axioms

IMPACT FACTOR 1.6

Article

# Two-Party Quantum Private Comparison with Pauli Operators

Min Hou, Yue Wu and Shibin Zhang

Special Issue
Recent Advances in Quantum Mechanics and Mathematical Physics

Edited by
Prof. Dr. Espen Gaarder Haug

MDPI

https://doi.org/10.3390/axioms14080549

*axioms*

MDPI

*Article*

# Two-Party Quantum Private Comparison with Pauli Operators

**Min Hou [1,2,3], Yue Wu [1] and Shibin Zhang [4,5,*]**

[1] School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China; houmin@scujj.edu.cn (M.H.); ywu@uestc.edu.cn (Y.W.)
[2] Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China
[3] State Key Laboratory of Cognitive Intelligence, Hefei 230088, China
[4] College of Artificial Intelligence (CUIT Shuangliu Industrial College), Chengdu University of Information Technology, Chengdu 610225, China
[5] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu 610225, China
* Correspondence: cuitzsb@cuit.edu.cn

**Abstract**

Quantum private comparison (QPC) is a quantum cryptographic protocol designed to enable two mutually distrustful parties to securely compare sensitive data without disclosing their private information to each other or any external entities. This study proposes a novel QPC protocol that leverages Bell states to ensure data privacy, utilizing the fundamental principles of quantum mechanics. Within this framework, two participants, each possessing a secret integer, encode the binary representation of their values using Pauli-X and Pauli-Z operators applied to quantum states transmitted from a semi-honest third party (TP). The TP, which is bound to protocol compliance and prohibited from colluding with either participant, measures the received sequences to determine the comparison result without accessing the participants' original inputs. Theoretical analyses and simulations validate the protocol's strong security, high efficiency, and practical feasibility in quantum computing environments. An advantage of the proposed protocol lies in its optimized utilization of Bell states, which enhances qubit efficiency and experimental practicality. Moreover, the proposed protocol outperforms several existing Bell-state-based QPC schemes in terms of efficiency.

**Keywords:** quantum private comparison (QPC); Pauli-X and Pauli-Z operators; semi-honest third party (TP); Bell states; quantum cryptographic protocol

**MSC:** 81P94; 81P65



Academic Editor: João Nuno Prata

Received: 10 June 2025
Revised: 8 July 2025
Accepted: 18 July 2025
Published: 22 July 2025

**Citation:** Hou, M.; Wu, Y.; Zhang, S. Two-Party Quantum Private Comparison with Pauli Operators. *Axioms* **2025**, *14*, 549. https://doi.org/10.3390/axioms14080549



## 1. Introduction

Secure multiparty computation (MPC) is a cryptographic technique, enabling multiple mutually distrustful parties to collaboratively compute a function over their private inputs while ensuring that no party accesses the confidential data of others [1]. Private comparison, an important branch of MPC, originated from Yao's millionaire problem [2], in which two millionaires meeting on the street desire to ascertain who has greater wealth without revealing their actual financial status to one another. Inspired by the millionaire problem, Boudot et al. [3] introduced a variation called the socialist millionaire problem, where two millionaires determine whether their wealth is equal without disclosing the exact amounts. Thus, solving the millionaire problem (designing privacy comparison protocols) has become a focal point in both classical and quantum cryptography fields.

Lo [4] pointed out that the inherent impossibility of securely evaluating a two-party function without compromising privacy in a purely bilateral framework is a critical challenge when designing privacy comparison protocols. To address this challenge, researchers have proposed incorporating a semi-honest third party (TP). Acting as a semi-trusted intermediary, the TP facilitates the secure comparison of private inputs but cannot collude with any participating parties.

The security of classical cryptographic protocols, regardless of those for privacy comparison and others, primarily rely on computationally hard mathematical problems such as integer factorization and discrete logarithms, which cannot be efficiently solved using classical computational resources under current conditions. Unfortunately, the emergence of quantum algorithms implemented on quantum computing platforms presents a substantial challenge to the security of classical cryptographic protocols. For example, Shor algorithm [5] leverages the parallelism of quantum computing and the superposition property of quantum states to reduce the complexity of solving these hard mathematical problems from exponential scale in classical computers to polynomial time. Consequently, once quantum computing matures sufficiently, existing cryptographic systems may become vulnerable. It is imperative to develop quantum-resistance protocols that are resilient to threats posed by quantum algorithms.

In response, researchers have investigated quantum-resistance protocols that integrate classical and quantum mechanics. These include quantum secret sharing [6–8], quantum key agreement [9–11], quantum secure direct communication [12–15], quantum private set intersection [16,17] and quantum secure multiparty computation (QMPC) [18]. The security of these quantum-resistance protocols is based on the principles of quantum mechanics, thereby resisting threats from quantum algorithms.

Quantum private comparison (QPC), a crucial branch of QMPC, enables parties to compare their confidential inputs without revealing each other's confidential data. In 2009, Yang and Wen [19] proposed the first QPC protocol, which utilized decoy photons and a one-way hash function to ensure security and confidentiality during the comparison process. Subsequent advancements by Tseng et al. [20] introduced a Bell-state-based QPC protocol that achieves a qubit efficiency of 50% by utilizing the two-particle entanglement correlation of Bell states. However, this protocol is vulnerable to attacks from the TP attempting to steal participants' private inputs by exploiting fake Bell states. To enhance its security, two feasible solutions are proposed in Ref. [21]. Lang [22] designed the QPC protocol that utilizes the quantum CNOT gate instead of classical exclusive-OR operations to facilitate comparison, but it cannot prevent the disturbance attack implemented by an outsider eavesdropper and the TP's measuring attack [23]. Huang et al. [24] designed the protocol by utilizing the entanglement swapping among three Bell states. Although it can compare three bits in each round, it is difficult to implement with the current technologies due to the effects of decoherence and environmental noise. Lang et al. [25] developed the protocol using a single Bell state, reducing the states generation switching costs but lowering qubit efficiency to 16.67%. Hou et al. [26] developed a protocol that encodes private inputs into Bell states using rotation operations, achieving a qubit efficiency of 25%. Similarly, Hou and Wu [27] employed a comparable method to encode private inputs into Bell states using unitary operations.

Additionally, various quantum states have been explored as carriers of quantum information for transmitting private data. These states include single photons [28–33], multi-qubit entangled states [34–39], cluster states [40,41], and d-level quantum states [42–45]. Among these, protocols that utilize simplified quantum resources (e.g., single photons and Bell states) are more feasible and practical than those relying on multi-qubit and d-level quantum states, due to the ease of operation and manipulation of single photons and Bell

states. Despite the advantages of Bell states, many existing Bell-state-based QPC protocols face challenges in achieving high qubit efficiency, with many achieving less than 50%.

Inspired by the aforementioned Bell-state-based QPC protocols and with the aim of enhancing their efficiency, we propose a novel approach that utilizes Bell states and Pauli operators to design a QPC protocol. The primary contributions of this work are as follows.

(1) By transmitting private information as Pauli operators applied to Bell states, the proposed protocol is more practical and efficient than those that rely on multi-qubit and d-level quantum states.
(2) The protocol achieves a qubit efficiency of 50%, requiring one Bell state and a bit of pre-shared key for each bit compared. This efficiency surpasses that of many existing Bell-state-based QPC protocols.
(3) By simulating a concrete example using IBM Quantum Qiskit simulator with a designed quantum circuit, the feasibility of the protocol has been validated.
(4) Security analyses confirm the protocol's resilience against both external attacks and insider threats.

