International Journal of Theoretical Physics (2019) 58:2872–2882
https://doi.org/10.1007/s10773-019-04170-z

Multiparty Quantum Computation for Summation and Multiplication with Mutually Unbiased Bases

Shu-Xin Lv[1,2] · Xian-Fang Jiao[1,2] · Ping Zhou[1,2,3]

Received: 7 January 2019 / Accepted: 27 May 2019 / Published online: 20 June 2019

Abstract
We present an efficient protocol to securely compute the summation and multiplication of the multiparty secure numbers via quantum states in MUBs. In our protocols, we assume the third party Alice is semi-honest which means Alice might want to steal the secret messages of the participants but cannot be corrupted by the participants. The agents use decoy photons which are randomly in one of $2d^m$ nonorthogonal multiparticle states to prevent the eavesdropper and potential dishonest agents from freely eavesdropping on the secure information. The scheme requires the agents of computation to transmit fewer particles for multiparty summation and multiplication, which makes the scheme more convenient to use than others. Moreover, it has the advantage of having high information capacity per photon for summation and multiplication in multiparty quantum computation.

Keywords Secure quantum summation · Secure quanum multiplication · Mutually unbiased bases

1 Introduction

The application of quantum state as an information carrier in quantum communication enables some novel ways to transmit messages securely, such as quantum key distribution[1–12], quantum secret sharing [13–18], quantum secure direct communication [19–27], deterministic secure quantum communication [28–31], quantum entanglement concentration [32, 33], quantum state transfer [34, 35], quantum Zeno effect [36], blind quantum computation [37], quantum machine learning [38, 39] and secure multiparty quantum computation [40–43].

✉ Ping Zhou
zhouping@gxun.edu.cn

1 College of Science, Guangxi University for Nationalities, Nanning, 530006, People's Republic of China

2 Key Lab of Quantum Information and Quantum Optics, Guangxi University for Nationalities, Nanning, 530006, People's Republic of China

3 Guangxi Key Laboratory of Hybrid Computational and IC Design Analysis, Nanning, 530006, People's Republic of China

In secret sharing, the secret message M is split into two parts $M = M_1 \oplus M_2$[13, 14]. The agents can reconstruct the secret message if and only if all the agents cooperate. Quantum secret sharing (QSS) has provided a secure way to share the secret message and it has progressed quickly since the original quantum secret sharing scheme was first proposed in 1999 by Hillery, Bužek and Berthiaume using three-particle entangled states[13]. Various protocols for QSS have been proposed via different quantum entangled states [44–46]. In 2003, Guo et al. presented a scheme for QSS without quantum entanglement and the efficiency of QSS has been improved to 100% [44]. Now, theoretical and experimental protocols for QSS have been studied by many groups [44–49].

Another important branch in cryptography is secure multiparty computation (SMC). Secure multiparty summation and secure multiparty multiplication play important roles in SMC. Similar to QSS, researchers have devoted much time to quantum secure multiparty summation and multiplication based on quantum entanglement, or quantum secure multiparty summation protocols based on single-particle states. For example, in 2006, Hillery et al. presented a protocol for multiparty quantum summation with two-particle high-dimensional entangled states [50]. Du et al. proposed a scheme for a quantum secure addition module $n + 1 (n \geq 2)$ based on non-orthogonal single-particle states [51]. Zhang et al. proposed a protocol for quantum multiparty secure summation based on single photons in both polarization and spatial-mode degrees of freedom [52]. In 2010, Chen et al. described a method for quantum summation between multiparties by using multiparticle entangled states as the information carrier [53]. Zhang proposed a protocol for three-party secure quantum summation with a six-qubit entangled state [54]. In 2016, Shi et al. presented a scheme for multiparty quantum summation with a 2m-qubit entangled state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i x_1 j}{N}} |jj\rangle$ [55]. Moreover, they proposed a scheme for multiparty quantum multiplication with the 2m-qubit entangled state. In 2017, Liu et al. presented a protocol for multiparty quantum secure summation with a two-particle Bell state [56]. Yang and Ye presented a protocol for multiparty quantum summation based on quantum Fourier transform [57]. Recently, the experimental realization of secure quantum summation via five-qubit IBM quantum computers on a cloud has been reported [58].

Mutually unbiased bases (MUBs), have attached much interest since the concept was first introduced by Ivanovic [59]. Wootters and Fields studied optimal state determination with the measurements in mutually unbiased bases [60]. Yuan et al. showed that measurements in MUB can be practically realized in the cavity quantum electrodynamics (QED) systems by performing corresponding unitary transmissions [61]. The security of a quantum key distribution with an MUB of d-dimensional system was discussed by Cerf et al. in 2002 [63]. Experimental realization of higher-dimensional quantum key distribution based on MUB via photons carrying orbital angular momentum was studied in [62], which demonstrated that the information capacity and key generation rate of quantum key distribution based on MUB increases with the dimension of the quantum system. MUBs in arbitrary bipartite spaces $C^d \otimes C^d$ are investigated via an unextendible maximally entangled basis [64].

