



Article

New Quantum Private Comparison Using Four-Particle Cluster State

Min Hou^{1,2} , Yue Wu¹ and Shibin Zhang^{3,4,*} 

¹ School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China; houmin@scujj.edu.cn (M.H.); ywu@uestc.edu.cn (Y.W.)

² Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China

³ School of Cybersecurity (Xin Gu Industrial College), Chengdu University of Information Technology, Chengdu 610225, China

⁴ Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu University of Information Technology, Chengdu 610225, China

* Correspondence: cuitzsb@cuit.edu.cn

Abstract: Quantum private comparison (QPC) enables two users to securely conduct private comparisons in a network characterized by mutual distrust while guaranteeing the confidentiality of their private inputs. Most previous QPC protocols were primarily used to determine the equality of private information between two users, which constrained their scalability. In this paper, we propose a QPC protocol that leverages the entanglement correlation between particles in a four-particle cluster state. This protocol can compare the information of two groups of users within one protocol execution, with each group consisting of two users. A semi-honest third party (TP), who will not deviate from the protocol execution or conspire with any participant, is involved in assisting users to achieve private comparisons. Users encode their inputs into specific angles of rotational operations performed on the received quantum sequence, which is then sent back to TP. Security analysis shows that both external attacks and insider threats are ineffective at stealing private data. Finally, we compare our protocol with some previously proposed QPC protocols.

Keywords: quantum private comparison (QPC); four-particle cluster state; entanglement correlation; rotation operation



Citation: Hou, M.; Wu, Y.; Zhang, S. New Quantum Private Comparison Using Four-Particle Cluster State. *Entropy* **2024**, *26*, 512. <https://doi.org/10.3390/e26060512>

Academic Editor: Rosario Lo Franco

Received: 15 May 2024

Revised: 11 June 2024

Accepted: 12 June 2024

Published: 14 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Traditional classical cryptography primarily relies on secure encryption methods, such as symmetrical secret key encryption and asymmetrical secret key encryption, as essential components for safeguarding private information. However, secure encryption methods face severe challenges due to the development of quantum computing and the advancements of Shor's algorithm [1] and Grover's algorithm [2]. In this context, quantum cryptography has emerged, leveraging the principles of quantum mechanics to enhance the security and privacy of information processing tasks in the communication process. Various quantum cryptography protocols, such as quantum key distribution (QKD) [3–6], quantum key agreement (QKA) [7,8], and quantum secure direct communication [9–11], have emerged to address various tasks.

Quantum private comparison, which originated from solving the millionaire's problem proposed by Yao [12] by combining quantum mechanics and private comparison, enables two users to securely perform private comparisons in a network of mutual distrust while keeping their private inputs undisclosed to each other and potential eavesdroppers. For a QPC protocol, the key is to ensure the security of the private inputs (meaning each user cannot access the secret data of the other, even if they have some intermediate data from the protocol execution) and the fairness of the comparison results (meaning both users are

aware of the final comparison result). Furthermore, Lo [13] pointed out that evaluating the equality function in a two-party setting is impossible. A semi-honest third party (TP) is involved to assist two users in comparing their secrets and announcing the results to each user. In this context, the private information should be processed and encrypted to prevent the disclosure of secrets to the parties involved in the comparison and to eliminate the possibility of inferring the secrets.

The original QPC protocol was proposed by Yang and Wen, who used EPR states and unitary operations to compare the equality of the secrets [14]. The security of private information is ensured by using decoy photons and hash functions. Subsequently, Chen et al. [15] utilized triplet GHZ states to propose an efficient QPC protocol. In this protocol, secrets are divided into multiple groups, which improves efficiency by eliminating the need to compare all groups of information. Since then, different QPC protocols have been continuously proposed, aiming to determine the relationship between private and these studies mainly utilize various quantum states, including single photons [16–23], Bell states [24–33], entangled states [34–39], cluster states [40–45] and d-level quantum states [46–49] as quantum resources. They also employ different quantum technologies, such as entanglement swapping and unitary operations, as well as determine whether to distribute keys for sharing secret keys to accomplish the comparison.

In 2020, Lang [50] utilized quantum gates instead of bitwise XOR operations to design a QPC protocol, eliminating classical computation and enhancing security by reducing attacks from classical attackers. In 2021, Huang et al. [51] utilized the entanglement swapping of Bell states to propose a QPC protocol and a QKD protocol for sharing secret keys to ensure the security of private inputs. In 2022, Fan et al. [52] utilized eight-qubit entangled states as quantum resources for private comparison and secret keys generated by QKD protocols to ensure security. In 2023, Liu et al. [53] employed 4D GHZ-like entangled states to design the QPC protocol, where one classical bit can be compared in each comparison. This protocol also needs a QKD protocol to share secret keys before the protocol begins. In 2024, Hou and Wu [54] designed a protocol for equality comparison using single photons and unitary operations. To prevent the disclosure of private inputs to the parties, QKD protocols are used to share secret keys for encrypting confidential information.

By analyzing the above QPC protocols, we can see that the majority of them involve two participants, and the private information of both participants can be compared within one protocol execution. To improve scalability, we propose a QPC protocol that leverages the entanglement correlation among particles in four-particle cluster states. This protocol can compare the information of two groups of users within one protocol execution, with each group consisting of two users. A semi-honest third party (TP), who will not deviate from the protocol execution or conspire with any participant, is involved in assisting the users to achieve private comparisons. Users encode their inputs into specific angles of rotational operations performed on the received quantum sequence, which is then returned to TP.

Compared with some previously proposed QPC protocols, our protocol maintains improved scalability by comparing the private information of two groups of users within one protocol execution. It utilizes four-particle cluster states, rotation operations, and single-particle measurements as the main quantum technologies without the need for high-dimensional quantum states, entanglement swapping, or joint measurements, making it more practical. Additionally, the security has been further enhanced because no classical results are produced. Security analysis shows that the proposed protocol is resistant to both outsider and insider attacks.

The rest of this paper is organized as follows: In Section 2, the steps of the proposed QPC protocol are described. The correctness of the protocol is shown in Section 3. The security analysis is provided in Section 4. The efficiency analysis and comparison are presented in Section 5. Finally, we will summarize our work in Section 6.

2. Quantum Private Comparison Protocol

2.1. Preliminaries

The four-particle cluster state is given by

$$|\Phi\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{1234} \tag{1}$$

By observing Equation (1), we can see that particles 1 and 2 are identical when measurements are performed on them with the Z-basis or X-basis. Similarly, particles 3 and 4 are also identical when measurements are performed on them using the Z-basis or X-basis.

The rotation operation is defined as

$$R_y(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \tag{2}$$

Equation (2) can be regarded as a unitary operation implemented by rotating an angle θ around the y-axis on the Bloch sphere.

Theorem 1. When performing the rotation operation $R_y(\theta)$ on the single qubit state $|0\rangle$ or $|1\rangle$, we can obtain a superposition state where both $|0\rangle$ and $|1\rangle$ exist simultaneously.

Proof. When performing the rotation operation $R_y(\theta)$ on $|0\rangle$, the resultant state can be written as

$$|\psi_0\rangle = R_y(\theta)|0\rangle = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} \end{pmatrix} = \cos \frac{\theta}{2}|0\rangle + \sin \frac{\theta}{2}|1\rangle \tag{3}$$

When performing the rotation operation $R_y(\theta)$ on $|1\rangle$, the resultant state can be written as

$$|\psi_1\rangle = R_y(\theta)|1\rangle = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin \frac{\theta}{2} \\ \cos \frac{\theta}{2} \end{pmatrix} = -\sin \frac{\theta}{2}|0\rangle + \cos \frac{\theta}{2}|1\rangle \tag{4}$$

It can be easily seen that both $|\psi_0\rangle$ and $|\psi_1\rangle$ are superposition states. Therefore, Theorem 1 holds.

