International Journal of Theoretical Physics (2020) 59:1992–2007
https://doi.org/10.1007/s10773-020-04471-8

Quantum Secure Multi-party Private Set Intersection Cardinality

Bai Liu[1] · Mingwu Zhang[1] · Runhua Shi[1]

Received: 25 November 2019 / Accepted: 16 April 2020 / Published online: 7 May 2020

Abstract

As we know that data sharing, a critical element in social networks, has the benefits of exploring important information, while also has the disadvantage of information leakage. Therefore, without the reliable third party arbitration agency, it is impossible to share information privately by distrustful multi-party. In this paper, we proposed a protocol called Quantum Secure Multi-party Private Set Intersection Cardinality (QSMS-IC), which has the capability of resisting quantum attacks. QSMS-IC, the extension of two-parity private set intersection cardinality which was proposed in Information Sciences(2016,147-158), utilizes quantum transformation, quantum measurements and quantum parallelism to solve multi-party private set intersection cardinality problems. Compared with two-party PSI-CA protocols, our proposed protocol can solve the data sharing among multi-party without the reliable third party arbitration agency. It also can be used in numerous applications and more suitable to the actual cases. For instance, large-scale social networks and privacy-preserving data ming.

Keywords Private set intersection cardinality · Privacy-preserving · Quantum computation · Secure multi-party computation

Manuscript received Nov xx, 2019; revised xx–xx, xxxx. This work was supported by the National Natural Science Foundation of China (No.61672010, No.61702168 and No.61701173), Ph. D. Programs Foundation(BSQD2019024), Provincial education project(B2018310)

✉ Bai Liu
liubai@hbut.edu.cn

Mingwu Zhang
csmwzhang@gmail.com

Runhua Shi
hfsrh@sina.com

[1] School of Computer Science, Hubei University of Technology, Wuhan 430068, China

1 Introduction

Secure multi-party computation (SMC) [1–3] enables three or more clients to evaluate the function without disclosing any private information about their privacy information. Since it was proposed by Yao [25], SMC had attracted wide attention from the scholars, which was used in numerous scenarios such as information-sharing [19, 20] and privacy preserving [4, 5].

Private set intersection (PSI) [9, 21], a typical application of information-sharing, enables two parties with privates sets to participate in calculation of the intersection without revealing any private inputs information. however, in some higher privacy-preserving scenarios, such as in medical systems and social networks, private set intersection reveals too much private personal information which may be exposed in part or in whole. In this case, Private Set Intersection Cardinality (PSI-CA) [6, 7] was introduced, which can meet the requirements on prevention of revealing the specific content, and make the outputting be the cardinality. In addition, in network circumstances, PSI-CA has huge practical application value in safeguarding users's privacy [22]. For example, in social networks, users can privately calculate the common hobbies and interesting by using the PSI-CA protocol, so that they can determine whether to become good friends or not [15]. In this situation, they use the elements of private sets on behalf of the hobbies and interesting. What's more, users can also privately calculate the distance of two physically independent parties. i.e. the Hamming distance which was proposed in literature [23]. Furthermore, there are other applications, such as anonymous authentication [8], location privacy [26], and privacy-preserving data mining [24] etc.

Due to the extensive and important application, there were some secure private set intersection cardinality protocols had been proposed [11–13]. In these existed protocols, most of them are classical cryptography. However, the increasing capability of quantum computing or algorithms has posed huge challenge to the security of these classical PSI-CA protocols which depend on some unconfirmed arduous hypothesis [14]. It means that if there were not strict constraint condition, it is impossible for two-party computations to fulfill the unconditional security e.g., a large integer factoring problem, which can be easily got over by fast quantum algorithms [14]. In addition, with the advent of quantum computer, these classical PSI-CA protocols are vulnerable to attack by quantum computers. Therefore, quantum cryptography which is the combination of quantum computer and cryptography is draw attention to the scholars. For instance, quantum sealed auction protocol [27], quantum anonymous voting protocol [28], quantum signature [29] and identity-based quantum signature [30].

The quantum protocols of PSI-CA [7, 8, 10] with unconditional security was also proposed. Compared with classical cryptography, the most important advantage of quantum cryptography is that an eavesdropper can easily be identified by using the characteristics of quantum mechanics. To the best of our knowledge, these proposed quantum PSI-CA protocols are all about two-party computation [8–10]. In order to solve the data sharing among multi-party, we, based on the ideas of quantum PSI-CA [8] and quantum counting [16, 17], presented an unconditionally quantum secure multi-party set intersection cardinality (QSMS-IC) protocol, which is extended two parties to multi-party. Unlike the existed protocols, our proposed QSMS-IC protocols has two clear advantages: for classical protocols it has higher security, and for existed quantum protocols, it is a real multi-party protocol, has wider applications and more practical.

In this paper, we present a practical and feasible quantum secure multi-party set intersection cardinality protocol, which can privately compute the intersection cardinality. The organization of the paper is following, the second section is the basic knowledge about quantum and the definition of QSMS-IC. We present a quantum secure multi-party set intersection cardinality protocol in Section 3. In addition, the security analysis and correctness are shown in Section 4. Finally, in Section 5, we give the conclusion of the paper.

2 Preliminaries

2.1 Quantum Computing

Quantum computing [17], a theory of physics, can also be used in computer science. In this section we give the basics of quantum computing that we will use.

2.1.1 Quantum Bits

Quantum bit is just like the classical bit, 0 or 1 in classical computation are corresponding to the states $|0\rangle$ and $|1\rangle$ in quantum, and $|0\rangle$ and $|1\rangle$ are two orthogonal unit vectors in 2-dimensional Hilbert space, these two states form a perfect complete orthogonal basis, which is also called computational basis. The qubits also is a linear combination state, namely superpositions:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Here, α, β are complex numbers, and $|\alpha^2\rangle + |\beta^2\rangle = 1$. Similarly, multiple qubits can be expressed, such as n-qubit can be in any superposition of the 2^n basis states

$$\begin{aligned} |\Psi\rangle &= \alpha_0|00...00\rangle + \alpha_1|00...01\rangle + \ldots \\ &\quad +\alpha_(2^n - 1)|11...11\rangle \end{aligned} \tag{2}$$

where $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$, $|00...00\rangle, |00...01\rangle, \ldots, |11...11\rangle$ are a perfect orthogonal basis in n-dimensional Hilbert space.

