

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository: <https://orca.cardiff.ac.uk/id/eprint/171295/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Prateek, Kumar, Maity, Soumyadev and Saxena, Neetesh 2024. QSKA: A quantum secured privacy-preserving mutual authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Transactions on Network and Service Management* 10.1109/TNSM.2024.3445972

Publishers page: <https://doi.org/10.1109/TNSM.2024.3445972>




Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



QSKA: A Quantum Secured Privacy-Preserving Mutual Authentication Scheme for Energy Internet-Based Vehicle-to-Grid Communication

Kumar Prateek , *Student Member, IEEE*, Soumyadev Maity , *Member, IEEE*, and Neetesh Saxena , *Senior Member, IEEE*

Abstract—Energy Internet is well-known nowadays for enabling bidirectional V2G communication; however, with communication and computation abilities, V2G systems become vulnerable to cyber-attacks and unauthorised access. An authentication protocol verifies the identity of an entity, establishes trust, and allows access to authorized resources while preventing unauthorized access. Research challenges for vehicle-to-grid authentication protocols include quantum security, privacy, resilience to attacks, and interoperability. The majority of authentication protocols in V2G systems are based on public-key cryptography and depend on some hard problems like integer factorization and discrete logs to guarantee security, which can be easily broken by a quantum adversary. Besides, ensuring both information security and entity privacy is equally crucial in V2G scenarios. Consequently, this work proposes a quantum-secured privacy-preserving key authentication and communication (QSKA) protocol using superdense coding and a hash function for unconditionally secure V2G communication and privacy. QSKA uses a password-based authentication mechanism, enabling V2G entities to securely transfer passwords using superdense coding. The QSKA security verification is performed in proof-assistant Coq. The security analysis and performance evaluation of the QSKA show its resiliency against well-known security attacks and reveal its enhanced reliability and efficiency with respect to state-of-the-art protocols in terms of computation, communication, and energy overhead.

Index Terms—Privacy-Preserving Authentication, Security Threats, Vehicle-to-Grid.

I. INTRODUCTION

The development of electric vehicles (EVs) can significantly improve fuel economy by lowering fuel costs, and greenhouse gas emissions consequently play an essential role in handling the climate crisis [1]. The goal of sustainable development can only be met if fossil fuel-based energy generation is eliminated and renewable energy sources are integrated into power generation and distribution. To meet the goal of sustainable development, the concept of energy internet (EI) comes into play, which integrates ICT, CPS, and power system technologies to develop sustainable smart grids [2]. With the ever-increasing use of electrical power in numerous devices involved in day-to-day activities, it is predicted that the demand for electrical power will increase

to 82% by 2030 [3]. In view of that, smart grids use demand response techniques to reduce power consumption, increase energy efficiency, and eliminate the need to install additional generators as required in conventional power grids. Despite the fact that the demand response technique brings forth many benefits, it poses crucial security and privacy issues due to the involvement of network communication and the exchange of information. The vehicle-to-grid (V2G) network serves as an indispensable component in efficient and smart transmission systems employing demand response techniques. It also enables energy transfer to and from smart grids. The efficient generation, distribution, and transmission of energy and the frequent interaction with SGs for demand response management make the V2G network open to cyberattacks. The entity of the V2G network, namely EVs, uses the battery to store electrical energy, which can be transferred to the smart grid and other energy deficit EVs whenever required. Also, to avoid wastage of energy, the stored energy of an EV battery can be transferred to the smart grid during high load on-grid and vice versa. However, to disrupt the V2G network, an adversary can perform many cyberattacks. Therefore, not only the protection of the exchanged messages between entities of the V2G network from an adversary is required, but also the identity privacy of entities, along with many other security measures, need to be deployed to either prevent or handle many cyber attacks, unfair energy transfers, criminal activities, and targeted advertising.

The EI-based V2G makes it possible for EVs to use energy from renewable sources, like solar and wind power, and reduces the load on the conventional power grid. It promotes the wider adoption of renewable energy as it allows individual households and EVs to trade energy without having their own transmission and distribution networks. The number of EVs is constantly increasing, making the V2G systems scalable. Besides, V2G systems handle the storage and management of energy that can be used to balance the grid and smooth out demand, making V2G systems flexible. V2G allows EVs to provide power to the grid, enabling them to be used as distributed energy resources featuring decentralization. Due to the scalability, mobility, flexibility, and decentralized characteristics of V2G systems, they offer increased grid stability, reduced peak demand, and the potential for lower electricity costs. The V2G system requires secure V2G entity authenti-

Kumar Prateek and Soumyadev Maity is with the Department of Information Technology, Indian Institute of Information Technology Allahabad, City Prayagraj, UP, 211015, India. E-mail: (PcI2017003@iiita.ac.in and soumyadev@iiita.ac.in)

Neetesh Saxena is with the School of Computer Science and Informatics, Cardiff University, Cardiff CF10 3AT, U.K. E-mail: nsaxena@ieee.org

TABLE I
COMPARATIVE ANALYSIS OF RELATED SCHEME

Scheme	Primitive Used	SP1	SP2	SP3	SP4	Strengths/Weakness/Potential Improvements
[4]	ECC	No	No	No	No	lightweight in nature but not secured against a quantum adversary
[5]	ECC	No	No	No	No	not secured against the quantum adversary; depends on computationally hard problems
[6]	Bilinear Pairing	No	No	No	No	high computation cost; depends on computationally hard problems
[7]	AES-CBC, Hash Function	No	Yes	No	No	threatened by Grover's search quantum algorithm
[8]	Bilinear Pairing, Hash Function	No	No	No	No	depends on computationally hard problems; conditionally secure
[9]	Bilinear Pairing, Hash Function	No	No	No	No	low communication cost; conditionally secure
[10]	Public Key, Sign-encryption	No	No	No	No	depends on computationally hard problems; limited applicability
IEC15118	ECDSA	No	No	No	No	ensures non-repudiation; quantum attacks possible
OCPP	ECDSA	No	No	No	No	depends on computationally hard problems; resistance to chosen message attacks.
[11]	Hash Function	Yes	Yes	No	No	threatened by the quantum adversary; vulnerable to length extension attacks
[12]	Hash Function	Yes	No	Yes	No	threatened by the quantum adversary and Grover search algorithm
[13]	PUF, MAC	Yes	No	Yes	No	threatened by the quantum adversary; keyed authentication; efficient
[14]	Hash Function	Yes	No	No	No	threatened by the quantum adversary; efficient
[15]	Lattice-based Cryptography	No	Yes	Yes	Yes	depends on the quantum hard problem; not future-safe
[16]	QKD (BB84), Hash Function	No	Yes	Yes	Yes	use of laws of quantum mechanics; future-safe
[17]	Lattice-based Cryptography	No	Yes	No	No	depends on the quantum hard problem; not future-safe
[18]	Lattice-based Signature	No	Yes	Yes	Yes	ensures non-repudiation; depends on the quantum hard problem; not future-safe
[19]	Lattice-based PKE	-	Yes	-	-	depends on the quantum hard problem; not future-safe
[20]	Lattice-based Signature	No	Yes	Yes	Yes	ensures non-repudiation; depends on the quantum hard problem; not future-safe
[21]	Lattice-based Signature	No	Yes	Yes	Yes	guarantees non-repudiation; depends on the quantum hard problem; not future-safe
[22]	QKD (BB84)	No	Yes	No	No	depends on the laws of quantum mechanics; future-safe
[23]	Lattices, Group Signature	No	Yes	No	Yes	anonymity; depends on the quantum hard problem; not future-safe
[24]	Lattices, Batch Verification	Yes	Yes	Yes	Yes	depends on the quantum hard problem; efficient in nature; not future-safe
QSKA	Quantum Communication, Hash Function	Yes	Yes	Yes	Yes	depends on the laws of quantum mechanics; future-safe
SP1: Location Privacy Support		SP2: Quantum Resistance		SP3: EV Identity Privacy Support		SP4: EV Traceability Support

cation to prevent unauthorised access since, with unauthorized access, an adversary could manipulate the flow of electricity, leading to power outages and demands. Also, V2G systems are vulnerable to cyberattacks like impersonation attacks, man-in-the-middle attacks, and many more that can compromise the grid's stability and reliability. Nevertheless, as an important entity in V2G systems, EVs face several attacks targeting their privacy and daily operations. Not only that, but V2G transactions involve the exchange of personal information about EVs, such as charging requests, the identity of each EV, and its location. This makes privacy attacks a risk for V2G transactions. For example, a privacy breach in an EV could include revealing the real name of the driver, the location of the EV, or the route it took. In short, the V2G system has security problems like weak and insecure authentication, vulnerability to cyberattacks, and privacy issues like the leakage of EV identity and location information, which puts sensitive personal information at risk. Many protocols have been designed following the standards defined by ISO/IEC/IEEE 18880 [25] to enable information exchange in EI-based systems. Specifically, ISO/IEC/IEEE 18880 specifies the communication architecture and protocols for EI, detailing data exchange protocols and network architecture for integrating many components, entities, data storage, and application services within the smart grid. Although ISO/IEC/IEEE 18880 utilizes a wide area network using TCP/IP protocols, it allows connections for non-TCP/IP protocols through the multi-protocol gateway. Despite several benefits associated with ISO/IEC/IEEE 18880 standards, security and network management issues were a big concern, which were eradicated later by the development of ISO/IEC/IEEE 18881 and ISO/IEC/IEEE 18883 standards [26]. Initially, the protocol, namely IEC 15118 [27], and OCPP [28] was widely used for establishing communication between EVs, charging stations (CSs), and management systems in EI-based V2G communication. Furthermore, several V2G authentication protocols are described in [4]–[10].

Despite the existence of various authentication and key establishment/exchange protocols [4]–[10], several research gaps persist, including susceptibility to cyber attacks, inadequate secure authentication mechanisms, and insufficient privacy protection measures. The majority of existing authentication and key establishment or key exchange protocols for V2G communication available in the literature utilize public-key cryptographic (PKC) techniques that use the notion of computationally hard problems to safeguard communication between entities of the V2G network and maintain the privacy of individual EVs. Specifically, the PKC-based protocols used in V2G systems harness the inability to compute the private key of EVs from the corresponding public key to ensure security. It assumes that there does not exist any probabilistic polynomial-time algorithm that can compute the private key of EVs from the corresponding public keys. However, the development of massive computation capabilities (quantum computers) enables the adversary to easily calculate the private key of EVs from the corresponding public key. Subsequently, most of the existing authentication and key establishment protocols [4]–[10] used in the V2G environment are jeopardized because of their dependency on the hardness of the computational capabilities of the adversary. Even existing quantum-resistant protocols [15], [17]–[21], [23], [24] harness the computational incapacities of a quantum adversary and depend on quantum-hard problems. Designing security protocols around quantum-hard problems protects against quantum adversaries today, but in the near future, efficient algorithm discovery could allow an adversary to solve quantum-hard problems and put [15], [17]–[21], [23], [24] protocols at risk, similar to what happened with computationally hard problems. Hence, V2G applications utilizing such protocols are not future-safe. Also, very often, the majority of existing V2G literature does not feature entity privacy protection, privacy-preserving mutual authentication & key agreement, or privacy-preserving message communication. Therefore, there is a strong need to develop new quantum-

resistant authentication and key exchange protocols in the V2G environment to guarantee the security of information exchange between entities. Besides, crucial privacy features also need careful consideration. Consequently, the proposed work describes a newly designed quantum communication-based authentication and key exchange protocol for V2G communication. The newly designed protocol does not depend on either computationally or quantum hard problems but rather uses the laws of quantum mechanics to guarantee quantum security, hence are future-safe. It supports privacy-preserving mutual authentication and key agreement as well as conditional privacy-preserving message communication, i.e., privacy-preserving EV charging request processing. Besides, it also protects V2G entities from privacy attacks and maintains EV and CS privacy, as well as safeguarding V2G communication from various known cyber attacks.

A. Contributions

This work first introduces a quantum communication-based system model for V2G systems. Afterward, the work describes EVs, CSs, and utility center (UC) registration and authentication processes. The key contribution of the proposed work, namely QSKA, is as follows:

- 1) We developed a new privacy-preserving mutual authentication scheme, QSKA, which employs a quantum communication protocol and hash functions to ensure authenticity between V2G entities such as EVs, CS, and UC.
- 2) QSKA ensures security features, including message integrity, message authentication, non-repudiation, and mutual identity authentication between EVs, CSs, and UC. Also, QSKA ensures crucial privacy features, including EV anonymity, EV message unlinkability, EV-identity privacy, and EV location privacy. Besides, QSKA withstands security attacks such as eavesdropping attacks, MITM attacks, impersonation attacks, and replay attacks.
- 3) QSKA is independent of the computational capabilities of the adversary to guarantee communication security, hence preventing quantum attacks. Additionally, QSKA enables eavesdropping detection and ensures efficient EV traceability if any EV misbehaves.
- 4) The extensive security and performance evaluation of QSKA against state-of-the-art work [11]–[14], [16], [29] indicates that it furnishes higher security and privacy features (as mentioned in Table I) and offers up to 82.93% and 25.89% lower communication and computation overhead, respectively. Also, QSKA consumes up to 69.98% less energy while maintaining the system's high security and privacy than existing solutions.

