Improvements on "Multi-Party Quantum Summation without a Third Party based on d-Dimensional Bell States"

Xiaobing Li, Jiale Hou, Haozhen Situ, Cai Zhang

College of Mathematics and Informatics, South China Agricultural University, No. 483 Wushan Road, Tianhe District, Guangzhou, 510642, Guangdong, China.

*Corresponding author(s). E-mail(s): zhangcai@scau.edu.cn; Contributing authors: 905035470@qq.com; 2821541172@qq.com; situhaozhen@gmail.com;

Abstract

In 2021, Wu et al. presented a multi-party quantum summation scheme exploiting the entanglement properties of **d**-dimensional Bell states (Wu et al. in Quantum Inf Process 20:200, 2021). In particular, the authors proposed a three-party quantum summation protocol and then extended their work to a multi-party case. It is claimed that their protocol is secure against outside and participants' attacks. However, this work points out that Wu's protocol has a loophole, i.e., two or more dishonest participants who meet a specific location relationship can conspire to obtain the private inputs of some honest participants without being detected. Accordingly, improvements are proposed to address these issues.

Keywords: Quantum summation, d-dimensional Bell states, Participant attacks

1 Introduction

Quantum cryptography, combined with classical cryptography and quantum mechanics, has gained much attention since the advent of the first quantum key distribution protocol proposed by Bennett and Brassard [1] in 1984, which has thus spawned many branches, such as quantum key distribution (QKD) [2, 3], quantum secret sharing (QSS) [4, 5], quantum secure multiparty computation (QSMC) [6–10], and so

on, and QSMC has been developed from the classical secure multiparty computation (MPC). Secure MPC is one of the core technologies to achieve privacy computing in the era of big data, which first originated from the millionaires' problem proposed by Yao [11] in 1982, i.e., two millionaires want to know who is richer without exposing their assets. With the quantum algorithms being put forward, such as Shor's algorithm [12] and Grover's algorithm [13], and quantum computers' arrival, however, classical MPC that is based on the complexity of the computation is no longer secure, which has led to the research on QSMC.

Quantum secure multiparty summation (QMPS) is one of the subfields in QMPC, whose target is to calculate the summation of inputs from different communicants without the input values leaking out, with the numerous applications in quantum anonymous voting [14, 15], quantum privacy comparison [16], data mining [17], etc. In 2002, Heinrich [18] applied quantum summation into integration. In 2007, Vaccaro et al. [19] first applied quantum summation in anonymous voting. To date, various QMPS schemes have been constructed from different viewpoints, such as summation with the help of a third party [20], semi-quantum multi-party summation [21], summation based on single states [22] or entangle states [23] and so on. In 2019, Ji et al. [24] proposed a QMPS protocol based on entanglement swapping with a semi-honest third party. Subsequently, Gan pointed out a loophole in Ji's protocol in Ref [25] and presented an improvement on the protocol. Zhang replaced the entanglement swapping between Cat states and Bell states in Ji's protocol with the entanglement swapping between Bell states in Ref [26]. Wang et al. [27] extended Ji's protocol to sum in decimalization. In addition, QMPS can be classified into tree-type, complete-graph-type, and circletype, according to the mode of particle transmission [28]. In 2021, Wu et al. proposed a quantum summation protocol in the circle-type in Ref [29], which we refer to as Wu's protocol hereafter, and claimed their scheme is secure against the attack pointed out by Liu in Ref [30].

However, it is indicated that Wu's protocol [29] has a security loophole in this work, i.e., two or more dishonest participants in their protocol can launch two kinds of attacks to learn about the specific party's private inputs without being detected. To make Wu's protocol secure, we propose improvements by adding random numbers and a detection mechanism.

The remaining part of this paper is organized as follows. Section 2 reviews Wu's protocol. Section 3 presents two kinds of attacks on Wu's protocol in detail. Section 4 puts forward improvements and gives the correctness and security analysis on the improved protocol. Discussion and conclusion are given in the section 5.

2 Review of Wu's Protocol

In Wu's protocol [29], the classical and quantum channels are authenticated, i.e., noiseless and lossless, and the d-dimensional Bell state is defined as following:

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

where $\omega = e^{\frac{2\pi i}{d}}, \ 0 \le u, v \le d-1$ and the operation in Dirac notation is modulo d.

The d-dimensional Bell states are orthogonal,

$$\langle \varphi(u_1, v_1) | \varphi(u_2, v_2) \rangle = \delta_{u_1 u_2} \delta_{v_1 v_2}, \tag{2}$$

where

$$\delta_{uv} = \begin{cases} 1, & u = v, \\ 0, & u \neq v, \end{cases} \tag{3}$$

is Kronecker delta.

The shifting operation is defined as

$$QS_k = \sum_{j=0}^{d-1} |j+k\rangle \langle j|, \qquad (4)$$

where the operation in Dirac notation is modulo d ($d \ge 2$) and $k \in \{0, 1, \dots, d-1\}$. In Wu's protocol, n players A_1, A_2, \dots, A_n ($n \ge 3$) are involved. Each participant A_i ($i = 1, 2, \dots, n$) has a private integer string x_i of length m in the following form

$$x_i = (x_{i1}, x_{i2}, \cdots, x_{im}),$$
 (5)

where $x_{ij} \in \{0, 1, \dots, d-1\}$ $(j = 1, 2, \dots, m; d = n-1)$. A_1, A_2, \dots, A_n intend to jointly compute the summation $x_1 + x_2 + \dots + x_n \pmod{d}$ without their private inputs x_i leaking out.

The participants agree on the following encoding:

$$v \to |\varphi(0,v)\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |j\rangle |d-j+v\rangle$$
 (6)

where $v \in \{0, 1, 2, \dots, d-1\}$.

The process of the three-party and the multi-party cases in Wu's protocol can be unified as n-party ($n \ge 3$) and described as follows.

Step 1: A_i $(i = 1, 2, \dots, n)$ prepares the initial states as

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

according to x_i , where $\left|\varphi_j^{(i)}\right\rangle = \left|\varphi(0,x_{ij})\right\rangle \ (j=1,\cdots,m)$. Subsequently, A_i divides the initial states into two sequences

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

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

where $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$ represent the first and the second particles of j-th Bell state in $S^{(i)}$ respectively.

Step 2: A_i $(i=1,2,\cdots,n)$ mixes $S_1^{(i)}$ with m decoy photons $D_j^{(i)}$ $(j=1,2,\cdots,m)$ for each particle randomly in $\{|r\rangle,F|r\rangle\}_{r=0}^{d-1}$ to form new sequences $S_1^{'(i)}$, where F is a quantum Fourier transform in d-level quantum system. Then A_i sends $S_1^{'(i)}$ to $A_{i\oplus 1}$, and keeps $S_2^{(i)}$ in hand, where " \oplus " satisfies the following arithmetic rules throughout the paper

$$a \oplus b = \begin{cases} a+b-n, & a+b > n, \\ a+b, & a+b \le n, \end{cases}$$
 (7)

and $a, b \in \{1, 2, \dots, n\}$.

