Int J Theor Phys (2010) 49: 2793–2804
DOI 10.1007/s10773-010-0472-5

An Efficient Protocol for the Secure Multi-party Quantum Summation

Xiu-Bo Chen · Gang Xu · Yi-Xian Yang · Qiao-Yan Wen

Received: 20 April 2010 / Accepted: 16 August 2010 / Published online: 7 September 2010

Abstract In this paper, a new and efficient quantum protocol which allows a group of mutually distrustful players to perform the summation computation is proposed. Different from previous protocols, we utilize the multi-particle entangled states as the information carriers. A third party, i.e. TP, is assumed semi-honest in the two-party quantum summation protocol. All various kinds of outside attacks and participant attacks are discussed in detail. In addition, we code all players' Bell-basis measurement outcomes into one classical bit (cbit). Not only the cost of classical information in the public communication network is decreased, but also the security of the protocol is improved. The protocol is also generalized into multiparty quantum summation. It is secure for the collusive attack performed by at most $n-2$ players.

Keywords Quantum summation · GHZ state · Security

1 Introduction

Secure multi-party computation has been an important and fruitful area of research in recent years. It is possible that quantum states could be used to efficiently deal with the classical problem. Now, secure multi-party computation has been extended to the quantum field [1–3]. Chau [4] proposed a scheme for speeding up classical multi-party computing using quantum techniques. Smith [5] established any multi-party quantum computation which

X.-B. Chen (✉) · Y.-X. Yang · Q.-Y. Wen
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: flyover100@163.com

X.-B. Chen · Y.-X. Yang
Key Laboratory of Network and Information Attack and Defense Technology of MOE, Beijing University of Posts and Telecommunications, Beijing 100876, China

G. Xu
College of Mechanical Engineering, Taiyuan University of Technology, Taiyuan 030024, China

can be securely performed as long as the number of dishonest players is less than $n/6$. Ben-Or et al. [3] investigated how much trust is necessary—that is, how many players must remain honest—in order for distributed quantum computations to be possible.

Secure multi-party summation is a kind of secure multi-party computation. The problem of secure multi-party summation is as follows: n players $(A_1, A_2, \ldots, A_n)$ wish to evaluate a summation function $F(x_1, x_2, \ldots, x_n)$, where x_i is a secret value provided by A_i. The result of this function can then be revealed publicly or privately to some particular player. The task of secure multi-party computation is to preserve the privacy of the party's inputs/outputs and guarantee the correctness of the computation. Heinrich [6, 7] studied summation of sequences in the quantum model of computation. Reference [8] investigated the quantum Boolean summation with repetitions in the Worst-Average Setting. In 2007, Du et al. [9] proposed a protocol for the secure quantum addition module $n+1$ $(n \geq 2)$ based on non-orthogonal single particle states, which allows a number to be added to an unknown number secretly. Almost previous protocols [6–9] are designed by means of single particle states. Recently, some researchers began to consider the problem of quantum computation with the entangled states. Yang et al. [10] proposed an efficient quantum private comparison protocol for comparing the equal information with the TP's help. Their protocol based on the two-particle entangled Einstein-Podolsky-Rosen (EPR) pairs. Hillery et al. [11] utilized the two-particle N-level entangled state to propose a protocol for calculating the summation of N players in voting procedures, and guaranteeing the anonymity of the players. In fact, Refs. [10, 11] have utilized one principal character of two-particle entangled state, i.e. the implementation of the certain unitary operation on one particle of two-particle entangled states can produce the mutually orthogonal state. However, the above character for the multi-particle entangled state is not existed. So, the research on the quantum summation with the multi-particle entangled state is few.

In this paper, we proposed a new and efficient protocol for the quantum summation with the multi-particle entangled GHZ states. It has been reported that up to six-photon GHZ state has been created in experiment [12]. Thus, it is significant to further research the quantum summation with the multi-particle entangled state. We first propose a protocol between two parties with the triplet GHZ state. Similar to the previous protocols [10, 11], this two-party quantum summation protocol includes a TP who prepares the initial states and records the results. In the Hillery's protocol [11], the TP is an honest authority. Yang's [10] protocol use a dishonest TP. In this paper, we assume TP is semi-honest. That is, TP executes the protocol loyally, keeps a record of all its intermediate computations and might try to steal the players' private inputs from the record, but he cannot be corrupted by the adversary. Many additional technologies of cryptography (such as hash function, QKD protocol, etc.) are not necessary. All various kinds of outside attacks and participant attacks are discussed in detail. It is necessary and important to study the multi-party quantum summation protocol without the help of the TP. So, we generalize the two-party protocol to multi-party quantum summation without TP. It is secure for the collusive attack performed by at most $n-2$ players. On the other hand, the problem of the cost of classical information has been emphasized in many quantum communication protocols [13, 14]. Based on the idea of the network coding, we code all players' Bell-basis measurement outcomes into one cbit. So, the cost of classical information in the public communication network is decreased, and the protocol's security is improved.