B. Organization

The remaining article is organized as follows: Related work is investigated in Section II. The system model of the proposed scheme is presented in Section III. Section IV discusses the details of the proposed privacy-preserving mutual authentication and communication scheme, QSKA. Section V thoroughly discusses the security features of the proposed scheme. Later,

Section VI outlines the overhead analysis describing performance evaluation and simulation results. Finally, Section VII concludes this article.

II. RELATED WORK

In the literature, many schemes have been proposed to safeguard energy-internet-based V2G communication, such as the scheme by Gope and Sikdar [11], which describes a new privacy-preserving authentication scheme for EI-based V2G networks. In the scheme, [4], an identity-based two-key exchange protocol employing ECC is described to efficiently handle the computational overhead of advanced metering infrastructure. Similarly, the scheme [5] proposes a two-key exchange protocol employing ECC and symmetric encryption (SE). Again using SE and ECC, the authors of [6] discuss a new scheme featuring replay attack and MITM attack protection. The scheme is based on the Needham Schroeder authentication protocol. An efficient key distribution scheme is proposed in [7], which ensures security in the V2G network and protects it from MITM attacks. Besides, Park et al. [8] put forward a new key generation and distribution scheme. However, the scheme suffers from impersonation attacks and does not feature privacy. To securely distribute the keys in SG, the scheme [9] integrates identity-based encryption and identity-based signature. However, the scheme does not provide session key security or smart meter privacy. Besides, the scheme [30] describes IoT environment authentication scenarios and their respective constraints and provides an authenticated key agreement between IoT devices and mobile clients. Table I compares related work about location privacy support, quantum resistance, EV identity privacy, EV traceability support, strengths and weaknesses. Many privacy-preserving schemes have been discussed in the literature; for instance, a protocol discussed by Yang et al. in [31] namely P^2 , which uses a rewarding scheme for EVs and features privacy for individual EVs. Another protocol, namely $AP3A$ featuring privacy for each EV, has been designed by Liu et al. [10]. The scheme also provides a facility to identify whether the individual EV is moving in the visitor network or the home network. The scheme [32] discusses a cross-domain model using blockchain for enhancing security and achieving patient anonymity. Similarly, the scheme [33] discusses a lightweight mutual authentication and key agreement protocol using physical unclonable function and a chaotic system for the Internet of drones featuring privacy preservation. The privacy-preserving scheme described in [34] for the V2G network uses a session key to provide security and a self-synchronized mechanism to provide privacy.

Despite the availability of many protocols featuring privacy, mutual authentication, and key establishment in the V2G network, most of them depend on an adversary's computational incapacities to ensure security. Traditional encryption and authentication techniques rely on computationally hard problems like integer factorization and discrete log problems to ensure security. These problems are currently unsolvable by classical computers in polynomial time but can be easily solved by quantum algorithms. Shor's algorithm reduces the

computational time for integer factorization, while the Grover search algorithm accelerates the inverse hash function search and has implications for symmetric cryptographic protocols. As a result, it is essential to develop new quantum-resistant protocols to counteract the threat posed by quantum computers. Two options exist: employ quantum cryptography or ensure the security of new quantum-resistant protocols on hard problems that can withstand quantum attacks. Recently, the work [17] described an authenticated key exchange protocol, namely LB-2PAKA, for the Internet of vehicles. The protocol uses the concepts of identity-based cryptography and lattices and depends on the hardness of bilateral small integer solution (Bi-SIS) and computational bilateral inhomogeneous small integer solution (cBi-ISIS) problems for security. Although the work [17] is quantum-resistant, it suffers from a key escrow problem and does not feature privacy. Later, the work [18] demonstrates a conditional privacy-preserving authentication protocol (CPPA) using lattice for vehicular communication that relies on the hardness of the SIS problem for security. The work [16], [35] presents a new quantum communication-based CPPA employing BB84 quantum key distribution and classical identity authentication in vehicular and smart grid communication, respectively. The work [29] designs a quantum-resistant mutual authentication scheme for securing the smart grid neighbourhood area network using quantum-resistant public key encryption. In the work [19], the authors present new quantum-resistant encryption and signature schemes depending on the hardness of the SIS problem. Besides, many quantum-resistant protocols using lattices [15], [20], [21], [23], [24] are available in the literature for ensuring vehicular communication security. However, all such protocols depend on some hard lattice problems like SIS, learning with errors (LWE), the shortest vector problem (SVP), and the closest vector problem (CVP) that are well known to ensure security against even quantum adversaries. The work [15] describes a quantum-resistant protocol whose security depends on SIS and LWE problems for edge-based vehicular communication featuring conditional privacy and batch verification. The work [20] describes a batch-verifiable lattice-based CPPA protocol that simultaneously achieves vehicle privacy preservation and message integrity and depends on the hardness of CVP and SVP. Similarly, the authors of [21] discussed the lattice-based CPPA protocol for vehicular communication featuring tamper-proof OBU requirements and depending on the hardness of SIS and ISIS problems. The scheme, [22] uses BB84-based QKD and designs a novel enrollment and verification mechanism for vehicles. The authors of [23] demonstrate a lattice-based group signature protocol, namely FSA-LGS, depending on the hardness of LWE and SIS lattice problems, whereas the protocol QBCPDA [24] features mutual authentication, batch verification, data security, & privacy and depends on the hardness of SIS problems.

The quantum-resistant protocols in the literature rely heavily on hard lattice problems or do not provide privacy protection. Besides, many quantum communication techniques have matured with the fast development of quantum platforms. Therefore, this article describes a quantum communication-based novel privacy-preserving quantum-resistant protocol that

does not depend on any hard problems, either computational or quantum, is future-safe, and is suitable for the V2G environment. Specifically, superdense coding is utilized in the proposed work to achieve efficient communication. Compared to other quantum communication protocols like quantum teleportation or BB84-based quantum key distribution, superdense coding uses a single qubit for two classical bits of transmission, making the protocol efficient and reducing network traffic. It is more efficient because it can send two classical bits of information using only one qubit, allowing for higher communication rates with fewer resources needed for communication. Besides, superdense coding minimizes the susceptibility of qubits to errors during information transmission by encoding qubits using a two-qubit encoding technique, resulting in simplicity, more reliable information transmission, and a reduction in the probability of error during transmission. In fact, for the same level of error correction, it requires fewer gates than other quantum approaches, like quantum teleportation. Also, it has low resource requirements, like the most basic quantum gates and techniques, making it simpler and more straightforward to implement. The proposed work, QSKA, incorporates V2G entity authentication depending on superdense coding-based key exchange to prevent unauthorized access. Also, QSKA provides resistance to quantum adversaries, which are anticipated to pose a serious challenge to classical authentication protocols. Furthermore, QSKA preserves the V2G entity's privacy, ensuring that no adversary can access any private information regarding the EV. Not only this, but QSKA generates low communication and computation overheads of 82.93% and 25.89%, respectively, as compared to the other protocols mentioned.

III. SYSTEM MODEL

This section describes the system model, adversary model, security and privacy requirements, adopted assumptions, and background details of the proposed QSKA.

A. System Model for EI-based V2G Network

The high-level view of the V2G network, along with its entities like electric vehicles (EVs), charging stations (CSs), and utility center (UC), have been described herewith and illustrated through Fig. 1. The details of each entity are as follows:

- **EVs:** It has installed an onboard unit (OBU) with low computation ability. The OBUs of EVs possess bidirectional communication ability and can transfer messages to both CSs and UC. EVs can act as energy producers and consumers as EVs can discharge and charge their installed battery during high demand and low demand on CSs. The EVs possess quantum communication ability and thus can run quantum key distribution.
- **CSs:** It possesses sufficient computation ability. It enables the charging of EVs whenever EV requests. It also has installed a smart meter to monitor and maintain energy transfer (either stored or withdrawn) between EVs and CSs. The CSs can be owned by many private companies to avoid monopoly and can be installed in different

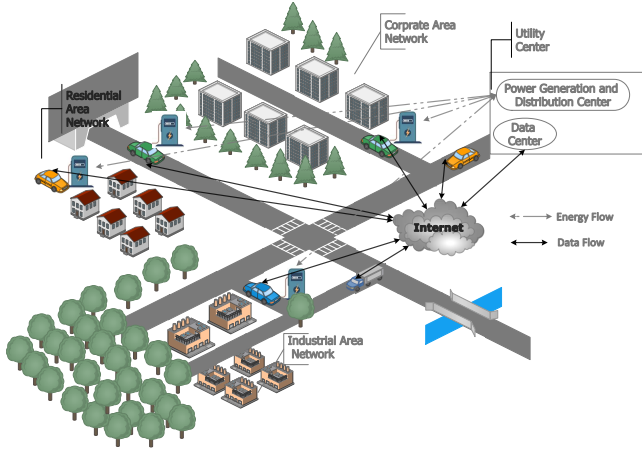


Fig. 1. System Model

localities within cities. Depending on the location of CSs, charging and discharging rates for any EV may vary. For instance, the charging rate may be higher in commercial area networks compared to public and residential area networks.

- **UC:** The responsibility of UC includes the registration of EVs and CSs. It comprises two components: power generation and distribution (PGDC) and data center (DC). The PGDC is responsible for supplying power to different CSs installed in different parts of the city and procuring electricity from different vendors. The DC stores and maintains all information on EVs and CSs registered with UC.

The EV registers themselves with the UC in the registration phase and authenticates each other through a public channel. Specifically, individual EVs pre-authenticate themselves through CSs to UC and receive secrets for further secure authentication and communication with CSs. The registration and pre-authentication phases use a type of quantum communication called superdense coding between EVs, CSs, and UC to generate shared secrets between EVs and/or CSs and UC. Since the communication involves an insecure public channel and a quantum channel, QSKA considers the following adversary model:

B. Adversary Model

The adversary model of QSKA considers EVs to interact with CSs and UC through a secure channel during the registration of EVs. Also, registration of CSs with UC is performed through a secure channel. Besides, the execution of the QSKA protocol uses an insecure public channel. In this context, the QSKA considers Dolev-Yao model [36] where an adversary can intercept the exchanged messages between EVs, CSs, and/or UC and access the public channel for performing many attacks. Also, an adversary can perform forgery, replay, and man-in-the-middle attacks. An adversary may utilize the public channel to acquire information related to the real identity of any EVs and can impersonate on behalf of the individual EV to take advantage of any services. Therefore, the identity privacy of EVs needs to be guaranteed. Additionally,

TABLE II
SECURITY AND PRIVACY REQUIREMENTS

Notations	Definition
SPR1: Mutual authentication	The authenticity of both the EV and UC can be mutually verified.
SPR2: Session Key agreement	The EV and CS generate a shared session key to facilitate secure data communication.
SPR3: Resistance to known attacks	The scheme is designed to withstand different types of attacks, including eavesdropping, replay, Man-in-the-Middle (MITM), and impersonation attacks.
SPR4: Anonymity	The identities of both EV and CS should not be revealed to potential attackers.
SPR5: Forward secrecy	The scheme ensures that even if an attacker obtains the secret keys of a specific session, they cannot gain access to the secret keys of previous sessions.
SPR6: No clock synchronization	The scheme does not address issues that arises from time delays and clock synchronization.
SPR7: EV location privacy	QSKA protects the EV location privacy.
SPR8: EV identity privacy	QSKA protects the EV real-identity privacy.
SPR9: EV message unlinkability	QSKA maintains the unlinkability between two messages originated from the same EV.
SPR10: EV traceability	QSKA enables the EV traceability, if the EV misbehaves.
SPR11: Unconditional security	QSKA achieves security without relying on computationally hard problems.

any adversary with malicious intent can try to extract the identity information of individual EVs during an exchange of messages through the insecure channel between EVs, CSs, and/or UC. The adversary may also try to discover whether or not two messages originated from the same vehicle. Besides, the location privacy of EVs is another major concern. Also, malicious EVs may report fake locations to incur low charging fees.

C. Security and Privacy Requirements

Considering the well-known evaluation criteria [37] for quantum-resistant protocols, we design QSKA to meet the security and privacy requirements as mentioned in Table II. The privacy requirements as described in Table II, such as anonymity, EV identity privacy, and EV message unlinkability, pertain to the assessment of conditional privacy-preserving features, while the other requirements primarily relate to the evaluation of security features.

