mathematics

IMPACT FACTOR 2.2

CITESCORE 4.6

Article

Quantum Private Array Content Comparison Based on Multi-Qubit Swap Test

Min Hou, Yue Wu and Shibin Zhang

Special Issue

Mathematical Physics and Applied Mathematics: Latest Advances and Prospects

Edited by

Prof. Dr. Màrius Josep Fullana i Alfonso

MDPI

https://doi.org/10.3390/math13233827

mathematics

MDPI

Article

Quantum Private Array Content Comparison Based on Multi-Qubit Swap Test

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

[1] School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China; houmin@scujj.edu.cn (M.H.); ywu@uestc.edu.cn (Y.W.)
[2] Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China
[3] College of Artificial Intelligence, 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

Current private comparison schemes primarily focus on comparing single secret integers using quantum technologies, while the area of private array content comparison remains relatively unexplored. To bridge this gap, we introduce a quantum private array content comparison (QPACC) scheme based on multi-qubit swap test. This scheme integrates rotation operation, quantum homomorphic encryption (QHE), and multi-qubit swap test to facilitate the equality comparison of array contents while ensuring their confidentiality. In our approach, participants encode their array elements into the phases of quantum states using rotation operations, which are then encrypted via QHE. These encrypted quantum states are sent to a semi-honest third party (TP) who decrypts the encoded quantum states and computes the modulus squared sum of the inner products of these decoded quantum states using the multi-qubit swap test, thereby determining the equality relationship of the array contents. To verify the feasibility of the proposed scheme, we conduct a case simulation using IBM Qiskit. Security analysis indicates that the proposed scheme is resistant to quantum attacks (including intercept-resend, entangle-measure, and quantum Trojan horse attacks) from outsider eavesdroppers and attempts by curious participants.

Keywords: quantum private array content comparison; rotation operation; quantum homomorphic encryption; multi-qubit swap test; quantum cryptography

MSC: 81P94; 81P65

Academic Editor: Màrius Josep Fullana i Alfonso

Received: 30 October 2025
Revised: 21 November 2025
Accepted: 26 November 2025
Published: 28 November 2025

Citation: Hou, M.; Wu, Y.; Zhang, S. Quantum Private Array Content Comparison Based on Multi-Qubit Swap Test. *Mathematics* **2025**, *13*, 3827. https://doi.org/10.3390/math13233827

1. Introduction

Quantum cryptography has emerged as a cornerstone of secure communication in the post-quantum era, leveraging fundamental principles of quantum mechanics such as superposition and entanglement to achieve security levels that are potentially unattainable by classical cryptographic protocols reliant on computational complexity [1]. Since the pioneering work of the BB84 quantum key distribution (QKD) protocol [2], the field has expanded rapidly, giving rise to a diverse suite of quantum cryptographic primitives including quantum key agreement [3–6], quantum secret sharing [7–9], quantum summation [10,11], and quantum private set intersection [12–14].

A pivotal subfield within cryptography is secure multiparty computation (MPC) [15], which enables multiple parties to jointly compute a function over their private inputs while

preserving the confidentiality of those inputs. The classic "millionaires' problem" [16] is a quintessential example, allowing two parties to compare their wealth without disclosure. Subsequent work extended this to equality checks [17], a fundamental building block for more complex protocols. However, traditional solutions based on computational hardness assumptions are critically threatened by the advent of quantum algorithms, notably Shor algorithm [18] and Grover algorithm [19]. This vulnerability has catalyzed the development of quantum private comparison (QPC) protocols, which integrate classical comparison tasks with the inherent security of quantum mechanics.

The original QPC framework, proposed by Yang and Wen [20], leverages the quantum correlations of EPR pairs and the security of a one-way hash function to verify that two classical integers held by different parties are equal. This seminal work catalyzed extensive research, leading to a diverse ecosystem of QPC protocols designed to enhance both functionality and security. Subsequent developments have explored a wide range of quantum state encodings, including single photons [21–23], various entangled states [24–30], cluster states [31,32], and d-level quantum systems [33–35], each offering distinct advantages. Moving beyond simple equality comparison, the scope of QPC has been expanded to include more complex comparisons. Wu and Zhao [36] extended the paradigm to d-level systems for comparing input sizes, a capability formalized as quantum private magnitude comparison (QPMC) by Lang [37] to identify the maximum of two private inputs. Addressing scalability, Huang et al. [38] later demonstrated that the swap test could be employed for the direct comparison of single-qubit states. Concurrently, to address the current limitations of quantum technology, the paradigm of semi-quantum private comparison (SQPC) [39–43] has emerged. SQPC protocols achieve the desired comparison functionality while relaxing the quantum requirements for participants, thereby alleviating resource constraints and reducing the high costs associated with full quantum capabilities.

Despite the considerable progress, a notable gap persists in the literature. The majority of existing QPC protocols are fundamentally designed for comparing individual integers, focusing primarily on determining equality or magnitude relationships. The more complex task of privately comparing the content of entire arrays remains relatively unexplored. The design of a secure quantum private array content comparison (QPACC) protocol poses a distinct challenge, as it requires the coordinated, confidential comparison of multiple elements without leaking information about the individual array contents.

To address this gap, we propose a QPACC scheme based on the multi-qubit swap test. Our work makes several key contributions:

(1) We introduce a QPACC scheme capable of securely determining the equality of two arrays, moving beyond the limitation of single-integer comparisons that characterizes existing schemes.
(2) The scheme is constructed using near-term feasible quantum technologies, including single-qubit states as quantum resources, rotation operations for encoding, quantum homomorphic encryption (QHE) for encrypting the encoded quantum states, and the multi-qubit swap test for comparison, avoiding the need for complex operations like entanglement swapping or high-dimensional quantum state preparation.
(3) The protocol incorporates decoy photons for eavesdropping detection and rotation operations to obscure the encoded data, thereby providing robustness against external attacks and the curiosity of internal participants.
(4) We construct a quantum circuit for a concrete case of the proposed scheme and perform simulations on the IBM Qiskit, providing empirical validation of its feasibility and correctness.

The remainder of this paper is organized as follows. Section 2 reviews the necessary preliminaries, including the rotation operation, QHE, and the multi-qubit swap test.

Section 3 details the step-by-step design of our proposed scheme. Section 4 presents the simulation experiments and results. A comprehensive analysis of the protocol's correctness, security and fairness is provided in Section 5. Discussion is given in Section 6, and finally, Section 7 concludes the paper.

2. Preliminaries

2.1. Rotation Operation

The rotation operation [44] is a unitary operator around the Y-axis of the Bloch sphere, denoted as $R_y(\theta)$. This operator is defined by the following matrix:

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

As a unitary operation, $R_y(\theta)$ satisfies the critical property $R_y^\dagger(\theta)R_y(\theta) = I$, where I is the identity matrix and $R_y^\dagger(\theta) = R_y(-\theta)$. This operation can be used to map classical integers to the rotation angles of a single qubit. For example, the number 6 can be converted into the angle $\pi/6$, which serves as a rotation angle that can be encoded into the quantum basis states $\{|0\rangle, |1\rangle\}$. The transformation of this process is given by

$$R_y\left(\frac{\pi}{6}\right)|0\rangle = \begin{pmatrix} \cos\frac{\pi}{12} & -\sin\frac{\pi}{12} \\ \sin\frac{\pi}{12} & \cos\frac{\pi}{12} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{12} \\ \sin\frac{\pi}{12} \end{pmatrix} = \cos\frac{\pi}{12}|0\rangle + \sin\frac{\pi}{12}|1\rangle \tag{2}$$

$$R_y\left(\frac{\pi}{6}\right)|1\rangle = \begin{pmatrix} \cos\frac{\pi}{12} & -\sin\frac{\pi}{12} \\ \sin\frac{\pi}{12} & \cos\frac{\pi}{12} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\frac{\pi}{12} \\ \cos\frac{\pi}{12} \end{pmatrix} = -\sin\frac{\pi}{12}|0\rangle + \cos\frac{\pi}{12}|1\rangle \tag{3}$$

This rotation operation rotates the states $\{|0\rangle, |1\rangle\}$ on the Bloch sphere, transforming it from a definite basis state into a superposition state.

