Quantum Information Processing (2021) 20:319
https://doi.org/10.1007/s11128-021-03262-2

Quantum secure multi-party summation based on entanglement swapping

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

Received: 1 May 2021 / Accepted: 14 September 2021 / Published online: 27 September 2021

Abstract

Quantum secure multi-party summation is a specific primitive of classical secure multi-party computation. Compared with classical secure multi-party summation based on mathematical difficulty problems such as integer factorization and discrete logarithm which has been threatened by potential quantum computers, the quantum version can provide unconditional security for the computing tasks. A quantum protocol based on the entanglement swapping between d-level Bell state and d-level cat state is constructed to perform secure multi-party summation. With the aid of a semi-honest third party who does not conspire with any participant, the proposed protocol can calculate the non-modular sum of the secret integers held by the participants who do not trust each other. Not only can the protocol resist the attacks from both outside and semi-honest third party, but also resist participants' attack, even though there are at most $n-2$ participants colluding together. (n is the number of participants.) This protocol only needs $O(\log M)$ (M is the maximum value of all secret integers) quantum resources to complete the computing task. Specially, under the condition of computing the sum of larger integers for a small number of participants, this protocol utilizes fewer quantum resources and has higher efficiency than other proposed protocols.

Keywords Quantum secure multi-party summation · Entanglement swapping · d-level Bell state · d-level cat state

✉ 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

1 Introduction

In the current period of big data, many organizations have accumulated large amounts of data; for example, the patients' treatment overcomes in the hospitals and the consumers' transaction records on e-commerce platforms. However, these data cannot be directly shared between organizations for reasons of security and privacy, and thus, the application value of them is greatly limited. To solve this problem, we can take advantage of the secure multi-party computation (MPC) technology to collaboratively calculate them at the same time of ensuring security and privacy. MPC is a theoretical framework to solve the problem of collaborative computing between a group of participants who do not trust each other without a trusted third party and can ensure the privacy of inputs and the correctness of calculations simultaneously. The idea of MPC was first put forward by Yao [1] in 1982, and then, Goldreich et al. [2] proposed a kind of construction method for universal security protocol. In 2007, Katz [3] proposed the definition of partial fairness. In 2008, Gordon et al. [4] studied the complete fairness of some special functions. MPC has also been widely researched in protocol application such as secure multi-party set operation [5], electronic auction [6], and secure multi-party cloud computation [7].

Secure multi-party summation (SMS), which is a specific primitive of MPC, can complete the task that multiple participants want to correctly compute the sum of their secret integers without revealing them. Not only can SMS be utilized to build more complicated protocols for MPC but also to other tasks such as data mining and electronic voting [8]. However, the appearance of Shor's algorithm [9] and Grover's algorithm [10] has threatened the security of the classical cryptography protocols based on traditional mathematical problems such as integer factorization and discrete logarithm, including classical MPC protocols. In order to solve this problem, people consider using the principles of quantum mechanics to construct cryptography protocols. In this respect, the pioneering work was put forward by Bennett and Brassard [11] in 1984. From then on, the research of quantum cryptography has made great progress in various branches. The method of using quantum mechanics to realize SMS was first put forward in Ref [12] for anonymous voting and surveying. Since then, various quantum secure multi-party summation (QSMS) protocols were proposed based on different technologies such as single photons [13], quantum Fourier transform [14], entanglement swapping between d-level quantum systems [15], phase shifting operation of d-level quantum system [16].

In the above proposed QSMS protocols, modular operation is necessary when the sum is calculated or plenty of quantum resources are consumed when large integers are calculated. For this reason, based on entanglement swapping between d-level Bell state and d-level cat state, we propose a secure quantum protocol to calculate the actual(non-modular) sum of the secret integers held by the parties who do not trust each other. With the aid of a semi-honest third party (TP), our QSMS protocol can fulfil the computing task securely by using only $O(\log M)$ qudits. (M is the maximum value of all secret integers.)

Our paper mainly consists of 6 sections. Besides the first section devoted to introduction, the remainder is organized as below: Sect. 2 is devoted to the preliminary knowledge used in our proposed protocol, and Sect. 3 is devoted to the details of the

protocol. Sections 4 and 5 are devoted to analyzing the correctness and security of the protocol, respectively, and the last section concludes the paper.

