entropy

MDPI

Article

Efficient Quantum Private Comparison Based on GHZ States

Min Hou [1,2], Yue Wu [1] 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, Chengdu University of Information Technology, Chengdu 610225, China
[4] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chendu 610225, China
* Correspondence: cuitzsb@cuit.edu.cn

Abstract: Quantum private comparison (QPC) is a fundamental cryptographic protocol that allows two parties to compare the equality of their private inputs without revealing any information about those inputs to each other. In recent years, QPC protocols utilizing various quantum resources have been proposed. However, these QPC protocols have lower utilization of quantum resources and qubit efficiency. To address this issue, we propose an efficient QPC protocol based on GHZ states, which leverages the unique properties of GHZ states and rotation operations to achieve secure and efficient private comparison. The secret information is encoded in the rotation angles of rotation operations performed on the received quantum sequence transmitted along the circular mode. This results in the multiplexing of quantum resources and enhances the utilization of quantum resources. Our protocol does not require quantum key distribution (QKD) for sharing a secret key to ensure the security of the inputs, resulting in no consumption of quantum resources for key sharing. One GHZ state can be compared to three bits of classical information in each comparison, leading to qubit efficiency reaching 100%. Compared with the existing QPC protocol, our protocol does not require quantum resources for sharing a secret key. It also demonstrates enhanced performance in qubit efficiency and the utilization of quantum resources.

Keywords: quantum private comparison (QPC); rotation operation; GHZ states; efficiency

Citation: Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. https://doi.org/10.3390/e26050413

Academic Editors: Sebastian Deffner, Harry Shaw and Ryan T. Glasser

Received: 19 April 2024
Revised: 6 May 2024
Accepted: 8 May 2024
Published: 10 May 2024

1. Introduction

Quantum private comparison (QPC) plays a crucial role in secure multi-party computation and privacy-preserving applications. It enables two parties, Alice and Bob, to compare their private inputs without disclosing any information about those inputs to each other or to any eavesdroppers. Traditional classical private comparison protocols are inherently vulnerable to information leakage because they rely on the assumption of number-theoretical complexity, which is no longer reliable due to the emergence of quantum algorithms (e.g., Shor's algorithm [1] and Grover's algorithm [2]). QPC, on the other hand, leverages the unique properties of quantum mechanics (such as quantum entanglement, non-cloning, the uncertainty principle, and the superposition principle) to conduct secure comparisons while safeguarding the privacy of the inputs and ensuring information-theoretic security.

The first QPC protocol was suggested by Yang and Wen [3], utilizing two-photon entangled states and four unitary operations to achieve the comparison. Decoy photons and hash functions are used to prevent eavesdropping on players' private inputs. In 2010, triplet GHZ states and single-particle measurements were used to develop an efficient QPC protocol [4]. This protocol divides secret messages into multiple groups, resulting in saved quantum resources. Nevertheless, Ref. [4] was susceptible to quantum attacks and, thus, results in information leakage. Some improvements have been proposed to

enhance its security [5]. Then, Tseng et al. [6] utilized quantum entanglement of Bell states to propose an easier implementation of the QPC protocol, achieving a qubit efficiency of 50%. Jia et al. [7] employed the entanglement properties of χ-type states as information carriers to accomplish private comparison. Local unitary operations are used to encode private information, and joint measurements are adopted to extract the results. Quantum superdense coding is utilized to achieve higher efficiency. Since then, several QPC protocols have been proposed, utilizing various quantum resources such as single photons [8–11], entangled states [12–21], and cluster states [22–26]. Additionally, two-atom product states and single-atom measurements are used in a QPC protocol [27]. This protocol enables the comparison of the equality of one classical bit in each round, resulting in the qubit efficiency reaching 50%. Another QPC protocol, which does not require any classical computation, was proposed by Lang [28] in 2020. In this protocol, quantum gates are utilized for classical calculations instead of the bitwise XOR operation, leading to improved security. Zhang et al. [29] utilized quantum homomorphic encryption to develop a multi-party QPC protocol with a TP who will faithfully perform homomorphic calculations, effectively reducing the quantum resources required. A different QPC protocol, developed by Huang et al. in 2023 [30], is used to determine the equality of single-qubit states. This protocol utilizes more accessible quantum technologies, such as rotation encryption and swap test, to compare qubits.

According to the analysis of previous QPC protocols, while the aforementioned QPC protocols have shown potential for achieving secure private comparison, they often encounter challenges related to the utilization of quantum resources and qubit efficiency. For example, in most cases, the equality of one classical bit can be compared with Bell states and GHZ states. The qubit efficiency only reaches 50% and 33%, respectively, which limits qubit efficiency. In addition, most QPC protocols require the implementation of QKD protocol to share a secret key used for encrypting private inputs, resulting in a decrease in the utilization of quantum states. Therefore, appropriate measures need to be selected to enhance the qubit efficiency of QPC protocols. Rotation operations, which are special unitary operations, have received widespread attention. Various rotation-operation-based quantum secure protocols have been proposed, such as quantum secret sharing (QSS) [31], quantum signature [32], and quantum key agreement [33]. Rotation operations can also be applied in designing QPC protocols due to their unique properties.

In this paper, we utilize GHZ states and rotation operations to propose an efficient QPC protocol, which achieves a qubit efficiency of 100% and a higher utilization rate of quantum resources. In our protocol, two users encode their secrets into the received quantum sequence, that is, performing the corresponding rotation operation on the received GHZ states. The secrets can be privately compared with a TP who will not deviate from the protocol execution or conspire with any participant, but may attempt to obtain the inputs of the users by learning the immediate data. The function of the TP is to prepare and encrypt an initial quantum sequence contained in GHZ states at the beginning and, then, decrypt and measure the decrypted quantum sequence at the end.

The main contributions of our paper are as follows.

(1) Our protocol does not require QKD protocol for sharing a secret key to ensure the security of the inputs. This results in no consumption of quantum resources for key sharing.
(2) The quantum sequence is transmitted between the TP and two users in a circular mode. The inputs of the two users are encoded into the transmitted quantum sequence, leading to the multiplexing of quantum resources and improving the utilization of quantum resources.
(3) One GHZ state can be compared to three-bit classical information, enabling qubit efficiency to reach 100%.

The rest of this paper is structured as follows. Preliminary knowledge is introduced in Section 2. The proposed quantum private comparison based on GHZ states is presented in Section 3. A simulation experiment demonstrating the correctness and feasibility of our

protocol is outlined in Section 4. Security analysis and qubit efficiency are discussed in Sections 5 and 6, respectively. Finally, the conclusion is provided in Section 5.

2. Preliminary Knowledge

Eight types of GHZ states in our protocol are denoted as

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{1}$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \tag{2}$$

$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle) \tag{3}$$

$$|\varphi_4\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle) \tag{4}$$

$$|\varphi_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle) \tag{5}$$

$$|\varphi_6\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle) \tag{6}$$

$$|\varphi_7\rangle = \frac{1}{\sqrt{2}}(|110\rangle + |001\rangle) \tag{7}$$

$$|\varphi_8\rangle = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle) \tag{8}$$

The rotation operation is denoted as

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{9}$$

Equation (9) represents a unitary matrix since $R_y^\dagger(\theta)R_y(\theta) = I$, and it can be implemented by rotating around the y-axis with θ on the Bloch sphere.

When performing rotation operations on GHZ states, we observe the following two features.

