

---

# Secure multi-party quantum summation based on quantum Fourier transform

Hui-Yi Yang, Tian-Yu Ye\*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R.China

\*E-mail: [happyty@aliyun.com](mailto:happyty@aliyun.com)

**Abstract:** In this paper, we propose a novel secure multi-party quantum summation protocol based on quantum Fourier transform, where the traveling particles are transmitted in a tree-type mode. The party who prepares the initial quantum states is assumed to be semi-honest, which means that she may misbehave on her own but will not conspire with anyone. The proposed protocol can resist both the outside attacks and the participant attacks. Especially, one party cannot obtain other parties' private integer strings; and it is secure for the colluding attack performed by at most  $n-2$  parties, where  $n$  is the number of parties. In addition, the proposed protocol calculates the addition of modulo  $d$  and implements the calculation of addition in a secret-by-secret way rather than a bit-by-bit way.

**Keywords:** Secure multi-party quantum summation; quantum Fourier transform; participant attack; addition of modulo  $d$ ; secret-by-secret way

## 1 Introduction

Quantum cryptography, which can be regarded as the combination of quantum mechanics and classical cryptography, has attracted a lot of attention since it was derived by Bennett and Brassard [1] in 1984, as it can attain unconditional security in theory through the physical principles of quantum mechanics. During the past three decades, quantum cryptography was widely investigated so that numerous branches have been established, such as quantum key distribution (QKD) [1-5], quantum secure direct communication (QSDC) [6-8], quantum secret sharing (QSS) [9-11], quantum key agreement (QKA) [12-40], quantum private query (QPQ) [41-45] *etc.*

Secure multi-party computation, first introduced by Yao [46] and extended by Goldreich *et al.* [47], is a significant subfield of classical cryptography. Naturally, whether the physical principle of quantum mechanics can be applied into secure multi-party computation is an important and interesting question. To date, many researchers have investigated secure multi-party computation within quantum settings [48-51]. Lo [48] thought that the equality function cannot be securely evaluated in a two-party scenario. Thus, some additional assumptions, such as a third party (TP), should be considered. Ben-Or *et al.* [49] studied the question that in order for distributed quantum computations to be possible, how many players must keep honest. Chau [50] put forward a scheme to improve the speed of classical multi-party computation with quantum techniques. Smith [51] pointed out that any multi-party quantum computation can be secure as long as the number of dishonest players is less than  $n/6$ .

Secure multi-party summation, which can be used to construct complex secure protocols for other multi-party computation, is a fundamental problem of secure multi-party computation. It can be formulated as follows [52]:  $n$  players,  $P_1, P_2, \dots, P_n$ , want to evaluate a summation function  $f(x_1, x_2, \dots, x_n)$ , where  $x_i$  is the secret value from  $P_i$ . The result of this function can be revealed publicly or privately to some particular player. The task of secure multi-party summation is to preserve the privacy of the players' inputs and guarantee the correctness of computation. In 2002, Heinrich [53] investigated quantum summation with an application to integration. In 2003, Heinrich [54] studied quantum Boolean summation with repetitions in the worst-average setting. In 2006, Hillery [55] put forward a multi-party quantum summation protocol by using two-particle  $N$ -level entangled states which accomplishes the summation of  $N$  players in voting procedure on the basis of ensuring the anonymity of players. In 2007, Du *et al.* [56] suggested a novel scheme of secure quantum addition modulo  $n+1$  ( $n \geq 2$ ) by using non-orthogonal states, which can add a number to an unknown number secretly. Here,  $n$  represents the number of parties carrying a secret. In 2010, Chen *et al.* [52] proposed a quantum addition modulo 2 protocol based on multi-particle GHZ entangled states. In 2014, Zhang *et al.* [57] constructed a high-capacity quantum addition modulo 2 protocol with single photons in both polarization and spatial-mode degrees of freedom. In 2015, Zhang *et al.* [58] suggested a three-party quantum addition modulo 2 protocol by using six-qubit genuinely maximally entangled states. In 2016, Shi *et al.* [59] thought that the protocols in Refs.[52,56] have two drawbacks: one the one hand, the modulo of these two protocols is too small, resulting in the limitation for more extensive applications; on the other hand, these two protocols do not possess an enough high computation efficiency because of their bit-by-bit computation. Then, they proposed a quantum addition modulo  $N$  protocol through quantum Fourier transform, controlled-not operation, oracle operation and inverse quantum Fourier transform, which implements the calculation of summation in a secret-by-secret way rather than a bit-by-bit way. Here,  $N=2^m$  and  $m$  is the number of qubits represented by one basis state. In this protocol, the calculations of

secure multi-party summation are securely transferred into the calculations of the corresponding phase information by quantum Fourier transform. And later, the phase information is extracted after an inverse quantum Fourier transform. In 2017, Shi and Zhang [60] presented a common quantum solution to a class of special two-party private summation problems. In the same year, Zhang *et al.* [61] put forward a multi-party quantum addition modulo 2 protocol without a trusted TP based on single particles.

Based on the above analysis, in this paper, we propose a novel secure multi-party quantum summation protocol based on quantum Fourier transform. The party who prepares the initial quantum states is assumed to be semi-honest, which means that she may misbehave on her own but will not conspire with anyone. The proposed protocol can resist both the outside attacks and the participant attacks. Especially, one party cannot obtain other parties' private integer strings; and it is secure for the colluding attack performed by at most  $n-2$  parties. In addition, the proposed protocol calculates the addition of modulo  $d$ , and implements the calculation of addition in a secret-by-secret way rather than a bit-by-bit way.

The rest of this paper is organized as follows. In Sect.2, we introduce the preliminary knowledge used in this paper. In Sect.3, we describe and analyze the proposed secure multi-party quantum summation protocol. Finally, discussion and conclusion are given in Sect.4.

