage attack resistance [77], [79]. We also assume that the adversary has quantum computing capabilities. Hence, the adversary can break the security of certain classical cryptographic techniques such as public key cryptography.

IV. Proposed Authentication Protocol

We present the proposed QSVP scheme in this section. QSVP consists of the following phases: setup, registration, mutual authentication between the followers and the leader, data transfer between the followers and the leader, mutual authentication between the leader and the RSU, and data transfer between the RSU and the cloud server through the RSU.

The registration phase is executed only once for each participant. The mutual authentication phase is performed whenever two participants want to communicate with each other. The high-level view of the proposed scheme is illustrated in Fig. 2.

A. Assumptions

- The RSUs and the cloud server are installed with QKD devices.
- We consider a generic quantum information transmission link between the cloud server and RSU for the generality of the proposed scheme. This could be free space or a fiber optic cable.

B. Setup Phase

In this phase, each protocol participant x invokes the key generation function $KeyG()$ as mentioned in Section II-B and generates a public key, pu_x, and a private key, pr_x.

C. Registration Phase

In this phase, the follower vehicles $\{\mathcal{F}_1, \mathcal{F}_2, \ldots \mathcal{F}_n\}$, the $\mathcal{L}$, and the $\mathcal{R}$ register with the $\mathcal{S}$. We assume that the messages are exchanged through a secure channel in the registration phase.

RSU Registration:

Step 1: The $\mathcal{R}$ sends a registration request and $pu_{\mathcal{R}}$ to the $\mathcal{S}$.

Step 2: The $\mathcal{S}$ registers the $\mathcal{R}$.

Leader Registration:

Step 1: The $\mathcal{L}$ with an identity ID_L generates a pseudo-identity PID_L. Then, the $\mathcal{L}$ sends a registration request, ID_L, PID_L, and $pu_{\mathcal{L}}$ to the $\mathcal{S}$.

Step 2: The $\mathcal{S}$ registers the $\mathcal{L}$. The $\mathcal{L}$ informs a set of paths with sources and destinations to the $\mathcal{S}$. The $\mathcal{S}$ broadcasts ID_L,

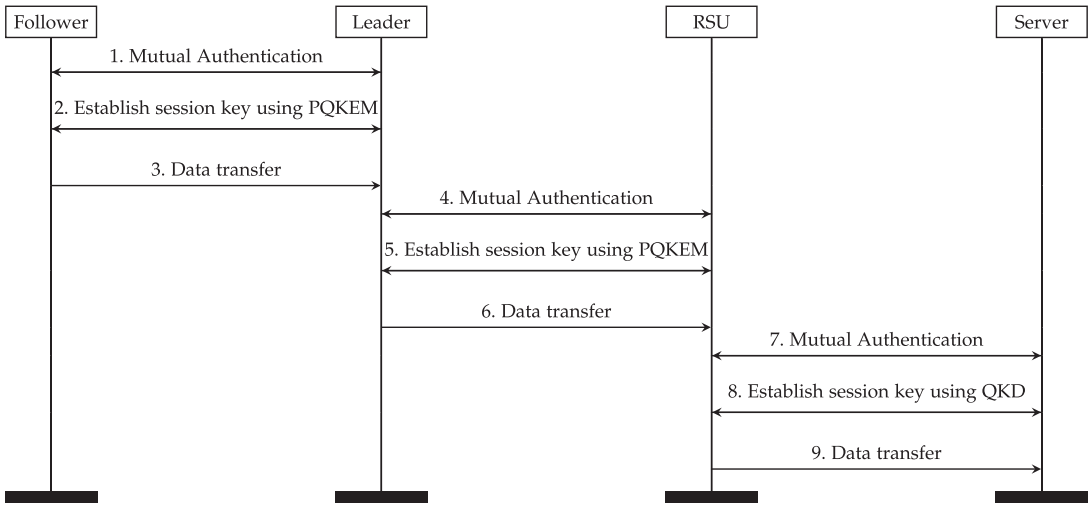


Fig. 2. High-level view of the protocol.

PID_L, and $pu_{\mathcal{L}}$ to the RSUs that cover the requested paths. It also distributes the public keys of the RSUs that cover the requested paths to the $\mathcal{L}$.

Registration of Follower Vehicles:

Step 1: The follower vehicle $\mathcal{F}_i$ with an identity ID_{Fi} generates a pseudo-identity PID_{Fi}. Then, $\mathcal{F}_i$ sends a registration request, ID_{Fi}, PID_{Fi}, and $pu_{\mathcal{F}i}$ to the $\mathcal{S}$.

Step 2: The $\mathcal{S}$ registers $\mathcal{F}_i$ and assigns it to the $\mathcal{L}$. The $\mathcal{S}$ sends $\{ID_L, pu_{\mathcal{L}}\}$ to $\mathcal{F}_i$. $\mathcal{F}_i$ stores ID_L and $pu_{\mathcal{L}}$. The $\mathcal{S}$ also sends $\{PID_{Fi}, pu_{\mathcal{F}i}\}$ to the $\mathcal{L}$. The $\mathcal{L}$ stores PID_{Fi} and $pu_{\mathcal{F}i}$.

Similarly, the $\mathcal{S}$ assigns n follower vehicles to the $\mathcal{L}$ to form a platoon.

D. Mutual Authentication Between a Follower and the Leader

The steps involved in the mutual authentication phase between the $\mathcal{L}$ and $\mathcal{F}_i$ are given below:

Step 1: $\mathcal{F}_i$ generates a value sk_1 and a random number x_j. As mentioned in Section II-B, $\mathcal{F}_i$ encapsulates sk_1 in a ciphertext c_j using $pu_{\mathcal{L}}$. Subsequently, $\mathcal{F}_i$ computes the authentication parameter $P_1 = h(x_j \parallel sk_1)$. Finally, $\mathcal{F}_i$ composes a message $A_1 = \{PID_{Fi}, c_j, x_j, P_1\}$ and sends it to the $\mathcal{L}$.

Step 2: The $\mathcal{L}$ decapsulates sk_1 from c_j using $pr_{\mathcal{L}}$ as mentioned in Section II-B. Next, $\mathcal{L}$ computes $h(x_j \parallel sk_1)$ and verifies it against the received P_1. After verifying P_1, the $\mathcal{L}$ generates a random number y_j and a random value sk_2. Then, $\mathcal{L}$ encapsulates sk_2 in a ciphertext c'_j using $pu_{\mathcal{F}i}$. Then, the $\mathcal{L}$ computes the authentication parameter $P_2 = h(y_j \parallel sk_2)$ and the session key $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$. After that, the $\mathcal{L}$ composes a message A_2 with c'_j, y_j, and P_2 as $A_2 = \{c'_j, y_j, P_2\}$ and sends it to $\mathcal{F}_i$.

Step 3: $\mathcal{F}_i$ decapsulates sk_2 from c'_j using $pr_{\mathcal{F}i}$ as mentioned in Section II-B. Then, $\mathcal{F}_i$ computes $h(y_j \parallel sk_2)$ and verifies it against the received P_2. After verification of P_2, $\mathcal{F}_i$ computes the session key as $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$. Thus, a session key $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$ is established between $\mathcal{F}_i$ and the $\mathcal{L}$. Fig. 3 shows the steps involved in this phase.

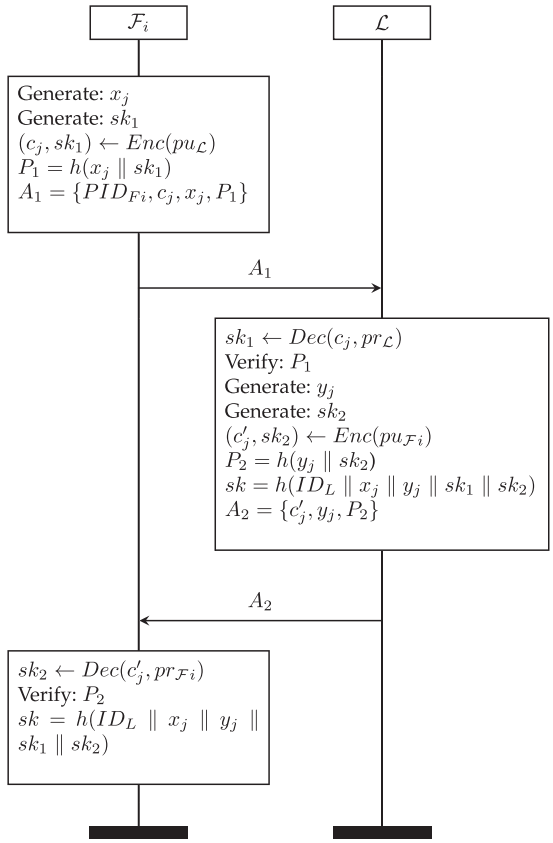


Fig. 3. Mutual authentication between a follower and the leader.

E. Data Transfer Between the Follower and the Leader

Once the session key sk is established between $\mathcal{F}_i$ and the $\mathcal{L}$, data can be sent to the $\mathcal{L}$. The steps involved in the data transfer phase between $\mathcal{F}_i$ and the $\mathcal{L}$ are given below:

Step 1: $\mathcal{F}_i$ generates a random number r_1 and the current timestamp t_F. Then, $\mathcal{F}_i$ performs an XOR operation on the data to send, $Data_F$, with sk to generate $Data^*_F$ as $Data^*_F =$

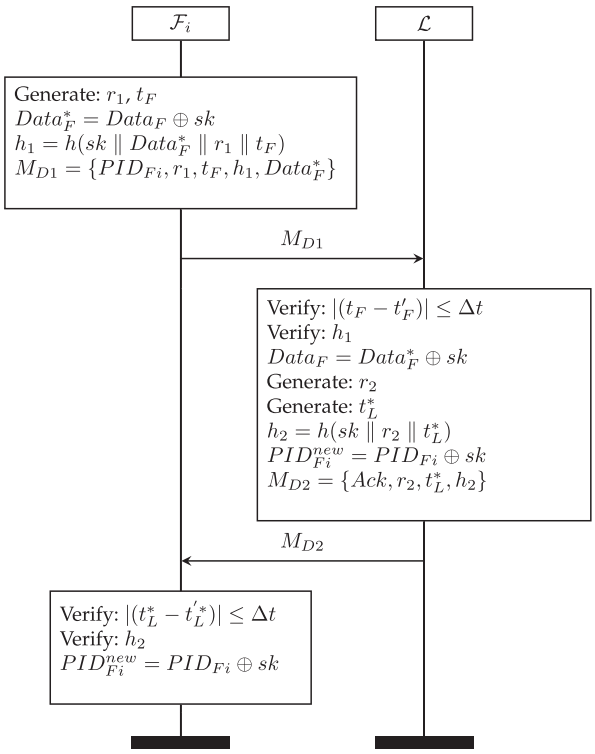


Fig. 4. Data transfer between the follower and the leader.

