International Journal of Theoretical Physics (2021) 60:3514–3528
https://doi.org/10.1007/s10773-021-04925-7

Quantum Protocols for Private Set Intersection Cardinality and Union Cardinality Based on Entanglement Swapping

Yongli Wang[1] · Peichu Hu[1] · Qiuliang Xu[2,3]

Received: 25 May 2021 / Accepted: 2 August 2021 / Published online: 10 August 2021

Abstract
Quantum private set intersection cardinality (PSI-CA) and private set union cardinality (PSU-CA) are two specific primitives of classical secure multi-party computation. Because of the appearance of quantum algorithms such as Shor's algorithm, the secure multi-party computation protocols based on classical mathematical problems such as large integer factorization and discrete logarithm have been threatened potentially. Thus, as one of the most powerful resources, quantum mechanics is widely used to construct various secure multi-party computation protocols for the reason that it can provide unconditional security. In this paper, based on entanglement swapping between d-level Bell states and d-level cat states, a quantum protocol is built to perform the calculations of private set intersection cardinality and private set union cardinality. With the help of a semi-honest third party who does not collude with any participant, the proposed protocol can simultaneously calculate intersection cardinality and union cardinality of the private sets held by multiple participants who do not trust each other without revealing the intersection, the union and the sets themselves. The protocol can resist attacks from external, semi-honest TP and participants, even though $m - 1$ participants collude together (m is the number of participants). In addition, the algorithm in the protocol is deterministic.

Keywords Private set intersection cardinality · Private set union cardinality · Entanglement swapping · d-level Bell state · d-level cat state

1 Introduction

Today, we have entered the era of big data. Vigorous data analysis and processing technologies such as deep learning have been widely applied in many fields such as disease

✉ Qiuliang Xu
xuqiuliang@sdu.edu.cn

[1] School of Mathematics, Shandong University, Jinan, 250100, People's Republic of China

[2] School of Software, Shandong University, Jinan, 250101, People's Republic of China

[3] Key Laboratory of Shandong Province for Software Engineering, Jinan, 250101, People's Republic of China

prediction and business decision-making. In order to acquiring more useful value, it is necessary to share data from multiple owners for analysis and processing. However, considering issues such as data security and personal privacy, most data owners show a very cautious attitude when sharing their data. For example, hospitals need to share their medical information with each other, but do not want to disclose the privacy of any patients; manufacturers want to test their products according to industry standards, but do not want to leak their actual production data to any competitors. In response to these "data island" problems, secure multi-party computation (MPC) technology has appeared and made a significant contribution to the realization of the secure sharing of data. MPC was originally proposed by Yao [1] in 1982. It allows multiple participants who do not trust each other to perform collaborative calculations and ensures that no participant can get anything except the desired results. In other words, MPC technology can help participants further mine the value of their data through sharing them without disclosing their privacy.

As a specific primitive of MPC, private set intersection cardinality (PSI-CA) can perform computation task that multiple participants want to calculate the intersection cardinality of their secret sets without revealing the intersection and the sets themselves. Similar to PSI-CA, private set union cardinality (PSU-CA) can help multiple participants calculate the union cardinality of their secret sets, and keep the union and the sets themselves secret. PSI-CA protocol was originally proposed by Freedman et al. [2] in *EUROCRYPT* 2004. Subsequently, some other PSI-CA protocols were presented in Refs [3–6], etc. These protocols are based on traditional mathematical problems such as large integer factorization and discrete logarithm. However, due to the emergency of Shor's algorithm [7] that can solve these problems in polynomial time, the above-mentioned protocols may be potentially threatened by quantum computer.

In order to overcome the threat posed by quantum technology, one of the beneficial options is to utilize quantum mechanics to construct cryptographic primitives. For this work, it can be traced back to the proposal of BB84, which is a quantum key distribution protocol, and was put forward by Bennett and Brassard [8] in 1984. Since then, various quantum MPC protocols such as quantum protocol for millionaire problem [9], quantum private query [10, 11], quantum private comparison [12] and so on have been proposed and have shown great power due to the unconditional security they provide. Based on various technologies such as quantum Fourier transform and quantum counting [13], single photons [14], GHZ states [15], some quantum PSI-CA protocols were also constructed. However, in these proposed PSI-CA protocols, some complex oracle operators are required [13] or they are probabilistic [13, 14], besides, they can only support two or three participants to perform calculations. For these reasons, based on entanglement swapping between d-level Bell states and d-level cat states, we propose a secure quantum protocol to deterministically calculate private set intersection cardinality and private set union cardinality for multiple participants.

Our paper mainly consists of 7 sections. Besides the first section for introduction, the remaining sections are organized as below: Section 2 is devoted to introducing the preliminary knowledge used in our protocol, Section 3 is devoted to the details of the protocol. Sections 4 and 5 are devoted to analyzing the correctness and the security of our protocol, respectively, Section 6 is devoted to the comparison between our protocol and some existing protocols, the last section concludes our paper.

2 Preliminary Knowledge

In our proposed protocol, the d-level Bell states, the d-level cat states and the entanglement swapping between them are utilized usually. Below we firstly review some useful details about them to ensure the legibility of the rest of the content.