2.2. Quantum Homomorphic Encryption (QHE)

The QHE scheme [45] on single qubits is built upon the following fundamental single-qubit operators:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4}$$

The set of permitted quantum operations for this QHE scheme is defined as $\{R_y(\theta)|\theta \in [0, 2\pi)\}$.

Let δ_m denote the quantum plaintext and δ_c denote the quantum ciphertext. The QHE scheme is as follows:

- **Key Generation (KeyGen):** Randomly select two classical bits $a, b \in \{0, 1\}$ to form the secret key.
- **Encryption (Enc):** Compute the quantum ciphertext by applying single-qubit operators to the quantum plaintext based on the secret key: $\delta_c = X^a Z^b \delta_m Z^b X^a$. This encryption method is proven theoretically secure in Ref. [46].
- **Decryption (Dec):** Recover the quantum plaintext by applying again single-qubit operators to the quantum ciphertext based on the secret key: $\delta_m = Z^b X^a \delta_c X^a Z^b$.
- **Evaluation (Eval):** To apply a permitted operation $R_y(\theta_1)$ homomorphically to the quantum ciphertext δ_c, the evaluator performs a transformed rotation $R_y(\theta_1')$, where the angle is adjusted based on the secret key: $\theta_1' = (-1)^{a+b}\theta_1$. This transformation satisfies the homomorphic property: $R_y((-1)^{a+b}\theta_1)X^a Z^b = X^a Z^b R_y(\theta_1)$. Consequently, the evaluation on the ciphertext is equivalent to performing the desired operation on the plaintext, followed by encryption. The output state is given by:

$R_y(\theta_1')\delta_c R_y(\theta_1')^\dagger = X^a Z^b \left(R_y(\theta_1)\delta_m R_y(\theta_1)^\dagger\right) Z^b X^a$. Crucially, this evaluation is performed directly on the ciphertext without any decryption.

In summary, this QHE scheme allows any unitary transformation in the set $\{R_y(\theta)|\theta \in [0, 2\pi)\}$ to be executed on encrypted data, with the evaluator requiring only a simple, key-dependent adjustment of the rotation angle.

2.3. Multi-Qubit Swap Test

The multi-qubit swap test [47] is a quantum algorithmic primitive that generalizes the standard two-state swap test. Its purpose is to evaluate the collective similarity between n pairs of quantum states. Specifically, for n pairs of qubits $(|\phi_1\rangle, |\varphi_1\rangle), (|\phi_2\rangle, |\varphi_2\rangle), \ldots, (|\phi_n\rangle, |\varphi_n\rangle)$, this provides an estimate of the modulus squared sum of their inner products, $\sum_{i=1}^{n} |\langle\phi_i | \varphi_i\rangle|^2$. The quantum circuit of the multi-qubit swap test, illustrated in Figure 1, requires k ancillary qubits, where $k = \lceil log_2 n \rceil + 1$.

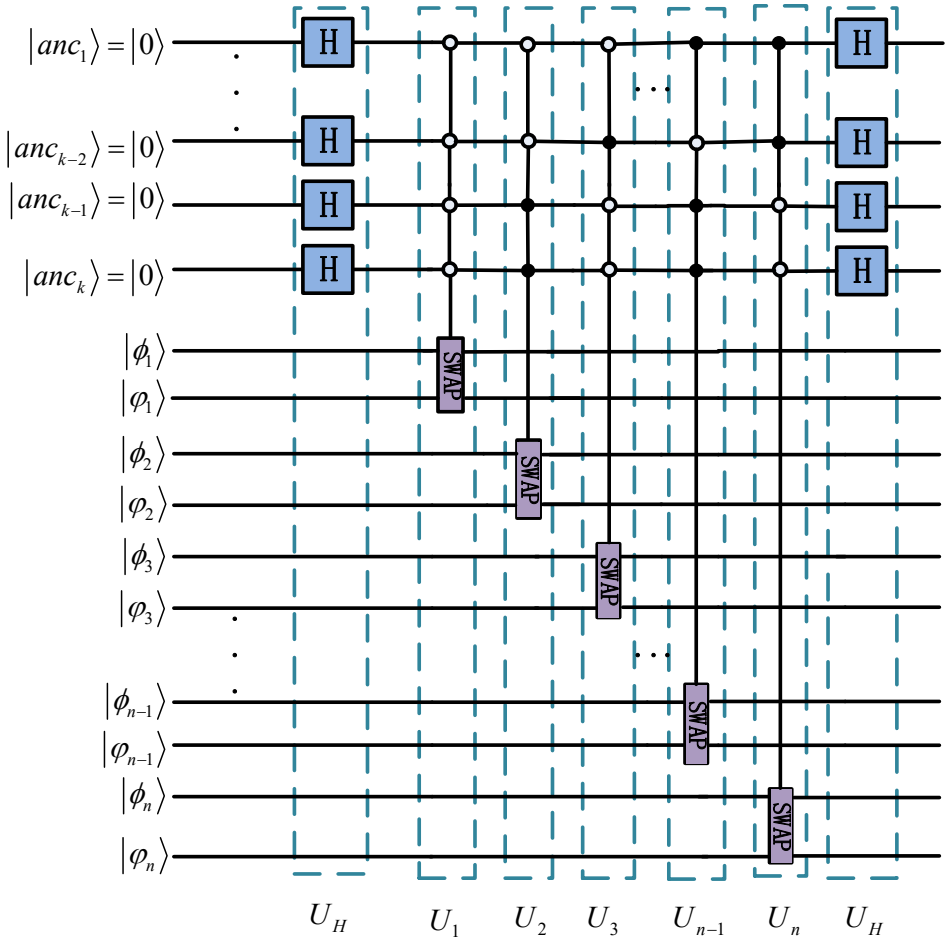

Figure 1. The quantum circuit of multi-qubit swap test.

The operation of the quantum circuit is governed by a sequence of unitary transformations:

$$\begin{cases} U_H = \mathrm{H}^{\otimes k} \otimes I^{\otimes 2n} \\ U_1 = \left(SWAP \oplus I^{\otimes 2} \oplus I^{\otimes 3} \oplus I^{\otimes 4} \oplus \ldots \otimes I^{\otimes (k+1)}\right) \otimes I^{\otimes 2(N-1)} \\ \vdots \\ U_n = I^{\otimes (2n+k-1)} \oplus \left(\left(I^{\otimes 2(n+1)} \oplus \left(\left(I^{\otimes 2(n-1)} \otimes SWAP\right) \oplus I^{\otimes 2n} \oplus I^{\otimes 2(n+1)}\right)\right) \oplus \cdots\right) \end{cases} \tag{5}$$

The overall unitary operation for the circuit is defined as $U = U_H U_n U_{n-1} \cdots U_2 U_1 U_H$.

