




A novel quantum private set intersection scheme with a semi-honest third party

Yumeng Chen¹ · Haozhen Situ¹ · Qiong Huang¹ · Cai Zhang¹ 

Received: 9 April 2023 / Accepted: 24 November 2023 / Published online: 8 December 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

In this paper, we propose a novel scheme with a semi-honest third party (TP) to compute the intersection of two parties' sets privately. In our scheme, two groups of particles are firstly prepared by TP and then transmitted circularly among TP and two participants who need the intersection of their private sets. The two participants then perform the unitary operations on their received particles according to an initial encoding rule for their private sets, respectively, to help TP to obtain the result. We analyse the security of our scheme and show that it can resist both outside and inside attacks over ideal and noisy quantum channels. In addition, our scheme is feasible with current quantum technologies as it only requires simple quantum resources and operations.

Keywords Quantum private set intersection · Semi-honest · Quantum cryptography

1 Introduction

Secure Multiparty Computation (MPC) [1], as a common cryptographic primitive, allows distributed participants to collaborate to obtain specific outputs without disclosing their original inputs. Due to its adequate protection of information privacy, the research on MPC has important application value in the current situation of the explosive growth of data and has gained increasing attention. MPC has several branches for different applications, such as secret sharing [2–5], private queries [6–8], and private set intersection [9–17]. And this paper mainly focuses on the topic of private set intersection.

Private Set Intersection (PSI) aims to find the common elements in the sets of all participants without exposing other elements of the participants' private sets. Generally,

✉ Cai Zhang
zhangcai@scau.edu.cn

¹ College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China

traditional MPC is based on classical cryptographic schemes. Therefore, many scholars have produced rich outcomes on PSI based on classical cryptography. For example, Freedman et al. [9] adopted homomorphic encryption and balanced hash function to achieve PSI, which effectively ensures the security of the scheme in the semi-honest setting. Wu et al. [10] combined an OT protocol and a universal hash function to present a PSI scheme in the client–server model. Hazay et al. [11] solved the PSI problem with a selected pseudorandom function. The security of the above schemes all relies on unproven mathematical assumptions, and it can be threatened by quantum computers that show powerful computing ability due to the high parallelism of quantum mechanics. It has already been known that Shor’s [18] algorithm could factor larger integers in polynomial arithmetic time and it can be used to break the RSA scheme that has a large number of applications in reality. Except this, Grover’s searching algorithm [19] can finish the task of function inversion and has a huge threat to symmetric-key cryptography. Therefore, the research on cryptography against quantum attacks should attract more attention.

Due to the vulnerability of the classical cryptographic schemes, Quantum Private Set Intersection (QPSI) came into being. But there are few outcomes on QPSI at present. Several published QPSI schemes [12, 14–16] are presented based on the quantum oblivious set member decision protocol [20]. Shi et al. [12] presented a two-party QPSI scheme in the server-client model. But Cheng et al. [14] found that the scheme has a fairness issue in that the server can arbitrarily manipulate the client’s outcome, and given this, they proposed an improved scheme by introducing a passive third party to discover the server’s dishonest behaviour. Maitra [15] proposed a scheme based on the assumption that all the participants are rational to maximize their utilities to guarantee the scheme’s fairness and security. All the above schemes need to use special encoded quantum states and complex oracle operators, which makes these schemes hard to be implemented. In 2021, Debnath et al. [16] presented a PSI scheme in the quantum setting based on a server-client model. The scheme adopted the Quantum Key Distribution (QKD) protocol to generate needed keys and then used the keys to accomplish the PSI steps with the quantum oblivious set member decision protocol. The scheme’s implementation only needs simple quantum resources and operations in the QKD period, so it has better feasibility compared with the above schemes. However, in this scheme, only one participant can eventually get the result of the final intersection. Liu et al. [13] proposed a two-party QPSI scheme based on quantum Fourier transform (QFT) with a semi-honest third party. Compared to the schemes based on the quantum oblivious set member decision protocol [20], both of the participants could get the result of the final intersection in their scheme. But Liu et al. [17] pointed out that this scheme has a shortage that the participants’ privacy could be leaked after executing the whole process and proposed an improvement by changing the quantum operation and adding the exclusive-or calculation steps to prevent the privacy leakage. Nevertheless, this improvement needs to operate the quantum operation fractional times, which is also not easy to be implemented with current quantum technology. Other schemes [21, 22] mainly focus on calculating the cardinality of the intersection or union of private sets.