2 Preliminary knowledge

In our protocol, d-level Bell states and d-level cat states are used as the basic resources, and the entanglement swapping between them is the key technical means. Therefore, it is necessary to review some details about them before describing the protocol.

2.1 *d*-level bell states

The d-level Bell states introduced in Refs [17–19] are a generalization of the classical Bell states for qudits. These states labeled by u_1, u_2 ($u_1, u_2 \in \mathbb{Z}_d$) have the explicit forms as follows

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

where the operation in ket is modulo d. Note that the following similar cases are also modulo d, and we will not mention them again.

The d-level Bell states are orthogonal,

$$\langle\Psi(v_1, v_2)|\Psi(u_1, u_2)\rangle = \delta_{u_1 v_1}\delta_{u_2 v_2},$$

where

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

is Kronecker delta.

For $d = 2$, they reduce to the classical Bell states. In addition, we can also get $|\Psi(0, 0)\rangle$ easily,

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

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 $|\Psi(0, 0)\rangle$,

$$|\Psi(u_1, u_2)\rangle = \left(I \otimes U_{u_1,u_2}\right) |\Psi(0, 0)\rangle , \tag{1}$$

where I is identical operator.

2.2 *d*-level *n*-particle cat states

The d-level n-particle cat states involved in many papers such as [20,21] are a generalization of the d-level Bell states from two qudits to n qudits. They have the form

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

where $u_1, u_2, \ldots, u_n \in \mathbb{Z}_d$. Similar to the Bell states, these cat states form the orthonormal basis of the d^n-dimensional Hilbert space made by n qudits.

An example of these states when $n = 3$ and $d = 2$ is the familiar GHZ state

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

2.3 Entanglement swapping between *d*-level bell states and *d*-level cat states

As mentioned in Ref [22], we tensor multiply the d-level Bell state and the d-level cat state, expand them in the computational basis, swap one particle in the Bell state and one particle in the cat state, re-expand the state in terms of the new Bell states and cat states, and finally get the entanglement swapping between d-level Bell state and d-level cat state. The result formula can be expressed as

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

where the particle labeled by s' in the Bell state and the particle labeled by $t_i\,(2 \le i \le n)$ in the cat state are swapped. After performing Bell measurement on particle s and particle t_i with the result of measurement, for example, $|\Psi(u-g, v_i-h)\rangle$, we obtain the cat state $\left|\Psi(v_1+g, v_2, \ldots, u'+h, \ldots v_n)\right\rangle$.

For a more intuitive understanding of this concept, we depict the process by using Fig. 1. 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 first particle in the Bell state and the first particle in the cat state denoted by square are not involved in the swapping. The arrow is meant to perform a Bell measurement on the particle s and the particle t_i, and the Bell state $|\Psi(u-g, v_i-h)\rangle$ is a possible outcome. After the measurement, the cat state correspondingly collapses into $\left|\Psi(v_1+g, v_2, \ldots, u'+h, \ldots v_n)\right\rangle$, as shown in the lower part of the figure.

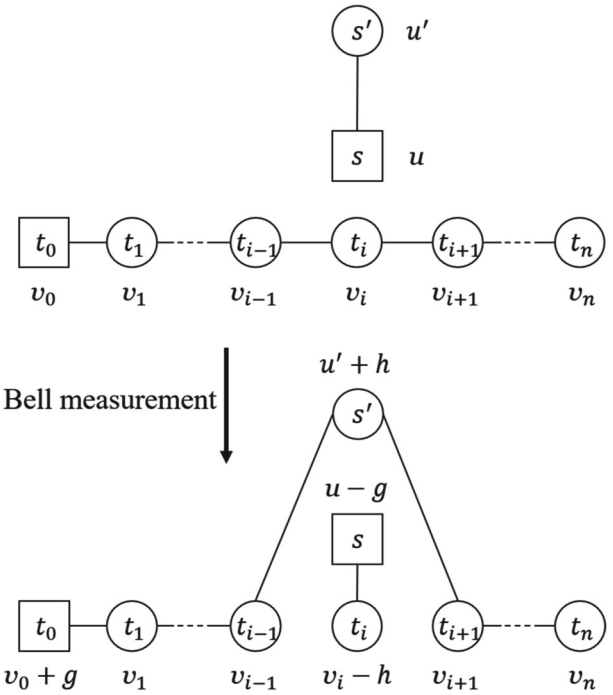

Fig. 1 Entanglement swapping between a Bell state and a cat state

3 The proposed protocol

Suppose that there exist $n(n \geq 3)$ parties named $P_1, P_2, \ldots, P_n$. Each $P_i(i = 1, 2, \ldots, n)$ holds a secret integer x_i with the binary length $|x_i| = L$ and the binary representation $(x_i^{L-1}, \ldots, x_i^1, x_i^0)$, that is, $x_i = \sum_{j=0}^{L-1} 2^j x_i^j$. Further, they would like to calculate the sum of all x_i with keeping their secret unknown to others.