The rest of the present paper is organized as follows. In Sect. 2, we propose an efficient method for computing the summation of two secrets which are distributed among two parties with the help of the semi-honest TP. The security with respect to various kinds of attacks is discussed in detail. In Sect. 3, we generalize the two-party quantum summation protocol to multi-party without the help of the TP. It is secure for the collusive attack performed by at most $n-2$ players. Finally, discussions and conclusions are drawn in Sect. 4.

2 Protocol of Two-party Quantum Summation

The task in this section is first to compute a function of summation with two players' private inputs such that in the end the final result is calculated by the semi-honest TP. Then, all various kinds of outside attacks and participant attacks are discussed.

All participants beforehand agree on the following encoding:

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \rightarrow 0; \qquad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \rightarrow 1 \tag{1}$$

Therefore, the qubit state carrying classical message r can be written as

$$|\varphi\rangle = [|0\rangle + (-1)^r |1\rangle]/\sqrt{2} \tag{2}$$

where superscript r is equal to 0 or 1.

2.1 The Process of Two-party Quantum Summation

Suppose that two players A_1 and A_2 have secret strings I_1 and I_2, respectively. They wish TP calculates the summation $I_1 \oplus I_2$. Here, $\oplus$ denotes the addition module 2.

$$I_1 = (i_{1L}, i_{1(L-1)}, \ldots, i_{11}) \tag{3}$$

$$I_2 = (i_{2L}, i_{2(L-1)}, \ldots, i_{21}) \tag{4}$$

$$I_1 \oplus I_2 = (i_{1L} \oplus i_{2L}, i_{1(L-1)} \oplus i_{2(L-1)}, \ldots, i_{11} \oplus i_{21}) \tag{5}$$

This two-party quantum summation protocol includes the following four steps.

Two players and TP are required to first share the reliable triplet GHZ states.

Sharing triplet GHZ states could have come about in many different ways [15, 16]. Here, similar to the previous protocols [10, 11], TP prepares GHZ states, and sends them to two players.

TP prepares ordered L triplet GHZ states in the same quantum state, i.e.

$$|\xi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{A_1' A_2' T} \tag{6}$$

Then, TP takes the first photon from each GHZ state to form an ordered photon sequence S_1, and the second photon to form sequence S_2. The remaining photons compose another sequence S_T.

For preventing the eavesdropping, TP prepares k decoy photons $\otimes_{j=1}^{k}|S_j\rangle$, here $|S_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ $(j = 1, 2, \ldots, k)$. Then, he inserts randomly the k decoy photons $\otimes_{j=1}^{k}|S_j\rangle$ into the sequences S_1 and S_2. Note that any one does not know the initial states and positions of the k decoy photons except TP. Finally, TP sends two sequences S_1 and S_2 with decoy photons to players A_1 and A_2, respectively.

Confirming that two players have received all the photons owned to themselves, TP publics the position of the decoy photons sent to them, but he keeps the initial states secret. In the following, two players measure every decoy photon with X-basis or Z-basis randomly, here $X = \{|+\rangle, |-\rangle\}$ and $Z = \{|0\rangle, |1\rangle\}$. (Note that there is 50% probability that two players will choose the wrong measurement basis, so half of the measurement outcomes are useless.) After that, TP can determine the error rate according to measurement outcome of these k sample photon's initial state. If the error rate exceeds the threshold, then this communication is aborted and repeat the step (S1). Otherwise, they can go on.

Two players encode their secret messages.

According to the secret messages, two players prepare L single photons and make them in the states $|+\rangle$ or $|-\rangle$. For example, if the secret messages are $0110\ldots1$, the states of single photons should be in $|+\rangle|-\rangle|-\rangle|+\rangle\cdots|-\rangle$.

Without loss of generality, the state of a system including one secret $i_1 \in I_1$, one secret $i_2 \in I_2$ and a triplet entangled GHZ is

$$\begin{aligned}|\Phi\rangle_{A_1A_2A_1'A_2'T} &= |\varphi\rangle_{A_1} \otimes |\varphi\rangle_{A_2} \otimes |\xi\rangle_{A_1'A_2'T}\\ &= \frac{1}{2\sqrt{2}}[|0\rangle + (-1)^{i_1}|1\rangle]_{A_1} \otimes [|0\rangle + (-1)^{i_2}|1\rangle]_{A_2}\\ &\quad \otimes (|000\rangle + |111\rangle)_{A_1'A_2'T} \qquad (7)\end{aligned}$$

Here, the player A_1 is in possession of particles A_1A_1', while particles A_2A_2' and particle T belong to the player A_2 and TP, respectively.