After applying the unitary operation U to the initial states, the system evolves into a complex superposition. The probability that the highest-order ancilla qubit, $|anc_k\rangle$, is measured in the state $|1\rangle$ is given by

$$p(|anc_k\rangle = |1\rangle) = \frac{n}{2^k} - \frac{\sum_{i=1}^{n} |\langle \phi_i | \varphi_i \rangle|^2}{2^k} \tag{6}$$

This relationship can be rearranged to solve for the target metric, yielding:

$$\sum_{i=1}^{n} |\langle \phi_i | \varphi_i \rangle|^2 = n - 2^k p(|anc_k\rangle = |1\rangle) \tag{7}$$

Therefore, by preparing the quantum circuit, executing it multiple times to estimate the probability $p(|anc_k\rangle = |1\rangle)$, and applying the formula above, one can directly compute the sum of the squared modulus overlaps for all n qubit pairs.

3. The Proposed QPACC Scheme

This section details the design of our proposed QPACC scheme. This protocol allows two parties, Alice and Bob, to verify the equality of their private arrays, $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$, without disclosing any element. The arrays are of equal length n, with each element x_i, y_i constrained to the set $\{0, 1, 2, \ldots, 9\}$. This process is facilitated by a semi-honest TP, who assists in the computation without colluding with either participant and without learning the arrays' contents.

The scheme is designed to satisfy the following fundamental properties:

- *Correctness*: If all participants adhere to the protocol, TP will always output the correct comparison result.
- *Security*: The proposed scheme protects the secrecy of the input arrays X and Y from two primary threat models: external attacks on the quantum channel and internal curiosity from all other parties, even the TP.
- *Fairness*: Both Alice and Bob receive the final result simultaneously, preventing either from gaining an advantage.

Additionally, the scheme operates under the following standard assumptions:

1. All quantum channels are assumed to be lossless and noiseless. In a practical implementation, the effects of noise and loss can be mitigated through quantum error-correcting codes [48].
2. All classical channels are authenticated to ensure integrity and prevent man-in-the-middle attacks.
3. Prior to the protocol's execution, Alice and Bob have securely established a shared secret key, $\Theta_{AB} = \left(\theta_1^{AB}, \theta_2^{AB}, \cdots, \theta_n^{AB}\right)$, using an unconditionally secure QKD protocol (e.g., the BB84 protocol [2]).

The scheme proceeds according to the following steps and its diagram is shown in Figure 2.

Step 1. Prepare initial encoded quantum states

Alice and Bob convert each i-th element in arrays X and Y into angles $\theta_i^A = \frac{\pi}{x_i}$ and $\theta_i^B = \frac{\pi}{y_i}$. Specially, if $x_i = 0$ or $y_i = 0$, they set the angles to $\theta_i^A = 0$ or $\theta_i^B = 0$, respectively. They perform the rotation operations $R_y\left(\theta_i^A + \theta_i^{AB}\right)$ and $R_y\left(\theta_i^B + \theta_i^{AB}\right)$ on the states $|0\rangle$ to encode the array elements into quantum states, respectively. These encoded quantum states are denoted as $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$, respectively.

$$\begin{aligned}\left|\alpha_i^A\right\rangle &= R_y(\theta_i^A+\theta_i^{AB})|0\rangle = \begin{pmatrix}\cos\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right) & -\sin\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)\\ \sin\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right) & \cos\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\cos\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)\\ \sin\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)\end{pmatrix}\\ &= \cos\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)|0\rangle+\sin\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)|1\rangle = \cos\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)|0\rangle+\sin\left(\frac{\pi}{2x_i}+\frac{\theta_i^{AB}}{2}\right)|1\rangle\end{aligned} \tag{8}$$

$$\begin{aligned}\left|\alpha_i^B\right\rangle &= R_y(\theta_i^B+\theta_i^{AB})|0\rangle = \begin{pmatrix}\cos\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right) & -\sin\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)\\ \sin\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right) & \cos\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\cos\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)\\ \sin\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)\end{pmatrix}\\ &= \cos\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)|0\rangle+\sin\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)|1\rangle = \cos\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)|0\rangle+\sin\left(\frac{\pi}{2y_i}+\frac{\theta_i^{AB}}{2}\right)|1\rangle\end{aligned} \tag{9}$$

Step 2. Encrypt the encoded quantum states

Alice (Bob) randomly selects two n-length classical bits a_i^A and b_i^A (a_i^B and b_i^B) to form two secret keys. They compute the encrypted quantum states $\left|\alpha_i^{Enc\_A}\right\rangle$ ($\left|\alpha_i^{Enc\_B}\right\rangle$) by applying single-qubit operators to the encoded quantum states $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$ based on the chosen secret keys. This can be expressed as:

$$\left|\alpha_i^{Enc\_A}\right\rangle = X^{a_i^A}Z^{b_i^A}\left|\alpha_i^A\right\rangle \tag{10}$$

$$\left|\alpha_i^{Enc\_B}\right\rangle = X^{a_i^B}Z^{b_i^B}\left|\alpha_i^B\right\rangle \tag{11}$$

Step 3. Insert decoy photons into encrypted quantum states

To prevent eavesdropping, Alice (Bob) random selects δ decoy photons chosen from four nonorthogonal states: $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into $\left|\alpha_i^{Enc\_A}\right\rangle$ ($\left|\alpha_i^{Enc\_B}\right\rangle$) at random positions. The resulting quantum states composed a quantum sequence, denoted as S_A (S_B). Then, Alice (Bob) records the chosen nonorthogonal states and positions of these decoy photons. Finally, Alice (Bob) sends S_A (S_B) to the TP via the quantum channel for the next eavesdropping detection.

Step 4. Eavesdropping detection between Alice (Bob) and the TP

Upon receiving S_A and S_B, the TP sends a confirmation to Alice and Bob, who then publicly announce the corresponding positions and measurement bases of the inserted decoy photons. Specifically, if the chosen decoy photons are in the states $|0\rangle$ or $|1\rangle$, the measurement base is the Z basis. Otherwise, the measurement base is the X basis. Next, the TP measures these decoy photons in S_A and S_B using the announced measurement bases to obtain the measurement results. These results are sent back to Alice and Bob to check whether the quantum sequences have been transmitted securely. Alice and Bob calculate the error rate by comparing the measurement results with the initially prepared decoy photons. If the error rate is higher than a threshold, approximately between 2% and 8.9% depending on the channel conditions (e.g., distance and noise) [49], the quantum channel is deemed insecure, and they will restart the protocol. Otherwise, the transmission of the quantum sequence is considered secure, and Alice and Bob will announce the secret keys to the TP for decrypting the encrypted quantum states.

Step 5. Decrypt the quantum states and conduct the multi-qubit swap test

The TP removes the decoy photons in S_A and S_B to recover the encrypted quantum states $\left|\alpha_i^{Enc\_A}\right\rangle$ and $\left|\alpha_i^{Enc\_B}\right\rangle$. Using the secret keys, it then recovers the encoded quantum states $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$ by applying again single-qubit operators to $\left|\alpha_i^{Enc\_A}\right\rangle$ ($\left|\alpha_i^{Enc\_B}\right\rangle$). This is expressed as:

$$\left|\alpha_i^A\right\rangle = Z^{b_i^A}X^{a_i^A}\left|\alpha_i^{Enc\_A}\right\rangle \tag{12}$$

$$\left|\alpha_i^B\right\rangle = Z^{b_i^B} X^{a_i^B} \left|\alpha_i^{Enc\_B}\right\rangle \tag{13}$$

Next, the TP conducts the multi-qubit swap test on all qubit pairs $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$, measuring the highest-order ancilla qubit $|anc_k\rangle$ to obtain a measurement result.

