Quantum Information Processing (2021) 20:200
https://doi.org/10.1007/s11128-021-03142-9

Multi-party quantum summation without a third party based on d-dimensional Bell states

WanQing Wu[1] · XiaoXue Ma[2]

Received: 20 April 2020 / Accepted: 25 May 2021 / Published online: 3 June 2021

Abstract
This paper presents a novel n-party quantum summation protocol without the help of a third party via using d-dimensional Bell states. The proposed protocol has inserted decoy photons to prevent various types of the outsider attacks. All participants, respectively, perform the shifting operation to encode their private secrets on quantum particle sequences composed of the first particles of all d-dimensional Bell states. Then, the proposed n-party quantum summation protocol can resist individual attack and $(n-2)$-party collusion attack. As an example, this paper compares the presented multi-party quantum summation protocol with other schemes in terms of different indicators.

Keywords Quantum cryptography · Quantum summation protocol · d-dimensional Bell states

1 Introduction

Ever since quantum mechanics was introduced into the cryptography field, numerous quantum cryptographic applications have been proposed, such as quantum private comparison [1–4], quantum secret sharing (QSS) [5,6], quantum public key cryptosystem ($QPKC$) [7,8] and so on.

Recently, quantum summation protocol becomes an important branch of quantum cryptography and has gained much attention these years. The task of secure quantum summation protocol is to preserve the privacy of the participants inputs and guarantee the correctness of computation. The quantum summation protocol is a kind of secure

✉ WanQing Wu
wuwanqing8888@126.com

✉ XiaoXue Ma
hbumxx@163.com

1 School of Cyber Security and computer, Hebei University, Baoding 071002, People's Republic of China

2 Department of Computer Teaching, Hebei University, Baoding 071002, People's Republic of China

multi-party quantum computation and has been studied by using different quantum resources. In 2006, Hillery et al. employed two-particle N-level entangled states to design a multi-party quantum summation protocol, which can be used to accomplish voting procedure [9]. In 2010, Chen et al. presented a binary quantum summation protocol based on GHZ entangled states [10]. In 2014, Zhang et al. proposed a high-capacity quantum summation protocol with single photons in both polarization and spatial-mode degrees of freedom [11]. In 2016, Shi et al. proposed a quantum summation protocol with the unconditional security and the perfect privacy protection based on quantum Fourier transform operation [12]. [13] presented a multi-party quantum summation with a single d-level quantum system [14]. These protocols have some additional security assumptions, i.e., semi-trusted third parties. But a semi-trusted TP might try to steal the player's private inputs.

With the advance in quantum entanglement swapping, many papers reconstructed the multi-party quantum summation protocol without the help of a third party. In 2015, Zhang et al. employed the genuinely maximally entangled six-qubit states to construct a quantum summation protocol without the help of a trusted third party [15]. In 2017, Zhang et al. presented a multi-party quantum summation protocol without a trusted third party based on quantum states [16]. In 2018, Ye et al. proposed a novel secure multi-party quantum summation protocol based on quantum Fourier transform, and the traveling particles of the presented protocol are transmitted in a tree-type mode [17].

So far, multi-party quantum summation protocol without the help of third party are rare. In addition, publishing more efficient and safer protocols is necessary. For the two reasons, this paper presents a new multi-party quantum summation protocol without a third party based on the d-dimensional Bell states. The paper is organized as follows. Section 2 introduces the relevant knowledge background. Section 3 presents a three-party quantum summation protocol, and discusses the security of the presented protocol. Section 4 generalizes the proposed three-party quantum summation protocol to multi-party. Section 5 compares with other protocols. Section 6 concludes the paper.

2 Preliminary knowledge

2.1 The d-level bell states and shifting operation

The explicit forms of the d-level Bell states are

$$|\varphi(u,v)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{ju} |j\rangle |d-j+v\rangle, \tag{1}$$

where $\omega = e^{\frac{2\pi i}{d}}$ and $0 \leq u, v \leq d-1$. When $d = 2$, $|\varphi(0,0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, $|\varphi(1,0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, $|\varphi(0,1)\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$ and $|\varphi(1,1)\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ are four Bell states.

The shifting operation is defined as

$$QS_k = \sum_{j=0}^{d-1} |j+k\rangle\langle j|, \tag{2}$$

where the symbol + denotes the addition modulo $d (d \geq 2)$ and $k \in \{0, 1, \cdots, d-1\}$ in [18].

It is easy to verify that the quantum particle $|m\rangle \in \{|0\rangle, \cdots, |d-1\rangle\}$ is converted into $|m+k\rangle$ after performing the shifting operation QS_k. When $d = 2$, the qudit shifting operation is $QS_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $QS_1 = |1\rangle\langle 0| + |0\rangle\langle 1|$.

2.2 Particle transmission mode

In general, there are three kinds of particle transmission mode in multi-party quantum protocols, i.e., the tree type, the circle type and the complete graph type [17]. In tree-type mode, one participant prepares the initial quantum states and sends each of the prepared particles to other participants. In the circle-type mode, all participants are arranged in a certain order. Every participant prepares the initial quantum states and sends out a sequence of quantum particles to the next one. In complete-graph-type mode, arbitrary participant forms tree-type mode with others.

3 The three-party quantum summation protocol

3.1 Proposed protocol

In this section, we provide an explicit description of the proposed three-party quantum summation protocol under the authenticated classical and quantum channels, i.e., noiseless and lossless. In the next section, we will discuss how to generalize this three-party quantum summation protocol to a multi-party one.