Lemma 1. *For any* $|\varphi_i\rangle (i = 1, 2, \cdots, 8)$, $\big(R_y(-\theta_1) \otimes R_y(-\theta_2) \otimes R_y(-\theta_3)\big)$ $(R_y(\theta_1) \otimes R_y(\theta_2) \otimes R_y(\theta_3))|\varphi_i\rangle = |\varphi_i\rangle$ *holds.*

Proof. Let us consider $|\varphi_1\rangle$ as an example. We have the following equation.

$$\begin{aligned}
&\big(R_y(-\theta_1) \otimes R_y(-\theta_2) \otimes R_y(-\theta_3)\big)\big(R_y(\theta_1) \otimes R_y(\theta_2) \otimes R_y(\theta_3)\big)|\varphi_1\rangle \\
&= \tfrac{1}{\sqrt{2}}\big(R_y(-\theta_1) \otimes R_y(-\theta_2) \otimes R_y(-\theta_3)\big)\begin{pmatrix} R_y(\theta_1)|0\rangle \otimes R_y(\theta_2)|0\rangle \otimes R_y(\theta_3)|0\rangle \\ +R_y(\theta_1)|1\rangle \otimes R_y(\theta_2)|1\rangle \otimes R_y(\theta_3)|1\rangle \end{pmatrix} \\
&= \tfrac{1}{\sqrt{2}}\begin{pmatrix} R_y(0)|0\rangle \otimes R_y(0)|0\rangle \otimes R_y(0)|0\rangle \\ +R_y(0)|1\rangle \otimes R_y(0)|1\rangle \otimes R_y(0)|1\rangle \end{pmatrix} \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \otimes |1\rangle) \\
&= |\varphi_1\rangle
\end{aligned} \tag{10}$$

In the same way, we can prove that

$$\big(R_y(-\theta_1) \otimes R_y(-\theta_2) \otimes R_y(-\theta_3)\big)\big(R_y(\theta_1) \otimes R_y(\theta_2) \otimes R_y(\theta_3)\big)|\varphi_i\rangle = |\varphi_i\rangle \tag{11}$$

Thus, Lemma 1 holds. □

Lemma 2. *For $\theta_j \in \{0, \pi\}, j \in \{1,2,3\}$,the resultant states, without considering the global phase, are shown in Table 1 when performing the corresponding rotation operation $R_y(\theta_j)$ on each particle of different GHZ states.*

Table 1. The resultant states without considering the global phase.

	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$	$\|\varphi_7\rangle$	$\|\varphi_8\rangle$
$\theta_1\theta_2\theta_3 = 000$	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$	$\|\varphi_7\rangle$	$\|\varphi_8\rangle$
$\theta_1\theta_2\theta_3 = 00\pi$	$\|\varphi_8\rangle$	$\|\varphi_7\rangle$	$\|\varphi_6\rangle$	$\|\varphi_5\rangle$	$\|\varphi_4\rangle$	$\|\varphi_3\rangle$	$\|\varphi_2\rangle$	$\|\varphi_1\rangle$
$\theta_1\theta_2\theta_3 = 0\pi0$	$\|\varphi_6\rangle$	$\|\varphi_5\rangle$	$\|\varphi_8\rangle$	$\|\varphi_7\rangle$	$\|\varphi_2\rangle$	$\|\varphi_1\rangle$	$\|\varphi_4\rangle$	$\|\varphi_3\rangle$
$\theta_1\theta_2\theta_3 = 0\pi\pi$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\varphi_7\rangle$	$\|\varphi_8\rangle$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$
$\theta_1\theta_2\theta_3 = \pi00$	$\|\varphi_4\rangle$	$\|\varphi_3\rangle$	$\|\varphi_2\rangle$	$\|\varphi_1\rangle$	$\|\varphi_8\rangle$	$\|\varphi_7\rangle$	$\|\varphi_6\rangle$	$\|\varphi_5\rangle$
$\theta_1\theta_2\theta_3 = \pi0\pi$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$	$\|\varphi_7\rangle$	$\|\varphi_8\rangle$	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$
$\theta_1\theta_2\theta_3 = \pi\pi0$	$\|\varphi_7\rangle$	$\|\varphi_8\rangle$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$
$\theta_1\theta_2\theta_3 = \pi\pi\pi$	$\|\varphi_2\rangle$	$\|\varphi_1\rangle$	$\|\varphi_4\rangle$	$\|\varphi_3\rangle$	$\|\varphi_6\rangle$	$\|\varphi_5\rangle$	$\|\varphi_8\rangle$	$\|\varphi_7\rangle$

3. Quantum Private Comparison Based on GHZ States

In this section, we will provide detailed steps of the proposed QPC protocol, where a semi-honest TP assists two distrustful players, Alice and Bob, in comparing whether their secrets are equal. The semi-honest TP will not deviate from the protocol execution or conspire with any participant, but may try to obtain useful information about the users' inputs through illicit means.

Suppose that Alice and Bob hold their private integers denoted as I_a and I_b, respectively. I_a and I_b can be represented in binary form as $X = \{x_1, x_2, \cdots, x_N\}$, $Y = \{y_1, y_2, \cdots, y_N\}$, respectively, where $x_i, y_i \in \{0,1\}, i = \{1,2,\cdots,N\}$, N is the length of the secrets, $X = \sum_{i=1}^{N} x_i 2^{i-1}$, and $Y = \sum_{i=1}^{N} y_i 2^{i-1}$. We assume that the quantum channel in the communication process is noiseless and lossless, while the classical channel is authenticated. By authenticating the classical channel, the identities of all communication parties can be verified, ensuring that only legitimate entities participate in the execution of the protocol. The detailed steps of the proposed QPC protocol based on GHZ states are as follows, and its diagram is depicted in Figure 1.

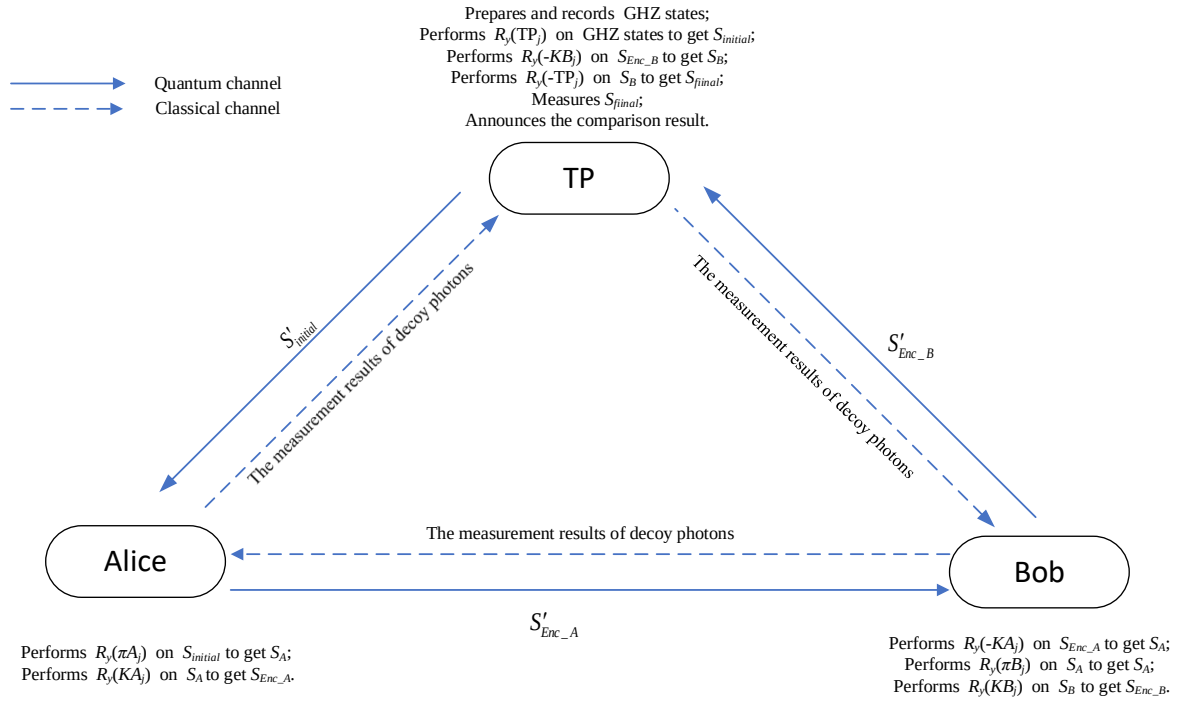

Figure 1. The diagram of the QPC protocol.

