entropy

MDPI

Article

Efficient Quantum Private Comparison without Sharing a Key

Jian Li [1,2], Fanting Che [3,*], Zhuo Wang [3] and Anqi Fu [2]

[1] School of Information Engineering, Ningxia University, Yinchuan 750021, China; lijian@bupt.edu.cn
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China; sirius1120@126.com
[3] School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China; zhuowang@bupt.edu.cn
* Correspondence: chefanting@bupt.edu.cn

Abstract: Quantum private comparison (QPC) allows at least two users to compare the equality of their secret information, for which the security is based on the properties of quantum mechanics. To improve the use of quantum resources and the efficiency of private comparison, a new QPC protocol based on GHZ-like states is proposed. The protocol adopts unitary operations to encode the secret information instead of performing quantum key distribution (QKD), which can reduce the amount of computation required to perform QKD and improve the utilization of quantum resources. The decoy photon technique used to detect channel eavesdropping ensures that the protocol is resistant to external attacks. The quantum efficiency of the protocol reaches 66%. Compared with many previous QPC schemes, the proposed protocol does not need to share a key and has advantages in quantum efficiency and quantum resources.

Keywords: quantum private comparison; GHZ-like states; unitary operation; decoy photon

check for updates

Citation: Li, J.; Che, F.; Wang, Z.; Fu, A. Efficient Quantum Private Comparison without Sharing a Key. *Entropy* **2023**, *25*, 1552. https://doi.org/10.3390/e25111552

Academic Editors: Osamu Hirota, Hua-Lei Yin, Kaizhi Huang and Guan-Jie Fan-Yuan

Received: 13 October 2023
Revised: 13 November 2023
Accepted: 14 November 2023
Published: 17 November 2023

1. Introduction

In the traditional field of information security, encryption technology has been the key to protecting sensitive information. However, with the rapid development of computing power, especially the development of quantum computing, securing traditional encryption methods has been substantially challenging. In this context, research on quantum cryptography, including quantum key distribution (QKD), quantum digital signature [1], quantum communication [2], and quantum private comparison (QPC), has become a research hotspot.

QKD technology primarily relies on the fundamental principles of quantum mechanics to ensure that users generate secure and dependable keys during the communication progress [3,4]. Moreover, the goal of quantum private comparison is to enable both parties to compare their secret data without revealing any information about the data to each other or any potential eavesdropper [5–7]. QPC has potential applications in a variety of fields, including secure online voting, financial transactions, and data sharing between government agencies. However, the majority of QPC protocols have a common feature that the protocols need to perform QKD [8] and then encrypt and compare secret information. Using QKD to avoid possible security risks can make the protocol simpler and easier at the physical implementation level; nevertheless, this type of QPC protocol has room for improvement in quantum efficiency and utilization of quantum resources [9].

For a QPC protocol, the privacy security issue is an unavoidable research focus. A qualified QPC protocol should meet the following two conditions: (1) the security of the private information and (2) the fairness of the comparison results. Both parties need to know the final result of the comparison and ensure that the result is the same as that of the actual calculation. Therefore, it is imperative to process or encrypt the secret information, guaranteeing that the parties involved in the comparison do not have direct access to each

other's secret data and eliminating the possibility of inferring secret information from measurement results. Furthermore, the involvement of a third party in the protocol can facilitate secure and equitable private comparison by assisting the two parties in comparing their secret data and publicly publishing the comparison result. However, the integrity and trustworthiness of the third party are crucial considerations. Ensuring the credibility of the third party and the smooth progress of the protocol necessitates the implementation of necessary measures to safeguard and regulate the behavior of the third party.

Based on the above analysis, we propose a new quantum privacy comparison protocol without a shared key. With the assistance of a semi-honest third party, this protocol ensures fairness in comparing users' secret information without the necessity for key sharing or direct user-to-user communication. This results in heightened privacy protection capabilities. Furthermore, the protocol incorporates decoy photon technology and hash functions to defend against internal and external attacks, effectively securing the performance of this protocol. Notably, this protocol boasts a higher quantum efficiency compared to the majority of previous QPC protocols.

The structure of this paper is as follows: the related work and the knowledge preparation are introduced in Section 2. The steps and description of the protocol are presented in Section 3. An example of the correctness of the protocol is shown in Section 4. The security analysis is explained in detail in Section 5. The quantum efficiency is analyzed in Section 6. Finally, a summary of this work is provided.

2. Preliminaries

2.1. Related Work

The earliest QPC protocol was inspired by quantum secret sharing protocols, and the privacy comparison problem originating from Yao's millionaires problem. In this problem, two millionaires sought to ascertain their relative wealth without revealing specific assets. The first QPC protocol was introduced by Yang and Wen in 2009 [10]. This protocol harnessed the entanglement exchange properties of EPR states and employed unitary operations to facilitate the comparison of private information. Additionally, the involvement of a third-party participant effectively ensured the security and fairness of the protocol. In current research, QPC protocols aim to compare the equality or the relative sizes of private information. The research predominantly focuses on using different quantum states and various encoding methods (whether to distribute keys) to implement comparison protocols.

In 2020, Lang [11] introduced a QPC protocol that leveraged quantum gates, simplifying the process by eliminating the classical computation in a QPC protocol. In the same year, Wu et al. [12] proposed a protocol that does not require the involvement of a third party, and Ji et al. [13] designed several QPC protocols with various quantum states, using dense coding instead of key distribution methods. In 2021, Huang et al. [14] introduced a semi-honest third party to assist in comparison. Lang [15] also proposed a QPC protocol using a single Bell state rather than multiple Bell states as the quantum resource. Chen et al. designed a QPC protocol that does not require the use of quantum entangled states as quantum resources [16]. In 2022, Fan et al. [17] utilized an eight-qubit entangled state for private data comparison through quantum key distribution and joint computation. In 2023, Liu [18] employed high-dimensional GHZ-like states as quantum resources, and Zhang et al. [19] introduced a QPC protocol based on homomorphic encryption, allowing multiple participants to engage in simultaneous comparisons.