In quantum secure communication, it's long been understood that the agents can utilize single-particle states in mutually unbiased bases (MUBs) or quantum entangled states to guarantee the security of communication. But there is still no general method to perform multiparty secure summation and multiplication via single-particle states in MUBs [53–56]. In this work, we will present a protocol for multiparty secure quantum summation and multiplication via two MUBs of a high-dimensional quantum system. In our protocols, we assume the third party Alice is semi-honest which means Alice might want to steal the secret messages of the participants but cannot be corrupted by the participants. The agent

uses decoy photons randomly chosen from d^{2m} nonorthogonal states to prevent eavesdropping and dishonest agents freely stealing the secret messages. Quantum entanglement is not necessary in our protocol for multiparty summation and multiplication, which makes this protocol more convenient to use than others. Moreover, the protocol has the advantage of having high efficiency since the information capacity and key generation rate per photon of quantum secure summation and multiplication increase with the dimensionality of the quantum system.

2 Secure Multiparty Quantum Summation Based on Mutually Unbiased Bases of D-Dimensional Quantum System

To present the principle of our scheme clearly, we first discuss a secure multiparty quantum summation based on the MUB of d-dimensional quantum system, then propose the protocol for secure multiparty quantum multiplication via d-dimension MUB.

Similar to Ref. [62], two orthonormal bases of N-dimensional quantum system $\{|\psi^{j_1}\rangle, j_1 = 0, \cdots, N-1\}$, $\{|\varphi^{j_2}\rangle, j_2 = 0, \cdots, N-1\}$ are said to be MUBs if and only if they satisfy:

$$|\langle\psi^{j_1}|\varphi^{j_2}\rangle| = \frac{1}{\sqrt{N}}. \tag{1}$$

The two MUBs of N-dimensional quantum system can be written as [63]:

$$\begin{aligned} |\psi^{l_1}\rangle &= |l_1\rangle \\ |\varphi^{l_2}\rangle &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i}{N} j l_2} |j\rangle \end{aligned} \tag{2}$$

where $l_1, l_2 = 0, 1, \cdots, N-1$. Similar to Ref. [65], the states $|\psi^{l_1}\rangle$, $|\varphi^{l_2}\rangle$ in the two MUBs can be written as a tensor product of m qudits ($N = d^m$).

$$\begin{aligned} |\psi^{l_1}\rangle &= |l_{1,m-1}\rangle \otimes |l_{1,m-2}\rangle \otimes \cdots \otimes |l_{1,0}\rangle \\ |\varphi^{l_2}\rangle &= \left(\frac{1}{\sqrt{d}} \sum_{j_{m-1}=0}^{d-1} e^{\frac{2\pi i}{N} d^{m-1} j_{m-1} l_2} |j_{m-1}\rangle \right) \\ &\quad \otimes \left(\frac{1}{\sqrt{d}} \sum_{j_{m-2}=0}^{d-1} e^{\frac{2\pi i}{N} d^{m-2} j_{m-2} l_2} |j_{m-2}\rangle \right) \\ &\quad \otimes \cdots \otimes \left(\frac{1}{\sqrt{d}} \sum_{j_0=0}^{d-1} e^{\frac{2\pi i}{N} j_0 l_2} |j_0\rangle \right), \end{aligned} \tag{3}$$

where

$$\begin{aligned} l_1 &= l_{1,m-1} d^{m-1} + l_{1,m-2} d^{m-2} + \cdots + l_{1,0} \\ j &= j_{m-1} d^{m-1} + j_{m-2} d^{m-2} + \cdots + j_0. \end{aligned} \tag{4}$$

Here $l_{1,m-1}, \cdots, l_{1,0}, j_{m-1}, \cdots, j_0 = 0, \cdots, d-1$.

The unitary operation

$$U_x^1 = \sum_{l=0}^{N-1} e^{\frac{2\pi i}{N} xl} |l \oplus x\rangle\langle l| \tag{5}$$

flips the m-qudit states into two mutually unbiased bases:

$$\begin{aligned} U_x^1 |\psi^l\rangle &= |\psi^{l\oplus x}\rangle \\ U_x^1 |\varphi^l\rangle &= |\varphi^{l\oplus x}\rangle. \end{aligned} \tag{6}$$

Suppose there are n participants $Alice_1$, $Alice_2$,$\cdots$, $Alice_n$. Each participant $Alice_i$(i = 1,2,$\cdots$,n) has a string of secret numbers $\mathbf{X}_i$.

$$\mathbf{X}_i = (x_{i1}, \cdots, x_{ip}), \tag{7}$$

where $x_{ij} \in$\{0,1,$\cdots$, $N-1$\}, $N = d^m$ and j = 1, 2,$\cdots$,p. Similar to Ref. [55], all the participants want Alice to calculate the summation $\sum_{i=1}^{n} \mathbf{X}_i mod N$ without revealing the secret number $\mathbf{X}_i$.