## 2 Preliminary knowledge

Before depicting the proposed protocol, it is necessary for us to introduce the preliminary knowledge first.

### 2.1 Quantum Fourier transform and its application

Let us define the  $d$ -level  $n$ -particle entangled state as follows:

$$|\omega\rangle_{12\dots n} = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1 |r\rangle_2 \dots |r\rangle_n, \quad (1)$$

where each  $|r\rangle$  is a  $d$ -level basis state,  $r \in \{0, 1, \dots, d-1\}$  and  $d \geq 2$ . For each  $d$ -level basis state  $|r\rangle$ , the  $d$ th order discrete quantum Fourier transform is defined to be

$$F|r\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \zeta^{lr} |l\rangle, \quad (2)$$

where  $\zeta = e^{2\pi i/d}$ . The two sets,  $V_1 = \{|r\rangle\}_{r=0}^{d-1}$  and  $V_2 = \{F|r\rangle\}_{r=0}^{d-1}$ , are two common conjugate bases.

Further, we define a transformation operation  $U_k$  as follows:

$$U_k = \sum_{u=0}^{d-1} |u \oplus k\rangle \langle u|, \quad (3)$$

where  $k$  runs from 0 to  $d-1$ . Throughout this paper,  $\oplus$  represents the addition modulo  $d$ . Apparently, after the operation  $U_k$  is performed on the  $d$ -level basis state  $|r\rangle$ , we can obtain

$$U_k|r\rangle = |r \oplus k\rangle. \quad (4)$$

After performing the operation  $(U_{k_1} F) \otimes (U_{k_2} F) \otimes \dots \otimes (U_{k_n} F)$  ( $k_1, k_2, \dots, k_n \in \{0, 1, \dots, d-1\}$ ) on the state  $|\omega\rangle_{12\dots n}$ , we can get

$$\begin{aligned} & (U_{k_1} F) \otimes (U_{k_2} F) \otimes \dots \otimes (U_{k_n} F) |\omega\rangle_{12\dots n} \\ &= \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} (U_{k_1} F) |r\rangle_1 \otimes (U_{k_2} F) |r\rangle_2 \otimes \dots \otimes (U_{k_n} F) |r\rangle_n \\ &= \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \left( U_{k_1} \frac{1}{\sqrt{d}} \sum_{l_1=0}^{d-1} \zeta^{l_1 r} |l_1\rangle \right) \otimes \left( U_{k_2} \frac{1}{\sqrt{d}} \sum_{l_2=0}^{d-1} \zeta^{l_2 r} |l_2\rangle \right) \otimes \dots \otimes \left( U_{k_n} \frac{1}{\sqrt{d}} \sum_{l_n=0}^{d-1} \zeta^{l_n r} |l_n\rangle \right) \\ &= d^{-\frac{n+1}{2}} \sum_{l_1, l_2, \dots, l_n} \left( \sum_{r=0}^{d-1} \zeta^{r(l_1 + l_2 + \dots + l_n)} \right) |l_1 \oplus k_1\rangle \otimes |l_2 \oplus k_2\rangle \otimes \dots \otimes |l_n \oplus k_n\rangle \\ &= d^{-\frac{n-1}{2}} \sum_{l_1 + l_2 + \dots + l_n \equiv 0 \pmod{d}} |l_1 \oplus k_1\rangle \otimes |l_2 \oplus k_2\rangle \otimes \dots \otimes |l_n \oplus k_n\rangle. \end{aligned} \quad (5)$$

If we perform quantum measurements with the  $V_1$  basis on the right of Eq.(5), we will get the results of  $l_i \oplus k_i$  ( $i=1, 2, \dots, n$ ). According to Eq.(5), it is apparent that

$$\begin{aligned} & (l_1 \oplus k_1) \oplus (l_2 \oplus k_2) \oplus \dots \oplus (l_n \oplus k_n) \\ &= (l_1 + k_1 + l_2 + k_2 + \dots + l_n + k_n) \bmod d \\ &= [(l_1 + l_2 + \dots + l_n) \bmod d + (k_1 + k_2 + \dots + k_n) \bmod d] \bmod d \\ &= (k_1 + k_2 + \dots + k_n) \bmod d \\ &= k_1 \oplus k_2 \oplus \dots \oplus k_n. \end{aligned} \quad (6)$$

## 2.2 Particle transmission mode of secure multi-party quantum computation

In secure multi-party quantum computation protocols (such as multi-party QKA), there are three kinds of particle transmission mode [32], i.e., the complete-graph-type, the circle-type and the tree-type (shown in Fig.1). In the complete-graph-type particle transmission mode, every party prepares the initial quantum states and sends each of the other parties a sequence of prepared particles; in the circle-type particle transmission mode, every party prepares the initial quantum states and only sends out one sequence of prepared particles which will be operated by each of the other parties in turn and finally sent back to the one who prepared it; and in the tree-type particle transmission mode, only one party prepares the initial quantum states and sends each of the other parties a sequence of prepared particles which may or may not be sent back after operation.

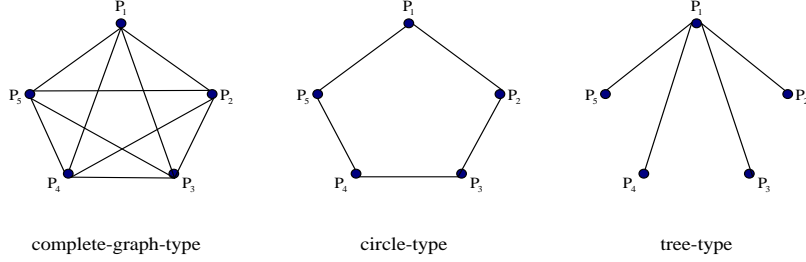


Fig.1 Three types of particle transmission mode in secure multi-party quantum computation protocols (taking five parties for example) [32]. Here, the vertices denote the parties while the edges denote the particle transmissions between two parties.