2.1 *d*-Level Bell States

The d-level Bell state originally introduced in Ref [16] is a generalization of the Bell states [17]. We can write out the explicit form of the d-level Bell states as follow,

$$|\Psi(u_1, u_2)\rangle := \frac{1}{\sqrt{d}} \sum_{g=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{gu_1} |g, g + u_2 \mod d\rangle,$$

where $u_1, u_2 \in \mathbb{Z}_d$. For $d = 2$, let u_1 and u_2 take values form 0, 1, respectively, we can get the classical Bell states,

$$\begin{aligned}
|\Psi(0,0)\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), \\
|\Psi(0,1)\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle), \\
|\Psi(1,0)\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle), \\
|\Psi(1,1)\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).
\end{aligned}$$

Through simple calculations, we can conclude that the d-level Bell states are pairwise orthogonal.

$$\begin{aligned}
\langle \Psi(v_1, v_2)|\Psi(u_1, u_2)\rangle &= \frac{1}{d} \sum_{g=0}^{d-1} \sum_{h=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{(gu_1 - hv_1)} \langle h|g\rangle \langle h + v_2 \mod d | g + u_2 \mod d\rangle \\
&= \frac{1}{d} \sum_{g=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{g(u_1 - v_1)} \langle g + v_2 \mod d | g + u_2 \mod d\rangle \\
&= \delta_{u_1 v_1} \delta_{u_2 v_2},
\end{aligned}$$

where

$$\delta_{uv} = \begin{cases} 1, & u = v \\ 0, & u \neq v \end{cases}$$

is Kronecker delta.

We can also get $|\Psi(0, 0)\rangle$ easily,

$$|\Psi(0,0)\rangle = \frac{1}{\sqrt{d}} \sum_{g=0}^{d-1} |g, g\rangle,$$

and by defining unitary operator

$$U_{u,v} := \sum_{g=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{gu} |g+v\rangle\langle g|,$$

we can get $|\Psi(u_1,u_2)\rangle$ from $|\Psi(0,0)\rangle$,

$$\begin{aligned}
\left(I \otimes U_{u_1,u_2}\right)|\Psi(0,0)\rangle &= \left(I \otimes \sum_{g'=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{g'u_1} |g'+u_2\rangle\langle g'|\right)\left(\frac{1}{\sqrt{d}}\sum_{g=0}^{d-1}|g,g\rangle\right) \\
&= \frac{1}{\sqrt{d}}\sum_{g=0}^{d-1}|g\rangle\left(\sum_{g'=0}^{d-1}\left(e^{\frac{2\pi i}{d}}\right)^{g'u_1}|g'+u_2\rangle\langle g'|g\rangle\right) \\
&= \frac{1}{\sqrt{d}}\sum_{g=0}^{d-1}\left(e^{\frac{2\pi i}{d}}\right)^{gu_1}|g\rangle|g+u_2\rangle \\
&= |\Psi(u_1,u_2)\rangle
\end{aligned} \tag{1}$$

where I is identical operator.

2.2 *d*-Level *n*-Particle Cat States

The d-level n-particle cat state, which was firstly introduced in Ref [18], is a generalization of the d-level Bell states from two qudits to n qudits. We can write out the form explicitly as below,

$$|\Psi(u_1,u_2,\ldots,u_n)\rangle := \frac{1}{\sqrt{d}}\sum_{g=0}^{d-1}\left(e^{\frac{2\pi i}{d}}\right)^{gu_1}|g,g+u_2,\ldots,g+u_n\rangle,$$

where $u_1,u_2,\ldots,u_n \in \mathbb{Z}_d$. It is not difficult to see that for $n=2$, they are reduced to d-level Bell states. In addition, when $n=3$ and $d=2$ they are the familiar 3-particle GHZ states [19, 20]. For example, the standard 3-particle GHZ state can be expressed as

$$|\Psi(0,0,0)\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right).$$

Similar to the d-level Bell states, d-level cat states are also pairwise orthogonal,

$$\langle\Psi(v_1,v_2,\ldots,v_n)|\Psi((u_1,u_2,\ldots,u_n))\rangle = \delta_{u_1v_1}\delta_{u_2v_2}\ldots\delta_{u_nv_n},$$

and they form a set of orthonomal basis of the d^n-dementional Hilbert space composed by n qudits.

2.3 Entanglement Swapping Between *d*-Level Bell States and *d*-Level Cat States

Entanglement Swapping between d-Level Bell States and d-Level Cat States was firstly introduced in Ref [18]. Imagine that we have a d-level Bell state and a d-level cat state. By performing d-level Bell measurement on one particle in the d-level Bell state and one particle in the d-level cat state the entanglement swapping occurs, and we obtain a new d-level

Bell state and a new d-level cat state. We can also use following mathematical expression to describe this process.