2.2. Theoretical Basis of GHZ-like States

GHZ-like states are a class of quantum states that have certain similarities to GHZ states, such as multi-partite entanglement, where the entanglement between these qubits of GHZ-like states is multipartite rather than just bipartite. Moreover, the GHZ-like state is not limited to specific forms of GHZ states.

The three-particle GHZ-like states used in the proposed QPC protocol are transformed from ordinary GHZ states. An n-particle GHZ state is a kind of quantum entanglement, which can be described as

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|q_1, q_2, \cdots, q_n\rangle + (-1)^{\Delta}|\overline{q_1, q_2, \cdots, q_n}\right) \tag{1}$$

where $q_1 = 0, q_2, q_3, \cdots, q_n \in \{0,1\}$ and $\Delta \in \{0,1\}$.

According to Equation (1), an n-particle GHZ-like state [20] transformed from the GHZ state can be written as

$$|GHZ\rangle' = \frac{1}{\sqrt{2^{n-1}}}\sum_{k=1}^{2^{n-1}}\left[(-1)^{\delta}|z_1, z_2, \cdots, z_n\rangle\right]_{num(1)} \tag{2}$$

where $\delta = (\sum_{j|z_j=1} q_j)(mod2)$, $z_j \in \{0,1\}$, and $num(1) = \begin{cases}\text{even, if } \Delta = 0\\ \text{odd, if } \Delta = 1\end{cases}$. When the parameter $num(1)$ is an even value, the number of 1 in each vector $|z_1, z_2, \cdots, z_n\rangle$ is even. When the parameter $num(1)$ is an odd value, the number of 1 in each vector $|z_1, z_2, \cdots, z_n\rangle$ is odd.

According to Equation (1), an n-particle GHZ state can exit 2^n different states. It should be noted that the state is a Bell state when n takes the value of 2. The Bell state is the simplest quantum entangled state of a two-qubit system, consisting of four specific maximum entangled quantum states, which can be expressed as Equations (3) and (4). For a three-particle GHZ state, there are eight possible states and eight corresponding GHZ-like states. The one used in the proposed protocol is $|GHZ\rangle_1$, in which the Δ has a value of 0 and $q_2 = q_3 = 0$. $|GHZ\rangle_1$ is a GHZ state, which is shown as Equation (5).

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle], \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle] \tag{3}$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle], |\Psi^- = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle] \tag{4}$$

$$|GHZ\rangle_1 = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{5}$$

According to Equations (1) and (2), the GHZ-like state ${|GHZ\rangle_1}'$ used in the proposed protocol can be described as

$$\begin{aligned}{|GHZ\rangle_1}' = \tfrac{1}{\sqrt{2^2}} & \sum_{k=1}^{2^2}\left[(-1)^{\delta}|z_1, z_2, \cdots, z_n\rangle\right]_{even}\\ & = \tfrac{1}{2}\left[(-1)^0|000\rangle + (-1)^{0\oplus 0}|011\rangle + (-1)^{0\oplus 0}|101\rangle + (-1)^{0\oplus 0}|110\rangle\right]\\ & = \tfrac{1}{2}[|000\rangle + |011\rangle + |101\rangle + |110\rangle]\end{aligned} \tag{6}$$

The ${|GHZ\rangle_1}'$ also can be written as

$${|GHZ\rangle_1}' = \frac{1}{2}[|0\rangle(|00\rangle + |11\rangle) + |1\rangle(|01\rangle + |10\rangle)] = \frac{1}{\sqrt{2}}\left[|0\rangle\left|\Phi^+\right\rangle + |1\rangle\left|\Psi^+\right\rangle\right] \tag{7}$$

According to Equation (7), when the state of the first particle of ${|GHZ\rangle_1}'$ is $|0\rangle$, the state of the other two particles of ${|GHZ\rangle_1}'$ corresponds to the Bell state $\left|\Phi^+\right\rangle$. When the state of the first particle of ${|GHZ\rangle_1}'$ is $|1\rangle$, the state of the rest particles of ${|GHZ\rangle_1}'$ corresponds to the Bell state $\left|\Psi^+\right\rangle$. These properties of ${|GHZ\rangle_1}'$ are used in our proposed protocol.

2.3. Unitary Operations

The unitary operations used in the proposed protocol are Pauli gates. Pauli gates (X, Y, Z) are three quantum gates, which operate on a single qubit. The Pauli-X gate flips the state of a qubit from $|0\rangle$ to $|1\rangle$ and vice versa. The Pauli-Y gate changes the state of a qubit from $|0\rangle$ to $-|1\rangle$ and $|1\rangle$ to $|0\rangle$. The Pauli-Z gate changes the state of a qubit from $|1\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$. Shown in Table 1, the outcomes of the state of a qubit, which passes through a Pauli gate or Identity gate, are listed.

Table 1. The operation outcome of the Pauli gates and Identity gate.

Qubit	X Gate	Y Gate	Z Gate	I Gate
$\|0\rangle$	$\|1\rangle$	$-\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$-\|1\rangle$	$\|1\rangle$

3. QPC Protocol Description

The protocol participants are introduced as follows:

TP: TP is a semi-honesty third party that can help compare the equality of the secret information. TP needs to honestly execute the steps specified in the protocol but allows it to attempt to obtain secret information through some illegal means.

Alice (Bob): Alice (Bob) is a quantum user with complete quantum capabilities who can achieve the preparation and complete measurement of quantum states.

