.

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Quantum Secure Multi-party Summation Based on entanglement swapping

HONG CHANG [1,2], (Fellow, IEEE), YITING WU[1,2], AND SONG LIN, JR.[1,2,3], (Member, IEEE)
[1]National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@boulder.nist.gov)
[2]Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu)
[3]Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA

Corresponding author: Song Lin (e-mail: lins95@fjnu.edu.cn).

This paragraph of the first footnote will contain support information, including sponsor and financial support acknowledgment. For example, "This work was supported in part by the U.S. Department of Commerce under Grant BS123456."

ABSTRACT In this paper, we present a quantum secure multi-party summation protocol, which allows multiple mutually distrustful parties to securely compute the summation of their secret data. In the presented protocol, a semitrusted third party is introduced to help multiple parties to achieve this secure task. Besides, the entanglement swapping of d-level cat states and Bell states is employed to securely transmit message between each party and the semitrusted third party. At last, its security against some common attacks is analyzed, which shows that the presented protocol is secure in theory.

INDEX TERMS Bell states, Cat states, Entanglement swapping, Quantum secure multi-party summation

I. INTRODUCTION

Secure multi-party computing (SMC)[1, 2], which enables $n(n \geq 2)$ parties to jointly compute functions based on their private inputs while maintaining the confidentiality of privacy inputs. It is a major branch of modern cryptography, which is widely used in private auctions, secret ballot elections, e-commerce and data mining, and so on. The security of classical SMC is based on the assumption of computational complexity. However, it is increasingly vulnerable with the proposing of quantum algorithms, e.g., Grover search algorithm[3, 5]and Shor search algorithm[4, 6]. In the meanwhile, Bennett and Brassard proposed a theoretically unconditional secure key distribution protocol (BB84)[7] in 1984, which aroused people's interest in extending classical SMC to the field of quantum mechanics. Recently, various quantum secure multiparty computing protocols have been proposed, such as quantum private query[8–11], quantum private comparison[12–15], quantum secure multiparty summation[19, 20].

Secure multi-party summation is a common secure task in real life, which can be described as follows. There are n participants, and each participant has a secret data. They want to correctly calculate the summation of these inputs without revealing any information about the secret inputs. In 2007, Vaccaro $et\ al$ first proposed a quantum secure multi-party summation protocol[21], which was used to implement the secure task of anonymous voting and survey. In this protocol, participants sent secret message to a trusted tallyman, who calculated and published the summation result. After that, Du $et\ al.$ designed a quantum secret summation protocol [22]based on non-orthogonal single particles, which allows participants to accumulate their private data to an unknown number in a serial manner, so as to achieve the goal of secure multi-party summation. This protocol can resist the collusion attack of $n-1$ participants and achieve asymptotic security.

We propose a quantum secure multi-party summation (QSMMS) protocol. Multiple parties that do not trust each other can securely compute the summation of their secret data, while keeping their data private. To achieve this task, these particles of Bell states and cat states are transmitted between participants as signal particles. Eavesdropping detection ensures the security of the transmission of these particles. The secret data of participants are encrypted by entanglement swapping. Finally, a third party is introduced to help all participants obtain the calculation. Here, we require the third party to be semitrusted, that is, she is allowed to conduct herself improperly, but not to collude with either party.

The rest of this paper is organized as follows. Some preliminaries are introduced in Sect. 2. We devote Sect. 3 to present the proposed QSMMS protocol. The security of the proposed protocol is analyzed in Sect. 4. Finally, a short conclusion is provided in Sect. 5.

II. PRELIMINARIES

In a d-level quantum system, the quantum Fourier transform[23] is a common tool, which can be described as follows,

$$F = \frac{1}{\sqrt{d}} \sum_{j,k=0}^{d-1} \xi^{kj} |j\rangle\langle k|, \tag{1}$$

where $\xi = e^{\frac{2\pi \mathrm{i}}{d}}$ and $\mathrm{i} = \sqrt{-1}$. So, we can construct two common mutually unbiased bases, $B_1 = \{|j\rangle, j \in D = \{0, 1, \cdots, d-1\}\}$ and $B_2 = \{F|j\rangle, j \in D\}$, directly. Besides F, X and Z are other common operators,

$$X = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j \oplus 1\rangle\langle j|, \; Z = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{j} |j\rangle\langle j|, \tag{2}$$

where sign $\oplus$ represents the addition module d. The d-level Bell state is a generalization form of EPR pairs in d-level system (qudits), which can be expressed as

$$|\Phi(r, w)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jr} |j\rangle|j \oplus w\rangle, \tag{3}$$

