Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Quantum Private Intersection Based on Single Qubits

Cai Zhang
South China Agricultural University
Zhuoxuan Zhan
South China Agricultural University
Zhiwei Sun
smeker@szpu.edu.cn

Shenzhen Polytechnic University

Research Article

Keywords: Quantum private set intersection, Semi-honest Participants, Quantum cryptography

Posted Date: July 9th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10073865/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at EPJ Quantum Technology on October 20th, 2026. See the published version at https://doi.org/10.1140/epjqt/s40507-026-00578-9.

Quantum Private Intersection Based on Single Qubits

Cai Zhang[a], Zhuoxuan Zhan[a], Zhiwei Sun (corresponding author)[b,*]

[a] *College of Mathematics and Informatics, South China Agricultural University, Guangzhou, 510642, Guangdong, China*
[b] *Undergraduate School of Artificial Intelligence, Shenzhen Polytechnic University, Shenzhen, 518055, Guangdong, China*

Abstract

Private Set Intersection (PSI) is a crucial Secure Multi-Party Computation (SMPC) primitive which enables participants to securely obtain the intersection of their private sets without revealing their individual set information. The advent of quantum computing threatens classical PSI protocols, driving the development of Quantum PSI (QPSI) alternatives. We propose a two-party QPSI protocol based on a semi-honest third party. This protocol achieves set intersection using only single-qubit unitary operations and single-qubit states. Security analysis shows that our protocol can resist common attacks. Validation experiments conducted on the IBM Qiskit simulator confirm the protocol's correctness and feasibility. Furthermore, we compare the proposed protocol with existing QPSI protocols in terms of quantum states, unitary operations, measurements, and fairness, demonstrating gains in quantum resource efficiency, fairness, and practical feasibility.

Keywords: Quantum private set intersection; Semi-honest Participants; Quantum cryptography

1. Introduction

Secure Multi-Party Computation (SMPC) [1], as a foundational cryptographic framework, enables mutually distrusting parties to collaboratively perform computational functions while only accessing the final result, thereby ensuring the confidentiality of raw data. Its importance lies in providing solutions that balance privacy and utility for sensitive scenarios such as financial

*Corresponding author Email: smeker@szpu.edu.cn

risk control and joint medical research [2]. SMPC can be categorized into multiple branches based on different application scenarios, such as secret sharing [3, 4, 5, 6], private queries [7, 8, 9, 10], and private set union [11]. In this paper, we focus on the private set intersection.

Private Set Intersection (PSI) enables multiple parties to discover common elements in their respective sets without disclosing any additional information. Traditional PSI protocols are mainly based on classical cryptographic tools. To address privacy in a semi-honest setting, Freedman et al. [11] designed a PSI protocol that utilizes homomorphic encryption, ensuring strong confidentiality during computation. For efficient client-server applications, Pinkas et al. [12] combined oblivious transfer with efficient hash functions, significantly improving runtime performance. Hazay and Lindell [13] utilized the oblivious polynomial evaluation to design a protocol for set intersection, which is secure under full simulation-based definitions in the presence of malicious adversaries. However, the security of these classical protocols relies on computational complexity assumptions, such as integer factorization or discrete logarithm problems. Shor's algorithm [22] and Grover's search [23] compromise asymmetric and symmetric cryptosystems, respectively, exposing existing PSI protocols to potential security risks. To address this fundamental challenge, researchers are exploring quantum PSI protocols grounded in the principles of quantum mechanics—such as the no-cloning theorem and measurement collapse—aiming to enhance security against quantum attacks.

Research on Quantum Private Set Intersection (QPSI) remains in its early stages, with its developmental trajectory reflecting an evolution from theoretical construction to practical exploration. The initial protocols were mainly based on quantum oblivious set membership decision protocols [21]. Shi et al. [14] pioneered a two-party QPSI protocol employing N-dimensional quantum states. But Cheng et al. [15] pointed out that this protocol has a fairness issue: the server can manipulate the intersection result obtained by the client. To solve this problem, they introduced a passive third-party to detect the server's dishonest behaviour. Maitra [16] assumed that all the participants are rational to maximize their utilities to guarantee the protocol's fairness and security. However, these protocols universally rely on multi-particle entanglement and complex quantum gates, posing significant technical implementation challenges. To enhance feasibility, Debnath et al. [17] adopted quantum key distribution (QKD) for key generation as a subprocedure to design a QPSI protocol. This protocol requires only single pho-

tons, thereby significantly lowering implementation barriers. However, only one participant can eventually get the result of the final intersection. Liu et al. [18] designed a two-party QPSI leveraging quantum Fourier transforms. Liu et al. [19] found that the protocol [17] has a privacy problem in that the participant can obtain the other party's private information. To solve this problem, they improved the protocol [18] by replacing quantum Fourier transforms with more implementable Hadamard gates and introducing the exclusive XOR operation for randomized privacy encoding, thus enhancing security while maintaining feasibility. Recently, Hou et al. [20] utilized the entanglement properties of Bell states and a QKD protocol to propose a PSI protocol, which is highly feasible under existing quantum technology.

Although existing QPSI protocols can securely compute the intersection of private sets, most of them require high quantum resource consumption and complex quantum operations. Therefore, we propose a secure two-party QPSI protocol with a semi-honest third party. The two participants only need single-qubit unitary operations and single-qubit quantum states to complete the task. This proposed protocol ensures that both participants obtain the final intersection, ensuring fairness while achieving security and privacy. Comparative analysis shows that our protocol achieves superior quantum resource efficiency and enhanced practical feasibility relative to comparable existing similar protocols.

The remainder of the paper is structured as follows: Section 2 discusses the correctness and security requirements of the proposed protocol, as well as relevant prerequisite knowledge; Section 3 provides a detailed description of our protocol; Section 4 verifies and analyzes the correctness of the protocol; Section 5 provides a comprehensive analysis of the protocol's security; Section 6 simulates the protocol using the Qiskit experimental platform; Section 7 compares and analyzes the proposed protocol with existing related protocols; Section 8 concludes this paper.

2. Preliminaries

In this section, we first describe the problem of private set intersection and the requirements of the proposed protocol. We then introduce two unitary operators that will be used in the protocol.

2.1. Problem Description

First, we define the universal set $U = \{0, 1, 2, \ldots, n-1\}$. Participants Alice and Bob hold private sets $A = \{a_0, a_1, \ldots, a_{x-2}, a_{x-1}\}$ of size i and $B = \{b_0, b_1, \ldots, b_{y-2}, b_{y-1}\}$ of size y, respectively, such that $A \subseteq U$ and $B \subseteq U$. The objective is to obtain the intersection $A \cap B$ with the assistance of a semi-honest third party, Charlie. (The semi-honest third party follows the protocol faithfully but may attempt to infer private information from the intermediate results.)

Alice (Bob) creates an n-bit string m_A (m_B) according to the following encoding rules:

$$m_A^j = \begin{cases} 1, & j \in A \\ 0, & j \notin A \end{cases}, \qquad m_B^j = \begin{cases} 1, & j \in B \\ 0, & j \notin B \end{cases}, \tag{1}$$

where j ranges from 0 to $n-1$ and m_A^j (m_B^j) denotes the j-th bit in string m_A (m_B).

