sensors

IMPACT FACTOR 3.4

Indexed in: PubMed

CITESCORE 7.3

Article

Quantum Privacy-Preserving Range Query Protocol for Encrypted Data in IoT Environments

Chong-Qiang Ye, Jian Li and Xiao-Yu Chen

Special Issue
IoT Network Security (Second Edition)

Edited by
Prof. Dr. Jian Li

MDPI

https://doi.org/10.3390/s24227405

sensors

MDPI

Article

Quantum Privacy-Preserving Range Query Protocol for Encrypted Data in IoT Environments

Chong-Qiang Ye [1], Jian Li [2,*] and Xiao-Yu Chen [1]

[1] School of Information and Electrical Engineering, Hangzhou City University, Hangzhou 310015, China; chongqiangye@bupt.edu.cn (C.-Q.Y.); chenxiaoyu@hzcu.edu.cn (X.-Y.C.)
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: lijian@bupt.edu.cn

Abstract: With the rapid development of IoT technology, securely querying sensitive data collected by devices within a specific range has become a focal concern for users. This paper proposes a privacy-preserving range query scheme based on quantum encryption, along with circuit simulations and performance analysis. We first propose a quantum private set similarity comparison protocol and then construct a privacy-preserving range query scheme for IoT environments. By leveraging the properties of quantum homomorphic encryption, the proposed scheme enables encrypted data comparisons, effectively preventing the leakage of sensitive data. The correctness and security analysis demonstrates that the designed protocol guarantees users receive the correct query results while resisting both external and internal attacks. Moreover, the protocol requires only simple quantum states and operations, and does not require users to bear the cost of complex quantum resources, making it feasible under current technological conditions.

Keywords: quantum communication; range query; privacy protection; IoT security

Citation: Ye, C.-Q.; Li, J.; Chen, X.-Y. Quantum Privacy-Preserving Range Query Protocol for Encrypted Data in IoT Environments. *Sensors* **2024**, *24*, 7405. https://doi.org/10.3390/s24227405

Academic Editor: Alessandra Rizzardi

Received: 13 October 2024
Revised: 9 November 2024
Accepted: 19 November 2024
Published: 20 November 2024

1. Introduction

The Internet of Things (IoT) is a cutting-edge technology [1] that seamlessly integrates physical devices into the digital world, creating a network capable of real-time monitoring, control, and automation. It has profoundly reshaped interactions with technology and the management of resources and is continually impacting our daily lives.

IoT systems or environments typically have the following characteristics: (1) a large number of devices: IoT systems consist of a large number of interconnected devices, ranging from simple sensors to complex processing units; (2) a dynamic and distributed nature: IoT environments are highly dynamic, with devices constantly joining, leaving, or moving within the network; (3) security and privacy: Security and privacy protection are critical issues in IoT environments. Since IoT devices often collect large amounts of sensitive data (such as personal health information, location data, etc.), special attention is required for the secure storage, transmission, and processing of such data.

Ensuring data security while enabling meaningful analysis is a critical issue in IoT ecosystems [2]. As a result, there is a growing need for privacy-preserving data processing techniques that can perform complex queries on sensitive data without compromising individual privacy. Among the various types of queries that are central to IoT applications, range queries, which retrieve data that fall within a specific range, are particularly important [3,4]. For example, in smart city management, range queries can be used for environmental monitoring, e.g., to query air quality sensor data in a certain area, or to query temperature changes in multiple areas over a specific time period. These data can help city managers optimize resource allocation and emergency responses. However, executing range queries on unencrypted data can lead to the exposure of sensitive information, making privacy protection a critical concern.

To address these challenges, privacy-preserving range query techniques have emerged as a powerful solution [5–8]. In these privacy-preserving scenarios, the querying user does not reveal the specific range of the query, and the data owner does not disclose any individual element to others, except for the queried data. To illustrate the concept of privacy-preserving range queries, let us consider a typical scheme described in Ref. [8]. In this protocol, there are m data owners (e.g., IoT devices) and one query user. Each data owner D_i has privacy data: w_i within the range $[1, n]$. The query user wants to know "What is the sum of the elements with indices in the range/interval $[l, u]$? where $1 \leq l < u \leq n$". In this specific example, the query user's range, $[l, u]$, is kept confidential, and the data owner's w_i will not be disclosed to others. Moreover, in addition to sum queries within a privacy-preserving range, queries for the maximum or minimum value are also frequently required in IoT applications. S. Sciancalepore et al. [9] and M. Zhou et al. [10] implemented privacy-preserving range query protocols for finding maximum or minimum values in IoT systems. These protocols utilize classical encryption techniques, such as homomorphic encryption [11], privacy comparison, and other algorithms.

However, traditional cryptographic protocols, which are based on mathematically hard problems, are increasingly vulnerable to the power of quantum computing. The emergence of quantum algorithms, such as Shor's algorithm [12], poses a significant threat to the security of classical encryption schemes, indirectly compromising the data security of the IoT ecosystem. In contrast, quantum cryptographic protocols [13–15] are inherently resistant to quantum attacks, providing long-term security assurances even in the presence of quantum adversaries. In 2023, based on quantum multiparty computing XOR and quantum privacy query, Shi et al. [16] designed a quantum-based privacy-preserving range query scheme. By integrating quantum cryptography with classical IoT systems, this method significantly enhances the security of traditional range query applications. In 2024, Shi et al. [17] proposed a quantum-based privacy-preserving range MAX/MIN query scheme, leveraging quantum private query and quantum oblivious set inclusion protocols. Their approach effectively ensures the privacy of both the query range and the query results. In summary, classical encryption-based privacy-preserving range query protocols may be easier to implement in the short term, but their security could be compromised as quantum computing advances, offering only short-term security. On the other hand, quantum encryption-based solutions, which leverage the principles of quantum encryption, offer long-term security by resisting attacks from quantum computers. However, it is important to note that research on quantum solutions is still in its early stages. Integrating quantum encryption technologies into IoT systems requires further investigation, and its implementation faces higher costs and challenges compared to classical solutions.

1.1. Motivation

The primary motivations for proposing the scheme in this paper are as follows:

- Given the rapidly increasing computational power, quantum cryptographic protocols have the potential to become a preferred solution for safeguarding the vast amounts of sensitive data generated by IoT devices. To the best of our knowledge, only Shi et al. [16,17] have proposed two relevant schemes suitable for IoT environments. This is clearly insufficient to meet the growing security demands. *Thus, there is a clear need to explore further integration of quantum encryption technologies within IoT systems.*
- Quantum homomorphic encryption (QHE) [18,19] is an advanced encryption technology that combines the principles of quantum computing with homomorphic encryption. Similar to classical homomorphic encryption, QHE allows computations to be performed directly on encrypted data without the need for decryption. In classical privacy-preserving range queries, homomorphic encryption is a key component. *However, there is currently no solution that employs quantum homomorphic encryption to address privacy-preserving range queries.*

These motivation inspired us to design a quantum-based privacy-preserving range query protocol for IoT systems.

1.2. Research Contributions

In this paper, we present a quantum privacy-preserving range query protocol for IoT environments. The design of the proposed scheme was inspired by the research findings of [17,20]. With the help of a semi-honest quantum cloud server, users can perform range queries on the data owners, such as edge servers. The proposed protocol employs QHE, ensuring that the quantum cloud server processes only encrypted data, thereby safeguarding sensitive information within the IoT system. The main contributions are summarized as follows.

(1) We propose a privacy set similarity comparison protocol based on quantum homomorphic encryption, which allows for the comparison of encrypted data.
(2) Based on the proposed privacy set similarity comparison protocol, we further give a feasible quantum privacy-preserving range query protocol for IoT environments.
(3) The quantum circuits corresponding to the proposed protocol are presented, and their feasibility is validated through simulation.

1.3. Organization

The rest of this paper is organized as follows. Section 2 briefly overviews the quantum resources utilized in this approach. Section 3 outlines the detailed steps of the proposed protocol. In Section 4, we discuss the protocol's correctness and present circuit simulation results. Section 5 covers the security analysis. Finally, the discussion and conclusions are presented in Sections 6 and 7.

2. Preliminaries

In this section, we provide an overview of the quantum resources to be used in this paper, including basic quantum gates and quantum homomorphic encryption.

2.1. Basic Quantum Gates

In quantum systems, quantum gates are the fundamental building blocks used to manipulate qubits. Below is an introduction to some of the basic quantum gates.

(1) Pauli Gate (X, Y, Z Gate): Pauli gates form a set of fundamental single-qubit gates that correspond to classical bit flips and phase flips.
X Gate (bit-flip gate): Similar to the classical NOT gate, it flips $|0\rangle$ to $|1\rangle$ and vice versa.
Y Gate: It both performs a bit flip and introduces a phase change. It maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$.
Z Gate (phase-flip gate): This gate only changes the phase of the qubit. It multiplies the $|1\rangle$ state by -1, while leaving $|0\rangle$ unchanged.
(2) Hadamard Gate (H Gate): The Hadamard gate is one of the most commonly used single-qubit gates. It maps $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$, $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$ and vice versa.
(3) CNOT Gate (Controlled-NOT Gate): The CNOT gate is a two-qubit gate where one qubit acts as the control and the other as the target. If the control qubit is $|1\rangle$, the target qubit undergoes an X gate operation (bit flip); if the control qubit is $|0\rangle$, the target qubit remains unchanged.