where $r, w \in D$. The state $|\Phi(r, w)\rangle$ can be generated through operations X and Z on particles of $|\Phi(0, 0)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle$,

$$(I \otimes X_w Z_r)|\Phi(0, 0)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jr} |j\rangle|j \oplus w\rangle = |\Phi(r, w)\rangle, \tag{4}$$

where $Z_r = (Z)^r$, $X_w = (X)^w$, and $(X)^0 = (Z)^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$. Similarly, the d-level cat states can be obtained, which can be described as follows,

$$|\Psi(u_1, u_2, \cdots, u_n)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{ju_1} |j, j \oplus u_2, j \oplus u_3, \cdots, j \oplus u_n\rangle. \tag{5}$$

In the proposed protocol, the d-level Bell states and the d-level cat states are used as information carriers.

Entanglement swapping is an important tool in quantum information field. In this paper, we use entanglement swapping between a n-particle cat state $|\Psi(v, u, \cdots, u)\rangle$ and n Bell states $|\Phi(r_i, w_i)\rangle (i = 1, 2, \cdots, n)$. When we make a Bell state measurement on the cat state particle and one particle of each Bell state, the remaining particles collapse into an entangled state. Specifically, it can be expressed by the following formula.

$$\begin{aligned} &|\Psi(v, u, \cdots, u)\rangle \otimes |\Phi(r_1, w_1)\rangle \otimes |\Phi(r_2, w_2)\rangle \otimes \cdots \\ &\otimes |\Phi(r_n, w_n)\rangle = \frac{1}{\sqrt{d}} \sum_{k,l} \xi^{-kl} |\Psi(\widetilde{v}, \widetilde{u}_1, \widetilde{u}_2, \cdots, \widetilde{u}_n)\rangle \\ &\otimes |\Phi(\widetilde{r}_1, \widetilde{w}_1)\rangle \otimes \cdots \otimes |\Phi(\widetilde{r}_n, \widetilde{w}_n)\rangle, \end{aligned} \tag{6}$$

where

$$\begin{cases} \widetilde{v} = v \oplus \sum_{i=1}^{n} k_i \\ \widetilde{u}_i = w_i \oplus l_i \\ \widetilde{r}_i = r_i \ominus k_i \\ \widetilde{w}_i = u \ominus l_i. \end{cases} \tag{7}$$

where, sign $\ominus$ represents the subtraction module d. Eavesdroppers are unable to extract any useful information from the particles before and after the entanglement. Thus, we can secretly embed private data for encryption operations. In addition, cat state particles and Bell state particles have the following deterministic relationships.

Theorem 1:

An $(n+1)$-qudit state is in the form of the state $|\Psi(v, u, \cdots, u)\rangle$, when and only when it satisfies both the following two conditions:

(c1)when each of its qudits is measured in B_1 basis, $n+1$ measurement results satisfy $k_0 \oplus u = k_1 = k_2 = \cdots = k_n$;

(c2)when each of its qudits is measured in B_2 basis, $n+1$ measurement results satisfy $k_0 \oplus k_1 \oplus k_2 \oplus \cdots \oplus k_n \oplus v = 0$.

Theorem 1 is proved as follows:

Simple calculation shows that when $n+1$ qudit is in state $|\Psi\rangle$, each particle is measured with B_1 or B_2 basis, and the measurement results meet condition (c1) and (c2).

Now, let's prove that if the state $|\Omega\rangle$ satisfies condition (c1) and (c2), then $|\Omega\rangle = \Psi(v, u, \cdots, u)\rangle$. From condition (c1), we can assume $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jv} |j\rangle|j \oplus u\rangle \cdots |j \oplus u\rangle$, then

$$\begin{aligned} |\Omega'\rangle &= X_u \otimes I^n |\Omega\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \lambda_j X_u |j\rangle|j \oplus u\rangle \cdots |j \oplus u\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \lambda_j |j\rangle|j\rangle \cdots |j\rangle \end{aligned} \tag{8}$$

$$\begin{aligned} &|\Omega''\rangle = F^{\otimes(n+1)}|\Omega'\rangle \frac{1}{\sqrt{d}} \sum_{j} \lambda_j (\frac{1}{\sqrt{d}} \sum_{k_0} \xi^{k_0 j} |k_0\rangle) \otimes \cdots \\ &\otimes (\frac{1}{\sqrt{d}} \sum_{k_n} \xi^{k_n j} |k_n\rangle) = \frac{1}{d^{\frac{n+2}{2}}} \sum_{k_0 \cdots k_n} (\sum_{j} \lambda_j \xi^{(k_0 \oplus \cdots + k_n) j} \\ &|k_0\rangle \cdots |k_n\rangle. \end{aligned} \tag{9}$$

