axioms

MDPI

Article

Multiparty Quantum Private Comparison Using Rotation Operations

Min Hou [1,2,3,*] and Yue Wu [1]

[1] School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China; ywu@uestc.edu.cn
[2] Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China
[3] State Key Laboratory of Cognitive Intelligence, Hefei 230088, China
* Correspondence: houmin@scujj.edu.cn

Abstract: This paper presents a multiparty quantum private comparison (MQPC) protocol that facilitates multiple users to compare the equality of their private inputs while preserving the confidentiality of each input through the principles of quantum mechanics. In our approach, users initially convert their secret integers into binary representations, which are then encoded into single photons that act as carriers of the information. These encoded single-photon states undergo encryption via rotational operations, effectively obscuring the original inputs before transmission to a semi-honest third party (TP). The TP decrypts the quantum states and conducts Z-basis measurements to derive the comparison results. To enhance security, the protocol incorporates decoy photons, enabling participants to detect potential eavesdropping on the quantum channel. Importantly, even if the TP or other participants attempt to glean insights into each other's inputs, the encryption via rotational operations ensures that private information remains inaccessible. This protocol demonstrates significant advancements in practicality compared to existing MQPC frameworks that rely on complex quantum technologies, such as entanglement swapping and multi-particle entanglement. By leveraging the simplicity of single photons, rotation operations, and Z-basis measurements, our protocol is more accessible for implementation.

Keywords: multiparty quantum private comparison (MQPC); semi-honest third party (TP); rotation operations; single photons; quantum cryptography

MSC: 81P94; 81P65

check for updates

Academic Editor: Oscar Montiel Ross

Received: 6 March 2025
Revised: 31 March 2025
Accepted: 2 April 2025
Published: 3 April 2025

Citation: Hou, M.; Wu, Y. Multiparty Quantum Private Comparison Using Rotation Operations. *Axioms* **2025**, *14*, 274. https://doi.org/10.3390/axioms14040274

Copyright: © 2025 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

The BB84 protocol [1], introduced by Bennett and Brassard in 1984, represents a pivotal advancement in quantum cryptography, showcasing the feasibility of unconditional security through the principles of quantum mechanics, notably the behavior of quantum states and the no-cloning theorem. Building on the success of BB84, a diverse array of quantum cryptographic protocols have emerged, including quantum key distribution (QKD) [2–6], quantum key agreement (QKA) [7,8], quantum secure direct communication (QSDC) [9–11], and quantum private set intersection [12–14]. These protocols are designed to fulfill traditional cryptographic objectives while ensuring resilience against quantum attacks.

Private comparison plays a crucial role in secure multiparty computation and was originally motivated by the millionaires' problem [15], where two millionaires aim to ascertain who possesses greater wealth without disclosing their actual financial amounts. A notable

variation proposed by Boudot et al. [16] centers on determining whether two millionaires possess identical wealth. In two-party computation scenarios, Lo [17] emphasized the challenges of constructing a secure equality function independently. To navigate these challenges, a semi-honest third party (TP) is employed to assist in the private comparison while preserving the privacy of the participants.

Historically, the security of private comparison protocols has relied on the computational complexity of specific mathematical problems, such as factoring large integers or solving discrete logarithms. These protocols utilize traditional cryptographic principles to ensure confidentiality and integrity. However, the rise in quantum computing presents significant threats to classical cryptographic systems. Quantum algorithms, notably the Shor algorithm [18], can efficiently solve problems previously deemed intractable, thereby undermining the security foundations of many classical protocols. In response to these vulnerabilities, researchers have begun developing innovative private comparison protocols that leverage quantum principles. These protocols aim to enhance security by utilizing the unique properties of quantum mechanics, such as superposition and entanglement, providing stronger guarantees against potential quantum attacks.

The primary goal of quantum private comparison (QPC) is to enable two parties to compare their confidential secrets while preserving the privacy of each participant. This is achieved by combining classical private comparison techniques with the unique properties of quantum mechanics. By leveraging quantum principles, QPC protocols enhance security and facilitate new methods for secure communication and data comparison. The foundational QPC protocol, developed by Yang and Wen in 2009 [19], employs Bell states to encode the confidential secrets of the participants. Additionally, the use of decoy states allows for the detection of any eavesdropping attempts, thereby maintaining the confidentiality of the participants' secrets. Following this pioneering work, a variety of quantum states have been explored for use in designing QPC protocols, including single-particle states [20–25], Bell states [26–33], multi-qubit entangled states [34–43], multi-qubit cluster states [44–50], and d-level quantum states [51–54]. Despite these advancements, most of the existing QPC protocols are primarily designed for comparing the private data of just two participants. This limitation poses challenges when scaling the protocol to multiple participants. When n participants wish to engage in a private comparison, the two-party QPC protocol needs to be executed multiple times, specifically running the protocol $n-1$ to $\frac{n(n-1)}{2}$ times in a repeated manner. This repeated execution can lead to significant inefficiencies and increased communication overhead. Therefore, there is a pressing need for the development of more efficient multiparty QPC protocols that can handle comparisons among n participants simultaneously, without the exponential increase in protocol executions.

A new branch multiparty quantum private comparison (MQPC) has emerged, aiming at reducing the number of required executions and improving efficiency. Chang et al. [55] introduced a pioneering MQPC protocol that utilizes n-particle Greenberger–Horne–Zeilinger class states, which allows for the comparison of arbitrary pairs of participants within a single execution. The participants utilize bitwise exclusive-OR (XOR) operations to encrypt their inputs, ensuring that their data remain confidential throughout the comparison process. Building on the pioneering MQPC protocol, Liu et al. [56] introduced a novel approach to multiparty quantum private comparison by performing local unitary operations on d-dimensional basis states, which enables n parties to compare their private inputs without encrypting them into ciphertext. Wang et al. [57] proposed two distinct MQPC protocols that utilize d-level entangled states to facilitate secure comparisons among multiple participants. These protocols are designed to operate in different modes: distributed mode and traveling mode. The first protocol employs d-level n-particle entangled states and quantum Fourier transform (QFT), which allows for comparisons involving multiple