2.2. Quantum Homomorphic Encryption

Quantum homomorphic encryption (QHE) is a cryptographic technique that allows computations to be performed directly on encrypted quantum data, without the need for decryption [18,19]. This capability is essential in privacy-preserving quantum computing, where a client wishes to delegate computations to a quantum server while maintaining the confidentiality of the underlying data.

The main advantage of QHE is that the server never learns anything about the input quantum data, intermediate states, or the final result, thus ensuring the confidentiality of the computation. Generally, a QHE scheme involves four stages:

- **Key Generation.** $QHE.KeyGen$: $1^\kappa \rightarrow (pk, sk, \rho_{evk})$. This process takes the unary representation of the security parameter as input and generates the classical keys pk and sk, along with a quantum evaluation key ρ_{evk} as output.
- **Encryption.** $QHE.Enc_{pk}$: $D(\mathcal{M}) \rightarrow D(\mathcal{C})$. This process uses the key pk to transform the message space $\mathcal{M}$ into the cipherspace $\mathcal{C}$.
- **Evaluation.** $QHE.Eval^{QC}_{\rho_{evk}}$: $D(\mathcal{C}) \rightarrow D(\mathcal{C}')$. Based on the evaluation key ρ_{evk}, a quantum evaluation circuit QC is applied to the ciphertext $\mathcal{C}$, and then it produces a new quantum ciphertext state $\mathcal{C}'$.
- **Decryption.** $QHE.Dec_{sk}$: $D(\mathcal{C}') \rightarrow \rho$. Using the private key sk, the ciphertext $\mathcal{C}'$ is decrypted to recover the plaintext state ρ, where ρ represents the output of the quantum evaluation circuit applied to the original plaintext $D(\mathcal{M})$.

QHE can be categorized into two main types: limited and fully homomorphic encryption. Limited QHE supports a restricted set of quantum operations, usually within the Clifford group, which can be easily implemented on encrypted data. Fully quantum homomorphic encryption (FQHE), on the other hand, supports arbitrary quantum operations, but it is still challenging to realize practical FQHE, due to the difficulty of implementing non-Clifford gates such as the T gate in an encrypted form. This paper focuses on the quantum homomorphic encryption of the CNOT gate, which is a member of the Clifford group.

The homomorphic encryption process for the CNOT gate can be summarized as follows: First, the quantum encryption key is established through a key generation process, where parameters α and β ($\alpha, \beta \in \{0,1\}^n$) belong to the key pk. Next, the quantum states $|\phi_k\rangle$ and $|\psi_l\rangle$ are encrypted using $X^{\alpha_k}Z^{\beta_k}$ and $X^{\alpha_l}Z^{\beta_l}$, respectively, resulting in encrypted quantum states that ensure confidentiality during transmission. The encrypted quantum states $X^{\alpha_k}Z^{\beta_k}|\phi_k\rangle$ and $X^{\alpha_l}Z^{\beta_l}|\psi_l\rangle$ are then sent to the quantum server, where the server performs the homomorphic evaluation of the CNOT gate directly on the encrypted states, ensuring the privacy of the data. Finally, the decryption operation is performed using the key sk (i.e., $\alpha_k, \beta_k \oplus \beta_l, \alpha_k \oplus \alpha_l, \beta_l$), and the corresponding quantum state is measured to obtain the final result. The whole process is also shown in Equation (1):

$$\begin{aligned} &\xrightarrow{\text{key generation}} (\alpha_k, \beta_k), (\alpha_l, \beta_l) \\ &\xrightarrow{\text{encryption}} (X^{\alpha_k}Z^{\beta_k} \otimes X^{\alpha_l}Z^{\beta_l})|\phi_k\rangle|\psi_l\rangle \\ &\xrightarrow{\text{CNOT}} (X^{\alpha_k}Z^{\beta_k \oplus \beta_l} \otimes X^{\alpha_k \oplus \alpha_l}Z^{\beta_l})|\phi_k\rangle|\phi_k \oplus \psi_l\rangle \\ &\xrightarrow{\text{decryption}} |\phi_k\rangle, |\phi_k \oplus \psi_l\rangle \end{aligned} . \tag{1}$$

3. Protocol Description

In this section, we first give a QHE-based privacy set similarity comparison scheme. Then, a privacy-preserving range query scheme is provided based on the designed privacy set comparison method.

3.1. Quantum Privacy Set Similarity Comparison Protocol Based on QHE

Before initiating the protocol, let us first introduce the basic requirements of the protocol. This protocol involves three participants: the server, Alice; the client, Bob; and a quantum cloud third party (TP). Alice and Bob each possess a private set, denoted as $S_A = \{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{Z}_N$ and $S_B = \{y_1, y_2, \ldots, y_m\} \subseteq \mathbb{Z}_N$, respectively. With the assistance of TP, they aim to compare their private sets' similarity using quantum homomorphic encryption based on CNOT gates.

In this paper, we utilize the Jaccard similarity [21] to measure the similarity between the two sets, which is defined as

$$J = \frac{|S_A \cap S_B|}{|S_A \cup S_B|}. \tag{2}$$

The detailed protocol step is described below.

1. Privacy set encoding phase: Alice and Bob encode their respective private datasets, transforming them into quantum state sequences.

Step 1-1: Alice and Bob execute a quantum key distribution protocol [22] to establish an integer key $k \subseteq \mathbb{Z}_N$. Then, the sets of S_A and S_B are transformed into specific privacy vectors: $S_A* = \{kx_1 \bmod N, kx_2 \bmod N, \ldots, kx_n \bmod N\}$ and $S_B* = \{ky_1 \bmod N, ky_2 \bmod N, \ldots, ky_m \bmod N\}$. The transformation above merely applies a uniform modular multiplication to the elements of sets S_A and S_B, without altering the intersection or union relationships between the two sets or the size of the set.

Step 1-2: using the sets S_A* and S_B*, Alice and Bob generate respective quantum sequences $(|A_0\rangle, |A_1\rangle, \ldots, |A_{N-1}\rangle)$ and $(|B_0\rangle, |B_1\rangle, \ldots, |B_{N-1}\rangle)$ in the following manner:

$$\begin{aligned} |A_i\rangle &= |0\rangle, \quad \text{if } i \notin S_A*, \qquad |A_i\rangle = |1\rangle, \quad \text{if } i \in S_A*, \\ |B_i\rangle &= |0\rangle, \quad \text{if } i \notin S_B*, \qquad |B_i\rangle = |1\rangle, \quad \text{if } i \in S_B*, \end{aligned} \tag{3}$$

where $i = 0, 1, \ldots, N-1$. It should be noted that after the encoding phase, the number of $|1\rangle$ in the quantum state sequences prepared by each Alice and Bob is n and m, respectively, which is consistent with the original set size.

2. Key generation phase: TP, Alice, and Bob execute the quantum secret sharing protocol to establish the key relationship.

Step 2-1: TP first prepares $8N + \delta$ Bell states, with each Bell state randomly belonging to either the $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. TP then uses R_j^T to record the different types of Bell states prepared. If the j-th Bell state is $|\Phi\rangle$, then $R_j^T = 0$; otherwise, if it is a $|\Psi\rangle$ state, $R_j^T = 1$. After that, TP splits these Bell states into two particle sequences, T_A and T_B, which are subsequently sent to Alice and Bob.

Step 2-2: For the received qubits, Alice and Bob randomly perform Z-basis (i.e., $\{|0\rangle, |1\rangle\}$) measurements or X-basis (i.e., $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$) measurements.

Step 2-3: Alice and Bob randomly select δ qubits as test qubits to perform a security check. They first instruct TP to reveal the type of Bell state for these test particles, namely whether they are in the $|\Phi\rangle$ or $|\Psi\rangle$ state. Based on the measurement basis and the corresponding outcomes, Alice and Bob can assess the security of the transmission and verify whether TP has prepared the Bell states as required by the protocol. The focus here is on the case where Alice and Bob choose the same measurement basis. The relationship between the measurement basis and the results is summarized in Table 1.

If the error rate of any of the eight cases in Table 1 exceeds the threshold, the protocol will terminate and restart. Otherwise, proceed to the next step.

Step 2-4: After confirming the security of the channel and verifying that TP has correctly prepared the Bell states as required, Alice and Bob select the particles on which they both performed Z-basis measurements (e.g., the two particles in the j-th Bell state). The corresponding measurement results are recorded as R_j^A and R_j^B, respectively. Correspondingly, Alice and Bob will also tell TP the position of the selected particle.

Step 2-5: TP, Alice, and Bob can establish a key relationship based on R_j^T, R_j^A, and R_j^B. Based on the properties of the Bell states $|\Psi\rangle$ and $|\Phi\rangle$, it can be easily derived that

$$R_j^T = R_j^A \oplus R_j^B, \tag{4}$$

where R_j^T is the Bell state type recorded in Step 2-1 (also see cases 1, 2, 5, and 6 of Table 1).

It is important to highlight that in this phase, TP only has access to the XOR result of R_j^A and R_j^B, without the ability to retrieve the individual values of R_j^A or R_j^B independently.

Table 1. Results corresponding to different types of Bell states and measurement bases.

