mathematics

Article

Two-Party Quantum Private Comparison Protocol for Direct Secret Comparison

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

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

Abstract: In this paper, we leverage the properties of the swap test to evaluate the similarity of two qubits and propose a two-party quantum private comparison (QPC) protocol involving a semi-trusted third party (TP). The TP facilitates the comparison between participants without accessing their private information, other than the final comparison results. Our protocol encodes participants' secret integers directly into the amplitudes of single-photon states and introduces a novel method for secret-to-secret comparison rather than the traditional bit-to-bit comparison, resulting in improved scalability. To ensure security, the encoded single-photon states are concealed using rotation operations. The comparison results are derived through the implementation of the swap test. A simulation on the IBM Quantum Platform demonstrates the protocol's feasibility, and a security analysis confirms its robustness against potential eavesdropping and participant attacks. Compared with existing QPC protocols that employ bit-to-bit comparison methods, our approach offers improved practicality and scalability. Specifically, it integrates single-photon states, rotation operations, and the swap test as key components for direct secret comparison, facilitating easier implementation with quantum technology.

Keywords: quantum private comparison (QPC); single photons; semi-trusted third party (TP); swap test; rotation operation; direct secret comparison

MSC: 81P45; 81P94

Academic Editor: Didier Felbacq

Received: 18 December 2024
Revised: 17 January 2025
Accepted: 19 January 2025
Published: 20 January 2025

Citation: Hou, M.; Wu, Y. Two-Party Quantum Private Comparison Protocol for Direct Secret Comparison. *Mathematics* **2025**, *13*, 326. https://doi.org/10.3390/math13020326

1. Introduction

Quantum information science has progressed significantly, particularly in quantum cryptography, which utilizes quantum mechanics for enhanced security compared with classical methods that depend on mathematical complexity. Following Bennett and Brassard's introduction of the first unconditional quantum cryptographic protocol in 1984 [1], a variety of protocols have been developed to tackle different cryptographic tasks, including quantum key distribution (QKD) [2–6], quantum secret sharing (QSS) [7–10], quantum key agreement (QKA) [11,12], quantum secure direct communication (QSDC) [13–16], and quantum private set intersection (QPSI) [17–20].

Secure multiparty computation (MPC) is a cryptographic framework that enables multiple parties to compute a function collaboratively while keeping their inputs confidential. A key development in this area is the private comparison proposed by Yao in the context of the millionaires' problem [21], which allows two millionaires to determine who is wealthier without disclosing their actual wealth. Boudot et al. [22] later expanded this concept to the socialist millionaires' problem, where two parties seek to establish whether their wealth is equal without revealing specific amounts. This issue has garnered significant attention in the cryptographic community, leading to various privacy-enhancing solutions. However, Lo [23] identified a significant limitation in two-party settings: it is fundamentally impossible to securely evaluate a computational function without compromising privacy. To overcome this challenge, the involvement of a semi-honest third party (TP) is crucial. The TP facilitates secure comparisons while potentially attempting to glean information about the participants' inputs.

The security of private comparison protocols relies on unproven mathematical assumptions, making them susceptible to threats from quantum computers, which exploit quantum mechanics for efficient parallel computation. Notably, the Shor algorithm [24] can factor large integers in polynomial time, rendering classical public-key cryptographic systems like RSA vulnerable to quantum attacks. Additionally, the Grover algorithm [25] poses a significant risk to symmetric-key cryptography by enabling faster search and function inversion, effectively reducing the effective key length of symmetric algorithms by half. In response to these vulnerabilities, quantum private comparison (QPC) has been developed. QPC utilizes quantum mechanics to enhance security features, ensuring that sensitive information remains confidential throughout the comparison process.

The first quantum private comparison (QPC) protocol was developed by Yang and Wen [26], utilizing EPR pairs for quantum information transmission along with decoy photons and a one-way hash function for security. Since then, various QPC protocols have emerged, employing different quantum states such as single particles [27–32], Bell states [33–40], and multi-particle entangled states [41–53]. Beyond merely comparing equality, researchers have also explored protocols for comparing the sizes of secret integers. For instance, Lin et al. [54] proposed a size comparison QPC protocol using d-level Bell states, while Guo et al. [55] utilized entanglement swapping of d-level Bell states. Yu et al. [56] introduced a similar protocol with d-level single-particle states, and Ye and Ye [57] presented two multiparty QPC protocols involving one or two semi-honest TPs. Additionally, Song et al. [58] developed an multiparty quantum private comparison (MQPC) using single-particle states.

The swap test [59], a fundamental algorithm in quantum computing, has become a key focus in the development of quantum cryptographic protocols. Its primary objective is to assess the similarity between two qubits. By measuring the probability of the ancilla qubit being in the $|1\rangle$ or $|0\rangle$ state, the square of the inner product of the two qubits is determined. Building on the principles of the swap test, various applications such as quantum signatures [60], quantum machine learning [61], and the blind millionaires' problem [62] have been proposed.

The previously discussed QPC protocols focus on converting secret integers into binary representations and comparing these classical bits (0 or 1) using a bit-by-bit approach, which inherently limits their scalability. Additionally, many existing QPC protocols employ multi-qubit states and d-dimensional states, which further constrain their practicality due to the complexities associated with manipulating these states. To overcome these limitations, we propose a two-party quantum private comparison (QPC) protocol that utilizes the swap test to evaluate the similarity of two encoded qubits. This process involves a semi-honest third party (TP) who facilitates the comparison between participants without accessing their private information, except for the final comparison results. In our protocol, the two participants encode their secret integers directly into the amplitudes of single-photon states through rotation operations, significantly enhancing scalability by eliminating the need for binary representations. The encoded single-photon states are secured through these rotation operations before being sent to the TP, who then derives the comparison results using the swap test. A simulation conducted on the IBM Quantum Platform confirms the feasibility of our protocol, and security analysis demonstrates its resilience against potential eavesdropping and participant attacks. Compared with existing QPC protocols that rely on bit-by-bit comparison methods, our approach offers improved practicality and scalability. Specifically, it integrates single-photon states, rotation operations, and the swap test as essential components for direct secret comparison, making it easier to implement with modern technology.

The remainder of this paper is structured as follows. Section 2 introduces the swap test and rotation operation. A detailed description of the proposed QPC protocol is provided in Section 3. Sections 4 and 5 present the simulation and analysis, respectively. Section 6 offers a comparison with existing protocols, and, finally, Section 7 concludes the paper.

2. Swap Test and Rotation Operation

2.1. Swap Test

The swap test was first introduced in [59] and is designed to assess the similarity between two arbitrary qubits. By measuring the probability that the ancilla qubit is in either state $|1\rangle$ or state $|0\rangle$, we can determine the square of the inner product of the two qubits [63]. The quantum circuit implementing the swap test is illustrated in Figure 1.

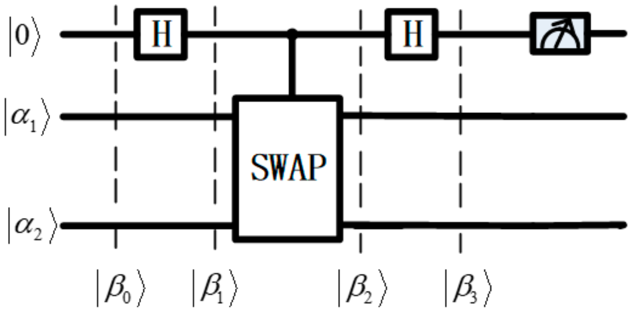

Figure 1. The quantum circuit implementing the swap test.

