This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

Privacy-Preserving Bidirectional Data Transmission of Smart Grid via Semi-Quantum Computation: On Mutual Identity and Message Authentication

Xiaoping Lou, *Member, IEEE*, Huiru Zan, *Member, IEEE*, Zidong Wang, *Fellow, IEEE*, Jinjing Shi, *Member, IEEE*, and Shichao Zhang, *Senior Member, IEEE*

***Abstract*—This paper is concerned with the privacy-preserving bidirectional electric power data transmission problem of the smart grid. A privacy-preserving bidirectional data transmission (BDT) protocol is developed over semi-quantum computation with aim to achieve bidirectional sensitive data flow between power suppliers and users. The minimal quantum cost is pursued under practical constraints while ensuring that power sensitive information is not leaked. To achieve the goal, a two-way data transmission protocol is first proposed that combines mutual identity authentication with message authentication for the benefits of enhanced security. Furthermore, for the preservation of privacy, a semi-quantum duplex communication approach is utilized, wherein the quantum state is randomly divided into two parts: teleportation and measurement qubits. The effectiveness of the privacy-preserving scheme against existing attack strategies is also rigorously analyzed. Lastly, simulation studies conducted on the IBM quantum cloud platform validate and underscore the superiority of the developed privacy-preserving BDT protocol.**

***Index Terms*—Privacy-preserving bidirectional data transmission, smart Grid, mutual authentication, semi-quantum teleportation, IBM quantum cloud platform.**

I. Introduction

With the increasing intelligence demands of the power grid and emerging environmental concerns, research into smart grids has been intensively pursued in recent years due to their convenience, efficiency, security, and stability [8], [16], [32], [43]. As one of the most fundamental challenges in smart grids, the bidirectional data transmission (BDT) has been identified as an active research area, where the primary objectives are real-time power data collection and electricity supply adjustment [24], [29], [30], [46], [48]. In the context of fair business competition and reliable operation of power grids, power sensitive information is considered essential [6], [28], [36], [37], [42]. Owing to the growing normalization and intelligence of the smart grid, significant challenges in privacy preservation and reliability are being faced.

Recently, several algorithms have been developed to address the privacy-preserving BDT problem in the smart grid, which can be broadly categorized into noise-based [13], [15], [18], [40], trusted-proxy-based [22], [25], [45], and cryptography-based methods [3], [5], [9], [10], [21], [23], [26], [27]. When compared to the first two techniques, cryptographic techniques are believed to provide stronger security. For instance, an identity authentication and key agreement scheme has been proposed in [26] for communication between a smart meter and a server in the smart grid, and it has been emphasized that the design of a mutual identity authentication scheme and a key management protocol is the primary step in addressing the privacy's security concerns. Furthermore, in [3], an identity authentication protocol has been introduced based on elliptic curve cryptography, which enables the establishment of a secret session key between smart grid devices and utility companies after mutual identity authentication. Unfortunately, vulnerabilities to man-in-the-middle (MITM) and device impersonation attacks have been identified in the proposed scheme.

In the realm of the smart grid, the achievement of two-way transmission of power-sensitive information remains a pivotal challenge. It is imperative to ascertain the legitimacy of both sides involved in the transmission, which emphasizes the need for mutual identity authentication. To date, several privacy-preserving schemes (e.g. mutual identity authentication schemes) have been introduced in the literature, see e.g. [9], [21]. However, mutual identity authentication and transmission protocols that lack post-processing (specifically, message authentication) can easily be compromised by adversaries with complete quantum capability. To address this limitation, a privacy-preserving message authentication scheme has been proposed in [11] by using the Hash-based Message Authentication Code (HMAC). However, the results related to identity and message authentication in the smart grid have been really scattered, and this drives our motivation to bridge this gap. In the smart grid, terminal smart meters are constrained by limited computation and memory capabilities. Consequently, classical identity authentication and transmission schemes with information-theoretical security are deemed infeasible as they can be compromised by the robust capabilities of advanced algorithms such as quantum computation [20], [35]. Fortunately, due to the characteristics of quantum mechanics, quantum

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) of the UK, the European Union's Horizon 2020 Research and Innovation Programme under Grant 820776 (INTEGRADDE), the Alexander von Humboldt Foundation of Germany, and the Royal Society of the UK.

Xiaoping Lou and Huiru Zan are with the College of Information Science and Engineering, Hunan Normal University, Changsha 410081, China. E-mail: louxiaoping@hunnu.edu.cn, zanhuiru@163.com.

Zidong Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. E-mail: Zidong.Wang@brunel.ac.uk.

Jinjing Shi and Shichao Zhang are with the School of Computer Science and Engineering, Central South Univerisity, Changsha 410083,China. E-mails: shijinjing@csu.edu.cn, zhangsc@mailbox.gxnu.edu.cn.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

information processing has been shown to be superior in many aspects as compared to its classical counterpart [1], and such a superiority is rooted in the intrinsic correlation of remote agents with quantum superposition and quantum entanglement. Quantum computing can address complex problems that are challenging for classical computation, such as factorization and discrete logarithm problems. The solution of these problems poses a threat to existing classical encryption and privacy protection systems [3], [5], [9], [10], [21], [23], [26], [27]. , such as RSA and elliptic curve cryptography. In contrast, quantum privacy protection can mitigate the vulnerabilities of traditional encryption technologies in the face of quantum computing threats. The employment of quantum information has been demonstrated to ensure information-theoretical security in tasks like quantum key distributions [4] and quantum teleportation [14].

A. Related Work

BDT in smart grids can be implemented using various technologies, which vary depending on specific application scenarios, geographical conditions, data transmission requirements, and other factors. Generally, these technologies can be categorized into wired and wireless communication technologies. Wired communication technologies are typically employed for long-distance and high-bandwidth backbone connections, such as fiber optic communication [55]. For low-cost local communication, such as the connection from substations to household consumers, existing power lines communication (PLC) are often used for data transmission [58]. Wireless communication technologies use dedicated or shared spectrum for wireless data transmission with radio frequency (RF) [59] and are suitable for applications such as meter reading and remote device control. The communication of wide-area mobile and fixed devices generally utilizes existing cellular network infrastructure (such as 5G) for data transmission [57]. High-bandwidth data transmission within households or local site areas typically employs Wi-Fi. With the advancement of the Internet of Things (IoT) [56], many smart grid devices and sensors have started using IoT communication protocols (such as LoRa and NB-IoT) to achieve low-power wide-area network (LPWAN) communication. These technologies collectively form the communication network of the smart grid, supporting real-time data transmission, remote monitoring and control, device management, and other functionalities, ensuring the intelligent and efficient operation of the grid. Additionally, classical cryptographic techniques are employed to ensure the confidentiality, integrity, and availability of data while protecting user privacy [3], [5], [9]–[11], [21], [23], [26], [27].

Diverging from classical cryptography methods, quantum-based techniques introduce quantum computation to mask sensitive information, exemplified by differential quantum identity authentication schemes [2], [12], [41], [44]. We are currently in the era of quantum computing. This era is characterized by the availability of operational quantum computing devices, though these devices have a limited number of qubits and are affected by noise and errors. While NISQ (Noisy Intermediate-Scale Quantum) [60] devices cannot perform fault-tolerant quantum computing, they are powerful enough to explore the potential of quantum computing and may be more effective than classical computers for certain specific tasks. It should be pointed out that the applicability of most quantum-based algorithms for smart grid is limited by the high cost of quantum devices [51], [52], [54]. To address the constraints of the previously mentioned privacy-preserving scheme, a semi-quantum-based privacy-preserving approach has been introduced in [17], where quantum states are partitioned randomly into two segments, namely, the measuring substate and the reflecting substate, where the former is used to exchange information with adjacent nodes, and the latter is employed to sense/detect if there appears any abnormal behavior resulting from other nodes, thereby achieving the purpose of privacy protection. Such a privacy-preserving technique has showcased various advantages which encompass enhanced security, reduced computational complexity, and superior privacy performance, and its versatility has been expanded to areas such as private key management for multiple proxies [34], direct communication between two entities [38], and private comparison [39]. One-way authentication [50] and two-way authentication protocols [53] for smart grid based on semi-quantum key distribution have also been proposed in smart grid. Although the aforementioned scheme assists in verifying the identity of smart meter users by generating symmetric keys based on semi-quantum principles, the BDT algorithm and data post-processing (message authentication) still rely on classical cryptography, making them vulnerable to powerful quantum computing attacks.

Pertaining to the previous discussions, it is important to highlight that BDT challenges addressed through semi-quantum have not been thoroughly explored in the context of smart grid, and this may be attributed to challenges stemming from the asymmetry in quantum communication capabilities between the two parties, which often results in unidirectional communication. The situation becomes even more complicated when taking into account the intricacies associated with preserving the privacy of the BDT problem. Clearly, a primary obstacle in formulating a semi-quantum protocol lies in striking a balance between the privacy level and efficiency since there is a tendency to sacrifice quantum ability utilization in favor of practicality. This identified gap has inspired the focus of our current study.

