

Controlled Authentication Semi-Quantum Key Agreement Protocol for the Internet of Medical Things

Yefeng He, Liaoyuan Shen* and Yichi Zhang

School of Cyberspace Security, Xi'an University of Post & Telecommunications, Xi'an 710121, China;
yefenghe2008@hotmail.com (Y.H.); chenug17@163.com (Y.Z.)

* Corresponding author: liaoyuan20260120@163.com

Received date: 12 October 2025; Accepted date: 6 January 2026; Published online: 25 January 2026

Abstract: In the Internet of Medical Things (IoMT), sensors automatically collect data and transmit it to hospital servers, where doctors provide professional medical advice. The emergence of IoMT has significantly reduced the burden on chronic-disease patients and improved their life security. However, the transmission of patients' medical data still faces serious confidentiality and integrity risks. This paper proposes a novel healthcare-system architecture that integrates a controlled-authentication semi-quantum key-negotiation (SQKN) protocol, leveraging the unconditional security of quantum cryptography to mitigate potential data attacks. The hospital server acts as a trusted controller that supervises every protocol run and authenticates all participants, which effectively thwarts man-in-the-middle and identity-spoofing attacks. The semi-quantum design further minimizes the quantum-device burden on patients' side. Experimental simulation under realistic noise ($QBER \approx 0.03$ at 0.02/0.04 noise level, 3 000 shots) shows the protocol keeps the quantum-bit error rate below 3 %, while the overall key-generation efficiency reaches 92 %, demonstrating that the scheme resists known attacks and maintains high quantum efficiency for safeguarding IoMT data security.

Keywords: quantum key agreement; W states; semi-quantum key agreement; identity authentication

1. Introduction

With the advent of the Internet of Medical Things (IoMT) [1–3], many patients with chronic diseases, such as cardiovascular diseases, chronic respiratory conditions and endocrine system disorders, among others, who cannot remain hospitalized for extended periods, now have improved access to timely assistance during emergencies. In the IoMT architecture, patients can transmit their medical data to hospital diagnostic systems in real-time via IoMT devices. Doctors can then provide timely and professional medical advice through the model, significantly reducing patient burdens and enhancing health protection. However, the security of existing IoMT systems still faces threats from network attacks. All public-key cryptography currently deployed to protect medical data—ECDH, RSA, DSA, ECDSA, and their variants—will collapse overnight once a sufficiently large quantum computer becomes available, instantly shattering the confidentiality, integrity, and availability of the entire Internet of Medical Things. Traditional cryptographic methods used to protect the data in the IoMT are no longer sufficient to ensure data security, as they are facing potential threats from quantum computing or quantum attack.

Quantum cryptography is an emerging discipline that combines the principles of quantum mechanics to secure information. It is primarily based on the Heisenberg Uncertainty Principle and the No-Cloning Theorem [4]. Compared to classical cryptography, quantum cryptography offers unconditional security in principle, which has garnered significant attention from cryptography researchers. Since the introduction of the famous BB84 protocol by Bennett and Brassard in 1984 [5], researchers have proposed a variety of quantum protocols. The main research directions in quantum protocols currently include quantum key distribution (QKD) [6–8], quantum key agreement (QKA) [9,10], quantum secret sharing (QSS) [11–13], and quantum private comparison (QPC) [14–16], among others.

Quantum key agreement (QKA) is one of the key research areas, primarily leveraging quantum resources to negotiate a shared encryption key among multiple communicators. In this process, no single participant can control the final shared key, ensuring that all parties contribute equally. In 2004, Zhou et al. [17] first proposed a QKA protocol based on quantum teleportation. Subsequently, various QKA protocols for multiple quantum states and participants

were proposed by researchers [18–20]. To address the issue of noise interference in practical communication, He et al. [21] introduced a noise resistant quantum key agreement protocol in 2016. In 2022, He et al. [22] proposed a two-party mutual authentication QKA protocol, further enhancing the security of the protocol. As researchers explored QKA protocols, many different requirements were added to adapt the protocols for real-world applications. Controlled quantum key agreement (CQKA) allows multiple participants to generate a shared key under the control of a third party, increasing the flexibility and security of the protocol. In 2017, Shukla et al. [23] proposed the CQKA protocol for secure direct communication. In 2023, Dutta et al. [24] proposed a CQKA protocol that does not require quantum memory. Mutual authentication quantum key agreement (MAQKA) not only enables key negotiation but also verifies the legitimacy of user identities, preventing security threats such as man-in-the-middle and replay attacks. In 2022, He et al. [25] proposed a MAQKA protocol based on Bell states. In 2024, He et al. [26] introduced a mutually authenticated semi-quantum key agreement protocol. These protocols have laid a solid foundation for the development of QKA, continuously improving its security, efficiency, and feasibility.

The aforementioned QKA protocols generally require communication participants to possess full quantum capabilities. However, in practical applications, participants may lack complete quantum processing capabilities due to the high cost of quantum equipment and the scarcity of resources. In 2007, Boyer et al. [27] introduced the concept of semi-quantum in the QKD protocol, where one user possesses full quantum capabilities, while the other can only perform classical operations, such as reflection and measurement. In 2017, Shukla et al. [23] extended the semi-quantum concept to key agreement and proposed the semi-quantum key agreement (SQKA) protocol, allowing quantum and classical users to generate a shared key without fully relying on quantum capabilities. In 2022, Xu et al. [18] introduced an SQKA protocol based on GHZ entangled states. In 2023, He et al. [28] proposed a four-party semi-quantum key agreement protocol based on four-particle cluster states. In 2024, He et al. [26] proposed a two-party mutually authenticated semi-quantum key agreement protocol using Bell states. These studies have advanced the SQKA protocol from concept to practical application, continuously enhancing its security and efficiency.

Given the continuous development of quantum cryptography and the increasing importance of its application in real-world scenarios, especially in healthcare systems, we propose a controlled authentication semi-quantum key agreement protocol (CASQKA) tailored for such environments. This protocol not only establishes a fair shared key among four parties but also allows the trusted party to authenticate the identities of the remaining participants. The protocol requires only one trusted party to possess full quantum capabilities, while the other three participants only need semi-quantum capabilities, furthermore the trusted party can oversee the execution of the protocol. The protocol ensures security by defending against identity impersonation attacks, interception and replay attacks among others, and exhibits a certain degree of quantum efficiency. When applied to health care systems, the protocol guarantees the confidentiality and integrity of communication data between patients and doctors, thereby protecting patient privacy. Specifically, our work targets the security vulnerabilities in key agreement and authentication within the IoMT ecosystem via the designed controlled authenticated semi-quantum key agreement (CASQKA) protocol. To further enhance the security, trustworthiness and scalability of smart healthcare systems, we will explore three promising research directions in future work: quantum-based privacy-preserving techniques for secure IoMT with in-depth analysis, controlled quantum authentication confidential communication protocols for smart healthcare [29], and novel privacy-preserving distributed multiparty data outsourcing schemes for cloud computing integrated with quantum key distribution [30].

The main contribution of this work are summarized as follows:

- (1) A novel internet of medical things (IoMT) security architecture is proposed, which integrates semi-quantum key agreement techniques. Within this architecture, resource-constrained semi-quantum medical devices can complete identity authentication, key agreement, and secure communication under the supervision of a fully quantum-capable controller.
- (2) Based on the proposed architecture, we design a controlled authenticated semi-quantum key agreement (CASQKA) protocol that incorporates both authentication and key agreement phases. The protocol ensures the legitimacy of participants and guarantees the confidentiality and consistency of the final shared key.
- (3) A comprehensive security analysis is conducted against various common attack strategies.
- (4) The feasibility of preparing the required quantum resources was verified through simulation, providing support for the potential practical implementation of the protocol.
- (5) According to simulation results, the protocol exhibits a low quantum bit error rate under both depolarizing noise and amplitude-damping noise, demonstrates robustness against these two types of noise, and achieves a high key-generation rate.

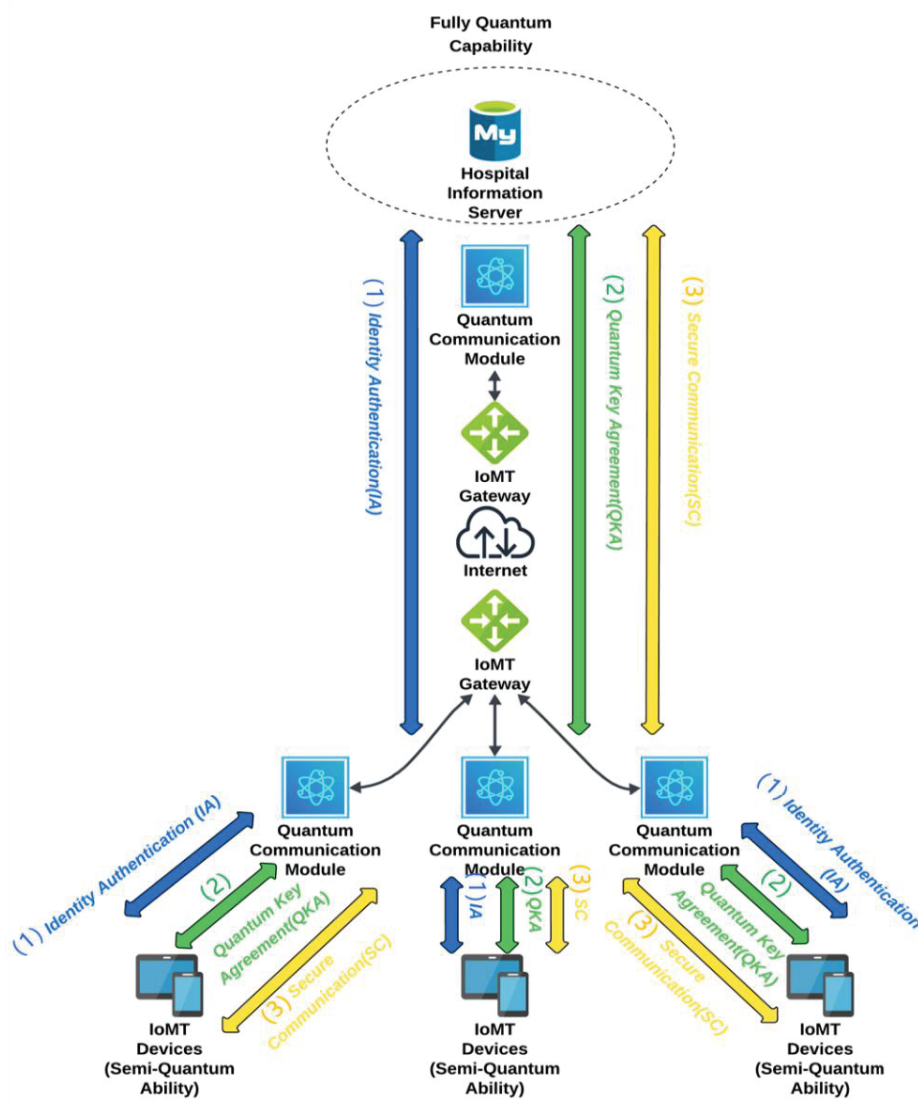


Figure 1. Healthcare model with CASQKA.

The organization of the paper is as follows: Section 2 introduces the new healthcare system based on the CASQKA protocol that we propose. Section 3 describes the basic theory of W states and our proposed CASQKA protocol. Section 4 provides a security analysis of the CASQKA protocol. Section 5 presents the simulation of our protocol and compares our CASQKA protocol with existing protocols. Section 6 concludes the paper.

2. Healthcare systems with quantum key agreement

2.1. Construction of healthcare system and workflow

In the internet of medical things (IoMT) systems, devices typically transmit critical data, such as patient physiological information, diagnostic data, and surgical control commands among others. This data requires a very high level of security, as traditional encryption methods based on mathematical problems may not withstand the growing threats of quantum cyberattacks. For this purpose, we propose a new healthcare system model (refer to Figure 1 for detailed information) that integrates CASQKA with the IoMT. In the new system model, the security of key agreement between IoMT devices is ensured by quantum principles. This system model not only provides highly secure keys for secure data communication and data integrity authentication between devices but also possesses the capability for identity authentication between devices, preventing data from being intercepted or eavesdropped on during transmission.

The new system model consists of the following modules, each with its respective functionality.

Hospital Information Server: Acting as a fully trusted party within the system model, is equipped with comprehensive quantum capabilities. It oversees identity authentication and key agreement processes. The server is responsible for storing the identity sequences of various IoMT devices, calculating error rates, and managing the final shared keys.

Table 1. Encoding rules.

Quantum states	Classical bits
$ 0\rangle$	0
$ 1\rangle$	1

Quantum Communication Module: It possesses the capability to prepare quantum state sequences, receive sequence information from both the hospital server and IoMT devices, and perform encoding and decoding according to Table 1.

IoMT Gateway: A quantum channel and a classical authentication channel are established between the hospital server and the IoMT devices.

IoMT Devices: They are equipped with semi-quantum capabilities. These include various medical sensors, wearable devices and smart diagnostic equipment for transmitting users' medical data.

The workflow of the new system model primarily consists of the Identity Authentication Phase, Key Agreement Phase, and Secure Communication Phase, as detailed below: During the authentication phase, the hospital's information server verifies the identity of the IoMT devices to protect against identity impersonation attacks. In the key agreement phase, the hospital's information server and the IoMT devices use the CASQKA protocol to establish a fair shared key. In the secure communication phase, the IoMT devices and the hospital's information server use the shared key to encrypt the transmitted message along with the message digest, ensuring the confidentiality and integrity of the messages.