2.1.2 Quantum Measurement

The measurement will use Hermitian operator, $M = \sum_m mP_m$, P_m is the projector onto the eigenspace of M with eigenvalue m. After measurement, we will get the state $\frac{p_m|\Psi\rangle}{\sqrt{p(m)}}$ with probability $p(m) = \langle\Psi|P_m|\Psi\rangle$.

For instance, in 2-dimensional Hilbert space $p_0 = |0\rangle\langle 0|$ and $p_1 = |1\rangle\langle 1|$ are sets of projector operators

$$\begin{aligned} P_0|\Psi\rangle &= |0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|0\rangle\langle 0|0\rangle + \beta|0\rangle\langle 0|1\rangle \\ &= \alpha|0\rangle \end{aligned} \tag{3}$$

$$\begin{aligned} P_1|\Psi\rangle &= |1\rangle\langle 1|(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|1\rangle\langle 1|0\rangle + \beta|1\rangle\langle 1|1\rangle \\ &= \beta|1\rangle \end{aligned} \tag{4}$$

$$\begin{aligned} p(0) &= \langle\Psi|P_0|\Psi\rangle \\ &= (\alpha^*\langle 0| + \beta^*\langle 1|)P_0(\alpha|0\rangle + \beta|1\rangle) \\ &= (\alpha^*\langle 0| + \beta^*\langle 1|)\alpha|0\rangle \\ &= |\alpha|^2 \end{aligned} \tag{5}$$

$$\begin{aligned} p(1) &= \langle \Psi | P_1 | \Psi > \\ &= (\alpha^* \langle 0| + \beta^* \langle 1|) P_1 (\alpha |0\rangle) + \beta |1\rangle) \\ &= (\alpha^* \langle 0| + \beta^* \langle 1|) \beta |1\rangle \\ &= |\beta|^2 \end{aligned} \tag{6}$$

So when making measurement on $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\Psi\rangle$ will be collapsed into the state $|0\rangle$ with probabilities $|\alpha|^2$ and state $|1\rangle$ with probabilities $|\beta|^2$

Similarly, when measuring $\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n-1\rangle$ in computational basis $\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n-1\rangle\}$ we will get $|i\rangle$ with probability $|\alpha_i|^2$.

2.1.3 Quantum Transformation

In quantum mechanics, unitary transformation is used to describe the evolution of a closed system, $|\Psi\rangle = U|\phi\rangle$, ($|\phi\rangle$ is the input state, $U|\phi\rangle$ is the output state, $|\Psi\rangle$ is the final state that is using unitary transformation U, and $U^+U = I$, I is the identity operator, U^+ is the conjugate transpose of U. NOT gate is the simplest one-qubit quantum logical gate, it maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The Hadamard gate is another one-qubit quantum logical gate, it is following,

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{7}$$

CNOT gate is multi-qubit quantum logic gate, CNOT gate: $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$ and $|11\rangle \rightarrow |10\rangle$, the first qubit in CNOT gate is called control qubit, and the second qubit is called target qubit. In this regard, if the control qubit is 0, the target qubit remain unchanged, if the control qubit is 1, then the target qubit need change.

Besides, we also need to use the quantum Fourier transform which is the standard discrete Fourier transform. For $x \in \{0, 1, \ldots M-1\}$, the definition of quantum Fourier transform and the inverse quantum Fourier transform is shown as follows [9]:

$$QFT : |x\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M} y} |y\rangle \tag{8}$$

$$QFT^{-1} : |x\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{-2\pi i \frac{x}{M} y} |y\rangle \tag{9}$$

$$\begin{aligned} QFT^{-1}(QFT|x\rangle) &= QFT^{-1}\left(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M} y} |y\rangle\right) \\ &= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M} y} QFT^{-1}|y\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M} y} \left(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1}\right. \end{aligned}$$

$$\begin{aligned}
&e^{-2\pi i \frac{x}{M} j} |j\rangle \Big) \\
&= \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M}(x-j)} |j\rangle \\
&= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} |x > + \frac{1}{\sqrt{M}} \sum_{j=0:j\neq}^{M-1} \\
&\left(\sum_{y=0}^{M-1} e^{2\pi i \frac{x}{M}(x-j)} |j\rangle \right) \\
&= |x\rangle
\end{aligned} \tag{10}$$

2.1.4 Quantum Parallelism

Quantum parallelism allows quantum computers to perform multiple computations simultaneously. In classical computer, parallel computing means that there are some processors that do the different computation simultaneously. In quantum compute, multiple computations are realized by the superposition of multiple states with a single quantum processor. It means that a quantum computer has more computation ability than a classical computer.

For example, If there is a 2-qubit quantum circuit, then we can make a quantum transformation U_f on it, U_f is following:

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \tag{11}$$

$f(x) : \{0, 1\} \rightarrow \{0, 1\}$ is a function, $\oplus$ is the operator of module 2. When $y = 0$, the second qubit is just the value $f(x)$. It means $U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$, Furthermore, when $|x\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned}
U_f \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle &= U_f \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} \\
&= \frac{U_f|0\rangle|0\rangle + U_f|1\rangle|0\rangle}{\sqrt{2}} \\
&= \frac{|0\rangle f(0) + |1\rangle f(1)}{\sqrt{2}}
\end{aligned} \tag{12}$$

U_f computes $f(0)$ and $f(1)$ simultaneously. It can generalize a more general function, $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$, such that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, the qubit lengths of $|x\rangle$ and $|y\rangle$are n and 1, respectively. Similarly, consider $|x\rangle = H^{\otimes n}$ and $|y\rangle = |0\rangle$. Then

$$\begin{aligned}
U_f|x\rangle|0\rangle &= U_f H^{\otimes n} |0\rangle^{\otimes n} |0\rangle \\
&= U_f \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right]^{\otimes n} |0\rangle \\
&= U_f \left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^{n-1}} |j\rangle \right) |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^{n-1}} |i\rangle|f(i)\rangle
\end{aligned} \tag{13}$$

So we know that the quantum transformation U_f can computes $f(i)$ for all values of i simultaneously by (13).

2.2 quantum Secure Multi-Party Set Intersection Cardinality

Here, we give the definition of quantum secure multi-party set intersection cardinality (QSMS-IC).