Given the preceding discussions, this paper concentrates on the privacy-preserving BDT challenge in the smart grid. Two primary complexities have emerged as follows from our analysis.

1) How can a bidirectional data transmission protocol be developed that operates over asymmetric quantum capability, thereby offering both heightened security and minimal quantum resource demands?
2) How can semi-quantum duplex communication methods be seamlessly integrated into a bidirectional protocol in order to ensure both efficiency and robust privacy preservation?

To tackle the above outlined challenges, our efforts are chan-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

neled towards the design of mutual identity and message authentication via semi-quantum computation with the overarching aim of achieving a privacy-preserving BDT.

B. Contribution

The core contributions of this research are encapsulated as follows.

1) A pioneering two-way data transmission protocol is introduced to address the BDT challenge within the semi-quantum framework, which integrates mutual identity [2], [12] and message authentication [11]. Comparing to the majority of privacy-preserving BDT protocols reliant on cryptography-based algorithms, our designed semi-quantum-based transmission protocol achieves superior security using minimal quantum resources.
2) For the first time, a duplex communication mechanism is incorporated within the BDT challenge under a semi-quantum model and, furthermore, a comprehensive security analysis is furnished, which underscores the resilience of our newly developed privacy-preserving protocol against a myriad of threats: man-in-the-middle, relay, impersonation, and de-synchronization attacks.
3) Standing in contrast to both cryptographic-based [3], [5], [9]–[11], [21], [23], [26], [27] and full-quantum privacy-preserving models [2], [12], [41], [44], our methodology showcases marked benefits in terms of heightened efficiency, reduced quantum demands, and robust privacy preservation.

The remaining sections of this paper are outlined as follows. Section II formulates the privacy-preserving BDT issue of smart grid. Section III presents the two-way data transmission protocol and instance. Section IV presents the security and efficiency analysis of the proposed protocol. Simulation results are presented in Section V to validate the obtained theoretical results. Finally, Section VI concludes this paper.

II. Problem Formulation and Preliminaries

A. The BDT problem

In this section, the BDT challenge within smart grids is articulated as a protocol whose ultimate aim is to ensure a bidirectional flow of power data while optimizing quantum resource consumption, all within realistic physical constraints.

We introduce a typical architecture for the Semi-Quantum Smart Grid (SQSG) to facilitate secure communication. As illustrated in Fig. 1, this architecture encompasses two primary entities: the Smart Meter (SM) and the Service Provider (SP).

1) Complete quantum party: The SP, which possesses full quantum capacity, interacts with the SMs to gather power equipment data and responds to the requests of the SMs. Furthermore, the SP communicates with the energy supply system, which enables intelligent regulation of energy supply within the smart grid.

- **ZBP**: Preparation on Z-basis $(\{|0\rangle, |1\rangle\})$
- **XBP**: Preparation on X-basis $(\{|0\rangle, |1\rangle\})$

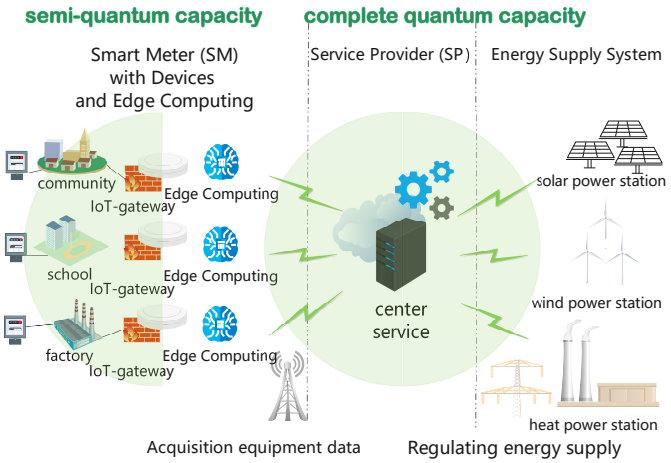

Fig. 1: A general architecture of semi-quantum smart grid.

- **BSP**: Preparation of Bell states on $\{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$
- **ZBM**: Measurement on Z-basis
- **XBM**: Measurement on X-basis.
- **BSM**: Measurement of Bell states on $\{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$

2) Semi-quantum party: The SMs, equipped with semi-quantum capacity, process users' electricity consumption data using edge computing technology and subsequently upload this data to the SP.

- **ZBM**: Measurement on Z-basis $(\{|0\rangle, |1\rangle\})$
- **REF**: Undisturbed reflection of particles

The quantum and classical bits, $|\omega\rangle^{i}_{\mathrm{SP}}$ and ω^{i}_{SM}, are the data sequences that the SP and the SM attempt to transmit, as depicted below:

$$\begin{aligned} \Omega_{\mathrm{SP}} &= \left\{ |\omega\rangle^{\mathrm{i}}{}_{\mathrm{SP}} \in \{|0\rangle, |1\rangle\}, \mathrm{i} = 1, 2, \ldots, \mathrm{n} \right\} \\ \Omega_{\mathrm{SM}} &= \left\{ \omega^{\mathrm{i}}{}_{\mathrm{SM}} \in \{0, 1\}, \mathrm{i} = 1, 2, \ldots, \mathrm{n} \right\} \end{aligned} \tag{1}$$

From the aforementioned observations, the exchange of sensitive information, as expressed in (1), can be redefined, where the objective is to devise a two-way data transmission protocol encompassing both identity (ex ante) and message (ex post) verifications, wherein the local SMs possess only the capacities of **ZBM** and **REF**.

It is crucial to emphasize that there exists a contradiction between the practicality and functionality of contemporary quantum approaches, and this disparity presents a challenge in deriving teleportation using semi-quantum computation.

B. The Adversaries Model

Before delving into the primary objective of this paper, we define four types of adversaries:

1) *MITM (Man-In-The-Middle)*: These are intermediaries attempting to intercept sensitive data flow between the SP and SM, with intentions to forge secret messages.
2) *Relay*: These eavesdroppers pose as legitimate agents, trying to capture a portion of the data flow and then replay it back to the service.
3) *Impersonation*: These are malicious entities attempting to authenticate themselves with the service or local user,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

with the end goal of gaining permission for further communication.

4) *De-synchronization*: These external attackers disrupt the synchronization between communicating agents, leading to lost, conflicting, or delayed messages.
5) *Quantum computation*: The computational power of these external attackers is based on quantum computation, which are efficient in dealing with certain computational problems, especially in breaking classical cryptography-based algorithms.

The primary objective of this paper is to design a bidirectional data transmission protocol, which incorporates both identity and message authentication in a semi-quantum environment, thereby ensuring the protection of power-sensitive information from the four types of adversaries previously described. While an agent endowed with full quantum capabilities can readily achieve this task, an agent with only semi-quantum capabilities is limited to quantum measurement operations. Consequently, establishing mutual identity and message authentication in a semi-quantum context is challenging due to the asymmetrical access to quantum information.

III. TWO-WAY DATA TRANSMISSION PROTOCOL AND INSTANCE

In this section, we investigate the privacy-preserving BDT issue initially by crafting a two-way data transmission protocol within a semi-quantum framework. This protocol synergizes identity authentication [2], [12] with message authentication [11]. Furthermore, a privacy-preservation scheme is introduced utilizing semi-quantum duplex communication, and examples of the implemented privacy-preserving scheme are furnished.

A. privacy-preserving two-way data transmission protocol

Before delving deeper, it's essential to note that the SM and SP share a $2n$ classical bits secret key sequence, K_{ab}, established via the quantum key distribution protocol [20]. This sequence is bifurcated into two subkeys: K_a and K_b. The representation of these classical secret key sequences can be found as follows:

$$\begin{aligned} K_{ab} &= \{k_a^i k_b^i, i = 1, 2, \ldots, n\} \\ K_a &= \left\{k_a^1, k_a^2, ...k_a^n\right\} \\ K_b &= \left\{k_b^1, k_b^2, ...k_b^n\right\} \end{aligned} \tag{2}$$

To address the privacy-preserving BDT challenge within the semi-quantum model, a novel bidirectional data transmission scheme is devised as follows by integrating mutual identity authentication with message authentication.