Theorem 2. When performing the rotation operation $R_y(\theta)$ on an arbitrary single qubit state $|\psi\rangle$ to obtain a resultant state $|\psi'\rangle$, we can recover $|\psi\rangle$ by performing the inverse rotation operation $R_y(-\theta)$ on $|\psi'\rangle$.

Proof. An arbitrary single qubit state can be written as

$$|\psi\rangle = \cos \frac{\theta_1}{2}|0\rangle + e^{i\varphi} \sin \frac{\theta_1}{2}|1\rangle \tag{5}$$

When performing the rotation operation $R_y(\theta)$ on $|\psi\rangle$, the resultant state can be given by

$$\begin{aligned} |\psi'\rangle &= R_y(\theta)|\psi\rangle = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \cos \frac{\theta_1}{2} \\ e^{i\varphi} \sin \frac{\theta_1}{2} \end{pmatrix} = \begin{pmatrix} \cos \frac{\theta}{2} \cos \frac{\theta_1}{2} - e^{i\varphi} \sin \frac{\theta}{2} \sin \frac{\theta_1}{2} \\ \sin \frac{\theta}{2} \cos \frac{\theta_1}{2} + e^{i\varphi} \cos \frac{\theta}{2} \sin \frac{\theta_1}{2} \end{pmatrix} \\ &= \left(\cos \frac{\theta}{2} \cos \frac{\theta_1}{2} - e^{i\varphi} \sin \frac{\theta}{2} \sin \frac{\theta_1}{2} \right) |0\rangle + \left(\sin \frac{\theta}{2} \cos \frac{\theta_1}{2} + e^{i\varphi} \cos \frac{\theta}{2} \sin \frac{\theta_1}{2} \right) |1\rangle \end{aligned} \tag{6}$$

When performing the rotation operation $R_y(-\theta)$ on $|\psi'\rangle$, we have the following equation:

$$\begin{aligned}
 R(-\theta)|\psi\rangle' &= \begin{pmatrix} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ -\sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \cos \frac{\theta}{2} \cos \frac{\theta_1}{2} - e^{i\varphi} \sin \frac{\theta}{2} \sin \frac{\theta_1}{2} \\ \sin \frac{\theta}{2} \cos \frac{\theta_1}{2} + e^{i\varphi} \cos \frac{\theta}{2} \sin \frac{\theta_1}{2} \end{pmatrix} = \begin{pmatrix} \cos \frac{\theta_1}{2} \\ e^{i\varphi} \sin \frac{\theta_1}{2} \end{pmatrix} \\
 &= \cos \frac{\theta_1}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta_1}{2} |1\rangle = |\psi\rangle
 \end{aligned} \tag{7}$$

From Equations (6) and (7), we can see that performing rotation operations $R_y(\theta)$ and $R_y(-\theta)$ on $|\psi\rangle$ is equivalent to performing the operation I on $|\psi\rangle$. In other words, $|\psi\rangle$ will be no change.

Therefore, Theorem 2 holds.

2.2. Protocol Description

The participants in our protocol are introduced as follows:

TP: TP is a semi-honest third party involved in facilitating the comparison of private information. TP has complete quantum capabilities, such as the preparation and measurement of quantum states. Moreover, since our protocol is designed in the semi-honest model, TP must strictly follow the specified steps. While TP may attempt to behave improperly to steal private information by exploiting immediate results and employing certain attack strategies, it is prohibited from colluding with or favoring any user involved.

Users: There are two groups of users: Alice, Bob, Charlie, and Dove. Alice and Bob form one group, while Charlie and Dove form another group. Both of them also have complete quantum capabilities similar to TP, and they are honest but curious. They follow the defined protocol and may try to access the private information of other users.

Assuming that the private information of Alice, Bob, Charlie, and Dove is expressed as $A = \{a_1, a_2, a_3, \dots, a_L\}$, $B = \{b_1, b_2, b_3, \dots, b_L\}$, $C = \{c_1, c_2, c_3, \dots, c_L\}$, $D = \{d_1, d_2, d_3, \dots, d_L\}$, where L is the length of private information. All a_i, b_i, c_i and d_i belong to 0 or 1, representing the i -th position of the bit in A, B, C , and D , respectively. The detailed steps of our protocol are described as follows:

Step 1. Alice and Bob utilize the QKD protocol (e.g., the BB84 protocol [3]) for sharing an L -length secret key $X_i = \{x_1, x_2, \dots, x_L\}$, where $x_i \in \{0, 1\}$. In the same way, Charlie and Dove share an L -length secret key $Y_i = \{y_1, y_2, \dots, y_L\}$, where $y_i \in \{0, 1\}$.

Step 2. TP prepares some ordered four-particle cluster states in $|\Phi\rangle_{1234}$, and divides them into four sequences S_1, S_2, S_3, S_4 , where S_i is composed of all the i -th particles of each four-particle cluster state.

Step 3. TP prepares 4δ decoy photons chosen from four single-qubit states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ randomly. Then, TP chooses these 4δ decoy photons and inserts them into the sequences S_1, S_2, S_3, S_4 in the same quantity. The positions where these photons are inserted are random. Due to the insertion of decoy photons, the sequences S_1, S_2, S_3, S_4 are converted into S'_1, S'_2, S'_3, S'_4 . TP records the positions and states of the inserted photons. It must be noted that the number of decoy photons δ can be any integer, but it should be sufficiently large. Finally, TP sends S'_1, S'_2, S'_3, S'_4 to Alice, Bob, Charlie, and Dove, respectively.

Step 4. When receiving the sequence transmitted from TP, Alice, Bob, Charlie, and Dove send an acknowledgment message to TP, who interacts with them to conduct eavesdropping detection. TP announces the inserted positions and basis of the decoy photons in S'_1, S'_2, S'_3, S'_4 . Alice, Bob, Charlie, and Dove measure these decoy photons in S'_1, S'_2, S'_3, S'_4 and send the measurement results to TP. TP will then determine whether eavesdroppers exist in the quantum channel by comparing the consistency of the initially-prepared decoy photons with the measurement results and calculating the error rate. If the error rate exceeds a predefined value, eavesdroppers will undoubtedly be present in the transmission process, leading to the termination and restart of the protocol.

Step 5. Alice, Bob, Charlie, and Dove discard decoy photons in S'_1, S'_2, S'_3, S'_4 , respectively, to recover S_1, S_2, S_3, S_4 . Thereafter, Alice, Bob, Charlie, and Dove perform the rotation operations $R_y(\pi x_i + \pi a_i)$, $R_y(\pi x_i + \pi b_i)$, $R_y(\pi y_i + \pi c_i)$, and $R_y(\pi y_i + \pi d_i)$ on

the i -th position of the qubit in S_1, S_2, S_3 and S_4 to get the sequences S_A, S_B, S_C and S_D , respectively.

Step 6. Alice, Bob, Charlie, and Dove generate their own secret keys $\Theta_A = \{ka_1, ka_2, \dots, ka_L\}$, $\Theta_B = \{kb_1, kb_2, \dots, kb_L\}$, $\Theta_C = \{kc_1, kc_2, \dots, kc_L\}$, and $\Theta_D = \{kd_1, kd_2, \dots, kd_L\}$, respectively. Then, Alice, Bob, Charlie, and Dove perform the rotation operations $R_y(ka_i)$, $R_y(kb_i)$, $R_y(kc_i)$, and $R_y(kd_i)$ on the i -th position of the qubit in S_A, S_B, S_C and S_D to get the sequences $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} , respectively. To prevent eavesdropping, they insert randomly chosen δ decoy photons into $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} in random positions to get the sequences $S'_{Enc_A}, S'_{Enc_B}, S'_{Enc_C}$ and S'_{Enc_D} . Finally, all of the sequences are sent to TP.