In the following, we propose a secure protocol to complete this task with the help of a semi-honest TP introduced in Ref [23]. The TP is allowed to try his best to get the parties' secrets but not to conspire with any party. The protocol makes use of d-level Bell states and d-level cat states ($d > n$).

Step 1: Each party $P_i(i = 1, 2, \ldots, n)$ prepares L d-level Bell state $|\boldsymbol{\Psi}(0, 0)\rangle$ and encodes his secret integer $x_i = \sum_{j=0}^{L-1} 2^j x_i^j$ according to Formula (1) as follows

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

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

Step 2: TP first prepares L d-level $n+1$ particle cat states

$$\left|\Psi(v_0^j, v_1^j, v_2^j, \ldots, v_n^j)\right\rangle_{t_0^j, t_1^j, \ldots, t_n^j},$$

where $j = 0, 1, 2, \ldots, L-1$, v_i^j is randomly chosen from $\mathbb{Z}_d$ and t_i^j is the label of the i-th particle of the j-th cat state ($i = 0, 1, 2, \ldots, n$). For $i = 1, 2, \ldots, n$, TP extracts the i-th particle from each cat state to form a particle sequence labeled by $(t_i^0, t_i^1, t_i^2, \ldots, t_i^{L-1})$, which is denoted as S_i. Then, TP prepares decoy particles for each S_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 S_i at random positions. The new particle sequence is denoted as S_i'. Finally, TP sends particle sequence S_i' to P_i. Note that the particle sequence labeled by $(t_0^0, t_0^1, t_0^2, \ldots, t_0^{L-1})$ is kept by TP on his own.

Step 3: For $i = 1, 2, \ldots, n$, after P_i receives S_i', TP first informs P_i of the positions and the bases of the decoy particles which has been inserted into S_i, and then, P_i measures the corresponding decoy particles in accordance with TP's information and informs TP of the measurement results; finally, TP checks whether there exist eavesdroppers in the quantum channel. If TP confirms that the channel is secure, they continue to carry out the protocol; otherwise, they abort it and restart a new communication.

Step 4: $P_i (i = 1, 2, \ldots, n)$ restores S_i from S_i' by discarding the decoy particles and then performs L times d-level Bell measurements on the particles from his own Bell states and the cat states that TP has sent to him. That is, for $j = 0, 1, \ldots, L-1$, P_i jointly measures the particle labeled by s_i^j from the Bell state $\left|\Psi(u_i^j, x_i^j)\right\rangle$ and the particle labeled by t_i^j from the cat state $\left|\Psi(v_0^j, v_1^j, v_2^j, \ldots, v_n^j)\right\rangle$. Suppose that the measurement result is $\left|\Psi(r_i^j, r'^j_i)\right\rangle_{s_i^j, t_i^j}$, 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 parties cooperate to compute

$$R^j = \sum_{i=1}^{n} r'^j_i \tag{3}$$

for $j = 0, 1, 2, \ldots, L-1$ and announce them to TP. To prevent TP from eavesdropping the data transmitted in this process, r'^j_i could be encrypted through the similar method mentioned in [24]. That is, using the pre-shared key sequences $(sk_i^0, sk_i^1, \ldots, sk_i^{L-1})$ subject to $\sum_{j=0}^{L-1} sk_i^j \mod d = 0$, $P_i (i = 1, 2, \ldots, n)$ encrypt r'^j_i by calculating $r'^j_i + sk_i^j \mod d$ and then cooperate to compute the sum of them. Next, each P_i sends the particle sequence labeled by $(s'^0_i, s'^1_i, \ldots, s'^{L-1}_i)$ to TP. Similar to the Step 3, the decoy state particles are used to prevent others from eavesdropping.

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

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

where

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

By computing

$$X_j = \sum_{i=1}^{n} \tilde{r}_i^j + R^j - \sum_{i=1}^{n} v_i^j \mod d, \tag{4}$$

TP can get the sum of all x_i

$$X = \sum_{j=0}^{L-1} X_j 2^j$$

and then announces it to each party.