participants simultaneously. The second protocol uses d-level two-particle entangled states and quantum phase shifting operation, focusing on pairwise comparisons while leveraging the entanglement properties of the states. In 2017, Ji and Ye [58] introduced a novel MQPC protocol that utilized entanglement swapping of d-level cat states and d-level Bell states. This protocol encodes participant inputs through unitary operations, allowing for secure comparisons among multiple parties. Despite this innovative approach, the realization of d-level cat states and d-level Bell states presents significant experimental challenges. These challenges can hinder the practical implementation of the protocol in real-world scenarios. Considering the difficulties associated with implementing the Ji and Ye protocol, Ye and Hu [59] proposed an alternative MQPC protocol that simplifies the process. Their protocol is based on d-level two-particle Bell entangled states, which are generally easier to realize experimentally compared to d-level cat states. While the existing MQPC protocols [55–59] are theoretically sound, they often rely on advanced technologies that are not yet fully realized in practice. Developing a practical MQPC protocol is critical for advancing the field of quantum cryptography. A protocol that can be reliably implemented using existing technologies would greatly enhance the applicability of quantum private comparison in real-world scenarios.

To address this challenge, we propose a multiparty quantum private comparison (MQPC) that employs rotation operations to protect the privacy of the inputs. Users begin by converting their secret integers into binary representations that are encoded into single photons. These single photons serve as carriers of the information, leveraging their quantum properties for secure communication. Once encoded, the single-photon states undergo encryption through rotation operations. This process effectively obscures the original inputs, ensuring that the information remains private during transmission to a semi-honest third party (TP). The TP, while semi-honest, is responsible for decrypting the quantum states received from the users and conducts Z-basis measurements on the quantum states. These measurements allow the TP to derive the comparison results between the users' secret integers without revealing the actual values of the inputs. The use of rotation operations and decoy photons provides a robust mechanism for protecting the privacy of participants' inputs, making the protocol resistant against the outsider eavesdropping and participant attacks. By using single photons and straightforward rotation operations, the protocol is designed to be easily implementable with current quantum technologies. Compared to existing MQPC frameworks that rely on complex quantum technologies, such as entanglement swapping and multi-particle entanglement, our protocol demonstrates advancements in practicality due to the simplicity of single photons, rotation operations, and Z-basis measurements.

The remainder of this paper is organized as follows. Section 2 provides an introduction of rotation operations used for encrypting the quantum states. The detailed steps of the proposed MQPC protocol and its analyses, including correctness, security, and fairness, are presented in Sections 3 and 4, respectively. Section 5 hosts a discussion. Finally, we summarize our work in Section 6.

2. Rotation Operation

The R_y rotation operator is defined as follows:

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad (1)$$

where I and Y represent the identity matrix and Pauli Y matrix, respectively. θ is the rotation angle around the y-axis on the Bloch sphere [60]. The R_y operator can be utilized as an

encryption mechanism in quantum communication. By applying $R_y(\theta)$ to a quantum state, we convert it into an unknown state, effectively obscuring the original information. The parameter θ serves as the encryption key, allowing for the transformation of the quantum state into a form that is not immediately recognizable.

Let $E_k[|\psi\rangle]$ denote the encryption of quantum state $|\psi\rangle = |0\rangle$ with the key k. When encrypting $|\psi\rangle$ with a key $k = \theta \in [0, 2\pi)$, this can be mathematically represented as follows:

$$|\psi'\rangle = E_\theta[|0\rangle] = R_y(\theta)|0\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \quad (2)$$

The decryption process is denoted by $D_k[|\psi\rangle]$. To decrypt the state, the same rotation angle $k = \theta$ is applied in the opposite direction:

$$|\psi\rangle = D_\theta[|\psi'\rangle] = R_y(-\theta)|\psi'\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2}\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2}\cos\frac{\theta}{2} + \cos\frac{\theta}{2}\sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\psi\rangle \quad (3)$$

By applying $R_y(-\theta)$ to the encrypted state, we can retrieve the original quantum state.

The R_y rotation operator is utilized as an encryption tool in quantum communication, transforming quantum states into unknown forms using the angle θ as the encryption key. Recovery of the original state is achieved through the application of the inverse operator $R_y(-\theta)$, ensuring that the quantum information remains confidential. Without knowledge of the key θ, an eavesdropper cannot easily deduce the original quantum state.

3. The Proposed MQPC Protocol

3.1. The Protocol Description

Suppose that n participants P_i $(i = 1, 2, \cdots, n)$ desire to determine whether their private inputs M_i are equal or not with the semi-honest third party (e.g., a quantum server with quantum abilities) while ensuring the privacy of their inputs. The semi-honest third party (TP) is one that follows protocol rules honestly while attempting to extract information from other parties' private data. While it cannot collude with dishonest parties [57,58], its behavior necessitates careful protocol design to ensure that the privacy of all participants is maintained. The binary representations M_i in F_2^L are written as $M_i = (m_{i,L-1}, m_{i,L-2}, \cdots, m_{i,0})$. If the length of M_i is less than L, pad with zeros in the higher-order bits. We assume that the following protocol operates under noise-free and lossless conditions and that the classical channel used for communication between the parties is authenticated.

Our protocol will satisfy the following requirements:

(1) *Correctness*. If each participant provides their respective inputs and performs the protocol faithfully, the comparison results announced by the third party are correct.
(2) *Privacy.* The participant's inputs remain confidential as long as the TP cannot collude with any participant, even in the presence of outsider eavesdropping or attacks from other participants aiming to learn about their inputs.
(3) *Fairness.* All the parties are perfect peer entities, and they can receive the comparison result simultaneously, ensuring that no participant has an advantage over the other.

The proposed protocol is as follows:

Step 1. The n participants run a multiparty quantum key agreement (MQKA) protocol [61] to share a secret non-zero binary key $K = (k_{L-1}, k_{L-2}, \cdots, k_0)$, where $k_j \in \{0, 1\}$ for $j = 0, 1, \cdots, L-1$.

Step 2. P_i performs the XOR operation with their binary inputs M_i and the secret non-zero binary key K, represented as $m_{i,j} \oplus k_j$. Based on the result of the XOR operation,

P_i prepares their respective single-photon sequence. If $m_{i,j} \oplus k_j = 0$, P_i prepares the single-photon state $|0\rangle$; otherwise, state $|1\rangle$ is prepared. The collection of all single-photon states prepared by P_i is denoted as S_i.