Although all of the existing QPSI schemes can solve the problem of private set intersection in the quantum setting, the schemes which satisfy different application

scenarios and have good feasibility are still demanded. We thus propose a two-party quantum private set intersection scheme with a semi-honest third party, in which participants only need basic unitary operations and simple quantum states to finish the task, and the final output of the intersection can be obtained by all participants. The security analysis shows that our scheme is secure against both internal and external attacks.

The rest of the paper is organized as follows: In Sect. 2, we give a detailed description of our scheme after its security requirements and necessary preliminaries. In Sect. 3, the analyses of the presented scheme’s correctness and security are conducted. In Sect. 4, we provide a detailed comparison between our scheme with the previous schemes. In the end, we make a conclusion in Sect. 5.

2 Quantum private set intersection scheme

In this section, we give the detailed description of our QPSI scheme in which a semi-honest third party Charlie who helps obtain the intersection of Alice’s private set A and Bob’s private set B is involved. The semi-honest third party Charlie would honestly follow the steps of the scheme and he would not collude with another dishonest participant to obtain the honest one’s private set.

Our scheme should satisfy the following requirements:

- Correctness: If Alice and Bob honestly offer their private sets A and B , respectively, Charlie will output the correct result $C = A \cap B$.
- Security: Outside attackers cannot learn any information about Alice’s and Bob’s private sets.
- Privacy: Except the intersection of private sets, the semi-honest third party and the dishonest participant learn nothing about the honest participant’s private set.

Two unitary operations are required in our scheme. One is the X gate: $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, which changes $|0\rangle(|1\rangle)$ to $|1\rangle(|0\rangle)$. The other is the controlled-NOT ($CNOT$) gate: $CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$, which transforms $|x\rangle|y\rangle$ to $|x\rangle|x \oplus y\rangle$, where $x, y \in \{0, 1\}$ and \oplus is the addition modulo two.

Assume that the universal set is $U = \{0, 1, 2, \dots, n - 1\}$, and Alice’s and Bob’s private sets are $A \subseteq U$ and $B \subseteq U$, respectively. Alice and Bob generate an n -bit string S_A and S_B , respectively, according to the following encoding rule:

$$S_A^j = \begin{cases} 1, & j \in A, \\ 0, & j \notin A, \end{cases} \quad S_B^j = \begin{cases} 1, & j \in B, \\ 0, & j \notin B, \end{cases} \quad (1)$$

where j ranges from 0 to $n - 1$ and S_A^j (S_B^j) denotes the j -th bit in String S_A (S_B).

Let us now move on to the description of our scheme. In this section, we assume that the quantum channel is noiseless and lossless, and the classical channel is authenticated. Note that Charlie is semi-honest and he assists Alice and Bob in computing the intersection of their private sets without disclosing the privacy of the sets.

The procedure of the scheme is as follows:

- Charlie first prepares two groups of single particles of size n and denotes them as $G_1 = \{q_0, q_1, \dots, q_{n-1}\}$ and $G_2 = \{f_0, f_1, \dots, f_{n-1}\}$ respectively. And the states of q_j and f_j ($j = 0, 1, \dots, n-1$) are all randomly selected from the $\{|0\rangle, |1\rangle\}$ basis. After this, Charlie randomly prepares $2d$ decoy particles, each of which is randomly in one of the states $\{|+\rangle, |-\rangle, |+\rangle, |-\rangle\}$ ($|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, $|+\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$). Then, Charlie inserts the d decoy particles in G_1 and G_2 at random, respectively, and records the inserted positions. Eventually, Charlie sends all of the particles to Alice.
- After Alice confirms that she has received all of the particles, she consults with Charlie for the eavesdropping detection: Charlie tells Alice the locations and the corresponding measurement basis of each decoy particle's state through the classical channel. Then, Alice measures each decoy particle's state with the corresponding basis and announces the measurement results to Charlie. Charlie then compares the sequence's measurement results with the initial states of the decoy particles and calculates the error rate. If the error rate exceeds the threshold, he tells Alice to discard all of the particles and goes back to Step 1. Otherwise, Alice discards all the decoy particles and proceeds to the next step.
- After Alice confirms that the detection has passed, she will perform unitary operations according to Sequence S_A . The operating rule is as follows: for each pair of particles of q_j in G_1 and f_j in G_2 ($j = 0, 1, \dots, n-1$), if $S_A^j = 0$, Alice performs nothing on these two particles, and if $S_A^j = 1$, Alice firstly performs X operation on q_j , then Alice performs the $CNOT$ operation on q_j and f_j where q_j is the control particle and f_j is the target particle. After Alice performs the operations on all particles, she finally obtains two new groups of particles: $G'_1 = \{q'_j(j = 0, 1, \dots, n-1)\}$ and $G'_2 = \{f'_j(j = 0, 1, \dots, n-1)\}$. Later, Alice respectively and randomly inserts d decoy particles into G'_1 and G'_2 , records the inserted positions, and sends all the particles to Bob.
- After Bob confirms that all particles have been received, he and Alice perform the same eavesdropping detection as that in Step 2. If passed, he discards all the decoy particles and goes to the next step. If not, the first step will be returned.
- After Bob confirms that the detection has passed, he will also perform unitary operations according to Sequence S_B . The operating rule is same as Alice's: for each pair of particles of q'_j in G'_1 and f'_j in G'_2 ($j = 0, 1, \dots, n-1$), if $S_B^j = 0$, Bob performs nothing on the two particles; and if $S_B^j = 1$, Bob firstly performs X operation on q'_j , then Bob perform the $CNOT$ operation on q'_j and f'_j where q'_j is the control particle and f'_j is the target particle. After Bob performs the operations on all particles, he finally obtains two new groups of particles: $G''_1 = \{q''_j(j = 0, 1, \dots, n-1)\}$ and $G''_2 = \{f''_j(j = 0, 1, \dots, n-1)\}$. After Bob gets G''_1 and G''_2 , he performs the following operations: Bob shuffles all the particles in G''_1 and G''_2 , and he writes down all the positions he has changed. Later, Bob randomly inserts d decoy particles into G''_1 and G''_2 , respectively and records the positions, and sends all the particles to Charlie.

6. After Charlie confirms that all particles have been received, he and Bob perform the same eavesdropping detection as above. If not passed, Charlie discards all the particles and goes back to Step 1. Otherwise, he only discards the decoy particles, and follows the next step to get the final intersection C .
7. After the detection has passed, Bob should firstly tell Charlie all the changed positions in G_1'' and G_2'' to recover the original sequence. Then, Charlie measures the state of each particle in G_1'' . If the state of q_j'' changes compared with that of q_j ($j = 0, 1, \dots, n - 1$), Charlie can ensure that the intersection C of A and B does not include the element j . But if the two states of q_j and q_j'' are the same, then Charlie measures the state of each particle in G_2'' in the $\{|0\rangle, |1\rangle\}$ basis, and compares the results with the state of each particle in G_2 . If the state of f_j'' is the same as the state of f_j , Charlie confirms that the intersection C of A and B does not contain j . And if the state of f_j'' is not the same as that of f_j , Charlie confirms that the intersection C of A and B contains j . Thus, Charlie obtains the intersection of the two sets without learning any additional information about A and B .

Note that our scheme could also be used in the noisy quantum channel. In this case, the threshold of eavesdropping detection may vary and the error rate could be higher due to different kinds of quantum noises. Thus, we may consider in detail the quantum noises' impact on our scheme in the future.

3 Analysis of the proposed scheme

In this section, we study the correctness and the security analysis of our proposed scheme.

3.1 Correctness

In this part, we show that if Alice and Bob honestly provide their private sets, Charlie will get the correct intersection of their private sets.

First, Alice and Bob perform X operation or nothing on q_j and q_j' ($j = 0, 1, \dots, n - 1$), respectively, according to the values of S_A^j and S_B^j .

- If $j \notin A$ and $j \in B$ or $j \in A$ and $j \notin B$, in both cases, the X operation is performed on the j -th particle in G_1 or G_1' only once, so the state of this particle will be flipped to the opposite state in the same basis. Thus if the states of q_j and q_j'' are different, then it can be inferred that the element j is not in the intersection.
- If $j \notin A$ and $j \notin B$, Alice and Bob all perform nothing on the j -th particle of G_1 and G_2 , respectively, so the state of q_j'' and f_j'' will be the same as their initial states. Thus if the states of q_j and q_j'' , f_j and f_j'' are all the same, then it can be inferred that the element j is not in A or B .
- If $j \in A$ and $j \in B$, in the step 3 of our scheme, Alice firstly performs the X operation on q_j , and then she performs the $CNOT$ operation on q_j and f_j where

q_j is the control particle and f_j is the target particle. That is,

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(X \otimes I), \tag{2}$$

is performed on q_j and f_j by Alice.

