International Journal of Theoretical Physics (2022) 61: 53
https://doi.org/10.1007/s10773-022-05048-3

An Improved Quantum Private Set Intersection Protocol Based on Hadamard Gates

Wen-Jie Liu[1,2] · Wen-Bo Li[1] · Hai-Bin Wang[1,2]

Received: 26 September 2021 / Accepted: 29 January 2022 / Published online: 3 March 2022

Abstract
Recently, Liu and Yin (Int. J. Theor. Phys. 60, 2074-2083 (2021)) proposed a two-party private set intersection protocol based on quantum Fourier transform. We find the participant can deduce the other party's private information, which violates the security requirement of private set computation. In order to solve this problem, an improved private set intersection protocol based on Hadamard gate is proposed. Firstly, the more feasible Hadamard gates are used to perform on the original n qubits instead of the quantum Fourier transform, which may reduce the difficulty of implementation. In addition, through the exclusive OR calculation, the participant's private information is randomly chosen and encoded on the additional n qubits, which prevents participants from obtaining the result of the difference set S_{diff}, and then avoids the internal leakage of private information. Finally, the correctness and security analysis are conducted to show the proposed protocol can guarantee the correctness of computation result as well as resist outside attacks and participant internal attacks.

Keywords Quantum secure multi-party computation · Private set intersection · Private information leakage · Hadamard gates

1 Introduction

Secure multiparty computation (SMC) is a collaborative computing problem that derived from the "Millionaire" problem [1] raised by Yao in 1982. Under the premise of correct computation, the private information of participants who do not trust each other will not be leaked. Private set computation (PSC) is an important aspect of SMC. It is the computing foundation of data mining and machine learning based on privacy protection, and it is also

✉ Wen-Jie Liu
wenjiel@163.com

Wen-Bo Li
lwb0408@163.com

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China

[2] Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing, 210044, China

one of the active research topics in the classic information security field in recent years. At present, the security of classical PSC protocol is basically based on computational complexity, and its security can be guaranteed under the condition of limited computing power. However, quantum computing has shown super-parallel computing capabilities that classical computing cannot match, such as solving RSA large prime factorization problem [2], secondary acceleration of out-of-order database retrieval [3], and quantum forgery attacks on COPA, AES-COPA and marble authenticated encryption algorithms [4] etc. The security of most classical protocols is not guaranteed in this situation. In this regard, many scholars have begun to study quantum algorithm [5, 6]. The privacy and security of quantum algorithm is based on the physical properties of quantum mechanics, such as the No-Cloning theorem [7], uncertainty principle [8], quantum entanglement, potential unconditional security [9], etc. At present, the corresponding study of QPSC mainly includes quantum private set intersection (QPSI) [10–14] and quantum private set cardinality [15–18].

Private set intersection is an important cryptographic primitive that performs joint operations on data sets in a privacy-protected manner. Specifically, multiple participants calculate the intersection without revealing their privacy to others (including internal participants). In 2016, Shi et al. [10] first proposed a quantum scheme for the intersection of private sets. However, the server could unilaterally manipulate the intersection results in this protocol. In order to solve this problem, Cheng et al. [11] introduced a passive third party to achieve the fairness of the protocol. After that, based on the decision-making protocol for oblivious set members [19], Maitra [12] proposed quantum secure two-party computation for set intersection with rational players. These studies [10–12] require “multi-particle entangled states” as quantum resources and some “complex oracle operators”, which are difficult to achieve under current technology. In 2021, Debnath [13] proposed a QPSI protocol between the client and the server, which has higher feasibility using single photon quantum resources. But the result of the intersection in this protocol can only be obtained by one participant (i.e., client). Recently, Liu et al. proposed a novel QPSI protocol [14] (we call it the NQPSI protocol) based on quantum Fourier transform. According to the published results, all participants can obtain the intersection. However, private information will be leaked inside the participants. In order to solve this problem, an improved QPSI protocol based on Hadamard (H) gate is proposed. This protocol has two obvious advantages. Firstly, the more feasible H gate is used to replace the original quantum Fourier transform, which reduces the difficulty of implementing the protocol. More importantly, through exclusive OR calculation, the participant’s private information is randomly chosen and encoded on the additional n qubits, which prevents participants from getting the result of difference set, and then avoids the internal leakage of private information.

The rest of the paper is organized as follows. Section 2 reviews the NQPSI protocol and analyzes its loopholes. In Section 3, an improved private set intersection protocol is proposed. Section 4 verifies the correctness of the two protocols through examples and analyzes the security when facing outside attacks and participant attacks. Section 5 gives a brief summary of the content of this paper and prospects for future work.

2 Review and Analysis of NQPSI Protocol

For clarity, the NQPSI protocol [14] of Liu et al. is reviewed and analyzed here. The specific content is as follows.