Suppose that three participants A_1, A_2, A_3 have secret bit strings x_1, x_2, x_3, respectively. They would compute the summation $x_1 + x_2 + x_3$ in public.

$$\begin{aligned}
x_1 &= (x_{11}, x_{12}, \cdots, x_{1m}),\\
x_2 &= (x_{21}, x_{22}, \cdots, x_{2m}),\\
x_3 &= (x_{31}, x_{32}, \cdots, x_{3m}),\\
x_1 + x_2 + x_3 &= (x_{11} \oplus x_{21} \oplus x_{31}, \cdots, x_{1m} \oplus x_{2m} \oplus x_{3m}),
\end{aligned}$$

where m represents the length of secret bit string. Here, $\oplus$ denotes the addition modulo 2.

The participants agree on the following encoding:

$$0 \rightarrow |\varphi(0,0)\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$1 \rightarrow |\varphi(0,1)\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{3}$$

The process of the three-party quantum summation protocol can be described as follows.

Step 1. A_i prepares the quantum initial state

$$S^{(i)} = \left\{ \left| \varphi_1^{(i)} \right\rangle, \cdots, \left| \varphi_m^{(i)} \right\rangle \right\},$$

according to each one bit of her secret message $x_i (i = 1, 2, 3)$, where '0' is $|\varphi(0,0)\rangle$ and '1' is $|\varphi(0,1)\rangle$. Then, A_i divides the quantum initial states into two sequences

$$S_1^{(i)} = \left(p_{11}^{(i)}, p_{12}^{(i)}, \cdots, p_{1m}^{(i)} \right),$$
$$S_2^{(i)} = \left(p_{21}^{(i)}, p_{22}^{(i)}, \cdots, p_{2m}^{(i)} \right),$$

which include the first and the second particles of all states, respectively.

For detecting eavesdropping, A_i mixes $S_1^{(i)}$ with k decoy photons $D_j^{(i)} (j = 1, \cdots, k)$ for each particle randomly in $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$ to form a new sequence $S_1'^{(i)}$. Finally, $A_1(A_2, A_3)$ keeps $S_2^{(1)} (S_2^{(2)}, S_2^{(3)})$ in her hand and sends $S_1'^{(1)} (S_1'^{(2)}, S_1'^{(3)})$ to $A_2(A_3, A_1)$.

Step 2. After confirming that $A_2(A_3, A_1)$ has received all the photons $S_1'^{(1)} (S_1'^{(2)}, S_1'^{(3)})$, $A_1(A_2, A_3)$ announces the positions and the measurement bases of decoy photons to $A_2(A_3, A_1)$ in public. Then, $A_2(A_3, A_1)$ uses the correct basis to measure the corresponding decoy photons and returns the measurement results to $A_1(S_1'^{(2)}, S_1'^{(3)})$. Thereafter, A_1 and A_2 (A_2 and A_3, A_3 and A_1) can check the existence of an Eve by a predetermined threshold of error rate. If the error rate is limited to a predetermined threshold, there is no Eve and the protocol continues. Otherwise, A_1 and A_2 (A_2 and A_3, A_3 and A_1) abort the protocol and repeat the Step 1.

Step 3. $A_1(A_2, A_3)$ extracts the particles $S_1^{(3)} (S_1^{(1)}, S_1^{(2)})$ through abandoning the decoy states. Then $A_1(A_2, A_3)$ chooses a random sequence $r_1 = (r_{11}, \cdots, r_{1m}) \in F_2^m (r_2 = (r_{21}, \cdots, r_{2m}) \in F_2^m, r_3 = (r_{31}, \cdots, r_{3m}) \in F_2^m)$. Then, $A_1(A_2, A_3)$ performs the shifting operation $(QS_{x_{11}+r_{11}}, \cdots, QS_{x_{1m}+r_{1m}}) \left((QS_{x_{21}+r_{21}}, \cdots, QS_{x_{2m}+r_{2m}}), (QS_{x_{31}+r_{31}}, \cdots, QS_{x_{3m}+r_{3m}}) \right)$ on quantum particle sequence $S_1^{(3)} (S_1^{(1)}, S_1^{(2)})$, and obtains

$$\overline{S}_1^{(3)} = \left(QS_{x_{11}+r_{11}} p_{11}^{(3)}, \cdots, QS_{x_{1m}+r_{1m}} p_{1m}^{(3)} \right).$$
$$\left(\overline{S}_1^{(1)} = \left(QS_{x_{21}+r_{21}} p_{11}^{(1)}, \cdots, QS_{x_{2m}+r_{2m}} p_{1m}^{(1)} \right) \right.$$
$$\left. \overline{S}_1^{(2)} = \left(QS_{x_{31}+r_{31}} p_{11}^{(2)}, \cdots, QS_{x_{3m}+r_{3m}} p_{1m}^{(2)} \right) \right)$$

Subsequently, $A_1(A_2, A_3)$ mixes $\overline{S}_1^{(3)}(\overline{S}_1^{(1)}, \overline{S}_1^{(2)})$ with k decoy states $D_j'^{(1)}(D_j'^{(2)}, D_j'^{(3)})$ for each particle randomly in $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}(j = 1, 2, \cdots, k)$ to form a new sequence $\ddot{S}_1^{(3)}(\ddot{S}_1^{(1)}, \ddot{S}_1^{(2)})$. $A_1(A_2, A_3)$ sends the $\ddot{S}_1^{(3)}(\ddot{S}_1^{(1)}, \ddot{S}_1^{(2)})$ to $A_2(A_3, A_1)$.

Step 4. A_1 and A_2, A_2 and A_3, A_3 and A_1 check the existence of an Eve just as Step 2 introduced, respectively.

