Quantum-Resilient Authentication Protocol for Secure V2G Communications

Rohini Poolat Parameswarath
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
rohini.p@nus.edu.sg

Biplab Sikdar
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—Vehicle-to-Grid (V2G) networks enable bidirectional energy and information exchange between electric vehicles and smart grids, playing a critical role in future intelligent transportation and energy systems. However, the authentication mechanisms currently deployed in V2G communications rely heavily on classical cryptographic primitives that are vulnerable to quantum adversaries, posing a significant security risk. In this paper, we propose a quantum-resilient authentication protocol for V2G communications that ensures secure and efficient mutual authentication between electric vehicles and charging stations. The proposed scheme leverages Quantum Key Distribution (QKD). Formal security analysis demonstrates the robust security features of the protocol, and performance evaluation shows that it achieves lower computation cost compared to similar V2G authentication schemes.**

***Index Terms*—Quantum Key Distribution, quantum security, V2G communications.**

I. Introduction

Smart grid networks integrate advanced communication, sensing, and control technologies to enable intelligent monitoring, automation, and optimization of power generation, transmission, and distribution systems [1]. Unlike traditional power grids, where electricity flows only from centralized utilities to end users, smart grids support bidirectional exchange of both energy and information between power providers and consumers. This two-way interaction enables real-time visibility and control across the grid. By leveraging mechanisms such as demand response and adaptive load management, smart grids enhance energy efficiency while maintaining system stability and balancing supply and demand [2]. Further, smart grid architectures facilitate the seamless integration of distributed energy resources, including renewable generation such as solar and wind, energy storage systems, and Electric Vehicles (EVs). Thus, it supports sustainable and resilient power infrastructures [3], [4].

The adoption of EVs has grown significantly over the past few years, driven largely by environmental concerns. Conventional internal combustion engine vehicles rely on hydrocarbon fuels, leading to air pollution and increased greenhouse gas emissions. In contrast, EVs operate on electricity and produce negligible direct emissions [5]. Hence, governments worldwide promote EV adoption through regulatory support and financial incentives.

979-8-3315-8117-6/26/ $31.00 ©2026 IEEE

The rapid adoption of EVs has intensified the need to address security challenges within charging infrastructures [6]–[8]. In a V2G environment, EVs and charging stations communicate billing data and user-related information, all of which are attractive targets for cyberattacks. Authentication between EVs and charging stations is a fundamental requirement for secure V2G communications, as it establishes mutual trust before any exchange of energy or sensitive information takes place. Without proper authentication, malicious entities can impersonate legitimate EVs or charging stations to perform unauthorized charging, energy theft, false billing, or injection of fraudulent control messages that may disrupt grid stability. Therefore, robust authentication between EVs and charging stations is essential to maintain trust, reliability, and operational security in V2G communications.

Most existing authentication protocols for V2G communications rely on conventional public-key cryptographic techniques. Such techniques ensure security by leveraging the computational difficulty of solving well-known mathematical problems, particularly integer factorization and discrete logarithm, which are considered infeasible to solve efficiently. However, advances in quantum computers and the development of quantum algorithms pose a significant threat to these assumptions. For example, quantum algorithms such as Shor's algorithm [9] can solve these problems in polynomial time. Classical public-key–based authentication mechanisms will be inadequate to provide security with the emergence of quantum computer-enabled adversaries. Hence, quantum-secure authentication protocols are essential for V2G communications.

Quantum Key Distribution (QKD) techniques can be employed to build quantum-safe solutions. QKD enables two parties to securely generate a shared key using the principles of quantum mechanics. Any eavesdropping on a QKD channel disturbs the quantum states and will be reflected in the outcome of the system [10], [11]. This allows legitimate parties to derive keys that are secure even against quantum-capable adversaries. MDI-QKD is a QKD protocol whose

security does not make any assumptions about measurement devices [12]–[15]. MDI-QKD is immune to side-channel attacks targeting the quantum receiver [13]. Also, MDI-QKD is ideal for expanding the network, since it can provide a natural star topology [16]. We propose an authentication protocol to secure V2G communications leveraging MDI-QKD.