Case	Bell State Type R_j^T	Measurement Basis of Alice	Measurement Basis of Bob	Alice's Results R_j^A	Bob's Results R_j^B
1	$\|\Phi\rangle$, $R_j^T = 0$	Z-basis	Z-basis	$\|0\rangle$	$\|0\rangle$
2	$\|\Phi\rangle$, $R_j^T = 0$	Z-basis	Z-basis	$\|1\rangle$	$\|1\rangle$
3	$\|\Phi\rangle$, $R_j^T = 0$	X-basis	X-basis	$\|+\rangle$	$\|+\rangle$
4	$\|\Phi\rangle$, $R_j^T = 0$	X-basis	X-basis	$\|-\rangle$	$\|-\rangle$
5	$\|\Psi\rangle$, $R_j^T = 1$	Z-basis	Z-basis	$\|0\rangle$	$\|1\rangle$
6	$\|\Psi\rangle$, $R_j^T = 1$	Z-basis	Z-basis	$\|1\rangle$	$\|0\rangle$
7	$\|\Psi\rangle$, $R_j^T = 1$	X-basis	X-basis	$\|+\rangle$	$\|+\rangle$
8	$\|\Psi\rangle$, $R_j^T = 1$	X-basis	X-basis	$\|-\rangle$	$\|-\rangle$

3. Quantum homomorphic encryption phase: Alice and Bob utilize the keys generated in the key generation phase, labeled here as R_i^A and R_i^B, to encrypt their individual quantum states. They then send the encrypted states to TP for the execution of the CNOT homomorphic evaluation and decryption.

Step 3-1: Alice and Bob use $R_i^A = (\alpha_i^A, \beta_i^A)$ and $R_i^B = (\alpha_i^B, \beta_i^B)$ to encrypt the i-th states $|A_i\rangle$ and $|B_i\rangle$. The encrypted quantum states are labeled as $X^{\alpha_i^A} Z^{\beta_i^A} |A_i\rangle$ and $X^{\alpha_i^B} Z^{\beta_i^B} |B_i\rangle$, respectively.

Step 3-2: Alice and Bob then send the encrypted quantum states to TP for further CNOT homomorphic evaluation.

Step 3-3: TP performs the CNOT-gate on the i-th states $X^{\alpha_i^A} Z^{\beta_i^A} |A_i\rangle$ and $X^{\alpha_i^B} Z^{\beta_i^B} |B_i\rangle$, yielding

$$\begin{aligned} &CNOT(X^{\alpha_i^A} Z^{\beta_i^A} \otimes X^{\alpha_i^B} Z^{\beta_i^B}) |A_i\rangle |B_i\rangle \\ &= (X^{\alpha_i^A} Z^{\beta_i^A \oplus \beta_i^B} \otimes X^{\alpha_i^A \oplus \alpha_i^B} Z^{\beta_i^B}) |A_i\rangle |A_i \oplus B_i\rangle \end{aligned}. \tag{5}$$

According to Equation (4), i.e., $R_i^T = R_i^A \oplus R_i^B$, TP can derive the value of $\alpha_i^A \oplus \alpha_i^B$ based on R_i^T. Subsequently, TP performs the decryption operation $X^{\alpha_i^A \oplus \alpha_i^B}$ on the second particle, corresponding to the second half of Equation (5). Specifically, this operation is carried out as shown in Equation (6).

$$\begin{aligned} &X^{\alpha_i^A} Z^{\beta_i^A \oplus \beta_i^B} |A_i\rangle \otimes X^{\alpha_i^A \oplus \alpha_i^B} X^{\alpha_i^A \oplus \alpha_i^B} Z^{\beta_i^B} |A_i \oplus B_i\rangle \\ &= X^{\alpha_i^A} Z^{\beta_i^A \oplus \beta_i^B} |A_i\rangle \otimes Z^{\beta_i^B} |A_i \oplus B_i\rangle \end{aligned}. \tag{6}$$

Since both $|A_i\rangle$ and $|B_i\rangle$ belong to $\{|0\rangle, |1\rangle\}$, the CNOT operation does not cause entanglement of $|A_i\rangle$ and $|B_i\rangle$, so the final quantum states $|A_i\rangle$ and $|A_i \oplus B_i\rangle$ are independent.

Step 3-4: TP performs the Z-basis measurements on the particle $|A_i \oplus B_i\rangle$ to obtain the comparison results. Note that the application of the Z-gate does not cause a state flip but only induces a phase shift. As a result, during Z-basis measurements, this phase shift has no effect, and thus, the influence of the Z-gate on the final outcome is disregarded.

Based on the measurement results, TP can infer the relationship between Alice's and Bob's private sets (see Table 2). Specifically, if $|A_i \oplus B_i\rangle = |0\rangle$, it indicates that element i either belongs to $S_A * \cap S_B *$ or $(S_A * \cup S_B *)^c$. Here, $(S_A * \cup S_B *)^c$ denotes the complement of the union of sets $S_A *$ and $S_B *$, meaning all elements that are in neither $S_A *$ nor $S_B *$. Conversely, if $|A_i \oplus B_i\rangle = |1\rangle$, it signifies that element i belongs to the symmetric difference of $S_A *$ and $S_B *$, i.e., $S_A * \Delta S_B * = (S_A * - S_B *) \cup (S_B * - S_A *)$.

Table 2. Measurement results and set relationships.

Alice' State	Bob's State	Measurement Results	Set Relationships
$i \notin S_A*, \|A_i\rangle = \|0\rangle$	$i \notin S_B*, \|B_i\rangle = \|0\rangle$	$\|A_i \oplus B_i\rangle = \|0\rangle$	$(S_A * \cup S_B*)^c$
$i \in S_A*, \|A_i\rangle = \|1\rangle$	$i \notin S_B*, \|B_i\rangle = \|0\rangle$	$\|A_i \oplus B_i\rangle = \|1\rangle$	$S_A * - S_B*$
$i \notin S_A*, \|A_i\rangle = \|0\rangle$	$i \in S_B*, \|B_i\rangle = \|1\rangle$	$\|A_i \oplus B_i\rangle = \|1\rangle$	$S_B * - S_A*$
$i \in S_A*, \|A_i\rangle = \|1\rangle$	$i \in S_B*, \|B_i\rangle = \|1\rangle$	$\|A_i \oplus B_i\rangle = \|0\rangle$	$S_A * \cap S_B*$

4. Set similarity calculation phase: Alice and Bob inform TP of the sizes of their respective sets, i.e., $|S_A| = |S_A*| = n$ and $|S_B| = |S_B*| = m$. Based on the measurement results, TP computes the set similarity and announces the outcome to Alice and Bob.

Step 4-1: Alice and Bob send their respective set sizes n and m to TP through a quantum secure direct communication protocol [23].

Step 4-2: TP counts the size of $|S_A * \Delta S_B *|$, i.e., the number of measurements with the result of $|1\rangle$ in Step 3-4, labeled as l. TP then performs the following calculations to derive the intersection and union sizes of sets S_A* and S_B*:

$$\begin{aligned} |S_A * \cap S_B *| &= (|S_A *| + |S_B *| - |S_A * \Delta S_B *|)/2 = (n + m - l)/2 \\ |S_A * \cup S_B *| &= |S_A *| + |S_B *| - |S_A * \cap S_B *| = n + m - (n + m - l)/2 \end{aligned}. \tag{7}$$

Thereby, TP can obtain the set similarity of S_A* and S_B* (i.e., S_A and S_B).

$$J_{AB} = \frac{|S_A * \cap S_B *|}{|S_A * \cup S_B *|} = \frac{|S_A \cap S_B|}{|S_A \cup S_B|} = \frac{n + m - l}{n + m + l}. \tag{8}$$

Finally, TP publishes the set similarity results to Alice and Bob.

3.2. Quantum Privacy-Preserving Range Query Protocol

In this part, a privacy-preserving range query protocol in the IoT environments is proposed, where the protocol model is depicted in Figure 1.

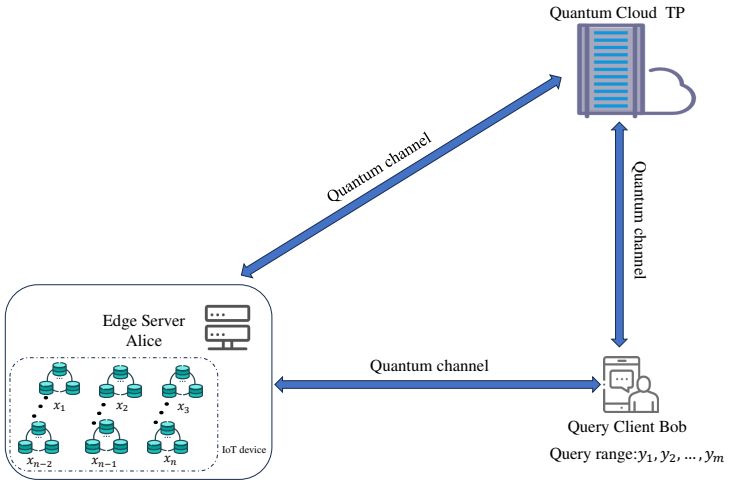


Figure 1. Basic protocol model.

This model involves three participants: Alice, Bob, and TP. Specifically, Alice acts as an edge server responsible for managing sensitive data collected from multiple IoT devices. The complete dataset can be represented as follows:

$$\begin{array}{l} x_1 : \{d_1^1, d_1^2, \ldots, d_1^G\} \\ x_2 : \{d_2^1, d_2^2, \ldots, d_2^G\} \\ \quad \vdots \quad \vdots \\ x_n : \{d_n^1, d_n^2, \ldots, d_n^G\} \end{array}, \tag{9}$$

where x_h ($h = 1, 2, \ldots, n$) denotes the h-th IoT device's index number, and $\{d_h^1, d_h^2, \ldots, d_h^G\}$ denotes the collected data of the h-th IoT device, with each $d_h^g \in [0, N)$ ($g = 1, 2, \ldots, G$). Here, the index numbers $x_1, x_2, \ldots, x_n$ constitute a privacy set, denoted as SA.