## 3 The proposed secure multi-party quantum summation protocol and its analysis

### 3.1 Protocol description

Secure multi-party quantum summation should meet the following requirements [52]:

- ① Correctness. The computation result of summation of players' inputs is correct.
- ② Security. An outside eavesdropper cannot obtain any useful information about each player's input without being detected.
- ③ Privacy. Each player cannot learn any useful information more than her prescribed out, i.e., each player's input can be kept secret.

However, the computation result of summation can be published.

Suppose that there are  $n$  ( $n > 2$ ) parties,  $P_1, P_2, \dots, P_n$ , where  $P_i$  ( $i = 1, 2, \dots, n$ ) has a private integer string  $K_i$  of length  $N$ . That is,

$$\begin{aligned} K_1 &= (k_1^1, k_1^2, \dots, k_1^N) \\ K_2 &= (k_2^1, k_2^2, \dots, k_2^N), \\ &\vdots \\ K_n &= (k_n^1, k_n^2, \dots, k_n^N) \end{aligned} \quad (7)$$

where  $k_t^i, k_2^i, \dots, k_n^i \in \{0, 1, \dots, d-1\}$  for  $t = 1, 2, \dots, N$ .  $P_1, P_2, \dots, P_n$  want to jointly derive the summation of their private integer strings shown in Eq.(8) without revealing the genuine contents of their private integer strings.

$$K = K_1 \oplus K_2 \oplus \dots \oplus K_n = (k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1, k_1^2 \oplus k_2^2 \oplus \dots \oplus k_n^2, \dots, k_1^N \oplus k_2^N \oplus \dots \oplus k_n^N). \quad (8)$$

The detailed procedures of the proposed secure multi-party quantum summation protocol can be illustrated as follows. Without loss of generality, we suppose that  $P_1$  is the party who prepares the initial quantum states. Moreover,  $P_1$  is assumed to be semi-honest, which means that she may misbehave on her own but will not conspire with anyone. Here, only ideal channel (without noise) is considered.

**Step 1:**  $P_1$  prepares  $N$   $d$ -level  $n$ -particle entangled states all in the state  $|\omega\rangle_{12\dots n}$ , and arranges them into an ordered sequence

$$\left[ \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^1 |r\rangle_2^1 \dots |r\rangle_n^1, \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^2 |r\rangle_2^2 \dots |r\rangle_n^2, \dots, \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^N |r\rangle_2^N \dots |r\rangle_n^N \right], \quad (9)$$

where the superscripts  $1, 2, \dots, N$  denote the order of  $d$ -level  $n$ -particle entangled states in the sequence. Afterward,  $P_1$  takes the  $i^{\text{th}}$  ( $i = 1, 2, \dots, n$ ) particle out from each state to construct  $n$  particle sequences which are labeled as:

$$\begin{aligned}
S_1 &= (p_1^1, p_1^2, \dots, p_1^N) \\
S_2 &= (p_2^1, p_2^2, \dots, p_2^N) \\
&\vdots \\
S_i &= (p_i^1, p_i^2, \dots, p_i^N) \\
&\vdots \\
S_n &= (p_n^1, p_n^2, \dots, p_n^N)
\end{aligned} \tag{10}$$

where  $p_i^t$  represents the  $i^{\text{th}}$  particle of the  $t^{\text{th}}$  entangled state and  $t=1,2,\dots,N$ . For detecting eavesdropping,  $P_1$  prepares  $n-1$  groups of decoy photons, each of which is randomly chosen from the set  $V_1$  or  $V_2$ . Then,  $P_1$  randomly picks out one group of decoy photons and randomly inserts the chosen decoy photons into particle sequence  $S_j$  to form a new sequence  $S_j'$ . Here,  $j=2,3,\dots,n$ . Finally,  $P_1$  keeps  $S_1$  in her hand and sends  $S_j'$  to  $P_j$ .

**Step 2:** After confirming that  $P_j$  ( $j=2,3,\dots,n$ ) has received all the particles in sequence  $S_j'$ ,  $P_1$  checks the transmission security of sequence  $S_j'$  together with  $P_j$ . Concretely,  $P_1$  tells  $P_j$  the positions and the measurement basis of decoy photons in sequence  $S_j'$ . In the following,  $P_j$  uses the correct basis to measure the corresponding decoy photons and tells  $P_1$  half of the measurement results. Afterward,  $P_1$  announces the initial states of the remaining half of decoy photons. Finally, they check whether the measurement results of decoy photons are consistent with their initial states. In this way,  $P_1$  and  $P_j$  can check the transmission security of sequence  $S_j'$ . If the error rate is greater than a predetermined threshold, they will terminate the protocol; otherwise, they will proceed to the next step.

**Step 3:**  $P_j$  ( $j=2,3,\dots,n$ ) discards the decoy photons in sequence  $S_j'$  and obtains sequence  $S_j$ . Then,  $P_j$  encodes her private integer string  $K_j$  on the particles in sequence  $S_j$ . Concretely,  $P_j$  performs  $U_{k_j} F$  on particle  $p_j^t$ , where  $t=1,2,\dots,N$ . The new sequence of  $S_j$  after encoded is denoted as  $ES_j$ .

In the same time,  $P_1$  also encodes her private integer string  $K_1$  on the particles in sequence  $S_1$  by performing  $U_{k_1} F$  on particle  $p_1^t$ . The new sequence of  $S_1$  after encoded is denoted as  $ES_1$ .