$$
\begin{aligned}
&|\boldsymbol{\Psi}(u,u')\rangle_{s,s'} \otimes |\boldsymbol{\Psi}(v_1,v_2,\ldots,v_i,\ldots,v_n)\rangle_{t_1,\ldots,t_i,\ldots,t_n} \\
&= \frac{1}{d}\sum_{g,h=0}^{d-1}\left(e^{\frac{2\pi i}{d}}\right)^{gh}|\boldsymbol{\Psi}(u-g,v_i-h)\rangle_{s,t_i} \\
&\otimes|\boldsymbol{\Psi}(v_1+g,v_2,\ldots,u'+h,\ldots v_n)\rangle_{t_1,\ldots,s',\ldots,t_n},
\end{aligned}
\tag{2}
$$

where s, s' are the labels of the two particles in the d-level Bell state, $t_1,\ldots,t_i,\ldots,t_n$ are the labels of the n particles in the d-level cat state. Particle s' and particle $t_i (2 \le i \le n)$ are the two particles on which the d-level Bell measurement is performed. Suppose that the measurement result is $|\boldsymbol{\Psi}(u-g,v_s-h)\rangle$, we obtain the new Bell state $|\boldsymbol{\Psi}(u-g,v_s-h)\rangle$ and the new cat state $|\boldsymbol{\Psi}(v_1+g,v_2,\ldots,u'+h,\ldots v_n)\rangle$.

In order to understand this process intuitively, we give out a figure (Fig. 1) to depict it. In the upper part of the figure, the horizontal line with n nodes represents the n-particle cat state, and the vertical line with two nodes represents the Bell state. The square nodes represent the first particles in the Bell state and the cat state which are not involved in the process of the entanglement swapping. The vertical downward arrow represents the d-level Bell measurement on the particle s and t_i, and $|\boldsymbol{\Psi}(u-g,v_i-h)\rangle$ is the measurement result. $|\boldsymbol{\Psi}(v_1+g,v_2,\ldots,u'+h,\ldots v_n)\rangle$ indicated by the broken line in the lower part of the figure is the swapped cat state.

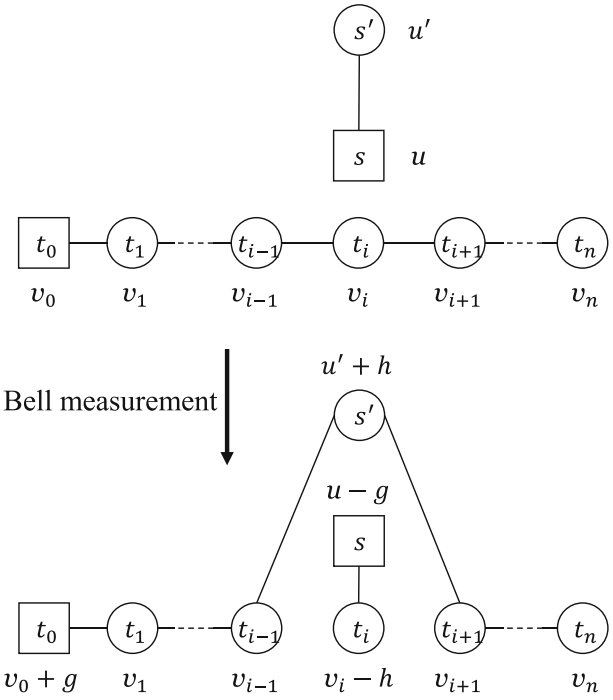

Fig. 1 Entanglement swapping between a Bell state and a cat state

3 The Proposed Protocol

Suppose that there exist $m(m \geq 2)$ participants named $P_1, P_2, \ldots, P_m$. Each $P_i(i = 1, 2, \ldots, m)$ holds a secret set A_i whose cardinality is less than or equal to N and whose elements are in $\mathbb{Z}_N$. We can express A_i as $\left(a_i^0, a_i^1, \ldots, a_i^{n_i}\right)$, where $a_i^j \in \mathbb{Z}_N (0 \leq j \leq n_i)$ and $n_i < N$. The participants hope to calculate the cardinalities of the intersection and the union of their secret sets with keeping their secret sets unknown to each other.

In the following, we propose a secure protocol to perform this task with the aid of a semi-honest TP introduced in Ref [21]. The semi-honest TP may misbehave himself as long as without collude with any participant. That is to say, in addition to not colluding with any other participants, TP is allowed to try his best, including actively eavesdropping, to obtain the participants' secrets. The protocol makes use of d-level Bell states and d-level cat states $(d > m)$.

Step 1: Each participant $P_i(i = 1, 2, \ldots, m)$ encodes his secret set $A_i = \left(a_i^0, a_i^1, \ldots, a_i^{n_i}\right)$ as below. First, P_i maps A_i to a binary set $\tilde{B}_i = \left(\tilde{x}_i^0, \tilde{x}_i^1, \ldots, \tilde{x}_i^{N-1}\right)$ according to the following rule:
for each j in $\mathbb{Z}_N$,

$$\tilde{x}_i^j = \begin{cases} 1, & \text{if } j \in A_i; \\ 0, & \text{if } j \notin A_i. \end{cases} \tag{3}$$

Second, P_i applies the permutation pre-shared privately by all participants except TP

$$\hat{P} = \begin{pmatrix} 1, & 2, & \ldots, & N \\ \hat{P}(1), & \hat{P}(2), & \ldots, & \hat{P}(N) \end{pmatrix}$$

on $\tilde{B}_i$ to mess it up and obtains a new binary set $B_i = \left(x_i^0, x_i^1, \ldots, x_i^{N-1}\right)$, where $x_i^j = \tilde{x}_i^{\hat{P}(j+1)-1} (j = 0, 1, \ldots, N-1)$. At last, P_i prepares N d-level Bell states $|\boldsymbol{\Psi}(0,0)\rangle$ and encodes B_i into d-level Bell states according to Formula (1),

$$|\boldsymbol{\Psi}(u_i^j, x_i^j)\rangle_{s_i^j, s'^j_i} = \left(I \otimes U_{u_i^j, x_i^j}\right) |\boldsymbol{\Psi}(0,0)\rangle,$$

where $j = 0, 1, \ldots, N-1$, u_i^j is randomly chose from $\mathbb{Z}_d$, s_i^j, s'^j_i are labels of the two particles of the j-th Bell state.