Step 7. Upon receiving all sequences, TP interacts with Alice, Bob, Charlie, and Dove to conduct eavesdropping detection in the same way as discussed in Step 4. Once no eavesdropper is detected on the communication channel, Alice, Bob, Charlie, and Dove announce the secret keys $\Theta_A, \Theta_B, \Theta_C$, and Θ_D to TP.

Step 8. TP discards decoy photons in $S'_{Enc_A}, S'_{Enc_B}, S'_{Enc_C}$ and S'_{Enc_D} to recover $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} , and performs the rotation operations $R_y(-ka_i)$, $R_y(-kb_i)$, $R_y(-kc_i)$, and $R_y(-kd_i)$ on the i -th position of the qubit in $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} to recover S_A, S_B, S_C and S_D . Then, TP measures S_A, S_B, S_C and S_D with Z-basis to obtain the measurement results. If all measurement results of Alice and Bob are the same, $A = B$. Otherwise $A \neq B$. If all measurement results of Charlie and Dove are the same, $C = D$. Otherwise $C \neq D$.

3. Correctness

3.1. An Example of the Proposed Protocol

Suppose that Alice and Bob intend to determine the equality of their private information $A = 110101$ and $B = 110101$. Charlie and Dove aim to determine whether their private information C and D are equal, where $C = 101100$ and $D = 111110$. Intuitively speaking, we can conclude that $A = B$ and $C \neq D$.

In order to verify the correctness of our protocol, we use the private information mentioned above as an example. We do not consider eavesdropping detection because the decoy photons in each eavesdropping detection are randomly inserted into the quantum sequence and discarded by the receiver when no eavesdropping occurs. In our protocol, suppose that the L -length secret key shared between Alice and Bob is $X = \{1, 1, 0, 1, 0, 0\}$, while the L -length secret key shared between Charlie and Dove is $Y = \{0, 1, 1, 1, 0, 0\}$.

TP prepares six four-particle clusters and divides them into four sequences S_1, S_2, S_3, S_4 . We can know that the sequences S_1 and S_2 are the same, while the sequences S_3 and S_4 are also identical.

When receiving the sequences S_1, S_2, S_3, S_4 , Alice, Bob, Charlie, and Dove perform the rotation operations $\{R_y(2\pi), R_y(2\pi), R_y(0), R_y(2\pi), R_y(0), R_y(\pi)\}$, $\{R_y(2\pi), R_y(2\pi), R_y(0), R_y(2\pi), R_y(0), R_y(\pi)\}$, $\{R_y(\pi), R_y(\pi), R_y(2\pi), R_y(2\pi), R_y(0), R_y(0)\}$, and $\{R_y(\pi), R_y(2\pi), R_y(2\pi), R_y(2\pi), R_y(\pi), R_y(0)\}$ corresponding to the private information on each qubit in S_1, S_2, S_3 and S_4 to get the sequences S_A, S_B, S_C and S_D , respectively. Afterwards, Alice, Bob, Charlie, and Dove perform the rotation operations $R_y(\Theta_A), R_y(\Theta_B), R_y(\Theta_C)$, and $R_y(\Theta_D)$ on S_A, S_B, S_C and S_D to get the sequences $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} . TP performs the rotation operations $R_y(-\Theta_A), R_y(-\Theta_B), R_y(-\Theta_C)$, and $R_y(-\Theta_D)$ on $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} to recover S_A, S_B, S_C and S_D . Finally, TP measures S_A, S_B, S_C and S_D with a Z-basis to obtain the measurement results and determine the comparison results.

Without loss of generality, suppose that $S_1 = S_2 = \{|0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |0\rangle\}$ and $S_3 = S_4 = \{|1\rangle, |0\rangle, |1\rangle, |0\rangle, |1\rangle, |1\rangle\}$. When performing the above rotation operations on S_1, S_2, S_3 and S_4 , the resultant sequences are as follows:

$$S_A = \{R_y(2\pi)|0\rangle, R_y(2\pi)|1\rangle, R_y(0)|0\rangle, R_y(2\pi)|0\rangle, R_y(0)|1\rangle, R_y(\pi)|0\rangle\} \\ = \{-|0\rangle, -|1\rangle, |0\rangle, -|0\rangle, |1\rangle, |1\rangle\} \tag{8}$$

$$S_B = \{R_y(2\pi)|0\rangle, R_y(2\pi)|1\rangle, R_y(0)|0\rangle, R_y(2\pi)|0\rangle, R_y(0)|1\rangle, R_y(\pi)|0\rangle\} \\ = \{-|0\rangle, -|1\rangle, |0\rangle, -|0\rangle, |1\rangle, |1\rangle\} \tag{9}$$

$$S_C = \{R_y(\pi)|1\rangle, R_y(\pi)|0\rangle, R_y(2\pi)|1\rangle, R_y(2\pi)|0\rangle, R_y(0)|1\rangle, R_y(0)|1\rangle\} \\ = \{-|0\rangle, |1\rangle, -|1\rangle, -|0\rangle, |1\rangle, |1\rangle\} \tag{10}$$

$$S_D = \{R_y(\pi)|1\rangle, R_y(2\pi)|0\rangle, R_y(2\pi)|1\rangle, R_y(2\pi)|0\rangle, R_y(\pi)|1\rangle, R_y(0)|1\rangle\} \\ = \{-|0\rangle, -|0\rangle, -|1\rangle, -|0\rangle, -|0\rangle, |1\rangle\} \tag{11}$$

Assuming that the secret keys each user generated are $\Theta_A = \{\pi, \frac{\pi}{6}, \frac{3\pi}{4}, \frac{11\pi}{9}, \frac{3\pi}{2}, \frac{9\pi}{8}\}$, $\Theta_B = \{\frac{\pi}{7}, \frac{4\pi}{11}, \frac{5\pi}{8}, \frac{\pi}{2}, \frac{7\pi}{4}, \frac{9\pi}{17}\}$, $\Theta_C = \{\frac{5\pi}{6}, \frac{5\pi}{8}, \frac{2\pi}{3}, \frac{8\pi}{7}, \frac{11\pi}{9}, \frac{9\pi}{16}\}$, $\Theta_D = \{\frac{17\pi}{36}, \frac{3\pi}{2}, \frac{7\pi}{4}, \frac{\pi}{9}, \frac{13\pi}{19}, \frac{11\pi}{6}\}$. When performing the rotation operations $R_y(\Theta_A)$, $R_y(\Theta_B)$, $R_y(\Theta_C)$, and $R_y(\Theta_D)$ on S_A, S_B, S_C and S_D , the resulting sequences are given by

$$S_{Enc_A} = R(\Theta_A)S_A = \left\{ \begin{array}{l} -R_y(\pi)|0\rangle, -R_y(\frac{\pi}{6})|1\rangle, R_y(\frac{3\pi}{4})|0\rangle, \\ -R_y(\frac{11\pi}{9})|0\rangle, R_y(\frac{3\pi}{2})|1\rangle, R_y(\frac{9\pi}{8})|1\rangle \end{array} \right\} \tag{12}$$

$$S_{Enc_B} = R(\Theta_B)S_B = \left\{ \begin{array}{l} -R_y(\frac{\pi}{7})|0\rangle, -R_y(\frac{4\pi}{11})|1\rangle, R_y(\frac{5\pi}{8})|0\rangle, \\ -R_y(\frac{\pi}{2})|0\rangle, R_y(\frac{7\pi}{4})|1\rangle, R_y(\frac{9\pi}{17})|1\rangle \end{array} \right\} \tag{13}$$

