International Journal of Theoretical Physics (2021) 60:2074–2083
https://doi.org/10.1007/s10773-021-04824-x

A Novel Quantum Protocol for Private Set Intersection

Wen Liu[1,2,3] · **Han-Wen Yin**[1,2,3]

Received: 4 January 2021 / Accepted: 28 April 2021 / Published online: 12 May 2021

Abstract
Private set intersection(PSI) allows two parties to get all common elements of their private sets without leaking any information about their sets. In this paper, we present a novel PSI protocol which is based on quantum Fourier transform. Correctness analysis shows that our protocol can get the result correctly. And the security of our protocol is also analyzed, it can resist most of outside attacks, such as Trojan horse attack, intercept-resend attack, entanglement-and-measure attack, man-in-the-middle attack and so on. And it also can overcome participant attacks.

Keywords Secure multiparty quantum computation · Private set intersection · Quantum fourier transform

1 Introduction

Protocols for private set intersection (PSI) allow two parties to compute the intersection $S_1 \cap S_2$ of their respective sets S_1, S_2 without disclosing anything about their sets [1]. PSI is an important problem of secure multi-party computation(SMC) and has many practical applications. It can be used to find the common customers of two companies directly [2] or perform scientific investigation of two hospitals on their private patients data [3]. It can also be used as a sub-protocol to perform privacy preserving data mining [4], to execute search queries of the outsourced data [5] and to test whether two parties are close or not [6].

Because PSI has a wide application, many protocols have been proposed based on classical cryptography. In Ref. [1], Freedman, M.J. et al. presented PSI protocols based on homomorphic encryption and balanced hashing. In Ref. [7], Wu et al. proposed a PSI scheme based on oblivious transfer and universal hash function. In Ref. [8], Hazay, C., Lindell, Y. constructed a PSI protocol based on secure pseudorandom function evaluations. In Ref. [9], Liu, L., Cao, Z. investigated an efficient private matching protocol which can be

✉ Wen Liu
lw_8206@163.com

[1] State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing, China

[2] School of Computer Science and cybersecurity, Communication University of China, Beijing, China

[3] Key Laboratory of Convergent Media and Intelligent Technology Communication University of China, Ministry of Education, Beijing, China

used in some scenarios without strong security requirement. In Ref. [10], Kerschbaum, F. presented a novel PSI protocol of malicious adversaries model based on Bloom filter and homomorphic encryption. In Ref. [11], Shao, Z.Y., Yan, B. obtained a novel approach to accomplish PSI, which used the public key encryption with keywords search.

Shor pointed out that SMC tasks can be performed more efficiently by models based on quantum setting than classical setting [12]. Many researchers explored the special SMC problems based on quantum cryptography Ref. [13–21]. But there are only few quantum schemes for PSI and its variants. In Ref. [22], Shi, R.H. et al. proposed a novel quantum scheme for PSI, which required $O(n)$ computation and communication complexities. In Ref. [23], Shi, R.H. et al. solved PSI cardinality problem using a quantum approach, which can achieve an exponential reduction in communication complexity. In Ref. [24], Shi, R.H. presented a novel quantum approach to solve PSI cardinality and private set union cardinality problems based on the principle of quantum mechanics, which can resist well-known quantum attacks. In this work, we use quantum Fourier transform approach to perform PSI. Our scheme only needs orbital angular momentum(OAM) basis, so it will be more practical than the schemes using multiple particles.

The structure of our paper is as follows: we introduce some preliminary in Section 2; we propose a PSI protocol based on a coding scheme and quantum Fourier transform in Section 3; and we analyze the correctness and security of our protocol in Section 4. A brief discussion and a concluding summary are given in Section 5.

2 Preliminary

2.1 Quantum Fourier Transform

There are two bases, Z-basis and X-basis. Z-basis can be expressed as $\{|j\rangle, j = -N, ..., 0, ..., N\}$, where N is a positive integer. X-basis can be expressed as $\{QFT\,|j\rangle, j = -N, ..., 0, ..., N\}$

Quantum Fourier transform performed on $|j\rangle$ in the Z basis can be described as $QFT\,|j\rangle = \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{jk} |k\rangle (j = -N, ..., 0, ..., N)$, where $\omega = e^{\frac{2\pi i}{2N+1}}$. We have $\omega^{2N+1} = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$ and $\sum_{k=-N}^{N} \omega^k = \frac{\omega^{-N}(1-\omega^{2N+1})}{1-\omega} = \frac{\omega^{-N}(1-1)}{1-\omega} = 0$.