The new system model begins with the authentication of IoMT devices. Next, key agreement is completed between the hospital information server and each IoMT device, resulting in the establishment of a shared key. During the Communication Phase, the IoMT devices automatically collect the user's pathological data and, after providing encryption and message integrity protection through the shared key, transmit the pathological data to the hospital's information server. The hospital server then transmits the data to the hospital diagnostic system. The doctor provides medical diagnoses and advice through the diagnostic system, encrypts the information and ensures message integrity using the shared key, and transmits it back to the IoMT devices. This completes the communication process of the new healthcare system, ensuring the confidentiality and integrity of data transmission between doctors and patients. It prevents the leakage of patient privacy and the tampering of pathological data.

2.2. Establishment and security assurance of quantum communication channels in mobile IoMT devices

IoMT devices, such as wearable sensors and mobile medical equipment, inherently involve mobility, which can pose challenges for establishing reliable quantum communication channels. In our proposed model, we address this challenge by leveraging quantum communication technologies such as fiber optics for stationary communication links and free space for mobile devices.

For the mobile IoMT devices, free-space optical links are employed, which utilize laser-based communication for quantum transmission. These links are robust enough to accommodate the dynamic movement of IoMT devices while maintaining secure and efficient quantum key exchange. Additionally, the quantum communication module at each IoMT device is designed to dynamically adjust to the mobile environment, optimizing the communication protocol for varying distances and line-of-sight conditions.

In scenarios where fiber optic connections are impractical due to the mobility of IoMT devices, we employ hybrid systems that combine classical and quantum communication techniques. Classical channels handle the control and synchronization of quantum keys, while quantum channels are responsible for the actual key agreement and encryption processes. This hybrid approach ensures that even in highly mobile environments, such as between the hospital server and roaming IoMT devices, secure key agreement and data integrity can be reliably maintained.

3. Controlled authentication semi-quantum key agreement protocol based on W states

3.1. Theoretical preparation

The W states was first proposed by Dür et al. [31]. It is a quantum state of m ($m > 2$) qubits involving an equal superposition of m terms, those with only one qubit in the state $|1\rangle$, while all the other qubits are in the state $|0\rangle$. The W state exhibits multi-body entanglement and retains partial entanglement properties within its subsystems [31]. This

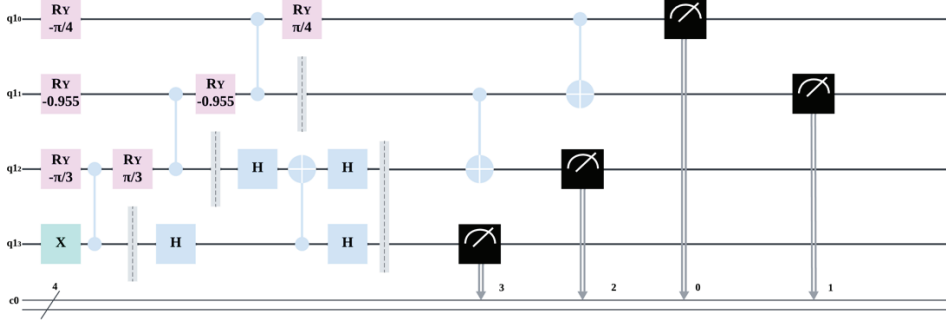


Figure 2. Quantum circuit diagram for preparing and measuring a 4-Particle W States.

means that even if one quantum bit is lost, the W states still maintains a certain degree of entanglement. The partial entanglement characteristic of the W states offers higher robustness in quantum communication. A four-particle W states (the preparation and measurement of the W states is shown in Figure 2) can be represented as follows:

$$|W\rangle_{ABCD} = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \quad (1)$$

$$= \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{12} \otimes |\Psi^+\rangle_{34} + |\Psi^+\rangle_{12} \otimes \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{34} \quad (2)$$

$$= \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{13} \otimes |\Psi^+\rangle_{24} + |\Psi^+\rangle_{13} \otimes \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{24} \quad (3)$$

$$= \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{14} \otimes |\Psi^+\rangle_{23} + |\Psi^+\rangle_{14} \otimes \frac{1}{2}(|\Phi^+\rangle + |\Phi^-\rangle)_{22} \quad (4)$$

Key properties of W states relevant to CASQKA protocol:

Entanglement robustness: For instance, if any single qubit is trace out from the four-particle W state, the remaining three-qubit reduced state is a mixed state that includes a three-qubit W state component. Specifically, tracing out qubit D yields:

$$\rho_{ABC} = \frac{3}{4}|\tilde{W}_3\rangle\langle\tilde{W}_3| + \frac{1}{4}|000\rangle\langle 000| \quad (5)$$

where $|\tilde{W}_3\rangle = 1/\sqrt{3}(|001\rangle + |010\rangle + |100\rangle)$. This residual entanglement ensures robustness against qubit loss, unlike GHZ states which become fully separable.

Bell-state decomposition and eavesdropping detection: The W state can be decomposed into combinations of Bell states (Equations 2-4). This property enables efficient parity checks via local Bell-state basis measurement. Any eavesdropping attempt disrupts the expected correlations, triggering protocol termination.

Efficiency advantage: W states enable deterministic entanglement swapping without postselection (unlike probabilistic GHZ-based schemes), achieving a qubit efficiency of $\eta = 1 - 0(1/m)$ for m -party key distribution.

Security proof against attacks: For an eavesdropper (Eve) inducing an error rate ϵ , the mutual information $I(A : E)$ between Alice and Eve is bounded by: $I(A : E) \leq 2\epsilon \log d + h(\epsilon)$, where d is the Hilbert space dimension and h is the binary entropy function.

The security bound holds only when the photon loss probability is below the W state's lossthreshold: for the 4-particle W state, this threshold is $p < 0.75$ [32], meaning the residuaW-state entanglement component remains dominant as long as the single-qubit lossprobability is less than 75% [33]. Exceeding this threshold reduces the residual entanglement anddegrades the QKD key rate following the relation $R \propto (1 - p_L)^4$ (where m is the number of qubits in the W state), highlighting the need for loss mitigation (e.g., entanglement purification) inhigh-loss OKD links.

3.2. Controlled authentication semi-quantum key agreement protocol

Assume the participants in the protocol are Alice, Bob, Charlie, and Dave. Alice corresponds to the hospital information server in the new healthcare system model described in Section 2, while Bob, Charlie, and Dave represent IoMT devices. Among them, Alice is a fully trusted party with complete quantum capabilities. Bob, Charlie, and Dave are semi-quantum participants who need to complete identity authentication before proceeding with the CASQKA protocol. They are only able to perform CTRL and SIFT operations. CTRL refers to sending back the particle without

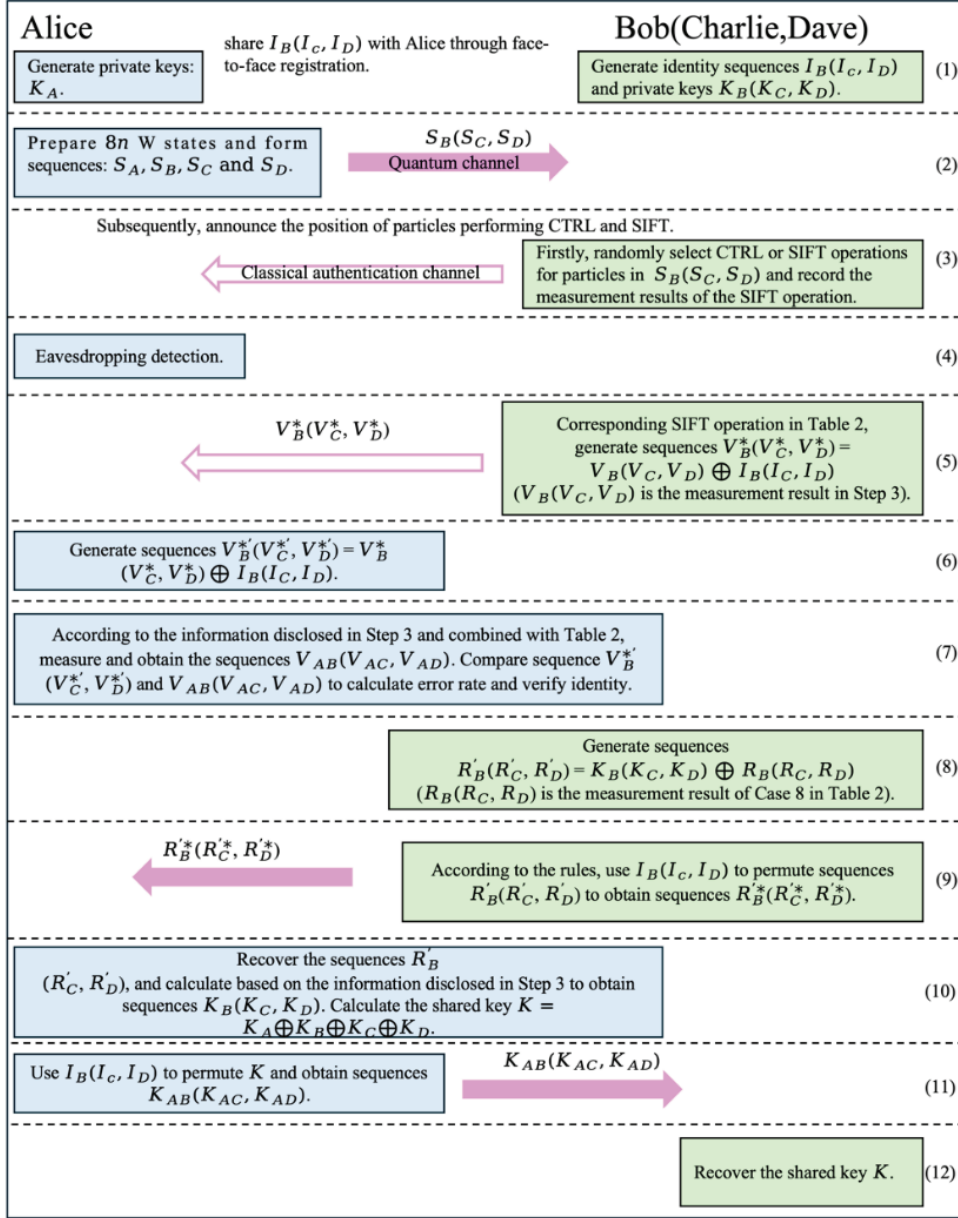


Figure 3. Workflow of the proposed protocol.

interference, while SIFT involves measuring the particle in the Z basis and preparing a new particle in the same state to send back to the sender. However, there are two situations for SIFT: one is to prepare a quantum state based on the measurement results and send it back to the receiver immediately, or to use a classical bit to record the measurement results. When the sender needs it, they can re prepare the quantum state based on the recorded classical bits and send it.

In the protocol design, the pre-shared authentication information is securely distributed during the users' initial face-to-face registration phase. That is to say, Alice used a random number generator to generate identity information for Bob, Charlie, and Dave, and then embeds the information into the device.

In our protocol, the classical authenticated channel is used to transmit public but integrity-sensitive information, such as whether a particle operation is a CTRL or SIFT operation, the positional information of these particles, and information about particles used for safety detection. Although encryption is not required, it is critical to prevent any unauthorized modification of these messages. To ensure authenticity and integrity, we employ lattice-based digital signature schemes, such as Dilithium or Falcon [34], which provide strong post-quantum security guarantees against both classical and quantum adversaries.

The specific protocol flow is show in Figure 3.

Table 2. All operational scenarios of Bob, Charlie, and Dave.

Case	Bob	Charlie	Dave	Protocol phase
1	CTRL	CTRL	CTRL	Security check
2	CTRL	CTRL	SIFT	
3	CTRL	SIFT	CTRL	
4	CTRL	SIFT	SIFT	
5	SIFT	CTRL	CTRL	
6	SIFT	CTRL	SIFT	
7	SIFT	SIFT	CTRL	
8	SIFT	SIFT	SIFT	Key agreement

Step 1. Before the protocol begins, Bob, Charlie, and Dave share their identity sequences: I_B , I_C , and I_D with Alice (complete through face-to-face registration). Each $I_i = \{I_i^{(1)}, I_i^{(2)}, I_i^{(3)} \dots I_i^{(n)}\}$, where i can be B, C, or D. The values $I_i^{(1)}, I_i^{(2)}, I_i^{(3)} \dots I_i^{(n)} \in \{0, 1\}$ (with approximately equal probabilities for 0 and 1). Alice, Bob, Charlie, and Dave randomly generate their private keys: $K_A = \{K_A^{(1)}, K_A^{(2)}, K_A^{(3)} \dots K_A^{(n)}\}$, $K_B = \{K_B^{(1)}, K_B^{(2)}, K_B^{(3)} \dots K_B^{(n)}\}$, $K_C = \{K_C^{(1)}, K_C^{(2)}, K_C^{(3)} \dots K_C^{(n)}\}$, $K_D = \{K_D^{(1)}, K_D^{(2)}, K_D^{(3)} \dots K_D^{(n)}\}$, where $K_A^{(i)}, K_B^{(i)}, K_C^{(i)}, K_D^{(i)} \in \{0, 1\}$ (with approximately equal probabilities for 0 and 1), and $i \in \{1, 2, \dots, n\}$.

Step 2. Alice prepares $8n$ W states, forming a W states sequence. Alice divides this W states sequence into four sequences: S_A , S_B , S_C , S_D . Sequence S_A consists of all the first particles from the W states, S_B consists of all the second particles, S_C consists of all the third particles, and S_D consists of all the fourth particles. Alice begins to transmit the sequences S_B , S_C , S_D to Bob, Charlie, and Dave in order, while keeping sequence S_A for herself.