Bob is a querying user who wishes to privately retrieve data from a specific range of IoT device nodes managed by Alice. Bob's query range is denoted as $y_1, y_2, \ldots, y_m$, which also forms a set, denoted as SB. TP is a semi-honest quantum cloud to assist with the privacy query task. However, TP is considered curious and may attempt to infer both Alice's data and the result of Bob's query.

The goal of this protocol is to enable privacy-preserving range queries between the edge server, Alice, and the querying client, Bob, with the assistance of the quantum cloud, TP, using quantum encryption techniques. The protocol's security requirements are twofold: (1) to ensure the privacy of both Bob's query range and the corresponding query results, and (2) to protect the privacy of all data elements in Alice's dataset that are not part of the query result. The detailed steps are as follows.

Step 1: Alice and Bob execute the first phase of the protocol in Section 3.1 to transform the two privacy sets SA and SB into $SA*$ and $SB*$.

$$SA* = \{x_1', x_2', \ldots, x_n'\}, \quad SB* = \{y_1', y_2', \ldots, y_m'\}, \tag{10}$$

where $x_h' = kx_h \bmod N$ and $y_w' = ky_w \bmod N$ ($w = 1, 2 \ldots, m$). Accordingly, Alice's original dataset is modified to be

$$\begin{array}{l} x_1' : \{d_1^1, d_1^2, \ldots, d_1^G\} \\ x_2' : \{d_2^1, d_2^2, \ldots, d_2^G\} \\ \quad \vdots \quad \vdots \\ x_n' : \{d_n^1, d_n^2, \ldots, d_n^G\} \end{array}, \tag{11}$$

Then, the two quantum sequences $(|A_0\rangle, |A_1\rangle, \ldots, |A_{N-1}\rangle)$ and $(|B_0\rangle, |B_1\rangle, \ldots, |B_{N-1}\rangle)$ are modified in the following manner:

$$\begin{array}{llll} |A_i\rangle = |0\rangle, & \text{if } i \neq x_h', & |A_i\rangle = |1\rangle, & \text{if } i = x_h', \\ |B_i\rangle = |0\rangle, & \text{if } i \neq y_w', & |B_i\rangle = |1\rangle, & \text{if } i = y_w', \end{array} \tag{12}$$

Step 2: Alice and Bob establish N integer keys $K_{AB} = \{k_0, k_1 \ldots, k_{N-1}\}$ via the QKD protocol. Similarly, Alice and TP, as well as Bob and TP, each establish N integer keys $K_{AT} = \{t_0, t_1, \ldots, t_{N-1}\}$ and $K_{BT} = \{b_0, b_1, \ldots, b_{N-1}\}$, respectively.

Step 3: According to the state of $|A_i\rangle$, Alice applies different manners to encrypt the private data. If $|A_i\rangle = |1\rangle$, it means that i belongs to the set $SA*$, i.e., $i = x_h'$; then, the corresponding privacy data $\{d_h^1, d_h^2, \ldots, d_h^G\}$ will be transformed to

$$d_h^1 + k_i + t_i,\ d_h^2 + k_i + t_i,\ \ldots,\ d_h^G + k_i + t_i. \tag{13}$$

If $|A_i\rangle = |0\rangle$, it indicates that i is not part of the set $SA*$, meaning $i \neq x_h'$. At this position, there were no original data, so Alice must generate a new set of identical data for padding. In this case, the generated data are assumed to be

$$a_i + k_i + t_i,\ a_i + k_i + t_i,\ \ldots,\ a_i + k_i + t_i. \tag{14}$$

where a_i is random and only known to Alice. Thus, after encryption, Alice's private dataset can be expressed as

$$\begin{cases} x'_h : \{d_h^1 + k_i + t_i,\ d_h^2 + k_i + t_i,\ \ldots,\ d_h^G + k_i + t_i\}, & if \quad |A_i\rangle = |1\rangle, i.e., i = x'_h \\ a'_i : \{a_i + k_i + t_i,\ a_i + k_i + t_i,\ \ldots,\ a_i + k_i + t_i\}, & if \quad |A_i\rangle = |0\rangle, i.e., i \neq x'_h \end{cases}, \tag{15}$$

where a'_i corresponds to the position where $|A_i\rangle = |0\rangle$, and the private data generated at these positions are the same.

Step 4: Executing the key generation phase of the protocol in Section 3.1, Alice, Bob and TP establish a key relationship as shown in Equation (4).

Step 5: Using the established keys, Alice and Bob encrypt their respective quantum state sequences, $(|A_0\rangle, |A_1\rangle, \ldots, |A_{N-1}\rangle)$ and $(|B_0\rangle, |B_1\rangle, \ldots, |B_{N-1}\rangle)$, before sending them to TP for quantum homomorphic evaluation. This corresponds to executing the quantum homomorphic encryption phase of the protocol in Section 3.1.

Step 6: According to Step 3-4 listed in Section 3.1, TP can obtain the value of $|A_i \oplus B_i\rangle$ through the Z-basis measurement. The focus here is on cases where the measurement result is $|0\rangle$. If $|A_i \oplus B_i\rangle = |0\rangle$, TP records the corresponding value of i. Then, based on the value of i and the keys t_i and b_i, TP generates a privacy vector $V = [v_0, v_1, \ldots, v_{N-1}]$ as follows:

$$v_i = \begin{cases} t_i - b_i, & \textbf{if} \quad |A_i \oplus B_i\rangle = |0\rangle \\ 0, & \textbf{if} \quad |A_i \oplus B_i\rangle = |1\rangle \end{cases}. \tag{16}$$

Step 7: Through a quantum secure direct communication protocol, Alice sends the privacy data corresponding to Equation (15) to TP. There are two situations to consider here. First, consider the case where $|A_i\rangle = |1\rangle$, i.e., $i = x'_h$. In this case, Alice sends the data as $\{d_h^1 + k_i + t_i, d_h^2 + k_i + t_i, \ldots, d_h^G + k_i + t_i\}$. In contrast, when $|A_i\rangle = |0\rangle$, Alice sends the data as $\{a_i + k_i + t_i, a_i + k_i + t_i, \ldots, a_i + k_i + t_i\}$. TP can easily distinguish whether $|A_i\rangle$ equals $|0\rangle$ or $|1\rangle$ based on the data sent by Alice. This is because when $|A_i\rangle = |0\rangle$, the data Alice sends are identical across all entries.

For the i-th set of data, where $|A_i \oplus B_i\rangle = |0\rangle$ and $|A_i\rangle = |1\rangle$, TP decrypts using the corresponding v_i to retrieve a new set of private data. Specifically, TP subtracts v_i from the data sent by Alice to obtain the final result:

$$\{d_h^1 + k_i + b_i,\ d_h^2 + k_i + b_i,\ \ldots,\ d_h^G + k_i + b_i\}, \tag{17}$$

where position i satisfies $|A_i \oplus B_i\rangle = |0\rangle$ and $|A_i\rangle = |1\rangle$.

For position i that does not meet the above conditions, TP prepares a set of identical random data as padding, denoted as $\{p_i^1, p_i^2, \ldots, p_i^G\}$.

Step 8: Through a quantum secure direct communication protocol, TP sends $\{d_h^1 + k_i + b_i,\ d_h^2 + k_i + b_i,\ \ldots,\ d_h^G + k_i + b_i\}$ and $\{p_i^1, p_i^2, \ldots, p_i^G\}$ to Bob. Here, Bob is only concerned with the case where $|B_i\rangle = |1\rangle$, because only these positions satisfy $|A_i\rangle = |B_i\rangle = |1\rangle$ and $SA* \cap SB*$. For other positions i, Bob will only obtain the same result $\{p_i^1, p_i^2, \ldots, p_i^G\}$.

Then, Bob uses the keys k_i and b_i to decrypt and retrieve the private data relevant to his query. Thus, for the i-th ($i = x'_h = y'_w$, i.e., $|A_i\rangle = |B_i\rangle = |1\rangle$) group of data $\{d_h^1 + k_i + b_i,\ d_h^2 + k_i + b_i,\ \ldots,\ d_h^G + k_i + b_i\}$, Bob performs the following calculation to obtain the final query results:

$$\begin{aligned} &d_h^1 + k_i + b_i - k_i - b_i = d_h^1, \\ &d_h^2 + k_i + b_i - k_i - b_i = d_h^2, \\ &\quad\vdots \\ &d_h^G + k_i + b_i - k_i - b_i = d_h^G. \end{aligned} \tag{18}$$

It is important to note that Bob can only access information within his queried range. For other cases, he cannot retrieve any data. This is because TP only reveals Alice's data for indices i that belong to the intersection of sets $SA*$ and $SB*$. For indices i in the other positions, Bob's decryption result will uniformly be $\{p_i^1, p_i^2, \ldots, p_i^G\}$, which contains no private information from Alice.

4. Correctness Analysis and Simulation

In this section, we will analyze the correctness of the protocol and conduct circuit simulations. We first analyze the correctness of the proposed quantum privacy set similarity comparison protocol, and then discuss the correctness of the privacy range query scheme applicable to IoT environments.