$$S_{Enc_C} = R(\Theta_C)S_C = \left\{ \begin{array}{l} -R_y(\frac{5\pi}{6})|0\rangle, R_y(\frac{5\pi}{8})|1\rangle, -R_y(\frac{2\pi}{3})|1\rangle, \\ -R_y(\frac{8\pi}{7})|0\rangle, R_y(\frac{11\pi}{9})|1\rangle, R_y(\frac{9\pi}{16})|1\rangle \end{array} \right\} \tag{14}$$

$$S_{Enc_D} = R(\Theta_D)S_D = \left\{ \begin{array}{l} -R_y(\frac{17\pi}{36})|0\rangle, -R_y(\frac{3\pi}{2})|0\rangle, -R_y(\frac{7\pi}{4})|1\rangle, \\ -R_y(\frac{\pi}{9})|0\rangle, -R_y(\frac{13\pi}{19})|0\rangle, R_y(\frac{11\pi}{6})|1\rangle \end{array} \right\} \tag{15}$$

According to Theorem 2, we can know that S_A, S_B, S_C and S_D can be recovered by performing the rotation operations $R_y(-\Theta_A)$, $R_y(-\Theta_B)$, $R_y(-\Theta_C)$, and $R_y(-\Theta_D)$ on $S_{Enc_A}, S_{Enc_B}, S_{Enc_C}$ and S_{Enc_D} . This process can be expressed as

$$R(-\Theta_A)S_{Enc_A} = \left\{ \begin{array}{l} -R_y(-\pi)R_y(\pi)|0\rangle, -R_y(-\frac{\pi}{6})R_y(\frac{\pi}{6})|1\rangle, \\ R_y(-\frac{3\pi}{4})R_y(\frac{3\pi}{4})|0\rangle, -R_y(-\frac{11\pi}{9})R_y(\frac{11\pi}{9})|0\rangle, \\ R_y(-\frac{3\pi}{2})R_y(\frac{3\pi}{2})|1\rangle, R_y(-\frac{9\pi}{8})R_y(\frac{9\pi}{8})|1\rangle \end{array} \right\} \tag{16} \\ = \{-|0\rangle, -|1\rangle, |0\rangle, |0\rangle, |1\rangle, |1\rangle\} = S_A$$

$$R(-\Theta_B)S_{Enc_B} = \left\{ \begin{array}{l} -R_y(-\frac{\pi}{7})R_y(\frac{\pi}{7})|0\rangle, -R_y(-\frac{4\pi}{11})R_y(\frac{4\pi}{11})|1\rangle, \\ R_y(-\frac{5\pi}{8})R_y(\frac{5\pi}{8})|0\rangle, -R_y(-\frac{\pi}{2})R_y(\frac{\pi}{2})|0\rangle, \\ R_y(-\frac{7\pi}{4})R_y(\frac{7\pi}{4})|1\rangle, R_y(-\frac{9\pi}{17})R_y(\frac{9\pi}{17})|1\rangle \end{array} \right\} \tag{17} \\ = \{-|0\rangle, -|1\rangle, |0\rangle, -|0\rangle, |1\rangle, |1\rangle\} = S_B$$

$$R(-\Theta_C)S_{Enc_C} = \left\{ \begin{array}{l} -R_y(-\frac{5\pi}{6})R_y(\frac{5\pi}{6})|0\rangle, R_y(-\frac{5\pi}{8})R_y(\frac{5\pi}{8})|1\rangle, \\ -R_y(-\frac{2\pi}{3})R_y(\frac{2\pi}{3})|1\rangle, -R_y(-\frac{8\pi}{7})R_y(\frac{8\pi}{7})|0\rangle, \\ R_y(-\frac{11\pi}{9})R_y(\frac{11\pi}{9})|1\rangle, R_y(-\frac{9\pi}{16})R_y(\frac{9\pi}{16})|1\rangle \end{array} \right\} \tag{18} \\ = \{-|0\rangle, |1\rangle, -|1\rangle, -|0\rangle, |1\rangle, |1\rangle\} = S_C$$

$$\begin{aligned}
 R(-\Theta_D)S_{Enc_D} &= \left\{ \begin{array}{l} -R_y\left(-\frac{17\pi}{36}\right)R_y\left(\frac{17\pi}{36}\right)|0\rangle, -R_y\left(-\frac{3\pi}{2}\right)R_y\left(\frac{3\pi}{2}\right)|0\rangle, \\ -R_y\left(-\frac{7\pi}{4}\right)R_y\left(\frac{7\pi}{4}\right)|1\rangle, -R_y\left(-\frac{\pi}{9}\right)R_y\left(\frac{\pi}{9}\right)|0\rangle, \\ -R_y\left(-\frac{13\pi}{19}\right)R_y\left(\frac{13\pi}{19}\right)|0\rangle, R_y\left(-\frac{11\pi}{6}\right)R_y\left(\frac{11\pi}{6}\right)|1\rangle \end{array} \right\} \quad (19) \\
 &= \{|-0\rangle, |-0\rangle, -|1\rangle, -|0\rangle, -|0\rangle, |1\rangle\} = S_D
 \end{aligned}$$

When conducting measurements on S_A, S_B, S_C and S_D with Z-basis, TP can obtain the measurement results $MR_A = \{|0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |1\rangle\}$, $MR_B = \{|0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |1\rangle\}$, $MR_C = \{|0\rangle, |1\rangle, |1\rangle, |0\rangle, |1\rangle, |1\rangle\}$, and $MR_D = \{|0\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle\}$. It can be easily seen that the measurement results of MR_A and MR_B are equal, which indicates that $A = B$. The measurement results of MR_C and MR_D are different, which indicates that $C \neq D$.

In conclusion, the above example reveals the correctness of our protocol.

3.2. Quantum Circuit Simulation

Without loss of generality, we assume that Alice’s bit is $A = 1$ and Bob’s bit is $B = 0$. Both the bits of Charlie and Dove are $C = D = 1$. We can conclude that the bits of Alice and Bob are different, while the bits of Charlie and Dove are identical. Suppose that the secret key shared between Alice and Bob is 1, while the secret key shared between Charlie and Dove is 0. The secret keys generated by each user are $\Theta_A = \frac{3\pi}{2}$, $\Theta_B = \frac{5\pi}{8}$, $\Theta_C = \frac{2\pi}{3}$, $\Theta_D = \frac{\pi}{9}$. The quantum circuit of this process can be seen in Figure 1, and the probability of its outputs is provided in Figure 2.

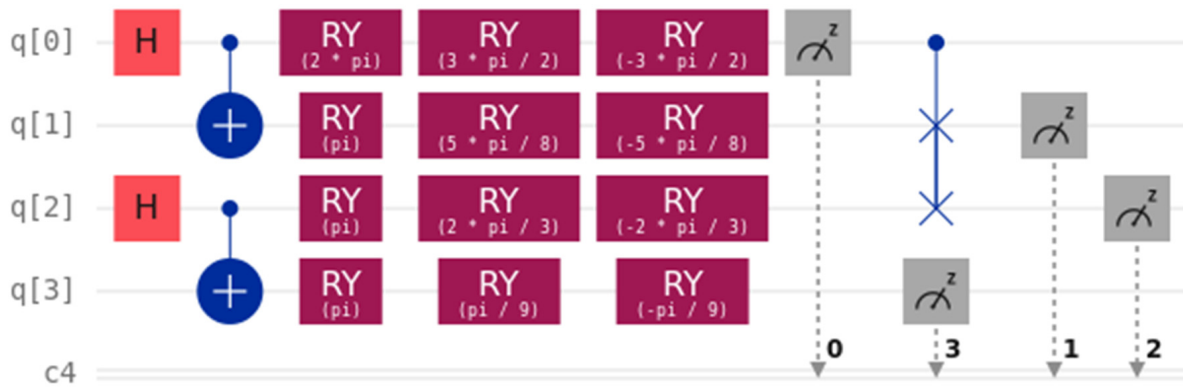


Figure 1. Quantum circuit.

