Research Article

A Privacy Preserving Authentication Protocol Using Quantum Computing for V2I Authentication in Vehicular Ad Hoc Networks

Kumar Prateek, 1 Fahiem Altaf, 1 Ruhul Amin, 2 and Soumyadev Maity 1

1 Indian Institute of Information Technology Allahabad, Prayagraj, India
2 Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India

Correspondence should be addressed to Ruhul Amin; ruhul@iiitnr.edu.in

Received 1 October 2021; Revised 13 December 2021; Accepted 4 February 2022; Published 4 March 2022

Copyright © 2022 Kumar Prateek et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Many cryptographic techniques have been proposed to conceive a secure and privacy-oriented vehicular ad hoc network (VANET) for its practical deployment. The security of these techniques requires a common secret key to be shared between the communicating entities or depend upon the premise that some mathematical problems are computationally hard. However, because of the open nature of the wireless medium, the communication cannot be kept confidential and is prone to eavesdropping. Furthermore, with the arrival of quantum computers, these techniques are prone to quantum attacks—the time complexity of the assumed hard problem gets reduced from millions of years to a few seconds. In this paper, we propose a conditional privacy-preserving authentication scheme based on a quantum key distribution protocol for vehicle-to-infrastructure (V2I) communication. Our scheme inherits the properties of the quantum key distribution protocol. It does not require a secret authentication key to be transmitted conventionally and is resistant to quantum attacks. Apart from protecting VANETs against generic security threats, including node impersonation, message tampering, and repudiation, our scheme defends VANETs against man-in-the-middle attacks, replay attacks, etc. Besides, our protocol ensures message unlinkability, vehicle-identity privacy, and vehicle traceability if a vehicle misbehaves. The results obtained from the performance evaluation of our scheme confirm reasonable values of information leakage, key length, bit error probability, etc.

1. Introduction

Recently, vehicular ad hoc networks (VANETs) [1–3] have received considerable attention from industry, academia, and governments worldwide. A typical VANET comprises fast-moving, self-organizing vehicles that exchange information over the wireless channel. By exploiting the received information, many applications are being deployed for commuter safety and convenience, traffic management, and commercial purposes. However, because of the open nature of the wireless channel, VANETs are prone to security risks, including vehicle impersonation, message tampering, and message-repudiation. Besides, vehicles are vulnerable to privacy attacks. For example, an ill-intentions party could track a vehicle from its transmitted messages with the help of publicly linkable identity information. Therefore, it is necessary to deploy procedures in order to conceive a truthful and privacy-oriented VANET [4–6]. Nevertheless, the privacy protection should not be absolute but conditional—the deployed procedure should allow identity disclosure if a vehicle misbehaves.

In literature, VANETs get safeguarded against security and privacy risks with the help of various techniques implemented using symmetric-key cryptography (SKC) [7–11], public-key cryptography (PKC) [12–17], or their combination. While using a generic symmetric key-based scheme such as Caesar’s [18] and one-time pad protocol [19], a vehicle may establish a unique secret key with all entities it intends to communicate with. The vehicle may derive this key from an initial seed value shared between the two pre-authenticated vehicles or can establish the key with the help of a trusted key distribution center (KDC). The security of these protocols depends on the robustness of the algorithm used and the secrecy of the key. Since VANETs are dynamic,
pre-authentication via a seed value is nearly impossible. On the other hand, KDC needs to establish the secret key securely to protect it from an eavesdropper and man-in-the-middle adversary.

The existence of trapdoor functions, which are easy to compute yet hard to invert without extra information, leads us to the techniques based on public key cryptography (PKC) [17]. PKC defends against the eavesdropping adversary without any need to share the common secret key between the communicating parties. Instead, Alice and Bob can easily verify the authenticity of messages exchanged using public keys of one another with no access to corresponding private keys. Yet, PKC-based techniques are slower than their symmetric key-based peers. However, the marriage of PKC with symmetric key-based protocols improves the efficiency when PKC gets employed only to distribute secret keys of symmetric key-based protocols. Once two parties share the common secret key, they can continue their communication using faster symmetric key-based protocol. The security of PKC-based algorithms are based on the premise that computation of a private key of a user from its public key is computationally hard, i.e., there exists no polynomial time algorithm to extract private keys from the corresponding public keys. The advancement in easy availability of computational resources, specifically the quantum computers, has paved the way for attackers to attack the classical PKC-based protocols, assuming their security on computationally hard problems.

The quantum cryptography [20–23], which combines quantum computations with classical cryptography, uses laws of physics and quantum mechanics for secure exchange of information between the participating parties. A quantum key exchange or distribution algorithm [24–29] does not depend on the computationally hard nature of some mathematical problem. Rather, it uses the laws of quantum mechanics to provide unconditional security. Such a key distribution has an edge over classical key distribution scheme because of its properties including impossibility for an eavesdropper to copy the quantum bits during transmission, no use of unbounded computational power to the attacker as it does not depend on computationally hard problem, and flexibility to participating parties to detect an eavesdropper, i.e., whether an attacker is observing data during transmission. This makes quantum key distribution a perfect candidate for key exchange in an open network like VANET.

The unconditional security of a quantum key distribution protocol arises because of: no-cloning theorem and Heisenberg Uncertainty Principle [30]. The no-cloning theorem prohibits an attacker from duplicating or copying the channel state of quantum bits (qubits) without preliminary information regarding bases [31]. Besides, in the absence of perfect prediction of sender’s random basis, an eavesdropper easily gets detected while eavesdropping on a quantum channel. Measuring of state in quantum computing destroys the state, which enables easy detection of the existence of eavesdroppers, alerting the participating parties that someone is trying to disturb the communication.

Recently, in Refs. [32–34], authentication protocols involving quantum key distributions have been proposed for various application areas, such as cloud computing etc. However, these protocols cannot provide the vehicle-identity privacy which is a crucial requirement in VANET scenarios. In these protocols, messages get transmitted using a single identity, thus risking the privacy of a user. Besides, authentication request sent by a vehicle to TA via RSU is susceptible to replay attack and could lead to impersonation attack. In this paper, we overcome these limitations and propose a new privacy-preserving authentication protocol for VANETs. Specifically, the contribution of this paper is as follows:

1. We propose a new conditional privacy-preserving authentication protocol for V2I communication in VANETs by employing quantum key distribution protocol and classical identity (CID)-based authentication. After registering its unique identity with a trusted authority (TA), both vehicle and TA execute a quantum key exchange protocol, resulting in both parties sharing a common secret key. Upon authenticating with a semi-trusted RSU via TA using the shared quantum secret, the vehicle receives key material as a set of pseudo-identities and secret keys from RSU. The vehicle then authenticates its outgoing messages by using the key material received from RSU.

2. We have comprehensively analyzed the security of the proposed scheme. Our analysis confirms that the proposed protocol successfully defends against the eavesdropping, replay attack, man-in-the-middle attack, etc., apart from ensuring message authentication, integrity and nonrepudiation. The proposed protocol also enables efficient traceability in case a vehicle misbehaves.

3. We have also evaluated the performance of our protocol by implementing it on QKD simulator [35]. The results obtained confirm that it performs reasonably regarding information leakage and key length.

The organization of the rest of the article is as follows. The basics of quantum computing and vehicular ad hoc networks (VANETs) are discussed in the preliminaries section. We investigated the related work in Section 2. We describe the background and design goal of the proposed protocol in Section 4. Section 5 describes the proposed privacy-preserving authentication protocol. Section 6 outlines privacy and security analysis, besides the evaluation of performance parameters with simulation results. Finally, Section 7 concludes the paper with future work.