Step 3. P_i prepares the secret key $\Theta_i = (\theta_{i,L-1}, \theta_{i,L-2}, \cdots, \theta_{i,0})$, where $\theta_{i,j} \in [0, 2\pi)$ for $j = 0, 1, \cdots, L-1$, and encrypts each state in S_i by applying the R_y rotation operator using the key Θ_i. The resulting encrypted sequence is denoted as E_i.

Step 4. To detect potential eavesdropping, P_i performs the following operations:

(1) P_i prepares δ decoy photons randomly selected from the set of four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, aiming at detecting potential eavesdropping.
(2) P_i inserts the prepared decoy photons into their encrypted quantum sequence E_i at random positions. This results in a new sequence denoted as E_i'.
(3) P_i keeps a record of the states and the exact positions of the decoy photons within the sequence E_i'.
(4) P_i sends E_i' to the TP via a quantum channel.

Step 5. After P_i confirms that the TP has received the sequence E_i', they proceed to the next steps.

(1) P_i discloses the positions of the δ decoy photons in the sequence E_i' via the authenticated classical channel.
(2) P_i publishes the measurement basis used for each decoy photon. Z-basis is used for measuring states $|0\rangle$ or $|1\rangle$ and X-basis is used for measuring states $|+\rangle$ or $|-\rangle$.
(3) The TP performs Z-basis or X-basis measurements on these decoy photons in sequence E_i' according to the published bases.
(4) The TP collects the measurement results and sends this information back to P_i via the authenticated classical channel.
(5) P_i calculates the error rate based on the measurement results received from the TP. The error rate is calculated as the ratio of the number of incorrect measurements to the total number of measurements.
(6) If the calculated error rate exceeds a pre-agreed threshold, the protocol is restarted from Step 5. Otherwise, P_i announces her/his secret key Θ_i to the TP via authenticated classical channel.

Step 6. TP recovers the sequence E_i by discarding all decoy photons from the sequence E_i' and decrypts E_i using the secret key Θ_i. The TP recovers the original quantum sequence S_i by applying the inverse operation. This involves performing the R_y $(-\Theta_i)$ operator on the encrypted quantum sequence E_i. The TP measures all states in S_i using the Z-basis and checks if all the measurement results from E_i are identical. If all the measurement results of S_i are identical, then $X = Y$; otherwise, $X \neq Y$. Finally, the TP announces the comparison results to the n participants.

3.2. A Toy Example

Let P_1, P_2, and P_3 be three participants with private inputs $M_1 = 9$, $M_2 = 10$, and $M_3 = 11$. The binary representations $M_i (i = 1, 2, 3)$ in F_2^L are as follows:

- $M_1 = (1001)$;
- $M_2 = (1010)$;
- $M_3 = (1011)$.

Step 1: The three participants share a non-zero binary key $K = (0101)$ via an MQKA protocol.

Step 2: The sequences $S_i (i = 1, 2, 3)$ are prepared based on the XOR operation of M_i and K:

- $S_1 = \{|1\rangle, |1\rangle, |0\rangle, |0\rangle\}$;

- $S_2 = \{|1\rangle, |1\rangle, |1\rangle, |1\rangle\}$;
- $S_3 = \{|1\rangle, |1\rangle, |1\rangle, |0\rangle\}$.

Step 3: Each participant P_i $(i = 1, 2, 3)$ prepares a secret key:

- $\Theta_1 = \left(\frac{\pi}{3}, \frac{5\pi}{6}, \frac{9\pi}{7}, \frac{5\pi}{8}\right)$;
- $\Theta_2 = \left(\frac{\pi}{7}, \frac{3\pi}{26}, \frac{9\pi}{5}, \frac{3\pi}{4}\right)$;
- $\Theta_3 = \left(\frac{\pi}{4}, \frac{3\pi}{2}, \frac{7\pi}{11}, \frac{4\pi}{5}\right)$.

By applying the $R_y(\Theta_i)$ on each state in S_i, the encrypted sequences E_i are as follows:

- $E_1 = \left\{R_y\left(\frac{\pi}{3}\right)|1\rangle, R_y\left(\frac{5\pi}{6}\right)|1\rangle, R_y\left(\frac{9\pi}{7}\right)|0\rangle, R_y\left(\frac{5\pi}{8}\right)|0\rangle\right\}$;
- $E_2 = \left\{R_y\left(\frac{\pi}{7}\right)|1\rangle, R_y\left(\frac{3\pi}{26}\right)|1\rangle, R_y\left(\frac{9\pi}{5}\right)|1\rangle, R_y\left(\frac{3\pi}{4}\right)|1\rangle\right\}$;
- $E_3 = \left\{R_y\left(\frac{\pi}{4}\right)|1\rangle, R_y\left(\frac{3\pi}{2}\right)|1\rangle, R_y\left(\frac{7\pi}{11}\right)|1\rangle, R_y\left(\frac{4\pi}{5}\right)|1\rangle\right\}$.

Step 4: Each P_i $(i = 1, 2, 3)$ prepares δ decoy photons and inserts them into E_i at random positions:

- For E_1 : 4th and 5th positions;
- For E_2 : 1st and 3rd positions;
- For E_3 : 2nd and 4th positions.

The new generated sequence E_i' are as follows:

- $E_1 = \left\{R_y\left(\frac{\pi}{3}\right)|1\rangle, R_y\left(\frac{5\pi}{6}\right)|1\rangle, R_y\left(\frac{9\pi}{7}\right)|0\rangle, |+\rangle, |0\rangle, R_y\left(\frac{5\pi}{8}\right)|0\rangle\right\}$;
- $E_2 = \left\{|1\rangle, R_y\left(\frac{\pi}{7}\right)|1\rangle, |-\rangle, R_y\left(\frac{3\pi}{26}\right)|1\rangle, R_y\left(\frac{9\pi}{5}\right)|1\rangle, R_y\left(\frac{3\pi}{4}\right)|1\rangle\right\}$;
- $E_3 = \left\{R_y\left(\frac{\pi}{4}\right)|1\rangle, |1\rangle, R_y\left(\frac{3\pi}{2}\right)|1\rangle, |+\rangle, R_y\left(\frac{7\pi}{11}\right)|1\rangle, R_y\left(\frac{4\pi}{5}\right)|1\rangle\right\}$.