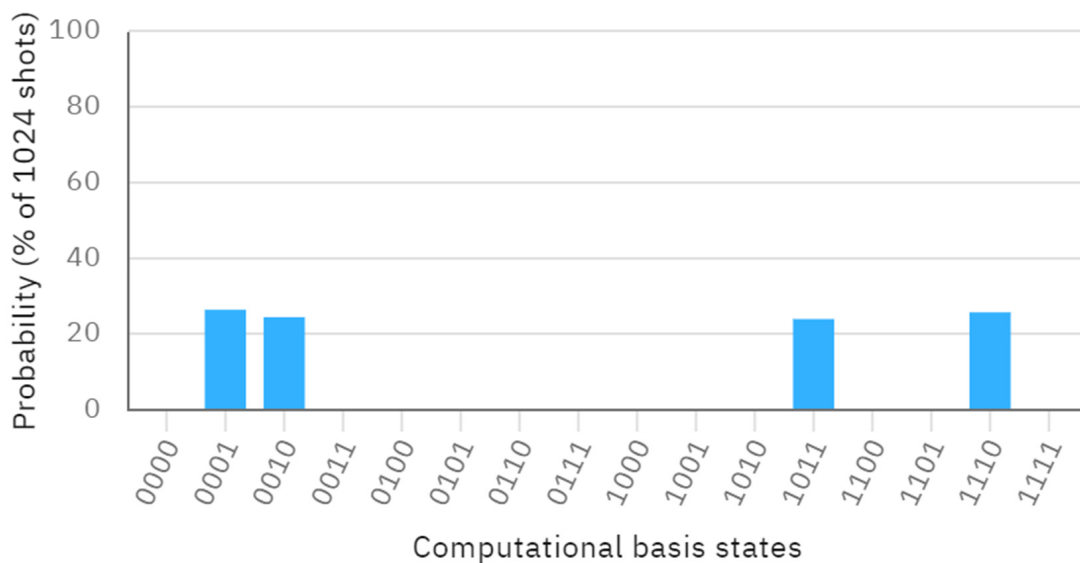


Figure 2. The probability visualization.

From Figure 2, the measurement outcomes of $q[0]$, $q[1]$, $q[2]$, and $q[3]$ yield four probability states $|1000\rangle$, $|0100\rangle$, $|1011\rangle$ and $|0111\rangle$. We can observe that the measurement results of $q[0]$ and $q[1]$ are different, while the measurement results of $q[2]$ and $q[3]$ are identical. This further indicates that the bits of Alice and Bob are different, and the bits of Charlie and Dove are identical. Our protocol has been shown to be feasible and correct through a concrete example. By increasing the number of qubits, we can extend the quantum circuit simulation to compare more classical bits.

4. Security Analysis

4.1. External Attacks

An external eavesdropper, Eve, may conduct a series of quantum attack strategies, such as intercept-measure-resend attacks, entangle-measure attacks, and Trojan Horse attacks to steal the private information of the users. However, these attack strategies fall short of achieving this goal due to the decoy-state method adopted in our protocol [55].

4.1.1. Intercept-Measure-Resend Attack

Eve may intercept the sequences transmitted on the communication channel, measure the intercepted sequences with guessed bases to steal the private information of users, and resend a fabricated sequence replacing the intercepted sequences to the original receiver. However, this malicious behavior will result in the error rate exceeding a predefined value during eavesdropping detection, leading to the termination of the protocol. This is because Eve has no chance to distinguish between the inserted decoy photons and the target particles, and the measurement bases are also unknown to her. For one intercepted decoy photon, there is a 50% chance that Eve can correctly guess the measurement base and bypass the detection eavesdropping. Also, there is a 50% probability that Eve chooses the wrong measurement base and can bypass detection eavesdropping with a 50% probability. In other words, if Eve chooses the wrong measurement base, the probability of Eve bypassing the detection of eavesdropping is 25%. For example, without loss of generality, assume that a decoy photon stays in state $|1\rangle$. When choosing the Z-basis to measure it, Eve can get a measurement result denoted as $|1\rangle$. Eve prepares a quantum state $|1\rangle$ and sends it to the receiver. When conducting eavesdropping detection, no errors occur due to the consistency between the initially prepared decoy photon and the measurement results. In this case, Eve can bypass the eavesdropping detection with a probability of 1 when choosing the Z-basis. When Eve chooses the X-basis to measure the decoy photon, the measurement result is $|+\rangle$ or $|-\rangle$. Eve prepares quantum states $|+\rangle$ or $|-\rangle$, and sends them to the receiver. When conducting eavesdropping detection, there is a 50% probability that Eve will not introduce an error. Eve can bypass eavesdropping detection with a probability of 25% when choosing the X-basis. An example of this process is shown in Table 1.

Table 1. The example that Eve eavesdrops the decoy photon with state $|1\rangle$.

State of a Decoy Photon		$ 1\rangle$			
Guesses measurement basis from Eve	Z-basis	X-basis			
Measurement result for Eve	$ 1\rangle$	$ +\rangle$	$ -\rangle$		
The fake state that Eve prepares	$ 1\rangle$	$ +\rangle$	$ -\rangle$		
Measurement basis from the receiver	Z-basis	Z-basis			
Measurement result of the receiver	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
Does it introduce an error?	No	Yes	No	Yes	No

Therefore, for δ decoy photons, the probability that Eve will be detected during the eavesdropping detection is $1 - (\frac{3}{4})^\delta$. The relationship between the number of decoy photons δ and the probability of Eve being detected is shown in Figure 3. When δ is large, Eve will be detected with a probability approaching 1. Therefore, the intercept-

measure-resend attack conducted by Eve will introduce errors, and this eavesdropping will be detected.