D. Assumptions

- 1) The utility center is considered as the trusted authority with sufficient computation and memory capabilities, whereas CSs are considered semi-trusted (honest but curious) entities. The EVs are considered resource constraints with limited computation and memory capabilities.
- 2) The EVs have installed equipment to extract biological details such as retina details, facial details, or fingerprint details of the driver of EVs.
- 3) The onboard units (OBUs) of EVs are tamper-proof.
- 4) Each entity of the V2G network, like EVs, CS, and UC, features quantum communication ability. Besides the clock of EVs, CSs and UC are also synchronized.

TABLE III
GENERATION OF ENCRYPTED IDENTITY

Bit Number	1	2	3	4	5	6	7	8
Vehicle Real-Identity (I_{EV_i})	1	1	1	1	0	0	0	1
Biological Characteristics	0	1	0	1	0	1	0	1
Encrypted Identity ($EncI_{EV_i}$)	0	1	0	1	1	0	1	1

E. Background of Proposed Work

QSKA uses superdense coding - a quantum communication protocol to establish the key between the V2G network entities. The superdense coding requires the pre-shared entangled key between entities to transfer the information between entities within the V2G network. Specifically, superdense coding uses one qubit to transfer information of two classical bits. The entangled key is shared between entities of the V2G network, for instance, EV and UC, as follows: EV and UC has individual qubit $|q_a\rangle$ and $|q_b\rangle$, respectively, which is set to $|0\rangle$. EV applies the H operator to his qubit, which results in state $|+\rangle = (\frac{1}{\sqrt{2}})$. Afterwards, EV and UC combine their

qubits $|q_a\rangle$ and $|q_b\rangle$ which results in $(\frac{1}{\sqrt{2}}) \otimes (1) = (\frac{1}{\sqrt{2}})$.

Henceforth, EV applies the CNOT operator on two qubits $|q_a\rangle$ and $|q_b\rangle$, which leads to a new quantum state

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Now, EV and UC qubits $|q_a\rangle$ and $|q_b\rangle$ are correlated with each other, i.e., EV and UC have established an entangled key. If EV and/or UC measure their qubits, they observe either $|00\rangle$ or $|11\rangle$. If EV observes his qubit now, i.e., EV observes his qubit after entanglement and finds $|0\rangle$, then UC qubit also collapses to $|0\rangle$. Otherwise, if EV finds the qubit as $|1\rangle$, the UC qubit collapses to $|1\rangle$. In literature, experimental results confirm that correlated particles affect each other even if there is a large physical distance between them. Besides, the EVs in QSKA encodes the real identity I_{EV_i} into encrypted identity $EncI_{EV_i}$ as reported through Table III. Specifically, the not translation of real identity I_{EV_i} of EV_i is XORed with EV_i 's driver biological characteristics to produce $EncI_{EV_i}$.

IV. PROPOSED PROTOCOL

QSKA is the privacy-preserving authentication protocol designed to enable secure communication between EV and CS by utilizing the properties of quantum mechanics. QSKA comprises four phases: system initialization, EV pre-authentication, EV pseudo-identity & session key generation, and EV message authentication & verification. In the EV pre-authentication phase, QSKA authenticates the EV with UC using a quantum communication protocol, namely superdense coding. Afterwards, UC produces a pseudo-identity, and CS produces a session key for EV in the pseudo-identity and session key generation phase. These secrets further allow privacy-preserving EV to CS communication during the message authentication and verification phase. QSKA uses superdense coding with a hash function to exchange the secret keys between EV, UC, and/or CS. The notations for the acronyms

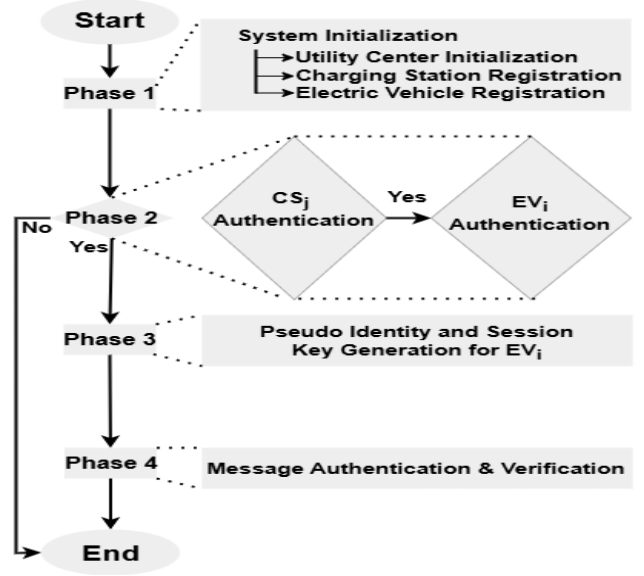


Fig. 2. Description of the QSKA

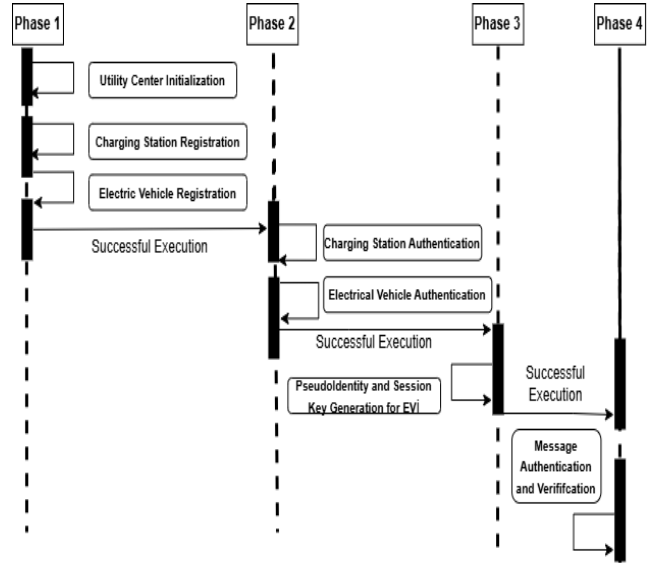


Fig. 3. Phase Sequences of the QSKA

used in the QSKA are denoted in Table IV, whereas Fig. 3 reveals the description of the QSKA.

A. System Initialization

This is the first phase of the proposed QSKA, and it covers the initialization processes of EV, CS, and UC.

1) *UC Initialization*: The UC handles the responsibility of generating secrets for EV and CS. The UC produces the entangled pair $|q_a\rangle$ and $|q_b\rangle$ as described in preliminaries. Generally, UC updates the databases of EV and CS with superdense coding-based secrets during the registration procedure for EV and CS. Also, UC checks the legitimacy of individual EV_i during the EV pre-authentication phase, where $i = 1, 2, \dots, n$ (n denotes the number of EVs in an area). The successful

TABLE IV
NOTATIONS FOR THE ACRONYMS USED

Notations	Descriptions
I_{EV_i}	Representing identity of i^{th} Electric Vehicle
I_{CS_j}	Representing identity of j^{th} Charging Station
$ q_m \rangle_i$	EV_i entangled pairs of quantum bits entangled with $ q_n \rangle_i$
$ q_n \rangle_i$	UC's entangled pairs of quantum bits entangled with $ q_m \rangle_i$
$ q_k \rangle_j$	CS_j entangled pairs of quantum bits entangled with $ q_l \rangle_j$
$ q_l \rangle_j$	UC's entangled pairs of quantum bits entangled with $ q_k \rangle_j$
EV_i	Representing i^{th} Electric Vehicle
CS_j	Representing j^{th} Charging Station
TS	Timestamps
$ q_{pm} \rangle_i$	EV_i entangled pairs of quantum bits, entangled with $ q_{pn} \rangle_i$ & used during EV pre-authentication phase
$ q_{pn} \rangle_i$	UC's entangled pairs of quantum bits, entangled with $ q_{pm} \rangle_i$ & used during EV pre-authentication phase
$ q_{pk} \rangle_j$	CS_j entangled pairs of quantum bits, entangled with $ q_{pl} \rangle_j$ & used during EV pre-authentication phase
$ q_{pl} \rangle_j$	UC's entangled pairs of quantum bits, entangled with $ q_{pk} \rangle_j$ & used during EV pre-authentication phase
Pwd_{EV_i}	Secret password of i^{th} Electric Vehicle (EV_i)
Pwd_{CS_j}	Secret password of j^{th} Charging Station (CS_j)
Pwd'_{EV_i}	Sent password by EV_i during EV pre-authentication phase
Pwd'_{CS_j}	Sent password by CS_j during EV pre-authentication phase

legitimacy inspection of individual EV_i enables UC to produce secrets and pseudo-identity for the corresponding EV_i .

2) *CS Initialization*: CS acquires a unique identity, I_{CS_j} , from the utility center (UC). The details of the registration process are depicted in Fig. 4 and described as follows:

- 1) Once CS acquires a unique identity I_{CS_j} , it establishes an entangled pair with the utility center, as discussed in the preliminaries. The length of entangled pairs $|q_{k_j} \rangle$ and $|q_{l_j} \rangle$ are same as length of I_{CS_j} .
- 2) UC sends $|q_{k_j} \rangle$ to CS and retain $|q_{l_j} \rangle$ to itself. Afterward, CS uses superdense coding to send two bits of a secret using recently received qubits $|q_{k_j} \rangle$.
- 3) CS chooses a random secret password with the length equals to I_{CS_j} and then for every two bits lets say $(a_1, b_1), (a_2, b_2), \dots, (a_j, b_j), \dots, (a_n, b_n)$ of the chosen secret password Pwd_{CS_j} , CS prepares individual one qubit $|q_{k_j} \rangle$. CS then inspects the individual value of every two bits from the chosen secret password i.e., CS checks the value of a_j and b_j where, $j = 1, 2, 3 \dots n$.
- 4) If the value of a_j equals to one, CS apply Z operator to corresponding $|q_{k_j} \rangle$. If the value of b_j equals to one, CS apply X gate (NOT operator) to corresponding $|q_{k_j} \rangle$. CS then sends $|q_{k_j} \rangle$ to utility center UC.
- 5) After receiving $|q_{k_j} \rangle$ from CS, UC applies controlled-X C_X gate to both qubit $|q_{k_j} \rangle$ and $|q_{l_j} \rangle$ with $|q_{k_j} \rangle$ as controller qubit. It may be noted that $|q_{k_j} \rangle$ denotes the recently received qubit from CS, and $|q_{l_j} \rangle$ denotes the already possessed qubit by UC.
- 6) UC applies H gate to each $|q_{k_j} \rangle$ and then measures both entangled qubits $|q_{k_j} \rangle$ and $|q_{l_j} \rangle$ thereby obtaining the sent secret password Pwd_{CS_j} of CS. Finally, UC stores the secret password corresponding to CS in its database.

3) *EV Initialization*: EV acquires a unique identity, I_{EV_i} , from the UC. Afterwards, the EV_i encodes I_{EV_i} to $EncI_{EV_i}$

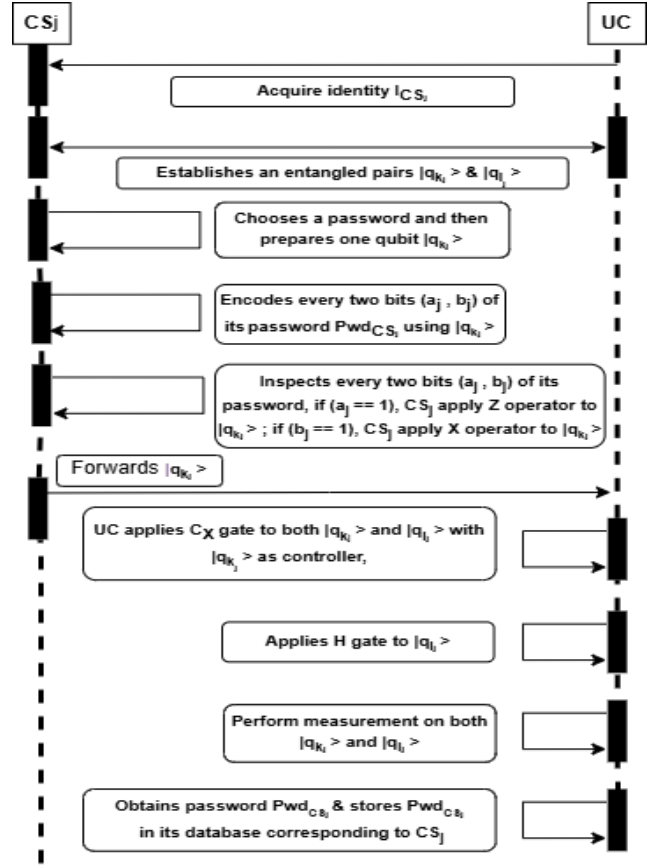


Fig. 4. CS registration process

with biological data like fingerprint details. The encoding process is already described in the preliminaries. The specific details of the EV_i registration process are depicted in Fig. 5 and described as follows:

- 1) As soon as i^{th} electric vehicle EV_i obtains a unique identity $EncI_{EV_i}$, it establishes entangled pair with the utility center as discussed in preliminaries. The length of entangled pairs $|q_{m_i} \rangle$ and $|q_{n_i} \rangle$ are same as length of $EncI_{EV_i}$.
- 2) UC sends $|q_{m_i} \rangle$ to EV_i and retain $|q_{n_i} \rangle$ to itself. Afterward, EV_i uses superdense coding to send two bits of a secret using recently received single qubit $|q_{m_i} \rangle$.
- 3) EV_i chooses its own secret password with the length equals to $EncI_{EV_i}$ and then for every two bits lets say $(a_1, b_1), (a_2, b_2), \dots, (a_i, b_i), \dots, (a_3, b_3)$ of chosen secret password Pwd_{EV_i} , EV_i prepares one qubit $|q_{m_i} \rangle$. Thereafter, EV_i checks the individual value of every two bits from chosen secret password i.e., EV_i checks the value of a_i and b_i where, $i = 1, 2, 3 \dots n$.
- 4) If the value of a_i equals to one then EV_i apply Z operator to $|q_{m_i} \rangle$. If the value of b_i equals to one then EV_i apply X gate (NOT operator) to $|q_{m_i} \rangle$. Afterwards, EV_i sends $|q_{m_i} \rangle$ to utility center UC.
- 5) After receiving $|q_{m_i} \rangle$ from EV_i , UC applies controlled-X C_X gate to both qubit $|q_{m_i} \rangle$ and $|q_{n_i} \rangle$ with $|q_{m_i} \rangle$ as controller qubit. It may be noted that $|q_{m_i} \rangle$ denotes the recently received qubit from EV_i and $|q_{n_i} \rangle$ denotes

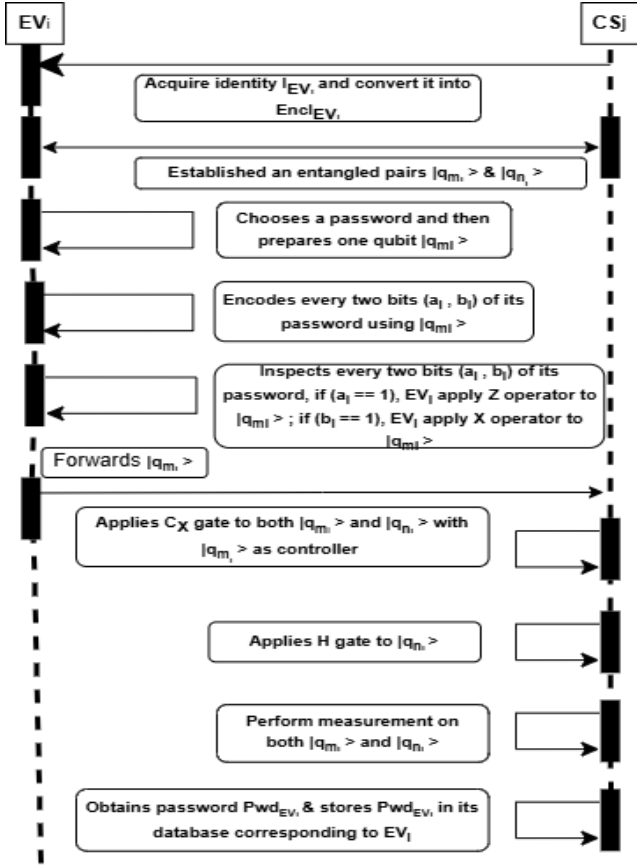


Fig. 5. EV registration process

the already possessed qubit by UC.

- 6) UC applies H gate to $|q_{m_i}\rangle$ and then measures both qubits $|q_{m_i}\rangle$ and $|q_{n_i}\rangle$ thereby obtaining the sent secret password Pwd_{EV_i} of EV_i . Finally, UC stores the secret password corresponding to EV_i in its database.

QSKA uses one qubit to enable the secure exchange of two bits of information between entities of the V2G network. Given that, for every two bits of the secret password of CS and EV_i , one qubit is transferred to UC. The chosen secret password by CS and EV_i may vary and can be more than two bits. Therefore, the total number of qubits required to exchange N bits of secret passwords is $N/2$. Here, to exchange n bits secret password represented by (a_1, b_1) , (a_2, b_2) , (a_3, b_3) ... $(a_{n/2}, b_{n/2})$, the total number of qubits required is $n/2$ represented by $|q_{k_1}\rangle$, $|q_{k_2}\rangle$, $|q_{k_3}\rangle$... $|q_{k_{n/2}}\rangle$.

B. EV Pre-Authentication

The EV pre-authentication phase examines the authenticity of each registered EV before it participates in energy trading with CS. UC examines EV's authenticity through CS. The EV_i transfers the request $V_{req} = HMAC(Pwd_{EV_i}, EncI_{EV_i}) || EncI_{EV_i} || TS$ to UC through CS_j for inspecting its identity $EncI_{EV_i}$. The EV pre-authentication phase of QSKA is depicted in Fig. 6. UC before inspecting $EncI_{EV_i}$, authenticates the identity of CS_j .

- 1) UC generates entangled pairs for CS, as discussed in the preliminaries. The length of entangled pairs $|q_{pk_j}\rangle$ and $|q_{pl_j}\rangle$ are same as length of I_{CS_j} .
- 2) UC sends $|q_{pk_j}\rangle$ to CS and retain $|q_{pl_j}\rangle$ to itself. Afterward, CS uses superdense coding to send two bits of a secret using recently received qubits $|q_{pk_j}\rangle$.
- 3) CS uses the secret password it received from UC during its own registration process and then for every two bits lets say (pa_1, pb_1) , (pa_2, pb_2) , ..., (pa_j, pb_j) , ..., (pa_n, pb_n) of received secret password during registration process, CS prepares individual one qubit $|q_{pk_j}\rangle$. CS then inspects the individual value of every two bits from its secret password i.e., CS checks the value of pa_j and pb_j where, $j = 1, 2, 3, \dots, n$.
- 4) If the value of pa_j equals to one, CS apply Z operator to corresponding $|q_{pk_j}\rangle$. If the value of pb_j equals to one, CS apply X gate (NOT operator) to corresponding $|q_{pk_j}\rangle$. CS then sends $|q_{pk_j}\rangle$ to utility center UC.
- 5) After receiving $|q_{pk_j}\rangle$ from CS, UC applies controlled-X C_X gate to both qubit $|q_{pk_j}\rangle$ and $|q_{pl_j}\rangle$ with $|q_{pk_j}\rangle$ as controller qubit. It may be noted that $|q_{pk_j}\rangle$ denotes the recently received qubit from CS, and $|q_{pl_j}\rangle$ denotes the already possessed qubit by UC at the start of the pre-authentication process, i.e., at step 1.
- 6) UC applies H gate to each $|q_{pk_j}\rangle$ and then measures both entangled qubits $|q_{pk_j}\rangle$ and $|q_{pl_j}\rangle$ thereby obtaining the sent secret password Pwd'_{CS_j} . Finally, UC matches the recently received secret password Pwd'_{CS_j} corresponding to CS in its database. If the match is unsuccessful, UC discards the request; otherwise, CS is considered legal, and CS starts the inspection of the EV's identity.
- 7) UC generates entangled pairs for EV, as discussed in the preliminaries. The length of entangled pairs $|q_{pm_i}\rangle$ and $|q_{pn_i}\rangle$ are same as length of $EncI_{EV_i}$.
- 8) UC sends $|q_{pm_i}\rangle$ to EV_i and retain $|q_{pn_i}\rangle$ to itself. Afterward, EV_i uses superdense coding to send two bits of a secret using recently received single qubit $|q_{pm_i}\rangle$.
- 9) EV_i uses its own secret password received during its own registration process and then for every two bits lets say (pa_1, pb_1) , (pa_2, pb_2) , ..., (pa_i, pb_i) , ..., (pa_3, pb_3) of its secret password (received during registration process), EV_i prepares one qubit $|q_{pm_i}\rangle$. Thereafter, EV_i checks the individual value of every two bits from chosen secret password i.e., EV_i checks the value of pa_i and pb_i where, $i = 1, 2, 3, \dots, n$.
- 10) If the value of pa_i equals to one then EV_i apply Z operator to $|q_{pm_i}\rangle$. If the value of pb_i equals to one then EV_i apply X gate (NOT operator) to $|q_{pm_i}\rangle$. Afterwards, EV_i sends $|q_{pm_i}\rangle$ to utility center UC.
- 11) After receiving $|q_{pm_i}\rangle$ from EV_i , UC applies controlled-X C_X gate to both qubit $|q_{pm_i}\rangle$ and $|q_{pn_i}\rangle$ with $|q_{pm_i}\rangle$ as controller qubit. It may be noted that $|q_{pm_i}\rangle$ denotes the recently received qubit from EV_i and $|q_{pn_i}\rangle$ denotes the already possessed qubit by UC at step 7.
- 12) UC applies H gate to $|q_{pm_i}\rangle$ and then measures

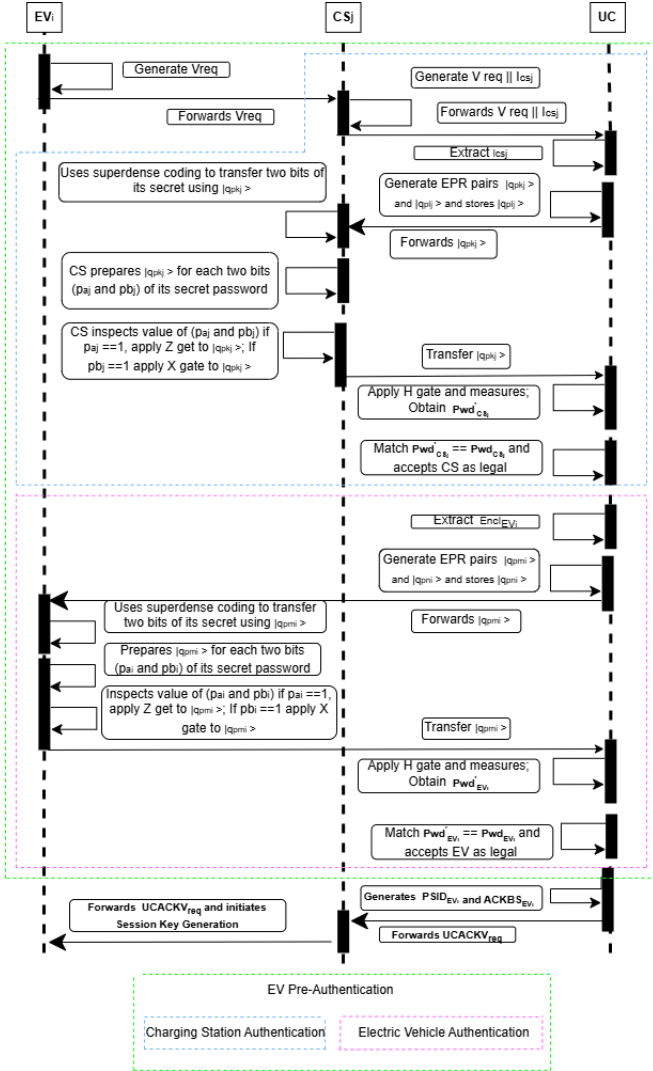


Fig. 6. EV pre-authentication phase of QSKA

both qubits $|q_{pm_i}\rangle$ and $|q_{pn_i}\rangle$ thereby obtaining the sent secret password $Pwd_{EV_i}^l$. Finally, UC matches the recently received secret password $Pwd_{EV_i}^l$ corresponding to EV_i in its database. If the match is unsuccessful, UC discards the request; otherwise, EV_i is considered legal.

C. Pseudo-identity and Session Key Generation

The successful EV_i authentication allows UC to generate a random number r and pseudo-identity $PSID_{EV_i} = E_{Pwd_{EV_i}}[I_{EV_i} || r]$ for particular EV_i . Afterwards, UC transmits back $UCACKV_{req} = PSID_{EV_i} || TS$ to CS_j . Following this, CS_j forwards the $UCACKV_{req}$ to EV_i and commences the procedure to establish a session key corresponding to $PSID_{EV_i}$. The session key generation steps are as follows:

- 1) As soon as EV_i receives $UCACKV_{req}$ from UC through CS_j , EV_i extracts $PSID_{EV_i}$ and verifies the $PSID_{EV_i}$ authenticity by performing decryption with Pwd_{EV_i} . After successful $PSID_{EV_i}$ authenticity verification, EV_i establishes entangled pair with CS_j as discussed in

preliminaries. The length of entangled pairs $|q_{sm_i}\rangle$ and $|q_{sn_i}\rangle$ are same as length of $PSID_{EV_i}$.