Finally, P_i $(i = 1, 2, 3)$ sends E_i' to the TP via a quantum channel.

Step 5: Each P_i discloses the positions and measurement bases of the decoy photons in the sequence E_i' via the authenticated classical channel, and the measurement bases for the decoy photons in E_i' are as follows:

- For E_1 : {X, Z};
- For E_2 : {Z, X};
- For E_{12} : {Z, X}.

The TP performs the corresponding measurements on these decoy photons and returns the results to P_i. Each P_i calculates the error rate. If the error rate does not exceed a pre-agreed threshold, they announce their secret key Θ_i to the TP via the authenticated classical channel.

Step 6: The TP recovers the sequence E_i by discarding all the decoy photons from E_i'. By performing the R_y $(-\Theta_i)$ operator on the encrypted quantum sequence E_i, the TP can recover the original quantum sequence:

- $S_1 = \{|1\rangle, |1\rangle, |0\rangle, |0\rangle\}$;
- $S_2 = \{|1\rangle, |1\rangle, |1\rangle, |1\rangle\}$;
- $S_3 = \{|1\rangle, |1\rangle, |1\rangle, |0\rangle\}$.

The TP measures all states in S_i using the Z-basis and determines that not all of the measurement results of S_i are identical. Finally, the TP announces the comparison results to the three participants.

4. Analyses

4.1. Correctness

In step 2, the sequence S_i prepared by P_i can be written as

$$S_i = |m_{i,L-1} \oplus k_{L-1}\rangle \otimes |m_{i,L-2} \oplus k_{L-2}\rangle \otimes \cdots \otimes |m_{i,0} \oplus k_0\rangle = \otimes_{j=0}^{L-1} |m_{i,j} \oplus k_j\rangle \quad (4)$$

In step 3, when P_i encrypts each single-photon state in S_i by applying the R_y rotation operator using the key Θ_i, the resulting encrypted quantum sequence E_i can be given by

$$\begin{aligned} E_i &= R(\Theta_i)S_j = R(\Theta_i) \otimes_{j=0}^{L-1} |m_{i,j} \oplus k_j\rangle \\ &= R(\theta_{i,L-1})|m_{i,L-1} \oplus k_{L-1}\rangle \otimes R(\theta_{i,L-2})|m_{i,L-2} \oplus k_{L-2}\rangle \otimes \cdots \otimes R(\theta_{i,0})|m_{i,0} \oplus k_0\rangle \\ &= \otimes_{j=0}^{L-1} R(\theta_{i,j})|m_{i,j} \oplus k_j\rangle \end{aligned} \tag{5}$$

Step 4 and step 5 are used for detecting eavesdropping.

In step 6, when P_i performs the $R_y(-\Theta_i)$ operator on the encrypted quantum sequence E_i to decrypt the sequence E_i using the secret key Θ_i, this process for recovering the original quantum sequence S_i can be given by

$$\begin{aligned} R(-\Theta_i)E_i &= R(-\Theta_i) \otimes_{j=0}^{L-1} R(\theta_{i,j})|m_{i,j} \oplus k_j\rangle \\ &= R(-\theta_{i,L-1})R(\theta_{i,L-1})|m_{i,L-1} \oplus k_{L-1}\rangle \otimes R(-\theta_{i,L-2})R(\theta_{i,L-2})|m_{i,L-2} \oplus k_{L-2}\rangle \\ &\otimes \cdots \otimes R(-\theta_{i,0})R(\theta_{i,0})|m_{i,0} \oplus k_0\rangle \\ &= \otimes_{j=0}^{L-1}|m_{i,j} \oplus k_j\rangle = S_i \end{aligned} \tag{6}$$

When measuring S_i using the Z-basis, we can know if all of the measurement results of S_i are identical, then $X = Y$; otherwise, $X \neq Y$.

4.2. Security

The proposed MQPC protocol should satisfy the following security requirements:

(1) Security against outsider eavesdropping: Any attempt at eavesdropping on the private information of the participants would be detectable, even if the outsider eavesdropper performs quantum-based attacks.
(2) Security against attacks from the semi-honest trusted party (TP): The private information of the participants will not be leaked, even if the semi-honest TP utilizes the received information to deduce private information.
(3) Security against attacks from participants: The participants' inputs remain confidential, even if some participants collude to attempt to steal another participant's inputs.

4.2.1. Outsider Eavesdropping

In quantum communication, the existence of an external eavesdropper, commonly known as Eve, presents a considerable threat. Eve may utilize a range of quantum-based attacks, such as intercept–resend [62], entangle–measure [63], and Trojan horse attacks [64], in an attempt to access private information. To mitigate these eavesdropping tactics, participants implement the decoy state strategy. This approach involves transmitting additional decoy states alongside the actual quantum states. Thanks to the decoy state technique, Eve's various quantum attack methods become ineffective. Alice and Bob can accurately identify any eavesdropping efforts through inconsistencies in the statistical characteristics of the decoy states, thereby securing their communication.

Case I: Intercept–resend attack

In this scenario, an external assailant, Eve, attempts an intercept–resend attack on the quantum communication occurring between the transmission of quantum states. Eve intercepts the quantum states during their transmission, storing these intercepted particles for future exploitation. After securing the quantum states, Eve generates her own single particles, which she sends to the receiver instead of the originals. Once the receiver processes the particles sent by Eve, she captures the quantum sequences returned to the sender and measures them to extract confidential information while returning her previously stored particles back to the sender.

Upon receiving the particle sequences, both sides initiate an eavesdropping detection process. The sender reveals the locations and measurement bases of the decoy particles utilized during the process of communication. Since Eve lacks knowledge of the specific states of these particles, there exists a 50% chance that the receiver will obtain an erroneous outcome when measuring the particles sent by Eve. For instance, if the original decoy photon is in state $|1\rangle$, but Eve prepares a particle in states $|+\rangle$ or $|-\rangle$, the measurement conducted by the receiver on Eve's particle has a 50% likelihood of resulting in an incorrect measurement. Therefore, the likelihood of Eve successfully evading detection is represented by

$$P(successfully\ evading\ detection) = \left(\frac{1}{2}\right)^{\delta} \tag{7}$$

As the parameter δ increases significantly, this probability approaches zero. Consequently, the intercept–resend attack becomes ineffective within this communication framework, thereby safeguarding the participants' private inputs M_i.