$$\sum_{i=1}^{n} \mathbf{X}_i mod N = \left(\sum_{i=1}^{n} x_{i1} mod N, \cdots, \sum_{i=1}^{n} x_{ip} mod N \right). \tag{8}$$

Similar to Ref. [52], the initiator Alice prepares a sequence of ordered p m-qudit states S which are randomly in one of two MUBs $\{|\psi^{l_j}\rangle, l_j = 0, 1, \cdots, N-1\}$, $\{|\varphi^{l_j}\rangle, l_j = 0, 1, \cdots, N-1\}$ (j = 1,2,$\cdots$,p). To prevent potential eavesdroppers and dishonest agents from stealing the secret information freely, Alice prepares the decoy photons which are randomly in one of two MUBs $\{|\psi^l\rangle, l = 0, 1, \cdots, N-1\}$, $\{|\varphi^l\rangle, l = 0, 1, \cdots, N-1\}$ and inserts them randomly into the sequence to form a new sequence S^1[52]. Since the position of decoy photons are unknown by the potential eavesdropper and dishonest agent, their eavesdropping will disturb the state of decoy photons and be detected by Alice in the secure check process. Alice sends the sequence S^1 to $Alice_1$.

After confirming that $Alice_1$ has received all the m-qudit states sent by Alice, Alice publishes the positions of the decoy photons. Similar to Refs. [52, 66], $Alice_1$ first measures the decoys randomly in one of two MUBs, then publishes the information about this measurement, including the measurement basis and the measurement results. Alice can determine the error rate by comparing $\text{Alice}_1's$ measurement results with the initial states of decoy photons. If the error rate exceeds the threshold, Alice aborts the secret communication. Otherwise, the protocol continues.

$Alice_1$ removes the decoy photons and applies unitary operation $U_{x_{1j}}^1$ (j = 1,2,$\cdots$,p) on the jth m-qudit state in the ordered m-qudit sequence S according to his secret message $\mathbf{X}_1$. Similar to Ref. [55], unitary operation $U_{x_{1j}}^1$ transforms the jth m-qudit state $|\psi^{l_j}\rangle$, $|\varphi^{l_j}\rangle$ in the ordered sequence S to the corresponding state $|\psi^{l_j \oplus x_{1j}}\rangle$, $|\varphi^{l_j \oplus x_{1j}}\rangle$. After performing the unitary operations, $Alice_1$ prepares the decoy photons in a way similar to Alice and then randomly inserts them into sequence S to form a new sequence S^2. $Alice_1$ sends the sequence S^2 to the next agent $Alice_2$. $Alice_2$ performs the process similar to $Alice_1$, then sends the particles to the next agent, and so on. After the last agent $Alice_n$applies the unitary operation $U_{x_{nj}}^1$ on the jth m-qudit state according to his secret message $\mathbf{X}_n$, the jth m-qudit state in the ordered m-qudit sequence S transforms to the corresponding state $|\psi^{l_j \oplus x_{1j} \oplus \cdots \oplus x_{nj}}\rangle$, $|\varphi^{l_j \oplus x_{1j} \oplus \cdots \oplus x_{nj}}\rangle$. Since the unitary operations $U_{x_{ij}}^1$ (i = 1,2,$\cdots$,n and j = 1,2,$\cdots$,p) do not change the measurement basis [67], Alice can deterministic get the value $l \oplus x_1 \oplus \cdots \oplus x_n$ by performing projective measurement on the each m-qudit state returned with the same MUB as he prepares it.

To perform the multiparty secure quantum summation protocol securely, $Alice_n$ prepares decoy photons in a similar way to the previous agents and then inserts the decoy photons into the ordered sequence to form the new m-qudit sequence named S^{n+1}. $Alice_n$ sends S^{n+1} back to Alice. After confirming that Alice has received all the m-qudit states sent from $Alice_n$, $Alice_n$ announces the positions of the decoy photons. Alice measures the decoy photons randomly in one of the two MUBs and publishes the information of this measurement, including measurement bases and measurement results. $Alice_n$ analyzes the error rate. If the error rate exceeds the threshold, they abort the communication.

After the security check, Alice can deterministically obtain the value of $l_{1j} \oplus x_{1j} \oplus \cdots \oplus x_{nj} (j = 1,2,\cdots,p)$ by performing a projective measurement on each m-qudit state returned with the same MUB as it is prepared. According to his knowledge of l_j, Alice can compute the summation $\sum_{i=1}^{n} x_{ij} mod N$.

$$\sum_{i=1}^{n} x_{ij} mod N = l_j \oplus x_{1j} \oplus x_{2j} \oplus \cdots \oplus x_{nj} \oplus (N - l_j), \tag{9}$$

where $j = 1,2,\cdots,p$.

