mathematics

IMPACT FACTOR 2.2

CITESCORE 4.6

Article

Swap Test-Based Quantum Protocol for Private Array Equality Comparison

Min Hou and Shibin Zhang

Special Issue

Recent Advances in Quantum Theory and Its Applications

Edited by

Dr. Laure Gouba

MDPI

https://doi.org/10.3390/math13152425

mathematics

MDPI

Article

Swap Test-Based Quantum Protocol for Private Array Equality Comparison

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

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

Abstract

Private array equality comparison (PAEC) aims to evaluate whether two arrays are equal while maintaining the confidentiality of their elements. Current private comparison protocols predominantly focus on determining the relationships of secret integers, lacking exploration of array comparisons. To address this issue, we propose a swap test-based quantum protocol for PAEC, which satisfies both functionality and security requirements using the principles of quantum mechanics. This protocol introduces a semi-honest third party (TP) that acts as a medium for generating Bell states as quantum resources and distributes the first and second qubits of these Bell states to the respective participants. They encode their array elements into the received qubits by performing rotation operations. These encoded qubits are sent to TP to derive the comparison results. To verify the feasibility of the proposed protocol, we construct a quantum circuit and conduct simulations on the IBM quantum platform. Security analysis further indicates that our protocol is resistant to various quantum attacks from outsider eavesdroppers and attempts by curious participants.

Keywords: private array equality comparison (PAEC); swap test; Bell states; rotation encryption; security

MSC: 81P94; 81P65

Academic Editor: Laure Gouba

Received: 25 June 2025
Revised: 24 July 2025
Accepted: 25 July 2025
Published: 28 July 2025

Citation: Hou, M.; Zhang, S. Swap Test-Based Quantum Protocol for Private Array Equality Comparison. *Mathematics* **2025**, *13*, 2425. https://doi.org/10.3390/math13152425

1. Introduction

Quantum information science has advanced significantly in recent decades, with quantum cryptography emerging as a pivotal field. By exploiting quantum mechanical principles, such as superposition and entanglement, quantum cryptography achieves security guarantees unattainable by classical methods reliant on computational complexity. The field originated with Bennett and Brassard's BB84 protocol [1], the first quantum cryptographic scheme proven unconditionally secure. Since then, numerous protocols integrating quantum mechanics with cryptographic primitives have been developed to counter threats from quantum computing, including quantum key distribution [2–4], quantum key agreement [5,6], quantum private set intersection [7–9], and quantum secure direct communication [10–13].

Secure multiparty computation (MPC) is a vital cryptographic framework that facilitates collaborative computation among multiple parties while ensuring the privacy of their private inputs [14]. The "millionaires' problem" [15] serves as a foundational MPC protocol, allowing two parties to compare wealth without disclosing their exact amounts. Boudot et al. [16] extended this to equality checks, enabling parties to verify if their inputs match while preserving secrecy. While early works focus on two-party scenarios, Lo [17] highlighted inherent security limitations in such settings, advocating for the involvement of a semi-honest third party (TP) to enhance security.

Traditional private comparison methods often rely on computational hardness assumptions, such as integer factorization—fundamental to public-key cryptosystems like RSA—and discrete logarithms, which underpin many cryptographic protocols. However, these foundations face significant threats from quantum algorithms: Shor algorithm [18] and Grover algorithm [19]. Shor algorithm solves integer factorization and discrete logarithm problems in polynomial time, posing a risk to public-key cryptosystems and potentially rendering them obsolete. Grover algorithm effectively halves the key lengths of symmetric-key cryptography, compromising security through accelerated search capabilities. These vulnerabilities highlight the urgent need for quantum-resistant cryptographic solutions in the post-quantum era. As quantum computing advances, developing secure protocols that can withstand these threats becomes increasingly critical.

To counter the threats posed by quantum computing, quantum private comparison (QPC) protocols have been developed by integrating classical comparison techniques with principles of quantum mechanics. These protocols offer enhanced security guarantees, ensuring the confidentiality of private inputs even against adversaries with quantum computational capabilities. Yang and Wen [20] introduced the first QPC protocol, utilizing Einstein–Podolsky–Rosen (EPR) pairs as quantum resources and employing a one-way hash function to securely verify the equality of two integers. Subsequent protocols have leveraged various quantum states (e.g., single photons [21,22], entangled states [23–28], cluster states [29–32], and d-level quantum states [33,34]) to enhance functionality and security. Wu and Zhao [35] expanded QPC to enable size relationship comparisons using d-dimensional Bell states. Lang [36] introduced quantum private magnitude comparison (QPMC), which allows for determining the larger of two inputs. Huang et al. [37] enhanced scalability by employing swap tests to compare single-qubit quantum states. Additionally, semi-quantum private comparison (SQPC) [38–43] protocols have been proposed to achieve private comparison functionality while alleviating the current shortage of quantum resources and avoiding the high costs associated with using complete quantum equipment. Despite the various QPC protocols proposed, most focus on determining the relationships of secret integers and lack exploration into array comparisons. Designing a private array equality comparison (PAEC) scheme remains a challenging issue.

The swap test [44] is a pivotal quantum subroutine used to measure the overlap between two quantum states, providing a means to determine their similarity without fully collapsing the states. Its unique properties make it a cornerstone in various quantum communication and computing applications, such as quantum signature [45], quantum-enhanced neural network [46,47], and the blind millionaire's problem [48]. The versatility of the swap test highlights its importance in addressing complex cryptographic and computational challenges in the quantum realm.

To address the limitation of existing QPC protocols, which are confined to comparing single integers, we propose the first swap test-based quantum protocol for PAEC. This approach allows for the comparison of arrays while maintaining confidentiality and robustness against various attacks. The key contributions of the protocol are as follows.

(1) We propose a swap test-based quantum protocol for PAEC, in which two participants encode their array elements into qubits received from a semi-honest TP by performing rotation operations. They then return the encoded states to TP to derive the results without revealing any array elements.
(2) The proposed protocol utilizes near-term feasible quantum technologies, including Bell states, rotation operations, and swap tests, as core components, which are easier to simulate on quantum platforms. To verify the feasibility of the proposed protocol, we simulate it using the IBM Quantum Composer.
(3) Due to the use of decoy photon insertion for eavesdropping detection and rotation operations to obfuscate encoded information, the protocol exhibits robustness against quantum attacks from outsider eavesdroppers and attempts by curious participants.
(4) Unlike existing QPC schemes that are typically limited to single-integer comparisons, the proposed protocol enables comparisons of two arrays.