Case II: The entangle–measure attack

Eve might also execute an entangle–measure attack by entangling her auxiliary quantum particle $|e\rangle$ with the intercepted particles. This technique enables her to glean information by measuring her auxiliary particles. When Eve employs a unitary operation U to entangle her particle $|e\rangle$ with the four potential states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the resultant states are as follows:

$$U|0\rangle|e\rangle = u_{00}|0\rangle|e_{00}\rangle + u_{01}|1\rangle|e_{01}\rangle \tag{8}$$

$$U|1\rangle|e\rangle = u_{10}|0\rangle|e_{10}\rangle + u_{11}|1\rangle|e_{11}\rangle \tag{9}$$

$$\begin{aligned} U|+\rangle|e\rangle \quad &= \tfrac{1}{2}|+\rangle(u_{00}|e_{00}\rangle + u_{01}|e_{01}\rangle + u_{10}|e_{10}\rangle + u_{11}|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(u_{00}|e_{00}\rangle - u_{01}|e_{01}\rangle + u_{10}|e_{10}\rangle - u_{11}|e_{11}\rangle) \end{aligned} \tag{10}$$

$$\begin{aligned} U|-\rangle|e\rangle \quad &= \tfrac{1}{2}|+\rangle(u_{00}|e_{00}\rangle + u_{01}|e_{01}\rangle - u_{10}|e_{10}\rangle - u_{11}|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(u_{00}|e_{00}\rangle - u_{01}|e_{01}\rangle - u_{10}|e_{10}\rangle + u_{11}|e_{11}\rangle) \end{aligned} \tag{11}$$

The coefficients must adhere to normalization conditions: $\|u_{00}\|^2 + \|u_{01}\|^2 = 1$ and $\|u_{10}\|^2 + \|u_{11}\|^2 = 1$. For Eve's attack to remain undetected, the following conditions need to be met.

$$u_{01} = u_{10} = 0, u_{00}|e_{00}\rangle = u_{11}|e_{11}\rangle \tag{12}$$

By substituting the results from Equation (12) into Equations (8)–(11), we obtain the following equation:

$$U|0\rangle|e\rangle = u_{00}|0\rangle|e_{00}\rangle \tag{13}$$

$$U|1\rangle|e\rangle = u_{11}|1\rangle|e_{11}\rangle = u_{00}|1\rangle|e_{00}\rangle \tag{14}$$

$$U|+\rangle|e\rangle = \frac{1}{2}|+\rangle(u_{00}|e_{00}\rangle + u_{11}|e_{11}\rangle) = u_{00}|+\rangle|e_{00}\rangle = u_{11}|+\rangle|e_{11}\rangle \tag{15}$$

$$U|-\rangle|e\rangle = \frac{1}{2}|-\rangle(u_{00}|e_{00}\rangle + u_{11}|e_{11}\rangle) = u_{00}|-\rangle|e_{00}\rangle = u_{11}|-\rangle|e_{11}\rangle \tag{16}$$

Based on Equations (13)–(16), Eve's auxiliary particles remain independent of the target particles to prevent introducing errors during eavesdropping detection. By measuring the auxiliary particles, Eve cannot obtain any information about the decoy photons.

We assume that Eve employs a unitary operation U to entangle her particle $|e\rangle$ with the j-th encrypted quantum state in E_i ($R(\theta_{i,j})|0\rangle$ *or* $R(\theta_{i,j})|1\rangle$), so we can derive the following relationship:

$$\begin{aligned} &U\left(R\left(\theta_{i,j}\right)|0\rangle|e_i\rangle\right) = U\left(\cos\tfrac{\theta_{i,j}}{2}|0\rangle + \sin\tfrac{\theta_{i,j}}{2}|1\rangle\right)|e\rangle \\ &= |0\rangle\left(u_{00}\cos\tfrac{\theta_{i,j}}{2}|e_{00}\rangle + u_{01}\sin\tfrac{\theta_{i,j}}{2}|e_{10}\rangle\right) + |1\rangle\left(u_{10}\cos\tfrac{\theta_{i,j}}{2}|e_{01}\rangle + u_{11}\sin\tfrac{\theta_{i,j}}{2}|e_{11}\rangle\right) \\ &or\ U\left(R\left(\theta_{i,j}\right)|1\rangle|e_i\rangle\right) = U\left(-\sin\tfrac{\theta_{i,j}}{2}|0\rangle + \cos\tfrac{\theta_{i,j}}{2}|1\rangle\right)|e\rangle \\ &= |0\rangle\left(-u_{00}\sin\tfrac{\theta_{i,j}}{2}|e_{00}\rangle + u_{01}\cos\tfrac{\theta_{i,j}}{2}|e_{10}\rangle\right) + |1\rangle\left(-u_{10}\sin\tfrac{\theta_{i,j}}{2}|e_{01}\rangle + u_{11}\cos\tfrac{\theta_{i,j}}{2}|e_{11}\rangle\right) \end{aligned} \tag{17}$$

By substituting the results from Equation (12) into Equation (17), we deduce that

$$\begin{aligned} &U\left(R\left(\theta_{i,j}\right)|0\rangle|e_i\rangle\right) = U^*\left(\cos\tfrac{\theta_{i,j}}{2}|0\rangle + \sin\tfrac{\theta_{i,j}}{2}|1\rangle\right)|e\rangle = u_{00}\cos\tfrac{\theta_{i,j}}{2}|0\rangle|e_{00}\rangle + u_{11}\sin\tfrac{\theta_{i,j}}{2}|1\rangle|e_{11}\rangle \\ &or\ U\left(R\left(\theta_{i,j}\right)|1\rangle|e_i\rangle\right) = U^*\left(-\sin\tfrac{\theta_{i,j}}{2}|0\rangle + \cos\tfrac{\theta_{i,j}}{2}|1\rangle\right)|e\rangle = -u_{00}\sin\tfrac{\theta_{i,j}}{2}|0\rangle|e_{00}\rangle + u_{11}\cos\tfrac{\theta_{i,j}}{2}|1\rangle|e_{11}\rangle \end{aligned} \tag{18}$$

The measurement results of Equation (17) are related with the secret key Θ_i that is disclosed to Eve, resulting in the fact that Eve cannot obtain the private inputs M_i.