For Z basis, we can get

$$
\begin{aligned}
QFT^2(|j\rangle) &= \tfrac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{jk} \left(\tfrac{1}{\sqrt{2N+1}} \sum_{l=-N}^{-N} \omega^{kl} |l\rangle \right) \\
&= \tfrac{1}{2N+1} \sum_{k=-N}^{N} \omega^{jk} \left(\sum_{l=-N}^{-N} \omega^{kl} |l\rangle \right) \\
&= \tfrac{1}{2N+1} \sum_{k=-N}^{N} \sum_{l=-N}^{N} \omega^{k(j+l)} |l\rangle \\
&= \tfrac{1}{2N+1} \sum_{k=-N}^{N} \sum_{l=-N}^{N} \omega^{k(j+l)} |l\rangle \\
&= \tfrac{1}{2N+1} \sum_{k=-N}^{N} \omega^{k(j-j)} |-j\rangle + \tfrac{1}{2N+1} \sum_{k=-N}^{N} \sum_{l=-N \wedge l \neq -j}^{N} \omega^{k(j+l)} |l\rangle \\
&= \tfrac{1}{2N+1} \sum_{k=-N}^{N} 1 \times |-j\rangle + \tfrac{1}{2N+1} \sum_{l=-N \wedge l \neq j}^{N} (0 \times |l\rangle) \\
&= |-j\rangle .
\end{aligned}
\tag{1}
$$

Then we can also get $QFT^4(|j\rangle) = |j\rangle$ [25].

3 Proposed Protocol

In this section we firstly give an informal definition of PSI and then present a PSI protocol using quantum Fourier transform.

Definition 1 Private Set Intersection(PSI)—-There are two parties, Alice and Bob. Supposed that $U = \{x_1, x_2, ..., x_n\}$ is a complete set. Alice inputs a private set $S_A = \left\{s_1^A, s_2^A, ..., s_{l_A}^A\right\}$ and Bob inputs a private set $S_B = \left\{s_1^B, s_2^B, ..., s_{l_B}^B\right\}$, where $S_A, S_B \subseteq U$. With the help of a semi-honest third party Calvin, Alice and Bob can get the intersection $S_A \cap S_B$ without leaking any information about their private sets.

Alice and Bob decode their private sets S_A, S_B into two $0-1$ sequences $C_A = \left(c_1^A, c_2^A, ..., c_n^A\right)$, $C_B = \left(c_1^B, c_2^B, ..., c_n^B\right)$:

$$\begin{cases} c_i^A = 1, & if\ x_i \in S_A \\ c_i^A = 0, & if\ x_i \notin S_A \end{cases} \quad \begin{cases} c_i^B = 1, & if\ x_i \in S_B \\ c_i^B = 0, & if\ x_i \notin S_B \end{cases} \tag{2}$$

The detailed quantum PSI protocol is described as follows:

(1) Calvin prepares a particles sequence $P_C = \left(p_1^C, p_2^C, ..., p_n^C\right)$ and $p_i^C (i = 1, 2, ..., n)$ is randomly chosen from $\{|-N\rangle, ..., |-1\rangle, |1\rangle, ..., |N\rangle\}$. He also inserts l_C particles into P_C for each particle in Z-basis and X-basis. After recording the insert positions Po_C, Calvin sends the sequence P_C' of $(n + l_C)$ particles to Alice.

(2) After receiving P_C', Calvin announces Po_C and measuring basis. Calvin and Alice measure those insert particles and can find the existence of an eavesdropper. If there are cheaters, the scheme will be aborted. Otherwise, Alice discards the insert photons in P_C' and continues the next step.

(3) Alice prepares two n-length strings $R_A = \left(r_1^A, r_2^A, ..., r_{n+l}^A\right)$ and $H_A = \left(h_1^A, h_2^A, ..., h_{n+l}^A\right)$, where $r_i^A (i = 1, ..., n)$ is randomly chosen from $\{0, 1\}$ and $h_i^A (i = 1, ..., n)$ is a random positive integer. Then she calculates $p_i^A = QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} p_i^C (i = 1, 2, ..., n)$. If $r_i^A = 0, r_i^A \times h_i^A = 0$, then Alice performs no quantum Fourier transform; If $r_i^A = 1, r_i^A \times h_i^A = h_i^A$, then Alice performs h_i^A quantum Fourier transform. The new particles sequence is denoted by $P_A = \left(p_1^A, p_2^A, ..., p_n^A\right)$.