Our protocol should satisfy the following requirements:

- **Correctness:** If Alice and Bob honestly provide their private sets A and B, respectively, the protocol correctly yields the intersection $A \cap B$ to both parties.
- **Security:** No external attacker can derive meaningful information about sets A or B from the protocol execution.
- **Privacy:** Except for the intersection of Alice's and Bob's private sets, the semi-honest third party and the dishonest participant cannot obtain any extra information about the honest participant's private set.

2.2. Unitary Operators

In this part, we provide definitions of two unitary operators and their properties used in the proposed protocol.

2.2.1. Unitary Operator U_1

One of the two unitary operators is $U_1 = -iY$, where Y is the the Pauli-Y operator $Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$. The unitary operator U_1 acts on the computational basis $\{|0\rangle, |1\rangle\}$ and the Hadamard basis $\{|+\rangle, |-\rangle\}$ ($|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$) as follows:

$$\begin{aligned} U_1|0\rangle = |1\rangle, \qquad U_1|1\rangle = -|0\rangle, \\ U_1|+\rangle = -|-\rangle, \quad U_1|-\rangle = |+\rangle. \end{aligned} \tag{2}$$

2.2.2. Unitary Operator U_2

The other unitary operator is $U_2 = \frac{1}{\sqrt{2}}(I - iY)$, which acts on the computational basis $\{|0\rangle, |1\rangle\}$ and the Hadamard basis $\{|+\rangle, |-\rangle\}$ as follows:

$$\begin{aligned} U_2|0\rangle = |+\rangle, \quad U_2|1\rangle = -|-\rangle, \\ U_2|+\rangle = |1\rangle, \quad U_2|-\rangle = |0\rangle. \end{aligned} \tag{3}$$

Furthermore, the relationship between U_1 and U_2 can be expressed as $U_2^2 = U_1$, as demonstrated below:

$$\begin{aligned} U_2^2 &= \left(\frac{1}{\sqrt{2}}(I - iY)\right)\left(\frac{1}{\sqrt{2}}(I - iY)\right) \\ &= \frac{1}{2}\left(I - iY - iY + (-iY)^2\right) \\ &= \frac{1}{2}\left(I - 2iY - I\right) \\ &= -iY \\ &= U_1. \end{aligned} \tag{4}$$

U_1 acts as a swapping operation on both the computational basis and the Hadamard basis, thus preserving the basis structure while interchanging the basis states. Applying U_2 twice to a quantum state is equivalent to performing U_1 on this quantum state. We will use these properties of U_1 and U_2 to obtain the intersection of the two participants' private sets.

3. Quantum private set intersection protocol

In this section, the quantum channels are assumed to be ideal (noise-free and lossless), while the classical channels are authenticated in our protocol. The protocol consists of two phases: Charlie first obtains $(A \cap B) \cup (\overline{A \cup B})$ in Phase I, and subsequently derives $A \cap B$ from $(A \cap B) \cup (\overline{A \cup B})$ in Phase II. Note that Charlie and a dishonest participant cannot obtain any additional information about an honest participant's private set in either phase.

3.1. Phase I

The detailed description of Phase I is as follows:

(Step 1) Charlie first prepares a sequence of n single particles and denotes it by $S = (s_0, s_1, \ldots, s_{n-2}, s_{n-1})$, where s_j $(j = 0, 1, \ldots, n-1)$ is randomly selected from the quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. After that, Charlie randomly prepares d decoy particles, each of which is randomly selected from the quantum states $\{|+\rangle, |-\rangle, |+y\rangle, |-y\rangle\}$ ($|+y\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $|-y\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$)(all subsequent decoy particles follow this selection). Charlie then randomly inserts these d particles into the sequence S to form a new sequence S', and records their insertion positions and corresponding basis states. Eventually, Charlie transmits S' to Alice.

(Step 2) After receiving the sequence S', Alice performs eavesdropping detection with Charlie. First, Charlie informs Alice via the classical channel of the insertion positions of all the decoy particles and their corresponding measurement bases. Alice then measures each decoy particle in the corresponding basis and announces the measurement result to Charlie. Finally, Charlie compares the measurement results with the initial states and calculates the error rate. If the error rate exceeds the eavesdropping threshold, Alice discards S' and returns to Step 1 to restart. Otherwise, Alice discards all the decoy particles in S' to obtain S and proceeds to the next step.

(Step 3) After Alice confirms that she has passed the eavesdropping detection, she performs appropriate unitary operators on S based on her bit string m_A: if $m_A^j = 0$ $(j = 0, 1, \ldots, n-1)$, she performs no operation on particle s_j; if $m_A^j = 1$, Alice applies the operator U_1 to particle s_j. Alice's operations transform the sequence $S = (s_0, s_1, \ldots, s_{n-1})$ into $S^A = (s_0^A, s_1^A, \ldots, s_{n-1}^A)$. Subsequently, Alice randomly chooses a permutation ψ_1 of $\{0, 1, 2, \ldots, n-1\}$ and changes $S^A = (s_0^A, s_1^A, \ldots, s_{n-1}^A)$ to $S_{\psi_1}^A = (s_{\psi_1(0)}^A, s_{\psi_1(1)}^A, \ldots, s_{\psi_1(n-1)}^A)$. After completing all operations, Alice randomly inserts d decoy particles into $S_{\psi_1}^A$ to form a new sequence $S_{\psi_1}^{A\prime}$. After recording the insertion positions of all the decoy particles and the corresponding bases, Alice sends $S_{\psi_1}^{A\prime}$ to Bob.

(Step 4) After receiving the sequence $S_{\psi_1}^{A\prime}$, Bob performs eavesdropping detection with Alice in the same manner as Step 2. If the error rate exceeds the eavesdropping threshold, Bob discards $S_{\psi_1}^{A\prime}$ and returns

to Step 1 to restart. Otherwise, Bob discards all the decoy particles in $S_{\psi_1}^{A\prime}$ to obtain $S_{\psi_1}^{A}$ and proceeds to the next step.

(Step 5) In this step, Alice first tells Bob the permutation ψ_1 based on which Bob can then recover the sequence S^A from $S_{\psi_1}^{A}$. Subsequently, Bob applies appropriate unitary operators to S^A according to his bit string m_B: If $m_B^j = 0$ $(j = 0, 1, \ldots, n-1)$, no operation is performed on particle s_j; if $m_B^j = 1$, Bob applies the operator U_1 to particle s_j. Bob's operations turn the sequence $S^A = (s_0^A, s_1^A, \ldots, s_{n-1}^A)$ into $S^{AB} = (s_0^{AB}, s_1^{AB}, \ldots, s_{n-1}^{AB})$. Subsequently, Bob randomly chooses a permutation ψ_2 of $\{0, 1, \ldots, n-1\}$ and changes $S^{AB} = (s_0^{AB}, s_1^{AB}, \ldots, s_{n-1}^{AB})$ to $S_{\psi_2}^{AB} = (s_{\psi_2(0)}^{AB}, s_{\psi_2(1)}^{AB}, \ldots, s_{\psi_2(n-1)}^{AB})$. After completing all operations, Bob randomly inserts d decoy particles into $S_{\psi_2}^{AB}$ to form a new sequence $S_{\psi_2}^{AB\prime}$. After recording the insertion positions of all the decoy particles and the corresponding bases, Bob sends $S_{\psi_2}^{AB\prime}$ to Charlie.

