entropy

IMPACT FACTOR 2.1

Indexed in: PubMed

CITESCORE 4.9

Article

New Quantum Private Comparison Using Bell States

Min Hou and Yue Wu

Special Issue

Quantum Entanglement—Second Edition

Edited by

Prof. Dr. Leong Chuan Kwek and Prof. Dr. Marco Genovese

MDPI

https://doi.org/10.3390/e26080682

entropy

MDPI

Article

New Quantum Private Comparison Using Bell States

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

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

Abstract: Quantum private comparison (QPC) represents a cryptographic approach that enables two parties to determine whether their confidential data are equivalent, without disclosing the actual values. Most existing QPC protocols utilizing single photons or Bell states are considered highly feasible, but they suffer from inefficiency. To address this issue, we present a novel QPC protocol that capitalizes on the entanglement property of Bell states and local operations to meet the requirements of efficiency. In the proposed protocol, two participants with private inputs perform local operations on shared Bell states received from a semi-honest third party (STP). Afterward, the modified qubits are returned to the STP, who can then determine the equality of the private inputs and relay the results to the participants. A simulation on the IBM Quantum Cloud Platform confirmed the feasibility of our protocol, and a security analysis further demonstrated that the STP and both participants were unable to learn anything about the individual private inputs. In comparison to other QPC protocols, our proposed solution offers superior performance in terms of efficiency.

Keywords: quantum private comparison; quantum entanglement; Bell state; local operation; quantum cryptography

Citation: Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. https://doi.org/10.3390/e26080682

Academic Editors: Marco Genovese and Leong Chuan Kwek

Received: 30 July 2024
Revised: 5 August 2024
Accepted: 11 August 2024
Published: 13 August 2024

1. Introduction

The advancement of quantum technology has rendered classical cryptographic algorithms such as RSA and ElGamal, which rely on the difficulty of factoring large numbers, vulnerable to quantum algorithm attacks such as the Shor algorithm [1]. Quantum cryptography, which integrates classical cryptography and quantum mechanics, provides unconditional security by leveraging quantum properties. Consequently, quantum cryptography has garnered considerable attention from the academic community. The pioneering BB84 protocol, proposed by Bennett and Brassard in 1984 [2], enhanced information transmission security and privacy. Since then, numerous quantum cryptographic protocols have emerged, targeting objectives like quantum key distribution (QKD) [3–6], quantum key agreement (QKA) [7–9], quantum secret sharing (QSS) [10–12], quantum secure direct communication (QSDC) [13,14], and quantum private set intersection [15].

Private comparison originated from Yao's millionaires' problem [16], which aims to determine the richer of two millionaires while keeping their wealth undisclosed. The socialist millionaires' problem, a variation of Yao's millionaires' problem, aims to determine whether two individuals have equal wealth, as proposed by Boudot et al. [17]. Since then, solving the millionaires' problem has become a fundamental task in the field of secure multiparty computing (SMC). When addressing this task, Lo [18] pointed out that designing a protocol to securely evaluate a two-party computational function is impossible. Consequently, the involvement of a semi-honest third party (STP) should be considered when developing private comparison protocols. The security of private comparison protocols is similar to classical cryptography, which relies on the difficulty of factorizing large numbers and is consequently vulnerable to quantum attacks. As a result, new measures need to be implemented to achieve quantum security.

Quantum private comparison (QPC) differentiates itself from classical private comparison by employing qubits as quantum information carriers, rather than classical bits. The goal of QPC is to compare the equality of two participants' private inputs while preserving the privacy of both parties and ensuring quantum-based security. In 2009, Yang and Wen [19] introduced the first QPC protocol, utilizing the property of Bell states to achieve private comparison and decoy photons to detect the presence of an eavesdropper. In 2010, Chen et al. [20] introduced a new QPC protocol by performing unitary operations on GHZ states to encode information, but it could not defend against interception attacks [21]. Since these early contributions, the field of QPC has seen a proliferation of proposed protocols, each exploring the use of diverse quantum states as information carriers. The current landscape of QPC protocols can be broadly categorized into two main streams:

- QPC protocols using low-dimensional quantum states;
- QPC protocols using high-dimensional quantum states.

Single photons, Bell states, GHZ states [22], and W states are commonly employed as quantum resources to achieve private comparison in low-dimensional quantum state-based QPC protocols. Huang et al. [23] utilized single photons and collective detection to design a QPC protocol, where a specific unitary operation was performed on single photons to encode information. However, this protocol consumed 4n qubits to compare n classical bits, resulting in a qubit efficiency of only 25%. Li et al. [24] introduced a novel protocol that leveraged the concept of entanglement swapping between Bell states and W-class states. This protocol enabled the comparison of two classical bits per round, achieving an efficiency of 40%. However, Gao et al. [25] argued that the STP assumption in the scheme presented in Ref. [24] is unreasonable, and that the scheme cannot withstand fake signal attacks when the STP restriction is tightened, leading to the disclosure of privacy to the STP. Lang et al. [26] utilized Bell states as quantum resources and employed quantum gates instead of classical exclusive-OR computations for classical computing, an approach that can enhance the security. However, Duan [27] noted that the scheme presented in Ref. [26] is vulnerable to measurement attacks from the STP and disturbance attacks from external adversaries, and proposed some improvements to address these security weaknesses. Huang et al. [28] introduced a novel protocol that harnessed the properties of entanglement swapping between three Bell states, enabling the comparison of three classical bits per round and achieving a qubit efficiency of 50%. Hou and Wu [29] proposed a QPC protocol that employed single photons as well as Identity or Hadamard operations to achieve private comparison. However, the need for multiple preparations of single photons as the initial quantum resources in this protocol leads to a reduction in qubit efficiency. While the low-dimensional quantum state-based QPC protocols can achieve private comparison while preserving the secrecy of the inputs, these protocols generally exhibit lower qubit efficiency.