Step 6. Perform multiple iterations and announce the comparison result

By conducting Steps 1 to 5 λ times (where λ depends on the desired accuracy of the multi-qubit swap test), the TP records the measurement results of each highest-order ancilla qubit $|anc_k\rangle$. The occurrence of the $|1\rangle$ state in any single iteration conclusively demonstrates a difference between arrays X and Y. Conversely, the consistent observation of $|0\rangle$ across all iterations certifies their equivalence. The TP is responsible for announcing the conclusive result to both parties.

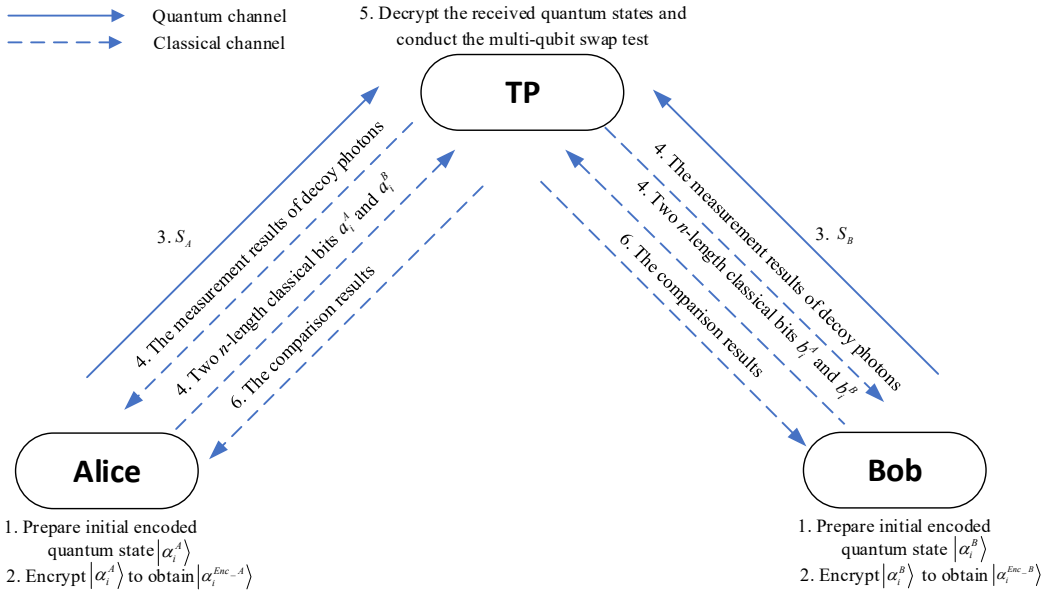

Figure 2. The diagram of the proposed scheme.

4. Simulation Experiment

We assume that Alice has her array $X = (2, 1, 3, 2)$ and Bob has his array $Y = (2, 1, 3, 1)$. Alice and Bob intend to determine whether the two arrays are equal. Additionally, it is given that Alice and Bob have securely established a shared secret key $K_{AB} = \left(\frac{3\pi}{4}, \frac{6\pi}{5}, \frac{\pi}{2}, \frac{5\pi}{6}\right)$ via a QKD protocol. For simplification, the eavesdropping detection is treated as an independent procedure, not considered in the simulation experiment.

To prepare the initial encoded quantum states, Alice performs the rotation operations $R_y\left(\frac{\pi}{2} + \frac{3\pi}{4}\right)$, $R_y\left(\pi + \frac{6\pi}{5}\right)$, $R_y\left(\frac{\pi}{3} + \frac{\pi}{2}\right)$, and $R_y\left(\frac{\pi}{2} + \frac{5\pi}{6}\right)$ on the states $|0\rangle$. The chosen secret keys for Alice are $\left(a_1^A, a_2^A, a_3^A, a_4^A\right) = (0, 0, 1, 1)$ and $\left(b_1^A, b_2^A, b_3^A, b_4^A\right) = (1, 0, 1, 0)$.

Similarly, to prepare the initial encoded quantum states, Bob applies the rotation operations $R_y\left(\frac{\pi}{2} + \frac{3\pi}{4}\right)$, $R_y\left(\pi + \frac{6\pi}{5}\right)$, $R_y\left(\frac{\pi}{3} + \frac{\pi}{2}\right)$, and $R_y\left(\pi + \frac{5\pi}{6}\right)$ to the states $|0\rangle$. The chosen secret keys for Bob are $\left(a_1^B, a_2^B, a_3^B, a_4^B\right) = (0, 1, 1, 0)$ and $\left(b_1^B, b_2^B, b_3^B, b_4^B\right) = (1, 1, 0, 0)$.

We evaluated the practical viability of our protocol by implementing it as a quantum circuit and conducting simulations via IBM Qiskit (version 0.44.1) on Python (version 3.11.4) running on Windows. It is important to note that the following simulation is conducted 1000 times. The corresponding quantum circuit to evaluate the equality of the arrays X and Y is shown in Figure 3, and its measurement results are presented in Figure 4. In Figure 3, quantum registers q[0] to q[2] serve as ancilla qubits, while registers q[3] to q[10] are used to encode the array elements and subsequently encrypt the resulting quantum states. A multi-qubit swap test is performed, which includes a Hadamard gate (H) on the

control ancilla qubits, q[0]–q[2]. The outcome of the protocol is obtained by measuring the ancilla qubit q[2]. In Figure 4, the measurement outcome is a bitstring representing the computational basis state of the ancilla qubits q[2], q[1], and q[0]. A result of '000' indicates the state $|000\rangle$, meaning all three ancilla qubits are in the $|0\rangle$ state. Conversely, a result of '100' corresponds to the state $|100\rangle$, signifying that q[2] is in state $|1\rangle$ while q[1] and q[0] remain in state $|0\rangle$.

