AIMS Mathematics, 11(3): 7573–7592.
DOI: 10.3934/math.2026311
Received: 20 January 2026
Revised: 03 March 2026
Accepted: 16 March 2026
Published: 23 March 2026

https://www.aimspress.com/journal/Math

Research article

Quantum secure privacy-preserving array equality comparison protocol

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

[1] School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China
[2] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu 610225, China
[3] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[4] College of Artificial Intelligence, Chengdu University of Information Technology, Chengdu 610225, China

* **Correspondence:** Email: cuitzsb@cuit.edu.cn.

Abstract: This paper presents a quantum protocol for the secure privacy-preserving equality comparison of private arrays. The design overcomes the scalability limitations of conventional quantum private comparison schemes, which are typically restricted to single integers. In the proposed approach, each array element is encoded into the amplitude of a single-photon state. Participants then encrypt the received states via local rotation operations with privately chosen random angles. A circular transmission mode is employed, whereby the encrypted states are sequentially exchanged among all parties, including a semi-honest third party. The TP performs single-particle measurements to determine the equality of the arrays and broadcasts the result simultaneously to ensure fairness. The protocol's functionality and practicality were validated through quantum circuit simulations on the IBM Qiskit platform. Security analysis confirms its robustness against both external eavesdropping attacks and internal privacy threats from honest-but-curious participants. By utilizing single-photon encoding, rotation-based encryption, and single-particle measurement, the protocol achieves enhanced scalability and practical feasibility for multi-element comparisons, advancing beyond the scope of existing single-integer comparison schemes.

Keywords: privacy-preserving equality array comparison; quantum private comparison; circular

transmission mode; rotation-based encryption; single photon
Mathematics Subject Classification: 81P65, 81P94

1. Introduction

The emergence of quantum cryptography [1] represents a fundamental departure from classical security models by basing its protection on the laws of quantum mechanics, rather than on computational assumptions. This shift began with the groundbreaking BB84 protocol for quantum key distribution (QKD) introduced by Bennett and Brassard [2], which laid the foundation for provably secure communication. Since then, the field has diversified into a broad range of quantum-enhanced cryptographic protocols, including quantum secret sharing (QSS) [3,4], quantum secure direct communication (QSDC) [5,6], quantum key agreement (QKA) [7], and quantum private set intersection (QPSI) [8–10]. Together, these advances form a critical safeguard for modern information systems, offering built-in resilience against future quantum attacks and establishing the groundwork for next-generation secure communications.

Secure multiparty computation (MPC) [11] introduces a transformative paradigm that enables multiple parties to jointly compute a function while keeping their inputs private, thus separating the act of computation from the need to reveal sensitive data. This capability has driven important advances in privacy-preserving applications, including collaborative data analysis [12], secure electronic voting [13], and machine learning [14,15]. A foundational problem in this area is the "millionaires' problem", pioneered by Yao [16], wherein two parties compare their private financial holdings without revealing the actual amounts. This was later extended by Boudot et al. [17] to the "socialist millionaires' problem", which allows two parties to verify whether their inputs are equal while preserving confidentiality. However, a fundamental constraint in two-party protocols was identified by Lo [18], who established that unconditional security for functions such as private comparison cannot be achieved without the involvement of a third party. To address this constraint, a common and practical resolution employs a semi-honest third party (TP). In this model, the TP follows the protocol specifications correctly but may passively analyze all accessible information in an attempt to infer private data. This well-defined, relaxed trust assumption allows MPC with proven input privacy.

While classical private comparison protocols rely on computational hardness assumptions for security, the emergence of quantum computing fundamentally undermines this foundation. For instance, Shor algorithm [19] can factor integers in polynomial time, thereby breaking widely used public-key cryptosystems such as RSA. Similarly, Grover algorithm [20] provides a quadratic speedup for unstructured search, effectively halving the security strength of symmetric-key primitives. Faced with these threats, quantum private comparison (QPC) represents a paradigm shift in secure computation. Rather than depending on mathematical intractability, QPC leverages inherent quantum mechanical principles—such as the no-cloning theorem and quantum indeterminacy—to achieve information-theoretic security that remains robust even against adversaries equipped with quantum computing capabilities.

The field of quantum private comparison (QPC) originated with the pioneering protocol by Yang and Wen [21], which employed Einstein–Podolsky–Rosen (EPR) pairs for secure integer equality testing. This foundational study stimulated extensive research, leading to protocols that

leverage a wide array of quantum resources—such as single photons [22–24], Bell states [25,26], multi-particle entangled systems [27–29], cluster states [30,31], and *d*-dimensional quantum states [32,33]—to improve security and efficiency. Subsequent work has broadened the functional scope of QPC. For example, Wu and Zhao [34] generalized the comparison task using *d*- dimensional Bell states to evaluate the relative magnitude of private inputs, an approach later refined by Lang [35] into a dedicated quantum private magnitude comparison protocol. Practical scalability has been enhanced through techniques such as the swap test, which enables direct comparison of secrets [36]. In parallel, semi-quantum protocols [37–39] have been developed to relax the quantum requirements of participants while preserving security, thereby improving feasibility under near-term technological constraints.

Existing QPC protocols predominantly depend on quantum resources such as multi-particle entangled systems or *d*-level quantum states, whose experimental generation remains challenging with current technology. In contrast, approaches based on simpler resources—notably single photons—offer greater feasibility for near-term implementation. Furthermore, a fundamental limitation within the research landscape is that most existing schemes are conceptually limited to the comparison of single integers. This narrow focus constrains their applicability to real-world scenarios that require privacy-preserving comparison of entire datasets or arrays. These two issues—the experimental overhead of complex states and the lack of scalable multi-element comparison—collectively represent a crucial research gap.

To address both challenges, this work introduces a quantum protocol for the secure privacy-preserving equality comparison of private arrays, thereby overcoming the scalability limitations of conventional QPC schemes, which are typically restricted to single integers. The main contributions are summarized as follows:

(1) We propose a quantum secure privacy-preserving array equality comparison (QSPPAEC) protocol assisted by a semi-honest third party (TP). Unlike prior quantum private comparison (QPC) schemes that rely on experimentally demanding resources such as multi-particle entanglement or high-dimensional states and are limited to bit-wise integer comparison, our protocol employs single-photon encoding with random rotation encryption and supports direct array-level comparison in a circular transmission mode. This design enhances both practical feasibility and scalability for multi-element private comparison.

(2) We demonstrate the protocol's practical feasibility by implementing a concrete case study via quantum circuit simulation on the IBM Qiskit simulator. The results verify the functional correctness and operational viability of the design using near-term accessible quantum components.

(3) A comprehensive security evaluation shows the protocol's resilience against both external attacks and honest-but-curious participant behaviors, ensuring fairness through broadcast of only the final comparison result.

The remainder of this paper is organized as follows: Section 2 introduces the principles of rotation-based encryption. A detailed description of the proposed QSPPAEC protocol is provided in Section 3. Simulation experiments and a comprehensive security analysis are presented in Sections 4 and 5, respectively. Section 6 evaluates the protocol through a comparative analysis with existing schemes, and Section 7 concludes the work.