A. Related Work

This section reviews the existing literature on authentication schemes for V2G communications. The authors of [17] proposed an authentication protocol for V2G networks based on the Elliptic Curve Cryptosystem (ECC) and bilinear pairing. Another authentication protocol for V2G networks based on bilinear pairing was proposed in [18]. An authentication scheme for EV charging leveraging the concept of decentralized identifiers was proposed in [19]. This protocol enables users to create their own identities, thus ensuring an enhanced level of privacy. An authentication protocol based on ECC to secure V2G communications was presented in [20]. Subramani et al. proposed a batch authentication scheme for V2G communication in [21]. It is also based on bilinear pairing. An authentication protocol with user revocation feature was proposed in [22]. Though the above protocols addressed some of the security issues in V2G communications, none of them are quantum-safe.

A V2G authentication scheme based on PUFs was presented in [23]. Hou et al. proposed an authentication protocol based on PUFs in [24] that explored 5G network and the grid integration. Studies have shown that PUFs are prone to modeling attacks and their response can be affected by environmental factors.

B. Motivation and Contributions

It is important to secure V2G communications through authentication protocols. In addition, authentication protocols should be quantum-secure to provide resilience against future quantum computer-enabled attacks. To address the above challenges, we make the following key contributions:

- **A quantum resilient authentication protocol for V2G communications:** We propose a quantum-secure authentication protocol for V2G communications. The proposed protocol leverages QKD to establish a session key between the EV and the charging station.
- **Protection from classical and quantum adversaries:** The proposed protocol provides security against common conventional attacks and future quantum attacks.
- **Security analysis:** A formal security analysis under the Real-Or-Random (RoR) model [25] and an informal security analysis are provided.
- **Performance analysis:** We assess the efficiency and practicality of the proposed protocol through performance analysis.

II. System and Adversary Models

A. System Model

Figure 1 illustrates the system model. The EVs are denoted as $\{\mathcal{V}_1, \mathcal{V}_2, ...\mathcal{V}_n\}$ and the charging station as $\mathcal{CS}$. The Central Controller ($\mathcal{CC}$) registers the EVs and stores the registration information in its data centre. The EVs and the charging stations hold a quantum transmitter each. They prepare quantum states and send them to the $\mathcal{CC}$ for Bell-state measurement.

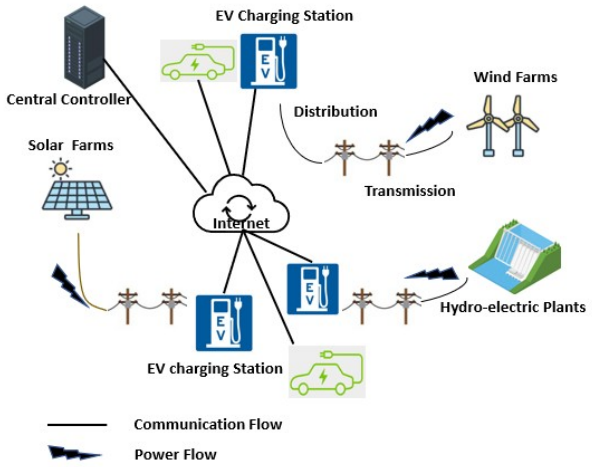

Fig. 1. System model.

B. Adversary Model

Since the EVs and the charging stations exchange messages over the insecure communication channel, an adversary can control this communication channel. He/she may eavesdrop on the messages, edit, or delete them. Also, the adversary may replay the messages after capturing or generate messages to impersonate a legitimate EV or charging station. Further, the adversary model considers an attacker with quantum computing capabilities, enabling the compromise of security mechanisms that rely on classical computational hardness assumptions.

III. Proposed Quantum-Resilient Authentication Protocol

The proposed authentication protocol consists of registration and mutual authentication phases. Each EV runs the registration phase only once. The mutual authentication phase is carried out whenever the EV and the charging station need to communicate.

A. Registration Phase

In this phase, an EV, $\mathcal{V}_i$, with an identity, ID, sends a registration request to the $\mathcal{CC}$. The $\mathcal{CC}$ registers $\mathcal{V}_i$.