2. Related Work

In this section, we discuss the existing work whose objectives are very similar to that of our proposed protocol and analyze their major limitations. The scheme proposed by Calandrillo et al. utilizes pseudonym to provide privacy using baseline pseudonym (BP) and group signature (GS), but the scheme suffers from the maintenance and distribution of
large certificate revocation list (CRL) [36]. Alazzawi and Lue tried to address the problem of VANETs by designing pseudo identities–based scheme to provide conditional anonymity, integrity, and authentication [37]. The scheme designed by Raya and Hubaux provides conditional privacy on public key infrastructure. The scheme stores different parameters like public key, private key pairs, and certificiates which result in the requirement of large storage capability of OBU’s in the vehicle [38]. Zhang et al. in their scheme address the problem of computational capabilities of OBU, i.e., they highlighted the inabilities of OBU to perform complex computations in short time. So, they proposed a method using bilinear pairings which not only allow the nearby RSU to assist the OBU in computations but also verify the messages[39].

Some message authentication schemes are also designed in VANETs using message authentication code, such as Lin et al. [40] and Rhim [41]. With the use of group signature [42], a conditional privacy-preserving authentication scheme is proposed by Wu et al. Also, a new privacy preserving scheme using hybrid cryptography gets proposed by Tangade et al. which abolishes the use of time-consuming CRL by utilizing public key infrastructure (PKI) for V2I preauthentication and HMAC for V2V authentication [43]. Privacy-preserving authentication along with group key agreement–based protocol is well discussed in Refs. [44, 45]. Various researchers also tried to leverage the power of cloud computing [46, 47] and fog computing in VANETS such as the proposal of a 3-layer architecture for fog-VANET in which the user vehicle acts as the data generation layer, RSU acts as intermediate fog nodes, and the cloud server as cloud Layer [48]. Use of the movable fog node by Ref. [49] for efficient V2V communication and traffic-related issues also have been proposed. A hybrid framework for vehicular cloud using fog computing in Ref. [50] is proposed which discusses various security issues such as authentication, privacy, availability of resources, etc. In addition, lightweight secure authentication and key agreement protocols are very well discussed in Refs. [51–54]. Leveraging authentication as service, a privacy-preserving implicit authentication framework utilizing cosine similarity and partial homomorphic public key encryption scheme is designed in Ref. [55]. The scheme resists the security and privacy threats of mobile intelligent terminals. Besides, the scheme [56] discusses a computationally efficient anonymous authentication framework enabling secure legitimacy inspection of authorized doctor, authorized patient, and medical experts with each other and features location privacy. Similarly, the scheme [57] constructs noninteractive zero knowledge scheme to protect data security and privacy of IoT devices responsible for collection and transmission of data in smart cities. Li et al. describe a novel lightweight privacy-preserving authentication protocol [58], which authenticates the vehicles guaranteeing anonymity, whereas Y. Wang et al. discuss the security issues and challenges related to fog computing, besides the comparison between cloud computing [59] and fog computing.

The fast-developing quantum computer brings hope for the increased application area of quantum computing. These days, different application areas such as simulation, machine learning, and transportation sector are exploring the use of quantum computing techniques. In quantum computation, the quantum key distribution (QKD) plays a pivotal role. Various protocols such as BB84 communication protocol [60], which utilizes quantum entanglement and no-cloning theorem, have the ability to encode a binary bit to quantum bits with the help of two polarizers, namely, circular polarizer and linear polarizer. The security and stability of these protocols are well discussed in Refs. [61–63]. A scheme [32] designed by Sharma and Kalra, namely, “Identity based secure authentication based on quantum key distribution for cloud computing” utilizes quantum key distribution and identity-based authentication for cloud infrastructure. Various researchers also discussed the authentication relying on quantum key distribution for cloud infrastructure in Refs. [64–66]. Also, Ref. [33] introduced a secure quantum algorithm which employs public key encryption to generate keys to enhance user authentication in quantum channel. In the scheme, Ref. [34] designed by Ankur and Karambir uses quantum key distribution and payload-based mutual authentication using elliptic curve cryptography (ECC) for Internet of things (IoT) devices. Using one-time quantum pad and five-particle cluster state, a secure quantum authentication and communication protocol gets discussed in Ref. [67]. In the scheme, [68], a novel enrollment and verification process for the entities of VANET using QKD gets investigated. However, this scheme is susceptible to replay attacks and does not preserve the privacy of a vehicle. In order to summarize the basic characteristics and the limitations of QKD network parameters, the practical implementation of the QKD network simulation module gets evaluated in network simulator NS-3 [69]. Although many QKD-based authentication protocols are available in the literature; they do not possess privacy preservation. This work aims to design a privacy-preserving QKD-based authentication protocol in VANETs.

3. Preliminaries

We aim this section to discuss the preliminarily concepts of quantum computing and vehicular ad hoc networks (VANETs).

3.1. Quantum Computing. This subsection summarizes quantum computing and summarizes the key quantum computing characteristics following a discussion on the basics of VANETs. The ability of the quantum computer to solve various problems such as integer factorization (IF) in a few seconds, which usually takes billions of years by classical computers, fascinate the extreme industry interest of major corporations such as Google Inc., Microsoft Inc., and Amazon Inc. The extreme industry interest will boost the arrival of a quantum computer to market much sooner than the expected time. The quantum computer comprises quantum chips rather than silicon chips used in classical computers.
3.1. Basics of Quantum Systems. Quantum mechanics works with complex numbers in contrast to real numbers. The generalization of the concept of bit, known as a qubit, gets used in quantum computing. As we know, the evolution of quantum systems is reversible and the bit is a way of describing the system that has two states, i.e., either 1 or 0, either true or false.

\[
\text{State}|0\rangle = [1, 0]^T, \\
\text{State}|1\rangle = [0, 1]^T. 
\] (1)

However, the above “either A (true/1) or B (false/0)” paradigm is not sufficient in the quantum world, i.e., any object can be in state A and state B simultaneously, which means there exists a system where the switch can be on and off at the same time. Therefore, a qubit is a way of describing a 2-D quantum system \([c_0, c_1]^T\) where

\[
|c_0|^2 + |c_1|^2 = 1, 
\] (2)

and \(|c_0|^2\) and \(|c_1|^2\) denote the probabilities that, after measuring qubit, it exists in state \(|0\rangle\) and state \(|1\rangle\), respectively. One can understand the implementation of the qubit in the universe by the fact that an electron might be in two different orbits around the nucleus. A photon may be in one of two polarized states. Therefore, there is an occurrence of enough quantum indeterminacy and superposition effects within all systems to represent qubits in the universe.

3.1.2. Architecture of Quantum Systems. The evolution of quantum systems is reversible, which means the manipulation that can be done must also be able to be undone. This undoing translates the architecture into reversible gates. All operations that are not measurements and represented by unitary matrices are reversible gates. Moreover, gates, such as identity gates, NOT gate, controlled NOT gate, Toffoli gate (similar to controlled NOT gate but with two controlling bits), and Fredkin gate, are classical examples of reversible gates which act as underlying hardware for quantum gate thus enabling quantum computations. Also, Toffoli and Fredkin gates are universal and unitary besides being reversible, but no-cloning theorem limits all quantum gates mimicking the fanout operation. Although in contrast to cloning, transportation of arbitrary quantum states from one system to another can be done.

3.1.3. Key Characteristics of Quantum Computing. The quantum computing harnesses the key behaviour of quantum mechanics, which is discussed in detail as follows:

(1) Superposition. It is also called as coherence which allows any particle to be in more than one state with some probability. We can better understand it with the light bulb example. In the usual scenario, one can either switch-on (state 1) or switch-off (state 0) the light bulb, but if the light bulb gets assumed to be a quantum particle, then it can be in both states with some probability, i.e., we can find the light bulb with probability \(P\) and probability \(Q\) in state 0 and state 1, respectively, where

\[
P + Q = 1, 
\] (3)
The detailed description of each component of VANETs is as follows:

(i) **Road Side Units (RSUs).** These devices have high computing and storage capabilities similar to servers. RSUs are located at junctions to facilitate accessible communication between vehicles and trusted authorities. In addition, RSUs feature quantum communication capabilities.