The initial quantum states are composed by two quantum states $|\alpha_1\rangle$ and $|\alpha_2\rangle$, as well as an ancillary state $|0\rangle$. That is,

$$|\beta_0\rangle = |0\rangle \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle = |0, \alpha_1, \alpha_2\rangle \tag{1}$$

When performing a Hadamard operation on the ancillary state $|0\rangle$, the initial quantum state $|\beta_0\rangle$ is converted as

$$|\beta_1\rangle = (H \otimes I \otimes I)|\beta_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle = \frac{1}{\sqrt{2}}(|0, \alpha_1, \alpha_2\rangle + |1, \alpha_1, \alpha_2\rangle) \tag{2}$$

When performing the controlled-swap gate where the ancillary is the control qubit, $|\beta_1\rangle$ is transformed into

$$|\beta_2\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\alpha_2\rangle \otimes |\alpha_1\rangle = \frac{1}{\sqrt{2}}(|0, \alpha_1, \alpha_2\rangle + |1, \alpha_2, \alpha_1\rangle) \tag{3}$$

When performing the Hadamard operation on the ancillary state $|0\rangle$ again, $|\beta_2\rangle$ is converted as

$$\begin{aligned}|\beta_3\rangle &= (H \otimes I \otimes I)|\beta_2\rangle = \tfrac{1}{\sqrt{2}}\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle + \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes |\alpha_2\rangle \otimes |\alpha_1\rangle\right) \\ &= \tfrac{1}{2}|0\rangle \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle + \tfrac{1}{2}|1\rangle \otimes |\alpha_1\rangle \otimes |\alpha_2\rangle + \tfrac{1}{2}|0\rangle \otimes |\alpha_2\rangle \otimes |\alpha_1\rangle - \tfrac{1}{2}|1\rangle \otimes |\alpha_2\rangle \otimes |\alpha_1\rangle \\ &= \tfrac{1}{2}|0\rangle(|\alpha_1, \alpha_2\rangle + |\alpha_2, \alpha_1\rangle) + \tfrac{1}{2}|1\rangle(|\alpha_1, \alpha_2\rangle - |\alpha_2, \alpha_1\rangle)\end{aligned} \tag{4}$$

When performing a projective measurement on the ancillary state with an operator $M = |1\rangle\langle 1|$, the probability that the ancillary state is in state $|1\rangle$ can be given by

$$\begin{aligned} P(|1\rangle) &= \langle\beta_3|M^\dagger M|\beta_3\rangle = \langle\beta_3|M|\beta_3\rangle \\ &= \tfrac{1}{4}(\langle 1,\alpha_1,\alpha_2| - \langle 1,\alpha_2,\alpha_1|) \otimes |1\rangle\langle 1| \otimes (|1,\alpha_1,\alpha_2\rangle - |1,\alpha_2,\alpha_1\rangle) \\ &= \tfrac{1}{4}(\langle\alpha_1,\alpha_2| - \langle\alpha_2,\alpha_1|) \otimes (|\alpha_1,\alpha_2\rangle - |\alpha_2,\alpha_1\rangle) \\ &= \tfrac{1}{2} - \tfrac{1}{2}|\langle\alpha_1|\alpha_2\rangle|^2 \end{aligned} \tag{5}$$

According to Equation (5), we can deduce that

$$|\langle\alpha_1|\alpha_2\rangle|^2 = 1 - 2P(|1\rangle) \tag{6}$$

2.2. Rotation Operation

The rotation operation around the Y-axis can be written as

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{7}$$

$R_y(\theta)$ is a unitary operation since ${R_y}^\dagger(\theta)R_y(\theta) = R_y(-\theta)R_y(\theta) = I$. For quantum states $|1\rangle$ and $|0\rangle$, when performing the rotation operation on them, we can obtain

$$R_y(\theta)|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix} = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \tag{8}$$

$$R_y(\theta)|0\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \tag{9}$$

From Equations (8) and (9), we can know that the single-photon states $|1\rangle$ and $|0\rangle$ are concealed. Without knowing the angle θ, $|1\rangle$ and $|0\rangle$ cannot be recovered.

To obtain the initial single-photon states $|1\rangle$ and $|0\rangle$, we need to rotate the resulting state with an angle of θ in the opposite direction. That is, the rotation angle is $-\theta$.

$$R_y(-\theta)\left(-\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle\right) = \begin{pmatrix} \cos\frac{-\theta}{2} & -\sin\frac{-\theta}{2} \\ \sin\frac{-\theta}{2} & \cos\frac{-\theta}{2} \end{pmatrix}\begin{pmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \tag{10}$$

$$R_y(-\theta)\left(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle\right) = \begin{pmatrix} \cos\frac{-\theta}{2} & -\sin\frac{-\theta}{2} \\ \sin\frac{-\theta}{2} & \cos\frac{-\theta}{2} \end{pmatrix}\begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{11}$$

Furthermore, the rotation operation can also be used to encode the secret integer. For instance, for the integer 10, we can consider it as $\frac{\pi}{10}$, which serves as the angle of the rotation operation performed on quantum state $|0\rangle$. Then, the encoded single-photon state is $R_y\left(\frac{\pi}{10}\right)|0\rangle = cos\frac{\pi}{20}|0\rangle + sin\frac{\pi}{20}|1\rangle$.

3. The Proposed QPC Protocol

The primary objective of the QPC protocol is to determine whether the secrets x and y held by Alice and Bob are equal with the assistance of a semi-honest third party (TP). The TP is expected to adhere to the protocol as designed and will not collude with the participants. However, despite following the rules, the TP may still attempt to extract additional information from the data it processes. This determination is achieved without either party disclosing any information about their respective secrets to one another, the TP, or any external observers. The protocol guarantees several key properties:

Privacy: Each participant's secret remains confidential throughout the entire process.

Correctness: The protocol's comparison result accurately indicates whether the secrets are equal.

Fairness: Both parties receive the comparison result simultaneously, ensuring that neither participant has an advantage over the other.

The protocol assumes the availability of a noise-free and lossless quantum channel, which allows for the transmission of quantum states without any degradation. Furthermore, it presumes that the classical channel used for communication between the parties is authenticated during transmission.

The detailed steps of the proposed QPC protocol are as follows, and its diagram is depicted in Figure 2.