- 2) CS_j sends $|q_{sm_i}\rangle$ to EV_i and retain $|q_{sn_i}\rangle$ to itself. Afterwards, EV_i uses superdense coding to send two bits of session key using recently received single qubit $|q_{sm_i}\rangle$.
- 3) EV_i chooses its own session key with the length equals to $PSID_{EV_i}$ and then for every two bits lets say $(a_1, b_1), (a_2, b_2), \dots, (a_i, b_i), \dots, (a_3, b_3)$ of chosen session key $SKey_{EV_i}$, EV_i prepares one qubit $|q_{sm_i}\rangle$. Thereafter, EV_i checks the individual value of every two bits from chosen session key i.e., EV_i checks the value of a_i and b_i where, $i = 1, 2, 3, \dots, n$.
- 4) If the value of a_i equals to one then EV_i apply Z operator to $|q_{sm_i}\rangle$. If the value of b_i equals to one then EV_i apply X gate (NOT operator) to $|q_{sm_i}\rangle$. Afterwards, EV_i sends $|q_{sm_i}\rangle$ to CS_j .
- 5) After receiving $|q_{sm_i}\rangle$ from EV_i , CS_j applies controlled-X C_X gate to both qubit $|q_{sm_i}\rangle$ and $|q_{sn_i}\rangle$ with $|q_{sm_i}\rangle$ as controller qubit. It may be noted that, $|q_{sm_i}\rangle$ denotes the recently received qubit from EV_i and $|q_{sn_i}\rangle$ denotes the already possessed qubit by CS_j .
- 6) CS_j applies H gate to $|q_{sm_i}\rangle$ and then measures both qubits $|q_{sm_i}\rangle$ and $|q_{sn_i}\rangle$ thereby obtaining the sent session key $SKey_{EV_i}$. Finally, CS_j stores the session key corresponding to $PSID_{EV_i}$ in its own database.

Later, EV_i uses the recently established session key $SKey_{EV_i}$ for future correspondence with CS_j . The end of this phase concludes that EV_i has received a pseudo-identity $PSID_{EV_i}$ corresponding to its identity I_{EV_i} from UC and established a session key $SKey_{EV_i}$ with CS_j corresponding to pseudo-identity $PSID_{EV_i}$ thereby enabling further privacy-preserving secure communication with CS_j . The pseudoidentity and session key generation phase of QSKA is depicted in Fig. 7. To generate a new session key after a session expires, the EV_i sends its pseudo-identity $PSID_{EV_i}$ and current session key encrypted using superdense coding. Afterwards, CS_j matches the received session key corresponding to the pseudo-identity in its database. CS_j uses the session key generation algorithm again to regenerate a new session key if the match is successful, otherwise, discard the request. Specifically, to generate a new session key corresponding to EV_i , CS_j successfully validates the previous session key, establishes a new EPR pair ($|q_{asm_i}\rangle$ and $|q_{asn_i}\rangle$) with the same length as $PSID_{EV_i}$, and follows steps 2) - 6) of the EV session key generation algorithm as discussed above. After the successful regeneration of a new session key corresponding to $PSID_{EV_i}$, CS_j updates the existing session key corresponding to pseudo-identity in its database.

D. Message Authentication and Verification

The EV_i under the range of particular CS_j sends the charging request $C_{req} = (M, E_{SKey_{EV_i}}(LID_{EV_i}), PSID_{EV_i}, TS)$ to CS_j . The CS_j authenticates the M embedded in C_{req} after looking each session key corresponding to $PSID_{EV_i}$ in its database. At the end, for verification of M included in C_{req} , CS_j computes HMAC digest M' . Following this, CS_j

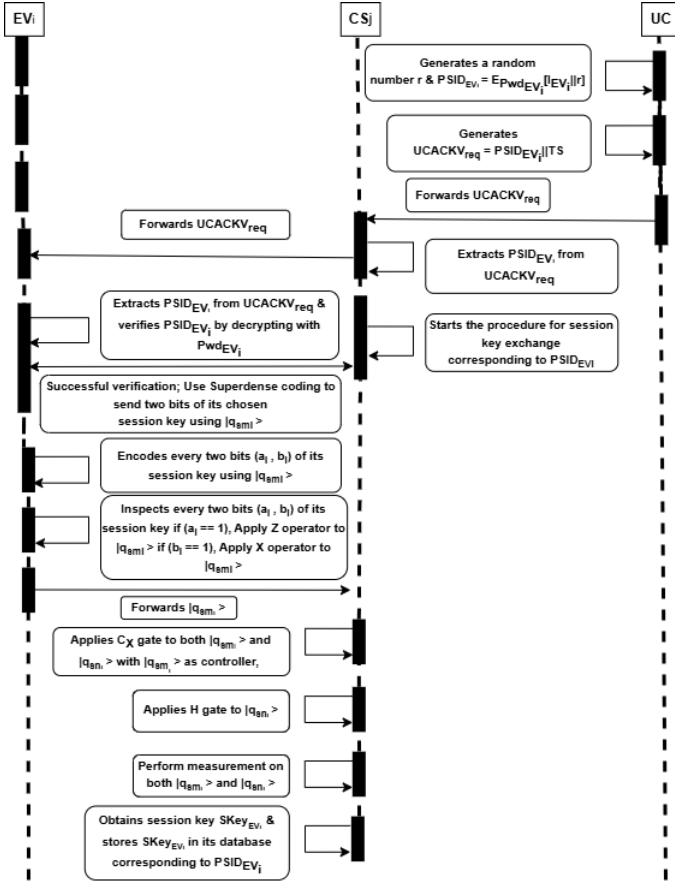


Fig. 7. Pseudoidentity and Session key generation phase of QSKA

compares the M' with M . The successful result allows the CS_j to consider C_{req} as legal otherwise C_{req} is considered illegal and CS_j reports back $PSID_{EV_i}$ to UC for EV_i traceability. In case of legal C_{req} , the CS_j looks for LID_{EV_i} by decrypting $E_{SKey_{EV_i}}(LID_{EV_i})$ with one of the shared session key corresponding to $PSID_{EV_i}$. Afterwards, CS_j process C_{req} only if LID_{EV_i} falls under his coverage area.

$$M = HMAC(SKey_{EV_i}, Z)$$

$$Z = E_{SKey_{EV_i}}(LID_{EV_i}) || PSID_{EV_i} || TS$$

V. SECURITY ANALYSIS

This section evaluates the security features supported by QSKA and compares the security feature with regard to existing work [11]–[14], [16], [29]. Provable security uses formal methods and well-known assumptions from complexity theory (like the insolvability of the discrete logs problem for classical authentication protocols and the insolvability of quantum hard problems for quantum-resistant protocols) to reach security goals that have already been set when evaluating and proving the security of cryptographic protocols [37]. Provable security is a more common way to analyze and evaluate protocols than heuristic methods because it makes it easier to define security goals in a way that can be used to justify security provisions. The work [38] shows that the five steps for evaluating and analyzing new cryptographic protocols are part of the methods

that can be shown to be secure. The steps are: (a) defining the adversarial model; (b) defining the security goal; (c) defining the cryptographic assumptions; (d) describing the protocol; and (e) proving by reduction. Most of the time, any cryptographic protocol that can be shown to be secure makes cryptographic assumptions based on a chosen security model in order to meet security goals that have already been set. The security proofs that come from formal methods might not have enough security models or the wrong reductions of security proofs, so they might not be able to guarantee security against real-world threats [38]. Adopting an inadequate security model frequently results in erroneous security proof that either fails to express a reasonable level of attacker proficiency or provides inaccurate security proof. Also, [39] shows that the correctness of a security proof depends heavily on the prover's experience as an attacker. Even with a correct security model and the right way to reduce security proof using provable security techniques, it is not possible to guarantee that a security functionality analysis will be perfect and error-free. So, the traditional heuristic approach is still useful for showing that newly designed protocols are safe. Consequently, we present QSKA security features evaluation based on heuristic approach corresponding to security and privacy requirements described in Table II.

A. Security Features Supported

The existing state-of-the-art protocols involve asymmetric cryptography or elliptic curve cryptography-based techniques that depend heavily on the computational hardness of either integer factorization problem, discrete log problem, or elliptic curve discrete log problem. However, running Shor's algorithm on a quantum computer can easily break the computational hardness of integer factorization, discrete log problem, and elliptic curve discrete log problem by solving it in polynomial time, thereby endangering existing state-of-art protocols used to secure communication between EV_i , CS_j and UC. Consequently, we designed a new quantum-resistant protocol - QSKA, which uses quantum communication protocol, namely superdense coding, for securely exchange the keys between entities and to generate secrets and pseudo-identities, which enables secure privacy-preserving communication between EV_i , CS_j and UC. However, the V2G network can still encounter internal and external attacks like eavesdropping attacks, replay attacks, man-in-the-middle attacks, and many more. Therefore, QSKA supports the following security goals: **1) Supports Mutual Authentication:** During registration process of EV_i and CS_j , the secret password chosen by individual EV_i and CS_j is sent to UC using qubits. Specifically, for every two bits of the chosen secret password of individual EV_i and CS_j , one individual qubit is sent to UC. UC then stores the received secret password corresponding to EV_i and CS_j in its database. During the EV pre-authentication phase of QSKA, EV_i and CS_j prepare and transfer one qubit for every two bits of its secret password shared during the registration process with UC. Therefore, only legitimate EV_i and CS_j can prepare intermediate qubits and successfully authenticate in QSKA. Each qubit and two bits of secret

password holds the corresponding relationship; hence qubits prepared corresponding to different secret password results in different secret password generation at the UC end. Afterward, UC discards such pre-authentication requests by scrutinizing its database. EV_i assumes UC to be legal when EV_i finds its own identity by decrypting the received $PSID_{EV_i}$ during the pseudo-identity and session key generation phase of QSKA. The $PSID_{EV_i}$ consists identity of individual EV_i and random salt value r encrypted with secret password Pwd of EV_i which is only shared between corresponding EV_i and UC. Therefore, QSKA enables mutual authentication.

2) Resists Impersonation Attack: To successfully impersonate EV_i , an attacker must perform a successful authentication process. To successfully authenticate, an attacker needs each quantum bit $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$ for EV_i and CS_j respectively. The length of quantum bit $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$ depends on the length of the chosen password by EV_i and CS_j respectively. Besides, copying quantum bits is prohibited because of the No cloning theorem. Hence, it is impossible for an attacker to prepare quantum bits exactly same as each $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$ without knowing exact secret password Pwd_{EV_i} and Pwd_{CS_j} of respective EV_i and CS_j .

3) Resists Replay Attack: The charging request C_{req} sent during the message authentication and verification phase of QSKA incorporates timestamp values (TS) and HMAC. Using timestamp values ensures connection termination, and using HMAC guarantees authentication error for an attacker. Even if an attacker uses old tokens and tries to establish message authentication with CS_j , he needs to modify message M , which contains timestamp values. The modification of M is only possible using session key $SKey_{EV_i}$, which is only shared between EV_i and CS_j ; hence an adversary cannot perform a successful replay attack.

4) Resists Eavesdropping Attack: During the registration and EV pre-authentication process, for every two bits of the secret password of EV_i and CS_j , one qubit is sent to UC through a quantum channel. The no-cloning theorem enforces collapsing of the sent qubit if any attacker eavesdropped in the quantum channel. Besides, during message authentication and verification, sniffing of charging request C_{req} by the adversary in the classical channel does not reveal any meaningful information. Hence, QSKA resists an eavesdropping attack.

5) Ensures EV Anonymity: The QSKA guarantees EV_i anonymity as QSKA disables any attacker from extracting identity information of individual EV_i during message exchange between EV_i and CS_j and/or UC. In the pseudo-identity & session key generation phase of QSKA, the charging station CS_j produces and saves session key for individual EV_i corresponding to pseudo-identity $PSID_{EV_i}$ received in $UACKV_{req}$ thus does not save any identification information related to individual vehicle EV_i . Also, a possible compromise of charging station CS_j will only inform pseudo-identity instead of real-identity of individual vehicle EV_i . Besides, the $PSID_{EV_i}$ embedded in $UACKV_{req}$ gets generated by UC and contains real-identity information of individual vehicle EV_i encrypted using corresponding Pwd_{EV_i} which is only known to corresponding vehicle and UC hence guarantees anonymity from semi-trusted charging station CS_j . Even C_{req}

sent during message authentication and verification phase involves $PSID_{EV_i}$ hence does not include any identification information of individual EV_i .