Step 3. Bob, Charlie, and Dave randomly perform either the CTRL or SIFT operations on particles in their respective sequence S_B , S_C , S_D and record the measurement results of the SIFT operations as classical bits according to the encoding rules in Table 1. After executing the operations on all particles, Bob, Charlie, and Dave disclose the positions about the CTRL and SIFT operations performed on the W states particles in sequences S_B , S_C , and S_D through the classical authentication channel. There are a total of eight scenarios (refer to Table 2 for detailed information).

Step 4. In Case 1, Alice uses Z-basis to measure the particles reflected by Bob, Charlie, and Dave, as well as the particles retained by herself, and calculates the error rate using Equation (1). In Cases 2, 3, and 4, Alice performs a Bell basis measurement on the particles reflected by Bob, as well as the particles retained by herself, and calculates the error rate using Equation (2). In Cases 5 and 6, Alice performs a Bell basis measurement on the particles reflected by Charlie, as well as the particles retained by herself, and calculates the error rate using Equation (3). In Case 7, Alice performs a Bell basis measurement on the particles reflected by Dave, as well as the particles retained by herself, and calculates the error rate using Equation (4). If the error rates for all seven cases mentioned above are below the threshold, the protocol continues; otherwise, it is terminated.

Step 5. After passing the security check, Bob, Charlie, and Dave proceed with their respective authentication operations. Taking Bob as an example, he constructs a classical bit sequence $V_B = \{V_B^{(1)}, V_B^{(2)}, V_B^{(3)} \dots V_B^{(n)}\}$ based on the measurement results recorded in Case 5 of Table 2, where each $V_B^{(i)}$ takes a value of 0 or 1 ($i \in \{1, 2, \dots, n\}$). Bob then performs a bitwise XOR operation between his identity sequence I_B and the sequence V_B , resulting in a new sequence V_B^* , defined as $V_B^* = \{V_B^{(1)} \oplus I_B^{(1)}, V_B^{(2)} \oplus I_B^{(2)}, V_B^{(3)} \oplus I_B^{(3)} \dots V_B^{(n)} \oplus I_B^{(n)}\}$. Finally, Bob announces the classical bit sequence V_B^* to Alice through the classical authentication channel. At the same time, Charlie and Dave perform the same operation as Bob based on the measurement results recorded in Case 3 and Case 2 in Table 2, respectively. Finally, Charlie and Dave announced the classical bit sequences V_C^* and V_D^* to Alice through the classical authentication channel. Symbols such as V_B , V_C , V_D are specifically explained in Table 3.

Step 6. Upon receiving the sequences V_B^* , V_C^* , and V_D^* , Alice processes them to verify authentication. Taking V_B^* as an example, Alice performs a bitwise XOR operation between Bob's pre-shared identity sequence I_B (from Step 1) and the received sequence V_B^* , generating a new sequence $V_B'^*$, $V_B'^* = \{V_B^{*(1)} \oplus I_B^{(1)}, V_B^{*(2)} \oplus I_B^{(2)}, V_B^{*(3)} \oplus I_B^{(3)} \dots V_B^{*(n)} \oplus I_B^{(n)}\}$. Alice performs the same operation on the sequences V_C^* , and V_D^* using Charlie's and Dave's pre-shared identity sequences I_C and I_D , respectively, obtaining the new sequences $V_C'^*$ and $V_D'^*$.

Step 7. Based on the position information disclosed by Bob, Charlie, and Dave in Step 3, Alice is able to obtain the measurement results corresponding to Case 5 in Table 2 (Bob's SIFT, Charlie and Dave's CTRL) by performing Z-basis measurements. These results form a classical bit sequence V_{AB} . Similarly, Alice extracts V_{AC} and V_{AD}

Table 3. Variable-Meaning.

I_B, I_C, I_D	Bob/Charlie/Dave's pre-shared identity bit strings (n bits)
K_A, K_B, K_C, K_D	Each party's private key string (n bits)
S_A, S_B, S_C, S_D	The four-particle sequences of the W state are held by Alice, Bob, Charlie, and Dave, respectively.
V_B, V_C, V_D	The n-bit outcomes of Z-basis measurements performed by Bob/Charlie/Dave at the SIFT positions.
V_B^*, V_C^*, V_D^*	The XOR of the measurement outcome with the identity string, $V_B^* = \{V_B^{(1)} \oplus I_B^{(1)}, V_B^{(2)} \oplus I_B^{(2)}, V_B^{(3)} \oplus I_B^{(3)} \dots V_B^{(n)} \oplus I_B^{(n)}\}$, used for authentication.
V_{AB}, V_{AC}, V_{AD}	The classical bit string actually measured by Alice at the corresponding positions, used for comparison and verification.
R_B, R_C, R_D	The n-bit SIFT measurement results of Bob/Charlie/Dave in Case-8
R'_B, R'_C, R'_D	used to conceal the private key
K	the final 4-party shared key
K_{AB}, K_{AC}, K_{AD}	The key segments permuted by Alice using I_B, I_C, I_D are sent to Bob/Charlie/Dave, respectively.

based on Case 3 (Charlie's SIFT) and Case 2 (Dave's SIFT), respectively. Each of these sequences is then converted into a classical bit sequence according to the encoding rules in Table 1. Finally, Alice compares V_B^* with V_{AB} to calculate the error rate and verify Bob's identity. The same process is applied to verify Charlie's and Dave's identities by comparing V_C^* with V_{AC} , and V_D^* with V_{AD} . If all the error rates are below the predefined threshold, the identity authentication passes and the protocol continues; otherwise, the protocol is terminated.

Completeness & soundness in a nutshell. Let n be the length of identity sequence I and P_e the single-bit QBER. Alice accepts if the mismatch rate $\leq \epsilon = 1/3$. (1) Honest Bob: mismatches $\sim \text{Bin}(n, P_e)$; Hoeffding gives $\Pr[\text{reject}] \leq \exp(-2n(1/3 - P_e)^2)$. (2) Any attacker ignorant of I faces a one-time pad; mismatch rate $\sim \text{Bin}(n, 1/2)$, so $\Pr[\text{accept}] \leq \exp(-2n(1/2 - 1/3)^2) = \exp(-n/18)$. Both bounds vanish exponentially in n .

Step 8. After successfully passing the identity authentication in Step 7, continue with the protocol. For Case 8, Bob, Charlie, and Dave encode the measurement results of the corresponding positions into classical sequences R_B, R_C , and R_D according to the rules specified in Table 1. Subsequently, Bob performs the operation $R'_B = K_B \oplus R_B$. Charlie and Dave perform the same operation to obtain the sequences R'_C and R'_D .

Step 9. Bob, Charlie, and Dave then iterate through their respective identity sequences I_B, I_C , and I_D . When $I_B^{(i)} = 0$, the positions of $R_B^{(j)}$ and $R_B^{(j+1)}$ in R'_B are not swapped. When $I_B^{(i)} = 1$, the positions of $R_B^{(j)}$ and $R_B^{(j+1)}$ in R'_B are swapped. When Bob reaches $I_B^{(\lfloor \frac{i}{2} \rfloor + 1)}$, he begins the second round of swapping. If the length n of I_B and R'_B is odd, the index j selected from the set $\{1, 3, 5, \dots, n, 2, 4, 6, \dots, n-1\}$. Conversely, if the length n is even, j is chosen from the set $\{1, 3, 5, \dots, n-1, 1, 3, 5, \dots, n-1\}$. Finally, the sequence R'_B is transformed into sequence R_B^* , while Charlie and Dave perform the same operations to obtain sequences R'_C and R'_D , respectively. Bob, Charlie, and Dave convert their respective sequences into quantum states according to the encoding rules in Table 1 and send them to Alice.

Step 10. Upon receiving the sequences sent by Bob, Charlie, and Dave, Alice uses her retained identity sequences I_B, I_C , and I_D to recover R'_B, R'_C , and R'_D . Based on the information disclosed by Bob, Charlie, and Dave in step 3, Alice measures the second, third, and fourth particles of the W states particles where all parties performed the SIFT operation to obtain the sequences R_{AB}, R_{AC}, R_{AD} . Alice applies the rules from step 8 with sequence R'_B and sequence R_{AB} to recover K_B . Alice performs the same operations on Charlie's and Dave's sequences to obtain K_C and K_D . Alice calculates the shared key $K = K_A \oplus K_B \oplus K_C \oplus K_D$ and converts K into quantum sequence according to Table 1.

Step 11. Alice iterates through the sequence I_B, I_C , and I_D . When $I_B^{(i)} = 0$, the positions of K^j and K^{j+1} in K are not swapped. When $I_B^{(i)} = 1$, the positions of K^j and K^{j+1} in K are swapped. When Alice reaches $I_B^{(\lfloor \frac{i}{2} \rfloor + 1)}$, she begins the second round of permutation. If the length n of I_B and K is odd, the index j selected from the set $\{1, 3, 5, \dots, n, 2, 4, 6, \dots, n-1\}$. Conversely, if the length n is even, j is chosen from the set $\{1, 3, 5, \dots, n-1, 1, 3, 5, \dots, n-1\}$. Finally, the sequence K is transformed into K_{AB} . Alice performs the same operations to obtain the sequence K_{AC} and K_{AD} by iterating sequence I_C and I_D . Alice sequentially sends the sequences K_{AB}, K_{AC} , and K_{AD} to Bob, Charlie, and Dave.

Step 12. Bob, Charlie, and Dave sequentially measure their received sequences and record the measurement results. Then, based on their respective identity sequences I_B , I_C , and I_D , they perform the inverse operations of those in Step 11 to reconstruct the shared key. Consequently, each of them successfully obtains the shared key.

3.3. Correctness Analysis

Initialization phase:

Alice prepares and distributes $8N$ W-states, splitting them into four sequences S_A , S_B , S_C , S_D that contain, respectively, the first, second, third, and fourth particle of every W-state. She keeps S_A for herself and sends S_B , S_C , S_D to Bob, Charlie, and Dave. Each of the three recipients randomly performs either a CTRL or a SIFT operation on the particles in his own sequence and, according to Table 1, records the measurement outcome of any SIFT operation as a classical bit. After all operations are finished, they publicly announce which operation was applied to each W-state particle and the corresponding positions. According to Table 2, the error rate is computed for all seven cases except Case 8. If the error rates of these seven cases are all below the prescribed threshold, the quantum channel is judged to be secure.

Authentication phase:

Bob constructs a classical sequence $V_B = \{V_B^{(1)}, V_B^{(2)}, V_B^{(3)} \dots V_B^{(n)}\}$ based on Case 5. He bitwise XORs V_B with I_B to obtain $V_B^* = \{V_B^{(1)} \oplus I_B^{(1)}, V_B^{(2)} \oplus I_B^{(2)}, V_B^{(3)} \oplus I_B^{(3)} \dots V_B^{(n)} \oplus I_B^{(n)}\}$ and sends V_B^* to Alice. Charlie and Dave perform the same operation with their own data. Alice XORs the received V_B^* with I_B to recover $V_B^{*'} = \{V_B^{*(1)} \oplus I_B^{(1)}, V_B^{*(2)} \oplus I_B^{(2)}, V_B^{*(3)} \oplus I_B^{(3)} \dots V_B^{*(n)} \oplus I_B^{(n)}\}$, and likewise computes $V_C^{*'}$ from V_C^* and I_C and $V_D^{*'}$ from V_D^* and I_D . Using Table 2, she derives the expected particle-measurement results for Case 5 and labels them V_{AB} ; similarly she obtains V_{AC} from Case 3 and V_{AD} from Case 2. By comparing V_{AB} with $V_B^{*'}$ she calculates the error rate and verifies Bob's identity; the same procedure is repeated to authenticate Charlie and Dave.

Key-agreement phase:

For every instance that falls into Case 8, Bob, Charlie and Dave encode their respective measurement outcomes into the classical strings R_B , R_C and R_D according to the rule given in Table 1. Bob computes $R'_B = K_B \oplus R_B$ and Charlie and Dave similarly obtain R'_C and R'_D . Next, Bob permutes R'_B with I_B to produce R'_B , prepares the corresponding quantum states, and transmits them to Alice. Alice applies the inverse of the I_B permutation to R'_B to recover R'_B , measures her own Case-8 particles (using the information revealed in Step 3) to obtain R_{AB} , and finally recovers Bob's key contribution as $K_B = R_{AB} \oplus R'_B$. Identical steps give Charlie and Dave K_C and K_D . Alice now forms the common key $K = K_A \oplus K_B \oplus K_C \oplus K_D$, converts K into a quantum sequence, and performs three separate permutations governed by I_B , I_C , and I_D to generate K_{AB} , K_{AC} , and K_{AD} , which she sends to Bob, Charlie, and Dave, respectively. Each recipient applies the inverse of his own permutation (I_B , I_C , and I_D) to retrieve the final shared key K .

A permutation is a bijective function π that rearranges the elements of a finite set: $\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. The inverse permutation π^{-1} is the reverse function of π , satisfying $\pi^{-1}(\pi(i)) = i$. A permutation reorders positions; its inverse "restores" the original order. In matrix form, the inverse of a permutation matrix is simply its transpose. Alice permutes K with I_B to obtain K_B ; only someone who knows I_B can apply the inverse permutation to K_B and recover K .

3.4. Example of the proposed CASQKA protocol

Before the protocol begins, Bob, Charlie, Dave and Alice share identity sequences. Suppose Bob's identity sequence is $I_B = \{1, 0\}$, Charlie's is $I_C = \{0, 1\}$, and Dave's is $I_D = \{1, 1\}$. Bob's private key is $K_B = \{1, 1\}$, Charlie's is $K_C = \{0, 0\}$, Dave's is $K_D = \{1, 0\}$, and Alice's private key is $K_A = \{1, 1\}$. Alice prepares 16 four-particle W states and divides them into four sequences: S_A , S_B , S_C , S_D . Sequences S_B , S_C , S_D are distributed to Bob, Charlie, and Dave respectively, while S_A is retained by Alice. Each party (Bob/Charlie/Dave) randomly performs CTRL or SIFT operations on their respective particle sequences, recording the SIFT measurement results as classical bits according to the encoding rules specified in Table 1. Alice then conducts the security verification using Cases 1-7 in Table 2 and Equations (1)-(4). The protocol proceeds only upon successful verification; otherwise, it is terminated immediately.