where $F = \frac{1}{\sqrt{d}} \sum_{j,k} \xi^{jk} |j\rangle\langle k|$, $Z_t = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jt} |j\rangle\langle l|$, $X_t = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jt} |j \oplus t\rangle\langle j|$. Because $F X_t = Z_t F$,

$$F^{\otimes(n+1)} X_u \otimes I^n |\Omega\rangle = Z_u \otimes I^n F^{\otimes(n+1)} |\Omega\rangle. \tag{10}$$

Since Z_u only changes the relative phase and does not change the measurement results of the calculation basis, then the measured results of of the state $|\Omega''\rangle$ in the calculation basis must satisfy condition (c2), which can be obtained $\sum_{j=0}^{d-1} \lambda_j \xi^{(k_0 \oplus k_1 \oplus \cdots \oplus k_n) j} = 0$ when $k_0 \oplus \cdots \oplus k_n \oplus v \neq 0$;

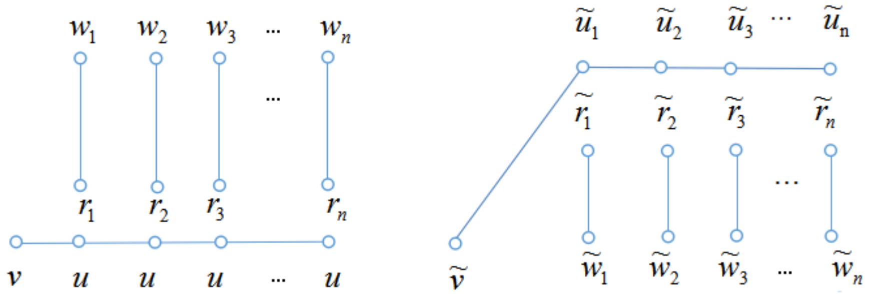

FIGURE 1: The graphical description of entanglement swapping between a d-level n-particle cat state and n d-level Bell states.

$\sum_{j=0}^{d-1} \mid \lambda_j \xi^{-vj} \mid^2 = \frac{1}{d}$ when $k_0 \oplus \cdots \oplus k_n \oplus v = 0$. Thus, we may get $\lambda_j = \frac{1}{\sqrt{d}} \xi^{vj}$. Now we have proved that

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \xi^{jv} |j\rangle |j \oplus u\rangle \cdots |j \oplus u\rangle |\Psi(v, u, \cdots, u)\rangle. \tag{11}$$

According to theorem 1, the particle can be guaranteed to be in state $|\Psi(v, u, \cdots, u)\rangle$ through condition (c1) and (c2). Since the Bell state is a special case of cat state, we can get a similar conclusion for the Bell state.

Corollary 1:

An 2-qudit state is in the form of the state $|\Phi(r, w)\rangle$, when and only when is satisfies both the following two conditions:

(c1')when each of its qudits is measured in B_1 basis, $n+1$ measurement results should satisfy $a_0 = a_i$;

(c2')when each of its qudits is measured in B_2 basis, the summation of the $n+1$ measurement results should satisfy $a_0 \oplus a_i = 0$.

III. THE PROPOSED PROTOCOL

In the proposed protocol, there are n mutually distrustful parties labeled $P_1, P_2, \cdots, P_n$. Each party $P_i (i = 1, 2, \cdots, n)$ has a secret dataset $D_i = \{x_i^1, x_i^2, \cdots, x_i^m\}$. We set $S = \{x_i^j | x_i^j \in N, 0 \leq x_i^j \leq d-1, i = 1, 2, \cdots, n, j = 1, 2, \cdots, m\}$, and then we have $d > \sup\{S\}$. $P_1, P_2, \cdots, P_n$ want to jointly compute the summation $\bigoplus_{i=1}^{n} x_i^j$ with the assistance of a semitrusted third party (TP), who is allowed to misbehave on her own but cannot conspire with others. Now let us describe steps of the proposed protocol in detail.