Alice also inserts l_A particles into P_A for each particle in Z-basis and X-basis. After recording the insert positions Po_A, the sequence P_A' of $(n + l_A)$ particles will be sent to Bob.

(4) After receiving P_A', Alice announces Po_A and measuring basis. Alice and Bob measure those insert particles to find the existence of an eavesdropper. If there is a cheater, the scheme will be aborted. Otherwise, Bob discards the insert photons in P_A' and continues the next step.

(5) Bob prepares two (n)-length strings $R_B = \left(r_1^B, r_2^B, ..., r_n^B\right)$ and $H_B = \left(h_1^B, h_2^B, ..., h_n^B\right)$, where $r_i^B (i = 1, ..., n)$ is randomly chosen from $\{0, 1\}$ and $h_i^B (i = 1, ..., n)$ is a random integer. Then he calculates $p_i^B = QFT^{c_i^B \times 2} QFT^{r_i^B \times h_i^B}\ p_i^A (i = 1, 2, ..., n)$. If $r_i^B = 0, r_i^B \times h_i^B = 0$, then Bob performs no quantum Fourier transform; If $r_i^B = 1, r_i^B \times h_i^B = h_i^B$, then Bob performs h_i^B quantum Fourier transform. The new particles sequence is denoted by $P_B = \left(p_1^B, p_2^B, ..., p_n^B\right)$.

Bob also inserts l_B particles into P_B for each particle in Z-basis and X-basis. After recording the insert positions Po_B, he sends the sequence P'_B of $(n + l_B)$ particles to Calvin.

(6) After receiving P'_B, Bob announces Po_B and and measuring basis. Bob and Calvin measure those insert particles to find the existence of an eavesdropper. If there is a cheater, the scheme will be aborted. Otherwise, Calvin discards the insert photons in P'_B and continues the next step.

(7) Alice and Bob compute $h_i^C = 4 - (\left(\left(r_i^A \times h_i^A\right) + \left(r_i^B \times h_i^B\right)\right) \mod 4)(i = 1, ..., n)$ and send $h_1^C, ..., h_n^C$ to Calvin.

Calvin calculates $p_i^{C'} = QFT^{h_i^C} p_i^B (i = 1, 2, ..., n)$ and measures it using $\{|-N\rangle, ..., |0\rangle, ..., |N\rangle\}$. If the measurement result of $p_i^{C'}$ is the same as p_i^C, Calvin know that $c_i^A = c_i^B$; Otherwise, Calvin knows that $c_i^A \neq c_i^B$. Calvin get $S_A \cap S_B$.

4 Analysis

4.1 Correctness Analysis

In this section, we verify the correctness of the protocol by taking a concrete example.

In our protocol, Alice performs $r_i^A \times h_i^A$ quantum Fourier transform on p_i^C in step (3); Bob performs $r_i^B \times h_i^B$ quantum Fourier transform on p_i^C in step(3); Calvin performs $h_i^C = 4 - (((r_i^A \times h_i^A) + (r_i^B \times h_i^B)) \mod 4)$ quantum Fourier transform on p_i^C in step(7). In Section 2, we know that the particle p_i^C will not change if it has been performed on four quantum Fourier transforms. So Alice, Bob and Calvin have no effects on p_i^C.

Then the particle $p_i^{C'}(i = 1, 2, ..., n)$ in step (7) is written as follows:

$$\begin{aligned} p_i^{C'} &= QFT^{h_i^C} QFT^{c_i^B \times 2} QFT^{r_i^B \times h_i^B} QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} p_i^C \\ &= QFT^{h_i^C + r_i^B \times h_i^B + r_i^A \times h_i^A} QFT^{\left(c_i^B + c_i^A\right) \times 2} p_i^C \\ &= QFT^{4k} QFT^{\left(c_i^B + c_i^A\right) \times 2} p_i^C \\ &= QFT^{\left(c_i^B + c_i^A\right) \times 2} p_i^C \end{aligned} \tag{3}$$

Alice and Bob perform $\left(c_i^A + c_i^B\right) \times 2$ quantum Fourier transform on p_i^C. If $c_i^A = c_i^B = 0$ or $c_i^A = c_i^B = 1$, Alice and Bob will perform zero or four quantum Fourier transform on p_i^C and the particle p_i^C will not change. If $c_i^A = 1, c_i^B = 0$ or $c_i^A = 0, c_i^B = 1$, Alice and Bob will perform two quantum Fourier transform on p_i^C and the particle p_i^C will change. When Calvin measures p_i^C, he can know whether c_i^A, c_i^B are equal or not by comparing the measurement result and the original particle. Alice and Bob discard l results which are used to protect U and determine $S_A \cap S_B$.