(Step 6) After receiving the sequence $S_{\psi_2}^{AB\prime}$, Charlie performs eavesdropping detection with Bob, similar to that in Step 2. If the error rate exceeds the eavesdropping threshold, Charlie discards $S^{AB\prime}$ and returns to Step 1 to restart. Otherwise, Charlie removes all the decoy particles from $S_{\psi_2}^{AB\prime}$ to obtain $S_{\psi_2}^{AB}$ and continues to the next step.

(Step 7) After passing the eavesdropping detection, Bob communicates the permutation ψ_2 to Bob, who can then recover the sequence S^{AB} from $S_{\psi_2}^{AB}$. After that, Charlie measures all the particles in the same bases as those used in the initial preparation. And he will obtain the measurement results $l = (l_0, l_1, \ldots, l_{n-1})$. Then he compares the measurement result l_j $(j = 0, 1, \ldots, n-1)$ with the original state of particle s_j. If the measurement result l_j contradicts the original state, it indicates that $j \in (A \cap \bar{B}) \cup (\bar{A} \cap B)$; otherwise, $j \in (A \cap B) \cup \overline{(A \cup B)}$. Finally, Charlie records a set $R = \{r_0, r_1, \ldots, r_{p-1}\}$, where $r_j \in (A \cap B) \cup \overline{(A \cup B)}$ for $j = 0, 1, \ldots, p-1$.

3.2. Phase II

The detailed description of Phase II is as follows:

(Step 1) After completing Phase I, Charlie possesses a sequence of single particles of size n that have been measured and denotes them by $Q = (q_0, q_1, \ldots, q_{n-1})$. Charlie prepares d decoy particles, each randomly chosen from the quantum states $\{|+\rangle, |-\rangle, |+y\rangle, |-y\rangle\}$ (all

subsequent decoy particles follow this selection). He then randomly inserts them into Q to form a new sequence Q' and records their insertion positions and corresponding bases. Charlie then sends Q' to Alice.

(Step 2) After receiving the sequence Q', Alice performs eavesdropping detection with Charlie, following the same steps as in Phase I. If the eavesdropping detection fails, Alice discards all the particles and returns to the first phase. Otherwise, Alice discards all the decoy particles in Q' to obtain Q and proceeds to the next step.

(Step 3) Alice performs appropriate unitary operations on the sequence Q according to her bit string m_A^j: if $m_A^j = 0$ ($j = 0, 1, \ldots, n-1$), she performs no operation on particle q_j; otherwise, Alice performs U_2 on particle q_j. The sequence $Q = (q_0, q_1, \ldots, q_{n-1})$ is transformed into $Q^A = (q_0^A, q_1^A, \ldots, q_{n-1}^A)$ under Alice's operations. Subsequently, Alice randomly chooses a permutation ψ_3 of $\{0, 1, 2, \ldots, n-1\}$ to map Q^A to $Q_{\psi_3}^A = (q_{\psi_3(0)}^A, q_{\psi_3(1)}^A, \ldots, q_{\psi_3(n-2)}^A, q_{\psi_3(n-1)}^A)$. After that, Alice randomly inserts d decoy particles into $Q_{\psi_3}^A$ to form a new sequence $Q_{\psi_3}^{A\prime}$, and records their insertion positions and corresponding bases. Then she sends $Q_{\psi_3}^{A\prime}$ to Bob.

(Step 4) After receiving the sequence $Q_{\psi_3}^{A\prime}$, Bob performs an eavesdropping detection with Alice in the same manner as Step 2. If the eavesdropping exists, Bob discards all the particles and returns to Step 1 of Phase I to restart. Otherwise, Bob discards all the decoy particles in $Q_{\psi_3}^{A\prime}$ to obtain $Q_{\psi_3}^A$ and proceeds to the subsequent steps.

(Step 5) Bob receives the permutation ψ_3 from Alice, which he uses to recover the sequence Q^A from $Q_{\psi_3}^A$. He then applies appropriate unitary operations to Q^A in accordance with his bit string m_B: If $m_B^j = 0$ ($j = 0, 1, \ldots, n-1$), no operation is performed on particle q_j; otherwise, Bob applies U_2 to particle q_j. Under Bob's operations, the sequence $Q^A = (q_0^A, q_1^A, \ldots, q_{n-1}^A)$ is turned into $Q^{AB} = (q_0^{AB}, q_1^{AB}, \ldots, q_{n-1}^{AB})$. Subsequently, Bob randomly chooses a permutation ψ_4 of $\{0, 1, 2, \ldots, n-1\}$ to convert $Q^{AB} = (q_0^{AB}, q_1^{AB}, \ldots, q_{n-1}^{AB})$ into $Q_{\psi_4}^{AB} = (q_{\psi_4(0)}^{AB}, q_{\psi_4(1)}^{AB}, \ldots, q_{\psi_4(n-1)}^{AB})$. After completing all operations, Bob randomly inserts d decoy particles into $Q_{\psi_4}^{AB}$ to form a new sequence $Q_{\psi_4}^{AB\prime}$ and records their insertion positions and corresponding bases. Finally, Bob transmits $Q_{\psi_4}^{AB\prime}$ to Charlie.

(Step 6) After confirming receipt of the sequence $Q_{\psi_4}^{AB\prime}$, Charlie performs

the same eavesdropping detection as above. If eavesdropping is detected, Charlie discards all the particles and returns to Step 1 of Phase I; otherwise, Charlie removes all the decoy particles from $Q_{\psi_4}^{AB\prime}$ to obtain $Q_{\psi_4}^{AB}$ and proceeds to the next step.

(Step 7) Charlie receives the permutation ψ_4 from Bob and recovers the sequence Q^{AB} from $Q_{\psi_4}^{AB}$. He then performs measurements on particle $q_{r_j}^{AB}$ $(j = 0, 1, \ldots, p-1)$ in the same basis as that of q_{r_j} according to $R = \{r_0, r_1, \ldots, r_{p-1}\}$. Charlie will obtain the measurement results $l' = (l'_{r_0}, l'_{r_1}, \ldots, l'_{r_{p-1}})$. Subsequently, he compares the measurement result l'_{r_j} $(j = 0, 1, \ldots, p-1)$ with the state of particle q_{r_j}. If l'_{r_j} differs from the state of particle q_{r_j}, $r_j \in A \cap B$; otherwise, $r_j \in \overline{A \cup B}$. Finally, Charlie obtains the intersection of A and B that can be simultaneously sent to Alice and Bob.

4. Correctness Analysis of the Proposed Protocol

In this section, we show that if Alice and Bob honestly submit their respective private sets, Charlie will eventually obtain the correct intersection of their private sets.

4.1. Phase I

We show first that at the end of Phase I, Charlie will correctly obtain $(A \cap B) \cup \overline{(A \cup B)}$.

In this phase, Alice and Bob will each perform U_1 or I on the j-th particle $(j = 0, 1, \ldots, n-1)$ according to their respective private set information m_A^j and m_B^j. For the j-th particle, four possible operators can be performed on it, as shown in Table 1.

Table 1: Operators on the j-th particle under different conditions for j in Phase I

	$j \notin A$	$j \in A$
$j \notin B$	$I \cdot I$	$I \cdot U_1$
$j \in B$	$U_1 \cdot I$	$U_1 \cdot U_1$

For the cases where $j \in A$, $j \notin B$ or $j \notin A$, $j \in B$, the j-th particle undergoes the operator U_1 exactly once, causing its state to flip in the same basis. When Charlie measures the j-th particle in the same basis as that used in the initial preparation, the measurement result differs from the corresponding initial prepared state.