(ii) **Trusted Authority (TAs).** TAs acts as controlling authority and have exceptionally high computing and storage capabilities. We assume it to be trusted and it generates secret keys and uploads parameters to RSUs and the vehicle’s OBU. TA also manages the master certificate revocation list (MCRL). We assume that TA gets equipped with QPUs, hence enabling quantum communication through quantum channels.

(iii) **Onboard Units (OBU).** These are the embedded processing units assembled in a vehicle. They are used for periodically broadcasting vehicle information ranging from the position, driver location, acceleration, and traffic-related data on the road through DSRC protocol. The assumption of QPUs attached with OBU enables quantum communication capabilities to vehicle.

### 3.2.2. Types of Communication

(1) **Vehicle to Vehicle (V2V).** V2V communication occurs when the participating vehicles desire to exchange a message with each other. During V2V communication, safety messages get broadcasted.

(2) **Vehicle to Infrastructure (V2I).** V2I communication occurs when the vehicle communicates with RSUs or communicates with trusted authority through RSUs. During V2I communication, each vehicle gets pre-authenticated through RSUs, which are usually at junctions.

Both V2V and V2I communication occurs with the help of wireless technology, i.e., dedicated short-range communication (DSRC). With the availability of DSRC, any vehicle can quickly transfer messages (voice, image) even to moving targets within short physical proximity.

### 3.2.3. Challenges of VANETs.**

Vehicular ad hoc network comprises three entities out of which the vehicle’s OBU storage capacity is of enormous concern. Moreover, vehicle continuously moves, thus encountering the following challenges:

- **(1) Resource Constraint.** The OBUs of vehicles are not capable enough to perform high computations.

- **(2) Intermittent Connectivity.** The network management of vehicles in VANETs needs to be efficient, i.e., less number of network packets loss needs to be maintained.

- **(3) Support of Network Intelligence.** The future of VANETs needs to be equipped with some sort of intelligence to meet the demands of thousands of vehicle’s cooperation in a congested traffic scenario.

- **(4) Privacy Requirement.** The privacy of users is of extreme importance. The data and location information are enough for any attacker to act. The infrastructure needs to give flexibility to vehicles regarding the information they want to share.

### 4. Background of the Proposed Protocol

#### 4.1. Design Goal of the Proposed Protocol.**

For providing secure communication in VANETs, the design goal of any protocol must consider security and privacy as the primary aim. Due to an increase in computing resources, the attacker nowadays started injecting malicious codes easily for one’s personal benefit. Therefore, prevention of the following is the design goal in VANETs.
(i) Impersonation Attack. Whenever legitimate parameters get stolen and used by an adversary to create chaos in VANETs to fulfill one’s personal motive, it leads to impersonation attack.

(ii) Sybil Attack. Whenever adversary subverts the VANETs by generating many pseudonymous identities and uses them to get an enormous influence in network, it leads to Sybil attack. With many pseudo identities, the large pool of bogus message gets broadcasted.

(iii) Message Modification Attack. Whenever any vehicle broadcasts the message, the adversary edits or changes the content in the communication channel, leading to message modification attack. Also, whenever the changed content gets replaced with fake data, it is known as bogus information attack.

(iv) Message Replay Attack. Whenever the adversary delays or resends the message to create an illusion of accidents of packets to a legitimate vehicle, it is known as message replay attack.

(v) Denial of Service Attack (DoS). It is typically accomplished by flooding the network with superfluous requests in order to overload the network, thus preventing legitimate requests from being entertained.

Now, we discuss primary security requirements with conditional privacy to tackle the abovementioned threats.

(i) Source Authentication. To prevent outsider attacks, authentication is a primary feature which needs to be performed. Source authentication checked the assurance of legitimacy of sender nodes before communication. Successful source authentication prohibits message replay attack.

(ii) Message Integrity. Assurance of message integrity means that the message is not altered or tampered during communication, thus preventing attackers from performing a message modification attack.

(iii) Identity Privacy Preservation. The real identities of participating vehicles in VANETs are required to be anonymous while communicating with each other. Pseudo identities are used to fulfill this requirement. The identity privacy preservation of entity disallows the attacker from generating a legitimate pseudo identity thus prohibiting a Sybil attack.

(iv) Traceability. It is the capability to trace the real identities of those vehicles that are acting maliciously in order to mislead other vehicles or disrupting the vehicular networks thus avoiding an impersonation attack.

(v) Unlinkability. This ensures that linking of various messages originating from one particular vehicle is prohibited to malicious vehicle, thus leading to untraceability of the vehicle, thereby denying the possibility of DoS attack.

4.2. Conversion of Bits from One State to Another. Since the proposed protocol deals with quantum properties, it involves the use of the quantum bit. The use of photon polarization and interconversion rule enables the interconversion process between binary and quantum bits. We described the photon polarization with two sequences, namely, the decision sequence and the measurement sequence. Decision and measurement sequences both have the same polarization but perform different functions. Besides, the notations used in the proposed work are reported in Table 1.

4.3. Decision Sequence. The conversion of a binary bit into a quantum bit is accomplished by the decision sequence, which comprises two kinds of polarizers: linear polarizer and circular polarizer. Furthermore, linear polarizer gets denoted by horizontal | → ⟩ and vertical | ↑ ⟩ directions, whereas circular polarizer is denoted by | ↗ ⟩ and | ↖ ⟩ directions. We used L and C notations for denoting linear and circular polarizers, respectively. Also, both polarizers have two states which possess the orthogonality property, i.e., they are orthogonal to each other.

4.4. Interconversion Rule. We define the interconversion rule between a binary and quantum bit as:

\[
\begin{align*}
|\rangle & \leftrightarrow 0 \\
|\uparrow\rangle & \leftrightarrow 1 \\
|\leftarrow\rangle & \leftrightarrow 0 \\
|\downarrow\rangle & \leftrightarrow 1
\end{align*}
\]  

4.5. Measurement Sequence. Measurement sequence accomplishes the conversion of the quantum bit back to a binary bit. It comprises two types of polarizers, namely, rectilinear (R) and diagonal (D) polarizers. These two polarizers were used to measure quantum bits corresponding to the L and C polarizers of the decision sequence. Under the uncertainty principle, decision sequence and measurement sequence are conjugate bases, whereas rectilinear and linear as well as diagonal and circular polarizers are conjugate states, i.e., to get specific results, the receiver needs to measure the R polarizer with L polarizer only and D polarizer with C polarizer only. In addition, nonorthogonality between R and L, as well as D and C, makes them indistinguishable.

As shown in Table 2, the conversion of binary bit to quantum bit takes place. With the help of the decision sequence [LLCLCLCL], the binary bit [10100010] gets converted to quantum bit [\\(|\uparrow\rangle| \leftarrow\rangle \rightarrow |\downarrow\rangle| \downarrow\rangle \rightarrow |\leftarrow\rangle| \rightarrow\rangle \rightarrow |\uparrow\rangle| \leftarrow\rangle \rightarrow |\downarrow\rangle| \leftarrow\rangle \rightarrow |\uparrow\rangle| \leftarrow\rangle \rightarrow |\downarrow\rangle| \leftarrow\rangle \rightarrow |\uparrow\rangle| \leftarrow\rangle \rightarrow |\downarrow\rangle| \leftarrow\rangle \rightarrow |\uparrow\rangle| \leftarrow\rangle \rightarrow |\downarrow\rangle]| and then the pre-master secret gets produced after applying measurement basis [RDDRRDDDR]. We may note that the receiver randomly chose a measurement basis.