3 Multiparty Secure Quantum Multiplication Based on MUBs

Similar to the case for multiparty secure quantum summation, suppose there are n participants $Alice_1, Alice_2, \cdots, Alice_n$, each participant $Alice_i$ $(i = 1,2,\cdots,n)$ has a string of secret numbers $\mathbf{X}_i = (x_{i1}, x_{i2}, \cdots, x_{ip})$, where $x_{ij} \in \{1, 2, \cdots, N-1\}$, $N = d^m$ and $j = 1, 2, \cdots, p$. All the participants want to Alice compute the multiplication $\prod_{i=1}^{n} \mathbf{X}_i mod N$ without revealing their secret numbers.

$$\prod_{i=1}^{n} \mathbf{X}_i mod N = \left(\prod_{i=1}^{n} x_{i1} mod N, \cdots, \prod_{i=1}^{n} x_{ip} mod N \right). \tag{10}$$

The arbitrary dimension of quantum system d can be factorized and expressed as:

$$d = q_1^{k^1} q_2^{k^2} \cdots q_r^{k^r}, \tag{11}$$

where $q_1, \cdots, q_r$ are prime numbers, $k^1, \cdots, k^r$ are r integers. Similar to Ref. [55], each secret number $x_{ij} (i = 1, \cdots, n; j = 1, \cdots, p)$ can be expressed as:

$$x_{ij} = s_{ij} q_1^{k_{ij}^1} q_2^{k_{ij}^2} \cdots q_r^{k_{ij}^r}. \tag{12}$$

Here, s_{ij} is coprime with d^m since s_{ij} is coprime with d. Similar to multiparty secure quantum multiplication with entangled states, the multiplication of n secret numbers $\prod_{i=1}^{n} x_{ij} mod N$ can be written as:

$$\prod_{i=1}^{n} x_{ij} mod N = \left(q_1^{\sum_{i=1}^{n} k_{ij}^1} \cdots q_r^{\sum_{i=1}^{n} k_{ij}^r} \prod_{i=1}^{n} s_{ij} \right) mod N \tag{13}$$

If we get the results of $\sum_{i=1}^{n} k_{ij}^1 mod N, \cdots, \sum_{i=1}^{n} k_{ij}^r \ mod N$ and $\prod_{i=1}^{n} s_{ij} \ mod N$, we can easily compute $\prod_{i=1}^{n} x_{ij} mod N$. Therefore, the computation of $\prod_{i=1}^{n} x_{ij} \ mod N$ can be translated into the computations of $\sum_{i=1}^{n} k_{ij}^1 mod N, \cdots, \sum_{i=1}^{n} k_{ij}^r \ mod N$ and $\prod_{i=1}^{n} s_{ij} \ mod N$. The method of computing $\sum_{i=1}^{n} k_{ij}^1 mod N, \cdots, \sum_{i=1}^{n} k_{ij}^r \ mod N$ has been proposed previously.

Below, we only discuss the method of computing $\prod_{j=1}^{n} s_j \ modN$ via two MUBs of based on high-dimensional quantum systems.

Similar to the case for multiparty secure quantum summation, The initiator Alice prepares a sequence of ordered p m-qudit states R randomly in one of two nonorthogonal states $|\psi^{l_j}\rangle$, $|\varphi^{l_j}\rangle$ ($j = 1,2,\cdots,p$) and l_j is coprime with N. To prevent the potentially dishonest agents from stealing the secret information freely, Alice prepares decoy photons in one of two MUBs $\{|\psi^l\rangle, l = 0, 1,\cdots, N-1\}$, $\{|\varphi^l\rangle, l = 0, 1,\cdots, N-1\}$ and inserts them randomly into the m-qudit sequence to form the new sequence R^1. Alice sends R^1 to $Alice_1$.

After confirming that $Alice_1$ has received all the particles sent by Alice, Alice announces the positions of the decoy photons. To check the security of the communication $Alice_1$ measures the decoy photons randomly in one of two MUBs and publishes the measurement results. Alice compares the measurement results with the initial states of decoy photons. If the error rate exceeds the threshold, they abort the communication. Otherwise, the protocol continues.