Two players implement the measurement.

Two players perform Bell-basis measurements on particles A_1A_1' and A_2A_2', respectively. To make TP know the state obtained with certainty, two players need to announce their measurement outcomes. For convenience, define that Bell-basis measurement outcomes $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ correspond to the cbit strings $M_1M_2 = 00$, 10, 01, 11. The measurement outcomes of players A_1 and A_2 are denoted as $M_1^{A_1}M_2^{A_1}$ and $M_1^{A_2}M_2^{A_2}$.

Maximizing information exchange over classical communication networks has been a major subject among both the information theory and the networking societies. On the other hand, the classical communication cost can be used to better understand the fundamental laws of quantum information processing, and also be regarded as the natural generalization of quantum communication complexity [17], it has been paid much attention in many quantum communication protocols, such as the remote state preparation (RSP) [13, 18], quantum secure direct communication (QSDC) [14], etc.

Here, considering the problem of the information exchange over the public communication network, we code two Bell-basis measurement outcomes into one cbit $X = M_1^{A_1} \oplus M_1^{A_2}$. Then, the cbit X is broadcasted by the player A_1 (or A_2) via the public channel. That is, four cbits (two Bell-basis measurement outcomes) are coded into one cbit. The advantage is that the cost of the classical information in the public communication network is cut down. Moreover, it will be seen that the security of the protocol is improved in the Sect. 2.2.

TP obtains the summation of two secret messages.

After two players perform Bell-basis measurements, the state of particle T collapses into one certain state at random. Depending on the cbit X, TP performs a unitary operation $U(X)$ on the particle T. Here, the independent variable X is the number 0 or 1. The transformation $U(X)$ is the Pauli operator I, Z.

$$U(0) = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad U(1) = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad (8)$$

Then, TP measures the particle T in the basis $\{|+\rangle, |-\rangle\}$ and obtains the summation of two players' secrets.

Table 1 Two players A_1 and A_2 have secrets i_1 and i_2. Bell-basis measurement outcomes obtained by players A_1 and A_2 are $M_1^{A_1}M_2^{A_1}$ and $M_1^{A_2}M_2^{A_2}$, respectively. The collapsed state on the particle in TP hand is denoted as T_S. Unitary transformation performed by TP is $U(X)$. The summation of the secrets i_1 and i_2 is r

$M_1^{A_1}M_2^{A_1}$	$M_1^{A_2}M_2^{A_2}$	T_S	$U(X)$	r
00	00	$[\|0\rangle + (-1)^{i_1}(-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	10	$[\|0\rangle - (-1)^{i_1}(-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	01	$[(-1)^{i_1}\|1\rangle + (-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	11	$[(-1)^{i_1}\|1\rangle - (-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
10	00	$[\|0\rangle - (-1)^{i_1}(-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	10	$[\|0\rangle + (-1)^{i_1}(-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	01	$[-(-1)^{i_1}\|1\rangle + (-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	11	$[-(-1)^{i_1}\|1\rangle - (-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
01	00	$[(-1)^{i_1}\|0\rangle + (-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	10	$[(-1)^{i_1}\|0\rangle - (-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	01	$[\|1\rangle + (-1)^{i_1}(-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	11	$[\|1\rangle - (-1)^{i_1}(-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
11	00	$[-(-1)^{i_1}\|0\rangle + (-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	10	$[-(-1)^{i_1}\|0\rangle - (-1)^{i_2}\|1\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$
	01	$[\|1\rangle - (-1)^{i_1}(-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(1)$	$i_1 \oplus i_2$
	11	$[\|1\rangle + (-1)^{i_1}(-1)^{i_2}\|0\rangle]_T/4\sqrt{2}$	$U(0)$	$i_1 \oplus i_2$

For example, as far as the player A_1's secret $i_1 \in I_1$, the player A_2's secret $i_2 \in I_2$ are concerned, if measurement result is $M_1^{A_1}M_2^{A_1} = 10$ and $M_1^{A_2}M_2^{A_2} = 01$, the state of particle T is

$$\langle\Psi^+|_{A_2A_2'}\langle\Phi^-|_{A_1A_1'}\Phi\rangle_{A_1A_2A_1'A_2'T} = \frac{1}{4\sqrt{2}}[(-1)(-1)^{i_1}|1\rangle + (-1)^{i_2}|0\rangle]_T \tag{9}$$