4.6. Encrypted Id. To protect the real id ID_v of the vehicle from the malicious attacker, we use the concept of encrypted id in our scheme, which is denoted by EncId_v.
Whenever biological characteristics of the user are XORed with NOT translation of the real id of the vehicle, then only we obtain 
EncId with NOT translation of the real id of the vehicle, then 
Whenever biological characteristics of the user are XORed

Table 1: Notations used in paper.

| Notation | Description |
|----------|-------------|
| C | Circular decision polarizer |
| L | Linear decision polarizer |
| R | Rectilinear measurement polarizer |
| D | Diagonal measurement polarizer |
| Id_i | The real identity of i\textsuperscript{th} vehicle |
| ID_i | The identity of i\textsuperscript{th} vehicle |
| | Vehicle’s entangled pairs of quantum bits entangled with |q_i\rangle |
| q_i >_i | TA’s entangled pairs of quantum bits entangled with |q_i\rangle |
| q_k >_k | RSU’s entangled pairs of quantum bits entangled with |q_k\rangle |
| q_k >_k | TA’s entangled pairs of quantum bits entangled with |q_k\rangle |
| V_i | Representing p\textsuperscript{th} vehicle, where (i = 0, ..., N) |
| MS_k | Randomly chosen measurement sequence corresponding to p\textsuperscript{th} vehicle |
| RSU_k | Representing k\textsuperscript{th} RSU, where (k = 0, ..., K) |
| DS_k | Random decision sequence of k\textsuperscript{th} RSU |
| | Vehicle’s entangled pairs of quantum bits, entangled with |q_{da}\rangle |
| | TA’s entangled pairs of quantum bits, entangled with |q_{da}\rangle |
| | RSU’s entangled pairs of quantum bits, entangled with |q_{da}\rangle |
| | TA’s entangled pairs of quantum bits, entangled with |q_{da}\rangle |
| EncKey_{v_i} | Encrypted key of i\textsuperscript{th} vehicle |
| EncKey_{k_i} | Encrypted key of k\textsuperscript{th} RSU |
| QEncKey_{v_i} | Encrypted query key of i\textsuperscript{th} vehicle |
| QEncKey_{k_i} | Encrypted query key of k\textsuperscript{th} RSU |

Table 2: Generation of the pre-master secret.

| Binary bit | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
|------------|---|---|---|---|---|---|---|---|
| Decision seq | L | L | C | C | L | C | C | L |
| Quantum bit | ↑ | → | ↖ | ↗ | → | ↗ | ↖ | → |
| Measurement seq | R | D | D | R | R | D | D | R |
| Pre-master secret | 1 | ? | 1 | ? | 0 | 0 | 1 | 0 |

Table 3: Generation of encrypted Id.

| Bit number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|------------|---|---|---|---|---|---|---|---|
| Vehicle identification | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Biological characteristics | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| Encrypted Id | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

4.7. Template and Encrypted Key Generation. The proposed scheme uses a decision sequence and a measurement sequence, which gets selected randomly by both parties involved in communication. After that, the decision sequence and measurement sequence together produce the template. In addition, the pre-master secret mentioned in the table comprises correct and incorrect binary bits. Therefore, the selection probability of the correct measurement sequence is 1/2\textsuperscript{k}, where k indicates the total length of the bit string. The green color shows the correct measurement base. Encrypted key [1000] gets generated with pre-master secret and template, as shown in Table 4.

5. Proposed Work

We propose a privacy-preserving authentication protocol for V2I communication, which utilizes the properties of quantum physics. The proposed protocol authenticates the vehicle with infrastructure and generates some secrets. These secrets enable further privacy-preserving V2I and V2V communication. The proposed protocol uses classical identity (CID)-based authentication and quantum key distribution to exchange keys with each other to secure privacy-preserving V2I communication.

The proposed scheme comprises four phases for V2I communication and two phases for V2V communication, which are described in detail as follows:
Table 4: Generation of encrypted key.

| Decision sequence | C | L | C | L | C | L | L |
|-------------------|---|---|---|---|---|---|---|
| Measurement sequence | R | D | D | R | R | D | D |
| Template           | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| Pre-master secret  | ? | ? | 1 | ? | 0 | 0 | 1 |
| Encrypted key      | ? | ? | 1 | ? | 0 | 0 | ? |

5.1. Phase 1: System Initialization. This phase includes the initialization process of all participating parties of VANETs, such as trusted authorities, roadside units, and vehicles.

5.1.1. Trusted Authority Initialization. The responsibility for generating the measurement sequence and the set of EPR entangled pair $|q_1\rangle >$ and $|q_2\rangle >$ is with trusted authority (TA). These two particles are entangled with each other, displaying entanglement property as discussed in preliminaries. During RSU and vehicle registration process, TA updates one’s database with the decision sequence, measurement sequence, and an encrypted key.

5.1.2. Road Side Unit Initialization. RSU obtains and unique id $ID_{rs}$ from TA. The detailed registration process of RSU is as follows:

(i) After obtaining the unique id $ID_{rs}$ from TA, RSU generates decision sequence $DS_{rs}$ and interconversion rule $IR_{rs}$ which converts the binary bit $ID_{rs}$ into a quantum bit. Classical channel is used to transfer decision sequence $DS_{rs}$ and interconversion rule $IR_{rs}$ to TA.

(ii) TA prepares a set of EPR entangled pair $|q_1\rangle >$ and $|q_2\rangle >$ into a set of EPR entangled pair $|q_1\rangle >$ and $|q_2\rangle >$. Finally, TA stores $|q_1\rangle >$ to itself and $|q_2\rangle >$ to RSU.

(iii) TA produces a measurement sequence $MS_{rs}$ randomly which measures $|q_1\rangle >$ quantum bit string, already available with the TA. As soon as $|q_1\rangle >$ quantum bit string gets measured, the EPR quantum bit string $|q_1\rangle >$ collapses into the same eigen state as the eigen states of $|q_1\rangle >$, quantum bit string. After that, RSU generates the quantum bit $|q_1\rangle >$ which corresponds to $|q_1\rangle >$, using $MS_{rs}$, thus collecting the same eigen state of $|q_1\rangle >$ because of the entanglement property, which has already been discussed in the preliminaries.

(iv) Now, RSU converts back $|q_1\rangle >$ into a binary string using the interconversion rule $IR_{rs}$ already available to RSU, thus generating a pre-master secret. Furthermore, TA compares decision sequence $DS_{rs}$ and measurement sequence $MS_{rs}$ to produce the template, as discussed in Table 4. In addition, TA generates the encrypted key $EncKey_{rs}$ with the help of the template and pre-master secret, as discussed in the previous section.

(v) Finally, TA saves the template, encrypted key $EncKey_{rs}$ in its database corresponding to $RSU_k$ for RSU authentication in V2I pre-authentication phase. Hence, RSU parameters after registration are: $RSU_k$ parameters: [$ID_{rs}$, Template, and $EncKey_{rs}$]

5.2. Vehicle Initialization. Vehicle obtains unique id $ID_{vi}$ from TA. With the received unique id $ID_{vi}$, it converts the unique id $ID_{vi}$ into encrypted id $EncId_{vi}$. The detail registration process of the vehicle is as follows:

(i) After converting the unique id into encrypted id $EncId_{vi}$, the vehicle generates a decision sequence $DS_{vi}$ and an interconversion rule $IR_{vi}$ which converts binary-bit $EncId_{vi}$ into quantum bit. Moreover, the vehicle uses classical channel to transfer decision sequence $DS_{vi}$ and interconversion rule $IR_{vi}$ to TA.

(ii) Meanwhile, TA prepares a set of EPR entangled pairs $|q_1\rangle >$ and $|q_2\rangle >$ for each quantum bit string obtained from $EncId_{vi}$. It may be noted that the length of entangled pairs $|q_1\rangle >$ and $|q_2\rangle >$ must be equal to the length of $EncID_{vi}$. Thereafter, TA separates the set of EPR entangled pair $|q_1\rangle >$ and $|q_2\rangle >$ into a set of EPR entangled pair $|q_1\rangle >$ and $|q_2\rangle >$. Finally, TA stores $|q_1\rangle >$ to its own quantum memory or database and sends $|q_2\rangle >$ to the vehicle.