Assume the length of the secret information that Alice and Bob need to compare is L. The secret information of Alice can be expressed as $X = \{x_1, x_2, \cdots, x_L\}$, and the secret information of Bob can be expressed as $Y = \{y_1, y_2, \cdots, y_L\}$, where x_i and y_i consist of the classical bits 0 and 1, and i represents the i-th particle of the particle sequence X or Y. Moreover, the protocol is described in detail as follows (also shown in Figure 1).

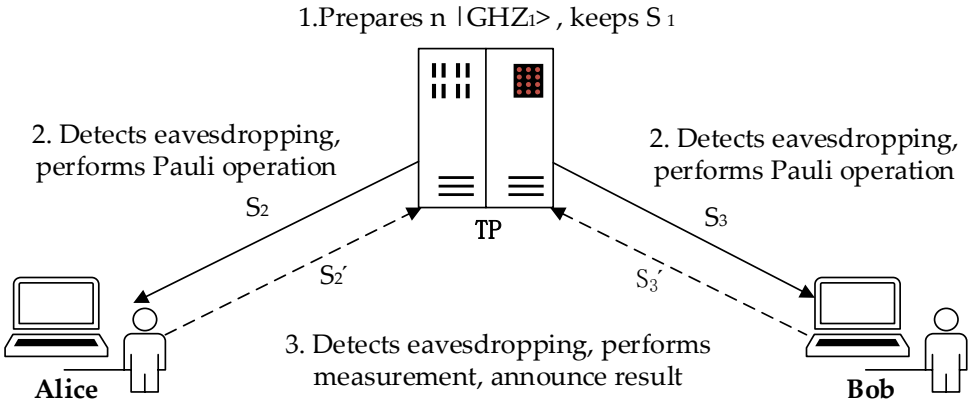

Figure 1. The model of the proposed protocol.

Step 1: TP prepares n $|GHZ\rangle_1{}'$ states and divides them into three sequences S_1, S_2, and S_3, where S_i includes all of the i-th particles of each state.

Step 2: TP generates $2m$ decoy photons. Each photon is prepared randomly from four states of single particles $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. Thereafter, TP chooses m decoy photons and randomly inserts them into S_2 and then randomly inserts the remaining m decoy photons into S_3. The position of insertion is random. After completing the insertion, the total number of particles of the particle string is $n + m$. TP records the location and state of these decoy photons. The value of m can be an arbitrary number, but it should be large enough to improve the performance of eavesdropping detection.

Step 3: TP keeps the sequence S_1 for his/her own and sends S_2 and S_3 to Alice and Bob, respectively.

Step 4: Upon receiving the sequences sent by TP, both Alice and Bob immediately conduct eavesdropping detection. Meanwhile, TP announces the location and basis of each

decoy photon. Then, Alice and Bob perform the corresponding measurement on these decoy photons, send the measurement results to TP, and discard the decoy photons in S_2 and S_3. Thereafter, TP determines whether the eavesdropper is on the transmission channel based on the received measurement results. If the error ratio of the measurement results exceeds a predefined threshold, it indicates the presence of eavesdroppers on the communication channel and the protocol needs to be terminated immediately.

Step 5: Alice and Bob perform a shared hash function H on their binary secret information to obtain a binary sequence of the specified length. The hash function H is described as Equation (8).

$$H : (0,\ 1)^L \rightarrow (0,\ 1)^K \tag{8}$$

where L denotes the initial length of the binary sequence and K denotes the length of the binary sequence after performing the shared hash function H.

$$H : X = \{x_1, x_2, \cdots, x_L\} \rightarrow X' = \{x_1, x_2, \cdots, x_K\} \tag{9}$$

$$H : Y = \{y_1, y_2, \cdots, y_L\} \rightarrow X' = \{y_1, y_2, \cdots, y_K\} \tag{10}$$

where K gets the value of $2n$ in the protocol.

Thereafter, Alice and Bob divide X' and Y' into $2n$ groups, respectively.

$$X' = \left\{\left(x_1{}', x_2{}'\right), \left(x_3{}', x_4{}'\right), \cdots, \left(x_{2n-1}{}', x_{2n}{}'\right)\right\} = \left\{m_1{}^A, m_2{}^A, \cdots, m_n{}^A\right\} \tag{11}$$

$$Y' = \left\{\left(y_1{}', y_2{}'\right), \left(y_3{}', y_4{}'\right), \cdots, \left(y_{2n-1}{}', y_{2n}{}'\right)\right\} = \left\{m_1{}^A, m_2{}^A, \cdots, m_n{}^A\right\} \tag{12}$$

where $m_i \in \{00,\ 01,\ 10,\ 11\}$.

Step 6: Alice and Bob perform a corresponding operation, which is shown in Table 2, on each particle in S_2 and S_3. After all the particles have been manipulated, Alice and Bob prepare m decoy photons each, insert them into S_2' and S_3' composed of the operation results, and send the sequences S_2' and S_3' back to TP.

Step 7: After receiving S_2' and S_3', TP carries out eavesdropping detection immediately to ensure that there is no eavesdropping. TP discards the decoy photons after eavesdropping detection.

Step 8: TP combines both sequences to form the $Q_i = \left(q_2^i, q_3^i\right)$, in which the q_2^i is the i-th particle of S_2' and the q_3^i is the i-th particle of S_3'. Then, TP measures the pairs Q_i with Bell basis and measures each particle of the sequence S_1 with $|0,1\rangle$ basis.

Step 9: TP judges the equality of the secret information of Alice and Bob based on the measurement results in Step 8. If the measurement results of Bell basis and $|0,1\rangle$ basis are $|\Phi^+\rangle$ and $|0\rangle$ or $|\Psi^+\rangle$ and $|1\rangle$, the secret information being compared is equal. Otherwise, if the measurement result occurs in another situation, the secret information being compared is different. The equal results are shown in Table 3, and the summary of all measurement results is shown in Table 4.