It is easy to calculate $X = M_1^{A_1} \oplus M_1^{A_2} = 1$. TP performs the unitary operation $U(X) = U(1)$. The above state is transformed into

$$\frac{1}{4}\frac{1}{\sqrt{2}}[(-1)^{i_2}|0\rangle + (-1)^{i_1}|1\rangle]_T \tag{10}$$

From the above state, it can be seen that if $i_1 = i_2$ (i.e. $i_1 = i_2 = 0$ or $i_1 = i_2 = 1$), TP will obtain the state $|+\rangle$ which corresponds to the value $r = 0$. On the contrary, if $i_1 \neq i_2$ (i.e. $i_1 = 0, i_2 = 1$ or $i_1 = 1, i_2 = 0$), TP can obtain the state $|-\rangle$ which corresponds to the value $r = 1$. In conclusion, TP obtains the value $r = i_1 \oplus i_2$.

Through calculating and summarizing, it is found that TP always obtains the value $r = i_1 \oplus i_2$ for any Bell-basis measurement outcomes. All cases are shown in the Table 1.

2.2 Security Analysis of Two-party Quantum Summation

Now, we analyze the security of this quantum summation protocol. As we know, the quantum summation's security is more complex than QKD, QSDC and quantum secret sharing (QSS) because the attack from all parties have to be considered in the design of quantum summation protocols. Outside eavesdroppers want to steal the players' secrets. Moreover, the participant might also try to derive the player's private information. Therefore, the security of this quantum summation protocol is to prevent from outside attack and the participant attack.

Case 1: Outside Attack

In this quantum summation protocol, TP use the decoy photons to prevent from eavesdropping. Obviously, this checking method is derived from the idea of the BB84 QKD protocol [19]. It has been proven to be unconditionally secure by several groups [20]. The BB84 QKD protocol is secure even when the channel is noisy. Because any eavesdropping will leave a trace in the outcomes of the decoy sampling photons [21], outside Eve's several kinds of attacks, such as the intercept-resend attack, the measurement-resend attack, the entanglement-measure attack and the denial-of-service (DOS) attack will be detected with nonzero probability during the security checking process. For example, Eve can make the simplest intercept-resend attack like this: she measures photons in randomly chosen basis, and then sends the fake photons prepared by herself based on the measurement outcomes to the receiver. If she chooses the correct basis, she can get the information; if she chooses the wrong basis, she gets the information by the possibility of 50%. Because Eve chooses the basis fully randomly, so she will send the wrong photons by the possibility of 25%, and she will be discovered in the eavesdropping detection process.

Trojan horse attack exists in two-way quantum communication, such as the delay-photon Trojan horse attack and the invisible photon eavesdropping (IPE) Trojan horse attack. The Trojan horse attack has no influence on the legitimate photons, can't be discovered by the checking progress. The delay-photon Trojan horse attack is inserting a spy photon of the same wavelength in a legitimate signal with a delay time, shorter than the time windows. Thus the sender will do the same operation to the spy photons and the legitimate photons. Eve can separate the spy photons after player's coding operation and do measurement to get the information. The IPE utilizes the fact that the single photon detector is only sensitive to the photons with a special wavelength. Therefore, Eve can insert a synchronized photon whose wavelength is far away from the authorized one. The unitary operation is often wavelength dependent, so the IPE attack will cause error, but the delay-photon attack can get the full information encoded. Similar to the Ref. [22], in order to defeat Eve's delay-photon Trojan horse attack, a photon number splitter should be introduced. Moreover, if a filter with which only the wavelengths close to the operating one can be let in is added before all parties devices, the Eve's IPE attack can be defeated.

As for the photon-number-splitting (PNS) attack, the player can insert a filter in front of his devices to filter out the photon signal with an illegitimate wavelength and use some beam splitters to split the sampling signals chosen for eavesdropping check before they measure the signals. If the multiphoton rate is unreasonably high, the transmission is terminated. Otherwise, the procedure continues to the next step.

It is well known that when a qubit of an entangled pair travels in a noise quantum channel, parts of the initial entanglement might be lost. Hence, a security problem for this protocol seems to arise. Fortunately, it has been proven that over any long distance, the reliably shared entanglement can be obtained by using the quantum-repeater technique, containing the entanglement purification and teleportation [23–25].

In addition, because the particles used to establish the quantum channel do not carry any secret messages, if eavesdropper exists, she not only can be detected but also obtain no any useful information in the process of security checking. Passing the security checking procedure certifies that they share the sufficiently secure entangled states. However, if eavesdropping occurs, they discard these triplets, and a new ensemble of triplets should be reproduced. After three parties ensure the security of the quantum channel, eavesdropper has not chance to attack the secret message any more because there is no longer the transmission of the qubit. In the process of the protocol, there are only the communications of classical information. However, in this quantum summation protocol the transmitted classical information about Bell-basis measurement outcomes are not relevant to the secrets.