(iii) TA produces a measurement sequence $MS_{vi}$ randomly which measures the $|q_1\rangle >$ quantum bit string, already available in the TA database. As soon as the $|q_1\rangle >$ quantum bit string gets measured, the EPR quantum bit string $|q_1\rangle >$ is collapsed into the same eigen state as the eigen states of $|q_1\rangle >$, quantum bit string. Thereafter, the vehicle $V_i$ measures the quantum bit $|q_1\rangle >$, which corresponds to $|q_2\rangle >$, using $MS_{vi}$, thus collecting the same eigen state of $|q_1\rangle >$ because of the entanglement property, which has already been discussed in the preliminaries.

(iv) Now, the vehicle converts back the quantum string $|q_1\rangle >$ into a binary string using the interconversion rule $IR_{vi}$ already available to a vehicle, thus generating a pre-master secret. Furthermore, TA compares decision sequence $DS_{vi}$ and measurement sequence $MS_{vi}$ to produce the template as discussed in Table 4. In addition, TA generates the encrypted key $EncKey_{vi}$ with the help of the template and pre-master secret, as described in the previous section.

(v) Finally, TA saves template, encrypted key $EncKey_{vi}$ corresponding to vehicle $V_i$ in its database for vehicle authentication in V2I pre-authentication phase. Hence, vehicle parameters after registration are: $V_i$ parameters: [$ID_{vi}$, $EncId_{vi}$, Template, and $EncKey_{vi}$]

5.3. Phase 2: V2I Pre-Authentication. This phase checks the legitimacy of each registered vehicle before one takes part in V2V communications. TA performs the process of verifying
whether any vehicle is legitimate through RSU. The detailed steps of the process which TA performs are as follows:

Whenever vehicle $V_i$ moves in an area administered by RSU$^i_k$, OBU of $V_i$ sends request BS$^i_v$ where $BS^i = HMAC(\text{template}, (\text{EncId}_v || TS) || \text{EncId}_v || \text{TS}$ to RSU$^i_k$ in order to verify its identity. The verification steps are as follows:

(i) First, TA checks the legitimacy of RSU$^i_k$ as follows:

(ii) TA sends decision sequence DS$^i_v$ and interconversion rule IR$^i_v$ to RSU$^i_k$. Thereafter, RSU$^i_k$ translates binary string ID$^v$ into quantum strings using the interconversion rule IR$^v$.

(iii) Meanwhile, RSU$^i_k$ generates a set of EPR entangled pairs $|q_{kt}>, |q_{kt}>$ with the length equaling that of quantum bit strings obtained from ID$^v$. RSU$^i_k$ separates a set of EPR entangled pair $|q_{kt}>, |q_{kt}>$ into a set of EPR entangled pair $|q_{kt}>, |q_{kt}>$. Finally, RSU$^i_k$ stores $|q_{kt}>$ to itself and sends $|q_{kt}>$ to TA.

(iv) Now, TA searches for measurement sequence MS$^i_v$ in its database corresponding to the received ID$^v$. After that, TA measures $|q_{kt}>$ quantum bit string, which were received from RSU$^i_k$ in the previous step using the measurement sequence MS$^i_v$. As soon as $|q_{kt}>$ quantum bit string gets measured, the EPR quantum bit string $|q_{kt}>$ gets collapsed into the same eigen state as eigen state of $|q_{kt}>$. TA also generates a query encrypted key QEncKey$^i_v$, using the template and pre-master secret.

(v) Next, RSU$^i_k$ converts back quantum string $|q_{kt}>$ into the binary string using already shared interconversion rule IR$^i_v$, available with it, thus producing a pre-master secret. Furthermore, TA generates the template by comparing the decision sequence DS$^i_v$, and the measurement sequence MS$^i_v$. In addition, TA also generates a query encrypted key QEncKey$^i_v$, using the template and pre-master secret.

(vi) Finally, TA searches the query encrypted key QEncKey$^i_v$ in its own database. If found, RSU$^i_k$ is considered legitimate otherwise, illegitimate, and TA discards the request.

(vii) Now, TA checks vehicle $V_i$ legitimacy through RSU$^i_k$. As soon as RSU$^i_k$ completes its verification stage, it transmits the request BS$^i_v$ to TA.

(viii) TA sends decision sequence DS$^i_v$ and interconversion rule IR$^i_v$ to vehicle $V_i$ through RSU$^i_k$. With the help of the interconversion rule IR$^i_v$, vehicle $V_i$ translates a binary string of EncId$^i_v$ into quantum strings.

(ix) Meanwhile, vehicle $V_i$ generates a set of EPR entangled pairs $|q_{kt}>, |q_{kt}>$ with the length equaling each quantum bit string obtained from EncId$^i_v$. After that, vehicle $V_i$ separates set of EPR entangled pair $|q_{kt}>, |q_{kt}>$ into a set of EPR entangled pair $|q_{kt}>, |q_{kt}>$. Finally, vehicle $V_i$ stores $|q_{kt}>$, to itself and sends $|q_{kt}>$ to TA.

(x) Now, with the received EncId$^i_v$, TA searches for the corresponding measurement sequence MS$^i_v$ in its database. Then, TA measures $|q_{kt}>$ quantum bit string, which the vehicle $V_i$ had transmitted to TA in the previous step. As soon as the $|q_{kt}>$ quantum bit string gets measured, the EPR quantum bit string $|q_{kt}>$ gets collapsed into the same eigen state as eigen state of $|q_{kt}>$. TA in the previous step. As soon as the $|q_{kt}>$ quantum bit string gets measured, the EPR quantum bit string $|q_{kt}>$ gets collapsed into the same eigen state as eigen state of $|q_{kt}>$. TA thereon, the quantum bit, which corresponds to $|q_{kt}>$, i.e., $|q_{kt}>$, is measured with the same MS$^i_v$ by vehicle $V_i$, thereby, the same eigen state of $|q_{kt}>$ is collected because of the entanglement property.

(xi) Next, vehicle $V_i$ converts back quantum string $|q_{kt}>$, to a binary string using an already shared interconversion rule IR$^i_v$, thus producing a pre-master secret. Furthermore, TA generates the template by comparing the decision sequence DS$^i_v$, and the measurement sequence MS$^i_v$. In addition, TA also generates a query encrypted key QEncKey$^i_v$, using the template and pre-master secret.

(xii) Finally, TA matches the query encrypted key QEncKey$^i_v$ in the database. If it matches with any previously stored EncKey$^i_v$, the vehicle is considered legitimate, otherwise illegitimate.

5.4. Phase 3: Pseudo Identity and Session Key Generation.
If the vehicle is legitimate, then TA generates a random number Psid1 and transfers the ACKBS$^i_v = E_{\text{template}}[\text{Psid}1]$ to RSU$^i_k$. After that, RSU$^i_k$ generates and stores a set of session keys SKEY$^i_v$, SKEY$^i_v$, ... SKEY$^i_v$, corresponding to received ACKBS$^i_v$, and sends back ACKBSR$^i_v$ to the vehicle. Figure 2 clearly illustrates the V2I pre-authentication and pseudo identity and session key generation phase through the flowchart. A randomly chosen key from the set of session keys SKEY$^i_v$, SKEY$^i_v$, ... SKEY$^i_v$ is used later as a session key between RSU$^i_k$ and vehicle $V_i$ for further communication, where

\[
\text{ACKBSR}^i_v = \text{ACKBS}^i_v \| \text{SKEY}^i_v, \ldots, \text{SKEY}^i_v \| \text{TS}.
\]

At the end of this phase, the vehicle is pre-authenticated in VANETs and has established a set of session keys SKEY$^i_v$, ... SKEY$^i_v$ with RSU$^i_k$ for further communication.