$Alice_1$ removes decoy photons and applies unitary operation $U^2_{s_{1j}}$ according to his private secret number s_{1j}($j = 1,2,\cdots,p$) on the jth m-qudit state of the ordered sequence R.

$$U^2_{s_{1j}} = \sum_{l=0}^{N-1} |ls_{1j}^{-1} modN\rangle\langle l|. \tag{14}$$

Similar to Ref. [55], since s_{1j} is coprime with N and therefore its modulo-N multiplication inverse s_{ij}^{-1} exists. The unitary operation flips the m-qudit states in the two MUBs and transforms the jth m-qudit state in the ordered sequence to the corresponding state

$$\begin{aligned} U^2_{s_{1j}}|\psi^{l_j}\rangle &= |\psi^{l_j s_{1j}^{-1} modN}\rangle \\ U^2_{s_{1j}}|\varphi^{l_j}\rangle &= |\varphi^{l_j s_{1j} modN}\rangle. \end{aligned} \tag{15}$$

To prevent the eavesdropper from stealing the secret information freely, $Alice_1$ prepares decoy photons in one of two MUBs by a method similar to Alice and inserts the decoy photons randomly into the ordered sequence R to form the new sequence R^2. $Alice_1$ sends the sequence R^2 to the next agent $Alice_2$. Similar to the case for multiparty secure summation, $Alice_2$ performs the process similar to $Alice_1$, then sends the particles to the next agent, and so on. The jth m-qudit state in the ordered m-qudit sequence R transform to the corresponding state $|\psi^{l_j s_{1j}^{-1}\cdots s_{nj}^{-1} modN}\rangle$, $|\varphi^{l_j s_{1j}\cdots s_{nj} modN}\rangle$ after the last agent $Alice_n$ applies unitary operation $U^2_{s_{nj}}$ on the jth m-qudit state according to his secret message $\mathbf{X}_n$.

Since the unitary operations $U^2_{s_{ij}}$ ($i = 1,2,\cdots,n$ and $j = 1,2,\cdots,p$) do not change the measurement basis, Alice can deterministically get the value $l_j s_{1j}^{-1}\cdots s_{nj}^{-1} modN$ or $l_j s_{1j}\cdots s_{nj} modN$ by performing projective measurement on each m-qudit state returned with the same MUB that they prepared.

To perform the multiparty quantum multiplication protocol securely, $Alice_n$ prepares the decoys photons in the same way as the previously agents and then inserts the decoy photons randomly into the ordered sequence R^n to form the new m-qudit sequence R^{n+1}.The last agent $Alice_n$ sends the new sequence R^{n+1} back to Alice. After conforming that Alice has received all the m-qudit states sent from $Alice_n$, $Alice_n$ announces the positions of the decoy photons. Similar to the case for multiparty secure quantum summation, Alice measures the decoy photons randomly in one of two MUBs and publishes the information of this measurement. $Alice_n$ analyzes the error rate. If the error rate exceeds the threshold, they abort the communication.

After the security check, Alice can deterministically obtain the value of $l_j s_{1j}^{-1} \cdots s_{nj}^{-1} mod N (j = 1,2,\cdots ,p)$ or $l_j s_{1j} s_{2j} \cdots s_{nj} mod N$ by performing projective measurement on each m-qudit state returned with the same MUB that they prepared. According to his information on l_j, Alice can compute the multiplication $\prod_{i=1}^{n} s_{ij} mod N$

$$\begin{aligned} \prod_{i=1}^{n} s_{ij} mod N &= l_j \varpi_1^{-1} mod N, \\ \prod_{i=1}^{n} s_{ij} mod N &= l_j^{-1} \varpi_2 mod N \end{aligned} \tag{16}$$

where

$$\begin{aligned} \varpi_1 &= l_j s_{1j}^{-1} \cdots s_{nj}^{-1} mod N, \\ \varpi_2 &= l_j s_{1j} \cdots s_{nj} mod N \end{aligned} \tag{17}$$

and $j = 1,2,\cdots ,p$.

It is interesting to notice that the agents can prepare an N-dimensional ($N = d^m$) single-qudit state for multiparty secure summation and multiplication. This method has the advantage of transmitting fewer particles for multiparty secure summation and multiplication via the arbitrary number N at the expense of preparing and manipulating a quantum system with a higher dimension.

4 Security Analysis

In this section, we will analyze the security of our protocols for multiparty quantum summation and multiplication via MUBs. In contrast to quantum key distribution, in the multiparty quantum summation protocol, the attacks from the outside and the attacks from the all the participants should be considered in security analysis. Not only do eavesdroppers from outside want to steal the participants' secret information but also some dishonest agents may try to steal other agents' private secret information. The security task in a quantum summation protocol is to prevent the eavesdropper and dishonest agents from freely eavesdropping on the participants' private secret inputs. To save the space, we only analyze the security of multiparty quantum summation protocol, since the security of multiparty quantum multiplication protocol is the same as that of multiparty quantum summation protocol.