Step 1. Alice and Bob divide an N-bit string X and Y into $N/3$ groups, respectively. Each group consists of 3-bit classical information. If $N\text{mod}3 \neq 0$, fill in $3-(N\text{mod}3)$ 0 for the last group. The N-bit strings X and Y are converted to $X = (A_1, A_2, \cdots, A_{N/3})$ and $Y = (B_1, B_2, \cdots, B_{N/3})$, respectively, where $A_j = \left(a_j^1, a_j^2, a_j^3\right)$, $B_j = \left(b_j^1, b_j^2, b_j^3\right)$ and $j = 1, 2, \cdots, N/3$.

Step 2. TP prepares $N/3$ *GHZ* states selected from Equations (1)–(8) and records these states. Then, she generates a secret key $\Theta_{TP} = (TP_1, TP_2, \cdots, TP_{N/3})$, where $TP_j = \left(tp_j^1, tp_j^2, tp_j^3\right) \in [0, 2\pi)$ and $j = 1, 2, \cdots, N/3$. Finally, she performs rotation operations $R_y\left(TP_j\right)$ on the j-th GHZ states to obtain a sequence $S_{initial}$.

Step 3. TP prepares $3M$ photons randomly chosen from four quantum states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ as decoy states. These photons are then inserted into $S_{initial}$ at random positions to obtain a new sequence $S'_{initial}$. The corresponding states and positions of decoy states are recorded by TP who will then send the sequence $S'_{initial}$ to Alice.

Step 4. Upon receiving the sequence $S'_{initial}$, Alice sends an acknowledgment to TP who will verify the presence of eavesdroppers. TP announces the corresponding bases and positions of decoy states to Alice, who will then conduct measurements on these states and return the measurement outcomes to TP. TP detects the presence of eavesdroppers in the transmission channel by comparing the consistency of the measurement outcomes with the initially prepared decoy states and calculates the error rate. If the error rate exceeds a predefined threshold, this protocol will be rebooted. Otherwise, the protocol proceeds to the following steps.

Step 5. Alice discards decoy states in $S'_{initial}$ to obtain $S_{initial}$ and performs rotation operations $R_y\left(\pi A_j\right)$ on the j-th states in $S_{initial}$ to obtain a sequence S_A. She then generates her secret key $\Theta_{KA} = (KA_1, KA_2, \cdots, KA_{N/3})$, where $KA_j = \left(ka_j^1, ka_j^2, ka_j^3\right) \in [0,\ 2\pi)$ and $j = 1, 2, \cdots, N/3$, and performs rotation operations $R_y\left(KA_j\right)$ on the j-th states in S_A to obtain a sequence S_{Enc_A}. To prevent eavesdropping, Alice randomly selects $3M$ photons from four quantum states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ as decoy states. These photons are then inserted into S_{Enc_A} at random positions to obtain a new sequence S'_{Enc_A}. Alice records the corresponding states and positions of decoy states and sends the sequence S'_{Enc_A} to Bob.

Step 6. Upon receiving the sequence S'_{Enc_A}, Bob interacts with Alice to check for the presence of eavesdroppers in the transmission process, similar to Step 4. If no outsider eavesdropper exists, Alice announces her secret key Θ_{KA} to Bob, who will then discard decoy states in S'_{Enc_A} to obtain S_{Enc_A} and perform rotation operations $R_y\left(-KA_j\right)$ on the j-th states in S_{Enc_A} to recover the sequence S_A.

Step 7. Bob performs rotation operations $R_y\left(\pi B_j\right)$ on the j-th states in S_A to obtain a sequence S_B. He then generates his secret key $\Theta_{KB} = (KB_1, KB_2, \cdots, KB_{N/3})$, where $KB_j = \left(kb_j^1, kb_j^2, kb_j^3\right) \in [0,\ 2\pi)$ and $j = 1, 2, \cdots, N/3$, and performs rotation operations $R_y\left(KB_j\right)$ on the j-th states in S_B to obtain a sequence S_{Enc_B}. To thwart potential external attacks by eavesdroppers, Bob randomly inserts 3M photons into S_{Enc_B} at various positions to obtain a new sequence S'_{Enc_B}. These photons are chosen from four quantum states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ as decoy states. Bob records the states and positions of decoy states and sends the sequence S'_{Enc_B} to TP.

Step 8. Upon receiving the sequence S'_{Enc_B}, TP interacts with Bob to detect eavesdropping, similar to Step 4. If no eavesdropper exists in the transmission process, Bob will announce his secret key Θ_{KB} to TP, who will then discard the decoy states in S'_{Enc_B} to obtain S_{Enc_B} and perform rotation operations $R_y\left(-KB_j\right)$ on the j-th states in S_{Enc_B} to recover the sequence S_B.

Step 9. TP performs rotation operations $R_y\left(-TP_j\right)$ on the j-th GHZ states in S_B to obtain a sequence S_{final} and, then, conducts GHZ-basis measurements on the j-th states in S_{final} to obtain the measurement outcomes. If each measurement outcome is consistent with the initially prepared GHZ states in Step 2, then $X = Y$. Otherwise, $X \neq Y$. TP announces the comparison results to Alice and Bob.

4. Simulation Experiment

In this section, we utilize a concrete example and its simulation on IBM Quantum Composer to show the correctness and feasibility of our protocol. Suppose that the private integers of Alice and Bob are $X = 10$ and $Y = 18$, which can be represented in binary form as $X = (x_1, x_2, x_3, x_4) = 0101$ and $Y = (y_1, y_2, y_3, y_4, y_5) = 01001$, respectively. Alice and Bob divide the strings X and Y into two groups, $X = (A_1, A_2) = (x_1x_2x_3, x_4)$ and $Y = (B_1, B_2) = (y_1y_2y_3, y_4y_5)$. Since the lengths of X and Y are not multiples of three, Alice and Bob will add two zero and one zero in the group of A_2 and B_2, respectively. Thereafter, $A_1 = (x_1x_2x_3) = (010)$, $A_2 = (x_400) = (100)$, $B_1 = (y_1y_2y_3) = (010)$, $B_2 = (y_4y_50) = (010)$.

We assume that the semi-honest TP prepares two GHZ states denoted as $|\varphi_1\rangle$ and $|\varphi_6\rangle$ and the secret key $\Theta_{TP} = (TP_1, TP_2) = \left(\left(tp_1^1, tp_1^2, tp_1^3\right), \left(tp_2^1, tp_2^2, tp_2^3\right)\right) = \left(\left(\frac{2\pi}{3}, \frac{\pi}{6}, \frac{\pi}{2}\right), \left(\frac{4\pi}{3}, \frac{3\pi}{4}, \frac{3\pi}{5}\right)\right)$. When performing rotation operations $R_y(TP_1)$ and $R_y(TP_2)$ on the two GHZ states, the resultant sequence $S_{initial}$ can be written as

$$S_{\text{initial}} = \begin{pmatrix} R_y\left(tp_1^1\right) \otimes R_y\left(tp_1^2\right) \otimes R_y\left(tp_1^3\right)|\varphi_1\rangle, \\ R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right)|\varphi_6\rangle \end{pmatrix} = \begin{pmatrix} R_y\left(\frac{2\pi}{3}\right) \otimes R_y\left(\frac{\pi}{6}\right) \otimes R_y\left(\frac{\pi}{2}\right)|\varphi_1\rangle, \\ R_y\left(\frac{4\pi}{3}\right) \otimes R_y\left(\frac{3\pi}{4}\right) \otimes R_y\left(\frac{3\pi}{5}\right)|\varphi_6\rangle \end{pmatrix} \tag{12}$$