The remainder of this paper is organized as follows: Section 2 introduces the Pauli operators and Bell states used in the protocol. Sections 3 and 4 detail the implementation steps of the proposed protocol and the simulations conducted via IBM Quantum Qiskit simulator, respectively. Section 5 presents a security analysis of the protocol. Section 6 discusses the findings, and Section 7 concludes the paper by summarizing the contributions and exploring potential future directions.

## 2. Pauli Operators and Bell States

The Pauli-X and Pauli-Z operators [46] are single-qubit gates that are mathematically defined as

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

Four Bell states are given by

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

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

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

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

When applying the operations $X^{a_1}Z^{a_2}$ and $X^{b_1}Z^{b_2}$ (where $a_1, a_2, b_1, b_2 \in \{0, 1\}$) to four Bell states, the resulting states are shown in Table 1.

According to Table 1, we find that the Bell states remain unchanged if and only if the same operations are performed on both the first and second particles of the Bell states. This property is crucial for the design of the proposed protocol that follows.

**Table 1.** The resulting states.

| Operations | $\|\boldsymbol{\varphi^+}\rangle$ | $\|\boldsymbol{\varphi^-}\rangle$ | $\|\boldsymbol{\psi^+}\rangle$ | $\|\boldsymbol{\psi^-}\rangle$ |
|---|---|---|---|---|
| $X^0Z^0 \otimes X^0Z^0$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ |
| $X^0Z^0 \otimes X^0Z^1$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ |
| $X^0Z^0 \otimes X^1Z^0$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ |
| $X^0Z^0 \otimes X^1Z^1$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ |
| $X^0Z^1 \otimes X^0Z^0$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ |
| $X^0Z^1 \otimes X^0Z^1$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ |
| $X^0Z^1 \otimes X^1Z^0$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ |
| $X^0Z^1 \otimes X^1Z^1$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ |
| $X^1Z^0 \otimes X^0Z^0$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ |
| $X^1Z^0 \otimes X^0Z^1$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ |
| $X^1Z^0 \otimes X^1Z^0$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ |
| $X^1Z^0 \otimes X^1Z^1$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ |
| $X^1Z^1 \otimes X^0Z^0$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ |
| $X^1Z^1 \otimes X^0Z^1$ | $\|\psi^+\rangle$ | $\|\varphi^+\rangle$ | $\|\varphi^+\rangle$ | $\|\psi^-\rangle$ |
| $X^1Z^1 \otimes X^1Z^0$ | $\|\varphi^-\rangle$ | $\|\varphi^+\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ |
| $X^1Z^1 \otimes X^1Z^1$ | $\|\varphi^+\rangle$ | $\|\varphi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ |

## 3. The Implementation Steps of the Proposed Protocol

The primary objective of the quantum private comparison (QPC) protocol is to determine whether the confidential inputs X and Y, held by Alice and Bob respectively, are equivalent. This comparison is facilitated by a semi-honest third party (TP), which complies with the protocol but is restricted from colluding with either participant. Crucially, the protocol ensures that neither Alice nor Bob leaks any information about their private inputs to each other or external adversaries.

The protocol assumes a noiseless and lossless quantum channel to guarantee the integrity of quantum state transmissions. Prior to execution, Alice and Bob convert their secrets into $n$-bit binary strings, denoted as $X = (x_{n-1}, x_{n-2}, \cdots, x_0)$ and $Y = (y_{n-1}, y_{n-2}, \cdots, y_0)$, where $x_i, y_i \in \{0,1\}$ for $i = 0, 1, \cdots, n-1$. If the length of $X$ or $Y$ is shorter than $n$, zeros are appended to the higher-order bits. The parameter $n$, determined by security requirements, is publicly disclosed to the TP. Subsequently, Alice and Bob employ a quantum key distribution (QKD) protocol (e.g., BB84 [47]) to establish a shared secret key $K_{AB} = (k_n k_{n-1} \cdots k_0)$, restructured as $K_{AB} = \left(k'_{\lceil n/2 \rceil - 1}, k'_{\lceil n/2 \rceil - 2}, \cdots, k'_0\right)$, where $k'_j = k_{2j+1}k_{2j}$ for $j = 0, 1, \cdots, \lceil n/2 \rceil - 2, \lceil n/2 \rceil - 1$.

Protocol Execution:

Step 1. Alice and Bob partition $X$ and $Y$ into $\lceil n/2 \rceil$ groups, where $\lceil \cdot \rceil$ is the ceiling function. If $n$ is odd, a padding bit (0) is added to the final group to ensure uniform group sizes of two bits.

Step 2. The TP prepares $\lceil n/2 \rceil$ Bell states, randomly selected from the set defined in Equations (2)–(5). These states are divided into two sequences: $S_A$ (first particles) and $S_B$ (second particles). For security validation, the TP generates decoy-photon sequences $D_A$ and $D_B$, composed of randomly chosen states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. All decoy photons in $D_A$ and $D_B$ are inserted into $S_A$ and $S_B$, forming modified sequences $S'_A$ and $S'_B$, which are transmitted to Alice and Bob, respectively.

Step 3. Upon receiving $S'_A (S'_B)$, Alice (Bob) acknowledges receipt. The TP then discloses the positions and measurement bases ($Z$-basis for $|0\rangle$ or $|1\rangle$; $X$-basis for $|+\rangle$ or $|-\rangle$) of the decoy photons. Alice (Bob) measures the decoy photons in $D_A (D_B)$, obtaining results $R_A (R_B)$, which are returned to the TP for error rate calculation. If the error rate exceeds a predefined threshold ($\tau = 2 \sim 8.9\%$) depending on the channel situation (e.g., the distance, etc.) [48,49], the protocol is terminated and restarted; otherwise, it proceeds to the next step.

Step 4. After removing decoy photons $D_A$ ($D_B$) from $S'_A(S'_B)$, Alice (Bob) applies operations $X^{a_{2j+1}}Z^{a_{2j}}$ ($X^{b_{2j+1}}Z^{b_{2j}}$) to $S_A(S_B)$, where $a_{2j+1} = x_{2j+1} \oplus k_{2j+1}$ and $a_{2j} = x_{2j} \oplus k_{2j}$ (similar for $b_{2j+1}$, $b_{2j}$). The resulting sequences $U_A(U_B)$ are embedded with new decoy-photon sequence $D'_A(D'_B)$, forming $G_A(G_B)$, which are sent to the TP.

Step 5. The TP verifies eavesdropping using the aforementioned decoy-photon method in Step 2. If secure, the TP removes $D'_A(D'_B)$ from $G_A(G_B)$ and performs Bell-state measurements on $U_A$ and $U_B$. A match between the measurement results $R_T$ and the initially prepared Bell states confirms $X = Y$; otherwise, $X \neq Y$.

## 4. Simulations for Two Concrete Examples

**Example 1.** *Comparison of the equality of the secret integers* $X_0 = 54$ *and* $Y_0 = 22$.

The binary representations of $X_0$ and $Y_0$ are $X_0 = (1,1,0,1,1,0)$ and $Y_0 = (1,0,1,1,0)$, respectively. The length of the strings is set to 6. Since the length of $Y_0$ is shorter than 6, zeros are appended to the higher-order bits, resulting in the restructured binary representation of $Y_0$ as $Y_0 = (0,\ 1,0,1,1,0)$. Alice and Bob partition them into three 2-bit groups: $X_0 = (11,01,10)$ and $Y_0 = (01,01,10)$. Let the shared secret key $K_{AB} = (1,1,0,0,0,1) = (11,00,01)$. The initial preparation includes three Bell states: $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$.