For the case where $j \notin A$, $j \notin B$, the j-th particle undergoes no operation and its state remains unchanged. When Charlie measures the j-th particle in the same basis as that used in the initial preparation, the measurement result and the corresponding initial prepared state are the same.

For the case where $j \in A$, $j \in B$, the j-th particle undergoes the U_1 operator twice, potentially introducing a global phase that is irrelevant to the measurement result. When Charlie measures this particle in the same basis as that used in the initial preparation, the measurement result is identical to the corresponding initial prepared state.

From the above analysis, Charlie can correctly determine $(A \cap B) \cup \overline{(A \cup B)}$ based on all the measurement results.

4.2. Phase II

In this subsection, we show that at the end of Phase II, Charlie will correctly obtain the intersection $A \cap B$.

In this phase, Alice and Bob each perform the operator U_2 or I on particle q_j $(j = 0, 1, \ldots, n-1)$, the j-th particle measured by Charlie at the end of Phase I, according to their respective private set information m_A^j and m_B^j. For the particle q_j, there are four possible operators that can be applied, as shown in Table 2.

Table 2: Operations on q_j under different conditions for j in Phase II

	$j \notin A$	$j \in A$
$j \notin B$	$I \cdot I$	$I \cdot U_2$
$j \in B$	$U_2 \cdot I$	$U_2 \cdot U_2$

Note that at the end of Phase I, Charlie has already obtained the set $R = \{r_0, r_1, \ldots, r_{p-1}\}$, where $r_j \in (A \cap B) \cup \overline{(A \cup B)}$ for $j = 0, 1, \ldots, p-1$. At the end of Phase II, Charlie only measures particle $q_{r_j}^{AB}$ $(j = 0, 1, \ldots, p-1)$ in the same basis as that of q_{r_j}. This implies that particle q_{r_j} undergoes either I or U_2 twice. Therefore, we only consider these two cases in detail.

For the case where $r_j \notin A$, $r_j \notin B$, particle q_{r_j} undergoes the operator I. At the end of Phase II, when Charlie measures particle $q_{r_j}^{AB}$ in the same basis as that of q_{r_j}, the measurement result is identical to the state of q_{r_j}.

For the case where $r_j \in A$, $r_j \in B$, particle q_{r_j} undergoes the operator U_2 twice, which is equivalent to undergoing the operator U_1 exactly once, accoding to Equation (4). Clearly, the operator U_1 flips the state of particle

q_{r_j} in the same basis. Therefore, when Charlie measures $q_{r_j}^{AB}$ in the same basis as that of q_{r_j}, the measurement result is different from the state of q_{r_j}.

The above analysis shows that Charlie can correctly obtain $A \cap B$ by removing the elements in $\overline{A \cup B}$ from $(A \cap B) \cup \overline{(A \cup B)}$ based on his measurement results.

5. Security Analysis of the Proposed Protocol

In this section, we demonstrate that our protocol is secure against attacks from external eavesdroppers and internal participants.

5.1. External Attacks

An external attack refers to a scenario in which an external attacker, Eve, employs various strategies on the particles transmitted between participants, aiming to obtain useful information about Alice's and Bob's private sets. This protocol uses decoy states to detect eavesdropping and can withstand common attacks, such as the intercept-resend attack and the entanglement-measurement attack [27]. It also employs various optical devices to defend against Trojan-Horse attacks [28, 29].

5.1.1. Intercept-Resend Attack

For an external attacker, Eve, the typical attack involves intercepting particles transmitted through the quantum channel. Suppose Eve intends to steal Alice's private input. The case where Eve attempts to obtain Bob's private input can be similarly analyzed. She may intercept the particles transmitted from Charlie to Alice and identify the encoding particles (i.e., those on which Alice will apply appropriate unitary operations selected according to her private bit string m_A). She then measures these particles in the right bases (the X basis or the Z basis) to determine the initial states of these particles. Subsequently, she prepares a sequence of particles matching the measurement results and sends all the particles to Alice. After these particles have been performed by Alice and sent to Bob, she can capture them again and measures them to infer the operators chosen by Alice. Finally, Eve can acquire m_A from these operators, thereby recovering Alice's private set A, as A is encoded in m_A. However, Eve cannot discriminate between the encoding particles and the decoy particles because their states are identical: Every particle is in the state $\frac{1}{4}(|0\rangle\langle 0 + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|) = \frac{1}{4}(|+\rangle\langle +| + |-\rangle\langle -| + |+y\rangle\langle +y| + |-y\rangle\langle -y| = \frac{I}{2}$. To gain information from

the encoding particles, Eve may measure these particles randomly in the X basis or in the Z basis. But she may measure the decoy particles, which introduces errors that can be detected by Charlie and Alice. For a decoy particle that has been measured by Eve, the probability of detecting such an attack is $\frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{8}$. If d decoy particles have been measured, the probability of detecting such an attack becomes $1 - (1 - \frac{3}{8})^d = 1 - (\frac{5}{8})^d$, which approaches 1 as d grows sufficiently large. Therefore, our protocol is secure against the intercept-resend attack.

5.1.2. Entanglement-Measurement Attack

In quantum cryptographic protocols, entanglement-measurement attacks represent a more covert eavesdropping method: the eavesdropper Eve entangles her auxiliary particles with the transmitted particles and later measures the auxiliary particles to gain information. Suppose Eve generates a set of auxiliary particles $\mathrm{P} = \{|\mathrm{P}_0\rangle, |\mathrm{P}_1\rangle, |\mathrm{P}_1\rangle, \ldots, |\mathrm{P}_{n-1}\rangle\}$, and entangles these auxiliary particles with the intercepted particles through some unitary operations. The unitary operation can be, in general, expressed as:

$$U|+\rangle|P_i\rangle = \alpha|+\rangle|p_{00}\rangle + \beta|-\rangle|p_{01}\rangle, \tag{5}$$

$$U|-\rangle|P_i\rangle = \gamma|+\rangle|p_{10}\rangle + \delta|-\rangle|p_{11}\rangle, \tag{6}$$

$$\begin{aligned} U|+y\rangle|P_i\rangle = {} & \frac{1}{2}|+y\rangle(\alpha|p_{00}\rangle + i\beta|p_{01}\rangle - i\gamma|p_{10}\rangle + \delta|p_{11}\rangle) \\ & + \frac{1}{2}|-y\rangle(i\alpha|p_{00}\rangle + \beta|p_{01}\rangle + \gamma|p_{10}\rangle - i\delta|p_{11}\rangle), \end{aligned} \tag{7}$$

$$\begin{aligned} U|-y\rangle|P_i\rangle = {} & \frac{1}{2}|-y\rangle(\alpha|p_{00}\rangle - i\beta|p_{01}\rangle + i\gamma|p_{10}\rangle + \delta|p_{11}\rangle) \\ & + \frac{1}{2}|+y\rangle(-i\alpha|p_{00}\rangle + \beta|p_{01}\rangle + \gamma|p_{10}\rangle + i\delta|p_{11}\rangle), \end{aligned} \tag{8}$$

where $|\alpha|^2 + |\beta|^2 = 1$, $|\gamma|^2 + |\delta|^2 = 1$, and $|p_{00}\rangle$, $|p_{01}\rangle$, $|p_{10}\rangle$, and $|p_{11}\rangle$ are the states determined by $|P_i\rangle$.