4 Correctness analysis

Now, we explain why our protocol is correct. Each party P_i has a secret integer $x_i = \sum_{j=0}^{L-1} x_i^j 2^j$. $(x_i^{L-1}, \ldots, x_i^1, x_i^0)$ is the binary expression, and L is the binary length. P_i encodes x_i into L d-level Bell states and forms the following particle sequences:

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

TP prepares L d-level $n+1$ particle cat states

$$\left|\Psi(v_0^0, v_1^0, v_2^0, \ldots, v_n^0)\right\rangle_{t_0^0, t_1^0, \ldots, t_n^0},$$
$$\left|\Psi(v_0^1, v_1^1, v_2^1, \ldots, v_n^1)\right\rangle_{t_0^1, t_1^1, \ldots, t_n^1},$$
$$\ldots,$$
$$\left|\Psi(v_0^{L-1}, v_1^{L-1}, v_2^{L-1}, \ldots, v_n^{L-1})\right\rangle_{t_0^{L-1}, t_1^{L-1}, \ldots, t_n^{L-1}}.$$

For $j = 0, 1, \ldots, L-1$, P_i performs d-level Bell measurement on particle s_i^j from his own Bell state and particle t_i^j from TP's cat state with the result

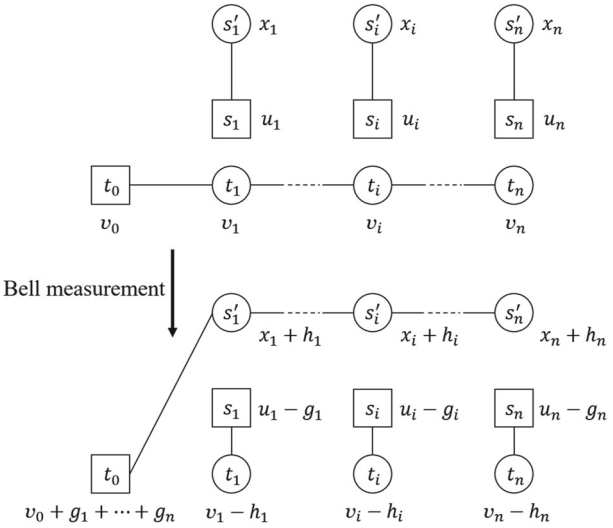

Fig. 2 Entanglement swappings between n Bell states and a cat state

$\left|\boldsymbol{\Psi}(u_i^j - g_i^j \mod d, v_i^j - h_i^j \mod d)\right\rangle$. After all parties finish Bell measurements, according to Formula (2), the j-th cat state becomes

$$\begin{aligned} |\boldsymbol{\Psi}(v_0^j + \sum_{i=1}^{n} g_i^j \mod d, \\ x_1^j + h_1^j \mod d, \\ x_2^j + h_2^j \mod d, \\ \cdots, \\ x_n^j + h_n^j \mod d)\rangle. \end{aligned}$$

The process and results can be intuitively shown in Fig. 2 (where the superscript j is omitted).

We can rewrite Formula (3) as follows

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

where $\alpha \leq n$ is the number of occurrences of modular operations. In Formula (4), $\sum_{i=1}^{n} \tilde{r}_i^j$ can be rewritten as

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

where $\beta \leq n$ is also the number of occurrences of modular operations. Thus,

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

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

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

and the sum of all x_i

$$X = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} \sum_{j=0}^{L-1} x_i^j 2^j = \sum_{j=0}^{L-1} X_j 2^j.$$

So, the correct result can be obtained by performing the protocol.

5 Security analysis

In this section, we will show our protocol is secure against three kinds of threats from external attack, participants' attack, and semi-honest TP's attack, respectively. In the aspect of defending against the external attack, we will show that an outside eavesdropper cannot steal any party's secret. In the aspect of resisting the participants' attack, we will show that at most $n - 2$ dishonest participants who conclude together to get others' secrets cannot succeed. At last, we will show that the semi-honest TP who does not collude with any participant cannot steal any party's secret.

5.1 External attack

In this subsection, we explain why an outside eavesdropper cannot get the secrets in each step.

In Step 1, 3, and 4, neither quantum nor classical information is transmitted, and the outside eavesdropper obtains nothing helpful.