2.1 Review on the NQPSI Protocol

First, they deduced that the second quantum Fourier transform of a single qubit is $QFT^2|j\rangle = -|j\rangle$, then $QFT^4|j\rangle = |j\rangle$. Suppose there is a complete set $U = \{x_1, x_2, \cdots x_n\}$. Participants Alice and Bob have private sets $S_A = \left\{s_1^A, s_2^A, \cdots s_{l_A}^A\right\}$ and $S_B = \left\{s_1^B, s_2^B, \cdots s_{l_A}^B\right\}$ respectively, where $S_A, S_B \subseteq U$. Alice and Bob coded their private set codes as $C_A = \left\{c_1^A, c_2^A, \cdots c_n^A\right\}$ and $C_B = \left\{c_1^B, c_2^B, \cdots c_n^B\right\}$ respectively. The coding rules are shown in (1) .

$$c_i^A = \begin{cases} 1, if \ \ x_i \in S_A \\ 0, if \ \ x_i \notin S_A \end{cases}, \ c_i^B = \begin{cases} 1, if \ \ x_i \in S_B \\ 0, if \ \ x_i \notin S_B \end{cases}. \tag{1}$$

Calvin is a semi-honest third party. The steps of their protocol are as follows.

Step 1 Calvin prepares a particles sequence $P_C = \left\{p_1^C, p_2^C, \cdots, p_n^C\right\}$. He inserts the decoy photon into P_C to form a new quantum sequence and sent it to Alice.

Step 2 Alice verifies the decoy particles. If the verification result is correct, she discards the decoy photon and continues the next step. Otherwise, the protocol will be aborted.

Step 3 Alice prepares two n-length strings $R_A = \left\{r_1^A, r_2^A, \cdots, r_n^A\right\}$ (The subscript n here is written as $n + l$ in the original protocol, which is probably a typing error of the author) and $H_A = \left\{h_1^A, h_2^A, \cdots, h_n^A\right\}$, where r_i^A $(i = 1, \cdots, n)$ is randomly chosen from $\{0, 1\}$ and h_i^A $(i = 1, \cdots, n)$ is a random positive integer. Then she gets the quantum sequence $P_A = \left\{p_1^A, p_2^A, \cdots, p_n^A\right\}$, where $p_i^A = QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} p_i^C$ $(i = 1, \cdots, n)$. She inserts the decoy photon into P_A to form a new quantum sequence and sends it to Bob.

Step 4 Bob verifies the decoy particles. If the verification result is correct, he discards the decoy photon and continues the next step. Otherwise, the protocol will be aborted.

Step 5 Bob prepares two n-length strings R_B and H_B, and he gets the quantum sequence $P_B = \left\{p_1^B, p_2^B, \cdots, p_n^B\right\}$, where $p_i^B = QFT^{c_i^B \times 2} QFT^{r_i^B \times h_i^B} p_i^A$ $(i = 1, \cdots, n)$. The rules are similar to Step 3. He inserts the decoy photon into P_A to form a new quantum sequence and sends it to Calvin.

Step 6 Calvin verifies the decoy particles. If the verification result is correct, he discards the decoy photon and continues the next step. Otherwise, the protocol will be aborted.

Step 7 Alice and Bob compute $h_i^C = 4 - \left(\left(r_i^A \times h_i^A\right) + \left(r_i^B \times h_i^B\right)\right) \bmod 4$ $(i = 1, \cdots, n)$ and send $h_1^C, \cdots, h_n^C$ to Calvin. Calvin calculates $p_i^{C'} = QFT^{h_i^C} p_i^B$ and measures it. If the measurement result of $p_i^{C'}$ is the same as p_i^C, Calvin knows whether c_i^A and c_i^B are equal. Calvin gets $S_A \cap S_B$.

2.2 Vulnerability Analysis

In Step 7, Calvin can get

$$p_i^{C'} = QFT^{h_i^C} p_i^B = QFT^{c_i^A \times 2 + c_i^B \times 2} p_i^C. \tag{2}$$

Table 1 Results of the NQPSI protocol

Case	c_i^A	c_i^B	$p_i^{C'}$
1	0	0	p_i^C
2	0	1	$-p_i^C$
3	1	0	$-p_i^C$
4	1	1	p_i^C

Table 1 shows the value of $p_i^{C'}$ for several paired c_i^A and c_i^B. Each of the four different pairs (c_i^A, c_i^B) corresponds to results: $p_i^{C'} = p_i^C$ or $p_i^{C'} = -p_i^C$. Specifically, as shown in Case 1 and Case 4, $p_i^{C'} = p_i^C$ is the measurement result corresponding to the "complement-intersection" set, $S_{c-in} = S_{com} \cup S_{in} = \mathcal{C}_U (S_A \cup S_B) \cup (S_A \cap S_B)$. In Case 2 and Case 3, $p_i^{C'} = -p_i^C$ is the result of difference set, $S_{diff} = (S_A - S_B) \cup (S_B - S_A)$.

Alice and Bob can obtain S_{in} according to whether the i-th information corresponding to $p_i^{C'} = p_i^C$ is included in their private set or not. However, they can know the i-th information corresponding to $p_i^{C'} = -p_i^C$ only contained in the own or the others private set. In Case 2, Alice can deduce that the i-th information is in the S_B. In Case 3, Bob can deduce that the i-th information is in the S_A. The privacy of set intersection requires that Alice (Bob) cannot know Bob's (Alice's) private set elements outside S_{in}. Obviously, the privacy of the NQPSI protocol cannot be guaranteed.