We give an example throughout the protocol to proof the correctness of our protocol. Supposed that $U = \{3, 4, 12\}$ and OAM basis is $\{|-2\rangle, |-1\rangle, |0\rangle, |1\rangle, |2\rangle\}$. Alice has a private set $S_A = \{3, 12\}$ and Bob has a private set $S_B = \{4, 12\}$, and their 0-1 codes are (1,0,1) and (0,1,1) respectively. The random strings chosen by Alice are $R_A = (1, 0, 0), H_A = (4, 2, 2)$. The random strings chosen by Bob are $R_B = (0, 1, 0), H_B = (2, 1, 5)$. Calvin prepares a particles sequence $P_C = \left(p_1^C, p_2^C, p_3^C\right) = (|2\rangle, |-2\rangle, |2\rangle)$.

According to R_A, H_A and the $0 - 1$ code of Alice, Alice performs four quantum Fourier transform on p_1^C firstly, then performs two quantum Fourier transform on

p_1^C, p_3^C. The new particles sequence generated by Alice is $P_A = \left(p_1^A, p_2^A, p_3^A\right) = (QFT^6 |2\rangle, |-2\rangle, QFT^2 |2\rangle)$.

Similarly, according to R_B, H_B and the $0-1$ code of Bob, Bob performs one quantum Fourier transform on p_2^A firstly, then performs two quantum Fourier transform on p_2^A, p_3^A. The new particles sequence generated by Bob is $P_B = \left(p_1^B, p_2^B, p_3^B\right) = (QFT^6 |2\rangle, QFT^3 |-2\rangle, QFT^4 |2\rangle)$.

According to $H_C = (4, 3, 0)$, Calvin performs three quantum Fourier transform on p_2^B, performs four quantum Fourier transform on p_1^B, performs no quantum Fourier transform on p_3^B. The new particles sequence of Calvin is $P_C' = \left(p_1^{C'}, p_2^{C'}, p_3^{C'}\right) = (QFT^{10} |2\rangle, QFT^6 |-2\rangle, QFT^4 |2\rangle) = (|-2\rangle, |2\rangle, |2\rangle)$. Calvin compares P_C and P_C'. He can knows that only the 5th particle is equal and others particles are not. Alice and Bob know $S_A \cap S_B = \{12\}$.

4.2 Security Analysis

Firstly, we show that the outside attack is invalid to our protocol. Secondly, we show that Alice and Bob can not get any information about the private information of each other.

4.2.1 Outside Attack

In this protocol, the outside eavesdroppers can attack the quantum channel and get particles sequences of Alice, Bob and Calvin in step (1)(3)(5). In order to resist outside attacks, there are some checking particles inserted by Alice, Bob and Calvin. The intercept-resend attack, the measurement-resend attack, entanglement- measure attack and the denial-of-service (DOS) attack can be detected with nonzero probability during the security checking process in step (2)(4)(6).

Outside eavesdroppers can also adopt some special attacks, such as the delay photon Trojan horse attack, the invisible photon eavesdropping (IPE) Trojan horse attack, the photon-number-splitting (PNS) attack. In order to defeat delay-photon Trojan horse attack, we can use a photon-number splitter. In order to defeat IPE attack, we can insert filters in front of their devices to filter out the photon signal with an illegitimate wavelength. In order to defeat PNS attack, we can use the technology of beam splitters to split the sampling signals and judge whether these received photons are single photons or multiple photons.

In step (7)(8), Alice, Bob and Calvin need to transfer some classical information, which is not relevant to the private sets S_A, S_B. Therefore, outside eavesdropper cannot deduce the private sets S_A, S_B from these classical information..

So we can say the protocol is security under the outside attack.

4.2.2 Participant Attack

The term "participant attack", which emphasizes that the attacks from dishonest users are generally more powerful and should be paid more attention to, is first proposed by Gao et al. in Ref. [26] and has attracted much attention in the cryptanalysis of quantum cryptography [27–33]. We analyze the possibility of three parties, Alice, Bob and Calvin, to get information about S_A, S_B in our protocol.