Bob, Charlie, and Dave begin the authentication process. For Bob, he performs a SIFT operation on the second-position particle of the 3rd and 5th W states. Meanwhile, Charlie and Dave perform CTRL operations on the third and fourth-position particles, respectively (Case 5 in Table 2). Based on the measurement results of the particles returned by the three participants and the measurement results of the particles retained by Alice, Alice determines the quantum states are $|1000\rangle$ and $|0010\rangle$, obtaining the classical bit sequence $V_{AB} = \{0, 0\}$. At this point, Bob obtains

the classical bit sequence $V_B = \{0, 0\}$ and performs an XOR operation with his identity sequence I_B , resulting in the new sequence $V_B^* = \{1, 0\}$. Bob then announces the sequence V_B^* over the classical verification channel. Alice begins verifying Bob's identity by performing an XOR operation between the sequence V_B^* and the corresponding bits from the shared identity sequence I_B , obtaining the new sequence $V_B^{*'} = \{0, 0\}$. By comparing the sequence $V_B^{*'}$ with V_{AB} , Alice can confirm Bob's identity sequence $I_B = \{1, 0\}$ as valid. Case 3 in Table 2 corresponds to the 10th and 14th W states, with Charlie completing the similar authentication process. Case 2 in Table 2 corresponds to the 2nd and 16th W states, with Dave completing the corresponding authentication process. Ultimately, Alice verifies Charlie's identity sequence $I_C = \{0, 1\}$ and Dave's identity sequence $I_D = \{1, 1\}$, and all identity verifications are successful, allowing the protocol to proceed.

At the 7th and 12th W states particles, Bob, Charlie, and Dave all perform a SIFT operation, Bob's measurement result are $|1\rangle$ and $|0\rangle$, Charlie's measurement result are $|0\rangle$ and $|0\rangle$, Dave's measurement results are $|0\rangle$ and $|1\rangle$. Bob obtains the sequence $R'_B = \{0, 1\}$, Charlie obtains $R'_C = \{0, 0\}$, and Dave obtains $R'_D = \{1, 1\}$. Bob, Charlie, and Dave permute R'_B , R'_C , and R'_D , convert them into quantum sequences, and send them to Alice. Alice uses inverse permutation to recover the sequences R'_B , R'_C , and R'_D allowing her to obtain Bob, Charlie, and Dave's private keys: $K_B = \{1, 1\}$, $K_C = \{0, 0\}$, and $K_D = \{1, 0\}$. Finally, Alice computes the shared key $K = \{1 \oplus 1 \oplus 0 \oplus 1, 1 \oplus 1 \oplus 0 \oplus 0\} = \{1, 0\}$. Alice then permutes and sends the shared key K to Bob, Charlie, and Dave, who use inverse permutation to obtain the final shared key K .

3.5. Cluster strategy of healthcare system

In this novel system model, despite the protocol utilizing four-particle W states and being designed for four participants, its scalability has been fully considered. Specifically, under an N-particle W state (express as follows) [42], the system's cluster scalability can be effectively enhanced.

$$|W_N\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^N |0\rangle^{\otimes(i-1)} |1\rangle |0\rangle^{\otimes(N-i)} \quad (6)$$

Experimental advancements have demonstrated the feasibility of generating large-scale W states. For instance, [43] reported the preparation of an eight-photon W state, while [44] achieved the generation of W states involving four to eight particles in an ion trap system. These developments provide a practical foundation for extending our protocol.

To support a larger number of IoMT devices and participants, several critical aspects are considered [45]:

- (1) Entanglement distribution and network latency: As the number of participants grows, the protocol relies on distributing multipartite W states across nodes. Since each participant requires only partial access to the global entangled state, the quantum channel's latency remains relatively constant compared to protocols that require full entanglement reinitialization for each new participant. Moreover, recent studies in quantum repeaters and network routing allow low-latency entanglement distribution even in large-scale settings.
- (2) Bandwidth and communication overhead: The communication bandwidth consumption grows linearly with the number of devices, as each additional IoMT device requires an entangled qubit and minimal classical communication. However, due to the W state's symmetric and robust entanglement structure, this overhead is significantly lower than that in protocols based on GHZ or cluster states, which often require global state reconstruction when nodes are added or removed.
- (3) Computational complexity and local operations: Each participant performs only local measurements and simple unitary operations, regardless of the total number of parties. This ensures that the computational overhead at each node remains constant ($O(1)$) with respect to N. Furthermore, because the protocol avoids complex global state manipulations, the system exhibits high parallelism and supports efficient identity authentication and key agreement across a large-scale network.
- (4) System integration and security scalability: Newly added IoMT devices can establish entanglement with hospital servers through dedicated quantum communication modules without requiring reconfiguration of existing participants. The inherent fault-tolerant nature of the W state allows the system to tolerate minor decoherence and measurement errors during dynamic node addition. This supports secure and scalable integration of multiple hospitals, wearable medical devices, and cloud-based information centers.

Therefore, by leveraging the symmetric structure and robust entanglement of the N-particle W state, the proposed protocol not only supports large-scale cluster expansion but also maintains stable performance in terms of latency, bandwidth, and computational cost. This make it particularly suitable for the heterogeneous and highly dynamic IoMT environment.

3.6. Fault tolerance and error handling

In practical quantum communication systems, quantum states are vulnerable to environmental noise, leading to transmission and measurement errors. To address this, the proposed protocol incorporates standard quantum error detection through sample testing and eavesdropping checks. Specifically, during the verification phase, Alice and Charlie randomly select a subset of qubits for comparison. The observed quantum bit error rate (QBER) is computed, and if it exceeds a predefined threshold, the protocol aborts. This mechanism helps identify potential channel disturbances or malicious interference.

Furthermore, although the protocol assumes ideal quantum channels in theory, in practice, fault tolerance is critical. If a quantum device—such as a photon detector or quantum memory—fails, the protocol is designed to be restarted without relying on the previously used qubits. Since each round of key agreement is independent, the impact of individual device failure is localized and does not compromise previously established keys.

Regarding network partitioning or unstable classical channels, the protocol includes acknowledgment messages after each quantum transmission stage. If acknowledgments are not received within a timeout period, the protocol times out and restarts the key agreement process. This mechanism ensures resilience in unstable IoMT environments.

4. Security Analysis

The controlled authentication semi-quantum key agreement (CASQKA) protocol consists of two main stages: identity authentication and key agreement. To ensure the robustness of the protocol, we conducted a comprehensive security analysis from both internal and external perspectives.

This analysis considers common quantum and classical attack strategies, including external attacks, participant attacks, and internal collusion during the authentication phase, as well as Trojan horse attacks, interception and substitution attacks, entanglement measurement attacks, and potential attacks such as quantum man-in-the-middle attacks and side-channel attacks during the key negotiation phase. In addition, we check whether the protocol meets the key control properties. Each type of threat is analyzed based on the attacker's capabilities, potential impact on the protocol, and how the protocol design mitigates or detects such attempts.

4.1. Identity authentication stage

4.1.1. External attacks

During the identity authentication stage, the quantum sequences are transmitted in Steps 2 and the classical bit sequences are published in Step 5. If Eve wants to intercept the identity sequences, she can only attempt to attack during Steps 2 and 5.

In Step 2, the sequences S_B , S_C , S_D are transmitted to Bob, Charlie, and Dave, respectively. Taking sequence S_B as an example, an eavesdropper, Eve, cannot determine the positions of the n particles used for the identity authentication operation among the total $8n$ particles in the sequence S_B , as these positions are completely random. Therefore, Eve can only guess randomly. The probability that Eve correctly identifies the position of the n authentication particles is $P_1 = \frac{1}{\binom{8n}{n}}$, while the probability that Eve is detected through security checking is $P_2 = 1 - P_1$. When the number of particles n is sufficiently large, the probability that Eve successfully obtains the sequence V_B approaches zero. The same analysis applies to sequences S_C and S_D .

In Step 5, Bob, Charlie, and Dave announce their processed sequence sequences V_B^* , V_C^* and V_D^* over the classical authentication channel. These sequences are derived from XOR operations between their identity sequences I_B , I_C , I_D and their measurement results V_B , V_C , V_D . Even if Eve knows V_B^* , she cannot recover I_B without knowledge of V_B . The probability of Eve successfully guessing V_B is $P_3 = (1/2)^n$, which rapidly approaches zero for large n . Additionally, any attempt by Eve to tamper with the transmitted sequences would introduce errors detectable during the verification process, as Alice compares the received sequences with her own measurements.

In our security analysis, we assumed that an adversary attempting to guess the secret introduces errors with certainty. However, to better reflect real-world scenarios, we now analyze the expected error introduced by the attacker based on different attack strategies. We will continue to investigate the expected error introduced by the attacker under different guessing probabilities [41]. Specifically, we consider the following three scenarios:

- (1) The attacker has partial information (correct guessing rate $p = 0.9$),
- (2) The attacker makes random guesses (correct guessing rate $p = 0.5$),
- (3) The attacker has perfect guessing ability (correct guessing rate $p = 1$).

When the attacker has partial information about the particle's measurement basis, the correct guessing probability is $p = 0.9$, meaning the attacker has a 90% chance of correctly guessing the measurement basis for each particle, and the probability of guessing incorrectly is $1 - p = 0.1$. In this case, the number of incorrect guesses k follows a binomial distribution $B(n, 0.1)$, and the expected value is given by:

$$E(\text{error}) = n(1 - p) = 0.1n \quad (7)$$

This indicates that the attacker is expected to cause errors in $0.1n$ particles out of the total n particles. The error introduced can be quantified by these incorrect particles. Each incorrect guess leads to errors in the final sequence, thus affecting subsequent authentication and verification steps. Therefore, the total error introduced by the attacker is approximately $0.1n$. However, as n increases, the impact of the errors will grow, though it will be much smaller compared to the scenario where the attacker guesses randomly.

When the attacker makes random guesses for each particle's measurement basis, the correct guessing probability is $p = 0.5$, with an error probability of 0.5. In this case, the number of incorrect guesses k still follows a binomial distribution $B(n, 0.5)$, and the expected value is:

$$E(\text{error}) = n(1 - p) = 0.5n \quad (8)$$

Thus, the attacker is expected to make errors in $0.5n$ particles out of n . Compared to the partial information scenario, the errors are more severe, as the attacker only has a 50% chance of guessing each particle correctly. When the attacker's guesses are completely random, the errors increase significantly as n grows, with an expected error of $0.5n$. This will result in a substantial increase in sequence errors, which will affect subsequent verification and identity authentication processes.

When the attacker perfectly guesses each particle's measurement basis (i.e., the attacker knows all the insertion positions and measurement bases), the correct guessing probability is $p = 1$, and the error probability is 0. In this case, the attacker will not make any errors, so the error introduced is 0:

$$E(\text{error}) = n(1 - p) = 0 \quad (9)$$

Since no errors are introduced, the sequence obtained by the attacker will be identical to the original sequence. Therefore, the attacker can completely control the process without introducing any errors.

These errors can severely impact the security of the protocol. However, through error-checking mechanisms and fault-tolerant techniques, the protocol can still detect these errors and take appropriate actions. Even with an error rate of $p = 0.5$ or higher, the protocol remains capable of resisting the attack effectively. As n increases, the probability of a successful attack by the attacker will dramatically decrease.

4.1.2. Participants attacks

Suppose Bob is a dishonest participant. Bob does not know the identity sequence I_B . According to the protocol, Bob has a probability of $\frac{1}{2}$ of choosing the correct operation. The probability of Bob successfully impersonates is $P_4 = (1/2)^n$. When n is sufficiently large, P_4 approaches zero. The same analysis applies to Charlie and Dave.

Next, we also consider the expected error introduced by Bob's random guesses. In the case where Bob makes random guesses, the number of incorrect permutation operations follows a binomial distribution. Specifically, if Bob has a 50% chance of guessing correctly for each operation, the expected number of incorrect permutations is $E(\text{error}) = n(1 - 1/2) = n/2$. This means that, on average, Bob will introduce errors in $0.5n$ out of n identity sequence positions. When n becomes sufficiently large, the probability of Bob successfully impersonating someone approaches zero. However, the expected error rate increases proportionally with n . These expected errors can be mitigated through the error-checking mechanisms within the protocol, designed to identify and correct inconsistencies caused by Bob's incorrect guesses. This analysis also applies to other dishonest participants, such as Charlie and Dave, who would introduce similar errors, with the same expected error rate.

4.1.3. Internal collusion attacks

Assume that up to t malicious participants may collude within the protocol, attempting to either compromise the secret key or disrupt the identity authentication. The following analysis evaluates the impact of different values of t on the security of the protocol:

Case 1: $t = 1$ (a single malicious participant). If Bob is the malicious participant, he may attempt to forge the identity sequences (I_C or I_D) of Charlie or Dave. However, as outlined in Step 5, 6, and 7 of the protocol, identity authentication relies on pre-shared keys. Since Bob cannot access the private keys of other participants, such an attack is infeasible. The success probability of the attack is therefore bounded by: $P_{success}^{(t=1)} \leq (1/2)^n$, which approaches zero as n increases.