Step 1: Preparation of the Quantum State

(a) SP prepares n pairs of Bell states $|\Phi^{\pm}\rangle_{12}$ (as in (3)) based on K_b for identity authentication:

$$\begin{cases} |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \\ |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \\ |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\ |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \end{cases} \tag{3}$$

After that, SP prepares n pairs of Bell states $|\Psi^+\rangle_{34}$ and n pairs of Bell states $|\Psi^-\rangle_{56}$ for classical message transmission. The subscript $1, 3, 5$ and $2, 4, 6$ represent the first qubit and the second qubit of each entangled state pair, respectively. SP divides these Bell states into six sequences as follows:

$$\begin{aligned} S_1 &= \left\{s_1^i, i = 1, 2, \ldots, n\right\} \\ S_2 &= \left\{s_2^i, i = 1, 2, \ldots, n\right\} \\ S_3 &= \left\{s_3^i, i = 1, 2, \ldots, n\right\} \\ S_4 &= \left\{s_4^i, i = 1, 2, \ldots, n\right\} \\ S_5 &= \left\{s_5^i, i = 1, 2, \ldots, n\right\} \\ S_6 &= \left\{s_6^i, i = 1, 2, \ldots, n\right\}. \end{aligned} \tag{4}$$

The above mentioned quantum states can be denoted in (5) as follows:

$$\begin{cases} k_b = 0 \rightarrow S_1 S_2 \in |\Phi^+\rangle_{12}, \\ k_b = 1 \rightarrow S_1 S_2 \in |\Phi^-\rangle_{12}. \\ \qquad\quad S_3 S_4 \in |\Psi^+\rangle_{34}, \\ \qquad\quad S_5 S_6 \in |\Psi^-\rangle_{56}. \end{cases} \tag{5}$$

(b) SP randomly prepares n single qubits $|\omega\rangle_{\mathrm{SP}}^i$ and records these states. Similarly, SM randomly prepares n classical bits ω_{SM}^i. These quantum and classical bit $|\omega\rangle_{\mathrm{SP}}^i$ and ω_{SM}^i form, respectively, the data sequence of SP and the data sequence of SM that are to be transmitted as shown in (1).
(c) SP prepares $\frac{n}{2}$ decoy states d_j according to secret key K_a as follows:

$$\begin{cases} k_a = 0 \rightarrow Z - basis : \mathrm{d}_j \in \{|0\rangle, |1\rangle\}, \\ k_a = 1 \rightarrow X - basis : \mathrm{d}_j \in \{|+\rangle, |-\rangle\} \end{cases} \tag{6}$$

The correct measurement basis can yield accurate results for decoy states measurements. Conversely, an incorrect measurement basis has only a 50% chance of yielding accurate results for decoy state measurements. Fig.2 shows the possible measurement results with **ZBM** and **XBM**. The quantum states $|0\rangle$ and the quantum states $|1\rangle$ are recorded as the classical bits 0 and 1, and the quantum state $|+\rangle$ and the quantum states $|-\rangle$ are recorded as the classical bits 0 and 1, respectively.

Step 2: Distribution and Eavesdropping Detection

(a) SP inserts decoy particles d_j (prepared as (6)) into sequence S_4, and forms the sequence S_4'. SP keeps sequences S_1, S_3 and S_5, sends sequences S_2, S_4' and S_6 to SM. SM informs SP after receiving all the particles. Then, SP announces the location of decoy states d_j through the public classical channel.
(b) As shown in Table I, SM performs either **ZBM** or **REF** operation on decoy states d_j and S_2 according to K_{ab}. SP publishes outcomes of **ZBP** of decoy states d_j to SM. SP performs **XBM** $(|+\rangle, |-\rangle)$ operation on decoy states d_j according to K_a.
(c) Then, SP compares the measurement results of **XBM** on **REF** part of decoy particles with decoy particles as (6). SM compares the measurement results of **ZBM** with those announced by SP. If the error rate exceeds

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

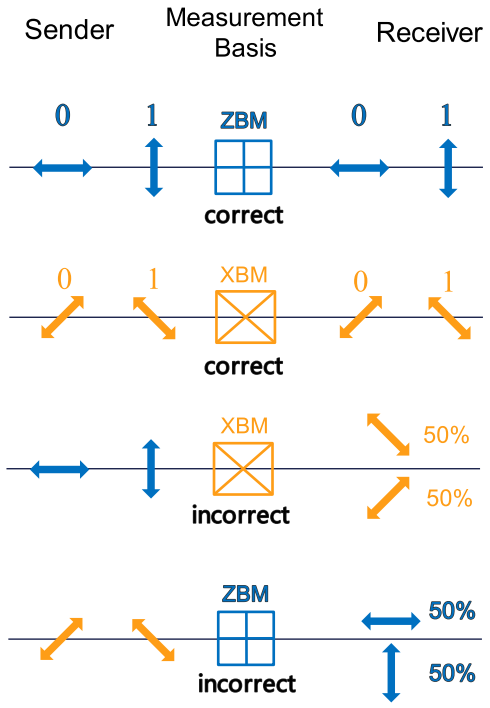

Fig. 2: Measurement results with **ZBM** and **XBM**.

a predetermined threshold, the protocol is terminated or restarted. Otherwise, it proceeds to the next step.

TABLE I: SM's operation on sequences d_j and S_2

K_{ab}	Operation on d_j for eavesdropping	Operation on S_2 for authentication
00	**ZBM**	**REF**
01	**ZBM**	**ZBM**
10	**REF**	**ZBM**
11	**REF**	**REF**

Step 3: Mutual Identity Authentication

(a) For identity authentication of SM by SP, the **REF** part of the sequence S_2 and corresponding part of S_1 work as identity authentication states. SP performs **BSM** on **REF** part of S_2 and S_1 ($K_{ab} \in \{00, 11\}$ in Table I). If the results of the measurement are consistent with the Bell state that SP has prepared as (5), the identity verification of SM passes. Otherwise, the protocol is terminated.

(b) For authentication of SP by SM, the **ZBM** part of the sequence S_2 and the remainder part of S_1 work as identity authentication states. SP performs the **ZBM** on S_1 and publishes these measurement results ($K_{ab} \in \{01, 10\}$ in Table I). If these measurement results are different from the **ZBM** outcomes of S_2 in *Step 2(b)*, the identity verification of SP passes. Otherwise, the protocol is terminated.

Step 4: Semi-quantum duplex communication To ensure the prevention of power sensitive data leakage, a privacy-preserving algorithm is proposed using a semi-quantum duplex communication approach. Lists (a-c) involve full quantum party to semi-quantum party communication, while lists (d-e) involve semi-quantum party to full quantum party communication.

(a) SM discards decoy particles and obtains the sequence S_4, which is entangled with S_3 held by SP as (3). In other words, SM and SP maintain a remote entangled relationship according to $\{S_3, S_4\}$ and $\{S_5, S_6\}$.

(b) The semi-quantum teleportation could be performed as in (7)-(8). Specifically, the system is composed of single qubits $|\omega\rangle^i_{\text{SP}}$ and Bell state sequence $\{S_3, S_4\}$. SP performs **BSM** on $\{s^i_3, |\omega\rangle^i_{\text{SP}}\}$, which leads to particles s^i_4 collapsed. SP announces the measurement results through the public classical channel.

$$\begin{aligned}
&\left|\Psi^+\right\rangle_{34} \otimes |\omega\rangle^i_{\text{SP}} \\
&= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)_{34} \otimes |0\rangle_c \\
&= \frac{1}{\sqrt{2}} (|000\rangle + |110\rangle)_{34c} \\
&= \frac{1}{\sqrt{2}} (|000\rangle + |101\rangle)_{3c4} \\
&= \frac{1}{2} (|\Psi^+\rangle |0\rangle + |\Psi^-\rangle |0\rangle + |\Phi^+\rangle |1\rangle - |\Phi^-\rangle |1\rangle)_{3c4}
\end{aligned} \tag{7}$$

$$\begin{aligned}
&\left|\Psi^+\right\rangle_{34} \otimes |\omega\rangle^i_{\text{SP}} \\
&= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)_{34} \otimes |1\rangle_c \\
&= \frac{1}{\sqrt{2}} (|001\rangle + |111\rangle)_{34c} \\
&= \frac{1}{\sqrt{2}} (|010\rangle + |111\rangle)_{3c4} \\
&= \frac{1}{2} (|\Psi^+\rangle |1\rangle - |\Psi^-\rangle |1\rangle + |\Phi^+\rangle |0\rangle + |\Phi^-\rangle |0\rangle)_{3c4}
\end{aligned} \tag{8}$$

TABLE II: Recovery of $|\omega\rangle^i_{\text{SP}}$ by semi-quantum teleportation

Bell state in Eq.(3)	**BSM** of $\{S_3, c\}$	**ZBM** of S_4	Value of $|\omega\rangle^i_{\text{SP}}$
$\left\|\Psi^+\right\rangle_{ab}$	$\|00\rangle$	$\|0\rangle$	$\|0\rangle$
		$\|1\rangle$	$\|1\rangle$
$\left\|\Psi^-\right\rangle_{ab}$	$\|10\rangle$	$\|0\rangle$	$\|0\rangle$
		$\|1\rangle$	$\|1\rangle$
$\left\|\Phi^+\right\rangle_{ab}$	$\|01\rangle$	$\|0\rangle$	$\|1\rangle$
		$\|1\rangle$	$\|0\rangle$
$\left\|\Phi^-\right\rangle_{ab}$	$\|11\rangle$	$\|0\rangle$	$\|1\rangle$
		$\|1\rangle$	$\|0\rangle$

(c) SM takes **ZBM** operation on s^i_4. According to Table II, semi-quantum capacity user SM deduces the value of $|\omega\rangle^i_{\text{SP}}$. By this way, SM obtains the data of Ω_{SP} as (1).