Table 2. Summary table of m_i and their corresponding unitary operations.

m_i	00	01	10	11
Unitary operation	I	X	Y	Z

Table 3. Summary table of equal results.

Measurement Method	Result 1	Result 2
$\|0,1\rangle$ basis	$\|0\rangle$	$\|1\rangle$
Bell basis	$\left\|\Phi^+\right\rangle$	$\left\|\Psi^+\right\rangle$

Table 4. Summary table of all measurement results.

Alice	Bob	$\|GHZ\rangle_1{}'_{①}$	Result	$\|GHZ\rangle_1{}'_{②}$
I	I	$(\|000\rangle + \|011\rangle + \|101\rangle + \|110\rangle)/2$	*Yes*	$(\|0\rangle\|\Phi^+\rangle + \|1\rangle\|\Psi^+\rangle)/\sqrt{2}$
I	X	$(\|001\rangle + \|010\rangle + \|100\rangle + \|111\rangle)/2$	*No*	$(\|0\rangle\|\Psi^+\rangle + \|1\rangle\|\Phi^+\rangle)/\sqrt{2}$
I	Y	$(-\|001\rangle + \|010\rangle + \|100\rangle - \|111\rangle)/2$	*No*	$(\|0\rangle\|\Psi^-\rangle + \|1\rangle\|\Phi^-\rangle)/\sqrt{2}$
I	Z	$(\|000\rangle - \|011\rangle - \|101\rangle + \|110\rangle)/2$	*No*	$(\|0\rangle\|\Phi^-\rangle + \|1\rangle\|\Psi^-\rangle)/\sqrt{2}$
X	I	$(\|010\rangle + \|001\rangle + \|111\rangle + \|100\rangle)/2$	*No*	$(\|0\rangle\|\Psi^+\rangle + \|1\rangle\|\Phi^+\rangle)/\sqrt{2}$
X	X	$(\|011\rangle + \|000\rangle + \|110\rangle + \|101\rangle)/2$	*Yes*	$(\|0\rangle\|\Phi^+\rangle + \|1\rangle\|\Psi^+\rangle)/\sqrt{2}$
X	Y	$(-\|011\rangle + \|000\rangle + \|110\rangle - \|101\rangle)/2$	*No*	$(\|0\rangle\|\Phi^-\rangle + \|1\rangle\|\Psi^-\rangle)/\sqrt{2}$
X	Z	$(\|010\rangle - \|001\rangle - \|111\rangle + \|100\rangle)/2$	*No*	$(\|0\rangle\|\Psi^-\rangle + \|1\rangle\|\Phi^-\rangle)/\sqrt{2}$
Y	I	$(-\|010\rangle + \|001\rangle - \|111\rangle + \|100\rangle)/2$	*No*	$(\|0\rangle\|\Psi^-\rangle + \|1\rangle\|\Phi^-\rangle)/\sqrt{2}$
Y	X	$(-\|011\rangle + \|000\rangle - \|110\rangle + \|101\rangle)/2$	*No*	$(\|0\rangle\|\Phi^-\rangle + \|1\rangle\|\Psi^-\rangle)/\sqrt{2}$
Y	Y	$(\|011\rangle + \|000\rangle - \|110\rangle - \|101\rangle)/2$	*Yes*	$(\|0\rangle\|\Phi^+\rangle + \|1\rangle\|\Psi^+\rangle)/\sqrt{2}$
Y	Z	$(-\|010\rangle - \|001\rangle + \|111\rangle + \|100\rangle)/2$	*No*	$(\|0\rangle\|\Psi^+\rangle + \|1\rangle\|\Phi^+\rangle)/\sqrt{2}$
Z	I	$(\|000\rangle - \|011\rangle + \|101\rangle - \|110\rangle)/2$	*No*	$(\|0\rangle\|\Phi^-\rangle + \|1\rangle\|\Psi^-\rangle)/\sqrt{2}$
Z	X	$(\|001\rangle - \|010\rangle + \|100\rangle - \|111\rangle)/2$	*No*	$(\|0\rangle\|\Phi^-\rangle + \|1\rangle\|\Psi^-\rangle)/\sqrt{2}$
Z	Y	$(-\|001\rangle - \|010\rangle + \|100\rangle + \|111\rangle)/2$	*No*	$(\|0\rangle\|\Psi^+\rangle + \|1\rangle\|\Phi^+\rangle)/\sqrt{2}$
Z	Z	$(\|000\rangle + \|011\rangle - \|101\rangle - \|110\rangle)/2$	*Yes*	$(\|0\rangle\|\Phi^+\rangle + \|1\rangle\|\Psi^+\rangle)/\sqrt{2}$

where $|GHZ\rangle_1{}'_{①}$ and $|GHZ\rangle_1{}'_{②}$ denote the two expressions of $|GHZ\rangle_1{}'$ performed unitary operations.

4. Correctness

Suppose the quantum users Alice and Bob want to compare the secret information $X = Y = 101100011001$, which would turn into X' and Y' after performing the shared hash function H (Shown as Equation (8)). The purpose of performing the hash operation is to convert the comparative secret information to a specific length and to perform the first encryption processing. For convenience of presentation, we assume that $X' = Y' = 10110001$.

TP prepares four three-particle GHZ-like states and divides them into three sequences $S_1 = s_1^1, s_1^2, s_1^3, s_1^4$, $S_2 = s_2^1, s_2^2, s_2^3, s_2^4$ and $S_3 = s_3^1, s_3^2, s_3^3, s_3^4$. Then, TP inserts decoy photons into S_2 and S_3. Thereafter, TP sends S_2 and S_3 to Alice and Bob, respectively. After receiving the sequences, Alice and Bob perform eavesdropping detection immediately and carry out the operations $\{Y, Z, I, X\}$ based on the result of secret information performed by the hash function H. Then, Alice and Bob prepare decoy photons each and send S_2' and S_3' back to TP.