Case III: The man-in-the-middle attack

Eve might also execute a man-in-the-middle attack by intercepting the sequence E_i' transmitted from P_i to the TP and preparing a fake sequence SE_i' instead of E_i'. SE_i' is sent to the TP. To evade the eavesdropping detection, Eve can prepare guessed decoy photons in specific states. Let D_i represent the i-th decoy photon in E_i', which may correspond to the j-th qubit in E_i'. Let D_i' denote the j-th qubit of SE_i'. The decoy photons D_i and D_i' are prepared in $B = \{|0\rangle, |1\rangle\}$ and $B' = \{|+\rangle, |-\rangle\}$, respectively. When P_i publishes the measurement basis of D_i, Eve measures D_i using basis B and obtains the results D_i''. The probability that $D_i'' = D_i$ is as follows.

(1) If $B' = B$ and $D'_i = D_i$, then the probability that $D''_i = D'_i$ is 1.
(2) If $B' = B$ and $D'_i \neq D_i$, then the probability that $D''_i = D_i$ is 0.
(3) If $B' \neq B$ and $D'_i = D_i$, then the probability that $D''_i = D_i$ is 1/2.

The probability of detecting the man-in-the-middle attack for a decoy photon is

$$\begin{aligned} P\left(D_i'' = D_i\right) &= P\left(D_i'' = D_i \middle| B' = B\right)P(B' = B) + P\left(D_i'' = D_i \middle| B' \neq B\right)P(B' \neq B) \\ &= \tfrac{1}{2}\left(P\left(D_i'' = D_i \middle| B' = B\right) + P\left(\left(D_i'' = D_i \middle| B' \neq B\right)\right)\right) \\ &= \tfrac{1}{2}\begin{pmatrix} P\left(D_i'' = D_i \middle| B' = B, D_i' = D_i\right)P\left(D_i' = D_i\right) + \\ P\left(D_i'' = D_i \middle| B' = B, D_i' \neq D_i\right)P\left(D_i' \neq D_i\right) + \frac{1}{2} \end{pmatrix} \\ &= \tfrac{1}{2}\left(1 \times \tfrac{1}{2} + 0 \times \tfrac{1}{2} + \tfrac{1}{2}\right) = \tfrac{1}{2} \end{aligned} \tag{19}$$

Since the δ decoy photons are included in E_i', the man-in-the-middle attack will be detected with a probability of $1 - \left(\frac{1}{2}\right)^{\delta}$. When δ is sufficiently large, this probability approached 1, making it impossible for the man-in-the-middle attack to succeed.

Case IV The Trojan horse attacks

Trojan horse attacks [64] are primarily categorized into two types: the invisible photon eavesdropping attack, where an eavesdropper uses undetectable photons to gather information about the transmitted quantum states, and the delay photon attack, in which an eavesdropper delays photons to manipulate communication between the parties. These attacks pose significant threats in quantum communication, particularly in bidirectional channels. However, the proposed protocol functions as a unidirectional cryptographic protocol, which inherently resists both types of Trojan horse attacks.

To conclude, any attempt at eavesdropping on the private information of the participants would be detectable, even if the outsider eavesdropper performs quantum-based attacks.

4.2.2. Participant Attacks

In this section, we will demonstrate that the proposed MQPC protocol is secure against attacks from the TP or the participants.

Case I: Security against attacks from the semi-honest party (TP)

In our protocol, the semi-honest third party (TP) adheres to the protocol rules while attempting to extract information from the private data of other parties. Although it cannot collude with dishonest parties, its actions require careful protocol design to ensure that the privacy of all participants is maintained. While the TP can apply the R_y $(-\Theta_i)$ operator on the encrypted quantum sequence E_i to decrypt it using the secret key Θ_i, aiming to recover the original quantum sequence S_i related to the binary inputs M_i and the secret non-zero binary key K, it cannot access the binary inputs M_i without knowing the shared key K between the participants. The secret non-zero binary key K, shared among n participants through a multiparty quantum key agreement (MQKA) protocol, remains undisclosed to the TP.

To conclude, the private information of the participants will not be leaked, even if the semi-honest TP utilizes the received information to deduce private information.

Case II: Security against attacks from participants

In our protocol, each participant sends E_i', which contains the encrypted quantum states and decoy photons, to the semi-honest third party (TP) via a quantum channel. If the quantum channel is secure, participant P_i announces their secret key Θ_i to the TP. Each participant can act as Eve to eavesdrop on the private information of others using quantum-based attacks. However, eavesdropping detection calculated by the ratio of incorrect measurements to the total number of measurements prevents participants from stealing the private inputs M_i. Additionally, the secret key Θ_i will only be announced if the eavesdropping detection is successful.

Even if the participants know the secret non-zero binary key K and attempt to intercept E_i' sent to the TP, they cannot pass the eavesdropping detection; the protocol will restart if any eavesdropping is detected. Furthermore, even if some participants collude, they cannot access another participant's inputs because they do not know the position and measurement bases of the decoy photons or the secret key Θ_i.

In conclusion, the participants' inputs remain confidential, even if some participants collude to attempt to steal another participant's inputs.

4.3. Fairness

Fairness is a fundamental aspect of secure computation protocols, ensuring that all participants have equal access to the results of the comparison process. In the proposed QPC protocol, the role of the third party (TP) is crucial in maintaining this fairness. By publishing the comparison results simultaneously, the TP prevents any participant from gaining an undue advantage over others. This simultaneous access eliminates the opportunity for one participant to act on the results before the others, thereby fostering an equitable environment. Consequently, the proposed protocol effectively addresses the critical issue of fairness through the strategic role of the trusted party, ensuring that all participants are treated equally throughout the comparison process.