B. Authentication Phase

In this phase, $\mathcal{V}_i$ and the $\mathcal{CS}$ generate a secure key through MDI-QKD and authenticate each other. The steps are given below:

Step 1: $\mathcal{V}_i$ and the $\mathcal{CS}$ prepare quantum states independently, based on their random choices of systems settings, including intensity selection, basis selection, and a random bit. $\mathcal{V}_i$ generates n states as $\{a*_{i1}, a*_{i2}, \ldots, a*_{in}\}$ and the $\mathcal{CS}$ also generates n states as $\{b*_{i1}, b*_{i2}, \ldots, b*_{in}\}$. After that, $\mathcal{V}_i$ and the $\mathcal{CS}$ send the prepared quantum states to the $\mathcal{CC}$ over the quantum channel.

Step 2: The $\mathcal{CC}$ performs Bell-state measurements on the received quantum states. Then, it announces the results of measurement via a public classical channel.

Step 3: If the $\mathcal{CC}$ announces a successful Bell-state measurement result, $\mathcal{V}_i$ and the $\mathcal{CS}$ broadcast their intensity and basis settings. The above process is continued till both have collected a sufficient number of successful measurement events. The $\mathcal{CS}$ flips its bits depending on the basis choice and the reported Bell-state. Both parties determine the error rate. The error rate should be below a predefined threshold. Then, information reconciliation is performed to check if both parties have a matching raw key. A random universal hash function is used to extract two shorter strings. Finally, these two strings are concatenated to form the final secret key.

Step 4: Let there be m retained bits from the measurements denoted as $\{a_{i1}, a_{i2}, \cdots, a_{im}\}$. Thus, a key $k_i = a_{i1}a_{i2}\ldots a_{im}$ is established through the QKD process between $\mathcal{V}_i$ and the $\mathcal{CS}$.

Step 5: $\mathcal{V}_i$ generates a random number r_i at time t_1. Then, $\mathcal{V}_i$ computes $r_i^* = r_i \oplus k_i$, $\gamma_1 = h(r_i \parallel k_i)$, and $\epsilon_1 = h(ID \parallel \gamma_1)$. Then,$\mathcal{V}_i$ composes a message M_1 with a request, its identity ID, r_i^*, t_1, and ϵ_1 as $M_1 = \{Req, ID, r_i^*, t_1, \epsilon_1\}$ and sends M_1 to the $\mathcal{CS}$.

Step 6: The $\mathcal{CS}$ receives M_1 at t_1^*. First, it verifies if $t_1 - t_1^*$ is less than or equal to a pre-defined communication delay. Then, it computes $r_i = r_i^* \oplus k_i$, $\gamma_1' = h(r_i \parallel k_i)$, and $\epsilon_1' = h(ID \parallel \gamma_1')$. After that, it verifies ϵ_1 against ϵ_1'. Then, the $\mathcal{CS}$ generates a random number n_i at time t_2 and computes $n_i^* = n_i \oplus k_i$. The $\mathcal{CS}$ generates the session key SK_i as $SK_i = h(ID \parallel r_i \parallel n_i)$ and stores it. After that, the $\mathcal{CS}$ computes $\gamma_2 = h(n_i \parallel k_i)$ and $\epsilon_2 = h(ID \parallel \gamma_2)$. Then, the $\mathcal{CS}$ composes $M_2 = \{Ack, n_i^*, t_2, \epsilon_2\}$ and sends it to $\mathcal{V}_i$.

Step 7: $\mathcal{V}_i$ receives M_2 at t_2^*. First, it verifies if $t_2 - t_2^*$ is less than or equal to a pre-defined communication delay. Then, it computes $n_i = n_i^* \oplus k_i$, $\gamma_2' = h(n_i \parallel k_i)$, and $\epsilon_2' = h(ID \parallel \gamma_2')$. Then, it verifies ϵ_2 against ϵ_2'. Finally, $\mathcal{V}_i$ generates the session key SK_i as $SK_i = h(ID \parallel r_i \parallel n_i)$ and stores it. The mutual authentication phase is illustrated in Figure 2.

