mathematics

IMPACT FACTOR 2.3

CITESCORE 4.0

Article

Efficient Quantum Private Comparison with Unitary Operations

Min Hou and Yue Wu

MDPI

https://doi.org/10.3390/math12223541

mathematics

Article

Efficient Quantum Private Comparison with Unitary Operations

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

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

Abstract: Quantum private comparison (QPC) is a crucial component of quantum multiparty computing (QMPC), allowing parties to compare their private inputs while ensuring that no sensitive information is disclosed. Many existing QPC protocols that utilize Bell states encounter efficiency challenges. In this paper, we present a novel and efficient QPC protocol that capitalizes on the distinct characteristics of Bell states to enable secure comparisons. Our method transforms private inputs into unitary operations on shared Bell states, which are then returned to a third party to obtain the comparison results. This approach enhances efficiency and decreases the reliance on complex quantum resources. A single Bell state can compare two classical bits, achieving a qubit efficiency of 100%. We illustrate the feasibility of the protocol through a simulation on the IBM Quantum Cloud Platform. The security analysis confirms that our protocol is resistant to both eavesdropping and attacks from participants.

Keywords: quantum private comparison (QPC); unitary operations; Bell states; security

MSC: 81P94; 81P65

1. Introduction

Secure multiparty computation (MPC), a cryptographic paradigm, allows multiple parties to collaboratively compute a function using their private inputs while maintaining the confidentiality of those inputs [1]. Recently, MPC has garnered significant attention due to its enhanced privacy protections and applicability across various domains. These include functions of secret-sharing [2,3], private set intersection [4,5], making private queries [6,7], and private comparison [8–10]. In this paper, we primarily concentrate on the development of protocols for private comparison. We aim to develop efficient and secure techniques that enable parties to compare their private data while keeping sensitive information confidential. This effort contributes to the wider domain of secure multiparty computation.

Private comparison protocols originate from the need to allow the parties to compare their private data without revealing the actual values to each other, which was first introduced in the millionaires' problem [11]. Boudot et al. [12] expanded the millionaires' problem to address the specific issue known as the socialist millionaires' problem, where two millionaires wish to determine if they have equal wealth without revealing their actual amounts. This problem has since attracted considerable interest in the cryptographic community, leading to various solutions that enhance privacy and security. In the context of designing private comparison protocols, Lo [13] highlighted a crucial limitation: securely evaluating a two-party computational function in a purely two-party setting is fundamentally impossible without compromising privacy. To overcome this challenge, the introduction of a semi-honest third party (TP) becomes essential. The TP assists the users in securely comparing their private data, acting as an intermediary that can facilitate the computation while ensuring that the individual inputs remain confidential.

check for updates

Citation: Hou, M.; Wu, Y. Efficient Quantum Private Comparison with Unitary Operations. *Mathematics* **2024**, *12*, 3541. https://doi.org/10.3390/math12223541

Academic Editor: João Nuno Prata

Received: 4 November 2024
Revised: 11 November 2024
Accepted: 12 November 2024
Published: 13 November 2024

The security of private comparison protocols hinges on unproven mathematical assumptions, making them vulnerable to threats posed by quantum computers, which leverage the principles of quantum mechanics for powerful parallel computation. Notably, the Shor algorithm [14] can factor large integers in polynomial time, rendering classical public-key cryptographic systems like RSA insecure against quantum attacks. Furthermore, the Grover algorithm [15] poses a significant threat to symmetric-key cryptography by allowing for faster search and function inversion, effectively halving the effective key length for symmetric algorithms. Therefore, quantum private comparison (QPC) came into being. It leverages quantum mechanics to provide enhanced security features, ensuring that sensitive information remains confidential during the comparison process.

The first quantum private comparison (QPC) protocol was introduced by Yang and Wen [16], who employed EPR pairs to transmit quantum information, alongside decoy photons and a one-way hash function to ensure security. Subsequently, Chen et al. [17] developed an efficient QPC protocol utilizing triplet entangled states, enhancing qubit efficiency by partitioning the secrets into multiple groups. Tseng et al. [18] took advantage of EPR pairs to facilitate comparisons, resulting in a more straightforward implementation and achieving 50% qubit efficiency. Lang et al. [19] introduced a QPC protocol that utilizes Bell states, also attaining 50% qubit efficiency. This protocol utilized quantum gates rather than classical exclusive-OR operations to perform the private calculations regarding the secrets, thereby improving security by minimizing reliance on classical computational methods. Hou et al. [20] employed rotation operations and Bell states for comparison, achieving 50% qubit efficiency. In their approach, two participants encoded their inputs into the angles of the rotation operations applied to the Bell states. Huang et al. [21] developed a QPC protocol utilizing entanglement swapping among three Bell states, also with 50% qubit efficiency. Similarly, Hou and Wu [22] encoded their private inputs as bit flip and phase shift operators applied to shared Bell states, also attaining 50% qubit efficiency. In contrast, Huang et al. [23] utilized GHZ-type states for private comparisons, where each could compare two-bit information, which led to a qubit efficiency of 67%. Moreover, other quantum states have been explored as information carriers in the design of QPC protocols, including multiple-qubit entangled states [24–28], multiple-qubit cluster states [29–32], and d-dimensional quantum states [33–42]. However, the QPC protocols that utilize easily implementable quantum states—such as single photon, Bell state, and GHZ state—facilitate higher practical implementation compared to those using d-dimensional quantum states. Despite this advantage, protocols based on single photons, Bell states, and GHZ states often face challenges related to lower qubit efficiency, with many achieving only 50% efficiency.