Similarly, in the step 5 of our scheme, after receiving the two particle groups of G'_1 and G'_2 , Bob performs the X operation on q'_j and then performs the $CNOT$ operation on q'_j and f'_j where q'_j is the control particle and f'_j is the target particle. Then, the equivalent operation

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(X \otimes I), \tag{3}$$

is performed on q'_j and f'_j by Bob.

With the quantum operations 2 and 3, we see that

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(X \otimes I)(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(X \otimes I) \tag{4}$$

$$= (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(X \otimes I)(|0\rangle\langle 1| \otimes I + |1\rangle\langle 0| \otimes X) \tag{5}$$

$$= (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(|1\rangle\langle 1| \otimes I + |0\rangle\langle 0| \otimes X) \tag{6}$$

$$= (|0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes X) \tag{7}$$

$$= I \otimes X, \tag{8}$$

which is performed on q_j and f_j .

Thus if the states of q_j and q''_j are the same, and the states of f_j and f''_j are different, then the element j must be in the intersection.

Moreover, in our scheme, we can get the set of $\overline{A \cup B}$ from the case where $j \notin A$ and $j \notin B$. With this, it is easy to obtain the set of $A \cup B$ by computing $U - \overline{A \cup B}$.

An example: Suppose that the initial states of the j -th pair of particle q_j and particle f_j are $|0\rangle$ and $|0\rangle$, respectively, then we have the following:

- If neither A nor B contains j , then $S_A^j=0$ and $S_B^j=0$. The changes of the states of q_j and f_j are

$$|0\rangle|0\rangle \xrightarrow[I \otimes I]{\text{Alice's operation}} |0\rangle|0\rangle \xrightarrow[I \otimes I]{\text{Bob's operation}} |0\rangle|0\rangle.$$

- If only set B contains j , then $S_A^j=0$ and $S_B^j=1$. The changes of the states of q_j and f_j are

$$|0\rangle|0\rangle \xrightarrow[I \otimes I]{\text{Alice's operation}} |0\rangle|0\rangle \xrightarrow[(X \otimes I)(CNOT_{q'_j, f'_j})]{\text{Bob's operation}} |1\rangle|1\rangle.$$

- If only set A contains j , then $S_A^j=1$ and $S_B^j=0$. The changes of the states of q_j and f_j are

$$|0\rangle|0\rangle \xrightarrow[(X \otimes I)(CNOT_{q_j, f_j})]{\text{Alice's operation}} |1\rangle|1\rangle \xrightarrow[I \otimes I]{\text{Bob's operation}} |1\rangle|1\rangle.$$

- If both sets A and B contain j , then $S_A^j=1$ and $S_B^j=1$. The changes of the states of q_j and f_j are

$$|0\rangle|0\rangle \xrightarrow[(X \otimes I)(CNOT_{q_j, f_j})]{\text{Alice's operation}} |1\rangle|1\rangle \xrightarrow[(X \otimes I)(CNOT_{q'_j, f'_j})]{\text{Bob's operation}} |0\rangle|1\rangle.$$

3.2 Security

In this subsection, we firstly analyse the security of the proposed scheme against external and internal attacks on the ideal quantum channel. We then analyse its security on lossy and noisy quantum channels. Let us first analyse the security against external attacks.

3.2.1 External attacks

External attacks refer to the possible attacks carried out by an outside attacker Eve, and she may intend to get useful information about Alice’s or Bob’s sets during the transmission of particles between participants. As the decoy states are employed for the eavesdropping detection and this technique has been proven to provide unconditional security, external attacks, such as the intercept-resend attack, the entanglement-measurement attack and the denial-of-service (DOS) attack, are invalid to our scheme. Here, we analyse the security of our scheme against the intercept-resend attack and the entanglement-measurement attack in detail.

1. Intercept-Resend Attack

For the external attacker Eve, a common attack is to intercept the particles sent by a certain party in the stage of transmitting particles.