Step 5. A_1 obtains quantum particle sequence $\overline{S}_1^{(2)}$ by abandoning the decoy states. Then, A_1 performs the shifting operation $(QS_{x_{11}+r_{11}}, \cdots, QS_{x_{1m}+r_{1m}})$ on quantum particle sequence $\overline{S}_1^{(2)}$ and obtains $\widetilde{S_1^{(2)}}$.

After the $|0\rangle, |1\rangle$ basis measurement, A_1 obtains the sequence of classical results $(s_{11}^{A_2} \oplus x_{11} \oplus r_{11} \oplus x_{31} \oplus r_{31}, \cdots, s_{1m}^{A_2} \oplus x_{1m} \oplus r_{1m} \oplus x_{3m} \oplus r_{3m})$, $(s_{21}^{A_1}, \cdots, s_{2m}^{A_1})$ from quantum particles $\widetilde{S_1^{(2)}}$ and $S_2^{(1)}$, respectively. Here, $s_{1j}^{A_i} \oplus s_{2j}^{A_i} = x_{ij}, i = 1, 2, 3, j = 1, \cdots, m$. A_1 computes $P_1 = (s_{11}^{A_2} \oplus x_{11} \oplus r_{11} \oplus x_{31} \oplus r_{31} \oplus s_{21}^{A_1}, \cdots, s_{1m}^{A_2} \oplus x_{1m} \oplus r_{1m} \oplus x_{3m} \oplus r_{3m} \oplus s_{2m}^{A_1})$ and publishes P_1.

In same way, A_2 computes and publishes the results $P_2 = (s_{11}^{A_3} \oplus x_{11} \oplus r_{11} \oplus x_{21} \oplus r_{21} \oplus s_{21}^{A_2}, \cdots, s_{1m}^{A_3} \oplus x_{1m} \oplus r_{1m} \oplus x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_2})$. A_3 computes and publishes the results $P_3 = (s_{11}^{A_1} \oplus x_{31} \oplus r_{31} \oplus x_{21} \oplus r_{21} \oplus s_{21}^{A_3}, \cdots, s_{1m}^{A_1} \oplus x_{3m} \oplus r_{3m} \oplus x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_3})$.

Step 6. A_1, A_2, A_3 obtain the summation of their inputs by computing $P_1 + P_2 + P_3$ by bitwise, and the privacy of each participant's input is preserved.

3.2 Correctness

In this part, we consider the correctness of the proposed three-party quantum summation protocol. Here, we will show that they will get the correct summation using the proposed protocol, namely

$$P_1 + P_2 + P_3 = x_1 + x_2 + x_3$$

is the summation of participants' input.

Before the protocol is implemented, three participants A_1, A_2 and A_3 negotiate a coding rule that the two Bell states $|\varphi(0, 0)\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\varphi(0, 1)\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ represent the classical bits 0, 1, respectively. After A_i performs $|0\rangle, |1\rangle$ basis measurement on Bell states, the first and second quantum particles of each Bell state collapse into classical information $s_{1j}^{A_i}, s_{2j}^{A_i}, i = 1, 2, 3, j = 1, \cdots, m$, respectively. It is clear that $x_{ij} = s_{1j}^{A_i} \oplus s_{2j}^{A_i}$.

In Step 6, three participants measure each particle of quantum sequences received in the basis $\{|0\rangle, |1\rangle\}$, respectively. They publish the results

$$P_1 = \left(s_{11}^{A_2} \oplus x_{11} \oplus r_{11} \oplus x_{31} \oplus r_{31} \oplus s_{21}^{A_1}, \cdots, s_{1m}^{A_2} \oplus x_{1m} \oplus r_{1m} \oplus x_{3m} \oplus r_{3m} \oplus s_{2m}^{A_1}\right),$$

$$P_2 = \left(s_{11}^{A_3} \oplus x_{11} \oplus r_{11} \oplus x_{21} \oplus r_{21} \oplus s_{21}^{A_2}, \cdots, s_{1m}^{A_3} \oplus x_{1m} \oplus r_{1m} \oplus x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_2}\right),$$

$$P_3 = \left(s_{11}^{A_1} \oplus x_{31} \oplus r_{31} \oplus x_{21} \oplus r_{21} \oplus s_{21}^{A_3}, \cdots, s_{1m}^{A_1} \oplus x_{3m} \oplus r_{3m} \oplus x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_3}\right).$$

Further, they then compute

$$\begin{aligned} P_1 + P_2 + P_3 &= \Big(s_{11}^{A_2} \oplus x_{11} \oplus r_{11} \oplus x_{31} \oplus r_{31} \oplus s_{21}^{A_1} \oplus s_{11}^{A_3} \oplus x_{11} \oplus r_{11} \oplus \\ &\quad x_{21} \oplus r_{21} \oplus s_{21}^{A_2} \oplus s_{11}^{A_1} \oplus x_{31} \oplus r_{31} \oplus x_{21} \oplus r_{21} \oplus s_{21}^{A_3}, \cdots, \\ &\quad s_{1m}^{A_2} \oplus x_{1m} \oplus r_{1m} \oplus x_{3m} \oplus r_{3m} \oplus s_{2m}^{A_1} \oplus s_{1m}^{A_3} \oplus x_{1m} \oplus r_{1m} \oplus \\ &\quad x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_2} \oplus s_{1m}^{A_1} \oplus x_{3m} \oplus r_{3m} \oplus x_{2m} \oplus r_{2m} \oplus s_{2m}^{A_3}\Big) \\ &= (x_{11} \oplus x_{21} \oplus x_{31}, \cdots, x_{1m} \oplus x_{2m} \oplus x_{3m}) \\ &= x_1 + x_2 + x_3, \end{aligned}$$

that is the summation of the participants' input.