The rest of this paper is organized as follows. Section 2 reviews the concepts of rotation operation and the swap test. Section 3 details the design of the proposed protocol, outlining its framework and operational steps. Section 4 presents the simulation experiment, demonstrating the protocol's feasibility and performance on a quantum computing platform. Section 5 offers a comprehensive analysis, including correctness, security, and fairness. Section 6 contains a comparison of the proposed protocol with existing QPC protocols, highlighting its advantages and enhancements. Section 7 concludes the work.

2. Preliminaries

2.1. Rotation Operation

The rotation operation around the y-axis [49] can be written as

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

This operation is a unitary transform that satisfies the following relation:

$$R_y{}^{\dagger}(\theta) R_y(\theta) = R_y(-\theta) R_y(\theta) = I \tag{2}$$

Here, I represents the identity matrix and the parameter θ can be viewed as an encryption key.

When applying $R_y(\theta)$ to the quantum states $|0\rangle$ and $|1\rangle$, we obtain the following results:

$$R_y(\theta)|0\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle \tag{3}$$

$$R_y(\theta)|0\rangle = \cos\left(\frac{\theta}{2}\right)|1\rangle - \sin\left(\frac{\theta}{2}\right)|0\rangle \tag{4}$$

Therefore, the transformation of the quantum states $|0\rangle$ and $|1\rangle$ into superposition states through the rotation operation $R_y(\theta)$ serves as an effective encryption mechanism. Without knowledge of the angle θ, it is impossible to recover the original states $|0\rangle$ and $|1\rangle$.

The recovery of the original quantum states is accomplished by executing $R_y(-\theta)$ on the resulting states. The recovery process is as follows.

$$R_y(-\theta)\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle\right) = R_y(-\theta) R_y(\theta)|0\rangle = |0\rangle \tag{5}$$

$$R_y(-\theta)\left(\cos\left(\frac{\theta}{2}\right)|1\rangle - \sin\left(\frac{\theta}{2}\right)|0\rangle\right) = R_y(-\theta) R_y(\theta)|1\rangle = |1\rangle \tag{6}$$

2.2. Swap Test

The swap test [44] is a quantum circuit designed to evaluate the similarity between two quantum states of identical dimensionality, which is shown in Figure 1. Its core is to estimate the modulus squared of the inner product $|\langle\psi_1 | \psi_2\rangle|^2$ between two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$. An ancillary qubit is introduced into the circuit, which plays a crucial role in measuring the similarity between the states and the measurement outcome of the ancilla qubit provides the probability related to the inner product of the two states.

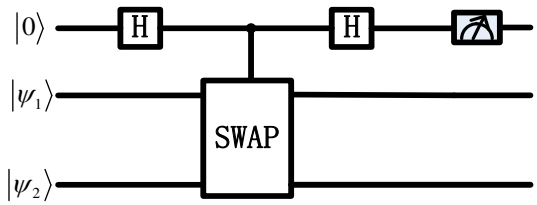

Figure 1. The quantum circuit of swap test.

A schematic representation of the swap test's quantum circuit typically includes the following:

- *Input states*: Two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$.
- *Ancillary qubit*: Initialized to $|0\rangle$.
- *Hadamard gate*: Applied to the ancillary qubit to create a superposition.
- *Controlled-SWAP gate*: The states $|\psi_1\rangle$ and $|\psi_2\rangle$ interact with the ancillary qubit via a controlled-SWAP operation.
- *Measurement*: The ancillary qubit is measured to determine the probability of being in state $|0\rangle$ or $|1\rangle$.

By conducting a swap test on two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$, the probability of the ancillary qubit being in state $|0\rangle$ or $|1\rangle$ are expressed as follows:

$$P(|0\rangle) = \frac{1}{2} + \frac{1}{2}|\langle\psi_1 | \psi_2\rangle|^2 \tag{7}$$

$$P(|1\rangle) = \frac{1}{2} - \frac{1}{2}|\langle\psi_1 | \psi_2\rangle|^2 \tag{8}$$

Therefore, we can derive that

$$|\langle\psi_1 | \psi_2\rangle|^2 = 2P(|0\rangle) - 1 \text{ or } |\langle\psi_1 | \psi_2\rangle|^2 = 1 - 2P(|1\rangle) \tag{9}$$

Theorem 1. *When performing the swap test on two quantum states* $|\psi_1\rangle = cos(\alpha_1)|0\rangle + sin(\alpha_1)|1\rangle$ *and* $|\psi_2\rangle = cos(\alpha_2)|0\rangle + sin(\alpha_2)|1\rangle$*, where* $\alpha_1, \alpha_2 \in [0, \pi)$*, the modulus squared of the inner product* $|\psi_1 | \psi_2|^2$ *is* $cos^2(\alpha_1 - \alpha_2)$.

Proof. The inner product $\psi_1|\psi_2$ is computed as follows:

$$\begin{aligned}
&\langle\psi_1|\psi_2\rangle = (\cos(\alpha_1)\langle 0| + \sin(\alpha_1)\langle 1|)(\cos(\alpha_2)|0\rangle + \sin(\alpha_2)|1\rangle) \\
&= \cos(\alpha_1)\cos(\alpha_2)\langle 0|0\rangle + \cos(\alpha_1)\sin(\alpha_2)\langle 0|1\rangle \\
&+ \sin(\alpha_1)\cos(\alpha_2)\langle 1|0\rangle + \sin(\alpha_1)\sin(\alpha_2)\langle 1|1\rangle \\
&= \cos(\alpha_1)\cos(\alpha_2) + \sin(\alpha_1)\sin(\alpha_2) \\
&= \cos(\alpha_1 - \alpha_2)
\end{aligned} \tag{10}$$

Combined Equations (8) and (10), we deduce that:

$$\begin{aligned} P(|1\rangle) &= \tfrac{1}{2} - \tfrac{1}{2}|\langle\psi_1 | \psi_2\rangle|^2 \\ &= \tfrac{1}{2} - \tfrac{1}{2}\cos^2(\alpha_1 - \alpha_2) \end{aligned} \tag{11}$$

Therefore, the modulus squared of the inner product $|\langle\psi_1 | \psi_2\rangle|^2$ is given by

$$\begin{aligned} |\langle\psi_1 | \psi_2\rangle|^2 &= 1 - 2P(|1\rangle) \\ &= 1 - 2\left(\tfrac{1}{2} - \tfrac{1}{2}\cos^2(\alpha_1 - \alpha_2)\right) \\ &= \cos^2(\alpha_1 - \alpha_2) \end{aligned} \tag{12}$$

□

3. Design of the Proposed Protocol

The proposed protocol is designed to securely determine the equality of two arrays A and B, owned by distinct parties, Alice and Bob, with the assistance of a semi-honest third party (TP). The two arrays are defined as $A = (a_0, a_1, \ldots, a_{L-1})$ and $B = (b_0, b_1, \ldots, b_{L-1})$. Both arrays must have the same length L, which is known to TP. TP prepares L Bell states as quantum resources and announces the comparison result to both Alice and Bob. As a semi-honest participant, TP follows the protocol without colluding with either party.