6) Ensures EV Message Unlinkability: The QSKA guarantees EV message unlinkability as QSKA disables any attacker from discovering whether two charging requests C_{req} and C'_{req} are sent by the same EV_i or two different EV_i . Assume, $C_{req} = (M, Z) = (\text{HMAC}(SKey_{EV_i}, Z), E_{SKey_{EV_i}}(LID_{EV_i} || PSID_{EV_i} || TS))$ and $C'_{req} = (M', Z') = (\text{HMAC}(SKey_{EV_i}, Z'), E_{SKey_{EV_i}}(LID_{EV_i} || PSID'_{EV_i} || TS'))$. Here, C_{req} and C'_{req} are indistinguishable to each other even if sent by the same EV_i . The charging request C_{req} and C'_{req} are completely random and hence cannot be predicted as C_{req} and C'_{req} uses HMAC which follows random oracle. HMAC produces a complete random output for any two input messages, even with a single bit of difference. Also, Z and Z' are unrelated because of difference in timestamp values and/or LID_{EV_i} . Most of the time, the LID_{EV_i} for individual EV_i varies whenever EV_i moves within the city. The message M used in C_{req} includes Z ; hence M keeps changing at each step. So, we can conclude that $M = \text{HMAC}(SKey_{EV_i}, Z) = \text{HMAC}(SKey_{EV_i}, E_{SKey_{EV_i}}(LID_{EV_i} || PSID_{EV_i} || TS))$ and $M' = \text{HMAC}(SKey_{EV_i}, Z') = \text{HMAC}(SKey_{EV_i}, E_{SKey_{EV_i}}(LID_{EV_i} || PSID_{EV_i} || TS))$ are unrelated either because of change in timestamp values, HMAC function and/or location values. Therefore, the attacker cannot link C_{req} and C'_{req} to particular EV_i thereby ensuring unlinkability of C_{req} and C'_{req} and subsequently untraceability of corresponding EV_i . Now, we can conclude that since QSKA guarantees EV_i anonymity and EV_i message (charging request C_{req}) unlinkability, therefore QSKA features privacy preservation.

7) Prevents MITM Attack: To successfully launch MITM attack in QSKA, an attacker requires the qubit $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$. The preparation of $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$ holds corresponding relationship with secret password Pwd_{EV_i} and Pwd_{CS_j} which is shared only between UC and individual EV_i and CS_j respectively. The copying of qubit $|q_{pm_i}\rangle$ and $|q_{pk_j}\rangle$ by adversary during communication is prohibited because of the No cloning theorem.

8) Preserves Location Privacy: The EV_i sends C_{req} to CS_j for charging its battery during the message authentication and verification phase of QSKA. The C_{req} consists location identifier LID encrypted with $SKey_{EV_i}$ which is shared only between CS_j and particular EV_i corresponding to $PSID_{EV_i}$, hence can only be decrypted by CS_j thereby preserving the location privacy of EV_i .

9) Preserves EV Identity Privacy: During the Pseudo-identity and Session key generation phase of QSKA, UC produces pseudo-identity $PSID_{EV_i}$ corresponding to received identity $EncI_{EV_i}$ after successful verification of $EncI_{EV_i}$ involving quantum communication protocol namely super-dense coding between UC and particular EV_i . Later, EV_i uses $PSID_{EV_i}$ for communication with CS_j to process C_{req} hence preserving real identity of EV_i . Besides, during EV pre-authentication phase of QSKA, EV_i sends $EncI_{EV_i}$ instead of I_{EV_i} to UC for verification of its identity. UC sends the produced pseudo-identity $PSID_{EV_i}$ to EV_i through semi-

trusted charging station CS_j . However, QSKA ensures the privacy of real identity of EV_i even from semi-trusted CS_j as $PSID_{EV_i}$ consists identity of EV_i encrypted with secret key shared only between UC and particular EV_i obtained to particular EV_i while EV_i registration phase. Apart from this, $PSID_{EV_i}$ also includes salt value r hence $PSID_{EV_i}$ itself does not disclose anything with respect to identity of EV_i .

10) Enables EV Traceability: QSKA enables EV_i traceability whenever CS_j encounters a illegal C_{req} and reports back to UC. Specifically, UC extracts $PSID_{EV_i}$ from C_{req} and search for $PSID_{EV_i}$ in its own database. If the search is successful, UC initiates the penalty procedure for corresponding EV_i as per the policy.

B. Security Verification

Coq is a formal proof management system that provides a programming language and logic for expressing mathematical assertions, algorithms, and theorems, together with tools for interactive development of machine-checked proofs. Coq has been widely used in various domains, including security verification of quantum communication-based protocols. Coq [40] allows for rigorous reasoning about the properties and behavior of quantum protocols, providing a high level of confidence in the security of these protocols. One of the benefits of using Coq for security verification of quantum communication-based protocols is that it allows for formal reasoning about the protocol’s behavior and properties. This helps to identify potential vulnerabilities in the protocol and provides a way to prove that the protocol meets its security requirements. Coq also enables the generation of machine-checked proofs that can be used to verify the correctness of the protocol’s security properties. Consequently, we have formally verified the security of QSKA using the Coq proof assistant.

C. Security Features Comparison

The comparison of QSKA with current state-of-art protocols is performed and presented through Table V. In Table V, “yes” indicates that the protocol supports the corresponding security feature, whereas “no” depicts that the protocol does not ensure the particular security feature. As it is evident from Table V that all mentioned protocols ensure mutual authentication and message integrity. The security feature, namely mutual authentication, allows all parties involved in communication to check each other authenticity. Message integrity allows communication parties to check whether the message has been modified during communication. QSKA uses HMAC to support message integrity. Additionally, most of the mentioned protocols resist MITM attacks and eavesdropping attacks. Similarly, the entities such as EVs, CSs, and UC are protected from MITM and eavesdropping attacks in QSKA. The protocol [11] is vulnerable to replay attack. The protocol [13] does not guarantee EV anonymity. The protocol [11], [14] and [16] does not ensure session key security. The protocols [11], [12], [13] and [14] depends on the hardness of computational problems to guarantee security thus does not ensure unconditional security. Out of all mentioned protocols, only [16], [29] and QSKA ensures unconditional security. Although, [29] and

[16] are quantum-resistant but they do not ensure man-in-the-middle attack protection and preserves session key security, respectively. However, QSKA using quantum communication, namely superdense coding, guarantee unconditional security and ensure higher security.

TABLE V
SECURITY FEATURE COMPARISON

Supports Security Feature	[11]	[12]	[13]	[14]	[16]	[29]	QSKA
Mutual Authentication	yes	yes	yes	yes	yes	yes	yes
Session Key Security	no	yes	yes	no	no	yes	yes
Message Integrity	yes	yes	yes	yes	yes	yes	yes
EV Anonymity	yes	yes	no	yes	yes	-	yes
Resists MITM Attack	yes	yes	yes	yes	yes	no	yes
Replay Protection	no	yes	yes	yes	yes	yes	yes
Resists Impersonation Attack	yes	yes	yes	yes	yes	yes	yes
Unconditional Security	no	no	no	no	yes	yes	yes

VI. PERFORMANCE EVALUATION

This section first discusses the benchmark schemes [11]–[14], [16], [29] and describes the evaluation setup. Afterwards, this section introduces the considered performance metrics: computation overhead, communication overhead, and energy overhead, and details the approach for QSKA performance evaluation. The QSKA is developed in python¹. We also present the correctness verification of superdense coding that is used in the QSKA to guarantee unconditionally secure key exchange between V2G entities. Finally, this section presents the detailed discussion on QSKA performance analysis corresponding to considered performance metrics with respect to the introduced benchmark schemes [11]–[14], [16], [29].

A. Simulation Setup and Benchmarks

We revisited the recent authentication and key agreement protocols and obtained the corresponding results for performance comparison and analysis as benchmark schemes. The core ideas of these benchmark schemes [11]–[14], [16], [29] are as follows: The scheme [11] describes a privacy-preserving authentication protocol for EV charging request processing and involves two phases: registration and authentication. The scheme [12] describes an authenticated key agreement protocol featuring lightweight primitives and involves three phases: registration, login and authentication, and password revision. Besides, [13] discusses a mutual authentication protocol using a physical unclonable function and features a different session key between EV and the aggregator. The scheme involves two phases: mutual authentication between vehicle and aggregator, and mutual authentication between aggregator and grid. The scheme [14] discusses signcryption-based privacy-preserving authentication and a key exchange protocol involving two phases: registration and mutual authentication. The other schemes, [16] and [29] are quantum-resistant schemes for vehicular communication and smart grid environments, respectively. The scheme [16] involves four phases, whereas the scheme [29] involves three phases: initialization, key establishment, and data transmission. The benchmark schemes [11]–[14] are not quantum resistant. Furthermore, [12], [13] do not consider privacy when designing secure authentication and

¹tinyurl.com/ieec-qsk

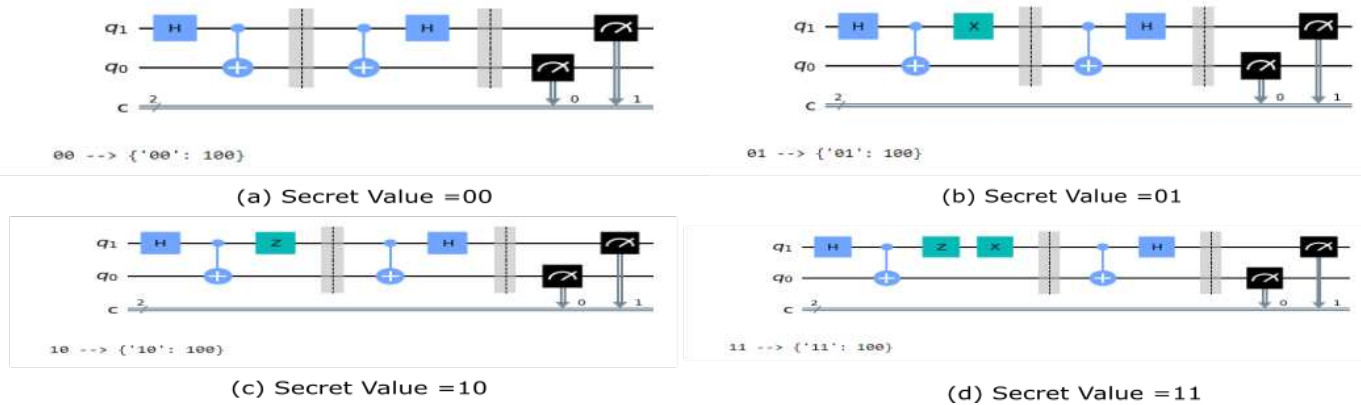


Fig. 8. Circuit used with varying secret and sent by EV to UC

do not include privacy-preserving secure data transmission. However, the schemes [11] and [14] feature privacy-preserving authentication but do not describe privacy-preserving data transmission. The schemes [16] and [29] are quantum-resistant and designed for different application areas, but can be well applicable to V2G scenarios. Although schemes [16] and [29] are quantum-resistant, similar to QSKA, they feature higher communication and energy overhead when compared to QSKA. Not only this, but QSKA features privacy-preserving message communication unlike others.

The quantum-capable edge devices that can simulate V2G entities are limited and yet to arrive in the market. Consequently, QSKA calculates the performance metric on the basis of classical and quantum primitives separately. To calculate the performance metric on the basis of classical primitives, QSKA considers the experimental setup comprising an Arduino ATmega328 to represent EV, a laptop powered by a core i3 processor @ 3.6 GHz base frequency together with 8 GB of RAM to represent CS, and a desktop server to represent UC. The considered desktop server features a configuration of a core i9 processor @ 5.8 GHz maximum frequency and 32 GB of RAM, whereas the Arduino ATmega328, representing an EV, has a clock speed of 16 MHz and 2 KB of SRAM, similar to the real world, where the exact amount of RAM varies by model in electric vehicles (EVs) of different vendors like the Audi e-tron, Volkswagen ID.4, or Nissan Leaf, with some models having as little as 2 KB of RAM and others having up to 2 GB. Finally, to obtain the results corresponding to the discussed performance metrics, QSKA measures the implementation time of different classical cryptographic operations on the Arduino ATmega328 to simulate values of EV_i . Similarly, the implementation time of classical cryptographic operations corresponding to CS_j is obtained on a laptop. In contrast, values corresponding to UC that require extremely high computing power are obtained on a desktop. Also, QSKA performance metrics on the basis of used quantum primitives are discussed in the respective performance metric subsections.