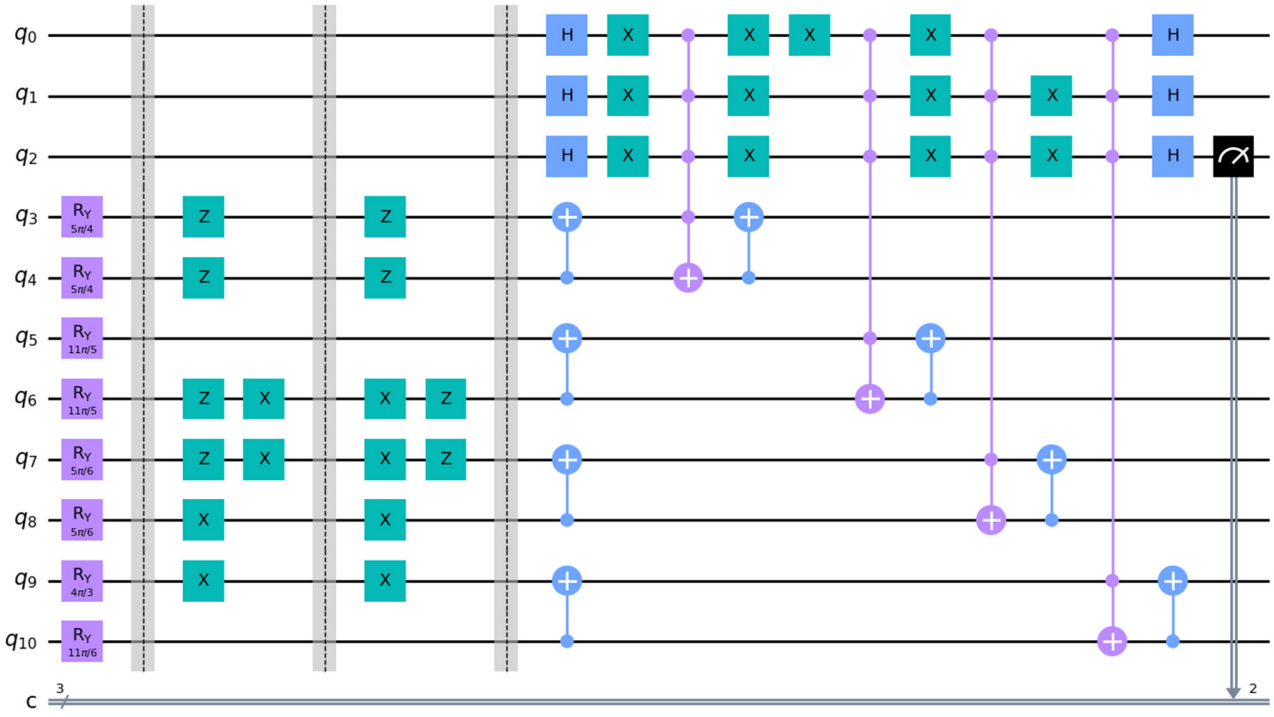

Figure 3. The quantum circuit for determining the equality of the arrays X and Y.

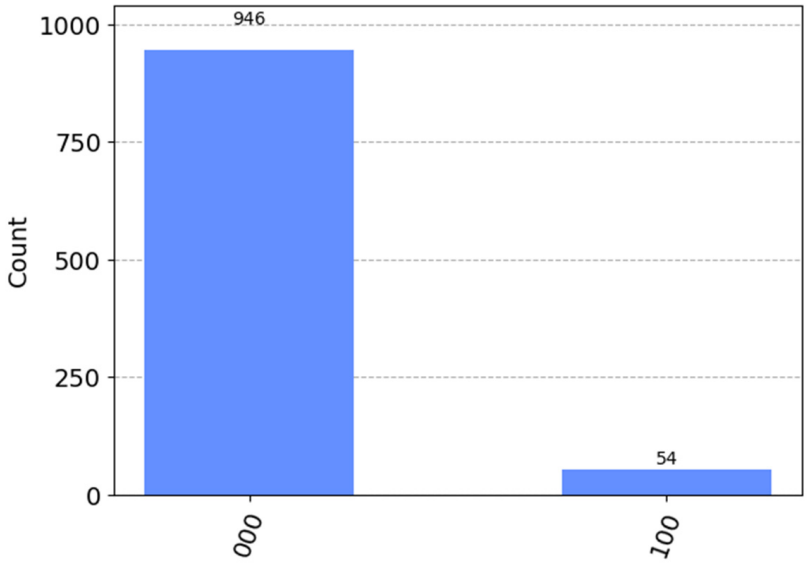

Figure 4. The measurement results.

Based on the measurement results presented in Figure 4, where the ancilla qubit q[2] is measured in the $|1\rangle$ state, we conclude that the scheme's output is correct and that the two input arrays are not identical.

5. Analysis

5.1. Correctness

Let $P(|anc_k\rangle = |1\rangle)$ denote the probability that the ancilla qubit $|anc_k\rangle$ is measured in the state $|1\rangle$ when conducting the multi-qubit swap test on all qubit pairs $|\alpha_i^A\rangle$ and $|\alpha_i^B\rangle$. The probability that $|anc_k\rangle = |1\rangle$ can be expressed as follows:

$$
\begin{aligned}
&p(|anc_k\rangle = |1\rangle) = \frac{n}{2^k} - \frac{\sum_{i=1}^{n} \left|\langle \alpha_i^A \mid \alpha_i^B \rangle\right|^2}{2^k} \\
&= \frac{n}{2^k} - \frac{1}{2^k}\left(\left|\langle \alpha_1^A \mid \alpha_1^B \rangle\right|^2 + \left|\langle \alpha_2^A \mid \alpha_2^B \rangle\right|^2 + \cdots + \left|\langle \alpha_n^A \mid \alpha_n^B \rangle\right|^2\right) \\
&= \frac{n}{2^k} - \frac{1}{2^k}\left(\begin{array}{l}
\left|\left(\cos\left(\frac{\pi}{2x_1} + \frac{\theta_1^{AB}}{2}\right)\langle 0| + \sin\left(\frac{\pi}{2x_1} + \frac{\theta_1^{AB}}{2}\right)\langle 1|\right)\left(\cos\left(\frac{\pi}{2y_1} + \frac{\theta_1^{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y_1} + \frac{\theta_1^{AB}}{2}\right)|1\rangle\right)\right|^2 \\
\left|\left(\cos\left(\frac{\pi}{2x_2} + \frac{\theta_2^{AB}}{2}\right)\langle 0| + \sin\left(\frac{\pi}{2x_2} + \frac{\theta_2^{AB}}{2}\right)\langle 1|\right)\left(\cos\left(\frac{\pi}{2y_2} + \frac{\theta_2^{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y_2} + \frac{\theta_2^{AB}}{2}\right)|1\rangle\right)\right|^2 \\
+ \cdots + \left|\left(\cos\left(\frac{\pi}{2x_n} + \frac{\theta_n^{AB}}{2}\right)\langle 0| + \sin\left(\frac{\pi}{2x_n} + \frac{\theta_n^{AB}}{2}\right)\langle 1|\right)\left(\cos\left(\frac{\pi}{2y_n} + \frac{\theta_n^{AB}}{2}\right)|0\rangle + \sin\left(\frac{\pi}{2y_n} + \frac{\theta_n^{AB}}{2}\right)|1\rangle\right)\right|^2
\end{array}\right) \\
&= \frac{n}{2^k} - \frac{1}{2^k}\left(\cos^2\left(\frac{\pi}{2x_1} - \frac{\pi}{2y_1}\right) + \cos^2\left(\frac{\pi}{2x_2} - \frac{\pi}{2y_2}\right) + \cdots + \cos^2\left(\frac{\pi}{2x_n} - \frac{\pi}{2y_n}\right)^2\right) \\
&= \frac{n}{2^k} - \frac{\sum_{i=1}^{n} \cos^2\left(\frac{\pi}{2x_i} - \frac{\pi}{2y_i}\right)}{2^k}
\end{aligned}
\tag{14}
$$

Based on Equation (14), we conclude that $P(|anc_k\rangle = |1\rangle) = 0$ if and only if all $x_i = y_i$. Thus, array equivalence is confirmed only if all ancilla qubits $|anc_k\rangle$ are measured in the $|0\rangle$ state; the detection of a $|1\rangle$ state in any one of them immediately establishes a mismatch.

5.2. Security Analysis

The proposed QPACC protocol is designed to withstand security threats originating from two primary sources: external eavesdroppers and honest-but-curious participants. External adversaries, such as Eve, may attempt to intercept quantum transmissions or deploy quantum Trojan horse attacks, while participants might seek to deduce private inputs from intermediate information. To counter these threats, the protocol integrates decoy photon technology for eavesdropping detection and employs cryptographic keys to encrypt quantum states. The following analysis will demonstrate that these measures effectively preserve the confidentiality of the private arrays X and Y against all considered attacks.