Definition 1. QSMS-IC, there are $n-1$ clients $U_i, i = 2, \ldots, n$ with the input are private set $A_i, (i = 2, 3, \ldots, n)$ and a server U_1 with the set $A_1 = \{1, \ldots, 1\}$. After running QSMS-IC protocol, the clients U_i can get nothing except the cardinality of the intersection $|A_1 \cap A_2 \cap \cdots \cap A_n|$. In addition, QSMS-IC should meet the following privacy requirements:

Clients U_i privacy: The clients U_i learn no information about the sets of other clients except about the set size $|A_i|$.

Fairness: All the clients U_i are peer entities, and no one can get the private information by deceiving from the others. Finally, all the clients get the result of cardinality with equal chance.

3 Quantum Secure multi-party Set Intersection Cardinality

3.1 System Model

Based on the quantum parallelism, quantum PSI-CA [7, 8] and Grovers search algorithm [18], we proposed a new QSMS-IC protocol. First we assume that the system model has n entities which are one server and $n-1$ clients, and the private set $A_i = \{a_1^i, a_2^i, \ldots, a_{n_c}^i\}$ the elements in A_i lie in Z_N, where $Z_N = \{0, 1, 2, \ldots, N-1\}$, $N = 2^n$ (i.e.$n = logN$,). Moreover, assume that $\sum_{i=1}^{n} n_{c_i} < \frac{N}{2}$, N and n_{c_i} are public. Figure 1 is the system model of QSMS-IC protocol.

As shown in Fig. 1, there are $n-1$ clients and a server. In the protocol, we suppose all the clients and server are semi-honest: they are curious with the privacy of others, but are honest to carry out the operations of the scheme.

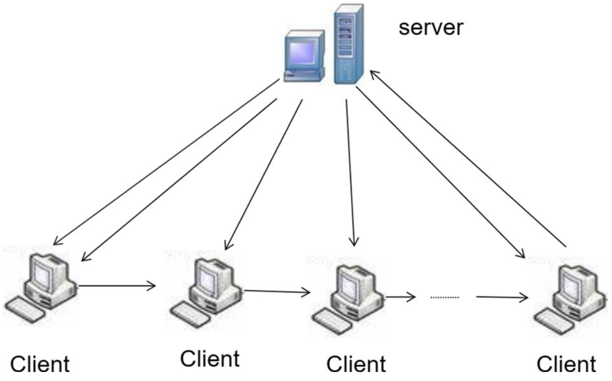

Fig. 1 System model

3.2 Operation Steps

The protocol consists nine steps as follows(also show in Fig. 2).

Step1. The server U_1 initializes the state $|\varphi_0\rangle$ in $|0\rangle^{\otimes n}$, then applies $H^{\otimes n}$ to $|\varphi_0\rangle$, and gets the state $|\varphi_1\rangle$, $|\varphi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}|x\rangle$.

Step2. Then the server U_1 gives an ancillary state $|r\rangle$, r is a random number in set $\{0, 1\}$, and does a transformation U_{f_s} on $|\varphi_1\rangle \otimes |r\rangle$, U_{f_s} is defined as follows:

$$f_{A_1}(x) = \begin{cases} 1 \ if x \in A_1 \\ 0 \ if x \notin A_1 \end{cases} \tag{14}$$

$$U_{f_s} : \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_{A_1}(x)\rangle \tag{15}$$

Let $|\varphi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_{A_1}(x)\rangle$. $\oplus$ is the operator of module 2. Then, we do the same transformation U_{f_s} on $|\varphi_2\rangle \otimes |1\rangle$, as follow:

$$U_{f_s} : |\varphi_2\rangle|1\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_{A_1}(x) \oplus 1\rangle \tag{16}$$

Let $|\varphi_2'\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_{A_1}(x) \oplus 1\rangle$. Then the server U_1 sends $|\varphi_2\rangle$, $|\varphi_2'\rangle$ to the client U_2 through the quantum channel.

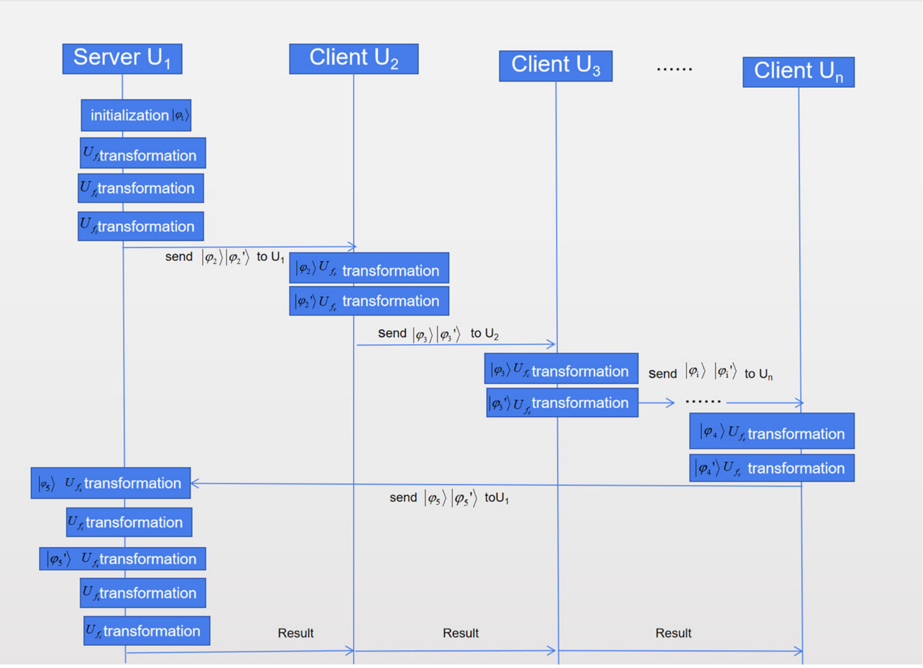
Server U_1
Client U_2
Client U_3
......
Client U_n
initialization $|\varphi_1\rangle$
U_{f_s}transformation
U_{f_c}transformation
U_{f_s}transformation
send $|\varphi_2\rangle|\varphi_2'\rangle$ to U_1
$|\varphi_2\rangle U_{f_c}$ transformation
$|\varphi_2'\rangle U_{f_c}$ transformation
send $|\varphi_3\rangle|\varphi_3'\rangle$ to U_2
$|\varphi_3\rangle U_{f_c}$ transformation
$|\varphi_3'\rangle U_{f_c}$ transformation
send $|\varphi_i\rangle$ $|\varphi_i'\rangle$ to U_n
......
$|\varphi_4\rangle U_{f_c}$ transformation
$|\varphi_4'\rangle U_{f_c}$ transformation
$|\varphi_5\rangle$ U_{f_s} transformation
send $|\varphi_5\rangle|\varphi_5'\rangle$ toU_1
U_{f_c} transformation
$|\varphi_5'\rangle$ U_{f_s}transformation
U_{f_s}transformation
U_{f_c}transformation
Result
Result
Result