In high-dimensional quantum state-based QPC protocols, quantum states with a large number of degrees of freedom or a large Hilbert space dimension are primarily employed as quantum resources to enable private comparison. Jia et al. [30] proposed a QPC protocol that utilizes d-level GHZ states as the quantum resources. In this protocol, the secrets are encoded into the phase of the d-level GHZ states through local operations, and the phase information can then be collectively measured to facilitate the private comparison. Lin et al. [31] designed a QPC protocol that employed d-dimensional Bell states as the quantum resources. Through the strategic use of unitary operations, the secrets are encoded, enabling the comparison of the size relationship of the private inputs. Guo et al. [32] employed entanglement swapping between d-level states to achieve the comparison and shifting operations to encode the private inputs of the participants. Recognizing the importance of practical implementation, Yu et al. [33] developed a QPC protocol that utilized easy-to-implement d-level single-particle states to compare the size relationship of the private inputs. Aiming to enhance capacity and reduce the quantum resource requirements, Xu and Zhao [34] proposed a QPC protocol that employed Bell states as the quantum resources, achieving a significantly higher capacity compared to previous approaches. Ji et al. [35] introduced a QPC protocol that employed (n + 1)-qubit GHZ states, where n represents the

number of qubits in the GHZ states, ensuring the privacy of the participants by generating a secret key and performing bit-flipping operations. Wu and Zhao [36] utilized d-level Bell states for private comparison to determine the relationship of the private inputs. While quantum state-based QPC protocols can encode more quantum information and achieve private comparison while maintaining secrecy, they pose significant challenges in practical implementation with current technology due to the difficulty of preparing complex quantum states.

An analysis of the existing QPC protocols revealed that those utilizing low-dimensional quantum states have lower qubit efficiency, while those employing high-dimensional quantum states pose significant challenges in practical implementation with the current technology. To address this issue, we propose a QPC protocol employs Bell states and local operations to facilitate private comparison. Specifically, the inputs are encoded into shared Bell states, which are then sent to the semi-trusted party (STP). The STP can subsequently determine the equality of the inputs without learning the individual values and communicate the results back to the participants. Simulation experiments conducted on the IBM Quantum Cloud Platform have demonstrated the practical viability of this approach. Additionally, the protocol's security analysis suggests its ability to withstand both outsider attacks from eavesdroppers and participant attacks aimed at learning the individual inputs. Compared to other QPC protocols, the proposed solution utilizes a Bell state, which is relatively straightforward to implement, to compare a single classical bit. This results in a notable qubit efficiency of 50%.

The remaining sections are organized as follows. Section 2 provides some preliminaries, introducing the necessary background information. Section 3 then presents the detailed steps of the designed QPC protocol. Simulations and security analyses are discussed in Sections 4 and 5, respectively. Section 6 includes an efficiency analysis and comparison. Finally, Section 7 summarizes the key findings of this work.

2. Preliminaries

The bit flip and phase shift operators can be given by

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

Applying the above two operators to an orthonormal basis $\{|0\rangle, |1\rangle\}$, we have

$$\begin{cases} X|0\rangle = |1\rangle, X|1\rangle = |0\rangle \\ Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle \end{cases} \tag{2}$$

Four Bell states can be written as

$$|\varphi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3}$$

$$|\varphi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{4}$$

$$|\varphi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{5}$$

$$|\varphi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{6}$$

Suppose that a third party prepares a Bell state $|\varphi_{ab}\rangle$ and distributes the first qubit to Alice and the second qubit to Bob. Subsequently, Alice and Bob perform the following operations: if $a = 0$, Alice applies the phase shift operator Z to her qubit; if $a = 1$, Alice applies the bit flip operator X to her qubit. Likewise, if $b = 0$, Bob applies the phase shift operator Z to his qubit, and if $b = 1$, Bob applies the bit flip operator X to his qubit. The

encoding rule is presented in Table 1. After Alice and Bob have applied their respective operations, they return their individual qubits to the third party. The third party then performs a Bell basis measurement on the combined state, obtaining the measurement result $|\varphi'_{ab}\rangle$. The resulting states when performing the bit flip and phase shift operators on $|\varphi_{ab}\rangle$ are shown in Table 2.

Table 1. The encoding rule.

	$a = 0$	$a = 1$
$b = 0$	$Z \otimes Z$	$X \otimes Z$
$b = 1$	$Z \otimes X$	$X \otimes X$

Table 2. The resulting states when performing the encoding rule on $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, $|\varphi_{10}\rangle$, and $|\varphi_{11}\rangle$.

	$a = 0, b = 0$	$a = 0, b = 1$	$a = 1, b = 0$	$a = 1, b = 1$
$\|\varphi_{00}\rangle$	$\|\varphi_{00}\rangle$	$\|\varphi_{11}\rangle$	$\|\varphi_{11}\rangle$	$\|\varphi_{00}\rangle$
$\|\varphi_{01}\rangle$	$\|\varphi_{01}\rangle$	$\|\varphi_{10}\rangle$	$\|\varphi_{10}\rangle$	$\|\varphi_{01}\rangle$
$\|\varphi_{10}\rangle$	$\|\varphi_{10}\rangle$	$\|\varphi_{01}\rangle$	$\|\varphi_{01}\rangle$	$\|\varphi_{10}\rangle$
$\|\varphi_{11}\rangle$	$\|\varphi_{11}\rangle$	$\|\varphi_{00}\rangle$	$\|\varphi_{00}\rangle$	$\|\varphi_{11}\rangle$

3. Quantum Private Comparison Protocol

The QPC protocol involves three entities.

Semi-honest third party (STP): STP has full quantum capabilities and operates in the semi-honest model. In the semi-honest model, the STP must strictly follow the defined protocol steps but may attempt to learn the users' secrets by utilizing the immediate results and performing quantum attacks. However, the STP is not allowed to collude with or favor any of the users involved.

Users: Two users, Alice and Bob are involved in the protocol to compare their secrets. Like the STP, both Alice and Bob have full quantum capabilities. However, they adopt an honest-but-curious posture—adhering strictly to the established protocol, while potentially seeking to uncover each other's secrets.

Participants Alice and Bob each possess their own private data, denoted as A and B, respectively. These secrets can be written in binary form as $A = \{a_{L-1}a_{L-2}\cdots a_1a_0\}$ and $B = \{b_{L-1}b_{L-2}\cdots b_1b_0\}$, where $a_i, b_i \in \{0,1\}, i = 0,1,2,\cdots L$, and L is the length of the strings A and B. The protocol assumes a quantum channel that is free from noise and loss, while the classical channel is authenticated during transmission. The detailed steps of the proposed QPC protocol are as follows, and its diagram is shown in Figure 1.