(**1**) Each party $P_i (i = 1, 2, \cdots, n)$ prepares $L + \sigma$ copies of d-level Bell state.

$$|\Phi(0, 0)\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle_{h_i^j} |a\rangle_{t_i^j}. \tag{7}$$

Here, the subscripts h_i^j and t_i^j denote two different qudits of a entangled pair, and $j (j = 1, 2, \cdots, L + \sigma)$ indicates the order of the entangled pairs. P_i takes particles h_i^j and t_i^j from each pair to form two ordered particle sequences $H_i = (h_i^1, h_i^2, \cdots, h_i^{L+\sigma})$ and $T_i = (t_i^1, t_i^2, \cdots, t_i^{L+\sigma})$. TP prepares $L + n\delta$ copies of d-level cat state $|\Psi(v^j, u^j, u^j, \cdots, u^j)\rangle_{s_0^j s_1^j \cdots s_n^j}$, then takes particle s_i^j from each cat state $|\Psi(v^j, u^j, u^j, \cdots, u^j)\rangle$ to construct $n+1$ ordered sequences $S_0 = (s_0^1, s_0^2, \cdots, s_0^{L+n\delta})$, $S_1 = (s_1^1, s_1^2, \cdots, s_1^{L+n\delta})$,$\cdots$, $S_n = (s_n^1, s_n^2, \cdots, s_n^{L+n\delta})$, where the superscript $j (j = 1, 2, \cdots, L + n\delta)$, represents the order of the copies.

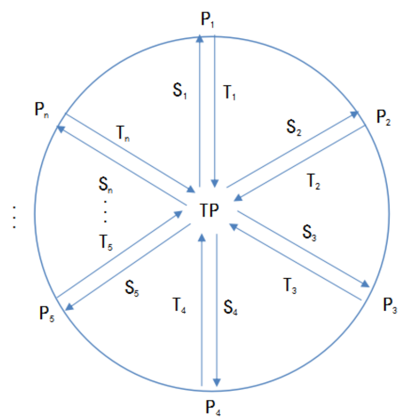

FIGURE 2: The distribution process of TP and P_i.

(**2**) TP remains particle sequence S_0 in her own hands, then sends particle sequence S_i to P_i. Meantime, P_i sends particle sequence T_i to TP, and remains particle sequence H_i. The above particles transmission process is shown in Figure 2.

(**3**) After both TP and participants confirm receiving the particle sequences, the $n+1$ parties (TP and n participants) cooperate to execute the following two eavesdropping detections.

$Detection1$:

First, P_i randomly chooses δ qudits from S_i as samples. For each sample particle, P_i measures it randomly in B_1 basis or B_2 basis. Then P_i requires TP and the other $n-1$ participants to measure the corresponding qudits in their hands with the same basis. After that, TP announces initial states of sample particles and her measurement result k_0, then $n-1$ participants announce their measurement results in a random order. According to the announced messages, P_i can check whether the measurement results satisfy the conditions (c1) and (c2). In this way, P_i can calculate the error rate. Once the error rate is higher than a certain threshold, he will abort the protocol. Otherwise, he will continue.

$\mathbf{D}etection2$:

First, TP randomly chooses σ qudits from T_i as samples. For each sample particle, TP measures it randomly in B_1 basis or B_2 basis. Then TP requires all P_i to measure the corresponding qudits with the same basis. After that, each P_i announces his measurement to TP. According to announced messages, TP can check whether the measurement results satisfy the conditions (c1') and (c2').

In this way, TP can calculate the error rate, once the error rate is higher than a certain threshold, she will abort the protocol. Otherwise, she will continue.

(**4**) P_i encodes his secret dataset. Concretely, P_i randomly generates two variables r_i^j and w_i^j and requires them to meet the condition $x_i^j = r_i^j \oplus w_i^j$. P_i performs $Z_{r_i^j} \otimes X_{w_i^j}$ operation on the Bell state $|\Phi(0,0)\rangle$. Therefore, the Bell state changes from $|\Phi(0,0)\rangle$ to $|\Phi(r_i^j, w_i^j)\rangle = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} \xi^{t r_i^j} |t\rangle |t \oplus\ w_i^j\rangle$.

(**5**) Each participant P_i performs the Bell state measurement on particle s_i^j and particle h_i^j. In this case, the particles $s_0^j, t_1^j, t_2^j, \cdots, t_n^j$ collapse to a cat state. After that, TP measures this cat state.

(**6**) After the entanglement swapping, the Bell state of P_i becomes $|\Phi(\widetilde{r}_i^j, \widetilde{w}_i^j)\rangle$, where $\widetilde{r}_i^j = r_i^j \ominus k_i^j$, $\widetilde{w}_i^j = u_i \ominus l_i^j$. Then, P_i calculates

$$q_i^j = \widetilde{r}_i^j \oplus \widetilde{w}_i^j = r_i^j \ominus k_i^j \oplus u_i \ominus l_i^j \tag{8}$$

and announces classical information q_i^j to TP.