4.1. Correctness of the Proposed Quantum Privacy Set Similarity Comparison Protocol

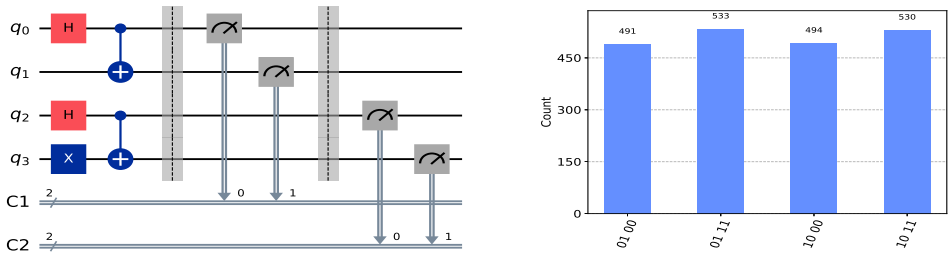
Assuming that Alice and Bob's privacy datasets are $S_A = \{2,3,5,6\} \subseteq \mathbb{Z}_7$ and $S_B = \{1,2,5\} \subseteq \mathbb{Z}_7$, respectively, the analysis proceeds step by step according to the four phases of the protocol.

In the privacy set encoding stage, we assume that Alice and Bob's privacy sets are transformed into $S_A* = \{2 \times 2 \bmod 7, 2 \times 3 \bmod 7, 2 \times 5 \bmod 7, 2 \times 6 \bmod 7\} = \{4,6,3,5\}$ and $S_B* = \{2 \times 1 \bmod 7, 2 \times 2 \bmod 7, 2 \times 5 \bmod 7\} = \{2,4,3\}$, where $k = 2$. Thus, the quantum state sequences generated by Alice and Bob are, respectively,

$$\begin{aligned} &|A_0\rangle = |0\rangle, |A_1\rangle = |0\rangle, |A_2\rangle = |0\rangle, |A_3\rangle = |1\rangle, \\ &|A_4\rangle = |1\rangle, |A_5\rangle = |1\rangle, |A_6\rangle = |1\rangle, \\ &|B_0\rangle = |0\rangle, |B_1\rangle = |0\rangle, |B_2\rangle = |1\rangle, |B_3\rangle = |1\rangle, \\ &|B_4\rangle = |1\rangle, |B_5\rangle = |0\rangle, |B_6\rangle = |0\rangle. \end{aligned} \tag{19}$$

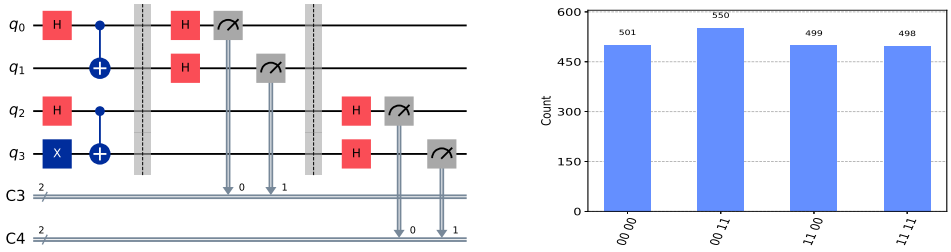
Then, in the key generation phase, Alice and Bob can establish a shared key with TP using Bell states, as described in Equation (4). Specifically, TP prepares and sends two sets of quantum states, $|\Psi\rangle$ and $|\Phi\rangle$, to Alice and Bob, respectively. Both Alice and Bob then perform measurements using the Z-basis and X-basis. The corresponding quantum circuit simulation and results are shown in Figures 2 and 3. It should be noted that in the simulation result diagrams of Figures 2 and 3, the values on the horizontal axis represent the measurement results of the corresponding qubits, while the vertical axis represents the number of times the corresponding results appear. The number of simulations in the experiment is 2048.

The focus here is on the cases where Alice and Bob choose the same measurement basis. Only in these cases can the resulting particles be used for eavesdropping detection and key generation.



(**a**) Execution of Z-based circuit diagram (**b**) Simulation results of (**a**)

Figure 2. Circuits and simulation results for Z-basis measurements. Classical registers C1 and C2, respectively, record the Z-basis measurement results of $|\Phi\rangle$ and $|\Psi\rangle$ by Alice and Bob. In subfigure (**b**), the horizontal axis represents the measurement results of the corresponding qubits, while the vertical axis indicates the frequency of each result.



(**a**) Execution of X-based circuit diagram (**b**) Simulation results of (**a**)

Figure 3. Circuits and simulation results for X-basis measurements. Classical registers *C*3 and *C*4, respectively, record the X-basis measurement results of $|\Phi\rangle$ and $|\Psi\rangle$ by Alice and Bob. The horizontal axis in subfigure (**b**) represents the measurement results of the corresponding qubits, while the vertical axis shows the frequency of each result.

As seen in Figure 2, when both Alice and Bob choose Z-basis measurements, their results for quantum state $|\Phi\rangle$ are identical, whereas for quantum state $|\Psi\rangle$, their measurement outcomes are opposite. This observation is consistent with the results in Table 1. When both Alice and Bob select X-basis measurements, their outcomes for both quantum states $|\Phi\rangle$ and $|\Psi\rangle$ are the same, with the corresponding results shown in Figure 3. We assume here that the key relationship established between Alice, Bob, and TP is

$$\begin{aligned}
&R_0^T = (\alpha_0^T = 0, \beta_0^T = 1),\ R_0^A = (\alpha_0^A = 1, \beta_0^A = 1),\ R_0^B = (\alpha_0^B = 1, \beta_0^B = 0),\\
&R_1^T = (\alpha_1^T = 1, \beta_1^T = 1),\ R_1^A = (\alpha_1^A = 1, \beta_1^A = 1),\ R_1^B = (\alpha_1^B = 0, \beta_1^B = 0),\\
&R_2^T = (\alpha_2^T = 0, \beta_2^T = 1),\ R_2^A = (\alpha_2^A = 1, \beta_2^A = 0),\ R_2^B = (\alpha_2^B = 1, \beta_2^B = 1),\\
&R_3^T = (\alpha_3^T = 1, \beta_3^T = 0),\ R_3^A = (\alpha_3^A = 1, \beta_3^A = 1),\ R_3^B = (\alpha_3^B = 0, \beta_3^B = 1),\\
&R_4^T = (\alpha_4^T = 0, \beta_4^T = 0),\ R_4^A = (\alpha_4^A = 1, \beta_4^A = 1),\ R_4^B = (\alpha_4^B = 1, \beta_4^B = 1),\\
&R_5^T = (\alpha_5^T = 1, \beta_5^T = 1),\ R_5^A = (\alpha_5^A = 0, \beta_5^A = 0),\ R_5^B = (\alpha_5^B = 1, \beta_5^B = 1),\\
&R_6^T = (\alpha_6^T = 1, \beta_6^T = 0),\ R_6^A = (\alpha_6^A = 0, \beta_6^A = 1),\ R_6^B = (\alpha_6^B = 1, \beta_6^B = 1),
\end{aligned} \tag{20}$$

where $R_i^T = R_i^A \oplus R_i^B$ (i.e., $\alpha_i^T = \alpha_i^A \oplus \alpha_i^B$, $\beta_i^T = \beta_i^A \oplus \beta_i^B$), and $i = 0, 1, \ldots, 6$.

Afterwards, the quantum homomorphic encryption stage is performed. Alice and Bob send the encrypted state $x^{\alpha_i^A} Z^{\beta_i^A} |A_i\rangle$ and $x^{\alpha_i^B} Z^{\beta_i^B} |B_i\rangle$, respectively, to TP. Then, TP performs CNOT evaluation, and the corresponding quantum circuit is shown in Figure 4. The specific parameter settings for the circuit can be found in Equations (19) and (20).

The corresponding simulation results are shown in Figure 5. As can be seen from the figure, the measurement results satisfy $A_i \oplus B_i$. The XOR results calculated from the initial states of $|A_i\rangle$ and $|B_i\rangle$ in Equation (19) are consistent with the simulation results.

In the final privacy set similarity calculation, Alice and Bob first inform TP of the sizes of their private sets, i.e., $n = 4$ and $m = 3$. Then, TP counts the number of measurement outcomes equal to $A_i \oplus B_i = 1$ from the homomorphic evaluation, denoted as l. From Figure 5, it can be seen that the number of measurements with a result of 1 is 3, i.e., $l = 3$. Based on Equation (7), the sizes of Alice and Bob's intersection and union are calculated accordingly.

$$\begin{aligned}
|S_A * \cap S_B *| &= (n + m - l)/2 = (4 + 3 - 3)/2 = 2\\
|S_A * \cup S_B *| &= n + m - (n + m - l)/2 = 4 + 3 - (4 + 3 - 3)/2 = 5
\end{aligned}. \tag{21}$$

Thereby, TP can obtain the set similarity of S_A* and S_B* (i.e., S_A and S_B).

$$J_{AB} = \frac{|S_A * \cap S_B *|}{|S_A * \cup S_B *|} = \frac{|S_A \cap S_B|}{|S_A \cup S_B|} = \frac{n + m - l}{n + m + l} = \frac{2}{5}. \tag{22}$$

This result is the same as directly calculating the similarity between $S_A = \{2, 3, 5, 6\} \subseteq \mathbb{Z}_7$ and $S_B = \{1, 2, 5\} \subseteq \mathbb{Z}_7$. Therefore, the output result of the designed protocol is correct.