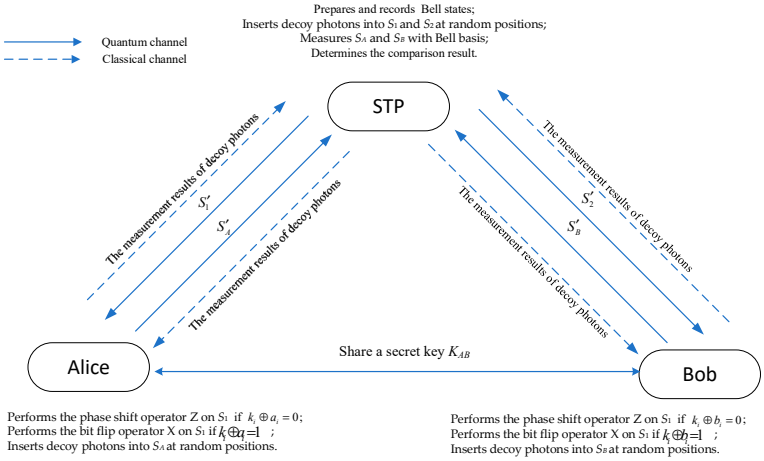

Figure 1. The diagram of the QPC protocol.

Step 1. Alice and Bob use a QKD protocol, such as the BB84 protocol [2], to generate a shared secret key $K_{AB} = (k_{L-1}k_{L-2}\cdots k_1k_0)$, where $k_i \in \{0,1\}, i = 0,1,2,\cdots,L$.

Step 2. STP prepares n Bell states, all randomly chosen from Equations (3)–(6), records these Bell states, and distributes the first qubits as sequence S_1 and the second qubits as sequence S_2. Then, she prepares 2δ decoy photons, each chosen from $\left\{|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ randomly, and inserts δ decoy photons into S_1 and another δ decoy photons into S_2 at random positions to generate two sequences, S_1' and S_2', respectively. Finally, she sends S_1' and S_2' to Alice and Bob, respectively, via the quantum channel.

Step 3. After receiving the respective photon sequences S_1' and S_2', Alice and Bob each send a confirmation message to the STP. In response, the STP announces the positions and measurement bases of the decoy photons within the sequences. For example, if the decoy photons are prepared in $|0\rangle$ or $|1\rangle$ states, the measurement base is the Z basis. Otherwise, the measurement basis is the X basis. Alice and Bob then measure the decoy photons using the announced bases and send the results back to the STP over a classical channel. The STP compares the initial decoy photon preparations with the measurement results to compute the error rate. If the error rate exceeds a predefined threshold, the protocol is terminated. Otherwise, the process continues to the next step.

Step 4. Alice (Bob) discards the decoy photons in $S_1'(S_2')$ to obtain S_1 and S_2.

For Alice:

(1) If $k_i \oplus a_i = 0$, she performs the phase shift operator Z on S_1. Otherwise, she performs the bit flip operator X on S_1. The resulting sequence is denoted as S_A.

(2) She inserts δ decoy photons, chosen from $\left\{|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, into S_A to generate a new sequence S_A'.

(3) She sends S_A' to the STP via a quantum channel.

For Bob:

(1) If $k_i \oplus b_i = 0$, he performs the phase shift operator Z on S_2. Otherwise, he performs the bit flip operator X on S_2. The resulting sequence is denoted as S_B.

(2) She inserts δ decoy photons, chosen from $\left\{|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, into S_B to generate a new sequence S_B'.

(3) She sends S_B' to the STP via a quantum channel.

Step 5. When the STP receives S_A' and S_B', she interacts with Alice and Bob to check for the presence of an eavesdropper, similar to the process carried out in Step 3. If no eavesdropper is detected, the protocol proceeds to the next step. However, if an eavesdropper is detected, the protocol is terminated.

Step 6. The STP discards the decoy photons in S_A' and S_B' to obtain S_A and S_B and then performs the Bell measurement on them. If the Bell measurement results match the initially prepared Bell states, the STP can conclude that the inputs provided by Alice and Bob are identical. Conversely, if the Bell measurement results differ from the initial Bell states, the STP determines that the inputs from Alice and Bob are different.

4. Simulation Experiments

Considering a concrete example, let us assume that Alice and Bob have their own secrets, A = 7 and B = 6, with their binary representations being $A = 111$ and $B = 110$, respectively. Since the length of both A and B is 3, three Bell states are assumed to be prepared as $|\varphi_{00}\rangle, |\varphi_{01}\rangle$, and $|\varphi_{11}\rangle$. The quantum circuit and measurement result are shown in Figures 2 and 3, respectively. For example, the Bell state $|\varphi_{00}\rangle$ can be produced using a Hadamard gate and a controlled-NOT gate, which is performed on two qubits corresponding to q [0] and q [1] of Figure 2, starting from the state $|0\rangle$. To measure the Bell state $|\varphi_{00}\rangle$, we can perform the Hadamard gate and the controlled-NOT gate once, and the measurement result will always be $|00\rangle$, corresponding to 00. For the other three Bell

states $|\varphi_{01}\rangle$, $|\varphi_{10}\rangle$, and $|\varphi_{11}\rangle$, their measurement outcomes using the Bell measurement will corresponding to 10, 01, and 11, respectively.