3.3 Security analysis

The classical and quantum channels of the presented protocol are assumed to be authenticated. The result of the summation protocol could be published in public, but all each participant's privacy input should be preserved.

In this section, we consider the security of the presented three-party quantum summation protocol. Outside eavesdroppers wish to steal the participants' inputs. In addition, some participants may try to derive other participants' private inputs. Therefore, the security goal of quantum summation protocol is to protect the privacy of participants' inputs from outside attacks and participant attacks.

In presented protocol, in order to resist the outside attacks, all parties check the existence of an eve in public. This idea is derived from the unconditionally secure BB84 QKD protocol [19]. Any attacks from outside will be detected in Step 2 and Step 4, such as entanglement-measure attack, measurement-resend attack, and intercept-resend. Since an Eve does not know the measuring bases and the positions of all decoy photons in Step 2. Eve will lead to an error to each decoy photon with a probability of $\frac{1}{4}$. Thus, let k be the number of decoy photons, if k is large enough, then the probability of detecting Eve's attack from the public discussion $1 - (\frac{3}{4})^k$ is close to 1. In step 4, all participants check the existence of Eve just as Step 2 introduced. In addition, the presented quantum summation protocol employs the one-step quantum transmission, and it is also congenitally free from Trojan horse attacks [18]. Hence, our protocol is secure against the outside attacks.

Next, we consider the two kinds of participant attacks in proposed protocol. In the above protocol, the roles of different A_is ($i = 1, 2, 3$) are the same, we can assume that A_1 is a dishonest participant trying to steal other participants' private information. In the presented protocol, A_1 can obtain quantum particle sequences $S_1^{(3)}$ and $\overline{S}_1^{(3)}$. According to coding rules in the presented protocol, A_1 can distinguish between $x_{3j} = 0$ and $x_{3j} = 1$, $j = 1, \cdots, m$, in quantum particle sequences $S_1^{(3)}$ if A_1 can distinguish between the two states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$. A_1 needs to distinguish

between the density matrices

$$\begin{aligned}\rho &= tr_2\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\frac{\langle 00|+\langle 11|}{\sqrt{2}}\right)\\ &= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}\sigma &= tr_2\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\frac{\langle 01|+\langle 10|}{\sqrt{2}}\right)\\ &= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}.\end{aligned}$$

It is clear that $\rho = \sigma$. Then, A_1 cannot distinguish the initial Bell states of A_3 by measuring the quantum particle sequences $S_1^{(3)}$.

In addition, even if A_1 can obtain the information $x_{3j} \oplus r_{3j}$ from quantum particle sequences $\overline{S}_1^{(3)}$, A_1 does not know the x_{3j}. The reason is that A_1 does not know random number sequence r_3 except A_3. So A_1 can only guess the correct random numbers with $\frac{1}{2^m}$ successful probability. If A_1 may intend to attack others quantum particle sequences, A_1 will be detected as an outside attacker. Furthermore, the presented protocol can resist the inside attacks from one single dishonest participant.

For the case of collusion attack, it is clear that any two dishonest participants can obtain the rest one's private information when the summation results is revealed in public. But the n-party summation protocol is secure resist $(n-2)$-party collusion attacks. We discuss this issue in the following section.

4 The multi-party quantum summation protocol

4.1 Proposed protocol

In this section, we discuss how to generalize the three-party quantum summation protocol to a multi-party one. Suppose that every participant $A_i, i = 1, \cdots, n$ has secret information $x_i = (x_{i1}, \cdots, x_{im})$, $x_{ij} \in \{0, 1, \cdots, n-2\}$, $j = 1, \cdots, m$, respectively. They want to compute the summation $\sum_{i=1}^{n} x_i = (x_{11}+\cdots+x_{n1}, \cdots, x_{1m}+\cdots+x_{nm})$ of their secret messages in public, and the privacy of each participant's input $x_i, i = 1, \cdots, n$ should be preserved, respectively. Here, $''+''$ denotes the addition modulo $n-1$.

The participants agree on the following encoding:

$$v \to |\varphi(0, v)\rangle = \frac{1}{\sqrt{n-1}}\sum_{j=0}^{n-2}|j\rangle|n-1-j+v\rangle, \tag{4}$$

where $v = 0, 1, \cdots, n-2$. We will introduce the details of the n-party quantum summation protocol in steps as follows.

Step 1. A_i encodes the secret information $x_i = (x_{i1}, \cdots, x_{im}), i = 1, \cdots, n$ according to the above agreement, and records these initial states as

$$S^{(i)} = \{|\varphi_1^{(i)}\rangle, \cdots, |\varphi_m^{(i)}\rangle\},$$

where $|\varphi_j^{(i)}\rangle \in \{|\varphi(0,0)\rangle, \cdots, |\varphi(0,n-2)\rangle\}, j = 1, \cdots, m$.

Further, A_i picks out the first particles and second particles from each state to form the sequences

$$S_1^{(i)} = \left(p_{11}^{(i)}, p_{12}^{(i)}, \cdots, p_{1m}^{(i)}\right),$$
$$S_2^{(i)} = \left(p_{21}^{(i)}, p_{22}^{(i)}, \cdots, p_{2m}^{(i)}\right).$$

Here, the $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$ represent $A_i's$ two different particles in one Bell state. The superscript $j = 1, \cdots, m$ indicates the Bell state orders in each sequence.