Furthermore, the author claims that Calvin can get S_{in}, which is impossible according to the protocol. And the author did not write the operation after Calvin got $c_i^A = c_i^B$ in the protocol.

3 QPSI Protocol Based on H Gates

From the analysis in the previous section, participants can obtain private information outside S_{in} of others based on S_{diff}, which leads to privacy leakage. In order to solve this problem, an improved QPSI protocol based on H gates is proposed, where $\mathrm{H} \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. The detailed procedures of our protocol are as follows (also shown in Fig. 1).

Step 1 Calvin prepares the quantum sequence $P_C = \overset{2n}{\underset{i=1}{\otimes}} P_i^C$, where P_i^C is randomly selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then he executes the operation of inserting decoy particle. Specifically, he prepares l_C decoy particles q_j^C and selects the measurement basis. After inserting q_j^C into P_C to form a new sequence P_C', Calvin records the position m_t^C $(t = 1, 2, \cdots l_C)$ of q_j^C in sequence P_C' and sends sequence P_C' to Alice.

Step 2 After receiving the sequence P_C', Alice executes the eavesdropper detection. To be specific, Calvin sends the position m_t^C of the decoy particle q_j^C in the sequence P_C' and the corresponding measurement basis to Alice. Alice compares the measurement result at this position with q_j^C. If $q_j^{C'}$ is different from q_j^C, return to Step 1. Otherwise, she discards q_j^C and proceeds to the next step.

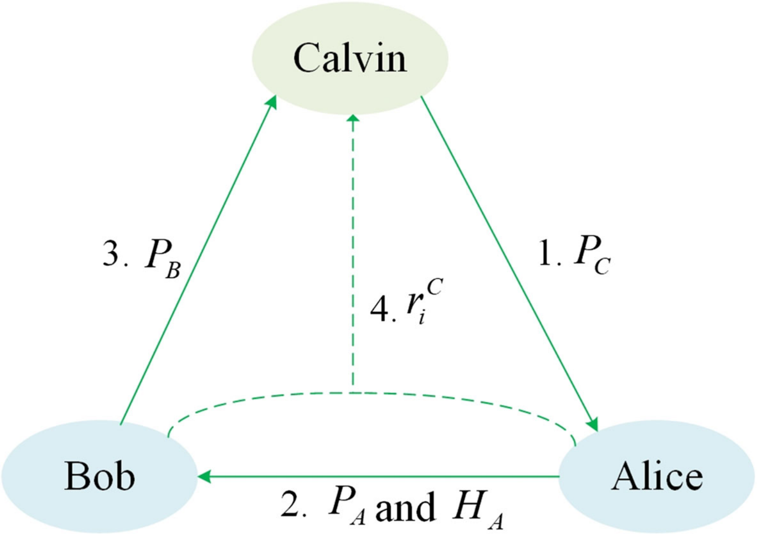

Fig. 1 Schematic diagram of QPSI protocol based on H gates. The line is the process from Step 1 to Step 6 in the protocol. Insertion of decoy photons and the eavesdropper detection are omitted here

Step 3 Alice prepares $2n$-length strings $R_A = \left\{ r_i^A \left| r_i^A \in \mathrm{N}^+, i = 1, 2, \cdots 2n \right. \right\}$ and $\mathrm{H_A} = \left\{ h_i^A \left| h_i^A \in \{0, 1\}, n < i \leq 2n \right. \right\}$. And she gets

$$\begin{aligned} P_A &= \overset{2n}{\underset{i=1}{\otimes}} P_i^A \\ &= \overset{n}{\underset{i=1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(c_i^A+2\right)} \mathrm{H}^{r_i^A} P_i^C \left\| \overset{2n}{\underset{i=n+1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(h_i^A c_i^A+2\right)} \mathrm{H}^{r_i^A} \right. , \end{aligned} \tag{3}$$

where $c_i^A = c_{i-n}^A$ $(i > n)$. Then she executes the operation of inserting decoy particles, which is similar to Step 1. After this, she sends sequence P_A' and $\mathrm{H_A}$ to Bob.

Step 4 After receiving sequence P_A', Bob executes the eavesdropper detection, which is similar to Step 2.

Step 5 Bob prepares $2n$-length strings $R_B = \left\{ r_i^B \left| r_i^B \in \mathrm{N}^+, i = 1, 2, \cdots 2n \right. \right\}$ and $\mathrm{H_B} = \left\{ h_i^B \left| h_i^B = h_i^A \oplus 1, n < i \leq 2n \right. \right\}$. And he gets

$$\begin{aligned} P_B &= \overset{2n}{\underset{i=1}{\otimes}} P_i^B \\ &= \overset{n}{\underset{i=1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(c_i^B+2\right)} \mathrm{H}^{r_i^B} P_i^A \left\| \overset{2n}{\underset{i=n+1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(h_i^B c_i^B+2\right)} \mathrm{H}^{r_i^B} P_i^A \right. , \end{aligned} \tag{4}$$

where $c_i^B = c_{i-n}^B$ $(i > n)$. Then he executes the operation of inserting decoy particles, which is similar to Step 1. After this, he sends sequence P_B' to Calvin.