In this protocol, eavesdropping detection is performed after each particle transmission. If a decoy particle is in the $\{|+\rangle, |-\rangle\}$ basis, the condition

$$\beta = \gamma = 0 \tag{9}$$

should hold for Eve to pass detection according to Equations (5) and (6);

otherwise, Eve should set

$$i\alpha|\mathrm{p}_{00}\rangle + \beta|\mathrm{p}_{01}\rangle + \gamma|\mathrm{p}_{10}\rangle - i\delta|\mathrm{p}_{11}\rangle = \vec{0}, \tag{10}$$

$$-i\alpha|p_{00}\rangle + \beta|p_{01}\rangle + \gamma|p_{10}\rangle + i\delta|p_{11}\rangle = \vec{0}, \tag{11}$$

based on Equations (7) and (8). Equations (9-11) yield $\alpha|\mathrm{p}_{00}\rangle = \delta|\mathrm{p}_{11}\rangle$. Combined with Equation (9), we can obtain

$$U|+\rangle|P_i\rangle = \alpha|+\rangle|p_{00}\rangle, \tag{12}$$

$$U|-\rangle|P_i\rangle = \delta|-\rangle|p_{11}\rangle, \tag{13}$$

$$U|+y\rangle|P_i\rangle = \alpha|+y\rangle|p_{00}\rangle, \tag{14}$$

$$U|-y\rangle|P_i\rangle = \alpha|-y\rangle|p_{00}\rangle, \tag{15}$$

which indicates that the auxiliary particle and the original transmitted particle are untangled if Eve intends to escape the eavesdropping detection. Therefore, Eve cannot obtain any useful information about the private sets of the two participants from measurements performed on her auxiliary particles.

5.1.3. Trojan-Horse Attacks

During the execution of quantum cartographical protocols in which particles are relayed, the Trojan horse attacks, such as delayed photon attacks and invisible photon eavesdropping, can be launched [28, 29]. We must also account for such security vulnerabilities in our protocol. To effectively address this issue, we can introduce wavelength quantum filters to filter out invisible photons and employ optical components such as photon splitters and photon number splitters to separate legitimate photons from delayed photons. Based on these technical measures, Trojan horse attacks can be effectively detected.

5.2. Participants' Attack

Compared to the external attackers, a dishonest participant typically has greater capability to gain information because she/he has direct access to the transmitted particles and can legitimately obtain the intermediate results. Based on the particles in her/his possession and these intermediate results, the dishonest participant attempts to infer the private set of the honest participant. We will analyze in detail the attacks mounted by Charlie, Alice, and Bob, respectively.

5.2.1. Charlie's Attack

During Phase I of the protocol, after Charlie prepares the sequence of the initial encoding particles and sends it to Alice, Alice performs the corresponding operations on the encoding particles based on her private set and then forwards the sequence to Bob. If Charlie intercepts the encoding particles from Alice to Bob, he can attempt to steal Alice's private set by directly measuring the particles, as he knows the initial preparation bases. Although the eavesdropping detection can identify such actions, Charlie may have already obtained part of m_A by comparing his measurement results in the correct bases with the corresponding initial states. Charlie can then recover part of the private set of Alice according to the encoding rules. To defend against this attack, Alice randomly chooses a permutation ψ_1 of $\{0, 1, \ldots, n-1\}$ to reorder the encoding particle sequence before sending it to Bob. Alice sends the permutation ψ_1 to Bob only when she has confirmed that nobody disturbs the transmission. This method ensures that even if Charlie successfully intercepts the encoding particle sequence, he cannot extract useful information because he lacks the mapping between the original encoding particle order and the measurement results. Similarly, Charlie cannot obtain Alice's private set due to his not knowing of the permutation ψ_3 used in Phase II. The case in which Charlie desires to acquire Bob's private set can be analyzed analogously.

Note that in the final step of Phase I, after Alice and Bob complete their respective operations on the encoding particle sequence and send it back to Charlie, Charlie will measure the received particles in the right bases. For the j-th s_j ($j \in \{0, 1, \ldots, n-1\}$), where $j \in A$, $j \notin B$ or $j \notin A$, $j \in B$, the j-th particle undergoes the operator U_1 exactly once, which flips its state to the opposite of the initial preparation. As a result, when Charlie measures it, he cannot determine which participant performed the U_1 operation from his measurement result and its corresponding initial state. Namely, Charlie knows the elements are in either Alice's set or Bob's set, but according to the encoding rules, he cannot determine whether they are exactly from Alice's set or from Bob's set. Thus, neither Alice's nor Bob's private information can be extracted by such measurements. An analogous analysis applies to the privacy of Alice's and Bob's sets in the final step of Phase II.

5.2.2. Alice's Attack

In the proposed protocol, the encoding particles received by Bob are forwarded by Alice. This means that Alice knows the operations the encoding

particles underwent before Bob performs the unitary operations. To acquire Bob's private m_B, Alice may intercept and measure the encoding particles sent to Charlie in the right bases after Bob's operations. However, this is impossible as Alice does not know the initial preparation bases of the encoding particles. Therefore, she may measure the particles in the wrong bases and cannot determine which elements belong to Bob's private set based on the measurement results. In addition, this attack can be detected in the eavesdropping detection.

As Alice is a legitimate participant who sends the encoding particles to Bob, she may even prepare fake particles in her preferred bases. Subsequently, Alice sends these fake particles instead of the encoding particles to Bob. After Bob manipulates the fake sequence in accordance with his private m_B and sends it to Charlie, Alice can intercept it and perform measurements on the fake particles in their initially prepared bases. Finally, Alice deduces what operators have been performed on the fake particles by Bob from her measurement results and the corresponding initial bases. Although the decoy-state techniques can detect such an eavesdropping, by the time of interception, Alice has already obtained some information about Bob's private set. To defend against this attack, Bob randomly chooses the permutations ψ_2 in Phase I to reorder the encoding particles. Therefore, the fake particles on which Bob performed unitary operators are also reordered before they are sent to Charlie. It should be noted that Bob sends the permutation ψ_2 to Charlie only upon confirming the absence of eavesdropping. Thus, Alice cannot determine which elements belong to Bob's private set based on her measurement results without the permutation ψ_2. Similarly, Alice fails to acquire Bob's private set in Phase II as she lacks the permutation ψ_4.

5.2.3. Bob's Attack

In this protocol, Bob receives two sequences of the encoding particles sent by Alice in Phase I and Phase II, respectively, each carrying information related to Alice's private set. Therefore, Bob can attempt to measure the particles in an effort to extract information from the measurement results. However, since Bob lacks knowledge of the bases Charlie used in the initial particle preparation, he may measure the particles in the wrong bases and cannot determine which elements belong to Alice's private set relying on the measurement results. This attack also disturbs the states of the decoy particles which leads to the detectable errors in the eavesdropping detection.

6. Simulation

To validate the correctness of the protocol, we conducted a small-scale experimental example and verified whether the intermediate and final results align with theoretical expectations.

To validate the protocol, we performed a small-scale experimental demonstration on IBM Qiskit simulator and confirmed that the intermediate and final results are consistent with theoretical expectations.

In the experiment, Charlie initially prepares quantum states in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis. When the quantum state is measured in the correct basis, the measurement probabilities are shown in Figures 1 (a) and (b). Conversely, when an incorrect basis is used, the probabilities are also shown in Figures 1 (c) and (d). These probabilities indicate that without knowledge of the preparation bases of the encoding particles, the measurement outcomes appear random. Therefore, neither the eavesdropper nor the participants (Alice and Bob) can extract information from the measurement results.