Step 2. A_i mixes $S_1^{(i)}$ with m decoy photons $D_j^{(i)} (j = 1, \cdots, m)$ for each particle randomly in $\{|0\rangle, \cdots, |n-2\rangle, F|0\rangle, \cdots, F|n-2\rangle\}$ to form a new sequence $S_1'^{(i)}$, where F is a quantum Fourier transform in $(n-1)$-level quantum system. Then, A_i sends $S_1'^{(i)}$ to $A_{i+1}, i = 1, \cdots, n-1$ and A_n sends $S_1'^{(n)}$ to A_1.

Step 3. After confirming that $A_{i+1}(A_1)$ has received all particles $S_1'^{(i)}(S_1'^{(n)})$, $A_{i+1}(A_1)$ checks the security of the transmission of $S_1'^{(i)}(S_1'^{(n)})$ with $A_i(A_n)$. Sender $A_i(A_n)$ announces the positions and the measurement bases of decoy photons to $A_{i+1}(A_1)$, where $i = 1, \cdots, n-1$.

According to the announced decoy photons, $A_{i+1}(A_1)$ measures the corresponding decoy photons and returns the measurement results to $A_i(A_n)$. Thereafter, $A_{i+1}(A_1)$ and $A_i(A_n)$ can check the existence of an Eve by a predetermined threshold of error rate. If the error rate is limited in a predetermined threshold, there is no Eve and the protocol continues. Otherwise, $A_{i+1}(A_1)$ and $A_i(A_n)$ abort the protocol and restart from Step 1 for $i = 1, \cdots, n-1$.

Step 4. $A_2, \cdots, A_n, A_1$, respectively, obtain the sequence $S_1^{(1)}, \cdots, S_1^{(n-1)}, S_1^{(n)}$ through abandoning the decoy states. A_{i+1} chooses a random sequence $r_{i+1} = (r_{i+11}, \cdots, r_{i+1m}) \in F_{n-1}^m (i = 1, \cdots, n-1)$, and A_1 chooses a random sequence $r_1 = (r_{11}, \cdots, r_{1m}) \in F_{n-1}^m$.

Then, $A_{i+1} (i = 1, \cdots, n-1)$ and A_1 obtain

$$\overline{S}_1^{(i)} = \left(QS_{x_{i+11}+r_{i+11}} p_{11}^{(i)}, \cdots, QS_{x_{i+1m}+r_{i+1m}} p_{1m}^{(i)}\right),$$
$$\overline{S}_1^{(n)} = \left(QS_{x_{11}+r_{11}} p_{11}^{(n)}, \cdots, QS_{x_{1m}+r_{1m}} p_{1m}^{(n)}\right) \quad (5)$$

through performing the shifting operation $(QS_{x_{i+11}+r_{i+11}}, \cdots, QS_{x_{i+1m}+r_{i+1m}})$, $(QS_{x_{11}+r_{11}}, \cdots, QS_{x_{1m}+r_{1m}})$ on quantum particle sequence $S_1^{(i)}$, $S_1^{(n)}$, respectively.

Subsequently, $A_{i+1}(i = 2, \cdots, n-1)$ and A_1 randomly prepare decoy states $\otimes_{j=1}^{m} D_j'^{(i)}$, $\otimes_{j=1}^{m} D_j'^{(n)}$ and inserts them in $\overline{S}_1^{(i)}$, $\overline{S}_1^{(n)}$ to form new sequences $\ddot{S}_1^{(i)}$, $\ddot{S}_1^{(n)}$. Then, A_1 sends $\ddot{S}_1^{(n)}$ to A_2, A_{i+1} sends $\ddot{S}_1^{(i)}$ to $A_{i+2}, i = 1, \cdots, n-2$ and A_n sends $\ddot{S}_1^{(n-1)}$ to A_1.

Step 5. After confirming that $\ddot{S}_1^{(n)}, \ddot{S}_1^{(1)}, \cdots, \ddot{S}_1^{(n-1)}$ have been securely received $A_2, A_3, \cdots, A_1$, they collaborate in checking the existence of an Eve. They can finish this check as follows. A_1 announces the positions and the measurement bases of decoy photons in $\ddot{S}_1^{(n)}$ to A_2. Then, A_2 measures the corresponding decoy photons and returns the measurement results to A_1. A_1 and A_2 can check the existence of an Eve by a predetermined threshold of error rate. If the error rate is limited in a predetermined threshold, there is no Eve and the protocol continues. Otherwise, A_1 and A_2 abort the protocol and restart from Step 1.

All participants check the existence of an Eve just as above, respectively. Then, $A_2, \cdots, A_n, A_1$ obtain quantum particle sequences $\overline{S}_1^{(n)}, \overline{S}_1^{(1)}, \cdots, \overline{S}_1^{(n-1)}$ by abandoning the decoy states, respectively.

Step 6. A_1 obtains the sequence of classical results $(x_{n1} + r_{n1} + s_{11}^{A_{n-1}}, \cdots, x_{nm} + r_{nm} + s_{1m}^{A_{n-1}})$, $(s_{21}^{A_1}, \cdots, s_{2m}^{A_1})$ from quantum particles $\overline{S}_1^{(n-1)}$ and $S_2^{(1)}$ after the $|0\rangle, |1\rangle, \cdots, |n-2\rangle$ basis measurement.

Then, A_1 computes $P_1 = (s_{11}^{A_{n-1}} + x_{n1} + r_{n1} + s_{21}^{A_1} + (n-1-x_{11}) + (n-1-r_{11}), \cdots, s_{1m}^{A_{n-1}} + x_{nm} + r_{nm} + s_{2m}^{A_1} + (n-1-x_{1m}) + (n-1-r_{1m}))$ and publishes them. In the same way, $A_i, i = 2, \cdots, n$ computes and publishes P_i, respectively.

