scientific reports

OPEN

Three-party quantum private computation of cardinalities of set intersection and union based on GHZ states

Cai Zhang[1]✉, Yinxiang Long[2], Zhiwei Sun[3]✉, Qin Li[4] & Qiong Huang[1]✉

Private Set Intersection Cardinality (PSI-CA) and Private Set Union Cardinality (PSU-CA) are two cryptographic primitives whereby two or more parties are able to obtain the cardinalities of the intersection and the union of their respective private sets, and the privacy of their sets is preserved. In this paper, we propose a three-party protocol to finish these tasks by using quantum resources, where every two, as well as three, parties can obtain the cardinalities of the intersection and the union of their private sets with the help of a semi-honest third party (TP). In our protocol, GHZ states play a role in encoding private information that will be used by TP to compute the cardinalities. We show that the presented protocol is secure against well-known quantum attacks. In addition, we analyze the influence of six typical kinds of Markovian noise on our protocol.

Quantum key distribution is one kind of important cryptographic protocols based on quantum mechanics, in which any outside eavesdropper attempting to obtain the secret key shared by two users will be detected. The successful detection comes from Heisenberg's uncertainty principle: the measurement of a quantum system, which is required to obtain information of that system, will generally disturb it. The disturbances provide two users with the information that there exists an outside eavesdropper, and they can therefore abort the communication. Nowadays, most people need to share some of their private information for certain services such as products recommendation for online shopping and collaborations between two companies depending on their comm interests. Private Set Intersection Cardinality (PSI-CA) and Private Set Union Cardinality (PSU-CA), which are two primitives in cryptography, involve two or more users who intend to obtain the cardinalities of the intersection and the union of their private sets through the minimum information disclosure of their sets[1–3].

The definition of Private Set Intersection (PSI), also called Private Matching (PM), was proposed by Freedman[4]. They employed balanced hashing and homomorphic encryption to design two PSI protocols and also investigated some variants of PSI. In 2012, Cristofaro et al.[1] developed several PSI-CA and PSU-CA protocols with linear computation and communication complexity based on the Diffie-Hellman key exchange which blinds the private information. Their protocols were the most efficient compared with the previous classical related ones. There are also other classical PSI-CA or PSU-CA protocols[5–8]. Nevertheless, the security of these protocols relies on the unproven difficulty assumptions, such as discrete logarithm, factoring, and quadratic residues assumptions, which will be insecure when quantum computers are available[9–11].

For the sake of improving the security of PSI-CA protocols for two parties, Shi et al.[3] designed a probabilistic protocol where multi-qubit entangled states, complicated oracle operators, and measurements in high N-dimensional Hilbert space were utilized. And the same method in Ref.[3] was later used to develop a PSI-CA protocol for multiple parties[12]. For easy implementation of a protocol, Shi et al.[13] leveraged Bell states to construct another protocol for PSI-CA and PSU-CA problems that was more practical than that in Ref.[3]. In both protocols Ref.[3] and Ref.[13], only two parties who intend to get the cardinalities of the intersection and the union of their private sets are involved. Although Ref.[12] works for multiple parties, it only solves the PSI-CA problem and requires multi-qubit entangled states, complicated oracle operators, and measurements. It then interests us that how we could design a more practical protocol for multiple parties to simultaneously solve PSI-CA and PSU-CA problems. Inspired

[1]College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China. [2]Department of Automation Engineering, Guangdong Technical College of Water Resources and Electric Engineering, Guangzhou 510925, China. [3]School of Artificial Intelligence, Shenzhen PolyTechnic, Shenzhen 518055, China. [4]School of Computer Science, Xiangtan University, Xiangtan 411105, China. ✉email: zhangcai@scau.edu.cn; smeker@szpt.edu.cn; qhuang@scau.edu.cn

by Shi et al.'s work, we are thus trying to design a three-party protocol to solve PSI-CA and PSU-CA problems, where every two and three parties can obtain the cardinalities of the intersection and the union of their respective private sets with the aid of a semi-honest third party (TP). TP is semi-honest means that he loyally executes the protocol, makes a note of all the intermediate results, and might desire to take other parties' private information, but he cannot collude with dishonest parties. We then give a detailed analysis of the presented protocol's security. Besides, the influence of six typical kinds of Markovian noise on our protocol is also analyzed.

Preliminaries

First of all, we introduce the properties of GHZ states, and then give a detailed description of our protocol.

The standard GHZ three-qubit state is usually given by

$$|\varphi_{000}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{1}$$

Let $U = ZX$, where $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Combining U and $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, we can deduce the following equations:

$$\begin{aligned}
(U \otimes I \otimes I)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle) = |\varphi_{100}\rangle,\\
(I \otimes U \otimes I)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|101\rangle - |010\rangle) = |\varphi_{010}\rangle,\\
(I \otimes I \otimes U)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle) = |\varphi_{001}\rangle,\\
(U \otimes U \otimes I)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) = |\varphi_{110}\rangle,\\
(U \otimes I \otimes U)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|101\rangle + |010\rangle) = |\varphi_{101}\rangle,\\
(I \otimes U \otimes U)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle) = |\varphi_{011}\rangle,\\
(U \otimes U \otimes U)|\varphi_{000}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = |\varphi_{111}\rangle.
\end{aligned} \tag{2}$$

Note that Eqs. (1)–(2) form a basis (we call it GHZ basis hereafter) for the space of the three-qubit quantum system.