V_i	**CS**
Generate k_i through QKD	
Generate: r_i $r_i^* = r_i \oplus k_i$ $\gamma_1 = h(r_i \parallel k_i)$ $\epsilon_1 = h(ID \parallel \gamma_1)$ $M_1 = \{Req, ID, r_i^*, t_1, \epsilon_1\}$ $\xrightarrow{M_1}$	
	Verify: $t_1 - t_1^* \leq \Delta t$ $r_i = r_i^* \oplus k_i$ $\gamma_1' = h(r_i \parallel k_i)$ $\epsilon_1' = h(ID \parallel \gamma_1')$ Verify: $\epsilon_1 ? = \epsilon_1'$ Generate: n_i $n_i^* = n_i \oplus k_i$ $SK_i = h(ID \parallel r_i \parallel n_i)$ $\gamma_2 = h(n_i \parallel k_i)$ $\epsilon_2 = h(ID \parallel \gamma_2)$ $M_2 = \{Ack, n_i^*, t_2, \epsilon_2\}$ $\xleftarrow{M_2}$
Verify: $t_2 - t_2^* \leq \Delta t$ $n_i = n_i^* \oplus k_i$ $\gamma_2' = h(n_i \parallel k_i)$ $\epsilon_2' = h(ID \parallel \gamma_2')$ Verify: $\epsilon_2 ? = \epsilon_2'$ $SK_i = h(ID \parallel r_i \parallel n_i)$	

Fig. 2. Authentication phase.

IV. Security Analysis

We first analyze the security of the proposed protocol using the RoR model [25], and then present an informal security analysis.

A. Formal Security Analysis

An adversary $\mathcal{A}$ tries to distinguish the session key in a protocol session between $\mathcal{V}_i$ and the $\mathcal{CS}$. We consider the oracle queries given below:

- *Execute($\mathcal{V}_i$, $\mathcal{CS}$):* With this query, $\mathcal{A}$ passively monitors the messages exchanged between $\mathcal{V}_i$ and the $\mathcal{CS}$.
- *Send(P, x):* With this query, $\mathcal{A}$ sends a message x to P where P is $\mathcal{V}_i$ or the $\mathcal{CS}$.
- *Reveal(P):* This query models the ephemeral secret leakage attack. It captures the ephemeral secrets of P where P is $\mathcal{V}_i$ or the $\mathcal{CS}$.
- *Corrupt(P):* This query captures the long-term secret credential of P where P is $\mathcal{V}_i$ or the $\mathcal{CS}$.
- *Test():* This query can be called only once. With the execution of this query, a bit b will be flipped. Depending on whether $b = 1$ or not, $\mathcal{A}$ receives the actual session key or a random string.

Definition 1: Let W denote the event when $\mathcal{A}$ correctly guesses b with the *Test()* query. $\mathcal{A}$'s advantage in compromising the security of the proposed protocol is measured by the probability of this successful guess. Hence, we can write that:

$$Adv_A = \mid 2.Pr[W] - 1 \mid .$$

The proposed protocol is secure if Adv_A is negligible.

Theorem 1. Let $\mathcal{A}$ send n_h, n_s, and n_e $Hash$, $Send$, and $Execute$ queries, respectively. The $Hash$ query denotes a

one-way hash function with a range space $|h|$. Let Adv_A^q denote $\mathcal{A}$'s advantage in finding the secure key established between $\mathcal{V}_i$ and the $\mathcal{CS}$ through QKD. Then, the advantage of $\mathcal{A}$ is $Adv_A \leq \frac{(n_h)^2}{2^{(h)}} + \frac{(n_s+n_e)^2}{l} + 2Adv_A^q$. Hence, Adv_A is negligible.

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

g_0: g_0 corresponds to a real attack by $\mathcal{A}$. Here $\mathcal{A}$ guesses b randomly. Hence, the advantage of $\mathcal{A}$ is:

$$Adv_A = \mid 2Pr[W_{A,g_0}] - 1 \mid . \tag{1}$$

g_1: In g_1, since all the queries $Execute$, $Send$, $Hash$, $Reveal$, and $Corrupt$ are simulated as in a real attack, games g_0 and g_1 are identical. Hence, it can be written that:

$$Pr[W_{A,g_1}] = Pr[W_{A,g_0}]. \tag{2}$$

g_2: Games g_2 and g_1 are similar. Until there are collisions in the hash or transcripts, $\mathcal{A}$ continues g_2. The collision probability of the hash function is at most $\frac{(n_h)^2}{2^{(h+1)}}$ as given by the birthday paradox and the collision probability in transcripts is $\frac{(n_s+n_e)^2}{2l}$ where l is the length of the transcripts. Hence, it can be written that:

$$Pr[W_{A,g_2}] - Pr[W_{A,g_1}] \leq \frac{(n_h)^2}{2^{(h+1)}} + \frac{(n_s+n_e)^2}{2l}. \tag{3}$$