Fig. 2 Sequence diagram

Step3. When the client U_2 received the state $|\varphi_2\rangle$, $|\varphi_2'\rangle$, then the client U_2 will do another transformation U_{f_c} on state $|\varphi_2\rangle$, the transformation $U_{f_c}$is defined as follow:

$$f_{A_2}(x) = \begin{cases} 1 \ if x \in A_2 \\ 0 \ if x \notin A_2 \end{cases} \tag{17}$$

$$U_{f_c} : \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|r \otimes f_{A_1}(x)\rangle|f_{A_2}(x)\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x)) \times f_{A_2}(x)\rangle \tag{18}$$

Here, Let $|\varphi_3\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x)) \times f_{A_2}(x)\rangle$, × is an operator that is logical multiplication. Then does the transformation U_{f_c} on $|\varphi_2'\rangle$ as follow:

$$f_{A_2}(x) = \begin{cases} 1 \ if x \in A_2 \\ 0 \ if x \notin A_2 \end{cases}$$

$$U_{f_c} : |\varphi_2'\rangle|f_{A_2}(x)\rangle \rightarrow$$

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x) \oplus 1) \times f_{A_2}(x)\rangle \tag{19}$$

Let $|\varphi_3'\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x) \oplus 1) \times f_{A_2}(x)\rangle$. Then client U_2 sends $|\varphi_3\rangle$, $|\varphi_3'\rangle$ to the client U_3 through the quantum channe2.

Step4. After client U_3 receives $|\varphi_3\rangle$, $|\varphi_3'\rangle$, the client U_3 does the same transformation U_{f_c} on state $|\varphi_3\rangle$. then we get the result:

$$U_{f_c}(\varphi_3) : \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x)) \times f_{A_2}(x) \times f_{A_3}(x)\rangle \tag{20}$$

Here, we use state $U_{f_c}(|\varphi_3\rangle)$ to expressed the results. Then the client U_3 does U_{f_c} transformation on $|\varphi_3'\rangle$. The result is $U_{f_c}(|\varphi_3'\rangle) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x) \oplus 1) \times f_{A_2}(x) \times f_{A_3}(x)\rangle$

Then send $U_{f_c}(|\varphi_3\rangle)$, $U_{f_c}(|\varphi_3'\rangle)$ to the client U_4 through the quantum channe3, after the client U_4 receives $U_{f_c}(|\varphi_3\rangle)$, $U_{f_c}(|\varphi_3'\rangle)$, and does U_{f_c} transformation on $U_{f_c}(|\varphi_3\rangle)$, $U_{f_c}(|\varphi_3'\rangle)$ respectively, then send the results to the next client and until the last client U_n, the last client U_n does U_{f_c} transformation respectively, uses $|\varphi\rangle$, $|\varphi'\rangle$ as the last results which will be sent to the server U_1.

Step5: when the server U_1 receives the state $|\varphi\rangle$, it will do the transformation U_{f_s} on $|\varphi\rangle \times |r\rangle$.

$$\begin{aligned} U_{f_s}(\varphi) = & \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|(r \oplus f_{A_1}(x)) \\ & \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r\rangle \end{aligned} \tag{21}$$

Then does U_{f_c} on state $U_{f_s}(|\varphi\rangle)$

$$\begin{aligned} U_{f_c}(U_{f_s}(\varphi)) = & \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|[(r \oplus f_{A_1}(x)) \\ & \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r] \times f_{A_1}(x)\rangle \end{aligned} \tag{22}$$

Let $|\varphi_4\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|[(r\oplus f_{A_1}(x))\times f_{A_2}(x)\times\cdots\times f_{A_n}(x)\oplus r]\times f_{A_1}(x)\rangle$ When the server U_1 receives the state $|\varphi'\rangle$, it will do two U_{f_s} transformation on $|\varphi'\rangle$

$$U_{f_s}(|\varphi'\rangle\oplus|r\rangle) = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|(r\oplus f_{A_1}(x)\oplus 1) \\ \times f_{A_2}(x)\times\cdots\times f_{A_n}(x)\oplus r\rangle \tag{23}$$

$$U_{f_s} \\ = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|(r\oplus f_{A_1}(x)\oplus 1)\times f_{A_2}(x)\times\ldots \\ \times f_{A_n}(x)\oplus r\oplus f_{A_1}(x)\rangle \tag{24}$$

Let$|\varphi_4'\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|(r\oplus f_{A_1}(x)\oplus 1)\times f_{A_2}(x)\times\cdots\times f_{A_n}(x)\oplus r\oplus f_{A_1}(x)\rangle$.

Step6: Then the server U_1 does U_f transformation on $|\varphi_4'\rangle$ and $|\varphi_4\rangle$. Then get

$$|\varphi_5\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|[(r\oplus f_{A_1}(x))\times f_{A_2}(x)\times\ldots \\ \times f_{A_n}(x)\oplus r\oplus f_{A_1}(x)]\times\sim\rangle \tag{25}$$

where $\sim = |[(r\oplus f_{A_1}(x)\oplus 1)\times f_{A_2}(x)\times\cdots\times f_{A_n}(x)\oplus r\oplus f_{A_1}(x)]\rangle$, and $|[(r\oplus f_{A_1}(x))\times f_{A_2}(x)\times\cdots\times f_{A_n}(x)\oplus r\oplus f_{A_1}(x)]\times\sim\rangle$ contains the classical information about the cardinality of their intersection.