(**7**) After the entanglement swapping, the cat state of TP becomes $|\Psi(\widetilde{v}^j, \widetilde{u}_1^j, \widetilde{u}_2^j, \cdots, \widetilde{u}_n^j)\rangle$, where $\widetilde{v}^j = v^j \oplus \sum_{i=1}^{n} k_i^j$, $\widetilde{u}_i^j = w_i^j \oplus l_i^j$. Then, TP carries out simple calculations and gets

$$\widetilde{v}^j \oplus \sum_{i=1}^{n} \widetilde{u}_i^j \oplus \sum_{i=1}^{n} q_i^j \ominus v^j \ominus n u^j = \sum_{i=1}^{n} r_i^j \oplus \sum_{i=1}^{n} w_i^j = \sum_{i=1}^{n} x_i^j \tag{9}$$

Finally, TP announces the summation to P_i.

Let us consider a simple case as an example to demonstrate the correctness of the presented protocol. Suppose that there are three participants P_1, P_2, and P_3, who have three private datasets $D_1 = \{1,3\}$, $D_2 = \{3,6\}$ and $D_3 = \{2,5\}$, respectively. Thus, we can assume that $d = 7 > 6$. For simplicity, we ignore the eavesdropping checks. Therefore, in step 1, every $P_i (i = 1,2,3)$ prepares four copies of d-level Bell state $|\Phi(0,0)\rangle$, and TP prepares four copies of d-level cat state $|\Psi^1(4,1,1,1)\rangle, |\Psi^2(3,2,2,2)\rangle, |\Psi^3(2,5,5,5)\rangle$ and $|\Psi^4(6,3,3,3)\rangle$. Every $P_i (i = 1,2,3)$ takes particle h_i^j and t_i^j from each Bell state to form two ordered particle sequences H_i and T_i. TP takes particle s_i^j from each cat state to construct four ordered sequences $S_0 = (4,3,2,6), S_1 = (1,2,5,3), S_2 = (1,2,5,3), S_3 = (1,2,5,3)$.

TABLE 1: The proposed protocol in the example.

i	j	x_i^j	r_i^j	w_i^j	$\|\Phi\rangle$	k_i^j	l_i^j	$\|\Phi'\rangle$	q_i^j
1	1	1	1	0	(1,0)	1	1	(0,1)	1
1	2	3	2	1	(2,1)	1	0	(1,2)	3
2	1	3	1	2	(1,2)	0	1	(1,0)	1
2	2	6	4	2	(4,2)	3	1	(1,1)	2
3	1	2	0	2	(0,2)	0	0	(0,1)	1
3	2	5	3	2	(3,2)	1	0	(2,2)	4

TABLE 2: The proposed protocol in the example.

j	$\|\Psi\rangle$	$\widetilde{v}^j$	$\widetilde{u}_1^j$	$\widetilde{u}_2^j$	$\widetilde{u}_3^j$	$\|\Psi'\rangle$	$\sum_{i=1}^{3} x_i^j$
1	(4,1,1,1)	5	0	3	2	(5,0,3,2)	6
2	(3,2,2,2)	1	1	3	2	(1,1,3,2)	0

The concrete value of each variable are shown in Table 1, and the new Bell states and q_i^j can be obtained after the entanglement swapping.

In step 7, the specific calculation results are shown in Table 2. It can be seen from this example that the results obtained by TP are correct.

IV. SECURITY ANALYSIS

In the following, we analyze the security of the proposed protocol. The security of every quantum channel between TP and participants is ensured by an eavesdropping-check process. Thus, it is evident that stealing information directly is not feasible. An inside attacker is more powerful than an outside attacker. Thus, we focus our attention on the security of protocol against the inside attacks. In addition to dishonest participants, TP is not fully trusted, and she may also steal secret inputs. Thus, two types of attacks will be discussed: attack by dishonest participants and attack by the semitrusted TP.

A.Attack by dishonest participants

In this attack, we will assume that P_m (referred to as P_m^*) is dishonest and wishes to eavesdrop on all or partial information about P_l's private data. He can perform one of two common attack strategies to attack the proposed protocol in this article, which are described as follows.