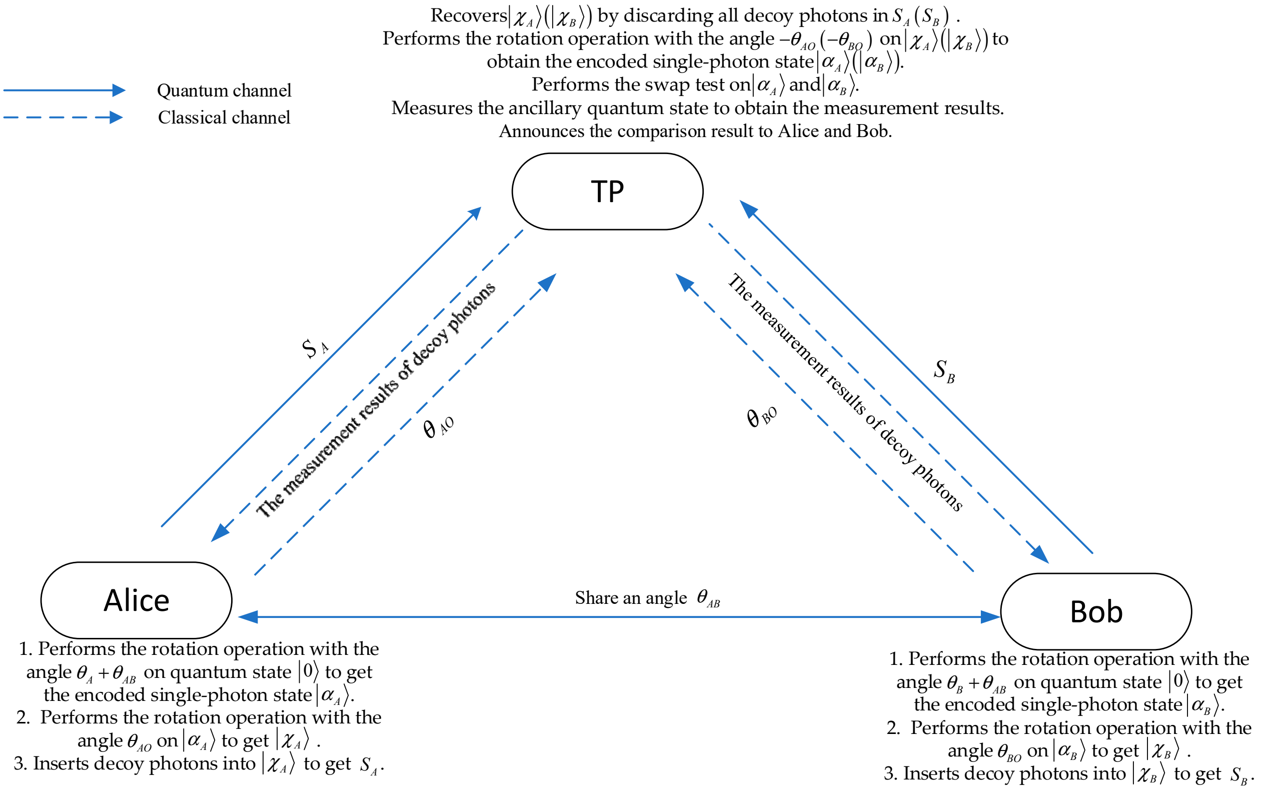
Recovers $|\chi_A\rangle(|\chi_B\rangle)$ by discarding all decoy photons in $S_A\,(S_B)$.
Performs the rotation operation with the angle $-\theta_{AO}\,(-\theta_{BO})$ on $|\chi_A\rangle(|\chi_B\rangle)$ to obtain the encoded single-photon state $|\alpha_A\rangle(|\alpha_B\rangle)$.
Performs the swap test on $|\alpha_A\rangle$ and $|\alpha_B\rangle$.
Measures the ancillary quantum state to obtain the measurement results.
Announces the comparison result to Alice and Bob.
Quantum channel
Classical channel
TP
S_A
The measurement results of decoy photons
θ_{AO}
θ_{BO}
The measurement results of decoy photons
S_B
Alice
Share an angle θ_{AB}
Bob
1. Performs the rotation operation with the angle $\theta_A+\theta_{AB}$ on quantum state $|0\rangle$ to get the encoded single-photon state $|\alpha_A\rangle$.
2. Performs the rotation operation with the angle θ_{AO} on $|\alpha_A\rangle$ to get $|\chi_A\rangle$.
3. Inserts decoy photons into $|\chi_A\rangle$ to get S_A.
1. Performs the rotation operation with the angle $\theta_B+\theta_{AB}$ on quantum state $|0\rangle$ to get the encoded single-photon state $|\alpha_B\rangle$.
2. Performs the rotation operation with the angle θ_{BO} on $|\alpha_B\rangle$ to get $|\chi_B\rangle$.
3. Inserts decoy photons into $|\chi_B\rangle$ to get S_B.

Figure 2. The diagram of the QPC protocol.

Step 1. Alice and Bob share an angle $\theta_{AB} \in [0, 2\pi)$ through a QKD protocol. Then, Alice (Bob) converts her (his) secret x (y) into an angle $\theta_A = \frac{\pi}{x}$ ($\theta_B = \frac{\pi}{y}$). Specifically, if $x = 0$ ($y = 0$), then $\theta_A = 0$ ($\theta_B = 0$). Finally, Alice (Bob) performs the rotation operation with the angle $\theta_A + \theta_{AB}$ ($\theta_B + \theta_{AB}$) on quantum state $|0\rangle$ to obtain the encoded single-photon state $|\alpha_A\rangle$ ($|\alpha_B\rangle$).

$$\begin{aligned}|\alpha_A\rangle &= R_y(\theta_A+\theta_{AB})|0\rangle = \begin{pmatrix} \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) & -\sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) & \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|1\rangle = \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|1\rangle\end{aligned} \tag{12}$$

$$\begin{aligned}|\alpha_B\rangle &= R_y(\theta_B+\theta_{AB})|0\rangle = \begin{pmatrix} \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) & -\sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) & \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|1\rangle = \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|1\rangle\end{aligned} \tag{13}$$

Step 2. Alice (Bob) randomly generates her (his) own secret key $\theta_{AO} \in [0, 2\pi)$ ($\theta_{BO} \in [0, 2\pi)$). She (he) performs the rotation operation with the angle θ_{AO} (θ_{BO}) on the encoded single-photon state $|\alpha_A\rangle$ ($|\alpha_B\rangle$). The resulting single-photon state is denoted as $|\chi_A\rangle$ ($|\chi_B\rangle$).

$$\begin{aligned}|\chi_A\rangle = R_y(\theta_{AO})|\alpha_A\rangle &= \begin{pmatrix} \cos\frac{\theta_{AO}}{2} & -\sin\frac{\theta_{AO}}{2} \\ \sin\frac{\theta_{AO}}{2} & \cos\frac{\theta_{AO}}{2} \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|1\rangle\end{aligned} \tag{14}$$

$$\begin{aligned}|\chi_B\rangle = R_y(\theta_{BO})|\alpha_B\rangle &= \begin{pmatrix} \cos\frac{\theta_{BO}}{2} & -\sin\frac{\theta_{BO}}{2} \\ \sin\frac{\theta_{BO}}{2} & \cos\frac{\theta_{BO}}{2} \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|1\rangle\end{aligned} \tag{15}$$

Step 3. To prevent eavesdropping, Alice (Bob) prepares a decoy-photon sequence D_A (D_B), randomly selecting from four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Alice (Bob) inserts D_A into $|\chi_A\rangle$ (D_B into $|\chi_B\rangle$) at random positions. Throughout this process, Alice (Bob) carefully records the states and positions of the decoy photons. After the insertion of the decoy photons, the modified sequence is denoted as S_A (S_B). Alice (Bob) then sends S_A (S_B) to the TP for further processing.