5.2.1. External Attacks

A malicious adversary, Eve, may employ various strategies, such as intercept-resend [50,51], entangle-measure [52], and quantum Trojan horse attacks [53,54], in an attempt to compromise the confidentiality of the participants' private inputs. To counter these threats, the scheme incorporates a robust security framework. The sensitive information is encoded into single-photon states, which are further protected by pre-shared secret keys. The following analysis details the protocol's robustness against these specific attack strategies.

Case I. Intercept-resend attack

In this attack scenario, an external eavesdropper, Eve, intercepts the encoded quantum sequences S_A and S_B during their transmission from Alice and Bob to the TP. She measures the intercepted qubits using a randomly chosen basis (Z or X) and, based on the results, prepares and forwards two counterfeit sequences to the TP. The security against this attack stems from the indistinguishable nature of the decoy photons, which are randomly inserted within the sequences from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Since Eve has no knowledge of their positions or bases, her random measurements inevitably disturb the decoy states. This disturbance introduces detectable errors during the subsequent eavesdropping check conducted by the legitimate parties.

The detection probability can be quantified as follows. Consider a decoy photon in the $|-\rangle$ state. If Eve measures it in the correct X-basis, she causes no disturbance. However, if she chooses the incorrect Z-basis, she has a 50% probability of obtaining an incorrect result, thus introducing a detectable error. Given that Eve selects either basis with a probability of 1/2, the overall probability that she measures a single decoy photon without introducing an error is $P_{pass} = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. Consequently, for δ decoy photons, the probability that Eve evades detection diminishes to $(3/4)^{\delta}$. Therefore, the probability of her attack being discovered is $1 - (3/4)^{\delta}$, which converges to 1 as δ increases. This guarantees that any intercept-resend attempt will be detected with near certainty, preventing Eve from extracting any meaningful information about the private arrays X and Y.

Case II. Entangle-measure attack

In this attack scenario, an external eavesdropper, Eve, intercepts the encoded quantum sequences S_A and S_B during their transmission from Alice and Bob to the TP. She then applies a unitary operation U to entangle each intercepted qubit with an ancillary qubit $|E\rangle$ in her possession, aiming to extract information by subsequently measuring this ancillary state.

The unitary interaction U on the basis states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and the ancillary state $|E\rangle$ is described by:

$$U|0\rangle|E\rangle = a_{00}|0\rangle|E_{00}\rangle + a_{01}|1\rangle|E_{01}\rangle \tag{15}$$

$$U|1\rangle|E\rangle = a_{10}|0\rangle|E_{10}\rangle + a_{11}|1\rangle|E_{11}\rangle \tag{16}$$

$$\begin{aligned} U|+\rangle|E\rangle = \; & \tfrac{1}{\sqrt{2}}(U|0\rangle|E\rangle + U|1\rangle|E\rangle) \\ & = \tfrac{1}{\sqrt{2}}(a_{00}|0\rangle|E_{00}\rangle + a_{01}|1\rangle|E_{01}\rangle + a_{10}|0\rangle|E_{10}\rangle + a_{11}|1\rangle|E_{11}\rangle) \\ & = \tfrac{1}{2}|+\rangle(a_{00}|E_{00}\rangle + a_{01}|E_{01}\rangle + a_{10}|E_{10}\rangle + a_{11}|E_{11}\rangle) \\ & + \tfrac{1}{2}|-\rangle(a_{00}|E_{00}\rangle - a_{01}|E_{01}\rangle + a_{10}|E_{10}\rangle - a_{11}|E_{11}\rangle) \end{aligned} \tag{17}$$

$$\begin{aligned} U|-\rangle|E\rangle = \; & \tfrac{1}{\sqrt{2}}(U|0\rangle|E\rangle - U|1\rangle|E\rangle) \\ & = \tfrac{1}{\sqrt{2}}(a_{00}|0\rangle|E_{00}\rangle + a_{01}|1\rangle|E_{01}\rangle - a_{10}|0\rangle|E_{10}\rangle - a_{11}|1\rangle|E_{11}\rangle) \\ & = \tfrac{1}{2}|+\rangle(a_{00}|E_{00}\rangle + a_{01}|E_{01}\rangle - a_{10}|E_{10}\rangle - a_{11}|E_{11}\rangle) \\ & + \tfrac{1}{2}|-\rangle(a_{00}|E_{00}\rangle - a_{01}|E_{01}\rangle - a_{10}|E_{10}\rangle + a_{11}|E_{11}\rangle) \end{aligned} \tag{18}$$

The coefficients satisfy the normalization conditions $|a_{00}|^2 + |a_{01}|^2 = 1$ and $|a_{10}|^2 + |a_{11}|^2 = 1$.

For the attack to remain undetected, the interaction must not introduce errors when the decoy photons are measured by the legitimate parties. This imperfection detection imposes strict constraints on the unitary operation. Specifically, to pass the eavesdropping check without inducing a measurable disturbance, the coefficients must satisfy $a_{01} = a_{10} = 0$ and $a_{00}|E_{00}\rangle = a_{11}|E_{11}\rangle$. Under these constraints, the evolution of the decoy states simplifies to the following form:

$$U|0\rangle|E\rangle = a_{00}|0\rangle|E_{00}\rangle \tag{19}$$

$$U|1\rangle|E\rangle = a_{11}|1\rangle|E_{11}\rangle = a_{00}|1\rangle|E_{00}\rangle \tag{20}$$

$$U|+\rangle|E\rangle = \frac{1}{2}|+\rangle(a_{00}|E_{00}\rangle + a_{11}|E_{11}\rangle) = a_{00}|+\rangle|E_{00}\rangle = a_{11}|+\rangle|E_{11}\rangle \tag{21}$$

$$U|-\rangle|E\rangle = \frac{1}{2}|-\rangle(a_{00}|E_{00}\rangle + a_{11}|E_{11}\rangle) = a_{00}|-\rangle|E_{00}\rangle = a_{11}|-\rangle|E_{11}\rangle \tag{22}$$

This result demonstrates that no meaningful entanglement is created between the decoy qubits and Eve's ancillary qubit. Consequently, her measurements on the ancilla yield no information about the qubit's state, rendering the attack futile.

Furthermore, even if Eve were to direct this attack at the encoded information qubits $\left|\alpha_i^{Enc\_A}\right\rangle$ ($\left|\alpha_i^{Enc\_B}\right\rangle$), her success is precluded. The final state after the interaction depends

on the secret parameters a_i^A, b_i^A and Θ_{AB} (a_i^B, b_i^B, and Θ_{AB}). Since Eve has no knowledge of these parameters, she cannot deduce the participants' private inputs from her ancillary measurements. The protocol's security is thus assured, as any attempt to glean information via an entangle-measure attack will either be detected through decoy state analysis or will fail due to a lack of essential secret parameters.

Case III. Quantum Trojan horse attacks

Quantum Trojan horse attacks, which include the delay-photon and invisible-photon attacks, represent a class of threats that typically exploit bidirectional quantum communication channels. The security of the proposed protocol against such attacks is inherent in its fundamental architecture. The protocol is inherently resilient to these attacks, as the quantum communication is exclusively one-way (from Alice and Bob to the TP), a design that eliminates the possibility of the two-way interaction these threats require. This structural characteristic inherently negates the primary vector for quantum Trojan horse attacks.

In summary, by employing decoy photon technology to counter external eavesdropping strategies, the protocol effectively safeguards the private arrays X and Y.