So, our quantum summation protocol is robust against outside attack.

Case 2: Participant Attack: One of two players attempts to eavesdrop the other's secret

Because the role of the player A_1 is the same as that of the player A_2, we assume the player A_1 wants to steal the player A_2's secret. After three participants securely share the reliable GHZ states, the player A_1' entangles an ancillary state $|E_i\rangle$ on the particle in his hand. The effect of the player A_1's attack can be described

$$\hat{U}_E|0\rangle|E_i\rangle = a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle \tag{11}$$

$$\hat{U}_E|1\rangle|E_i\rangle = c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle \tag{12}$$

Therefore, the combination system can be rewritten as

$$\begin{aligned}
&\hat{U}_E|\xi\rangle_{A_1'A_2'T}|E_i\rangle \\
&\quad = \hat{U}_E[(|000\rangle + |111\rangle)_{A_1'A_2'T}/\sqrt{2}]|E_i\rangle \\
&\quad = [a|000\rangle_{A_1'A_2'T}|\delta_{00}\rangle + b|100\rangle_{A_1'A_2'T}|\delta_{01}\rangle + c|011\rangle_{A_1'A_2'T}|\delta_{10}\rangle \\
&\qquad + d|111\rangle_{A_1'A_2'T}|\delta_{11}\rangle]/\sqrt{2}
\end{aligned} \tag{13}$$

Players A_1 and A_2 perform Bell-basis measurement on particles A_1A_1' and A_2A_2', respectively. Suppose that the $M_1^{A_1}M_2^{A_1} = M_1^{A_2}M_2^{A_2} = 00$. The following state can be obtained (up to the global phase factor)

$$\begin{aligned}
&a|0\rangle_T|\delta_{00}\rangle + b(-1)^{i_1}|0\rangle_T|\delta_{01}\rangle + c(-1)^{i_2}|1\rangle_T|\delta_{10}\rangle + d(-1)^{i_1}(-1)^{i_2}|1\rangle_T|\delta_{11}\rangle \\
&\quad = |+\rangle_T[a|\delta_{00}\rangle + b(-1)^{i_1}|\delta_{01}\rangle + c(-1)^{i_2}|\delta_{10}\rangle + d(-1)^{i_1}(-1)^{i_2}|\delta_{11}\rangle] \\
&\qquad + |-\rangle_T[a|\delta_{00}\rangle + b(-1)^{i_1}|\delta_{01}\rangle - c(-1)^{i_2}|\delta_{10}\rangle - d(-1)^{i_1}(-1)^{i_2}|\delta_{11}\rangle]
\end{aligned} \tag{14}$$

If the player A_1 knows the TP's measurement outcome on the particle T in the basis $\{|+\rangle, |-\rangle\}$, he will know the player A_2's secret i_2 because he know the unitary operation $\hat{U}_E$ and the secret i_1. Unfortunately, TP may not be corrupted by the adversary. Under the circumstances, the player A_1 cannot steal valuable information about the player A_2's secret i_2. In addition, the player A_1 wants to have no effect on the whole system. So, there must be the relation $b = c = 0$, and $a|\delta_{00}\rangle = d|\delta_{11}\rangle$. Thus, the ancillary state $|E_i\rangle$ and the entangled GHZ state are product states, in essence. Overall, the attack that one of two players attempts to eavesdrop the other's secret is invalid.

Case 3: Participant Attack: The semi-honest TP attempts to steal the players' secrets

In this paper, two players interact with the TP who is semi-honest. It means that TP is required to execute the protocol loyally, and cannot cooperate with the player A_1 or A_2. The TP's attack only is he keeps a record of all its intermediate computations and might try to derive the parties' private inputs from the record. Because TP in this protocol is semi-honest, he can guess the partial secrets owned by players. But, he cannot steal all the secrets. The main goal of the security for the TP's attack in this quantum summation protocol is to prevent TP to determinately steal all messages in the secret strings I_1 and I_2. In this protocol, TP obtains the sharing secret message $r = i_1 \oplus i_2$. That is, TP only know if the secret $i_1 = i_2$ or not. For example, under the condition of $i_1 = i_2$, he cannot determinately know $i_1 = i_2 = 0$ or $i_1 = i_2 = 1$.