Step7: The state $|\varphi_5\rangle$ carried the cardinality of their intersection, so we should extract the intersection cardinality from $|\varphi_5\rangle$, the server U_1 prepares quantum state $\frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle$, M is a big integer, so the value of $\frac{2\pi}{\sqrt{t(N-t)}}+\frac{\pi^2}{M^2}|N-2t|$ is very small (t is defined in Step8). Let $|\varphi_6\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes|\varphi_5\rangle$. Then, the server U_1 does a quantum operator C_F on $|\varphi_6\rangle$, the result is state $|\varphi_7\rangle$, C_F is the following:

$$C_F : |\varphi_6\rangle \rightarrow |\varphi_7\rangle$$

$$C_F : \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes|\varphi_5\rangle \rightarrow \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes G^y|\varphi_5\rangle \tag{26}$$

$$|\varphi_7\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes G^y|\varphi_6\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes G^y \\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|[(r\oplus f_{A_1}(x))\times f_{A_2}(x)\times\cdots\times f_{A_n}(x) \\ \oplus r\oplus f_{A_1}(x)]\times\sim\rangle \tag{27}$$

G is defined by $G = U_{\varphi_6}U_{f_r}$, G is an operator of amplitude amplification .

$$U_{f_r}|x\rangle|r\rangle = \begin{cases} -|x\rangle|1\rangle & ifr = 1 \\ |x\rangle|0\rangle & ifr = 0 \end{cases} \tag{28}$$

$$U_{\varphi_6} = 2|\varphi_6\rangle\langle\varphi_6| - I \tag{29}$$

I is the identity operator.

Step8: The server U_1 does QFT^{-1} on the first $logM$ qubits of $|\varphi_7\rangle$ and then measures the first $logM$ qubits to obtain $|x\rangle$, and outputs $Nsin^2(\frac{x}{M}\pi)$ as the estimation of t, t is the number of the items that the last one qubit of $|\varphi_6\rangle$ is in $|1\rangle$, for example, just like $|x\rangle|1\rangle$ in $|\varphi_6\rangle$. If $t < \frac{N}{2}$, then server U_1 outputs $\frac{\sum_{i=1}^{n} n_{c_i} - t}{2}$, means, $|A_1 \cap A_2 \cap \cdots \cap A_n| = \frac{\sum_{i=1}^{n} n_{c_i} - t}{2}$; otherwise $\frac{(n_c+n_s+t)-N}{2}$, means, $|A_1 \cap A_2 \cap \cdots \cap A_n| = \frac{(n_c+n_s+t)-N}{2}$.

Step9: The server sends the result t to all the clients.

If we want to whether someone is intercepting in the channel, the bait technology can be used. That is, when qubit sequence are transmitted, the sender randomly inserts some bait particles which is prepared randomly with either Z-basis (i.e.,$\{|0\rangle, |1\rangle\}$ or X-basis (i.e.,$\{\frac{1}{\sqrt{2}} + |1\rangle, \frac{1}{\sqrt{2}} - |1\rangle\}$. When the receiver received the sequence, the sender would public the bait particles positions and the measurement basis. Then the receiver's measures the bait particles accord to the public and tells his measurement results to the sender. The sender compares the receiver results with the bait particles of the initial and then analyzes it. If the error is too much according to the channel noise, then drop the protocol and restart transmitting. Otherwise, it will continue to proceed next step.

4 Analysis

Let's proof the correctness. Based on the state $|\varphi_5\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|[(r \oplus f_{A_1}(x)) \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r \times f_{A_1}(x)] \times \sim\rangle$, $[(r \oplus f_{A_1}(x)) \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r \times f_{A_1}(x)] \times \sim$ is 0 or 1, so we define

$$|\alpha\rangle = \frac{1}{\sqrt{t}}|x\rangle|1\rangle \tag{30}$$

$$|\beta\rangle = \frac{1}{\sqrt{t}}|x\rangle|0\rangle \tag{31}$$

Then we know that the state $|\varphi_5\rangle$ can be re-expressed by (32)

$$|\varphi_5\rangle = \sqrt{\frac{N-t}{N}}|\beta\rangle + \sqrt{\frac{t}{N}}|\alpha\rangle \tag{32}$$

Equation (32) means that $|\varphi_5\rangle$ is the uniform superposition of all product states, $|\alpha\rangle$ is the uniform superposition of these product states satisfying $[(r \oplus f_{A_1}(x)) \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r \times f_{A_1}(x)] \times \sim = 1$ and β is opposite of α , means $[(r \oplus f_{A_1}(x)) \times f_{A_2}(x) \times \cdots \times f_{A_n}(x) \oplus r \times f_{A_1}(x)] \times \sim = 0$. Obviously, $\alpha \perp \beta$. if we choose $\theta \in (0, \frac{\pi}{2})$, $sin^2\theta = \frac{t}{N}$. then $sin\theta = \sqrt{\frac{t}{N}}$, $cos\theta = \sqrt{\frac{N-t}{N}}$, and thus $|\varphi_4\rangle = cos|\beta\rangle + sin|\alpha\rangle$. Then , we can get the following equations:

$$\begin{aligned} G|\beta\rangle &= U_{\varphi_6} U_{f_r}|\beta\rangle = U_{\varphi_6}|\beta|\rangle \\ &= (2|\varphi_6\rangle\langle\varphi_6| - I)|\beta\rangle \\ &= 2|\varphi_6\rangle\langle\varphi_6|\beta\rangle - |\beta\rangle \\ &= 2cos\theta|\varphi_6\rangle - |\beta\rangle \\ &= 2cos\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) - |\beta\rangle \\ &= (2cos^2\theta - 1)|\beta\rangle + 2sin\theta cos\theta|\alpha\rangle \\ &= cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle \end{aligned} \tag{33}$$

$$
\begin{aligned}
G|\alpha\rangle &= U_{\varphi_6}U_{f_r}|\alpha\rangle = U_{\varphi_6}(-|\alpha|\rangle) \\
&= (2|\varphi_6\rangle\langle\varphi_6| - I)(-|\alpha\rangle) \\
&= 2|\varphi_6\rangle\langle\varphi_6|\alpha\rangle + |\alpha\rangle \\
&= -2sin\theta|\varphi_6\rangle + |\alpha\rangle \\
&= -2sin\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) + |\alpha\rangle \\
&= -2sin\theta cos\theta|\beta\rangle + (1 - 2sin^2\theta)|\alpha\rangle \\
&= -sin2\theta|\beta\rangle + cos2\theta|\alpha\rangle
\end{aligned}
\tag{34}
$$