- Step 3: In this step, $A_{i\oplus 1}$ $(i=1,2,\cdots,n)$ utilizes the decoy photons to check whether the transmission of $S_1^{'(i)}$ is secure with A_i . If the error rate is limited in a predeterminded threshold, there is no eavesdropper and the protocol continues; otherwise, the protocol will be terminated.
- Step 4: Confirming that there is no eavesdropper in the channel, $A_{i\oplus 1}$ $(i=1,2,\cdots,n)$ obtains the sequences $S_1^{(i)}$ by discarding the decoy photons. Then $A_{i\oplus 1}$ chooses a random sequence $r_{i\oplus 1}=\left(r_{(i\oplus 1)1},\cdots,r_{(i\oplus 1)m}\right)\in\{0,1,\cdots,d-1\}$ and obtains

$$\bar{S}_{1}^{(i)} = \left\{ QS_{x_{(i\oplus 1)1} + r_{(i\oplus 1)1}} p_{11}^{(i)}, \cdots, QS_{x_{(i\oplus 1)m} + r_{(i\oplus 1)m}} p_{1m}^{(i)} \right\}$$

through performing the shifting operation $\left(QS_{x_{(i\oplus 1)1}+r_{(i\oplus 1)1}},\cdots,QS_{x_{(i\oplus 1)m}+r_{(i\oplus 1)m}}\right)$ on particle sequence $S_1^{(i)}$. Subsequently, $A_{i\oplus 1}$ mixes $\bar{S}_1^{(i)}$ with m decoy photons $D_j^{'(i\oplus 1)}$ $(j=1,2,\cdots,m)$ to form new sequence $\ddot{S}_1^{(i)}$ and sends it to $A_{i\oplus 2}$.

- form new sequence $\ddot{S}_{1}^{(i)}$ and sends it to $A_{i\oplus 2}$. Step 5: In this step, $A_{i\oplus 2}$ $(i=1,2,\cdots,n)$ uses the decoy photons to check whether there is an eavesdropper in the channel with $A_{i\oplus 1}$. If the error rate is limited in a predeterminded threshold, there is no eavesdropper and the protocol continues; otherwise, the protocol will be terminated.
- Step 6: After confirming that there is no eavesdropper in Step 5, A_2, \dots, A_n, A_1 obtain the particle sequences $\bar{S}_1^{(n)}, \dots, \bar{S}_1^{(n-2)}, \bar{S}_1^{(n-1)}$ by discarding the decoy photons. Then A_1 obtains the classical results $\left(x_{n1}+r_{n1}+s_{11}^{A_{n-1}}, \dots, x_{nm}+r_{nm}+s_{1m}^{A_{n-1}}\right), \quad \left(s_{21}^{A_1}, \dots, s_{2m}^{A_1}\right)$ after the $|0\rangle, \dots, |d-1\rangle$ basis measurement on sequences $\bar{S}_1^{(n-1)}$ and $S_2^{(1)}$. Subsequently, A_1 computes and publishes

$$P_{1} = (s_{11}^{A_{n-1}} + x_{n1} + r_{n1} + s_{21}^{A_{1}} + (d - x_{11}) + (d - r_{11}), \cdots, s_{1m}^{A_{n-1}} + x_{nm} + r_{nm} + s_{2m}^{A_{1}} + (d - x_{1m}) + (d - r_{1m})).$$

$$(8)$$

In the same way, A_i $(i = 2, 3, \dots, n)$ computes and publishes P_i respectively as follows:

$$P_{2} = \left(s_{11}^{A_{n}} + x_{11} + r_{11} + s_{21}^{A_{2}} + (d - x_{21}) + (d - r_{21}), \cdots, s_{1m}^{A_{n}} + x_{1m} + r_{1m} + s_{2m}^{A_{2}} + (d - x_{2m}) + (d - r_{2m})\right),$$

$$\cdots,$$

$$P_{n} = \left(s_{11}^{A_{n-2}} + x_{(n-1)1} + r_{(n-1)1} + s_{21}^{A_{n}} + (d - x_{n1}) + (d - r_{n1}), \cdots, s_{1m}^{A_{n-2}} + x_{(n-1)m} + r_{(n-1)m} + s_{2m}^{A_{n}} + (d - x_{nm}) + (d - r_{nm})\right),$$

$$(9)$$

where $s_{1j}^{A_i}$ and $s_{2j}^{A_i}$ $(i=1,2,\cdots,n;\ j=1,\cdots,m)$ represent the classical results of particles $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$ after $|0\rangle,\cdots,|d-1\rangle$ basis measurement. Here, $s_{1j}^{A_i}+s_{2j}^{A_i}=x_{ij}$. Eventually, each participant obtains the summation of their private integer strings by computing $P_1+P_2+\cdots+P_n$.

3 Security Analysis of Wu's Protocol

Because of the existence of the decoy photons, an outside attack is invalid in Wu's protocol. Conversely, the participant attack should be paid more attention, which is always more powerful referred in Ref [31]. In the following, two kinds of participant attacks on Wu's protocol are analyzed in detail. Without loss of generality, we assume that each participant A_i $(i = 1, 2, \dots, n)$ has x_i as input, where $x_i \in \{0, 1, \dots, d-1\}$ and d = n - 1.

The Collusive Attack from Two Dishonest Participants Suppose that A_1 and A_3 are the dishonest participants, who work together to obtain A_2 's private information x_2 . Following the protocol, the computation results P_i $(i = 1, 2, \dots, n)$ from each participant A_i in Step 6 are available as follows.

$$P_{1} = s_{1}^{A_{n-1}} + x_{n} + r_{n} + s_{2}^{A_{1}} + (d - x_{1}) + (d - r_{1}),$$

$$P_{2} = s_{1}^{A_{n}} + x_{1} + r_{1} + s_{2}^{A_{2}} + (d - x_{2}) + (d - r_{2}),$$

$$P_{3} = s_{1}^{A_{1}} + x_{2} + r_{2} + s_{2}^{A_{3}} + (d - x_{3}) + (d - r_{3}),$$

$$P_{4} = s_{1}^{A_{2}} + x_{3} + r_{3} + s_{2}^{A_{4}} + (d - x_{4}) + (d - r_{4}),$$

$$\cdots,$$

$$P_{n} = s_{1}^{A_{n-2}} + x_{n-1} + r_{n-1} + s_{2}^{A_{n}} + (d - x_{n}) + (d - r_{n}).$$

$$(10)$$

Firstly, A_1 makes the first particle of his own d-dimensional Bell state collapse into $s_1^{A_1}$ by performing the $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ basis measurement in Step 1, and announces $s_1^{A_1}$ to A_3 . In Step 4, A_3 and A_1 obtain $s_1^{A_2}$ and $s_1^{A_n}$, respectively, after the $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ basis measurement on the particles sent from A_2 and A_n , and then A_3 tells $s_1^{A_2}$ to A_1 . Hereafter, A_3 obtains $(s_1^{A_1} + x_2 + r_2)$ after the $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ basis measurement on the particle sent from A_2 in Step 6. Then,

 A_3 gets the result of x_2+r_2 by computing $\left(s_1^{A_1}+x_2+r_2\right)-s_1^{A_1}$, and announces the result to A_1 . Finally, A_1 obtains $s_2^{A_2}$ by calculating $P_2-\left(s_1^{A_n}+x_1+r_1\right)+\left(x_2+r_2\right)$ in Step 6, and he can learn about A_2 's private input x_2 , where $x_2=s_1^{A_2}+s_2^{A_2}$. Clearly, A_i $(i=1,2,\cdots,n)$ can easily extract $A_{i\oplus 1}$'s secret information conspiring with $A_{i\oplus 2}$ without being detected when $n\geq 4$.