The proposed protocol must guarantee the following properties:

- *Correctness*: If both Alice and Bob input their arrays honestly and comply with the protocol, TP will accurately announce the comparison result.
- *Security*: The arrays A and B remain confidential from both other participants and potential attackers, ensuring the confidentiality of the participants' inputs.
- *Fairness*: Each party receives the comparison result simultaneously, preventing any asymmetric information advantages.

The protocol assumes lossless and noiseless quantum channels. Classical channels between the participants are authenticated to prevent unauthorized access. However, in practical scenarios, quantum error-correcting codes [50] can be implemented to detect and correct errors induced by noise. Before the protocol begins, it is assumed that Alice and Bob share a secret key $K_{AB} = (\theta_0^{AB}, \theta_1^{AB}, \ldots, \theta_{L-1}^{AB})$ using a quantum key distribution protocol. This key facilitates secure communications and operations within the protocol. A detailed outline of the steps is as follows, and the diagram is shown in Figure 2.

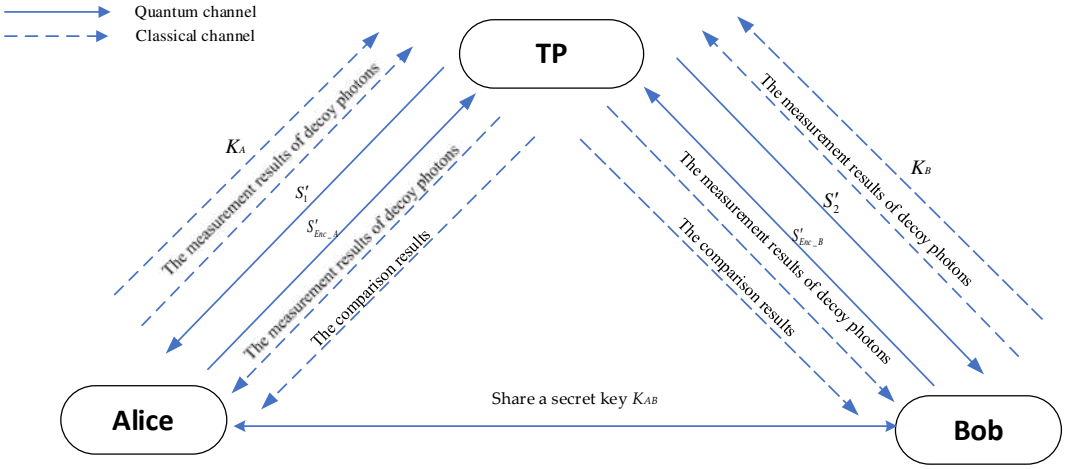

Figure 2. The diagram of the proposed protocol.

Step 1: Preparation byTP

(1) TP prepares L Bell states in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and organizes the first and second particles into two quantum sequences S_1 and S_2, respectively.
(2) To mitigate eavesdropping risks, TP prepares 2δ decoy photons from the set $\left\{|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, inserts δ decoy photons into S_1 to create S'_1, and inserts another δ decoy photons into S_2 to create S'_2.
(3) TP records the positions and states of the decoy photons, and sends S'_1 and S'_2 to Alice and Bob via quantum channels, respectively.

Step 2. Confirmation and Measurement of Decoy Photons

(1) Upon receiving S'_1 and S'_2, Alice and Bob send confirmation information to TP via an authenticated classical channel.
(2) TP announces the positions and measurement bases for the decoy photons. If the decoy photon is in states $|0\rangle$ or $|1\rangle$, the Z basis is used; otherwise, the X basis is applied.
(3) Alice and Bob measure the decoy photons and send results back to TP, which computes the error rate. If the error rate exceeds a predefined threshold ($\tau = 2\sim8.9\%$) depending on the channel situation [51,52], the protocol is aborted and restarted.

Step 3. Encoding and Encrypting Arrays

(1) Alice and Bob remove the decoy photons from S'_1 and S'_2 to recover S_1 and S_2, respectively.
(2) Alice encodes each element a_i in array A as $\theta_i^A = \frac{\pi}{a_i}$ (notably, if $a_i = 0$, then $\theta_i^A = 0$). Bob encodes each element b_i in array B using the same method.
(3) Alice applies $R_y\left(\theta_i^A + \theta_i^{AB}\right)$ to the i-th qubit in S_1, and Bob applies $R_y\left(\theta_i^B + \theta_i^{AB}\right)$ to the i-th qubit in S_2, generating sequences S_A and S_B, respectively.
(4) Alice generates an encrypted key $K_A = \left(\theta_0^{Enc\_A}, \theta_1^{Enc\_A}, \ldots, \theta_L^{Enc\_A}\right)$, and Bob generates $K_B = \left(\theta_0^{Enc\_B}, \theta_1^{Enc\_B}, \ldots, \theta_L^{Enc\_B}\right)$.
(5) Alice and Bob apply the rotation operations $R_y\left(\theta_i^{Enc\_A}\right)$ and $R_y\left(\theta_i^{Enc\_B}\right)$ to the i-th qubit in S_A and S_B, resulting in encrypted sequences S_{Enc_A} and S_{Enc_B}, respectively.
(6) Both Alice and Bob prepare δ decoy photons and insert them into their respective encrypted sequences, forming S'_{Enc_A} and S'_{Enc_B}, and send these to TP via quantum channels.

Step 4. Eavesdropping Detection

(1) When TP receives S'_{Enc_A} and S'_{Enc_B}, he interacts with Alice and Bob to check for eavesdropping.
(2) Alice and Bob compute the error rate as in Step 2. If the error rate is acceptable, they publish their secret keys K_A and K_B to TP.