Case 1: Intercept-resend attack

In Step 2, TP transmits sequence S_l to P_l, P_l transmits sequence T_l to TP. Thus, P_m^* can utilize this opportunity to execute his attack action. Concretely, P_m^* prepares several fake particles and replaces the signal particles with these fake particles. First, let's analyze the case where TP transmits sequence S_i to P_i. When sequence S_l, which contains partial information about P_l, is transmitted in Step 2, P_m^* intercepts this particle sequence. After interception, P_m^* can obtain the value of u in the calculation in Step 6 by measuring the sequence S_l. However, this action can be detected in Detection 1. Therefore, the attack will fail. Next, let's analyze the other case where P_i transmits sequence T_i to TP. Similarly, when sequence T_l is transmitted in Step 2, P_m^* intercepts and measures this particle sequence. After then, P_m^* can obtain the value of w_l^j in the calculation in Step 6. However, this action can be detected in Detection 2. Therefore, the attack will fail, too. Consequently, this protocol is secure against intercept-resend attack.

Case 2: Entangle-ancilla attack

In this attack, let's first analyze the case where P_i transmits sequence T_i to TP. Before P_l sends sequence T_l to TP, P_m^* prepares an ancilla and performs a certain unitary operation on this ancillary particle and the transmitted particle in the sequence T_l, which causes the two particles to become entangled. At the end of the protocol, he may utilize this ancilla to eavesdrop on all or some of the information about P_l. In the following, we will show that even if he has unlimited computing power, with technology limited only by the laws of quantum mechanics, P_m^* cannot obtain any information about P_l's secret input under the condition that no errors are to occur in Detection 2.

We can write the most general operation that P_m^* could apply to t_l^j particle in sequence T_l (particle T) and the ancilla (particle E) as follows:

$$U : |f\rangle_T|0\rangle_E \rightarrow \sum_{g=0}^{d-1} |g\rangle_T|\varepsilon_{f,g}\rangle_E \tag{14}$$

where $f \in D$. The states $|\varepsilon_{f,g}\rangle$ are pure ancilla states that are uniquely determined by U. The following conditions can be derived from the unitary nature of U:

$$\sum_{g=0}^{d-1}(|\varepsilon_{f,g}\rangle, |\varepsilon_{f',g}\rangle) = \delta_{f,f'} \tag{15}$$

where $f, f' \in D, \delta_{f,f'} = 0(\text{or } 1)$ when $f \neq f'(\text{or } f = f')$.

After P_3^* performs U operation the quantum system composed of particle H, particle T and particle E will be in the state,

$$\begin{aligned}|\Delta\rangle &= U\frac{1}{\sqrt{d}}\sum_{f=0}^{d-1}|f\rangle_H|f\rangle_T|0\rangle_E \\ &= \frac{1}{\sqrt{d}}\sum_{k=f\oplus g=0}^{d-1}(\sum_{f=0}^{d-1}|f\rangle|f\oplus k\rangle|\varepsilon_{f,f\oplus k}\rangle)_{HTE}.\end{aligned} \tag{16}$$

In Detection 2, we can get from Eq.(L'1)

$$\sum_{f=0}^{d-1}|f\rangle|f\oplus k\rangle|\varepsilon_{f,f\oplus k}\rangle = \overrightarrow{0}, \tag{17}$$

where $k = 1, 2, \cdots, d-1$.

According to Eqs.(16) and (17), we can further obtain

$$\begin{aligned}|\Delta\rangle &= \frac{1}{\sqrt{d}}\sum_{k=f\oplus g=0}^{d-1}(\sum_{f=0}^{d-1}|f\rangle|f\oplus k\rangle|\varepsilon_{f,f\oplus k}\rangle) \\ &= \frac{1}{\sqrt{d}}\sum_{f=0}^{d-1}|f\rangle|f\rangle|\varepsilon_{f,f}\rangle.\end{aligned} \tag{18}$$

When P_i and TP measure particles with B_2 basis, the state of the system can be written as

$$\begin{aligned}&F\otimes F|\Delta\rangle = F\otimes\frac{1}{\sqrt{d}}\sum_{f=0}^{d-1}|f\rangle|f\rangle|\varepsilon_{f,f}\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}\sum_{y_H}\sum_{f}\xi^{fy_H\oplus f(k\ominus y_H)}|y_H\rangle|k\ominus y_H\rangle)|\varepsilon_{f,f}\rangle.\end{aligned} \tag{19}$$

We get from Eq.(L'2)

$$\sum_{y_H}\sum_{f}\xi^{fy_H\oplus f(k\ominus y_H)}|y_H\rangle|k\ominus y_H\rangle)|\varepsilon_{f,f}\rangle = \overrightarrow{0}. \tag{20}$$

where $k = 1, 2, \cdots, d-1$. Then,

$$\sum_{f}\xi^{fk}|\varepsilon_{f,f}\rangle = \overrightarrow{0}. \tag{21}$$

After a simple calculation, we can get

$$|\varepsilon_{0,0}\rangle = |\varepsilon_{1,1}\rangle = \cdots = |\varepsilon_{d-1,d-1}\rangle. \tag{22}$$