The quantum circuit implementation of these three Bell states $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$ is composed of Hadamard and CNOT gates, as shown in Figure 1. The left half of Figure 1 separated by barrier lines is for preparing Bell states, while the right half is for measuring Bell states using $Z$ basis. The measurement results of the three Bell states, obtained using the IBM Quantum Qiskit simulator (Qiskit: 0.44.1; Python: 3.11.4; OS: Windows) with 1024 shots, are displayed in Figure 2.

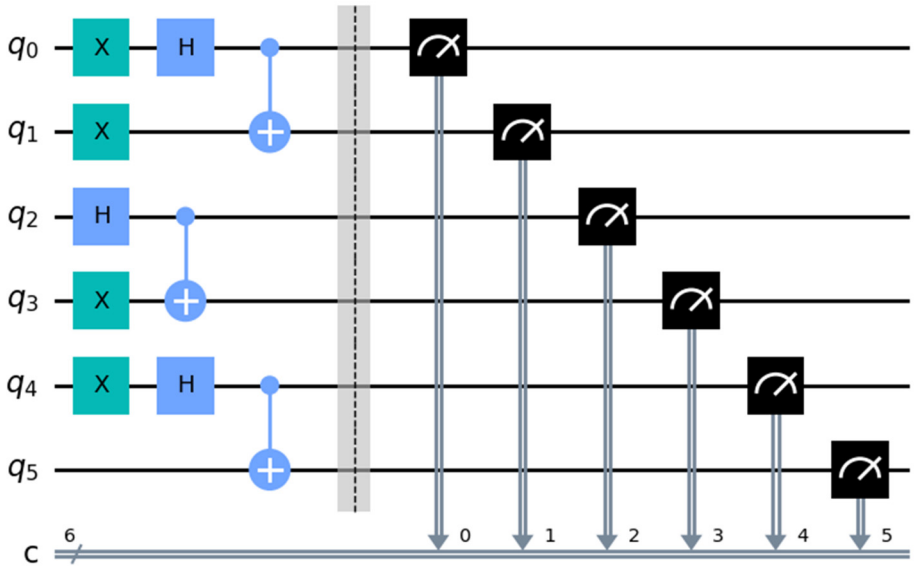


**Figure 1.** The circuit implementation of the three Bell states $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$.

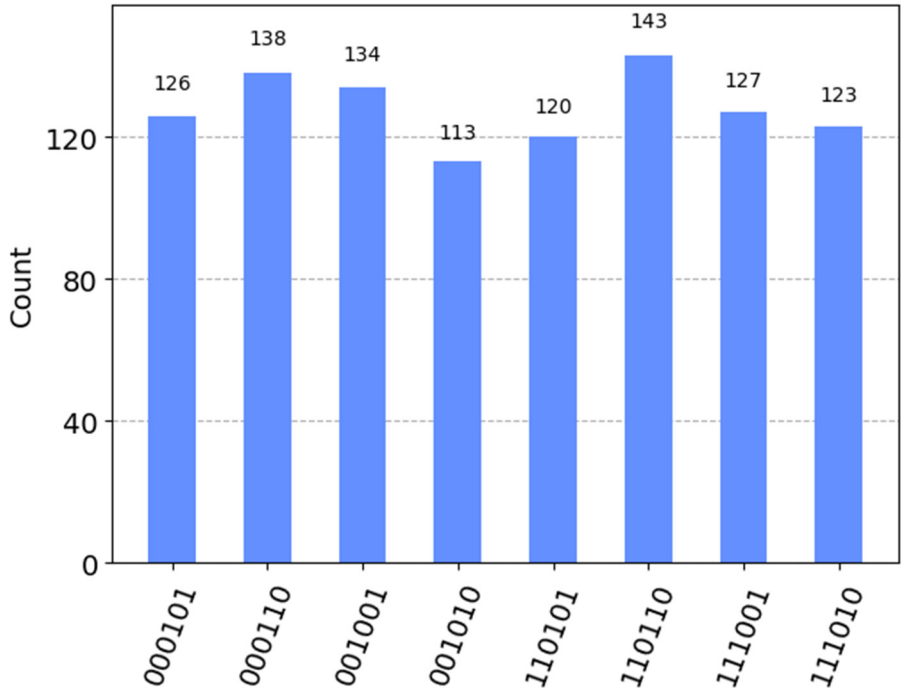


**Figure 2.** The measurement results of three Bell states with 1024 shots.

Based on $X_0$, $Y_0$ and $K_{AB}$, the corresponding operations on the three Bell states $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$ are $\{II \otimes XI,\ IZ \otimes IZ,\ XZ \otimes XZ\}$. The quantum circuit implementation for comparing the equality of the secret integers $X_0 = 54$ and $Y_0 = 22$ is shown in Figure 3, and the results of its probability measurements are presented in Figure 4.

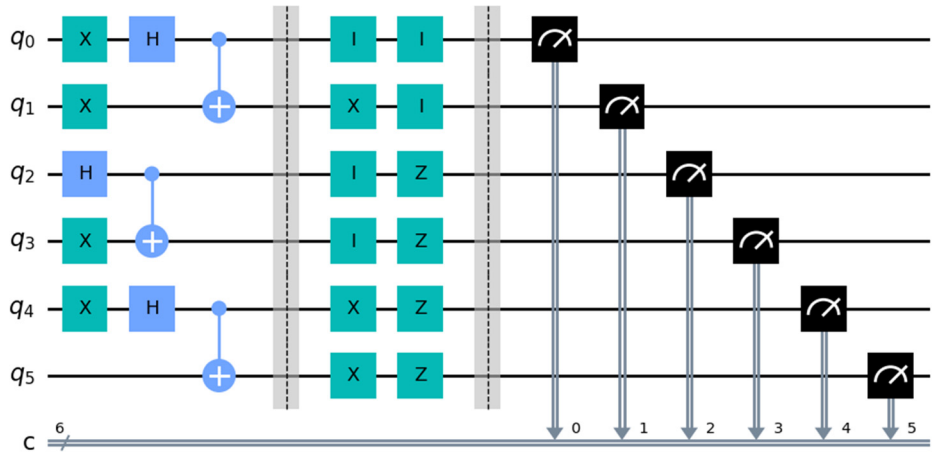


**Figure 3.** The quantum circuit implementation for comparing the equality of the secret integers $X_0 = 54$ and $Y_0 = 22$.

According to the bar chart in Figure 4, the measurement results of the computational basis states do not match those in Figure 2. This indicates that the measurement outcomes do not align with the initially prepared Bell states. Consequently, we can conclude that $X_0 \neq Y_0$.