In Step 2, qudits are transmitted and some usual attacks such as intercept–resend attack, entangle–measure attack, and measure–resend attack may be launched by an outside eavesdropper. In our protocol, decoy state technique [25], which is an effective

method for eavesdropping check just like in BB84 [11], is used to guarantee that the qudits can be transmitted securely. In [26], the reason why the decoy states used in 2-level quantum system can efficiently resist these attacks has been explicitly analyzed. Similarly, the decoy states in d-level quantum system adopted by our protocol can also ensure the security of qudit transmission. That is, an outside eavesdropper can be detected if it exists. In addition, the qudit particles transmitted in this step are independent of any participants' secret and therefore no secret can be stolen.

In Step 5, $R^j (j = 0, 1, \ldots, L-1)$ is announced to TP and no information about x_i is leaked because R^j has no concern with x_i^j. In the process of the qudits transmission, an outside eavesdropping can be detected for the same reason as in Step 2. Moreover, we declare there is no information leakage when each party sends particle ${s'}_i^j$ to TP. After each P_i completes d-level Bell measurement, the density operator ρ for the entire quantum system is

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

where

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

Tracing out the other qudits, we get the reduced density operator of the qudit ${s'}_i^j$

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

where $\mathrm{Tr}^{'}$ stands for tracing out qudits with label $t_0^j, s'^j_1, \ldots, s'^j_{i-1}, s'^j_{i+1}, \ldots, s'^j_n$, and I is identical operator. So the qudit s'^j_i is completely depolarized, and it does not leak any information.

In Step 6, TP announces the final result and the attackers cannot obtain any party's secret.

5.2 Participant attack

Participant attack, which was put forward in [27], is a kind of powerful attack by either one dishonest participant or more dishonest participants who conspire together. We will discuss these two cases separately.

First, we discuss the case that one dishonest participant, without loss of generality, P_1, wants to steal other participants' secret. In our proposed protocol, P_1 does not transmit any qudits to others except TP and other parties do not transmit any qudits to P_1. If P_1 intercepts the particles transmitted between other parties and TP in Steps 2 and 5, he will be revealed just as an outside eavesdropper because he does not know the bases and the positions of the decoy particles, and he cannot get any information from the intercepted qudits for the same reason analyzed above. In Step 5, although knowing R^j, P_1 cannot steal other participants' secrets because R^j does not contain any information about x_i.

Second, we explain that more participants colluding together also cannot obtain others' secret. Without loss of generality, we consider the extreme case in which there are $n-2$ participants $P_1, P_2, \ldots, P_{n-2}$ who collude together to steal the secret of P_{n-1} or P_n. As there is no qudit transmitted between $P_1, P_2, \ldots, P_{n-2}$ and P_{n-1}, P_n, the conspiring participants cannot get the qudits from P_{n-1} or P_n unless intercepting the qudits transmitted from them to TP. When intercepting the qudits, the conspiring participants can be put in light just like external attackers. Even though they have intercepted the qudits, they cannot be successful because the intercepted qudits are completely depolarized just like the above analysis. Besides, $P_1, P_2, \ldots, P_{n-2}$ also cannot get anything about x_{n-1}, x_n from R^j in Step 5.

5.3 Semi-honest TP's attack

In the process of performing the protocol, the semi-honest TP can get $x_i^j + h_i^j$ and R^j, but he cannot know x_i^j because of not knowing h_i^j from R^j. If TP conspires with some participants, he can get h_i^j from them and then know x_i^j. From the above, we know that an semi-honest TP who does not conspire with other participants cannot succeed in stealing the participants' secrets.

6 Conclusion

At present, almost all of the existing QSMS protocols require modular operation; even some of them are modulo-2 summation. Thus, the actual sum cannot be completed in

these protocols, or the modulus need to be increased, which requires more complex quantum systems. In Ref [15], the non-modular summation can be achieved, but the number of the required qudits must be greater than the maximum value of all parties' secret integers. When securely computing the sum of very large integers, participants need to consume a lot of quantum resources. In addition, the protocol is probabilistic and there exists a possibility of failure. Our protocol is deterministic, and the number of required quantum qudits only depends on the digit number of the secret integers. In other words, we only need $O(\log M)$ qudits (M is the maximum value of all secret integers) to complete the task. Specially, under the condition of computing the sum of larger integers for a small number of participants, our protocol utilizes few quantum resources and has higher efficiency.