Results

The proposed protocol.

Our protocol will satisfy the following requirements:

(1) *Correctness* The respective cardinalities of the intersection and the union of every two and three parties' sets are correct.
(2) *Privacy* TP and dishonest parties cannot learn about the elements of any party's set.
(3) *Fairness* All the parties are perfect peer entities and they can get the cardinalities with equal opportunities.

In our protocol, TP is assumed to be semi-honest which means that he honestly follows the protocol, writes down all the intermediate results and might attempt to obtain the elements of any party's private set, but he cannot be collusive with any dishonest party.

Suppose that Alice, Bob and Charlie have private sets $A = \{a_1, a_2, \ldots, a_l\}$, $B = \{b_1, b_2, \ldots, b_m\}$ and $C = \{c_1, c_2, \ldots, c_n\}$, respectively, and each element of these sets lies in Z_p, where $Z_p = \{0, 1, 2 \ldots, p-1\}$ and p is a large prime number. TP helps compute the cardinalities $|A \cap B|$ $(|A \cup B|)$, $|A \cap C|$ $(|A \cup C|)$, $|B \cap C|$ $(|B \cup C|)$, and $|A \cap B \cap C|$ $(|A \cup B \cup C|)$. Our protocol works as follows:

(*Step 1*) Alice, Bob and Charlie run a Quantum Key Agreement (QKA) protocol[14–16] to share a secret non-zero binary key k that corresponds to a secret integer over Z_p. Then, Alice, Bob and Charlie compute

$$\begin{aligned}
A^* &= \{ka_1 \text{ (mod } p), \ldots, ka_l \text{ (mod } p)\},\\
B^* &= \{kb_1 \text{ (mod } p), \ldots, kb_m \text{ (mod } p)\},
\end{aligned}$$

and

$$C^* = \{kc_1 \text{ (mod } p), \ldots, kc_n \text{ (mod } p)\},$$

respectively.

(*Step 2*) Alice, Bob and Charlie encode their respective sets A^*, B^* and C^* into three private vectors over Z_p^2 as follows: Alice constructs a private vector $(x_0, x_1, \ldots, x_{p-1}) \in Z_2^p$, where $x_i = 1$ if $i \in A^*$ and $x_i = 0$, otherwise, for $i = 0, 1, \ldots, p-1$; Bob produces a private vector $(y_0, y_1, \ldots, y_{p-1}) \in Z_2^p$, where $y_i = 1$ if $i \in B^*$ and $y_i = 0$, otherwise, for $i = 0, 1, \ldots, p-1$; Charlie generates a private vector $(z_0, z_1, \ldots, z_{p-1}) \in Z_2^p$, where $z_i = 1$ if $i \in C^*$ and $z_i = 0$, otherwise, for $i = 0, 1, \ldots, p-1$.

(*Step 3*) TP prepares p GHZ states $(G_{A0}, G_{B0}, G_{C0}), (G_{A1}, G_{B1}, G_{C1}), \cdots, (G_{A(p-1)}, G_{B(p-1)}, G_{C(p-1)})$, with each GHZ state being in the state $|\varphi_{000}\rangle$. These GHZ states are referred to as encoding states. Next, TP divides all particles into three ordered sequences: $(G_{A0}, G_{A1}, \ldots, G_{A(p-1)})$, $(G_{B0}, G_{B1}, \ldots, G_{B(p-1)})$, and $(G_{C0}, G_{C1}, \ldots, G_{C(p-1)})$, which are denoted as T_A, T_B, and T_C, respectively.

(*Step 4*) TP generates $3d$ decoy particles, each of which is randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Afterwards, TP randomly inserts d decoy particles into T_A (T_B, T_C) to form a new sequence T'_A (T'_B, T'_C). TP then sends T'_A (T'_B, T'_C) to Alice (Bob, Charlie) through a quantum channel.

(*Step 5*) Confirming that Alice (Bob, Charlie) has successfully received T'_A (T'_B, T'_C), TP announces the inserted positions of all the d decoy particles in T'_A (T'_B, T'_C) and their corresponding measurement bases. Then, Alice (Bob, Charlie) measures all the decoy particles in the correct bases and announces the measurement results to TP. Next, TP compares the measurement results with their corresponding initial states. If the error rate is higher than the threshold determined by the channel noise, this protocol will be aborted. Otherwise, the protocol will continue to the next step.

(*Step 6*) Alice (Bob, Charlie) removes all the decoy particles from the sequence T'_A (T'_B, T'_C) to obtain the initial sequence T_A (T_B, T_C). For each particle in T_A (T_B, T_C), Alice (Bob, Charlie) performs U on G_{Ai} (G_{Bi}, G_{Ci}) $(i = 0, 1, \ldots, P-1)$ if $x_i = 1$ $(y_i = 1, z_i = 1)$; otherwise, Alice (Bob, Charlie) does nothing on G_{Ai} (G_{Bi}, G_{Ci}).

(*Step 7*) Alice (Bob, Charlie) prepares d decoy particles to detect eavesdropping. Each decoy states is randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Later, Alice (Bob, Charlie) randomly inserts these d decoy particles into T_A (T_B, T_C) to form a new sequence T^*_A (T^*_B, T^*_C), and writes down the positions and the states of these inserted states. At last, Alice (Bob, Charlie) sends T^*_A (T^*_B, T^*_C) to TP through a quantum channel.