2. Rotation-based encryption

The rotation operation [40] around the y-axis is defined as

$$R_y(\gamma) = e^{-i\frac{\gamma}{2}Y} = \cos\frac{\gamma}{2} I - i\sin\frac{\gamma}{2} Y = \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \tag{1}$$

Where Y is the Pauli-Y matrix and $\gamma \in [0,2\pi)$. Let δ_m and δ_c denote the quantum plaintext and ciphertext. A rotation-based encryption framework for a single-qubit state $|\psi\rangle$ operates as follows:

- **Key Generation (KeyGen):** Randomly select an encryption key $\gamma \in [0,2\pi)$.
- **Encryption (Enc):** Applying $R_y(\gamma)$ to the plaintext δ_m: $\delta_c = R_y(\gamma)\delta_m$.
- **Decryption (Dec):** Applying $R_y(-\gamma)$ to the ciphertext δ_c: $\delta_m = R_y(-\gamma)\delta_c$.

Consider a single-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as an example. Its encryption yields:

$$\begin{aligned} |\psi_{Enc}\rangle = R_y(\gamma)|\psi\rangle &= \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha\cos\frac{\gamma}{2} - \beta\sin\frac{\gamma}{2} \\ \alpha\sin\frac{\gamma}{2} + \beta\cos\frac{\gamma}{2} \end{pmatrix} \\ &= \left(\alpha\cos\frac{\gamma}{2} - \beta\sin\frac{\gamma}{2}\right)|0\rangle + \left(\alpha\sin\frac{\gamma}{2} + \beta\cos\frac{\gamma}{2}\right)|1\rangle \end{aligned} \tag{2}$$

The rotation transforms $|\psi\rangle$ into an unknown state that cannot be deterministically recovered without knowledge of the key γ, thereby implementing encryption. Decryption is achieved by applying $R_y(-\gamma)$ to $|\psi_{Enc}\rangle$, which returns the original state $|\psi\rangle$.

$$\begin{aligned} R_y(-\gamma)|\psi_{Enc}\rangle &= \begin{pmatrix} \cos\frac{\gamma}{2} & \sin\frac{\gamma}{2} \\ -\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} \alpha\cos\frac{\gamma}{2} - \beta\sin\frac{\gamma}{2} \\ \alpha\sin\frac{\gamma}{2} + \beta\cos\frac{\gamma}{2} \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \alpha|0\rangle + \beta|1\rangle = |\psi\rangle \end{aligned} \tag{3}$$

An essential property of rotation operations is their homomorphic addition: for any two angles θ_1 and θ_2, we have

$$R_y(\gamma_1)R_y(\gamma_2)=R_y(\gamma_2)R_y(\gamma_1)=\begin{pmatrix}\cos\frac{\gamma_1}{2} & -\sin\frac{\gamma_1}{2}\\ \sin\frac{\gamma_1}{2} & \cos\frac{\gamma_1}{2}\end{pmatrix}\begin{pmatrix}\cos\frac{\gamma_2}{2} & -\sin\frac{\gamma_2}{2}\\ \sin\frac{\gamma_2}{2} & \cos\frac{\gamma_2}{2}\end{pmatrix}$$
$$=\begin{pmatrix}\cos\frac{\gamma_1+\gamma_2}{2} & -\sin\frac{\gamma_1+\gamma_2}{2}\\ \sin\frac{\gamma_1+\gamma_2}{2} & \cos\frac{\gamma_1+\gamma_2}{2}\end{pmatrix}=R_y(\gamma_1+\gamma_2) \tag{4}$$

This property is fundamental to the design of the protocol presented in the next section.

3. The proposed QSPPAEC protocol

We now present the proposed QSPPAEC protocol for array comparison. In this framework, two participants, Alice and Bob, wish to determine whether their respective private arrays $A=(a_1,a_2,\ldots,a_L)$ and $B=(b_1,b_2,\ldots,b_L)$ are equal, i.e., whether $A=B$. A semi-honest (honest-but-curious) third party (TP) assists in the computation without knowing the elements of the arrays and without colluding with either participant.

The protocol satisfies the following properties:

Correctness: If all parties follow the protocol honestly, the TP obtains the correct comparison result and announces it reliably.

Privacy: The contents of A and B remain confidential against external eavesdroppers as well as against other participants, including the TP.

Fairness: The final result is communicated to Alice and Bob simultaneously, preventing either party from gaining an advantage or acting on the outcome before the other.

Prior to protocol execution, the following conditions are assumed:

- Quantum states are transmitted without photon loss or degradation from environmental noise.
- All parties have access to perfect single-photon sources, detectors, and quantum memories.
- The classical communication channel is authenticated, preventing man-in-the-middle attacks on classical processing.
- Alice and Bob share a secret key sequence $\Theta^{AB}=(\theta_1^{AB},\theta_2^{AB},\ldots,\theta_L^{AB})$, established beforehand via a QKD protocol, such as the BB84 protocol [2].

These assumptions are standard in the theoretical analysis of quantum communication protocols. They allow us to establish the theoretical feasibility of the protocol by isolating the core quantum mechanical principles from the complexities of physical implementation. This enables rigorous analysis of the protocol's security and functionality, providing a necessary benchmark against which all practical realizations can be compared.

However, a practical implementation must contend with real-world imperfections. For instance, quantum channels are inherently noisy and lossy. While techniques such as quantum error-correcting codes [41–43] can mitigate these effects, they introduce significant trade-offs due to the overhead of encoding and error correction.

The detailed steps of the protocol are described below:

Step 1. State preparation by the TP

The TP initializes a quantum sequence S of length L, with each qubit prepared in the state $|0\rangle$.

$$S = |0\rangle|0\rangle \mathrm{L}\ |0\rangle = |0\rangle^{\otimes L} \tag{5}$$

The TP then generates a secret key sequence $\Theta^{TP} = (\theta_1^{TP}, \theta_2^{TP}, \ldots, \theta_L^{TP})$, where each $\theta_i^{TP} \in [0,2\pi)$. For the i-th qubit, the TP applies the rotation operation $R_y(\theta_i^{TP})$ to produce the encrypted initial sequence S_{Enc}.

$$\begin{aligned} S_{Enc} &= R_y\left(\theta_i^{TP}\right) S = R_y\left(\theta_1^{TP}\right)|0\rangle R_y\left(\theta_2^{TP}\right)|0\rangle \mathrm{L}\ R_y\left(\theta_L^{TP}\right)|0\rangle \\ &= \left(R_y\left(\theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \end{aligned} \tag{6}$$

Step 2. Insertion of decoy photons and transmission to Alice

To enable eavesdropping detection, the TP prepares δ decoy photons, each randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. These decoy photons are inserted at random positions into S_{Enc}, forming a new sequence S'_{Enc}. The TP records the positions and initial states of all decoy photons and sends S'_{Enc} to Alice.