The Collusive Attack from Four Dishonest Participants In this kind of attack, no particle is measured to collapse until the measurement in Step 6. Here, we suppose that A_1, A_3, A_4 and A_n are the dishonest participants, who work together to launch active attack to acquire A_2 's secret input x_2 . Firstly, A_1, A_3, A_4 and A_n perform the $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis measurement on the particles remained in their own hands and record the measurement result respectively in Step 6. After that, $A_1(A_n)$ announces $s_1^{A_1}(s_1^{A_n})$ to $A_3(A_1)$ according to their measurement results in the above and their secret information, i.e., $s_1^{A_1} = x_1 - s_2^{A_1} \left(s_1^{A_n} = x_n - s_2^{A_n} \right)$. Afterward, A_3 obtains the value of $x_2 + r_2$ by computing $P_3 - s_1^{A_1} - s_2^{A_3} + (x_3 + r_3)$, and announces it to A_1 . Meanwhile, A_3 announces the value of $x_3 + r_3$ to A_4 . A_1 then obtains the value of $s_2^{A_2}$ by computing $P_2 - s_1^{A_n} - (x_1 + r_1) + (x_2 + r_2)$ and A_4 obtains the value of $s_1^{A_2}$ by computing $P_4 - (x_3 + r_3) - s_2^{A_4} + (x_4 + r_4)$, and announces it to A_1 . Eventually, A_1 obtains the value of x_2 by computing $s_1^{A_2} + s_2^{A_2}$. It is easy to verify that $a_1, a_{1\oplus 1}, a_{1\oplus 3}$ and $a_{1\oplus 4}$ ($i=1,2,\cdots,n$) can work together to extract $a_{1\oplus 2}$'s secret information without being detected when $n \geq 6$.

4 The Improved Protocols

Detailed security analysis in the previous section reveals that Wu's protocol [29] has insufficient random numbers for encryption, and lacks detection mechanism to check whether the particles are measured collapsed during the transmission. In this section, the improved protocols are proposed to make Wu's protocol secure and they also remove the secret input encoding operated by each participant in Wu's protocol. The assumptions of the improved protocols are the same as that of Wu's protocol. The detailed revised protocols are as follows.

4.1 Three-party protocol

Compared with Wu's protocol, the improved three-party protocol removes the process to encode secret information and random numbers, and reduces the number of times that particles are transmitted in the channel.

4.1.1 Scheme Description

Step 1: A_i (i = 1, 2, 3) prepares the quantum initial state

$$S^{(i)} = \left\{ \left| \varphi_1^{(i)} \right\rangle, \left| \varphi_2^{(i)} \right\rangle, \cdots, \left| \varphi_m^{(i)} \right\rangle \right\},$$

according to her secret message x_i as same as (5), where '0' is $|\varphi(0,0)\rangle$ and '1' is $|\varphi(0,1)\rangle$. Then A_i splits $S^{(i)}$ into two particle sequences

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

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

where $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$ $(j=1,2,\cdots,m)$ represent the first and the second particle of each state in $S^{(i)}$ respectively. After that, A_i (i=1,2,3) inserts m decoy photons $D_j^{(i)}$, which is randomly in $\{|r\rangle, F|r\rangle \mid r \in \{0,1\}\}$, into $S_1^{(i)}$ to form a new sequence $S_1^{'(i)}$, Then A_1 (A_2, A_3) sends $S_1^{'(1)}$ $(S_1^{'(2)}, S_1^{'(3)})$ to A_2 (A_3, A_1) and keeps $S_2^{(1)}$ $(S_2^{(2)}, S_2^{(3)})$ in hand.

- Step 2: In this step, A_1 (A_2 , A_3) utilizes the decoy photons to check whether the transmission of $S_1^{'(1)}$ ($S_1^{'(2)}$, $S_1^{'(3)}$) is secure with A_2 (A_3 , A_1). If the error rate is higher than the predeterminded threshold, they will abort the protocol and restart from Step 1; otherwise, they will proceed to the next step.
- restart from Step 1; otherwise, they will proceed to the next step. Step 3: A_2 (A_3 , A_1) restores $S_1^{(1)}$ ($S_1^{(2)}$, $S_1^{(3)}$) by discarding the decoy photons. Then A_1 obtains the classical results ($s_{11}^{A_3}, s_{12}^{A_3}, \cdots, s_{1m}^{A_3}$), ($s_{21}^{A_1}, s_{21}^{A_2}, \cdots, s_{2m}^{A_1}$) after performing the $\{|0\rangle, |1\rangle\}$ basis measurement on $S_1^{(3)}$ and $S_2^{(1)}$. A_1 computes and publishes the value of $P_1 = \left(s_{11}^{A_3} + s_{21}^{A_1}, s_{12}^{A_3} + s_{22}^{A_1}, \cdots, s_{1m}^{A_m} + s_{2m}^{A_1}\right)$. In the same way, A_2 computes and publishes the results $P_2 = \left(s_{11}^{A_1} + s_{21}^{A_2}, s_{12}^{A_1} + s_{22}^{A_2}, \cdots, s_{1m}^{A_1} + s_{2m}^{A_2}\right)$. A_3 computes and publishes the results $P_3 = \left(s_{11}^{A_2} + s_{22}^{A_3}, \cdots, s_{1m}^{A_1} + s_{2m}^{A_2}\right)$, where $s_{1j}^{A_i} + s_{2j}^{A_i} = x_{ij}$ (i = 1, 2, 3; $j = 1, 2, \cdots, m$).
- Step 4: A_1, A_2, A_3 can obtain the summation of each participant's input by computing $P_1 + P_2 + P_3$ without their own secret information leaking out.

4.1.2 Correctness

The target of each participant in the proposed three-party summation protocol is to obtain the value of $x_1 + x_2 + x_3$ through computing $P_1 + P_2 + P_3$. In this section, the detail proof is presented.

 A_1, A_2, A_3 agree with the encoding rule in Step 1 beforehand. In Step 3, A_1, A_2, A_3 compute and announce the results as follows:

$$P_{1} = \left(s_{11}^{A_{3}} + s_{21}^{A_{1}}, s_{12}^{A_{3}} + s_{22}^{A_{1}}, \cdots, s_{1m}^{A_{3}} + s_{2m}^{A_{1}}\right),$$

$$P_{2} = \left(s_{11}^{A_{1}} + s_{21}^{A_{2}}, s_{12}^{A_{1}} + s_{22}^{A_{2}}, \cdots, s_{1m}^{A_{1}} + s_{2m}^{A_{2}}\right),$$

$$P_{3} = \left(s_{11}^{A_{2}} + s_{21}^{A_{3}}, s_{12}^{A_{2}} + s_{22}^{A_{3}}, \cdots, s_{1m}^{A_{2}} + s_{2m}^{A_{3}}\right),$$

$$(11)$$

where $s_{1j}^{A_i}$ and $s_{2j}^{A_i}$ $(i=1,2,3;\ j=1,2,\cdots,m)$ denote the classical information after the $\{|0\rangle,|1\rangle\}$ basis measurement on $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$, and $s_{1j}^{A_i}+s_{2j}^{A_i}=x_{ij}$. As a result, we have

$$P_{1} + P_{2} + P_{3} = \left(s_{11}^{A_{3}} + s_{21}^{A_{1}} + s_{11}^{A_{1}} + s_{21}^{A_{2}} + s_{11}^{A_{2}} + s_{21}^{A_{3}}, s_{12}^{A_{3}} + s_{22}^{A_{1}} + s_{12}^{A_{1}} + s_{22}^{A_{2}} + s_{12}^{A_{2}} + s_{12}^{A_{2}$$

computed by all participants in Step 4 which is the summation of the participants' inputs.