TP performs eavesdropping detection and carries out the Bell basis and $|0, 1\rangle$ basis measurement. The measurement results are $|\Phi^+\rangle$ and $|0\rangle$, $|\Psi^+\rangle$ and $|1\rangle$. The result means that the secret information being compared is equal. The comparison process is shown in Table 5, and an example of unequal secret information is shown in Table 6. The decoy photons are not displayed in the comparison process shown in Tables 5 and 6. The decoy photons are randomly located in the quantum sentences and discarded after eavesdropping detection.

Table 5. The comparison process of equal secret information.

	Alice	Bob	TP
Secret information	$X = 101100011001$	$Y = 101100011001$	
After hash function H	$X' = 10110001$	$Y' = 10110001$	
Unitary operations	$\{Y, Z, I, X\}$	$\{Y, Z, I, X\}$	
S_2 and S_3	$S_2 = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$	$S_3 = \{\|0\rangle, \|1\rangle, \|1\rangle, \|0\rangle\}$	$S_1 = \{\|0\rangle, \|0\rangle, \|1\rangle, \|1\rangle\}$
S_2' and S_3'	$S_2' = \{-\|1\rangle, -\|1\rangle, \|0\rangle, \|0\rangle\}$	$S_3' = \{-\|1\rangle, -\|1\rangle, \|1\rangle, \|1\rangle\}$	
Combined pairs	$\{Q_1, Q_2, Q_3, Q_4\} = \{\|11\rangle, \|11\rangle, \|01\rangle, \|01\rangle\}$		
Measurement results	$\{\|\Phi^+\rangle, \|\Phi^+\rangle, \|\Psi^+\rangle, \|\Psi^+\rangle\}$		$\{\|0\rangle, \|0\rangle, \|1\rangle, \|1\rangle$
Equality of secret	Yes		

Table 6. The comparison process of unequal secret information.

	Alice	**Bob**	**TP**
Secret information	$X = 101100011011$	$Y = 101100011001$	
After hash function H	$X' = 10110011$	$Y' = 10110001$	
Unitary operations	$\{Y, Z, I, Z\}$	$\{Y, Z, I, X\}$	
S_2 and S_3	$S_2 = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$	$S_3 = \{\|0\rangle, \|1\rangle, \|1\rangle, \|0\rangle\}$	$S_1 = \{\|0\rangle, \|0\rangle, \|1\rangle, \|1\rangle\}$
S_2' and S_3'	$S_2' = \{-\|1\rangle, -\|1\rangle, \|0\rangle, -\|1\rangle\}$	$S_3' = \{-\|1\rangle, -\|1\rangle, \|1\rangle, \|1\rangle\}$	
Combined pairs	$\{Q_1, Q_2, Q_3, Q_4\} = \{\|11\rangle, \|11\rangle, \|01\rangle, -\|11\rangle\}$		
Measurement results	$\{\|\Phi^+\rangle\|, , \Phi^+\rangle, \|\Psi^+\rangle, \|\Phi^-\rangle\}$		$\{\|0\rangle, \|0\rangle, \|1\rangle, \|1\rangle$
Equality of secret	No		

5. Security Analyses

5.1. External Attacks

Assume the external attacker is Eve. The attack methods that Eve can use to steal the secret information of Alice or Bob or both Alice and Bob are intercept-resend attack, measure-resend attack, and entanglement attack. The following is a detailed analysis of these three attacks.

5.1.1. Intercept-Resend Attack

The external attacker Eve may carry out an intercept-resend attack by first intercepting the particle sequences sent by TP to Alice and Bob and storing them. Then, Eve prepares the same and specified amount of single particles and sends them to Alice and Bob. After Alice and Bob perform their operations, Eve again intercepts the quantum particle sequences sent by Alice and Bob to TP and makes measurements to obtain secret information about Alice and Bob, while returning the previously stored quantum particle sequences to TP.

However, Eve's attack will inevitably introduce errors because Alice, Bob, and TP will perform eavesdropping detection as soon as they receive the particle sequence. The receivers will require the sender to disclose the location and measurement basis of the bait particles, and Eve cannot know the specific state of these particles. When the receiver selects the measurement basis announced by the sender to measure the single particle sent by Eve, there is a 50% probability of obtaining an incorrect result. Eve does not prepare a single particle with the same state as the particle sequences, for example, the original decoy photon has a state of $|1\rangle$, but Eve prepares a single particle with a state of $|0\rangle$. The probability of Eve preparing particles in the wrong state is $1/2$. The probability of Eve successfully deceiving the detection is $(1/2)^n$, where n is the number of decoy photons measured in the eavesdropping detection. When the value of n is large enough, the probability of Eve being discovered is infinitely close to 1. Therefore, the intercept-resend attack is invalid for the method of the present invention.

5.1.2. Measure-Resend Attack

The external attacker Eve can execute the measure-resend attack by first intercepting the particle sequences sent by TP to Alice and Bob and performing $|0, 1\rangle$ basis measurement. Then, based on the measurement results, new quantum particles are prepared and sent to Alice and Bob. After Alice and Bob complete their operations, Eve intercepts the quantum particle sequence sent by Alice and Bob to TP again and conducts measurements to try to obtain the secret information encoded in the quantum particle sequences. At the same time, a new quantum particle sequence is prepared based on the measurement results and transmitted back to TP.