5. Discussion

The calculation of qubit efficiency [58] in the proposed QPC protocol focuses solely on the resources directly utilized for the comparison of private data, which can be defined as follows:

$$\eta_e = \frac{\eta_c}{\eta_t} \tag{20}$$

where η_c denotes the length of binary representations M_i, and η_t denotes the qubits consumed during the comparison process, excluding those allocated for eavesdropping detection and quantum key distribution. In this protocol, comparing an L-bit classical binary message requires preparing nL qubits as quantum resources; thus, we can obtain $\eta_c = L$ and $\eta_t = nL$. Consequently, the qubit efficiency of the proposed protocol is $\eta_e = \frac{\eta_c}{\eta_t} = \frac{L}{nL}$.

A comparative analysis of the proposed MQPC protocol against previous protocols is summarized in Table 1. The protocol demonstrates improvements in the following areas.

Table 1. A comparison between the proposed MQPC protocol and previous protocols.

Protocol	Quantum Resource Used	Unitary Operation for Users	Quantum Technology Used	Key Sharing	Quantum Measurement for Users	Quantum Measurement for TP	Qubit Efficiency
Ref. [55]	n-particle GHZ class states	No	The entanglement correlation	No	Single particle	No	$\frac{L}{nL}$
Ref. [56]	d-dimensional basis state	Yes	Quantum Fourier transform and unitary operation	No	No	d-level single particle	$\frac{L}{nL}$
Ref. [57]	d-level n-particle entangled state and d-level two-particle entangled state	No	Quantum Fourier transform	No	d-level single particle	d-level single particle	$\frac{L}{3nL}$
Ref. [58]	d-level n + 1-particle cat state and d-level two-particle Bell state	Yes	Quantum entanglement swapping	No	d-level two-particle Bell state	d-level n + 1-particle cat state	$\frac{L}{3nL+L}$
Ref. [59]	d-level two-particle Bell entangled state	Yes	Quantum entanglement swapping and unitary operation	No	d-level two-particle Bell entangled state	d-level two-particle Bell entangled state	$\frac{L}{2nL+2L}$
Ours	Single photons	Yes	Rotation operation	Yes	No	Z-basis	$\frac{L}{nL}$

Firstly, unlike the protocols proposed in Refs. [55–59], which require the preparation of intricate high-dimensional quantum states, including n-particle GHZ class states or d-dimensional quantum states, posing significant challenges in implementation, our protocol simplifies these requirements. It does not necessitate the preparation of complex quantum states and instead utilizes single photons as quantum resources. This design makes it easily implementable with current quantum technologies due to the straightforward preparation of single photons.

Secondly, some existing MQPC protocols necessitate complex quantum technologies, such as the entanglement correlation of n-particles [55], the quantum entanglement swapping of d-level quantum states [58,59], and unitary operations for d-level quantum states [56], which are difficult to implement with current technologies. In contrast, our protocol employs rotation operations performed on single photons, which are readily implementable with existing quantum technologies.

Thirdly, our protocol utilizes single-particle measurements instead of d-level quantum state measurements, aligning it with current technical feasibility.

Although the qubit efficiency of our protocol is identical to that of Refs. [55,56] and requires the sharing of a secret key, it demonstrates superior performance due to the easier-to-implement quantum technologies used, particularly in terms of quantum resources, unitary operations, and quantum measurements.

6. Conclusions

In this paper, we propose a multiparty quantum private comparison (MQPC) protocol based on rotation operations to facilitate the comparison of equality relationships among n participants while preserving the confidentiality of their inputs. In this protocol, each participant's inputs are encoded into single photons, which serve as easier-to-implement quantum resources. Rotation operations are employed for the encryption and decryption of these single photons, while Z-basis measurements are used to obtain comparison results. This design aligns the proposed protocol with current technical feasibility while providing a robust mechanism for protecting the privacy of participants' inputs. Compared to existing MQPC frameworks that rely on complex quantum technologies, such as the entanglement correlation of n-particles, quantum entanglement swapping of d-level quantum states, and unitary operations for d-level quantum states, our protocol demonstrates significant advancements in practicality due to the simplicity of single photons, rotation operations, and Z-basis measurements. An illustrative example demonstrates the readability of the proposed protocol. The security analysis shows that the use of rotation operations and decoy photons provides a robust mechanism for protecting the privacy of the participants' inputs, making the protocol resistant to outsider eavesdropping and participant attacks. Additionally, the protocol meets the requirement of fairness, as all participants access the comparison results simultaneously. However, since all participants in our protocol must possess full quantum capabilities to perform the equality comparison, there is an increased demand for quantum resources. Under current quantum technology conditions, not all users can afford the high cost associated with complete quantum equipment. In the future, we will focus on developing the MQPC protocol to compare size relations among n participants and designing semi-quantum privacy comparison protocols [39].

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

Funding: This research was funded by the Open Fund of Network and Data Security Key Laboratory of Sichuan Province (Grant No. NDS2024-1) and Gongga Plan for the "Double World-class Project".

Data Availability Statement: Data are contained within the article.