5.5. Phase 4: Message Authentication and Verification.
Vehicle $V_i$ sends a tuple $T = (\text{MSG} 2, \text{MSG}, \text{TS})$ to RSU$^i_k$ to report MSG containing the information related to its status such as speed, position, traffic congestion, etc. The MSG is embedded in MSG1 after proper time stamping (TS). After receiving the tuple $T$, RSU$^i_k$ authenticates the MSG2 by
looking at each session key in a set of session keys SKEY, ..., SKEY corresponding to sender vehicle, in its database. Finally, to verify the MSG 2, the RSU_k computes the HMAC digest MSG 2 using each session key stored in its database corresponding to vehicle V_j and then compares the received HMAC digest MSG 2 with its computed one MSG 2'. If the results match, then MSG 2 is accepted as legal; otherwise, the message is illegal, and RSU_k discards the message.

\[
\text{MSG 2} = \text{HMAC} (\text{SKEY}, \text{MSG 1}) \\
\text{MSG 1} = \text{MSG}||\text{TS}. 
\]

5.6. V2V Communication. If vehicle V_j wants to communicate message M with vehicle V_i then vehicle V_i executes two phases, namely, V2V common key establishment phase and V2V message authentication and verification phase.

5.6.1. V2V Common Key Establishment Phase. In this phase, vehicle V_i sends the tuple S = (R_{V_i}, ACKBS_{V_i}, TS) to RSU_k to establish a common secret key shared only between vehicle V_i and vehicle V_j. After receiving the tuple S from vehicle V_i, RSU_k authenticates the R_{V_i} by looking at each session key in a set of session keys SKEY, ..., SKEY corresponding to the sender vehicle V_j, in its database. Finally, to verify the R_{V_i}, the RSU_k computes the HMAC digest R_{V_i} using each session key stored in its database corresponding to vehicle V_j and then compares the received HMAC digest R_{V_i} with its computed one R'_{V_i}. If the results match, then R_{V_i} is accepted as legal. In case of a legal vehicle V_j, RSU_k generates a common secret key Key_{V_j} and sends back tuple ACKS_{V} = (Reply_{R_{V_i}}, Key_{V_j}, TS) to vehicle V_i, and also sends tuple ACKS_{j} = (Reply_{R_{V_j}}, Key_{V_j}, TS) to ACKBS_{V_j} which corresponds to vehicle V_j. As soon as vehicle V_j and vehicle V_j receive ACKS_{i} and ACKS_{j}, respectively, they authenticate Reply_{R_{V_i}} and Reply_{R_{V_j}} by looking at each session key received from RSU_k, respectively, during phase 3 of the proposed protocol. Since, Reply_{R_{V_i}} and Reply_{R_{V_j}} are HMAC authenticated with corresponding session key shared between RSU_k and corresponding vehicle during phase 3, namely, pseudo-identity and session key generation of the proposed protocol, both vehicle V_i and V_j can easily extract the common key Key_{V_i}. Here, the session key SKEY and SKEY represents one out of any
session key shared between vehicle \( V_i \) and \( V_j \) respectively during phase 3 of the proposed protocol. At the end of this phase, a common key \( Key_{V_{ij}} \) is established between vehicle \( V_i \) and \( V_j \), which can later be used by vehicle \( V_i \) and \( V_j \) for secure V2V communication with each other.

\[
R_{V_i} = \text{HMAC}(\text{SKEY}_{V_{ij}}, \text{ACKBS}_{V_j})
\]

\[
\text{Reply}_{R_{V_i}} = \text{HMAC}(\text{SKEY}_{V_{ij}}, \text{Key}_{V_{ij}})
\]

\[
\text{Reply}_{R_{V_j}} = \text{HMAC}(\text{SKEY}_{V_{ij}}, \text{Key}_{V_{ij}})
\]

5.6.2. V2V Message Authentication and Verification Phase. In this phase, vehicle \( V_i \) sends tuple \( B = (\text{Msg}_{V_{ij}}, M, \text{TS}) \) to transfer message \( M \) to vehicle \( V_j \). As soon as vehicle \( V_j \) receives tuple \( B \), it authenticates the \( \text{Msg}_{V_{ij}} \) using the shared common key \( Key_{V_{ij}} \) a established during V2V common key establishment phase. Finally, to verify the \( \text{Msg}_{V_{ij}} \), vehicle \( V_j \) computes HMAC digest \( \text{Msg}_{V_{ij}}' \) using \( Key_{V_{ij}} \) and then compares the received HMAC digest \( \text{Msg}_{V_{ij}} \) with its computed one \( \text{Msg}_{V_{ij}}' \). If the result matches, then \( \text{Msg}_{V_{ij}} \) is accepted as legal otherwise vehicle \( V_j \) discards the message.

\[
\text{Msg}_{V_{ij}} = \text{HMAC}(\text{Key}_{V_{ij}}, M).
\]

6. Evaluation

This section discusses the assessment of the proposed privacy-preserving authentication protocol, which includes privacy and security analysis and measurement of performance parameters subsequently.

6.1. Privacy and Security Analysis. We analyze the security and privacy of the proposed authentication protocol in two criteria. First, we discuss the security analysis of quantum communication, which provides unconditional security. Second, we investigate the security and privacy analysis of our protocol in a particular context.

Our protocol uses BB84 quantum key distribution algorithm, whose security and privacy are demonstrated in Ref. [61]. Also, our protocol does not depend on any hard problem, rather uses the inherent properties of quantum physics. Therefore, the proposed protocol obtains the same theoretically unconditional security as described in detail in Ref. [62]. The security in VANETs from various attacks, as mentioned in the designed goal of the proposed protocol, gets also ensured by the proposed protocol as follows:

6.1.1. Authentication. During the V2I pre-authentication phase in our proposed protocol, the authentication gets enabled by checking the legitimacy of roadside units (RSUs) and vehicles. In addition, the assurance that TA can successfully discard the illegitimate vehicle’s request gets performed by TA upon looking in its database. TA stores \( \text{EncKey}_{V_i} \) and \( \text{EncKey}_{V_j} \) corresponding to one’s real identities \( \text{EncId}_{V_i} \) and \( \text{Id}_{V_j} \). For instance, TA produces an encrypted key from real identities (binary bit) after applying a decision sequence (randomly chosen by TA), resulting in a quantum bit containing imprecise quantum states. These quantum bits are now converted back to a binary bit using the interconversion rule. We note that the converted binary bit is not the same as that of the original binary bit. The TA stores the encrypted key in its database after applying the corresponding template. Although, encrypted keys and real identities are different, they hold corresponding relationships, enabling TA to discard illegitimate vehicles by looking up its database. Also, during the system initialization of the proposed protocol, RSU and vehicle register themselves with TA and get corresponding \( \text{EncKey}_{V_i} \) and \( \text{EncKey}_{V_j} \). During V2I pre-authentication phase, TA uses the same encrypted key of the corresponding vehicle and RSU to investigate the legitimacy of the vehicle and RSU.

6.1.2. Identity Revocation. The secret keys are stored in the OBU of the vehicle and RSU. If an attacker can access these keys, i.e., \( \text{EncKey}_{V_i} \), then the attacker becomes capable of communicating with TA easily. However, the assumption of tamper-proof OBU prevents this scenario. Even if an attacker gains access to \( \text{EncKey}_{V_i} \), he or she cannot get any information about the user, as \( \text{EncKey}_{V_i} \), does not reveal the real identity of the user. We recommend that whenever the system gets compromised, generation of a new decision sequence, interconversion rule, template, and \( \text{EncKey}_{V_i} \) can be performed, and old credentials can be deleted immediately. The vehicle can update one’s \( \text{EncKey}_{V_i} \) and template after a specific interval of time by executing updating secret key phase. Although, the newly generated template key, \( \text{EncKey}_{V_i} \), is from the same real id of the vehicle, they are different because TA and vehicle choose a decision sequence and measurement sequence randomly forbidding attacker from using previously compromised keys.