Nonetheless, Eve's attack will unavoidably result in errors because the decoy photons prepared by Alice, Bob, and TP have four states, $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. The state $|0\rangle$ and $|1\rangle$ can be measured using the $|0, 1\rangle$ basis. The state $|+\rangle$ and $|-\rangle$ can be measured using

the X basis. Moreover, Eve cannot know the position of these decoy photons in the state $|+\rangle$ and $|-\rangle$, so it is impossible to prepare corresponding quantum particles and send them to the receivers. Eve may choose the $|0,1\rangle$ basis to measure these quantum particles to get much more secret information. When the receivers conduct eavesdropping detection, the senders announce the position and measurement basis of the decoy photons, and the receivers select the corresponding measurement basis for measurement. If the measurement basis is $|0,1\rangle$ basis, no errors will be found; if the measurement basis is X, there is a 50% probability of obtaining incorrect results (shown in Table 7). Therefore, the measure-resend attack is invalid for the method of the present invention.

Table 7. The example of the process that Eve eavesdrops (the decoy photon is $|+\rangle$).

The state of the decoy photon	$\|+\rangle$			
The measurement basis Eve chooses	$\|0,1\rangle$ basis			
The measurement result	$\|0\rangle$		$\|1\rangle$	
The measurement basis the receivers choose	X basis			
The measurement result	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$
Is the result correct or not	Yes	No	Yes	No

5.1.3. Entanglement Attack

The external attacker Eve can perform the entanglement attack by first entangling her auxiliary quantum particles $|\varepsilon\rangle$ with the target particle; then, Eve measures her auxiliary particles to obtain useful information. The proposed protocol uses a bidirectional quantum channel for quantum communication, so Eve's entanglement measurement attack can be modeled as two unitary operations U_E and U_F. U_E is performed on the channel TP to Alice and Bob, while U_F is performed on the channel Alice and Bob to TP. When the proposed protocol performs eavesdropping detection, only decoy particles are measured, and if Eve can deceive the detection in this stage, the attack can be undetected. Therefore, the following analysis demonstrates that the decoy particle technology applied in the present invention can resist Eve's entanglement attack.

When Eve uses the unitary operation U_E to entangle with the particle that stays in the state $|0\rangle$ and $|1\rangle$, the state of $|0\rangle$ or $|1\rangle$ has been changed. Its state can be reformulated as:

$$U_E|0,\varepsilon\rangle_{TE} = \lambda_{00}|0\rangle|\epsilon_{00}\rangle + \lambda_{01}|1\rangle|\epsilon_{01}\rangle \tag{13}$$

$$U_E|1,\varepsilon\rangle_{TE} = \lambda_{10}|0\rangle|\epsilon_{10}\rangle + \lambda_{11}|1\rangle|\epsilon_{11}\rangle \tag{14}$$

where T and E represent the decoy particles of users and the auxiliary particles of Eve. $|\epsilon_{00}\rangle$, $|\epsilon_{01}\rangle$, $|\epsilon_{10}\rangle$, and $|\epsilon_{11}\rangle$ represent the pure states selected by Eve in the unitary operation U_E. λ_{00}, λ_{01}, λ_{10}, and λ_{11} must meet the conditions: $\|\lambda_{00}\|^2 + \|\lambda_{01}\|^2 = 1$, $\|\lambda_{10}\|^2 + \|\lambda_{11}\|^2 = 1$.

The decoy particles $|+\rangle$ and $|-\rangle$ can be expressed as

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{15}$$

When Eve uses the auxiliary particle $|\varepsilon\rangle$ to entangle with $|+\rangle$ or $|-\rangle$ in the operation U_E, the state of $|+\rangle$ or $|-\rangle$ has been changed. And its state can be reformulated as

$$\begin{aligned} U_E|+,\varepsilon\rangle_{TE} &= \tfrac{1}{\sqrt{2}}(\lambda_{00}|0\rangle|\epsilon_{00}\rangle + \lambda_{01}|1\rangle|\epsilon_{01}\rangle + \lambda_{10}|0\rangle|\epsilon_{10}\rangle + \lambda_{11}|1\rangle|\epsilon_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(\lambda_{00}|\epsilon_{00}\rangle + \lambda_{01}|\epsilon_{01}\rangle + \lambda_{10}|\epsilon_{10}\rangle + \lambda_{11}|\epsilon_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(\lambda_{00}|\epsilon_{00}\rangle - \lambda_{01}|\epsilon_{01}\rangle + \lambda_{10}|\epsilon_{10}\rangle - \lambda_{11}|\epsilon_{11}\rangle) \end{aligned} \tag{16}$$

$$\begin{aligned} U_E|-,\varepsilon\rangle_{TE} &= \tfrac{1}{\sqrt{2}}(\lambda_{00}|0\rangle|\epsilon_{00}\rangle + \lambda_{01}|1\rangle|\epsilon_{01}\rangle - \lambda_{10}|0\rangle|\epsilon_{10}\rangle - \lambda_{11}|1\rangle|\epsilon_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(\lambda_{00}|\epsilon_{00}\rangle + \lambda_{01}|\epsilon_{01}\rangle - \lambda_{10}|\epsilon_{10}\rangle - \lambda_{11}|\epsilon_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(\lambda_{00}|\epsilon_{00}\rangle - \lambda_{01}|\epsilon_{01}\rangle - \lambda_{10}|\epsilon_{10}\rangle + \lambda_{11}|\epsilon_{11}\rangle) \end{aligned} \tag{17}$$

In the above equation, some conditions must be satisfied to avoid Eve introducing errors when the users perform eavesdropping detection.

$$\lambda_{01} = \lambda_{10} = 0, \lambda_{00}|\epsilon_{00}\rangle = \lambda_{11}|\epsilon_{11}\rangle \tag{18}$$