(*Step 8*) Confirming that TP has successfully received T^*_A (T^*_B, T^*_C), Alice (Bob, Charlie) announces the inserted positions of all d decoy particles in T^*_A (T^*_B, T^*_C) and their corresponding measurement bases. TP measures all decoy particles in the correct bases and announces the measurement results. Alice (Bob, Charlie) then compares the measurement results with their corresponding initial states. If the error rate is higher than the threshold determined by the channel noise, the protocol will be aborted. Otherwise, the protocol will continue to the next step.

(*Step 9*) TP discards all decoy particles from T^*_A (T^*_B, T^*_C) to attain T_A (T_B, T_C). TP then selects eight variables S_{000}, S_{100}, S_{010}, S_{001}, S_{110}, S_{101}, S_{011} and S_{111} as the counters and sets them all to zero. Next, TP measures each trio $(G_{Ai}G_{Bi}G_{Ci})$ $(i = 0, 1, \ldots, p-1)$ in the GHZ basis. If the measurement result is $|\varphi_r\rangle$ $(r \in \{0,1\}^3)$, TP computes $S_r = S_r + 1$. Finally, TP can calculate the cardinalities $|A \cap B| = S_{110} + S_{111}$, $|A \cap C| = S_{101} + S_{111}$, $|B \cap C| = S_{011} + S_{111}$, $|A \cap B \cap C| = S_{111}$, $|A \cup B| = p - S_{000} - S_{001}$, $|A \cup C| = p - S_{000} - S_{010}$, $|B \cup C| = p - S_{000} - S_{100}$, and $|A \cup B \cup C| = p - S_{000}$.

Correctness and security analyzes.

In this section, we will analyze the correctness and the security of our protocol. Let us first give the analysis of the correctness.

Correctness. On the one hand, for any $x, y \in Z_p$ and $k \in Z_P - \{0\}$, $x = y$ if and only if $kx = ky$ $(mod\ p)$. It is easy to deduce that

$$\begin{aligned}
|A \cap B| &= |A^* \cap B^*|,\\
|A \cap C| &= |A^* \cap C^*|,\\
|B \cap C| &= |B^* \cap C^*|,\\
|A \cap B \cap C| &= |A^* \cap B^* \cap C^*|,\\
|A \cup B| &= |A^* \cup B^*|,\\
|A \cup C| &= |A^* \cup C^*|,\\
|B \cup C| &= |B^* \cup C^*|,\\
|A \cup B \cup C| &= |A^* \cup B^* \cup C^*|.
\end{aligned} \tag{3}$$

On the other hand, by the coding rules in (Step 2) and (Step 6), for any $i \in Z_p$, if $i \notin A^* \wedge i \notin B^* \wedge i \notin C^*$ $(i \in \overline{A^* \cup B^* \cup C^*})$, then $x_i = y_i = z_i = 0$, and Alice (Bob, Charlie) does nothing on the particle G_{Ai} (G_{Bi}, G_{Ci}) when she (he, he) receives it. TP will get the measurement result $|\varphi_{000}\rangle$ in step 9. Clearly, S_{000} is used to count the number of GHZ trios whose states are the same as their original states. The cardinality of the union of the sets A^*, B^* and C^* therefore equals $p - S_{000}$. Namely, $|A \cup B \cup C| = |A^* \cup B^* \cup C^*| = p - S_{000}$. Similarly, we

$i \in Z_p$	Alice's operations	Bob's operations	Charlie's operations	TP's measurment results
$i \in \overline{A^*} \cap \overline{B^*} \cap \overline{C^*}$	I	I	I	$\|\varphi_{000}\rangle$
$i \in A^* \cap \overline{B^*} \cap \overline{C^*}$	U	I	I	$\|\varphi_{100}\rangle$
$i \in \overline{A^*} \cap B^* \cap \overline{C^*}$	I	U	I	$\|\varphi_{010}\rangle$
$i \in \overline{A^*} \cap \overline{B^*} \cap C^*$	I	I	U	$\|\varphi_{001}\rangle$
$i \in A^* \cap B^* \cap \overline{C^*}$	U	U	I	$\|\varphi_{110}\rangle$
$i \in A^* \cap \overline{B^*} \cap C^*$	U	I	U	$\|\varphi_{101}\rangle$
$i \in \overline{A^*} \cap B^* \cap C^*$	I	U	U	$\|\varphi_{011}\rangle$
$i \in A^* \cap B^* \cap C^*$	U	U	U	$\|\varphi_{111}\rangle$

Table 1. The relationship between i and three parties' operations.