Step 3. Eavesdropping check on the TP–Alice channel

Upon receiving S'_{Enc}, Alice acknowledges receipt via the authenticated classical channel. The TP then publicly announces the positions and corresponding measurement bases (Z-basis for $\{|0\rangle, |1\rangle\}$, X-basis for $\{|+\rangle, |-\rangle\}$) of the decoy photons. Alice measures the indicated decoy photons in the given bases and reports her outcomes to the TP. The TP compares these results with the initial states of the decoy photons and computes the quantum bit error rate (QBER). If the QBER exceeds a predefined threshold (typically 2%–8.9%, depending on channel conditions), the protocol is aborted and restarted, as this indicates a high probability of eavesdropping. If the QBER remains below the threshold, the quantum channel is considered secure, and the protocol proceeds.

Step 4. Encoding and encryption by Alice

After confirming the channel is secure, Alice removes the decoy photons from S'_{Enc} to recover S_{Enc}. She encodes her private array $A = (a_1, a_2, \ldots, a_L)$ as a sequence of rotation angles $\Theta_A = (\theta_1^A, \theta_2^A, \ldots . \theta_L^A)$, where

$$\theta_i^A = \begin{cases} 0 & if\ a_i = 0, \\ \pi / a_i & otherwise. \end{cases}$$

Using her pre-shared key Θ^{AB}, Alice applies the rotation operation $R_y(\theta_i^A + \theta_i^{AB})$ to the i-th qubit in S_{Enc}, obtaining the transformed sequence S_A.

$$\begin{aligned} S_A &= R_y\left(\theta_i^A + \theta_i^{AB}\right) S_{Enc} = \left(R_y\left(\theta_i^A + \theta_i^{AB}\right)\left(R_y\left(\theta_i^{TP}\right)|0\rangle\right)\right)^{\otimes_{i=1}^{L}} \\ &= \left(R_y\left(\theta_i^A + \theta_i^{AB} + \theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \end{aligned} \tag{7}$$

For further encryption, she generates a random local key $K_A = (\theta_1^{Enc\_A}, \theta_2^{Enc\_A}, \cdots, \theta_L^{Enc\_A})$ with $\theta_i^{Enc\_A} \in [0,2\pi)$, and applies $R_y(\theta_i^{Enc\_A})$ to each qubit, yielding the encrypted sequence S_{Enc_A}.

$$S_{Enc\_A} = R_y\left(\theta_i^{Enc-A}\right)S_A = \left(R_y\left(\theta_i^{Enc-A}\right)\left(R_y\left(\theta_i^{A} + \theta_i^{AB} + \theta_i^{TP}\right)|0\rangle\right)\right)^{\otimes_{i=1}^{L}}$$
$$= \left(R_y\left(\theta_i^{Enc-A} + \theta_i^{A} + \theta_i^{AB} + \theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \quad (8)$$

Finally, she inserts δ decoy photons (randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ at random positions to form S'_{Enc_A}, records their positions and states, and sends S'_{Enc_A} to Bob.

Step 5. Eavesdropping check on the Alice–Bob channel

Bob and Alice perform an eavesdropping check on S'_{Enc_A} using the same procedure described in Step 3. If the computed QBER exceeds the predefined threshold, the protocol is aborted and restarted; otherwise, it proceeds.

Step 6. Encoding and encryption by Bob

Bob removes the decoy photons to recover S_{Enc_A}. He encodes his array $B = (b_1, b_2, \ldots, b_L)$ as $\Theta_B = (\theta_1^B, \theta_2^B, \ldots . \theta_L^B)$, where

$$\theta_i^B = \begin{cases} 0 & if\ b_i = 0, \\ \pi / b_i & otherwise. \end{cases}$$

Bob then applies $R_y(-\theta_i^B - \theta_i^{AB})$ to the i-th qubit, obtaining S_B.

$$S_B = R_y\left(-\theta_i^B - \theta_i^{AB}\right)S_{Enc\_A} = \left(R_y\left(-\theta_i^B - \theta_i^{AB}\right)\left(\left(R_y\left(\theta_i^{Enc-A} + \theta_i^{A} + \theta_i^{AB} + \theta_i^{TP}\right)|0\rangle\right)\right)\right)^{\otimes_{i=1}^{L}}$$
$$= \left(R_y\left(-\theta_i^B + \theta_i^{Enc-A} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \quad (9)$$

Next, he generates his own random encryption key $K_B = (\theta_1^{Enc\_B}, \theta_2^{Enc\_B}, \cdots, \theta_{L-1}^{Enc\_B})$ and applies $R_y(\theta_i^{Enc\_B})$ to each qubit, producing S_{Enc_B}.

$$S_{Enc\_B} = R_y\left(\theta_i^{Enc-B}\right)S_B = \left(R_y\left(\theta_i^{Enc-B}\right)\left(R_y\left(-\theta_i^{B} + \theta_i^{Enc-A} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)\right)^{\otimes_{i=1}^{L}}$$
$$= \left(R_y\left(\theta_i^{Enc-B} - \theta_i^{B} + \theta_i^{Enc-A} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \quad (10)$$

After inserting δ decoy photons (similarly chosen and recorded), he transmits the resulting sequence S'_{Enc_B} to the TP.

Step 7. Eavesdropping check on the Bob–TP channel

The TP and Bob conduct an eavesdropping check on S'_{Enc_B} as in Step 3. If the QBER is within tolerance, the protocol continues; otherwise, it is terminated and restarted.

Step 8. Key disclosure

Alice and Bob simultaneously disclose their respective encryption keys K_A and K_B to the TP via the authenticated classical channel. The TP records both keys for the decryption phase.

Step 9. Decryption and measurement by the TP

The TP removes the decoy photons from S'_{Enc_B} to recover S_{Enc_B}. Sequentially, for each qubit, the TP applies:

1) $R_y\left(-\theta_i^{Enc\_A} - \theta_i^{Enc\_B}\right)$ (using the disclosed keys), yielding an intermediate sequence S_{AB}.

$$\begin{aligned} S_{AB} &= R_y\left(-\theta_i^{Enc\_A} - \theta_i^{Enc\_B}\right) S_{Enc\_B} \\ &= \left(R_y\left(-\theta_i^{Enc\_A} - \theta_i^{Enc\_B}\right)\left(R_y\left(\theta_i^{Enc\_B} - \theta_i^{B} + \theta_i^{Enc\_A} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)\right)^{\otimes_{i=1}^{L}} \\ &= \left(R_y\left(-\theta_i^{B} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \end{aligned} \tag{11}$$

2) $R_y(-\theta_i^{TP})$ (using its own secret key Θ^{TP}), producing the final sequence S_R.

$$S_R = R_y\left(-\theta_i^{TP}\right) S_{AB} = \left(R_y\left(-\theta_i^{TP}\right)\left(R_y\left(-\theta_i^{B} + \theta_i^{A} + \theta_i^{TP}\right)|0\rangle\right)\right)^{\otimes_{i=1}^{L}} = \left(R_y\left(-\theta_i^{B} + \theta_i^{A}\right)|0\rangle\right)^{\otimes_{i=1}^{L}} \tag{12}$$

The TP then measures each qubit in S_R using the Z-basis $\{|0\rangle, |1\rangle\}$ and records the outcome.