From Eqs.(20),(21) and (22) we can derive

$$F\otimes F\frac{1}{\sqrt{d}}\sum_{f=0}^{d-1}|f\rangle|f\rangle|\varepsilon_{f,f}\rangle = \frac{1}{\sqrt{d}}\sum_{f=0}^{d-1}F|f\rangle F|f\rangle\otimes|\varepsilon\rangle, \tag{23}$$

where $|\varepsilon\rangle$ is independent of $|f\rangle$.

Above we have deduced P_m^* successful eavesdropping conditions. When P_m^* entangles an ancilla particle on a particle T, the probability that f is equal to g is $\frac{1}{d}$. When a sequence has n particles, the probability that f is equal to g is $(\frac{1}{d})^n$. As n tends to infinity, the probability of P_m^* successful eavesdropping tends to 0.

For analysis of P_m^* eavesdropping S_l, see Appendix 1.

B.Attack by the semitrusted TP

Now, we will discuss the case in which TP attempts to eavesdrop on private data. In the proposed protocol, TP is allowed to behave improperly, but she cannot conspire with other participants. To get useful information about a participant, TP must get r and w of the participant without introducing any errors into the detection. If TP implements the protocol honestly, then she can obtain v^j, u^j, and w_i^j by measurement in step 2 before entanglement swapping. After entanglement swapping, in step 6, due to the publication of P_i , TP can know q_i^j, namely, $\widetilde{r}_i^j \oplus \widetilde{w}_i^j$. In step 7, she can obtain $\widetilde{v}^j$ and $\widetilde{u}_i^j$ by measurement after entanglement swapping. At the end of the protocol, she also can know$\sum_{i=1}^n x_i^j$. Even if

TP knew so much information, it could not eavesdrop on the value of $r_i^j \oplus w_i^j$. If TP adopts intercept-resend attack and entangle-ancilla attack , the analysis results are the same as above.

V. SUMMARY AND CONCLUSION

Before giving a conclusion, we first compare and analyze the proposed with other QMS protocols. In order to highlight the advantages of the proposed protocol more intuitively, we make the following comparisons. Please refer to Table 3 for detailed comparison results. First, several QSMS algorithms were proposed in quantum anonymous voting and surveying protocols in order to calculate the summation of some private data including binary numbers and integers[24]. In 2005, Hillery et al. proposed a QSMS algorithm in their quantum anonymous voting protocol, in which each number is 0 or 1. In 2007, Vaccaro et al. proposed another QSMS algorithm for calculating the summation of n integers, where n denotes the number of parties (voters) in their quantum anonymous surveying protocol, in which a $(n-1)$-particle entangled state is employed. Each party makes a vote by performing a phase-shifting operation on its respective particles[25]. Then all parties send their particles to the tallyman who is responsible for counting the votes (i.e., calculating the summation of n integers).

From Table 2, we can clearly find the advantages of the proposed protocol. In addition, even if the eavesdropper escaped all detection risks, he would still not have access to useful information.

In the proposed protocol, we propose a QMS protocol that allows multiple parties to securely compute the summation of their secret data. The special feature of the proposed protocol is employing entanglement swapping between cat states and Bell states to encode secret data. The proposed protocols use entanglement swapping between cat states and Bell states to securely transmit message between each party and TP. It is worthy pointing that all parties employ unitary operation to encode their secret data, and generate Bell states. With the help of the semitrusted TP, they can obtain the summation successfully at the end of the protocol.

ACKNOWLEDGMENT

This work is partially supported by Fujian Normal University.

REFERENCES

[1] A. C. Yao, "Protocols for Secure Computations,"*Foundations of Computer Science*, 1982, 160-164.

[2] C. Lovis, "Privacy-preserving Analysis of Distributed Biomedical Data: Designing Efficient and Secure Multiparty Computations Using Distributed Statistical Learning Theory," *JMIR Medical Informatics*, 2019,7(2).

[3] K. H. Yee, Y. K. Hyuk, B. Jeongho, et al., "Speedup of Grover's Search Algorithm and Closed Timelike Curves,"*Quantum Science and Technology*, 2020,5(4):045011.

[4] W. Arya, A. Anthony, W. A. Wahyu, "Web-app Realization of Shor's Quantum Factoring Algorithm and Grover's Quantum Search Algorithm," *TELKOMNIKA*, 2020,18(3).