Step 5. Recovery and Comparison

(1) TP removes decoy photons from S'_{Enc_A} and S'_{Enc_B} to recover S_{Enc_A} and S_{Enc_B}, respectively.
(2) TP applies $R_y\left(-\theta_i^{Enc\_A}\right)$ and $R_y\left(-\theta_i^{Enc\_B}\right)$ to the i-th qubit in S_{Enc_A} and S_{Enc_B}, respectively, to obtain sequences S_A and S_B.
(3) TP conducts swap tests on each i-th qubit in sequences S_A and S_B.
(4) TP measures the ancilla qubits from the swap tests to obtain measurement results.

Step 6: Final Result Announcement

(1) By performing the above steps λ times, TP collects multiple measurement results.

(2) If any measurement result indicates $|1\rangle$, the arrays A and B are not identical. If all results indicate $|0\rangle$, the arrays are the same.
(3) TP announces the result to Alice and Bob simultaneously.

4. Simulation

Consider a case where Alice and Bob wish to determine whether their arrays $A = [3, 6]$ and $B = [3, 2]$ are identical without revealing any elements. Suppose that they share a secret key $K_{AB} = \left(\frac{\pi}{3}, \frac{3\pi}{4}\right)$ in advance. Since both the lengths of arrays A and B are 2, TP prepares 2 Bell states in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. TP organizes the first and second particles into quantum sequences S_1 and S_2.

For simplification, we do not take the eavesdropping detection process into account. Alice encodes her array A as angles $\theta^A = \left[\frac{\pi}{3}, \frac{\pi}{6}\right]$ and Bob encodes his array B as angles $\theta^B = \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$, respectively. Alice applies $R_y\left(\frac{\pi}{3} + \frac{\pi}{3}\right)$ and $R_y\left(\frac{\pi}{6} + \frac{3\pi}{4}\right)$ to the qubits in S_1, generating sequence S_A. Bob applies $R_y\left(\frac{\pi}{3} + \frac{\pi}{3}\right)$ and $R_y\left(\frac{\pi}{2} + \frac{3\pi}{4}\right)$ to the qubits in S_2, generating sequence S_B. The encrypted keys generated by Alice and Bob are assumed to be $K_A = \left(\frac{4\pi}{5}, \frac{5\pi}{6}\right)$ and $K_B = \left(\frac{5\pi}{8}, \frac{\pi}{7}\right)$, respectively. Alice applies $R_y\left(\frac{4\pi}{5}\right)$ and $R_y\left(\frac{5\pi}{6}\right)$ to the qubits in S_A, generating sequence S_{Enc_A}. Bob applies $R_y\left(\frac{5\pi}{8}\right)$ and $R_y\left(\frac{\pi}{7}\right)$ to the qubits in S_B, producing sequence S_{Enc_B}.

Disregard eavesdropping detection for simplification. When receiving K_A and K_B, TP applies $R_y\left(-\frac{4\pi}{5}\right)$ and $R_y\left(-\frac{5\pi}{6}\right)$ to qubits in S_{Enc_A} to obtain S_A, and applies $R_y\left(-\frac{5\pi}{8}\right)$ and $R_y\left(-\frac{\pi}{7}\right)$ to obtain S_B. TP performs swap tests on the first and second qubits of S_A and S_B, measuring the ancilla qubits to obtain the measurement results.

To validate the feasibility of the proposed protocol using this case, we construct a quantum circuit and simulate it using the IBM Quantum Composer. The IBM Quantum Composer is a user-friendly graphical tool designed for constructing and executing quantum circuits. Users can easily build quantum circuits by dragging and dropping various quantum operations (including single-qubit gates, controlled-qubit gates, and measurement operations) onto a canvas. When simulating this protocol, eavesdropping detection, a separate procedure for identifying eavesdropping rather than for encoding information, is excluded from the simulation. The quantum circuit for comparing arrays A and B is shown in Figure 3, and the measurement results displayed in the form of histograms after executing the quantum circuit are shown in Figure 4.

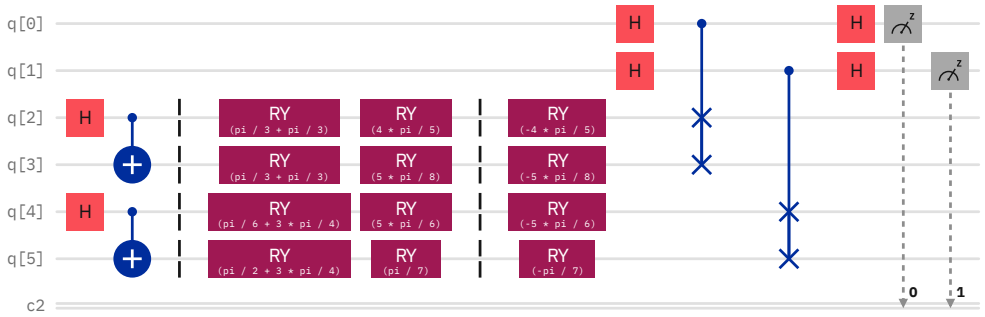

Figure 3. The quantum circuit for comparing the arrays A and B (where q[0] to q[5] are quantum registers with 6 qubits, c2 is a classical register with 2 bits, and H represents the Hadamard operation).

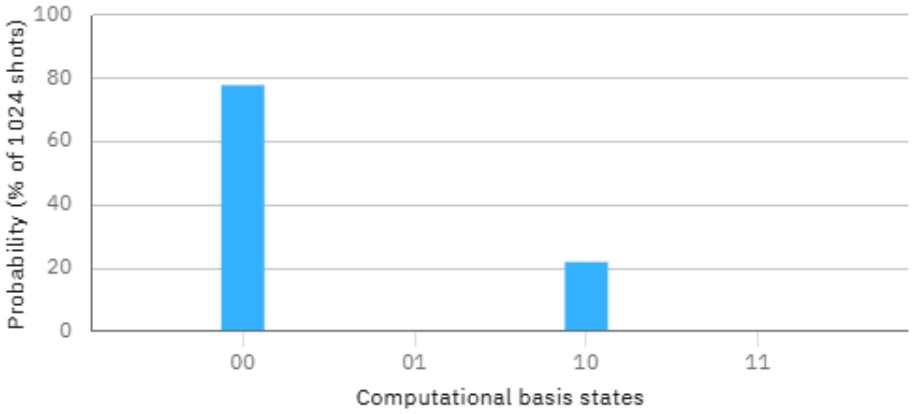

Figure 4. The measurement results obtained from executing the quantum circuit 1024 times (where 0 and 1 on the horizontal axis denote the quantum states $|0\rangle$ and $|1\rangle$, respectively).