Step 10. Iteration and result announcement

Steps 1–9 are repeated for λ independent iterations. After collecting all measurement outcomes, the TP decides:

- If any measurement yields $|1\rangle$, the arrays A and B are not equal.
- If all measurements yield $|0\rangle$, the arrays are equal.

The TP broadcasts the final result simultaneously to Alice and Bob.

4. Simulation experiment

To validate the proposed protocol's functionality, we implemented and simulated the complete quantum workflow using the IBM Qiskit framework (version 0.44.1) in a Python 3.11.4 environment. All simulations were executed with 1000 measurement shots per experiment to ensure statistically meaningful results. In this initial study, the simulations were configured to run in an ideal, noise-free environment. This deliberate choice allows us to first isolate and verify the core logical correctness and operational feasibility of the protocol before introducing the complexities of realistic quantum noise and hardware imperfections. For clarity, eavesdropping detection—implemented via decoy photons—is treated as a separate security module and is therefore not incorporated into the current computational simulation.

Two concrete test cases are presented below to demonstrate the protocol's feasibility.

Case I. Equality test of arrays $A = (3, 1, 1, 2, 4)$ and $B = (3, 2, 1, 4, 4)$

Consider a scenario where Alice and Bob possess the private arrays $A = (3,1,1,2,4)$ and $B = (3,2,1,4,4)$. The objective is to determine whether $A = B$. The simulation uses the following fixed parameters:

- Pre-shared secret key (via QKD): $K_{AB} = \left(\frac{\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}, \frac{\pi}{4}, \frac{\pi}{2}\right)$.
- TP's secret key: $\Theta^{TP} = \left(\frac{5\pi}{6}, \frac{\pi}{2}, \frac{3\pi}{4}, \frac{\pi}{3}, \frac{11\pi}{12}\right)$.
- Alice's random encryption key: $K_A = \left(\frac{\pi}{3}, \frac{\pi}{4}, \frac{\pi}{2}, \frac{11\pi}{6}, \pi\right)$.
- Bob's random encryption key: $K_B = \left(\frac{3\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}, \frac{\pi}{6}, \frac{2\pi}{3}\right)$.
- Initial quantum sequence: $S = \{|0\rangle, |0\rangle, |0\rangle, |0\rangle, |0\rangle\}$.

The quantum circuit implementing the comparison protocol for arrays $A = (3,1,1,2,4)$ and $B = (3,2,1,4,4)$ is presented in Figure 1. The statistical distribution of the final Z-basis measurement outcomes, collected over 1000 shots, is shown in Figure 2.

Figure 2 presents the measurement outcomes from 1000 circuit executions, as confirmed by the sum of the four bar heights (404 + 445 + 72 + 79 = 1000). The bitstrings on the x-axis adhere to Qiskit's little-endian convention: the rightmost bit represents qubit q_0, and the leftmost bit represents qubit q_4, yielding the format $q_4q_3q_2q_1q_0$.

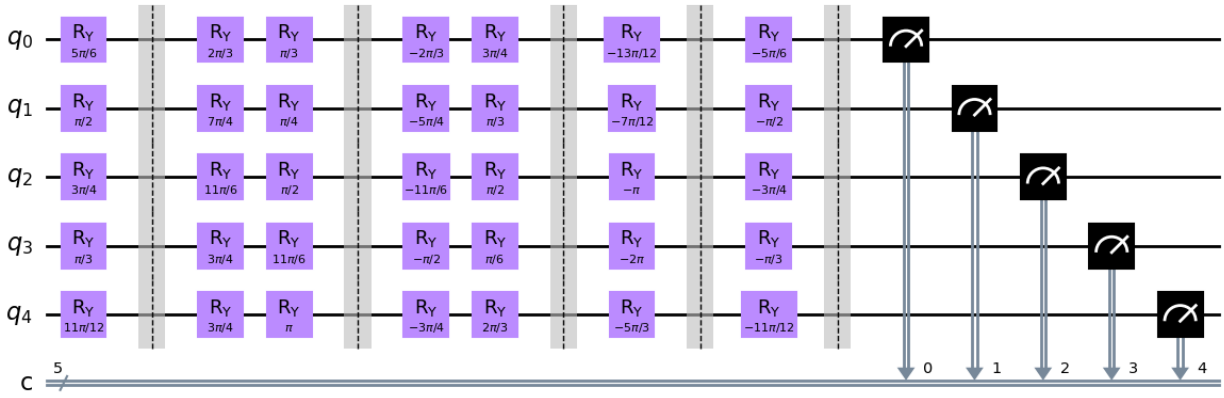

Figure 1. Quantum circuit implementing the comparison protocol for arrays A = (3,1,1,2,4) and B = (3,2,1,4,4).

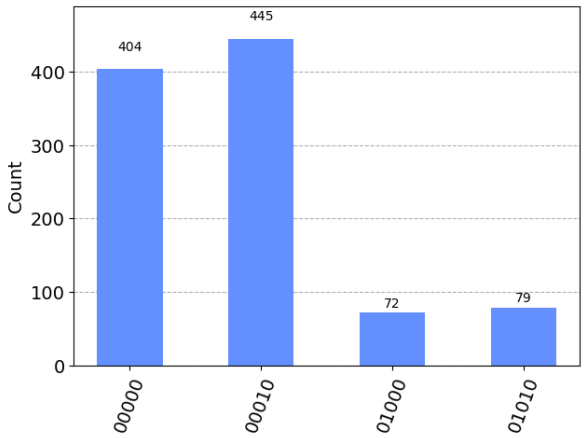

Figure 2. Statistical distribution of the final Z-basis measurement outcomes for the circuit in Figure 1, collected over 1000 shots.

From the four observed outcomes—00000, 00010, 01000, and 01010—we can infer the pre-measurement states of the qubits as follows:

- Qubits q_0, q_2, and q_4 consistently measured 0 in all cases, indicating they remained in the ground state $|0\rangle$ throughout the circuit.
- Qubits q_1 and q_3, however, exhibited both 0 and 1 measurement outcomes, demonstrating that

they were successfully placed into superposition states. The non-zero probabilities of finding these qubits in the $|1\rangle$ state further support this observation.

According to the protocol's decision rule—where any $|1\rangle$ measurement definitively indicates inequality—this result confirms that arrays A and B are not equal.

Case II. Equality test of arrays $A' = (3,1,4,2,6)$ and $B' = (3,1,4,2,6)$

In this scenario, Alice and Bob possess identical private arrays $A' = (3,1,4,2,6)$ and $B' = (3,1,4,2,6)$. The objective is to determine whether $A' = B'$. All other parameters—the pre-shared key K_{AB}, the TP's secret key Θ^{TP}, and the participants' random encryption keys K_A and K_B—are identical to those used in Case I.

The corresponding quantum circuit is shown in Figure 3. The statistical distribution of the final Z-basis measurement outcomes, collected over 1000 shots, is presented in Figure 4.