Case 1: Alice wants to learn Bob's private set $S_B = \left\{s_1^B, s_2^B, ..., s_{l_B}^B\right\}$.

In our protocol, Alice only gets a particles sequence $P_C = \left(p_1^C, p_2^C, ..., p_n^C\right)$, which is randomly chosen by Calvin. These particles didn't have any secret information about the Bob's input S_B. So for Alice, all possible attacks which she can perform with the present technology can not help her to eavesdrop Bob's secret set.

Case 2: Bob wants to learn Alice's private set $S_A = \left\{s_1^A, s_2^A, ..., s_{l_A}^A\right\}$.

In our protocol, Bob's legal resource in his hand is the sequence $P_A = \left(p_1^A, p_2^A, ..., p_n^A\right)$, where $p_i^A = QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} p_i^C (i = 1, 2, ..., n)$ and c_i^A is related to Alice's private set. Bob's eavesdropping is carried out by an unitary operation $\widehat{U_{AB}}$, which acts on $p_i^A = |j\rangle_A$ and an ancillary particle $|0\rangle_B$. Using the similar analysis in [34], the effect of Bob's attack can be described using the following equations:

$$\widehat{U_{AB}} |j\rangle_A |0\rangle_B = \sqrt{\eta_j} |j\rangle_A |\phi(j)\rangle_B + \sqrt{1-\eta_j} |V(j)\rangle_{AB} . \tag{4}$$

where $|V(j)\rangle_{AB}$ is a vector orthogonal to $|j\rangle_A |\phi(j)\rangle_B$.

In order to pass the eavesdropping checking, it can easily deduce $\eta_j = 1$. After perform $\widehat{U_{AB}}$, the particle $p_i^A (i = 1, 2, ..., n + l)$ in P_A should be in the following state:

$$\begin{aligned}
&\widehat{U_{AB}} p_i^A |0\rangle_B \\
&= \widehat{U_{AB}} QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} |j\rangle_A |0\rangle_B \\
&= \begin{cases}
\left(\frac{1}{\sqrt{2N+1}}\right)^{2+h_i^A} \sum_{k_1=-N}^{-N} \sum_{k_2=-N}^{-N} ... \sum_{k_{(2+h_i^A)}=-N}^{-N} \omega^{jk_1+k_1k_2+...+k_{1+h_i^A}k_{2+h_i^A}} \left|k_{2+h_i^A}\right\rangle_A |\phi(j)\rangle_B & \left(c_i^A = 1, r_i^A = 1\right) \\
\left(\frac{1}{\sqrt{2N+1}}\right)^{h_i^A} \sum_{k_1=-N}^{-N} \sum_{k_2=-N}^{-N} ... \sum_{k_{(h_i^A)}=-N}^{-N} \omega^{jk_1+k_1k_2+...+k_{h_i^A-1}k_{h_i^A}} \left|k_{h_i^A}\right\rangle_A |\phi(j)\rangle_B & \left(c_i^A = 0, r_i^A = 1\right) \\
\left(\frac{1}{\sqrt{2N+1}}\right)^2 \sum_{k_1=-N}^{-N} \sum_{k_2=-N}^{-N} \omega^{jk_1+k_1k_2} |k_2\rangle_A |\phi(j)\rangle_B & \left(c_i^A = 1, r_i^A = 0\right) \\
|j\rangle_A |\phi(j)\rangle_B & \left(c_i^A = 0, r_i^A = 0\right)
\end{cases}
\end{aligned} \tag{5}$$

It implies that Bob cannot get any secret information about Alice's private set, because he cannot extract out the global phase information from the partial qubits of the entangled quantum systems with the subscripts A and B. In fact, any local unitary operator on the partial qubits cannot fully disentangle the entanglement of the composite system unless it directly measures them.

Case 3: Calvin wants to learn Alice's and Bob's private sets $S_A = \left\{s_1^A, s_2^A, ..., s_{l_A}^A\right\}$, $S_B = \left\{s_1^B, s_2^B, ..., s_{l_B}^B\right\}$.

In our protocol, Calvin can get $P_B = \left(p_1^B, p_2^B, ..., p_{n+l}^B\right)$, where $p_i^B = QFT^{c_i^B \times 2} QFT^{r_i^B \times h_i^B} QFT^{c_i^A \times 2} QFT^{r_i^A \times h_i^A} |j\rangle_C$ $(i = 1, 2, ..., n)$ and c_i^B, c_i^A is related to Alice's and Bob's private sets.