4.1.3 Security Analysis

The improved protocol is still secure against all kinds of outside attacks since the existence of decoy photons. Consequently, the security against the participant attacks in the protocol should be analyzed in detail. Obviously, any two dishonest participants can gain the honest one's secret input in this three-party protocol. Thus, the case where only one dishonest participant launches attacks is considered.

In the three-party protocol, the role of each party is identical. Without loss of generality, A_2 is assumed to be the dishonest participant who attempts to obtain A_1 's and A_3 's inputs. To this end, A_2 has to learn about the values of $s_{1j}^{A_1} + s_{2j}^{A_1}$ and $s_{1j}^{A_3} + s_{2j}^{A_3}$ ($j = 1, 2, \dots, m$). A_2 can get $s_{1j}^{A_2}$ and $s_{2j}^{A_2}$ by performing the $\{|0\rangle, |1\rangle\}$ basis measurement on $p_{1j}^{(2)}$ and $p_{2j}^{(2)}$, respectively, in Step 1. In Step 3, A_2 extracts the values of $s_{1j}^{A_1}$ and $s_{2j}^{A_3}$ after A_1 and A_3 announced P_1 and P_3 , respectively, according to Eq.(11). However, A_2 can not learn about the exact values of $s_{2j}^{A_1}$ and $s_{1j}^{A_3}$ from P_1 published by A_1 . Hence, the participant attack is invalid in the improved protocol.

4.2 Four or Five-party Protocol

In the improved four or five-party protocol, besides removing the process of secret information encoding operated by each participant, we take advantage of detection mechanism to detect dishonest participants. What's more, there is no longer any need for decoy photons in the following improved protocol.

4.2.1 Scheme Description

Step 1: A_i $(i=1,2,\cdots,n \text{ and } n=4 \text{ or } n=5)$ changes secret information $x_i=(x_{i1},x_{i2},\cdots,x_{im})$ into $\overline{x_i}=\left(x_{i1}',x_{i2}',\cdots,x_{i(2m)}'\right)$, where $x_{i(2j-1)}'+x_{i(2j)}'=x_{ij}$ and $x_{i(2j-1)}',x_{i(2j)}'\in\{0,1,\cdots,d-1\}$ $(j=1,2,\cdots,m;\ d=n-1)$. Later, A_i encodes $\overline{x_i}$ according to Eq.(6) and prepares the initial states as

$$S^{(i)} = \left\{ \left| \varphi_1^{(i)} \right\rangle, \left| \varphi_2^{(i)} \right\rangle, \cdots, \left| \varphi_{2m}^{(i)} \right\rangle \right\},\,$$

where $\left|\varphi_k^{(i)}\right>=\left|\varphi(0,x_{ik}')\right>$ $(k=1,2,\cdots,2m).$ Then, A_i divides $S^{(i)}$ into particle sequences

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

where $p_{1k}^{(i)}$ and $p_{2k}^{(i)}$ indicate the first and the second particle of each state in $S^{(i)}$ respectively, and sends $S_1^{(i)}$ to $A_{i\oplus 1}$, remaining $S_2^{(i)}$ in her hand.

Step 2: Upon receiving $S_1^{(i)}$ $(i=1,2,\cdots,n)$ from $A_i,\ A_{i\oplus 1}$ selects a group of random sequence $r_{i\oplus 1}=\left(r_{(i\oplus 1)1},r_{(i\oplus 1)2},\cdots,r_{(i\oplus 1)2m}\right)\in\{0,1,\cdots,d-1\}$. Then, $A_{i\oplus 1}$ obtains

$$\bar{S}_{1}^{(i)} = \left\{ QS_{r_{(i \oplus 1)1}} p_{11}^{(i)}, QS_{r_{(i \oplus 1)2}} p_{12}^{(i)}, \cdots, QS_{r_{(i \oplus 1)2m}} p_{1(2m)}^{(i)} \right\}$$

by performing the shifting operation $(QS_{r_{(i\oplus 1)1}},QS_{r_{(i\oplus 1)2}},\cdots,QS_{r_{(i\oplus 1)2m}})$ on $S_1^{(i)}$ and sends $\bar{S}_1^{(i)}$ to $A_{i\oplus 2}$.

- Step 3: After receiving $\bar{S}_1^{(1)}$ ($\bar{S}_1^{(2)}$,..., $\bar{S}_1^{(n-1)}$, $\bar{S}_1^{(n)}$) from A_2 (A_3 ,..., A_n , A_1), A_3 (A_4 ,..., A_1 , A_2) sends the ACK signal to A_1 (A_2 ,..., A_{n-1} , A_n). Confirming that all participants have received ACK signals, A_1 selects t particles in $S_2^{(1)}$ as checking qudits, denoted as $T^{(1)}$, in which any two particles should not be both $p_{2(2k-1)}^{(1)}$ and $p_{2(2k)}^{(1)}$ ($k=1,2,\cdots,m$) in $S_2^{(1)}$. Note that $T^{(1)} = \left\{p_{2T_1}^{(1)},\cdots,p_{2T_t}^{(1)}\right\}$ and $T_j^1 \in \{1,2,\cdots,2m\}$ ($j=1,2,\cdots,t$). Then, A_1 sends $T^{(1)}$ to A_3 , and announces the positions of $T^{(1)}$ in $S_2^{(1)}$. Thereafter, A_2 selects t particles in $S_2^{(2)}$, denoted as $T^{(2)}$, according to the positions of $T^{(1)}$ in $S_2^{(1)}$ published by A_1 in the following way: (1) if A_1 takes the (2k-1)-th particle in $S_2^{(1)}$ as the checking qudit, A_2 should not take her 2k-th particle in $S_2^{(2)}$ as the checking qudit; (2) if A_1 takes the 2k-th particle in $S_2^{(1)}$ as the checking qudit, where $T^{(2)} = \left\{p_{2T_1}^{(2)},\cdots,p_{2T_t}^{(2)}\right\}$ and $T_j^2 \in \{1,2,\cdots,2m\}$ ($j=1,2,\cdots,t$). Besides, any two particles in $T^{(2)}$ also should not be both $T^{(2)}$ and $T^{(2)}$ in $T^{(2)}$. Subsequently, according to the same way as $T^{(2)}$ and $T^{(2)}$ in $T^{(2)}$ in order, and send $T^{(3)}$,..., $T^{(n)}$ with their positions in $T^{(2)}$,..., $T^{(n)}$ in order, and send $T^{(3)}$,..., $T^{(n)}$ with their positions in $T^{(2)}$,..., $T^{(n)}$ in order, $T^{(n)}$, where $T^{(n)}$ in the positions in $T^{(n)}$, in order, $T^{(n)}$, where $T^{(n)}$ in the here $T^{(n)}$, and $T^{(n)}$ in order, and send $T^{(n)}$, and $T^{(n)}$ in the following to the same way as $T^{(n)}$ and $T^{(n)}$ in $T^{(n)}$ in the following to the same way as $T^{(n)}$ in the following takes the checking qudit, $T^{$
- Step 4: In this Step, $A_{i\oplus 1}$ $(i=1,2,\cdots,n)$ needs to divulge the values of $(r_{(i\oplus 1)T_1^1},\cdots,r_{(i\oplus 1)T_1^1})$ after $A_{i\oplus 2}$ receiving $T^{(i)}$ with its position in $S_2^{(i)}$. Then, $A_{i\oplus 2}$ performs d-dimensional Bell measurement on particle pairs $(p_{1T_i^i}^{(i)'},p_{2T_i^i}^{(i)})$, and announces the measurement results to A_i , where $p_{1T_i^i}^{(i)'}=$