Figure 4 displays the measurement outcomes from 1000 shots, revealing a single result: 00000. Under the little-endian convention, where the bitstring is ordered as $q_4q_3q_2q_1q_0$ (with q_0 as the rightmost bit), this outcome signifies that qubits q_0 through q_4 were all measured as 0 in every execution. Consequently, we can conclude that all five qubits remained in the ground state $|0\rangle$, exhibiting purely deterministic behavior throughout the experiment. In accordance with the protocol's decision rule—where uniform $|0\rangle$ results across all trials signify equality—we conclusively determine that $A' = B'$.

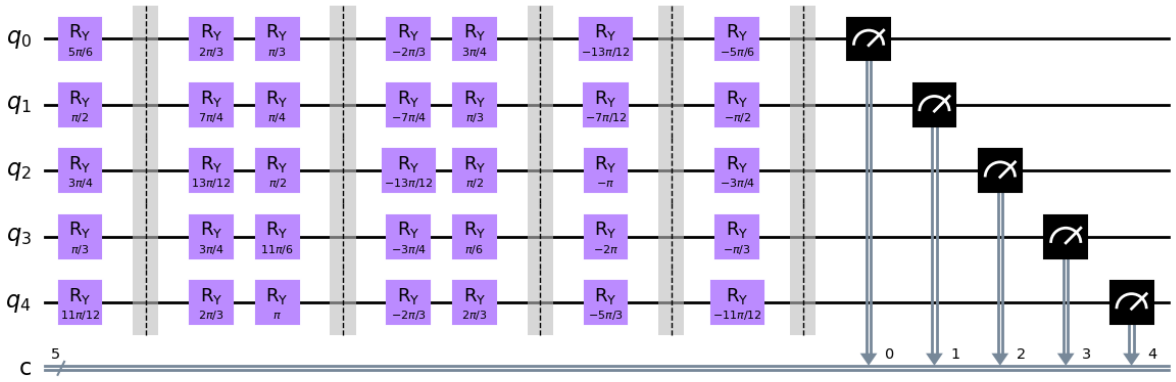

Figure 3. Quantum circuit implementing the comparison protocol for arrays $A' = (3,1,4,2,6)$ and $B' = (3,1,4,2,6)$.

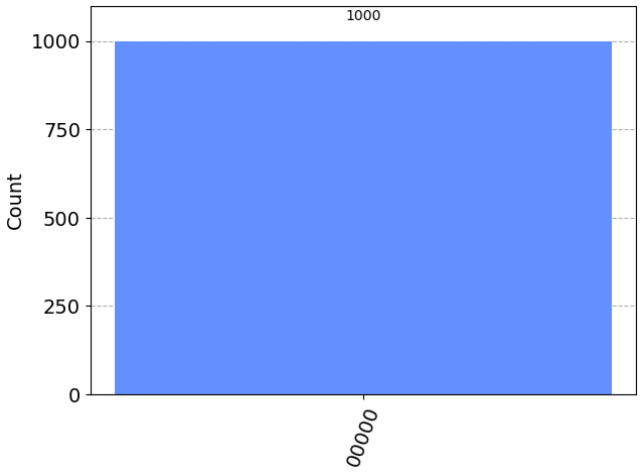

Figure 4. Statistical distribution of the final Z-basis measurement outcomes for the circuit in Figure 3, collected over 1000 shots.

Together, the two simulated cases—one where the arrays differ and another where they are identical—successfully validate the correctness and feasibility of the proposed protocol.

5. Analysis

5.1. Security analysis

The security of the proposed QPC protocol is evaluated against threats from both external adversaries and honest-but-curious (semi-honest) participants. External eavesdroppers may attempt attacks on the quantum channels—such as intercept-resend, entangle-measure, or Trojan horse attacks—while participating entities could leverage their legitimate access to intermediate data to infer private inputs. To address these challenges, the protocol employs a dual-layer defense strategy: (1) active quantum-channel monitoring using decoy photons, and (2) cryptographic encryption of all transmitted quantum states. External and participant attacks are analyzed as follows.

5.1.1. External attacks

The protocol is designed to resist external eavesdropping attempts by adversaries seeking to extract the private arrays A and B. Its security is built on two complementary pillars: (1) the encryption of sensitive information into single-photon states using pre-shared secret keys, and (2) the use of decoy photons for active channel monitoring. Decoy photons, randomly drawn from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserted at unknown positions, enable the detection of eavesdropping without requiring prior knowledge of their location or basis. External attack strategies are analyzed as follows:

Case I. Intercept-resend attack

In an intercept-resend attack, an eavesdropper (Eve) captures the transmitted quantum sequence, measures each qubit in a randomly chosen basis, and prepares a new state to forward based on her outcome. Because Eve cannot distinguish between information carriers and decoy photons, any

interaction with a decoy is likely to disturb its state and introduce a detectable error during the subsequent verification phase.

Consider a decoy photon prepared in the $|-\rangle$ state (X-basis). If Eve measures it in the Z-basis $\{|0\rangle, |1\rangle\}$, the measurement randomly projects the state onto $|0\rangle$ or $|1\rangle$ with equal probability. Resending this projected state will, with probability $1/2$, produce a mismatch when the legitimate party later measures it using X-basis. Since Eve chooses her measurement basis uniformly at random, the overall probability that her action on a single decoy photon goes undetected is:

$$P_{pass} = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}.$$

The first term corresponds to her correctly guessing the decoy's basis (no error), and the second term corresponds to guessing wrongly, where an error occurs with probability $1/2$. For a sequence containing δ decoy photons, the probability that Eve avoids detection on all of them is:

$$P_{eavde} = (3/4)^{\delta}.$$

Consequently, the protocol's detection probability is:

$$P_{detect} = 1 - (3/4)^{\delta}$$

As δ increases, this probability approaches 1. For instance, with $\delta = 30$ decoy photons, $P_{\text{evade}} \approx 0.0002$, meaning the attack is detected with probability >99.98%. This exponentially decaying evasion probability ensures that any intercept-resend attempt is virtually certain to be detected, thereby preventing information leakage about A and B.

Case II. Entangle-measure attack

An eavesdropper (Eve) intercepts the transmitted sequences S'_{Enc_A} or S'_{Enc_B} and applies a unitary operation U to create a correlation between the intercepted qubit and her ancillary state $|E\rangle$, thereby creating entanglement between the transmitted state and her probe system.