Case 2: $t = 2$ (two malicious participants). If Bob and Charlie collude, they may attempt to impersonate Dave or tamper with the key agreement process. In this case, the attack requires breaking both the identity (I_D) and the key distribution (K_D). However, according to the security analysis of the previous authentication phase, the protocol will detect the impersonation attempts by Bob and Charlie at this stage, rendering the attack ineffective. In the key agreement phase, Bob and Charlie may attempt to manipulate K_B and K_C to influence the final shared key K ; however, this is infeasible, as K is jointly determined by all participants. Similarly, any attempt to obtain K_D in advance is also thwarted by the protocol's security checking mechanisms and the analysis of insider attacks. The success probability of such an attack is bounded by: $P_{success}^{(t=2)} \leq (1/2)^{2n}$.

Case 3: $t = 3$ (three malicious participants). If Bob, Charlie, and Dave collude, they may theoretically gain full control over the final key K . However, the protocol mandates that the trusted third party (TTP), Alice must remain honest. As Alice possesses full quantum capabilities and orchestrates the protocol execution, colluding tripartite adversaries cannot forge Alice's private key K_A unless Alice itself is compromised. If Alice is compromised ($t = 4$), the protocol's security collapses entirely, but this violates the predefined TTP assumption.

Under the premise that the fully trusted party Alice remains uncompromised, the protocol resists collusive attacks involving up to $t = 3$ malicious participants. The security strength is exponentially enhanced with n , ensuring robustness against polynomial-time adversarial strategies.

4.2. Key agreement stage

4.2.1. Trojan horse attack

In the protocol, quantum state sequences are transmitted multiple times. An attacker like Eve could attempt to intercept quantum state information by sending malicious optical signals to the quantum communication devices [35]. To mitigate this risk, the protocol requires the integration of optical power monitors in the communication devices. If an optical signal intensity exceeding normal ranges is detected, the protocol will be interrupted. Additionally, narrow-band optical filters are used to allow only specific wavelengths of light to enter the communication devices, reducing the risk of wavelength-based attacks.

4.2.2. Intercept-substitute attack

Intercept-substitute attacks refer to the attacker intercepting transmitted particles and replacing them with particles of their choice for the attack. There are two specific situations for the operation. One type of replacement particles is prepared by the attacker themselves, and the other type of replacement particles is the transmitted particles after being measured. The following analysis examines how the protocol withstands them.

The attacker Eve intercepts quantum states in the quantum channel and substitutes the original particles with ones she has prepared, sending them to the legitimate participants to steal information. This substitution leads to disturbances in the quantum states, resulting in an increased error rate. In Step 3, Eve cannot determine which particles Bob, Charlie, and Dave applied the CTRL operation to, which makes it possible for Alice to detect Eve's attack. Consequently, the protocol demonstrates resistance against this mode of attacks.

The attacker Eve intercepts quantum states in the quantum channel and measures them, then resends the states to the legitimate participants. However, in Step 3, the SIFT and CTRL operations are chosen entirely at random, so Eve does not know which particles had the CTRL operation applied. As a result, Alice will be able to detect Eve's attack. Therefore, the protocol can resist measure-resend attacks.

The above analysis demonstrates that our protocol can resist intercept-substitute attacks.

4.2.3. Entanglement-measure attack

The attacker Eve intercepts the sequence S_B , S_C , and S_D from Step2, as well as the sequences $R_B'^*$, $R_C'^*$ and $R_D'^*$ from Step 9. Eve then uses an auxiliary particle $|E\rangle$ to perform an entangling operation U on the four-particle W states, creating a complex entangled state.

We set the dimension of $|E\rangle$ to 4 to map onto a quantum system containing 4 basis states. This choice of dimension complies with the design requirements of the protocol and the structure of the composite system and is consistent with the multi-encoding techniques commonly used in classical quantum communication protocols. The 4-dimensional

space allows us to introduce multiple possibilities for quantum state superposition, which meets the minimum requirements for error discrimination in a four-qubit system, thereby enhancing the security and complexity of the protocol.

Eve measures the auxiliary quantum states to extract information. Consider the entanglement evolution between system ABCD and environment E. Let the initial state of ABCD be the W state $|W\rangle_{ABCD}$, and the environment state be a pure state $|E\rangle$. Their joint density matrix is given by $|W\rangle\langle W|_{ABCD} \otimes |E\rangle\langle E|$. After unitary evolution U , the coupled system environment state becomes a mixed state as shown in Equation (10). The right-hand side indicates that each computational basis state $|k\rangle$ of ABCD is correlated with a set of orthogonal environment states $\{|e_i\rangle\}$, where the environment exhibits classical probabilistic mixing (described by coefficients $c_{i,k}$).

The resulting state can be expressed as:

$$U(|W\rangle\langle W|_{ABCD} \otimes |E\rangle\langle E|)U^\dagger = \frac{1}{4} \sum_{k=0}^3 (|k\rangle\langle k|_{ABCD} \otimes \sum_{i=0}^3 c_{i,k} |e_i\rangle\langle e_i|) \quad (10)$$

Among them, $|k\rangle_{ABCD}$ represents the four computational basis vectors of the four particle W state, ($K = 0: |0001\rangle, K = 1: |0010\rangle, K = 2: |0100\rangle, K = 3: |1000\rangle$). The coefficients $c_{i,k}$ need to satisfy $\sum_{i=0}^3 c_{i,k} = 1$ (for each k).

We can obtain a mixed system of Alice, Bob, Charlie and Dave:

$$\begin{aligned} \rho_{ABCDE} = \frac{1}{4} & \left[|0\rangle_A \langle 0| \otimes |0\rangle_B \langle 0| \otimes |0\rangle_C \langle 0| \otimes |1\rangle_D \langle 1| \left(\sum_{i=0}^3 c_{i,0} |e_i\rangle\langle e_i| \right) \right. \\ & + |0\rangle_A \langle 0| \otimes |0\rangle_B \langle 0| \otimes |1\rangle_C \langle 1| \otimes |0\rangle_D \langle 0| \left(\sum_{i=0}^3 c_{i,1} |e_i\rangle\langle e_i| \right) \\ & + |0\rangle_A \langle 0| \otimes |1\rangle_B \langle 1| \otimes |0\rangle_C \langle 0| \otimes |0\rangle_D \langle 0| \left(\sum_{i=0}^3 c_{i,2} |e_i\rangle\langle e_i| \right) \\ & \left. + |1\rangle_A \langle 1| \otimes |0\rangle_B \langle 0| \otimes |0\rangle_C \langle 0| \otimes |0\rangle_D \langle 0| \left(\sum_{i=0}^3 c_{i,3} |e_i\rangle\langle e_i| \right) \right] \quad (11) \end{aligned}$$

In Case 8 of Step 3, Bob, Charlie, and Dave perform Z basis measurements on the particles, and the measurement results can only be $|1\rangle$ or $|0\rangle$. Based on the post-interaction state of the global system, the probability that each party (Alice, Bob, Charlie, or Dave) obtains a specific measurement outcome is calculated by summing the relevant weights $c_{i,k}$ over the corresponding indicates. For instance, the probability that Alice obtains outcome “0” corresponds to the sum of the weights associated with basis states $|0001\rangle, |0010\rangle$, and $|0100\rangle$ in the joint system. The exact expressions are given in Equations (12)-(19).

Therefore, the probability for Alice, Bob, Charlie, and Dave to obtain $|1\rangle$ or $|0\rangle$ is [31,32]:

$$P_{A_0} = \frac{1}{4} \left(\sum_{i=0}^3 c_{i,0} + \sum_{i=0}^3 c_{i,1} + \sum_{i=0}^3 c_{i,2} \right) \quad (12)$$

$$P_{A_1} = \frac{1}{4} \sum_{i=0}^3 c_{i,3} \quad (13)$$

$$P_{B_0} = \frac{1}{4} \left(\sum_{i=0}^3 c_{i,0} + \sum_{i=0}^3 c_{i,1} + \sum_{i=0}^3 c_{i,3} \right) \quad (14)$$

$$P_{B_1} = \frac{1}{4} \sum_{i=0}^3 c_{i,2} \quad (15)$$

$$P_{C_0} = \frac{1}{4} \left(\sum_{i=0}^3 c_{i,0} + \sum_{i=0}^3 c_{i,2} + \sum_{i=0}^3 c_{i,3} \right) \quad (16)$$

$$P_{C_1} = \frac{1}{4} \sum_{i=0}^3 c_{i,1} \quad (17)$$

$$P_{D_0} = \frac{1}{4} \left(\sum_{i=0}^3 c_{i,1} + \sum_{i=0}^3 c_{i,2} + \sum_{i=0}^3 c_{i,3} \right) \quad (18)$$

$$P_{D_1} = \frac{1}{4} \sum_{i=0}^3 c_{i,0} \quad (19)$$

The above equation, where $\sum_{i=0}^3 c_{i,k} = 1$ for each $K \in \{0, 1, 2, 3\}$, ensuring proper normalization of the conditional mixed states.

When the error rate does not exceed the threshold, Alice's measurement results P_{A_0} and P_{A_1} are approximately equal, and the same applies to Bob, Charlie, and Dave. The Shanno entropy of Bob's system can be expressed as: $H(A) = h(P_{A_0}, P_{A_1}) = 1$. Since Alice can infer Bob's particle state by measuring her own particle, the conditional entropy is: $H(B|A) = 0$, and the mutual information between Alice and Bob is: $I(A:B) = H(B) - H(B|A) = 1$. Furthermore, the mutual information between the eavesdropper Eve and Alice is given by $I(A:E)$. When Bob, Charlie, and Dave perform the CTRL operation on their respective particles, Alice's measurement outcome should be: $|W\rangle_{ABCD}$. Thus, Alice must ensure that:

$$\left(\sum_{i=0}^3 c_{i,0} |e_i\rangle \langle e_i| \right) = \left(\sum_{i=0}^3 c_{i,1} |e_i\rangle \langle e_i| \right) = \left(\sum_{i=0}^3 c_{i,2} |e_i\rangle \langle e_i| \right) = \left(\sum_{i=0}^3 c_{i,3} |e_i\rangle \langle e_i| \right) \quad (20)$$

Otherwise, Alice will detect Eve's interference. However, in this case, the mutual information between Alice and Eve satisfies: $I(A:E) = 0$. Consequently, $I(A:B) > I(A:E)$. This implies that Eve cannot obtain any valuable information through an entanglement-based measurement attack.

4.2.4. Quantum man-in-the-middle attack

Quantum man-in-the-middle attacks (QMIM) refer to a scenario where an adversary, Eve, attempts to impersonate both legitimate parties and establishes separate quantum session with each, thereby gaining access to the key negotiation process. In a standard QKA protocol lacking proper authentication, this type of attack poses a severe threat, as Eve can replace quantum states and deceive both parties.

In our CASQKA protocol, this threat is mitigated through the incorporation of a controlled authentication mechanism. A fully trusted third party, Alice performs identity verification prior to key negotiation. The use of pre-shared identity sequences and the authentication XOR process ensures that each party must prove its identity based on prior registration.

Furthermore, any alteration in the quantum states during the identity authentication phase will increase the observable error rate in Case 1-7 scenarios, which are monitored using Bell-basis and Z-basis measurement. If Eve attempts to interfere or impersonate a legitimate participant, the probability of success without detection is: $P_{success}^{Eve} \leq (1/2)^n$.

Which approaches zero as n increases. Therefore, our protocol is resistant to QMIM attacks under the assumption of a trusted authentication center.

4.2.5. Side-channel attack

Side-channel attacks exploit physical characteristics of communication devices (e.g., power consumption, electromagnetic emissions, timing variations) to extract information. In practical quantum communication systems, hardware imperfections may expose vulnerabilities, enabling adversaries to exploit temporal characteristics such as detector response times, photon arrival time distributions, and synchronization discrepancies to launch time-dependent attacks.

To counter these threats, our protocol adopts a multi-layered defense strategy, including device homogenization through randomized timing delays, physical-layer security design to suppress device-specific signatures, periodic verification of device states to detect anomalous outputs, and incorporation of principles inspired by device-independent approaches to enhance robustness against side-channel attacks [46].

By addressing the gap between theoretical security and practical vulnerabilities, the proposed CASQKA protocol significantly reduces the risk of successful side-channel attacks. Through physical isolation, continuous signal monitoring, and robust communication authentication, combined with the potential integration of scalable measurement-device-independent mechanisms, the protocol demonstrates strong resistance to physical-layer threats and high feasibility for deployment in complex IoT environments requiring enhanced security.

4.2.6. Denial-of-service attack

Denial-of-service attacks (DoS) aim to disrupt protocol execution by flooding the communication channel with invalid particles or jamming signals, thereby preventing participants from completing key agreement.

Our CASQKA protocol is designed with several built-in mechanisms to handle such disruptions: (1) W state robustness: Even if one particle is lost due to an attack, the remaining W state retains partial entanglement, ensuring

that the protocol can still proceed unless multiple losses occur. (2) Session timeout and reinitialization: The protocol defines limits on the number of retries and the time allotted for communication. In case of repeated failures, the system automatically terminates the session and alerts the server. (3) Error-threshold mechanism: During the identity authentication and key agreement phases, the protocol performs continuous error rate verification. If the error exceeds the acceptable threshold, the protocol is terminated early [47].

Therefore, while DoS attacks may hinder temporary communication, they cannot compromise the confidentiality or integrity of the key, nor can they extract meaningful information.

4.2.7. Summary of security analysis

In summary, the proposed CASQKA protocol has strong resistance to various quantum and classical attacks. This design ensures that any unauthorized manipulation or eavesdropping attempts will cause detectable interference, which can be identified through verification steps based on randomly detected particles. In addition, the protocol implements key control properties, ensuring that neither party can unilaterally determine or manipulate the final key. These results confirm that the protocol is both robust and practical for secure communication in semi quantum environments, particularly in the context of IoMT.