To tackle this challenge, we put forward an efficient QPC protocol that takes advantage of the distinctive characteristics of Bell states to enable secure comparisons. Our approach involves transforming private inputs into unitary operations applied to shared Bell states. After these operations, the states are returned to a third party, who can then obtain the comparison results. The primary contributions of this paper include the following:

(1) We introduce an efficient QPC protocol that enables two participants to compare their secrets by encoding their inputs as unitary operations applied to shared Bell states.

(2) Our protocol employs Bell states and unitary operations as fundamental components, which are easier to implement than QPC protocols based on d-dimensional quantum states. We illustrate the feasibility of the protocol through a simulation on the IBM Quantum Cloud Platform.

(3) Our protocol achieves 100% qubit efficiency since a single Bell state can compare two bits of classical information.

(4) A comprehensive security analysis verifies that our protocol is resilient against eavesdropping and participant attacks, ensuring robust protection of private information.

The remaining sections are organized as follows: Section 2 introduces the unitary operations. Sections 3 and 4 present the detailed steps of the proposed QPC protocol and its correctness, respectively. Section 5 conducts a simulation, while Section 6 discusses the security analysis of the protocol. Section 7 provides an efficiency analysis and comparison. Finally, Section 8 concludes with a summary of our contributions.

2. Unitary Operations

The bit flip and phase shift operations are

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

The two operations described above are unitary operations as they satisfy the conditions $XX^{\dagger} = XX = I$ and $ZZ^{\dagger} = ZZ = I$, where I represents the 2×2 identity matrix.

The four Bell states can be expressed as follows:

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{2}$$

$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \tag{3}$$

$$|\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \tag{4}$$

$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \tag{5}$$

We applied the operation $X^a Z^b$(where $a, b \in \{0,1\}$) to the first qubit of the four Bell states; the resulting states are presented in Table 1.

Table 1. The resulting Bell states.

Bell States	X^0Z^0	X^1Z^0	X^0Z^1	X^1Z^1
$\|\psi_{00}\rangle$	$\|\psi_{00}\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{01}\rangle$	$\|\psi_{11}\rangle$
$\|\psi_{01}\rangle$	$\|\psi_{01}\rangle$	$\|\psi_{11}\rangle$	$\|\psi_{00}\rangle$	$\|\psi_{10}\rangle$
$\|\psi_{10}\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{00}\rangle$	$\|\psi_{11}\rangle$	$\|\psi_{01}\rangle$
$\|\psi_{11}\rangle$	$\|\psi_{11}\rangle$	$\|\psi_{01}\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{00}\rangle$

The Bell states in Table 1 do not include the global phase factor, as measurements performed using the Bell basis do not affect the measurement outcomes.

3. The Proposed QPC Protocol

The goal of the QPC protocol was to determine whether the secrets X and Y held by two users, Alice and Bob, were equal. They sought assistance from a semi-trusted third party (TP), who acted as an intermediary that needed to adhere to the protocol steps and could not collude with the participants, who were considered honest but curious. The binary representations of X and Y could be represented as $X = (x_{L-1}, x_{L-2}, \cdots, x_1, x_0)$ and $Y = (y_{L-1}, y_{L-2}, \cdots, y_1, y_0)$, where $x_i, y_i \in \{0,1\}$ for $i = 0, 1, \cdots, L-1$. The protocol assumed a quantum channel that was free from noise and loss, while the classical channel was authenticated during transmission.