[5] D. Fernandes, I. Dutra,"Inês Dutra. Using Grover's Search Quantum Algorithm to Solve Boolean Satisfiability Problems: Part I," *XRDS: Crossroads, The ACM Magazine for Students*, 2019,26(1).

[6] P. R. Giri, V. E. Korepin, " A Review on Quantum Search Algorithms," *Quantum Information Processing*, 2017,16(12).

[7] F. Gao, S. J. Qin, W. Huang, Q. Y. Wen, "Quantum Private Query: A New Kind of Practical Quantum Cryptographic Protocol," *Science China Physics,Mechanics and Astronomy*, 2019,62(07):10-21.

[8] Y. Wang, F.Z. Guo, L. Liu, et al., "A New Protocol for Quantum Private Query Against Joint-Measurement Attack,"*International Journal of Theoretical Physics*, 2019,58(6):1828-1835.

[9] T.R. Pei, X.L. Meng, C.Y. Wei, et al., "Practical Quantum Private Query of Blocks Based on the Two-dimensional QKD System," *Quantum Information Processing*,2019,18(8):1-13.

[10] "Information Technology,Study Results from Chengdu University of Information and Technology Provide New Insights into Information Technology (Practical Quantum Database Private Query Protocol With Classical Database Owner)," *Journal of Physics Research*, 2020.

[11] B. Liu, D. Xiao , W. Huang, et al., "Quantum Private Comparison Employing Single-photon Interference," *Quantum Information Processing*, 2017,16(7).

[12] Z. X. Ji, P. R. Fan, H. G. Zhang, H. Z. "Cryptanalysis and improvement of several quantum private comparison protocols," *Communications in Theoretical Physics*, 2020,72(08):59-64.

[13] L. Z. Jiang, "Semi-quantum private comparison-based on Bell states,"*Quantum Information Processing*, 2020,19(1).

[14] Y. F. Lang, "Quantum Gate-Based Quantum Private Comparison," *International Journal of Theoretical Physics*, 2020,59(3).

[15] Y. H. Yang, F. Gao, X. Wu, et al., "Quantum Secret Sharing via Local Operations and Classical Communication," *Scientific Reports*,2015,5(1).

[16] L. Hong, J. Pieprzyk, L. Pan, "Analysis of weighted quantum secret sharing based on matrix product states," *Quantum Information Processing*,2020,19(12).

[17] Z. K. Gao,Z. H. Li, "Deterministic Measurement-device-independent Quantum Secret Sharing," *Science China Physics,Mechanics and Astronomy*, 2020,63(12):76-83.

[18] S. Kartick, O. Har, "Hybrid Quantum Protocols for Secure Multiparty Summation and Multiplication," *Scientific Reports*, 2020,10(1):9097.

TABLE 3: The comparion among proposed protocol and Refs.[24,25]

Protocol	Information carriers	User's operations	Data type
proposed protocol	cat states and Bell states	Single operations	Nonnegative integer
Refs.[24]	Cat states and Bell states	Single operations	Binary number
Refs.[25]	N-particle entangled states	Phase-shifting operation	Integer

[19] W. Liu,Y. B. Wang, W. Q," An Novel Protocol for the Quantum Secure Multi-Party Summation Based on Two-Particle Bell States," *International Journal of Theoretical Physics*, 2017,56(9):2783-2791.

[20] J. A. Vaccaro, J. Spring, Chefles, "Quantum Protocols for Anonymous Voting and Surveying," *Phys.Rev.A*, 2007,75(1):012333.

[21] J. Z. Du, X. B. Chen,Q. Y. Wen, F. C. Zhu, "Secure Multipartite Quantum Summation," *Journal of Physics*, 2007,(11):6214-6219.

[22] Z. X. Ji, H. G. Zhang, H. Z. Wang, F. S. Wu,J. W. Jia,W. Q. Wu,"Quantum Protocols for Secure Multiparty Summation," *Quantum Inf. Process*, 2019,18(6).

[23] A. Shakeel,"Efficient and Scalable Quantum Walk Algorithms via the Quantum Fourier Transform," *Quantum Information Processing*, 2020,19(9).

[24] J. A. Vaccaro, J. Spring,A. Chefles, "Quantum Protocols for Anonymous Voting and Surveying," *Phys.Rev.A*, 2007,75(1):012333.

[25] M. Hillery, M. Ziman, V. Buek, M. Bielikova, "Towards Quantum-based Privacy and Voting," *Physics Letters A*, 2006,349(1):75-81.