Calvin calculates $p_i^{C'} = QFT^{4-(((r_i^A \times h_i^A)+(r_i^B \times h_i^B)) \bmod 4)+r_i^B \times h_i^B + r_i^A \times h_i^A} QFT^{c_i^B \times 2} QFT^{c_i^A \times 2} |j\rangle_C$ $(i = 1, 2, ..., n)$.

Calvin measures $p_i^{C'}$: If the measuring result is $|j\rangle_C$, he cannot determine $c_i^A = c_i^B = 1$ or $c_i^A = c_i^B = 0$; If the measuring result is $|-j\rangle_C$, he cannot determine $c_i^A = 1, c_i^B = 0$ or $c_i^A = 0, c_i^B = 1$. The maximal probability of correct messages guessed by Calvin is $\left(\frac{1}{2}\right)^n$, where n is the length of Alice's and Bob's $0-1$ codes. Alice and Bob can insert some extra codes to obtain higher security.

Table 1 The comparison of Ref. [22–24] and our protocol

Scheme	Ref. [22]	Ref. [23]	Ref. [24]	Our protocol
Quantum resource	n encoded states $\frac{\|0\rangle+\|c_i\rangle}{\sqrt{2}}$	single photons	ERP pairs	n single photons
Quantum measurement	von Neumann measurement	single-photon projective measurement	Bell-base measurement	OAM basis measurement
Quantum technology used	U_0 and U_S	single-photon operator	single-particle operators	QFT
Output	$A \cap B$	$\|A \cap B\|$	$\|A \cap B\|$ and $\|A \cup B\|$	$A \cap B$

4.3 Comparison of our Protocol with Previous Studies

In this sub-section, we will take a simple comparison between the a scheme in Ref. [22–24] and our scheme, which are used to solve private set intersection problem. With the help of the third party(TP), the comparison result(s) can be known from the following six aspects: the cost of quantum resource, quantum measurement and quantum technology used. The details of differences between our protocol and related studies Ref. [22–24] are shown in Table 1.

Obviously, we can very easily find that our scheme has the remarkable advantages of consuming fewer quantum resources. Our protocol is easy to implement and it only needs simple quantum technology QFT.

5 Discussion and Conclusions

In summary, we put forward a novel quantum solution for PSI problem. After performing quantum Fourier transform on particles randomly chosen by Calvin, Alice and Bob privately get all common elements of their respective sets. Our protocol can resist various outside attacks, such as disturbance attack, Trojan horse attack, intercept-resend attack, entanglement-and-measure attack and man-in-the-middle attack. It can also avoid the problem of information leakage with acceptable efficiency.

Acknowledgements This work was supported in part by the 2019 National Social Science Foundation Art Major Project, Network Culture Security Research, under Grant 19zd12, in part by the High-Quality and Cutting-Edge Disciplines Construction Project for Universities in Beijing (Internet Information, Communication University of China), in part by the National Natural Science Foundation of China under Grant 61502437 and Grant 61773352, and in part by the Fundamental Research Funds for the Central Universities.

Author Contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Wen Liu and Hanwen Yin. The first draft of the manuscript was written by Wen Liu and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Declarations

- The research didn't involve animals and human participants.
- This work was supported in part by the 2019 National Social Science Foundation Art Major Project, Network Culture Security Research, under Grant 19zd12, in part by the High-Quality and Cutting-Edge Disciplines Construction Project for Universities in Beijing (Internet Information, Communication University of China), in part by the National Natural Science Foundation of China under Grant 61502437 and Grant 61773352, and in part by the Fundamental Research Funds for the Central Universities.
- The authors have no relevant financial or non-financial interests to disclose.
- The authors have no conflicts of interest to declare that are relevant to the content of this article.
- All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
- The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Freedman, M.J., Nissim, K., Pinkas, B.: Efficient private matching and set intersection. In: Proc. of EUROCRYPT, LNCS 3027, Interlaken, Switzerland, pp. 1–19 (2004)