Step 6 After receiving sequence P_B', Calvin executes the eavesdropper detection, which is similar to Step 2.

Step 7 Alice and Bob calculate $r_i^C = r_i^A + r_i^B$ and send the result to Calvin. Calvin gets

$$\begin{aligned} P_C{}'' &= \bigotimes_{i=1}^{2n} P_i{}^{C''} \\ &= \bigotimes_{i=1}^{2n} \mathrm{H}^{r_i^C} P_i^B \\ &= \bigotimes_{i=1}^{n} \mathrm{H}^{\frac{1}{3}(c_i^B + c_i^A + 4)} P_i^C \,\Bigg\|\, \bigotimes_{i=n+1}^{2n} \mathrm{H}^{\frac{1}{3}(h_i^B c_i^B + h_i^A c_i^A + 4)} P_i^C \,, \end{aligned} \tag{5}$$

($\mathrm{H}^2 = I$, and applying H twice to single-qubit does nothing to it). Charlie then announces the position information i ($i \leq n$) that satisfies $P_i{}^{C''} = P_i^C$ and $P_{i+n}{}^{C''} \neq P_{i+n}^C$.

Step 8 Alice and Bob get S_{in} based on the results announced by Calvin.

It is worth noting that in Step 3 and Step 5, through exclusive OR calculation, the private information of a participant is randomly encoded in the last n qubits, which prevents participants from getting S_{diff} and avoids the problem of their internal private information leakage.

4 Correctness and Security Analysis

4.1 Correctness Analysis

The corresponding results of $P_i{}^{C''}$ for several paired c_i^A and c_i^B are shown in Table 2. The spectral decomposition form of the H gate can be expressed as $\mathrm{H} = |y_1\rangle\langle y_1| - |y_2\rangle\langle y_2|$, where $|y_1\rangle = \begin{pmatrix} \sqrt{2}-1 \\ 3-2\sqrt{2} \end{pmatrix}$ and $|y_2\rangle = \begin{pmatrix} 3-2\sqrt{2} \\ 1-\sqrt{2} \end{pmatrix}$. We can calculate $\mathrm{H}^{\frac{4}{3}} = |y_1\rangle\langle y_1| + (-1)^{\frac{4}{3}} |y_2\rangle\langle y_2| = I$, and $\mathrm{H}^{\frac{5}{3}} = |y_1\rangle\langle y_1| + (-1)^{\frac{5}{3}} |y_2\rangle\langle y_2| = \mathrm{H}$. Therefore, if $c_i^A = c_i^B$ ($i \leq n$), Calvin can get $P_i{}^{C''} = P_i^C$. Otherwise, $P_i{}^{C''} \neq P_i^C$. If $c_{i+n}^A = c_{i+n}^B = 0$, Calvin can get $P_{i+n}{}^{C''} = P_{i+n}^C$. If $c_{i+n}^A = c_{i+n}^B = 1$, Calvin can get $P_{i+n}{}^{C''} \neq P_{i+n}^C$. If $c_{i+n}^A \neq c_{i+n}^B$, $P_{i+n}{}^{C''}$ and P_{i+n}^C may be equal or not. So, if $P_i{}^{C''} = P_i^C$ and $P_{i+n}{}^{C''} \neq P_{i+n}^C$, the i-th number is the S_{in} element.

We use an example to verify the correctness of the protocol. In this section, insertion of decoy photons and the eavesdropper detection are omitted. Suppose Alice and Bob have private sets $S_A = \{5, 7, 17, 20\}$ and $S_B = \{7, 13, 17, 35\}$, respectively. The universal set is $U = \{2, 5, 7, 9, 13, 17, 20, 35\}$. They encode sets S_A and S_B as $C_A = \{0, 1, 1, 0, 0, 1, 1, 0\}$ and $C_B = \{0, 0, 1, 0, 1, 1, 0, 1\}$, respectively.

Table 2 QPSI protocol results

Case	c_i^A	c_i^B	$P_i{}^{C''}(i \leq n)$	$P_i{}^{C''}(n < i \leq 2n)$
1	0	0	$\mathrm{H}^{\frac{4}{3}} P_i^C$	$\mathrm{H}^{\frac{4}{3}} P_i^C$
2	0	1	$\mathrm{H}^{\frac{5}{3}} P_i^C$	$\mathrm{H}^{\frac{5}{3}} P_i^C / \mathrm{H}^{\frac{4}{3}} P_i^C$
3	1	0	$\mathrm{H}^{\frac{5}{3}} P_i^C$	$\mathrm{H}^{\frac{4}{3}} P_i^C / \mathrm{H}^{\frac{5}{3}} P_i^C$
4	1	1	$\mathrm{H}^2 P_i^C$	$\mathrm{H}^{\frac{5}{3}} P_i^C$