Step 4. After confirming that the trusted party (TP) has received the sequences S_A (S_B), Alice (Bob) will publicly disclose the measurement bases for measuring the decoy photons. Specifically, the Z-basis was utilized for measuring states $|0\rangle$ and $|1\rangle$, and the X-basis was used for measuring states $|+\rangle$ and $|-\rangle$. Alice (Bob) will also publish the positions of the decoy photons D_A (D_B). The TP then performs quantum measurements on the decoy photons D_A and D_B to obtain the measurement results. These results are sent back to Alice and Bob, who can detect the presence of an eavesdropper (commonly referred to as "Eve") by comparing the measurement results with the initially prepared decoy photons. If the error rate exceeds a pre-agreed threshold, Alice and Bob will conclude that the communication has been compromised and will restart the protocol from Step 2. Conversely, if the error rates for both Alice and Bob are acceptable, the TP will send a confirmation message back to them. Subsequently, Alice announces her key θ_{AO} and Bob announces his key θ_{BO} to the TP.

Step 5. The TP recovers $|\chi_A\rangle$ ($|\chi_B\rangle$) by discarding all decoy photons in S_A (S_B). The TP then performs the rotation operation with the angle $-\theta_{AO}$ ($-\theta_{BO}$) on $|\chi_A\rangle$ ($|\chi_B\rangle$) to obtain the encoded single-photon state $|\alpha_A\rangle$ ($|\alpha_B\rangle$). This process can be given by

$$\begin{aligned}R_y(-\theta_{AO})|\chi_A\rangle &= \begin{pmatrix} \cos\frac{-\theta_{AO}}{2} & -\sin\frac{-\theta_{AO}}{2} \\ \sin\frac{-\theta_{AO}}{2} & \cos\frac{-\theta_{AO}}{2} \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\theta_{AO}}{2}+\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2x}+\frac{\theta_{AB}}{2}\right)|1\rangle = |\alpha_A\rangle\end{aligned} \tag{16}$$

$$\begin{aligned}R_y(-\theta_{BO})|\chi_B\rangle &= \begin{pmatrix} \cos\frac{-\theta_{BO}}{2} & -\sin\frac{-\theta_{BO}}{2} \\ \sin\frac{-\theta_{BO}}{2} & \cos\frac{-\theta_{BO}}{2} \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\theta_{BO}}{2}+\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \\ \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right) \end{pmatrix} \\ &= \cos\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y}+\frac{\theta_{AB}}{2}\right)|1\rangle = |\alpha_B\rangle\end{aligned} \tag{17}$$

Finally, the TP performs the swap test on $|\alpha_A\rangle$ and $|\alpha_B\rangle$ and measures the ancillary quantum state to obtain the measurement results.

Step 6. By executing Steps 2–5 a total of λ times, the process allows the TP to gather multiple measurement results from the ancillary quantum state. Once one of the measurement results appears as $|1\rangle$, TP can conclude that $x \neq y$; otherwise, $x = y$. The TP announces the comparison result to Alice and Bob at the same time.

4. Simulation

Consider a case in which Alice and Bob hold their own secret $x = 3$ and $y = 20$, respectively, and they want to determine whether $x = y$ without revealing x and y to each other, the TP, and any eavesdropper.

According to the protocol description, we assume that Alice and Bob share an angle $\theta_{AB} = \frac{3\pi}{4}$ through a QKD protocol. Alice (Bob) converts her (his) secret x (y) into an angle $\theta_A = \frac{\pi}{3}$ ($\theta_B = \frac{\pi}{20}$). When performing the rotation operation with the angle $\theta_A = \frac{\pi}{3}$ ($\theta_B = \frac{\pi}{20}$) on quantum state $|0\rangle$, the encoded single-photon state $|\alpha_A\rangle(|\alpha_B\rangle)$ can be expressed as

$$\begin{aligned} |\alpha_A\rangle = R_y\left(\tfrac{\pi}{3} + \tfrac{3\pi}{4}\right)|0\rangle = \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) & -\sin\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) & \cos\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|1\rangle = \cos\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|1\rangle \end{aligned} \tag{18}$$

$$\begin{aligned} |\alpha_B\rangle = R_y\left(\tfrac{\pi}{20} + \tfrac{3\pi}{4}\right)|0\rangle = \begin{pmatrix} \cos\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) & -\sin\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) & \cos\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|1\rangle = \cos\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|1\rangle \end{aligned} \tag{19}$$

Following that, we assume that Alice (Bob) generates her (his) own secret key $\theta_{AO} = \frac{7\pi}{8}$ ($\theta_{BO} = \frac{\pi}{3}$). When performing the rotation operation with the angle $\theta_{AO} = \frac{7\pi}{8}$ ($\theta_{BO} = \frac{\pi}{3}$) on the encoded single-photon state $|\alpha_A\rangle$ ($|\alpha_B\rangle$), the resulting single-photon state $|\chi_A\rangle(|\chi_B\rangle)$ can be given by

$$\begin{aligned} |\chi_A\rangle = R_y(\theta_{AO})|\alpha_A\rangle = \begin{pmatrix} \cos\frac{7\pi}{16} & -\sin\frac{7\pi}{16} \\ \sin\frac{7\pi}{16} & \cos\frac{7\pi}{16} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{7\pi}{16} + \frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{7\pi}{16} + \frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{7\pi}{16} + \tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{7\pi}{16} + \tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|1\rangle \end{aligned} \tag{20}$$

$$\begin{aligned} |\chi_B\rangle = R_y(\theta_{BO})|\alpha_B\rangle = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{\pi}{68} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{\pi}{68} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{\pi}{6} + \tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{6} + \tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|1\rangle \end{aligned} \tag{21}$$

Without considering the eavesdropping in Step 3 and Step 4 for simplification, the TP can recover $|\chi_A\rangle$ ($|\chi_B\rangle$) in Step 5. When performing the rotation operation with the angle $-\frac{7\pi}{8}$ $\left(-\frac{\pi}{3}\right)$ on $|\chi_A\rangle$ ($|\chi_B\rangle$) to obtain the encoded single-photon state $|\alpha_A\rangle(|\alpha_B\rangle)$, this process can be written as

$$\begin{aligned} R_y(-\theta_{AO})|\chi_A\rangle = \begin{pmatrix} \cos\frac{-7\pi}{16} & -\sin\frac{-7\pi}{16} \\ \sin\frac{-7\pi}{16} & \cos\frac{-7\pi}{16} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{7\pi}{16} + \frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{7\pi}{16} + \frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)|1\rangle = |\alpha_A\rangle \end{aligned} \tag{22}$$

$$\begin{aligned} R_y(-\theta_{BO})|\chi_B\rangle = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\pi}{6} + \frac{\pi}{68} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{6} + \frac{\pi}{68} + \frac{3\pi}{8}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \\ \sin\left(\frac{\pi}{40} + \frac{3\pi}{8}\right) \end{pmatrix} \\ = \cos\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|1\rangle = |\alpha_B\rangle \end{aligned} \tag{23}$$

When performing the swap test on $|\alpha_A\rangle$ and $|\alpha_B\rangle$ and measuring the ancillary quantum state, the probability that the measurement results are $|1\rangle$ is

$$\begin{aligned} P(|1\rangle) &= \tfrac{1}{2} - \tfrac{1}{2}\left|\left\langle\left(\cos\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)\langle 0| + \sin\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)\langle 1|\right)\middle|\cos\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|0\rangle + \sin\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)|1\rangle\right\rangle\right|^2 \\ &= \tfrac{1}{2} - \tfrac{1}{2}\left|\cos\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)\cos\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right) + \sin\left(\tfrac{\pi}{6} + \tfrac{3\pi}{8}\right)\sin\left(\tfrac{\pi}{40} + \tfrac{3\pi}{8}\right)\right| \\ &= \tfrac{1}{2} - \tfrac{1}{2}\left|\cos\left(\tfrac{\pi}{6} - \tfrac{\pi}{40}\right)\right|^2 = \tfrac{1}{2} - \tfrac{1}{2}\cos^2\left(\tfrac{\pi}{6} - \tfrac{\pi}{40}\right) = \tfrac{1}{2} - \tfrac{1}{2}\cos^2\left(\frac{17\pi}{120}\right) = 0.09267 \end{aligned} \tag{24}$$

Since the probability that the measurement results appear to be $|1\rangle$ is not 0, we can conclude that $x \neq y$.