**Step 4:** After all parties have finishing encoding of their private integer strings, each of them measures all particles in their respective hand with the basis  $V_1$  and obtains the corresponding measurement results. As a result, it can be derived that

$$\begin{aligned}
M_1 &= (m_1^1, m_1^2, \dots, m_1^N) \\
M_2 &= (m_2^1, m_2^2, \dots, m_2^N) \\
&\vdots \\
M_i &= (m_i^1, m_i^2, \dots, m_i^N) \\
&\vdots \\
M_n &= (m_n^1, m_n^2, \dots, m_n^N)
\end{aligned} \tag{11}$$

where  $m_i^t$  is the measurement result of particle  $p_i^t$  after encoded,  $i=1,2,\dots,n$  and  $t=1,2,\dots,N$ . According to Eq.(5), it can be obtained that  $m_i^t = l_i^t \oplus k_i^t$  and  $l_1^t + l_2^t + \dots + l_n^t \equiv 0 \pmod{d}$ . Then,  $P_j$  ( $j=2,3,\dots,n$ ) announces  $M_j$  to  $P_1$ . Finally, according to Eq.(6),  $P_1$  obtains the summation of all parties' private integer strings by computing

$$\begin{aligned}
M_1 \oplus M_2 \oplus \dots \oplus M_n &= (m_1^1 \oplus m_2^1 \oplus \dots \oplus m_n^1, m_1^2 \oplus m_2^2 \oplus \dots \oplus m_n^2, \dots, m_1^N \oplus m_2^N \oplus \dots \oplus m_n^N) \\
&= (k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1, k_1^2 \oplus k_2^2 \oplus \dots \oplus k_n^2, \dots, k_1^N \oplus k_2^N \oplus \dots \oplus k_n^N) \\
&= K_1 \oplus K_2 \oplus \dots \oplus K_n = K.
\end{aligned} \tag{12}$$

In order to let the other parties know the result of summation,  $P_1$  announces it publicly.

It concludes the description of the proposed secure multi-party quantum summation protocol. It is apparent that in the above protocol, only  $P_1$  prepares the initial quantum states and sends each of the other parties a sequence of prepared particles. Thus, the above protocol adopts the tree-type particle transmission mode.

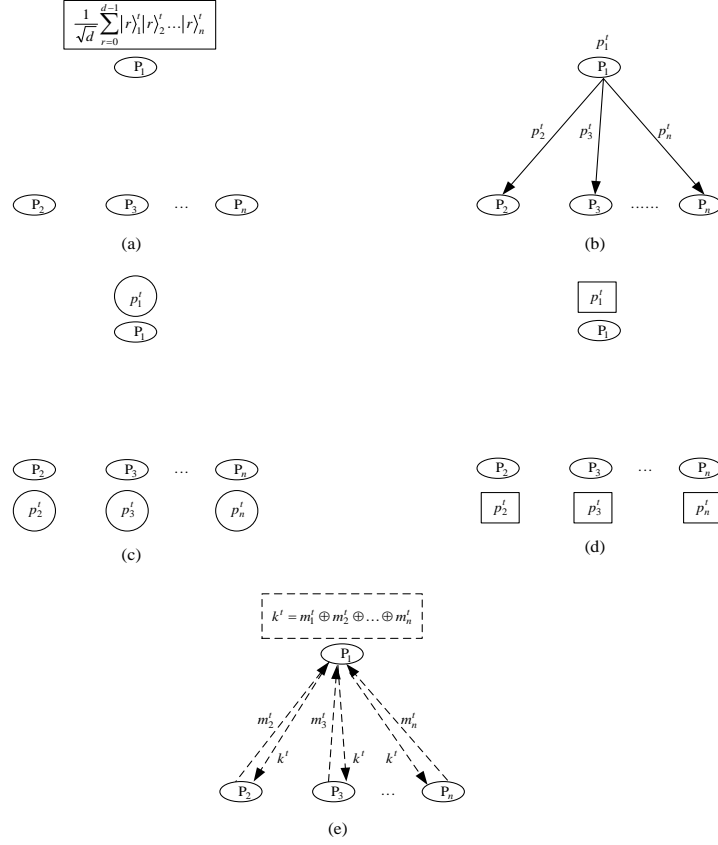


Fig.2 The flow chart of the proposed secure multi-party quantum summation protocol

(taking  $\frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^Y |r\rangle_2^Y \dots |r\rangle_n^Y$  for example)

(a)  $P_1$  prepares quantum state  $\frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^Y |r\rangle_2^Y \dots |r\rangle_n^Y$  as the quantum carrier. Here, the rectangle with solid lines denotes the quantum state preparation operation; (b)  $P_1$  transmits particle  $p'_j$  ( $j=2,3,\dots,n$ ) to  $P_j$ , and keeps particle  $p'_1$  intact. Here, the solid line with an arrow denotes the quantum state transmission operation; (c)  $P_i$  ( $i=1,2,\dots,n$ ) encodes particle  $p'_i$  by performing  $U_{k_i} F$  on it. Here, the solid circle denotes the encoding operation. (d)  $P_i$  ( $i=1,2,\dots,n$ ) measures particle  $p'_i$  after encoded with the basis  $V_1$ . Here, the square denotes the quantum state measurement operation. (e)  $P_j$  ( $j=2,3,\dots,n$ ) sends  $m'_j$  to  $P_1$ . Then,  $P_1$  computes  $k'$  and sends it to  $P_j$ . Here, the dotted line with an arrow and the rectangle with dotted lines denote the classical information transmission operation and the classical computation operation, respectively.

### 3.2 Analysis

#### A. Output correctness

In this subsection, we verify that the output of the above protocol is correct. There are  $n$  parties named  $P_1, P_2, \dots, P_n$ , where  $P_i$  ( $i=1,2,\dots,n$ ) has a private integer string  $K_i$  of length  $N$ . Without loss of generality, after ignoring the eavesdropping check processes, we take the first integer of each private integer string (i.e.,  $k_i^1$ ,  $i=1,2,\dots,n$ ) for example, to illustrate the output correctness.