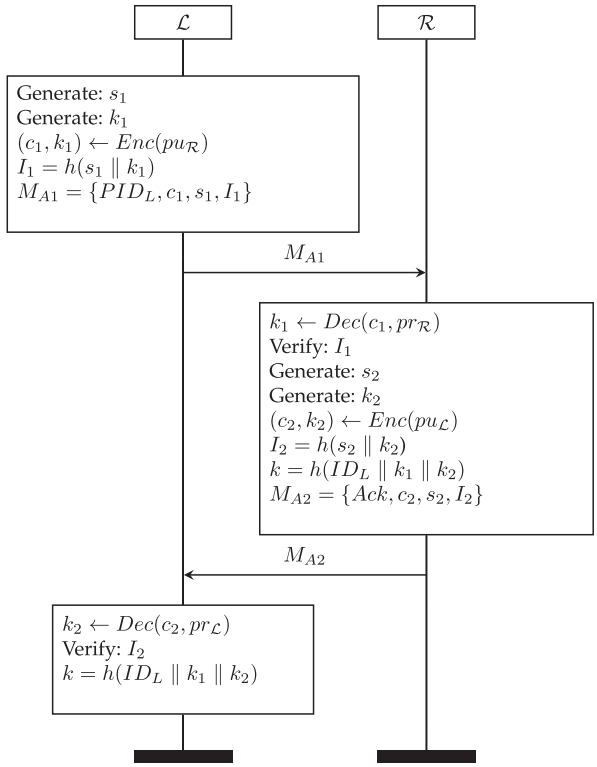


Fig. 5. Mutual authentication between the leader and the RSU.

$Data_F \oplus sk$. After that, $\mathcal{F}_i$ computes the authentication parameter $h_1 = h(sk \parallel Data_F^* \parallel r_1 \parallel t_F)$ and composes message $M_{D1} = \{PID_{Fi}, r_1, t_F, h_1, Data_F^*\}$. Finally, $\mathcal{F}_i$ sends M_{D1} to the $\mathcal{L}$.

Step 2: Upon receiving M_{D1} from $\mathcal{F}_i$ at time t'_F, the $\mathcal{L}$ first checks the validity of timestamp by verifying that $|(t_F - t'_F)| \leq \Delta t$, a threshold value. If t_F is a valid timestamp, $\mathcal{L}$ computes $h(sk \parallel Data_F^* \parallel r_1 \parallel t_F)$ and verifies it against received h_1. If the authentication parameter verification is successful, the $\mathcal{L}$ computes $Data_F = Data_F^* \oplus sk$ and generates a random number r_2 and the current timestamp t_L^*. Then, the $\mathcal{L}$ computes $h_2 = h(sk \parallel r_2 \parallel t_L^*)$. The $\mathcal{L}$ generates a new pseudo-identity for $\mathcal{F}_i$ to use in the next session as $PID_{Fi}^{new} = PID_{Fi} \oplus sk$ and stores it. Finally, the $\mathcal{L}$ composes message $M_{D2} = \{Ack, r_2, t_L^*, h_2\}$ where Ack is the acknowledgment that the data is received successfully. Finally, the $\mathcal{L}$ sends M_{D2} to $\mathcal{F}_i$.

Step 3: Upon receiving the acknowledgement through M_{D2} from the $\mathcal{L}$ at time $t_L^{'*}$, $\mathcal{F}_i$ first checks the validity of the timestamp by verifying that $|(t_L^* - t_L^{'*})| \leq \Delta t$, a threshold value. If t_L^* is a valid timestamp, $\mathcal{F}_i$ computes $h(sk \parallel r_2 \parallel t_L^*)$ and verifies it against received h_2. If the verification is successful, it can be confirmed that the data has been received successfully by the $\mathcal{L}$. $\mathcal{F}_i$ generates a new pseudo-identity to use in the next session as $PID_{Fi}^{new} = PID_{Fi} \oplus sk$ and stores it.

The steps involved in the data transfer phase are given in Fig. 4.

F. Mutual Authentication Between the Leader and the RSU

The $\mathcal{L}$ sends data to the $\mathcal{S}$ through the $\mathcal{R}$. First, the $\mathcal{L}$ and the $\mathcal{R}$ authenticate each other and establish a session key. The steps are similar to the steps in the mutual authentication between the leader and the followers. The steps involved in the mutual authentication phase between the $\mathcal{L}$ and the $\mathcal{R}$ are given below:

Step 1: The $\mathcal{L}$ generates random numbers s_1 and k_1. Then, the $\mathcal{L}$ encapsulates k_1 in a ciphertext c_1 using $pu_{\mathcal{R}}$. Subsequently, the $\mathcal{L}$ computes the authentication parameter $I_1 = h(s_1 \parallel k_1)$. Finally, the $\mathcal{L}$ generates a message $M_{A1} = \{PID_L, c_1, s_1, I_1\}$ and sends it to the $\mathcal{R}$.

Step 2: The $\mathcal{R}$ decapsulates k_1 from c_1 using $pr_{\mathcal{R}}$. Next, the $\mathcal{R}$ computes $h(s_1 \parallel k_1)$ and verifies it against received I_1. After successfully verifying I_1, the $\mathcal{R}$ generates random numbers s_2 and k_2. Then, the $\mathcal{R}$ encapsulates k_2 in a ciphertext c_2 using $pu_{\mathcal{L}}$ as mentioned in Section II-B. Then, the $\mathcal{R}$ computes the authentication parameter $I_2 = h(s_2 \parallel k_2)$ and the session key $k = h(ID_L \parallel k_1 \parallel k_2)$. Finally, the $\mathcal{R}$ composes a message M_{A2} with an acknowledgement Ack, c_2, s_2, and I_2 as $M_{A2} = \{Ack, c_2, s_2, I_2\}$ and sends it to the $\mathcal{L}$.

Step 3: Upon receiving M_{A2}, the $\mathcal{L}$ decapsulates k_2 from c_2 using $pr_{\mathcal{L}}$. Then, the $\mathcal{L}$ computes $h(s_2 \parallel k_2)$ and verifies it against the received I_2. After that, the session key is calculated as $k = h(ID_L \parallel k_1 \parallel k_2)$. Thus, a session key is established between the $\mathcal{L}$ and the $\mathcal{R}$. The steps involved in this phase are given in Fig. 5.

G. Data Transfer Between the Leader and the Cloud Server Through the RSU

Once a session key is established between the $\mathcal{L}$ and the $\mathcal{R}$, data can be sent from the $\mathcal{L}$ to the $\mathcal{S}$ through the $\mathcal{R}$. The steps

involved in the data transfer phase between the $\mathcal{L}$ and $\mathcal{S}$ through the $\mathcal{R}$ are given below:

Step 1: The $\mathcal{L}$ generates a random number n_1 and the current timestamp t_L. Then, the $\mathcal{L}$ performs an XOR operation on the data to send, $Data_L$, with k to generate $Data_L^*$ as $Data_L^* = Data_L \oplus k$. After that, the $\mathcal{L}$ computes the authentication parameter $H_1 = h(k \parallel Data_L^* \parallel n_1 \parallel t_L)$ and composes a message $D_1 = \{PID_L, n_1, t_L, H_1, Data_L^*\}$. Finally, the $\mathcal{L}$ sends D_1 to the $\mathcal{R}$.

Step 2: Upon receiving D_1 from the $\mathcal{L}$ at time t'_L, the $\mathcal{R}$ first checks the validity of timestamp by verifying that $|(t_L - t'_L)| \leq \Delta t$, a threshold value. If t_L is a valid timestamp, the $\mathcal{R}$ computes $h(k \parallel Data_L^* \parallel n_1 \parallel t_L)$ and verifies it against received H_1. Then, the $\mathcal{R}$ computes $Data_L = Data_L^* \oplus k$ and generates a random number n_2. Subsequently, the $\mathcal{R}$ runs QKD protocol with the $\mathcal{S}$ as mentioned in Section II-A and establishes a key k_{QKD} with the $\mathcal{S}$. Then, the $\mathcal{R}$ generates the current timestamp t_R and performs an XOR operation on $Data$ as $Data_R = Data_L \oplus k_{QKD}$ and computes $H_2 = h(k_{QKD} \parallel Data_R \parallel n_2 \parallel t_R)$. Finally, the $\mathcal{R}$ composes a message $D_2 = \{ID_R, n_2, t_R, H_2, Data_R\}$ and sends it to the $\mathcal{S}$.