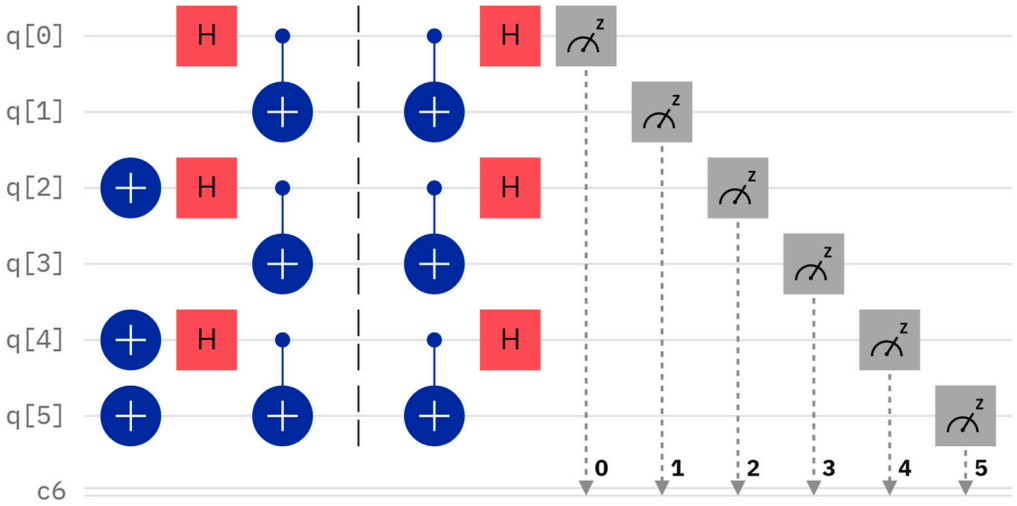

Figure 2. Preparation of Bell states.

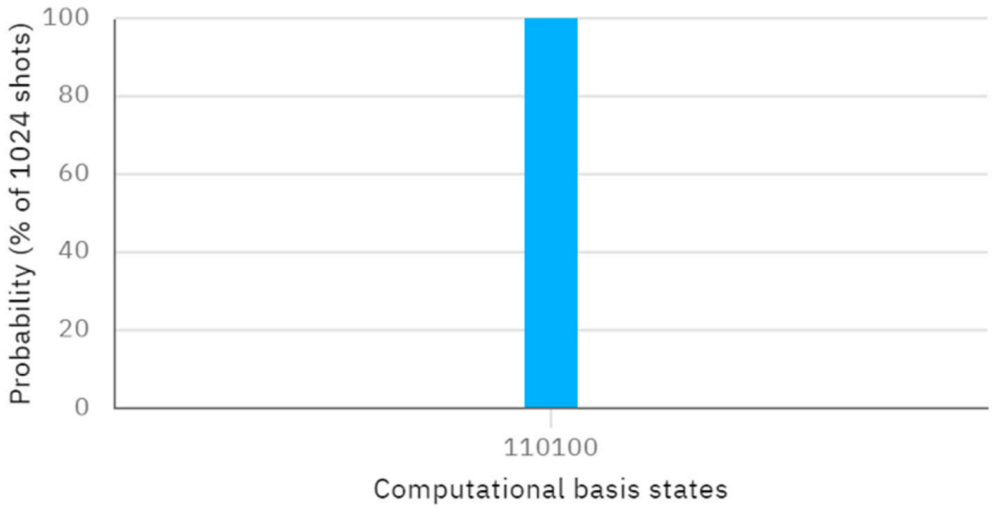

Figure 3. Measurement results of the Bell states.

Assume a secret key $K_{AB} = 011$ of length L is shared. According to this protocol, when Alice performs X, Z, and Z operators on the first qubit of $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, and $|\varphi_{11}\rangle$, and Bob performs X, Z, and X operators on the second qubit of $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, and $|\varphi_{11}\rangle$, the resulting quantum circuit without considering the eavesdropping detection, which can be considered as an independent procedure, and the corresponding measurement outcome, obtained through Bell measurement, are depicted in Figures 4 and 5, respectively. Examining Figure 5, the measured outcome of the quantum circuit in Figure 4 is 001000, corresponding to q [0]–q [5]. This differs from the measurement result of 001011, corresponding to q [0]–q [5], as shown in Figure 3. The discrepancy between the actual and expected measurement outcomes suggests that the measurement results do not match the initially prepared Bell states. This indicates that the inputs provided by Alice and Bob are not identical (i.e., the comparison result is $A \neq B$).

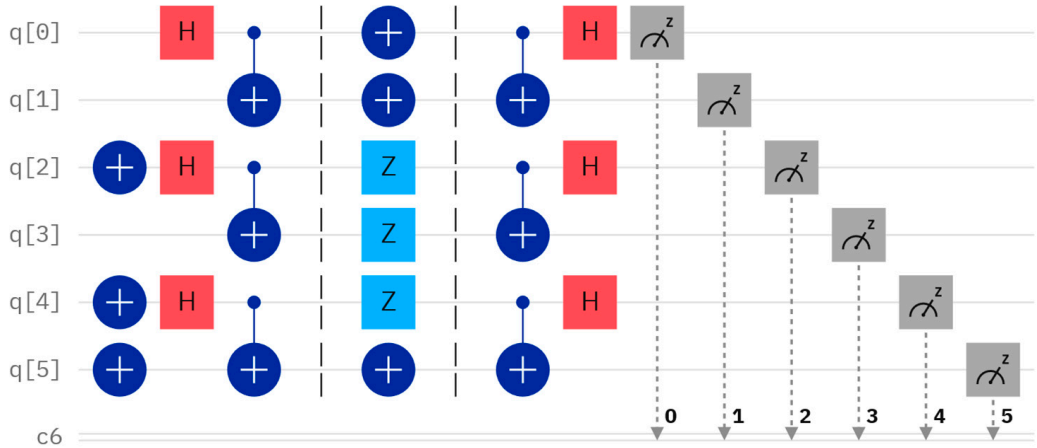

Figure 4. Quantum circuit for comparing A and B.