g_3: This game considers the leakage of session key. Without knowing k_i, $\mathcal{A}$ cannot decode n_i from n_i^* and r_i from r_i^*. $\mathcal{A}$ needs to know n_i and r_i to compute the session key SK_i. By principles of quantum mechanics, $\mathcal{A}$ cannot get k_i. As a result, the difference between g_3 and g_2 is negligible. Hence, we can write that:

$$Pr[W_{A,g_3}] - Pr[W_{A,g_2}] \leq Adv_A^q. \tag{4}$$

As a final attempt, $\mathcal{A}$ guesses the bit b. It can be written that:

$$Pr[W_{A,g_4}] = \frac{1}{2}. \tag{5}$$

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

$$\begin{aligned} \frac{1}{2}Adv_A &= \mid Pr[W_{A,g_0}] - \frac{1}{2} \mid \\ &= \mid Pr[W_{A,g_1}] - \frac{1}{2} \mid . \end{aligned} \tag{6}$$

By applying the triangle inequality with equations (3) to (6), we can write:

$$\begin{aligned} \frac{1}{2}Adv_A &= \mid Pr[W_{A,g_1}] - \frac{1}{2} \mid \\ &= \mid Pr[W_{A,g_1}] - Pr[W_{A,g_4}] \mid \\ &\leq \frac{(n_h)^2}{2^{(h+1)}} + \frac{(n_s+n_e)^2}{2l} + Adv_A^q. \end{aligned} \tag{7}$$

Hence, we can write that:

$$Adv_A \leq \frac{(n_h)^2}{2^{(h)}} + \frac{(n_s+n_e)^2}{l} + 2Adv_A^q. \tag{8}$$

■

B. Informal Security Analysis

- **Resilience Against Quantum Attacks:** The proposed authentication protocol leverages MDI-QKD. The security offered by QKD arises from the principles of quantum mechanics and not from the hardness of solving the underlying mathematical problems, as in traditional public key cryptography. Hence, the proposed protocol is secure even against attacks by an adversary with quantum computing capabilities. Further, MDI-QKD is immune to side-channel attacks targeting the quantum receiver as well.
- **Eavesdropping Protection:** The random number r_1 used in M_1 is not sent in plain text. It is encoded before composing the message. Further, ϵ_1 is a hash value. Hence, an adversary cannot extract useful information even if he/she eavesdrops on M_1. Similarly, the adversary cannot extract useful information by listening to M_2. Thus, the proposed protocol is resilient to eavesdropping attacks.
- **Replay Attack Resistance:** Timestamps and fresh random numbers are used in composing the messages each time. Hence, if the adversary captures and replays messages, it will be detected by the receiver. Thus, there is replay attack protection.
- **Authentication:** $\mathcal{V}_i$ encodes r_i as r_i^* using k_i. Only the $\mathcal{CS}$ can decode r_i from r_i^*. Similarly, the $\mathcal{CS}$ verifies ϵ_1 since it knows the key, k_i. The $\mathcal{CS}$ encodes n_i as n_i^* using k_i. Only $\mathcal{V}_i$ can decode n_i from n_i^*. Similarly, $\mathcal{V}_i$ verifies ϵ_2 since it knows the key, k_i. As a result, both parties are authenticated under the proposed protocol.
- **Session Key Security:** $\mathcal{V}_i$ and the $\mathcal{CS}$ verify the legitimacy of each other and generate a session key SK_i. Thus, the proposed protocol ensures session key security.

V. Performance Analysis

In this section, first, we compare the security features of the proposed protocol with that of similar protocols. After that, we evaluate the computation cost of the proposed protocol.

A. Security Features

We compare the proposed authentication protocol with schemes proposed in recent works [21], [26], and [27]. The key feature of the proposed protocol is its resilience against attacks by quantum computer-enabled adversaries. In addition to that, the proposed protocol ensures authentication and session key security. It provides protection from common attacks such as eavesdropping and replay attacks. Although the protocols proposed in [21], [26], and [27] offer several security features, they do not provide quantum security. Hence, the proposed authentication protocol provides an enhanced set of security properties compared to other schemes.