Step 3: Upon receiving D_2 from the $\mathcal{R}$ at time t'_R, the $\mathcal{S}$ first checks the validity of timestamp by verifying that $|(t_R - t'_R)| \leq \Delta t$, a threshold value. If t_R is a valid timestamp, $\mathcal{S}$ computes $h(k_{QKD} \parallel Data_R \parallel n_2 \parallel t_R)$ and verifies it against received H_2. Then, the $\mathcal{S}$ computes $Data_L = Data_R \oplus k_{QKD}$. Then, the $\mathcal{S}$ generates a random number n_3 and the current time stamp t_S. Subsequently, the $\mathcal{S}$ computes $H_3 = h(k_{QKD} \parallel n_2 \parallel n_3 \parallel t_S)$. The $\mathcal{S}$ composes a message $D_3 = \{Ack, n_3, t_S, H_3\}$, where Ack is the acknowledgment that the data is received successfully. Finally, the $\mathcal{S}$ sends D_3 to the $\mathcal{R}$.

Step 4: After receiving the acknowledgement through D_3 from the $\mathcal{S}$ at time t'_S, the $\mathcal{R}$ first checks the validity of timestamp by verifying that $|(t_S - t'_S)| \leq \Delta t$, a threshold value. If t_S is a valid timestamp, the $\mathcal{R}$ computes $h(k_{QKD} \parallel n_2 \parallel n_3 \parallel t_S)$ and verifies it against the received H_3. Then, the $\mathcal{R}$ generates the current time stamp t_R^*. Subsequently, the $\mathcal{R}$ computes $H_4 = h(k \parallel n_1 \parallel n_2 \parallel t_R^*)$. The $\mathcal{R}$ generates a new pseudo-identity for the $\mathcal{L}$ as $PID_L^{new} = PID_L \oplus k$ and stores it. Finally, the $\mathcal{R}$ composes a message $D_4 = \{Ack, n_2, t_R^*, H_4\}$ and sends it to the $\mathcal{L}$.

Step 5: Upon receiving the acknowledgement through D_4 from the $\mathcal{R}$ at time $t_R^{*'}$, the $\mathcal{L}$ first checks the validity of timestamp by verifying that $|(t_R^* - t_R^{*'})| \leq \Delta t$, a threshold value. If t_R^* is a valid timestamp, $\mathcal{L}$ computes $h(k \parallel n_1 \parallel n_2 \parallel t_R^*)$ and verifies it against the received H_4. If the verification is successful, it can be confirmed that the data has been received successfully by the $\mathcal{S}$. Then, the $\mathcal{L}$ generates a new pseudo-identity as $PID_L^{new} = PID_L \oplus k$ and stores it to use in the next authentication session.

The steps of the data transfer phase between the leader and the server through the RSU are given in Fig. 6.

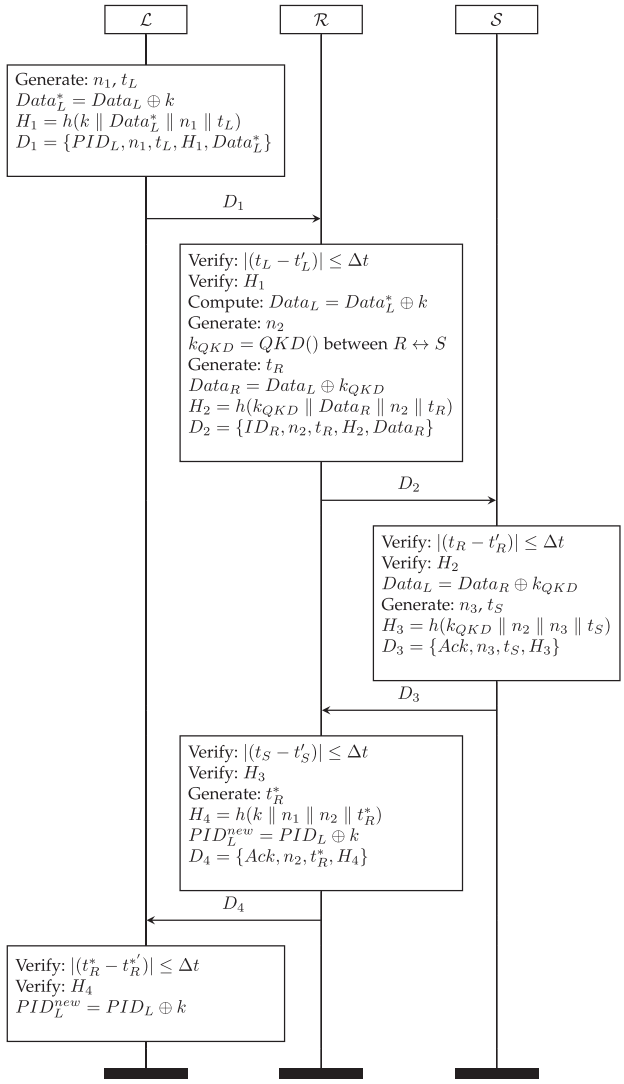


Fig. 6. Data transfer between the leader and the server through the RSU.

V. Security Analysis

A. Formal Security Analysis

Next, we provide formal proof of QSVP using the RoR model [80].

An adversary A's aim is to distinguish the established session key in a protocol session. A calls the following queries while interacting with the follower, leader, RSU, and the cloud server:

- $Execute(P_i, P_j)$*:* This query models a passive attack where the adversary eavesdrops on honest executions of the protocol between participants P_i and P_j. This query returns the transcript (all exchanged messages) to the adversary. Since this is a passive attack, no modification or intervention is allowed by the adversary. This query is useful for the adversary to learn the flow of protocol messages.
- $Send(P, x)$*:* This query models active attacks where the adversary interacts with the protocol participant P by sending a message x. This query returns the response message generated by P to the adversary. The adversary can control the flow of the protocol, impersonate parties, replay earlier messages, or perform man-in-the-middle attacks by using this query.
- *Reveal(P): Reveal(P)* query returns the ephemeral secrets of the protocol participant P.
- *Corrupt(P): Corrupt(P)* query returns the stored information such as the ID of protocol participant P.

- *Test(P):* This query is about the security of the session key and can be called only once. When A invokes this query, a bit b will be flipped. If $b = 1$, A receives the session key from the protocol participant P. Otherwise, A receives a random string.

Definition 1: A QKD protocol is said to be ϵ-secure if the actual QKD and ideal output states satisfy the condition $\Delta(\rho_{real}, \rho_{ideal}) \leq \epsilon$ where ρ is the density operator representing the state of a generic quantum system [81] and ϵ is a negligible value.

Definition 2: According to the quantum no-cloning theorem, the creation of identical copies of a quantum state is impossible [82]. Further, an adversary's attempt to capture and measure the photons to derive the symmetric key will increase the error rate [83] and will be detected by the participants in the QKD process. Due to these two quantum properties, the advantage of A in getting the key established through the QKD process is negligible. If we use a ϵ-secure QKD protocol as mentioned in Definition 1, the advantage of A in getting the secret keys established through QKD can be upper-bounded by ϵ, i.e., $Adv_A^{QKD} \leq \epsilon$.

Definition 3: The advantage of A in breaking the security of Kyber is negligible, i.e., $Adv_A^{KEM} \leq \alpha$, where α is a negligible value.

Definition 4: Let $Pr[Win_A]$ denote the probability that A wins the game. The protocol is secure if the advantage of A in breaking its semantic security, $Adv_A = \mid 2Pr[Win_A] - 1 \mid$, is negligible.

Theorem 1: Consider an adversary A sending n_h, n_s, and n_e $Hash$, $Send$, and $Execute$ queries, respectively. The $Hash$ query denotes a one-way hash function. Let $|h|$ denote the range space of $Hash$. Then, the advantage of A winning against QSVP is $Adv_A \leq \frac{(n_h)^2}{2^{(h)}} + \frac{(n_s+n_e)^2}{l} + \frac{n_s}{2^{(h-1)}} + 2Adv_A^{QKD} + 4Adv_A^{KEM}$ which is negligible.

Proof: Consider a series of games $Game_i$ for $i \in \{0, 1, 2, 3, 4, 5, 6\}$.

$Game_0$:: $Game_0$ corresponds to a real attack by A against QSVP. Since A guesses the bit b randomly in $Game_0$, according to Definition 4, the advantage of A in guessing b is:

$$Adv_A = \mid 2Pr[Win_{A,Game_0}] - 1 \mid . \tag{1}$$

$Game_1$: In $Game_1$, all the queries are simulated. Since the queries $Execute$, $Send$, $Hash$, $Reveal$, and $Corrupt$ are simulated as in a real attack, games $Game_0$ and $Game_1$ are identical. Hence, we can write that:

$$Pr[Win_{A,Game_1}] = Pr[Win_{A,Game_0}]. \tag{2}$$

$Game_2$: Games $Game_2$ and $Game_1$ are similar if there are no collisions in hash or transcripts. However, A stops $Game_2$ if there are collisions in hash or transcripts. From the birthday paradox, the collision probability of the hash function is at most $\frac{(n_h)^2}{2^{(h+1)}}$ and the collision probability in transcripts is $\frac{(n_s+n_e)^2}{2l}$ where l is the length of the transcripts. Hence, we can write that:

$$Pr[Win_{A,Game_2}] - Pr[Win_{A,Game_1}] \leq \frac{(n_h)^2}{2^{(h+1)}} + \frac{(n_s+n_e)^2}{2l}. \tag{3}$$