In the two-dimensional subspace, G is a rotation operator of angle 2θ oriented from $|\beta\rangle$ to $|\alpha\rangle$ spanned by $|\alpha\rangle$ and $|\beta\rangle$. From $|\varphi_6\rangle$, apply G and rotate it toward $|\alpha\rangle$ by 2θ. Reapply G and rotate it close to $|\alpha\rangle$. Moreover, there are two orthogonal states defined in the following:

$$
|\phi_+\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle)
\tag{35}
$$

$$
|\phi_-\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle + i|\alpha\rangle)
\tag{36}
$$

$$
\begin{aligned}
G|\phi_+\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle - iG|\alpha\rangle) \\
&= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle \\
&\quad +isin2\theta|\beta - icos2\theta|\alpha\rangle)(by(33and34)) \\
&= \frac{e^{i2\theta}}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle)(by(e^{i2\theta} = cos2\theta + isin2\theta)) \\
&= e^{i2\theta}|\phi_+\rangle
\end{aligned}
\tag{37}
$$

$$
\begin{aligned}
G|\phi_-\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle + iG|\alpha\rangle) \\
&= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle \\
&\quad -isin2\theta|\beta + icos2\theta|\alpha\rangle)(by26and27) \\
&= \frac{e^{-i2\theta}}{\sqrt{2}}(|\beta\rangle + i|\alpha\rangle)(by(e^{-i2\theta} = cos2\theta - isin2\theta)) \\
&= e^{-i2\theta}|\phi_-\rangle
\end{aligned}
\tag{38}
$$

$|\phi_+\rangle$ and $|\phi_-\rangle$ are eigenvectors of G, $e^{i2\theta}$and $e^{-i2\theta}$ are eigenvalues, respectively. Let $\theta = \pi\omega$, then $|\varphi_6\rangle = cos|\beta\rangle + sin|\alpha\rangle = \frac{e^{i\pi\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\phi_-\rangle$ .If we apply G rotation operator to $|\varphi_6$ for y times, then

$$
G^y|\varphi_6\rangle = \frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle
\tag{39}
$$

Then, we can get

$$
\begin{aligned}
|\varphi_8\rangle &= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle\otimes G^{y}|\varphi_5\rangle \\
&= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}[|y\rangle\otimes(\frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle+\frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle)] \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle+\frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{-i2\pi y\omega}|y\rangle|\phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle \\
&\quad +\frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{-i2\pi y\omega(1-\omega)}|y\rangle|\phi_-\rangle
\end{aligned}
\tag{40}
$$

then applying QFT^{-1} to the first $logM$ qubits of $|\varphi_8\rangle$, we can get

$$
\begin{aligned}
QFT^{-1}|\varphi_7\rangle &= QFT^{-1}\left[\frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle\right. \\
&\qquad \left.+\frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega})|y\rangle|\phi_-\rangle\right] \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}(QFT^{-1}|y\rangle)|\phi_+\rangle \\
&\quad +\frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}(QFT^{-1}|y\rangle)|\phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}\left(\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}e^{i2\pi\frac{y}{M}x}|x\rangle\right) \\
&\quad |\phi_+\rangle+\frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)} \\
&\quad \left(\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}e^{-i2\pi\frac{y}{M}x}|x\rangle\right)|\phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2}}\sum_{y=0}^{M-1}\left(\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(\omega-\frac{x}{M}})|x\rangle\right)|\phi_+\rangle \\
&\quad +\frac{e^{-i\pi\omega}}{\sqrt{2}}\sum_{y=0}^{M-1}\left(\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y[(1-\omega)-\frac{x}{M}]}|x\rangle\right)|\phi_-\rangle
\end{aligned}
$$

$$= \frac{e^{i\pi\omega}}{\sqrt{2}}|\widetilde{x}_{+}\rangle|\phi_{+}\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\widetilde{x}_{-}\rangle|\phi_{-}\rangle \tag{41}$$

with

$$|\widetilde{x}_{+}\rangle = \sum_{y=0}^{M-1}\left(\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(\omega-\frac{x}{M})}\right)|x\rangle \tag{42}$$

$$|\widetilde{x}_{-}\rangle = \sum_{y=0}^{M-1}\left(\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega-\frac{x}{M})}\right)|x\rangle \tag{43}$$

Make a measurement on $|\widetilde{x}_{+}\rangle$ in the computational basis $\{|0\rangle, |1\rangle, \ldots, |M-1\rangle\}$ then get $|x\rangle$ with the probability $|\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(\omega-\frac{x}{M})}|^2$. so,

$$\begin{aligned}
&P\left(|\frac{x}{M}-\omega| \le \frac{1}{M}\right) = P(|x-M\omega| \le 1)\\
=\;& P(x=\lfloor M\omega\rfloor) + P(x=\lceil M\omega\rceil)\\
=\;& |\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(\omega-\frac{\lfloor M\omega\rfloor}{M})}|^2\\
&+|\frac{1}{M}\sum_{y=0}^{M-1}e^{i2\pi y(\omega-\frac{\lceil M\omega\rceil}{M})}|^2\\
=\;& |\frac{1-e^{i2\pi y(\omega-\frac{\lfloor M\omega\rfloor}{M})}}{M(1-e^{i2\pi y(\omega-\frac{\lfloor M\omega\rfloor}{M})})}|^2\\
&+|\frac{1-e^{i2\pi y(\omega-\frac{\lceil M\omega\rceil}{M})}}{M(1-e^{i2\pi y(\omega-\frac{\lceil M\omega\rceil}{M})})}|^2\\
=\;& |\frac{sin[\pi M(\omega-\frac{\lfloor M\omega\rfloor}{M})]}{Msin[\pi(\omega-\frac{\lfloor M\omega\rfloor}{M})]}|^2\\
&+|\frac{sin[\pi M(\omega-\frac{\lceil M\omega\rceil}{M})]}{Msin[\pi(\omega-\frac{\lceil M\omega\rceil}{M})]}|^2\\
=\;& \frac{sin^2[\pi M(\omega-\frac{\lfloor M\omega\rfloor}{M})]}{M^2sin^2[\pi(\omega-\frac{\lfloor M\omega\rfloor}{M})]}\\
&+\frac{sin^2[\pi M(\omega-\frac{\lceil M\omega\rceil}{M})]}{M^2sin^2[\pi(\omega-\frac{\lceil M\omega\rceil}{M})]}\\
\ge\;& \frac{1}{M^2sin^2(\frac{\pi}{2M})} + \ge \frac{1}{M^2sin^2(\frac{\pi}{2M})}\\
=\;& \ge \frac{2}{M^2sin^2(\frac{\pi}{2M})}\\
>\;& \frac{2}{M^2(\frac{\pi}{2M})^2} = \frac{8}{\pi^2}
\end{aligned} \tag{44}$$