5.2.2. Participant Attacks

Insider threats from participants pose a more significant security challenge than external attacks, as honest-but-curious participants possess legitimate access to intermediate computational data and can leverage this knowledge to infer private inputs. The following analysis demonstrates the protocol's resilience against such attacks, considering potential curious behaviour from any of the parties involved: TP, Alice, or Bob.

Case I. Security against the semi-honest TP

Within the security model, the TP is assumed to be semi-honest; it faithfully executes the protocol's procedures but may attempt to infer the private arrays A and B from the information it legitimately acquires. The TP's vantage point includes access to the encoded quantum states $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$, which are prepared by applying the 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 states $|0\rangle$. The angles θ_i^A and θ_i^B are encoded from the array elements x_i and y_i, respectively. The critical security mechanism lies in the pre-shared secret angle Θ_{AB}, known exclusively to Alice and Bob. From the TP's perspective, the processed qubits, denoted as $\left|\alpha_i^A\right\rangle$ and $\left|\alpha_i^B\right\rangle$, are equivalent to states rotated by a single, composite angle. Without knowledge of the component Θ_{AB}, the TP faces the fundamental principle of quantum indeterminacy; it cannot resolve the individual contributions of θ_i^A and θ_i^B from the superposition. Consequently, the unknown quantum states remain indistinguishable, and the private arrays X and Y are provably concealed from the TP, ensuring security against this semi-honest adversary.

Case II. Security against honest-but-curious Alice or Bob

The protocol ensures identical roles between participants Alice and Bob. To illustrate, consider a scenario where Alice, while adhering to the protocol, attempts to deduce Bob's private array Y. Each element b_i of Bob's array is encoded into a rotation angle θ_i^B. The corresponding quantum state $\left|\alpha_i^B\right\rangle$ is prepared by applying the unitary operation $R_y\left(\theta_i^B + \theta_i^{AB}\right)$ to the state $|0\rangle$, where θ_i^{AB} is a pre-shared secret key. Subsequently, this state is encrypted using single-qubit operators determined by Bob's secret keys a_i^B and b_i^B, resulting in the state $\left|\alpha_i^{Enc\_B}\right\rangle$. Decoy photons are inserted into the final sequence S_B before its transmission to the TP.

While Alice could intercept S_B, her ability to gain information is nullified by multiple security layers. First, any attempt to intercept and resend the sequence would be detected during the eavesdropping detection process. Second, even if she accessed the sequence S_B by conducting intercept-resend attacks, the encrypted states $\left|\alpha_i^{Enc\_B}\right\rangle$ remain indistinguishable without knowledge of the encryption keys a_i^B and b_i^B, which are only revealed after a

successful security verification, a condition Alice cannot satisfy without causing detectable disturbances. Consequently, Alice faces the fundamental barrier of quantum indeterminacy and cannot resolve θ_i^B to deduce array Y. An equivalent analysis applies to Bob's attempts to ascertain array X, confirming the protocol's resilience against honest-but-curious Alice or Bob.

To conclude, the protocol guarantees the confidentiality of the private arrays against honest-but-curious adversaries, encompassing all participating entities: the TP, Alice, and Bob.

5.3. Fairness

The fairness is ensured through the involvement of a semi-honest TP. The TP performs measurements on the highest-order ancilla qubit $|anc_k\rangle$ of the multi-qubit swap test to determine the equality relationship between arrays X and Y, and subsequently announces the result simultaneously to both the parties. This process of simultaneous disclosure prevents either party from gaining precedence in learning the outcome, thereby upholding strict fairness throughout the protocol execution.

6. Discussion

A comparative analysis between the proposed protocol and existing QPC schemes is summarized in Table 1, evaluating aspects such as quantum resource, quantum operations, quantum communication method, quantum measurement for users, quantum measurement for TP, and the scope of comparison.

Table 1. A comparative between our protocol and existing QPC schemes.

Protocol	Quantum Resource	Quantum Operations	Quantum Communication Method	Quantum Measurement for Users	Quantum Measurement for TP	Comparison Scope
Ref. [30]	Bell state	Entanglement swapping	One-way	GHZ-basis	No	Integer
Ref. [31]	Hyper-entangled GHZ state	Entanglement swapping	One-way	Bell-basis	Bell-basis	Integer
Ref. [32]	Bell state	Rotation operation	Two-way	No	Bell-basis	Integer
Ref. [33]	Four-particle cluster and extend Bell state	Entanglement swapping	One-way	Bell basis and extended Bell basis	No	Integer
Ref. [34]	Four-particle cluster state	Bit-flip and phase-shift	One-way	No	Bell-basis	Integer
Ref. [35]	d-dimensional Bell state	Unitary operation	One-way	d-dimensional single-particle	No	Integer
Ref. [36]	d-dimensional Bell state	Entanglement swapping and qudit shifting	One-way	d-dimensional Bell state	d-dimensional Bell state	Integer
Ours	Singe photons	Rotation operation	One-way	No	single-particle	Array

As illustrated, our scheme exhibits the following distinct advantages:

(1) It extends comparison capability from single integer to full array, improving functional scalability for practical applications.

(2) In contrast to protocols that rely on complex multi-qubit or high-dimensional states, our scheme utilizes only single-photon states, single-qubit rotations, and the multi-qubit swap test. All of these components are compatible with current quantum technology, which significantly enhances its experimental feasibility.

(3) The substitution of Bell-basis measurements with single-particle measurements streamlines the measurement process, thereby lowering the experimental overhead.

The operational range of the proposed scheme is limited to array elements in $\{0, 1, 2, \ldots, 9\}$, a constraint imposed to safeguard against accuracy degradation from large numerical values. Consequently, a salient application is in data integrity checks. By quantifying data block features into arrays within this bounded set, the scheme can be deployed to verify error-free data transmission or to audit the consistency of backup data against its original source.

7. Conclusions

This paper presents a quantum private array content comparison (QPACC) scheme based on a multi-qubit swap test framework. The protocol integrates rotation operations for encoding array elements into quantum states, QHE for state protection, and a multi-qubit swap test executed by the TP acting as a cloud processor. Through this architecture, the TP can compute the modulus squared sum of inner products between the decoded quantum states to determine array equality without learning the actual content of the arrays. Simulations conducted via IBM Qiskit confirm the scheme's practical viability. The protocol ensures security through multiple layers: decoy photon technology safeguards against external eavesdropping, while the combined use of rotation operations and QHE protects against curious participants attempting to infer private inputs. Furthermore, fairness is guaranteed by the TP's simultaneous announcement of the comparison result. Compared to existing quantum private comparison schemes limited to single integers, the proposed approach enables efficient array comparisons, offering enhanced scalability and practical applicability. By utilizing single photons and avoiding entanglement swapping, the protocol reduces operational complexity and aligns with near-term quantum technological capabilities. Future research will explore semi-quantum implementations to further minimize quantum resource requirements while preserving security guarantees.