$P_1$  prepares one  $d$ -level  $n$ -particle entangled state in the state  $\frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1^1 |r\rangle_2^1 \dots |r\rangle_n^1$ . Then,  $P_1$  keeps particle  $p_1^1$  in her hand and sends particle  $p_j^1$  to  $P_j$ . Here,  $j=2,3,\dots,n$ . After receiving particle  $p_j^1$ ,  $P_j$  performs  $U_{k_j^1} F$  on particle  $p_j^1$  to encode the private integer  $k_j^1$ . In the same time,  $P_1$  also encodes her private integer  $k_1^1$  by performing  $U_{k_1^1} F$  on particle  $p_1^1$ . Then,  $P_j$  measures particle  $p_j^1$  after encoded with the basis  $V_1$  and tells  $P_1$  the measurement result  $m_j^1$ .  $P_1$  also uses the basis  $V_1$  to measure  $p_1^1$  after encoded and obtains the measurement result  $m_1^1$ . Here,  $m_i^1 = l_i^1 \oplus k_i^1$  and  $i=1,2,\dots,n$ . Finally, according to Eq.(6),  $P_1$  obtains  $k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1$  by computing  $m_1^1 \oplus m_2^1 \oplus \dots \oplus m_n^1$ . Concretely,

$$m_1^1 \oplus m_2^1 \oplus \dots \oplus m_n^1 = (l_1^1 \oplus k_1^1) \oplus (l_2^1 \oplus k_2^1) \oplus \dots \oplus (l_n^1 \oplus k_n^1)$$

$$\begin{aligned}
&= (l_1^1 + k_1^1 + l_2^1 + k_2^1 + \dots + l_n^1 + k_n^1) \bmod d \\
&= \left[ (l_1^1 + l_2^1 + \dots + l_n^1) \bmod d + (k_1^1 + k_2^1 + \dots + k_n^1) \bmod d \right] \bmod d \\
&= (k_1^1 + k_2^1 + \dots + k_n^1) \bmod d \\
&= k_1^1 \oplus k_2^1 \oplus \dots \oplus k_n^1 = k^1.
\end{aligned} \tag{13}$$

It can be concluded now that the output of the above protocol is correct.

## B. Security

In this subsection, we verify that both the outside attack and the participant attack are ineffective for the above protocol.

### (i) Outside attack

We analyze the possibility for an outside eavesdropper to steal the private integer strings from all parties here.

In the above protocol, in order to get something useful about the private integer strings, an outside eavesdropper may utilize the particle transmission that  $P_1$  sends  $S_j'$  ( $j = 2, 3, \dots, n$ ) to  $P_j$  in Step 1 to launch active attacks, such as the intercept-resend attack, the measure-resend attack and the entangle-measure attack and so on. However, the above protocol employs the decoy photons, which are randomly chosen from the two conjugate bases,  $V_1$  and  $V_2$ , to detect the presence of an outside eavesdropper. Note that the decoy photon technique [62,63] can be thought as a variant of the BB84 eavesdropping check method [1] which has been proven to be unconditionally secure [64]. Moreover, the effectiveness of decoy photon technology in 2-level quantum system against an outside eavesdropper's attacks has also been validated in Refs.[65,66]. It is straightforward that the decoy photon technology is also effective against an outside eavesdropper's attacks in  $d$ -level quantum system. Therefore, if an outside eavesdropper launches active attacks during the particle transmissions, due to having no knowledge about the positions and the measurement basis of decoy photons before the announcement on them, she will inevitably leave her trace on decoy photons and be detected by the eavesdropping check process.

On the other hand, in Step 4, an outside eavesdropper may hear of  $M_j$  when  $P_j$  ( $j = 2, 3, \dots, n$ ) announces it to  $P_1$  and the result of summation when  $P_1$  publishes it. However, she still cannot decrypt out  $k_j^t$  ( $t = 1, 2, \dots, N$ ) from  $m_j^t$ , because she does not know the value of  $l_j^t$ . In addition, an outside eavesdropper can deduce  $M_1$  from  $M_2, M_3, \dots, M_n$  and the result of summation. However, due to lack of the knowledge of the value of  $l_1^t$ , she cannot know  $k_1^t$  either.

### (ii) Participant attack

In 2007, Gao *et al.* [67] first pointed out that the participant attack, i.e., the attack from one or more dishonest parties, is generally more powerful and should be paid more attention to. To date, the participant attack has attracted much attention in the cryptanalysis of quantum cryptography [68-70]. To see this in a sufficient way, we consider two cases of participant attack. Firstly, we discuss the participant attack from one single dishonest party; and then, we analyze the colluding attack from two or more dishonest parties.

#### a) The participant attack from one single dishonest party

In the above protocol, the roles of different  $P_j$ s ( $j = 2, 3, \dots, n$ ) are the same, but are different from  $P_1$  who prepares the initial quantum states and distributes the prepared particle sequences. Thus, there are two kinds of the participant attack from one single dishonest party, i.e., the participant attack from a single dishonest  $P_j$  and the participant attack from semi-honest  $P_1$ .

With respect to the participant attack from a single dishonest  $P_j$ , if  $P_j$  launches attacks on the particles in  $S_j'$  from  $P_1$  to  $P_j$  ( $j' = 2, 3, \dots, n$  and  $j' \neq j$ ) in Step 1, due to having no knowledge about the positions and the measurement basis of the inserted decoy photons in  $S_j'$ , she will inevitably be caught as an outside eavesdropper. In addition,  $P_j$  may hear of  $M_j$  when  $P_j$  announces it to  $P_1$  in Step 4. However, due to having no access to the value of  $l_j^t$  ( $t = 1, 2, \dots, N$ ), she still cannot decrypt out  $k_j^t$  from  $m_j^t$ . On the other hand,  $P_j$  can deduce  $M_1$  from  $M_2, M_3, \dots, M_n$  and the result of summation. However, due to lack of the knowledge of the value of  $l_1^t$ ,  $P_j$  cannot know  $k_1^t$  either.