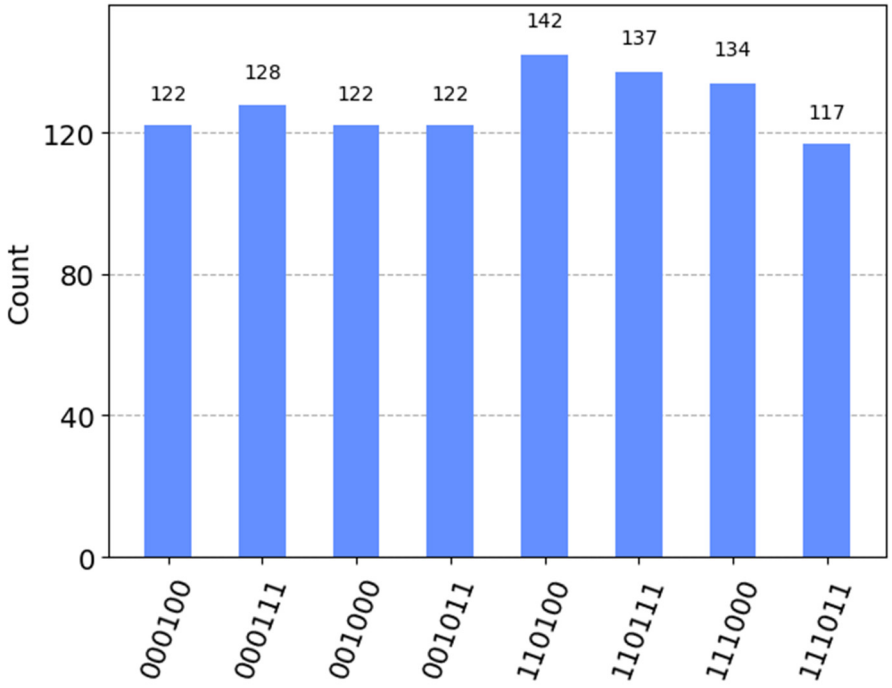


**Figure 4.** The results of the probability measurements with 1024 shots for Figure 3.

**Example 2.** *Comparison of the equality of the secret integers* $X_1 = 63$ *and* $Y_1 = 63$.

The binary representations of $X_1$ and $Y_1$ are $X_1 = (1,1,1,1,1,1)$ and $Y_1 = (1,1,1,1,1,1)$, respectively. Alice and Bob partition them into three 2-bit groups: $X_1 = (11,11,11)$ and $Y_1 = (11,11,11)$. Let the shared secret key $K_{AB} = (1,1,0,0,0,1) = (11,00,01)$. The initial preparation includes three Bell states: $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$.

Based on $X_1$, $Y_1$ and $K_{AB}$, the corresponding operations on three Bell states $\{|\psi^-\rangle, |\psi^+\rangle, |\varphi^-\rangle\}$ are $\{II \otimes II$, XZ⊗XZ, XI⊗XI$\}$. The quantum circuit implementation for comparing the equality of the secret integers $X_1 = 63$ and $Y_1 = 63$ is shown in Figure 5, and the results of its probability measurements are presented in Figure 6.

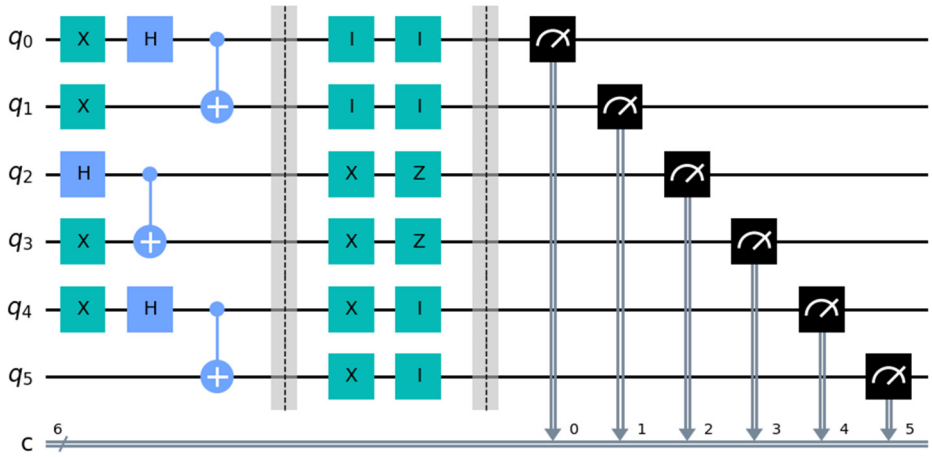


**Figure 5.** The quantum circuit implementation for comparing the equality of the secret integers $X_1 = 63$ and $Y_1 = 63$.

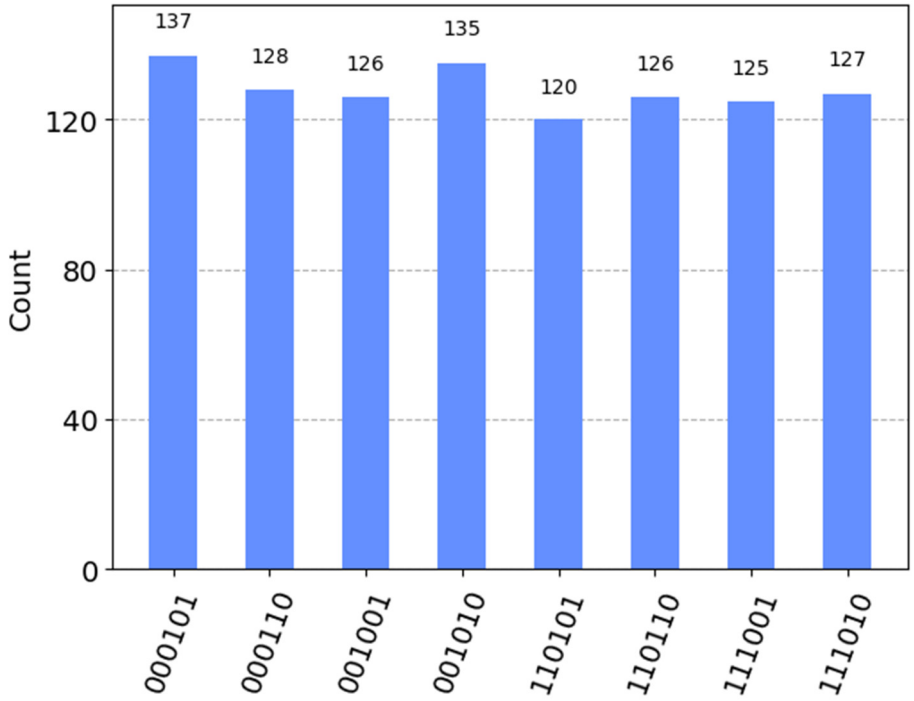


**Figure 6.** The results of the probability measurements with 1024 shots for Figure 5.

According to the bar chart in Figure 6, the measurement results of the computational basis states are identical to those in Figure 2, although the counts of each computational basis state may differ due to the influence of noise and decoherence. This result indicates that the measurement results align with the initially prepared Bell states. Consequently, we can conclude that $X_1 = Y_1$.

Although we utilize two example simulation experiments to demonstrate the feasibility of the proposed protocol, its scalability when comparing multiple bits remains unaffected. It has been reported that Zuchongzhi 3.0 [50], a superconducting quantum computer prototype comprising 105 qubits and achieving high operational fidelities, was constructed in 2025. As the number of available qubits increases, our protocol can further demonstrate its scalability on actual quantum hardware.

## 5. Security Analysis

In the execution of the protocol, the entanglement correlation between particles in Bell states is utilized to ensure the security of the particle distribution phase. The insertion of decoy photons into the particles, along with the implementation of quantum key distribution for sharing a pre-shared key, enhances security during the information transfer phase. In this section, we demonstrate that the proposed protocol is resilient against both external and participant attacks.