When Eve gets the intercepted particles, she may measure them in the Z-basis. Then, she generates a new sequence of particles in the Z-basis whose states are same as her measurement results and sends all the particles to the original receiver. Assume that all particles Eve sends are in the Z-basis and d decoy particles are used for the eavesdropping detection. For any randomly selected decoy particle, the error rate of the state of a single particle’s measurement introduced by eavesdropping operation is $(1 - \frac{1}{2} * 1 - \frac{1}{2} * \frac{1}{2}) = \frac{1}{4}$. Given this, the probability that at least one of the introduced decoy particles will be detected incorrectly is $1 - (\frac{3}{4})^d$. When d is large enough, the probability of detecting an error will approach 1. Then, there is a high probability that Eve’s eavesdropping will be detected by the receiver, at which point the receiver discards all received particles and returns to the first step of the scheme to re-execute. Therefore, Eve will not be able to get any information about the Alice’s or Bob’s private sets, and the scheme is secure against this attack.

2. Entanglement-Measurement Attack

Besides the intercept-resend attack, Eve may carry out the entanglement-measurement attack on the proposed scheme during the particles’ transmission. It specifically means that Eve firstly intercepts the particles during a certain stage of transmission, then she entangles her generated auxiliary particle sequence $E = \{|E_0\rangle, |E_1\rangle, |E_2\rangle, \dots, |E_{n-1}\rangle\}$ with the intercepted particles through some

unitary operations. And the corresponding unitary operations could be denoted as

$$\begin{aligned}
 U|+\rangle|E_i\rangle &= \alpha|+\rangle|e_{00}\rangle + \beta|-\rangle|e_{01}\rangle, \\
 U|-\rangle|E_i\rangle &= \gamma|+\rangle|e_{10}\rangle + \delta|-\rangle|e_{11}\rangle, \\
 U|+y\rangle|E_i\rangle &= \frac{1}{2}|+y\rangle(\alpha|e_{00}\rangle + i\beta|e_{01}\rangle - i\gamma|e_{10}\rangle + \delta|e_{11}\rangle) \\
 &\quad + \frac{1}{2}| -y\rangle(i\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \gamma|e_{10}\rangle - i\delta|e_{11}\rangle), \\
 U|-y\rangle|E_i\rangle &= \frac{1}{2}| -y\rangle(\alpha|e_{00}\rangle - i\beta|e_{01}\rangle + i\gamma|e_{10}\rangle + \delta|e_{11}\rangle) \\
 &\quad + \frac{1}{2}|+y\rangle(-i\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \gamma|e_{10}\rangle + i\delta|e_{11}\rangle).
 \end{aligned}$$

The parameters above also should satisfy: $|\alpha|^2 + |\beta|^2 = 1, |\gamma|^2 + |\delta|^2 = 1$.

In our scheme, the eavesdropping detection is always required after the transmitting process. If the state of a decoy particle is in the $\{|+\rangle, |-\rangle\}$ basis and Eve attempts to pass the detection, she must set $\beta = \gamma = 0$.

Similarly, if the state of a decoy particle is in the $\{|+y\rangle, |-y\rangle\}$ basis and Eve attempts to pass the detection, the equation $i\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \gamma|e_{10}\rangle - i\delta|e_{11}\rangle$ should be a zero vector. Combined with four values of $\alpha, \beta, \gamma, \delta$, it can deduced that $\alpha|e_{00}\rangle = \delta|e_{11}\rangle$.

Finally, we have

$$\begin{aligned}
 U|+\rangle|E_i\rangle &= \alpha|+\rangle|e_{00}\rangle, \\
 U|-\rangle|E_i\rangle &= \delta|-\rangle|e_{11}\rangle = \alpha|-\rangle|e_{00}\rangle, \\
 U|+y\rangle|E_i\rangle &= \frac{1}{2}|+y\rangle(\alpha|e_{00}\rangle + 0 + 0 + \delta|e_{11}\rangle) = \alpha|+y\rangle|e_{00}\rangle, \\
 U|-y\rangle|E_i\rangle &= \frac{1}{2}| -y\rangle(\alpha|e_{00}\rangle + 0 + 0 + \delta|e_{11}\rangle) = \alpha| -y\rangle|e_{00}\rangle,
 \end{aligned}$$

which mean Eve only gets the particles whose states are unrelated to the intercepted ones. Therefore, Eve cannot get any private information through this attack. Otherwise, she will fail to pass the eavesdropping detection with a high probability.

3. Trojan-Horse Attacks

Trojan-Horse Attacks [23], such as the delay-photon Trojan-horse attack and the invisible photon eavesdropping Trojan horse attack, may occur in quantum communication protocols where quantum states are relayed. Our scheme may thus face such potential security risk. However, there have already been techniques that we can utilize to eliminate the risk.