With respect to the participant attack from semi-honest  $P_1$ , in order to obtain the private integer strings of the other parties,  $P_1$  can take the chance of preparing the initial quantum states to launch the following attack:

①  $P_1$  prepares  $N$   $d$ -level  $n$ -particle entangled states all in the state  $|\omega\rangle_{12\dots n}$ , and measures each of them with the basis  $V_1$ . The collapsed states after measurement are denoted as

$$\left[ \left( |r^1\rangle_1, |r^1\rangle_2, \dots, |r^1\rangle_n \right), \left( |r^2\rangle_1, |r^2\rangle_2, \dots, |r^2\rangle_n \right), \dots, \left( |r^N\rangle_1, |r^N\rangle_2, \dots, |r^N\rangle_n \right) \right], \quad (14)$$

where  $|r^t\rangle_i$  denotes the collapsed state of the  $i^{\text{th}}$  particle in the  $t^{\text{th}}$   $d$ -level  $n$ -particle entangled state after measurement. Here,  $t = 1, 2, \dots, N$  and  $i = 1, 2, \dots, n$ . Afterward,  $P_1$  constructs  $n$  particle sequences as follows:

$$\begin{aligned} S_1 &= \left( |r^1\rangle_1, |r^2\rangle_1, \dots, |r^N\rangle_1 \right) \\ S_2 &= \left( |r^1\rangle_2, |r^2\rangle_2, \dots, |r^N\rangle_2 \right) \\ &\vdots \\ S_i &= \left( |r^1\rangle_i, |r^2\rangle_i, \dots, |r^N\rangle_i \right) \\ &\vdots \\ S_n &= \left( |r^1\rangle_n, |r^2\rangle_n, \dots, |r^N\rangle_n \right) \end{aligned} \quad (15)$$

For detecting eavesdropping,  $P_1$  prepares  $n-1$  groups of decoy photons, each of which is randomly chosen from the set  $V_1$  or  $V_2$ , and randomly inserts one group of decoy photons into particle sequence  $S_j$  to form a new sequence  $S'_j$ . Here,  $j = 2, 3, \dots, n$ . Then,  $P_1$  keeps  $S_1$  in her hand and sends  $S'_j$  to  $P_j$ .

②  $P_1$  and  $P_j$  ( $j = 2, 3, \dots, n$ ) check the transmission security of sequence  $S'_j$  together as illustrated in Step 2. Apparently,  $P_j$  cannot discover the misbehavior of  $P_1$ . Therefore,  $P_j$  discards the decoy photons in sequence  $S'_j$  to restore sequence  $S_j$  and performs  $U_{k'_j} F$  on particle  $|r^t\rangle_j$ , where  $t = 1, 2, \dots, N$ . The corresponding encoded particle of  $|r^t\rangle_j$  is

$$\left( U_{k'_j} F \right) |r^t\rangle_j = U_{k'_j} \frac{1}{\sqrt{d}} \sum_{l'_j=0}^{d-1} \zeta^{l'_j t} |l'_j\rangle = \frac{1}{\sqrt{d}} \sum_{l'_j=0}^{d-1} \zeta^{l'_j t} |l'_j \oplus k'_j\rangle. \quad (16)$$

Afterward,  $P_j$  measures all particles in her hand with the basis  $V_1$  and publishes her measurement result

$$M_j = (m_j^1, m_j^2, \dots, m_j^N). \quad (17)$$

Here,  $m_j^t = l'_j \oplus k'_j$ . Then,  $P_j$  announces  $M_j$  to  $P_1$ . Finally,  $P_1$  tries to extract  $k'_j$  from  $m_j^t$ .

However, although  $P_1$  knows  $m_j^t$  from the announcement of  $P_j$ , she still cannot extract  $k'_j$ , as she has no knowledge about  $l'_j$ . It can be concluded that the participant attack from semi-honest  $P_1$  is ineffective.

#### b) The participant attack from two or more dishonest parties

Since  $P_1$  is not allowed to collude with other parties, if the other  $n-1$  parties collude together, they can easily deduce the private integer string of  $P_1$  from the result of summation. Therefore, the above protocol cannot resist the colluding attack from  $n-1$  parties.

Next, we will demonstrate that the above protocol can resist the colluding attack from  $n-2$  parties. Without loss of generality, assume that the dishonest  $P_2, \dots, P_{i-1}, P_{i+1}, \dots, P_n$  try to collude together to obtain the private integer strings of  $P_1$  and  $P_i$ . Firstly, if  $P_2, \dots, P_{i-1}, P_{i+1}, \dots, P_n$  try to launch attacks on the particles in  $S'_i$  from  $P_1$  to  $P_i$  in Step 1, due to having no knowledge about the positions and the measurement basis of the inserted decoy photons in  $S'_i$ , they will inevitably be caught as an outside eavesdropper. Secondly, in Step 4,  $P_s$  ( $s = 2, \dots, i-1, i+1, \dots, n$ ) can know  $M_s$ , and may hear of  $M_i$  when  $P_i$  announces it to  $P_1$  and the result of summation when  $P_1$  publishes it.  $P_s$  can deduce  $M_1$  from  $M_2, M_3, \dots, M_n$  and the result of summation. Moreover,  $P_s$  can deduce  $l'_s$  ( $t = 1, 2, \dots, N$ ) from  $k'_s$  and  $m_s^t$ . However, even though the  $n-2$  parties conclude together, they still cannot obtain the accurate values of  $l'_i$  and  $l'_1$ . Therefore,  $P_2, \dots, P_{i-1}, P_{i+1}, \dots, P_n$  cannot decrypt out  $k'_i$  and  $k'_1$  from  $m_i^t$  and  $m_1^t$ , respectively.