In Step 1, Calvin prepares the quantum sequence $P_C = |101+00-++01+-0-1\rangle$. In Step 3, Alice prepares $R_A = \{3, 6, 4, 2, 4, 1, 9, 7, 3, 6, 4, 2, 4, 1, 9, 7\}$ and $\mathrm{H_A} = \{1, 1, 0, 0, 1, 0, 0, 1\}$. And she executes the H gates on the P_C, she gets

$$\begin{aligned} P_A = \; & \bigotimes_{i=1}^{8} \mathrm{H}^{\frac{1}{3}(c_i^A+2)+r_i^A} P_i^{C1} \Bigg\| \bigotimes_{i=9}^{16} \mathrm{H}^{\frac{1}{3}(h_i^A c_i^A+2)+r_i^A} \\ = \; & \mathrm{H}^{\frac{2}{3}+3}|1\rangle \otimes \mathrm{HH}^{1+6}|0\rangle \otimes \mathrm{H}^{1+4}|1\rangle \otimes \mathrm{H}^{\frac{2}{3}+2}|+\rangle \\ & \otimes \mathrm{H}^{\frac{2}{3}+4}|0\rangle \otimes \mathrm{H}^{1+1}|0\rangle \otimes \mathrm{H}^{1+9}|-\rangle \otimes \mathrm{H}^{\frac{2}{3}+7}|+\rangle \\ & \otimes \mathrm{H}^{3}|+\rangle \otimes \mathrm{H}^{\frac{5}{3}+5}|0\rangle \otimes \mathrm{H}^{6}|1\rangle \otimes \mathrm{H}|+\rangle \\ & \otimes \mathrm{H}^{3}|-\rangle \otimes \mathrm{H}^{9}|0\rangle \otimes \mathrm{H}^{2}|-\rangle \otimes \mathrm{H}^{4}|1\rangle . \end{aligned} \tag{6}$$

In Step 5, Bob prepares random numbers $R_B = \{7, 9, 8, 5, 4, 2, 3, 6, 7, 9, 8, 5, 4, 2, 3, 6\}$. He calculates $\mathrm{H_B} = \{0, 0, 1, 1, 0, 1, 1, 0\}$ and executes the H gates on the P_A. He gets:

$$\begin{aligned} P_B = \; & \bigotimes_{i=1}^{8} \mathrm{H}^{\frac{1}{3}(c_i^B+c_i^A+4)+r_i^B+r_i^A} P_i^{C} \Bigg\| \bigotimes_{i=9}^{16} \mathrm{H}^{\frac{1}{3}(h_i^B c_i^B+h_i^A c_i^A+4)+r_i^B+r_i^A} P_i^{C} \\ = \; & \mathrm{H}^{\frac{4}{3}+10}|1\rangle \otimes \mathrm{H}^{\frac{5}{3}+15}|0\rangle \otimes \mathrm{H}^{2+12}|1\rangle \otimes \mathrm{H}^{\frac{4}{3}+7}|+\rangle \\ & \otimes \mathrm{H}^{\frac{5}{3}+8}|0\rangle \otimes \mathrm{H}^{2+3}|0\rangle \otimes \mathrm{H}^{\frac{5}{3}+12}|-\rangle \otimes \mathrm{H}^{\frac{5}{3}+13}|+\rangle \\ & \otimes \mathrm{H}^{\frac{4}{3}+4}|+\rangle \otimes \mathrm{H}^{\frac{5}{3}+8}|0\rangle \otimes \mathrm{H}^{\frac{5}{3}+11}|1\rangle \otimes \mathrm{H}^{\frac{4}{3}+3}|+\rangle \\ & \otimes \mathrm{H}^{\frac{4}{3}+7}|-\rangle \otimes \mathrm{H}^{\frac{5}{3}+12}|0\rangle \otimes \mathrm{H}^{\frac{4}{3}+8}|-\rangle \otimes \mathrm{H}^{\frac{4}{3}+13}|1\rangle . \end{aligned} \tag{7}$$

In Step 7, Alice and Bob calculate $r_i^C = r_i^A + r_i^B$ and send the results to Calvin. Calvin gets:

$$\begin{aligned} P_C{}'' = \; & \bigotimes_{i=1}^{n} \mathrm{H}^{r_i^C} P_i^B \\ = \; & \mathrm{H}^{10}\mathrm{H}^{\frac{4}{3}+10}|1\rangle \otimes \mathrm{H}^{15}\mathrm{H}^{\frac{5}{3}+15}|0\rangle \otimes \mathrm{H}^{12}\mathrm{H}^{2+12}|1\rangle \otimes \mathrm{H}^{7}\mathrm{H}^{\frac{4}{3}+7}|+\rangle \\ & \otimes \mathrm{H}^{8}\mathrm{H}^{\frac{5}{3}+8}|0\rangle \otimes \mathrm{H}^{3}\mathrm{H}^{2+3}|0\rangle \otimes \mathrm{H}^{12}\mathrm{H}^{\frac{5}{3}+12}| \text{-} \rangle \otimes \mathrm{H}^{13}\mathrm{H}^{\frac{5}{3}+13}|+\rangle \\ & \otimes \mathrm{H}^{4}\mathrm{H}^{\frac{4}{3}+4}|+\rangle \otimes \mathrm{H}^{8}\mathrm{H}^{\frac{5}{3}+8}|0\rangle \otimes \mathrm{H}^{11}\mathrm{H}^{\frac{5}{3}+11}|1\rangle \otimes \mathrm{H}^{3}\mathrm{H}^{\frac{4}{3}+3}|+\rangle \\ & \otimes \mathrm{H}^{7}\mathrm{H}^{\frac{4}{3}+7}|-\rangle \otimes \mathrm{H}^{12}\mathrm{H}^{\frac{5}{3}+12}|0\rangle \otimes \mathrm{H}^{8}\mathrm{H}^{\frac{4}{3}+8}|-\rangle \otimes \mathrm{H}^{13}\mathrm{H}^{\frac{4}{3}+13}|1\rangle \\ = \; & \mathrm{H}^{\frac{4}{3}}|1\rangle \otimes \mathrm{H}^{\frac{5}{3}}|0\rangle \otimes |1\rangle \otimes \mathrm{H}^{\frac{4}{3}}|+\rangle \\ & \otimes \mathrm{H}^{\frac{5}{3}}|0\rangle \otimes |0\rangle \otimes \mathrm{H}^{\frac{5}{3}}| \text{-} \rangle \otimes \mathrm{H}^{\frac{5}{3}}|+\rangle \\ & \otimes \mathrm{H}^{\frac{4}{3}}|+\rangle \otimes \mathrm{H}^{\frac{5}{3}}|0\rangle \otimes \mathrm{H}^{\frac{5}{3}}|1\rangle \otimes \mathrm{H}^{\frac{4}{3}}|+\rangle \\ & \otimes \mathrm{H}^{\frac{4}{3}}|-\rangle \otimes \mathrm{H}^{\frac{5}{3}}|0\rangle \otimes \mathrm{H}^{\frac{4}{3}}|-\rangle \otimes \mathrm{H}^{\frac{4}{3}}|1\rangle \\ = \; & |1\rangle \otimes \mathrm{H}|0\rangle \otimes |1\rangle \otimes |+\rangle \otimes \mathrm{H}|0\rangle \otimes |0\rangle \otimes \mathrm{H}| \text{-} \rangle \otimes \mathrm{H}|+\rangle \\ & \otimes |+\rangle \otimes \mathrm{H}|0\rangle \otimes \mathrm{H}|1\rangle \otimes |+\rangle \otimes |-\rangle \otimes \mathrm{H}|0\rangle \otimes |-\rangle \otimes |1\rangle . \end{aligned} \tag{8}$$

He obtains $P_1{}^{C''} = P_1^C$, $P_3{}^{C''} = P_3^C$, $P_4{}^{C''} = P_4^C$, $P_6{}^{C''} = P_6^C$, $P_{10}^C \neq P_{10}{}^{C''}$, $P_{11}^C \neq P_{11}{}^{C''}$, $P_{14}^C \neq P_{14}{}^{C''}$. Calvin gets the 3rd and 6th position to meet the conditions and announces it to Alice and Bob. In the end, Alice and Bob get $S_{in} = \{7, 17\}$.

4.2 Security Analysis

In this section, we conduct security analysis from two aspects: participant attack and outside attack.

4.2.1 Participant Attack

Participant attack [20, 21] means that dishonest participants try to steal other's information during the calculation process, which will lead to the leakage of private information inside the participants. Ensuring the internal information security of participants is one of the important criteria for evaluating the security of the protocol.

Case 1: Alice tries to steal Bob's private information.

During the protocol process, Alice can only receive the quantum sequence $P_C = \overset{n}{\underset{i=1}{\otimes}} P_i^C$ sent by Calvin, and P_i^C is randomly determined by Calvin, so Alice cannot obtain Bob's private information in this case.

At the end of the protocol, Alice gets the information of $c_i^A = c_i^B = 1$, and then gets S_{in}. In other cases, she does not know whether the element satisfies $c_i^A = c_i^B = 0$ or $c_i^A \neq c_i^B$, so she cannot deduce $c_i^B = 1$ and cannot obtain Bob's private information outside S_{in}.

Case 2: Bob tries to steal Alice's private information.