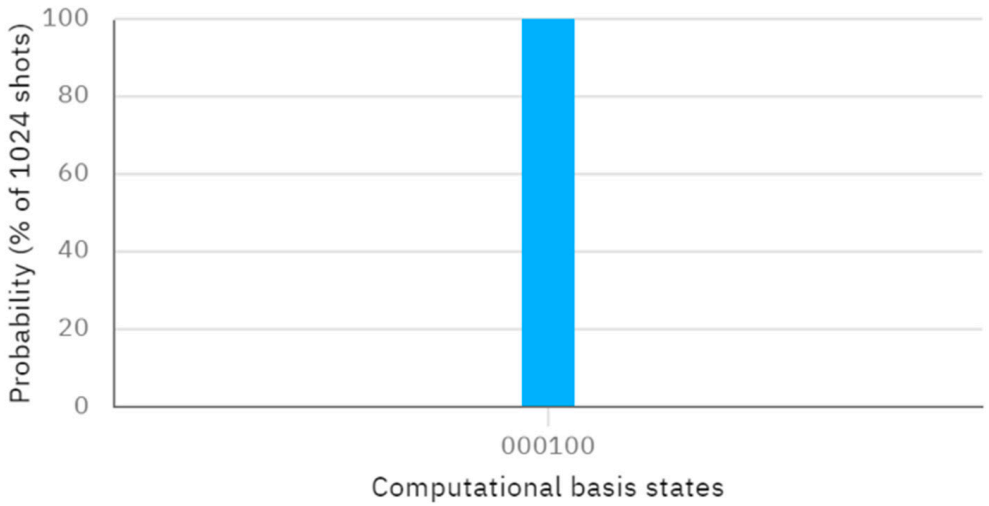

Figure 5. The measurement results of Figure 4.

Considering another concrete case, let us assume that Alice and Bob have their own secrets, $A' = 7$ and $B' = 7$, with their binary representations being $A' = 111$ and $B' = 111$, respectively. The initially-prepared Bell states and K_{AB} are the same as the previous assumptions. According to this protocol, when Alice performs X, Z, and Z operators on the first qubit of $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, and $|\varphi_{11}\rangle$, and Bob performs X, Z, and Z operators on the second qubit of $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, and $|\varphi_{11}\rangle$, The resulting quantum circuit and the corresponding measurement outcome, obtained through Bell measurement, are depicted in Figures 6 and 7, respectively. Examining Figure 7, the measured outcome of the quantum circuit in Figure 6 is 001011, corresponding to q [0]–q [5]. This is consistent with the measurement result of 001011, as shown in Figure 3. The fact that the actual and expected measurement outcomes match indicates that the measurement results are the same as the initially prepared Bell states. This suggests that the inputs provided by Alice and Bob are identical (i.e., the comparison result is $A' = B'$).

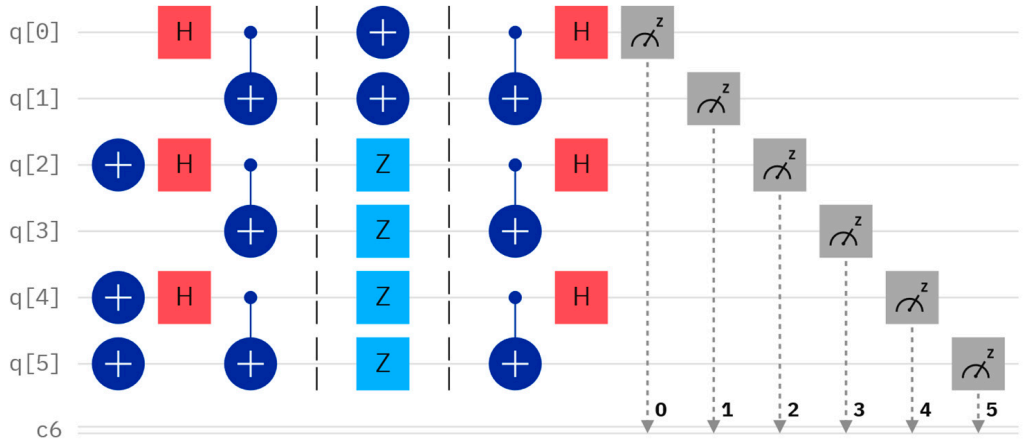

Figure 6. Quantum circuit for comparing A' and B'.

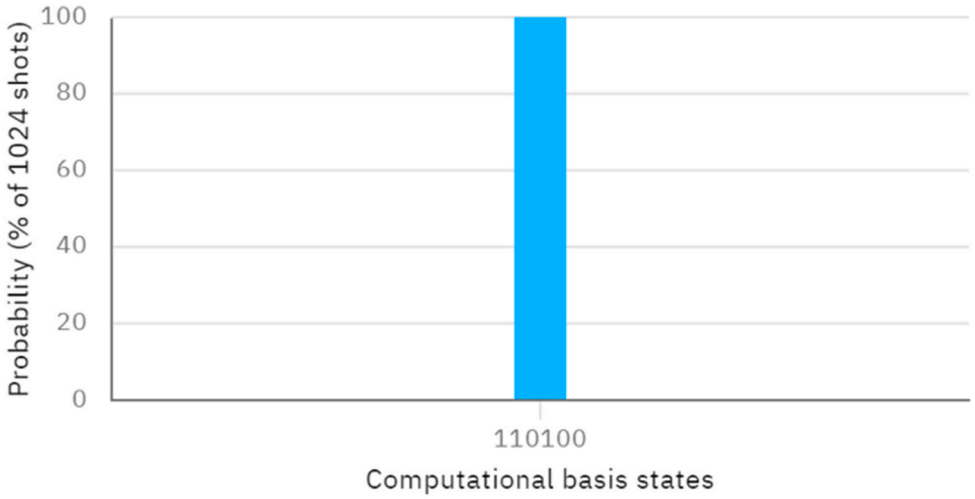

Figure 7. The measurement result of Figure 6.

To conclude, the above two concrete cases reveal the feasibility of our protocol.

5. Security Analysis

During the transmission of quantum information, external attackers may eavesdrop on the quantum channel to steal useful information about the inputs of the users. Additionally, the users themselves may try to utilize some received immediate results to deduce the private inputs of another user. However, our protocol is designed to resist both eavesdropping and participant attacks. This is achieved through the decoy state method and quantum key distribution (QKD) techniques employed in the protocol.

On the one hand, the protocol can detect the presence of eavesdroppers by randomly inserting decoy states, which are states with known properties, into the transmitted signal. Any tampering or eavesdropping on the quantum channel can be detected by analyzing the properties of the received decoy states. On the other hand, the protocol utilizes QKD to establish a shared secret key between the participating users. This shared key is then used to covert the transmitted information, ensuring that even if an attacker manages to intercept the quantum signals, they will not be able to extract any meaningful information without the secret key. By employing these techniques, the proposed protocol is able to effectively mitigate the risks of both external eavesdropping and participant attacks, thereby ensuring the security and integrity of the transmitted quantum information.