On the other hand, a kind of TP's attack is required to be considered when three participants share the entangled GHZ state in the step (S1). TP can take the attack of fake particle. That is, he first prepares $2L$ two-particle EPR entangled states. And then, he shares L EPR pairs with two players, respectively. If TP knows the measurement outcomes $M_1^{A_j} M_2^{A_j}$ $(j = 1, 2)$ in the step (S3), he can steal the player's secrets. However, only one cbit $\oplus \sum_{j=1}^{2} M_1^{A_j}$, which is not relevant to every player's secret, is broadcasted via the public communication network. Under the circumstances, TP should not determinedly learn the player's secrets.

In order to prevent TP from the attack of the fake particle, two players can utilize the relation of entanglement to ensure sharing the reliable GHZ states. The triplet entangled GHZ state can be written as follows.

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{A_1' A_2' T}\\&\quad = \frac{1}{2\sqrt{2}}[|+\rangle|+\rangle|+\rangle + |+\rangle|-\rangle|-\rangle + |-\rangle|+\rangle|-\rangle + |-\rangle|-\rangle|+\rangle]_{A_1' A_2' T}\end{aligned} \tag{15}$$

Similar to many protocols [26], three participants can choose two basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ to measure their particles. By comparing the measurement result, they can determine whether the reliable GHZ entangled state is shared. Therefore, our quantum summation protocol is secure for the semi-honest TP's attack.

3 Protocol of Multi-party Quantum Summation

Now, many experiments about the creation of the multi-particle entangled GHZ state have been reported [12]. Thus, it is essential to generalize the above two-party quantum summation protocol to n-party $(n > 2)$. In this case, one player, suppose that the player A_1 can act as TP.

All players agree on the conditions in (2). Like the (3), the j-th player has the secret sequence I_j $(j = 1, 2, \ldots, n)$. The player A_1 distributes the entangled state and calculates the summation $\oplus \sum_{j=1}^{n} I_j$. Here, $\oplus \sum$ denotes the addition module 2. The process of the n-party quantum summation protocol is as follows.

All players first share the reliable n-particle GHZ states.

The player A_1 prepares ordered L entangled states in the same quantum state, i.e.

$$|\xi\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n}_{A_1' A_2', \ldots, A_n'} + |1\rangle^{\otimes n}_{A_1' A_2', \ldots, A_n'}) \tag{16}$$

Then, the player A_1 takes the first photon from each GHZ to form the ordered photon sequence S_1, the second photon to form the sequence $S_2, \ldots$, and the n-th photon to form the sequence S_n.

For preventing the eavesdropping, the player A_1 adopts the same technique, that is, randomly inserting some decoy photons in the $n-1$ sequences $S_2, S_3, \ldots,$ and S_n. Then, he sends $n-1$ sequences with decoy photons to players $A_2, A_3, \ldots,$ and A_n, respectively.

Confirming that the other $n-1$ players have received all the photons owned to themselves, the player A_1 analyses the error rate. If the error rate is enough low, they can go on. Otherwise, they discard these GHZ states and repeat the step (S1).

Players encode their secret messages.

The player A_j $(j = 2, 3, \ldots, n)$ prepares L single photons and makes them in the states $|+\rangle$ or $|-\rangle$ according to his secrets. Because the player A_1 can add his secret to the final result, he does not prepare L single photons.

Without loss of generality, the state of a system including the player A_j's secret $i_j \in I_j$ $(j = 2, 3, \ldots, n)$ and an n-particle entangled GHZ state is

$$\begin{aligned}|\Phi\rangle_{A_2A_3,\ldots,A_nA_1'A_2',\ldots,A_n'} &= (|\varphi\rangle_{A_2} \otimes |\varphi\rangle_{A_3} \otimes \cdots \otimes |\varphi\rangle_{A_n}) \otimes |\xi\rangle_{A_1'A_2',\ldots,A_n'} \\ &= \frac{1}{(\sqrt{2})^n}[|0\rangle + (-1)^{i_2}|1\rangle]_{A_2} \otimes [|0\rangle + (-1)^{i_3}|1\rangle]_{A_3} \\ &\quad \otimes \cdots \otimes [|0\rangle + (-1)^{i_n}|1\rangle]_{A_n} \\ &\quad \otimes (|0\rangle^{\otimes n}_{A_1'A_2',\ldots,A_n'} + |1\rangle^{\otimes n}_{A_1'A_2',\ldots,A_n'}) \end{aligned} \tag{17}$$

Here, the player A_j is in possession of particles A_jA_j' $(j = 2, 3, \ldots, n)$, while the particle A_1' belongs to the player A_1.

Players implement the measurement.