- $QS_{r_{(i\oplus 1)T^i_j}}p_{1T^i_j}^{(i)}$ $(j=1,2,\cdots,t)$. A_i checks whether the measurement results announced by $A_{i\oplus 2}$ are consistent with $\left|\varphi\left(0,x'_{iT^1_j}+r_{(i\oplus 1)T^1_j}\right)\right\rangle$. If the error rate surpasses the predefined threshold, the protocol will be aborted; otherwise, the protocol continues.
- Step 5: Confirming that there is no malicious participant in Step 4, $A_{i\oplus 2}$ $(i=1,2,\cdots,n)$ informs the measurement results to A_i after the $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ basis measurement on $T^{(i)}$. Thereafter, A_1 obtains the sequence of classical results $\left(s_{11}^{A_{n-1}}+r_{n1},\cdots,s_{1(2m)}^{A_{n-1}}+r_{n(2m)}\right)$, $\left(s_{21}^{A_1},\cdots,s_{2(2m)}^{A_1}\right)$ through performing the $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ basis measurements on $\bar{S}_1^{(n-1)}$ and $S_2^{(1)}$. Then, A_1 computes and publishes

$$P_{1} = \left(s_{11}^{A_{n-1}} + r_{n1} + s_{21}^{A_{1}} + (d - r_{11}), \cdots, s_{1(2m)}^{A_{n-1}} + r_{n(2m)} + s_{2(2m)}^{A_{1}} + (d - r_{1(2m)})\right). \tag{12}$$

In the same way, A_i $(i=2,\cdots,n)$ compute and publish the following results:

$$P_{2} = \left(s_{11}^{A_{n}} + r_{11} + s_{21}^{A_{2}} + (d - r_{21}), \cdots, s_{1(2m)}^{A_{n}} + r_{1(2m)} + s_{2(2m)}^{A_{2}} + (d - r_{2(2m)})\right),$$

$$\cdots,$$

$$P_{n} = \left(s_{11}^{A_{n-2}} + r_{(n-1)1} + s_{21}^{A_{n}} + (d - r_{n1}), \cdots, s_{1(2m)}^{A_{n-2}} + r_{(n-1)2m} + s_{2(2m)}^{A_{n}} + (d - r_{n(2m)})\right).$$

$$(13)$$

Step 6: A_1, \dots, A_n compute $P_1 + P_2 + \dots + P_n = (T_1, \dots, T_{2m})$, where $(T_1 + T_2, T_3 + T_4, \dots, T_{2m-1} + T_{2m})$ is the summation of each participant's secret input.

4.2.2 Correctness

In Step 6 of the above protocol, A_1, A_2, \dots, A_n (n = 4 or 5), according to Eq.(12,13), calculate the value of

$$P_{1} + P_{2} + \dots + P_{n} = \left(s_{11}^{A_{n-1}} + r_{n1} + s_{21}^{A_{1}} + (d - r_{11}) + s_{11}^{A_{n}} + r_{11} + s_{21}^{A_{2}} + (d - r_{21})\right) + \dots + s_{11}^{A_{n-2}} + r_{(n-1)1} + s_{21}^{A_{n}} + (d - r_{n1}), \dots,$$

$$s_{1(2m)}^{A_{n-1}} + r_{n(2m)} + s_{2(2m)}^{A_{1}} + (d - r_{1(2m)}) + s_{1(2m)}^{A_{n}} + r_{1(2m)} + s_{2(2m)}^{A_{2}} + (d - r_{2(2m)}) + \dots + s_{1(2m)}^{A_{n-2}} + r_{(n-1)2m} + s_{2(2m)}^{A_{n}} + (d - r_{n(2m)})\right)$$

$$= \left(x'_{11} + x'_{21} + \dots + x'_{n1}, \dots, x'_{1(2m)} + x'_{2(2m)} + \dots + x'_{n(2m)}\right),$$

$$(14)$$

where
$$x'_{i(2j-1)} + x'_{i(2j)} = x_{ij}$$
 $(i = 1, 2, \cdots, n; j = 1, 2, \cdots, m)$ and $\left((x'_{11} + x'_{21} + \cdots + x'_{n1}) + (x'_{12} + x'_{22} + \cdots + x'_{n2}), \cdots, (x'_{1(2m-1)} + x'_{2(2m-1)} + \cdots + x'_{n(2m-1)}) + (x'_{1(2m)} + x'_{2(2m)} + \cdots + x'_{n(2m)})\right)$ is the summation of all participants' inputs and the correctness of the improved protocol guaranteed.

4.2.3 Security Analysis

In this section, it is first shown that the improved protocol is immune to the collusive attack from two participants referred in Sect.3. Without loss of generality, A_1, A_3 are assumed to be the dishonest participants, aiming to obtain A_2 's secret input. To this end, A_3 has to perform the $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis measurement on particle $p_{1j}^{(2)}$ to obtain $s_{1j}^{A_2}$ $(j=1,2,\cdots,2m)$, which will be detected with the probability of $\frac{t}{2m}$ in Step 4. Further, if an outside eavesdropper launches active attacks on the particle transmitted in the channel, he will be also detected with the same probability in Step 4.

In the case of the collusive attack from n-2 participants, except for A_k and A_l $(k,l\in\{1,2,\cdots,n\}$ and k< l), the remaining n-2 participants are assumed to be attackers. If l=k+2 or l=k+n-2, according to Eq.(12,13), the remaining n-2 participants can obtain the value of $s_{1j}^{A_k}+s_{2j}^{A_l}$ in Step 5, but they can not deduce x_{kj} and x_{lj} $(j=1,2,\cdots,2m,)$ without knowing the exact values of $s_{1j}^{A_k}$ and $s_{2j}^{A_l}$. If $l\neq k+2$ and $l\neq k+n-2$, the remaining n-2 participants can obtain the values of $s_{1j}^{A_l}+r_{kj}$ or $s_{2j}^{A_l}+r_{kj}$, but they can not obtain x_{lj} without the exact value of r_{kj} . In conclusion, the improved protocol is secure against the participant attacks.