5.1. External Attacks

Potential attacker, Eve, may attempt diverse classical or quantum-based assaults to acquire information about the user inputs. Possible attacks encompass intercept-measure-resend, entangle-measure, and Trojan horse techniques [37–40]. Nonetheless, the proposed protocol leverages the decoy state method during qubit transmission between parties. This approach effectively counters these varied attack vectors.

5.1.1. Intercept-Measure-Resend Attack

In an intercept-measure-resend attack, the adversary (Eve) intercepts the quantum channel, measures the intercepted sequence using guessed bases, and resends a new sequence with the same measurement results. However, this would trigger protocol termination, as the computed error rate exceeds the threshold. Eve lacks knowledge to distinguish decoy photons from target particles, and the decoy photon measurement bases are unknown to her. Eve may attempt to use guessed bases to obtain some information. For a decoy photon, there is a 50% chance of correctly guessing the base. Similarly, choosing the wrong base can still bypass detection half the time. This means that Eve can bypass detection with a 25% probability when using the wrong base. For example, measuring a $|+\rangle$ decoy photon using the Z-basis results in $|0\rangle$ or $|1\rangle$ states. When preparing $|0\rangle$ or $|1\rangle$ and sending them to the receiver, Eve will not introduce any error with a probability of 50%. Measuring the decoy with the X-basis gives $|+\rangle$, which can be sent without error, bypassing detection with 100% probability. Overall, the probability that Eve can intercept a decoy photon without introducing error and bypass detection is 0.75.

In summary, the probability of detecting the adversary (Eve) during the detection process is given by $1-\left(\frac{3}{4}\right)^{\delta}$, where δ is the number of decoy photons. When $\delta = 27$, the probability of detecting Eve is 0.9996, and as δ increases further, the probability of detecting Eve tends toward 1. Consequently, when an adversary performs the intercept-measure-resend attack, they will inevitably introduce errors into the transmitted sequence, which can then be detected by the legitimate users. Due to the high probability of detection and the introduction of errors, the adversary cannot learn anything about the inputs of the users during the QPC process.

5.1.2. Entangle-Measure Attack

The entangle-measure attack refers to a strategy where Eve performs an interception operation on the quantum channel to obtain the transmitted quantum sequence. Eve then prepares auxiliary particles $|e\rangle$ and entangles them with each intercepted particle, with the aim of stealing the secrets of the users. When the target particles are measured, Eve can measure the auxiliary particles to learn the states of the target particles. However, the success of this attack is contingent on Eve being able to avoid detection by the eavesdropping detection mechanism.

When entangling the auxiliary particle $|e\rangle$ with a target particle in state $|0\rangle$ or $|1\rangle$, we have the following equations:

$$U|e\rangle|0\rangle = \lambda_0|0e_{00}\rangle + \lambda_1|0e_{01}\rangle \tag{7}$$

$$U|e\rangle|1\rangle = \lambda_2|0e_{10}\rangle + \lambda_3|0e_{11}\rangle \tag{8}$$

where the parameters λ_0, λ_1, λ_2, and λ_3 satisfy $\|\lambda_0\|^2 + \|\lambda_1\|^2 = \|\lambda_2\|^2 + \|\lambda_3\|^2 = 1$. Four quantum states $\{|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle\}$ are determined by U.

When entangling the auxiliary particle $|e\rangle$ with a target particle in state $|+\rangle$ or $|-\rangle$, the resultant process can be written as:

$$\begin{aligned} &U|e\rangle|+\rangle = \tfrac{1}{\sqrt{2}}(\lambda_0|0e_{00}\rangle + \lambda_1|1e_{01}\rangle + \lambda_2|0e_{10}\rangle + \lambda_3|1e_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(\lambda_0|e_{00}\rangle + \lambda_1|e_{01}\rangle + \lambda_2|e_{10}\rangle + \lambda_3|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(\lambda_0|e_{00}\rangle - \lambda_1|e_{01}\rangle + \lambda_2|e_{10}\rangle - \lambda_3|e_{11}\rangle) \end{aligned} \tag{9}$$

$$\begin{array}{l} U|e\rangle|-\rangle = \frac{1}{\sqrt{2}}(\lambda_0|0e_{00}\rangle + \lambda_1|1e_{01}\rangle - \lambda_2|0e_{10}\rangle - \lambda_3|1e_{11}\rangle) \\ = \frac{1}{2}|+\rangle(\lambda_0|e_{00}\rangle + \lambda_1|e_{01}\rangle - \lambda_2|e_{10}\rangle - \lambda_3|e_{11}\rangle) \\ +\frac{1}{2}|-\rangle(\lambda_0|e_{00}\rangle - \lambda_1|e_{01}\rangle - \lambda_2|e_{10}\rangle + \lambda_3|e_{11}\rangle) \end{array} \quad (10)$$

To introduce no error, the above Equations (7)–(10) should meet the following conditions:

$$\lambda_1 = \lambda_2 = 0 \quad (11)$$

$$\lambda_0 = \lambda_3 = 1 \quad (12)$$

$$\lambda_0|e_{00}\rangle - \lambda_1|e_{01}\rangle + \lambda_2|e_{10}\rangle - \lambda_3|e_{11}\rangle = \vec{0} \quad (13)$$

$$\lambda_0|e_{00}\rangle + \lambda_1|e_{01}\rangle - \lambda_2|e_{10}\rangle - \lambda_3|e_{11}\rangle = \vec{0} \quad (14)$$

From Equations (11)–(14), we can further obtain $\lambda_0 = \lambda_3 = 1$ and $|e_{00}\rangle = |e_{11}\rangle$. When substituting these results into Equations (7)–(10), we have

$$U|e\rangle|0\rangle = |0e_{00}\rangle = |0e_{11}\rangle \quad (15)$$

$$U|e\rangle|1\rangle = |1e_{00}\rangle = |1e_{11}\rangle \quad (16)$$

$$U|e\rangle|+\rangle = |+e_{00}\rangle = |+e_{11}\rangle \quad (17)$$

$$U|e\rangle|-\rangle = |-e_{00}\rangle = |-e_{11}\rangle \quad (18)$$

We can conclude that the auxiliary and target particles exist in a product form, rather than a tensor product. This independent relationship between the auxiliary and target particles indicates an absence of entanglement. Furthermore, when the target particles are measured, Eve cannot know the states of the target particles when performing the measurement on the auxiliary particles. As a result, Eve cannot infer the secrets by conducting the entangle-measure attack.