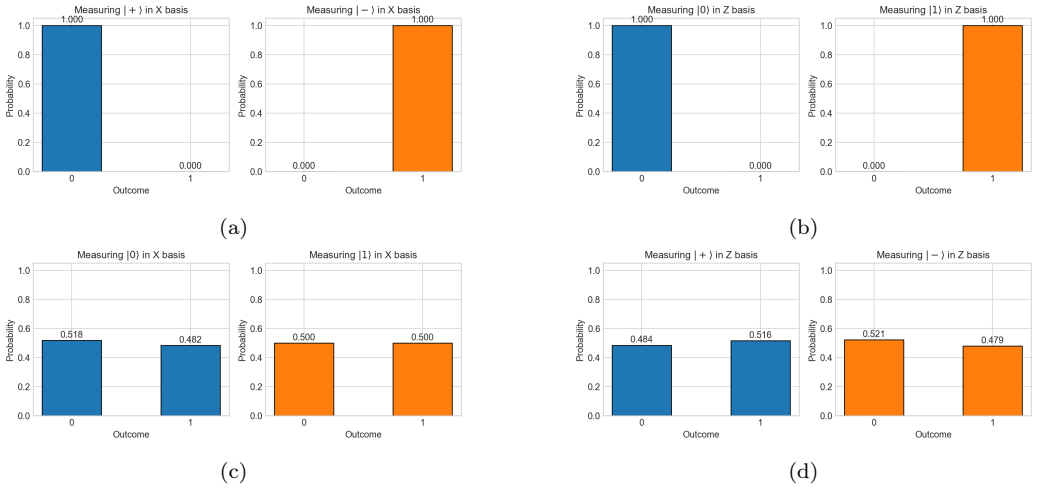


Figure 1: Probabilities of measurement results with respect to the $\{|0\rangle, |1\rangle\}$ basis and the $\{|+\rangle, |-\rangle\}$ basis

In the protocol, Alice and Bob perform quantum operations on the quantum state based on their respective bit strings m_A and m_B. In Phase I, Alice (Bob) executes the unitary operator U_1 on the j-th ($j = 0, 1, \ldots, n-1$) particle if $m_A^j = 1$ ($m_B^j = 1$); otherwise, Alice (Bob) performs no operation on it. Similarly, the U_2 can be performed on the encoding particles

according to m_A and m_B in Phase II. U_1 and U_2 can be implemented as $U_1 = -iY = R_Y(\pi)$ and $U_2 = (I - iY) = R_Y(\frac{\pi}{2})$ on IBM Qiskit simulator, where $R_Y(\theta) = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Y$ is a rotation operator about the $\hat{y}$ axis.

We validate the proposed protocol with an example. We will present the results for each step of the protocol and determine whether the final result is correct. If the experimental result matches the theoretical intersection exactly, this indicates that the protocol correctly computed the intersection of the participants' private sets, thereby confirming the validity of the protocol's execution. In this experiment, the universal set is defined as $\{0, 1, 2, 3, 4, 5, 6, 7\}$, with Alice's private set being $\{1, 3, 5, 7\}$ and Bob's private set as $\{2, 3, 4, 7\}$. The theoretical intersection of the two sets is $\{3, 7\}$. For simplicity, we omit the eavesdropping detection and the particle reorder operations.

The quantum circuits for Phase I and Phase II are shown in Figures 2 and 3, respectively. Figure 2 depicts the quantum circuit for the Phase I, which consists of three parts: Charlie initially prepares the encoding particles $(|0\rangle, |-\rangle, |1\rangle, |0\rangle, |+\rangle, |+\rangle, |-\rangle, |1\rangle)$; Alice and Bob each apply the U_1 operation to the particles according to their respective private sets; and finally, Charlie measures the particles in the corresponding initial preparation bases.

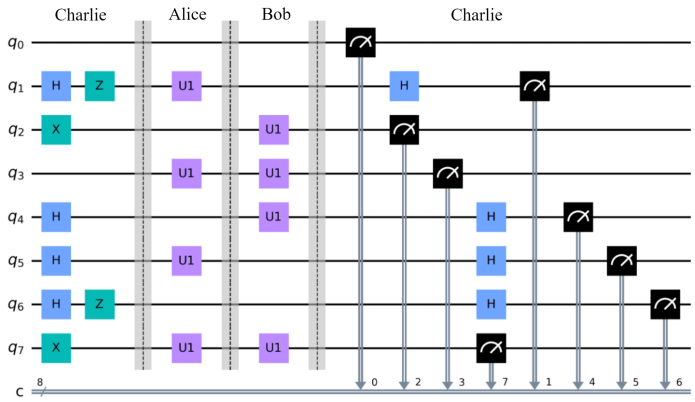


Figure 2: Quantum circuit for Phase I

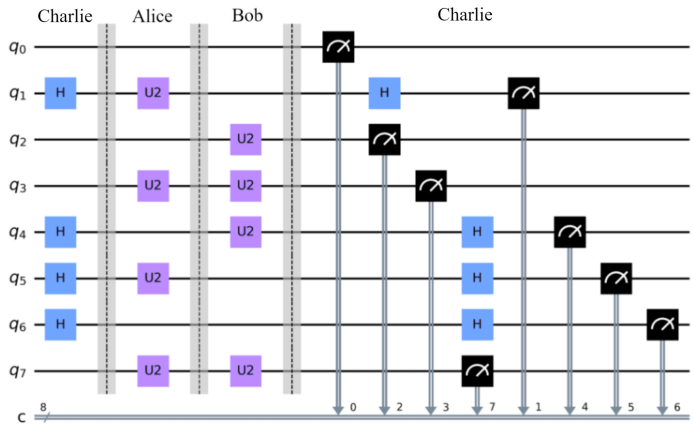


Figure 3: Quantum circuit for Phase II

The quantum circuit for Phase II is shown in Figure 3. Note that Charlie sends the measured encoding particles in Phase I to Alice, who applies the U_2 operations on them based on her private set and then forwards these particles to Bob. Then Bob applies the U_2 operations according to his private set and returns all the particles to Charlie. Finally, Charlie measures the particles based on the results he obtained in Phase I and gets the intersection result.

Let us now move on to the details of Phase I. Firstly, Charlie sends the particle sequence $(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7)$ with the corresponding states $(|0\rangle, |-\rangle, |1\rangle, |0\rangle, |+\rangle, |+\rangle, |-\rangle, |1\rangle)$ to Alice. We assume that $|0\rangle$ and $|+\rangle$ represent 0, while $|1\rangle$ and $|-\rangle$ represent 1. Based on this, Charlie's initial sequence is encoded as $(0, 1, 1, 0, 0, 0, 1, 1)$. According to her private set $\{1, 3, 5, 7\}$, Alice applies the U_1 to particles q_1, q_3, q_5 and q_7 and then sends all the particles to Bob. After receiving the particles, Bob performs U_1 on particles q_2, q_3, q_4 and q_7 based on his private set $\{2, 3, 4, 7\}$ and then sends them to Charlie. At the last step of Phase I, Charlie measures the particles sent by Bob in the corresponding preparation bases and records the measurement results $(0, 0, 0, 0, 1, 1, 1, 1)$, as shown in Figure 5. Comparing the measurement results $(0, 0, 0, 0, 1, 1, 1, 1)$ with the initial sequence $(0, 1, 1, 0, 0, 0, 1, 1)$, we see that particles q_1, q_2, q_4, and q_5 are flipped, so the elements $\{1, 2, 4, 5\}$ are in set A or set B and the elements $\{0, 3, 6, 7\}$ are in $R = (A \cap B) \cup (\overline{A \cup B})$.