$Game_3$: The difference between $Game_3$ and $Game_2$ is that in $Game_3$, A guesses the verifier's value correctly without sending the $Hash()$ query and only by sending $Send$ queries. If A can guess this value correctly, A wins and stops $Game_3$. Hence, we can write:

$$Pr[Win_{A,Game_3}] - Pr[Win_{A,Game_2}] \leq \frac{n_s}{2^{(h)}}. \tag{4}$$

$Game_4$: In this game, A calls queries to get k_{QKD} so that from $Data_R = Data \oplus k_{QKD}$, $Data$ can be extracted. However, without knowing the key established through the QKD process (k_{QKD}), A cannot decode $Data$. We use an ϵ-secure QKD protocol as given in Definition 1. By Definition 2, the advantage of A in getting the secret keys established through QKD is upper-bounded by ϵ. Hence, the difference between $Game_3$ and $Game_4$ is negligible and we can write that:

$$Pr[Win_{A,Game_4}] - Pr[Win_{A,Game_3}] \leq Adv_A^{QKD}. \tag{5}$$

$Game_5$: This game considers the scenario of leakage of the session key k between the $\mathcal{L}$ and the $\mathcal{R}$. A calls $Corrupt()$ and $Reveal()$ queries in an attempt to get k so that from $Data_L = Data \oplus k$, $Data$ can be extracted. The session key is calculated as $k = h(ID_L \parallel k_1 \parallel k_2)$. The keys k_1 and k_2 are encapsulated as $(c_2, k_2) \leftarrow Enc(pu_{\mathcal{L}})$ and $(c_1, k_1) \leftarrow Enc(pu_{\mathcal{R}})$. To decapsulate k_1 and k_2 as $k_1 \leftarrow Dec(c_1, pr_{\mathcal{R}})$ and $k_2 \leftarrow Dec(c_2, pr_{\mathcal{L}})$, A needs to break the security offered by Kyber. By Definition 3, A has a negligible advantage in compromising Kyber. As a result, the difference between $Game_4$ and $Game_5$ is negligible. Hence, we can write that:

$$Pr[Win_{A,Game_5}] - Pr[Win_{A,Game_4}] \leq Adv_A^{KEM}. \tag{6}$$

$Game_6$: This game considers the scenario of leakage of the session key sk between $\mathcal{F}_i$ and the $\mathcal{L}$. A calls $Corrupt()$ and $Reveal()$ queries in an attempt to get sk so that from $Data_F^* = Data_F \oplus sk$, $Data$ can be extracted. The session key is established between $\mathcal{F}_i$ and the $\mathcal{L}$ as $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$. The keys sk_1 and sk_2 are encapsulated as $(c_j, sk_1) \leftarrow Enc(pu_{\mathcal{L}})$ and $(c_j', sk_2) \leftarrow Enc(pu_{\mathcal{F}i})$. To decapsulate sk_1 and sk_2 as $sk_1 \leftarrow Dec(c_j, pr_{\mathcal{L}})$ and $sk_2 \leftarrow Dec(c_j', pr_{\mathcal{F}i})$, A needs to break the security offered by Kyber. By Definition 3, the advantage of A in breaking the security of Kyber is negligible. As a result, the difference between $Game_5$ and $Game_6$ is negligible. Hence, we can write that:

$$Pr[Win_{A,Game_6}] - Pr[Win_{A,Game_5}] \leq Adv_A^{KEM}. \tag{7}$$

As a final attempt, A guesses the bit b and calls the $Reveal()$ query to win the game. Then, we can write that:

$$Pr[Win_{A,Game_6}] = \frac{1}{2}. \tag{8}$$

From (1) and (2), we can write the following:

$$\begin{aligned} \frac{1}{2}Adv_A &= \mid Pr[Win_{A,Game_0}] - \frac{1}{2} \mid \\ &= \mid Pr[Win_{A,Game_1}] - \frac{1}{2} \mid . \end{aligned} \tag{9}$$

By applying the triangle inequality with (3) to (9), we can write:

$$\begin{aligned}\frac{1}{2}Adv_A &= \mid Pr[Win_{A,Game_1}] - \frac{1}{2} \mid \\ &= \mid Pr[Win_{A,Game_1}] - Pr[Win_{A,Game_6}] \mid \\ &\leq \frac{(n_h)^2}{2^{(h+1)}} + \frac{(n_s+n_e)^2}{2l} + \frac{n_s}{2^{(h)}} + Adv_A^{QKD} + 2Adv_A^{KEM}.\end{aligned} \tag{10}$$

By multiplying both sides of (10) by 2, we have:

$$\begin{aligned}Adv_A \leq \frac{(n_h)^2}{2^{(h)}} + \frac{(n_s+n_e)^2}{l} + \frac{n_s}{2^{(h-1)}} + 2Adv_A^{QKD} \\ + 4Adv_A^{KEM}.\end{aligned} \tag{11}$$

■

B. Formal Privacy Analysis

Now, we formally analyze the privacy provided by the proposed protocol using the model given in [84].

Proof: A game played between A and the protocol participants is used to demonstrate that the proposed scheme offers unlinkability and privacy. The game has three phases:

- *Learning phase:* A chooses two vehicles $\mathcal{F}_0$ and $\mathcal{F}_1$ and listens to the messages on their i^{th} round of authentication. A learns the exchanged parameters for both the chosen vehicles.
- *Challenge phase:* The challenger randomly chooses $\mathcal{F}_b$ where the random bit $b \in \{0,1\}$ and gives it to A. After that, A eavesdrops on the messages of $\mathcal{F}_b$ on its $(i+1)^{th}$ round of authentication and learns the exchanged parameters for $\mathcal{F}_b$.
- *Guess phase:* In this phase, A needs to determine b. A has learnt the parameters for both $\mathcal{F}_0$ and $\mathcal{F}_1$ in session i and the parameters for $\mathcal{F}_b$ in session $i+1$. Suppose $b=0$, i.e., the challenger chose $\mathcal{F}_0$ as $\mathcal{F}_b$. Further, if PID_{F0} is $\mathcal{F}_0$'s pseudo-identity and sk is the session key for the i^{th} authentication session, $\mathcal{F}_0$ generates its pseudo-identity for $i+1^{th}$ session as $PID_{F0}^{new} = PID_{F0} \oplus sk$. As a result, $PID_{F0}^{new} \neq PID_{F0}$. The session key sk is calculated as $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$. Since x_j, y_j, sk_1, sk_2 are generated in each session, sk and hence, PID_{Fi}^{new} are unique to each session. Hence, A has to make a random guess on the bit b even after eavesdropping on the messages in session i as A does not know sk. A guesses a bit $d \in \{0,1\}$. A wins the game if $b=d$. Here, the advantage of A is the advantage over random guessing of the bit. The advantage of A in this game is $Adv_A = Pr((b=d) - \frac{1}{2}) = 0$. Hence, A cannot confirm that two messages come from the same vehicle. Thus, QSVP offers unlinkability and privacy.

C. Informal Security Analysis

Protection from Quantum Attacks: An attacker with quantum-computing capabilities can solve the underlying problems of conventional cryptographic techniques quickly using quantum algorithms. Hence, the security of the vehicular platoon communication protocols based on conventional cryptographic techniques could be compromised by quantum computer-enabled adversaries. QSVP leverages PQKEM and QKD techniques. QKD provides information-theoretic security rather than computational security, which fundamentally differs from classical cryptographic approaches. The quantum resistance of QKD stems from the fundamental laws of quantum mechanics, which ensure that any eavesdropping attempt will introduce measurable errors in the quantum channel. From this error analysis, the amount of information the adversary obtained can be evaluated, enabling legitimate parties to establish provably secure keys. Importantly, this security guarantee holds regardless of the computational power available to the adversary, including quantum computers. As such, in principle, QKD can provide security guarantees against all kinds of attacks on the channel that are allowed by classical and quantum physics. Further, Kyber offers protection from quantum attacks by relying on the hardness of the LWE problem, which remains computationally infeasible to solve even with powerful quantum computers. Unlike classical cryptographic schemes such as RSA and ECC that are vulnerable to Shor's algorithm, Kyber's security is based on lattice-based cryptography, which currently has no known efficient quantum algorithms capable of breaking it. As a result, even if the attacker has quantum computing capabilities, the security offered by QSVP is not affected. Thus, QSVP provides protection against quantum computer-enabled attacks.

Mutual Authentication: Verifying that only legitimate, registered vehicles participate in platoon communications is important to prevent unauthorized access to platoon's communications. In QSVP, before data transfer, $\mathcal{F}_i$ and the $\mathcal{L}$ authenticate each other using PQKEM. Similarly, the $\mathcal{L}$ and the $\mathcal{R}$ authenticate each other using PQKEM and the $\mathcal{R}$ and the $\mathcal{S}$ authenticate each other using QKD before data transfer. Thus, QSVP ensures mutual authentication between the participants before data transfer.

Perfect Forward Secrecy: Perfect forward secrecy guarantees the security of past session keys even if long-term secret keys are known to an adversary [77], [79]. An adversary can capture all exchanged messages and wait for the long-term secret key leakage. Then, the adversary may compute the session keys from the long-term secret key and decode the captured messages if the protocol does not offer perfect forward secrecy [79]. Hence, random secrets must also be used to compute the session key [79]. In QSVP, a session key $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$ is established between $\mathcal{F}_i$ and the $\mathcal{L}$. Similarly, a session key $k = h(ID_L \parallel k_1 \parallel k_2)$ is established between the $\mathcal{L}$ and the $\mathcal{R}$. Ephemeral numbers x_j, y_j, sk_1, and sk_2, in addition to ID_L, are used in the computation of sk. Similarly, ephemeral numbers k_1 and k_2, in addition to ID_L, are used in the computation of k. Hence, even if the long-term credential, ID_L, is leaked, the adversary cannot compute the previous session keys because the ephemeral numbers, which change in every session, are also used to compute session keys.