Bob gets sequence P_A (as shown in (3)) after receiving the decoy photon information published by Alice. If dishonest Bob wants to use the measure-resend attack to get Alice's private information, he prepares the ancillary qubits $|0\rangle_B^n$ and entangles Alice's quantum sequence P_i^A that has been received with the ancillary qubits. He wants to get Alice's private information c_i^A by measuring the ancillary qubits sequence. After receiving P_i^A, Bob uses the unitary operator $\tilde{U}_{AB}$ to operate on P_i^A and $|0\rangle_B^n$. According to Ref. [22], Bob's attack process is as follows:

$$\tilde{U}_{AB} P_i^A \, |0\rangle_B^n = \sqrt{\eta} P_i^A \left| u\left(P_i^A\right)\right\rangle + \sqrt{1-\eta} \left| v\left(P_i^A\right)\right\rangle_{AB}, \tag{9}$$

where $P_i^A \left| u\left(P_i^A\right)\right\rangle$ and $\left| v\left(P_i^A\right)\right\rangle_{AB}$ are orthogonal vectors.

$$\left\langle v\left(P_i^A\right)\right|_{AB} P_i^A \left| u\left(P_i^A\right)\right\rangle = 0. \tag{10}$$

In order to successfully pass the eavesdropping detection stage, Eve's operation will not change the state of the original photon, so η should be equal to 1. He can get:

$$\begin{aligned} \tilde{U}_{AB} P_i^A \, |0\rangle_B^n &= P_i^A \left| u\left(P_i^A\right)\right\rangle \\ &= \mathrm{H}^{\frac{1}{3}\left(h_i^A c_i^A+2\right)+r_i^A} P_i^C \left| u\left(P_i^A\right)\right\rangle \\ &= \begin{cases} \mathrm{H}^{\frac{2}{3}+r_i^A} P_i^C \left| u\left(P_i^A\right)\right\rangle, if c_i^A = 0 \\ \mathrm{H}^{1+r_i^A} P_i^C \left| u\left(P_i^A\right)\right\rangle, if c_i^A = 1 \, . \end{cases} \end{aligned} \tag{11}$$

Bob cannot extract the global phase information from the partial qubits of the entangled quantum, so he cannot obtain any information about Alice.

At the end of the protocol, Bob gets the information of $c_i^A = c_i^B = 1$ and gets S_{in}. In other cases, similar to Alice, he does not know whether the element satisfies $c_i^A = c_i^B = 0$ or $c_i^A \neq c_i^B$, so he cannot deduce $c_i^A = 1$ and cannot obtain Alice's private information outside S_{in}.

Case 3: Calvin tries to steal Alice's and Bob's private information.

After Calvin receives the decoy photon information published by Bob, he gets the sequence P_B.

$$P_B = \overset{n}{\underset{i=1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(c_i^B+2\right)} \mathrm{H}^{r_i^B} P_i^A \left\| \overset{2n}{\underset{i=n+1}{\otimes}} \mathrm{H}^{\frac{1}{3}\left(h_i^B c_i^B+2\right)} \mathrm{H}^{r_i^B} P_i^A \right. . \tag{12}$$

Calvin receives r_i^C and operates on sequence P_B to get the new sequence $P_C{}''$.

$$P_C{}'' = \bigotimes_{i=1}^{n} \mathrm{H}^{\frac{1}{3}\left(c_i^B + c_i^A + 4\right)} P_i^C \, \Big\| \bigotimes_{i=n+1}^{2n} \mathrm{H}^{\frac{1}{3}\left(h_i^B c_i^B + h_i^A c_i^A + 4\right)} P_i^C \ . \tag{13}$$

Because the last n qubits information is randomly determined by Alice and Bob, Charlie can only infer the private information of Alice and Bob based on the first n qubits. If $P_i{}^{C''} \neq P_i^C$ $(i \leq n)$, Calvin can deduce that the i-th position element is in the private set of Alice or Bob (i.e. $c_i^A = 1$ or $c_i^B = 1$), but he is not sure which one. Therefore, Calvin cannot obtain all the private information of Alice or Bob, and the protocol satisfies privacy.

4.2.2 Outside Attack

At present, the common quantum channel attacks include intercept-measuring-retransmission attack, Trojan horse attack [23], man-in-the-middle attack [24], invisible photon attack [25], etc. In the communication between the two parties, the third-party attacker Eve is the object with strong attack ability, and its eavesdropping technology is only limited by the basic principles of quantum mechanics. The decoy photon eavesdropping detection method [26, 27] is an important method to detect whether there is eavesdropping in the quantum communication process. Its safety has been proved in refs [28].

In our protocol, the external attacker Eve can attack the quantum channel during the transmission of the photon sequence between Calvin, Alice and Bob. In these steps, the participants insert some particles into the quantum sequence in the form of decoy states. Take the information transfer between Calvin and Alice in Step 1 to Step 2 as an example. When Calvin sends the quantum sequence inserted into the decoy photon to Alice, if Eve launches an attack, he will inevitably change the original sequence after stealing the information. After receiving the quantum sequence, Alice can judge whether there is a malicious attack based on the position information of the decoy photon and the measurement base information given by Calvin.

5 Conclusion

In this paper, we point out the problem of private information leakage between participants in the NQPSI protocol [14]. To solve this problem, we propose an improved QPSI protocol based on H gates. We use the more feasible H gates to replace the original quantum Fourier transform, which may reduce the difficulty of the protocol implementation. Through the exclusive OR calculation on the last n qubits, this scheme ensures that participants cannot get S_{diff}, which prevents them from getting the private information of the others outside S_{in}. It is worth noting that if the third party is malicious or there is an error in the protocol process, the participant will get wrong results without knowing it. In this regard, attention should be paid to the verifiability of QPSC and the integrity of third parties. At present, the verifiable blind quantum computing framework based on the idea of delegating private computations [29] has attracted much attention. We believe that learning from this idea to solve the PSC problem is a feasible way.