We simulate the quantum communication protocol utilized in QSKA, namely, superdense coding, on the “qasm simulator” and verify its correctness. Specifically, the simulation of superdense coding is performed using Qiskit [41], the python pro-

gramming language, and Jupyter Notebook on the Linux-based machine powered with a core i9 processor with a 3.6 GHz base frequency and 32 GB RAM. Qiskit is an open-source software development kit that integrates different simulators at the backend, like “qasm simulator”, “Aer simulator,” and many more, with multiple configuration options. For simulation of superdense coding, we have created a quantum circuit with two qubits namely EV_i qubit and UC qubit for each pair of (a,b) belongs to (0,0), (0,1), (1,0), (1,1) with both qubits initially set to $|0\rangle$. Afterward, we apply h-gate (Hadamard) to EV_i qubit and then apply C_X gate on both EV_i qubit and UC qubit with EV_i qubit as controller. Afterward, assuming EV_i qubit and UC qubit are separated from each other, we apply Z-gate to EV_i qubit if a equals to 1 and we apply X-gate (NOT Gate) to EV_i qubit if b equals to 1. Afterward, EV_i sends its qubit to UC. Upon receiving a qubit from EV_i , UC applies C_X gate on both UC and EV_i qubits. Finally, UC measure both UC and EV_i qubits and compare the result with input secret (a,b). We have performed the simulation 100 times, i.e., we have considered shots = 100. The obtained result for four possible secret values (combination of (a,b)) is depicted through Fig 8. It may be noted that all four figures follow the output format $ab \rightarrow \{‘ab’: k\}$ where ab represents the input bits, ‘ab’ represents the output bits of the simulator, and k signifies the frequency, i.e., how many times/shots simulation output is obtained from the simulator. Here, in the subfigure (a) of Fig. 8, the output format- 00 --> {'00': 100}, signifies for input 00, simulator output is ‘00’ with 100% probability (since we have considered shots = 100 while simulating and received output is also 100). It is evident from the figures that for each combination of shared secrets in the form of classical bits (a,b), we received the output of measurement corresponding to the input we provided in the circuit. In other words, the simulation results reveal that the receiver will receive the same secret sent by the sender if the superdense coding is used during communication. Therefore, we can conclude that the UC will receive the same secret (in the form of classical bits) that the EV_i transfers using qubits through the quantum communication protocol, superdense coding, and henceforth verify the correctness of QSKA.

B. Results and Analysis

We used computation overhead, communication overhead, and energy overhead as performance metrics for evaluating QSKA's performance. The communication overhead of the security protocol is the extra data transmission and processing needed for security, whereas the computation overhead refers to the additional processing time and resources required to implement a security protocol. Encryption, authentication, and other security mechanisms cause communicational and computational overhead, which affects efficiency, security, compatibility, and cost and needs careful balance. Similarly, energy overhead refers to the additional energy consumption required to implement a security protocol and incurs the extra energy usage introduced by encryption, decryption, and other security mechanisms. To calculate the communication overhead of QSKA, we took into account both the size of each message and the number of messages transmitted between the V2G entities, whereas the implementation time of various cryptographic operations used in different phases of QSKA determines the computation overhead. QSKA's energy consumption measurement is based on maximum CPU power and computational cost [14]. We also measured the performance of the discussed benchmark schemes on the basis of the considered performance metric and compared them with QSKA for performance analysis. The specific details of QSKA's computational overhead, energy consumption, and communication overhead are described in the respective subsections **VI-C**, **VI-D** and **VI-E**.

C. Computation Overhead

QSKA, while calculating computation overhead, obtains the implementation time of cryptographic function like one-way hash (T_h) as 0.001352 ms, 0.001752 ms, and 0.0001030 ms at EV_i , CS_j and UC, respectively in the experimental setup discussed above. The obtained execution time of the HMAC function for the vehicle, charging station, and UC is 0.001352 ms, 0.001752 ms, and 0.0001030 ms. Similarly, the execution time of encryption/decryption function at vehicle, charging station and UC is 0.00936 ms, 0.001823 ms, 0.0001030 ms [14]. QSKA uses superdense coding to securely transfer the secrets between different entities of the V2G network; thus, QSKA also calculates the quantum cost of superdense coding. Basically, the quantum cost of the superdense coding protocol means the quantum cost of the corresponding superdense circuit. Usually, basic gates feature unit cost regardless of their internal structure, and the gates H_d , H_d^ψ , $U_{ab,2}$, Z_k and CNOT gate are considered basic gates [42]. In the proposed protocol QSKA, the superdense coding circuit used is assumed of dimension $d = 2$, which means QSKA uses a 2-dimensional superdense circuit. Given that, QSKA incurs the quantum cost $QCost_{ab,d}$ for the classical message (a,b) and dimension d as follows:

$$\begin{aligned}
 QCost_{ab,d} &= QCost_{ab,2} \\
 QCost_{ab,2} &= QCost(H) + QCost(U_{ab,2}) \\
 &\quad + QCost(CN_2) + QCost(M) \\
 &= 2 \times 1 + QCost(U_{ab,2}) + 2 \times 1 + 1 \\
 &= QCost(U_{ab,2}) + 5
 \end{aligned} \tag{1}$$

where $QCost(H)$, $QCost(U_{ab,2})$, $QCost(CN_2)$ and $QCost(M)$ denote the quantum cost of the Hadamard gate, unitary operations, CNOT gate, and final measurement operation, respectively. Based on the corresponding gate $U_{ab,2}$ for message (a, b), the $QCost(U_{ab,2})$ is depicted through Table VI. Also, the total quantum cost of an individual classical message (a,b) in QSKA is reported in Table VI. So, for every two bits transferred through superdense coding, QSKA incurs a quantum cost of either 5 (when both bits are zero) or 6 (when both bits are not zero). Similarly, for n -bit message exchange, QSKA will incur a quantum cost of $5(n/2)$ (when all n -bits are zero); otherwise, $6(n/2)$ and can be represented as $O(n)$. In the EV pre-authentication phase of QSKA, EV_i computes V_{req} and uses superdense coding to transfer the password for authenticating itself, incurring computational cost $T_{Hmac} = 0.001352ms$ and quantum cost $O(n)$. During pseudo-identity generation of EV_i , UC uses the encryption function while encrypting the EV identity, incurring a computation cost $T_E = 0.0001030ms$. Afterward, EV_i computes the decryption function for verifying the authenticity of the received $PSID_{EV_i}$ thus incurring the computation cost $T_D = 0.00936ms$. Also, EV_i and CS_j establish a $SKey_{EV_i}$ corresponding to $PSID_{EV_i}$ using superdense coding and thus incur a quantum cost $O(n)$. Subsequently, during the EV_i message authentication and verification phase, EV_i sends M in C_{req} thus computation cost incurred by EV is $T_{Hmac} = 0.001352ms$. Also, to verify the M , CS_j incurs the computation cost of $T_{Hmac} = 0.001352ms$. Therefore, QSKA features a $2 T_{Hmac} + T_E + 2T_{Hmac} + T_D = 2 \times 0.001352ms + 0.00936ms + 0.001752ms + 0.0001030ms = 0.013919ms$ computation cost and $O(n)$ quantum cost. In the scheme [11], the EV_i , CS_j and UC requires time cost of $7T_H = 7 \times 0.001352ms = 0.009464ms$, $2T_H = 2 \times 0.001752ms = 0.003504ms$ and $7 T_H = 7 \times 0.0001030ms = 0.000721ms$ respectively. The scheme [12] requires time costs of $7T_H = 7 \times 0.001352ms = 0.009464ms$, $2T_H = 2 \times 0.001752ms = 0.003504ms$ and $7 T_H = 7 \times 0.0001030ms = 0.000721ms$ respectively, whereas the scheme by Bansal et al. [13] requires time cost of $4T_H = 4 \times 0.001352ms = 0.005408ms$ & $1T_{E/D} = 0.00936ms$ at EV_i , $2T_H = 2 \times 0.001752ms$ & $2T_{E/D} = 2 \times 0.001823ms$ at CS_j and $3T_H = 0.0001030ms$ & $2T_{E/D} = 2 \times 0.0001030ms$ at UC. Also, the scheme [14] incurs $5T_H = 5 \times 0.001352ms$, $2T_H = 2 \times 0.001752ms$ & $5T_H = 5 \times 0.0001030ms$ at EV_i , CS_j and UC, respectively. Similarly, the scheme [16] requires the time cost of $5T_{Hmac} = 5 \times 0.001352ms = 0.00676ms$ and $T_D = 0.00936ms$ at EV_i , $5T_{Hmac} = 5 \times 0.001352ms = 0.00676ms$ at CS_j and $T_E = 0.0001030ms$ at UC. Also, QSKA ignores the cost of pairing operations of [29] while comparing. Consequently, the work [29] requires the time cost of $3T_h = 3 \times 0.001352ms = 0.004056ms + 2T_E = 2 \times 0.00936ms$ and $T_D = 0.00936ms$ at EV_i , $5T_h = 5 \times 0.001752ms = 0.00876ms + 2T_E = 2 \times 0.001823ms$ and $T_D = 0.001823ms$ at CS_j . As a result, the schemes [16] and [29] incur total computation costs of 0.024983ms and 0.04636ms, respectively. The relative comparison of the QSKA computation cost is presented in Table VII. It is clearly evident from the table VII that QSKA requires least computation cost than [11]–[14], [16] & [29]

and offers higher security and privacy goals including quantum resistance.

TABLE VI
QUANTUM COST

Classical Message	Number of Basics Gates	Operations $U_{ab,2}$	$QC_{ost}(U_{ab,2})$	$QC_{ost_{ab,2}}$
(0, 0)	2	$U_{00,2} = I$	0	5
(0, 1)	3	$U_{01,2} = \sigma_X$	1	6
(1, 0)	3	$U_{10,2} = \sigma_Z$	1	6
(1, 1)	3	$U_{11,2} = i\sigma_Y$	1	6

TABLE VII
COMPUTATION OVERHEAD

Scheme	Electric (EV_i)	Vehicle	CS_j / NAN Gateway / RSU	Utility Center (UC)
[11]	$7T_h$	$2T_h$	$2T_h$	$7T_h$
[12]	$7T_h$	$2T_h$	$2T_h$	$7T_h$
[13]	$T_{E/D} + 4T_h$	$2T_{E/D} + 2T_h$	$2T_{E/D} + 2T_h$	$3T_h + 2T_{E/D}$
[14]	$5T_h$	$2T_h$	$2T_h$	$5T_h$
[16]	$5T_{Hmac} + T_D$	$5T_{Hmac}$	$5T_{Hmac}$	T_E
[29]	$3T_h + 2T_E + T_D$	$5T_h + 2T_E + T_D$	$5T_h + 2T_E + T_D$	-
QSKA	$2T_{Hmac} + T_D$	$2T_{Hmac}$	$2T_{Hmac}$	T_E

D. Energy Consumption

The energy consumed by QSKA is measured as the sum total of energy consumed due to communication overhead and computation overhead. QSKA energy consumption due to computational overhead is measured as $CC \times P_p$ [14] where CC and P_p represent total computational cost and maximum CPU power = $10.88W$ respectively. Also, QSKA energy consumption due to communicational overhead is measured as the energy required to send/receive 1 bit of data \times the number of bits involved in the communication [35]. The obtained execution time of the HMAC function for the vehicle, charging station, and UC is 0.001352 ms, 0.001752 ms, and 0.0001030 ms in the experimental setup as described earlier. Similarly, the execution time of the encryption/decryption functions at the vehicle, charging station, and UC are 0.00936 ms, 0.001823 ms, and 0.0001030 ms, respectively [14]. Also, it is assumed that EV consumes $0.72 \mu J$ to communicate one bit of data. The QSKA consumes energy equivalent to $0.013919ms \times 10.88W = 0.154452mJ = 154.452\mu J$ due to computational overhead and $0.72 \mu J \times 1184 = 852.48\mu J$ due to communicational overhead. Consequently, the total energy consumption of QSKA is equivalent to $1003.91 \mu J$. Similarly, the schemes [16] and [29] incur computational overhead of $0.024983ms \times 10.88W = 0.27181mJ = 271.81\mu J$ and $0.04636ms \times 10.88W = 0.50441mJ = 504.45\mu J$, respectively. Also, because of communicational overhead, the schemes [16] and [29] incurs $0.72 \times 2864 = 2062.08\mu J$ and $0.72 \times 6938 = 5499.81\mu J$, respectively. Therefore, the schemes [16] and [29] incur a total of $2533.89 \mu J$ and $5499.81 \mu J$ respectively. The relative energy consumption comparison of QSKA with existing state-of-the-art protocols [11]–[14], [16] and [29] due to computational overhead is depicted in Table VIII and illustrated in Fig. 9. It is clearly visible from Table VIII that the QSKA consumes 37.94%, 44.28% and 69.98% less energy when compared to [13], [16], and [29], respectively. However, QSKA consumes slightly more energy

when compared to [11], [12], and [14], but it features higher security and privacy goals and provides unconditional security, unlike [11], [12] and [14].