The specific steps are outlined as follows:

Step 1. Alice and Bob divide their secret integers X and Y into $\lceil L/2 \rceil$ groups, respectively, with each group containing two-bit classical information. If $L mod 2 = 1$, they add a 0 to the last group. Consequently, we can rewrite X and Y as $X' = \left(x'_{\lceil L/2 \rceil - 1}, x'_{\lceil L/2 \rceil - 2}, \cdots, x'_1, x'_0\right)$ and $Y' = \left(y'_{\lceil L/2 \rceil - 1}, y'_{\lceil L/2 \rceil - 2}, \cdots, y'_1, y'_0\right)$, respectively, where $x'_j = x_{2j+1}x_{2j}$ and $y'_j = y_{2j+1}y_{2j}$ for $j = 0, 1, \cdots, \lceil L/2 \rceil - 2, \lceil L/2 \rceil - 1$.

Step 2. TP prepares $\lceil L/2 \rceil$ Bell states and takes the first and second qubits of all Bell states to form two ordered quantum sequences, S_{TA} and S_T. To detecting eavesdropping, TP prepares a set of decoy states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into S_{TA} at random positions to generate a sequence S'_{TA}, which is sent to Alice via a quantum channel. The sequence S_T is kept by TP.

Step 3. Upon receiving S'_{TA}, Alice informs TP that she has received the sequence. TP then announces the positions of the decoy states and the measurement basis to Alice. Alice measures the corresponding qubits using the correct basis and returns the measurement results to TP, who compares the consistency of the measurement results with the prepared decoy states to determine whether the quantum channel has been compromised by eavesdropping. TP calculates the error rate; if this rate falls below a predefined threshold, the quantum channel is deemed secure, allowing the protocol to advance to the next step. If the error rate exceeds the threshold, the protocol is terminated and restarted.

Step 4. Alice discards all decoy states from S'_{TA} to cover S_{TA} and performs the following operations:

(1) She applies $U_{x'_j} = X^{x_{2j+1}} Z^{x_{2j}}$ on each j-th qubit in S_{TA} to produce a transformed sequence denoted as S_A.
(2) She generates her own secret key $K_A = \left(a_{\lceil L/2 \rceil -1}, a_{\lceil L/2 \rceil -2}, \cdots, a_1, a_0\right)$, where $a_j \in \{00, 01, 10, 11\}$ for $j = 0, 1, \cdots, \lceil L/2 \rceil - 2, \lceil L/2 \rceil - 1$.
(3) She performs $U_{a_j}\left(\text{where } U_{a_j} \in \left\{X^0Z^0, X^0Z^1, X^1Z^0, X^1Z^1\right\} \text{ correspond to } a_j\right)$ on each j-th qubit in S_A to produce a transformed sequence denoted as S'_A.
(4) She prepares decoy states chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into S'_A to create a sequence S''_A.
(5) She sends S''_A to Bob via a quantum channel.

Step 5. Upon receiving S'_A, Bob interacts with Alice to detect eavesdropping in the quantum channel in the same manner as TP and Alice did. If the quantum channel is secure, Bob discards all decoy states from S''_A to cover S'_A and performs the following operations:

(1) He applies $U_{y'_j} = X^{y_{2j+1}} Z^{y_{2j}}$ on each j-th qubit in S'_A to produce a transformed sequence denoted as S_B.
(2) He generates his own secret key $K_B = \left(b_{\lceil L/2 \rceil -1}, b_{\lceil L/2 \rceil -2}, \cdots, b_1, b_0\right)$, where $b_j \in \{00, 01, 10, 11\}$ for $j = 0, 1, \cdots, \lceil L/2 \rceil - 2, \lceil L/2 \rceil - 1$.
(3) He performs $U_{b_j}\left(\text{where } U_{b_j} \in \left\{X^0Z^0, X^0Z^1, X^1Z^0, X^1Z^1\right\} \text{ correspond to } b_j\right)$ on each j-th qubit in S_B to produce a transformed sequence denoted as S'_B.
(4) He prepares decoy states chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into S'_B to create a sequence S''_B.
(5) He sends S''_B to TP through a quantum channel.

Step 6. TP detects eavesdropping by interacting with Bob upon receiving S''_B, similar to the process in Step 3. Alice and Bob then announce their respective secret keys K_A and K_B to TP.

Step 7. TP discards all decoy states from S''_B to cover S'_B, and performs the following operations:

(1) TP applies U_{a_j} and U_{b_j} on each j-th qubit in S'_B to produce a transformed sequence denoted as S_{TAB}.
(2) TP performs a Bell basis measurement on the qubits in S_{TAB} and S_T to obtain the measurement results.
(3) TP compares the measurement results with the prepared Bell states to determine whether $X = Y$. If they are identical, $X = Y$; otherwise, $X \neq Y$.
(4) TP conveys the outcomes of the comparison to Alice and Bob.