In our protocol, the agents use decoy photon technique to prevent the eavesdropper from eavesdropping freely on the secret information. The principle of the decoy technique according to Li et al. is that the sender prepares some photons which are randomly in one of N^2 nonorthogonal states $\{|\psi^l\rangle, l = 0, 1,\cdots, N-1\}$, $\{|\varphi^l\rangle, l = 0, 1,\cdots, N-1\}$, and then inserts them into the photon sequences [66]. As the states and the positions of decoy photons are unknown for the outside eavesdropper, the eavesdropper will inevitably disturb the state of decoy photons and will be caught during the detection procedure. Thus, the outside eavesdropper's different kinds of attacks, such as intercept-resend attack, measurement-resend attack and the denial-of-service attack, will be detected during the check procedure. Let us take the intercept-resend attack as an example. Suppose the state of decoy photon is $|0\rangle$, the eavesdropper measures the photon randomly in one of two MUBs since he does not know the initial state of the decoy photon. After the measurement, he prepares and sends the fake single photon according to his measurement result. Therefore, the probability of his

eavesdropping being detected during the check procedure is $\frac{N-1}{2N}$. The probability of the eavesdropper being detected will be $1-\left(\frac{N+1}{2N}\right)^k$ when the sender uses k decoy photons for checking the eavesdropping. The eavesdropper will be detected in a secure check procedure and our protocol is secure against outside attack.

We now discuss the participant attacks in our protocol for multiparty quantum secure summation, which are more complicated in secure analysis than outside attacks. As we know, there are two sorts of participant attacks: individual attack and collusion attack. We first analyze the security of our protocol against an individual attack, then analyze the security of the protocol against a collusion attack. Suppose one of the participants wants to steal the other participant's secret information. Without loss of generality, suppose $Alice_1$ wants to steal $Alice_j$'s ($j = 2,3,\cdots, n$) secret key X_j, then $Alice_1$ has to intercept the sequence S^j sent from $Alice_j$, and measures the photons sequence. $Alice_1$'s eavesdropping will disturb the state of the decoy photons in the sequence S^j since $Alice_1$ does not know the states and the positions of the decoy photons. Therefore, the eavesdropping will be detected during the security check procedure. Our protocol is secure against an individual attack. However, if the agents $Alice_{l-1}$ and $Alice_{l+1}$ are dishonest agents, they can collude to get $Alice_l$'s secret information. To resist the collusion of fewer than n-1 agents, we can use a random order communication model instead of the fixed order communication, as suggested by Shi et al. [55]. That is, the method to choose the next agent is randomly determined by $Alice_l$, and not predetermined by other agents. Similar to Refs. [54, 55], since any eavesdropping done by an eavesdropper or dishonest agent will inevitably disturb the state of decoy photon and will be detected in security check process [66], the agents can exploit the decoy-photon technique and the random order communication model to prevent outside and participant attacks.

5 Discussion and Summary

If we set p = 1 for all the agents, the vectors X_i is composed of single numbers. All agents can jointly compute the summation of n single numbers $\sum_{i=1}^{n} X_i mod N$ and the multiplication of n single numbers $\prod_{i=1}^{n} X_i mod N$ without revealing their secret information. Moreover, if we set m = 1, the m-qudit state is randomly in one of d^2 nonorthogonal states, which means the agents can calculate the multiparty quantum summation and multiplication with an arbitrary general number d. Similar to Ref. [55], our protocols have the advantage of performing multiparty summation and multiplication in the N-dimension ($N = d^m$) space by using qudits as the quantum information carriers. The agents can obtain the desired results with the general number d without revealing their respective secret information. From the perspective of entropy, the summation of n single numbers $\sum_{i=1}^{n} X_i mod N$ ($N = d^m$) and the multiplication of n single numbers $\prod_{i=1}^{n} X_i mod N$ with qudits contain more information than the summation of n single numbers $\sum_{i=1}^{n} X_i mod N$ ($N = 2^m$) and the multiplication of n single numbers $\prod_{i=1}^{n} X_i mod N$ with qubits.

In Ref. [55], the agents can exploit the nonlocal correlation of 2m-particle quantum entangled state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |jj\rangle$ to avoid the requirement of the application of decoy photons technique to prevent eavesdropper or dishonest agent from freely eavesdropping on the secure information. However, when the agents perform the multiparty secure quantum computation via m-particle state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$, the approach in Ref. [55] does not work. To compute multiparty quantum summation $\sum_{i=1}^{n} X_i mod N$ with the general number

N, the protocol for multiparty quantum summation based on the qubit system has to transmit $\log_2^N$ qubits to accomplish the computation. However, in the protocol for multiparty quantum summation based on qudit system, the agents only need to transmit the single qudit. Similar to Refs. [54, 62]. the protocols for multiparty quantum summation and multiplication with the high-dimensional quantum system have the advantage of having high information capacity and communication efficiency.

In summary, we have presented a protocol for multiparty secure quantum summation based on a high-dimensional quantum system. The agents utilize the decoy photons, which are randomly in one of two MUBs, to prevent the dishonest agents or the eavesdropper form eavesdropping freely on the secure information. The protocol is more convenient to use since it not require a 2m-particle entangled state for multiparty secure summation. We also discuss the protocol for multiparty secure quantum multiplication based on high-dimensional quantum system which is rarely considered in previous papers. Compared with previous protocols, our protocols for multiparty secure quantum summation and multiplication based on high-dimensional quantum system have the advantage of having high quantum communication efficiency.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grant Nos. 61501129 and 11564004, Natural Science Foundation of Guangxi under Grant Nos. 2014GXNSFAA118008, Special Funds of Guangxi Distinguished Experts Construction Engineering and Xiangsihu Young Scholars and Innovative Research Team of GXUN.