The player A_j $(j = 2, 3, \ldots, n)$ performs Bell-basis measurement on two particles in his hand. To make the player A_1 know the state obtained with certainty, other players need to announce their measurement outcomes. For convenience, the Bell-basis measurement outcomes is denoted as $M_1^{A_j}M_2^{A_j}$ $(j = 2, 3, \ldots, n)$. As a result, the particle A_1' collapses into the following states.

$$\begin{aligned}&\frac{1}{(\sqrt{2})^{2n-1}}\left[\prod_{j=2}^{n}(-1)^{(M_2^{A_j})(M_1^{A_j})}(-1)^{\oplus\sum_{j=2}^{n} i_j(M_2^{A_j})}|0\rangle_{A_1'}\right. \\ &\quad \left. + \prod_{j=2}^{n}(-1)^{[(M_2^{A_j}\oplus 1)(M_1^{A_j})]}(-1)^{\oplus\sum_{j=2}^{n} i_j[(M_2^{A_j})\oplus 1]}|1\rangle_{A_1'}\right]\end{aligned} \tag{18}$$

Here, the symbol $\prod$ is multiplication.

In order to save the cost of classical information in the public communication network and improve the security of the quantum summation protocol, we code $n-1$ Bell-basis measurement outcomes $M_1^{A_j}M_2^{A_j}$ $(j = 2, 3, \ldots, n)$ into one cbit $X = \oplus\sum_{j=2}^{n} M_1^{A_j}$, and then broadcast it to the player A_1 via the public channel.

(S4) The player A_1 obtains the summation of secret messages.

Depending on the cbit X, the player A_1 first performs a unitary operation $U(X)$ in (8) on the particle A_1'. Then, he measures the particle A_1' in the basis $\{|+\rangle, |-\rangle\}$ and obtains the summation $\oplus\sum_{j=2}^{n} i_j$. Finally, the player A_1 adds his secret i_1 to the above summation and obtains the final result.

For example, suppose that the player A_j has the secret $i_j \in I_j$ $(j = 1, 2, 3, \ldots, n)$. The Bell-basis measurement outcomes $M_1^{A_2}M_2^{A_2} = 10$ and $M_1^{A_j}M_2^{A_j} = 00$ $(j = 3, 4, \ldots, n)$.

Then, the state of the particle A_1' is

$$\frac{1}{(\sqrt{2})^{2n-1}}[|0\rangle_{A_1'} + (-1)(-1)^{\oplus\sum_{j=2}^{n} i_j}|1\rangle_{A_1'}] \tag{19}$$

After the player A_1 performs the operation $U(X) = U(\oplus\sum_{j=2}^{n} M_1^{A_j}) = U(1)$, the above state is transformed into

$$\frac{1}{(\sqrt{2})^{2n-1}}[|0\rangle_{A_1'} + (-1)^{\oplus\sum_{j=2}^{n} i_j}|1\rangle_{A_1'}] \tag{20}$$

The player A_1 measures the particle A_1' in the basis $\{|+\rangle, |-\rangle\}$ and gets the summation $\oplus\sum_{j=2}^{n} i_j$. Then, he adds his secret i_1 to the summation and obtains the final result, i.e. the value $\oplus\sum_{j=1}^{n} i_j$.

The security of the present multi-party quantum summation protocol is the same as the two-party quantum summation protocol. The collusive attack performed by at most $n-2$ players is invalid for this protocol.

4 Conclusions

In summary, secure multi-party quantum summation protocol is often of paramount importance, and in some situations it is an essential condition. Multi-particle entangled state plays an important role in the general quantum network communication and quantum distributed computation. However, there are few protocols for quantum summation protocol with the entangled states. Thus, it is interest to further research the quantum summation protocol with the multi-particle entangled state. The central theme of this paper is to propose a new and efficient protocol for the secure multi-party quantum summation. We first investigate the two-party quantum summation protocol with the help of a semi-honest third party. Then, the protocol is generalized into multi-party quantum summation protocol without the help of the TP.

This protocol has the following features. (i) Compared to the previous protocols [10, 11], the similarity is our two-party quantum summation protocol also includes a TP. However, the difference is that the TP in our protocol is assumed semi-honest. Thus, many additional technologies of cryptography are not necessary. (ii) Our quantum summation protocol does not repeatedly transmit the particles carried the secret messages. In our protocol, the outside attacks including intercept-resend attack, the measurement-resend attack, entanglement-measure attack, DOS attack, delay-photon Trojan horse attack and the IPE Trojan horse attack, the PNS attack, etc., are invalid. Generally, a participant has more advantages in an attack than an outside eavesdropper, because he can know and utilize partial information legally. As far as the participant attack is concerned, we consider two cases. One is that one of two players attempts to eavesdrop the other's secret. The other is that the semi-honest TP attempts to steal the players' secrets. It is demonstrated that the participant attacks are also invalid for our protocol. (iii) Up to now, many experiments for preparation of the multi-particle entangled state have been reported [12]. Moreover, the utilization of the multi-particle entangled state may has some different features in the process of the quantum information. It is important and interest to study the multi-party quantum summation protocol. So, we generalize the two-party protocol to multi-party quantum summation without the help of the TP. (iv) The cost of the classical information in the communication network has been considered by more and more researchers in the field of the quantum information. This quantum summation protocol codes all players' Bell-basis measurement outcomes into one cbit. Thus, not only the classical information exchange over public communication network is decreased, but also the protocol's security is improved.