To avoid Trojan-Horse attacks, our scheme can be equipped with the Wavelength Quantum Filter (WQF) to remove invisible Photons and with Optical filters, such as photons Splitter and Photons Number Splitter (PNS) to separate legitimate photons from delayed photons. In this way, it can efficiently detect the Trojan-Horse Attacks. Once the attacks are detected, the discoverer will drop all the particles and repeat the scheme back again.

3.2.2 Participants' attack

Compared to the outside attackers, the participants usually have the advantage to get more information, thus the dishonest participant poses high security risk to obtain the honest one's private information. Here, we thoroughly analyse this kind of attack on our scheme.

- **Charlie's Attack:** In this paper, we assume that the third party Charlie is semi-honest, which means that Charlie will not launch a conspiracy attack with Alice or Bob.

If Charlie wants to capture information about Alice's or Bob's set, he may behave just like the outside attackers. However, according to the above analysis, he will fail to pass the eavesdropping detection. Besides, for preparing the quantum states used for the computation of the intersection of Alice's and Bob's sets, Charlie can also utilize such an advantage and try to learn extra information about the participants' sets. It is obvious that Charlie is able to learn that some elements are in the intersection of Alice's and Bob's sets or they are not. But for the case where some elements are in either Alice's or Bob's set, he cannot determine whether these elements are exactly from Alice's set or from Bob's set according to the operating rule used in our scheme. Therefore, our scheme is still secure against Charlie's attack.

- **Alice's:** In the scheme, all the particles' states are kept in the $\{|0\rangle, |1\rangle\}$ basis, so Alice can measure and know the exact state of each particle of G'_1 and G'_2 after her operation, which means she knows the initial states of Bob's received particles. After the detection has passed, then Bob performs unitary operations on his received G'_1 and G'_2 according to his coding and then transmits G''_1 and G''_2 to Charlie with the decoy particles.

Alice may launch the intercept-resend attack for the particles Bob sends to Charlie. Specifically, Alice can measure all particles of G''_1 , G''_2 and the decoy particles in the $\{|0\rangle, |1\rangle\}$ basis and obtain the measurement results. With the information about the inserted positions of decoy particles announced by Bob due to the eavesdropping detection, Alice will obtain Bob's private set. Although this attack will be detected, Alice has already known Bob's private set by comparing the measurement results with the states of particles of G'_1 and G'_2 .

In order to resist this kind of attack, in the step 5 of our protocol, Bob shuffles the particles of G''_1 and G''_2 . After the detection has been confirmed to be passed, Bob tells Charlie to recover the right sequence. But if not passed, Bob will not announce the right order. Therefore, Alice cannot get any information about Bob's private set from the disordered sequence.

- **Bob's:** Just like Alice, after discarding all of the decoy particles, Bob can also measure each particle of G'_1 and G'_2 in the $\{|0\rangle, |1\rangle\}$ basis and get the measurement results. By Comparing these results with the states of particles of G_1 and G_2 , he can infer which operations has been performed by Alice, thus learning Alice's private set based on the encoding rules.

However, Bob will fail to finish this task. First, Charlie does not share the states of particles of G_1 and G_2 because of his semi-honesty. Then, Bob may try to learn

these states in a way as the external attackers do. There is no doubt that Bob cannot pass the eavesdropping detection; thus, he cannot get the states of G_1 and G_2 . For not knowing the whole of Alice's group's before-after states, Bob cannot get the information about Alice's private set.

- Note that there exists an internal attack in the set-encoding model for the quantum private set intersection schemes. This attack happens when Charlie needs to announce the result of the final intersection in some situations. Once a dishonest participant, Alice or Bob, encodes their own set as the complete set, and the other one honestly encodes his private set. Both of them perform the defined operations based on the encoding rule. The final result published by Charlie would be the honest participant's private set. Because all inputs are private, then no one can discover this cheating during the protocol. This attack exists in current QPSI scheme [13] and how to remove it will be our future work.

3.2.3 Security over the lossy and noisy quantum channels

As above, we have already analysed the security of our scheme on the ideal quantum channels. However, in reality, the quantum channels are usually lossy and noisy, which may influence the security of our scheme. Errors introduced by attacks can be regarded as the results of quantum noises. In what follows, we analyse the security on the two non-ideal situations.

- Case 1: Security over the lossy quantum channels

In this situation, the outside attacker Eve may use the property of lossy quantum channel to make an attack.