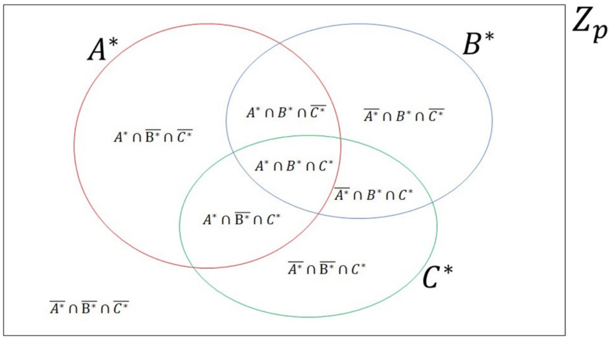
Z_p
A^*
B^*
$A^* \cap B^* \cap \overline{C^*}$
$\overline{A^*} \cap B^* \cap \overline{C^*}$
$A^* \cap \overline{B^*} \cap \overline{C^*}$
$A^* \cap B^* \cap C^*$
$\overline{A^*} \cap B^* \cap C^*$
$A^* \cap \overline{B^*} \cap C^*$
$\overline{A^*} \cap \overline{B^*} \cap C^*$
C^*
$\overline{A^*} \cap \overline{B^*} \cap \overline{C^*}$

Figure 1. The relationships among Z_p, A^*, B^* and C^*.

can analyze other cases where i belonging to different sets corresponds to three parties' different operations; see Table 1. From step 9, we have

$$\begin{aligned} S_{100} &= |A^* \cap \overline{B^*} \cap \overline{C^*}|, \\ S_{010} &= |\overline{A^*} \cap B^* \cap \overline{C^*}|, \\ S_{001} &= |\overline{A^*} \cap \overline{B^*} \cap C^*|, \\ S_{110} &= |A^* \cap B^* \cap \overline{C^*}|, \\ S_{101} &= |A^* \cap \overline{B^*} \cap C^*|, \\ S_{011} &= |\overline{A^*} \cap B^* \cap C^*|, \\ S_{111} &= |A^* \cap B^* \cap C^*|, \end{aligned} \tag{4}$$

where $\overline{A^*} = Z_p - A^*$, $\overline{B^*} = Z_p - B^*$, and $\overline{C^*} = Z_p - C^*$.

Furthermore, the relationships among A^*, B^*, C^* and Z_p can be illustrated by a Venn Diagram in Fig. 1, where red, blue, and green circles represent the sets A^*, B^* and C^*, respectively, and Z_p is the universal set. According to the Venn Diagram, we obtain the following equations:

$$
\begin{aligned}
|A^* \cap B^*| &= |A^* \cap B^* \cap \overline{C^*}| + |A^* \cap B^* \cap C^*| \\
&= S_{110} + S_{111}, \\
|A^* \cap C^*| &= |A^* \cap \overline{B^*} \cap C^*| + |A^* \cap B^* \cap C^*| \\
&= S_{101} + S_{111}, \\
|B^* \cap C^*| &= |\overline{A^*} \cap B^* \cap C^*| + |A^* \cap B^* \cap C^*| \\
&= S_{011} + S_{111}, \\
|A^* \cup B^*| &= |Z_p| - |\overline{A^*} \cap \overline{B^*} \cap C^*| - |\overline{A^*} \cap \overline{B^*} \cap \overline{C^*}| \\
&= p - S_{001} - S_{000}, \\
|A^* \cup C^*| &= |Z_p| - |\overline{A^*} \cap B^* \cap \overline{C^*}| - |\overline{A^*} \cap \overline{B^*} \cap \overline{C^*}| \\
&= p - S_{010} - S_{000}, \\
|B^* \cup C^*| &= |Z_p| - |A^* \cap \overline{B^*} \cap \overline{C^*}| - |\overline{A^*} \cap \overline{B^*} \cap \overline{C^*}| \\
&= p - S_{100} - S_{000}, \\
|A^* \cup B^* \cup C^*| &= |Z_p| - |\overline{A^*} \cap \overline{B^*} \cap \overline{C^*}| \\
&= p - S_{000}.
\end{aligned}
\tag{5}
$$

According to Eqs. (3)–(5), TP will finally obtain

$$
\begin{aligned}
|A \cap B| &= S_{110} + S_{111}, \\
|A \cap C| &= S_{101} + S_{111}, \\
|B \cap C| &= S_{011} + S_{111}, \\
|A \cap B \cap C| &= S_{111}, \\
|A \cup B| &= p - S_{001} - S_{000}, \\
|A \cup C| &= p - S_{010} - S_{000}, \\
|B \cup C| &= p - S_{100} - S_{000}, \\
|A \cup B \cup C| &= p - S_{000},
\end{aligned}
\tag{6}
$$

which are the correct results.

Security. In this subsection, we move on to the analysis of our protocol's security. Two kinds of attacks, outside and participant attacks, on our protocol will be considered. Outside attacks come from an outside eavesdropper, Eve. Participant attacks can be launched by TP or dishonest parties.

Outside attacks In our protocol, TP and three parties employ decoy particles to prevent eavesdropping, which is derived from the BB84 QKD protocol[17]. And it has been proven to be unconditionally secure[18]. As we know, BB84 protocol remains secure even if the quantum channel is noisy, and our protocol can thus work on the noisy channels as well. Any eavesdropping will be detected in (Step 5) or (Step 8). Concretely, since the decoy state is randomly chosen from the set $\{|0\rangle, |1\rangle|+\rangle|-\rangle\}$, it is in the state $\rho = \frac{I}{2}$. For any trio (G_{Ai}, G_{Bi}, G_{Ci}) $(i = 0, 1, \ldots, p-1)$, we have $\rho_{Ai} = \rho_{Bi} = \rho_{Ci} = \frac{I}{2} = \rho$. Eve thus cannot distinguish these two states. Without loss of generality, the most general strategy for Eve is that she performs an operation U_E which causes the encoding states to interact coherently with an auxiliary quantum system $|e\rangle$, which can be described as follows:

$$
\begin{aligned}
U_E|0\rangle|e\rangle &= \alpha|0\rangle|e_{00}\rangle + \beta|1\rangle|e_{01}\rangle, \\
U_E|1\rangle|e\rangle &= \gamma|0\rangle|e_{10}\rangle + \delta|1\rangle|e_{11}\rangle,
\end{aligned}
\tag{7}
$$

where $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$. In what follows, we will show that in order to pass the detection, Eve's ancillary state and the encoding state should be product states.