Ephemeral Secret Leakage Protection: Session keys must be secure even if ephemeral secrets are leaked to an adversary. In QSVP, a session key $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$

TABLE II
COMPARISON BASED ON SECURITY FEATURES

Scheme	S1	S2	S3	S4	S5	S6	S7	S8	S9
Junaidi et al. [35]	N	Y	Y	Y	Y	Y	Y	Y	N
Lai et al. [37]	N	Y	Y	Y	Y	Y	Y	Y	N
Xie et al. [39]	N	Y	Y	Y	Y	Y	Y	Y	Y
Wang and Liu [40]	N	Y	Y	Y	Y	Y	Y	Y	Y
Bagga et al. [42]	N	Y	Y	Y	Y	Y	N	N	N
Wang et al. [54]	N	Y	Y	Y	Y	Y	Y	Y	N
QSVP	Y	Y	Y	Y	Y	Y	Y	Y	Y

S1: Protection against quantum computer-enabled attacks;
S2: Mutual authentication;
S3: Session key; **S4:** Replay attack protection;
S5: Protection against impersonation attacks;
S6: Eavesdropping attack protection;
S7: Anonymity; **S8:** Privacy; **S9:** Unlinkability

is established between $\mathcal{F}_i$ and the $\mathcal{L}$. Similarly, a session key $k = h(ID_L \parallel k_1 \parallel k_2)$ is established between the $\mathcal{L}$ and the $\mathcal{R}$. Long-term credential, ID_L is used in the computation of sk and k in QSVP. Hence, even if the ephemeral secrets x_j, y_j, sk_1, and sk_2, k_1 and k_2 are leaked, the adversary cannot calculate the session keys without knowing the long-term credential. Thus, the proposed protocol ensures that the session key is secure even if the ephemeral secrets are leaked.

Session Key Agreement: QSVP enables the generation of a session key $sk = h(ID_L \parallel x_j \parallel y_j \parallel sk_1 \parallel sk_2)$ between $\mathcal{F}_i$ and the $\mathcal{L}$ after mutual authentication. Similarly, a session key $k = h(ID_L \parallel k_1 \parallel k_2)$ is generated between the $\mathcal{L}$ and the $\mathcal{R}$ after mutual authentication. Thus, QSVP provides session key security.

Replay Attack Protection: In a replay attack, an adversary captures messages and replays them later. The parameters used, e.g., random numbers from $\mathcal{F}_i$, the $\mathcal{L}$, the $\mathcal{R}$, and $\mathcal{S}$ are changed during each authentication session. As a result, the adversary cannot replay the previous messages successfully with QSVP. This shows that QSVP provides protection against replay attacks.

Protection Against Impersonation Attacks: To impersonate $\mathcal{F}_i$ and to get authenticated during mutual authentication between $\mathcal{F}_i$ and the $\mathcal{L}$, the adversary must compose a valid message $A_1 = \{PID_{Fi}, c_j, x_j, P_1\}$ and send it to the $\mathcal{L}$. Similarly, to impersonate the $\mathcal{L}$ and to get authenticated during mutual authentication between the $\mathcal{L}$ and the $\mathcal{R}$, the adversary must compose a valid message $M_{A1} = \{PID_L, c_1, s_1, I_1\}$ and send it to the $\mathcal{R}$. However, the parameters required to compose valid messages are not accessible to A. As a result, QSVP protects against impersonation attacks.

Eavesdropping Attack Protection: Before sending data $Data_F$ to the $\mathcal{L}$, $\mathcal{F}_i$ encodes it as $Data_F^* = Data_F \oplus sk$. Similarly, before sending data $Data_L$ to the $\mathcal{R}$, the $\mathcal{L}$ encodes it as $Data_L^* = Data_L \oplus k$ and before sending it to the $\mathcal{S}$, the $\mathcal{R}$ encodes it as $Data_R = Data_L \oplus k_{QKD}$. As a result, even if the attacker eavesdrops on the messages, since the messages are encoded, the attacker will not be able to decode and understand the data. As a result, the proposed protocol protects against eavesdropping attacks.

Anonymity: Pseudo-identities of vehicles are used during the authentication phase, thereby maintaining their anonymity. In Section IV-F (Data transfer between the follower and the leader), $\mathcal{F}_i$ sends $M_{D1} = \{PID_{Fi}, r_1, t_F, h_1, Data_F^*\}$ to the $\mathcal{L}$. Here, $\mathcal{F}_i$ does not send its real identity ID_{Fi} and instead sends the pseudo-identity PID_{Fi} so that it remains anonymous. However, if the same pseudo-identity is reused, multiple sessions of $\mathcal{F}_i$ will be linkable. The pseudo-identities must be changed in each iteration of the protocol so that the messages are unlinkable and the protocol offers strong anonymity. Hence, the pseudo-identity of $\mathcal{F}_i$ is updated as $PID_{Fi}^{new} = PID_{Fi} \oplus sk$ for the next protocol iteration. Thus, QSVP offers strong anonymity.

Privacy: Platoon communications involve the exchange of sensitive data about the location, speed, and direction of the vehicles in the platoon. QSVP ensures that data exchanged between vehicles, RSUs, and the server is only accessible to authorized parties. This prevents unauthorized tracking and eavesdropping and thus ensures data privacy.

Unlinkability: The parameters and pseudo-identities of vehicles used in each authentication session are not repeated. Thus, different authentication sessions of the same vehicle are not linkable.

VI. PERFORMANCE ANALYSIS

In this section, first, we compare the proposed protocol with other existing protocols in terms of the achieved security properties. Subsequently, we analyze the computation and communications costs of the proposed protocol and compare them with those of other protocols. Finally, we discuss details of the QKD system simulation and the costs associated with establishing and maintaining the QKD links.

A. Security Properties

A summary of the comparison of the security features of various protocols (mentioned earlier in Section I.A) is given in Table II. The main security feature that differentiates the proposed protocol from other protocols is that it provides post-quantum security. In addition to that, the proposed protocol offers mutual authentication between the participants, anonymity, privacy, session key agreement, and protection from replay, impersonation, and eavesdropping attacks. Hence, the proposed protocol offers conventional security features and post-quantum security by using the PQKEM and QKD techniques. The protocol proposed in [35] reuses some parameters in every session. Hence, it does not guarantee unlinkability between sessions. Similarly, the protocol in [37] also does not offer unlinkability between different sessions of the protocol. The protocol in [42] does not offer anonymity, unlinkability, and privacy. It can be concluded that though the protocols in [35], [37], [39], [40], [42], and [54] offer some of the security features, some of them do not meet all the imperative security properties and none of them provide post-quantum security. On the other hand, QSVP offers all the imperative security properties and provides robust post-quantum security.

B. Computation Cost

In this subsection, we analyze QSVP's computation cost and compare it with that of six recent protocols. Since the vehicles and the RSU must register with the server only once, the registration phase of QSVP is executed only once for each

TABLE III
COMPARISON OF COMPUTATION COST

Scheme	Vehicle	RSU / Server
Junaidi et al. [35]	$2t_s + 2t_v + 3t_{sm} + 2t_h = 5.32$ ms	$2t_s + 2t_v + 3t_{sm} + 2t_h = 5.32$ ms
Lai et al. [37]	$5t_h = 1.35$ ms	$7t_h = 1.89$ ms
Xie et al. [39]	$5t_h + 5t_{sm} = 6.95$ ms	$4t_h + 5t_{sm} = 6.68$ ms
Wang and Liu [40]	$4t_{sm} + t_{bp} = 8.7$ ms	$t_s = 0.32$ms
Bagga et al. [42]	$6t_{sm} + 2t_{pa} + 8t_h = 9.12$ ms	$5\ t_{sm} + t_{pa} + 8t_h = 7.88$ ms
Wang et al. [54]	$4t_{sm} + 2t_{pa} + 6t_h = 6.34$ ms	$6\ t_{sm} + 2t_{pa} + t_m + 5t_h = 8.31$ ms
QSVP	$t_{encap} + t_{decap} + 3t_h = 3.57$ ms	$t_{encap} + t_{decap} + 3t_h = 3.57$ ms

participant. However, the mutual authentication phase is executed whenever data is sent to the server. Hence, the computation cost of QSVP mainly depends on the computation cost during the mutual authentication phase. Hence, we only evaluate the computation cost of the mutual authentication phase. When the $\mathcal{L}$ sends data to the $\mathcal{S}$, the $\mathcal{L}$ executes one decapsulation, one encapsulation, and three hash operations. Since the time taken by the XOR and concatenation operations is negligible, we do not consider them for the computation cost calculation. The $\mathcal{R}$ executes one decapsulation, one encapsulation, and three hash operations during one iteration of the authentication phase. The simulations are carried out on a personal computer with Intel (R) Core (TM) i5-11320H @3.20GHz and 8GB of RAM. We use liboqs [72] which is an open source C library for quantum-safe KEM under the MIT license. The implementations of algorithms in liboqs are based on the resources from the NIST post-quantum cryptography standardization project [72].

To calculate the time required to execute various cryptographic operations, we use MIRACL [73]. Let t_h, t_{encap}, and t_{decap} represent the time taken by hash, encapsulation, and decapsulation operations, respectively. From the analysis, $t_h = 0.27$ ms, $t_{encap} = 1.34$ ms, and $t_{decap} = 1.42$ ms. The time taken by the leader vehicle is $t_{encap} + t_{decap} + 3t_h = 3.57$ ms during authentication. Similarly, the time taken by the RSU/server is $t_{encap} + t_{decap} + 3t_h = 3.57$ ms during authentication.

Next, we analyze the computation costs of QSVP and other similar protocols. We consider protocols in [35], [37], [39], [40], [42], and [54] for the comparison. Let t_s, t_v, t_{sm}, t_{bp}, and t_{pa} represent the time taken by signature generation, signature verification, scalar multiplication, bilinear pairing, and point addition operations, respectively. From the experiments, $t_s = 0.32$ ms, $t_v = 0.39$ ms, $t_{sm} = 1.12$ ms, $t_{bp} = 2.11$ ms, and $t_{pa} = 0.12$ ms. The computation costs of various protocols are summarised in Table III.

We have also plotted the computation costs (in ms) at the vehicle and at the RSU/server in Figs. 7 and 8, respectively. Further, computation cost is plotted against the number of platoons in Fig. 9. Though the computation cost at RSU/Server of QSVP is slightly higher than that of protocols in [37] and [40], QSVP offers more security features as shown in Table II. Hence, the computation cost of QSVP is justified.