### *5.1. External Attacks*

When quantum sequences are transmitted through a quantum channel, an external eavesdropper, often referred to as Eve, may employ quantum-attack strategies to compromise the private inputs. The primary quantum attack strategies include intercept-measure-resend [51], entangle-measure [52], man-in-the-middle [53], and quantum Trojan-Horse attacks [54]. We will analyze whether the proposed protocol is secure against these quantum attack strategies as follows.

5.1.1. Intercept-Measure-Resend Attack

In the proposed QPC protocol, the intercept-measure-resend attack refers to Eve intercepting the quantum sequences $G_A$ and $G_B$, measuring them with Z-basis or X-basis, and resending the modified sequences to the TP. Unfortunately, this attack faces significant challenges due to the lack of information regarding the inserted positions and measurement bases of the decoy photons. These specific details will be disclosed when the TP receives the sequences.

As an example, consider a decoy photon prepared in the state $|1\rangle$. When Eve measures this decoy photon using the Z basis ($|0\rangle, |1\rangle$), she successfully passes the eavesdropping detection. Conversely, when she measures the decoy photon using the X basis ($|+\rangle, |-\rangle$), she passes the eavesdropping detection with a probability of 50%, since $|0\rangle$ and $|1\rangle$ are equal superpositions of $|+\rangle$ and $|-\rangle$. The choice between the Z basis and the X basis occurs with equal probability, each having a 50% chance. Thus, the probability of choosing the X basis and passing the eavesdropping detection is $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. Consequently, for each decoy photon, Eve has a 3/4 probability of successfully performing the intercept-measure-resend attack. However, for $d$ decoy photons, the detection probability becomes $1 - \left(\frac{3}{4}\right)^d$. The relationship between the number of decoy photons and the detection probability is illustrated in Figure 7.

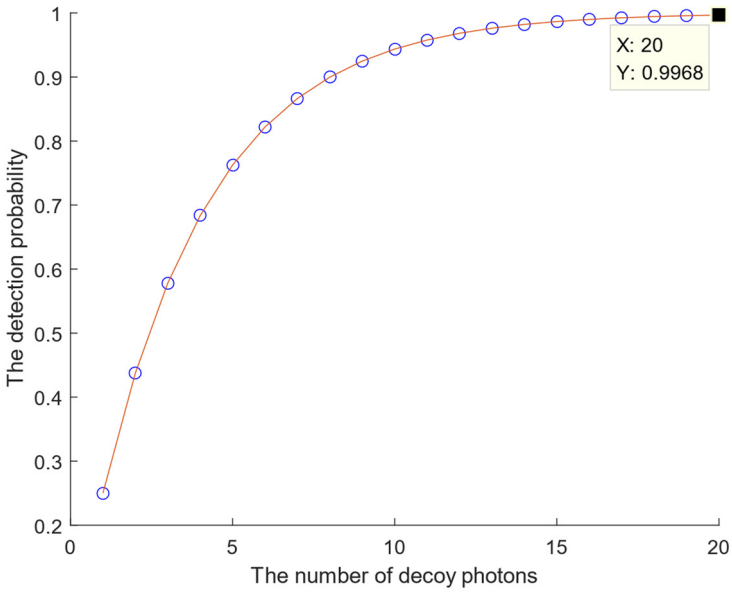


**Figure 7.** The relationship between the number of decoy photons ($d$, ranging from 1 to 20) and the detection probability.

According to the results presented in Figure 7, when $d$ = 20, the detection probability reaches 0.9968. However, as the number of decoy photons increases, the detection probability approaches 1. Consequently, Eve will not succeed in executing the intercept-measure-resend attack.

5.1.2. Entangle-Measure Attack

This attack involves Eve intercepting the quantum sequences $S'_A$ and $S'_B$, and entangling them with the prepared auxiliary state $|u_1\rangle$ through a specific unitary operation $U_1$ during the first quantum sequence transmission. During the second quantum sequence transmission, Eve intercepts the quantum sequences $G_A$ and $G_B$, and performs the specific unitary operation $U_2$ to entangle them with the prepared auxiliary state $|u_2\rangle$. Eve can then

measure the prepared auxiliary states $|e_1\rangle$ and $|e_2\rangle$ to extract private information about the confidential inputs.

During the first quantum sequence transmission, performing $U_1$ on $|e_1\rangle$ and states $|0\rangle$ and $|1\rangle$ proceeds as follows:

$$U_1|0\rangle|u_1\rangle = |0\rangle|u_{00}\rangle + |1\rangle|u_{01}\rangle = \sqrt{A}|0\rangle|\hat{u}_{00}\rangle + \sqrt{B}|1\rangle|\hat{u}_{01}\rangle \tag{6}$$

$$U_1|1\rangle|u_1\rangle = |0\rangle|u_{10}\rangle + |1\rangle|u_{11}\rangle = \sqrt{B}|0\rangle|\hat{u}_{10}\rangle + \sqrt{A}|1\rangle|\hat{u}_{11}\rangle \tag{7}$$

$$\begin{aligned} U_1|+\rangle|u_1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|u_{00}\rangle + |1\rangle|u_{01}\rangle + |0\rangle|u_{10}\rangle + |1\rangle|u_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(|u_{00}\rangle + |u_{01}\rangle + |u_{10}\rangle + |u_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(|u_{00}\rangle - |u_{01}\rangle + |u_{10}\rangle - |u_{11}\rangle) \\ &= |+\rangle|u_{++}\rangle + |-\rangle|u_{+-}\rangle \end{aligned} \tag{8}$$

$$\begin{aligned} U_1|-\rangle|u_1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|u_{00}\rangle + |1\rangle|u_{01}\rangle + |0\rangle|u_{10}\rangle - |1\rangle|u_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(|u_{00}\rangle + |u_{01}\rangle - |u_{10}\rangle - |u_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(|u_{00}\rangle - |u_{01}\rangle - |u_{10}\rangle + |u_{11}\rangle) \\ &= |+\rangle|u_{-+}\rangle + |-\rangle|u_{--}\rangle \end{aligned} \tag{9}$$

The states $\{|u_{00}\rangle, |u_{01}\rangle, |u_{10}\rangle, |u_{11}\rangle\}$ are four pure states determined by unitary operation $U_1$ and satisfy the following conditions.

$$\langle u_{00}|u_{00}\rangle = \langle u_{01}|u_{01}\rangle = A + B = 1 \tag{10}$$

$$\langle u_{10}|u_{10}\rangle = \langle u_{11}|u_{11}\rangle = B + A = 1 \tag{11}$$

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

Without loss of generality, we can set

$$\langle u_{00}|u_{01}\rangle = \langle u_{10}|u_{11}\rangle = \langle u_{00}|u_{10}\rangle = \langle u_{01}|u_{11}\rangle = 0 \tag{13}$$

We specify the angles between nonorthogonal vectors as

$$\langle \hat{u}_{00}|\hat{u}_{11}\rangle = \cos x, \langle \hat{u}_{01}|\hat{u}_{10}\rangle = \cos y, 0 \le x, y \le \frac{\pi}{2} \tag{14}$$

Furthermore, the probability of Eve not being detected is given as

$$P(|0\rangle) = \langle u_{00}|u_{00}\rangle = P(|1\rangle) = \langle u_{11}|u_{11}\rangle = A \tag{15}$$

$$P(|+\rangle) = P(|-\rangle) = \frac{1}{2}(1 + A\cos x + B\cos y) \tag{16}$$

Therefore, the average detection probability during the first quantum sequence transmission is given by

$$P_d^1 = \frac{A}{2} + \frac{(1 - A\cos x - B\cos y)}{4} \tag{17}$$

When $A = 0, B = 1$, $P_d^1$ comes to the minimum.