TABLE VIII
COMMUNICATION AND ENERGY OVERHEAD

Scheme	Communication Cost (bits)	Energy Consumption (μJ)
[11]	2936	148.93
[12]	3744	148.93
[13]	3168	244.03
[14]	2816	117.2
[16]	2864	271.81
[29]	6938	504.45
QSKA	1184	151.43

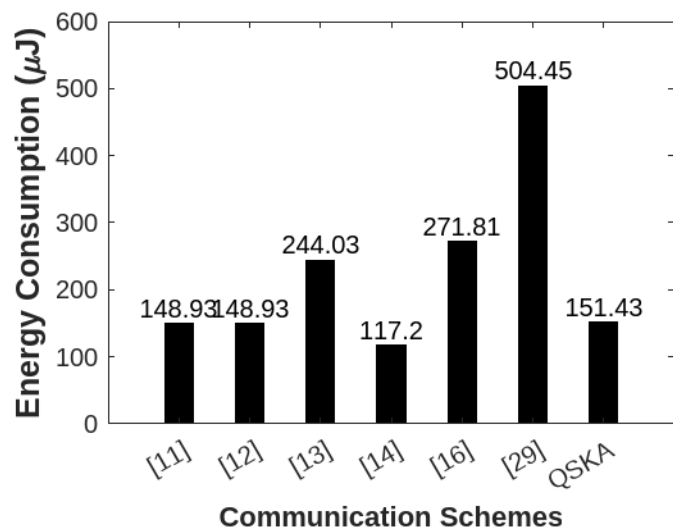


Fig. 9. Energy Consumption Comparison

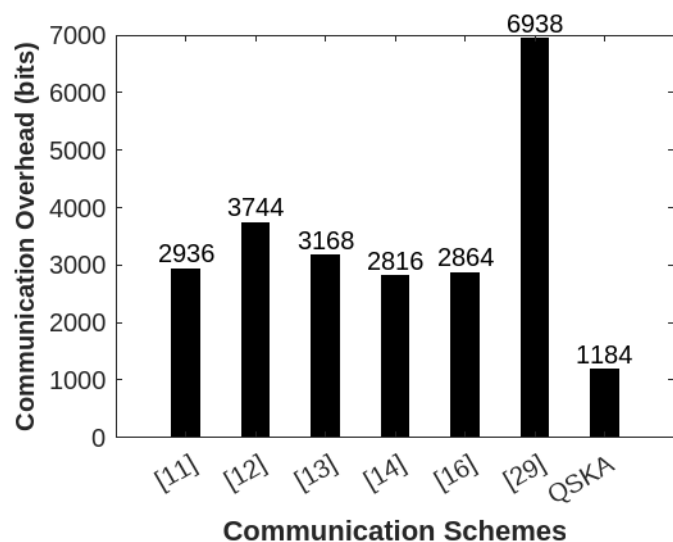


Fig. 10. Communication Cost Comparison

E. Communication Overhead

The total number of messages exchanged between EV_i , CS_j , and UC, along with the corresponding message size,

is considered while calculating the communication overhead incurred by QSKA. We have considered the size of different cryptographic functions included in the exchanged message as follows: size of identity = 160 bits, size of random number = 160 bits; size of secret key = 160 bits; size of encryption/decryption function = 128 bits; size of hash function = 256 bits; and size of HMAC function = 256 bits [14]. In the QSKA, the EV sends $V_{req} = HMAC(Pwd_{EV_i}, EncI_{EV_i}) || EncI_{EV_i} || TS$ to verify its identity during the EV pre-authentication phase, incurring a communication cost of $32B + 20B + 4B = 56B$. Also, EV_i receives $UCACKV_{req} = PSID_{EV_i} || TS$ from UC through charging station CS_j thereby incurring communication costs of $20B + 4B = 24B$. Finally, the message authentication and verification phase of QSKA sends $C_{req} = (M, ESKey_{EV_i}(LID_{EV_i}), PSID_{EV_i}, TS)$ thereby incurring communication costs of $32B + 16B + 16B + 4B = 68B$. Henceforth, the total communication cost of QSKA equals $56B + 24B + 68B = 148B = 1184$ bits. In the scheme, [11], exchanged messages involve one identity, five random numbers, and 13 hash functions, thus incurring communication costs equivalent to 2936 bits. The scheme [12] uses five times identities, three random numbers, and eight hash functions during the exchange of messages, thereby incurring communication costs of $5 \times 160 + 3 \times 160 + 8 \times 256 = 3744$ bits. Also, the scheme [13] during the exchange of messages involves two times identity, six random numbers, four hash functions, and four encryption/decryption functions, thus incurring the communication cost of $2 \times 160 + 6 \times 160 + 4 \times 256 + 4 \times 128 = 3168$ bits. The scheme [14] uses five hash function and the six signcrypt/unsigncrypt functions while exchanging messages, incurring a communication cost equivalent to $5 \times 256 + 6 \times 256 = 2816$ bits. Similarly, the communication costs incurred by [16] and [29] are 2864 bits and 6938 bits, respectively. The relative comparison of QSKA with existing protocols [11]–[14], [16] and [29] is depicted in Table VIII and illustrated in Fig. 10. Table VIII clearly shows that QSKA incurs 59.67%, 68.37%, 62.62%, 57.95%, 58.65% and 82.93% lower communication overhead compared to current state-of-the-art protocols [11]–[14], [16] and [29], respectively and offers higher security and privacy goals.

VII. CONCLUSION AND FUTURE WORK

This work describes a new quantum-secured privacy-preserving authentication protocol for the EI-based V2G environment. Specifically, the protocol uses superdense coding for the verification of entities. The successful authentication enables the generation of secrets that are subsequently shared between entities within the V2G environment. The generated secrets further enable privacy-preserving communication between entities within the V2G environment. The security evaluation section demonstrates that the proposed scheme, QSKA, resists numerous security attacks and protects the privacy of entities. Also, QSKA enables quantum security by utilizing the laws of quantum mechanics. The performance evaluation section reveals that QSKA consumes less energy and has low communication and computation costs. In the

future, we will upgrade QSKA by integrating hyperledger technology to incorporate decentralization.

REFERENCES

- [1] M. Ashfaq, O. Butt, J. Selvaraj, and N. Rahim, "Assessment of electric vehicle charging infrastructure and its impact on the electric grid: A review," *International Journal of Green Energy*, vol. 18, no. 7, pp. 657–686, 2021.
- [2] W. Han and Y. Xiao, "Privacy preservation for v2g networks in smart grid: A survey," *Computer Communications*, vol. 91, pp. 17–28, 2016.
- [3] S. Ali, "The future of indian electricity demand: How much, by whom, and under what conditions?" 2018.
- [4] A. Mohammadali, M. S. Haghghi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2834–2842, 2016.
- [5] H. Nicanfar and V. C. Leung, "Multilayer consensus ecc-based password authenticated key-exchange (mcepak) protocol for smart grid system," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 253–264, 2013.
- [6] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375–381, 2011.
- [7] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.
- [8] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution scheme proposed by xia and wang," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1613–1614, 2013.
- [9] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE transactions on smart grid*, vol. 7, no. 2, pp. 906–914, 2015.
- [10] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1722–1733, 2012.
- [11] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.
- [12] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.
- [13] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for v2g using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020.
- [14] S. Ahmed, S. Shamsad, Z. Ghaffar, K. Mahmood, N. Kumar, R. M. Parizi, and K.-K. R. Choo, "Signcrypt based authenticated and key exchange protocol for ei-based v2g environment," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5290–5298, 2021.
- [15] D. Dharminder, S. Kumari, and U. Kumar, "Post quantum secure conditional privacy preserving authentication for edge based vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, p. e4346, 2021.
- [16] K. Prateek, F. Altaf, R. Amin, and S. Maity, "A privacy preserving authentication protocol using quantum computing for v2i authentication in vehicular ad hoc networks," *Security and Communication Networks*, vol. 2022, 2022.
- [17] D. S. Gupta, S. Ray, T. Singh, and M. Kumari, "Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security," *Computer Communications*, vol. 181, pp. 69–79, 2022.
- [18] Q. Li, D. He, Z. Yang, Q. Xie, and K.-K. R. Choo, "Lattice-based conditional privacy-preserving authentication protocol for the vehicular ad hoc network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4336–4347, 2022.
- [19] D. S. Gupta and G. Biswas, "Design of lattice-based elgamal encryption and signature schemes using sis problem," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 6, p. e3255, 2018.
- [20] S. Mukherjee, D. S. Gupta, and G. Biswas, "An efficient and batch verifiable conditional privacy-preserving authentication scheme for vanets using lattice," *Computing*, vol. 101, no. 12, pp. 1763–1788, 2019.
- [21] D. Dharminder and D. Mishra, "Lcappa: Lattice-based conditional privacy preserving authentication in vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, p. e3810, 2020.

- [22] Z. Chen, K. Zhou, and Q. Liao, "Quantum identity authentication scheme of vehicular ad-hoc networks," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 40–57, 2019.
- [23] Y. Cao, S. Xu, X. Chen, Y. He, and S. Jiang, "A forward-secure and efficient authentication protocol through lattice-based group signature in vanets scenarios," *Computer Networks*, vol. 214, p. 109149, 2022.
- [24] D. S. Gupta, A. Karati, W. Saad, and D. B. da Costa, "Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 3, pp. 3255–3266, 2022.
- [25] *ISO/IEC/IEEE Information Technology-Ubiquitous Green Community Control Network Protocol, ISO/IEC/IEEE Standard 18880:2015*, pp. 1–78, 2015.
- [26] *ISO/IEC/IEEE International Standard-Information Technology-Ubiquitous Green Community Control Network-Security, ISO/IEC/IEEE Standard 18883 First Edition*, pp. 1–35, 2016.
- [27] J. Schmutzler, C. Wietfeld, and C. A. Andersen, "Distributed energy resource management for electric vehicles using iec 61850 and iso/iec 15118," in *2012 IEEE Vehicle Power and Propulsion Conference*. IEEE, 2012, pp. 1457–1462.
- [28] Á. Rodríguez-Serrano, A. Torralba, E. Rodríguez-Valencia, and J. Tarifa-Galisteo, "A communication system from ev to ev service provider based on ocpp over a wireless network," in *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2013, pp. 5434–5438.
- [29] C. Cheng, Y. Qin, R. Lu, T. Jiang, and T. Takagi, "Batten down the hatches: Securing neighborhood area networks of smart grid in the quantum era," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6386–6395, 2019.
- [30] A. G. Reddy, D. Suresh, K. Phaneendra, J. S. Shin, and V. Odelu, "Provably secure pseudo-identity based device authentication for smart cities environment," *Sustainable cities and society*, vol. 41, pp. 878–885, 2018.
- [31] Z. Yang, S. Yu, W. Lou, and C. Liu, " $\mathcal{P}\{2\}$: Privacy-preserving communication and precise reward architecture for v2g networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.
- [32] L. Xue, H. Huang, F. Xiao, and W. Wang, "A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2409–2420, 2022.
- [33] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9918–9933, 2022.
- [34] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things," *IEEE Internet of things Journal*, vol. 5, no. 4, pp. 2526–2536, 2017.
- [35] K. Prateek, S. Maity, and R. Amin, "An unconditionally secured privacy-preserving authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Network Science and Engineering*, 2022.
- [36] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1. Citeseer, 2001, pp. 1–2.
- [37] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2fa: efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, 2021.
- [38] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2014.
- [39] A. Menezes, "Another look at provable security," in *Advances in Cryptology—EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31*. Springer, 2012, pp. 8–8.
- [40] The Coq development team, *The Coq proof assistant reference manual*, 2004, Version 8.0. [Online]. Available: <http://coq.inria.fr>
- [41] V. M. R. (Ginni), "IBM QISKIT Github Project," <https://github.com/QISKit>, 2018, [Online; accessed 12-Jan-2022].
- [42] X. Qiu and L. Chen, "Quantum cost of dense coding and teleportation," *arXiv preprint arXiv:2202.12544*, 2022.



Kumar Prateek received the M.Tech. Degree from the Indian Institute of Information Technology Allahabad, Prayagraj, India, in 2019. He is currently working towards the Ph.D. Degree at the Department of Information Technology, Indian Institute of Information Technology Allahabad, Prayagraj, India. His research interests includes, Classical, Quantum and Post-Quantum Cryptography, Privacy and Security issues of Internet of Things, Smart Grids and Vehicular Ad Hoc Networks.



Soumyadev Maity received the M.Tech. Degree in Information Technology from the University of Calcutta, Kolkata, India, in 2007, and the Ph.D. Degree in Computer Science from the Department of Computer Science & Automation, Indian Institute of Science (IISc), Bangalore, India, in 2015. He is currently working as an Assistant Professor with the Department of Information Technology, Indian Institute of Information Technology, Allahabad, Prayagraj, India. He has many national and international publications in renowned journals and conferences.

His research interests includes Key management and Authentication protocols, Intrusion Detection systems, Internet of Things(IoT), Intelligent Transportation system (ITS), Privacy and Security.



Neetesh Saxena (SM'18) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Indore, India. He is currently an Associate Professor of cyber security with Cardiff University (CU), U.K. Before joining to CU, he was an Assistant Professor (Lecturer) with Bournemouth University, U.K. Prior to this, he was a Postdoctoral Researcher with the Georgia Institute of Technology, USA, and The State University of New York, South Korea (SUNY Korea), and a Visiting Scholar with Stony Brook University, USA. He

has published several articles in international peer-reviewed journals and conferences. He was a DAAD and TCS Research Fellow and is currently a member of the ACM.