When any participant in our scheme transmits the particles on which operations have been performed to the receiver, Eve may intercept some of the particles and send the other particles to the receiver via an ideal quantum channel. During this process, if Eve gets some valid particles which are not decoy photons, she could get to know the states by measuring them in the Z-basis.

However, our private inputs are all encoded by the quantum operations instead of the states. Thus, even Eve knows the measurement results in this round, she still cannot get any private information.

Besides, in our scheme, the sender always makes sure that the receiver has got all the particles. So this attack will finally be discovered by both of the two parties. The receiver will not act his quantum operations on the intercepted particles, and Eve will get nothing from the intercepted particles.

- Case 2: Security over the noisy quantum channels

Similar to Case 1, the outside attacker may launch attacks over the noisy quantum channel.

For example, in the process of transmitting particles in our scheme, Eve firstly intercepts all the particles, then she may adopt the intercept-resend or entangle-measure attack. In the end, Eve sends all the tampered particles to the receiver over a self-established channel and pretends the possible errors are introduced by the noises.

In this situation, Eve tries to use the channel's noises to cover up her attack; however, according to the above security analysis under the intercept-resend and

entangle-measure attack, once these attacks occur, the error rate of 25% will make it always be discovered. So the eavesdropping detection will not pass, then all the received particles will finally be thrown away.

4 Comparison

In this section, we compare our scheme with the proposed schemes in terms of quantum resources, quantum measurement, and quantum operations in Table 1.

Suppose that the size of the complete set is n , and d decoy particles are employed to check the eavesdropping. To get the intersection of the two private sets, our scheme needs $2n + 3d$ particles ($2n$ particles for encoding and $3d$ particles for eavesdropping detection).

We can see from Table 1 that our scheme uses more particles than the schemes in Refs. [12] and [13]. Nevertheless, for the schemes' feasibility, the scheme in Ref. [12] needs to prepare multi-particle entangled states, and the scheme in Ref. [13] requires the OAM states of single photons. The OAM state is a special high-dimensional state of a single photon corresponding to its physical inner property of orbital angular momentum. However, only the Z-basis states of single photons are used in our scheme, in the current technology, our scheme is easier to be implemented for the preparation of the quantum states than the schemes in Refs. [12] and [13].

Besides, the scheme in Ref. [12] requires two operations U_0 and U_s ,

$$U_0 = \sum_{x \neq 0} |x\rangle\langle x| - |0\rangle\langle 0| \quad U_s = \sum_{x \notin S} |x\rangle\langle x| - \sum_{x \in S} |x\rangle\langle x|$$

and adopts the Von Neumann Measurement. The two operators U_0 and U_s are realized by complex oracles and their inputs need multi-particle entangled states that are related to the size of the client's set. It can be inferred that when the size of the client's set is larger than 4, then the quantum operations of their scheme will be performed more times than ours. The scheme in Ref. [13] takes the QFT operation on the OAM state of a single photon, and adopts the related OAM basis measurement. Compared to the two schemes, our scheme only adopts the X and $CNOT$ operations on single photons, thus our scheme is also easier to be implemented on the quantum operations and measurements.

5 Conclusion

In this article, we propose a QPSI scheme with a semi-honest third party using just single particles. And we also give the detailed correctness and security analyses of our proposed scheme.

Compared to other QPSI schemes, one of the advantages of our scheme is that it only needs simple quantum resources and operations, and it is easier to implement with current quantum technology. In addition, our proposed scheme can also obtain the

Table 1 Comparison of our proposed scheme to others

Schemes	Quantum resources	Quantum operations	Quantum measurement
Scheme in Ref. [12]	n encoded states $\frac{ 0\rangle+ c_i\rangle}{\sqrt{2}}$	U_0 and U_s	Von Neumann Measurement
Scheme in Ref. [13]	$(n + 3d)$ single photons	QFT	OAM basis Measurement
Our scheme	$(2n + 3d)$ single photons	X and $CNOT$	Z-basis Measurement

union of two private sets. Through this scheme, the intersection and the union of two private sets can be obtained at the same time and the privacy of the sets is preserved.

The current proposed QPSI schemes including ours are just used to calculate the intersection of two private sets and we will consider how to design the schemes of the quantum secure intersection of multi-parties' private sets in the future.

Acknowledgements This work was supported by the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2021A1515011985), the National Natural Science Foundation of China (Grant No. 61902132), the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2022A1515140116) and the National Natural Science Foundation of China (Grant No. 61872152).