$$d_1 = \min\left(P_d^1\right) = \frac{1}{4} - \frac{\cos x}{4}, 0 \le d_1 \le \frac{1}{4} \tag{18}$$

During the second quantum sequence transmission, performing $U_2$ on $|e_2\rangle$ and states $|0\rangle$ and $|1\rangle$ proceeds as follows:

$$U_2|0\rangle|u_2\rangle = |0\rangle|u'_{00}\rangle + |1\rangle|u'_{01}\rangle = \sqrt{A'}|0\rangle|\hat{u}'_{00}\rangle + \sqrt{B'}|1\rangle|\hat{u}'_{01}\rangle \tag{19}$$

$$U_2|1\rangle|u_2\rangle = |0\rangle|u'_{10}\rangle + |1\rangle|u'_{11}\rangle = \sqrt{B'}|0\rangle|\hat{u}'_{10}\rangle + \sqrt{A'}|1\rangle|\hat{u}'_{11}\rangle \tag{20}$$

$$\begin{aligned} U_2|+\rangle|u_2\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|u'_{00}\rangle + |1\rangle|u'_{01}\rangle + |0\rangle|u'_{10}\rangle + |1\rangle|u'_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(|u'_{00}\rangle + |u'_{01}\rangle + |u'_{10}\rangle + |u'_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(|u'_{00}\rangle - |u'_{01}\rangle + |u'_{10}\rangle - |u'_{11}\rangle) \\ &= |+\rangle|u'_{++}\rangle + |-\rangle|u'_{+-}\rangle \end{aligned} \tag{21}$$

$$\begin{aligned} U_2|-\rangle|u_2\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|u'_{00}\rangle + |1\rangle|u'_{01}\rangle + |0\rangle|u'_{10}\rangle - |1\rangle|u'_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(|u'_{00}\rangle + |u'_{01}\rangle - |u'_{10}\rangle - |u'_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(|u'_{00}\rangle - |u'_{01}\rangle - |u'_{10}\rangle + |u'_{11}\rangle) \\ &= |+\rangle|u'_{-+}\rangle + |-\rangle|u'_{--}\rangle \end{aligned} \tag{22}$$

The states $\{|u\prime_{00}\rangle, |u\prime_{01}\rangle, |u\prime_{10}\rangle, |u\prime_{11}\rangle\}$ are four pure states determined by unitary operation $U_2$ and satisfy the following conditions.

$$\langle u'_{00}|u'_{00}\rangle = \langle u'_{01}|u'_{01}\rangle = A' + B' = 1 \tag{23}$$

$$\langle u'_{10}|u'_{10}\rangle = \langle u'_{11}|u'_{11}\rangle = B' + A' = 1 \tag{24}$$

$$\langle u'_{00}|u'_{10}\rangle = \langle u'_{01}|u'_{11}\rangle = 0 \tag{25}$$

Without loss of generality, we can set

$$\langle u'_{00}|u'_{01}\rangle = \langle u'_{10}|u'_{11}\rangle = \langle u'_{00}|u'_{10}\rangle = \langle u'_{01}|u'_{11}\rangle = 0 \tag{26}$$

We specify the angles between nonorthogonal vectors as

$$\langle \hat{u}'_{00}|\hat{u}'_{11}\rangle = \cos x', \langle \hat{u}'_{01}|\hat{u}'_{10}\rangle = \cos y', 0 \le x', y' \le \frac{\pi}{2} \tag{27}$$

In the same way, the average detection probability during the second quantum sequence transmission is given by

$$d_2 = \frac{1}{4} - \frac{\cos x'}{4}, 0 \le d_2 \le \frac{1}{4} \tag{28}$$

Reference [55] pointed out that the optimal incoherent attack by Eve consists of a balanced strategy, where $x = x'$. Therefore, we have

$$d = d_1 = d_2 = \frac{1}{4} - \frac{\cos x}{4}, 0 \le d \le \frac{1}{4} \tag{29}$$

The mutual information between the participants and Eve is written as

$$I(A:E) = 1 - h\left(\frac{1+\sin^2 x}{2}\right) = 1 - h\left(1 - \frac{(1-4d)^2}{2}\right) \tag{30}$$

where $h$ denotes the Shannon binary entropy. From Equation (30), we can infer that $I(A:E)$ is a monotonic increasing function. The more information Eve seeks to obtain, the greater the detection probability she will induce. Therefore, Eve will not succeed in executing the entangle-measure attack.

#### 5.1.3. Man-in-the-Middle Attack

This attack involves Eve intercepting the sequences containing the encoded private inputs and preparing fake sequences in place of the intercepted sequence. We take intercepting the sequence $G_A$ and preparing $G\prime_A$ as an example. The same method can be applied to analyze the interception of sequence $G_B$. For security validation, Eve prepares

guessed states as decoy photons, denoting the $i$-th decoy photon as $D_i$, which corresponds to the $j$-th qubit in $G_A$. The $j$-th qubit of $G\prime_A$ is denoted as $D\prime_i$. Both $D_i$ and $D\prime_i$ are prepared using basis $B = \{|0\rangle, |1\rangle\}$ and $B' = \{|+\rangle, |-\rangle\}$. When Alice discloses the measurement basis of $D_i$, Eve measures $D\prime_i$ using the basis $B'$ and obtains the results $D''_i$. The probability that $D''_i = D_i$ is as follows.

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

The detection probability for a decoy photon is

$$\begin{aligned} P(D''_i = D_i) &= P(D''_i = D_i | B' = B)P(B' = B) + P(D''_i = D_i | B' \neq B)P(B' \neq B) \\ &= \tfrac{1}{2}\left(P(D''_i = D_i | B' = B) + P((D''_i = D_i | B' \neq B))\right) \\ &= \tfrac{1}{2}\begin{pmatrix} P(D''_i = D_i | B' = B, D'_i = D_i)P(D'_i = D_i) + \\ P(D''_i = D_i | B' = B,\ D'_i \neq D_i)P(D'_i \neq D_i) + \tfrac{1}{2} \end{pmatrix} \\ &= \tfrac{1}{2}\left(1 \times \tfrac{1}{2} + 0 \times \tfrac{1}{2} + \tfrac{1}{2}\right) = \tfrac{1}{2} \end{aligned} \tag{31}$$

For $d$ decoy photons, the detection probability becomes $1 - \left(\frac{1}{2}\right)^d$. When $d = 10$, the detection probability reaches 0.999. However, as the number of decoy photons increases, the detection probability approaches 1. Consequently, Eve will not succeed in executing the man-in-the-middle attack.

#### 5.1.4. Quantum Trojan-Horse Attacks

Quantum Trojan horse attacks are broadly classified into two categories: (1) invisible photon attacks [36], where an eavesdropper injects undetectable photons into the quantum channel to probe transmitted states, and (2) delayed photon attacks [38], where photons are strategically delayed to intercept or alter communication. These attacks represent critical vulnerabilities in bidirectional quantum communication systems. The round-trip transmission mechanism inherent to the proposed protocol is particularly susceptible to such threats. To counter these risks, the protocol integrates wavelength filters to eliminate extraneous photon wavelengths and photon-number splitters to detect anomalous photon counts, thereby neutralizing covert eavesdropping attempts.