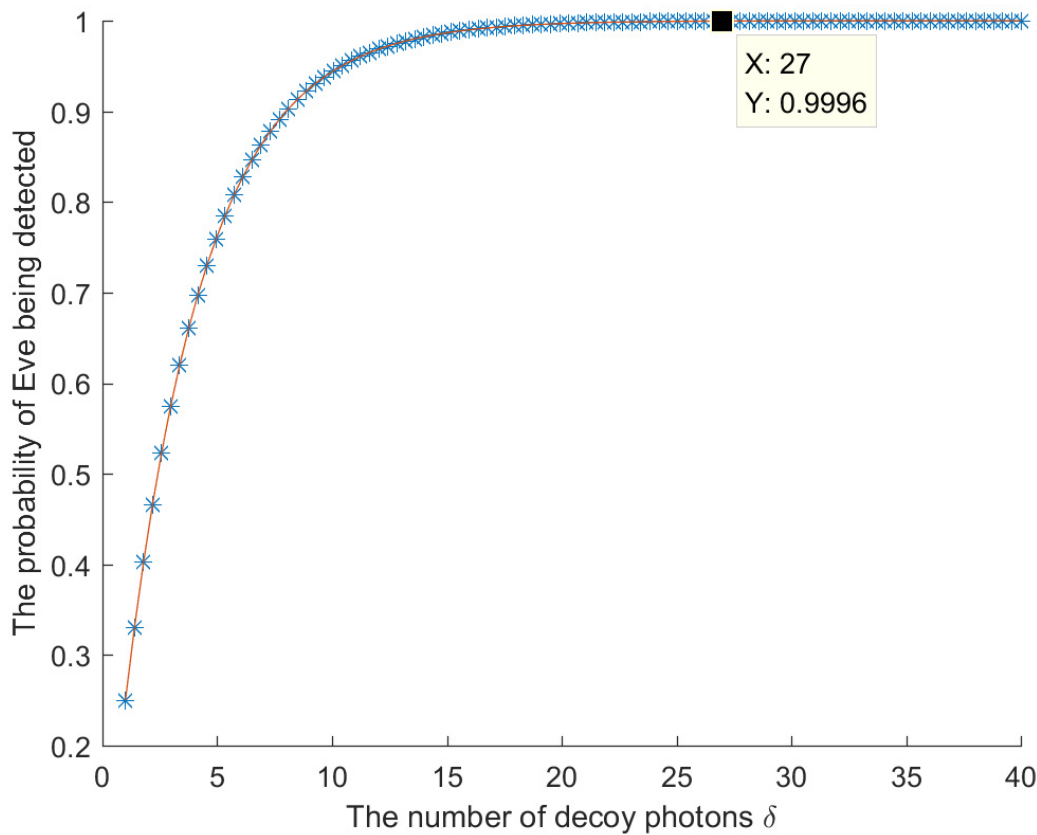


Figure 3. The relationship between the number of decoy photons δ and the probability of Eve being detected.

4.1.2. Entangle-Measure Attack

Eve may intercept the sequences transmitted on the communication channel and entangle her prepared auxiliary particles $|e\rangle$ with the intercepted particle by utilizing a specific unitary operation U_1 to steal the private information. When eavesdropping detection is conducted between the sequence sender and the receiver and the auxiliary particles are measured by Eve, this malicious behavior will succeed under the condition that Eve can deceive the eavesdropping detection.

When Eve entangles her prepared auxiliary particle $|e\rangle$ with the intercepted particle stayed in states $|0\rangle$ or $|1\rangle$ by using the unitary operation U_1 , this process can be expressed as

$$U_1|0, e\rangle = a_{00}|0\rangle|e_{00}\rangle + a_{01}|1\rangle|e_{01}\rangle \tag{20}$$

$$U_1|1, e\rangle = a_{10}|0\rangle|e_{10}\rangle + a_{11}|1\rangle|e_{11}\rangle \tag{21}$$

Four quantum states $\{|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle\}$ are pure states, which are determined by the unitary operation U_1 . The parameters $a_{00}, a_{01}, a_{10}, a_{11}$ must satisfy the following conditions: $\|a_{00}\|^2 + \|a_{01}\|^2 = \|a_{10}\|^2 + \|a_{11}\|^2 = 1$.

When Eve utilizes the unitary operation U_1 to entangle the auxiliary particle $|e\rangle$ and the intercepted particles $|+\rangle$ or $|-\rangle$, this process can be given by

$$\begin{aligned} U_1|+, e\rangle &= \frac{1}{\sqrt{2}}(a_{00}|0\rangle|e_{00}\rangle + a_{01}|e_{01}\rangle|1\rangle + a_{10}|0\rangle|e_{10}\rangle + a_{11}|1\rangle|e_{11}\rangle) \\ &= \frac{1}{2}|+\rangle(a_{00}|e_{00}\rangle + a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle + a_{11}|e_{11}\rangle) \\ &\quad + \frac{1}{2}|-\rangle(a_{00}|e_{00}\rangle - a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle - a_{11}|e_{11}\rangle) \end{aligned} \tag{22}$$

$$\begin{aligned}
 U_1|-,e\rangle &= \frac{1}{\sqrt{2}}(a_{00}|0\rangle|e_{00}\rangle + a_{01}|e_{01}\rangle|1\rangle - a_{10}|0\rangle|e_{10}\rangle - a_{11}|1\rangle|e_{11}\rangle) \\
 &= \frac{1}{2}|+\rangle(a_{00}|e_{00}\rangle + a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle - a_{11}|e_{11}\rangle) \\
 &\quad + \frac{1}{2}|-\rangle(a_{00}|e_{00}\rangle - a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle + a_{11}|e_{11}\rangle)
 \end{aligned}
 \tag{23}$$

To avoid introducing errors during eavesdropping detection and being detected, certain conditions should be met.

$$a_{01} = a_{10} = 0 \tag{24}$$

$$a_{00} = a_{11} = 1 \tag{25}$$

$$a_{00}|e_{00}\rangle - a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle - a_{11}|e_{11}\rangle = \vec{0} \tag{26}$$

$$a_{00}|e_{00}\rangle + a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle - a_{11}|e_{11}\rangle = \vec{0} \tag{27}$$

where $\vec{0}$ is column zero vector. From Equations (24)–(27), we can infer that $a_{00} = a_{11} = 1$ and $|e_{00}\rangle = |e_{11}\rangle$. Substituting the two results into Equations (20)–(23), we have the following equations:

$$U_1|0,e\rangle = |0\rangle|e_{00}\rangle = |0\rangle|e_{11}\rangle \tag{28}$$

$$U_1|1,e\rangle = |1\rangle|e_{00}\rangle = |1\rangle|e_{11}\rangle \tag{29}$$

$$U_1|+,e\rangle = |+\rangle|e_{00}\rangle = |+\rangle|e_{11}\rangle \tag{30}$$

$$U_1|-,e\rangle = |-\rangle|e_{00}\rangle = |-\rangle|e_{11}\rangle \tag{31}$$

From Equations (28)–(31) above, we can easily see that the auxiliary particle and the intercepted particle are in a product rather than a tensor product of these two particles. This suggests that the auxiliary particle and the intercepted one are independent of each other. In other words, there is no entanglement between auxiliary particles and intercepted particles, making the entangle-measure attack invalid in our protocol.

4.1.3. Trojan Horse Attack

Since our protocol is designed for two-way quantum computing using a bidirectional quantum channel to exchange information, it is susceptible to the Trojan Horse attack [56]. Two types of Trojan Horse attacks, such as the delay-photon attack and the invisible photon eavesdropping attack, can be detected by implementing additional techniques. For instance, the Wavelength Quantum Filter (WQF) and the Photons Number Splitter (PNS) can be used. The WQF employs optical filters to eliminate invisible photons, while the PNS is utilized to distinguish legitimate photons from delayed photons.

4.2. Participant Attacks

Different from external attacks, if a quantum protocol is secure against attacks from internal participants, then it must also be secure against external eavesdroppers due to the fact that internal participants can adopt attack strategies used by outsiders. Participants who can access immediate data containing the encoded results of private information have a higher chance of deducing the secrets of other participants, leading to significant security challenges. In the following section, different attack strategies by internal participants are discussed.

4.2.1. Attack from TP

As a semi-honest party, TP strictly follows the specified steps but cannot collude with or favor any involved user. The possible attack strategy for TP involves measuring each four-particle cluster state before sending the divided sequences to each participant. In this way, she can determine the states of the received particles that each participant obtains. This result and the resulting sequence she obtained can be used to deduce the private information of each participant. However, the malicious behaviors from TP cannot succeed due to the lack of knowledge of the secret keys X_i and Y_i . Therefore, even if TP knows

the particles each participant obtains and the resultant sequence, she still has no chance of obtaining the private information of each participant.