Based on the measurement results shown in Figure 4, we conclude that the measurement result of q[0] is in the state $|0\rangle$, while the measurement results of q[1] can be either $|0\rangle$ or $|1\rangle$. According to the proposed scheme, if any measurement result indicates the state $|1\rangle$, it confirms that the arrays A and B are not identical. Since the measurement results of q[1] include the state $|1\rangle$, we conclude that the arrays A and B are indeed not identical. This simulation illustrates the feasibility of the proposed protocol by providing a concrete example on a quantum computing platform.

5. Analysis

5.1. Correctness

Let $P(|1\rangle)$ denote the probability of measuring the ancilla qubit in state $|1\rangle$. When conducting swap tests on each i-th qubit in sequences S_A and S_B, the probability that the i-th ancilla qubit is in the state $|1\rangle$ can be expressed as

$$\begin{aligned} P_i(|1\rangle) &= \frac{1}{2} - \frac{1}{2}\left|\left\langle \left(\cos\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\langle 0| + \sin\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\langle 1|\right) \middle| \cos\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)|0\rangle + \sin\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)|1\rangle \right\rangle\right|^2 \\ &= \frac{1}{2} - \frac{1}{2}\left|\cos\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\cos\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right) + \sin\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\sin\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)\right| \\ &= \frac{1}{2} - \frac{1}{2}\left|\cos\left(\frac{\theta_i^A}{2}-\frac{\theta_i^B}{2}\right)\right|^2 = \frac{1}{2} - \frac{1}{2}\cos^2\left(\frac{\theta_i^A}{2}-\frac{\theta_i^B}{2}\right) \end{aligned} \tag{13}$$

$$\begin{aligned} P_i(|1\rangle) &= \frac{1}{2} - \frac{1}{2}\left|\left\langle \left(-\sin\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\langle 0| + \cos\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\langle 1|\right) \middle| -\sin\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)|0\rangle + \cos\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)|1\rangle \right\rangle\right|^2 \\ &= \frac{1}{2} - \frac{1}{2}\left|\left(-\sin\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\right)\left(-\sin\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)\right) + \cos\left(\frac{\theta_i^A}{2}+\frac{\theta_i^{AB}}{2}\right)\cos\left(\frac{\theta_i^B}{2}+\frac{\theta_i^{AB}}{2}\right)\right| \\ &= \frac{1}{2} - \frac{1}{2}\left|\cos\left(\frac{\theta_i^A}{2}-\frac{\theta_i^B}{2}\right)\right|^2 = \frac{1}{2} - \frac{1}{2}\cos^2\left(\frac{\theta_i^A}{2}-\frac{\theta_i^B}{2}\right) \end{aligned} \tag{14}$$

Based on Equations (13) and (14), we conclude that the ancilla qubit yields the state $|1\rangle$ with a probability of 0 if and only if the angles θ_i^A and θ_i^B are identical. That is, $P(|1\rangle) = 0$ if and only if $\theta_i^A = \theta_i^B$. In other words, if any measurement result of the ancilla qubit indicates the state $|1\rangle$, it indicates that the arrays A and B are not identical. Conversely, if all measurement results yield the state $|0\rangle$, it confirms that the arrays A and B are the same.

5.2. Security

Eavesdroppers may attempt to intercept the quantum sequences transmitted between Alice, Bob, and TP, or use Trojan horse methods to gain access to the quantum systems

and deduce information about the inputs. Additionally, participating entities, such as TP, could potentially exploit information from the protocol to infer the inputs of Alice and Bob. To counter these threats, decoy photons are employed to detect eavesdropping attempts. By inserting decoy photons into the quantum sequences, the sender can monitor for discrepancies in measurement outcomes. An elevated error rate in measurements indicates potential eavesdropping, prompting the protocol to abort if necessary. The secret keys are used to encrypt the quantum states, ensuring that even if the quantum sequences are intercepted, the actual information remains concealed from eavesdroppers. Furthermore, the use of rotation operations based on the secret keys adds another layer of security, making it difficult for attackers to deduce the original input values. The combined use of decoy photons and secret key encryption maintains the confidentiality of the arrays A and B. Below, we will provide a concrete analysis regarding the confidentiality of the arrays A and B.

5.2.1. Outside Attacks

In the context of the proposed protocol, an external attacker, often referred to as Eve, may attempt various quantum-based attacks to extract the arrays A and B. These attacks include intercept-measure-resend, entangle-measure, and Trojan horse attacks.

Case I. Intercept-measure-resend attack

Eve intercepts the quantum sequences S'_{Enc_A} and S'_{Enc_B} that contain encoded private information sent from Alice and Bob to TP. She measures these sequences using randomly chosen measurement bases (either Z-basis or X-basis). Based on her measurement results (e.g., $|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$), Eve prepares and sends two fake sequences to TP. However, decoy photons are inserted at random positions within the quantum sequences specifically to detect eavesdropping. Eve cannot differentiate between the actual target states and the decoy photons when she intercepts the sequences. If Eve measures a decoy photon using an incorrect basis (e.g., measuring a decoy in the X-basis when it was prepared in the Z-basis), the measurement results will be $|+\rangle$ or $|-\rangle$, leading to an increased error rate. For a decoy photon prepared in the Z-basis (e.g., $|0\rangle$), if she uses the Z-basis, she may obtain the correct result $|0\rangle$. If she uses the X-basis, she has a 50% chance of getting the correct result. In the X-basis, measuring $|0\rangle$ gives outcomes $|+\rangle$ or $|-\rangle$, and measuring $|1\rangle$ also results in $|+\rangle$ or $|-\rangle$). Therefore, the probability that Eve gets the correct result and passes the eavesdropping detection for a single decoy photon is calculated as follows:

$$P(\text{pass for a decoy photon}) = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \tag{15}$$

For δ decoy photons, the probability that Eve passes the eavesdropping detection becomes

$$P(\text{pass for } \delta \text{ decoy photon}) = 1 - \left(\frac{3}{4}\right)^{\delta} \tag{16}$$

When $\delta = 20$, $P(\text{pass for 20 decoy photons}) = 1 - \left(\frac{3}{4}\right)^{20} = 0.9968$. As δ increases, this probability approaches 1, indicating that Eve's behavior will likely be detected during the eavesdropping detection process.