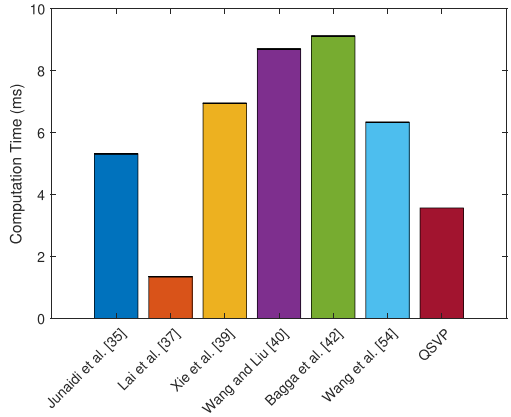


Fig. 7. Computation cost at the vehicle.

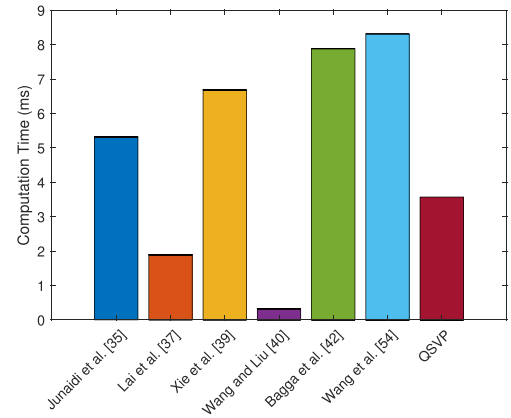


Fig. 8. Computation cost at RSU/server.

C. Communication Cost

Next, we perform a comparison analysis of the communication costs of QSVP with the protocols during mutual authentication. The protocols considered for comparison are [35], [37], [39], [40], [42], and [54]. We consider the lengths of the identity of the vehicle, the hash function, the timestamp, and the random nonce as 32, 160, 160, 32, and 160 bits, respectively. Hence, the communication cost during mutual authentication of QSVP is 1000 bits. The communication costs of the protocols in [35], [37], [39], [40], [42], and [54] are 1232, 1312, 1344, 1792, 1856, and 1376 bits, respectively. Fig. 10 shows communication costs (in bits) of various schemes. Communication cost is plotted against the number of platoons in Fig. 11. Figs. 10 and 11 show that QSVP has the lowest communication cost compared to other similar schemes.

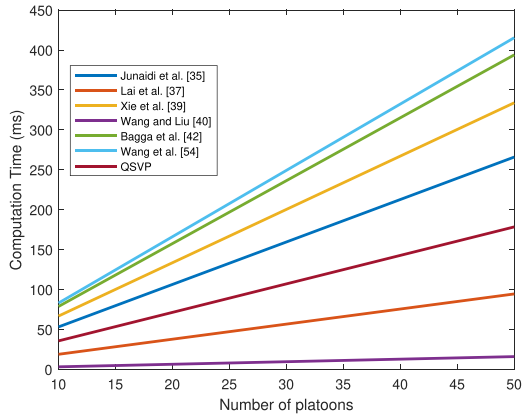


Fig. 9. Computation cost at RSU/server as a function of number of platoons.

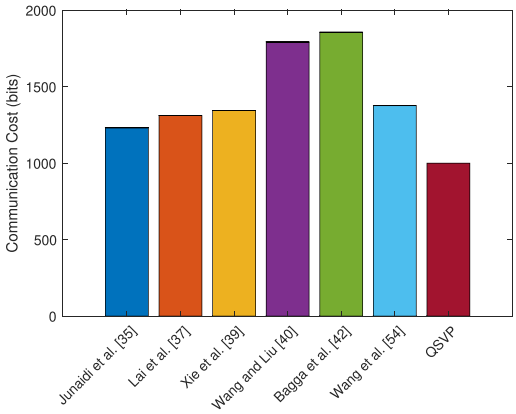


Fig. 10. Communication cost.

D. QKD System Simulation

In this subsection, we present the details of the evaluation of the QKD system using realistic experimental parameters to demonstrate how QKD can be implemented.

1) QKD System: To assess the feasibility of using QKD technology in QSVP, we provide a simulation of the BB84 protocol using realistic experimental settings. The parameters for simulation are chosen from free-space quantum communication reported in [85], with a detection efficiency of 14.5%, a dark count rate of 6.02×10^{-6}, and a system misalignment error of 1.5%.

In QKD, the transmission distance is typically based on the unit of km. For example, the standard optical fibre has a typical transmission loss of 0.2 dB/km. Moreover, we assume the utilization of a single-photon source in the QKD system for simplicity in simulation and illustration. Nonetheless, it is important to note that the decoy state technique [86], [87], [88] can be easily integrated to enable the use of practical quantum sources, such as coherent states, in more realistic scenarios. Furthermore, we utilize quantum states prepared in the $\mathbb{Z}$-basis for key generation, with the probability of selecting $\mathbb{Z}$-basis states set to 50%. The simulation parameters are given in Table IV.

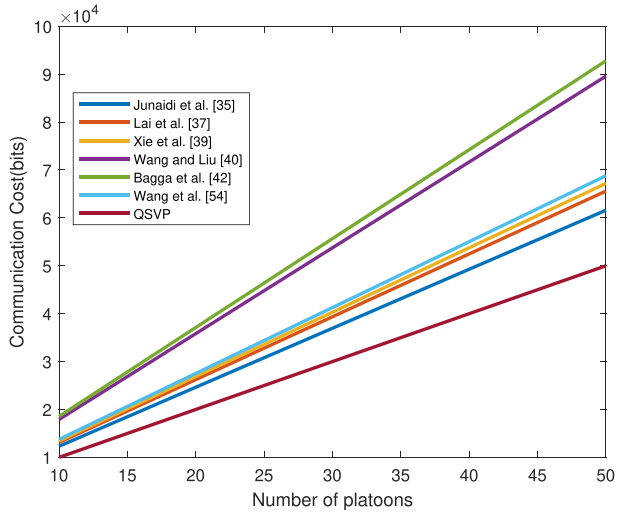


Fig. 11. Communication cost as a function of number of platoons.

TABLE IV
SIMULATION PARAMETERS

Parameter	Value
Detection efficiency	14.5%
Dark count rate	6.02×10^{-6}
System misalignment error	1.5%

The final secure key rate in its asymptotic form can be given by [89]:

$$R \geq Q_{\mathbb{Z}}(1 - fH_2(e_{\mathbb{Z}}) - H_2(e_{\mathbb{X}})),$$

where $Q_{\mathbb{Z}}$ represents the fraction of detection events when both Alice and Bob prepare and measure quantum states in the $\mathbb{Z}$-basis. $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary Shannon entropy. $e_{\mathbb{Z}}$ and $e_{\mathbb{X}}$ represent the bit error rates in the $\mathbb{Z}$-basis and $\mathbb{X}$-basis, respectively. f is the error correction efficiency.

In our system simulation, we deployed rate-adaptive low density parity check (LDPC) for information reconciliation, with an average error correction efficiency of 1.37. Then, Toeplitz hashing accelerated by fast Fourier transform was utilised for privacy amplification to obtain the final secure keys.

E. Costs Associated With Establishing and Maintaining the QKD Links

The costs associated with establishing QKD links represent a one-time infrastructure investment that provides long-term security guarantees against attacks from both classical and quantum adversaries. Once deployed, QKD networks can continuously generate quantum-secure keys without the recurring cryptographic upgrade costs that traditional systems may face in the post-quantum era.

Hardware Requirements: While QKD systems do require dedicated optical components and infrastructure, costs are decreasing with technological advances such as integrated photonic chips and improved manufacturing processes. Relevant discussions can be found in [90] and [91].

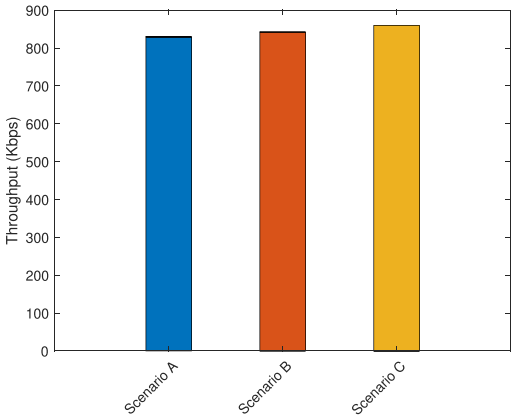


Fig. 12. Throughput.

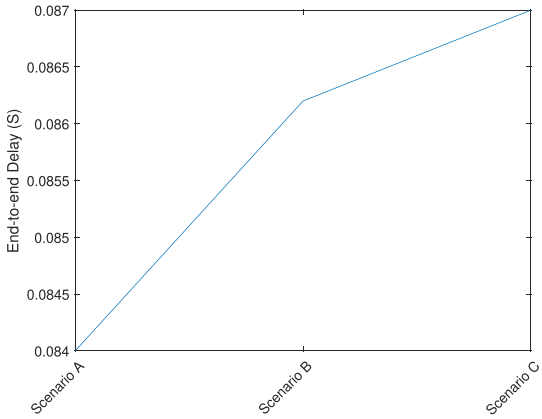


Fig. 13. End-to-end delay.

Key generation rate of QKD: State-of-the-art QKD experiment using integrated photonics technology has reported 1.213 Gbit per second at a 10 km transmission distance [91], providing a practical and cost-effective solution for the proposed authentication scheme in vehicular platoon communication.

Since these infrastructure considerations are orthogonal to our main contribution in the authentication protocol, we have focused our analysis on the protocol-level performance metrics that directly relate to our proposed improvements.

VII. Simulation of the Proposed Protocol Using NS3

In this section, we present the experimental details and results of the simulation of QSVP using the network simulator NS3 [92]. We measure the performance of QSVP using the metrics network throughput (in Kbps), end-to-end delay (in seconds), and Packet Delivery Ratio (PDR).

A. Simulation Settings

Simulations were conducted using NS 3.38 on Ubuntu 18.04.6 LTS. We consider three scenarios in the simulation: Scenario A with 20, Scenario B with 40, and Scenario C with 60 vehicles. In all three scenarios, we consider one RSU. The network simulation area was 1000 $\times$ 1000 m^2 and the simulation duration was 1800 s. The protocol was IEEE 802.11p and the mobility model was ConstantVelocityMobilityModel. The vehicles moved at 20 m/s, and the channel bandwidth was 6 Mbps.