Author Contributions: Conceptualization, M.H. and S.Z.; methodology, M.H. and S.Z.; Writing—original draft, M.H.; writing—review and editing, Y.W. and 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 General Program of Sichuan Science and Technology & Education Joint Fund (No.2025NSFSC2098), 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), 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. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
2. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
3. Zhang, Y.; Bian, Y.; Li, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution system: Past, present, and future. *Appl. Phys. Rev.* **2024**, *11*, 011318. [CrossRef]
4. Zhang, W.; van Leent, T.; Redeker, K.; Garthoff, R.; Schwonnek, R.; Fertig, F.; Eppelt, S.; Rosenfeld, W.; Scarani, V.; Lim, C.C.; et al. A device-independent quantum key distribution system for distant users. *Nature* **2022**, *607*, 687–691. [CrossRef]
5. Li, W.; Zhang, L.; Tan, H.; Lu, Y.; Liao, S.K.; Huang, J.; Li, H.; Wang, Z.; Mao, H.K.; Yan, B.; et al. High-rate quantum key distribution exceeding 110 Mb s^{-1}. *Nat. Photonics* **2023**, *17*, 416–421. [CrossRef]
6. Nadlinger, D.P.; Drmota, P.; Nichol, B.C.; Araneda, G.; Main, D.; Srinivas, R.; Lucas, D.M.; Ballance, C.J.; Ivanov, K.; Tan, E.Z.; et al. Experimental quantum key distribution certified by Bell's theorem. *Nature* **2022**, *607*, 682–686. [CrossRef]
7. Shen, A.; Cao, X.Y.; Wang, Y.; Fu, Y.; Gu, J.; Liu, W.B.; Weng, C.X.; Yin, H.L.; Chen, Z.B. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci. China Phys. Mech. Astron.* **2023**, *66*, 260311. [CrossRef]
8. Zhang, Q.; Zhong, W.; Du, M.M.; Shen, S.T.; Li, X.Y.; Zhang, A.L.; Zhou, L.; Sheng, Y.B. Device-independent quantum secret sharing with noise preprocessing and postselection. *Phys. Rev. A* **2024**, *110*, 042403. [CrossRef]
9. Qin, Y.; Cheng, J.; Ma, J.; Zhao, D.; Yan, Z.; Jia, X.; Xie, C.; Peng, K. Efficient and secure quantum secret sharing for eight users. *Phys. Rev. Res.* **2024**, *6*, 033036. [CrossRef]

10. Zhang, C.; Long, Y.; Li, Q. Quantum summation using d-level entanglement swapping. *Quantum Inf. Process.* **2021**, *20*, 137. [CrossRef]
11. Shi, R.H.; Liu, B.; Zhang, M. Measurement-device-independent quantum secure multiparty summation. *Quantum Inf. Process.* **2022**, *21*, 1. [CrossRef]
12. Hou, M.; Wu, Y.; Zhang, S. Quantum Private Set Intersection Scheme Based on Bell States. *Axioms* **2025**, *14*, 120. [CrossRef]
13. Huang, X.; Zhang, W.; Zhang, S. Quantum multi-party private set intersection using single photons. *Phys. A Stat. Mech. Appl.* **2024**, *649*, 129974. [CrossRef]
14. Guo, G.D.; Zheng, L.Q.; Yu, K.; Lin, S. Authenticated Multi-Party Quantum Private Set Intersection with Single Particles. *Mathematics* **2025**, *13*, 2019. [CrossRef]
15. Lindell, Y. Secure multiparty computation. *Commun. ACM* **2020**, *64*, 86–96. [CrossRef]
16. Yao, A.C. Protocols for secure computations. In Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Chicago, IL, USA, 3–5 November 1982; p. 160.
17. Boudot, F.; Schoenmakers, B.; Traore, J. A fair and efficient solution to the socialist millionaires' problem. *Discret. Appl. Math.* **2001**, *111*, 23–36. [CrossRef]
18. 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. Hou, M.; Wu, Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. *Front. Phys.* **2024**, *12*, 1364140. [CrossRef]
22. Kou, T.Y.; Che, B.C.; Dou, Z.; Chen, X.B.; Lai, Y.P.; Li, J. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. *Chin. Phys. B* **2022**, *31*, 060307. [CrossRef]
23. Liu, B.; Xiao, D.; Huang, W.; Jia, H.Y.; Song, T.T. Quantum private comparison employing single-photon interference. *Quantum Inf. Process.* **2017**, *16*, 180. [CrossRef]
24. Sun, Q. Quantum private comparison with six-particle maximally entangled states. *Mod. Phys. Lett. A* **2022**, *37*, 2250149. [CrossRef]
25. 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]
26. 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]
27. 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]
28. 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]
29. 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]
30. Gianni, J.; Qu, Z. New quantum private comparison using hyperentangled ghz state. *J. Quantum Comput.* **2021**, *3*, 45–54. [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*, 1–12. [CrossRef]
32. Hou, M.; Wu, Y. Quantum Private Comparison Protocol with Cluster States. *Axioms* **2025**, *14*, 70. [CrossRef]
33. Lin, S.; Sun, Y.; Liu, X.F.; Yao, Z.Q. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf Process* **2013**, *12*, 559–568. [CrossRef]
34. 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]
35. Ye, T.Y.; Hu, J.L. Multi-party quantum private comparison based on entanglement swapping of Bell entangled states within d-level quantum system. *Int. J. Theor. Phys.* **2021**, *60*, 1471–1480. [CrossRef]
36. Wu, W.Q.; Zhao, Y.X. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 1. [CrossRef]
37. Lang, Y.F. Quantum private magnitude comparison. *Int. J. Theor. Phys.* **2022**, *61*, 100. [CrossRef]
38. 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]
39. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, C.Y.; Hou, Y.Y. An efficient semi-quantum private comparison without pre-shared keys. *Quantum Inf. Process.* **2021**, *20*, 360. [CrossRef]

40. Jiang, L.Z. Semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 1. [CrossRef]
41. 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]
42. 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.* **2025**, *8*, 2400530. [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. Huang, X.; Zhang, W.; Wang, X.; Zhang, S.; Khan, M.K. QF2PM: Quantum-Secure Fine-Grained Privacy-Preserving Profile Matching for Mobile Social Networks. *IEEE Trans. Netw. Sci. Eng.* **2025**. [CrossRef]
45. Huang, X.; Zhang, S.; Chang, Y.; Yang, F.; Hou, M.; Cheng, W. Quantum secure direct communication based on quantum homomorphic encryption. *Mod. Phys. Lett. A* **2021**, *36*, 2150263. [CrossRef]
46. Liang, M. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum Inf. Process.* **2013**, *12*, 3675–3687. [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. Saiyed, A.I. Quantum Error Correction in Cryptographic Applications: Ensuring Robustness against Quantum Noise and Attacks. *Acad. Nexus J.* **2025**, *4*. Available online: http://academianexusjournal.com/index.php/anj/article/view/16 (accessed on 25 November 2025).
49. Tsai, C.W.; Hwang, T. Deterministic quantum communication using the symmetric W state. *Sci. China Phys. Mech. Astron.* **2013**, *56*, 1903–1908. [CrossRef]
50. Kozubov, A.; Gaidash, A.; Miroshnichenko, G. Quantum control attack: Towards joint estimation of protocol and hardware loopholes. *Phys. Rev. A* **2021**, *104*, 022603. [CrossRef]
51. 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]
52. He, F.; Xin, X.; Li, C.; Li, F. Security analysis of the semi-quantum secret-sharing protocol of specific bits and its improvement. *Quantum Inf. Process.* **2024**, *23*, 51. [CrossRef]
53. Li, Z.; Zheng, B.; Zhang, C.; Zhang, Z.; Xie, H.B.; Wei, K. Improved security bounds against the Trojan-horse attack in decoy-state quantum key distribution. *Quantum Inf. Process.* **2024**, *23*, 40. [CrossRef]
54. Ding, H.J.; Liu, J.Y.; Zhou, X.Y.; Zhang, C.H.; Li, J.; Wang, Q. Improved finite-key security analysis of measurement-device-independent quantum key distribution against a trojan-horse attack. *Phys. Rev. Appl.* **2023**, *19*, 044022. [CrossRef]