(d) SM and SP perform the **ZBM** on $\{S_5, S_6\}$ respectively. SM compares private data ω^i_{SM} and **ZBM** result of s^i_6. If they are the same, SM asks SP to take the **ZBM** results as ω^i_{SM} directly. If they are different, SM asks SP to take a flip on the **ZBM** results of ω^i_{SM}. Here, classical message $\{0, 1\}$ are corresponding to quantum state $\{|0\rangle, |1\rangle\}$.By this way, SM obtains the data of Ω_{SM} as (1).

Step 5: Mutual Message Authentication

(a) SP and SM generate message authentication codes (MAC) m^i_a and m^i_b based on private key K_{ab}, and record them as sequences $\{MAC_{\text{SP}}, MAC_{\text{SM}}\}$, i.e.,

$$\begin{aligned}
MAC_{\text{SP}} &= \{m^i_a, i = 1, 2, \ldots, n\} \\
MAC_{\text{SM}} &= \{m^i_b, i = 1, 2, \ldots, n\}
\end{aligned} \tag{9}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

The specific sequences MAC_{SP} andMAC_{SM} are shown as (10). SP and SM publish the values of m_a^i and m_b^i through the public classical channel.

$$\begin{cases} k_a^i=0, |\omega\rangle_{\mathrm{SP}}^i &= |0\rangle \rightarrow m_a^i=0 \\ k_a^i=0, |\omega\rangle_{\mathrm{SP}}^i &= |1\rangle \rightarrow m_a^i=1 \\ k_a^i=1, |\omega\rangle_{\mathrm{SP}}^i &= |0\rangle \rightarrow m_a^i=1 \\ k_a^i=1, |\omega\rangle_{\mathrm{SP}}^i &= |1\rangle \rightarrow m_a^i=0 \\ k_b^i=0,\ \omega_{\mathrm{SM}}^i &= 0 \rightarrow m_b^i=0 \\ k_b^i=0,\ \omega_{\mathrm{SM}}^i &= 1 \rightarrow m_b^i=1 \\ k_b^i=1,\ \omega_{\mathrm{SM}}^i &= 0 \rightarrow m_b^i=1 \\ k_b^i=1,\ \omega_{\mathrm{SM}}^i &= 1 \rightarrow m_b^i=0 \end{cases} \tag{10}$$

(b) According to Table III, SM and SP take mutual message verification based on private K_{ab}, $|\omega\rangle_{\mathrm{SP}}^i$ and ω_{SM}^i.

The process of the proposed two-way data transmission scheme is detailed in Algorithm 1.

Algorithm 1 Two-way data transmission scheme

Output: $|\omega\rangle_{\mathrm{SP}}^i$ and ω_{SM}^i Data Transmission
Initialiazation: K_{ab}=$\{Key\ \ Generation\}$,
execute the Step 1 - Step 3,
if there exist eavesdroppers **then**
  abort.
else
  Identity authentication pass,
  execute the Step 4 - Step 5,
  if there exist eavesdroppers **then**
    abort.
  else
    Message authentication pass.

B. Protocol instance

In this section, a instance example of the protocol is provided to prove the correctness and feasibility. Suppose that SP and SM share an eight-bit pre-key $K_{ab}=\{00110010\}$, i.e., $K_a=\{0101\}$ and $K_b=\{0100\}$. Table IV shows the details of this example.

IV. Security Analysis and Efficiency comparison

In this section, we analyze the security and efficiency of the protocol. The results of the security comparison with that of existing identity authentication protocols are shown in Table V.

A. Security Analysis

1) Man-in-the-middle (MITM) attack: In the SQSG, the man-in-the-middle (MITM) attack strategy intercepts communication messages between the SP and SM, modifies or forges secret message without being observed. Specifically, malicious attacker Eve intercepts these sequences S_2, S_4' and S_6 that are sent from SP to SM in *Step 2(a)*. Then, Eve prepares auxiliary qubits $|\varepsilon\rangle$ and entangles them with particles that are intercepted with unitary operation U_E (as shown in (11)), i.e.

$$\begin{aligned} U_E|0\rangle|\varepsilon\rangle =&\alpha|0\rangle|\varepsilon_{00}\rangle+\beta|1\rangle|\varepsilon_{01}\rangle \\ U_E|1\rangle|\varepsilon\rangle =&\gamma|0\rangle|\varepsilon_{10}\rangle+\delta|1\rangle|\varepsilon_{11}\rangle \\ U_E|+\rangle|\varepsilon\rangle =&\frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle+\beta|\varepsilon_{01}\rangle+\gamma|\varepsilon_{10}\rangle+\delta|\varepsilon_{11}\rangle) \\ &+|-\rangle(\alpha|\varepsilon_{00}\rangle-\beta|\varepsilon_{01}\rangle+\gamma|\varepsilon_{10}\rangle-\delta|\varepsilon_{11}\rangle)] \\ U_E|-\rangle|\varepsilon\rangle =&\frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle+\beta|\varepsilon_{01}\rangle-\gamma|\varepsilon_{10}\rangle-\delta|\varepsilon_{11}\rangle) \\ &+|-\rangle(\alpha|\varepsilon_{00}\rangle-\beta|\varepsilon_{01}\rangle-\gamma|\varepsilon_{10}\rangle+\delta|\varepsilon_{11}\rangle)] \end{aligned} \tag{11}$$

where $|\alpha^2|+|\beta^2|=|\gamma^2|+|\delta^2|=1$. After the transmission, Eve measures auxiliary qubits $|\varepsilon\rangle$ with attempt to obtain SM's operation and key K_{ab}. Eve will evade eavesdropping detection only if the condition of (12) is met when the decoy state are $\{|0\rangle,|1\rangle\}$:

$$\beta|\varepsilon_{01}\rangle=\gamma|\varepsilon_{10}\rangle=0 \tag{12}$$

Similarly, Eve will evade eavesdropping detection only if the condition of (13) is met when the decoy states are $\{|+\rangle,|-\rangle\}$.

$$\begin{aligned} \alpha|\varepsilon_{00}\rangle-\beta|\varepsilon_{01}\rangle+\gamma|\varepsilon_{10}\rangle-\delta|\varepsilon_{11}\rangle=0 \\ \alpha|\varepsilon_{00}\rangle+\beta|\varepsilon_{01}\rangle-\gamma|\varepsilon_{10}\rangle-\delta|\varepsilon_{11}\rangle=0 \end{aligned} \tag{13}$$

It follows from (12) and (13) that $\alpha|\varepsilon_{00}\rangle=\delta|\varepsilon_{11}\rangle$ should be satisfied, which indicates that Eve cannot distinguish between $\{|0\rangle,|1\rangle\}$. So, it is concluded that Eve cannot obtain any useful information with the help of auxiliary qubit. Therefore, MITM attack is ineffective.

2) Replay attack: In *Step 2(a)*, Eve intercepts sequences S_4' that SP sends to SM, and selects an operation of **ZBM** or **XBM** randomly. After that, Eve prepares a copy of sequence E_e ($E_e\in|0\rangle,|1\rangle,|+\rangle,|-\rangle$) based on measurement results and sends E_e to SM. In *Step 2(b)*, Eve attempts to eavesdrop part of private key K_{ab} based on **REF** particles from SM.

The **REF** particles include all of decoy states in S_4' and parts of S_2. To avoid being captured in the eavesdropping check, Eve tries to choose the correct measurement operation. However, the probability of false operation on each qubit performed by Eve is 0.5 without K_a, which leads to false result of probability $0.5^{\frac{n}{2}}$. As a result, replay attack launched by Eve will inevitably introduce error, and the eavesdropping check will not pass.

3) Impersonation attack: Case 1: As an SP's impersonator, Eve attempts to be authenticated by SM. In *Step 2(a)*, Eve can only prepare decoy qubits $d_j\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ at random without secret key K_a. SM chooses an operation of **REF** and **ZBM** based on K_a. The probability that decoy state $\{|+\rangle,|-\rangle\}$ is operated by SM on **ZBM** is 0.5, which leads error in eavesdropping check. Even though the eavesdrop checking passes, the identity authentication will never pass since the false results of **ZBM** on part of S_1 published by the impersonator Eve are inevitable without private key K_b in *Step 3(a)*.