6.1.3. Irreversibility. Till now, we described whether the attacker can get access to TA, if the attacker can get \( \text{EncKey}_{V_i} \). Now we discuss, in the same situation, the difficulty of recovering original \( \text{Id}_{V_i} \). In our proposed protocol, \( \text{EncKey}_{V_i} \) is generated because of the template and pre-master secret, where the template is obtained as the difference of the measurement sequence and decision sequence. However, measurement sequence and decision sequences are chosen randomly. Therefore, an attacker never generates the exact template as done by \( V_i \) at the time of registration. In the scenario when the attacker somehow gets the exact template and \( \text{EncKey}_{V_i} \), the attacker does not become capable of retrieving real identity \( \text{Id}_{V_i} \), because there exists nonorthogonality relationship between the circularly polarized photon and the linear polarized photon, thus making them indistinguishable. In addition, a measurement sequence is needed to measure quantum bits, which are
randomly selected by TA successfully. If the attacker tries to choose the measurement sequence randomly, he or she obtains uncertain and fragmented results.

6.1.4. Defense against Quantum Attacks. The special type of attacks such as entanglement, missing decision sequence, missing measurement sequence, missing quantum bit string, etc., can also be encountered in the proposed protocol. Losing the decision sequence, measurement sequence, and interconversion rule does not reveal any information about the vehicle user because these are chosen randomly and contain no information about the user. These are used to generate an EPR quantum bit for the legitimate vehicle. Also, losing a template used to generate encrypted keys reveals to the attacker the bits which are correct, but the inability to know exact information of that bit persists. However, if an attacker somehow knows the template, he or she will still require a pre-master secret to generate the encrypted key.

6.1.5. Anonymity. Given a message \( M_i \), the inability of the adversary to retrieve any identification information of the sender vehicle results in anonymity. Anonymity is further classified as void anonymity, apparent anonymity, revocable anonymity, and forfeitable anonymity based on recognizability (identifiability or traceability) of the vehicle. The void and apparent anonymity are unconditional types of anonymity, whereas revocable and forfeitable anonymity are conditional types of anonymity. In VANETs, anonymity is not unconditional in nature, i.e., in case transmission of fake messages by the vehicle occurs, TA should be able to trace the real identities of vehicle. In phase 4 of the proposed protocol, tuple \( T \) is sent to RSU by vehicle for authentication and verification. However, tuple \( T = (\text{MSG}2, \text{MSG}, \text{TS}) \) does not contain any identification information related to the vehicle, thus ensuring anonymity. In addition, in phase 3 of the proposed protocol, RSU stores and generates session keys corresponding to the received encrypted pseudo identities for a particular vehicle. Whenever any vehicle transmits fake messages to RSU, encrypted pseudo identities are used by RSU to report to TA. Later, TA can trace and penalize the vehicle as per policy. Thus, the proposed protocol ensures conditional anonymity, in particular, revocable anonymity.

6.1.6. Protection against Replay Attack. In the proposed scheme, protection against replay attack by RSU\(_i\) is ensured as BS\(_i\), which comprises EncId\(_i\) is properly timestamped and authenticated using HMAC. Also, MSG 2 is properly timestamped and authenticated using HMAC in phase 4 of the proposed protocol.

6.1.7. Information Integrity. Information integrity is one of the key features for secure communication in VANETs. In VANETs, information integrity is basically the guarantee of accuracy and consistency of message exchanged between entities of VANET like vehicles, RSU, and TA. It ensures that the exchanged message has not been changed in transit. Generally, cryptographic techniques such as message integrity code (MIC) also known as message authentication code (MAC) are used to protect information integrity. During the V2I pre-authentication phase of the proposed protocol, TA receives request BS\(_i\) containing HMAC from OBU of vehicle \( V_i \) through RSU\(_i\) for the purpose of verification of vehicle \( V_i \) identity. Also, during message authentication and verification phase of the proposed protocol, tuple \( T \) is sent by vehicle \( V_i \) to RSU\(_i\) for message authentication and verification. The tuple \( T \) consists of MSG 2 which contains HMAC, an extension of MAC, which not only enables authentication of source of messages but also information integrity.

6.1.8. Unlinkability. Given two messages \( M_1 \) and \( M'_1 \), an adversary cannot determine whether the messages get generated from a single vehicle or two different vehicles, resulting in unlinkability. Note that, \( M_1 = (\text{MSG}2, \text{MSG}1) \) = (HMAC(SKEY\(_{v1}'\), MSG 1), MSG1|TS) and \( M'_1 = (\text{MSG}2', \text{MSG}1') \) = (HMAC(SKEY\(_{v2}'\), MSG 1'), MSG1'). In other words, \( M_1 \) is indistinguishable to \( M'_1 \) even if \( M_1 \) and \( M'_1 \) are generated from the same vehicle. Also, \( M_1 \) and \( M'_1 \) are completely random and are not predictable. Since HMAC is a hash function which satisfies random oracle, even a single bit change in its input leads to uniform random output. In the proposed protocol, MSG 1 and SKEY\(_{v1}'\), SKEY\(_{v2}'\), ..., SKEY\(_{vk}'\) are drastically changing from one message to another. Also, (MSG 1|TS) and MSG1' are unrelated because of the difference in timestamp (TS). Similarly, MSG 2 = HMAC(SKEY\(_{v1}'\), MSG 1) = HMAC(SKEY\(_{v2}'\), MSG1|TS) and MSG 2' = HMAC(SKEY\(_{v3}'\), MSG 1') = HMAC(SKEY\(_{v4}'\), MSG1') remain unrelated due to the use of different session keys and timestamps. Therefore, the adversary cannot link MSG 2 and MSG 2' to a particular vehicle, ensuring unlinkability between two messages. Hence, privacy preservation is achieved.

6.1.9. Traceability. TA can trace whenever RSU\(_k\) reports a fake yet authentic message to TA by sending ACKBS\(_i\). TA extracts Psid 1 from ACKBS\(_i\) and generates H(Psid 1) to check whether it matches an entry in its database. If so, TA initiates action on the vehicle according to the policy.

6.1.10. Collusive Attack from Vehicles. Resistance against collusive attack guarantee prohibition of the leakage of secret keys i.e., if two vehicles collude, they should not be able to obtain session keys of the proposed protocol in order to avoid any attacks afterward. In phase 4 of the proposed protocol i.e., in the message authentication and verification phase, each vehicle anonymously authenticates its message by sending request tuple \( T = (\text{MSG}2, \text{MSG}, \text{TS}) \) to RSU without revealing its real identity. Also, RSU verifies the message authenticity by investigating tuple \( T \). If two vehicles collude, they cannot infer the session keys because tuple \( T \) is
not linkable. Moreover, any random session key that does not correspond to any vehicle within database of RSU gets discarded immediately by RSU.

6.1.11. Design Challenges. The traditional authentication protocol deals with classical bits, whereas the proposed privacy-preserving authentication protocol makes use of qubits, thus the quality of qubits, error correction, and qubit control are the significant challenges for large-scale practical implementation. The requirement of high-quality qubits for the generation of gate operations and complex instructions cannot be overlooked while designing any quantum computing–based authentication protocol. Although few qubit quantum computers are accessible through cloud, their efficiency is of high concern. Frequently, they produce incorrect results while performing any calculation using qubits and thus efficient error correction algorithms are indeed the need of the hour. In addition, implementation of error control algorithms require control over multiple qubits with low latency, preferably in nanoseconds. Therefore, multiple qubits control is also one of the significant design challenges for the practical implementation of quantum computing–based authentication protocol.