When receiving the sequence $S_{initial}$, Alice performs the rotation operations $R_y(\pi A_1)$ and $R_y(\pi A_2)$ on the two states in $S_{initial}$ to obtain a sequence S_A, which can be expressed as

$$\begin{aligned} S_A &= \begin{pmatrix} \left(R_y(\pi x_1) \otimes R_y(\pi x_2) \otimes R_y(\pi x_3)\right)\left(R_y\left(tp_1^1\right) \otimes R_y\left(tp_1^2\right) \otimes R_y\left(tp_1^3\right)\right)|\varphi_1\rangle, \\ \left(R_y(\pi x_4) \otimes R_y(\pi x_5) \otimes R_y(\pi x_6)\right)\left(R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right)\right)|\varphi_6\rangle \end{pmatrix} \\ &= \begin{pmatrix} \left(R_y(0) \otimes R_y(\pi) \otimes R_y(0)\right)\left(R_y\left(\frac{2\pi}{3}\right) \otimes R_y\left(\frac{\pi}{6}\right) \otimes R_y\left(\frac{\pi}{2}\right)\right)|\varphi_1\rangle, \\ \left(R_y(\pi) \otimes R_y(0) \otimes R_y(0)\right)\left(R_y\left(\frac{4\pi}{3}\right) \otimes R_y\left(\frac{3\pi}{4}\right) \otimes R_y\left(\frac{3\pi}{5}\right)\right)|\varphi_6\rangle \end{pmatrix} \end{aligned} \tag{13}$$

We assume that the secret key $\Theta_{KA} = (KA_1, KA_2) = \left(\left(ka_1^1, ka_1^2, ka_1^3\right), \left(ka_2^1, ka_2^2, ka_2^3\right)\right) = \left(\left(\frac{\pi}{3}, \frac{5\pi}{6}, \frac{\pi}{4}\right), \left(\frac{3\pi}{4}, \frac{\pi}{2}, \frac{\pi}{6}\right)\right)$. When performing rotation operations $R_y(KA_1)$ and $R_y(KA_2)$ on the two states in S_A, the resultant sequence S_{Enc_A} can be written as

$$\begin{aligned} S_{Enc\_A} &= \begin{pmatrix} \left(R_y\left(ka_1^1\right) \otimes R_y\left(ka_1^2\right) \otimes R_y\left(ka_1^3\right)\right)\left(R_y(\pi x_1) \otimes R_y(\pi x_2) \otimes R_y(\pi x_3)\right)\left(R_y\left(tp_1^1\right) \otimes R_y\left(tp_1^2\right) \otimes R_y\left(tp_1^3\right)\right)|\varphi_1\rangle, \\ \left(R_y\left(ka_2^1\right) \otimes R_y\left(ka_2^1\right) \otimes R_y\left(ka_2^1\right)\right)\left(R_y(\pi x_4) \otimes R_y(\pi x_5) \otimes R_y(\pi x_6)\right)\left(R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right)\right)|\varphi_6\rangle \end{pmatrix} \\ &= \begin{pmatrix} \left(R_y\left(\frac{\pi}{3}\right) \otimes R_y\left(\frac{5\pi}{6}\right) \otimes R_y\left(\frac{\pi}{4}\right)\right)\left(R_y(0) \otimes R_y(\pi) \otimes R_y(0)\right)\left(R_y\left(\frac{2\pi}{3}\right) \otimes R_y\left(\frac{\pi}{6}\right) \otimes R_y\left(\frac{\pi}{2}\right)\right)|\varphi_1\rangle, \\ \left(R_y\left(\frac{3\pi}{4}\right) \otimes R_y\left(\frac{\pi}{2}\right) \otimes R_y\left(\frac{\pi}{6}\right)\right)\left(R_y(\pi) \otimes R_y(0) \otimes R_y(0)\right)\left(R_y\left(\frac{4\pi}{3}\right) \otimes R_y\left(\frac{3\pi}{4}\right) \otimes R_y\left(\frac{3\pi}{5}\right)\right)|\varphi_6\rangle \end{pmatrix} \end{aligned} \tag{14}$$

When receiving the secret key Θ_{KA} and obtaining the sequence S_{Enc_A}, Bob performs rotation operations $R_y(-KA_1)$ and $R_y(-KA_2)$ on the two states in S_{Enc_A} to recover the sequence S_A. This process can be written as

$$\begin{aligned} S_A &= \begin{pmatrix} \begin{pmatrix} \left(R_y\left(-ka_1^1\right) \otimes R_y\left(-ka_1^2\right) \otimes R_y\left(-ka_1^3\right)\right)\left(R_y\left(ka_1^1\right) \otimes R_y\left(ka_1^2\right) \otimes R_y\left(ka_1^3\right)\right) \\ \left(R_y(\pi x_1) \otimes R_y(\pi x_2) \otimes R_y(\pi x_3)\right)\left(R_y\left(tp_1^1\right) \otimes R_y\left(tp_1^2\right) \otimes R_y\left(tp_1^3\right)\right) \end{pmatrix}|\varphi_1\rangle, \\ \begin{pmatrix} \left(R_y\left(-ka_2^1\right) \otimes R_y\left(-ka_2^1\right) \otimes R_y\left(-ka_2^1\right)\right)\left(R_y\left(ka_2^1\right) \otimes R_y\left(ka_2^1\right) \otimes R_y\left(ka_2^1\right)\right) \\ \left(R_y(\pi x_4) \otimes R_y(\pi x_5) \otimes R_y(\pi x_6)\right)\left(R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right)\right) \end{pmatrix}|\varphi_6\rangle \end{pmatrix} \\ &= \begin{pmatrix} \left(R_y(\pi x_1) \otimes R_y(\pi x_2) \otimes R_y(\pi x_3)\right)\left(R_y\left(tp_1^1\right) \otimes R_y\left(tp_1^2\right) \otimes R_y\left(tp_1^3\right)\right)|\varphi_1\rangle, \\ \left(R_y(\pi x_4) \otimes R_y(\pi x_5) \otimes R_y(\pi x_6)\right)\left(R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right) \otimes R_y\left(tp_2^1\right)\right)|\varphi_6\rangle \end{pmatrix} \\ &= \begin{pmatrix} \left(R_y(0) \otimes R_y(\pi) \otimes R_y(0)\right)\left(R_y\left(\frac{2\pi}{3}\right) \otimes R_y\left(\frac{\pi}{6}\right) \otimes R_y\left(\frac{\pi}{2}\right)\right)|\varphi_1\rangle, \\ \left(R_y(\pi) \otimes R_y(0) \otimes R_y(0)\right)\left(R_y\left(\frac{4\pi}{3}\right) \otimes R_y\left(\frac{3\pi}{4}\right) \otimes R_y\left(\frac{3\pi}{5}\right)\right)|\varphi_6\rangle \end{pmatrix} \end{aligned} \tag{15}$$

When performing rotation operations $R_y(\pi B_1)$ and $R_y(\pi B_2)$ on the two states in S_A, the resulting sequence S_B can be written as

$$
\begin{aligned}
S_B &= \begin{pmatrix} (R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3))(R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))(R_y(tp_1^1)\otimes R_y(tp_1^2)\otimes R_y(tp_1^3))|\varphi_1\rangle, \\ (R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6))(R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))(R_y(tp_2^1)\otimes R_y(tp_2^1)\otimes R_y(tp_2^1))|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} (R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\frac{2\pi}{3})\otimes R_y(\frac{\pi}{6})\otimes R_y(\frac{\pi}{2}))|\varphi_1\rangle, \\ (R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\pi)\otimes R_y(0)\otimes R_y(0))\left(R_y\left(\frac{4\pi}{3}\right)\otimes R_y(\frac{3\pi}{4})\otimes R_y(\frac{3\pi}{5})\right)|\varphi_6\rangle \end{pmatrix}
\end{aligned} \tag{16}
$$