Case 2: As an SM's impersonator, Eve attempts to be authenticated by SP. In *Step 2(b)*, Eve can only perform an operation of **ZBM** or **REF** randomly without secret key K_a. The probability of choosing the false operation by Eve is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

TABLE III: Mutual message authentication results

Case	m_a^i	k_a^i	$\|\omega\rangle_{\mathrm{SP}}^i$	Message from SP authenticated by SM	Case	m_b^i	k_b^i	ω_{SM}^i	Message from SM authenticated by SP
case1	0	0	$\|0\rangle$	pass	case1	0	0	0	pass
case2		1	$\|1\rangle$	pass	case2		1	1	pass
case3		0	$\|1\rangle$	fail	case3		0	1	fail
case4		1	$\|0\rangle$	fail	case4		1	0	fail
case5	1	0	$\|0\rangle$	fail	case5	1	0	0	fail
case6		1	$\|1\rangle$	fail	case6		1	1	fail
case7		0	$\|1\rangle$	pass	case7		0	1	pass
case8		1	$\|0\rangle$	pass	case8		1	0	pass

TABLE IV: An example of the protocol

Step	SP	SM	Result
Step 1	$K_a = \{0101\}$,$K_b = \{0100\}$ $S_1S_2 = \{\|\Phi^+\rangle_{12}, \|\Phi^-\rangle_{12}, \|\Phi^+\rangle_{12}, \|\Phi^+\rangle_{12}\}$ $S_3S_4 = \{\|\Psi^+\rangle_{34}, \|\Psi^+\rangle_{34}, \|\Psi^+\rangle_{34}, \|\Psi^+\rangle_{34}\}$ $S_5S_6 = \{\|\Psi^-\rangle_{56}, \|\Psi^-\rangle_{56}, \|\Psi^-\rangle_{56}, \|\Psi^-\rangle_{56}\}$ $d_1 = \|0\rangle$,$d_2 = \|+\rangle$ $\Omega_{\mathrm{SP}} = \{\|1\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$	$K_a = \{0101\}$,$K_b = \{0100\}$ $\Omega_{\mathrm{SM}} = \{0, 1, 1, 0\}$	
Step 2	$S_1 = \{s_1^1, s_1^2, s_1^3, s_1^4\}$ $S_3 = \{s_3^1, s_3^2, s_3^3, s_3^4\}$ $S_5 = \{s_5^1, s_5^2, s_5^3, s_5^4\}$ **XBM** on $\{d_2\}$ check eavesdroppers	$S_2 = \{s_2^1, s_2^2, s_2^3, s_2^4\}$ $S_4' = \{s_4^1, s_4^2, \|0\rangle, s_4^3, s_4^4, \|+\rangle\}$ $S_5 = \{s_5^1, s_5^2, s_5^3, s_5^4\}$ **REF** on d_2, **ZBM** on d_1 **REF** on $\{s_2^1, s_2^2, s_2^3\}$, **ZBM** on $\{\underline{s_2^4}, s_1^4\}$ check eavesdroppers	$d_1 = \|0\rangle$,$d_2 = \|+\rangle$ $s_2^4 = \|1\rangle$ No eavesdroppers
Step 3	**BSM** on $\{s_1^1, s_2^1\}$, $\{s_1^2, s_2^2\}$, $\{s_1^3, s_2^3\}$ **ZBM** on $\{\underline{s_1^4}, s_2^4\}$		$\|\Phi^+\rangle_{12}$,$\|\Phi^-\rangle_{12}$,$\|\Phi^+\rangle_{12}$ $s_1^4 = \|0\rangle$ Identity authentication pass
Step 4	**BSM** on $\{s_3^1, \|1\rangle\}$, $\{s_3^2, \|0\rangle\}$, $\{s_3^3, \|0\rangle\}$, $\{s_3^4, \|1\rangle\}$ **ZBM** on $\{s_5^1, s_5^2, s_5^3, s_5^4\}$ prepare $\Omega_{SM} = \{0, 1, 1, 0\}$	$S_4 = \{s_4^1, s_4^2, s_4^3, s_4^4\}$ **ZBM** on $\{s_4^1, s_4^2, s_4^3, s_4^4\}$ **ZBM** on $\{s_6^1, s_6^2, s_6^3, s_6^4\}$ get $\Omega_{SP} = \{\|1\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$ according to Table II	$\|\Psi^-\rangle$, $\|\Psi^+\rangle$, $\|\Psi^-\rangle$, $\|\Phi^-\rangle$ $S_4 = \{\|1\rangle, \|0\rangle, \|0\rangle, \|0\rangle\}$ $S_5 = \{\|0\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$ $S_6 = \{\|0\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$
Step 5	$\mathrm{MAC}_{\mathrm{SP}} = \{1100\}$ according to Table III	$\mathrm{MAC}_{\mathrm{SM}} = \{0010\}$ according to Table III	Message authentication pass

TABLE V: Security comparison with classical quantum, semi-quantum identity authentication protocols for smart grid

reference	scheme	Quantum computation attack	MITM attack	Replay attack	Impersonation attack	Des attack
Ref [27]	classical	No	No	Yes	No	Yes
Ref [23]	classical	No	Yes	Yes	No	Yes
Ref [21]	classical	No	No	Yes	No	Yes
Ref [9]	classical	No	No	Yes	Yes	Yes
Ref [5]	classical	No	Yes	Yes	No	No
Ref [52]	quantum	Yes	Yes	Yes	No	No
Ref [51]	quantum	Yes	Yes	Yes	Yes	No
Ref [50]	semi-quantum	Yes	Yes	Yes	Yes	No
Ref [53]	semi-quantum	Yes	Yes	No	No	No
Ref [54]	quantum	Yes	Yes	Yes	No	No
Proposed protocol	semi-quantum	Yes	Yes	Yes	Yes	Yes

0.5. The **REF** decoy state operated on **XBM** by SP will inevitably introduce error, which leads error in eavesdropping check. Even though the eavesdrop checking passes, the identity authentication will never pass since the false results of **BSM** on **REF** part of $\{S_1, S_2\}$ are inevitable without private key K_b in *Step 3(b)*.

4) De-synchronization (Des) attack: In a de-synchronization (Des) attack, the synchronization between communication devices in the smart grid is attempted to be disrupted by an external attacker. This disruption causes the message in *Step 4* to be delivered at unexpected time intervals, subsequently affecting the communication's quality and reliability due to message losses, conflicts, or delays [31].

Interestingly, in the scheme, the message's semi-quantum duplex communication is facilitated by semi-quantum teleportation (from SP to SM) and the **ZBM** of Bell states (from SM to SP). Thanks to the unique quality of quantum entanglement over remote distances, no information is directly transferred between the two agents. Instead, the result of the measurement is announced in a public channel, effectively sidestepping the aforementioned issue. Moreover, in *Step 5*, the authenticity and integrity of the message are ensured through verification by MAC_{SP} and MAC_{SM}.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

TABLE VI: Comparison of semi-quantum and quantum identity authentication protocols

Protocol	Quantum resources	Hash function	Verification method	Experiment	Efficiency
Ref [47]	Single photons	No	One-way	No	≈50%
Ref [33]	W states and GHZ-like states	Yes	Two-way	No	≈66.7%
Ref [19]	Bell states	No	Two-way	No	≈88.9%
Ref [50]	Single photons	Yes	one-way	Yes	≈50%
Ref [51]	Single photons	Yes	Two-way	Yes	≈50%
Ref [52]	Single photons	Yes	Two-way	No	≈50%
Ref [53]	Single photons	Yes	Two-way	Yes	≈50%
Ref [54]	Single photons	No	one-way	No	≈50%
Proposed protocol	Bell states and single photons	No	Two-way	Yes	≈94.1%

B. Efficiency Comparison

In the presented scheme, the quantum resources consist of sequences of qubits, which can be categorized into signal qubits (SQ) and eavesdropping check qubits (CQ). Within the structure of the SQSG, classical-bits, specifically $\mathrm{MAC_{SP}}$ and $\mathrm{MAC_{SM}}$, are also conveyed via the public channel. The efficiency calculation pertinent to the quantum communication scheme was proposed by Cabello [7]:

$$\eta = \frac{b_s}{q_t + b_t} \times 100\% \tag{14}$$

where b_s represents the number of both signal classical-bit and qubits, and $\{b_t, q_t\}$ represents the total number of classical-bits and qubits (including both SQ and CQ) utilized in the protocol.

In the described scenario, the exchanged classical-bit count between SP and SM stands at $2n$, which is consistent with the length of $(\mathrm{MAC_{SP}}, \mathrm{MAC_{SM}})$. In terms of quantum resources, the number of SQ required for identity and message authentication equals $6n$, corresponding to the lengths of the sequences $\{S_1, S_2, S_3, S_4, S_5, S_6\}$. Furthermore, decoy particles serving as CQ is $\frac{n}{2}$. So, we have $b_s = 2n + 6n$, $b_t = 2n$ and $q_t = 6n + \frac{n}{2}$. The efficiency of proposed scheme is $\eta = \frac{2n+6n}{6n+\frac{n}{2}+2n} \times 100\% \approx 94.1\%$. Table VI contrasts the efficiency of the proposed scheme with that of other semi-quantum and quantum identity authentication protocols [19], [33], [47], [51], [52].