Step 7. The participants A_i will get the summation of their inputs by computing $P_1 + \cdots + P_n$ by bitwise, and the privacy of each participant's input is preserved.

4.2 Correctness

Next, we discuss the correctness and the security of the presented multi-party quantum summation protocol. For the correctness, combining with the correctness analysis of three-party quantum summation, the correctness of the multi-party quantum summation protocol can be guaranteed.

Before the protocol is implemented, the participants $A_i, i = 1, \cdots, n$ negotiate a coding rule (4). After A_i performs $|0\rangle, |1\rangle, \cdots, |n-2\rangle$ basis measurement on Bell states, the first and second quantum particles of each Bell state collapse into classical information $s_{1j}^{A_i}, s_{2j}^{A_i}, i = 1, 2, 3, j = 1, \cdots, m$, respectively. It is clear that $x_{ij} = s_{1j}^{A_i} \oplus s_{2j}^{A_i}$.

In step 4, A_n performs the shifting operation on quantum particle sequence $S_1^{(n-1)}$, and obtains $\overline{S}_1^{(n-1)} = (QS_{x_{n1}+r_{n1}} p_{11}^{(n-1)}, \cdots, QS_{x_{nm}+r_{nm}} p_{1m}^{(n-1)})$, where $QS_{x_{ni}+r_{ni}} (i = 1, \cdots, m)$ can be defined in equation (2). Then, A_n inserts decoy states to form $\ddot{S}_1^{(n-1)}$, and sends $\ddot{S}_1^{(n-1)}$ to A_1.

After checking the existence of an Eve, A_1 obtains $\overline{S}_1^{(n-1)}$ by abandoning the decoy states. In step 6, after the $|0\rangle, |1\rangle, \cdots, |n-2\rangle$ basis measurement, A_1 obtains the

sequence of classical results $(x_{n1}+r_{n1}+s_{11}^{A_{n-1}},\cdots,x_{nm}+r_{nm}+s_{1m}^{A_{n-1}})$ from quantum particles $\overline{S_1}^{(n-1)}$, and A_1 obtains the $(s_{21}^{A_1},\cdots,s_{2m}^{A_1})$ from $S_2^{(1)}$.

In Step 6, all participants $A_i(i=1,2,\cdots,n)$ compute and publish the following results:

$$\begin{aligned}
P_1 &= \Big(s_{11}^{A_{n-1}}+(n-1-x_{11})+(n-1-r_{11})+x_{n1}+r_{n1}+s_{21}^{A_1},\cdots,\\
&\quad s_{1m}^{A_{n-1}}+(n-1-x_{1m})+(n-1-r_{1m})+x_{nm}+r_{nm}+s_{2m}^{A_1}\Big),\\
P_2 &= \Big(s_{11}^{A_n}+x_{11}+r_{11}+(n-1-x_{21})+(n-1-r_{21})+s_{21}^{A_2},\cdots,\\
&\quad s_{1m}^{A_n}+x_{1m}+r_{1m}+(n-1-x_{2m})+(n-1-r_{2m})+s_{2m}^{A_2}\Big),\\
P_3 &= \Big(s_{11}^{A_1}+x_{21}+r_{21}+(n-1-x_{31})+(n-1-r_{31})+s_{21}^{A_3},\cdots,\\
&\quad s_{1m}^{A_1}+x_{2m}+r_{2m}+(n-1-x_{3m})+(n-1-r_{3m})+s_{2m}^{A_3}\Big),\\
&\quad\cdots\\
P_n &= \Big(s_{11}^{A_{n-2}}+x_{n-11}+r_{n-11}+(n-1-x_{n1})+(n-1-r_{n1})+s_{21}^{A_n},\cdots,\\
&\quad s_{1m}^{A_{n-2}}+x_{n-1m}+r_{n-1m}+(n-1-x_{nm})+(n-1-r_{nm})+s_{2m}^{A_n}\Big).
\end{aligned}$$

In Step 7, by the equation (4), they compute

$$\begin{aligned}
&P_1+P_2+P_3+\cdots+P_n\\
&=\Big(s_{11}^{A_{n-1}}+(n-1-x_{11})+(n-1-r_{11})+x_{n1}+r_{n1}+s_{21}^{A_1}\\
&\quad+s_{11}^{A_n}+x_{11}+r_{11}+(n-1-x_{21})+(n-1-r_{21})+s_{21}^{A_2}\\
&\quad+s_{11}^{A_1}+x_{21}+r_{21}+(n-1-x_{31})+(n-1-r_{31})+s_{21}^{A_3}\\
&\quad+\cdots+s_{11}^{A_{n-2}}+x_{n-11}+r_{n-11}+(n-1-x_{n1})+(n-1-r_{n1})+s_{21}^{A_n},\\
&\quad\cdots,\\
&s_{1m}^{A_{n-1}}+(n-1-x_{1m})+(n-1-r_{1m})+x_{nm}+r_{nm}+s_{2m}^{A_1}\\
&\quad+s_{1m}^{A_n}+x_{1m}+r_{1m}+(n-1-x_{2m})+(n-1-r_{2m})+s_{2m}^{A_2}\\
&\quad+s_{1m}^{A_1}+x_{2m}+r_{2m}+(n-1-x_{3m})+(n-1-r_{3m})+s_{2m}^{A_3}\\
&\quad+\cdots+s_{1m}^{A_{n-2}}+x_{n-1m}+r_{n-1m}+(n-1-x_{nm})+(n-1-r_{nm})+s_{2m}^{A_n}\Big)\\
&=(x_{11}+x_{21}+\cdots+x_{n1},\cdots,x_{1m}+x_{2m}+\cdots+x_{nm})\\
&=x_1+x_2+\cdots+x_n
\end{aligned}$$

that is the summation of the participants' input.