From Eq. (7), if the decoy state is $|0\rangle$ or $|1\rangle$ and Eve introduces no error in the eavesdropping check, the following condition should be satisfied:

$$
\beta = \gamma = 0. \tag{8}
$$

If the decoy state is $|+\rangle$ or $|-\rangle$ and Eve introduces no error in the eavesdropping check, we should have

$$
\begin{aligned}
& U_E|+\rangle|e\rangle \\
&= \frac{1}{\sqrt{2}}(\alpha|0\rangle|e_{00}\rangle + \beta|1\rangle|e_{01}\rangle + \gamma|0\rangle|e_{10}\rangle + \delta|1\rangle|e_{11}\rangle) \\
&= \frac{1}{2}(|+\rangle(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \gamma|e_{10}\rangle + \delta|e_{11}\rangle)) \\
&+ \frac{1}{2}(|-\rangle(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \gamma|e_{10}\rangle - \delta|e_{11}\rangle)) \\
&= \frac{1}{2}(|+\rangle(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \gamma|e_{10}\rangle + \delta|e_{11}\rangle)),
\end{aligned}
\tag{9}
$$

or

$$
\begin{aligned}
&U_E|-\rangle|e\rangle\\
&=\frac{1}{\sqrt{2}}(\alpha|0\rangle|e_{00}\rangle+\beta|1\rangle|e_{01}\rangle-\gamma|0\rangle|e_{10}\rangle-\delta|1\rangle|e_{11}\rangle)\\
&=\frac{1}{2}(|+\rangle(\alpha|e_{00}\rangle+\beta|e_{01}\rangle-\gamma|e_{10}\rangle-\delta|e_{11}\rangle))\\
&+\frac{1}{2}(|-\rangle(\alpha|e_{00}\rangle-\beta|e_{01}\rangle-\gamma|e_{10}\rangle+\delta|e_{11}\rangle))\\
&=\frac{1}{2}(|-\rangle(\alpha|e_{00}\rangle-\beta|e_{01}\rangle-\gamma|e_{10}\rangle+\delta|e_{11}\rangle)).
\end{aligned}
\tag{10}
$$

Namely, the following equations

$$
\begin{aligned}
\alpha|e_{00}\rangle-\beta|e_{01}\rangle+\gamma|e_{10}\rangle-\delta|e_{11}\rangle=0,\\
\alpha|e_{00}\rangle+\beta|e_{01}\rangle-\gamma|e_{10}\rangle-\delta|e_{11}\rangle=0,
\end{aligned}
\tag{11}
$$

should hold, with 0 denoting a column zero vector. Depending on Eqs. (8) and (11), we can deduce that

$$
\begin{aligned}
\alpha &=\delta=1,\\
\beta &=\gamma=0,\\
|e_{00}\rangle &=|e_{11}\rangle.
\end{aligned}
\tag{12}
$$

Finally, we have

$$
\begin{aligned}
U_E|0\rangle|e\rangle &=|0\rangle|e_{00}\rangle,\\
U_E|1\rangle|e\rangle &=|1\rangle|e_{00}\rangle,\\
U_E|+\rangle|e\rangle &=|+\rangle|e_{00}\rangle,\\
U_E|-\rangle|e\rangle &=|-\rangle|e_{00}\rangle.
\end{aligned}
\tag{13}
$$

That is to say, Eve introduces no error in the eavesdropping only when her ancillary state and the encoding states are product states. Eve therefore cannot obtain useful information without being detected.

Note that our protocol involves two-way quantum transmission that may incur Trojan horse attacks[19,20]. We do not even need the photon number splitter and the optical wavelength filter devices[21,22] to detect such an attack because the attacker knows nothing about three parties' share key k that are employed to encrypt their private information.

Dishonest parties' attacks Note that TP cannot collude with these dishonest parties. Suppose that Alice and Bob are the dishonest parties who intend to learn about Charlie's set C. After they remove their respective decoy particles and do nothing on their particles, they may try to figure out what operations Charlie has perform on his particles to obtain $(z_0, z_1, \ldots, z_{p-1})$. If Alice and Bob can get $(z_0, z_1, \ldots, z_{p-1})$, they can easily steal Charlie's private information because they share the same key k. Let's consider the i-th trio of GHZ state. If $i \in C^*$, Charlie performs $U = ZX$ on the particle G_{Ci} and then the state of (G_{Ai}, G_{Bi}, G_{Ci}) turns into $|\varphi_{001}\rangle_{G_{Ai}G_{Bi}G_{Ci}} = \frac{1}{\sqrt{2}}(|110\rangle_{G_{Ai}G_{Bi}G_{Ci}} - |001\rangle_{G_{Ai}G_{Bi}G_{Ci}})$; otherwise, the the state of (G_{Ai}, G_{Bi}, G_{Ci}) remains $|\varphi_{000}\rangle_{G_{Ai}G_{Bi}G_{Ci}} = \frac{1}{\sqrt{2}}(|000\rangle_{G_{Ai}G_{Bi}G_{Ci}} + |111\rangle_{G_{Ai}G_{Bi}G_{Ci}})$. In both case, $\rho_{G_{Ai}G_{Bi}} = \frac{1}{\sqrt{2}}(|00\rangle_{G_{Ai}G_{Bi}}\langle 00| + |11\rangle_{G_{Ai}G_{Bi}}\langle 11|)$, which means Alice and Bob cannot extract any private information from partial qubits of GHZ states. Thus, this attack by Alice and Bob is also invalid to our protocol.