In the simulation environment, the experimental setup is as follows: Windows 11 operating system, Intel(R) Core(TM) i5 CPU, 8GB RAM, VS Code development environment, Python 3.12.3, Qiskit 1.1.1. The time taken for computation cost is as follows: identity authentication algorithm - 2.4 seconds, BDT algorithm - 2.1 seconds, message authentication algorithm - 1.1 seconds.

V. Simulation Study

In this section, the validity of the formulated protocol is appraised through a simulation example executed on the IBM Quantum Cloud Platform. The respective parameters associated with each agent can be found in Table IV. The simulation employs both the idealized environment, labeled **ibmq qasm** simulator, and the more realistic, noise-prone quantum environment designated as **ibmq quito**. To ensure precise experimental outcomes, the quantum circuit's number of runs (which equates to the emitted photon count, termed 'shots') has been fixed at 8192.

*1) **The simulation results under ideal environment**:* Fig. 3 illustrates the results of identity authentication. Four pairs of Bell state

$$\begin{aligned}[q_0, q_1] = |\Phi^+\rangle_{12}, [q_2, q_3] = |\Phi^-\rangle_{12},\\ [q_4, q_5] = |\Phi^+\rangle_{12}, [q_6, q_7] = |\Phi^+\rangle_{12}.\end{aligned} \tag{15}$$

are prepared as shown on the left side of the first and second barriers. SP distributes $S_2 = \{q_1, q_3, q_5, q_7\}$ and holds $S_1 = \{q_0, q_2, q_4, q_6\}$. Fig. 4 depicts the data transmission from SM to SP, four pairs of Bell state

$$\begin{aligned}[q_0] = |1\rangle, \quad [q_1, q_2] = |\Psi^+\rangle_{34},\\ [q_3] = |0\rangle, \quad [q_4, q_5] = |\Psi^-\rangle_{34},\\ [q_6] = |0\rangle, \quad [q_7, q_8] = |\Psi^+\rangle_{34},\\ [q_9] = |1\rangle, \quad [q_{10}, q_{11}] = |\Psi^+\rangle_{34}.\end{aligned} \tag{16}$$

are prepared as shown on the left of first barrier. SP distributes $S_4 = \{q_2, q_5, q_8, q_{11}\}$ and holds $S_3 = \{q_1, q_4, q_7, q_{10}\}$. Fig. 5 depicts data transmission from SM to SP, four pairs of Bell state

$$\begin{aligned}[q_0, q_1] = |\Psi^-\rangle_{56}, [q_2, q_3] = |\Psi^-\rangle_{56},\\ [q_4, q_5] = |\Psi^-\rangle_{56}, [q_6, q_7] = |\Psi^-\rangle_{56}.\end{aligned} \tag{17}$$

are prepared as shown on the left of first barrier. SP distributes $S_6 = \{q_1, q_3, q_5, q_7\}$ and holds $S_5 = \{q_0, q_2, q_4, q_6\}$. The gray disk represents $|0\rangle$ and the blue disk represents $|1\rangle$.

It should be observed that the outcomes align perfectly with the initial states presented in Eqs. (15), (16), and (17). This simulation substantiates both the precision and the benefits of the privacy-preserving bidirectional data transmission within a semi-quantum framework.

*2) **The simulation results under real noisy environment**:* Fig. 6 shows the results of eavesdropping detection performed by **ZBM** and **XBM** on $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Fig. 7 shows the mutual identity authentication performed by **BSM** and **ZBM** on Bell states. Fig. 8 shows the mutual message authentication performed by semi-quantum teleportation on Bell states.

In the results, it is evident that the correct measurement basis can yield accurate results with a probability exceeding 90%, while an incorrect measurement basis can produce erroneous results with a likelihood of over 45%. Moreover, in a noisy environment, the two agents can authenticate each other's identity using **BSM** and **ZBM** with a probability surpassing 90%, which could be considered as the threshold for the identity authentication in Step 3. This simulation underscores the heightened security of the proposed protocol.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

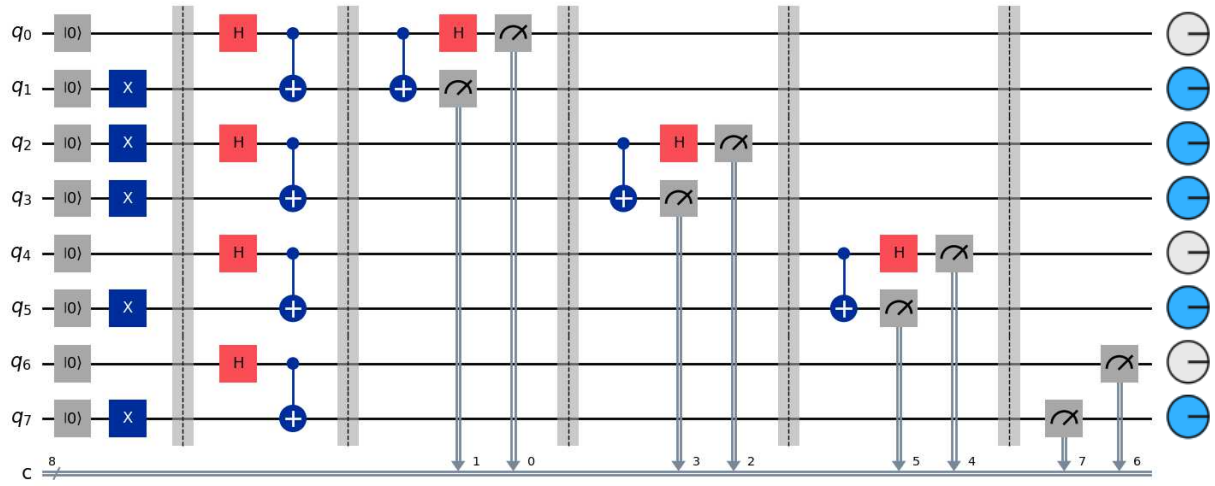

Fig. 3: Construction of quantum circuit identity authentication on IBM Quantum Cloud experimental platform.

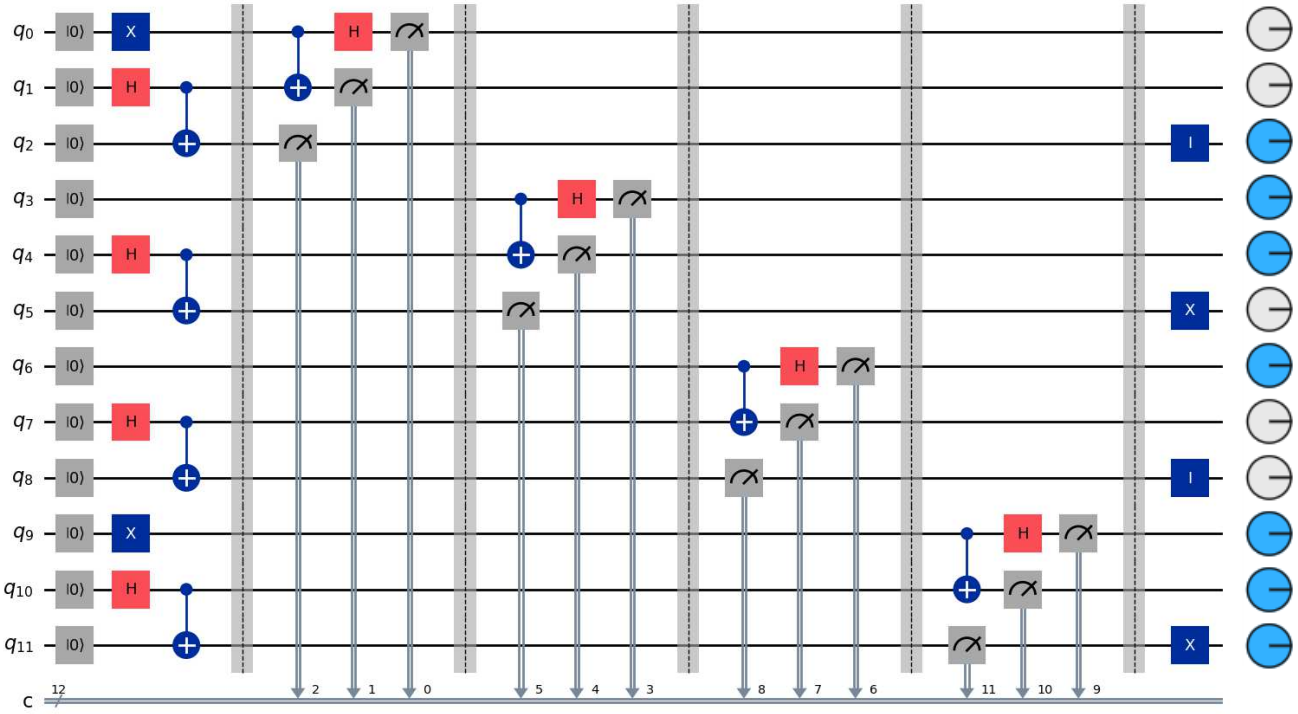

Fig. 4: Construction of quantum circuit message $|\omega\rangle_{\mathrm{SP}}^{i}$ deliver on IBM Quantum Cloud experimental platform.