The quantum circuit implementation of the above process for determining whether $x = y$ is shown in Figure 3. The measurement results obtained by executing the quantum circuit on the IBM Quantum Experience are presented in Figure 4.

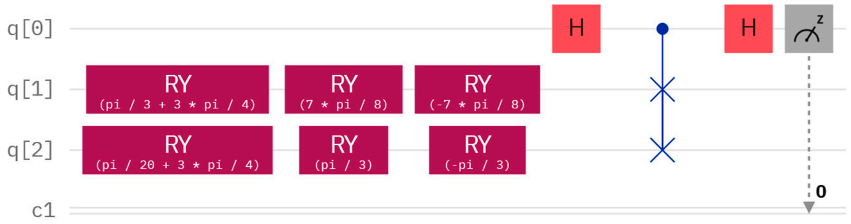

Figure 3. The quantum circuit for comparing x and y.

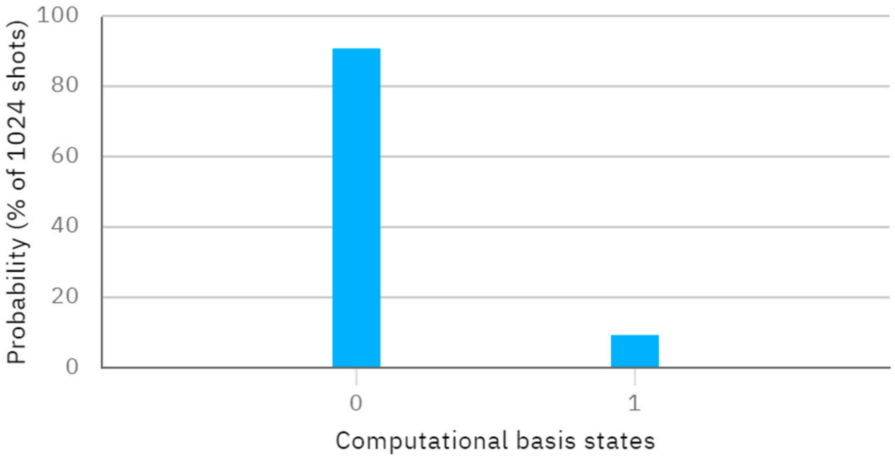

Figure 4. The measurement results correspond to the quantum circuit executed on the IBM Quantum Experience.

According to the measurement results, we find that quantum state $|1\rangle$ appears. This indicates that $x \neq y$.

Therefore, we verify the feasibility of the proposed protocol by performing a quantum circuit to compare x = 3 and y = 20 on the IBM Quantum Platform.

5. Analysis

5.1. Correctness

When performing the swap test on $|\alpha_A\rangle$ and $|\alpha_B\rangle$, the probability of $|1\rangle$ appearing can be expressed as

$$\begin{aligned}
P(|1\rangle) &= \frac{1}{2} - \frac{1}{2}\left|\left\langle\left(\cos\left(\frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\langle 0| + \sin\left(\frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\langle 1|\right)\right|\cos\left(\frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|1\rangle\right\rangle\right|^2 \\
&= \frac{1}{2} - \frac{1}{2}\left|\cos\left(\frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\cos\left(\frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right) + \sin\left(\frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\sin\left(\frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)\right| \\
&= \frac{1}{2} - \frac{1}{2}\left|\cos\left(\frac{\pi}{2x} - \frac{\pi}{2y}\right)\right|^2 = \frac{1}{2} - \frac{1}{2}\cos^2\left(\frac{\pi}{2x} - \frac{\pi}{2y}\right)
\end{aligned} \tag{25}$$

From Equation (25), we can know that $P(|1\rangle) = 0$ if and only if $x = y$. Therefore, we can conclude that $x \neq y$ once the measurement results appear as $|1\rangle$; otherwise, $x = y$.

5.2. Security

For the proposed QPC protocol, the attacks mainly come from the external adversary often referred to as Eve, who may intercept the quantum sequence transmitted in the quantum channel and the participants who utilize their intermediate calculation results to uncover the private information. In the following, we will show that our protocol is secure against these attacks.

5.2.1. External Attacks

External attacks refer to Eve's attempts to perform various common attack strategies, including intercept-resend, direct measurement, entangle-measure, and Trojan horse attacks, to extract information about the participants' secret integer to the greatest extent possible. However, the participants' secret integer is encoded as a single-photon state, which is transmitted to the TP. The TP's own secret key and decoy photon technology can be used to effectively prevent eavesdropping during this process. The following cases consider different attack strategies.

Case I. The intercept-resend attack

During this attack, Eve attempts to intercept the sequences S_A and S_B, measure them on a guessed measurement basis, and resend two fake sequences to the TP. S_A and S_B consist of decoy photons that are randomly chosen from four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which are used to enhance security against eavesdropping. After intercepting the quantum sequences, Eve can measure them but cannot distinguish between the decoy photons and the actual encoded qubits since Eve lacks knowledge of the specific positions of the decoy photons. Her measurements introduce disturbances that can be detected by Alice and Bob, thereby resulting in the termination of this protocol. For instance, for a decoy photon in state $|+\rangle$, if Eve chooses the X basis to measure it, she will pass the eavesdropping detection with a probability of 100%. Conversely, if Eve selects the Z basis to measure it, she will pass the eavesdropping detection with a probability of 50%. For Alice, the probability of choosing the X basis or the Z basis is 50%. Therefore, the probability that Eve can pass the eavesdropping detection is $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. For m decoy photons, the probability of this attack being detected is $1 - \left(\frac{3}{4}\right)^m$. As the number of decoy photons m increases sufficiently, the probability of detecting an intercept-resend attack approaches 1. This enhancement in detection capability means that Eve, attempting to execute the intercept-resend strategy, is unable to extract any meaningful information regarding Alice's or Bob's encoded qubits.