Acknowledgements The authors would like to thank the anonymous reviewers and editors for their comments that improved the quality of this paper. This work is supported by the National Natural Science Foundation of China (62071240, 61802002), and the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD).

Declarations

Ethics statement Articles do not rely on clinical trials.

Human and animal participants All submitted manuscripts containing research which does not involve human participants and/or animal experimentation.

Conflict of Interests The authors declare that they have no conflict of interest.

References

1. Yao, A.C.: Protocols for secure computations. Symp. Found. Comput. Sci. (FOCS). **23**, 160–164 (1982)
2. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. Symp. Found. Comput. Sci. (FOCS). **35**, 124–134 (1994)
3. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325–328 (1997)
4. Xu, Y.S., Liu, W.J., Yu, W.: Quantum forgery attacks on COPA, AES-COPA and marble authenticated encryption algorithms. Quantum Inf. Process. **20**(4), 131 (2021)
5. Liu, W.J., Xu, Y., Yang, C.N., et al.: An efficient and secure arbitrary N-Party quantum key agreement protocol using bell states. Int. J. Theor. Phys. **57**(1), 195–207 (2018)
6. Liu, W.J., Li, C.T., Zheng, Y., et al.: Quantum Privacy-Preserving price E-Negotiation. Int. J. Theor. Phys. **58**(10), 3259–3270 (2019)
7. Wooters, W.K., Zurek, W.K.: Quantum no-cloning theorem. Nature, 299 (1982)
8. Folland, G.B., Sitaram, A.: The uncertainty principle: A mathematical survey. J. Fourier Anal. Appl. **3**(3), 207–238 (1997)
9. Mayers, D.: Unconditional security in quantum cryptography. ACM. https://doi.org/10.1145/382780.382781 (1998)
10. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: An efficient quantum scheme for Private Set Intersection. Quantum Inf. Process. **15**(1), 363–371 (2016)
11. Cheng, X., Guo, R., Chen, Y.: Cryptanalysis and improvement of a quantum private set intersection protocol. Quantum Inf. Process. **16**(2), 37 (2016)
12. Maitra, A.: Quantum secure two-party computation for set intersection with rational players. Quantum Inf. Process. **17**(8), 197 (2018)
13. Debnath, S.K., Dey, K., Kundu, N., et al.: Feasible private set intersection in quantum domain. Quantum Inf. Process. **20**(1), 41 (2021)
14. Liu, W., Yin, H.W.: A novel quantum protocol for private set intersection. Int. J. Theor. Phys. **60**, 2074–2083 (2021)
15. Shi, R.H.: Quantum Private Computation of Cardinality of Set Intersection and union.The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics. https://doi.org/10.1140/epjd/e2018-90380-7 (2018)
16. Shi, R.H.: Efficient quantum protocol for private set intersection cardinality. IEEE Access. **99**, 1–1 (2018)
17. Shi, R.H., Zhang, M.: A feasible quantum protocol for private set intersection cardinality. IEEE Access. **7**, 72105–72112 (2019)
18. Liu, B., Zhang, M.W., Shi, R.H.: Quantum secure multi-party private set intersection cardinality. Int. J. Theor. Phys. **59**, 1992–2007 (2020)
19. Shi, R.H., Mu, Y., Zhong, H., Zhang, S.: Quantum oblivious set-member decision protocol. Phys. Rev. A. **92**(2), 5 (2015)
20. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inform. Comput. **7**(4), 329–334 (2007)
21. Song, T.T., Wen, Q.Y., Gao, F., et al.: Participant attack and improvement to multiparty quantum secret sharing based on GHZ states. Int. J. Theor. Phys. **52**(1), 293–301 (2013)
22. Li, L., Shi, R.H.: A novel and efficient quantum private comparison scheme. J. Korean Phys. Soc. **75**(1), 15–21 (2019)
23. Deng, F.G., Han, X., et al.: Erratum: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A. **73**(4), 49901–49901 (2006)

24. Peev, M., Pacher, C., Lorunser, T., et al.: Response to “Vulnerability of ’A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography’ ”. Int. J. Quantum Inf. **07**(7), 1401 (2009)
25. Kye, W.H., Kim, C.M., Kim, M.S., et al.: Security against the invisible photon attack for the quantum key distribution with blind polarization bases. Phys. Rev. Lett. **95**(4), 040501 (2005)
26. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**(23), 230504 (2005)
27. Ma, X., Qi, B., Zhao, Y., et al.: Practical decoy state for quantum key distribution. Phys. Rev. A. **72**(1), 1–127 (2005)
28. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin. Phys. Lett. **30**(4), 40305–040305 (2013)
29. Liu, W.J., Chen, Z.Y., Liu, J.S., et al.: Full-Blind Delegating private quantum computation. CMC-Computers Materials and Continua **56**(2), 211–223 (2018)