Remark 1: So far, we have investigated the problem of privacy-preserving bidirectional electric power data transmission for the smart grid. Comparing to the existing results in the literature, our developed protocol exhibits the following distinguishing feature: 1) a novel two-way data transmission is empowered by using the semi-quantum paradigm to address the BDT problem, which seamlessly melds mutual identity with message authentication; 2) our semi-quantum-centric protocol accomplishes superior security with a conservative quantum resource footprint; 3) a meticulous security evaluation is presented which highlights the robust defense mechanisms of our avant-garde privacy-preserving protocol against a spectrum of threats (including man-in-the-middle, relay, impersonation, and de-synchronization attacks), and 4) our approach unveils pronounced advantages, encompassing enhanced efficiency, curtailed quantum requisites, and steadfast privacy protection.

VI. Conclusion

In this paper, we have addressed the privacy-preserving BDT problem of smart grid over semi-quantum. By combining the mutual identity authentication with the mutual message authentication, it has been demonstrated that the proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.
Citation information: DOI 10.1109/TDSC.2025.3568707, IEEE Transactions on Dependable and Secure Computing

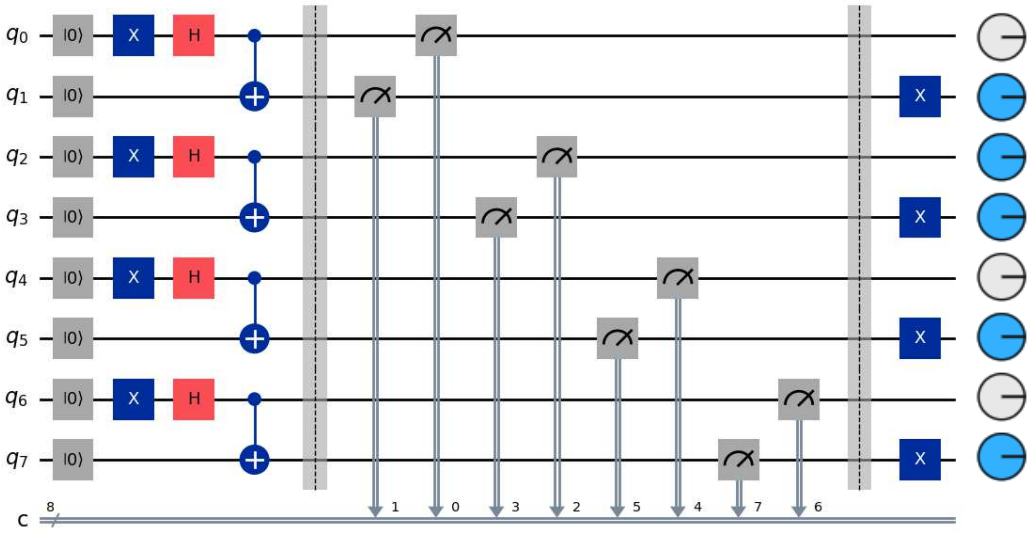

Fig. 5: Construction of quantum circuit message ω^i_{SM} deliver on IBM Quantum Cloud experimental platform.

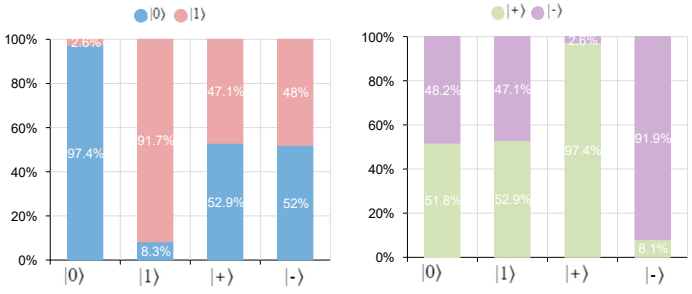

Fig. 6: The results of eavesdropping detection by **ZBM** and **XBM** on $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ in IBM noisy environment

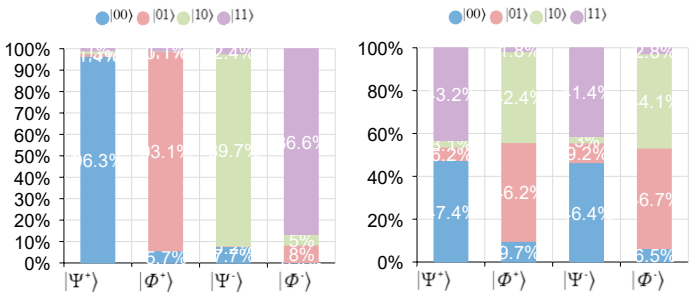

Fig. 7: The results of mutual identity authentication by **BSM** and **ZBM** on Bell states in IBM noisy environment

two-way data transmission protocol achieves enhanced security over semi-quantum with low quantum capacity. To prevent the leakage of power sensitive information, a privacy-preserving scheme has been integrated into the bidirectional data transmission protocol using the semi-quantum duplex communication, which exhibits the privacy property against attacks and high efficiency. Finally, simulation experiments have been carried out to validate the effectiveness of the developed protocol.

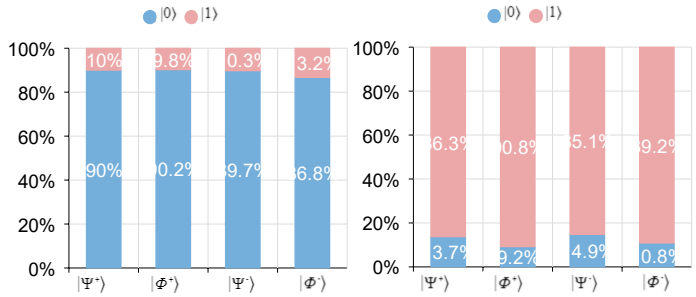

Fig. 8: The results of message $|0\rangle$ and $|1\rangle$ transmission by semi-quantum teleportation with Bell states in IBM noisy environment

The source code, including algorithm and examples, experimental setup, data for reproducing figures and explore further settings can be found in the GitHub repository [49].

REFERENCES

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, art. no. 230501, Jun. 2007.
[2] M. Alshowkan and K. Elleithy, "Quantum mutual authentication scheme based on bell state measurement," *in Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, State Univ New York, Farmingdale State Coll, Apr. 2016. pp. 1-6.
[3] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood and N. Kumar, "An identity based authentication protocol for smart grid environment using physical uncloneable function," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4426-4434, Sept. 2021.
[4] C. H. Bennett, "Quantum cryptography: Public key distribution and coin tossing." *in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, Dec. 1984, pp. 175-179.
[5] B. Bera, S. Saha, A. K. Das and A. Vasilakos, "Designing blockchain based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744-5761, Apr. 2021.
[6] R. Caballero-Águila, A. Hermoso-Carazo, and J. Linares-Pérez, "Networked fusion estimation with multiple uncertainties and time-correlated channel noise," *Information Fusion*, vol. 54, pp. 161–171, 2020.