TABLE I
COMPUTATION COST

Scheme	EV	CS/Server
Subramani et al. [21]	$2T_p + 2T_e + T_h \approx$2.832 ms	$T_p + 2T_e + T_h \approx$ 1.932 ms
Liang et al. [26]	$9T_h + 4T_{xor} + 2T_{puf} + 3T_{fe} \approx$ 1.443 ms	$20T_h + 8T_{xor} + 2T_{puf} + 2T_{fe} \approx$ 1.346 ms
Yu and Park [27]	$9T_h \approx$ 0.108 ms	$15T_h + 4T_s \approx$ 0.34 ms
Proposed Protocol	$5T_h \approx$ 0.06 ms	$5T_h \approx$ 0.06 ms

B. Computation Cost

To estimate the execution time during authentication, we conducted the simulations on a personal computer with Intel (R) Core i7-10750H CPU and 8 GB RAM capacity. We employed the MIRACL [28] library to evaluate the execution time of various cryptographic operations. During authentication, the EV executes five hash operations. Similarly, the CS also executes five hash operations. Let T_h represent the execution time of the hash operation. The execution time of XOR and concatenation operations is negligible. From the analysis, T_h = 0.012 ms. The time taken to execute the authentication phase is 0.06 ms at the EV and at the CS each.

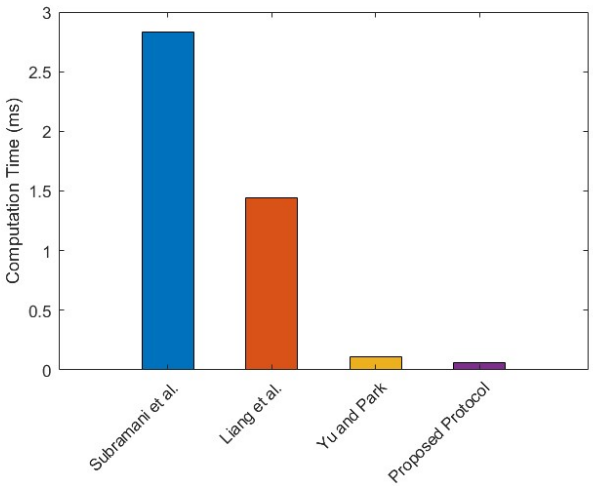

Fig. 3. Computation cost at the EV.

Next, we provide a comparative analysis of the computation cost of the proposed protocol with the schemes in [21], [26], and [27]. The time taken by symmetric key encryption/decryption T_s is 0.04 ms, pairing operation T_p is 0.9 ms, and exponential operation T_e is 0.51 ms. The time for PUF computation is T_{puf} = 0.324 ms and fuzzy extraction is T_{fe} = 0.229 ms [26]. The computation time taken by the schemes in [21], [26], and [27] are given in Table I and plotted in Figure 3 and Figure 4, respectively. From the analysis, the proposed protocol has the lowest computation cost compared to other schemes.

VI. CONCLUSION

This paper presented a secure authentication protocol for V2G communications leveraging QKD to address emerging security threats in smart grids. By leveraging the information-theoretic security of QKD, the proposed protocol enables robust mutual authentication and secure key establishment between EVs and charging stations, ensuring resistance against classical and quantum-enabled attacks. Compared to conventional schemes, the proposed QKD-based authentication framework provides future-proof security without relying on computational hardness assumptions, making it a promising solution for securing V2G communications.

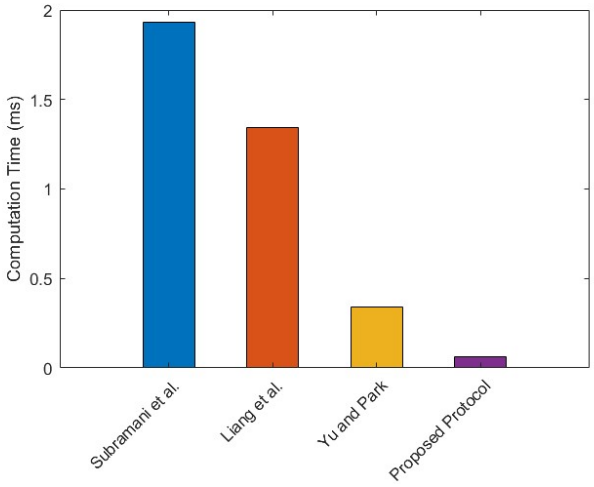

Fig. 4. Computation cost at the CS/Server.