Step 2: TP first prepares N d-level $m+1$ particle cat states

$$|\boldsymbol{\Psi}(v_0^j, v_1^j, v_2^j, \ldots, v_m^j)\rangle_{t_0^j, t_1^j, \ldots, t_m^j},$$

where $j = 0, 1, 2, \ldots, N-1$, v_i^j is randomly chose from $\mathbb{Z}_d$, t_i^j is the label of the i-th particle of the j-th cat state $(i = 0, 1, 2, \ldots, m)$. For $i = 1, 2, \ldots, m$, TP extracts the i-th particle from each cat state to form a particle sequence labeled by $(t_i^0, t_i^1, t_i^2, \ldots, t_i^{N-1})$, which is denoted as Q_i. Then, TP prepares decoy particles for each Q_i to prevent from eavesdropping by randomly choosing particles from $\left\{|k\rangle, \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{jk} |j\rangle\right\} (k = 0, 1, \ldots, d-1)$ and inserting them into Q_i at random positions. The new particle sequence is denoted as Q_i'. Finally, TP sends particle sequence Q_i' to participant P_i. Note that the particle sequence labeled $(t_0^0, t_0^1, t_0^2, \ldots, t_0^{N-1})$ is kept by TP on his own.

Step 3: For each P_i, after he receives Q_i', TP first informs P_i of the positions and the bases of the decoy particles in Q_i', then P_i measures the decoy particles according

to the information that TP has told him and sends the measurement results to TP, finally, TP checks whether there exist eavesdroppers in the quantum channel in accordance with the results sent by P_i. If TP confirms that the channel is not secure, he aborts the protocol and restart a new one, otherwise he continues to perform the protocol.

Step 4: Each $P_i (i = 1, 2, \ldots, m)$ restores Q_i from Q_i' by discarding the decoy particles, and then performs N times d-level Bell measurements on the first particles from his own Bell states and the particles sent by TP. Concretely, for $j = 0, 1, \ldots, N-1$, P_i jointly measures the particle labeled by s_i^j from the Bell state $|\Psi(u_i^j, x_i^j)\rangle_{s_i^j, s'^j_i}$ and the particle labeled by t_i^j from the cat state $|\Psi(v_0^j, v_1^j, v_2^j, \ldots, v_m^j)\rangle_{t_0^j, t_1^j, \ldots, t_m^j}$. Suppose that the measurement results are $|\Psi(r_i^j, r'^j_i)\rangle_{s_i^j, t_i^j}$, where $r_i^j = u_i^j - g_i^j \mod d, r'^j_i = v_i^j - h_i^j \mod d$.

Step 5: All participants cooperate to compute

$$R^j = \sum_{i=1}^{m} r'^j_i \tag{4}$$

for $j = 0, 1, 2, \ldots, N-1$. In order to prevent TP from eavesdropping on the data transmitted in this process, r'^j_i can be encrypted with a pre-shared key in advance. Next, the R^j and the particle sequences labeled by $(s'^0_i, s'^1_i, \ldots, s'^{N-1}_i)$ are sent to TP. Similar to Step 3, the decoy state particles are used to prevent others from eavesdropping.

Step 6: After receiving all particle sequences sent by all participants, for $j = 0, 1, 2, \ldots, N-1$, TP performs d-level cat state measurement on d-level $m+1$ particle cat state labeled by $(t_0^j, s'^j_1, s'^j_2, \ldots, s'^j_m)$, and gets the result, for example,

$$|\Psi(\tilde{r}_0^j, \tilde{r}_1^j, \tilde{r}_2^j, \ldots, \tilde{r}_m^j)\rangle,$$

where

$$\begin{aligned} \tilde{r}_0^j &= v_0^j + \sum_{i=1}^{m} g_i^j \mod d, \\ \tilde{r}_i^j &= x_i^j + h_i^j \mod d, (i = 1, 2, \ldots, m). \end{aligned}$$

Next, TP generates two variables C_I, C_U and initiates them to zero. For each j in $\mathbb{Z}_N$, TP computes

$$X_j = \sum_{i=1}^{m} \tilde{r}_i^j + R^j - \sum_{i=1}^{m} v_i^j \mod d, \tag{5}$$

and updates the values of C_I, C_U according to

$$C_I = \begin{cases} C_I + 1, & \text{if } X_j = m; \\ C_I, & \text{if } X_j \neq m, \end{cases}$$

$$C_U = \begin{cases} C_U + 1, & \text{if } X_j > 0; \\ C_U, & \text{if } X_j = 0. \end{cases}$$

At last, TP obtains the intersection cardinality C_I and the union cardinality C_U and announces them to all participants.