5. Performance analysis and simulation

5.1. Simulation

In the simulation process of the protocol, the design of the quantum circuit is crucial. We utilized Qiskit to design the quantum circuit. In Step 3 of Section 3.2, the quantum circuits of eight cases that Bob, Charlie, and Dave can perform are approximately depicted in Figure 4. In these quantum circuits, q_{10} to q_{13} represent the four particles of the W states, which is formed using C-NOT gates, H gates, and Ry gates. To the right of the 5th barrier, Bob, Charlie, and Dave perform operations on q_{11} , q_{12} , and q_{13} , respectively. To the right of the 6th barrier, Alice operates on q_{10} to q_{13} .

(a) Case-1 (CTRL-CTRL-CTRL, eavesdropping-check only)

Alice:

1. Prepares the 4-qubit W state by applying $RY(\pi/4)$ to q_{10} , then three CNOTs with q_{10} as control and q_{11} , q_{12} , q_{13} as targets, and a final $RY(\pi/4)$ on each of q_{11} , q_{12} , q_{13} .
2. Sends q_{11} , q_{12} , q_{13} to Bob, Charlie and Dave, who immediately reflect them without measurement.
3. Upon return, Alice measures all four qubits in the Z basis, computes the error rate and aborts if it exceeds the threshold.

(b) Case-2,3,5 (two CTRL + one SIFT, mixed check)

Identical W-state preparation. Remote action:

The qubit marked SIFT (e.g., q_{11}) is Z-measured, the classical result recorded, a fresh qubit in the same state is prepared and sent back.

The other two qubits are simply reflected. Alice: performs a Bell measurement (CNOT then H followed by Z measurements) on the reflected pair, and a separate Z measurement on the SIFT-returned qubit; results are combined to compute the error rate.

(c) Case-4,6,7 (one CTRL + two SIFT, majority-measure mode) Preparation as above. Remote action:

Two qubits undergo SIFT (measure-resend); one qubit is reflected.

Alice: Bell-measures the reflected qubit together with her retained q_{10} , Z-measures the two SIFT-returned qubits, records the classical bits for later authentication.

(d) Case-8 (SIFT-SIFT-SIFT, key-agreement mode) Preparation unchanged. Remote action:

Bob, Charlie and Dave each SIFT their qubit: Z-measure $\rightarrow$ obtain classical bit $r_i \rightarrow$ XOR with private key $K_i \rightarrow$ permute bit positions according to identity string $I_i \rightarrow$ encode the new classical bit into a fresh $|0\rangle/|1\rangle$ qubit $\rightarrow$ send back to Alice. Alice:

1. Z-measures the three returned qubits to recover the classical bits.
2. Reverses the I_i -based permutation to extract KB, KC, KD.
3. Computes the final shared key $K = K_A \otimes K_B \otimes K_C \otimes K_D$.

Figure 5 illustrates the simulation results of the aforementioned quantum circuit. By comparing Figure 5 with Equation (1) we observe that the measurement results from the simulation consistently correspond to Equation (1), with no erroneous measurement outcomes present in Figure 5. This confirms that the four particles in the protocol

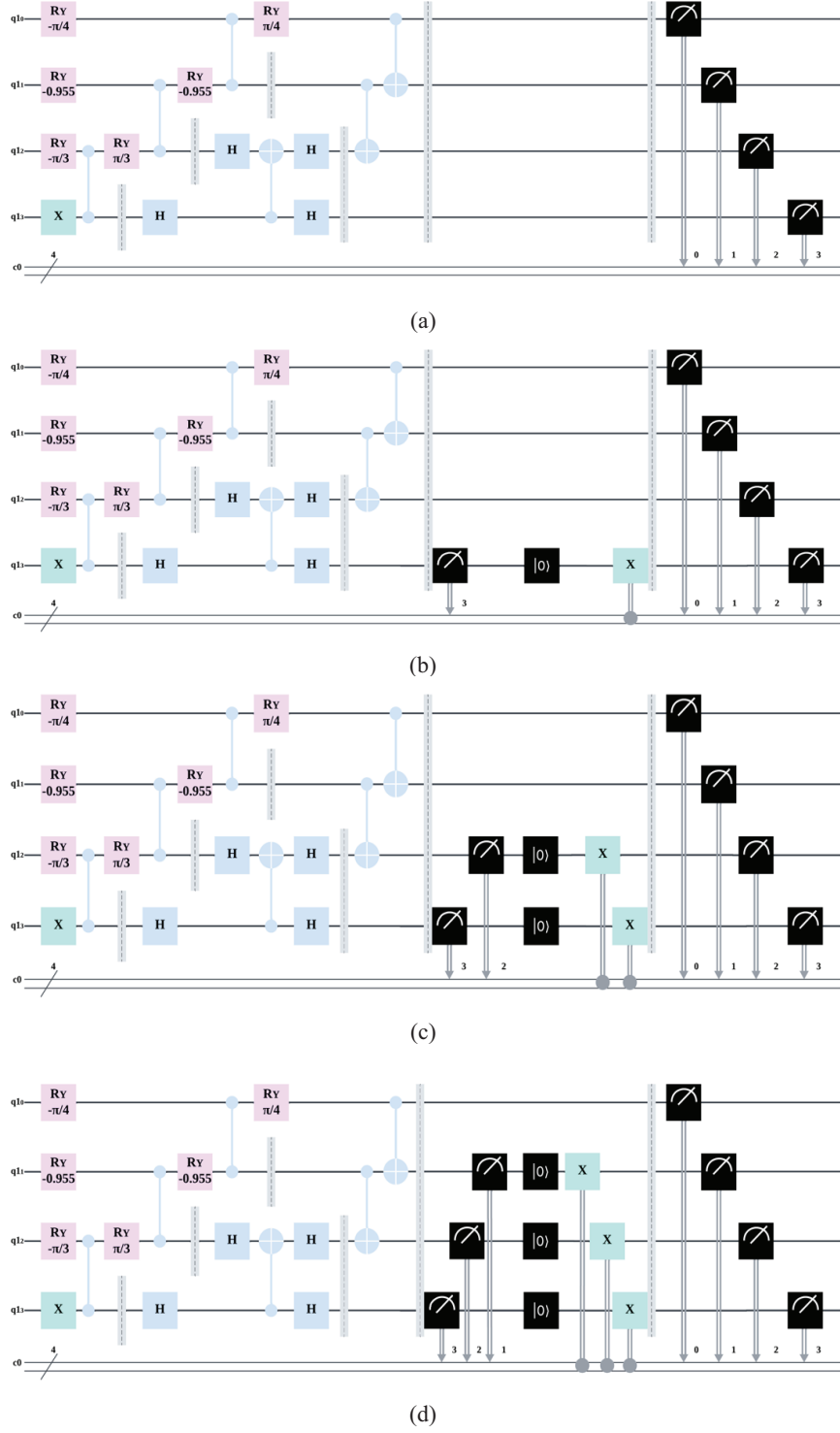


Figure 4. (a) Quantum circuit for case 1 in Table 2. (b) Quantum circuit for case 2 in Table 2 (similar to case 3 and case 5 in Table 2). (c) Quantum circuit for case 4 in Table 2 (similar to case 6 and case 7 in Table 2). (d) Quantum circuit for case 8 in Table 2.

maintain their entanglement characteristics in the W states. Consequently, since our proposed protocol is primarily based on the entanglement properties of the W states, this validates the security of the protocol we have proposed.

5.2. Simulation of protocol in noise channel

We also used Qiskit in Table 4 to simulate the protocol's performance in a noisy environment by introducing two types of quantum noise, which were applied to single-qubit and two-qubit gates, respectively.

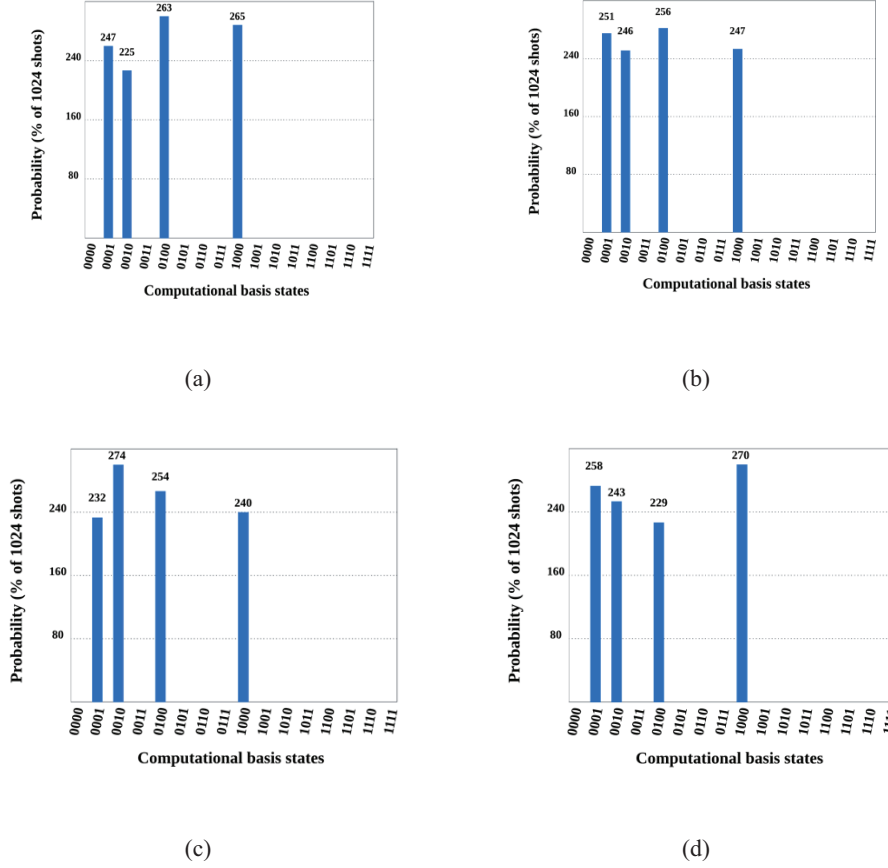


Figure 5. (a) Run results of (a) in Figure 4. (b) Run results of (b) in Figure 4. (c) Run results of (c) in Figure 4. (d) Run results of (d) in Figure 4.

Table 4. Simulation-Experiment Parameter.

Platform	IBM Quantum
Software Development Kit	Qiskit (2.1.1)
Noise parameters (amplitude damping noise, depolarizing noise)	(0.001,0.01) (0.005,0.02) (0.01,0.03) (0.02,0.04)

The single-qubit noise was modeled as amplitude damping noise, which simulates the energy dissipation of a qubit (e.g., spontaneous emission) causing a decay from the excited state $|1\rangle$ to the ground state $|0\rangle$. For instance, after applying an X gate, the qubit initialized in $|0\rangle$ may fail to fully flip to $|1\rangle$ due to noise. This type of noise was applied to all single-qubit gates, including X, H, and RY gates.

The two-qubit noise was modeled as depolarizing noise, which simulates the effect of environmental disturbance that randomly transforms a quantum state into a maximally mixed state (e.g., bit-flip or phase-flip errors). For example, after applying a CX gate, the entanglement between the two qubits may be lost due to noise. This noise was applied to all two-qubit gates, including CX and CZ gates.

Amplitude damping noise is a major source of noise in real quantum hardware, while depolarizing noise is suitable for modeling complex disturbances in multi-qubit operations. Therefore, we selected these two noise models. The noise parameter was set to 0.01, indicating a 1% probability of noise occurrence per gate operation.

According to the measurement results in Figure 6, it can be seen that the target W state still dominates the measurement results. Therefore, our protocol and quantum circuit have a certain robustness to noise.

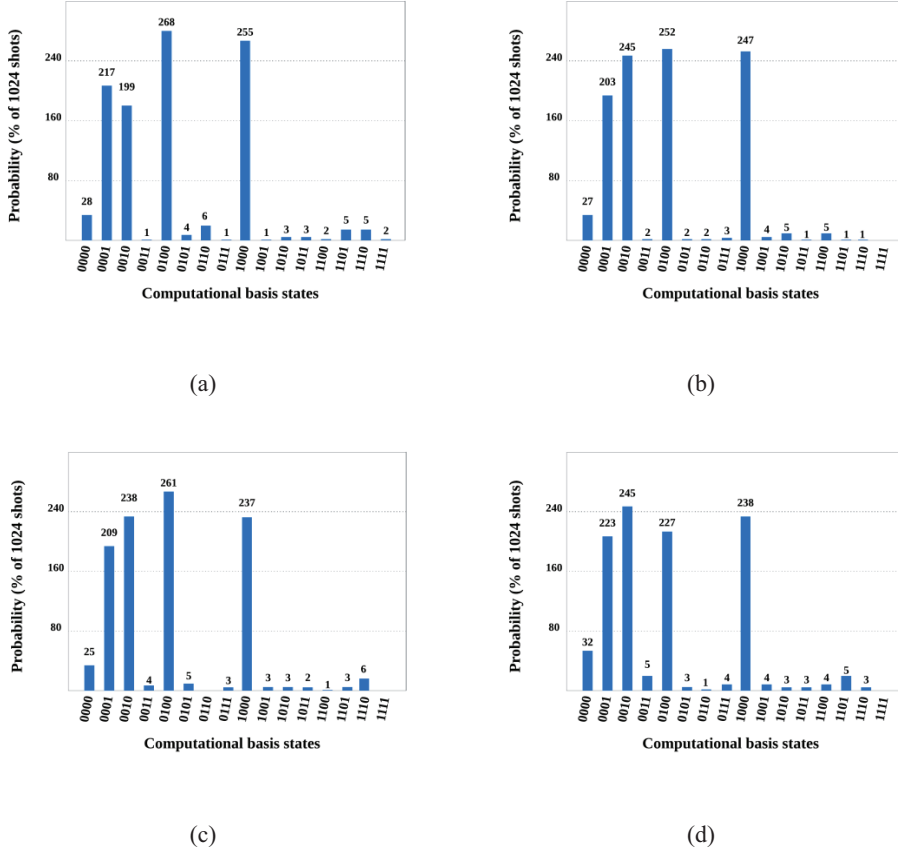


Figure 6. Measurement results of the quantum circuit in Figure 4 under noisy environment.