4. Correctness

In our designed protocol, decoy states are ignored when demonstrating correctness, as they are only used for eavesdropping detection. When performing $U_{x'_j}$ on each j-th qubit in S_{TA}, the resulting sequence S_A can be given by

$$S_A = \left(U_{x'_j}\right) S_{TA} = (X^{x_{2j+1}} Z^{x_{2j}}) S_{TA} \tag{6}$$

When performing $U_{a_j}\left(\text{where } U_{a_j} \in \left\{X^0Z^0, X^0Z^1, X^1Z^0, X^1Z^1\right\} \text{ correspond to } a_j\right)$ on each j-th qubit in S_A, the resulting sequence $S_A^{'}$ can be written as

$$S'_A = \left(U_{a_j}\right) S_A = \left(U_{a_j} X^{x_{2j+1}} Z^{x_{2j}}\right) S_{TA} \tag{7}$$

When performing $U_{y'_j}$ on each j-th qubit in S'_A, the resulting sequence S_B can be given by

$$S_B = \left(U_{y'_j}\right) S'_A = \left(X^{y_{2j+1}} Z^{y_{2j}} U_{a_j} X^{x_{2j+1}} Z^{x_{2j}}\right) S_{TA} \tag{8}$$

When performing $U_{b_j}\left(\text{where } U_{b_j} \in \left\{X^0Z^0, X^0Z^1, X^1Z^0, X^1Z^1\right\} \text{ correspond to } b_j\right)$ on each j-th qubit in S_B, the resulting sequence $S_B^{'}$ can be given by

$$S'_B = \left(U_{b_j}\right) S'_A = \left(U_{b_j} X^{y_{2j+1}} Z^{y_{2j}} U_{a_j} X^{x_{2j+1}} Z^{x_{2j}}\right) S_{TA} \tag{9}$$

When performing U_{a_j} and U_{b_j} on each j-th qubit in S'_B, the resulting sequence S_{TAB} can be given by

$$S_{TAB} = \left(U_{b_j} U_{a_j}\right) S'_B = \left(U_{b_j} U_{a_j} U_{b_j} X^{y_{2j+1}} Z^{y_{2j}} U_{a_j} X^{x_{2j+1}} Z^{x_{2j}}\right) S_{TA} = (X^{y_{2j+1}} Z^{y_{2j}} X^{x_{2j+1}} Z^{x_{2j}}) S_{TA} \tag{10}$$

From Equation (10), we can deduce that the initial sequence S_{TA} remains unchanged if and only if both the 2j-th and (2j + 1)-th bits in secrets X and Y are identical. Consequently, TP can ascertain the comparison results by juxtaposing the prepared Bell states with the measurement results obtained from performing a Bell basis measurement on the qubits in S_{TAB} and S_T.

5. Simulation

In this section, we illustrate the feasibility of the protocol through a simulation on the IBM Quantum Cloud Platform.

Consider the case in which Alice possesses a secret $X = 45$ and Bob has a secret $Y = 49$. The binary representations of X and Y are $X = (x_5,\ x_4, \cdots, x_1, x_0) = (10, 11, 01)$ and $Y = (y_5,\ y_4, \cdots, y_1, y_0) = (11, 00, 01)$, respectively. When dividing X and Y into three groups, we obtain $X' = (x'_2, x'_1, x'_0) = (10, 11, 01)$ and $Y' = (y'_2, , y'_1, y'_0) = (11, 00, 01)$. We assume that the initially prepared three Bell states are $S_A = \{|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{10}\rangle\}$ and the secret keys are $K_A = (a_2, a_1, a_0) = (11, 00, 11)$ and $K_B = (b_2, b_1, b_0) = (10, 11, 10)$. When performing a Bell measurement, equivalent to applying the CNOT and Hadamard gates once on the three initially prepared Bell states, the measurement results correspond to 00, 01, and 10. Additionally, when performing a Bell measurement on $|\psi_{11}\rangle$, the measurement result corresponds to 11. Without considering eavesdropping detection, the quantum circuit for comparing X and Y, along with the measurement results obtained from executing this quantum circuit in the IBM Quantum Experience, are presented in Figures 1 and 2, respectively.

Figure 1. Quantum circuit for comparing $X = 45$ and $Y = 49$.

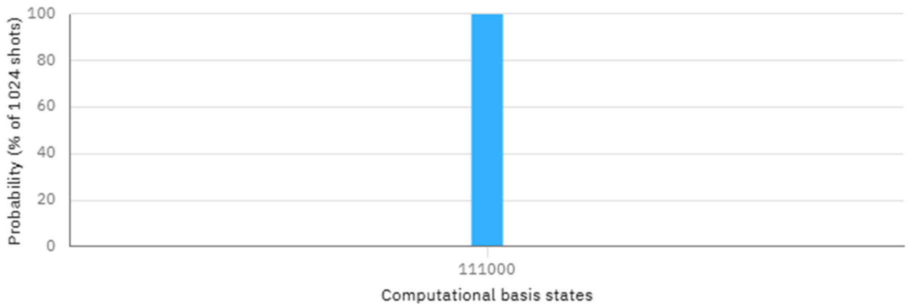

Figure 2. The measurement result corresponds to Figure 1.