4.3 Multi-party Protocol

Based on the revised protocol described in the above section, we expand the four or five-party protocol to multi-party scenarios by slightly changing the steps. In addition to the same improvement as the protocol described above, the primary disparity

between Wu's protocol and the improved protocol in multi-party case is the increase in the number of random numbers.

4.3.1 Scheme Description

Step 1: A_i $(i = 1, 2, \dots, n \text{ and } n \ge 6)$ splits secret message $x_i = (x_{i1}, \dots, x_{im})$ into $\overline{x_i} = (x'_{i1}, x'_{i2}, \dots, x'_{i(2m)})$, where $x'_{i(2j-1)} + x'_{i(2j)} = x_{ij}$ and $x'_{i(2j-1)}, x'_{i(2j)} \in \{0, 1, \dots, d-1\}$ $(j = 1, 2, \dots, m; d = n-1)$. Then, A_i encodes $\overline{x_i}$ according to Eq.(6) and prepares the initial states as

$$S^{(i)} = \left\{ \left| \varphi_1^{(i)} \right\rangle, \left| \varphi_2^{(i)} \right\rangle, \cdots, \left| \varphi_{2m}^{(i)} \right\rangle \right\},$$

where $\left|\varphi_{k}^{(i)}\right\rangle = \left|\varphi(0, x_{ik}')\right\rangle$ $(k = 1, 2, \dots, 2m)$. Further, A_{i} divides $S^{(i)}$ into particle sequences

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

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

where $p_{1k}^{(i)}$ and $p_{2k}^{(i)}$ represent the first and the second particle of each Bell state in $S^{(i)}$ respectively. After that, A_i prepares $\lambda - 1$ ($\lambda = \left\lfloor \frac{n}{2} \right\rfloor$) groups of random sequences $r_i^g = \left(r_{i1}^g, r_{i2}^g, \cdots, r_{i(2m)}^g\right) \in \{0, 1, \cdots, d-1\} \ (g = 1, 2, \cdots, \lambda - 1).$ Then, A_i obtains

$$S_1^{(i)1} = \left\{ QS_{(d-r_{i1}^1)} p_{11}^{(i)}, QS_{(d-r_{i2}^1)} p_{12}^{(i)}, \cdots, QS_{(d-r_{i(2m)}^1)} p_{1(2m)}^{(i)} \right\}$$

through performing the shifting operation $\left(QS_{(d-r_{ij}^1)}, \cdots, QS_{(d-r_{i(2m)}^1)}\right)$ on

 $S_1^{(i)}$. Afterward, A_i sends $S_1^{(i)1}$ to $A_{i\oplus 1}$ and keeps $S_2^{(i)}$ in hand. Step 2: $A_{i\oplus 1}$ $(i=1,2,\cdots,n)$ obtains $S_1^{(i)2}$ by performing the shifting operation $\left(QS_{r_{(i\oplus 1)1}^1},\cdots,QS_{r_{(i\oplus 1)2m}^1}\right)$ on sequence $S_1^{(i)1}$ after receiving $S_1^{(i)1}$, and sends $S_1^{(i)2}$ to $A_{i\oplus 2}$. $A_{i\oplus 2}, \cdots, A_{i\oplus (\lambda-1)}$ do the same as $A_{i\oplus 1}$ in turn; namely, $A_{i\oplus 2}, \cdots, A_{i\oplus (\lambda-1)}$ take turns to perform $\left(QS_{r_{(i\oplus 2)1}^2},\cdots,QS_{r_{(i\oplus 2)2m}^2}\right),\cdots,\left(QS_{r_{(i\oplus (\lambda-1))1}^{\lambda-1}},\cdots,QS_{r_{(i\oplus (\lambda-1))2m}^{\lambda-1}}\right) \text{ on the particle sequences sent by the previous participants. The specific transmission process is shown in Fig.1. Finally, <math>A_{i\oplus \lambda}$ receives $S_1^{(i)\lambda}$ from $A_{i\oplus (\lambda-1)}$, where

$$S_{1}^{(i)\lambda} = \left\{ QS_{r_{(i\oplus\lambda-1)1}^{\lambda-1}} \cdots QS_{r_{(i\oplus1)1}^{1}} QS_{(d-r_{i1}^{1})} p_{11}^{(i)}, \cdots, QS_{r_{(i\oplus\lambda-1)2m}^{\lambda-1}} \cdots QS_{r_{(i\oplus1)2m}^{1}} QS_{(d-r_{i(2m)}^{1})} p_{1(2m)}^{(i)} \right\},$$

$$(15)$$

for simplicity, denoting Eq.15 as

$$S_1^{(i)\lambda} = \{p_{11}^{(i)'}, \cdots, p_{1(2m)}^{(i)'}\}. \tag{16}$$

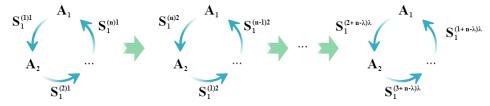


Fig. 1 The flowchart of the particle sequences transmission in the improved multi-party protocol. It's worth noting that each sequence is performed shifting operators and transported λ times in total.

Then $A_{i \oplus \lambda}$ sends ACK signal to A_i .

Step 3: After A_1, \cdots, A_n receiving ACK signals from $A_{1\oplus\lambda}, \cdots, A_{n\oplus\lambda}$, A_1 randomly selects t particles in $S_2^{(1)}$ as checking qudits, denoted as $T^{(1)}$, in which any two particles should not be both $p_{2(2k-1)}^{(1)}$ and $p_{2(2k)}^{(1)}$ in $S_2^{(1)}$, where $T^{(1)} = \left\{p_{2T_1^1}^{(1)}, \cdots, p_{2T_t^1}^{(1)}\right\}$ and $T_j^1 \in \{1, 2, \cdots, 2m\}$ $(j=1, 2, \cdots, t; \ k=1, 2, \cdots, m)$. Then, A_1 sends $T^{(1)}$ to $A_{1\oplus\lambda}$, and announces the positions of $T^{(1)}$ in $S_2^{(1)}$ publicly. Thereafter, A_2 selects t particles in $S_2^{(2)}$, denoted as $T^{(2)}$, according to the positions of $T^{(1)}$ in $S_2^{(1)}$ published by A_1 in the following way: (1) if A_1 takes the (2k-1)-th particle in $S_2^{(1)}$ as checking qudit, A_2, \cdots, A_{λ} should not take their 2k-th particles in $S_2^{(2)}, \cdots, S_2^{(\lambda)}$ as the checking qudits; (2) if A_1 takes the 2k-th particle in $S_2^{(1)}$ as the checking qudit, A_2, \cdots, A_{λ} should not take their (2k-1)-th particles in $S_2^{(2)}, \cdots, S_2^{(\lambda)}$ as the checking qudits, where $T^{(2)} = \left\{p_{2T_1^2}^{(2)}, \cdots, p_{2T_1^2}^{(2)}\right\}$ and $T_j^2 \in \{1, 2, \cdots, 2m\}$ $(j=1, 2, \cdots, t; \ k=1, 2, \cdots, m)$. Besides, any two particles in $T^{(2)}$ also shouldn't be both $T^{(2)}$ and $T^{(2)}$ in $T^{(2)}$ subsequently, $T^{(2)}$ in $T^{(2)}$ and publishes the positions of $T^{(2)}$ in $T^{(2)}$ subsequently, $T^{(2)}$ in $T^{(2)}$ and send $T^{(3)}$, $T^{(n)}$ to $T^{(n)}$ and $T^{(2)}$ subsequently, $T^{(2)}$ and $T^{(2)}$ subsequently, $T^{(2)}$ and $T^{(2)}$ and send $T^{(3)}$, $T^{(2)}$ to $T^{(2)}$ in order, according to the same rules as $T^{(2)}$ and send $T^{(3)}$, $T^{(2)}$ to $T^{(2)}$ and $T^{(2)}$ and $T^{(2)}$ and $T^{(2)}$ and send $T^{(3)}$, $T^{(n)}$ to $T^{(2)}$ and $T^{(2)}$ an