6.2. Performance Evaluation and Comparison. The demonstration and comparison of the computational and communication cost of the proposed protocol with Refs. [44, 45, 58] is discussed. The comparison standard includes the vehicle joining and vehicle leaving phase; thus, a scenario where some vehicles enter within the range of \( K^{th} \) RSU and other vehicle leaves that range simultaneously is not overlooked. The detection distance \( d_{dr} \), which equals 300 m using DSRC, is the coverage distance for any RSU on each side concerning its installation [70]; thus, a total distance of 600 m gets covered by any RSU. The safe distance \( d_s \) is the distance between two vehicles that need to be maintained to avoid accidents and is calculated based on the speed of vehicles [71]. For example, \( d_s \) should be 70 m between two vehicles, moving at a speed of 70 km/h. Therefore, considering fixed \( d_s \) corresponding to the moving vehicle speed, our performance simulation uses a fixed number of vehicles within any RSU range, i.e., considering vehicle length to be 5 m [72], vehicle speed to be 55 km/h, \( d_s \) to be 55 m, a maximum of 9 vehicles can commute the journey including the entering vehicle within any RSU range. Similarly, a maximum of ten vehicles can commute in another lane, which leads to a maximum of 19 vehicles where \( n_j \) denotes the number of joining vehicles and \( n_l \) denotes the number the leaving vehicles. The calculation and comparison of communication and computation cost are performed considering \( n_j \) and \( n_l \) whenever any vehicle commutes through the \( K^{th} \) RSU detection scope. For the calculation of computation cost, the parameters such as time cost for the multiplicative group, time cost for a hash function, time cost for inversion in the group, time cost for the calculation of Chinese remainder theorem are denoted by \( t_m \), \( t_H \), \( t_S \), \( t_{CRT} \), and has values 1.80, 3.20, 25.58, and 150.589, respectively. In addition, \( t_S \) and \( t_E \) denote searching time and encryption time. For the calculation of the communication cost, the bit length of timestamp, random number, identity, and pseudo-identity are assumed as 64b, 160b, 160b, and 160b, respectively. We obtain the time parameter for computation cost using Miracle library [73] on ubuntu 18.04, and we use SHA-256 for performing a comparison with Refs. [44, 45, 58]. Also, a qualitative comparison of security features with some existing authentication protocols has been shown in Table 5, whereas the individual computation cost of TA, RSU, and vehicle, along with the total communication cost, is reported in Table 6. The computation cost of our protocol at vehicle, RSU, and TA are \( t_{H}, f \star t \ast (1 + n_j)t_{H}, \) and \((1 + n_j)(t_S \ast t_E)\), respectively, which is a significant reduction of the computation overhead when compared to Refs. [44, 45, 58]. Also, the communication overhead of our protocol is \( 2864 \ast (1 + n_j) \), which is again a significant reduction in communication overhead when compared to Refs. [44, 45, 58]. However, the obtained communication cost of the proposed protocol is higher when compared to Ref. [45], but the proposed work provides unconditional security, which is not guaranteed by any of the other works. In addition, as the proposed protocol utilizes one of the quantum key distribution protocols, namely, BB84 protocol, we have also evaluated the parameter values of BB84 protocol by performing simulation in QKD simulator [35]. QKD simulator, which is purely written in Python and applies standard libraries such as Scipy, Numpy, Pycrypto, etc., is well-known for returning simulation results by utilizing QKD stack, which includes a quantum channel, shifting, authentication using hashing, error estimation, error correction, and privacy amplification. Figure depicts the variation when several initial qubits, which equals 600, are constant, and the eavesdropping rate varies from 0.1 to 0.6 one after another, i.e., Figure 3 shows the variation of performance parameters with the constant number of initial qubits. In contrast, Figure 4 shows how performance parameters vary when the eavesdropping rate, which equals 0.1, is taken to be constant. It is clear from the figures that the final key length and key length before privacy amplification increase linearly as the initial number of qubits get increased. In contrast, there is a linear decrement in key size and linear growth in information leakage regarding increasing eavesdropping rate.

6.3. Storage Overhead. In the proposed protocol, TA generates and stores a pseudo-identity for vehicle \( V_j \) after successfully pre-authenticating vehicle \( V_j \) using the BB84 protocol featuring unconditional security. Assuming all vehicles can pass through a particular RSU in 10 min, \( f \)
denotes the number of messages sent by the vehicle per second, and \( t \) shows time (in seconds). The number of session keys \( N = f \times 10 \times 60 \) gets generated. Besides, in the proposed protocol, RSU generates and stores \( N \) number of session keys corresponding to the encrypted pseudo-identity of the vehicle as soon as RSU receives them from TA. Therefore, the vehicle gets one pseudo-identity and two quantum secrets, namely, template and \( Q \) EncKey, from TA along with \( N \) number of session keys from RSU. Therefore, based on the already defined bit length of keys and identities, the storage overhead of the vehicle is \( (N + 2) \times t_m \) times the size of the secret key. The storage overhead of TA for a particular vehicle \( V_i \), assuming a vehicle updates its pseudo-identity \( n \) times, equals the size of \( (N + 1) \) pseudo identities + 2 \times size of quantum secret + size of the real identity of the vehicle. The storage overhead for RSU for a particular vehicle \( V_i \) equals \( N \times \) the size of session keys + length of the encrypted pseudo-identity.

7. Conclusion

The efficient use of quantum computing techniques can enhance the privacy and security of VANETs. This article proposes a novel V2I privacy-preserving authentication protocol by combining quantum communication protocol and CID-based authentication. In addition, the proposed protocol exploits the inherent properties of quantum mechanics, such as no-cloning theorem and entanglement, thus providing unconditional security to vehicles and RSUs. The proposed mechanism authenticates the vehicle with infrastructure and provides a mechanism for the vehicle to communicate with RSU and TA. The privacy and security analysis section reveals that our protocol, utilizing the inherent properties of quantum mechanics, provides unconditional security, is scalable, and possesses a privacy-preserving nature.

The proposed work assumes the TA to be completely trusted; therefore, modification of the current protocol under the assumption of malicious TA could be included in future work. Also, future work may incorporate decentralization by adopting blockchain technology, i.e., to propose an extended version of our protocol in the blockchain environment.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Ministry of Education, GoI.

References

[1] R. Hussain, J. Lee, and S. Zeadally, “Trust in VANET: a survey of current solutions and future research opportunities,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 5, pp. 2553–2571, May 2021.
[2] A. Ullah, X. Yao, S. Shaheen, and H. Ning, “Advances in position based routing towards ITS enabled FoG-oriented VANET-A survey,” IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 2, pp. 828–840, 2020.
[3] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, “Vehicular ad-hoc network (VANET): Review,” in Proceedings of the 2018 IEEE International Conference on
[14] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, “Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs,” *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, Dec. 2020.

[15] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, “Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1681–1695, 2021.

[16] D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, “Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1124–1132, 2020.

[17] S. Adi, “A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem,” in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science* (sfcs 1982), pp. 145–152, IEEE, Chicago, IL, USA, 3 November 1982.

[18] L. Dennis and P. Gordon, “Cryptography: from caesar ciphers to public-key cryptosystems,” *The College Mathematics Journal*, vol. 18, no. 1, pp. 2–17, Jan. 1987.

[19] C. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, pp. 656–715, Apr. 1949.

[20] O. Galindo, V. Krennovich, and O. Kosheleva, “Current quantum cryptography algorithm is optimal: a proof,” in *Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 295–300, IEEE, Bangalore, India, 18 November 2018.
[69] M. Mehic, O. Maurhart, and S. Rass, "Implementation of quantum key distribution network simulation module in the network simulator NS-3," *Quantum Information Processing*, vol. 16, p. 253, 2017.

[70] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "Dsrsr versus 4g lte for connected vehicle applications: a study on field experiments of vehicular communication performance," *Journal of Advanced Transportation*, vol. 2017, Article ID 2750452, 2017.

[71] "Advice for driving on expressways," 2021, https://en.driveplaza.com/rules/rules.html.

[72] "Vehicle size class," 2021, https://en.wikipedia.org/wiki/Vehicle_size_class.

[73] 2021 https://github.com/miracl/MIRACL.