Data availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare they have no competing interests.

References

1. Yao, Andrew C.: Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982), pp. 160–164. IEEE, (1982)
2. Shamir, Adi: How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)
3. Chen, Xiaoxiao, Lou, Xiaoping: An efficient verifiable quantum secret sharing scheme via quantum walk teleportation. *Int. J. Theor. Phys.* **61**(4), 99 (2022)
4. Jiang, Shaohua, Liu, Zehong, Lou, Xiaoping, Fan, Zhou, Wang, Sheng, Shi, Jinjing: Efficient verifiable quantum secret sharing schemes via eight-quantum-entangled states. *Int. J. Theor. Phys.* **60**, 1757–1766 (2021)
5. Khorrampanah, Mahsa, Houshmand, Monireh: Effectively combined multi-party quantum secret sharing and secure direct communication. *Opt. Quantum Electron.* **54**(4), 213 (2022)
6. Chor, Benny, Kushilevitz, Eyal, Goldreich, Oded, Sudan, Madhu: Private information retrieval. *J. ACM (JACM)* **45**(6), 965–981 (1998)
7. Gao, Fei, Qin, SuJuan, Huang, Wei, Wen, QiaoYan: Quantum private query: a new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **62**, 1–12 (2019)
8. Xiao, Min, Lei, Shumei: Quantum private query with authentication. *Quantum Inf. Process.* **20**, 1–13 (2021)
9. Freedman, Michael J., Nissim Kobbi, Pinkas Benny: Efficient private matching and set intersection. In: *Advances in Cryptology-EUROCRYPT 2004: international conference on the theory and applications of cryptographic techniques, Interlaken, Switzerland. Proceedings 23*, pp. 1–19. Springer, (2004)
10. Mu-En, Wu., Chang, Shih-Ying., Chi-Jen, Lu., Sun, Hung-Min.: A communication-efficient private matching scheme in client-server model. *Inf. Sci.* **275**, 348–359 (2014)
11. Hazay, Carmit: Oblivious polynomial evaluation and secure set-intersection from algebraic PRFS. *J. Cryptol.* **31**(2), 537–586 (2018)
12. Shi, Run-hua, Yi, Mu., Zhong, Hong, Cui, Jie, Zhang, Shun: An efficient quantum scheme for private set intersection. *Quantum Inf. Process.* **15**, 363–371 (2016)
13. Liu, Wen, Yin, Han-Wen.: A novel quantum protocol for private set intersection. *Int. J. Theor. Phys.* **60**(6), 2074–2083 (2021)
14. Cheng, Xiaogang, Guo, Ren, Chen, Yonghong: Cryptanalysis and improvement of a quantum private set intersection protocol. *Quantum Inf. Process.* **16**, 1–8 (2017)
15. Maitra, Arpita: Quantum secure two-party computation for set intersection with rational players. *Quantum Inf. Process.* **17**, 1–21 (2018)
16. Debnath, S.K., Dey, K., Kundu, N., Choudhury, T.: Feasible private set intersection in quantum domain. *Quantum Inf. Process.* **20**, 1–11 (2021)

17. Liu, Wen-Jie., Li, Wen-Bo., Wang, Hai-Bin.: An improved quantum private set intersection protocol based on Hadamard gates. *Int. J. Theor. Phys.* **61**(3), 53 (2022)
18. Shor Peter W.: Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134. IEEE, (1994)
19. Grover Lov K.: A fast quantum mechanical algorithm for database search. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, (1996)
20. Shi, Run-hua, Yi, Mu., Zhong, Hong, Cui, Jie, Zhang, Shun: Two quantum protocols for oblivious set-member decision problem. *Sci. Rep.* **5**(1), 1–9 (2015)
21. Liu, Bai, Zhang, Mingwu, Shi, Runhua: Quantum secure multi-party private set intersection cardinality. *Int. J. Theor. Phys.* **59**, 1992–2007 (2020)
22. Wang, Yongli, Peichu, Hu., Qiuliang, Xu.: Quantum protocols for private set intersection cardinality and union cardinality based on entanglement swapping. *Int. J. Theor. Phys.* **60**, 3514–3528 (2021)
23. Zeng Guihua. Trojan horse attacking strategy on quantum cryptography. In: *The Physics Of Communication*, pp. 495–502. World Scientific, (2003)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.