Case II. Entangle-measure attack

In the entangle-measure attack, Eve applies a special unitary transformation U to entangle the intercepted states with the ancilla qubits. The goal is to create a situation where she can infer the target states by measuring the ancilla qubits. The transformation

U acts on the intercepted qubits in states such as $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ along with the ancilla states $|a_i\rangle$. The operation can be represented as follows:

$$U|0\rangle|a_i\rangle = u_{00}|0\rangle|a_{00}\rangle + u_{01}|1\rangle|a_{01}\rangle \tag{17}$$

$$U|1\rangle|a_i\rangle = u_{10}|0\rangle|a_{10}\rangle + u_{11}|1\rangle|a_{11}\rangle \tag{18}$$

$$\begin{aligned} U|+\rangle|a_i\rangle &= \tfrac{1}{\sqrt{2}}(U|0\rangle|a_i\rangle + U|1\rangle|a_i\rangle) \\ &= \tfrac{1}{\sqrt{2}}(u_{00}|0\rangle|a_{00}\rangle + u_{01}|1\rangle|a_{01}\rangle + u_{10}|0\rangle|a_{10}\rangle + u_{11}|1\rangle|a_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(u_{00}|a_{00}\rangle + u_{01}|a_{01}\rangle + u_{10}|a_{10}\rangle + u_{11}|a_{11}\rangle) \\ &+ \tfrac{1}{2}|-\rangle(u_{00}|a_{00}\rangle - u_{01}|a_{01}\rangle + u_{10}|a_{10}\rangle - u_{11}|a_{11}\rangle) \end{aligned} \tag{19}$$

$$\begin{aligned} U|-\rangle|a_i\rangle &= \tfrac{1}{\sqrt{2}}(U|0\rangle|a_i\rangle - U|1\rangle|a_i\rangle) \\ &= \tfrac{1}{\sqrt{2}}(u_{00}|0\rangle|a_{00}\rangle + u_{01}|1\rangle|a_{01}\rangle - u_{10}|0\rangle|a_{10}\rangle - u_{11}|1\rangle|a_{11}\rangle) \\ &= \tfrac{1}{2}|+\rangle(u_{00}|a_{00}\rangle + u_{01}|a_{01}\rangle - u_{10}|a_{10}\rangle - u_{11}|a_{11}\rangle) \\ &+ \tfrac{1}{2}|-\rangle(u_{00}|a_{00}\rangle - u_{01}|a_{01}\rangle - u_{10}|a_{10}\rangle + u_{11}|a_{11}\rangle) \end{aligned} \tag{20}$$

where $\{|a_{00}\rangle, |a_{01}\rangle, |a_{10}\rangle, |a_{11}\rangle\}$ are four pure states determined by the operation U and the parameters satisfy the following:

$$|u_{10}|^2 + |u_{11}|^2 = 1 \tag{21}$$

$$|u_{00}|^2 + |u_{01}|^2 = 1 \tag{22}$$

To avoid detection during eavesdropping, the following conditions must be met.

$$u_{01} = 0, u_{10} = 0 \tag{23}$$

$$u_{00}|a_{00}\rangle = u_{11}|a_{11}\rangle \tag{24}$$

Substituting the results from Equations (23) and (24) into Equations (17)–(20), we derive the following:

$$U|0\rangle|a_i\rangle = u_{00}|0\rangle|a_{00}\rangle \tag{25}$$

$$U|1\rangle|a_i\rangle = u_{11}|1\rangle|a_{11}\rangle = u_{00}|1\rangle|a_{00}\rangle \tag{26}$$

$$U|+\rangle|a_i\rangle = \frac{1}{2}|+\rangle(u_{00}|a_{00}\rangle + u_{11}|a_{11}\rangle) = u_{00}|+\rangle|a_{00}\rangle = u_{11}|+\rangle|a_{11}\rangle \tag{27}$$

$$U|-\rangle|a_i\rangle = \frac{1}{2}|-\rangle(u_{00}|a_{00}\rangle + u_{11}|a_{11}\rangle) = u_{00}|-\rangle|a_{00}\rangle = u_{11}|-\rangle|a_{11}\rangle \tag{28}$$

Based on Equations (25)–(28), we conclude that no entanglement exists between the intercepted qubits and the ancilla states. If Eve measures the ancilla qubits and obtains the result $|a_{00}\rangle$, she still cannot determine the states of the intercepted qubits, which could be $|0\rangle$ or $|1\rangle$. Similarly, if Eve measures the ancilla qubits and obtains the result $|a_{11}\rangle$, she remains unable to infer the states of the intercepted qubits, which could be $|+\rangle$ or $|-\rangle$. Consequently, the entangle-measure attack does not succeed.

Case III. Trojan horse attacks

Trojan horse attacks pose a significant threat to quantum communication protocols, particularly those utilizing bidirectional quantum channels. These attacks include two categories: delay-photon and invisible photon attacks [53]. Given that the proposed protocol utilizes Bell states as information carriers transmitted between TP, Alice, and Bob, it is inherently vulnerable to these Trojan horse attacks. However, by implementing wavelength quantum filters and photon number splitters, the scheme can maintain its confidentiality

and integrity against these attacks. Such measures ensure that only legitimate photons are transmitted, effectively securing the communication against potential eavesdropping.

5.2.2. Participant Attacks

The proposed protocol effectively secures the confidentiality of arrays A and B against potential threats from TP, Alice, and Bob. Below are detailed analyses of how the protocol addresses these threats.

Case I. Security Against TP's Threat

TP is considered semi-honest, meaning it follows the protocol without colluding with either participant. However, it has access to the initial quantum sequences S_1 and S_2 as well as the final sequences S_A and S_B. The sequences S_A and S_B are generated by applying rotation operations $R_y\left(\theta_i^A + \theta_i^{AB}\right)$ and $R_y\left(\theta_i^B + \theta_i^{AB}\right)$ to the i-th qubit in S_1 and S_2, and the angles θ_i^A and θ_i^B are derived from the elements a_i and b_i in arrays A and B. However, the angle θ_i^{AB} is shared between Alice and Bob but remains unknown to TP. Without knowledge of θ_i^{AB}, TP cannot access the angles θ_i^A and θ_i^B due to the quantum indeterminacy. Even if TP measures sequences S_A and S_B, the results will only yield the measurement outcomes of $|0\rangle$ or $|1\rangle$, without revealing the specifics of the rotation angles. Therefore, the arrays A and B remain confidential from TP, demonstrating the scheme's security against threats from TP.