4 Correctness Analysis

In this section we will explain why our protocol is correct. Each participant P_i has a secret set $A_i = \left(a_i^0, a_i^1, \ldots, a_i^{n_i}\right)$. In step 1, the set A_i is mapped to $\tilde{B}_i = \left(\tilde{x}_i^0, \tilde{x}_i^1, \ldots, \tilde{x}_i^{N-1}\right)$ in accordance with Formula (3). That is, for $j = 0, 1, \ldots, N-1$,

$$\tilde{x}_i^j = \begin{cases} 1, & \text{if } j \in A_i; \\ 0, & \text{if } j \notin A_i. \end{cases}$$

Then the set $\tilde{B}_i$ is shuffled into $B_i = \left(x_i^0, x_i^1, \ldots, x_i^{N-1}\right)$ by a random permutation $\hat{P}$, where $x_i^j = \tilde{x}_i^{\hat{P}(j+1)-1} (j = 0, 1, \ldots, N-1)$. Let's give a simple example. Assuming $N = 7$, $A_i = (1, 4, 5)$ and

$$\hat{P} = \begin{pmatrix} 0, & 1, & 2, & 3, & 4, & 5, & 6 \\ 3, & 6, & 4, & 1, & 5, & 0, & 2 \end{pmatrix},$$

thus, $\tilde{B}_i = (0, 1, 0, 0, 1, 1, 0)$ can be obtained after mapping, and then $B_i = (0, 0, 1, 1, 1, 0, 0)$ can be obtained after shuffling.

At the end of step 1, B_i is encoded into N d-level Bell states and the following particle sequence are formed,

$$|\boldsymbol{\Psi}(u_i^0, x_i^0)\rangle_{s_i^0, s'^0_i}, |\boldsymbol{\Psi}(u_i^1, x_i^1)\rangle_{s_i^1, s'^1_i}, \ldots, |\boldsymbol{\Psi}(u_i^{N-1}, x_i^{N-1})\rangle_{s_i^{N-1}, s'^{N-1}_i}.$$

TP prepares N d-level $m+1$ particle cat states

$$\begin{aligned} &|\boldsymbol{\Psi}(v_0^0, v_1^0, v_2^0, \ldots, v_m^0)\rangle_{t_0^0, t_1^0, \ldots, t_m^0}, \\ &|\boldsymbol{\Psi}(v_0^1, v_1^1, v_2^1, \ldots, v_m^1)\rangle_{t_0^1, t_1^1, \ldots, t_m^1}, \\ &\ldots, \\ &|\boldsymbol{\Psi}(v_0^{N-1}, v_1^{N-1}, v_2^{N-1}, \ldots, v_m^{N-1})\rangle_{t_0^{N-1}, t_1^{N-1}, \ldots, t_m^{N-1}}. \end{aligned}$$

For $j = 0, 1, \ldots, N-1$, P_i performs d-level Bell measurement on the particle s_i^j from his own Bell state and the particle t_i^j from TP's cat state with the measurement result $|\boldsymbol{\Psi}(u_i^j - g_i^j \mod d, v_i^j - h_i^j \mod d)\rangle$. After all participants complete Bell measurements, according to Formula (2), the j-th cat state becomes

$$\begin{aligned} |\boldsymbol{\Psi}(v_0^j + \sum_{i=1}^{m} g_i^j \quad &\mod d, \\ x_1^j + h_1^j \quad &\mod d, \\ x_2^j + h_2^j \quad &\mod d, \\ &\ldots, \\ x_m^j + h_m^j \quad &\mod d)\rangle. \end{aligned}$$

This process and result can be visually showed in Fig. 2 (the superscript j is omitted).

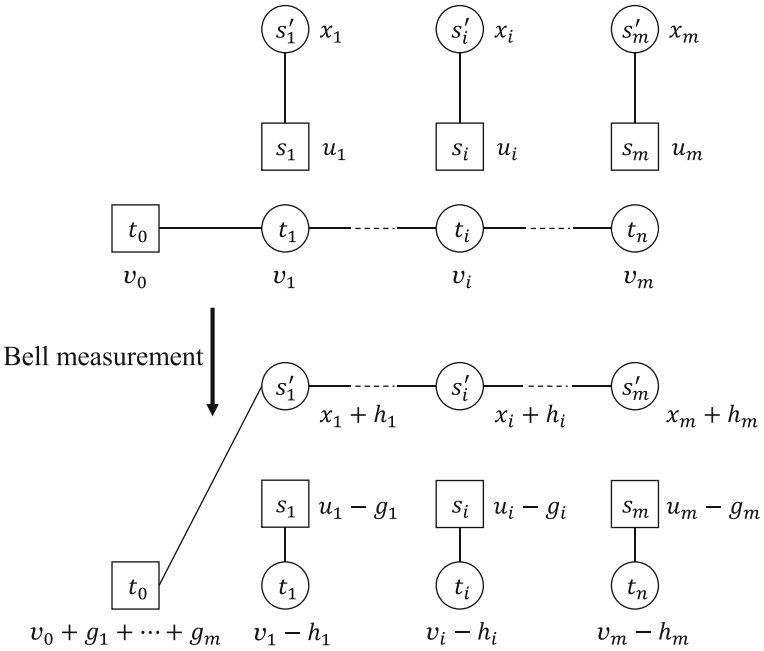

Fig. 2 Entanglement swappings between n Bell states and a cat state

We can rewrite Formula (4) as

$$\begin{aligned}\sum_{i=1}^{m} r'^{j}_{i} &= \sum_{i=1}^{m} \left(v_i^j - h_i^j \mod d\right) \\ &= \sum_{i=1}^{m} v_i^j - \sum_{i=1}^{m} h_i^j + \alpha d,\end{aligned}$$