4.2.2. Attack from Alice or Bob (Charlie or Dove)

The roles of two user groups are identical, and both Alice and Bob have the same role. Without loss of generality, we consider the potential attack from Alice. Alice may want to deduce Bob's private information because they are part of a group of users who do not trust each other. Since the received sequence and the secret key of Alice are the same as Bob's, Alice has a great opportunity to steal Bob's private information. The potential attack strategy by Alice involves intercepting the sequence transmitted from Bob and TP. However, this malicious behavior will not succeed due to the lack of knowledge about the inserted positions and states of decoy photons. Once the eavesdropping is detected, the protocol will be terminated. Although Alice has obtained the targeted particles containing the encoded results of the private information and the mixed decoy photons, she still cannot access the private information because she does not know the secret keys selected by each participant. If Alice attempts to steal the private information of Charlie or Dove, she will not succeed because the only way to attack is by behaving like an eavesdropper. Therefore, Alice's attack strategy falls short of achieving her goal. The attack strategy of the other participants is similar to Alice's but also falls short of achieving her goal.

4.2.3. Attack from Conspiring Participants

There are three types of conspiratorial attacks: when any three users collude together, when any two users collude together, and cross-group conspiracy. For any three users colluding together, we consider an example where Bob colludes with Charlie and Dove to steal Alice's private information. This demonstrates that our protocol is secure against such malicious behavior. Although Bob, Charlie, and Dove know the initial sequence transmitted from TP to Alice and the secret key shared between Alice and Bob, they will not succeed because they lack knowledge of the inserted positions and states of the decoy photons and the secret key selected by Alice. For any two users colluding together, we analyze Alice colluding with Bob to steal the private information of Charlie and Dove. This attack is fundamentally impossible to realize because we have no knowledge about the transmitted information between TP and Charlie or Dove. For a cross-group conspiracy, let's consider an example where Alice colludes with Dove to illustrate that they are unable to obtain any secrets about Bob and Dove. Although Alice and Dove can determine the initial sequence transmitted from TP to Bob and TP to Charlie, as well as the secret key shared between Alice and Bob and Charlie and Dove, they will not succeed because they have no way of knowing the inserted positions and states of the decoy photons, as well as the secret keys selected by Bob and Charlie. Therefore, attacks from conspiring participants will not succeed.

5. Efficiency Analysis and Comparison

Qubit efficiency, which is used for estimating the efficiency of the QPC protocol, is defined as

$$\eta = c/t \quad (32)$$

where η is the qubit efficiency, c represents the classical bits to be compared, and t denotes the total particles for the comparison while excluding the decoy photons. In our protocol, one four-particle cluster state can be used for comparing the private information of two groups of users, each with one classical-bit information, and we can know that $c = 2$ and $t = 4$. Therefore, the qubit efficiency of our protocol is 50%.

The comparison between our protocol and some other previous QPC protocols is shown in Table 2. We compare our protocol with others in terms of quantum resources, unitary operations, entanglement swapping, quantum measurement, the pairs of private information compared, and qubit efficiency. Our protocol utilizes four-particle cluster state, rotation operation, and single-particle measurements as the main quantum technologies,

making it more practical. Although the qubit efficiency of our protocol and Refs. [40,41,51] is the same, our protocol exhibits improved scalability due to the comparison of the private information of two groups of users within one protocol execution. Both the protocol in Ref. [43] and our protocol can compare two-pair private information within one protocol execution, but our protocol has a higher qubit efficiency compared to Ref. [43]. Compared with the other QPC protocols based on the four-particle cluster state, our protocol has improved performance in terms of efficiency and scalability.

Table 2. The comparison between our protocol and some previous QPC protocols.

	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [51]	Ours
Quantum resource	Four-qubit cluster state and extended Bell state	Four-qubit cluster state	Four-particle cluster state	Five-particle cluster state	Bell states	Four-particle cluster state
Unitary operation	No	Yes	Yes	Yes	No	Yes
Entanglement swapping	Yes	No	No	No	Yes	No
the pairs of private information compared	1	1	1	2	1	2
Quantum measurement	Bell-basis and extend Bell basis	single-particle	Single-particle	single-particle	GHZ-basis	Single-particle
Qubit efficiency	50%	50%	25%	40%	50%	50%

6. Conclusions

In this paper, we put forward a new quantum private comparison protocol based on cluster state, which can compare the information of two groups of users within one protocol execution and achieve a qubit efficiency of 50%. Our protocol utilizes four-particle cluster state, rotation operation, and single-particle measurements as the main quantum technologies, making it more practical. Additionally, the security has been further enhanced because no classical results are produced. Security analysis shows that the proposed protocol is immune to both outsider and insider attacks.

Author Contributions: Conceptualization, M.H. and S.Z.; methodology, M.H. and S.Z.; writing—original draft, M.H.; writing—review and editing, Y.W. and S.Z.; supervision, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 62076042), the National Key Research and Development Plan of China, the Key Project of Cyberspace Security Governance (No. 2022YFB3103103), the Key Research and Development Project of Chengdu (No. 2023-XT00-00002-GX), the Key Research and Development Project of Sichuan Province (No. 2022YFS0571), the Open Fund of Network and Data Security Key Laboratory of Sichuan Province (Grant No. NDS2024-1), and the Gongga Plan for the “Double World-class Project”.

Data Availability Statement: No new data was created or analyzed in this study. Data sharing is not applicable to this article.

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

References

- Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [\[CrossRef\]](#)
- Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [\[CrossRef\]](#)
- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
- Zhang, W.; van Leent, T.; Redeker, K.; Garthoff, R.; Schwonnek, R.; Fertig, F.; Eppelt, S.; Rosenfeld, W.; Scarani, V.; Lim, C.C.-W.; et al. A device-independent quantum key distribution system for distant users. *Nature* **2022**, *607*, 687–691. [\[CrossRef\]](#) [\[PubMed\]](#)
- Fang, X.T.; Zeng, P.; Liu, H.; Zou, M.; Wu, W.; Tang, Y.L.; Sheng, Y.J.; Xiang, Y.; Zhang, W.; Li, H.; et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **2020**, *14*, 422–425. [\[CrossRef\]](#)
- Sun, S.; Huang, A. A review of security evaluation of practical quantum key distribution system. *Entropy* **2022**, *24*, 260. [\[CrossRef\]](#) [\[PubMed\]](#)