### *5.2. Participant Attacks*

Participants may maliciously attempt to deduce or alter each other's private inputs, thereby compromising data confidentiality. A detailed security analysis of insider threats is provided below.

#### 5.2.1. Security Against Attacks from Alice or Bob

In this protocol, Alice and Bob assume symmetrical roles. For generality, we analyze the scenario where Bob acts maliciously to deduce Alice's secret. Alice encodes her secrets through quantum operations (Pauli-X and Pauli-Z gates) on sequence $S_A$. To reconstruct Alice's secrets, Bob would require both $S_A$ and the transformed sequence $U_A$. However, since no direct quantum channel exists between Alice and Bob, Bob's only opportunity to obtain $S_A$ and $U_A$ lies in intercepting transmissions between the TP and Alice. Such interception falls under external eavesdropping, which the protocol neutralizes via the decoy-state method described in Steps 3 and 5. An analogous analysis applies if Alice attempts to compromise Bob's secrets. Therefore, the protocol's design inherently safeguards both parties' secrets against collusion and insider attacks.

5.2.2. Security Against Attacks from TP

While the semi-honest TP might attempt to extract additional information by analyzing intermediate results or deviating from the protocol, its capabilities are limited by the protocol's architectural constraints. The TP is solely responsible for the initial preparation and distribution of Bell states and subsequent Bell-basis measurements. Although the TP possesses knowledge of the initially prepared and post-transformation Bell states, it cannot reverse-engineer the participants' secrets ($X$ or $Y$) from these correlations. Even if the TP hypothetically substitutes Bell states with single photons and measures the returned particles, it lacks knowledge of the shared secret key $K_{AB}$, which is exclusively held by Alice and Bob. Without $K_{AB}$, the TP cannot resolve the encoded values $X$ and $Y$. As a result, the protocol ensures that the TP gains no information about the participants' secrets beyond the final comparison outcome.

## 6. Discussion

Qubit efficiency [29], a critical metric for evaluating quantum resource utilization, quantifies the ratio of classical bits securely compared to the total quantum resources consumed excluding those used for eavesdropping detection. Given that $\eta_c$ denotes the number of classical bits compared, $\eta_t$ denotes the qubits used for encoding private inputs, and $\eta_k$ denotes the bits allocated for pre-shared key, the qubit efficiency is defined as:

$$\eta_e = \frac{\eta_c}{\eta_t + \eta_k} \tag{32}$$

In our protocol, $\lceil n/2 \rceil$ Bell states (two-qubit systems) and an $n$-bit pre-shared key enable the comparison of $n$ classical bits, yielding $\eta_c = n$, $\eta_t = n$, and $\eta_k = n$. This results in a qubit efficiency of 50%. A comparative analysis with existing protocols is detailed in Table 2.

**Table 2.** A comparison with other Bell-state-based QPC protocols.

| Protocol | Quantum Resource | Usage of Unitary Operation | Usage of Quantum Entanglement Swapping | Usage of Pre-Shared Key | Quantum Measurement | Privacy Disclosure | Bit Number Compared Each Round | Compare Rounds | Qubit Efficiency |
|---|---|---|---|---|---|---|---|---|---|
| Ref. [20] | Bell states | No | No | No | Single particle | Yes | 1 | $n$ | 50% |
| Ref. [22] | Bell states | Yes | No | No | $\{\|0\rangle, \|1\rangle\}$ basis | Yes | 1 | $n$ | 50% |
| Ref. [24] | Bell states | No | Yes | Yes | GHZ-basis | No | 3 | $\lceil n/3 \rceil$ | 20% |
| Ref. [25] | Bell states | No | No | No | $\{\|0\rangle, \|1\rangle\}$ basis | No | 1 | $n$ | 16.67% |
| Ref. [26] | Bell states | Yes | No | Yes | Bell-basis | No | 1 | $n$ | 25% |
| Ref. [27] | Bell states | Yes | No | Yes | Bell-basis | No | 1 | $n$ | 25% |
| Ours | Bell states | Yes | No | Yes | Bell-basis | No | 2 | $\lceil n/2 \rceil$ | 50% |

Ref. [20] utilizes Bell states and XOR operations with single-particle measurements, achieving 50% efficiency. However, it is vulnerable to semi-honest TP attacks via fake Bell states. Ref. [22] employs Bell states and CNOT gates with Z-basis measurements, attaining 50% efficiency but is susceptible to outsider disturbance attacks and TP measuring attacks. Ref. [24] relies on entanglement swapping and GHZ-basis measurements, requiring three Bell states and nine pre-shared key bits to compare three classical bits, yielding 20% efficiency. Ref. [25] uses single Bell states $|\varphi^+\rangle$ and XOR operations, achieving only 16.67% efficiency (three Bell states per compared bit). Refs. [26,27] incorporate rotation/unitary

operations and Bell measurements, achieving 25% efficiency (one Bell state and one pre-shared key bit per compared bit).

Compared with existing Bell-state-based QPC protocols, our protocol offers the following improvements.

(1) Our protocol employs Bell states, Pauli-X and Pauli-Z encoding, and Bell measurements without entanglement swapping [24], further enhancing its feasible implementation.
(2) By leveraging a single Bell state and two pre-shared key bits to compare two classical bits, it achieves 50% qubit efficiency—double that of Refs. [26,27] and higher than Refs. [24,25].
(3) Although the proposed protocol has equal qubit efficiency with Refs. [20,22], it provides security against the TP's attack and external eavesdropping through decoy-state validation and the QKD-secured key, while the schemes in Refs. [20,22] are not secure and may result in privacy disclosure.

## 7. Conclusions

In this study, we propose an efficient quantum private comparison (QPC) protocol that harnesses the entanglement properties of Bell states to enable secure and privacy-preserving comparisons of confidential data. Participants encode their private inputs using Pauli-X and Pauli-Z operators on quantum sequences distributed by a semi-honest third party (TP). This design achieves 50% qubit efficiency—a significant improvement over existing Bell-state-based protocols—by utilizing a single Bell state and two pre-shared key bits to compare two classical bits. The protocol's practicality is validated through experimental simulations on the IBM Quantum Qiskit simulator, confirming its operational feasibility in real-world quantum environments. A comprehensive security analysis demonstrates the protocol's robustness against both external attacks and insider threats. By integrating Bell-state encoding, QKD-secured keys, and decoy-state validation, our protocol addresses vulnerabilities in prior works, such as susceptibility to fake Bell states and disturbance attacks. Compared to existing QPC schemes, our protocol offers superior efficiency and experimental viability, achieved through minimal quantum resource requirements and simplified operations (no entanglement swapping or GHZ-basis measurements). Future work will extend this framework to noisy intermediate-scale quantum (NISQ) environments, incorporating error mitigation techniques for real-world deployment. Additionally, we aim to design semi-quantum private comparison protocols to reduce reliance on quantum devices, further alleviating resource constraints in practical applications.

**Author Contributions:** Conceptualization, M.H. and S.Z.; methodology, M.H.; software, M.H.; validation, M.H. and S.Z.; formal analysis, M.H.; investigation, M.H.; resources, M.H.; data curation, M.H.; writing—original draft preparation, M.H.; writing—review and editing, Y.W. and S.Z.; visualization, S.Z.; supervision, S.Z.; project administration, S.Z.; funding acquisition, S.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Research Project of Key R&D Programs in Tibet Autonomous Region (No. XZ202501ZY0094), the National Natural Science Foundation of China (No. 62076042), the National Key Research and Development Plan of China, Key Project of Cyberspace Security Governance (No. 2022YFB3103103), the Key Research and Development Project of Chengdu (No. 2023-XT00-00002-GX), the Key Research and Development Support Program Project of Chengdu (No. 2024-YF05-01227-SN), and the Open Fund of Network and Data Security Key Laboratory of Sichuan Province (Grant No. NDS2024-1).