where $\alpha \leq m$ is the number of occurrences of modular operations. In Formula (5), $\sum_{i=1}^{m} \tilde{r}_i^j$ can be rewritten as

$$\begin{aligned}\sum_{i=1}^{m} \tilde{r}_i^j &= \sum_{i=1}^{m} \left(x_i^j + h_i^j \mod d\right) \\ &= \sum_{i=1}^{m} x_i^j + \sum_{i=1}^{m} h_i^j - \beta d\end{aligned}$$

where $\beta \leq m$ is also the number of occurrences of modular operations. Thus, $X_j = \sum_{i=1}^{m} x_i^j$ can be calculated as follow,

$$X_j = \sum_{i=1}^{m} x_i^j = \sum_{i=1}^{m} \tilde{r}_i^j + \sum_{i=1}^{m} r'^{j}_{i} - \sum_{i=1}^{m} v_i^j - (\alpha - \beta)d.$$

Consider $d > m$ and therefore $\sum_{i=1}^{m} x_i^j < d$, we have

$$X_j = \sum_{i=1}^{m} \tilde{r}_i^j + R^j - \sum_{i=1}^{m} v_i^j \mod d.$$

Obviously, X_j is the number of "1"s in the j-th (starting from 0) position of all $B_i (i = 1, 2, \ldots, m)$. If $X_j = m$, it means that every participant has $\hat{P}^{-1}(j)$ in his secret set, namely, $\hat{P}^{-1}(j)$ is in the $\bigcap_{i=1}^{m} A_i$. By counting the number of $X_j = m$ for $j = 0, 1, \ldots, N-1$, we can obtain the cardinality of the intersection $\bigcap_{i=1}^{m} A_i$, i.e. $C_I = |\bigcap_{i=1}^{m} A_i|$. Similarly, If $X_j > 0$, it means that at least one participant has $\hat{P}^{-1}(j)$ in his secret set, namely, $\hat{P}^{-1}(j)$ is in the $\bigcup_{i=1}^{m} A_i$. Through counting the number of $X_j > 0$ for $j = 0, 1, \ldots, N-1$, we can get the cardinality of the union $\bigcup_{i=1}^{m} A_i$, i.e. $C_U = |\bigcup_{i=1}^{m} A_i|$. Therefor, the correct result can be acquired by performing our proposed protocol.

5 Security Analysis

In this section, it is showed that our protocol can resist three types of threats: external attack, participants' attack and semi-honest TP's attack. For defending against external attack, it is showed that the external eavesdroppers cannot steal the secret set held by every participant. For defending against participants' attack, it is showed that at most $n-1$ dishonest participants who collude together cannot succeed. For defending against semi-honest TP's attack, it is showed that the TP cannot successfully steal the secrets as long as he does not collude with any participants.

5.1 External Attack

In this subsection, we analyze the reason why the eavesdroppers from outside cannot obtain the secrets in each step of the protocol.

In Step 1, Step 3 and Step 4, since neither quantum nor classical information is transmitted, any external eavesdroppers cannot obtain anything useful.

In Step 2, the qudits from d-level cat states prepared by semi-honest TP are transmitted. Therefor, some attacks, for example, intercept–resend attack, entangle–measure attack and measure–resend attack, may be launched by eavesdroppers. Our protocol use decoy states [22] to prevent outside eavesdroppers from stealing secrets through these attacks. Just like BB84 protocol [8], decoy state technology is an effective means to check whether there are outside eavesdroppers. In the process of transporting qudit particle sequences, decoy state particles are randomly inserted into them. Similar to the reason analyzed in Ref [23], the decoy states in d-level quantum system can also ensure the security of qudit sequences transportation. If an outside eavesdropper exists, he can be detected efficiently. Moreover, the qudit sequences transmitted in this step does not carry any participants' secret information and therefore nothing can be stolen.

In Step 5, $R^j (j = 0, 1, \ldots, N-1)$ is transmitted to TP. Because R^j is independent of x_i^j, there is no information about x_i is leaked. In the quantum transmission stage, just as in Step 2, decoy particles are utilized and eavesdroppers can be detected. In addition, we can know that there are not any information leaked while particles s'^j_i are transmitted to TP through the following analysis. After each participant P_i completes the d-level Bell measurement,

the density operator of the j-th quantum system $\bigotimes_{i=1}^{m} |\Psi(u_i^j, x_i^j)\rangle \otimes |\Psi(v_0^j, v_1^j, \ldots, v_n^j)\rangle$ becomes

$$\rho = \left(\bigotimes_{i=1}^{m} |\Psi(u_i, u'_i)\rangle \otimes |\Psi(v_0, v_1, \ldots, v_m)\rangle\right) \left(\bigotimes_{i=1}^{m} \langle\Psi(u_i, u'_i)| \otimes \langle\Psi(v_0, v_1, \ldots, v_m)|\right),$$

where

$$\begin{aligned} u_i &= u_i^j - g_i^j, \quad u'_i = v_i^j - h_i^j, \\ v_0 &= v_0^j + \sum_{i=1}^{m} g_i^j, \\ v_i &= x_i^j + h_i^j, \quad (i = 1, 2, \ldots, m). \end{aligned}$$