4.3 Security analysis

We can observe that this multi-party quantum summation is similar to the presented three-party quantum summation because the idea is the same. For the security, we use the same method to prevent the outside and participant attacks in both three-party and multi-party quantum summation.

(i) Outside attack
We consider the possibility for an outside Eve to study the private inputs from all participants here.
In the presented protocol, in order to study the private inputs, an outside Eve may intercept information from the particle transmission in Step 2 to launch active attacks, such as the entangle-measure attack, the intercept-resend attack and the measure-resend attack and so on. However, the presented protocol employs the decoy photons to detect an outside Eve, which are randomly chosen from the conjugate bases $\{|0\rangle, \cdots, |n-2\rangle, F|0\rangle, \cdots, F|n-2\rangle\}$. Moreover, if an outside Eve launches the attacks during the particle transmissions, she will be detected by the eavesdropping check process. Since an Eve cannot get any information about the positions and the measurement basis of all decoy photons before the announcement.

On the other hand, in Step 4, even if an outside Eve may capture $x_i + r_i$ when $A_i (i = 1, 2, \cdots, n)$ announces it to A_{i+1}. However, an Eve still cannot recover out $x_i (i = 1, 2, \cdots, n)$ from it, because an Eve does not know the value of r_i. In addition, an Eve cannot deduce x_i from the result of summation $P_1 + P_2 + \cdots + P_n$, due to lack of the knowledge of the values.

(ii) Participant attack
Gao(2007) pointed out that the participant attack from one or more dishonest parties is generally more powerful [20]. Because participant attacks have more advantages than outside attacks. To show this in a sufficient way, we discuss three cases of participant attack. Firstly, we consider the participant attack from one single dishonest party. Secondly, we discuss collusive from two or more dishonest parties. Thirdly, we analyze the collusive attacks to circle-type multi-party quantum key agreement (CT-MQKA) protocols.

(1) The participant attack from one single dishonest party
In our protocol, the roles of every $A_j (j = 1, 2, \cdots, n)$ are the same. Without loss of generality, we assume that A_1 is a dishonest participant.
If a single dishonest A_1 captures the particles in $S_1^{\prime(n)}$ from A_j to $A_{j+1} (j = 2, 3, \cdots, n-1)$ in Step 2, she is considered an outside attacker because she does not know the location of the decoy photon. the positions and the measurement basis of the inserted decoy photons in $S_1^{\prime(n)}$. In addition, even if A_1 can capture the information $x_j + r_j$ from $\ddot{S}_1^{(j)} (j = 1, 2, \cdots, n)$ in Step 4, due to having no knowledge access to the value of $r_j (j = 1, 2, \cdots, n)$, she can not recover the x_j either. So the proposed protocol can resist attacks from a dishonest participant.

(2) The participant attack from two or more dishonest parties
For the case of collusion attack in the multi-party quantum summation, the proposed multi-party quantum summation can prevent $(n-2)$-party collusion attacks. The reason is as follows. Any $n-2$ participants can obtain the other two participants' public information $x_i + r_i + (n-1-x_j) + (n-1-r_j)$ according to this protocol, but any $n-2$ dishonest participants do not obtain the exact values of r_i and $r_j, i \neq j$. Consequently, they cannot determine the exact values of x_i and x_j. In this sense, the $(n-2)$-party collusion attack is still invalid to our multi-party quantum summation protocol.
Note that the presented quantum summation protocol is not prevent the $(n-1)$-party collusion attack. Since the public information is a linear equation, $(n-1)$-party can know the rest one. If one participant becomes a trusted center, it can resist the $(n-1)$-party collusion attack. But the aim of this paper is to design a quantum summation protocol without the help of a trusted third party.

(3) The collusive attacks to CT-MQKA protocols
In addition Liu (2016) et al. presented a collusive attack to the special CT-MQKA protocols [21]. Our protocol is a "circle-type" protocol in a model, but it is secure against their attacks. The reason is as follows. In [21], every sequence will be sent back to the participants who generated it. Then A_i can measure these sequences to obtain the bitwise results of all the other participants' keys. Finally, they can calculate the final key $K_{final} = \oplus_{i=0}^{n-1} K_i$, where K_i is a secret input. In the collusive attacks to CT-MQKA protocols, if two dishonest participants A_j and A_m want to control the final key, as long as their positions in the circle satisfy the conditions, $j - m = \frac{n}{2}$ for an even, or $j - m = \frac{n-1}{2} (j - m = \frac{n+1}{2})$ for an odd n. If more dishonest participants $A_j (j \leq n-2)$ want to control the final key, they can obtain the legal final key in $\frac{n}{j} > 1$ periods, while our protocol only has one period of secret information transmission. This is not enough to get more information against the presented protocol. Secondly, the $n-2$ dishonest participants $A_i (i = 3, \cdots, n)$ can capture the information $x_1 + r_1 + x_2 + r_1$. Without this knowledge of r_1, r_2, the dishonest participants can not derive the information x_1 and x_2 by the honest participants. Finally, they cannot get the honest participants' private inputs.

5 Comparison

In this subsection, we compare the previous quantum summation protocols with the presented quantum summation protocol from the quantum resource, the qubit efficiency, the protocol model and the quantum operations in Table 1.