## 4 Discussion and conclusion

We compare the proposed protocol with previous quantum summation protocols with respect to type of addition and type of computation. The comparison result is summarized in Table 1. From Table 1, it can be concluded that the modulo of the proposed protocol can easily be bigger than those of Refs.[52,56-58,61], which may result in more extensive applications; and compared with the protocols of Refs.[52,56-58,60,61], the proposed protocol easily has higher computation efficiency because of its secret-by-secret computation.

Further, we give a more detailed comparison between the proposed protocol and the protocol of Ref.[59] by ignoring their security check processes, since both of them utilize quantum Fourier transform. The comparison result is summarized in Table 2.

Table 1 Comparison of previous quantum summation protocols and the proposed protocol

	The protocol of Ref.[52]	The protocol of Ref.[56]	The protocol of Ref.[57]	The protocol of Ref.[58]	The protocol of Ref.[59]	The protocol of Ref.[60]	The protocol of Ref.[61]	The proposed protocol
Type of addition	addition modulo 2	addition modulo $n+1$	addition modulo 2	addition modulo 2	addition modulo $N$	addition	addition modulo 2	addition modulo $d$
Type of computation	bit-by-bit	bit-by-bit	bit-by-bit	bit-by-bit	secret-by-secret	bit-by-bit	bit-by-bit	secret-by-secret

\*In Ref.[56],  $n$  represents the number of parties carrying a secret and  $n \geq 2$ ; and in Ref.[59],  $N=2^m$ , where  $m$  is the number of qubits represented by one basis state; and in the proposed protocol,  $d \geq 2$ .

Table 2 Comparison of quantum summation protocol in Ref.[59] and the proposed protocol

	Quantum resource	Quantum operation	Quantum measurement	Position for encoding a secret	Particle transmission mode	Type of addition	Type of computation
The protocol of Ref.[59]	basis state	quantum transform, controlled-not operation, oracle operation $C_j$ , inverse quantum Fourier transform	Fourier $V_i$ basis measurement	global phase	circle-type	addition modulo $N$	secret-by-secret
The proposed protocol	$d$ -level $n$ -particle entangled state	quantum Fourier transform, transformation operation $U_k$	$V_i$ basis measurement	basis state	tree-type	addition modulo $d$	secret-by-secret

In addition, in some circumstance, it is necessary to make all parties share the result of summation privately among them. In other words, anyone else except all parties is not allowed to know the result of summation. In order to achieve this goal, every party can launch the proposed protocol acting as  $P_i$  and does not announce the result of summation publicly.

To sum up, in this paper, a novel secure multi-party quantum summation protocol based on quantum Fourier transform is proposed, where the traveling particles are transmitted in a tree-type mode. We verify in detail that the proposed protocol can resist both the outside attacks and the participant attacks. Especially, one party cannot obtain other parties' private integer strings; and it is secure for the colluding attack performed by at most  $n-2$  parties. The proposed protocol calculates the addition of modulo  $d$  and implements the calculation of addition in a secret-by-secret way rather than a bit-by-bit way. In addition, the proposed protocol only considers ideal channel. When noise is concerned, additional operation such as quantum private amplification is needed.

## Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments that help enhancing the quality of this paper. Funding by the National Natural Science Foundation of China (Grant Nos.61402407 and 11375152) and the Natural Science Foundation of Zhejiang Province (Grant No.LY18F020007) is gratefully acknowledged.

## Compliance with ethical standards

Conflict of interest: The authors declare that they have no conflict of interest.

## Reference

- [1] Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore: IEEE Press, 1984, pp.175-179
- [2] Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67(6):661-663
- [3] Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68(21), 3121
- [4] Cabello, A.: Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85:5635
- [5] Shih, H.C., Lee, K.C., Hwang, T.: New efficient three-party quantum key distribution protocols. IEEE J Sel Top Quantum Electron, 2009,15(6), 1602-1606
- [6] Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002,65: 032302
- [7] 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, 2003, 68:042317
- [8] Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
- [9] Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys Rev A, 1999,59:1829-1834
- [10] Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59:162-168
- [11] Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004,69: 052307
- [12] Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron Lett, 2004, 40:1149
- [13] Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on quantum key agreement protocol with maximally entangled states. Int J Theor Phys, 2011, 50:1793-1802
- [14] Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt Commun, 2010, 283:1192-1195