2. Li, Y., Tygar, J., Hellerstein, J.: Private matching. In: Proceedings of Computer Security in the 21st Century, pp. 25–50 (2005)
3. Zhan, J., Cabrera, L., Osman, G., Shah, R.: Using private matching for securely querying genomic sequences. In: Proceedings of IEEE Third International Conference on Privacy, Security, Risk and Trust (passat) and Third International Conference On Social Computing (socialcom), pp 1163–1168 (2011)
4. Chun, J.Y., Hong, D., Jeong, I.R., Lee, D.H.: Privacy-preserving disjunctive normal form operations on distributed sets. Inform. Sci. **231**(10), 113–122 (2013)
5. Pervez, Z., Awan, A.A., Khattak, A.M., Lee, S., Huh, E.N.: Privacy-aware searching with oblivious term matching for cloud storage. J. Supercomput. **63**(2), 538–560 (2013)
6. Narayanan, A., Thiagarajan, N., Lakhani, M., Hamburg, M., Boneh, D.: Location privacy via private proximity testing. In: Proceedings of the Network and Distributed System Security Symposium, (San Diego, CA USA) (2011)
7. Wu, M.E., Chang, S.Y., Lu, C.J., Sun, H.M.: A communication-efficient private matching scheme in Client-Server model. Inform. Sci. **275**(10), 348–359 (2014)
8. Hazay, C., Lindell, Y.: Efficient protocols for set intersection and patten matching with security against malicious and covert adversaries. In: Proceedings of Theory of Cryptography Conference (TCC), New York, USA, LNCS 4948: pp. 155–175 (2008)
9. Liu, L., Cao, Z.: Private matching protocols without error probability
10. Kerschbaum, F.: Outsourced private set intersection using homomorphic encryption. In: Proc. ACM ASIACCS, pp. 85–86 (2012)
11. Shao, Z.Y., Yan, B.: Private set intersection via public key encryption with keywords search. Secur. Commun. Netw. **8**(3), 396–402 (2015)
12. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer SIAM. J. Comput. **26**, 1484 (1997)
13. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**, 055305 (2009)
14. Chen, X.B., Xu, G., Niu, X.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1561–1565 (2010)
15. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with w state. Opt. Commun. **284**, 1561–1565 (2011)
16. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with chi-type state. Int. J. Theor. Phys. **51**(1), 69–77 (2011)
17. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793–2804 (2010)
18. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
19. Wei, C.Y. et al.: Error Tolerance Bound in QKD-based Quantum Private Query. IEEE J. Sel. Areas Commun. **38**, 517–527 (2020)
20. Gao, F., Qin, S.J., Huang, W., Wen, Q.Y.: Quantum private query: a new kind of practical quantum cryptographic protocols. Sci. China-Phys. Mech. Astron. **62**, 070301 (2019)
21. Wei, C.Y., Cai, X.Q., Liu, B., et al.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. **67**, 2–8 (2018)
22. Shi, R.H., Mu, Y., Zhong, H., et al.: An efficient quantum scheme for Private Set Intersection. Quantum Inf. Process. **15**, 363–371 (2016)
23. Shi, R.H., Zhang, M.W.: A feasible quantum protocol for private set intersection cardinality. IEEE ACCESS **7**, 72105–72112 (2019)
24. Shi, R.H.: Quantum private computation of cardinality of set intersection and union. European Phys. J. D, 72(221) (2018)
25. Qin, H.W., Tso, R.L., Dai, Y.W.: Quantum secret sharing by using Fourier transform on orbital angular momentum. IET Information Security (2018)
26. Chaabouni, R., Lipmaa, H., Zhang, B.: A non-interactive range proof with constant communication. In: Proceedings of International Conference on Financial Cryptography and Data Security, Kralendijk, 179–199 (2012)
27. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
28. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secretsharing protocol. Phys. Rev. A **76**(06), 2007 (2324)
29. Lin, S., Gao, F., Guo, F.Z., et al.: Comment on Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **76**, 036301 (2007)

30. Lin, S., Wen, Q.Y., Gao, F., et al.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553 (2008)
31. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comment on experimental demonstration of a quantum protocol for byzantine agreement and liar detection. Phys. Rev. Lett. **101**, 208901 (2008)
32. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
33. Chen, X.B., Tang, X., Xu, G., Dou, Z., Chen, Y.L., Yang, Y.X.: Cryptanalysis of secret sharing with a single d-level quantum system. Quantum Inf. Process. **17**, 225 (2018)
34. Li, L., Shi, R.H.: A Novel and Efficient Quantum Private Comparison Scheme. J. Korean Phys. Soc. **75**(1), 15–21 (2019)