We assume that the secret key $\Theta_{KB} = (KB_1, KB_2) = \left(\left(kb_1^1, kb_1^2, kb_1^3\right), \left(kb_2^1, kb_2^2, kb_2^3\right)\right) = \left(\left(\frac{\pi}{2}, \frac{\pi}{3}, \frac{5\pi}{6}\right), \left(\frac{\pi}{4}, \frac{\pi}{8}, \frac{\pi}{3}\right)\right)$. When performing rotation operations $R_y(KB_1)$ and $R_y(KB_2)$ on the two states in S_B, the resultant sequence S_{Enc_B} can be written as

$$
\begin{aligned}
S_{Enc\_B} &= \begin{pmatrix} \begin{pmatrix} (R_y(kb_1^1)\otimes R_y(kb_1^2)\otimes R_y(kb_1^3))(R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3)) \\ (R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))(R_y(tp_1^1)\otimes R_y(tp_1^2)\otimes R_y(tp_1^3)) \end{pmatrix}|\varphi_1\rangle, \\ \begin{pmatrix} (R_y(kb_2^1)\otimes R_y(kb_2^1)\otimes R_y(kb_2^1))(R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6)) \\ (R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))(R_y(tp_2^1)\otimes R_y(tp_2^1)\otimes R_y(tp_2^1)) \end{pmatrix}|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} \begin{pmatrix} (R_y(\frac{\pi}{2})\otimes R_y(\frac{\pi}{3})\otimes R_y(\frac{5\pi}{6}))(R_y(0)\otimes R_y(\pi)\otimes R_y(0)) \\ (R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\frac{2\pi}{3})\otimes R_y(\frac{\pi}{6})\otimes R_y(\frac{\pi}{2})) \end{pmatrix}|\varphi_1\rangle, \\ \begin{pmatrix} (R_y(\frac{\pi}{4})\otimes R_y(\frac{\pi}{8})\otimes R_y(\frac{\pi}{3}))(R_y(0)\otimes R_y(\pi)\otimes R_y(0)) \\ (R_y(\pi)\otimes R_y(0)\otimes R_y(0))\left(R_y\left(\frac{4\pi}{3}\right)\otimes R_y(\frac{3\pi}{4})\otimes R_y(\frac{3\pi}{5})\right) \end{pmatrix}|\varphi_6\rangle \end{pmatrix}
\end{aligned} \tag{17}
$$

When receiving the secret key Θ_{KB} and obtaining the sequence S_{Enc_B}, the semi-honest TP performs rotation operations $R_y(-KB_1)$ and $R_y(-KB_2)$ on the two states in S_{Enc_B} to recover the sequence S_B. This process can be expressed as

$$
\begin{aligned}
S_B &= \begin{pmatrix} \begin{pmatrix} (R_y(-kb_1^1)\otimes R_y(-kb_1^2)\otimes R_y(-kb_1^3))(R_y(kb_1^1)\otimes R_y(kb_1^2)\otimes R_y(kb_1^3))(R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3)) \\ (R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))(R_y(tp_1^1)\otimes R_y(tp_1^2)\otimes R_y(tp_1^3)) \end{pmatrix}|\varphi_1\rangle, \\ \begin{pmatrix} (R_y(-kb_2^1)\otimes R_y(-kb_2^1)\otimes R_y(-kb_2^1))(R_y(kb_2^1)\otimes R_y(kb_2^1)\otimes R_y(kb_2^1))(R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6)) \\ (R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))(R_y(tp_2^1)\otimes R_y(tp_2^1)\otimes R_y(tp_2^1)) \end{pmatrix}|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} ((R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3))(R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))(R_y(tp_1^1)\otimes R_y(tp_1^2)\otimes R_y(tp_1^3)))|\varphi_1\rangle, \\ ((R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6))(R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))(R_y(tp_2^1)\otimes R_y(tp_2^1)\otimes R_y(tp_2^1)))|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} ((R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\frac{2\pi}{3})\otimes R_y(\frac{\pi}{6})\otimes R_y(\frac{\pi}{2})))|\varphi_1\rangle, \\ \left((R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\pi)\otimes R_y(0)\otimes R_y(0))\left(R_y\left(\frac{4\pi}{3}\right)\otimes R_y(\frac{3\pi}{4})\otimes R_y(\frac{3\pi}{5})\right)\right)|\varphi_6\rangle \end{pmatrix}
\end{aligned} \tag{18}
$$

When performing rotation operations $R_y(-TP_1)$ and $R_y(-TP_2)$ on the two states in S_B, the resultant sequence S_{final} can be given by

$$
\begin{aligned}
S_{final} &= \begin{pmatrix} \begin{pmatrix} (R_y(-tp_1^1)\otimes R_y(-tp_1^2)\otimes R_y(-tp_1^3))(R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3)) \\ (R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))(R_y(tp_1^1)\otimes R_y(tp_1^2)\otimes R_y(tp_1^3)) \end{pmatrix}|\varphi_1\rangle, \\ \begin{pmatrix} (R_y(-tp_2^1)\otimes R_y(-tp_2^1)\otimes R_y(-tp_2^1))(R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6)) \\ (R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))(R_y(tp_2^1)\otimes R_y(tp_2^1)\otimes R_y(tp_2^1)) \end{pmatrix}|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} (R_y(\pi y_1)\otimes R_y(\pi y_2)\otimes R_y(\pi y_3))(R_y(\pi x_1)\otimes R_y(\pi x_2)\otimes R_y(\pi x_3))|\varphi_1\rangle, \\ (R_y(\pi y_4)\otimes R_y(\pi y_5)\otimes R_y(\pi y_6))(R_y(\pi x_4)\otimes R_y(\pi x_5)\otimes R_y(\pi x_6))|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} (R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(0)\otimes R_y(\pi)\otimes R_y(0))|\varphi_1\rangle, \\ (R_y(0)\otimes R_y(\pi)\otimes R_y(0))(R_y(\pi)\otimes R_y(0)\otimes R_y(0))|\varphi_6\rangle \end{pmatrix} \\
&= \begin{pmatrix} (R_y(0)\otimes R_y(0)\otimes R_y(0))|\varphi_1\rangle, \\ (R_y(\pi)\otimes R_y(\pi)\otimes R_y(0))|\varphi_6\rangle \end{pmatrix} = (|\varphi_1\rangle, |\varphi_4\rangle)
\end{aligned} \tag{19}
$$

When conducting GHZ-basis measurements on the two states in S_{final}, the measurement outcomes are $|\varphi_1\rangle$ and $|\varphi_4\rangle$. Since the measurement outcomes $|\varphi_1\rangle$ and $|\varphi_4\rangle$ are not consistent with the initially prepared GHZ states $|\varphi_1\rangle$ and $|\varphi_6\rangle$, TP can obtain the comparison result $X \neq Y$.

For the concrete example mentioned above, the quantum circuit of two GHZ states $|\varphi_1\rangle$ and $|\varphi_6\rangle$, and its measurement outcome when executing this quantum circuit on IBM Quantum Composer are shown in Figures 2 and 3, respectively. The quantum circuit

corresponding to the concrete example and the final measurement outcome can be seen in Figures 4 and 5, respectively.

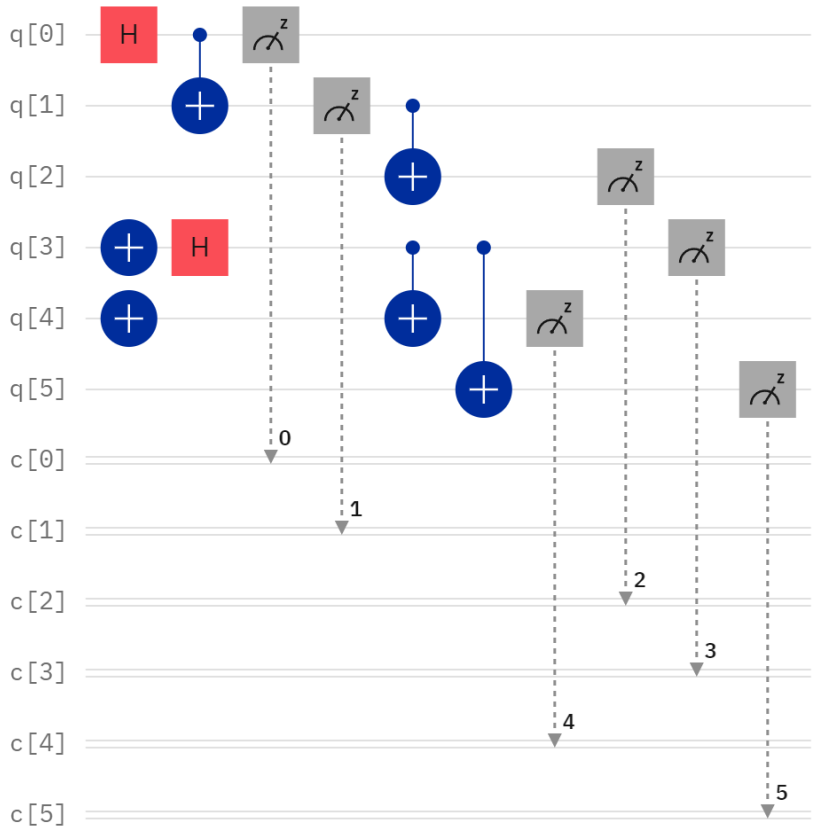

Figure 2. The quantum circuit of two GHZ states $|\varphi_1$ and $|\varphi_6\rangle$.