Tracing out the other qudits, we get the reduced density operator of the qudit s'^j_i,

$$\begin{aligned} \rho_{s'^j_i} &= \mathrm{Tr}_{others}(\rho) \\ &= \mathrm{Tr}'\left(|\Psi(v_0, v_1, \ldots, v_m)\rangle\langle\Psi(v_0, v_1, \ldots, v_m)|\right) \\ &= \frac{1}{d}\mathrm{Tr}'\left[\left(\sum_{g=0}^{d-1}\left(e^{\frac{2\pi i}{d}}\right)^{gv_0} |g, \ldots, g + v_i\rangle\right)\right. \\ &\qquad \left.\left(\sum_{g'=0}^{d-1}\left(e^{\frac{-2\pi i}{d}}\right)^{g'v_0} \langle g', \ldots, g' + v_i|\right)\right] \\ &= \frac{1}{d}\sum_{g=0}^{d-1} |g + v_i\rangle\langle g + v_i| \\ &= \frac{I}{d}, \end{aligned}$$

where Tr' stands for tracing out qudits labeled by $t_0^j, s'^j_1, \ldots, s'^j_{i-1}, s'^j_{i+1}, \ldots, s'^j_m$, I is identical operator. So, the qudit s'^j_i is completely depolarized and no information is leaked while it is being transmitted.

In Step 6, TP announces the final results and the external attackers can not obtain any participants' secret.

5.2 Participants' Attack

As a powerful form of attack, participants' attack [24] is launched by either one or more dishonest participants. In situation involving multiple dishonest participants, the collusion between them need to be considered. Below, we will analyze the security of our protocol under the attacks launched by one dishonest participant and by multiple conspiring dishonest participants, respectively.

First, we analyze the security in the case of only one dishonest participant attacking the protocol. Without loss of generality, we suppose that P_1 wants to steal other participants' secret sets or the intersection or the union. In our protocol, there is no qudit particle transmission between P_1 and other participants, and the qudit particle transmission only exists between participants and the semi-honest TP. If P_1 wants to steal information, he must intercept the qudit particles transmitted between TP and other participants in Step 2 and Step 5. Thus, P_1 can be revealed just like an outside eavesdropper due to the use of decoy particles and cannot obtain any useful information from the intercepted particles for the same reason analyzed in the above subsection. In Step 5, R^j can be known by P_1, but it is helpless for P_1 to get x_i because x_i and R^j are not related. In addition, because P_1 does not collude with TP, he cannot know which "j" satisfies $X_j = m$ or $X_j > 0$, namely, he cannot know the positions of the elements in the intersection or in the union. Even though he knows the random permutation, he cannot obtain the intersection or the union. Therefore, a dishonest participant cannot steal the corresponding secrets held by other participants.

Second, we analyze the security of the protocol when multiple dishonest participants collude together. In order to explain the security to a greater extent, we consider the extreme case, that is, there are $m-1$ participants collude together to steal the set held by the remaining one participant or the intersection or the union. Without loss of generality, we suppose that $P_1, P_2, \ldots, P_{m-1}$ collude together to steal the secret set of P_m. Since P_m only transmits qudit particles with TP, the conspiring dishonest participants need to intercept the particles transmitted between P_m and TP to obtain the secrets of P_m. Thus, they can be put in light as external attackers due to the utilization of decoy state technology and cannot obtain any useful information from the intercepted qudits since these qudits are completely depolarized. Besides, $P_1, P_2, \ldots, P_{m-1}$ cannot get x_m from R^j in Step 5 due to the independence of x_m and R^j, and cannot know the intersection and the union for the same reason mentioned above. So, even though up to $m-1$ dishonest participants collude together, they still cannot obtain the secrets they shouldn't deserve.

5.3 Semi-honest TP's Attack

In our proposed protocol, although the semi-honest TP can obtain $x_i^j + h_i^j$ and R^j, he still can not know x_i^j because h_i^j cannot be deduced from R^j if he does not collude with other participants. Furthermore, TP can not know the concrete elements in the intersection and the union of the secret sets since the random permutation is used. That is, TP cannot deduce the $\hat{P}^{-1}(j)$ from j because he does not know $\hat{P}$. So, a semi-honest TP, as long as he does not collude whit other participants, he cannot successfully obtain the secrets of the participants, including the secret sets themselves, the intersection and the union.

6 Comparison

In this section, we will compare our newly proposed protocol with some existing protocols in terms of quantum resource, quantum operators, quantum measurement, the maximum number of participants, the output and the type (probabilistic or deterministic). The details of the comparison are shown in Table 1. We can obviously find that our protocol has the significant advantages of simultaneously calculating the intersection cardinality and the union cardinality of multiple private sets with deterministic results.