- 
- [15] Liu, B., Gao, F., Huang, W., et al.: Multiparty quantum key agreement with single particles. *Quantum Inf Process*, 2013, 12(4):1797-1805
  - [16] Yin, X.R., Wen, W.P., Shen, D.S., et al.: Three-party quantum key agreement with Bell states. *Acta Phys Sin*, 2013, 62(17): 170304
  - [17] Shi, R.H., Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements. *Quantum Inf Process*, 2013, 12(2):921-932
  - [18] Yin, X.R., Wen, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. *Int J Theor Phys*, 2013, 52(11), 3915-3921
  - [19] Sun, Z.W., Zhang, C., Wang, B.H., et al.: Improvements on “multiparty quantum key agreement with single particles”. *Quantum Inf Process*, 2013, 12(11):3411-3420
  - [20] Huang, W., Wen, Q.Y., Liu, B., et al.: Quantum key agreement with EPR pairs and single-particle measurements. *Quantum Inf Process*, 2014, 13(3):649-663
  - [21] Huang, W., Su, Q., Wu, X., et al.: Quantum key agreement against collective decoherence. *Int J Theor Phys*, 2014, 53: 2891-2901
  - [22] Shen, D.S., Ma, W.P., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. *Quantum Inf Process*, 2014, 13(10):2313-2324
  - [23] Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Novel multiparty quantum key agreement protocol with GHZ states. *Quantum Inf Process*, 2014, 13(12):2587-2594
  - [24] Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf Process*, 2014, 13(11):2391-2405
  - [25] Huang, W., Wen, Q.Y., Liu, B., et al.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. *Quantum Inf Process*, 2014, 13(7):1651-1657
  - [26] He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. *Quantum Inf Process*, 2015, 14(9): 3483-3498
  - [27] Zhu, Z.C., Hu, A.Q., Fu, A.M.: Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf Process*, 2015, 14(11):4245-4254
  - [28] Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. *Quantum Inf Process*, 2016, 15(1):373-384
  - [29] Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. *Int J Theor Phys*, 2016, 55(3):1920-1929
  - [30] Zhu, Z.C., Hu, A.Q., Fu, A.M.: Participant attack on three-party quantum key agreement with two-photon entanglement. *Int J Theor Phys*, 2016, 55:55-61
  - [31] He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. *Quantum Inf Process*, 2016, 15:5023-5035
  - [32] Liu, B., Xiao, D., Jia, H.Y., Liu, R.Z.: Collusive attacks to “circle-type” multi-party quantum key agreement protocols. *Quantum Inf Process*, 2016, 15:2113-2124
  - [33] Sun, Z.W., Huang, J.W., Wang, P.: Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf Process*, 2016, 15:2101-2111
  - [34] 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*, 2016, 59:120311
  - [35] Mohajer, R., Eslami, Z.: Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf Process*, 2017, 16:197
  - [36] Cao, H., Ma, W.P.: Multiparty quantum key agreement based on quantum search algorithm. *Sci Rep*, 2017, 7:45046
  - [37] Wang, P., Sun, Z.W., Sun, X.Q.: Multi-party quantum key agreement protocol secure against collusion attacks. *Quantum Inf Process*, 2017, 16:170
  - [38] Cai, B.B., Guo, G.D., Lin, S.: Multi-party quantum key agreement without entanglement. *Int J Theor Phys*, 2017, 56: 1039-1051
  - [39] Wang, L.L., Ma, W.P.: Quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom. *Quantum Inf Process*, 2017, 16:130
  - [40] He, Y.F., Ma, W.P.: Two quantum key agreement protocols immune to collective noise. *Int J Theor Phys*, 2017, 56(2):328-338
  - [41] Jakobi, M., Simon, C., Gisin, N., et al.: Practical private database queries based on a quantum-key-distribution protocol. *Phys Rev A*, 2011, 83:022301
  - [42] Gao, F., Liu, B., Huang, W., Wen, Q. Y.: Postprocessing of the oblivious key in quantum private query. *IEEE J Sel Top Quant*, 2015, 21:6600111
  - [43] Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. *Phys Rev A*, 2016, 93:042318
  - [44] Wei, C.Y., Cai, X.Q., Liu, B., et al.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. *IEEE T Comput*, 2018, 67:2-8
  - [45] Liu, B., Gao, F., Huang, W.: QKD-based quantum private query without a failure probability. *Sci China-Phys Mech Astron*, 2015, 58:100301
  - [46] Yao, A.C.: Protocols for secure computations. In: *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82)*, Washington, DC, USA, 1982, pp.160
  - [47] Goldreich, O., Micali, S., Wigderson, A.: How to play ANY mental game. In: *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC'87)*, 1987, pp.218 缺会议地点和国家
  - [48] Lo, H.K.: Insecurity of quantum secure computations. *Phys Rev A*, 1997, 56(2): 1154-1162
  - [49] Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, 2006, pp.249-260. IEEE, New York 缺会议地点和国家
  - [50] Chau, H.F.: Quantum-classical complexity-security tradeoff in secure multiparty computations. *Phys Rev A*, 2000, 61(3): 032308
  - [51] Smith, A.: Multi-party quantum computation. 2010, arXiv:quant-ph/0111030
  - [52] 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*, 2010, 49(11):2793-2804
  - [53] Heinrich, S.: Quantum summation with an application to integration. *J Complex*, 2002, 18:1-50
  - [54] Heinrich, S., Kwas, M., Wozniakowski, H.: Quantum Boolean summation with repetitions in the worst-average setting. 2003,

- [55] Hillery, M., Ziman, M., Buzek, V., Bielikova, M.: Towards quantum-based privacy and voting. *Phys Lett A*, 2006, 349:75
- [56] Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. *Acta Phys Sin*, 2007, 56(11):6214-6219
- [57] 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*, 2014, 53(3):933-941
- [58] Zhang, C., Sun, Z.W., Huang, X.: Three-party quantum summation without a trusted third party. *Int J Quantum Inf*, 2015, 13(2):1550011
- [59] Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. *Sci Rep*, 2016, 6:19655
- [60] Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. *Quantum Inf Process*, 2017, 16:225
- [61] Zhang, C., Situ, H.Z., Huang, Q., Yang, P.: Multi-party quantum summation without a trusted third party based on single particles. *Int J Quantum Inf*, 2017, 15(2):1750010.
- [62] 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*, 2005, 22(5):1049
- [63] Li, C.Y., Li, X. H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. *Chin Phys Lett*, 2006, 23(11):2896
- [64] Shor P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*, 2000, 85(2):441
- [65] Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. *Chin Phys Lett*, 2007, 24(1):19
- [66] Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. *Chin Phys Lett*, 2013, 30(4):040305
- [67] Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. *Quantum Inf Comput*, 2007, 7:329
- [68] Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "quantum exam"[*Phys Lett A* 350(2006)174]. *Phys Lett A*, 2007, 360(6):748-750
- [69] Guo, F.Z., Qin, S.J., Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. *Eur. Phys. J. D*, 2010, 56(3):445-448
- [70] Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol. *Phys Rev A*, 2007, 76(6):062324