The action of U on the four possible decoy states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ can be described as follows:

$$U|0\rangle|E\rangle = \alpha_{00}|0\rangle|E_{00}\rangle + \alpha_{01}|1\rangle|E_{01}\rangle \tag{13}$$

$$U|1\rangle|E\rangle = \alpha_{10}|0\rangle|E_{10}\rangle + \alpha_{11}|1\rangle|E_{11}\rangle \tag{14}$$

$$\begin{aligned} U|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}\ U|0\rangle|E\rangle + U|1\rangle|E\rangle \\ &= \frac{1}{\sqrt{2}}\ \alpha_{00}|0\rangle|E_{00}\rangle + \alpha_{01}|1\rangle|E_{01}\rangle + \alpha_{10}|0\rangle|E_{10}\rangle + \alpha_{11}|1\rangle|E_{11}\rangle \\ &= \frac{1}{2}|+\rangle\ \alpha_{00}|E_{00}\rangle + \alpha_{01}|E_{01}\rangle + \alpha_{10}|E_{10}\rangle + \alpha_{11}|E_{11}\rangle \\ &\quad + \frac{1}{2}|-\rangle\ a_{00}|E_{00}\rangle - a_{01}|E_{01}\rangle + a_{10}|E_{10}\rangle - a_{11}|E_{11}\rangle \end{aligned} \tag{15}$$

$$\begin{aligned} U|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}\ U|0\rangle|E\rangle - U|1\rangle|E\rangle \\ &= \frac{1}{\sqrt{2}}\ \alpha_{00}|0\rangle|E_{00}\rangle + \alpha_{01}|1\rangle|E_{01}\rangle - \alpha_{10}|0\rangle|E_{10}\rangle - \alpha_{11}|1\rangle|E_{11}\rangle \\ &= \frac{1}{2}|+\rangle\ \alpha_{00}|E_{00}\rangle + \alpha_{01}|E_{01}\rangle - \alpha_{10}|E_{10}\rangle - \alpha_{11}|E_{11}\rangle \\ &+ \frac{1}{2}|-\rangle\ a_{00}|E_{00}\rangle - a_{01}|E_{01}\rangle - a_{10}|E_{10}\rangle + a_{11}|E_{11}\rangle \end{aligned} \tag{16}$$

Here, $\{|E_{00}\rangle, |E_{01}\rangle, |E_{10}\rangle, |E_{11}\rangle\}$ are states of Eve's ancilla determined by U, and the complex coefficients satisfy the normalization conditions:

$$|\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{17}$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 = 1 \tag{18}$$

For the attack to remain undetected during the decoy-photon verification, the unitary operation must not introduce any observable disturbance to the decoy states. This requirement imposes the constraints: $\alpha_{01} = \alpha_{10} = 0$ and $\alpha_{00}|E_{00}\rangle = \alpha_{11}|E_{11}\rangle$. Under these conditions, we have:

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

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

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

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

Thus, the output states in Eqs (19)–(22) are all product states; that is, the transmitted qubit and Eve's ancilla remain completely unentangled. Consequently, any subsequent measurement on Eve's probe yields no information about the intercepted quantum data. This renders the entanglement-measure attack ineffective.

Case III. Trojan horse attacks

Although Trojan horse attacks—specifically the delay-photon and invisible-photon variants [44]—typically target protocols with explicit bidirectional quantum exchange, the proposed circular transmission mode could, in principle, introduce a vulnerability if an adversary injects extra photons into the channel. To counter this, the protocol can integrate standard physical-layer defenses: a wavelength filter and a photon number splitter (PNS). Wavelength filtering restricts incoming signals to a narrow band around the legitimate operational wavelength, thereby blocking out-of-band invisible photons. PNS detection allows the receiver to randomly sample the signal and measure the photon number per pulse. An anomalously high multi-photon rate would indicate the presence of delayed photons, triggering session termination. These well-established countermeasures [47]

effectively neutralize both primary forms of Trojan horse attacks, ensuring that no information is leaked through such side channels.

The combined use of decoy-photon-based eavesdropping checks and the aforementioned physical countermeasures provides robust, multi-layered protection for the private arrays A and B. The intercept-resend and entangle-measure attacks are detected with exponentially high probability, while Trojan horse attacks are prevented by optical filtering and photon-number verification. Consequently, the protocol ensures the confidentiality of the transmitted data against the considered external adversarial strategies.

5.1.2. Participant attacks

Because honest-but-curious participants legitimately receive and process intermediate information during the protocol's execution, insider threats represent a particularly critical security challenge. The following analysis evaluates the protocol's privacy guarantees against both the semi-honest TP and each participant (Alice or Bob), confirming that no single party can successfully deduce the private inputs.

Case I. Semi-honest TP adversary

Under the semi-honest adversary model, the TP is assumed to execute all protocol operations correctly while potentially analyzing any accessible data in an attempt to learn A and B. Although the TP prepares the initial sequence S and receives the processed sequence S_{AB}, these sequences are the result of composite rotations that depend on the private encoding angles θ_i^A, θ_i^B and the secret pre-shared key. Crucially, θ_i^B is known exclusively to Alice and Bob and is never disclosed to the TP.

The encoding angles θ_i^A and θ_i^B (which directly correspond to the array elements a_i and b_i) remain concealed due to quantum indeterminacy. Without knowledge of θ_i^{AB}, the TP cannot resolve the combined rotation $R_y(\theta_i^A + \theta_i^{AB})$ and $R_y(-\theta_i^B - \theta_i^{AB})$ applied to $R_y(\theta_i^{TP})|0\rangle$. Consequently, even with access to the intermediate quantum states, the TP cannot extract meaningful information about A or B.

Case II. Honest-but-curious Alice or Bob

We consider the adversarial scenario in which one participant, while adhering to the protocol, attempts to deduce the other's private data. As the design enforces symmetric roles, the analysis for Alice inferring Bob's array B applies identically to Bob inferring array A.

Bob proceeds to encode his private array B by mapping each element b_i to a corresponding rotation angle θ_i^B. This angle is applied via the operation $R_y(\theta_i^B)$ to each qubit in the sequence S_{Enc_A}, followed by an additional encryption using Bob's private key $\theta_i^{Enc\_B}$. The resulting sequence S'_{Enc_B} (protected by decoy photons) is transmitted directly to the TP. Alice never receives S_{Enc_B} or S'_{Enc_B} during normal protocol execution.

Even if Alice were to intercept and analyze the encrypted sequence, her ability to extract information is fundamentally constrained. Without access to Bob's secret encryption key $\theta_i^{Enc\_B}$ (which is disclosed only to the TP after successful eavesdropping checks) and the pre-shared key θ_i^{AB}, the encoded state cannot be resolved. Furthermore, the inherent quantum indeterminacy of unknown quantum states prevents their unambiguous determination from a single copy.

Thus, the confidentiality of array B is guaranteed as long as the encoding angle θ_i^B remains undisclosed—a condition upheld by the protocol's design. An identical argument applies symmetrically to protect array A from curious attempts by Bob.

The protocol ensures end-to-end confidentiality of the private arrays against all insider threats. Under the semi-honest adversarial model—applied to the TP, Alice, or Bob—all critical parameters required to infer the private inputs (specifically the pre-shared key θ_i^{AB} and the individual encoding angles θ_i^A, θ_i^B) remain provably inaccessible. Consequently, even when behaving curiously, no single party can successfully deduce the contents of A or B.

5.2. Fairness

Fairness is guaranteed by delegating the final measurement and announcement to the TP. After measuring S_R in the Z-basis, the TP simultaneously communicates the outcome to both parties, ensuring neither Alice nor Bob gains premature knowledge or any procedural advantage.