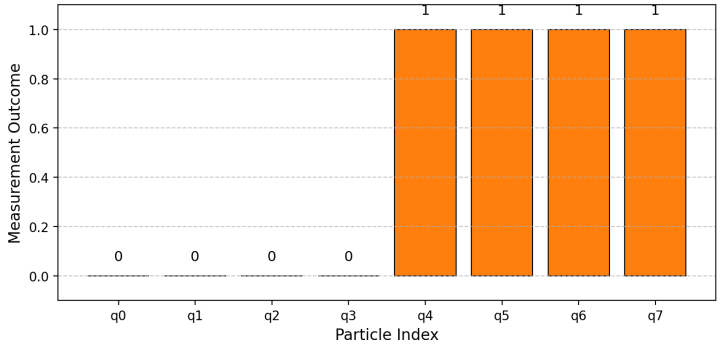


Figure 4: Measurement results in Phase I

Subsequently, we simulate Phase II of the protocol. After Phase I, the states of the particles $(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7)$ become $(|0\rangle, |+\rangle, |0\rangle, |0\rangle, |-\rangle, |-\rangle, |-\rangle, |1\rangle)$. Charlie sends these particles to Alice. Then Alice performs U_2 to particles q_1, q_3, q_5, and q_7 and sends all the particles to Bob. After receiving the sequence of particles, Bob performs U_2 on particles q_2, q_3, q_4, and q_7 and sends all the particles to Charlie. In contrast to Phase I, Charlie only measures particles q_0, q_3, q_6, and q_7 according to $R = \{0, 3, 6, 7\}$ and records the respective measurement results 0, 1, 0, and 1, as shown in Figure 6. Combined with the respective measurement results 0, 0, 1, and 1 of particles q_0, q_3, q_6, and q_7 at the end of Phase I, we observe that particles q_3 and q_7 are flipped. This implies that the elements {3,7} are in $(A \cap B)$. The agreement between the experimental simulation and theoretical analysis validates the protocol's correctness.

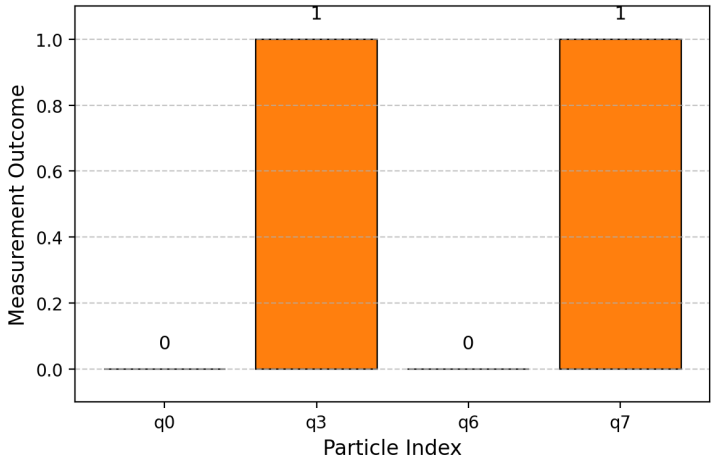


Figure 5: Measurement results in Phase II

7. Comparison

This section compares the proposed protocol with existing similar protocols in terms of quantum states, quantum operations, quantum measurements, and fairness, as summarized in Table 3. For all protocols under comparison, we adopt the following conventions: the universal set contains n elements, and each eavesdropping detection incurs a cost of d decoy particles whenever such detection is employed. The proposed protocol requires $n+6d$ particles to obtain the intersection of two private sets. Only single qubits and single unitary operators are required in our protocol.

The protocol in Ref. [14] requires the client to prepare n encoded states $|\psi_i\rangle = \frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ $(i = 1, 2, \ldots, n)$ and does not require decoy particles. However, the approach proposed in this paper raises a fairness concern which is that the server can manipulate the intersection result obtained by the client [15]. The protocol requires the preparation of high-dimensional quantum states and the implementation of high-dimensional unitary operators (i.e., U_0 and U_S defined as Equations (16) and (17), respectively), rendering it more complex than ours.

$$U_0|x\rangle = \begin{cases} |x\rangle, & x \neq 0, \\ -|0\rangle, & x = 0, \end{cases} \tag{16}$$

$$U_S|x\rangle = \begin{cases} -|x\rangle, & x \in S, \\ |x\rangle, & x \notin S, \end{cases} \tag{17}$$

The protocol in Ref. [17] involves only two parties: the client and the server. The client shares an n-bits asymmetric key with the server through QKD [30] in which the Z-basis measurement and the θ-basis ($\{cos\theta|0\rangle + sin\theta|1\rangle, sin\theta|0\rangle - cos\theta|1\rangle\}$) measurement are required. The two parties compute the intersection using XOR operations. Although the protocol requires only $n + d$ single particles, it also has a fairness issue in that only one party can obtain the final result.

The protocol in Ref. [18] requires a semi-honest third party, Calvin, to prepare n particles and send them to Alice. It involves three rounds of quantum communication, with each round requiring n decoy particles. The total particle consumption is $n + 3d$. Compared to our protocol, it consumes fewer particles but has higher operational complexity due to the requirements of preparing single high-dimensional quantum states and single high-dimensional OAM basis measurements.

The protocol in Ref. [20] utilizes the entanglement properties of Bell states. The protocol generates a $2n$-bit secret key K_{AB} through QKD [31] that consumes about $4n + d$ particles. Additionally, n Bell states are required to obtain the intersection and $4d$ decoy particles are used for eavesdropping detection. Totally, this protocol requires $6n + 5d$ particles, which exceeds the consumption of our protocol. The operators X, Z, and $R_y(\theta) = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Y$ are required in this protocol.

Table 3: Comparison of our protocol with related protocols

Protocols	Quantum States	Quantum Operations	Quantum Measurements	Fairness
Protocol in Ref. [14]	n encoded states $\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	U_0 and U_S	Von Neumann Measurement	No
Protocol in Ref. [17]	$(n+d)$ single particles	——	Z-basis and θ-basis measurements	No
Protocol in Ref. [18]	$(n+3d)$ single particles	Quantum Fourier Transform	OAM basis Measurement	Yes
Protocol in Ref. [20]	$(6n+5d)$ particles (including Bell states)	X, Z and $R_y(\theta)$	Bell-basis State Measurement	Yes
Protocol in Ref. [24]	$(2n+3d)$ single particles	X and $CNOT$	Z-basis Measurement	Yes
Protocol in Ref. [25]	$(4nm+\lambda n+5d)$ single particles	$R_y(\theta)$	Z-basis and X-basis Measurements	Yes
Protocol in Ref. [26]	$(n+d)$ particles	$E_{x'}^d$ and $S_{y'}^d$	High-dimensional Measurement	Yes
Our protocol	$(n+6d)$ single particles	U_1 and U_2(see Section 2)	X-basis, Y-basis, and Z-basis Measurements	Yes

The protocol in Ref. [24] is based on single particles for the intersection calculation. Both its quantum operations and measurements are relatively

easy to implement. However, the protocol requires $(2n + 3d)$ particles which consumes more particles than our protocol when n is sufficiently large.