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

References

1. 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.
2. 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]
3. Nadlinger, D.P.; Drmota, P.; Nichol, B.C.; Araneda, G.; Main, D.; Srinivas, R.; Lucas, D.M.; Ballance, C.J.; Ivanov, K.; Tan, E.Y.-Z.; et al. Experimental quantum key distribution certified by Bell's theorem. *Nature* **2022**, *607*, 682–686. [CrossRef] [PubMed]
4. Li, W.; Zhang, L.; Tan, H.; Lu, Y.; Liao, S.-K.; Huang, J.; Li, H.; Wang, Z.; Mao, H.-K.; Yan, B.; et al. High-rate quantum key distribution exceeding 110 Mb s^{-1}. *Nat. Photon.* **2023**, *17*, 416–421. [CrossRef]
5. Basset, F.B.; Valeri, M.; Roccia, E.; Muredda, V.; Poderini, D.; Neuwirth, J.; Spagnolo, N.; Rota, M.B.; Carvacho, G.; Sciarrino, F.; et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **2021**, *7*, eabe6379. [CrossRef]
6. Zahidy, M.; Ribezzo, D.; De Lazzari, C.; Vagniluca, I.; Biagi, N.; Müller, R.; Occhipinti, T.; Oxenløwe, L.K.; Galili, M.; Hayashi, T.; et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **2024**, *15*, 1651. [CrossRef]
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. Lin, S.; Zhang, X.; Guo, G.-D.; Wang, L.-L.; Liu, X.-F. Multiparty quantum key agreement. *Phys. Rev. A* **2021**, *104*, 042421. [CrossRef]
9. 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*, 21502631. [CrossRef]
10. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374.
11. Ying, J.W.; Wang, J.Y.; Xiao, Y.X.; Gu, S.P.; Wang, X.F.; Zhong, W.; Du, M.M.; Li, X.Y.; Shen, S.T.; Zhang, A.L.; et al. Passive-state preparation for quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2025**, *68*, 240312.
12. Chen, Y.; Situ, H.; Huang, Q.; Zhang, C. A novel quantum private set intersection scheme with a semi-honest third party. *Quantum Inf. Process.* **2023**, *22*, 429. [CrossRef]
13. Huang, X.; Zhang, W.; Zhang, S. Quantum multi-party private set intersection using single photons. *Phys. A Stat. Mech. Its Appl.* **2024**, *649*, 129974. [CrossRef]
14. Hou, M.; Wu, Y.; Zhang, S. Quantum Private Set Intersection Scheme Based on Bell States. *Axioms* **2025**, *14*, 120. [CrossRef]
15. 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.
16. Boudot, F.; Schoenmakers, B.; Traoré, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
17. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
18. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
19. 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]
20. 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]
21. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
22. Liu, B.; Gao, F.; Jia, H.-Y.; Huang, W.; Zhang, W.-W.; Wen, Q.-Y. Efficient quantum private comparison employing single photons and collective detection. *Quantum Inf. Process.* **2012**, *12*, 887–897. [CrossRef]
23. Hou, M.; Wu, Y. Two-Party Quantum Private Comparison Protocol Based on Rotational Encryption. *Appl. Sci.* **2025**, *15*, 722. [CrossRef]
24. 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]
25. 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.
26. Pan, H.M. Two-party quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3389–3395.
27. Wen, L.; Wang, Y.B.; Wei, C. Quantum private comparison protocol based on Bell entangled states. *Commun. Theor. Phys.* **2012**, *57*, 583.
28. Tseng, H.-Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **2012**, *11*, 373–384. [CrossRef]
29. Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. [CrossRef]
30. 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]
31. Lang, Y.F. Quantum private comparison using single bell state. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036.
32. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840.
33. Hou, M.; Wu, Y. Efficient Quantum Private Comparison with Unitary Operations. *Mathematics* **2024**, *12*, 3541. [CrossRef]
34. Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. [CrossRef] [PubMed]
35. Huang, X.; Zhang, S.B.; Cheng, W. Quantum Private Comparison Based on GHZ-type States. In Proceedings of the 2021 IEEE AFRICON, Arusha, Tanzania, 13–15 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
36. Ye, T.Y.; Ji, Z.X. Two-party quantum private comparison with five-qubit entangled states. *Int. J. Theor. Phys.* **2017**, *56*, 1517–1529.
37. Sun, Q. Quantum private comparison with six-particle maximally entangled states. *Mod. Phys. Lett. A* **2022**, *37*, 22501498. [CrossRef]
38. 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.
39. 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*, 22500262. [CrossRef]

40. 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]
41. Jia, H.Y.; Wen, Q.Y.; Li, Y.B.; Gao, F. Quantum private comparison using genuine four-particle entangled states. *Int. J. Theor. Phys.* **2012**, *51*, 1187–1194.
42. Pan, H.M. Quantum Private Comparison Based on χ-Type Entangled States. *Int. J. Theor. Phys.* **2017**, *56*, 3340–3347. [CrossRef]
43. 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.
44. Sun, Z.; Long, D. Quantum Private Comparison Protocol Based on Cluster States. *Int. J. Theor. Phys.* **2012**, *52*, 212–218. [CrossRef]
45. 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]
46. 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*, 621–628. [CrossRef]
47. 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.
48. Zhou, M.K. Improvements of quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2018**, *57*, 42–47. [CrossRef]
49. 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.
50. Hou, M.; Wu, Y. Quantum Private Comparison Protocol with Cluster States. *Axioms* **2025**, *14*, 70. [CrossRef]
51. Lin, S.; Sun, Y.; Liu, X.-F.; Yao, Z.-Q. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf. Process.* **2012**, *12*, 559–568. [CrossRef]
52. Guo, F.Z.; Gao, F.; Qin, S.J.; Zhang, J.; Wen, Q.Y. Quantum private comparison protocol based on entanglement swapping of d-level Bell states. *Quantum Inf. Process.* **2013**, *12*, 2793–2802. [CrossRef]
53. Yu, C.H.; Guo, G.D.; Lin, S. Quantum private comparison with d-level single-particle states. *Phys. Scr.* **2013**, *88*, 065013. [CrossRef]
54. 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]
55. Chang, Y.-J.; Tsai, C.-W.; Hwang, T. Multi-user private comparison protocol using GHZ class states. *Quantum Inf. Process.* **2013**, *12*, 1077–1088. [CrossRef]
56. Liu, W.; Wang, Y.B.; Wang, X.M. Multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping. *Int. J. Theor. Phys.* **2014**, *53*, 1085–1091.
57. Wang, Q.L.; Sun, H.X.; Huang, W. Multi-party quantum private comparison protocol with n-level entangled states. *Quantum Inf. Process.* **2014**, *13*, 2375–2389. [CrossRef]
58. Ji, Z.X.; Yu, Y.T. 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]
59. 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]
60. 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]
61. Cao, H.; Ma, W. Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. *Sci. Rep.* **2017**, *7*, srep45046. [CrossRef]
62. Lin, J.; Tseng, H.-Y.; Hwang, T. Intercept–resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. *Opt. Commun.* **2011**, *284*, 2412–2414. [CrossRef]
63. Huang, X.; Zhang, S.; Xia, J. Efficient Quantum Private Comparison Using Locally Indistinguishable Orthogonal Product States. In *International Conference on Artificial Intelligence and Security, Proceedings of the 8th International Conference on Artificial Intelligence and Security, ICAIS 2022, Qinghai, China, 15–20 July 2022*; Springer International Publishing: Cham, Switzerland, 2022; pp. 260–273.
64. Yang, X.; Wei, K.; Ma, H.; Sun, S.; Du, Y.; Wu, L. Trojan horse attacks on counterfactual quantum key distribution. *Phys. Lett. A* **2016**, *380*, 1589–1592. [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.