5.1.3. Trojan Horse Attack

Two-way quantum communication protocols are susceptible to Trojan horse attacks, which encompass the delay-photon Trojan-horse attack and the invisible photon eavesdropping Trojan-horse attack [41]. Given that the proposed protocol is a two-way quantum communication protocol, it may be vulnerable to such attacks. However, several existing techniques can be employed to detect and mitigate Trojan horse attacks. For example, the wavelength quantum filter (WQF) and the photons number splitter (PNS) can be utilized to eliminate invisible photons and separate legitimate photons when encountering Trojan horse attacks.

5.2. Participant Attacks

Insider participants may launch more powerful attacks to steal the secrets. The following discusses two cases of attacks from the semi-honest third party (STP) and Alice or Bob.

5.2.1. Attacks from the STP

In the semi-honest model, the STP is involved and must strictly follow the defined steps of the protocol, but is not allowed to collude or favor any of the users. STP may attempt to learn the users' secrets by utilizing the immediate results and performing quantum attacks. In the proposed protocol, the STP is primarily involved in preparing Bell states and performing Bell-basis measurement. Although the STP knows the initially-prepared Bell state and the final Bell states, it cannot infer the secrets by utilizing the relationship between them. On the one hand, the STP may prepare a single-photon sequence to replace the Bell state sequence and measure the final received quantum sequence with single-particle measurement. For example, suppose that the STP prepares a single photon in state $|1\rangle$, which is sent to Alice. The final measurement result is $|1\rangle$ when the Z operator is performed

by Alice, and the final measurement result is $|0\rangle$ when the X operator is performed by Alice. Therefore, regardless of the Z or X operators performed by Alice, the STP can know them by measuring the received quantum sequence with single-particle measurement. However, the STP has the opportunity to know which operations are performed by Alice and Bob, but has no way of knowing the secret key, since K_{AB} is unknown to her, making it impossible to eavesdrop on the secrets. On the other hand, the STP may launch attacks that are similar to the malicious behavior performed by Eve, but these will be inevitably detected, as discussed in Section 5.1. As a result, the STP has no way of learning the secrets.

5.2.2. Attacks from Alice or Bob

The proposed protocol assumes the same roles for the participants, Alice and Bob, without loss of generality. The protocol presumes that Bob seeks to ascertain Alice's secrets, which are encoded into quantum operations, such as bit flip and phase shift, used to transform the received quantum sequence S_1. If Bob intends to know the secrets of Alice, he must know the converted quantum sequence S_A and the initially prepared Bell state sequence. However, there is no direct communication between the participants; the only way for Bob to obtain S_1 and S_A is to intercept the quantum communication between the STP and Alice. This behavior is equivalent to performing external eavesdropping and will inevitably be detected due to the decoy state method employed. A similar method can be used to analyze the situation where Alice intends to know the secrets of Bob. Consequently, the secrets of both participants will remain undisclosed, even in the event of participant attacks.

6. Efficiency Analysis and Comparison

The qubit efficiency [42] is a crucial metric for evaluating the efficiency of a quantum communication protocol, which can be expressed as:

$$e = \frac{c}{t} \tag{19}$$

where e represents the qubit efficiency, c denotes the number of classical bits compared, and t represents the total number of qubits consumed during the entire process excluding the decoy photons, which can be considered as an independent procedure. In the protocol, a Bell state with two qubits can be used to compare one classical bit, and therefore, $c = L$ and $t = 2L$. Therefore, the qubit efficiency of the protocol is 50%.

Table 3 presents a comparison of the proposed QPC protocol with some existing QPC protocols in terms of quantum resource, entanglement swapping, unitary operation, quantum measurement, and qubit efficiency.

Table 3. Comparison of our protocol among some of the existing QPC protocols.

	Ref. [19]	**Ref. [20]**	**Ref. [22]**	**Ref. [23]**	**Ref. [28]**	**Ours**
Quantum resource	Bell states	GHZ states	GHZ states	Single photons	Bell states	Bell states
Entanglement swapping	No	No	Yes	No	Yes	No
Unitary operation	Yes	Yes	No	Yes	No	Yes
Quantum measurement	Bell basis	Single-particle	Bell basis	Single-particle	GHZ basis	Bell basis
Qubit efficiency	25%	33%	33%	25%	50%	50%

The quantum resource usage and qubit efficiency of the proposed protocol are the same as the protocol presented in Ref [28], as demonstrated in Table 3. However, the unitary operations, such as bit flip and phase shift, employed in the proposed protocol are comparatively more straightforward to implement than the entanglement swapping and GHZ-basis measurements required in Ref [28]. While the quantum resources in Refs. [19,20,22,23,28] and the proposed protocol are easy to implement, the qubit efficiency

in Refs. [19,20,22,23] is relatively low. Therefore, the proposed QPC protocol not only has a higher qubit efficiency, but also offers easier implementation due to the simpler unitary operations required, resulting in an overall superior performance.

7. Conclusions

In this paper, we proposed a novel QPC protocol that harnesses the entanglement property of Bell states to enable the comparison of private inputs. The proposed protocol employs a readily implementable Bell state to compare a single classical bit, thereby achieving a qubit efficiency of 50%. Furthermore, the protocol's architecture, which is grounded in the utilization of Bell states, unitary operations, and Bell measurements, confers greater practicality and feasibility. We conducted the simulation experiments on the IBM Quantum Cloud Platform, which validated the feasibility of the proposed protocol. Furthermore, our security analysis substantiates the proposed protocol's ability to effectively safeguard the participants' secrets from both external eavesdropping and participant-based attacks.

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

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

Institutional Review Board Statement: Not applicable.