We also compare our protocol with two single-photon QMPSI protocols [25, 26] in the two-party setting. The protocol in Ref. [25] accomplishes its goal using only rotation operations and simple measurements. However, the third party must separately share a secret key of n angles with Alice and Bob via QKD [31]. Assuming each angle is represented by m bits, this requires sharing nm bits with each party, consuming $4nm + 2d$ particles in total, where $2d$ particles are allocated for eavesdropping detection. Furthermore, λn $(\lambda \geq 1)$ particles are used to compute the intersection, with an additional $3d$ decoy particles ensuring their secure transmission. Consequently, the protocol requires $4nm + \lambda n + 5d$ particles altogether.

The protocol in Ref.[26] requires only $(n + d)$ particles, where d denotes the number of particles used for eavesdropping detection. Note that each participant must, in advance, share a secret key with the third party, which would cost more particles if the secret key is generated via QKD. The protocol needs to apply unitary operators $E^h_{x'}$ and $S^h_{y'}$ for encoding and encryption, defined as

$$E^h_{x'} = \sum_{k=0}^{h-1} \omega^{kx'} |k\rangle\langle k|, \tag{18}$$

$$S^h_{y'} = \sum_{k=0}^{h-1} \omega^{k^2 y'} |k\rangle\langle k|, \tag{19}$$

where h is the dimension of particles, $\omega = e^{2\pi i/d}$, and $x', y' \in \mathbb{Z}_d$. In addition, high-dimensional measurements are required.

The comparison demonstrates that our protocol requires fewer quantum resources than most existing similar protocols, and it is easier to implement with current quantum technology.

8. Conclusion

In this paper, we proposed a two-party QPSI protocol with a semi-honest third party based solely on single particles and single-qubit unitary operators, and showed its correctness and security. We also validated the correctness of the protocol by simulation on IBM Qiskit simulator. The protocol is highly feasible with respect to state preparation, quantum operations, and measurements. Furthermore, it consumes fewer quantum resources than most existing protocols.

Declarations

Availability of data and materials

No datasets were generated or analysed during the current study.

Competing interests

The authors declare no competing interests.

Acknowledgments

This work is supported by the Shenzhen Polytechnic University Research Fund (Grant No. 6024310040K), Research Projects of Department of Education of Guangdong Province (Grant No. 2023ZDZX1081), and the National Natural Science Foundation of China (Grant No. 62471187).

Author's contributions

C.Z. and Z.Z contributed to conceptualization, investigation, methodology, and writing the original draft. Z.S. contributed to supervision, project administration, validation, reviewing, and editing of the writing.

Ethics, Consent to Participate, and Consent to Publish declarations: not applicable.

References

[1] Yao AC. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982: 160-164.

[2] Ma R, Li Y, Li C, et al. Secure multiparty computation for privacy-preserving drug discovery[J]. Bioinformatics, 2020, 36(9): 2872-2880.

[3] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[4] Shen A, Cao XY, Wang Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states[J]. Science China Physics, Mechanics & Astronomy, 2023, 66(6): 260311.

[5] Khorrampanah M, Houshmand M. Effectively combined multi-party quantum secret sharing and secure direct communication[J]. Optical and Quantum Electronics, 2022, 54(4): 213.

[6] Jiang S, Liu Z, Lou X, et al. Efficient verifiable quantum secret sharing protocols via eight-quantum-entangled states[J]. International Journal of Theoretical Physics, 2021, 60(5): 1757-1766.

[7] Gao F, Qin SJ, Huang W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol[J]. Science China Physics, Mechanics & Astronomy, 2019, 62(7): 70301.

[8] Liu B, Liang Z, Huang W, et al. Decoy-state quantum-key-distribution-based quantum private query with error tolerance bound[J]. Physical Review A, 2024, 109(5): 052442.

[9] Liu D, Li J, Chen X, et al. Quantum private query protocol based on counterfactual quantum key distribution with noiseless attack[J]. Quantum Information Processing, 2024, 23(10): 352.

[10] Qin L, Liu B, Gao F, et al. Decoy-state quantum private query protocol with two-way communication[J]. Physica A: Statistical Mechanics and its Applications, 2024, 633: 129427.

[11] Freedman MJ, Nissim K, Pinkas B. Efficient private matching and set intersection[C]//International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 1-19.

[12] Wu ME, Chang SY, Lu CJ, et al. A communication-efficient private matching protocol in client-server model[J]. Information sciences, 2014, 275: 348-359.

[13] Hazay C. Oblivious polynomial evaluation and secure set-intersection from algebraic PREs[J]. Journal of Cryptology, 2018, 31(2): 537-586.

[14] Shi R, Mu Y, Zhong H, et al. An efficient quantum protocol for private set intersection[J]. Quantum Information Processing, 2016, 15(1): 363-371.

[15] Cheng X, Guo R, Chen Y. Cryptanalysis and improvement of a quantum private set intersection protocol[J]. Quantum Information Processing, 2017, 16(2): 37.

[16] Maitra A. Quantum secure two party computation for set intersection with rational players[J]. arXiv preprint arXiv:1801.08319, 2018.

[17] Debnath SK, Dey K, Kundu N, et al. Feasible private set intersection in quantum domain[J]. Quantum Information Processing, 2021, 20(1): 41.

[18] Liu W, Yin HW. A novel quantum protocol for private set intersection[J]. International Journal of Theoretical Physics, 2021, 60(6): 2074-2083.

[19] Liu WJ, Li WB, Wang HB. An improved quantum private set intersection protocol based on Hadamard gates[J]. International Journal of Theoretical Physics, 2022, 61(3): 53.

[20] Hou M, Wu Y, Zhang S. Quantum Private Set Intersection protocol Based on Bell States[J]. Axioms, 2025, 14(2): 120.

[21] Shi R, Mu Y, Zhong H, et al. Two quantum protocols for oblivious set-member decision problem[J]. Scientific Reports, 2015, 5(1): 15914.

[22] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. IEEE, 1994: 124-134.

[23] Grover LK. A fast quantum mechanical algorithm for database search[C]//Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996: 212-219.

[24] Chen Y, Situ H, Huang Q, et al. A novel quantum private set intersection protocol with a semi-honest third party[J]. Quantum Information Processing, 2023, 22(12).

[25] Huang X, Zhang W, Zhang S. Quantum multi-party private set intersection using single photons[J]. Physica A: Statistical Mechanics and its Applications, 2024, 649: 129974.

[26] Guo G D, Zheng L Q, Yu K, et al. Authenticated Multi-Party Quantum Private Set Intersection with Single Particles[J]. Mathematics, 2025, 13(12): 2019.

[27] Trushechkin A S, Kiktenko E O, Kronberg D A, et al. Security of the decoy state method for quantum key distribution[J]. Physics–Uspekhi, 2021, 64(1): 88-102.

[28] Peng J, He G, Xiong J, et al. Trojan horse attack strategy on quantum private communication[C]//International Conference on Information Security Practice and Experience. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 177-186.

[29] Jain N, Anisimova E, Khan I, et al. Trojan-horse attacks threaten the security of practical quantum cryptography[J]. New Journal of Physics, 2014, 16(12): 123030.

[30] Gao F, Liu B, Wen Q Y, et al. Flexible quantum private queries based on quantum key distribution[J]. Optics express, 2012, 20(16): 17411-17420.

[31] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical computer science, 2014, 560: 7-11.