References

1. Bennett, C.H., Brassad, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. IEEE, New York. pp. 175. IEEE Press, New York (1984)
2. Ekert, A.K.: Quantum cryptography based on Bells theorem. Phys. Rev. Lett. **67**, 661 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bells theorem. Phys. Rev. Lett. **68**, 557 (1992)
4. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
5. Pinheiro, P., Ramos, R.: Two-layer quantum key distribution. Quantum Inf. Process. **14**, 2111 (2015)
6. Zhang, C.M., Li, M., Yin, Z.Q., Li, H.W., Chen, W., Han, Z.F.: Decoy-state measurement-device-independent quantum key distribution with mismatched-basis statistics. Sci. China-Phys. Mech. Astron. **58**, 590301 (2015)
7. Bai, Z.L., Wang, X.Y., Yang, S.S., Li, Y.H.: High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution. Sci. China-Phys. Mech. Astron. **59**, 614201 (2016)
8. Cao, D.Y., Liu, B.H., Wang, Z., Huang, Y.F., Li, C.F., Guo, G.C.: Multiuser-to-multiuser entanglement distribution based on 1550 nm polarization-entangled photons. Sci. Bull. **60**, 1128 (2015)
9. Liu, X.M., Zhang, L.J., Wang, Y.G., Chen, W., Huang, D.J., Li, D., Wang, S., He, D.Y., Yin, Z.Q., Zhou, Y., Hui, C., Han, Z.F.: FPGA based digital phase-coding quantum key distribution system. Sci. China-Phys. Mech. Astron. **58**, 120301 (2015)
10. Huang, W., Su, Q., Xu, B.J., Liu, B., Fan, F., Jia, H.Y., Yang, Y.H.: Improved multiparty quantum key agreement in travelling mode. Sci. China-Phys. Mech. Astron. **59**, 120311 (2016)
11. Leverrier, A.: Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys. Rev. Lett. **118**, 200501 (2017)
12. Park, B.K., Lee, M.S., Woo, M.K., Kim, Y.S., Han, S.W., Moon, S.: QKD system with fast active optical path length compensation. Sci. China-Phys. Mech. Astron. **60**, 060311 (2017)
13. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
14. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
15. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 052307 (2004)

16. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
17. Karimipour, V., Asoudeh, M.: Quantum secret sharing and random hopping: using single states instead of entanglement. Phys. Rev. A **92**, 030301 (2015)
18. Lin, S., Guo, G.D., Xu, Y.Z., Sun, Y., Liu, X.F.: Cryptanalysis of quantum secret sharing with d-level single particles. Phys. Rev. A **93**, 062343 (2016)
19. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
20. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
21. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
22. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
23. Hu, J.Y., Yu, B., Jing, M.Y., Xiao, L.T., Jia, S.T., Qin, G.Q., Long, G.L.: Experimental quantum secure direct communication with single photons. Light: Sci. Appl. **5**, e16144 (2005)
24. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L., Shi, B.S., Guo, G.C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**, 220501 (2017)
25. Wu, F.Z., Yang, G.J., Wang, H.B., Xiong, J., Alzahrani, F., Hobiny, A., Deng, F.G.: High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states. Sci. China-Phys. Mech. Astron. **60**, 120313 (2017)
26. Chen, S.S., Zhou, L., Zhong, W., Sheng, Y.B.: Three-step three-party quantum secure direct communication. Sci. China-Phys. Mech. Astron. **61**, 090312 (2018)
27. Qi, R.Y., Sun, Z., Lin, Z.S., Niu, P.H., Hao, W.T., Song, L.Y., Huang, Q., Gao, J.C., Yin, L.G., Long, G.L.: Implementation and security analysis of practical quantum secure direct communication. Light Sci. Appl. **8**, 22 (2019)
28. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Acta Phys. Pol. A **101**, 357 (2002)
29. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**, 054302 (2006)
30. Li, N., Li, J., Li, L.L., Wang, Z., Wang, T.: Deterministic secure quantum communication and authentication protocol based on extended GHZ-w state and quantum one-time pad. Int. J. Theor. Phys. **55**, 3579 (2016)
31. Jiang, D., Chen, Y.Y., Gu, X.M., Xie, L., Chen, L.J.: Deterministic secure quantum communication using a single d-level system. Sci. Rep. **7**, 44934 (2017)
32. Ren, B.C., Long, G.L.: General hyperentanglement concentration for photon systems assisted by quantum-dot spins inside optical microcavities. Opt. Express **22**, 6547 (2014)
33. Cao, C., Chen, X., Duan, Y.W., Fan, L., Zhang, R., Wang, T.J., Wang, C.: Concentrating partially entangled W-class states on nonlocal atoms using low-Q optical cavity and linear optical elements. Sci. China-Phys. Mech. Astron. **59**, 100315 (2016)
34. Sillanpää, M.A., Park, J.I., Simmonds, R.W.: Coherent quantum state storage and transfer between two phase qubits via a resonant cavity. Nature **449**, 438 (2007)
35. Tao, M.J., Hua, M., Ai, Q., Deng, F.G.: Quantum-information processing on nitrogen-vacancy ensembles with the local resonance assisted by circuit QED. Phys. Rev. A **91**, 062325 (2015)
36. Qiu, J., Wang, Y.Y., Yin, Z.Q., Zhang, M., Ai, Q., Deng, F.G.: Quantum Zeno and Zeno-like effects in nitrogen vacancy centers. Sci. Rep. **5**, 17615 (2015)
37. Sheng, Y.B., Zhou, L.: Blind quantum computation with a noise channel. Phys. Rev. A **98**, 052343 (2018)
38. Rebentrost, P., Mohseni, M., Lloyd, S.: Quantum support vector machine for big data classification. Phys. Rev. Lett. **113**, 130503 (2014)
39. Sheng, Y.B., Zhou, L.: Distributed secure quantum machine learning. Sci. Bull. **62**, 1025 (2017)
40. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1554 (1997)
41. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, p 643. ACM (2002)
42. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 47th Annual IEEE Symposium on Foundations of Computer Science, FOCS'06, p. 249. IEEE (2006)
43. Loukopoulos, K., Browne, D.E.: Secure multiparty computation with a dishonest majority via quantum means. Phys. Rev. A **81**, 062336 (2010)
44. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247 (2003)