B. Results

Throughput: Throughput is the amount of data (in bits) successfully transmitted over a network within a given unit of time. Throughput is calculated as $\frac{n_p \times n_i}{t}$ where n_p is the number of packets received, n_i is the size of the packet (number of bits) and t is the total time taken. From the simulation of QSVP, throughput values are 829.3 Kbps, 842.2 Kbps, and 859.8 Kbps for scenarios A, B, and C, respectively. Fig. 12 illustrates the network throughput (in Kbps) of QSVP under the scenarios A, B, and C. The number of exchanged messages increases with the number of vehicles. Hence, the throughput increases from Scenario A to Scenario C.

End-to-End Delay: End-to-end delay refers to the time it takes for packets to travel from the source to the destination. From the simulation of the proposed protocol, end-to-end delay values are 0.084 s, 0.0862 s, and 0.087 s for scenarios A, B, and C, respectively. Fig. 13 illustrates the end-to-end delay values for scenarios A, B, and C. The end-to-end delay in Scenario B is more than that in Scenario A. This is because there are more vehicles in Scenario B than in Scenario A. With the increase in the number of vehicles, more messages are exchanged, and hence, the congestion increases from Scenario A to Scenario B. Similarly, the end-to-end delay increases from Scenario B to Scenario C.

PDR: PDR is the proportion of packets successfully received at the destination compared to the total number of packets sent by the source. It is calculated using:

$$\text{PDR} = \frac{n_r}{n_s}$$

where n_r and n_s represent the number of packets received and packets sent by the sender, respectively. From the simulations, the PDRs for scenarios A, B, and C are 98.4%, 97.9%, and 96.8%, respectively. Fig. 14 illustrates the PDR for these three scenarios. The PDR results show that as the number of vehicles increases, congestion increases, and the PDR decreases.

C. NS-3 Evaluation With QKD Layer

In our NS-3 evaluation, the measured throughput and delay do not incorporate QKD-layer constraints such as secret-key rate, refresh intervals, and key exhaustion because we isolated and measured the network-layer performance of the proposed authentication protocol in the simulation. Since the focus of the experiments is the networking behaviour under the assumption of adequate key supply, the QKD layer is not considered. The QKD subsystem functions as an external key-generation service that runs independently and continuously in the background, supplying keys to the classical layer. Hence, secret key generation rate, refresh interval, and possible key exhaustion do

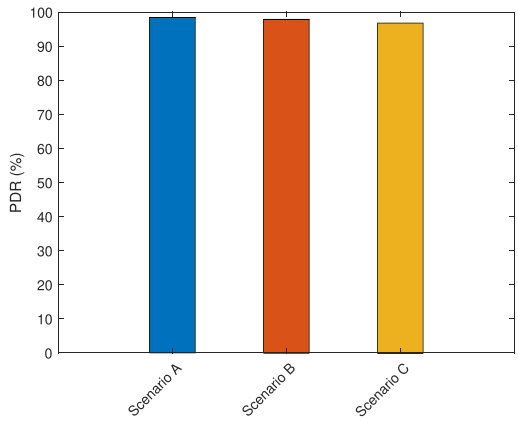


Fig. 14. Packet delivery ratio.

not affect the throughput and latency measurements. This is similar to practical deployments where QKD keys are typically buffered and stored for later use, to apply for One-Time-Pad or AES symmetric-key cryptographic operations. This is a standard industry approach used in commercial QKD systems (e.g., ID Quantique deployments). Additionally, QKD key rate performance is heavily dependent on hardware, distance, channel conditions, and vendor-specific implementations, which are orthogonal to assessing the efficiency of our authentication protocol. Therefore, our reported throughput and delay measurements reflect the properties of the proposed authentication protocol, independent of the variability and assumptions tied to specific QKD-layer implementations. The detailed rate–distance trade-offs of the QKD layer are out of scope for the throughput and delay results of the proposed protocol.

VIII. Conclusion

To ensure continued safety and reliability of vehicular platoon systems, it is important to protect vehicular platoon communications from threats arising from technological advancements. In this paper, we proposed a quantum secure mutual authentication protocol, QSVP, for vehicular platoon communications. The proposed protocol leverages PQKEM and QKD to withstand quantum attacks. This approach ensures that vehicular platoons can communicate securely even in the presence of evolving quantum threats while maintaining current security standards, providing a robust solution to a critical problem. Through formal and informal security analyses, we have demonstrated that QSVP is secure against classical and quantum computer-enabled attacks. We compared the computation cost of QSVP with that of similar schemes. The comparisons showed that QSVP's computation cost is reasonable and QSVP has the lowest communication cost compared to other similar schemes. We hope that QSVP not only enhances the security of vehicular platoon communications but also sets a precedent for future innovations in the security of vehicular communications.

References

[1] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proc. Int. Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, 2017, pp. 73–78, doi: 10.1145/3032970.3032987.

[2] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Veh. Commun.*, vol. 2, no. 2, pp. 110–123, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209615000145

[3] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, First Quarter 2016.

[4] S. Ellwanger and E. Wohlfarth, "Truck platooning application," in *Proc. 2017 IEEE Intell. Veh. Symp.*, 2017, pp. 966–971.

[5] S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh, D. Evans, and D. Price, "Vehicular platoon communication: Cybersecurity threats and open challenges," in *Proc. 51st Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops*, 2021, pp. 19–26.

[6] A. Ghosal et al., "Truck platoon security: State-of-the-art and road ahead," *Comput. Netw.*, vol. 185, 2021, Art. no. 107658.

[7] S. J. Taylor, F. Ahmad, H. N. Nguyen, and S. A. Shaikh, "Vehicular platoon communication: Architecture, security threats and open challenges," *Sensors*, vol. 23, no. 1, 2022, Art. no. 134.

[8] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.

[9] Z. Wang, G. Wu, and M. J. Barth, "A review on cooperative adaptive cruise control (CACC) systems: Architectures, controls, and applications," in *Proc. 21st Int. Conf. Intell. Transp. Syst.*, 2018, pp. 2884–2891.

[10] K. C. Dey et al., "A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CACC)," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 491–509, Feb. 2016.

[11] A. Balador, A. Bazzi, U. Hernandez-Jayo, I. de la Iglesia, and H. Ahmadvand, "A survey on vehicular communication for cooperative truck platooning application," *Veh. Commun.*, vol. 35, 2022, Art. no. 100460. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209622000079

[12] A. T. Sheik, C. Maple, G. Epiphaniou, and M. Dianati, "A comprehensive survey of threats in platooning–A cloud-assisted connected and autonomous vehicle application," *Information*, vol. 15, no. 1, 2023, Art. no. 14.

[13] W. Zeng, M. A. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1552–1571, Third Quarter 2016.

[14] R. Khan, A. Mehmood, H. Song, and C. Maple, "A decentralized, secure, and reliable vehicle platoon formation with privacy protection for autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 5, pp. 6441–6450, May 2025.

[15] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.

[17] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying grover's algorithm to AES: Quantum resource estimates," in *Proc. Post-Quantum Cryptogr.*, 2016, pp. 29–43.

[18] R. Asif, "Post-Quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021.

[19] "National Institute of Standards and Technology, U.S. Department of Commerce," Accessed: Mar. 2025. [Online]. Available: https://www.nist.gov/

[20] "Post-Quantum Cryptography (PQC) standardization," 2024. Accessed: Mar. 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[21] J. Bos et al., "CRYSTALS-kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Secur. Privacy*, 2018, pp. 353–367.

[22] "CRYSTALS-kyber algorithm," 2023. Accessed: Jan. 2024. [Online]. Available: https://www.ibm.com/docs/en/zos/2.5.0?topic=cryptography-crystals-kyber-algorithm

[23] M. Kumar and P. Pattnaik, "Post quantum cryptography (PQC)–An overview," in *Proc. IEEE High Perform. Extreme Comput. Conf.*, 2020, pp. 1–9.

[24] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[25] L. Sattler and D. Pacella, "Quantum key distribution (QKD): Safeguarding for the future," 2022. Accessed: Feb. 2023. [Online]. Available: https://www.comsoc.org/publications/ctn/quantum-key-distribution-qkd-safeguarding-future

[26] N. Xu et al., "An efficient and multi-dimensional privacy-preserving platoon communication scheme in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 5, pp. 6831–6847, May 2025.

[27] C. Zhang et al., "TPPR: A trust-based and privacy-preserving platoon recommendation scheme in VANET," *IEEE Trans. Serv. Comput.*, vol. 15, no. 2, pp. 806–818, Mar./Apr. 2022.

[28] R. Li et al., "RPPM: A reputation-based and privacy-preserving platoon management scheme in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 6, pp. 6147–6160, Jun. 2024.

[29] H. Cheng, X. Zhang, J. Yang, and Y. Liu, "PPRT: Privacy preserving and reliable trust-aware platoon recommendation scheme in IoV," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4922–4933, Sep. 2023.

[30] Z. Liu et al., "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 74, no. 2, pp. 1877–1892, Feb. 2025.

[31] K. Bian, G. Zhang, and L. Song, "Toward secure crowd sensing in vehicle-to-everything networks," *IEEE Netw.*, vol. 32, no. 2, pp. 126–131, Mar./Apr. 2018.

[32] C. Dickey et al., "Wiggle: Physical challenge-response verification of vehicle platooning," in *Proc. Int. Conf. Comput. Netw. Commun.*, 2023, pp. 54–60.

[33] C. Vaas, M. Juuti, N. Asokan, and I. Martinovic, "Get in line: On-going co-presence verification of a vehicle formation based on driving trajectories," in *Proc. IEEE Eur. Symp. Secur. Privacy*, 2018, pp. 199–213.