From Figure 2, we observe that the measurement outcomes in the computational basis states were 00, 10, 11, which corresponded to $|\psi_{00}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle$. This indicated that the final measurement results differed from the prepared Bell states, leading to the conclusion that $X \neq Y$.

6. Security Analysis

In this section, we present a comprehensive security analysis that verifies our protocol's resilience against eavesdropping and participant attacks, providing strong safeguards for private information.

6.1. External Attacks

External attacks refer to any attempts by an eavesdropper, Eve, to uncover the secrets of Alice and Bob by intercepting or eavesdropping on the quantum channel during the transmission of quantum sequences between the participating entities. However, the proposed protocol employs decoy photon technology, which is designed to detect eavesdropping and provides unconditional security. This technology has been proven effective in resisting external attacks, primarily including intercept–resend and entangle–measure attacks. We demonstrate that our protocol can effectively counter both intercept–resend and entangle–measure attacks as follows.

6.1.1. Intercept–Resend Attack

The intercept–resend attack involves Eve intercepting the quantum sequence during transmission, measuring it using her guessed Z-basis or X-basis, generating a new sequence where each state corresponds to the measurement results, and then sending this new sequence to the original receiver [43–45]. If a quantum state remains in the state $|1\rangle$, measuring it with the Z-basis yields a measurement result of $|1\rangle$, resulting in a new state that is identical to the initial state, thereby introducing no error. Conversely, when measuring with the X-basis, the measurement result can be either $|+\rangle$ or $|-\rangle$, each with a probability of 50%, leading to a new state that is not identical to the initial state. This means that there is a 50% probability of introducing no error and a 50% probability of introducing an error. Consequently, for a randomly chosen decoy state, the errors introduced by performing measurements with the guessed basis during eavesdropping detection are calculated as $\left(1 - \frac{1}{2} \times 1 - \frac{1}{2} \times \frac{1}{2}\right) = \frac{1}{4}$. Given this, the probability that d newly generated decoy states will be detected is $1-\left(\frac{3}{4}\right)^d$. When d is sufficiently large, the detection rate of the introduced decoy states approaches 1, which means that Eve's eavesdropping behavior will be detected, leading to the termination of the protocol and a return to the first step for re-execution. Therefore, Alice's and Bob's secrets remain confidential from Eve, even if she attempts the intercept–resend attack.

6.1.2. Entangle–Measure Attack

The entangle–measure attack involves Eve first intercepting the quantum sequence during transmission and then entangling her auxiliary state sequence $E=\{|E_0\rangle, |E_1\rangle, \cdots, |E_{n-1}\rangle\}$ with the intercepted states using specific unitary operations. The unitary operations performed on the intercepted states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and the auxiliary state can be expressed as follows:

$$U|0\rangle|E_i\rangle = a_0|0\rangle|e_{00}\rangle + b_0|1\rangle|e_{01}\rangle \tag{11}$$

$$U|1\rangle|E_i\rangle = a_1|1\rangle|e_{10}\rangle + b_1|1\rangle|e_{11}\rangle \tag{12}$$

$$\begin{aligned} U|+\rangle|E_i\rangle &= \tfrac{1}{2}|+\rangle(a_0|e_{00}\rangle + b_0|e_{01}\rangle + a_1|e_{10}\rangle + b_1|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(a_0|e_{00}\rangle - b_0|e_{01}\rangle + a_1|e_{10}\rangle - b_1|e_{11}\rangle) \end{aligned} \tag{13}$$

$$\begin{aligned} U|-\rangle|E_i\rangle &= \tfrac{1}{2}|+\rangle(a_0|e_{00}\rangle + b_0|e_{01}\rangle - a_1|e_{10}\rangle - b_1|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(a_0|e_{00}\rangle - b_0|e_{01}\rangle - a_1|e_{10}\rangle + b_1|e_{11}\rangle) \end{aligned} \tag{14}$$

The parameters a_0, b_0, a_1, and b_1 should satisfy

$$|a_0|^2 + |b_0|^2 = 1 \tag{15}$$

$$|a_1|^2 + |b_1|^2 = 1 \tag{16}$$

During the transmission of quantum sequences between two parties, eavesdropping detection is always a consideration. If the prepared decoy state is chosen to be $|0\rangle$ or $|1\rangle$, and Eve is able to bypass detection, she must set $a_1 = b_0 = 0$. Similarly, if the prepared decoy state is chosen to be $|+\rangle$ or $|-\rangle$, and Eve can bypass detection, the following condition must be satisfied:

$$a_0|e_{00}\rangle - b_0|e_{01}\rangle + a_1|e_{10}\rangle - b_1|e_{11}\rangle = \mathbf{0} \tag{17}$$

$$a_0|e_{00}\rangle + b_0|e_{01}\rangle - a_1|e_{10}\rangle - b_1|e_{11}\rangle = \mathbf{0} \tag{18}$$