After measuring, $\frac{x}{M}$ is close to or equal to ω with high probability. In fact, when make a measurement on $|\widetilde{x}_{+}\rangle$, the probability of getting either $\lfloor M\omega\rfloor$ or $\lceil M\omega\rceil$ is at least $\frac{8}{\pi^2}$, with the estimation ω within the error $\frac{1}{M}$. Similarly, make a measurement on $|\widetilde{x}_-\rangle$, the probability of getting either $\lfloor M(1-\omega)\rfloor$ or $\lceil M(1-\omega)\rceil$ is at least $\frac{8}{\pi^2}$, with the estimation $1-\omega$ within the error $\frac{1}{M}$, so $\frac{x}{M}$ is close to or equal to $1-\omega$ with high probability. For $\theta = \pi\omega$ and $sin^2\theta = \frac{t}{N}$, $t = Nsin^2\pi\omega$.For the first case (i.e.,$|\widetilde{x}_+\rangle$), $\omega = \frac{x}{M}$, so $t = Nsin^2(\pi\frac{x}{M})$;for the second case (i.e,$|\widetilde{x}_-\rangle$),$\omega \approx 1-\frac{x}{M}$, so $t = Nsin^2(\pi - \pi\frac{x}{M}) = Nsin^2(\pi\frac{x}{M})$.For the two cases, get the same estimation t.

Theorem 1 [16]. For $\forall M \in Z$, $|t-\widetilde{t}| \leq \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N-2t|$, the least probability is $\frac{8}{\pi^2}$,so $\widetilde{t}$ is an estimate of t. the error is $\varepsilon \leq \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N-2t|$.

Then we know the relations between t and $|A_1 \cap A_2 \cap \cdots \cap A_n|$

$$|A_1 \cap A_2 \cap \cdots \cap A_n| = t \tag{45}$$

In Step 8, we can get the estimation of t with the high probability p, and $p \geq \frac{8}{\pi_2}$, error is ε, error is very small, and $\varepsilon \leq \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N-2t|$; so the QSMS-IC protocol can get the estimation of $|A_1 \cap A_2 \cap \cdots \cap A_n|$ with high probability $p \geq \frac{8}{\pi_2}$ and small error ε.

Then analyze the security.

Theorem 2 (client Privacy). In QSMS-IC protocol, the client U_i can not get the information about the elements of A_1 except the set size, and the server U_1 also can not get the information about the elements of A_i except the set size.

Proof. In QSMS-IC protocol, the server U_1 sends a quantum state $|\varphi_2\rangle$ to the server U_2, without revealing the elements of the set. Though the state $|\varphi_2\rangle$ including the information of $f_{A_1}(x)$, the client U_2 cannot extract $f_{A_1}(x)$ from $|\varphi_2\rangle$. Supposed that the quantum state $|\varphi_2\rangle$ consists of two subsystems: the n-qubit system $\widetilde{C}$ and the 1-qubit system $\widetilde{S}$, $\widetilde{S}$ is ancillary system. Suppose the clients are half a honest client which is curious about other client's information and actually transmits personal information. The client makes a projective measurement on $|\varphi_2\rangle$, it can get $|x\rangle|r \oplus f_{A_1}(x)\rangle$ with probability$\frac{1}{n}$. Thus, $\widetilde{S}$ can be characterized by quantum ensemble $\xi \equiv \{p_x, \rho_{\widetilde{S}}(x)\}$, and $p_x = \frac{1}{n}$,

$$\begin{aligned}\rho_{\widetilde{S}}(x) &= Tr_{\widetilde{C}}(|x\rangle|r \oplus f_{A_1}(x)\rangle\langle r \oplus f_{A_1}(x)|\langle x|) \\ &= |r \oplus f_{A_1}(x)\rangle\langle r \oplus f_{A_1}(x)|\end{aligned} \tag{46}$$

For $|\varphi_2\rangle = \frac{1}{N}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_{A_1}(x)\rangle$, so $\widetilde{S}$ can also be described by the following density operator,

$$\begin{aligned}\rho_{\widetilde{S}}(x) &= Tr_{\widetilde{C}}|\varphi_2\rangle\langle\varphi_2| \\ &= \langle 0|\varphi_2\rangle\langle\varphi_2|0\rangle + \langle 1|\varphi_2\rangle\langle\varphi_2|1\rangle + \ldots \\ &\quad +\langle N-1|\varphi_2\rangle\langle\varphi_2|N-1\rangle \\ &= \frac{N-t}{N}|0\rangle\langle 0| + \frac{t}{N}|1\rangle\langle 1|\end{aligned} \tag{47}$$

Thus, $\rho_{\widetilde{S}}$ is the average state of $\widetilde{S}$. based on Holevo bound [14], we can get

$$\begin{aligned}1 \leq \chi(\xi) &= S(\rho_{\widetilde{S}}) - \frac{1}{N}\sum_{x=0}^{N-1} S(\rho_{\widetilde{S}}(x)) \\ &= S(\rho_{\widetilde{S}}) \\ &= S(\frac{N-t}{N}|0\rangle\langle 0| + \frac{t}{N}|1\rangle\langle 1|)\end{aligned} \tag{48}$$

Get the maximum value at $t = \frac{N}{2}$. namely

$$I \leq S\left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right) = 1 \tag{49}$$

It is the upper bound that the clients can get from $\widetilde{S}$ through the measurement. But the client U_2 does not know the random r which is selected by the server U_1 , so $H(r) = 1$ ($H(.)$is Shannon entropy and $S(.)$is Von Neumann entropy). Namely, it encrypts $f_{A_1}(x)$ by using the random R in one-time pad method. So, from $|\varphi_2\rangle$, U_2 cannot get the information of $f_{A_1}(x)$.

In addition, if the client does not honestly execute this protocol, he can send a fake state $|X\rangle$to the server, instead of the state $|\varphi_1\rangle$. Accordingly, the returned state from the server will be $|x\rangle|r \oplus f_{A_1}(x)\rangle$, not $|\varphi_2\rangle$. Due to the random number r obviously the client can still not get any information about $f_{A_1}(x)$.