45. Wang, X.J., An, L.X., Yu, X.T., Zhang, Z.C.: Multilayer quantum secret sharing based on GHZ state and generalized Bell basis measurement in multiparty agents. Phys. Lett. A **381**, 3282 (2017)
46. Kogias, I., Xiang, Y., He, Q.Y., Adesso, G.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A **95**, 012315 (2017)
47. Chen, Y.A., Zhang, A.N., Zhao, Z., Zhou, X.Q., Lu, C.Y., Peng, C.Z., Yang, T., Pan, J.W.: Experimental quantum secret sharing and third-man quantum cryptography. Phys. Rev. Lett. **95**, 200502 (2005)
48. Gaertner, S., Kurtsiefer, C., Bourennane, M., Weinfurter, H.: Experimental demonstration of four-party quantum secret sharing. Phys. Rev. Lett. **98**, 020503 (2007)
49. Bell, B.A., Markham, D., Herrera-Martí, D.A., Marin, A., Wadsworth, W.J., Rarity, J.G., Tame, M.S.: Experimental demonstration of graph-state quantum secret sharing. Nat. Commun. **5**, 5480 (2014)
50. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**, 75 (2006)
51. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**, 6214 (2007)
52. Zhang, C., Sun, Z.W., Huang, Y., Long, D.Y.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**, 933 (2014)
53. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793 (2010)
54. Zhang, C., Sun, Z.W., Huang, X., Long, D.Y.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inform. **13**, 1550011 (2015)
55. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
56. Liu, W., Wang, Y.B., Fan, W.Q.: An novel protocol for the quantum secure multi-party summation based on two-particle Bell states. Int. J. Theor. Phys. **56**, 2783 (2017)
57. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**, 129 (2018)
58. Majumder, A., Mohapatra, S., Kumar, A.: Experimental realization of secure multiparty quantum summation using five-qubit IBM quantum computer on cloud. arXiv:1707.07460 (2017)
59. Ivonovic, I.D.: Geometrical description of quantal state determination. J. Phys. A **14**, 3241 (1981)
60. Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**, 363 (1989)
61. Yuan, H., Zhou, Z.W., Guo, G.C.: Quantum state tomography via mutually unbiased measurements in driven cavity QED systems. New J. Phys. **18**, 043013 (2016)
62. Mafu, M., Dudley, A., Goyal, S., Giovannini, D., McLaren, M., Padgett, M.J., Konrad, T., Petruccione, F., Lütkenhaus, N., Forbes, A.: Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. Phys. Rev. A **88**, 032305 (2013)
63. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using d-level systems. Phys. Rev. Lett. **88**, 127902 (2002)
64. Chen, B., Fei, S.M.: Unextendible maximally entangled bases and mutually unbiased bases. Phys. Rev. A **88**, 034301 (2013)
65. Stroud, A.M.C.: Unextendible maximally entangled bases and mutually unbiased bases. J. Mod. Optic **49**, 2115 (2002)
66. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin. Phys. Lett. **22**, 1049 (2005)
67. Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. J. Phys. A **39**, 14089 (2006)