Combining $a_1 = b_0 = 0$, we can deduce that $a_0|e_{00}\rangle = b_1|e_{11}\rangle$. Substituting this result into Equations (11)–(14), we obtain

$$U|0\rangle|E_i\rangle = a_0|0\rangle|e_{00}\rangle \tag{19}$$

$$U|1\rangle|E_i\rangle = b_1|1\rangle|e_{11}\rangle = a_0|0\rangle|e_{00}\rangle \tag{20}$$

$$U|+\rangle|E_i\rangle = \frac{1}{2}|+\rangle(a_0|e_{00}\rangle + 0 + 0 + b_1|e_{11}\rangle) = a_0|+\rangle|e_{00}\rangle \tag{21}$$

$$U|-\rangle|E_i\rangle = \frac{1}{2}|-\rangle(a_0|e_{00}\rangle - 0 - 0 + b_1|e_{11}\rangle) = a_0|-\rangle|e_{00}\rangle \tag{22}$$

From Equations (19)–(22), we can conclude that the auxiliary states prepared by Eve do not entangle with the intercepted states. Therefore, performing the entangle–measure attack cannot succeed in acquiring the private information of Alice and Bob.

6.1.3. Trojan Horse Attacks

Since the proposed protocol utilizes a bidirectional quantum channel for transmitting the quantum sequence, it is inevitably susceptible to Trojan horse attacks, which include invisible photon attacks and delay photon attacks [46]. Each participant can affix a filter that allows only wavelengths close to the operating wavelength to resist the invisible photon attack, while photon number splitting can be used to counter the delay photon attack. Upon detecting these attacks, the discoverer will restart the protocol.

6.2. Participant Attacks

Participants can receive immediate results regarding the encoded quantum sequence, which poses a higher security risk for obtaining the private information of other participants compared to outsider attacks. A security analysis of participant attacks is presented below.

6.2.1. TP's Attacks

In our protocol, TP is regarded as semi-honest. This indicates that while TP cannot conspire with Alice and Bob, they may still try to access their confidential information. If TP seeks to gather insights into Alice's or Bob's private data, they might execute an intercept attack on the quantum sequence being transmitted, akin to the methods used by external attackers. However, this activity will be identified during the eavesdropping detection phase without knowing the exact locations and associated measurement bases of the decoy states. Additionally, while preparing the quantum sequences used to facilitate private comparison and knowing the secret keys K_A and K_B, TP may exploit this information to try to learn additional details about the participants' private information. It is evident that TP can establish whether a single bit of Alice's and Bob's secrets is equal. However, TP cannot completely determine their secrets, as identical results may emerge from two distinct scenarios. Consequently, our protocol remains secure against attacks from TP.

6.2.2. Alice's Attacks

Alice may perform an intercept–resend attack on S''_B. By utilizing the information regarding the locations of the inserted decoy particles that Bob discloses during the eavesdropping detection phase, Alice is able to recover S'_B, even though this attack will ultimately be detected. Knowing the sequence S'_A, Alice can deduce the encoding operations performed on S'_A. However, in our protocol, when Bob receives the sequence S'_A sent from Alice, he applies $U_{y'_j} = X^{y_{2j+1}} Z^{y_{2j}}$ corresponding to his secrets, followed by U_{b_j} corresponding to his own secret key K_B on S'_A. For Alice, she cannot know the secret key K_B since the eavesdropping detection has not been confirmed to have passed, meaning that the secret key K_B will not be announced. Therefore, Alice cannot obtain Bob's private information.

6.2.3. Bob's Attack

When Bob receives S''_A and discards all decoy states to recover S'_A, he can compare the states in S'_A and S_{TA} to deduce the operations performed by Alice, thus gaining access to her private information according to the encoding rules. However, Bob is unable to accomplish this. On one hand, TP does not reveal the prepared Bell states to anyone due to their semi-honesty. If Bob intends to learn S_{TA}, he would need to intercept S'_{TA} in the same manner as external attackers, which would prevent him from passing the eavesdropping detection, resulting in his inability to obtain S_{TA}. Additionally, the sequence S'_A is encoded with X' and K_A. Even if K_A is announced, Bob still cannot deduce X' due to his lack of knowledge regarding the secret sequence S_{TA}. Therefore, Bob attempts to ascertain Alice's secret would ultimately be unsuccessful.