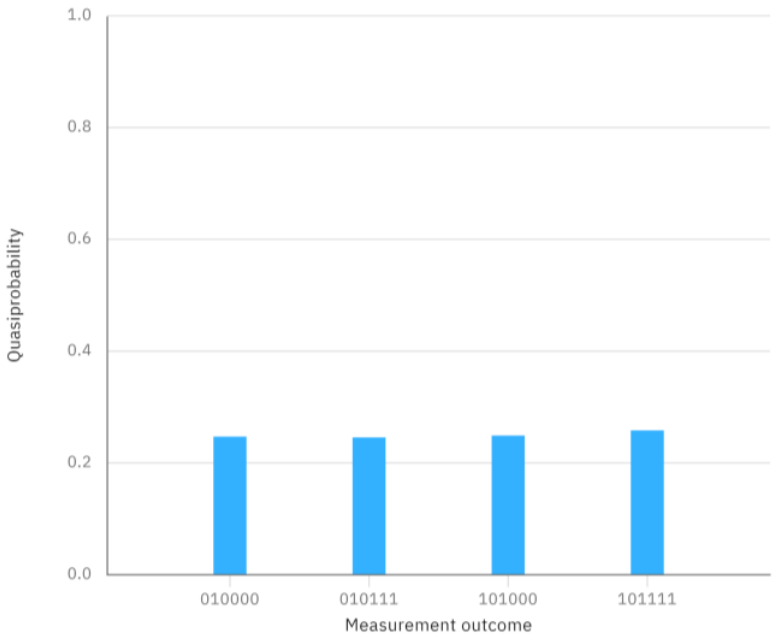

Figure 3. The measurement outcome in Figure 2.

Figure 4. The quantum circuit corresponding to the concrete example.

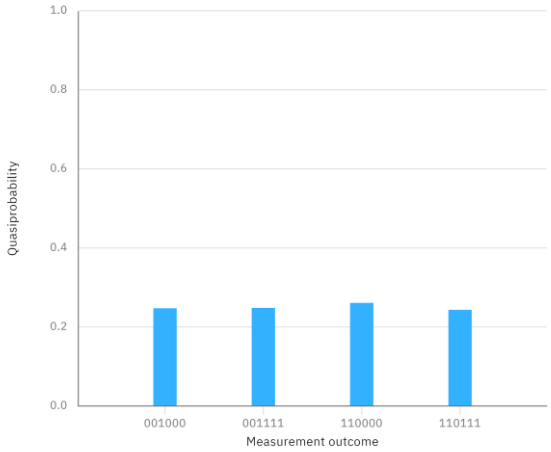

Figure 5. The measurement outcome in Figure 4.

From Figure 5, however, we can clearly observe that the measurement outcome when performing the quantum circuit of Figure 4 is different from the measurement outcome of the initially prepared two GHZ states in Figure 3. This discrepancy indicates that the measurement outcome is not consistent with the initially prepared GHZ states, suggesting that the comparison result is $X \neq Y$.

5. Security Analysis

In this section, we will consider both external and participant attacks and demonstrate that our protocol is resistant to these attacks.

5.1. External Attacks

We assume that the external attacker, Eve, may adopt quantum attack methods (e.g., the intercept–measurement–resend attack, the entanglement-measure attack, and the Trojan-horse attacks) to steal the secrets of Alice or Bob. We will demonstrate that these attacks are ineffective due to the decoy-state method utilized in our protocol.

5.1.1. The Intercept–Measurement–Resend Attack

The intercept–measurement–resend attack occurs when an external attacker, Eve, intercepts the quantum sequence in the quantum channel, measures the intercepted quantum sequence to steal secrets of Alice or Bob, and then resends a fake quantum sequence to the receiver in place of the intercepted one. However, the attack will inevitably introduce

errors due to eavesdropping detection between the quantum sequence sender and receiver. When the receiver receives the quantum sequence, she will measure the decoy states using the measurement basis announced by the sender and, then, send the measurement results back to the sender. Eve has no chance to know the specific state of the decoy states, resulting in inconsistencies between the intercepted decoy states and the measurement results. When Eve intercepts the sequence, there is a 50% probability of selecting the incorrect measurement basis, resulting in a correct and incorrect outcome of 50% each, respectively. For example, the sender prepares a decoy state with a quantum state $|1\rangle$. The probability of Eve choosing the correct measurement basis with Z-basis ($\{|0\rangle, |1\rangle\}$ basis) is 50%, and Eve will deceive the eavesdropping detection with a probability of 1. Simultaneously, the probability of Eve choosing the incorrect measurement basis with X-basis ($\{|+\rangle, |-\rangle\}$ basis) is also 50%, and the probability of Eve deceiving the eavesdropping detection is $1/2$. For n decoy states, the probability that Eve will deceive the eavesdropping detection is $(3/4)^n$. The relationship between the number of decoy photons and the probability of Eve deceiving the eavesdropping detection is shown in Figure 6. When the number of decoy photons, n, is large enough, the probability of Eve being discovered in the eavesdropping detection approaches 1 infinitely. Therefore, the intercept–measurement–resend attack launched by Eve is invalid for stealing the secrets of Alice or Bob.

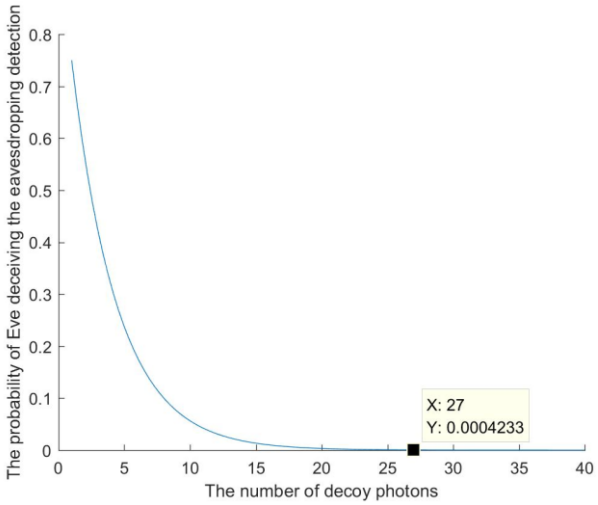

Figure 6. The relationship between the number of decoy photons and the probability that Eve will deceive the eavesdropping detection.

5.1.2. The Entanglement-Measure Attack

The entanglement-measure attack occurs when Eve intercepts the quantum particles during transmission and, then, utilizes unitary operations to entangle her auxiliary particles $|\varepsilon\rangle$ with the intercepted particles. She then measures the auxiliary particles to obtain private information about Alice or Bob.

When using the unitary operation U to entangle the intercepted particle with quantum states $|0\rangle$ and $|1\rangle$, this process can be expressed as

$$U|0,\varepsilon\rangle_{TE} = \alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle \tag{20}$$

$$U|1,\varepsilon\rangle_{TE} = \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle \tag{21}$$

where the subscript T and E denote the intercepted particle and the auxiliary particle, respectively. Four states $|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle$, *and* $|\varepsilon_{11}\rangle$ are pure states determined by the unitary operation U. The parameters $\alpha, \beta, \gamma, \delta$ should meet the specified conditions: $\alpha^2 + \beta^2 = 1, \gamma^2 + \delta^2 = 1$.