6. Comparison

The proposed protocol is compared with existing QPC schemes in Table 1, with respect to quantum resource requirements, unitary operations, entanglement swapping, measurement for users and the TP, and the scope of comparison. This analysis highlights three principal advantages of our approach:

(1) The protocol directly supports privacy-preserving equality checks of entire arrays, moving beyond the conventional focus on single integers.
(2) By relying on single-photon states, rotation operations, and single-particle measurements, this design eliminates the need for entanglement swapping and other experimentally demanding resources, such as multi-particle entangled states or high-dimensional quantum systems, which improves its feasibility for near-term implementation.
(3) The protocol employs only Z-basis measurements, rather than Bell-state or joint measurements, thereby reducing the implementation complexity.

Table 1. A comparative analysis between the proposed protocol and existing QPC schemes.

Protocol	Quantum resource requirements	Unitary operation	Entanglement swapping	Quantum measurement for users	Quantum measurement for TP	Comparison scope
Ref. [25]	Bell states	Yes	No	No	Bell-basis	Integer
Ref. [26]	Bell states	No	No	Z-basis	Z-basis	Integer
Ref. [27]	Bell states	No	Yes	GHZ-basis	No	Integer
Ref. [28]	Five-qubit entangled states	No	No	Z-basis and Bell-basis	Z-basis	Integer
Ref. [29]	Six-particle entangled states	No	Yes	Bell-basis	Bell-basis	Integer
Ref. [30]	Four-particle cluster and extend Bell state	No	Yes	Bell basis and extended Bell basis	No	Integer
Ref. [31]	Four-particle cluster state	Yes	No	No	Bell-basis	Integer

Continued on next page

Protocol	Quantum resource requirements	Unitary operation	Entanglement swapping	Quantum measurement for users	Quantum measurement for TP	Comparison scope
Ref. [32]	d-dimensional Bell state	Yes	No	d-dimensional single-particle	No	Integer
Ref. [33]	d-dimensional Bell state	Yes	Yes	d-dimensional Bell basis	d-dimensional Bell basis	Integer
Ref. [38]	Bell state	No	Yes	Z-basis	Z-basis and Bell-basis	Integer
Ref. [39]	d-dimensional Bell state	Yes	No	No	d-dimensional Bell basis	Integer
Ours	Singe photons	Yes	No	No	Z-basis	Array

7. Conclusions

This study successfully developed and validated a highly scalable quantum protocol for the privacy-preserving equality comparison of private arrays, resolving the scalability bottlenecks inherent to conventional single-integer QPC schemes. By utilizing single-photon states as information carriers and employing rotation-based encoding with privately chosen random angles, the protocol ensures strict data confidentiality for multi-element structures. Validation on the IBM Qiskit platform confirmed the protocol's functional correctness, demonstrating its operational viability without the need for deep or complex quantum circuits. Furthermore, security analysis established that the integration of decoy-photon detection and quantum state encryption provides robust, provable defense mechanisms against both external eavesdropping (e.g., intercept-resend and entanglement-based attacks) and internal privacy breaches from honest-but-curious participants or the semi-honest third party. Crucially, this work advances experimental feasibility by entirely eliminating the reliance on complex entanglement swapping, requiring only single-photon preparation and single-particle measurements.

The protocol is presently designed under idealized assumptions (e.g., lossless and noiseless channels, perfect devices). In real-world implementations, quantum channels inevitably suffer from noise and loss. While quantum error correction codes offer a means to counteract these effects, they also introduce significant performance trade-offs. Consequently, our future work will focus on a comprehensive analysis of the protocol's performance and optimization under realistic noisy conditions, specifically addressing the complex trade-offs associated with quantum error correction.

Author contributions

Min Hou: Conceptualization, Methodology, Writing–original draft, Formal analysis, Validation of results, Writing–review and editing; Yue Wu: Investigation, Writing–review and editing; Shibin Zhang: Conceptualization, Funding acquisition, Supervision, Writing–review & editing.

Use of Generative-AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This research was supported by Science and Technology Projects of Xizang Autonomous Region，China (No. XZ202501ZY0094), the Key Research and Development Project of Chengdu (No. 2023-XT00-00002-GX), the General Program of Sichuan Science and Technology & Education Joint Fund (No.2025NSFSC2098), and the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS-202605).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. C. Portmann, R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.*, **94** (2022), 025008. https://doi.org/10.1103/RevModPhys.94.025008
2. C. H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, *Theor. Comput. Sci.*, **560** (2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025
3. Y. Qin, J. Cheng, J. Ma, D. Zhao, Z. Yan, X. Jia, et al., Efficient and secure quantum secret sharing for eight users, *Phys. Rev. Res.*, **6** (2024), 033036. https://doi.org/10.1103/PhysRevResearch.6.033036
4. A. Di Santo, W. Tiberti, D. Cassioli, Security and fairness in multi-party quantum secret sharing protocol, *IEEE Trans. Quantum Eng.*, **6** (2025), 4100518. https://doi.org/10.1109/TQE.2025.3535823
5. Y.-B. Sheng, L. Zhou, G.-L. Long, One-step quantum secure direct communication, *Sci. Bull.*, **67** (2022), 367–374. https://doi.org/10.1016/j.scib.2021.11.002
6. H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, J. Yu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states, *Light Sci. Appl.*, **11** (2022), 83. https://doi.org/10.1038/s41377-022-00769-w
7. Y.-X. Shu, C.-M. Bai, S. Zhang, Multiparty quantum key agreement based on GHZ states, *EPJ Quantum Technol*., **12** (2025): 48. https://doi.org/10.1140/epjqt/s40507-025-00353-2
8. R.-H. Shi, Y.-F. Li, Quantum private set intersection cardinality protocol with application to privacy-preserving condition query, *IEEE Trans. Circuits Syst. I Regul. Pap.*, **69** (2022), 2399–2411. https://doi.org/10.1109/TCSI.2022.3152591
9. R.-H. Shi, Y.-F. Li, Quantum protocol for secure multiparty logical AND with application to multiparty private set intersection cardinality, *IEEE Trans. Circuits Syst. I Regul. Pap.*, **69** (2022), 5206–5218. https://doi.org/10.1109/TCSI.2022.3200974
10. M. Hou, Y. Wu, S. Zhang, Quantum private set intersection scheme based on Bell states, *Axioms*, **14** (2025), 120. https://doi.org/10.3390/axioms14020120
11. D. Feng, K. Yang, Concretely efficient secure multi-party computation protocols: survey and more, *Security and Safety*, **1** (2022), 2021001. https://doi.org/10.1051/sands/2021001