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

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

References

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. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
3. Nadlinger, D.P.; Drmota, P.; Nichol, B.C.; Araneda, G.; Main, D.; Srinivas, R.; Lucas, D.M.; Balance, C.J.; Ivanov, K.; Tan, E.Y.-Z.; et al. Experimental quantum key distribution certified by Bell's theorem. *Nature* **2022**, *607*, 682–686. [CrossRef] [PubMed]
4. Fang, X.T.; Zeng, P.; Liu, H.; Zou, M.; Wu, W.; Tang, Y.-L.; Sheng, Y.-J.; Xiang, Y.; Zhang, W.; Li, H.; et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **2020**, *14*, 422–425. [CrossRef]
5. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.-K.; Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
6. Basso Basset, F.; Valeri, M.; Roccia, E.; Muredda, V.; Poderini, D.; Neuwirth, J.; Spagnolo, N.; Rota, M.B.; Carvacho, G.; Sciarrino, F.; et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **2021**, *7*, eabe6379. [CrossRef]
7. Huang, X.; Zhang, S.B.; Chang, Y.; Qiu, C.; Liu, D.-M.; Hou, M. Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 838–847. [CrossRef]
8. Zhou, Y.H.; Wang, M.F.; Shi, W.M.; Yang, Y.-G.; Zhang, J. Two-party quantum key agreement against collective noisy channel. *Quantum Inf. Process.* **2020**, *19*, 100. [CrossRef]
9. Li, L.; Li, Z. A verifiable multiparty quantum key agreement based on bivariate polynomial. *Inf. Sci.* **2020**, *521*, 343–349. [CrossRef]
10. Senthoor, K.; Sarvepalli, P.K. Theory of communication efficient quantum secret sharing. *IEEE Trans. Inf. Theory* **2022**, *68*, 3164–3186. [CrossRef]
11. Shen, A.; Cao, X.Y.; Wang, Y.; Fu, Y.; Gu, J.; Liu, W.-B.; Weng, C.-X.; Yin, H.-L.; Chen, Z.-B. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci. China Phys. Mech. Astron.* **2023**, *66*, 260311. [CrossRef]
12. Liao, Q.; Liu, H.; Zhu, L.; Guo, Y. Quantum secret sharing using discretely modulated coherent states. *Phys. Rev. A* **2021**, *103*, 032410. [CrossRef]
13. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef] [PubMed]

14. Huang, X.; Zhang, S.; Chang, Y.; Yang, F.; Hou, M.; Cheng, W. Quantum secure direct communication based on quantum homomorphic encryption. *Mod. Phys. Lett. A* **2021**, *36*, 2150263. [CrossRef]
15. Huang, X.; Zhang, W.; Zhang, S. Quantum multi-party private set intersection using single photons. *Phys. A Stat. Mech. Its Appl.* **2024**, *649*, 129974. [CrossRef]
16. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Chicago, IL, USA, 3–5 November 1982; p. 160.
17. Boudot, F.; Schoenmakers, B.; Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
18. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
19. Yang, Y.G.; Wen, Q.Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J. Phys. A Math. Theor.* **2009**, *42*, 055305. [CrossRef]
20. 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]
21. Lin, J.; Tseng, H.Y.; Hwang, T. Intercept–resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. *Opt. Commun.* **2011**, *284*, 2412–2414. [CrossRef]
22. Liu, W.; Wang, Y.B. Quantum private comparison based on GHZ entangled states. *Int. J. Theor. Phys.* **2012**, *51*, 3596–3604. [CrossRef]
23. 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]
24. Li, J.; Jia, L.; Zhou, H.F.; Zhang, T.-T. Secure quantum private comparison protocol based on the entanglement swapping between three-particle W-class state and bell state. *Int. J. Theor. Phys.* **2016**, *55*, 1710–1718. [CrossRef]
25. Gao, X.; Zhang, S.B.; Chang, Y.; Yang, F.; Zhang, Y. Cryptanalysis of the quantum private comparison protocol based on the entanglement swapping between three-particle W-class state and bell state. *Int. J. Theor. Phys.* **2018**, *57*, 1716–1722. [CrossRef]
26. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
27. Duan, M.-Y. Cryptanalysis and improvement of quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2021**, *60*, 195–199.
28. 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]
29. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
30. Jia, H.Y.; Wen, Q.Y.; Song, T.T.; Gao, F. Quantum protocol for millionaire problem. *Opt. Commun.* **2011**, *284*, 545–549. [CrossRef]
31. Lin, S.; Sun, Y.; Liu, X.F.; Yao, Z.-Q. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf. Process.* **2013**, *12*, 559–568. [CrossRef]
32. Guo, F.Z.; Gao, F.; Qin, S.J.; Zhang, J.; Wen, Q.Y. Quantum private comparison protocol based on entanglement swapping of-level Bell states. *Quantum Inf. Process.* **2013**, *12*, 2793–2802. [CrossRef]
33. Yu, C.H.; Guo, G.D.; Lin, S. Quantum private comparison with d-level single-particle states. *Phys. Scr.* **2013**, *88*, 065013. [CrossRef]
34. Xu, L.; Zhao, Z. High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom. *Eur. Phys. J. D* **2019**, *73*, 58. [CrossRef]
35. Ji, Z.; Fan, P.; Zhang, H.; Wang, H. Greenberger-Horne-Zeilinger-based quantum private comparison protocol with bit-flipping. *Phys. Scr.* **2020**, *96*, 015103. [CrossRef]
36. Wu, W.Q.; Zhao, Y.X. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 155. [CrossRef]
37. Hou, M.; Sun, S.Y.; Zhang, W. Quantum private comparison for the socialist millionaire problem. *Front. Phys.* **2024**, *12*, 1408446. [CrossRef]
38. Hou, M.; Wu, Y.; Zhang, S. New Quantum Private Comparison Using Four-Particle Cluster State. *Entropy* **2024**, *26*, 512. [CrossRef] [PubMed]
39. 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]
40. Huang, X.; Zhang, W.; Zhang, S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. *Phys. A Stat. Mech. Its Appl.* **2024**, *637*, 129614. [CrossRef]
41. Jain, N.; Stiller, B.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron.* **2014**, *21*, 168–177. [CrossRef]
42. Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. [CrossRef]