When using the unitary operation U to entangle the intercepted particles with quantum state $|+\rangle$ and $|-\rangle$, this process can be expressed as

$$\begin{array}{l} U|+,\varepsilon\rangle_{TE} = \frac{1}{\sqrt{2}}(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle|1\rangle + \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle) \\ = \frac{1}{2}\begin{pmatrix} |+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle + \gamma|\varepsilon_{10}\rangle + \delta|e_{11}\rangle) \\ +|-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle + \gamma|\varepsilon_{10}\rangle - \delta|e_{11}\rangle) \end{pmatrix} \end{array} \tag{22}$$

$$\begin{array}{l} U|-,\varepsilon\rangle_{TE} = \frac{1}{\sqrt{2}}(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle|1\rangle - \gamma|0\rangle|\varepsilon_{10}\rangle - \delta|1\rangle|\varepsilon_{11}\rangle) \\ = \frac{1}{2}\begin{pmatrix} |+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle - \gamma|\varepsilon_{10}\rangle - \delta|e_{11}\rangle) \\ +|-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle - \gamma|\varepsilon_{10}\rangle + \delta|e_{11}\rangle) \end{pmatrix} \end{array} \tag{23}$$

In our protocol, the eavesdropping detection process occurs throughout the entire quantum sequence transmission. If the decoy state stays in $\{|0\rangle, |1\rangle\}$ basis and Eve tries to trick the eavesdropping detection, the parameters in Equations (20) and (21) should be set as $\beta = \gamma = 0$. If the decoy state stays in $\{|+\rangle, |-\rangle\}$ basis and Eve tries to trick the eavesdropping detection, $\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle + \gamma|\varepsilon_{10}\rangle - \delta|e_{11}\rangle$ and $\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle - \gamma|\varepsilon_{10}\rangle - \delta|e_{11}\rangle$ should be a zero vector. Thus, we can conclude that $\alpha|\varepsilon_{00}\rangle = \delta|e_{11}\rangle$. Finally, Equations (20)–(23) can be reformulated as

$$U|0,\varepsilon\rangle_{TE} = \alpha|0\rangle|\varepsilon_{00}\rangle \tag{24}$$

$$U|1,\varepsilon\rangle_{TE} = \delta|1\rangle|\varepsilon_{11}\rangle = \alpha|1\rangle|\varepsilon_{00}\rangle \tag{25}$$

$$\begin{array}{l} U|+,\varepsilon\rangle_{TE} = \frac{1}{2}|+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle + \gamma|\varepsilon_{10}\rangle + \delta|e_{11}\rangle) \\ = \frac{1}{2}|+\rangle(\alpha|\varepsilon_{00}\rangle + 0 + 0 + \delta|e_{11}\rangle) = \alpha|+\rangle|\varepsilon_{00}\rangle \end{array} \tag{26}$$

$$\begin{array}{l} U|-,\varepsilon\rangle_{TE} = \frac{1}{2}|-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle - \gamma|\varepsilon_{10}\rangle + \delta|e_{11}\rangle) \\ = \frac{1}{2}|-\rangle(\alpha|\varepsilon_{00}\rangle - 0 - 0 + \delta|e_{11}\rangle) = \alpha|-\rangle|\varepsilon_{00}\rangle \end{array} \tag{27}$$

According to Equations (24)–(27), it can be inferred that the tensor product of the intercepted particle and the auxiliary particle results in a product of two quantum states, indicating that the auxiliary particle is independent of the intercepted particle. Even if Eve measures the auxiliary particles, she cannot obtain any information about the intercepted particles.

Additionally, assuming that Eve entangles her auxiliary particles with the transmitted GHZ states, her behavior will not succeed since the transmitted GHZ states are encrypted by the rotation operations, which are unknown to her. Therefore, the rotation operations ensure the concealment of the transmitted quantum states from external attackers, and the decoy state method can be employed to safeguard the security of the quantum channel.

5.1.3. The Trojan-Horse Attacks

The Trojan-horse attacks [34], including the delay-photon Trojan-horse attack and the invisible photon eavesdropping Trojan-horse attack, mainly occur in two-way quantum communication. Since the quantum states in our protocol are transmitted in a circular mode, there may be potential security risks due to Trojan-horse attacks. However, these attacks can be detected using existing techniques. The Wavelength Quantum Filter (WQF) can be used to remove invisible photons using optical filters, and the Photons Number Splitter (PNS) can be used to separate legitimate photons from delayed photons. Once these attacks are detected, the protocol will be aborted and restarted.

5.2. Participant Attacks

The participants who have access to immediate results may deduce private information by launching more powerful attacks, which poses a security challenge for our protocol [35]. In the following, three cases of attacks will be analyzed in detail.

5.2.1. TP's Attack

In the proposed protocol, TP is assumed to be semi-honest, which means she cannot conspire with Alice and Bob but may attempt to steal the secrets of Alice and Bob. If TP wants to learn information about Alice or Bob's inputs, she can act as an external attacker and perform the corresponding attacks. However, her behavior will be detected during the eavesdropping detection process as discussed in Section 5.1. In this scenario, we are examining a special case where TP executes an intercept–resend attack on the sequence sent from Alice to Bob. TP intercepts the sequence S'_{Enc_A} and resends a fake sequence to Bob. When Alice announces the positions where decoy states were inserted, TP discards the decoy states in S'_{Enc_A} and obtains the sequence S_{Enc_A} containing Alice's encoding inputs. Although this attack will be detected, TP may perform rotation operations $R_y(-TP_j)$ on the j-th GHZ states in S_{Enc_A} to obtain a sequence $S_{A\to B}$ and, then, conduct GHZ-basis measurements on the j-th states in $S_{A\to B}$ to obtain the measurement outcomes. TP may deduce Alice's private inputs by comparing the measurement outcomes with the initially prepared GHZ states. Unfortunately, the sequence S_{Enc_A} is obtained by performing rotation operations $R_y(KA_j)$ on the j-th states in S_A, and the secret key Θ_{KA} will be disclosed by Alice under the condition that no external eavesdropper exists. TP has no chance to obtain Θ_{KA}, and she cannot obtain the sequence S_A, making it inaccessible to deduce the rotation operations $R_y(KA_j)$. TP's lack of knowledge about $R_y(KA_j)$ is equivalent to her inability to access Alice's private inputs. Additionally, TP can leverage the benefits of preparing the initial GHZ states to compute the comparison results and infer the inputs of Alice or Bob based on the final measurement outcomes. In this case, the inputs of Alice and Bob will not be disclosed since each measurement outcome only reveals the XOR value of three bits. Therefore, our protocol is secure against TP's attacks.

5.2.2. Alice's Attack

For Alice, she may send a fake sequence S_A to Bob, intercept the sequence S'_{Enc_B} sent from Bob to TP, and then, resend another fake sequence to TP. Once the secret key Θ_{KB} is announced by Bob, Alice can recover S_B by performing rotation operation $R_y(-KB_j)$ on the j-th states in S_{Enc_B}. However, this attack method is invalid in our protocol. Once Alice intercepts the sequence S_{Enc_B}, her behavior will inevitably be detected during the eavesdropping between Bob and TP. Once the eavesdropper intervenes in the transmission process, Bob will not disclose the secret key to TP. The protocol will be aborted and restarted. Therefore, Alice has no chance of learning Bob's inputs.

5.2.3. Bob's Attack

For Bob, he can measure the sequence S_B in the GHZ-basis and obtain the measurement outcomes. He may deduce which rotation operations have been performed by Alice by comparing the measurement outcomes with the initially prepared GHZ states and learn Alice's inputs. However, this method does not work. On the one hand, the initially prepared GHZ states are only known to TP who cannot conspire with any participants, resulting in Bob having no chance to know them. On the other hand, Bob may attempt to obtain the sequence $S_{initial}$ by performing an intercept–resend attack on the sequence $S'_{initial}$ and infer the initially prepared GHZ states. Although his behavior will be detected, and he can obtain $S_{initial}$, he still has no chance to learn the initially prepared GHZ states. This is because the sequence $S_{initial}$ is obtained by performing rotation operations $R_y(TP_j)$ on the j-th GHZ states, and no one can know the initially prepared GHZ states without knowing the secret key Θ_{TP}. Without knowledge of the initially prepared GHZ states, Bob is unable to acquire information about Alice's inputs.