**Data Availability Statement:** Data is contained within the article.

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

## References


1. Lindell, Y. Secure multiparty computation. *Commun. ACM* **2020**, *64*, 86–96. [CrossRef]
2. 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.
3. Boudot, F.; Schoenmakers, B.; Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
4. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
5. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
6. Qin, Y.; Cheng, J.; Ma, J.; Zhao, D.; Yan, Z.; Jia, X.; Xie, C.; Peng, K. Efficient and secure quantum secret sharing for eight users. *Phys. Rev. Res.* **2024**, *6*, 033036. [CrossRef]
7. 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]
8. Senthoor, K.; Sarvepalli, P.K. Theory of communication efficient quantum secret sharing. *IEEE Trans. Inf. Theory* **2022**, *68*, 3164–3186. [CrossRef]
9. Huang, X.; Zhang, S.B.; Chang, Y.; Chi, Q.; Dong-Mei, L.; Min, H. Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 838–847. [CrossRef]
10. Karim, F.; Abulkasim, H.; Alabdulkreem, E.; Ahmed, N.; Jamjoom, M.; Abbas, S. Improvements on new quantum key agreement protocol with five-qubit Brown states. *Mod. Phys. Lett. A* **2022**, *37*, 2250128. [CrossRef]
11. Wang, C.; Zhang, Q.; Liang, S.; Zhu, H. Secure mutual authentication quantum key agreement scheme for two-party setting with key recycling. *Quantum Inf. Process.* **2024**, *23*, 139. [CrossRef]
12. Pan, D.; Long, G.L.; Yin, L.; Sheng, Y.-B.; Ruan, D.; Ng, S.X.; Lu, J.; Hanzo, L. The evolution of quantum secure direct communication: On the road to the qinternet. *IEEE Commun. Surv. Tutor.* **2024**, *23*, 1898–1949. [CrossRef]
13. Pan, D.; Song, X.T.; Long, G.L. Free-space quantum secure direct communication: Basics, progress, and outlook. *Adv. Devices Instrum.* **2023**, *4*, 0004. [CrossRef]
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. Zhang, H.; Sun, Z.; Qi, R.; Yin, L.; Long, G.-L.; Lu, J. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci. Appl.* **2022**, *11*, 83. [CrossRef] [PubMed]
16. Chen, Y.; Situ, H.; Huang, Q.; Zhang, C. A novel quantum private set intersection scheme with a semi-honest third party. *Quantum Inf. Process.* **2023**, *22*, 429. [CrossRef]
17. 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]
18. Sutradhar, K.; Om, H. An efficient simulation for quantum secure multiparty computation. *Sci. Rep.* **2021**, *11*, 2206. [CrossRef] [PubMed]
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. Tseng, H.Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process.* **2012**, *11*, 373–384. [CrossRef]
21. Wang, C.; Xu, G.; Yang, Y.X. Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. *Int. J. Quantum Inf.* **2013**, *11*, 1350039. [CrossRef]
22. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
23. Ming-Yi, D. Cryptanalysis and improvement of quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2021**, *60*, 195–199. [CrossRef]
24. 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]
25. Lang, Y.F. Quantum private comparison using single bell state. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036. [CrossRef]
26. Hou, M.; Sun, S.Y.; Zhang, W. Quantum private comparison for the socialist millionaire problem. *Front. Phys.* **2024**, *12*, 1408446. [CrossRef]
27. Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. [CrossRef] [PubMed]
28. 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]
29. Kou, T.Y.; Che, B.C.; Dou, Z.; Chen, X.-B.; Lai, Y.-P.; Li, J. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. *Chin. Phys. B* **2022**, *31*, 060307. [CrossRef]

30. Liu, B.; Xiao, D.; Huang, W.; Jia, H.-Y.; Song, T.-T. Quantum private comparison employing single-photon interference. *Quantum Inf. Process.* **2017**, *16*, 180. [CrossRef]
31. Pan, H.M. Two-party quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3389–3395. [CrossRef]
32. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
33. Liu, B.; Gao, F.; Jia, H.; Huang, W.; Zhang, W.-W.; Wen, Q.-Y. Efficient quantum private comparison employing single photons and collective detection. *Quantum Inf. Process.* **2013**, *12*, 887–897. [CrossRef]
34. 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]
35. 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]
36. 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]
37. Ji, Z.X.; Ye, T.Y. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. *Commun. Theor. Phys.* **2016**, *65*, 711. [CrossRef]
38. Ji, Z.X.; Zhang, H.G.; Fan, P.R. Two-party quantum private comparison protocol with maximally entangled seven-qubit state. *Mod. Phys. Lett. A* **2019**, *34*, 1950229. [CrossRef]
39. Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. [CrossRef] [PubMed]
40. 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]
41. 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]
42. Wang, B.; Liu, S.Q.; Gong, L.H. Semi-quantum private comparison protocol of size relation with d-dimensional GHZ states. *Chin. Phys. B* **2022**, *31*, 010302. [CrossRef]
43. 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]
44. Wang, B.; Gong, L.H.; Liu, S.Q. Multi-party semi-quantum private comparison protocol of size relation based on two-dimensional Bell states. *Chin. Phys. B* **2024**, *33*, 110303. [CrossRef]
45. Zhou, N.R.; Chen, Z.Y.; Liu, Y.Y.; Gong, L.-H. Multi-Party Semi-Quantum Private Comparison Protocol of Size Relation with d-Level GHZ States. *Adv. Quantum Technol.* **2024**, *8*, 2400530. [CrossRef]
46. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
47. 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, 12 December 1984; pp. 175–179.
48. Jennewein, T.; Simon, C.; Weihs, G.; Weinfurter, H.; Zeilinger, A. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **2000**, *84*, 4729. [CrossRef] [PubMed]
49. Hughes, R.J.; Nordholt, J.E.; Derkacs, D.; Peterson, C.G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **2002**, *4*, 43. [CrossRef]
50. Gao, D.; Fan, D.; Zha, C.; Bei, J.; Cai, G.; Cai, J.; Cao, S.; Chen, F.; Chen, J.; Chen, K.; et al. Establishing a new benchmark in quantum computational advantage with 105-qubit zuchongzhi 3.0 processor. *Phys. Rev. Lett.* **2025**, *134*, 090601. [CrossRef] [PubMed]
51. Liu, X.F.; Li, D.F.; Zheng, Y.D.; Yang, X.-L.; Zhou, J.; Tan, Y.-Q.; Liu, M.-Z. Experimental realization of quantum controlled teleportation of arbitrary two-qubit state via a five-qubit entangled state. *Chin. Phys. B* **2022**, *31*, 050301. [CrossRef]
52. Ye, T.Y.; Ye, C.Q. Measure-resend semi-quantum private comparison without entanglement. *Int. J. Theor. Phys.* **2018**, *57*, 3819–3834. [CrossRef]
53. 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]
54. 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]
55. Lucamarini, M.; Mancini, S. Secure deterministic communication without entanglement. *Phys. Rev. Lett.* **2005**, *94*, 140501. [CrossRef] [PubMed]