Case II. The direct measure attack

In a direct measurement attack, Eve intercepts the sequences S_A and S_B from Alice and Bob, respectively, and conducts measurements on them. However, without prior knowledge of the positions of the decoy photons, Eve faces significant challenges in accurately distinguishing between these decoys and the actual encoded qubits. Eve might attempt to substitute the original quantum sequences with a fabricated version when sending them to the TP. After the TP confirms the receipt of the sequence, Alice and Bob will disclose the positions of the decoy photons. At this stage, Eve can eliminate the decoy photons from S_A and S_B to obtain encoded single-photon states $|\chi_A\rangle$ and $|\chi_B\rangle$. Eve can then proceed to measure them using the measurement operator $M = |1\rangle\langle 1|$, allowing her to derive the measurement outcomes MA and MB corresponding to Alice's and Bob's encoded qubits, respectively.

$$\begin{aligned} MA &= |\chi_A\rangle|1\rangle\langle 1||\chi_A\rangle \\ &= \left(\cos\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\langle 0| + \sin\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)\langle 1|\right)|1\rangle\langle 1|\cos\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)|1\rangle \\ &= \sin^2\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right) \end{aligned} \tag{26}$$

$$\begin{aligned} MB &= |\chi_B\rangle|1\rangle\langle 1||\chi_B\rangle \\ &= \left(\cos\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)\langle 0| + \sin\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)\langle 1|\right)|1\rangle\langle 1|\cos\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|1\rangle \\ &= \sin^2\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right) \end{aligned} \tag{27}$$

However, the measurement outcome MA (MB) is intrinsically linked to the keys $\theta_{AO}(\theta_{BO})$ and θ_{AB}. Consequently, Eve cannot deduce the confidentiality of Alice's or Bob's secret integer without possessing knowledge of these keys.

Case III. The entangle-measure attack

In the entangle-measure attack, Eve intercepts the transmitted qubits and applies a unitary operation U_O to entangle her ancilla qubits $|e_i\rangle$ with the intercepted qubits. When performing the unitary operation U_O on the intercepted qubits in states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $|e_i\rangle$, the process can be described as follows:

$$U_O|0\rangle|e_i\rangle = c_{00}|0\rangle|e_{00}\rangle + c_{01}|1\rangle|e_{01}\rangle \tag{28}$$

$$U_O|1\rangle|e_i\rangle = c_{10}|0\rangle|e_{10}\rangle + c_{11}|1\rangle|e_{11}\rangle \tag{29}$$

$$\begin{aligned} U_O|+\rangle|e_i\rangle &= \tfrac{1}{\sqrt{2}}(U_O|0\rangle|e_i\rangle + U_O|1\rangle|e_i\rangle) \\ &= \tfrac{1}{\sqrt{2}}(c_{00}|0\rangle|e_{00}\rangle + c_{01}|1\rangle|e_{01}\rangle + c_{10}|0\rangle|e_{10}\rangle + c_{11}|1\rangle|e_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(c_{00}|e_{00}\rangle + c_{01}|e_{01}\rangle + c_{10}|e_{10}\rangle + c_{11}|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(c_{00}|e_{00}\rangle - c_{01}|e_{01}\rangle + c_{10}|e_{10}\rangle - c_{11}|e_{11}\rangle) \end{aligned} \tag{30}$$

$$\begin{aligned} U_O|-\rangle|e_i\rangle &= \tfrac{1}{\sqrt{2}}(U_O|0\rangle|e_i\rangle - U_O|1\rangle|e_i\rangle) \\ &= \tfrac{1}{\sqrt{2}}(c_{00}|0\rangle|e_{00}\rangle + c_{01}|1\rangle|e_{01}\rangle - c_{10}|0\rangle|e_{10}\rangle - c_{11}|1\rangle|e_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(c_{00}|e_{00}\rangle + c_{01}|e_{01}\rangle - c_{10}|e_{10}\rangle - c_{11}|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(c_{00}|e_{00}\rangle - c_{01}|e_{01}\rangle - c_{10}|e_{10}\rangle + c_{11}|e_{11}\rangle) \end{aligned} \tag{31}$$

Four quantum states $\{|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle\}$ are pure states uniquely defined by the unitary operation U_O, with coefficients that satisfy the conditions $|c_{00}|^2 + |c_{01}|^2 = 1$ and $|c_{10}|^2 + |c_{11}|^2 = 1$. Specifically, we have $|c_{00}|^2 = |c_{11}|^2 = F$ and $|c_{01}|^2 = |c_{10}|^2 = D$, where F represents fidelity and D denotes the quantum bit error rate (QBER). When the decoy photon is in the states $\{|0\rangle, |1\rangle\}$, the probability of obtaining the correct result is F. In contrast, when the decoy photon is in the states $\{|+\rangle, |-\rangle\}$, the probability of correctness drops to $1/2$. Therefore, for a decoy photon, the probability of obtaining the result successfully is written as

$$P_{\text{successful}} = \frac{1}{2}\left(F + \frac{1}{2}\right) \tag{32}$$

The probability of detecting Eve is given by

$$P_{\text{detected}} = 1 - p^m \tag{33}$$

where m represents the number of decoy photons. As m increases sufficiently, the probability of detecting Eve approaches 1.

When performing the entangle-measure attack on single-photon states $|\chi_A\rangle$ and $|\chi_B\rangle$, the process can be given by

$$\begin{aligned} U_o(|\chi_A\rangle|e_i\rangle) &= U_O\left(\cos\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|1\rangle\right)|e_i\rangle \\ &= |0\rangle\left(c_{00}\cos\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|e_{00}\rangle + c_{10}\sin\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|e_{10}\rangle\right) \\ &+|1\rangle\left(c_{01}\cos\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|e_{01}\rangle + c_{11}\sin\left(\tfrac{\theta_{AO}}{2} + \tfrac{\pi}{2x} + \tfrac{\theta_{AB}}{2}\right)|e_{11}\rangle\right) \end{aligned} \tag{34}$$

$$\begin{aligned} U_o(|\chi_B\rangle|e_i\rangle) &= U_O\left(\cos\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|0\rangle + \sin\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|1\rangle\right)|e_i\rangle \\ &= |0\rangle\left(c_{00}\cos\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|e_{00}\rangle + c_{10}\sin\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|e_{10}\rangle\right) \\ &+|1\rangle\left(c_{01}\cos\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|e_{01}\rangle + c_{11}\sin\left(\tfrac{\theta_{BO}}{2} + \tfrac{\pi}{2y} + \tfrac{\theta_{AB}}{2}\right)|e_{11}\rangle\right) \end{aligned} \tag{35}$$

To pass the eavesdropping detection, the coefficients in Equations (34) and (35) should satisfy $c_{10} = c_{01} = 0$ and $c_{00} = c_{11} = 1$. Therefore, Equations (34) and (35) can be written as

$$U_o(|\chi_A\rangle|e_i\rangle) = \cos\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)|0\rangle|e_{00}\rangle + \sin\left(\frac{\theta_{AO}}{2} + \frac{\pi}{2x} + \frac{\theta_{AB}}{2}\right)|1\rangle|e_{11}\rangle \quad (36)$$

$$U_o(|\chi_B\rangle|e_i\rangle) = \cos\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|0\rangle|e_{00}\rangle + \sin\left(\frac{\theta_{BO}}{2} + \frac{\pi}{2y} + \frac{\theta_{AB}}{2}\right)|1\rangle|e_{11}\rangle \quad (37)$$

From Equations (34) and (35), we know that the resulting quantum states are directly related to θ_{AO}, θ_{BO} and θ_{AB}. However, Eve has no chance of obtaining θ_{AO}, θ_{BO}, and θ_{AB}; therefore, it is impossible for Eve to deduce Alice's and Bob's secret integer.