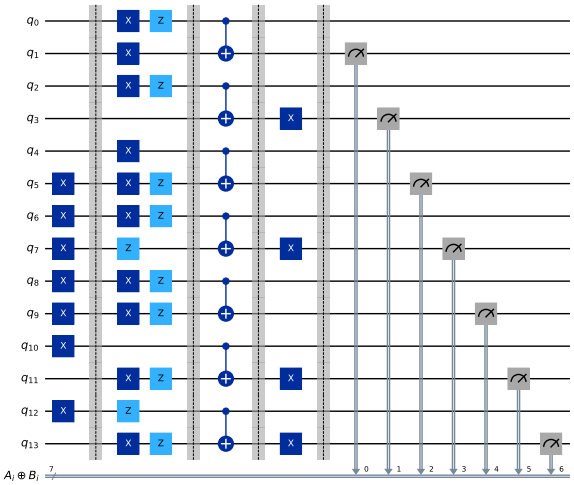


Figure 4. CNOT homomorphic evaluation quantum circuit diagram. In this circuit, registers $q_0, q_2, q_4, q_6, q_8, q_{10}, q_{12}$ denote the quantum states $(|A_0\rangle, |A_1\rangle, \ldots, |A_6\rangle)$ prepared by Alice, while $q_1, q_3, q_5, q_7, q_9, q_{11}, q_{13}$ denote the quantum states $(|B_0\rangle, |B_1\rangle, \ldots, |B_6\rangle)$ prepared by Bob. The entire circuit is divided into five stages, separated by barriers, which correspond to the preparation of quantum states, encryption, CNOT evaluation, decryption, and the final measurement.

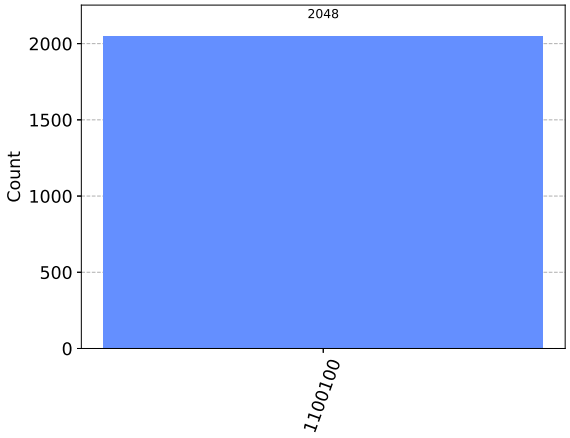


Figure 5. Simulation results of circuits listed in Figure 4. The horizontal axis "11000100" in the figure represents the measurement result of $|A_i \oplus B_i\rangle$, and the result is consistent with the setting of Equation (19). For example, the measurement result of $|A_6 \oplus B_6\rangle$ is equal to 1, and the result of $|A_5 \oplus B_5\rangle$ is also equal to 1.

4.2. Correctness of the Proposed Quantum Privacy-Preserving Range Query Protocol

In this part, we analyze the correctness of the proposed quantum privacy-preserving range query protocol step by step. Assume that Alice has a dataset represented as

$$\begin{aligned} x_1 = 2 &: \{d_1^1, d_1^2, \ldots, d_1^G\} \\ x_2 = 3 &: \{d_2^1, d_2^2, \ldots, d_2^G\} \\ x_3 = 5 &: \{d_3^1, d_3^2, \ldots, d_3^G\} \\ x_4 = 6 &: \{d_4^1, d_4^2, \ldots, d_4^G\} \end{aligned}. \tag{23}$$

Here, the index numbers x_1, x_2, x_3, x_4 constitute a privacy set, denoted as SA. Bob's query range $\{y_1 = 1, y_2 = 2, y_3 = 5\}$ also forms a set, denoted SB.

Similar to Section 4.1, Alice and Bob first carry out the private set encoding phase, where we also assume $k = 2$. As a result, they obtain the same transformed private sets,

i.e., $S_A* = \{4, 6, 3, 5\}$ and $S_B* = \{2, 4, 3\}$. Correspondingly, the quantum state sequences prepared by Alice and Bob are identical, as shown in Equation (19).

Performing steps 1, 2, and 3, Alice obtains the transformed privacy dataset as follows:

$$\begin{aligned}
x'_1 = 4 &: \{d_1^1 + k_4 + t_4,\ d_1^2 + k_4 + t_4,\ \ldots,\ d_1^G + k_4 + t_4\},\\
x'_2 = 6 &: \{d_2^1 + k_6 + t_6,\ d_2^2 + k_6 + t_6,\ \ldots,\ d_2^G + k_6 + t_6\},\\
x'_3 = 3 &: \{d_3^1 + k_3 + t_3,\ d_3^2 + k_3 + t_3,\ \ldots,\ d_3^G + k_3 + t_3\},\\
x'_4 = 5 &: \{d_4^1 + k_5 + t_5,\ d_4^2 + k_5 + t_5,\ \ldots,\ d_4^G + k_5 + t_5\},\\
a'_0 = 0 &: \{a_0 + k_0 + t_0,\ a_0 + k_0 + t_0,\ \ldots,\ a_0 + k_0 + t_0\},\\
a'_1 = 1 &: \{a_1 + k_1 + t_1,\ a_1 + k_1 + t_1,\ \ldots,\ a_1 + k_1 + t_1\},\\
a'_2 = 2 &: \{a_2 + k_2 + t_2,\ a_2 + k_2 + t_2,\ \ldots,\ a_2 + k_2 + t_2\},
\end{aligned} \tag{24}$$

where a_i is randomly generated by Alice, and k_i and t_i are the keys generated in step 1. a'_0, a'_1, and a'_2 represent the index numbers corresponding to the set that is not part of the set S_A*.

After completing steps 4, 5, and 6 (i.e., the key generation phase and the quantum homomorphic encryption phase), TP obtains the result of $|A_i \oplus B_i\rangle$. The correctness of this result was already verified in Section 4.1, so it will not be repeated here. TP then focuses on the case where $|A_i \oplus B_i\rangle = |0\rangle$. From the results in Figure 5, it can be concluded that $|A_0 \oplus B_0\rangle = |0\rangle$, $|A_1 \oplus B_1\rangle = |0\rangle$, $|A_3 \oplus B_3\rangle = |0\rangle$, and $|A_4 \oplus B_4\rangle = |0\rangle$. TP prepares a new data point v_i, at the corresponding position, as specified in Equation (16). The specific vector V here is $V = [t_0 - b_0, t_1 - b_1, 0, t_3 - b_3, t_4 - b_4, 0, 0]$.

After step 7, Alice sends the encrypted private dataset to TP, who then checks whether each set of data is identical, allowing it to infer which positions satisfy $|A_i\rangle = |0\rangle$. For the i-th set of data, where $|A_i \oplus B_i\rangle = |0\rangle$ and $|A_i\rangle = |1\rangle$, TP decrypts it using v_i to retrieve a new set of private data. Thus, at the index numbers $x'_1 = 4$ and $x'_3 = 3$, the private data after TP decryption is

$$\begin{aligned}
x'_1 = 4 &: \{d_1^1 + k_4 + b_4,\ d_1^2 + k_4 + b_4,\ \ldots,\ d_1^G + k_4 + b_4\},\\
x'_3 = 3 &: \{d_3^1 + k_3 + b_3,\ d_3^2 + k_3 + b_3,\ \ldots,\ d_3^G + k_3 + b_3\}.
\end{aligned} \tag{25}$$

For the data corresponding to other index numbers, TP randomly prepares the same data, denoted as $\{p_i^1, p_i^2, \ldots, p_i^G\}$.

Finally, TP sends the data in Equation (25) and $\{p_i^1, p_i^2, \ldots, p_i^G\}$ to Bob. Here, Bob is only concerned with the case where $|B_i\rangle = |1\rangle$, because only these positions satisfy $|A_i\rangle = |B_i\rangle = |1\rangle$ and $SA* \cap SB*$. Combined with the specific assumptions, here, Bob would obtain the data in Equation (25) at positions $i = 3$ and $i = 4$. For other positions i, Bob will only obtain the same result $\{p_i^1, p_i^2, \ldots, p_i^G\}$. Thus, for the data $\{d_1^1 + k_4 + b_4,\ d_1^2 + k_4 + b_4,\ \ldots,\ d_1^G + k_4 + b_4\}$ and $\{d_3^1 + k_3 + b_3,\ d_3^2 + k_3 + b_3,\ \ldots,\ d_3^G + k_3 + b_3\}$, Bob decrypts using keys k_3, k_4 and b_3, b_4 to obtain the final query result

$$\begin{aligned}
&\{d_1^1,\ d_1^2,\ \ldots,\ d_1^G\},\\
&\{d_3^1,\ d_3^2,\ \ldots,\ d_3^G\}.
\end{aligned} \tag{26}$$

Based on the initial assumption, Bob's queried indices are $\{1, 2, 5\}$, while Alice's set of indices is $\{2, 3, 5, 6\}$. Therefore, the result of the query should be the private data corresponding to indices 2 and 5. According to Equation (23), Bob's query result should be $\{d_1^1, d_1^2, \ldots, d_1^G\}$ and $\{d_3^1, d_3^2, \ldots, d_3^G\}$. Consequently, the output of our protocol is correct.

5. Security Analysis

This section will discuss the security of the protocol. In the following, the security of the quantum privacy set similarity comparison protocol is first discussed, followed by analyzing the security of the privacy range query protocol.

5.1. Security Analysis for Quantum Privacy Set Similarity Comparison Protocol

For the quantum private set similarity comparison protocol, the security of the protocol primarily depends on the security of the keys generated during the key generation phase, which is closely related to the security of the subsequent homomorphic encryption and CNOT evaluation.