Case II. Security Against Alice's or Bob's Threat

Both participants have analogous roles. In this scenario, we assume Alice attempts to extract Bob's array B. The i-th element in Bob's array B is encoded into the angle θ_i^B, used to transform the i-th qubit in sequence S_2. The sequence S_B is then encrypted using $R_y\left(\theta_i^{Enc\_B}\right)$ to the i-th qubit in S_B, and the encrypted sequence S_{Enc_B} includes decoy photons, resulting in a modified sequence S'_{Enc_B} sent to TP. Although Alice can measure the sequence S_1 to know the corresponding qubits in S_2 due to entanglement (for example, if Alice's measurement result is $|0\rangle$, then Bob's measurement result must also be $|0\rangle$, owing to the entanglement correlation in Bell states), she cannot determine the target states in S_{Enc_B}. If Alice intercepts S'_{Enc_B} and tries to resend a fake sequence, this behavior will be detected, leading to an aborted protocol. Even if Alice discards the decoy photons to access S_{Enc_B} and measures S_{Enc_B} to obtain the measurement results $|0\rangle$ or $|1\rangle$, she cannot deduce θ_i^B without also knowing $\theta_i^{Enc\_B}$. The angle $\theta_i^{Enc\_B}$ is only announced if the eavesdropping detection is passed—something Alice cannot achieve if she attempts to tamper with the sequences. The quantum nature of the sequences ensures that Alice cannot ascertain any information about S_B without also knowing $\theta_i^{Enc\_B}$. Thus, the array B remains undisclosed to her. A similar argument holds for Bob regarding Alice's array A. Therefore, our protocol is secure against threats from either Alice or Bob.

5.3. Fairness

The introduction of a third party (TP) in the proposed protocol plays a crucial role in ensuring the fairness of the protocol while determining the equality of the arrays A and B. TP measures the ancilla qubits resulting from the swap tests conducted between the sequences S_A and S_B, and analyzes the measurement results from the ancilla qubits. If any result indicates the state $|1\rangle$, it signifies that the arrays are not identical. If all results indicate $|0\rangle$, it confirms that the arrays are the same. After obtaining the measurement results, TP announces the comparison outcome to both Alice and Bob at the same time. This simultaneous announcement prevents either participant from gaining any advantage over the other, ensuring that both parties have equal access to the results.

6. Comparison

The proposed protocol presents several advantages over existing QPC schemes. Below, we compare our protocol with previous QPC schemes in terms of quantum resources, unitary operation, entanglement swapping operation, quantum measurement, and comparison object (Table 1).

Table 1. A comparison between the proposed protocol and previous schemes.

Protocol	Quantum Resources	Unitary Operation	Entanglement Swapping Operation	Quantum Measurement	Comparison Object
Ref. [25]	$2L$ Bell states	No	Yes	GHZ-basis	Binary representation of integer
Ref. [26]	$L + 4m$ χ-type entangled states	Yes	Yes	Joint	Binary representation of integer
Ref. [31]	$2L$ Four-qubit cluster state and extended Bell state	No	Yes	Bell basis and extended Bell basis	Binary representation of integer
Ref. [33]	$(1 + \delta)$ d-level Bell state	Yes	Yes	d-level Bell basis	Integer
Ref. [34]	$2L$ d-level Bell state	No	No	d-level single-particle	Integer
Ours	$2\lambda L$ Bell states	Yes	No	Single-particle (Z basis)	Array

(1) Unlike existing QPC schemes [25,26,31,33,34] that are typically limited to single-integer comparisons, the proposed protocol enables comparisons of two arrays. This scalability makes it more suitable for practical applications.

(2) The proposed protocol utilizes Bell states, rotation operations, and swap tests, avoiding the need for entanglement swapping [25,26,31,33] and d-level quantum states [33,34]. This simplification reduces the operational complexity of the protocol and enhances its compatibility with current quantum technologies, facilitating implementation.

(3) The proposed protocol employs single-particle measurements rather than Bell-basis measurements [31], joint measurements [26], or d-level quantum state measurements [33,34]. Single-particle measurements require base vector projection of a single quantum state (e.g., Z-basis, X-basis), without the need for multi-particle cooperative operations. In contrast, joint measurements necessitate multi-particle interference, which is hindered by imperfections in light sources. Additionally, d-dimensional quantum state measurements require the design of d orthogonal basis vectors, and high-dimensional control is vulnerable to decoherence effects. For instance, in remote state preparation, d-level Bell state measurement demands customized quantum gates and entanglement sources, with experimental difficulty increasing exponentially with d. This approach reduces the measurement requirements, making the protocol more practical and easier to implement.

7. Conclusions

In this paper, we introduce the first swap test-based quantum protocol specifically designed for private array equality comparison. Participants encode their array elements

into rotation angles of operations performed on shared Bell states, which are encrypted before being transmitted to the TP. TP decrypts the received states and conducts swap tests on two particles of the Bell states to derive the results of the array comparison. Due to the utilization of decoy photon technology for detecting eavesdropping and the rotation operations used for encoding and encrypting quantum information, the proposed protocol is resilient against both external eavesdroppers and internal threats. By announcing the results simultaneously, the protocol ensures fairness, preventing any participant from gaining an advantage over the other. Unlike existing QPC schemes that focus on single-integer comparisons, our protocol supports array comparisons, making it more applicable to real-world scenarios. The elimination of entanglement swapping and d-level quantum states simplifies the protocol, relying on components (Bell states, rotation operations, swap tests) that are compatible with current quantum technologies. Future research will focus on adapting the protocol to function efficiently in noisy quantum environments and exploring semi-quantum architectures that can reduce quantum resource demands while maintaining the security of the protocol.