In the proposed protocol, the entanglement attack of Eve mainly acts on the second and third particles of the GHZ-like states used for transmitting information. The GHZ-like state $|GHZ\rangle_1{}'$ used in the proposed protocol can be written as follows:

$$|GHZ\rangle_1{}' = \tfrac{1}{2}[|0\rangle(|00\rangle + |11\rangle) + |1\rangle(|01\rangle + |10\rangle)] = \tfrac{1}{\sqrt{2}}[|0\rangle|\Phi^+\rangle + |1\rangle|\Psi^-\rangle] \tag{19}$$

The second and third particles of the GHZ-like state can be considered as a Bell state together. Without losing generality, the following Bell state expressions are used for analysis.

$$|\Gamma^{\pm}\rangle = \tfrac{1}{\sqrt{2}}[|0q\rangle \pm |1\overline{q}\rangle] \tag{20}$$

After Eve performs the unitary operation U_E^A and U_E^B on the two particles, respectively, the state of the two particles is changed.

$$\begin{aligned} U_E^A \otimes U_E^B|0q,\varepsilon_A\varepsilon_B\rangle &= U_E^A|0\rangle|\varepsilon_A\rangle \otimes U_E^B|q\rangle|\varepsilon_B\rangle = \lambda_{00}|0\rangle|\epsilon_{00}\rangle \otimes \lambda_{qq}|1\rangle|\epsilon_{qq}\rangle \\ &= \lambda_{00}\lambda_{qq}|0q\rangle|\epsilon_{00}\rangle|\epsilon_{qq}\rangle \end{aligned} \tag{21}$$

$$\begin{aligned} U_E^A \otimes U_E^B|1\overline{q},\varepsilon_A\varepsilon_B\rangle &= U_E^A|1\rangle|\varepsilon_A\rangle \otimes U_E^B|\overline{q}\rangle|\varepsilon_B\rangle = \lambda_{11}|1\rangle|\epsilon_{11}\rangle \otimes \lambda_{\overline{qq}}|\overline{q}\rangle|\epsilon_{\overline{qq}}\rangle \\ &= \lambda_{11}\lambda_{\overline{qq}}|1\overline{q}\rangle|\epsilon_{11}\rangle|\epsilon_{\overline{qq}}\rangle = \lambda_{00}\lambda_{qq}|1\overline{q}\rangle|\epsilon_{00}\rangle|\epsilon_{qq}\rangle \end{aligned} \tag{22}$$

where Equation (22) can be simplified, combined with Equation (18). The result is given as follows.

$$\begin{aligned} U_E^A \otimes U_E^B|\psi^{\pm},\varepsilon_A\varepsilon_B\rangle &= \tfrac{1}{\sqrt{2}}U_E^A \otimes U_E^B(|0q,\varepsilon_A\varepsilon_B\rangle \pm |1\overline{q},\varepsilon_A\varepsilon_B\rangle) \\ &= \tfrac{1}{\sqrt{2}}(\lambda_{00}\lambda_{qq}|0q\rangle|\epsilon_{00}\rangle|\epsilon_{qq}\rangle \pm \lambda_{00}\lambda_{qq}|1\overline{q}\rangle|\epsilon_{00}\rangle|\epsilon_{qq}\rangle) \\ &= \lambda_{00}\lambda_{qq}|\psi^{\pm}\rangle|\epsilon_{00}\rangle|\epsilon_{qq}\rangle \end{aligned} \tag{23}$$

According to Equation (14), the tensor product of the attacker Eve's auxiliary particle and its target particle can be expressed as a simple product of the two, so Eve's auxiliary particle and target particle are independent of each other. Overall, if Eve does not want to introduce errors in eavesdropping detection in the present invention, Eve's auxiliary particles and target particles are independent of each other, which means that there is no entanglement. Eve is unable to obtain information about the target particle by measuring her auxiliary particles. Hence, the entanglement attacks are ineffective against our protocol.

Above all, this protocol is impervious to external attacks. The protocol uses the decoy photon technique, which also has been proven to be unconditional security [21,22], to ensure the security of the quantum communication channel and counter most external attacks.

5.2. Participant Attacks

Apart from external attacks, a QPC protocol may also be attacked by internal participants. In the following, two attacks from the participants are analyzed in detail.

5.2.1. The Attack from Alice or Bob

Without loss of generality, assume that Bob is a malicious user aiming to acquire Alice's sensitive information. As mentioned in our protocol, S_2' is computed from Alice's secret.

Since there is no direct communication between Alice and Bob, to get Alice's operations on each particle of S_2', Bob needs to intercept the sequence S_2 sent by TP to Alice and the sequence S_2' sent by Alice to TP. However, the attack methods that Bob may use cannot work, which has been analyzed in the previous part.

5.2.2. The Attack from TP

The impact of a semi-honest third-party TP on the QPC protocol cannot be disregarded, as he/she communicates directly with the participants. In our protocol, TP participated in the preparation of GHZ-like state particles and the measurement of encoded quantum particles. TP may infer the secret information being compared based on the final measurement results, but this approach is not feasible. On the one hand, the user's secret information is encoded on GHZ-like particles through unitary operations, and TP cannot know the specific unitary operations selected by the users. On the other hand, the two binary bits corresponding to each unitary operation are not actual secret information but ciphertext formed after performing a hash function. As a participant in the protocol, TP may also engage in side-channel attacks, which analyze and obtain relevant information of secret information from the physical characteristics of the system, such as the power consumption and processing time during the preparation or encoding of quantum particles. However, the application of decoy photon technology in this protocol can effectively interfere with the execution of side-channel attacks, while hash operations also avoid the leakage of true secret information. In addition, TP may adopt attack methods similar to Eve, but such attacks can be effectively resisted by our protocol. Therefore, the proposed protocol can resist an attack from TP.