5.3. Performance analysis

When sharing the key, if preparing one qubit takes time t_1 and the interval between the preparation of two successive qubits is t_2 , the total time required to generate a key of length N is $T = nt_1 + (n - 1)t_2$.

Currently, the performance of quantum key agreement protocols is primarily evaluated using the quantum bit efficiency $\eta = c / (q + b)$ proposed by Cabello [33], where c represents the bit length of the shared key obtained after the protocol is completed, q represents the total number of quantum bits used by the protocol, and b represents the number of classical bits used. In this protocol, the length of the final shared key is $c = n$ bits. Alice prepares $8n$ W states particles, and the particles sent and returned during key negotiation are $6n$ in total, so $q = 8n \times 4 + 6n = 38n$. The total number of classical bits used by Bob, Charlie, and Dave is $3n$, so $b = 3n$. The quantum bit efficiency of this protocol is calculated as $\eta = n / (38n + 3n) = 2.43\%$.

Table 5 presents a comparative analysis of the proposed CASQKA protocol against several existing quantum key agreement protocols in terms of quantum resource, identity authentication, semi-quantum properties, and qubit efficiency. Unlike most existing protocols, which either lack identity authentication or do not support semi quantum capabilities, the proposed protocol achieves both functions simultaneously. This dual capability enhances the applicability of our protocol in scenarios such as IoMT, where resource constrained devices and secure authentication are essential.

Although the qubit efficiency (3.03%) of the proposed protocol is moderate compared to certain high-efficiency protocols such as Ref [22] (53.33%) or Ref [25] (16.67%), it balances functionality and security requirements more comprehensively. Additionally, the use of W states offers robustness against particle loss, which is beneficial in practical noisy environments.

Moreover, the CASQKA protocol has the potential to be extended to support multi-user environments, dynamic participant joining, or even hierarchical key agreement structures in future research. This flexibility makes it a promising candidate for secure communication in emerging quantum-enhanced networks.

In this protocol, Alice is responsible for preparing all quantum states: a total of $8N$ W-states, each built with five single-qubit gates plus three CNOT gates, i.e., eight quantum gates per state. During the authentication phase,

Table 5. Comparison of the proposed CASQKA protocol with other protocols.

Protocol	Quantum resource	Identity authentication function	Semi-quantum properties	Qubit efficiency (%)
Ref. [36]	Cluster states	No	Yes	2.08
Ref. [28]	Cluster states	No	Yes	1.60
Ref. [39]	Five qubit entangled states	Yes	No	7.70
Ref. [40]	Bell states	No	Yes	6.70
Ref. [25]	Bell states	Yes	No	16.67
Ref. [22]	Four-particle GHZ states	Yes	No	53.33
Ref. [49]	Single-particle states	Yes	No	16.67
Ref. [50]	three-particle GHZ-like states	No	Yes	16.67
Proposed protocol	W states	Yes	Yes	2.43

Bob handles three classical strings V_B , I_B and V_B^* —amounting to $3N$ bits. Charlie and Dave perform the same computations, giving another $3N$ each. Alice processes the corresponding strings for all three parties (V_B^* , I_B and V_B^* , etc.), so her related classical data also sum to $9N$. Consequently, the total classical information that must be manipulated in the authentication stage is $18N$ bits.

As shown in Table 5, cluster states cannot be used for identity verification at all. Five-qubit entangled states, four-particle GHZ states, and single-particle states do not permit semi-quantum operation. Bell states support either semi-quantum communication or authentication, but not both simultaneously. Although W-states are more complex to prepare than Bell states, they enable both tasks—authenticated identification and semi-quantum key distribution—in a single scheme.

To investigate the impact of noise on the stability of the protocol, we implement a simulation framework using Qiskit to evaluate the quantum bit error rate (QBER) under various noise conditions. The quantum circuit first prepares a 4-qubit W state and introduces noise models before measurement. Two common types of quantum noise were considered: (1) amplitude damping noise, which models energy dissipation from the system to the environment. (2) depolarizing noise, which captures random transitions of the quantum state into a maximally mixed state. These noise types are representative of dominant errors in current quantum computing hardware.

In our simulations, we select four pairs of noise parameters (P_a, P_d) , where P_a denotes the amplitude damping probability and P_d denotes the depolarizing probability. Specifically, the tested parameter sets were (0.001, 0.01), (0.005, 0.02), (0.01, 0.03), and (0.02, 0.04). For each configuration, the circuit was executed with increasing numbers of measurement shots to collect output distributions, from which the QBER was calculated by comparing with the ideal W state outcomes (i.e., computational basis states with Hamming weight one).

The results are visualized as QBER versus the number of measurement shots. In Figure 7, the notation “Noise Level: P_a, P_d ” indicates the amplitude damping and depolarizing probabilities, respectively. Experimental findings indicate that as the number of particles increases, the QBER gradually decreases and eventually stabilizes. It is noteworthy that under higher noise level conditions (e.g., in the range of 0.02-0.04), the system maintains relatively higher QBER values, while lower noise configurations (e.g., 0.001-0.01) exhibit significantly superior low-error performance.

Based on the aforementioned noise model and the study of quantum bit error rate (QBER), we proceed to investigate the key generation rate (KGR) of the protocol. The estimated formula for the key generation rate is given by:

$$KGR = \max(0, 1 - H(\text{QBER})), \quad (21)$$

where $H(\text{QBER}) = -\text{QBER} \cdot \log_2(\text{QBER}) - (1 - \text{QBER}) \cdot \log_2(1 - \text{QBER})$ is the binary Shannon entropy function, also referred to as the bit entropy function, which quantifies the uncertainty of a single bit. In the simulation, we estimate the final usable key generation rate (KGR) by calculating the QBER from the measurement results and substituting it into the Shannon entropy function.

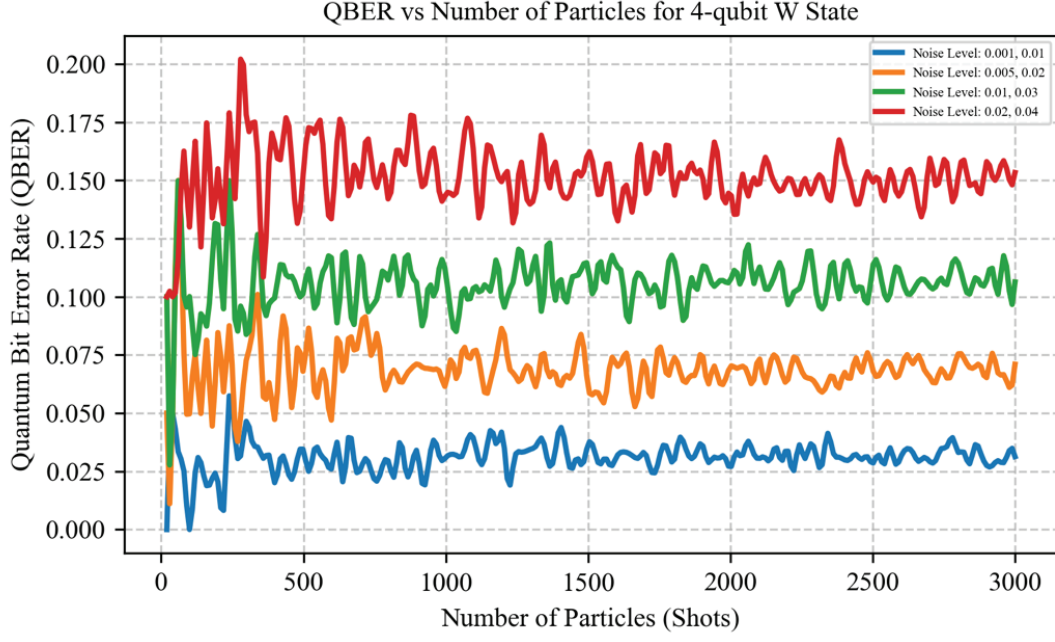


Figure 7. Quantum bit error rate under various noise levels.

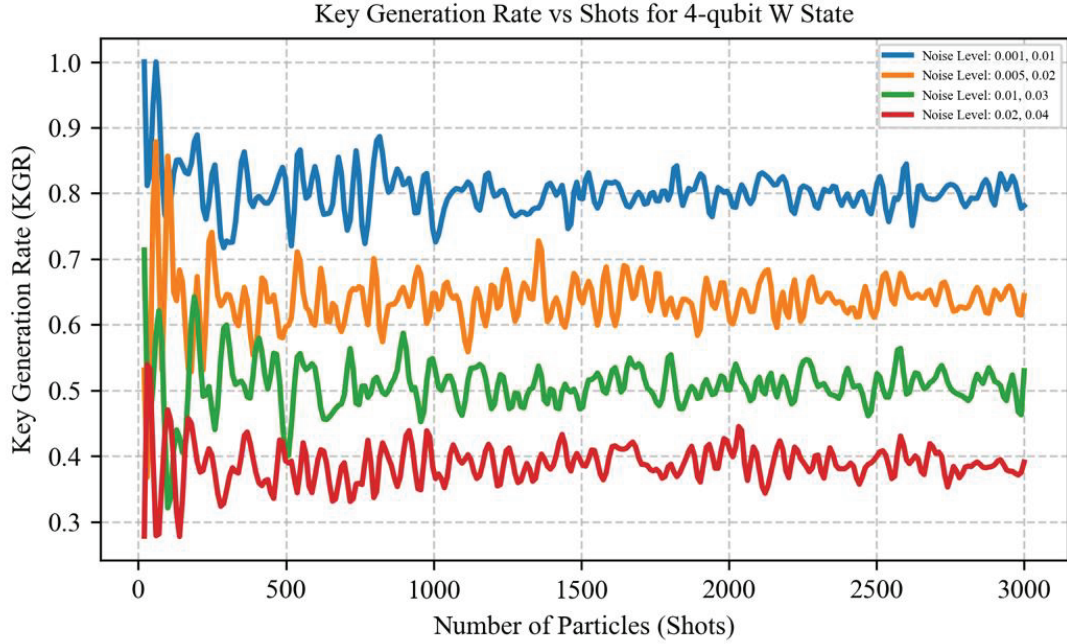


Figure 8. Key generation rate under various noise levels.

Figure 8 illustrates the relationship between the key generation rate and the number of particles (shots) for our protocol under varying noise levels. The results demonstrate that the key generation rate gradually increases with the number of shots and eventually approaches saturation. Notably, as the noise level escalates (e.g., from 0.001 to 0.04), the key generation rate exhibits a declining trend. Under elevated noise conditions (e.g., 0.04), the rate stabilizes at a comparatively lower level (below 0.5).

Next, we compare the communication complexity of the proposed protocol with that of the protocol in Ref [5] (see Table 6 for details). Our proposed CASQKA protocol, as a multiparty semi-quantum key agreement scheme, features both identity authentication and controllability. It is well-suited for systems with strict security requirements and sufficient resources on the controller's side. Although it offers more advanced functionalities, it sacrifices some effi-

Table 6. Communication complexity comparison.

Metric	Proposed protocol	Ref [5]
Quantum communication complexity	$30n$ qubits	n qubits
Classical communication complexity	$3n$ classical bits	$\sim 0.5n$ classical bits
Total communication complexity	$33n$ bits	$1.5n$ bits
Qubit efficiency (η)	3.03%	$\sim 66.67\%$

ciency. In contrast, the protocol in Ref [5] is designed for point-to-point quantum key distribution, making it suitable for simple two-party key distribution scenarios. While its functionality is limited, it achieves optimal efficiency.

6. Discussion

6.1. Limitations of CASQKA and directions for future research

Despite the advantages offered by the proposed controlled authentication semi-quantum key agreement (CASQKA) protocol in terms of security and efficiency within IoMT environments, there are several limitations that warrant further discussion.

First, the protocol assumes the presence of a trusted controller, which may not always be feasible or cost-effective in large-scale or decentralized IoMT systems. The compromise or malfunction of this controller could critically impact the protocol's security.

Second, while the protocol reduces the quantum requirements for semi-quantum participants, it still assumes their ability to perform specific classical operations with high reliability.

Third, the simulation and evaluation of the protocol are performed under idealized noise models. Real-world quantum channels may exhibit more complex or unpredictable noise behavior, which could lead to higher error rates and lower key generation efficiency.

Future work will focus on addressing these challenges through experimental validation, controller decentralization, and adaptive noise-resilient techniques.

6.2. Practical implementation considerations

While the CASQKA protocol demonstrates theoretical feasibility and security, several practical challenges must be addressed to enable deployment in real-world IoMT systems:

Device compatibility: Most IoMT devices, such as wearable sensors and home-use medical instruments, lack full quantum capabilities. Our protocol accommodates this limitation by allowing these devices to operate in a semi-quantum mode, performing only basic classical operations (e.g., SIFT and CTRL). However, implementing even these operations requires the integration of lightweight quantum communication modules, which remains an ongoing engineering challenge.

Interoperability: The IoMT ecosystem comprises heterogeneous devices from multiple manufacturers. To ensure smooth interoperability, standardization of quantum communication interfaces (e.g., encoding rules, authentication formats) is essential. Our protocol is designed to rely on simple and well-defined encoding rules (see Table 1), facilitating integration across diverse device types.