Step 4: In this Step, $A_{i\oplus 1}, \cdots, A_{i\oplus (\lambda-1)}$ (i=1,2,...,n) need to publish the values of $\left(r_{(i\oplus 1)T_1^i}^1, \cdots, r_{(i\oplus 1)T_t^i}^1\right), \cdots, \left(r_{(i\oplus \lambda-1)T_1^i}^{\lambda-1}, \cdots, r_{(i\oplus \lambda-1)T_t^i}^{\lambda-1}\right)$ respectively, where $T_j^i \in \{1,2,\cdots,2m\}$ $(j=1,2,\cdots,t)$. Then, $A_{i\oplus \lambda}$ performs d-dimensional Bell measurement on particle pairs $\left(p_{1T_j^i}^{(i)'}, p_{2T_j^i}^{(i)}\right)$ and informs the measurement results to A_i . A_i checks whether the measurement results are consistent with $\left|\varphi\left(0, x_{iT_j^i}' + (d-r_{iT_j^i}^i) + r_{(i\oplus 1)T_j^i}^1 + \cdots + r_{(i\oplus \lambda-1)T_j^i}^{\lambda-1}\right)\right\rangle$ $(j=1,2,\cdots,t)$. If the error rate is higher than the predefined threshold, A_i will abort the protocol; otherwise, the protocol continues.

Step 5: Upon confirming that there is no dishonest participant in Step 4, $A_{i \oplus \lambda}$ $(i = 1, 2, \dots, n)$ informs the measurement results after $|0\rangle, |1\rangle, \dots, |d-1\rangle$ basis measurement on $T^{(i)}$ to A_i . Then, A_1, \dots, A_n perform $|0\rangle, |1\rangle, \dots, |d-1\rangle$

basis measurements on $\left(S_1^{(1+n-\lambda)\lambda},S_2^{(1)}\right),\cdots,\left(S_1^{(n-\lambda)\lambda},S_2^{(n)}\right)$ respectively. Eventually, $A_1,...,A_n$ compute and publish the following results:

$$P_{1} = \left(s_{11}^{A_{1+n-\lambda}} + r_{(2+n-\lambda)1}^{1} + \dots + r_{n1}^{\lambda-1} + s_{21}^{A_{1}} + \left(d - r_{(1+n-\lambda)1}^{1}\right) + \sum_{g=2}^{\lambda-1} (d - r_{11}^{g}), \dots, s_{1(2m)}^{A_{1+n-\lambda}} + r_{(2+n-\lambda)2m}^{1} + \dots + r_{n(2m)}^{\lambda-1} + s_{2(2m)}^{A_{1}} + \left(d - r_{(1+n-\lambda)2m}^{1}\right) + \sum_{g=2}^{\lambda-1} \left(d - r_{1(2m)}^{g}\right)\right),$$

$$P_{2} = \left(s_{11}^{A_{2+n-\lambda}} + r_{(3+n-\lambda)1}^{1} + \dots + r_{11}^{\lambda-1} + s_{21}^{A_{2}} + \left(d - r_{(2+n-\lambda)1}^{1}\right) + \sum_{g=2}^{\lambda-1} (d - r_{21}^{g}), \dots, s_{1(2m)}^{A_{2+n-\lambda}} + r_{(3+n-\lambda)2m}^{1} + \dots + r_{1(2m)}^{\lambda-1} + s_{2(2m)}^{A_{2}} + \left(d - r_{(2+n-\lambda)2m}^{1}\right) + \sum_{g=2}^{\lambda-1} \left(d - r_{2(2m)}^{g}\right),$$

$$(17)$$

. . . ,

$$P_{n} = \left(s_{11}^{A_{n-\lambda}} + r_{(n+1-\lambda)1}^{1} + \dots + r_{(n-1)1}^{\lambda-1} + s_{21}^{A_{n}} + \left(d - r_{(n-\lambda)1}^{1}\right)\right)$$

$$+ \sum_{g=2}^{\lambda-1} (d - r_{n1}^{g}), \dots, s_{1(2m)}^{A_{n-\lambda}} + r_{(n+1-\lambda)2m}^{1} + \dots + r_{(n-1)2m}^{\lambda-1}$$

$$+ s_{2(2m)}^{A_{n}} + \left(d - r_{(n-\lambda)2m}^{1}\right) + \sum_{g=2}^{\lambda-1} \left(d - r_{n(2m)}^{g}\right)\right)$$

where $s_{1j}^{A_i}$ and $s_{2j}^{A_i}$ $(i=1,2,\cdots,n;\ j=1,2,\cdots,2m)$ present the classical results of particles $p_{1j}^{(i)}$ and $p_{2j}^{(i)}$ after $|0\rangle,\cdots,|d-1\rangle$ basis measurement. Step 6: All participants compute $P_1+P_2+\cdots+P_n=(T_1,\cdots,T_{2m})$, where

Step 6: All participants compute $P_1 + P_2 + \cdots + P_n = (T_1, \cdots, T_{2m})$, where $(T_1 + T_2, T_3 + T_4, \cdots, T_{2m-1} + T_{2m})$ is the summation of the participants' inputs.

4.3.2 Correctness

Similar to the analysis in the Sect.4.2.2, A_1, A_2, \dots, A_n $(n \ge 6)$ obtain the value of Eq.(17) and compute

$$P_{1} + \dots + P_{n} = \left(s_{11}^{A_{1+n-\lambda}} + r_{(2+n-\lambda)1}^{1} + \dots + r_{n1}^{\lambda-1} + s_{21}^{A_{1}} + \left(d - r_{(1+n-\lambda)1}^{1}\right)\right)$$

$$+ \sum_{g=2}^{\lambda-1} (d - r_{11}^{g}) + \dots + s_{11}^{A_{n-\lambda}} + r_{(n+1-\lambda)1}^{1} + \dots + r_{(n-1)1}^{\lambda-1}$$

$$+ s_{21}^{A_{n}} + \left(d - r_{(n-\lambda)1}^{1}\right) + \sum_{g=2}^{\lambda-1} (d - r_{n1}^{g}), \dots, s_{1(2m)}^{A_{1+n-\lambda}}$$