7. Huang, X.; Zhang, S.B.; Chang, Y.; Qiu, C.; Liu, D.-M.; Hou, M. Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 838–847. [[CrossRef](#)]
8. Zhou, N.R.; Zhu, K.N.; Wang, Y.Q. Three-party semi-quantum key agreement protocol. *Int. J. Theor. Phys.* **2020**, *59*, 663–676. [[CrossRef](#)]
9. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [[CrossRef](#)] [[PubMed](#)]
10. Huang, X.; Zhang, S.; Chang, Y.; Yang, F.; Hou, M.; Cheng, W. Quantum secure direct communication based on quantum homomorphic encryption. *Mod. Phys. Lett. A* **2021**, *36*, 2150263. [[CrossRef](#)]
11. Yang, C.W.; Lin, J.; Wang, K.L.; Tsai, C.W. Cryptanalysis and improvement of a controlled quantum secure direct communication with authentication protocol based on five-particle cluster state. *Quantum Inf. Process.* **2023**, *22*, 196. [[CrossRef](#)]
12. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Washington, DC, USA, 3–5 November 1982; p. 160.
13. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [[CrossRef](#)]
14. Yang, Y.G.; Wen, Q.Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J. Phys. A Math. Theor.* **2009**, *42*, 055305. [[CrossRef](#)]
15. Chen, X.B.; Xu, G.; Niu, X.X.; Wen, Q.Y.; Yang, Y.X. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. *Opt. Commun.* **2010**, *283*, 1561–1565. [[CrossRef](#)]
16. Lin, P.H.; Hwang, T.; Tsai, C.W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [[CrossRef](#)]
17. Yan-Feng, L. Semi-quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3048–3055. [[CrossRef](#)]
18. Pan, H.M. Two-party quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3389–3395. [[CrossRef](#)]
19. Huang, X.; Chang, Y.; Cheng, W.; Hou, M.; Zhang, S.B. Quantum private comparison of arbitrary single qubit states based on swap test. *Chin. Phys. B* **2022**, *31*, 040303. [[CrossRef](#)]
20. Sun, Z.; Yu, J.; Wang, P.; Xu, L.; Wu, C. Quantum private comparison with a malicious third party. *Quantum Inf. Process.* **2015**, *14*, 2125–2133. [[CrossRef](#)]
21. Kou, T.Y.; Che, B.C.; Dou, Z.; Chen, X.B.; Lai, Y.P.; Li, J. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. *Chin. Phys. B* **2022**, *31*, 060307. [[CrossRef](#)]
22. Huang, X.; Zhang, W.F.; Zhang, S.B. Efficient multiparty quantum private comparison protocol based on single photons and rotation encryption. *Quantum Inf. Process.* **2023**, *22*, 272. [[CrossRef](#)]
23. Liu, B.; Xiao, D.; Huang, W.; Jia, H.-Y.; Song, T.-T. Quantum private comparison employing single-photon interference. *Quantum Inf. Process.* **2017**, *16*, 180. [[CrossRef](#)]
24. Tseng, H.Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **2012**, *11*, 373–384. [[CrossRef](#)]
25. Lang, Y.F. Quantum private comparison using single bell state. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036. [[CrossRef](#)]
26. Jiang, L.Z. Semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 180. [[CrossRef](#)]
27. Geng, M.J.; Chen, Y.; Xu, T.J.; Ye, T.Y. Single-state semiquantum private comparison based on Bell states. *EPJ Quantum Technol.* **2022**, *9*, 36. [[CrossRef](#)]
28. Gong, L.H.; Li, M.L.; Cao, H.; Wang, B. Novel semi-quantum private comparison protocol with Bell states. *Laser Phys. Lett.* **2024**, *21*, 055209. [[CrossRef](#)]
29. Wu, W.; Wu, J.; Guo, L. Multi-Party Quantum Private Comparison Based on Bell States. *Entropy* **2023**, *25*, 1156. [[CrossRef](#)] [[PubMed](#)]
30. Xie, L.; Li, Q.; Yu, F.; Lou, X.; Zhang, C. Cryptanalysis and improvement of a semi-quantum private comparison protocol based on Bell states. *Quantum Inf. Process.* **2021**, *20*, 244. [[CrossRef](#)]
31. Ye, C.Q.; Li, J.; Chen, X.B.; Hou, Y. A feasible semi-quantum private comparison based on entanglement swapping of Bell states. *Phys. A Stat. Mech. Its Appl.* **2023**, *625*, 129023. [[CrossRef](#)]
32. Tsai, C.W.; Lin, J.; Yang, C.W. Cryptanalysis and improvement in semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2021**, *20*, 1–14. [[CrossRef](#)]
33. Sun, Y.; Yan, L.; Sun, Z.; Zhang, S. A novel semi-quantum private comparison scheme using bell entangle states. *Comput. Mater. Contin.* **2021**, *66*, 2385–2395. [[CrossRef](#)]
34. Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. [[CrossRef](#)]
35. Ji, Z.X.; Zhang, H.G.; Fan, P.R. Two-party quantum private comparison protocol with maximally entangled seven-qubit state. *Mod. Phys. Lett. A* **2019**, *34*, 1950229. [[CrossRef](#)]
36. Ji, Z.; Zhang, H.; Wang, H. Quantum private comparison protocols with a number of multi-particle entangled states. *IEEE Access* **2019**, *7*, 44613–44621. [[CrossRef](#)]
37. Ji, Z.X.; Ye, T.Y. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. *Commun. Theor. Phys.* **2016**, *65*, 711. [[CrossRef](#)]
38. Hong-Ming, P. Quantum private comparison based on χ -type entangled states. *Int. J. Theor. Phys.* **2017**, *56*, 3340–3347. [[CrossRef](#)]
39. Li, J.; Che, F.; Wang, Z.; Fu, A. Efficient Quantum Private Comparison without Sharing a Key. *Entropy* **2023**, *25*, 1552. [[CrossRef](#)] [[PubMed](#)]

40. Li, C.; Chen, X.; Li, H.; Yang, Y.; Li, J. Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state. *Quantum Inf. Process.* **2019**, *18*, 158. [[CrossRef](#)]
41. Xu, G.A.; Chen, X.B.; Wei, Z.H.; Li, M.J.; Yang, Y.X. An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. *Int. J. Quantum Inf.* **2012**, *10*, 1250045. [[CrossRef](#)]
42. Sun, Z.; Long, D. Quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2013**, *52*, 212–218. [[CrossRef](#)]
43. Chang, Y.; Zhang, W.B.; Zhang, S.B.; Wang, H.C.; Yan, L.L.; Han, G.H.; Sheng, Z.W.; Huang, Y.Y.; Suo, W.; Xiong, J.X. Quantum private comparison of equality based on five-particle cluster state. *Commun. Theor. Phys.* **2016**, *66*, 621. [[CrossRef](#)]
44. Zhou, M.K. Improvements of quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2018**, *57*, 42–47. [[CrossRef](#)]
45. Zha, X.W.; Yu, X.Y.; Cao, Y.; Wang, S.K. Quantum private comparison protocol with five-particle cluster states. *Int. J. Theor. Phys.* **2018**, *57*, 3874–3881. [[CrossRef](#)]
46. Ye, T.Y.; Hu, J.L. Multi-party quantum private comparison based on entanglement swapping of Bell entangled states within d-level quantum system. *Int. J. Theor. Phys.* **2021**, *60*, 1471–1480. [[CrossRef](#)]
47. Cao, H.; Ma, W.; Lü, L.; He, Y.; Liu, G. Multi-party quantum privacy comparison of size based on d-level GHZ states. *Quantum Inf. Process.* **2019**, *18*, 287. [[CrossRef](#)]
48. Wu, W.Q.; Zhao, Y.X. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 155. [[CrossRef](#)]
49. Zhao-Xu, J.; Tian-Yu, Y. Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states. *Quantum Inf. Process.* **2017**, *16*, 177. [[CrossRef](#)]
50. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [[CrossRef](#)]
51. Huang, X.; Zhang, S.B.; Chang, Y.; Hou, M.; Cheng, W. Efficient quantum private comparison based on entanglement swapping of bell states. *Int. J. Theor. Phys.* **2021**, *60*, 3783–3796. [[CrossRef](#)]
52. Fan, P.; Rahman, A.U.; Ji, Z.; Ji, X.; Hao, Z.; Zhang, H. Two-party quantum private comparison based on eight-qubit entangled state. *Mod. Phys. Lett. A* **2022**, *37*, 2250026. [[CrossRef](#)]
53. Liu, C.; Zhou, S.; Gong, L.H.; Chen, H.Y. Quantum private comparison protocol based on 4D GHZ-like states. *Quantum Inf. Process.* **2023**, *22*, 255. [[CrossRef](#)]
54. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [[CrossRef](#)]
55. Huang, X.; Zhang, W.; Zhang, S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. *Phys. A Stat. Mech. Its Appl.* **2024**, *637*, 129614. [[CrossRef](#)]
56. Lucamarini, M.; Choi, I.; Ward, M.B.; Dynes, J.F.; Yuan, Z.L.; Shields, A.J. Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X* **2015**, *5*, 031030. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.