Integration with existing healthcare systems: Deploying CASQKA requires compatibility with traditional electronic health record (EHR) systems, hospital information systems (HIS), and communication infrastructures. This can be achieved by encapsulating the CASQKA protocol within existing network layers as a secure key distribution module, which provides encryption keys to classical protocols (e.g., TLS) used in healthcare data transfer.

Scalability and maintenance: The centralized trusted hospital server must manage entanglement distribution, identity verification, and error rate monitoring. This necessitates robust server-side hardware with quantum-capable interfaces, as well as efficient key management mechanisms. Periodic calibration, channel noise tracking, and synchronization across mobile IoMT nodes are required to maintain long-term system stability.

In summary, while the CASQKA protocol is conceptually well-suited for IoMT, real-world implementation requires careful attention to hardware design, protocol interoperability, and system integration. Future work will explore hardware prototypes and standard interface frameworks for practical deployment.

7. Conclusions

In this paper, we proposed a novel healthcare system framework enhanced by the controlled authentication semi-quantum key agreement (CASQKA) protocol, aimed at strengthening the security of communications within the internet of medical things (IoMT). The new CASQKA protocol introduces a unique combination of identity authentication and semi-quantum capabilities, allowing classical users with limited quantum resources to participate in secure key agreement. This significantly reduces the burden on resource-constrained medical devices while ensuring robust protection against identity impersonation, man-in-the-middle attacks, and various insider and outsider threats.

Our comprehensive security analysis confirms the protocol's resilience in adversarial environments, and the comparative study highlights its advantages over existing protocols, especially in balancing functionality, efficiency, and practicality. By employing W states as quantum resources, the protocol achieves enhanced robustness against qubit loss—an important consideration for real-world deployment.

The integration of the CASQKA protocol into existing healthcare infrastructures holds significant promise. For example, it can be embedded in IoMT ecosystems to secure sensitive communications between patients, wearable sensors, and medical service providers, thereby improving data privacy, trust, and system reliability. The protocol's lightweight requirements make it particularly suitable for large-scale, decentralized deployments across hospital networks and personal health monitoring systems.

In future work, we plan to investigate the deployment of CASQKA in more complex multi-user and hierarchical communication models. We also aim to implement and simulate the protocol in realistic healthcare scenarios to assess its performance under various network conditions. These efforts will further bridge the gap between theoretical development and practical application, paving the way for secure, scalable, and quantum-resilient healthcare communication systems.

The protocol currently assumes that the third party, Alice, is fully trusted. Future work could explore scenarios where Alice is only semi-trusted, thereby enhancing the protocol's practical applicability and aligning it with more realistic deployment environments.

Author Contributions

Yefeng He: conceptualization, security analysis, and overall supervision of the paper. Liaoyuan Shen: primary writing, performance analysis and writing review & editing. Yichi Zhang: protocol design, simulation, figure plotting, and table preparation. All authors have read and agreed to the published version of the manuscript.

Funding

National Natural Science Foundation of China (61802302); Basic Research Project of Natural Science of Shaanxi Province (2021JM-462).

Conflicts of Interest

Please state conflicts of interest or add The authors declare no conflicts of interest. Author declares no conflict of interest.

Data Availability Statement

Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. A. Ghubaish, T. Salman, M. Zolnvari, et al. (2022). "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet Things J.*, **8**(11), 8707–8718. DOI:10.1109/JIOT.2020.3045653
2. S. Razdan and S. Sharma (2022). "Internet of medical things (IoMT): Overview, emerging technologies, and case studies," *IETE Tech Rev.*, **39**(4), 775–788. DOI:10.1080/02564602.2021.1927863
3. D. Koutras, G. Stergiopoulos, T. Dasaklis, et al. (2020). "Security in IoMT communications: A survey," *Sensors*, **20**(17), 4828. DOI:10.3390/s20174828
4. W. K. Wootters and W. H. Zurek (1982). "A single quantum cannot be cloned," *Nature*, **299**(5886), 802–803. DOI: 10.1038/299802a0
5. C. H. Bennett and G. Brassard (1984). "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE)*, pp. 175–179. DOI: <https://doi.org/10.1016/j.tcs.2014.05.025>
6. Y. Cao, Y. Zhao, Q. Wang, et al. (2022). "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surv. Tut.*, **24**(2), 839–894. DOI:10.1109/COMST.2022.3144219

7. M. Mehic, M. Niemiec, S. Rass, et al. (2020). "Quantum key distribution: A networking perspective," *ACM Comput. Surv.*, **53**(5), 1–41. DOI:10.1145/3402192
8. W. Z. Liu, Y. Z. Zhang, Y. Z. Zhen, et al. (2022). "Toward a photonic demonstration of device-independent quantum key distribution," *Phys. Rev. Lett.*, **129**(5), 050502. DOI: 10.1103/PhysRevLett.129.050502
9. S. Lin, X. Zhang, G. D. Guo, et al. (2021). "Multiparty quantum key agreement," *Phys. Rev. A*, **104**(4), 042421. DOI: 10.1103/PhysRevA.104.042421
10. L. Li and Z. Li (2020). "A verifiable multiparty quantum key agreement based on bivariate polynomial," *Inf. Sci.*, **521**, 343–349. DOI: <https://doi.org/10.1016/j.ins.2020.02.057>
11. A. Shen, X. Y. Cao, Y. Wang, et al. (2023). "Experimental quantum secret sharing based on phase encoding of coherent states," *Sci China Phys. Mech. Astron.*, **66**(6), 260311.
12. Y. Tian, J. Li, X. B. Chen, et al. (2021). "An efficient semi-quantum secret sharing protocol of specific bits," *Quantum Inf. Process.*, **20**(6), 217.
13. Q. Liao, H. Liu, L. Zhu, et al. (2021). "Quantum secret sharing using discretely modulated coherent states," *Phys. Rev. A*, **103**(3), 032410. DOI: 10.1103/PhysRevA.103.032410
14. N. R. Zhou, Q. D. Xu, N. S. Du, et al. (2021). "Semi-quantum private comparison protocol of size relation with d-dimensional Bell states," *Quantum Inf. Process.*, **20**, 1–15.
15. L. Z. Jiang (2020). "Semi-quantum private comparison based on Bell states," *Quantum Inf. Process.*, **19**(6), 180.
16. L. Yan, S. Zhang, Y. Chang, et al. (2021). "Semi-quantum private comparison protocol with three-particle G-like states," *Quantum Inf. Process.*, **20**, 1–16.
17. N. Zhou, G. Zeng and J. Xiong (2004). "Quantum key agreement protocol," *Electron. Lett.*, **40**(18), 1. DOI: 10.1049/el:20045183
18. T. J. Xu, Y. Chen, M. J. Geng, et al. (2022). "Single-state multi-party semi-quantum key agreement protocol based on multi-particle GHZ entangled states," *Quantum Inf. Process.*, **21**(7), 266.
19. H. Yang, S. Lu, Q. Zhou, et al. (2024). "Efficient single-state multi-party quantum key agreement," *Quantum Inf. Process.*, **23**(4), 150.
20. A. Elhadad, S. Abbas, H. Abulkasim, et al. (2020). "Improving the security of multi-party quantum key agreement with five-qubit Brown states," *Comput. Commun.*, **159**, 155–160.
21. Y. F. He and W. P. Ma (2016). "Two-party quantum key agreement against collective noise," *Quantum Inf. Process.*, **15**(12), 5023–5035.
22. Y. F. He, Y. R. Yue and M. Di (2022). "Two-party mutual authentication quantum key agreement protocol," *Int. J. Theor. Phys.*, **61**(1), 145.
23. C. Shukla, K. Thapliyal and A. Pathak (2017). "Semi-quantum communication: Protocols for key agreement, controlled secure direct communication, and dialogue," *Quantum Inf. Process.*, **16**, 295. DOI: <https://doi.org/10.1007/s11128-017-1736-2>
24. A. Dutta and A. Pathak (2023). "Collective attack free controlled quantum key agreement without quantum memory," *arXiv preprint arXiv:2308.05470*. DOI: <https://doi.org/10.1088/1402-4896/adaa30>
25. Y. F. He, Y. B. Pang and M. Di (2022). "Mutual authentication quantum key agreement protocol based on Bell states," *Quantum Inf. Process.*, **21**, 290.
26. Y. F. He, X. Y. Liang and M. Y. Cai (2024). "Two-party mutual authentication semi-quantum key agreement protocol based on Bell states," *Acta Opt. Sin.*, **05**, 261–268.
27. M. Boyer, D. Kenigsberg and T. Mor (2007). "Quantum key distribution with classical Bob," in *2007 First International Conference on Quantum, Nano, and Micro Technologies* (IEEE), pp. 10-10. DOI: <https://doi.org/10.1103/PhysRevLett.99.140501>
28. Y. F. He, Y. B. Pang, M. Di, et al. (2023). "Four-party semi-quantum key agreement protocol based on four-particle cluster states," *Acta Opt. Sin.*, **43**(20), 271–277.
29. Y.F. He, J.Q. Fan and Y.C. Zhang (2025). "Controlled quantum authentication confidential communication protocol for smart healthcare," *Sci. Rep.*, 15.
30. D. Damodaran, S. Damodaran, N. Dharini, et al. (2024). "Towards a novel privacy-preserving distributed multi-party data outsourcing scheme for cloud computing with quantum key distribution," *arXiv*.
31. W. Dür, G. Vidal and J. I. Cirac (2000). "Three qubits can be entangled in two inequivalent ways," *Phys. Rev. A*, **62**(6), 062314. DOI: <https://doi.org/10.1103/PhysRevA.62.062314>
32. R. Hamzehof, M. Ashrafpour and D. Afshar (2025). "Genuine entanglement and quantum coherence of a multi-partite W state in non-inertial frames," *Eur. Phys. J. Plus*, **140** (10), 986.

33. Y.Liu (2023). “Decoherence-free subspace and entanglement sudden death of multi-photon polarization states in fiber channels,” *Commun. Theor. Phys.*, 75 (4), 045104.
34. C. Peikert (2016). “A Decade of Lattice Cryptography,” *Found. Trends Theor. Comput. Sci.*, 10, 283–424. DOI: <https://doi.org/10.1561/04000000074>
35. Q. Y. Cai (2006). “Eavesdropping on the two-way quantum communication protocols with invisible photons,” *Phys. Lett. A*, **351**(1-2), 23–25. DOI: <https://doi.org/10.1016/j.physleta.2005.10.050>
36. N. R. Zhou, K. N. Zhu and Y. Q. Wang (2020). “Three-party semi-quantum key agreement protocol,” *Int. J. Theor. Phys.*, **59**, 663–676.
37. L. Y. Chen, L. H. Gong and N. R. Zhou (2020). “Two semi-quantum key distribution protocols with G-like states,” *Int. J. Theor. Phys.*, **59**, 1884–1896.
38. A. Cabello (2000). “Quantum key distribution in the Holevo limit,” *Phys. Rev. Lett.*, **85**(26), 5635. DOI: <https://doi.org/10.1103/PhysRevLett.85.5635>
39. X. Ma, J. Hur, Z. Li and H. Zhu (2021). “Quantum mutual authentication key agreement scheme using five-qubit entangle ment towards different realm architecture,” *Int. J. Theor. Phys.*, **60**(5), 1933–1948.
40. L. Yan, S. Zhang, Y. Chang, et al. (2019). “Semi-quantum key agreement and private comparison protocols using Bell states,” *Int. J. Theor. Phys.*, **58**, 3852–3862.
41. R. Loura, Á. J. Almeida, P. S. André, et al., “Noise and measurement errors in a practical two-state quantum bit commitment protocol,” *Phys. Rev. A*, **89**, 052336 (2014). DOI: <http://dx.doi.org/10.1103/PhysRevA.89.052336>
42. A. Cabello, “N-particle N-level singlet states: Some properties and applications,” *Phys. Rev. A*, **66**, 042314 (2002). DOI: <https://doi.org/10.1103/physrevlett.89.100402>
43. J. Gao, L. Santos, G. Krishna, et al. (2023). “Scalable generation and detection of on-demand W states in nanophotonic circuits,” *Nano Lett.*, **23**(11), 5350–5357. DOI: <https://doi.org/10.1021/acs.nanolett.3c01551>
44. H. Häffner, W. Hänsel, C. Roos, et al. (2005). “Scalable multiparticle entanglement of trapped ions,” *Nature*, **438**, 643–646. DOI: <https://doi.org/10.1038/nature04279>
45. Y. F. He, X. J. Wei, M. Di, et al. (2021). “Quantum key agreement with higher-dimensional Bell states,” *Quantum Inf. Process.*, **20**(4), 103.
46. S. Hoque, A. Aydeger and E. Zeydan (2024). “Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design,” *Proc. 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, 9–16. DOI: <https://doi.org/10.48550/arXiv.2404.10602>
47. H. T. Li, Y. R. Zhang, X. J. Wang, et al. (2019). “Device-independent quantum key distribution based on entangled states,” *Quantum Inf. Comput.*, **19**(3), 221–238.
48. T. K. Ng, W. K. Wong, C. S. Tsai, et al. (2021). “Quantum protocols for multi-party secure communication,” *Phys. Lett. A*, **383**(12), 1631–1637.
49. M. S. Zhan, S. K. Zhang, R. M. Lin, et al. (2023). “Quantum semi-communication protocols and their security analysis,” *Quantum Inf. Comput.*, **21**(6), 450–467.
50. Chun-Wei Yang, Yu-Yun Huang, Jason Lin, et al. (2024). “Efficient and secure semi-quantum private comparison protocol using three-particle GHZ-like states against participant attack,” *Modern Physics Letters A*, Vol.39, No.10, 2450037. DOI: <https://doi.org/10.1142/S0217732324500378>
51. **S. Prajapat, P Kumar and S. Kumar** (2024). “A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks.” *Cluster Computing*, 1-17.