Theorem 1. *With the assistance of a semi-honest quantum cloud TP, Alice and Bob can establish a secure key relationship $R_j^T = R_j^A \oplus R_j^B$ using Bell states, ensuring that none of the three parties can access each other's private information.*

Proof. In the key generation phase, TP randomly prepares Bell states $|\Phi\rangle$ and $|\Psi\rangle$, while Alice and Bob randomly perform measurements in either the Z-basis or the X-basis. Subsequently, Alice and Bob select a subset of particles for eavesdropping detection.

We consider two scenarios: one involving an external eavesdropper, Eve, attempting to steal the key, and the other involving internal eavesdroppers, which include the semi-honest TP as well as dishonest Alice or Bob, trying to obtain the key.

External attack analysis: Suppose TP prepares $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to send to Alice and Bob, and Eve launches an entangle-measure attack [24] on the particles transmitted between TP and Alice. Specifically, Eve utilizes the unitary operation U_E to entangle the auxiliary particle, $|0\rangle_E$, to the target particle and then steals information by observing the state of the auxiliary particle [25]. After Eve's attack, the state of the system will change to

$$\begin{aligned} U_E(|\Phi\rangle|0\rangle_E) &= \frac{1}{\sqrt{2}}(|00\rangle|e_0\rangle + |11\rangle|e_1\rangle), \\ &= \frac{1}{\sqrt{2}}\Big[\frac{1}{2}(|++\rangle + |-+\rangle + |+-\rangle + |--\rangle|e_0\rangle)\,, \\ &\quad + \frac{1}{2}(|++\rangle - |-+\rangle - |+-\rangle + |--\rangle|e_1\rangle)\Big] \end{aligned} \tag{27}$$

where the effect U_E can be described as $U_E(|0\rangle|0\rangle_E) = |0\rangle|e_0\rangle$ and $U_E(|1\rangle|0\rangle_E) = |1\rangle|e_1\rangle$.

For $|\Phi\rangle$, when Alice and Bob perform the same measurement basis on the received particles, either in the Z-basis or the X-basis, their measurement results will be identical. This implies that the condition $|e_0\rangle = |e_1\rangle$ must hold in Equation (27). Only in this scenario can Alice and Bob observe the same results using different measurement bases. Furthermore, satisfying $|e_0\rangle = |e_1\rangle$ indicates that Eve cannot obtain any secret information from the auxiliary particles. Regardless of the state of the target particle, she will receive the same measurement outcome. Therefore, Eve cannot steal information through the entangle-measure attack without introducing errors.

Internal attack analysis: Suppose the semi-honest TP intends to steal Alice's secret information. In this scenario, since TP plays a role in the initial quantum state preparation, it poses a greater threat than external attackers. TP could prepare false particles, such as single-particle states, to gain access to Alice and Bob's measurement results. However, this attack cannot evade the eavesdropping detection mechanisms of the protocol. During the eavesdropping detection process, Alice and Bob will verify whether the quantum states prepared by TP meet the required conditions by performing measurements with different bases. Moreover, if TP prepares quantum states $|\Phi\rangle$ and $|\Psi\rangle$ according to the protocol, then TP's attempt to obtain Alice's secret information will be the same as an external attacker. Therefore, TP's attack cannot effectively steal the secret information without introducing an error.

Regarding the case where a dishonest Alice seeks to steal Bob's key, there is no quantum communication between Alice and Bob during the key generation phase. Therefore, if Alice wishes to steal Bob's information, she can only attack the particles directly transmitted between TP and Bob. In this scenario, Alice essentially acts as an external attacker; thus, her attack is also ineffective in the absence of errors.

In summary, in the key generation phase, Alice, Bob, and TP can establish a key relationship and cannot obtain each other's keys. □

In addition, the privacy sets of Alice and Bob are kept confidential. TP can only obtain the size of the privacy sets of Alice and Bob, while Alice and Bob can only know the similarity of the privacy sets.

Theorem 2. *After executing the quantum privacy set similarity comparison protocol, both Alice and Bob's private sets remain confidential, and TP can only obtain the sizes of Alice and Bob's private sets.*

Proof. During the privacy set encoding phase of the protocol, Alice and Bob establish a key k using the QKD protocol and encode their respective private sets with this key. Without knowledge of the key k, external attackers and TP are unable to access the actual private set data. In the homomorphic encryption phase, the quantum states corresponding to the private sets are also encrypted and the transmitted quantum states are all maximally mixed states:

$$\begin{aligned} \sum_{\alpha_i^A,\, \beta_i^A \in \{0,1\}} X^{\alpha_i^A} Z^{\beta_i^A} |A_i\rangle\langle A_i| X^{\alpha_i^A} Z^{\beta_i^A} &= \frac{I_2}{2}, \\ \sum_{\alpha_i^B,\, \beta_i^B \in \{0,1\}} X^{\alpha_i^B} Z^{\beta_i^B} |B_i\rangle\langle B_i| X^{\alpha_i^B} Z^{\beta_i^B} &= \frac{I_2}{2}. \end{aligned} \tag{28}$$

TP as well as the external attacker cannot effectively perform decryption to obtain useful information. Finally, in the set similarity calculation phase, Alice and Bob only inform TP about the size of their respective sets. Therefore, the proposed protocol can ensure the security of Alice and Bob's private set data without causing information leakage. □

5.2. Security Analysis for Quantum Privacy-Preserving Range Query Protocol

In the privacy-preserving range query protocol, the focus needs to be on ensuring the security of Bob's query range and the corresponding query results, as well as on protecting the security of the data in Alice's dataset.

Theorem 3. *After executing the privacy-preserving range query protocol, Bob's query range and query results as well as Alice's dataset are confidential.*

Proof. In the proposed protocol, Alice's data consist of two parts: the index numbers of IoT devices and the private data collected by the corresponding devices. Bob's query range is the IoT device index numbers, and the query content is the data collected by those respective devices.

The protocol considers the IoT device index numbers collected by Alice and the query range of Bob as two private sets and executes the set similarity comparison protocol described in Section 3.1 to determine the query range. Section 4.1 analyzed the security of the set similarity comparison protocol, so the security of the protocol in the query range determination process is guaranteed.

Additionally, for the private data collected by IoT devices, Alice, Bob, and TP establish key relationships through QKD, denoted as $K_{AB} = \{k_0, k_1 \ldots, k_{N-1}\}$, $K_{AT} = \{t_0, t_1, \ldots, t_{N-1}\}$, and $K_{BT} = \{b_0, b_1, \ldots, b_{N-1}\}$, respectively. Alice encrypts her data using keys K_{AB} and K_{AT} before sending it to TP. TP then decrypts the data at the corresponding positions using keys K_{AT} and K_{BT} and forwards the result to Bob. Finally, Bob uses keys K_{AB} and K_{BT} to decrypt and obtain the query results that match the specified query range. During this process, since TP lacks key K_{AB}, TP cannot independently decrypt Alice's private data. For Bob, TP only sends the encrypted data that correspond to the query range. Bob then decrypts these data to obtain the final query results. Therefore, Bob only gains access to the specific query results, without any of Alice's other data.

Finally, in terms of Bob's query results and query range, Alice cannot identify Bob's exact query range since she is unaware of the specific comparison of the index numbers. Furthermore, TP securely transmits the private query results directly to Bob using the quantum secure communication protocol, preventing Alice from obtaining any knowledge of the results. For TP, the encrypted index numbers from both Bob and Alice ensure that TP cannot determine the actual query range. Moreover, without key K_{AB}, TP is also unable to retrieve the query results. □

6. Discussion

In the proposed quantum privacy-preserving range query protocol designed for IoT environments, three main quantum sub-protocols are included: the QHE-based quantum private set similarity comparison protocol, the quantum key distribution (QKD) protocol, and the quantum secure direct communication (QSDC) protocol. The following analysis will focus on the quantum resource requirements, communication overhead, protocol complexity, and performance.

Firstly, in terms of quantum resource requirements, the proposed set similarity comparison protocol only requires Bell states, single particles, and simple unitary operations combined with projection measurements. As for the other two quantum protocols, they can also be implemented using single particle states and projection measurements [26,27]. Therefore, the overall quantum resource demand of the protocol is not complex, making the proposed quantum privacy-preserving range query protocol feasible under current technological conditions.

Secondly, consider the communication overhead of the protocol. In our protocol, the quantum communication process includes the following steps. (1) Key generation phase: To ensure data security, pairs of participants—Alice and TP, Alice and Bob, and Bob and TP—use a QKD protocol to establish encryption keys for protecting their private data. For instance, in the BB84 protocol, generating an N-bit key requires approximately $4N$ qubits of communication [28]. Thus, the communication overhead for this phase is around $3 \times 4N$ qubits. (2) Homomorphic encryption phase: During this phase, a series of Bell states are shared between Alice, Bob, and TP to generate keys necessary for homomorphic encryption. This process requires around $8N$ Bell states to produce N keys, resulting in a total communication overhead of approximately $2 \times 8N$ qubits transmitted between TP, Alice, and Bob. Then, Alice and Bob transmit N encrypted quantum states to TP for homomorphic evaluation. (3) Data transmission: After key generation and homomorphic encryption, Alice securely transmits her encrypted quantum states using a QSDC protocol. Then, TP also transmits encrypted quantum states to Bob via a QSDC protocol for final decryption to obtain query results. Typically, a QSDC protocol requires about $4N$ qubits to securely transmit an N-bit of information, such as in the protocol of Deng et al. [29]. Therefore, in order to achieve an N-bit privacy range query, the overall quantum communication overhead is approximately $3 \times 4N + 2 \times 8N + 2N + 2 \times 4N = 38N$ qubits.