Case IV. The Trojan horse attacks

The Trojan horse attacks, including the invisible photon eavesdropping attack and the delay-photon attack [64], mainly work in two-way quantum communication when a quantum sequence is transmitted in a bidirectional quantum channel. However, the quantum sequences S_A and S_B are transmitted in a unidirectional quantum channel to the TP. This indicates that our protocol is a one-way communication protocol, which can prevent the Trojan horse attacks automatically.

Based on the analysis presented above, external eavesdropping performed by Eve cannot be used to successfully acquire the participants' secret integer.

5.2.2. Participant Attacks

Participant attacks are, in fact, more formidable than outsider attacks. For participants, they have a chance of knowing some immediate results and can legally utilize this information to infer the participant's secret integer. The following two cases of participant attacks are considered.

Case 1. Attacks from Alice (Bob)

In this protocol, the quantum sequence S_A (S_B) encoding the secret integer is transmitted to the TP, whose security is ensured by the decoy state technology and the rotation operation with the angle on the secret key. The role of Alice in this protocol is analogous to that of Bob. We assume that Bob intercepts the sequence S_A like Eve does and resends a fake sequence to the TP who will then announce the positions of the decoy photons in S_A. Bob can recover the quantum state $|\chi_A\rangle$ by discarding all decoy photons in S_A. Even though this behavior has been detected, Bob has obtained the quantum state $|\chi_A\rangle$ and can deduce the secret integer x. $|\chi_A\rangle$ is generated by performing the rotation operation with the angle θ_{AO} on the encoded single-photon state $|\alpha_A\rangle$, and θ_{AO} will not be published once the quantum channel is not secure. Therefore, Bob has no chance of obtaining θ_{AO}, resulting in the quantum state $|\chi_A\rangle$ being concealed. Additionally, the quantum state $|\chi_A\rangle$, in fact, is unknown to the other participants, and an unknown quantum state is indistinguishable. This results in it being impossible for Bob to steal Alice's secret integer x. A similar analysis can be conducted on Alice with respect to stealing Bob's secret integer y. To conclude, x and y remain confidential throughout the whole process.

Case 2. Attacks from the TP

The TP is expected to adhere to the protocol as designed and will not collude with the participants. However, despite following the rules, the TP may still attempt to extract additional information from the data it processes. Although the TP has knowledge of $|\alpha_A\rangle$ ($|\alpha_B\rangle$) , which are generated by performing the rotation operation with the angle $\theta_A + \theta_{AB}$ ($\theta_B + \theta_{AB}$) on quantum state $|0\rangle$, she cannot extract Alice's or Bob's private information without access to the shared secret key θ_{AB}. Without knowing θ_{AB}, $|\alpha_A\rangle$ ($|\alpha_B\rangle$)

is unknown to the TP. Since an unknown quantum state is indistinguishable, the TP has no chance of knowing Alice's secret integer x and Bob's secret integer y. Therefore, the participants' secret integers remain undisclosed to the TP.

5.3. Fairness

The fairness of the protocol is guaranteed by the introduction of a TP who announces the comparison result to both Alice and Bob. This simultaneous disclosure ensures that neither participant has an advantage over the other.

6. Comparison

A comparison between our protocol and several existing QPC protocols is presented in Table 1, focusing on the quantum states used, the need for entanglement swapping, quantum communication methods, the technology used, the quantum measurement method, and the comparison method.

Table 1. A comparison between our protocol and several existing QPC protocols.

Protocol	Quantum States Used	Need of Entanglement Swapping	Quantum Communication Methods	Technology Used	Quantum Measurement Method	Comparison Method
Ref. [26]	EPR pairs	No	Two-way	Unitary operations and hash function	Bell-basis	Bit-to-bit
Ref. [27]	Single photon	No	Two-way	Unitary operations	Single-particle	Bit-to-bit
Ref. [41]	GHZ states	No	Two-way	Rotation operations	GHZ-basis	Bit-to-bit
Ref. [42]	Four-particle cluster and extended Bell state	Yes	One-way	quantum-one-time pad	Bell-basis and extended-Bell-basis	Bit-to-bit
Ref. [43]	hyper-entangled GHZ states	Yes	One-way	quantum-one-time pad	Bell-basis	Bit-to-bit
Ref. [54]	d-dimensional Bell state	No	One-way	Unitary operation	Single-particle	Bit-to-bit
Ours	Single photon	No	One-way	Rotation operation	Single-particle	Secret-to-secret

According to Table 1, our protocol offers several advantages over existing QPC protocols, including the following:

(1) It uses a novel method for secret-to-secret comparison rather than the traditional bit-to-bit comparison, resulting in improved scalability;

(2) It does not require entanglement swapping technology and integrates single-photon states, rotation operations, and the swap test as key components, facilitating easier implementation with quantum technology;

(3) All qubits are transmitted using one-way communication, eliminating the need for wavelength quantum filters and photon number splitters to mitigate Trojan horse attacks;

(4) It employs single-particle measurements instead of Bell-basis measurements, thereby reducing the measurement requirements.

7. Conclusions

In this paper, we propose a two-party quantum private comparison (QPC) protocol that utilizes the properties of the swap test to evaluate the similarity of two qubits. The participants compare their secret integers by encoding these integers directly into the amplitudes of single-photon states, which are concealed using rotation operations. Without knowledge of the rotation angles, the encoded single-photon states remain secure. By introducing a semi-honest third party (TP) to facilitate the comparison between participants without accessing their private information, the protocol ensures fairness. Simulations conducted on the IBM Quantum Platform demonstrate the protocol's feasibility, while a security analysis confirms its resilience against potential eavesdropping and participant attacks. Compared with existing QPC protocols that employ bit-to-bit comparison methods, our approach offers enhanced practicality and scalability. The integration of single-photon states, rotation operations, and the swap test as key components for direct secret comparison simplifies implementation with modern technology. In the future, we will focus on applying this protocol to the areas of quantum voting and quantum auctions, exploring its potential to enhance security and privacy in these critical applications.