In our paper, we proposed a novel quantum protocol to securely calculate multi-party summation based on d-level quantum system. In the protocol, a semi-honest TP prepares d-level cat states and transmits parts of them to the participants who want to compute the sum of their integers securely and secretly. These participants encode their secret integers into d-level Bell states and then complete entanglement swapping between the d-level cat states and the d-level Bell states by performing d-level Bell measurements. Finally, TP can obtain the sum of participants' secret integers by performing d-level cat state measurements on new cat states and then performing appropriate calculations. Our protocol can resist both external attack and participant' attack even though there are multiple participants colluding together. In addition, the protocol can also resist a semi-honest TP's attack so long as he does not make a collusion with any participant.

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

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

References

1. Yao, A.C.: in *Proc. of the 23rd Annual IEEE Symposium on Foundations of Computer Science, 1982* (1982), pp. 160–164
2. Goldreich, O., Micali, S., Wigderson, A.: in *Proc. of the nineteenth annual ACM symposium on Theory of computing* (1987), pp. 218–229
3. Katz, J.: in *Proc. of the 39th annual ACM symposium on Theory of computing* (2007), pp. 10–20
4. Gordon, S.D., Hazay, C., Katz, J., Lindell, Y.: in *Proc. of the 40th annual ACM symposium on Theory of computing* (2008), p. 413
5. Freedman, M.J., Nissim, K., Pinkas, B.: in *Proc. of EUROCRYPT 2004* (Berlin, Heidelberg, 2004), pp. 1–19
6. Aly, A., Van Vyve, M.: in International Conference on Financial Cryptography and Data Security, pp. 110–129. , (Berlin, Heidelberg (2017)
7. Maheshwari, N., Kiyawat, K.: in 2011 Fifth Asia Modelling Symposium, pp. 187–192. (2011)

8. Du, W., Atallah, M.J.: in *Proc. of the 2001 Workshop on New Security Paradigms* (2001), pp. 13–22
9. Shor, P.: in Proc. of 35th Annual Symposium on the Foundations of Computer Science (Los Alamitos. CA , 124–134 (1994)
10. Grover, L.K.: in *Proc. of the 28 Annual ACM Symposium on Theory of Computing* (1996), pp. 212–219
11. Bennett, C.H, Brassard, G.: in *Proc. of IEEE International Conference on Computers* (Bangalore, Indian, 1984), pp. 175–179
12. Vaccaro, J.A., Spring, J., Chefles, A.: Physical Review A **75**(1), 012333 (2007)
13. Zhang, C., Situ, H., Huang, Q., Yang, P.: Int. J. Quant. Inf. **15**(2), 1750010 (2017)
14. Shi, R.H., Zhang, S.: Quant. Inf. Proc. **16**(9), 225 (2017)
15. Ji, Z.X., Zhang, H.G., Wang, H.Z., Wu, F.S., Jia, J.W., Wu, W.Q.: Quant. Inf. Proc. **18**(6), 168 (2019)
16. Duan, M.Y.: Int. J. Theor. Phys. **59**(11), 1638 (2020)
17. Cerf, N.J.: Acta Physica Slovaca **48**(3), 115 (1998)
18. Cerf, N.J.: J. Modern Opt. **47**(2–3), 187 (2000)
19. Cerf, N.J.: Phys. Rev. Lett. **84**(19), 4497 (2000)
20. Guo, F.Z., Gao, F., Qin, S.J., Zhang, J., Wen, Q.Y.: Quant. Inf. Proc. **12**(8), 2793 (2013)
21. Ji, Z.X., Ye, T.Y.: Quant. Inf. Proc. **16**(7), 177 (2017)
22. Karimipour, V., Bagherinezhad, S., Bahraminasab, A.: Physical Review A **65**(4), 042320 (2002)
23. Yang, Y.G., Xia, J., Jia, X., Hua, Z.: Quant. Inf. Proc. **12**(2), 877 (2013)
24. Gan, Z.G.: Int. J. Theoret. Phys. **59**(10), 3086 (2020)
25. Li, C.Y., Zhou, H., Y, Y. Wang, F.G. Deng, : Chin. Phys. Lett. **22**(5), 1049 (2005)
26. Chen, Y., Man, Z.X., Xia, Y.J.: Chin. Phys. Lett. **24**(1), 19 (2007)
27. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Quant. Inf. Comput. **7**(4), 329 (2007)