Table 1 Comparison between our protocol and some existing protocols

Protocols	Ref. [13]	Ref. [14]	Ref. [15]	Our protocol
Quantum resources	Entangled states	Single photons	GHZ states	d-level Bell states and cat states
Quantum operators	Phase operator, QFT and QFT^{-1}	Qubit operator	Qubit operator	Qudit operator
Quantum measurements	Projective measurement	Projective measurement	Projective measurement	d-level Bell measurement
Maximum number of participants	2	2	3	$N(\geq 2)$
Outputs	$\|A \cap B\|$	$\|A \cap B\|$	$\|A \cap B \cap C\|$ and $\|A \cup B \cup C\|$	$\left\|\bigcap_{i=1}^{N} A_i\right\|$ and $\left\|\bigcup_{i=1}^{N} A_i\right\|$
Type	Probabilistic	Probabilistic	Deterministic	Deterministic

7 Conclusion

In this paper, based on the entanglement swapping between d-level Bell states and d-level cat states, we proposed a novel quantum protocol to simultaneously calculate private set intersection cardinality and private set union cardinality with the aid of a semi-honest TP. First, TP prepares d-level cat states and then distributes the corresponding part of them to each participant who wants to compute the intersection cardinality and the union cardinality without disclosing his own secret. Second, All participants encode their private sets into d-level Bell states and perform the measurements on the first particles of their own Bell states and the particles received from TP to complete the entanglement swapping. At last, TP performs d-level cat state measurements on the particles sent back by all participants and calculate the final result. In the case of TP and participants not colluding, our protocol can resist attacks from external attackers, participants and semi-honest TP, even though at most $m - 1$ participants collude together (m is the number of participants).

Acknowledgements This work was supported in part by the National Natural Science Foundation of China (No. 61632020), the Science and Technology Innovation Bases Special Project of Key Laboratory of Shandong Province for Software Engineering(No. 11480004042015), the NSFC of Shandong (No. ZR2018MA014), the PCSIRT (No. IRT1264), and the Fundamental Research Funds of Shandong University (No. 2017JC019).

Declarations

Conflict of Interests The authors declared that they have no conflicts of interest to this work.

References

1. Yao, A.C.: In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science 1982, pp. 160–164 (1982)
2. Freedman, M.J., Nissim, K., Pinkas, B.: In: Cachin, C., Camenisch, J. (eds.) Proceedings of EUROCRYPT, pp. 1–19. Springer, Berlin (2004)
3. Kissner, L., Song, D.: In: Franklin, M. (ed.) Proceedings of CRYPTO, pp. 241–257. Springer, Berlin (2005)
4. Cristofaro, E.D., Gasti, P., Tsudik, G.: In: Proceedings of Cryptology and Network Security, pp. 218–231. Springer, Berlin (2012)
5. Debnath, S.K., Dutta, R.: In: Proceedings of International Information Security Conference, pp. 209–226. Springer, Berlin (2015)
6. Debnath, S.K., Stanica, P., Kundu, N., Choudhury, T.: Adv. Math. Commun. **15**(2), 365 (2021)
7. Shor, P.: In: Proc. of 35th Annual Symposium on the Foundations of Computer Science, pp. 124–134. IEEE Computer Society Press, Los Alamitos, CA (1994)
8. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference on Computers, Bangalore, Indian, pp. 175–179 (1984)
9. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Opt. Commun. **284**(1), 545 (2011)
10. Wei, C.Y., Cai, X.Q., Wang, T.Y., Qin, S.J., Gao, F., Wen, Q.Y.: IEEE J. Sel. Areas Commun. **38**(3), 517 (2020)
11. Gao, F., Qin, S.J., Huang, W., Wen, Q.Y.: Sci. China: Phys. Mech. Astron. **62**(7), 070301 (2019)
12. Yang, Y.G., Wen, Q.Y.: J. Phys. A Math. Theor. **42**(5), 055305 (2009)
13. Shi, R., Mu, Y., Zhong, H., Zhang, S., Cui, J.: Inform. Sci. **370**, 147 (2016)
14. Shi, R.H., Zhang, M.W.: IEEE Access **7**, 72105 (2019)
15. Zhang, C., Long, Y.X., Sun, Z.W., Li, Q., Huang, Q.: Sci. Rep. **10**(1), 22246 (2020)
16. Cerf, N.J.: Acta Physica Slovaca **48**(3), 115 (1998)
17. Bell, J.S.: Physics **1**(3), 195 (1964)
18. Karimipour, V., Bagherinezhad, S., Bahraminasab, A.: Phys. Rev. A **65**(4), 042320 (2002)

19. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Bell's Theorem, Quantum Theory and Conceptions of the Universe, pp. 69–72. Kluwer Academic, Dordrecht (1989). Chap. Going Beyond Bell's Theorem
20. Greenberger, D.M., Horne, M.A., Shimony, A., Zeilinger, A.: Am. J. Phys. **58**(12), 1131 (1990)
21. Yang, Y.G., Xia, J., Jia, X., Hua, Z.: Quantum Inf. Process. **12**(2), 877 (2013)
22. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Chin. Phys. Lett. **22**(5), 1049 (2005)
23. Chen, Y., Man, Z.X., Xia, Y.J.: Chin. Phys. Lett. **24**(1), 19 (2007)
24. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Quantum Inf. Comput. **7**(4), 329 (2007)