12. P. Tamilselvi, V. Lathika, S. Jayachitra, S Arunkumar, M. Balasubramani, V Kalaichelvi, Secure multi-party computation for collaborative data analysis in network security, In: *2024 International conference on intelligent and innovative technologies in computing, electrical and electronics (IITCEE)*, Bangalore, India, 2024, 1–5. https://doi.org/10.1109/IITCEE59897.2024.10467913
13. X. Qian, L. Wei, J. Zhang, L. Zhang, Malicious-secure threshold multi-party private set intersection for anonymous electronic voting, *Cryptography*, **9** (2025), 23. https://doi.org/10.3390/cryptography9020023
14. I. Zhou, F. Tofigh, M. Piccardi, M. Abolhasan, D. Franklin, J. Lipman, Secure multi-party computation for machine learning: a survey, *IEEE Access*, **12** (2024), 53881–53899. https://doi.org/10.1109/ACCESS.2024.3388992
15. Y.-Y. Li, F.-C. Qian, G.-R. Zhang, X.-C. Li, L.-W. Zhou, Z.-M. Yu, et al., FunlncModel: integrating multi-omic features from upstream and downstream regulatory networks into a machine learning framework to identify functional lncRNAs, *Brief. Binioform*., **26** (2025), bbae623. https://doi.org/10.1093/bib/bbae623
16. A. C. Yao, Protocols for secure computations, In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, Chicago, IL, USA, 1982, 160–164. https://doi.org/10.1109/SFCS.1982.38
17. F. Boudot, B. Schoenmakers, J. Traoré, A fair and efficient solution to the socialist millionaires' problem, *Discrete Appl. Math.*, **111** (2001), 23–36. https://doi.org/10.1016/S0166-218X(00)00342-5
18. H.-K. Lo, Insecurity of quantum secure computations, *Phys. Rev. A*, **56** (1997), 1154–1162. https://doi.org/10.1103/PhysRevA.56.1154
19. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev.*, **41** (1999), 303–332. https://doi.org/10.1137/S0036144598347011
20. L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.*, **79** (1997), 325–328. https://doi.org/10.1103/PhysRevLett.79.325
21. Y.-G. Yang, Q.-Y. Wen, An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement, *J. Phys. A: Math. Theor.*, **42** (2009), 055305. https://doi.org/10.1088/1751-8113/42/5/055305
22. B. Liu, D. Xiao, W. Huang, H.-Y. Jia, T.-T. Song, Quantum private comparison employing single-photon interference, *Quantum Inf. Process.*, **16** (2017), 180. https://doi.org/10.1007/s11128-017-1630-y
23. H.-M. Pan, Two-party quantum private comparison using single photons, *Int. J. Theor. Phys.*, **57** (2018), 3389–3395. https://doi.org/10.1007/s10773-018-3852-x
24. J.-W. Zhang, G. Xu, X.-B. Chen, Y. Chang, Z.-C. Dong, Improved multiparty quantum private comparison based on quantum homomorphic encryption, *Physica A*, **610** (2023), 128397. https://doi.org/10.1016/j.physa.2022.128397
25. M. Hou, Y. Wu, New quantum private comparison using Bell states, *Entropy*, **26** (2024), 682. https://doi.org/10.3390/e26080682
26. Y.-F. Lang, Quantum private comparison using single bell state, *Int. J. Theor. Phys.*, **60** (2021), 4030–4036. https://doi.org/10.1007/s10773-021-04937-3

27. X. Huang, S. B. Zhang, Y. Chang, M. Hou, W. Cheng, Efficient quantum private comparison based on entanglement swapping of bell states, *Int. J. Theor. Phys.*, **60** (2021), 3783–3796. https://doi.org/10.1007/s10773-021-04915-9
28. T.-Y. Ye, Z.-X. Ji, Two-party quantum private comparison with five-qubit entangled states, *Int. J. Theor. Phys.*, **56** (2017), 1517–1529. https://doi.org/10.1007/s10773-017-3291-0
29. Q. Sun, Quantum private comparison with six-particle maximally entangled states, *Mod. Phys. Lett. A*, **37** (2022), 2250149. https://doi.org/10.1142/S0217732322501498
30. C. Li, X. Chen, H. Li, Y. Yang, J. Li, Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state, *Quantum Inf. Process.*, **18** (2019), 158. https://doi.org/10.1007/s11128-019-2266-x
31. M. Hou, Y. Wu, Quantum private comparison protocol with cluster states, *Axioms*, **14** (2025), 70. https://doi.org/10.3390/axioms14010070
32. S. Lin, Y. Sun, X.-F. Liu, Z.-Q. Yao, Quantum private comparison protocol with d-dimensional Bell states, *Quantum Inf. Process.*, **12** (2013), 559–568. https://doi.org/10.1007/s11128-012-0395-6
33. F. Z. Guo, F. Gao, S. J. Qin, J. Zhang, Q. Y. Wen, Quantum private comparison protocol based on entanglement swapping of d-level Bell states, *Quantum Inf. Process.*, **12** (2013), 2793–2802. https://doi.org/10.1007/s11128-013-0536-6
34. W. Q. Wu, Y. X. Zhao, Quantum private comparison of size using *d*-level Bell states with a semi-honest third party, *Quantum Inf. Process.*, **20** (2021), 155. https://doi.org/10.1007/s11128-021-03059-3
35. Y.-F. Lang, Quantum private magnitude comparison, *Int. J. Theor. Phys.*, **61** (2022), 100. https://doi.org/10.1007/s10773-022-05043-8
36. M. Hou, Y. Wu, Two-party quantum private comparison protocol for direct secret comparison, *Mathematics*, **13** (2025), 326. https://doi.org/10.3390/math13020326
37. Y.-F. Hu, L.-H. Gong, Q.-W. Zeng, Efficient and robust multi-party semi-quantum private comparison protocols with decoherence-free states over the collective noises channel, *Quantum Inf. Process.*, **24** (2025), 216. https://doi.org/10.1007/s11128-025-04832-4
38. C.-Q. Ye, J. Li, X.-B. Chen, Y. Hou, A feasible semi-quantum private comparison based on entanglement swapping of Bell states, *Physica A*, **625** (2023), 129023. https://doi.org/10.1016/j.physa.2023.129023
39. J.-H. Huang, M.-L. Li, Y.-Y. Liu, L.-G. Qin, L.-H. Gong, Efficient semi-quantum private comparison protocol of size relation based on high dimensional Bell states, *Chinese Phys. B*, in press. https://doi.org/10.1088/1674-1056/ae2abd
40. X. Huang, W. Zhang, X. Wang, S. Zhang, M. K. Khan, QF2PM: quantum-secure fine-grained privacy-preserving profile matching for mobile social networks, *IEEE Trans. Netw. Sci. Eng.*, **13** (2026), 2678–2693. https://doi.org/10.1109/TNSE.2025.3619531
41. E. Campbell, A series of fast-paced advances in quantum error correction, *Nat. Rev. Phys.*, **6** (2024), 160–161. https://doi.org/10.1038/s42254-024-00706-3
42. V. V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, et al., Real-time quantum error correction beyond break-even, *Nature*, **616** (2023), 50–55. https://doi.org/10.1038/s41586-023-05782-6
43. Google Quantum AI and Collaborators, Quantum error correction below the surface code threshold, *Nature*, **638** (2025), 920–926. https://doi.org/10.1038/s41586-024-08449-y

44. X. Huang, W. Zhang, S. Zhang, M. K. Khan, Quantum-secure privacy-preserving profile matching for proximity-based mobile social networks, *IEEE Trans. Consum. Electr.*, in press. https://doi.org/10.1109/TCE.2026.3666093

AIMS Press