TP's attacks In our protocol, TP is assumed to be semi-honest, which means he will loyally execute the protocol, and he may use all the intermediate results to derive the other parties' private information. However, he cannot collude with other dishonest parties.

Clearly, in 3.1, TP is able to derive $(x_0, x_1, \ldots, x_{p-1})$, $(y_0, y_1, \ldots, y_{p-1})$ and $(z_0, z_1, \ldots, z_{p-1})$ according to the original GHZ states and the measurement results in the GHZ basis. Namely, TP knows what operations Alice, Bob and Charlie have done on their particles. Even though TP can then deduce whether or not $i \in A^*$ $(i \in B^*, i \in C^*)$, he can still not learn any information about the elements in A (B, C). For example, suppose TP knows that $i \in A^*$ (i.e. $i = ka_j (\mathrm{mod}\ p) \in A^*$), he knows nothing about $a_j \in A$ because he does not have the secret key k, whose security is guaranteed by Quantum Key Agreement. Hence, TP cannot steal three parties' private information.

Influence of Markovian Noise on the Protocol.

In this section, assuming that the quantum state generator, quantum memories, and measurement devices in our protocol are perfect, we analyze the influence of six typical sorts of Markovian noise on our protocol. The effect of quantum noise on a tripartite quantum state ρ_{123} can be characterized as follows:

$$
\rho'_{123} = \sum_{i,j,k} K_1^{(i)} \otimes K_2^{(j)} \otimes K_3^{(k)} \rho_{123} K_1^{(i)\dagger} \otimes K_2^{(j)\dagger} \otimes K_3^{(k)\dagger},
\tag{14}
$$

where $\{K^i\}$ are Kraus operators characterizing quantum noise[23] .

Flip channels. The flip channels have the following Kraus operators[23]

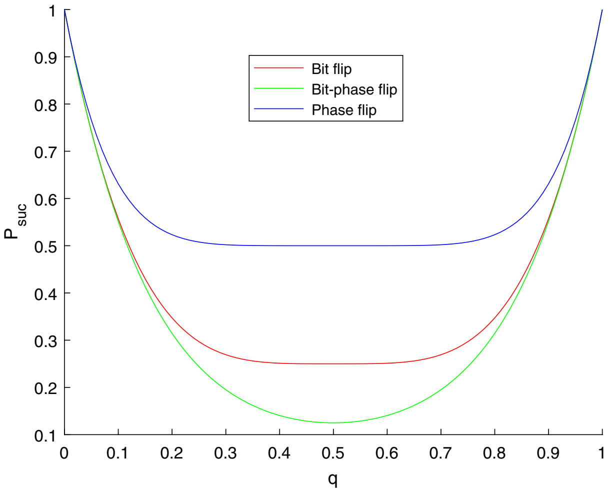

Figure 2. The variations of the success probabilities P_{suc} using three kinds of flip channel with noise strength q.

$$K^{(0)} = \sqrt{1-q}I, K^{(1)} = \sqrt{q}\sigma_i, \tag{15}$$

where $i = 1, 2, 3$ represents the bit flip ($\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$) , bit-phase flip ($\sigma_2 = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$) and phase flip ($\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$) channels, respectively, and $q \in [0, 1]$ denotes the noise strength.

Suppose that the channel between TP and Alice, the channel between TP and Bob, and the channel between TP and Charlie are the same. We first consider the bit flip channel. For a GHZ state $\rho_{ABC} = |\varphi_{000}\rangle_{ABC}\langle\varphi_{000}|$ used for computation, after three particles arrived at Alice, Bob, and Charlie, respectively, the state of this tripartite system ABC becomes

$$\rho'_{ABC} = \sum_{i,j,k=0}^{1} K_A^{(i)} \otimes K_B^{(j)} \otimes K_C^{(k)} \rho_{ABC} K_A^{(i)\dagger} \otimes K_B^{(j)\dagger} \otimes K_C^{(k)\dagger}, \tag{16}$$

where $K_s^{(0)} = \sqrt{1-q}I, K_s^{(1)} = \sqrt{q}\sigma_1$ ($s \in \{A, B, C\}$).