Qubit efficiency can be defined as $\eta = \frac{c}{q+b}$, where c denotes the total number of the classical plaintext message bits, q denotes the total number of qubits used in quantum scheme and b denotes the number of classical bits exchanged for decoding the message. Suppose that the number of participants is N, the length of the secret information is m and m decoy particles are employed to check eavesdropping. In our protocol, there are $2mN$ particles for encoding, $2mN$ decoy particles for eavesdropping detection. In

Table 1 Comparison of the proposed protocol to the others

Shemes	Quantum resource	Qubit efficiency	TP	Quantum operations
Zhang et al.'s [11]	Single-photon state	$\frac{2}{2N+3}$	Yes	Single photons R
Zhang et al.'s [16]	Entanglement of three particles	$\frac{1}{4N-1}$	No	CNOT and Hadamard operators
Shi et al's [12]	$(N+1)$-partite entangled state	$\frac{1}{3N-2}$	No	Quantum Fourier, CNOT and oracle operators
Ye et al's [17]	N-particle entangled states	$\frac{1}{3N-2}$	No	Quantum Fourier and Pauli operators
Zhang et al's [22]	Bell states	$\frac{1}{2N+3}$	No	Pauli operators and Bell measurement
Proposed protocol	Bell states	$\frac{1}{5N}$	No	NOT, identity operators and $\{0, 1\}$ measurement

addition, to compute the summation, participants need to announce mN classical bits. Then, the qubit efficiency of the presented protocol is $\eta = \frac{m}{5mN} = \frac{1}{5N}$.

Observe that the qubit efficiency of the presented protocol is not the best from Table 1. However, the proposed protocol is much easier implemented compared with other protocols based on current quantum techniques. It uses a semi-honest trusted party to help the summation computation in [23]. The protocols in [12,16,17] are hard to be generated based on the multi-bit entangled states. For implementation, the protocol in [22] requires more quantum resources and communication complexity than ours.

6 Conclusion

In this paper, we described a quantum summation protocol based on d-dimensional Bell states, where the encoded particles are transmitted in a circular way. Every participant employ the shifting operation to encode their private secrets on quantum particle sequences. The proposed quantum summation protocol can overcome the outside attack, individual attack and $(n-2)$-party collusion attack.

Acknowledgements The authors are supported by the Natural Science Foundation of HeBei Province Nos. F2021201199, Science and technology research project of Hebei higher education Nos. ZD2021011.

References

1. He, G.P.: Quantum private comparison protocol without a third party. Int. J. Quantum Inf. **15**(2), 1750014 (2016)
2. Wu, W.Q., Cai, Q.Y., Wu, S.M., et al.: Cryptanalysis and improvement of Ye et al's quantum private comparison protocol. Int. J. Theor. Phys. **58**(6), 1892–1900 (2019)
3. Wu, W.Q., Zhang, H.G.: Cryptanalysis of Zhang et al's Quantum Private Comparison and the Improvement. Int. J. Theor. Phys. **58**(6), 1854–1860 (2019)
4. Wu, W.Q., Ma, X.X.: Quantum private comparison protocol without a third party. Int. J. Theor. Phys. **59**(6), 1854–1865 (2020)
5. Xu, T.T., Li, Z.H., Bai, C.M., et al.: A New Improving Quantum Secret Sharing Scheme. Int. J. Theor. Phys. **56**, 1–10 (2017)
6. Bai, C.M., Li, Z.H., Xu, T.T., et al.: Quantum secret sharing using the d-dimensional GHZ state. Quantum Inf. Process. **16**(3), 59 (2017)
7. Wu, W.Q., Cai, Q.Y., Zhang, H.G., et al.: Quantum public key cryptosystem based on bell states. Int. J. Theor. Phys. **56**(11), 3431–3440 (2017)
8. Wu, W.Q., Cai, Q.Y., Zhang, H.G., et al.: Bit-oriented quantum public-key cryptosystem based on bell states. Int. J. Theor. Phys. **57**(12), 1–11 (2018)
9. Hillery, M., Ziman, M., Bužek, V., et al.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1–4), 75–81 (2006)
10. Chen, X.B., Xu, G., Yang, Y.X., et al.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**(11), 2793–2804 (2010)
11. Zhang, C., Sun, Z., Huang, Y., et al.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933–941 (2014)
12. Shi, R.H., Mu, Y., Zhong, H., et al.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
13. Zhang, C., Razavi, M., Sun, Z.W., et al.: Improvements on "Secure multi-party quantum summation based on quantum Fourier transform." Quantum Inf. Process. **18**, 336 (2019)

14. Zhang, C., Situ, H., Huang, Q., et al.: Multi-party quantum summation with a single d-level quantum system. Int. J. Quantum Inf. **17**(03), 1154–652 (2019)
15. Zhang, C., Sun, Z.W., Huang, X., et al.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
16. Zhang, C., Situ, H., Huang, Q., et al.: Multi-party quantum summation without a trusted third party based on single particles. Int. J. Quantum Inf. **15**(2), 1750010 (2017)
17. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)
18. Wu, W.Q., Zhang, H.G.: A quantum query algorithm for computing the degree of a perfect nonlinear Boolean function. Quantum Inf. Process. **18**(3), 62 (2019)
19. 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, pp. 175–179 (1984)
20. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**(4), 329–334 (2007)
21. Liu, B., Xiao, D., Jia, H.Y., et al.: Collusive attacks to circle-type multi-party quantum key agreement protocols. Quantum Inf. Process. **15**, 2113–2124 (2016)
22. Zhang, C., Razavi, M., Sun, Z.W., et al.: Multi-party quantum summation based on quantum teleportation. Entropy **21**(7), 719 (2019)
23. Zhang, C., Sun, Z., Huang, Y., et al.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933–941 (2014)