6. Efficiency Analysis and Discussion

In this section, the quantum efficiency of our protocol is analyzed in detail. The quantum efficiency of a QPC protocol can be evaluated by comparing the number of classical bits to the number of quantum particles used in the comparison. It is well known that the efficiency of a QPC protocol can be expressed with the following equation [23]:

$$\eta_e = \frac{\eta_c}{\eta_t} \tag{24}$$

where η_e denotes the QPC protocol's efficiency, η_c denotes the number of compared classical bits in each comparison, and η_t denotes the number of generated particles in each comparison.

In the proposed protocol, we generated n three-particle GHZ-like states to compare L classical bits of secret data. After performing the hash operation, the length of classical bits transforms into K, which is given the value of $2n$. The total number of quantum particles is $3n$. Therefore, the quantum efficiency is $2n/3n = 66\%$. The comparison of this protocol with other previously proposed QPC protocols is shown in Table 8.

Table 8. The comparison between our protocol and some previous protocols.

	Ref. [17]	**Ref. [23]**	**Ref. [24]**	**Ref. [25]**	**Our Protocol**
Quantum resource	eight-qubit entangled states	hyper-entangled GHZ states	five-qubit entangled states	four-qubit Cluster state and X-type state	three-particle GHZ-like state
QKD method	Yes	Yes	Yes	Yes	No
Decoy photon	Yes	Yes	Yes	Yes	Yes
Unitary operation	No	No	No	No	Yes
Entanglement swapping	No	Yes	No	No	No
Quantum efficiency	25%	66%	40%	50%	66%

7. Conclusions

A secure and efficient QPC protocol using GHZ-like states is proposed in this paper. Two quantum users, Alice and Bob, can compare the equality of their secret information

with the help of a third-party TP. Compared with most previous QPC protocols, the proposed protocol is more efficient. And in the proposed protocol, the GHZ-like state is used to disseminate quantum information. The unitary operations are used to encode the GHZ-like state particles according to secret information encrypted with a shared hash function. The main feature of the protocol is that users can complete the comparison without sharing a quantum key and communicating, which makes the protocol greatly improved in terms of efficiency while ensuring security, and the protocol makes good use of quantum resources.

Author Contributions: Writing—original draft preparation, F.C., Z.W. and A.F.; writing—review and editing, F.C. and J.L.; and Supervision, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key Research and Development Program of Ningxia Hui Autonomous Region, grant number "2021BEG02007" and the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province, grant number "No. ZCL21006".

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

Acknowledgments: We acknowledge fruitful discussions with Chongyang Ye.

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

References

1. Yin, H.L.; Fu, Y.; Li, C.L.; Weng, C.X.; Li, B.H.; Gu, J.; Lu, Y.S.; Huang, S.; Chen, Z.B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef]
2. Zhou, L.; Lin, J.; Xie, Y.; Lu, Y.; Jing, Y.; Yin, H.; Yuan, Z. Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking. *Phys. Rev. Lett.* **2023**, *130*, 250801. [CrossRef]
3. Xie, Y.M.; Lu, Y.S.; Weng, C.X.; Cao, X.Y.; Jia, Z.Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **2022**, *3*, 020315. [CrossRef]
4. Gu, J.; Cao, X.Y.; Fu, Y.; He, Z.W.; Yin, Z.J.; Yin, H.L.; Chen, Z.B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175. [CrossRef]
5. Huang, X.; Chang, Y.; Cheng, W.; Hou, M.; Zhang, S. Quantum private comparison of arbitrary single qubit states based on swap test. *Chin. Phys. B* **2022**, *31*, 040303. [CrossRef]
6. Lang, Y.-F. Fast Quantum Private Comparison without Keys and Entanglement. *Int. J. Theor. Phys.* **2022**, *61*, 45. [CrossRef]
7. Lian, Y.; Li, X.; Ye, T. Multi-party quantum private comparison of size relationship with two third parties based on -dimensional Bell states. *Phys. Scr.* **2023**, *98*, 035011. [CrossRef]
8. Nilesh, K. Simple proof of security of the multiparty prepare and measure QKD. *Quantum Inf. Process.* **2022**, *21*, 351. [CrossRef]
9. Liu, W.; Liu, C.; Wang, H.; Jia, T. Quantum private comparison: A review. *IETE Tech. Rev.* **2013**, *30*, 439–445. [CrossRef]
10. 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]
11. Lang, Y.-F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
12. Wu, W.Q.; Zhou, G.L.; Zhao, Y.X.; Zhang, H.G. New quantum private comparison protocol without a third party. *Int. J. Theor. Phys.* **2020**, *59*, 1866–1875. [CrossRef]
13. Ji, Z.X.; Fan, P.R.; Zhang, H.G.; Wang, H.Z. Several two-party protocols for quantum private comparison using entanglement and dense coding. *Opt. Commun.* **2020**, *459*, 124911. [CrossRef]
14. 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]
15. Lang, Y.-F. Quantum private comparison using single bell state. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036. [CrossRef]
16. Chen, F.L.; Zhang, H.; Chen, S.G.; Cheng, W.T. Novel two-party quantum private comparison via quantum walks on circle. *Quantum Inf. Process.* **2021**, *20*, 178. [CrossRef]
17. 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]
18. 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]
19. 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]
20. Yu, K.F.; Gu, J.; Hwang, T. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. *Quantum Inf. Process.* **2017**, *16*, 1–14. [CrossRef]

21. Yang, C.W. Encryption chain based on measurement result and its applications on semi-quantum key distribution protocol. *Sci. Rep.* **2022**, *12*, 18381. [CrossRef]
22. Frigyik, A. Quantum Cryptography: Quantum Key Distribution, a Non-technical Approach. *arXiv* **2022**, arXiv:2211.17089.
23. Gianni, J.; Qu, Z. New quantum private comparison using hyperentangled ghz state. *J. Quantum Comput.* **2021**, *3*, 45–54. [CrossRef]
24. 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]
25. 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]