Later, Alice, Bob, and Charlie perform unitary operations U_A, U_B and U_C on particle A, B, C, respectively, as described in (Step 6) of the proposed protocol, with $U_A, U_B, U_C \in \{I, U = ZX\}$. We denote $U_{ABC} = U_A \otimes U_B \otimes U_C$, the state after Alice's, Bob's, and Charlie's operations turns into

$$\rho''_{ABC} = U_{ABC} \rho'_{ABC} U^{\dagger}_{ABC}. \tag{17}$$

When TP receives these three particles from Alice, Bob, Charlie, the state of this system ABC is

$$\rho'''_{ABC} = \sum_{i,j,k=0}^{1} K_A^{(i)} \otimes K_B^{(j)} \otimes K_C^{(k)} \rho''_{ABC} K_A^{(i)\dagger} \otimes K_B^{(j)\dagger} \otimes K_C^{(k)\dagger}. \tag{18}$$

When TP measures the system ABC in the GHZ basis, he expects to obtain the measure result $U_{ABC}\rho_{ABC}U^{\dagger}_{ABC}$, through which he can compute the cardinalities of intersections and unions, as described in 3.1 of our protocol. In this case, TP succeeds in the computation. We found that for all possible choices of U_{ABC}, the success probability is

$$P^{\mathrm{BF}}_{\mathrm{suc}} = 1 - 6q + 18q^2 - 24q^3 + 12q^4. \tag{19}$$

Similarly, for bit-phase and phase channels, the success probabilities are

$$P^{\mathrm{BPF}}_{\mathrm{suc}} = (1 - 2q + 2q^2)^3, \tag{20}$$

and

$$P^{\mathrm{PF}}_{\mathrm{suc}} = 1 - 6q + 30q^2 - 80q^3 + 120q^4 - 96q^5 + 32q^6, \tag{21}$$

respectively.

The variation of these three success probabilities for flip channels are depicted in Fig. 2.

Depolarizing. The depolarizing channel can be characterized by the following Kraus operators[23]

$$\begin{aligned} K^{(1)} &= \sqrt{1-\frac{3}{4}q}I, \quad K^{(2)} = \frac{\sqrt{q}}{2}\sigma_1, \\ K^{(3)} &= \frac{\sqrt{q}}{2}\sigma_2, \qquad K^{(4)} = \frac{\sqrt{q}}{2}\sigma_3, \end{aligned} \tag{22}$$

where $\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_2 = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$, $\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$, and $q \in [0, 1]$ is the noise strength.

Suppose that the channel between TP and Alice, the channel between TP and Bob, and the channel between TP and Charlie are the same. Using the similar method in Flip channels analysis, the success probability of TP obtaining the correct measurement result is

$$P_{\text{suc}}^{\text{Dep}} = \frac{1}{8}(8 - 36q + 78q^2 - 92q^3 + 63q^4 - 24q^5 + 4q^6), \tag{23}$$

for all different choices of U_{ABC}.

Amplitude damping. The amplitude damping channel is used for the description of energy dissipation, which contains the Kraus operators[23] as follows

$$K^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{bmatrix}, K^{(2)} = \begin{bmatrix} 0 & \sqrt{q} \\ 0 & 0 \end{bmatrix}, \tag{24}$$

where $q \in [0, 1]$ is the noise strength.

Suppose that the channel between TP and Alice, the channel between TP and Bob and the channel between TP and Charlie are the same. Using the similar method in Flip channels analysis, the success probability of TP obtaining the correct measurement result is

$$\begin{aligned} P_{\text{suc}}^{\text{AD1}} =& \frac{1}{4}(4 - 12q + 21q^2 + (-22 + 8\sqrt{1-q})q^3 \\ &+ (15 - 8\sqrt{1-q})q^4 - 6q^5 + q^6), \end{aligned} \tag{25}$$

for the cases where $U_{ABC} = I \otimes I \otimes I$ and $U_{ABC} = U \otimes U \otimes U$. For other cases, the success probability changes to

$$P_{\text{suc}}^{\text{AD2}} = -\frac{1}{4}(-1 + q)(4 - 8q + 9q^2 + (-5 + 4\sqrt{1-q})q^3 + q^4). \tag{26}$$

Phase damping. The phase damping channel is characterized by the Kraus operators[23] as follows

$$K^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{bmatrix}, K^{(2)} = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{q} \end{bmatrix}, \tag{27}$$

where $q \in [0, 1]$ is the noise strength.

Suppose that the channel between TP and Alice, the channel between TP and Bob, and the channel between TP and Charlie are the same. Using the similar method in Flip channels analysis, the success probability of TP obtaining the correct measurement result is

$$P_{\text{suc}}^{\text{PD}} = \frac{1}{2}(2 - 3q + 3q^2 - q^3), \tag{28}$$

for all sorts of choices of U_{ABC}.

The variations of the success probabilities of depolarizing, amplitude damping and phase damping channels are depicted in Fig. 3.

Discussion and Conclusions

We presented a three-party protocol to compute the cardinalities of the intersection and the union between any two sets and among three sets with the help a semi-honest party TP. The security analysis showed that our protocol can resist some well-known quantum attacks. In addition, we analyzed the influence of six typical sorts of Markovian noise on the success probabilities of a GHZ state used for computation. The analysis showed that among three kinds of flip channels, the bit-phase flip channel affects our protocol most. It is interesting to see that on the amplitude damping channel, the success probabilities of the cases where $U_{ABC} = I \otimes I \otimes I$ and $U_{ABC} = U \otimes U \otimes U$ are the same, but for other cases, they share another success probabilities.

In practice, quantum error correction codes are usually employed to protect quantum states from errors induced by noise. There is also research on designing robust quantum cryptographic protocols based on some specific quantum states over special noisy channels (e.g. collective noise channels)[16]. Note that imperfect devices, such as quantum state generators and measurement devices, may also affect the robust of quantum cryptographic protocol, we will further conduct research on these topics in the future.