Thirdly, regarding the protocol's complexity, in the QKD and QSDC protocols, the two communicating parties need to exchange qubits and use classical communication to share measurement basis information for subsequent measurement operations. This implies that the communication complexity and computational complexity are proportional to the number of qubits N, i.e., $\mathcal{O}(N)$. For the set similarity comparison protocol, the privacy set encoding stage requires executing a single QKD protocol, which has a complexity of $\mathcal{O}(N)$. In the key generation stage, Alice, Bob, and TP establish key relationships using Bell states and single-particle measurements, and this stage also has a complexity of $\mathcal{O}(N)$. Finally, in the quantum homomorphic encryption stage, the CNOT evaluations, decryption, and measurement operations performed by TP are proportional to the number of photons N. Thus, the complexity of this stage is $\mathcal{O}(N)$. Therefore, considering all the above, the overall complexity of the proposed protocol is $\mathcal{O}(N)$.

In terms of protocol performance, our protocol leverages the properties of quantum homomorphic encryption to perform set similarity comparison and range queries without

revealing the private data of either party. This encryption method allows operations to be conducted directly on encrypted data, thus avoiding the leakage of the original sensitive data. Additionally, the QKD and QSDC protocols securely transmit keys and query results through quantum channels, effectively preventing eavesdropper's attacks and enhancing the overall security of the protocol.

Furthermore, we conducted a comparison between our proposed quantum privacy-preserving range query scheme and previous related works, as outlined in Table 3. As shown in Table 3, our protocol provides users with long-term security guarantees. With the advancement of quantum technology, previous schemes [8–10] based on classical encryption may become vulnerable to attacks from quantum computers, leading to the leakage of private data. Furthermore, our approach leverages quantum homomorphic encryption, ensuring that even a powerful quantum cloud TP cannot extract any secret information from the encrypted quantum states.

Table 3. Comparison between our protocol and previous related works.

Protocols	Method	Security Level	Long-Term Security	Query Range	QHE-Based
Ref. [8]	CHE	CS	No	Privacy	/
Ref. [9]	XOR + hash-based authentication	CS	No	Public	/
Ref. [10]	CHE + PC	CS	No	Public	/
Ref. [16]	QSP + QSMCX + QPQ	QS	Yes	Privacy	No
Ref. [17]	Quantum OSID + QPQ	QS	Yes	Privacy	No
Our protocol	QPSSC + QKD + QSDC	QS	Yes	Privacy	Yes

Note. CHE: classical homomorphic encryption; QHE: quantum homomorphic encryption; PC: privacy comparison; CS: classical security; QS: quantum security; QSP: quantum secret permutating; QSMCX: quantum secure multi-party computing XOR; QPQ: quantum privacy query; OSID: oblivious set inclusion decision; QPSSC: quantum privacy set similarity comparison.

In summary, the proposed quantum privacy-preserving range query protocol offers advantages in security and privacy protection. With the application of QHE, data processing and query operations can be performed in the encrypted domain, thereby reducing the risk of exposing the original sensitive information.

7. Conclusions

In this work, we proposed a quantum privacy-preserving range query scheme for IoT environments, along with corresponding circuit simulations and performance analysis. The scheme models the data owner's index and the query user's range as private sets, with the query range being determined through our quantum private set similarity comparison protocol. The query results are then securely transmitted via QKD and QSDC protocols. In the quantum private set similarity comparison protocol, we first employ a QKD protocol to establish keys and encode private sets into quantum states. Then, quantum homomorphic encryption with CNOT evaluation is used to perform privacy-preserving data comparisons, enabling the comparison of set similarity. Our proposed quantum privacy-preserving range query scheme ensures long-term security with the help of quantum cryptography.

Moreover, our scheme requires only simple and easily prepared quantum states, such as Bell states and single-photon states, as information carriers. Users need only perform basic operations like CNOT, X, and Z gates and projection measurements. This makes the protocol feasible for practical implementation in the IoT ecosystem.

Author Contributions: Conceptualization, J.L.; Writing—original draft, C.-Q.Y.; Writing—review & editing, X.-Y.C.; Supervision, J.L. and X.-Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China, No. 61871347.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xing, L. Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet Things J.* **2020**, *7*, 6704–6721. [CrossRef]
2. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things* **2021**, *14*, 100129. [CrossRef]
3. Li, D.S.; Cao, J.; Lu, X.C.; Chan, K.C. Efficient range query processing in peer-to-peer systems. *IEEE Trans. Knowl. Data Eng.* **2008**, *21*, 78–91. [CrossRef]
4. Li, M.; Gao, J.; Zhang, Z.; Conti, M.; Alazab, M. Secure, Available, Verifiable, and Efficient Range Query Processing on Outsourced Datasets. In Proceedings of the ICC 2024-IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024 ; IEEE: Piscataway, NJ, USA, 2024; pp. 1376–1381.
5. Shi, E.; Bethencourt, J.; Chan, T.H.; Song, D.; Perrig, A. Multi-dimensional range query over encrypted data. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Berkeley, CA, USA, 20–23 May 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 350–364.
6. Zheng, Y.; Lu, R.; Guan, Y.; Shao, J.; Zhu, H. Efficient and privacy-preserving similarity range query over encrypted time series data. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2501–2516. [CrossRef]
7. Li, K.C.; Shi, R.H.; Guo, W.P.; Wang, P.B.; Shao, B.S. Dynamic range query privacy-preserving scheme for blockchain-enhanced smart grid based on lattice. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 1652–1664. [CrossRef]
8. Lu, R. A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT. *IEEE Internet Things J.* **2018**, *6*, 2497–2505. [CrossRef]
9. Sciancalepore, S.; Di Pietro, R. PPRQ: Privacy-preserving MAX/MIN range queries in IoT networks. *IEEE Internet Things J.* **2020**, *8*, 5075–5092. [CrossRef]
10. Zhou, M.; Zheng, Y.; Guan, Y.; Peng, L.; Lu, R. Efficient and privacy-preserving range-max query in fog-based agricultural IoT. *Peer-Peer Netw. Appl.* **2021**, *14*, 2156–2170. [CrossRef]
11. Min, Z.; Yang, G.; Wang, J.; Kim, G.J. A privacy-preserving BGN-type parallel homomorphic encryption algorithm based on LWE. *J. Internet Technol.* **2019**, *20*, 2189–2200.
12. Monz, T.; Nigg, D.; Martinez, E.A.; Brandl, M.F.; Schindler, P.; Rines, R.; Wang, S.X.; Chuang, I.L.; Blatt, R. Realization of a scalable Shor algorithm. *Science* **2016**, *351*, 1068–1070. [CrossRef]
13. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
14. Xu, D.; Yu, K.; Ritcey, J.A. Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0. *IEEE Trans. Ind. Inform.* **2021**, *18*, 6368–6378. [CrossRef]
15. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **2013**, *15*, 113007. [CrossRef]
16. Shi, R.H.; Yu, H. Privacy-preserving range query quantum scheme with single photons in edge-based Internet of Things. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 4923–4936. [CrossRef]
17. Shi, R.H.; Fang, X.Q. Quantum scheme for privacy-preserving range max/min query in edge-based internet of things. *IEEE Trans. Netw. Serv. Manag.* **2024** . [CrossRef]
18. Broadbent, A.; Jeffery, S. Quantum homomorphic encryption for circuits of low T-gate complexity. In Proceedings of the Annual Cryptology Conference, Barbara, CA, USA, 16–20 August 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 609–629.
19. Tan, S.H.; Kettlewell, J.A.; Ouyang, Y.; Chen, L.; Fitzsimons, J.F. A quantum approach to homomorphic encryption. *Sci. Rep.* **2016**, *6*, 33467. [CrossRef]
20. Zhang, J.W.; Xu, G.; Chen, X.B.; Chang, Y.; Dong, Z.C. Improved multiparty quantum private comparison based on quantum homomorphic encryption. *Phys. A Stat. Mech. Its Appl.* **2023**, *610*, 128397. [CrossRef]
21. Niwattanakul, S.; Singthongchai, J.; Naenudorn, E.; Wanapu, S. Using of Jaccard coefficient for keywords similarity. In Proceedings of the International Multiconference of Engineers and Computer Scientists, Kowloon, Hong Kong, 13–15 March 2013; Voume 1, pp. 380–384.
22. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
23. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef]

24. Li, X.; Zhang, K.; Zhang, L.; Zhao, X. A new quantum multiparty simultaneous identity authentication protocol with the classical third-party. *Entropy* **2022**, *24*, 483. [CrossRef]
25. Sutradhar, K. A quantum cryptographic protocol for secure vehicular communication. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 3513–3522. [CrossRef]
26. Schiavon, M.; Vallone, G.; Ticozzi, F.; Villoresi, P. Heralded single-photon sources for quantum-key-distribution applications. *Phys. Rev. A* **2016**, *93*, 012331. [CrossRef]
27. Zhou, L.; Xu, B.W.; Zhong, W.; Sheng, Y.B. Device-independent quantum secure direct communication with single-photon sources. *Phys. Rev. Appl.* **2023**, *19*, 014036. [CrossRef]
28. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
29. Fuguo, D.; Guilu, L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *69*, 052319.