[34] M. Plattner, E. Sonnleitner, and G. Ostermayer, "A security protocol for vehicle platoon verification using optical camera communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 10, pp. 14698–14709, Oct. 2024.

[35] D. R. Junaidi, M. Ma, and R. Su, "Secure vehicular platoon management against sybil attacks," *Sensors*, vol. 22, no. 22, 2022, Art. no. 9000.

[36] F. Gonçalves et al., "Secure management of autonomous vehicle platooning," in *Proc. 14th ACM Int. Symp. QoS Secur. Wireless Mobile Netw.*, 2018, pp. 15–22.

[37] C. Lai, R. Lu, and D. Zheng, "SPGS: A secure and privacy-preserving group setup framework for platoon-based vehicular cyber-physical systems," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3854–3867, 2016.

[38] M. H. Basiri, M. Pirani, N. L. Azad, and S. Fischmeister, "Security of vehicle platooning: A game-theoretic approach," *IEEE Access*, vol. 7, pp. 185565–185579, 2019.

[39] Q. Xie, Z. Ding, and P. Zheng, "Provably secure and anonymous V2I and V2V authentication protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7318–7327, Jul. 2023.

[40] P. Wang and Y. Liu, "SEMA: Secure and efficient message authentication protocol for VANETs," *IEEE Syst. J.*, vol. 15, no. 1, pp. 846–855, Mar. 2021.

[41] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May/Jun. 2022.

[42] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, Feb. 2021.

[43] C. Lai, G. Li, and D. Zheng, "SPSC: A secure and privacy-preserving autonomous platoon setup and communication scheme," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, 2021, Art. no. e3982.

[44] R. P. Parameswarath and B. Sikdar, "Mutual authentication protocol for secure vehicular platoon admission," in *Proc. IEEE 100th Veh. Technol. Conf.*, 2024, pp. 1–6.

[45] W. Li, C. Meese, H. Guo, and M. Nejad, "Aggregated zero-knowledge proof and blockchain-empowered authentication for autonomous truck platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 9309–9323, Sep. 2023.

[46] X. Yan, M. Ma, and R. Su, "Efficient group handover authentication for secure 5G-based communications in platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3104–3116, Mar. 2023.

[47] Y. Zhao, Y. Wang, Y. Liang, H. Yu, and Y. Ren, "Identity-based broadcast signcryption scheme for vehicular platoon communication," *IEEE Trans. Ind. Informat.*, vol. 19, no. 6, pp. 7814–7824, Jun. 2023.

[48] Y. Zhao, H. Yu, Y. Yang, L. Xu, S. Pan, and Y. Ren, "Flexible and secure cross-domain signcrypted data authorization in multi-platoon vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 3, pp. 3166–3176, Mar. 2024.

[49] H. Abulkasim, B. Goncalves, A. Mashatan, and S. Ghose, "Authenticated secure quantum-based communication scheme in Internet-of-Drones deployment," *IEEE Access*, vol. 10, pp. 94963–94972, 2022.

[50] D. Mishra et al., "Quantum-safe secure and authorized communication protocol for Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16499–16507, Dec. 2023.

[51] S. Zemmoudj, N. Bermad, and L. Bouallouche-Medjkoune, "Detection and mitigation of vehicle platooning disruption attacks," *Veh. Commun.*, vol. 47, 2024, Art. no. 100765.

[52] F. Jiang, B. Qi, T. Wu, K. Zhu, and L. Zhang, "CPSS: CP-ABE based platoon secure sensing scheme against cyber-attacks," in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 3218–3223.

[53] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," *Comput. Commun.*, vol. 122, pp. 59–75, 2018.

[54] J. Wang, L. Wu, H. Wang, K.-K. R. Choo, L. Wang, and D. He, "A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24398–24416, Dec. 2022.

[55] D. S. Gupta, S. H. Islam, M. S. Obaidat, A. Karati, and B. Sadoun, "LAAC: Lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3620–3627, Sep. 2021.

[56] D. Chaudhary, U. Kumar, and K. Saleem, "A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ECC cryptography," *IEEE Access*, vol. 11, pp. 136947–136957, 2023.

[57] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, 2002, Art. no. 145.

[58] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, 2009, Art. no. 1301.

[59] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, 2020, Art. no. 025002.

[60] M. Peev et al., "The SECOQC quantum key distribution network in vienna," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001.

[61] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, 2011, Art. no. 10387.

[62] S. Wang et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, 2014, Art. no. 21739.

[63] Y.-H. Yang et al., "All optical metropolitan quantum key distribution network with post-quantum cryptography authentication," *Opt. Exp.*, vol. 29, no. 16, 2021, Art. no. 25859 .

[64] S.-K. Liao et al., "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, 2018, Art. no. 030501.

[65] S. Wang et al., "Twin-field quantum key distribution over 830-km fibre," *Nat. Photon.*, vol. 16, pp. 154–161, 2022.

[66] Y. Liu et al., "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, 2023, Art. no. 210801.

[67] H. Chun et al., "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Exp.*, vol. 25, no. 6, pp. 6784–6795, 2017.

[68] G. Vest et al., "Quantum key distribution with a hand-held sender unit," *Phys. Rev. Appl.*, vol. 18, no. 2, 2022, Art. no. 024067.

[69] J.-P. Bourgoin et al., "Free-Space quantum key distribution to a moving receiver," *Opt. Exp.*, vol. 23, no. 26, pp. 33437–33447, 2015.

[70] G. Tasopoulos, J. Li, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld, "Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems," in *Proc. Int. Conf. Inf. Secur. Pract. Exp.*, 2022, pp. 432–451.

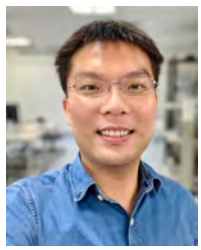
[71] M. Mehic et al., "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 302–346, First Quarter 2024.

[72] "Liboqs," 2025. Accessed: Jan. 2024. [Online]. Available: https://openquantumsafe.org/liboqs/

[73] "MIRACL cryptographic SDK," 2019. Accessed: Jan. 2024. [Online]. Available: https://github.com/miracl/MIRACL

[74] "Kyber post-quantum KEM," 2024. Accessed: Nov. 2025. [Online]. Available: https://www.ietf.org/archive/id/draft-cfrg-schwabe-kyber-04.html
[75] L.-J. Wang et al., "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Inf.*, vol. 7, no. 1, May 2021, Art. no. 67.
[76] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[77] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2001, pp. 453–474.
[78] A. Shahidinejad and D. Abbasinezhad-Mood, "Ultra-lightweight and secure blockchain-assisted charging scheduling scheme for vehicular edge networks by utilization of NanoPO NEO," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8116–8123, Aug. 2022.
[79] A. Shahidinejad and J. Abawajy, "An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT," *ACM Comput. Surv.*, vol. 56, 2024, Art. no. 186, doi: 10.1145/3645087.
[80] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr.*, Les Diablerets, Switzerland, 2005, pp. 65–84.
[81] W. Y. Kon and C. C. W. Lim, "Provably secure symmetric private information retrieval with quantum cryptography," *Entropy*, vol. 23, no. 1, 2020, Art. no. 54.
[82] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
[83] S. J. Lomonaco, "A quick glance at quantum cryptography," *Cryptologia*, vol. 23, no. 1, pp. 1–41, 1999.
[84] K. Ouafi and R. C. W. Phan, "Privacy of recent RFID authentication protocols," in *Proc. 4th Int. Conf. Inf. Secur. Pract. Exp.*, Sydney, Australia, 2008, pp. 263–277.
[85] R. Ursin et al., "Entanglement-based quantum communication over 144 km," *Nature Phys.*, vol. 3, no. 7, pp. 481–486, 2007.
[86] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, 2003, Art. no. 057901.
[87] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504.
[88] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230503.
[89] G. Daniel, L. Hoi-Kwong, L. Norbert, and P. John, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, no. 5, pp. 325–360, 2004.
[90] G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nature Photon.*, vol. 13, no. 12, pp. 839–842, 2019.
[91] S. Q. Ng, F. Kanitschar, G. Zhang, and C. Wang, "Gigabit-rate quantum key distribution on integrated photonic chips," 2025, *arXiv:2504.08298*.
[92] "ns-3," 2024. Accessed: Sep. 2024. [Online]. Available: https://www.nsnam.org/releases/ns-3-42/

Rohini Poolat Parameswarath (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. She was a Software Engineer with multinational companies. She was part of the cybersecurity research team with the Singapore University of Technology and Design, Singapore. She is currently a Cybersecurity Researcher with the National University of Singapore. She is passionate about finding solutions to the current challenges in the cybersecurity landscape. Her research interests include protocols for security and privacy in vehicular environments, cyberattack detection, privacy, and authentication protocols in domains, such as the Internet of Things (IoT), cyber-physical systems, and vehicular networks. Her papers have been published in prestigious journals and conferences.



Chao Wang received the B.Sc. degree in physics from the Huazhong University of Science and Technology, Wuhan, China, in 2013, and the Ph.D. degree in physics from the University of Science and Technology of China, Hefei, China, in 2018. He is currently a Research Assistant Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include quantum communication, quantum cryptography, and quantum networks.

Biplab Sikdar (Fellow, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. From 2001 to 2007, he was an Assistant Professor and Associate Professor from 2007 to 2013 with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute from 2001 to 2013. He is currently a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he also serves as the Head of the Department of Electrical and Computer Engineering. He was the recipient of the NSF CAREER Award, Tan Chin Tuan fellowship from NTU Singapore, Japan Society for Promotion of Science fellowship, and Leiv Eiriksson fellowship from the Research Council of Norway. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. He is a member of Eta Kappa Nu and Tau Beta Pi. He has served as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE INTERNET OF THINGS JOURNAL. He is an IEEE COMSOC, VTS Distinguished Lecturer, and ACM Distinguished Speaker.