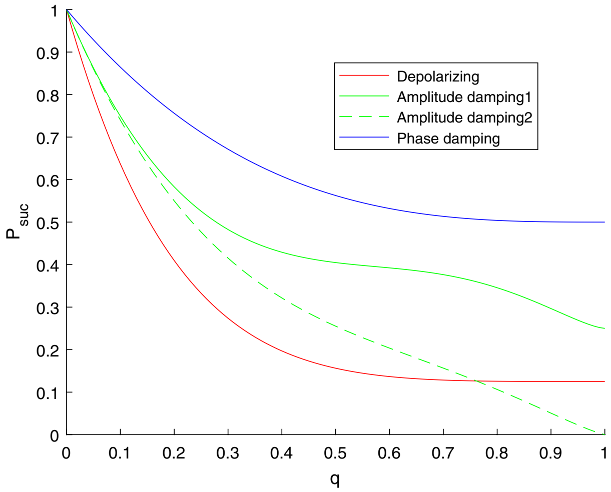

Figure 3. The variations of the success probabilities P_{suc} on the depolarizing, amplitude damping, and phase damping channels with noise strength q.

Received: 11 September 2020; Accepted: 10 November 2020
Published online: 17 December 2020

References

1. De Cristofaro, E., Gasti, P. & Tsudik, G. Fast and private computation of cardinality of set intersection and union. In *International Conference on Cryptology and Network Security*, 218–231 (Springer, 2012).
2. Wu, M.-E., Chang, S.-Y., Lu, C.-J. & Sun, H.-M. A communication-efficient private matching scheme in client-server model. Information Sciences 275, 348–359 (2014).
3. Shi, R.-H., Mu, Y., Zhong, H., Zhang, S. & Cui, J. Quantum private set intersection cardinality and its application to anonymous authentication. Information Sciences 370, 147–158 (2016).
4. Freedman, M. J., Nissim, K. & Pinkas, B. Efficient private matching and set intersection. In *International conference on the theory and applications of cryptographic techniques*, 1–19 (Springer, 2004).
5. Vaidya, J. & Clifton, C. Secure set intersection cardinality with application to association rule mining. Journal of Computer Security 13, 593–622 (2005).
6. Kissner, L. & Song, D. Privacy-preserving set operations. In *Annual International Cryptology Conference*, 241–257 (Springer, 2005).
7. Zander, S., Andrew, L. L. & Armitage, G. Scalable private set intersection cardinality for capture-recapture with multiple private datasets. *Centre for Advanced Internet Architectures, Technical Report 130930A* (2013).
8. Debnath, S. K. & Dutta, R. Secure and efficient private set intersection cardinality using bloom filter. In *International Conference on Information Security*, 209–226 (Springer, 2015).
9. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, 124–134 (IEEE, 1994).
10. Grover, L. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 28th Annual ACM Symposium on the Theory of computation*, 212–219 (ACM Press, 1996).
11. Grover, L. Quantum mechanics helps in searching for a needle in a haystack. Physics Review Letter 79, 325 (1997).
12. Liu, B., Zhang, M. & Shi, R. Quantum secure multi-party private set intersection cardinality. International Journal of Theoretical Physics 59, 1992–2007 (2020).
13. Shi, R.-H. Quantum private computation of cardinality of set intersection and union. The European Physical Journal D 72, 221 (2018).
14. Sun, Z. et al. Multi-party quantum key agreement by an entangled six-qubit state. International Journal of Theoretical Physics 55, 1920–1929 (2016).
15. Liu, W.-J., Xu, Y., Yang, C.-N., Gao, P.-P. & Yu, W.-B. An efficient and secure arbitrary n-party quantum key agreement protocol using bell states. International Journal of Theoretical Physics 57, 195–207 (2018).
16. Cai, B., Guo, G., Lin, S., Zuo, H. & Yu, C. Multipartite quantum key agreement over collective noise channels. IEEE Photonics Journal 10, 1–11 (2018).
17. Bennett, C. H. & Brassard, G. Quantum cryptography: public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computer, System and Signal*, 175–179 (1984).
18. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. Physical Review Letters 85, 441 (2000).
19. Cai, Q.-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A 351, 23–25 (2006).
20. Kraus, B. et al. Quantum memory for nonstationary light fields based on controlled reversible inhomogeneous broadening. Phys. Rev. A 73, 020302 (2006).
21. Deng, F.-G., Li, X.-H., Zhou, H.-Y. & Zhang, Z.-J. Improving the security of multiparty quantum secret sharing against trojan horse attack. Physical Review A 72, 044302 (2005).
22. Li, X.-H., Deng, F.-G. & Zhou, H.-Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Physical Review A 74, 054302 (2006).
23. Nielsen, M. A., Chuang, I. (2002) Quantum Computation and Quantum Information. Cambridge University Press, Cambridge

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Nos. 61902132, 11647140, 61872152, 61602316 and U1736113), the Natural Science Foundation of Guangdong Province, China (No.

2018A030310147), the Guangdong Major Project of Basic and Applied Basic Research (No. 2019B030302008), and the Shenzhen Fundamental Research Fund (No. JCYJ20190809152003992).

Author contributions

Study conception, design, and writing of the manuscript: C.Z., Z.S. and Q.H. Analysis and discussion: Y.L., Z.S. and Q.L. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to C.Z., Z.S. or Q.H.

Reprints and permissions information is available at www.nature.com/reprints.

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