Author Contributions: Conceptualization, M.H.; methodology, M.H.; Writing—original draft, M.H.; writing—review and editing, S.Z.; supervision, 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 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: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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, 9–12 December 1984; pp. 175–179.
2. Li, Y.; Cai, W.Q.; Ren, J.G.; Wang, C.Z.; Yang, M.; Zhang, L.; Wu, H.Y.; Chang, L.; Wu, J.C.; Jin, B.; et al. Microsatellite-based real-time quantum key distribution. *Nature* **2025**, *640*, 47–54. [CrossRef]
3. Liu, Y.; Zhang, W.-J.; Jiang, C.; Chen, J.-P.; Zhang, C.; Pan, W.-X.; Ma, D.; Dong, H.; Xiong, J.-M.; Zhang, C.-J.; et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **2023**, *130*, 210801. [CrossRef] [PubMed]
4. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 839–894. [CrossRef]
5. Huang, X.; Zhang, S.-B.; Chang, Y.; Qiu, C.; Liu, D.-M.; Hou, M. Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 838–847. [CrossRef]
6. Lin, S.; Zhang, X.; Guo, G.-D.; Wang, L.-L.; Liu, X.-F. Multiparty quantum key agreement. *Phys. Rev. A* **2021**, *104*, 042421. [CrossRef]
7. 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]
8. Hou, M.; Wu, Y.; Zhang, S. Quantum Private Set Intersection Scheme Based on Bell States. *Axioms* **2025**, *14*, 120. [CrossRef]
9. 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]
10. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef]
11. 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]
12. Ying, J.W.; Wang, J.Y.; Xiao, Y.X.; Gu, S.P.; Wang, X.F.; Zhong, W.; Du, M.M.; Li, X.Y.; Shen, S.T.; Zhang, A.L.; et al. Passive-state preparation for quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2025**, *68*, 240312. [CrossRef]

13. 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]
14. Lindell, Y. Secure multiparty computation. *Commun. ACM* **2020**, *64*, 86–96. [CrossRef]
15. 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.
16. Boudot, F.; Schoenmakers, B.; Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
17. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A.* **1997**, *56*, 1154–1162. [CrossRef]
18. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
19. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]
20. 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]
21. 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]
22. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
23. 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]
24. 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]
25. 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]
26. Jia, H.Y.; Wen, Q.Y.; Li, Y.B.; Gao, F. Quantum private comparison using genuine four-particle entangled states. *Int. J. Theor. Phys.* **2012**, *51*, 1187–1194. [CrossRef]
27. Sun, Q. Quantum private comparison with six-particle maximally entangled states. *Mod. Phys. Lett. A* **2022**, *37*, 2250149. [CrossRef]
28. Hou, M.; Wu, Y. Efficient Quantum Private Comparison with Unitary Operations. *Mathematics* **2024**, *12*, 3541. [CrossRef]
29. Hou, M.; Wu, Y.; Zhang, S. New Quantum Private Comparison Using Four-Particle Cluster State. *Entropy* **2024**, *26*, 512. [CrossRef]
30. Xu, G.A.; Chen, X.B.; Wei, Z.H.; Li, M.J.; Yang, Y.X. An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. *Int. J. Quantum Inf.* **2012**, *10*, 1250045. [CrossRef]
31. 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]
32. Chang, Y.; Zhang, W.-B.; Zhang, S.-B.; Wang, H.-C.; Yan, L.-L.; Han, G.-H.; Sheng, Z.-W.; Huang, Y.-Y.; Suo, W.; Xiong, J.-X. Quantum private comparison of equality based on five-particle cluster state. *Commun. Theor. Phys.* **2016**, *66*, 621. [CrossRef]
33. Guo, F.Z.; Gao, F.; Qin, S.J.; Zhang, J.; Wen, Q.Y. Quantum private comparison protocol based on entanglement swapping of d-level Bell states. *Quantum Inf. Process.* **2013**, *12*, 2793–2802. [CrossRef]
34. Wang, B.; Gong, L.H.; Liu, S.Q. Multi-party quantum private size comparison protocol with d-dimensional Bell states. *Front. Phys.* **2022**, *10*, 981376. [CrossRef]
35. Wu, W.Q.; Zhao, Y.X. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 155. [CrossRef]
36. Lang, Y.F. Quantum private magnitude comparison. *Int. J. Theor. Phys.* **2022**, *61*, 100. [CrossRef]
37. Huang, X.; Chang, Y.; Cheng, W.; Hou, M.; Zhang, S.-B. Quantum private comparison of arbitrary single qubit states based on swap test. *Chin. Phys. B* **2022**, *31*, 040303. [CrossRef]
38. Lin, P.H.; Hwang, T.; Tsai, C.W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [CrossRef]
39. 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]
40. 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]
41. Lian, J.Y.; Li, X.; Ye, T.Y. Multi-party semiquantum private comparison of size relationship with d-dimensional Bell states. *EPJ Quantum Technol.* **2023**, *10*, 207. [CrossRef]
42. Gong, L.H.; Li, M.L.; Cao, H.; Wang, B. Novel semi-quantum private comparison protocol with Bell states. *Laser Phys. Lett.* **2024**, *21*, 055209. [CrossRef]

43. Gong, L.H.; Ye, Z.J.; Liu, C.; Zhou, S. One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations. *Laser Phys. Lett.* **2024**, *21*, 035207. [CrossRef]
44. Buhrman, H.; Cleve, R.; Watrous, J.; de Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett.* **2001**, *87*, 167902. [CrossRef] [PubMed]
45. Kang, M.S.; Choi, H.W.; Pramanik, T.; Han, S.W.; Moon, S. Universal quantum encryption for quantum signature using the swap test. *Quantum Inf. Process.* **2018**, *17*, 254. [CrossRef]
46. Zhao, J.; Zhang, Y.-H.; Shao, C.-P.; Wu, Y.-C.; Guo, G.-C.; Guo, G.-P. Building quantum neural networks based on a swap test. *Phys. Rev. A* **2019**, *100*, 012334. [CrossRef]
47. Li, P.; Wang, B. Quantum neural networks model based on swap test and phase estimation. *Neural Netw.* **2020**, *130*, 152–164. [CrossRef] [PubMed]
48. 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]
49. Hou, M.; Wu, Y. Quantum Privacy Comparison with Ry Rotation Operation. *Mathematics* **2025**, *13*, 1071. [CrossRef]
50. Beale, S.J.; Wallman, J.J.; Gutiérrez, M.; Brown, K.R.; Laflamme, R. Quantum error correction decoheres noise. *Phys. Rev. Lett.* **2018**, *121*, 190501. [CrossRef]
51. Jennewein, T.; Simon, C.; Weihs, G.; Weinfurter, H.; Zeilinger, A. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **2000**, *84*, 4729. [CrossRef]
52. Hughes, R.J.E.; Nordholt, J.; 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]
53. Li, Z.H.; Wang, L.; Xu, J.; Yang, Y.; Al-Amri, M.; Zubairy, M.S. Counterfactual trojan horse attack. *Phys. Rev. A* **2020**, *101*, 022336. [CrossRef]