7. Efficiency Analysis and Comparison

The qubit efficiency serves as a crucial metric for assessing the utilization rate of qubits, which can be defined as follows:

$$\eta_e = \frac{\eta_c}{\eta_t} \tag{23}$$

where η_c represents the total number of classical bits compared, while η_t denotes the total number of qubits used, excluding those allocated for eavesdropping detection, which is treated as a separate process within the quantum communication protocol. In our approach,

L Bell states act as the carriers of quantum information to enable private comparisons, facilitating the comparison of $2L$ classical bits. This results in 100% qubit efficiency.

Table 2 provides a comparison between our protocol and several existing QPC protocols. While protocols discussed in Refs. [16–22] and ours utilize quantum resources that are easier to prepare, exhibiting better practicality, our protocol achieves 100% qubit efficiency. Additionally, our protocol does not require a quantum key distribution (QKD) [47–50] protocol for sharing a secret key, unlike the methods described in Refs. [20–22]. Unlike Ref. [19], which utilizes entanglement swapping to achieve private comparison, our protocol is easier to implement using unitary operations.

Table 2. Comparison between our protocol and several existing QPC protocols.

Protocol	Quantum Resource	Unitary Operation	Entanglement Swapping	Quantum Measurement	QKD	Qubit Efficiency
Ref. [16]	EPR pairs	Yes	No	Bell-basis	No	25%
Ref. [17]	GHZ state	Yes	No	Single-particle	No	33%
Ref. [18]	EPR pairs	No	No	Single-particle	No	50%
Ref. [19]	Bell states	Yes	No	$\{\|0\rangle, \|1\rangle\}$ basis	No	50%
Ref. [20]	Bell states	Yes	No	Bell-basis	Yes	50%
Ref. [21]	Bell state	No	Yes	GHZ-basis	Yes	50%
Ref. [22]	Bell states	Yes	No	Bell-basis	Yes	50%
Ours	Bell states	Yes	No	Bell-basis	No	100%

8. Conclusions

In this paper, we presented a quantum private comparison protocol that harnesses the distinctive properties of Bell states to facilitate secure comparisons. Users encode their private information using bit flip and phase shift operators and utilize a circular transmission mode to send the quantum sequence, achieving 100% qubit efficiency. We demonstrated the protocol's feasibility through a simulation conducted on the IBM Quantum Cloud Platform. Additionally, the security analysis verified that our method is resilient against both eavesdropping and attacks from participants. Compared to existing QPC protocols, our protocol demonstrates enhanced performance in terms of both qubit efficiency and practical implementation by employing easier-to-implement Bell states, unitary operations, and Bell measurements as fundamental components.

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

Funding: This research was funded by the Open Fund of Network and Data Security Key Laboratorg of Sichuan Province (Grant no. NDS2024-1), the Opening Foundation of State Key Laboratory of Cognitive Intelligence iFLYTEK (grant no. COGOS-2024HE03), and the Gongga Plan for the "Double World-class Project".

Data Availability Statement: Data are contained within the article.

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

References

1. Cramer, R.; Damgård, I.B. *Secure Multiparty Computation*; Cambridge University Press: Cambridge, UK, 2015.
2. Beimel, A. Secret-sharing schemes: A survey. In Proceedings of the International Conference on Coding and Cryptology, Qingdao, China, 30 May–3 June 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 11–46.
3. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
4. Morales, D.; Agudo, I.; Lopez, J. Private set intersection: A systematic literature review. *Comput. Sci. Rev.* **2023**, *49*, 100567. [CrossRef]
5. 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]

6. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef]
7. Gao, F.; Qin, S.; Huang, W.; Wen, Q. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 70301. [CrossRef]
8. Sutradhar, K.; Om, H. A Privacy-preserving comparison protocol. *IEEE Trans. Comput.* **2022**, *72*, 1815–1821. [CrossRef]
9. 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]
10. Huang, X.; Zhang, S.; Xia, J. Efficient Quantum Private Comparison Using Locally Indistinguishable Orthogonal Product States. In Proceedings of the International Conference on Artificial Intelligence and Security, Qinghai, China, 15–20 July 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 260–273.
11. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Washington, DC, USA, 3–5 November 1982; p. 160.
12. Boudot, F.; Schoenmakers, B.; Traoré, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
13. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
14. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
15. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325–328. [CrossRef]
16. 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]
17. 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]
18. Tseng, H.-Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **2011**, *11*, 373–384. [CrossRef]
19. Lang, Y.-F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
20. Hou, M.; Sun, S.-Y.; Zhang, W. Quantum private comparison for the socialist millionaire problem. *Front. Phys.* **2024**, *12*, 1408446. [CrossRef]
21. 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]
22. Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. [CrossRef]
23. Huang, X.; Zhang, S.-B.; Cheng, W. Quantum Private Comparison Based on GHZ-type States. In Proceedings of the 2021 IEEE AFRICON, Arusha, Tanzania, 13–15 September 2021; IEEE: New York, NY, USA, 2021; pp. 1–4.
24. 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]
25. 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]
26. 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]
27. 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]
28. Reimer, C.; Kues, M.; Roztocki, P.; Wetzel, B.; Grazioso, F.; Little, B.E.; Chu, S.T.; Johnston, T.; Bromberg, Y.; Caspani, L.; et al. Generation of multiphoton entangled quantum states by means of integrated frequency combs. *Science* **2016**, *351*, 1176–1180. [CrossRef] [PubMed]
29. Hou, M.; Wu, Y.; Zhang, S. New Quantum Private Comparison Using Four-Particle Cluster State. *Entropy* **2024**, *26*, 512. [CrossRef]
30. Sun, Z.; Long, D. Quantum private comparison protocol based on cluster states. *Int. J. Theor. Phys.* **2013**, *52*, 212–218. [CrossRef]
31. 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]
32. Chang, Y.; Zhang, W.-B.; Zhang, S.-B.; Wang, H.-C.; Yan, L.-L.; Han, G.-H.; Sheng, Z.-W.; Huang, Y.-Y.; Suo, W.; Xiong, J.-X. Quantum private comparison of equality based on five-particle cluster state. *Commun. Theor. Phys.* **2016**, *66*, 621–628. [CrossRef]
33. Zhao-Xu, J.; Tian-Yu, Y. Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states. *Quantum Inf. Process.* **2017**, *16*, 177. [CrossRef]
34. Lin, S.; Sun, Y.; Liu, X.-F.; Yao, Z.-Q. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf. Process.* **2012**, *12*, 559–568. [CrossRef]
35. 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]
36. Wu, W.; Zhao, Y. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 155. [CrossRef]
37. Cao, H.; Ma, W.; Lü, L.; He, Y.; Liu, G. Multi-party quantum privacy comparison of size based on d-level GHZ states. *Quantum Inf. Process.* **2019**, *18*, 287. [CrossRef]

38. Zhou, N.-R.; Xu, Q.-D.; Du, N.-S.; Gong, L.-H. Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. *Quantum Inf. Process.* **2021**, *20*, 124. [CrossRef]
39. Wang, B.; Gong, L.-H.; Liu, S.-Q. Multi-party quantum private size comparison protocol with d-dimensional Bell states. *Front. Phys.* **2022**, *10*, 981376. [CrossRef]
40. Ye, T.Y.; Lian, J.Y. A novel multi-party semiquantum private comparison protocol of size relationship with d-dimensional single-particle states. *Phys. A Stat. Mech. Its Appl.* **2023**, *611*, 128424. [CrossRef]
41. Kues, M.; Reimer, C.; Roztocki, P.; Cortés, L.R.; Sciara, S.; Wetzel, B.; Zhang, Y.; Cino, A.; Chu, S.T.; Little, B.E.; et al. On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature* **2017**, *546*, 622–626. [CrossRef]
42. Reimer, C.; Sciara, S.; Roztocki, P.; Islam, M.; Cortés, L.R.; Zhang, Y.; Fischer, B.; Loranger, S.; Kashyap, R.; Cino, A.; et al. High-dimensional one-way quantum processing implemented on d-level cluster states. *Nat. Phys.* **2018**, *15*, 148–153. [CrossRef]
43. 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]
44. 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]
45. 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]
46. 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]
47. Mower, J.; Zhang, Z.; Desjardins, P.; Lee, C.; Shapiro, J.H.; Englund, D. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **2013**, *87*, 062322. [CrossRef]
48. Zhong, T.; Zhou, H.; Horansky, R.D.; Lee, C.; Verma, V.B.; Lita, A.E.; Restelli, A.; Bienfang, J.C.; Mirin, R.P.; Gerrits, T.; et al. Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding. *New J. Phys.* **2015**, *17*, 022002. [CrossRef]
49. Yang, S.; Sarihan, M.C.; Chang, K.-C.; Wong, C.W.; Dolecek, L. Efficient information reconciliation for energy-time entanglement quantum key distribution. In Proceedings of the 2019 53rd Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 3–6 November 2019; IEEE: New York, NY, USA, 2019; pp. 1364–1368.
50. Boutros, J.J.; Soljanin, E. Time-entanglement QKD: Secret key rates and information reconciliation Coding. *IEEE Trans. Commun.* **2023**, *71*, 7174–7188. [CrossRef]