6. Efficiency Analysis and Comparison

6.1. Efficiency Analysis

The qubit efficiency [36], as a measure of the utilization rate of quantum states, can be defined as

$$\eta_e = \frac{\eta_c}{\eta_t} \tag{28}$$

where η_e denotes the qubit efficiency of the QPC protocol, η_c represents the number of compared classical bits, and η_t denotes the total consumed qubits excluding the decoy photons used. In our protocol, one GHZ state can be compared to three bits of classical information in each comparison, and we can obtain $\eta_c = \eta_t$. Therefore, the qubit efficiency of our protocol is 100%.

6.2. Comparison

We compare our protocol with QPC protocols proposed in Refs. [9,16,18,22,26] in Table 2. The comparison between our protocol and other QPC protocols based on GHZ state is shown in Table 3.

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

	Ref. [9]	**Ref. [16]**	**Ref. [18]**	**Ref. [22]**	**Ref. [26]**	**Ours**
Quantum resource	Single photons	Bell states	Eight-qubit entangled state	Four-qubit cluster state and extended Bell state	Five-particle cluster state	GHZ states
Unitary operation	No	No	No	No	Yes	Yes
Entanglement swapping	No	Yes	No	Yes	No	No
QKD method	Yes	Yes	Yes	Yes	No	No
Quantum measurement	Single-particle	GHZ-basis	single-particle	Bell-basis and extend Bell basis	single-particle	GHZ-basis
Qubit efficiency	33%	50%	25%	50%	40%	100%

Table 3. The comparison between our protocol and other QPC protocols based on GHZ state.

	Ref. [37]	**Ref. [38]**	**Ref. [39]**	**Ref. [40]**	**Ours**
Quantum resource	Hyperentangled GHZ state	4D GHZ-like states	GHZ state	four-particle GHZ state	GHZ states
Unitary operation	No	No	No	Yes	Yes
Entanglement swapping	Yes	No	Yes	No	No
QKD method	Yes	Yes	No	Yes	No
Quantum measurement	Bell-basis	single-particle	Bell-basis	Bell-basis and single-particle	GHZ-basis
Qubit efficiency	66%	33%	33%	75%	100%

Compared with QPC protocols in Refs. [9,16,18,22,26,37–40], our protocol has the following advantages. First, our protocol does not require QKD protocol for sharing a secret key to ensure the security of the inputs. This results in no consumption of quantum resources for key sharing, unlike QKD-based QPC protocols [8,16,18,22,37,38,40]. Secondly, the quantum sequence is transmitted between the TP and the two users in a circular mode. The inputs of the two users are encoded into the transmitted quantum sequence, leading to the multiplexing of quantum resources and improving the utilization of these resources.

Third, our protocol reaches the maximum theoretical efficiency of 100%, because one GHZ state can be compared to three bits of classical information in each comparison. To sum up, our protocol requires no quantum resources for sharing a secret key, and it has shown improved performance in qubit efficiency and the utilization of quantum resources.

7. Conclusions

In this article, we propose an efficient QPC protocol based on GHZ states. With the assistance of a semi-honest TP, two users can compare their secrets by utilizing the properties of GHZ states and rotation operations. Compared with other QPC protocols, one of the advantages of our protocol is that it utilizes secret keys distributed through classical channels instead of QKD protocols to share a secret key, which results in no consumption of quantum resources for key sharing. The quantum sequence is transmitted between the TP and two users in a circular mode. The inputs of the two users are encoded into the transmitted quantum sequence, leading to the multiplexing of quantum resources and improving the utilization of quantum resources. More importantly, our protocol achieves a qubit efficiency of 100%, which is the theoretical maximum.

Author Contributions: Conceptualization, M.H. and S.Z.; methodology, M.H. and S.Z.; writing—original draft preparation, 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, 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 Gongga Plan for the "Double World-class Project".

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

References

1. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
2. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]
3. 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]
4. 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]
5. 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.
6. Tseng, H.Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **2012**, *11*, 373–384. [CrossRef]
7. 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. [CrossRef]
8. Huang, W.; Wen, Q.Y.; Liu, B.; Gao, F.; Sun, Y. Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. *Sci. China Phys. Mech. Astron.* **2013**, *56*, 1670–1678. [CrossRef]
9. 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]
10. 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]
11. 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]
12. Ye, T.Y.; Ji, Z.X. Two-party quantum private comparison with five-qubit entangled states. *Int. J. Theor. Phys.* **2017**, *56*, 1517–1529. [CrossRef]
13. Li, J.; Wang, Z.; Yang, J.; Ye, C.; Che, F. A Semi-Quantum Private Comparison Base on W-States. *Entropy* **2023**, *25*, 1269. [CrossRef]

14. 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]
15. 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]
16. 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]
17. Wu, W.; Wu, J.; Guo, L. Multi-Party Quantum Private Comparison Based on Bell States. *Entropy* **2023**, *25*, 1156. [CrossRef] [PubMed]
18. 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]
19. Hong-Ming, P. Quantum private comparison based on χ-type entangled states. *Int. J. Theor. Phys.* **2017**, *56*, 3340–3347. [CrossRef]
20. 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]
21. Li, J.; Che, F.; Wang, Z.; Fu, A. Efficient Quantum Private Comparison without Sharing a Key. *Entropy* **2023**, *25*, 1552. [CrossRef] [PubMed]
22. 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]
23. Sun, Z.; Long, D. Quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2013**, *52*, 212–218. [CrossRef]
24. Zhou, M.K. Improvements of quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2018**, *57*, 42–47. [CrossRef]
25. 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]
26. 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]
27. Ye, T.Y. Quantum private comparison via cavity QED. *Commun. Theor. Phys.* **2017**, *67*, 147. [CrossRef]
28. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
29. Zhang, J.W.; Xu, G.; Chen, X.B.; Chang, Y.; Dong, Z.-C. Improved multiparty quantum private comparison based on quantum homomorphic encryption. *Phys. A Stat. Mech. Its Appl.* **2023**, *610*, 128397. [CrossRef]
30. 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]
31. Wang, N.; Zhang, X.; Zhang, X.; Lin, S. (t, n) Threshold Quantum Secret Sharing Using Rotation Operation. *Int. J. Theor. Phys.* **2022**, *61*, 166. [CrossRef]
32. Kang, M.S.; Hong, C.H.; Heo, J.; Lim, J.-I.; Yang, H.-J. Quantum signature scheme using a single qubit rotation operator. *Int. J. Theor. Phys.* **2015**, *54*, 614–629. [CrossRef]
33. Sun, Z.; Huang, J.; Wang, P. Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process.* **2016**, *15*, 2101–2111. [CrossRef]
34. Jain, N.; Anisimova, E.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030. [CrossRef]
35. Huang, X.; Zhang, W.; Zhang, S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. *Phys. A Stat. Mech. Appl.* **2024**, *637*, 129614. [CrossRef]
36. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef] [PubMed]
37. Gianni, J.; Qu, Z. New quantum private comparison using hyperentangled ghz state. *J. Quantum Comput.* **2021**, *3*, 45. [CrossRef]
38. 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]
39. Liu, W.; Wang, Y.B. Quantum private comparison based on GHZ entangled states. *Int. J. Theor. Phys.* **2012**, *51*, 3596–3604. [CrossRef]
40. Xu, Q.D.; Chen, H.Y.; Gong, L.H.; Zhou, N.R. Quantum private comparison protocol based on four-particle GHZ states. *Int. J. Theor. Phys.* **2020**, *59*, 1798–1806. [CrossRef]