So, the client A_i can't get the information of $f_{A_1}(x)$, due to the random r. Therefore, in QSMS-IC protocol, the client A_i can't get the set elements of A_1 except the set size n_{c_i}. similarly the client A_1 also can't get the information of the elements of A_i set except the set size.

5 Conclusion

In this paper, we proposed a protocol called Quantum Secure Multiparty Set Intersection Cardinality Protocol to privately compute the cardinality of set intersection. Unlike the classical PSI-CA protocols, the proposed QSMS-IC protocol achieves the unconditional security, because it is guaranteed by the basic principle of quantum mechanics; compared with quantum PSI-CA protocol for two-party set Intersection, the proposed protocol can achieve multi-party set intersection. In addition, our proposed scheme is very simple to deal with dynamic updating, because it only needs to compute some set operations if adding or deleting a new client. What's more, the applications of the protocol is frequently used in large-scale social networks, for instance, users can privately calculate the common hobbies.

References

1. Vu, D.H., Luong, D., Ho, T.B.: An Eefficient approach for secure multi-party computation without authenticated channel, Information Sciences online (2019)
2. Zhao, C., Zhao, S.N., Zhao, M.H., Chen, Z.X., Gao, C.Z., Li, H.W., Tan, Y.A.: Secure multi-party computation: Theory, practice and applications. Inform. Sci. **476**, 357–372 (2019)
3. Wang, Z., Cheung, S.C.S., Luo, Y.: Information theoretic secure multi-party computation with collusion deterrence. IEEE Trans. Inf. Forensi. Secur. **4**(12), 980–995 (2017)
4. Xu, L., bao, T., Zhu, L.H., Zhang, Y.: Trust-based privacy-preserving photo sharing in online social networks. IEEE Trans. Multimed. **21**(3), 591–602 (2019)

5. Xiong, H., Zhang, H., Sun, J.F.: Attribute-based privacy-preserving data Sharing for dynamic groups in cloud computing. IEEE Syst. J. **3**(13), 2739–2750 (2019)
6. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: An efficient quantum scheme for private set intersection. Quantum Inf. Process **1**(15), 363–371 (2016)
7. Shi, R.H.: Quantum private computation of cardinality of set intersection and union, European Physical Journal. vol.12(72) (2018)
8. Shi, R.H., Mu, Y., Zhong, H., Zhang, S., Cui, J.: Quantum private set intersection cardinality and its application to anonymous authentication. Inform. Sci. **370-371**, 147–158 (2016)
9. Wen, Y.M., Gong, Z., Huang, Z.G., Qiu, W.D.: A new efficient authorized private set intersection protocol from Schnorr signature and its applications. Cluster Comput. J. Netw. Soft. Tools Appl. **1**, 287–297 (2018)
10. Shi, R.H.: Efficient quantum protocol for private set intersection cardinality. IEEE Access **6**, 73102–73109 (2018)
11. Cristofaro, E.D., Gasti, P., Tsudik, G.: Fast and private computation of cardinality of set intersection and union, cryptology and network security (CANC 2010), Springer. LNCS **7712**, 218–231 (2012)
12. Debnath, S.K., Dutta, R.: New realizations of efficient and secure private set intersection protocols preserving fairness. Inf. Secur. Crypt. **10157**, 254–284 (2017)
13. Kissner, L., Song, D.: Privacy-preserving set operations. In: Proc. advances in cryptology - Crypto 2005, Springer, LNCS 3621, pp. 241–257 (2005)
14. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proc. 28th annual ACM symposium on theory of computing, ACM, pp. 212–219 (1996)
15. Buccafurri, F., Fotia, L., Lax, G., Saraswat, V.: Analysis-preserving protection of user privacy against information leakage of social-network likes. Inf. Sci. **328**, 340–358 (2016)
16. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press, Cambridge (2010)
17. Boyer, M., Brassard, G., Hyer, P., Tapp, A.: Tight bounds on quantum searching Fortschritte der Physik. 46 **4-5**, 493–505 (1998)
18. Carminati, B., Ferrari, E., Guglielmi, M.: Detection of unspecified emergencies for controlled information sharing. IEEE Trans. Dependable Secure Comput. **6**(13), 630–643 (2016)
19. Xu, J., Schaar, M.V.D.: Efficient working and shirking in information sharing networks. IEEE J. Select. Areas Commun. **4**(33), 651–662 (2015)
20. Wang, X.A., Fatos, X.F., Luo, X.S., Zhang, S.W., Yong, D.: A privacy-preserving fuzzy interest matching protocol for friends finding in social networks. Soft Compu. **8**(22), 2517–2526 (2018)
21. Wu, M.E., Chang, S.Y., Lu, C.J., Sun, H.M.: A communicationefficient private matching scheme in Client-Server model. Inf. Sci. **275**, 348–359 (2014)
22. Diao, Z.J., Huang, C.F., Wang, K.: Quantum counting: Algorithm and error distribution. Acta Appl. Math. **118**, 147–159 (2012)
23. Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. Quantum Inf. Process. **16**, 225 (2017)
24. Vaidya, J., Shafiq, B., Fan, W., Mehmood, D., Lorenzi, D.: A random decision tree framework for privacy-preserving data mining. IEEE Trans. Dependable Secure Comput. **11**, 399–411 (2014)
25. Yao, A.: Protocols for secure computations, in Proc. 23th Annu, Symp. Found. Comput. Sci. (FOCS), pp. 160–164 (1982)
26. Narayanan, A., Thiagarajan, N., Lakhani, M., Hamburg, M., Boneh, D.: Location privacy via private proximity testing, in Proc. Netw. Distrib. Syst. Secur, Symp., Online (2011)
27. Wang, Q., Shi, R., Chen, Z., Wang, S.: A Quantum sealed auction protocol based on secret sharing. Int. J. Theor. Phys. **58**, 1128–1137 (2019)
28. Zhang, S., Wang, S., Wang, Q., Shi, R.: Quantum anonymous voting protocol with the privacy protection of the candidate. Int. J. Theor. Phys. **58**, 3323–3332 (2019)
29. Xu, G., Zou, X.: Security analysis of an arbitrated quantum signature scheme with bell states. Int. J. Theor. Phys. **55**(9), 1–15 (2016)
30. Chen, Y., Chou, J., Zhou, F.: A publicly verfiable quantum signature scheme based on asymmetruc quantum crytography. IACR Crypology e Print Archive **2019**, 24 (2019)

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