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 the Network and Data Security Key Laboratory of Sichuan Province (Grant No. NDS2024-1) 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. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Zhang, W.; van Leent, T.; Redeker, K. A device-independent quantum key distribution system for distant users. *Nature* **2022**, *607*, 687–691. [CrossRef] [PubMed]
3. Xu, F.; Ma, X.; Zhang, Q. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
4. Liu, Y.; Zhang, W.J.; Jiang, C. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **2023**, *130*, 210801. [CrossRef] [PubMed]
5. Liu, W.Z.; Zhang, Y.Z.; Zhen, Y.Z. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.* **2022**, *129*, 050502. [CrossRef] [PubMed]
6. Mehic, M.; Niemiec, M.; Rass, S. Quantum key distribution: A networking perspective. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–41. [CrossRef]
7. Tsai, C.W.; Yang, C.W.; Lin, J. Multiparty mediated quantum secret sharing protocol. *Quantum Inf. Process.* **2022**, *21*, 63. [CrossRef]
8. Hu, W.W.; Zhou, R.G.; Li, X. A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quantum Inf. Process.* **2021**, *20*, 159. [CrossRef]
9. Wang, S.; Liu, B.; Huang, W. Memory-free quantum secret sharing protocol with collective detection. *Quantum Inf. Process.* **2023**, *22*, 181. [CrossRef]
10. Shen, A.; Cao, X.Y.; Wang, Y. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci. China Phys. Mech. Astron.* **2023**, *66*, 260311. [CrossRef]
11. Huang, X.; Zhang, S.B.; Chang, Y. Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 838–847. [CrossRef]
12. Karim, F.; Abulkasim, H.; Alabdulkreem, E. Improvements on new quantum key agreement protocol with five-qubit Brown states. *Mod. Phys. Lett. A* **2022**, *37*, 2250128. [CrossRef]
13. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef] [PubMed]
14. Zhang, H.; Sun, Z.; Qi, R. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci. Appl.* **2022**, *11*, 83. [CrossRef]
15. Cao, Z.; Lu, Y.; Chai, G. Realization of quantum secure direct communication with continuous variable. *Research* **2023**, *6*, 0193. [CrossRef] [PubMed]
16. Huang, X.; Zhang, S.; Chang, Y. Quantum secure direct communication based on quantum homomorphic encryption. *Mod. Phys. Lett. A* **2021**, *36*, 2150263. [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. Debnath, S.K.; Dey, K.; Kundu, N. Feasible private set intersection in quantum domain. *Quantum Inf. Process.* **2021**, *20*, 41. [CrossRef]
19. Liu, W.J.; Li, W.B.; Wang, H.B. An improved quantum private set intersection protocol based on hadamard gates. *Int. J. Theor. Phys.* **2022**, *61*, 53. [CrossRef]

20. Chen, Y.; Situ, H.; Huang, Q. A novel quantum private set intersection scheme with a semi-honest third party. *Quantum Inf. Process.* **2023**, *22*, 429. [CrossRef]
21. 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.
22. Boudot, F.; Schoenmakers, B.; Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
23. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
24. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
25. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]
26. 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]
27. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
28. Liu, B.; Gao, F.; Jia, H.Y. Efficient quantum private comparison employing single photons and collective detection. *Quantum Inf. Process.* **2013**, *12*, 887–897. [CrossRef]
29. Chen, X.B.; Su, Y.; Niu, X.X. Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. *Quantum Inf. Process.* **2014**, *13*, 101–112. [CrossRef]
30. Liu, B.; Xiao, D.; Huang, W. Quantum private comparison employing single-photon interference. *Quantum Inf. Process.* **2017**, *16*, 180. [CrossRef]
31. Kou, T.Y.; Che, B.C.; Dou, Z. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. *Chin. Phys. B* **2022**, *31*, 060307. [CrossRef]
32. 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]
33. Wen, L.; Wang, Y.B.; Wei, C. Quantum private comparison protocol based on Bell entangled states. *Commun. Theor. Phys.* **2012**, *57*, 583.
34. Tseng, H.Y.; Lin, J.; Hwang, T. New quantum private comparison protocol using EPR pairs. *Quantum Inf. Process* **2012**, *11*, 373–384. [CrossRef]
35. Hou, M.; Sun, S.Y.; Zhang, W. Quantum private comparison for the socialist millionaire problem. *Front. Phys.* **2024**, *12*, 1408446. [CrossRef]
36. Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. [CrossRef] [PubMed]
37. Lang, Y.F. Quantum private comparison using single bell state. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036. [CrossRef]
38. Lang, Y.F. Quantum gate-based quantum private comparison. *Int. J. Theor. Phys.* **2020**, *59*, 833–840. [CrossRef]
39. Huang, X.; Zhang, S.B.; Chang, Y. Efficient quantum private comparison based on entanglement swapping of bell states. *Int. J. Theor. Phys.* **2021**, *60*, 3783–3796. [CrossRef]
40. Hou, M.; Wu, Y. Efficient Quantum Private Comparison with Unitary Operations. *Mathematics* **2024**, *12*, 3541. [CrossRef]
41. Hou, M.; Wu, Y.; Zhang, S. Efficient Quantum Private Comparison Based on GHZ States. *Entropy* **2024**, *26*, 413. [CrossRef] [PubMed]
42. Li, C.; Chen, X.; Li, H. 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]
43. Gianni, J.; Qu, Z. New quantum private comparison using hyperentangled ghz state. *J. Quantum Comput.* **2021**, *3*, 45–54. [CrossRef]
44. 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]
45. 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]
46. Sun, Q. Quantum private comparison with six-particle maximally entangled states. *Mod. Phys. Lett. A* **2022**, *37*, 2250149. [CrossRef]
47. 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]
48. Fan, P.; Rahman, A.U.; Ji, Z. Two-party quantum private comparison based on eight-qubit entangled state. *Mod. Phys. Lett. A* **2022**, *37*, 2250026. [CrossRef]
49. 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; pp. 1–4.
50. 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]

51. Hou, M.; Wu, Y.; Zhang, S. New Quantum Private Comparison Using Four-Particle Cluster State. *Entropy* **2024**, *26*, 512. [CrossRef]
52. Chang, Y.; Zhang, W.B.; Zhang, S.B. Quantum private comparison of equality based on five-particle cluster state. *Commun. Theor. Phys.* **2016**, *66*, 621. [CrossRef]
53. Huang, X.; Zhang, S.; Xia, J. Efficient Quantum Private Comparison Using Locally Indistinguishable Orthogonal Product States. In Proceedings of the 8th International Conference on Artificial Intelligence and Security, Qinghai, China, 15–20 July 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 260–273.
54. Lin, S.; Sun, Y.; Liu, X.F. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf. Process.* **2013**, *12*, 559–568. [CrossRef]
55. Guo, F.Z.; Gao, F.; Qin, S.J. Quantum private comparison protocol based on entanglement swapping of d-level Bell states. *Quantum Inf. Process.* **2013**, *12*, 2793–2802. [CrossRef]
56. Yu, C.H.; Guo, G.D.; Lin, S. Quantum private comparison with d-level single-particle states. *Phys. Scr.* **2013**, *88*, 065013. [CrossRef]
57. Ye, C.Q.; Ye, T.Y. Multi-party quantum private comparison of size relation with d-level single-particle states. *Quantum Inf. Process.* **2018**, *17*, 252. [CrossRef]
58. Song, X.L.; Wen, A.J.; Gou, R. Multiparty quantum private comparison of size relation based on single-particle states. *IEEE Access* **2019**, *7*, 142507–142514. [CrossRef]
59. Buhrman, H.; Cleve, R.; Watrous, J. Quantum fingerprinting. *Phys. Rev. Lett.* **2001**, *87*, 167902. [CrossRef] [PubMed]
60. Kang, M.S.; Choi, H.W.; Pramanik, T. Universal quantum encryption for quantum signature using the swap test. *Quantum Inf. Process.* **2018**, *17*, 254. [CrossRef]
61. Huang, X.; Zhang, S.; Lin, C. Quantum Fuzzy Support Vector Machine for Binary Classification. *Comput. Syst. Sci. Eng.* **2023**, *45*, 2783–2794. [CrossRef]
62. 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]
63. Huang, X.; Chang, Y.; Cheng, W. Quantum private comparison of arbitrary single qubit states based on swap test. *Chin. Phys. B* **2022**, *31*, 040303. [CrossRef]
64. Li, Z.H.; Wang, L.; Xu, J. Counterfactual trojan horse attack. *Phys. Rev. A* **2020**, *101*, 022336. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.