This protocol has some useful applications. The direct application of the two-party quantum summation protocol is to efficiently solve the socialist millionaires' problem [27] in which two millionaires want to know whether they happen to be equally rich. From our quantum summation protocol, it can be seen that if $i_1 = i_2 = 0$ or $i_1 = i_2 = 1$, TP will obtain the result 0. If $i_1 \neq i_2$, TP will obtain the result 1. TP may public only one cbit to make the two players know whether their secrets are equal or not. Additionally, our two-party quantum summation protocol is useful for one-way oblivious identification, which would allow the first user to identify herself in front of a second user, by means of a password, known only to both. It can be prescribed a function $f\ (i, j) = 0$ if $i = j$, and $f\ (i, j) = 1$ otherwise. In other words, $f\ (i, j)$ gives a yes or no answer to the question whether the two persons have the same password. Furthermore, our multi-party quantum summation protocol has a wide application in efficiently solving many problems, such as converging the split information at one point, and so on.

Acknowledgements Project supported by the National Basic Research Program of China (973 Program) (No. 2007CB311203), the National Natural Science Foundation of China and the Research Grants Council of Hong Kong Joint Research Scheme (No. 60731160626), the National Natural Science Foundation of China (Nos. 60821001, 60873191, 61003287) and the Fundamental Research Funds for the Central Universities (No. BUPT2009RC0220).

References

1. Lo, H.K.: Phys. Rev. A **56**, 1154 (1997)
2. Crepeau, C., Gottesman, D., Smith, A.: Secure Multi-Party Quantum Computation. ACM, New York (2002)
3. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: (FOCS 2006). Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (2006)
4. Chau, H.F.: Phys. Rev. A **61**, 032308 (2000)
5. Smith, A.: arXiv:quant-ph/0111030 (2001)
6. Heinrich, S.: J. Complex. **18**, 1 (2002)
7. Heinrich, S., Novak, E.: J. Complex. **19**, 1 (2003)
8. Heinrich, S., Kwas, M., Wozniakowski, H.: arXiv:quant-ph/0311036 (2003)
9. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Acta Phys. Sin. **56**, 6214 (2007)
10. Yang, Y.G., Wen, Q.Y.: J. Phys. A, Math. Theor. **42**, 055305 (2009)
11. Hillery, M., Ziman, M., Buzek, V., Bielikova, M.: Phys. Lett. A **349**, 75 (2006)
12. Lu, C.Y., Zhou, X.Q., Guhne, O., Gao, W.B., Zhang, J., Yuan, Z.S., Goebel, A., Yang, T., Pan, J.W.: Nat. Phys. **3**, 91 (2007)
13. Lo, H.K.: Phys. Rev. A **62**, 012313 (2000)
14. Chen, X.B., Wen, Q.Y., Guo, F.Z., Sun, Y., Xu, G., Zhu, F.C.: Int. J. Quant. Inform. **6**, 899 (2008)
15. Gao, T., Yan, F.L., Wang, Z.X.: J. Phys. A, Math. Gen. **38**, 5761 (2005)
16. Gao, T.: Z. Naturforschung A, J. Phys. Sci. **59**, 597 (2004)
17. Buhrman, H., Cleve, R., van Dam, W.: arXiv:quant-ph/9705033 (1997)
18. Xia, Y., Song, J., Song, H.S.: J. Phys. B **40**, 3719 (2007)
19. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, p. 175. IEEE, New York/Bangalore (1984)
20. Shor, P.W., Preskill, J.: Phys. Rev. Lett. **85**, 441 (2000)
21. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: Opt. Commun. **281**, 6130 (2008)

22. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)
23. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Phys. Rev. A **54**, 3824 (1996)
24. Briegel, H.J., Dur, W., Cirac, J.I., Zoller, P.: Phys. Rev. Lett. **81**, 5932 (1998)
25. Dur, W., Briegel, H.J., Cirac, J.I., Zoller, P.: Phys. Rev. A **59**, 169 (1999)
26. Xia, Y., Song, H.S.: Phys. Lett. A **364**, 117 (2007)
27. Boudot, F., Schoenmakers, B., Traore, J.: Discrete Appl. Math. **111**, 23 (2001)