VII. ACKNOWLEDGEMENT

This work is fully supported by the Advanced Research and Technology Innovation Centre (ARTIC), the National University of Singapore under Grant (project number: AFP-RP2).

REFERENCES

[1] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11 883–11 915, 2015.

[2] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Başar, "Demand response management in the smart grid in a large population regime," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 189–199, 2015.

[3] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814–2825, 2018.

[4] N. Javaid, G. Hafeez, S. Iqbal, N. Alrajeh, M. S. Alabed, and M. Guizani, "Energy efficient integration of renewable energy sources in the smart grid for demand side management," *IEEE Access*, vol. 6, pp. 77 077–77 096, 2018.

[5] H. Li, D. Han, and M. Tang, "A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing," *IEEE Systems Journal*, 2020.

[6] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp)," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1504–1533, 2022.

[7] R. P. Parameswarath, N. V. Abhishek, and B. Sikdar, "Prevent: A mechanism for preventing message tampering attacks in electric vehicle networks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–5.

[8] S. Shirvani, Y. Baseri, and A. Ghorbani, "Evaluation framework for electric vehicle security risk assessment," *IEEE transactions on intelligent transportation systems*, vol. 25, no. 1, pp. 33–56, 2023.

[9] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[10] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[12] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130502, 2012.

[13] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[14] C. Wang, W. Y. Kon, H. J. Ng, and C. C.-W. Lim, "Experimental symmetric private information retrieval with measurement-device-independent quantum network," *Light: Science & Applications*, vol. 11, no. 1, p. 268, 2022.

[15] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature communications*, vol. 5, no. 1, p. 3732, 2014.

[16] R. P. Parameswarath, C. Wang, and B. Sikdar, "A quantum safe mutual authentication protocol for smart meter communications with experimental evaluation," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 5, pp. 5058–5072, 2024.

[17] Y. Zhang, J. Zou, and R. Guo, "Efficient privacy-preserving authentication for v2g networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1366–1378, 2021.

[18] L. F. Roman, P. R. Gondim, and J. Lloret, "Pairing-based authentication protocol for v2g networks in smart grid," *Ad Hoc Networks*, vol. 90, p. 101745, 2019.

[19] R. P. Parameswarath, P. Gope, and B. Sikdar, "User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential," *ACM Transactions on Management Information Systems (TMIS)*, 2022.

[20] Z. Sun and Y. Wang, "An anonymous authentication protocol for vehicle to grid based on elliptic curve cryptography," *Frontiers in Physics*, vol. 13, p. 1589195, 2025.

[21] J. Subramani, A. Maria, A. Sekar Rajasekaran, and B. Prasad Chapa, "Mutual and batch authentication with conditional privacy-preserving scheme for v2g communication system," *IEEE Access*, vol. 12, pp. 69 593–69 602, 2024.

[22] R. P. Parameswarath, P. Gope, and B. Sikdar, "A privacy-preserving authenticated key exchange protocol for v2g communications using ssi," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 11, pp. 14 771–14 786, 2023.

[23] M. Kaveh, D. Martín, and M. R. Mosavi, "A lightweight authentication scheme for v2g communications: A puf-based approach ensuring cyber/physical security and identity/location privacy," *Electronics*, vol. 9, no. 9, p. 1479, 2020.

[24] W. Hou, Y. Sun, D. Li, Z. Guan, and J. Liu, "Lightweight and privacy-preserving charging reservation authentication protocol for 5g-v2g," *IEEE Transactions on Vehicular Technology*, 2023.

[25] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*. Springer, 2005, pp. 65–84.

[26] Y. Liang, H. Sun, X. Zhang, Q. Xie, G. Liu, Z. Liu, Z. Tan, and Y. Liu, "Lightweight multifactor authentication and key agreement scheme in vehicle-to-grid networks," *IEEE Transactions on Vehicular Technology*, pp. 1–18, 2025.

[27] S. Yu and K. Park, "Puf-based robust and anonymous authentication and key establishment scheme for v2g networks," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 450–15 464, 2024.

[28] "MIRACL Cryptographic SDK," Online,https://github.com/miracl/MIRACL, [Accessed: Jan 2024].