[7] A. Cabello, "Quantum key distribution in the Holevo limit," *Physical Review Letters*, vol. 85, no. 26, pp. 5635-5638, Dec. 2000.
[8] J. Cao, Z. Bu, Y. Wang, H. Yang, J. Jiang and H. Li, "Detecting prosumer-community group in smart grids from the multiagent perspective," *IEEE Transactions on Systems Man Cybernetics: Systems*, vol. 49, no. 8, pp. 1652-1664, 2019.
[9] S. A. Chaudhry, H. Alhakami, A. Baz and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235-101243, Jul. 2022.
[10] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir and Y. B. Zikria, "Gcacs-iod: a certificate based generic access control scheme for internet of drones," *Computer Networks*, vol. 191, art. no. 107999, May 2021.
[11] T. W. Chim, S. M. Yiu, L. C. Hui and V. O. Li, "Pass: privacy-preserving authentication scheme for smart grid network," *in Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, BELGIUM, Oct. 2011.
[12] C. Crépeau and L. Salvail, "Quantum oblivious mutual identification," *Eurocrypt'95*, Berlin, Heidelberg: Springer-Verla, pp. 133-146, 1995.
[13] C. Dou, D. Yue and J. M. Guerrero, "Multiagent system-based event-triggered hybrid controls for high-security hybrid energy generation systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 584-594, 2017.
[14] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706-709, Oct. 1998.
[15] C. Gao, Z. Wang, X. He and D. Yue, "Sampled-data-based fault-tolerant consensus control for multi-agent systems: A data privacy preserving scheme," *Automatica*, vol. 133, art. no. 109847, 2021.
[16] V. C. Gungo, D. Sahi, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on industrial informatics*, vol. 9, no. 1, pp. 28-42, Feb. 2013.
[17] H. Iqbal and W. O. Krawec, "Semi-quantum cryptography," *Quantum Information Processing*, vol. 19, no. 3, pp. 1-52, Feb. 2020.
[18] S. K. Jain and N. Kesswani, "A noise-based privacy preserving model for internet of things," *Complex and Intelligent Systems*, vol. 9, no. 4, pp. 3655-3679, Aug. 2021.
[19] S. Q. Jiang, R. G. Zhou and W. W. Hu, "Semi-quantum mutual identity authentication using bell states," *International Journal of Theoretical Physics*, vol. 60, no. 9, pp. 3353-3362, Sept. 2021.
[20] M. Kaur and S. Kalra, "Security in iot-based smart grid through quantum key distribution," *in Proceedings of Computer and Computational Sciences*, Springer, Singapore, 2018, pp. 523-530.
[21] N. Kumar, G. S. Aujla, A. K. Das and M. Conti, "Eccauth: a secure authentication protocol for demand response management in a smart grid system," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6572-6582, Dec. 2019.
[22] W. Li and F. Yang, "Information fusion over network dynamics with unknown correlations: An overview," *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, art. no. 100003, Jun. 2023.
[23] X. Li, F. Wu, S, Kumari, L. Xu, A. K. Sangaiah and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 242-249, Oct. 2019.
[24] J. Liu, Y. Gu, L. Zha, Y. Liu and J. Cao, "Event-triggered H_∞ load frequency control for multi-area power systems under hybrid cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1665-1678, 2019.
[25] H. Mohammed, S. Tonyali, K. Rabieh, M. Mahmoud and K. Akkaya, "Efficient privacy-preserving data collection scheme for smart grid ami networks," *in Proceedings of IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, Dec. 2016, pp. 1-6.
[26] H. Nicanfar, P. Jokar, K. Beznosov and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640, Jun. 2014.
[27] V. Odelu, A. K. Das, M. Wazid and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900-1910, May 2018.
[28] Z. H. Pang, L. Z. Fan, H. Guo, Y. Shi, R. Chai, J. Sun and G. Liu, "Security of networked control systems subject to deception attacks: a survey," *International Journal of Systems Science*, vol. 53, no. 16, pp. 3577-3598, 2022.
[29] B. Qu, Z. Wang, B. Shen and H. Dong, "Outlier-resistant recursive state estimation for renewable-electricity-generation-based microgrids," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 7133-7144, May 2023.
[30] B. Qu, Z. Wang, B. Shen, H. Dong and H. Liu, "Event-based joint state and unknown input estimation for energy networks: Handling multi-machine power grids," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 1, pp. 253-264, Jan.-Feb. 2023.
[31] M. Shuai, L. Xiong, C. Wang and N. Yu, "Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs," *IET Information Security*, vol. 14, no. 4, pp. 380-390, Jul. 2020.
[32] V. Sood, D. Fischer, J. Eklund and T. Brown, "Developing a communication infrastructure for the smart grid," *in Proceedings of IEEE Electrical Power and Energy Conference (EPEC)*, Montreal, QC, Canada, Oct. 2009, pp. 1-7.
[33] M. Tanveer and H. Alasmary, "LACP-SG: lightweight authentication protocol for smart grids," *Sensors*, vol. 23, no. 4, Feb. 2023.
[34] Y. Tian, J. Li, X. Chen, C.-Q. Ye and H-J. Li, "An efficient semi-quantum secret sharing protocol of specific bits," *Quantum Information Processing*, vol. 20, no. 6, pp. 1-11, Jun. 2021.
[35] M. H. Ullah, R. Eskandarpour, H. Zheng and A. Khodaei, "Quantum computing for smart grid applications," *IET Generation, Transmission and Distribution*, vol. 16, no. 21, pp. 4239-4257, Nov. 2022.
[36] Y.-A. Wang, B. Shen, L. Zou and Q.-L. Han, "A survey on recent advances in distributed filtering over sensor networks subject to communication constraints," *International Journal of Network Dynamics and Intelligence*, vol. 2, no. 2, art. no. 100007, Jun. 2023.
[37] J. Wu, C. Peng, H. Yang and Y. L. Wang, "Recent advances in event-triggered security control of networked systems: a survey," *International Journal of Systems Science*, vol. 53, no. 12, pp. 2624-2643, 2022.
[38] C. Xie, L. Li, H. Situ and J. He, "Semi-quantum secure direct communication scheme based on bell states," *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1881-1887, Jun. 2018.
[39] L. Yan, S. Zhang and Y. Chang, "Semi-quantum identification," *Quantum Information Processing*, vol. 20, no. 7, 2021.
[40] Z. Yang, Y. Liu, W. Zhang, F. E. Alsaadi and K. H. Alharbi, "Differentially private containment control for multi-agent systems," *International Journal of Systems Science*, vol. 53, no. 13, pp. 2814-2831, 2022.
[41] H. Yuan, Y.-M. Liu, G. Pan, G. Zhang, J. Zhou and Z.-J. Zhang, "Quantum identity authentication based on ping-pong technique without entanglement," *Quantum Information Processing*, vol. 13, no. 11, pp. 2535-2549, Nov. 2014.
[42] Y. Yuan, X. Tang, W. Zhou, W. Pan, X. Li, H.-T. Zhang, H. Ding and J. Goncalves, "Data driven discovery of cyber physical systems," *Nature Communications*, vol. 10, no. 1, pp. 1-9, 2019.
[43] H. Zhang, D. Yue, C. Dou, X. Xie, K. Li and G. P. Hancke, "Resilient optimal defensive strategy of TSK fuzzy-model-based Microgrids' system via a novel reinforcement learning approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 4, pp. 1921-1931, Apr. 2023.
[44] S. Zhang, Z. Chen, R.-H. Shi and F.-Y. Liang, "A novel quantum identity authentication based on bell states," *International Journal of Theoretical Physics*, vol. 59, no. 1, pp. 236-249, Jan. 2020.
[45] W. Zhang, S. Liu and Z. Xia, "A distributed privacy-preserving data aggregation scheme for smart grid with fine-grained access control," *Journal of Information Security and Applications*, vol. 66, art. no. 103118, May 2022.
[46] J. Zheng, D. W. Gao and L. Lin, "Smart meters in smart grid: an overview," *in Proceedings of IEEE Green Technologies Conference (GreenTech)*, Denver, CO, Apr. 2013. pp. 57-64.
[47] N. Zhou, K. Zhu, W. Bi and L.-H. Gong, "Semi-quantum identification," *Quantum information processing*, vol. 18, no. 6, Jun. 2019.
[48] P. Zhuang, T. Zamir and H. Liang, "Blockchain for cybersecurity in smart grid: a comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 16, pp, 3-19, Jan. 2021.
[49] https://github.com/XiaopingLou/BDT-with-authencitcation.git
[50] K. Prateek, M. Das, S. Surve, S. Maity and R. Amin, "Q-Secure-P2-SMA: Quantum-Secure Privacy-Preserving Smart Meter Authentication for Unbreakable Security in Smart Grid," *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2024.3357103.
[51] 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*, doi: 10.1109/TNSE.2024.3427110
[52] S. Aggarwal and G. Kaddoum, "Authentication of Smart Grid by Integrating QKD and Blockchain in SCADA Systems," *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2024.3423762.

[53] H. C. Chen, C. Damarjati, E. Prasetyo, C. L. Chou, T. L. Kung and C. E. Weng, "Generating Multi-Issued Session Key by Using Semi Quantum Key Distribution With Time-Constraint," *IEEE Access*, vol. 10, pp. 20839-20851, 2022,
[54] R. Yan, Y. Wang, J. Dai, Y. Xu and A. Q. Liu, "Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement," *IEEE Transactions on Industry Applications*, vol. 58, no. 3, pp. 3076-3086, May-June. 2022,
[55] G. Xu, Q. Zhang, Z. Song and B. Ai, "Relay-assisted deep space optical communication system over coronal fading channels," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 6, 2023.
[56] W. Chen, X. Qiu, T. Cai, H. N. Dai, Z. Zheng, and Y. Zhang, "Deep reinforcement learning for Internet of Things: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 1659-1692, 2021.
[57] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, "Overview of 5G security challenges and solutions". *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, 2018.
[58] Z. Zeng, S. Fu, H. Zhang, Y. Dong, J. Cheng, "A survey of underwater optical wireless communications," *IEEE communications surveys and tutorials*, vol. 19, no. 1, pp. 204-238, 2016.
[59] D. Said, "A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities," *IEEE Engineering Management Review*, vol. 51, no. 1, pp. 76-107, 2022.
[60] K. Bertels, A. Sarkar, I. Ashraf, "Quantum computingłFrom NISQ to PISQ," *IEEE Micro*, vol. 41, no. 5, pp. 24-32, 2021