$$+ r_{(2+n-\lambda)2m}^{1} + \dots + r_{n(2m)}^{\lambda-1} + s_{2(2m)}^{A_{1}} + \left(d - r_{(1+n-\lambda)2m}^{1}\right)$$

$$+ \sum_{g=2}^{\lambda-1} \left(d - r_{1(2m)}^{g}\right) + \dots + s_{1(2m)}^{A_{n-\lambda}} + r_{(n+1-\lambda)2m}^{1} + \dots$$

$$+ r_{(n-1)2m}^{\lambda-1} + s_{2(2m)}^{A_{n}} + \left(d - r_{(n-\lambda)2m}^{1}\right) + \sum_{g=2}^{\lambda-1} \left(d - r_{n(2m)}^{g}\right)\right)$$

$$= \left(x_{11}' + \dots + x_{n1}', \dots, x_{1(2m)}' + \dots + x_{n(2m)}'\right),$$

$$(18)$$

where $x'_{i(2j-1)} + x'_{i(2j)} = x_{ij}$ $(i = 1, 2, \dots, n; j = 1, 2, \dots, m)$, and $\left((x'_{11} + \dots + x'_{n1}) + (x'_{12} + \dots + x_{n2})', \dots, \left(x'_{1(2m-1)} + \dots + x'_{n(2m-1)}\right) + \left(x'_{1(2m)} + \dots + x'_{n(2m)}\right)\right)$ is the summation of all participants' inputs.

4.3.3 Security Analysis

The collusive attack from two participants referred in Sect.3 and the outside attack is invalid for the improved protocol, whose analysis is similar to Sect.4.2.3. For the collusive attack from n-2 participants, except for A_k and A_l $(k,l=1,2,\cdots,n$ and k < l), we also suppose the remaining n-2 parties as the dishonest participants. If $l=k+\lambda$ or $l=k+n-\lambda$, the remaining n-2 parties can get the value of $s_{1j}^{A_k}+s_{2j}^{A_l}$ in Step 5, but they can't obtain x_{kj} and x_{lj} $(j=1,2,\cdots,2m)$ since loss of the exact value of $s_{1j}^{A_k}$ and $s_{2j}^{A_l}$. If $l \neq k+\lambda$ and $l \neq k+n-\lambda$, the remaining parties can obtain the value of $s_{1j}^{A_l}+r_{kj}$ or $s_{2j}^{A_l}+r_{kj}$, but they also can't restore x_{lj} since loss of the knowledge of r_{kj} . Consequently, any n-2 participants have no chance to reap the remaining two parties' secret inputs and the security of the improved protocol can be guaranteed.

5 Discussion and Conclusion

In the improved protocol proposed in this paper, we have not only addressed the security vulnerabilities present in Wu's protocol, but also improved the efficiency. The comparison results on efficiency are showed as follows. Here, the qubit efficiency is defined beforehand 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. In the multi-party improved protocol, 4mn particles are used for encoding. Participants need to publish $(\lambda-1)nt$ classical bits in Step 4, and announce 2mn classical bits in Step 5. Accordingly, the qubit efficiency is $\eta = \frac{2m}{\left((\lambda-1)t+2m\right)n}$, when t is small enough, excellent efficiency can be achieved.

In conclusion, in this paper, improved protocols based on d-dimensional Bell states is proposed, whose security is verified in detail, guaranteed that it can resist both outside attack and participant attack. In addition, the improved protocol removes the decoy photons technology to detect eavesdropper, replaced by the method that checks whether the particles are collapsed during the transmission in Step 4 of the improved four or five-party protocol and the improved multi-party protocol.

Acknowledgments. This work was supported by the Guangdong Basic and Applied Basic Research Foundation (Grant Nos. 2021A1515011985, 2022A1515140116) and the National Natural Science Foundation of China (Grant No. 61902132).

References

- [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, pp. 175–179 (1984)
- [2] Liu, Z.-R., Hwang, T.: Mediated semi quantum key distribution without invoking quantum measurement. ANNALEN DER PHYSIK **530**(4), 9 (2018) https://doi.org/10.1002/andp.201700206
- [3] Yang, C.-W.: Encryption chain based on measurement result and its applications on semi-quantum key distribution protocol. SCIENTIFIC REPORTS 12(1), 12 (2022) https://doi.org/10.1038/s41598-022-23135-7
- [4] Chen, Y., Ye, T.-Y.: Semiquantum secret sharing by using x-type states. The European Physical Journal Plus ${\bf 137}(12)$ (2022) https://doi.org/10.1140/epjp/s13360-022-03521-w
- [5] Qin, H., Tso, R., Dai, Y.: Multi-dimensional quantum state sharing based on quantum fourier transform. QUANTUM INFORMATION PROCESSING 17(3), 12 (2018) https://doi.org/10.1007/s11128-018-1827-8

- [6] Guo, F.Z., Gao, F., Qin, S.J., Zhang, J., Wen, Q.Y.: Quantum private comparison protocol based on entanglement swapping of d-level bell states. Quantum Information Processing 12(8), 2793–2802 (2013) https://doi.org/10.1007/s11128-013-0536-6
- [7] Lian, J.-Y., Li, X., Ye, T.-Y.: Multi-party semiquantum private comparison of size relationship with d-dimensional bell states. EPJ Quantum Technology **10**(1) (2023) https://doi.org/10.1140/epjqt/s40507-023-00167-0
- [8] Shi, R.-h., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Scientific Reports 6(1) (2016) https://doi.org/10.1038/srep19655
- [9] Ye, T.-Y., Hu, J.-L.: Multi-party quantum private comparison based on entanglement swapping of bell entangled states within d-level quantum system. International Journal of Theoretical Physics 60(4), 1471–1480 (2021) https://doi.org/10.1007/s10773-021-04771-7
- [10] Ye, T.-Y., Hu, J.-L.: Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. International Journal of Theoretical Physics 60(3), 819–827 (2021) https://doi.org/10.1007/ s10773-020-04700-0
- [11] A., C.Y.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), pp. 160–164 (1982)
- [12] P., W.S.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994)
- [13] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212–219 (1996)
- [14] Huang, W., Wen, Q.-Y., Liu, B., Su, Q., Qin, S.-J., Gao, F.: Quantum anonymous ranking. PHYSICAL REVIEW A 89(3), 13 (2014) https://doi.org/10.1103/PhysRevA.89.032325
- [15] Lin, S., Guo, G.-D., Huang, F., Liu, X.-F.: Quantum anonymous ranking based on the chinese remainder theorem. PHYSICAL REVIEW A 93(1), 9 (2016) https://doi.org/10.1103/PhysRevA.93.012318
- [16] Sun, Z., Yu, J., Wang, P., Xu, L., Wu, C.: Quantum private comparison with a malicious third party. Quantum Information Processing 14(6), 2125–2133 (2015) https://doi.org/10.1007/s11128-015-0956-6

- [17] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., Zhu, M.Y.: Tools for privacy preserving distributed data mining. ACM SIGKDD Explorations Newsletter 4(2), 28–34 (2002) https://doi.org/10.1145/772862.772867
- [18] Heinrich, S.: Quantum summation with an application to integration. Journal of Complexity **18**(1), 1–50 (2002) https://doi.org/10.1006/jcom.2001.0629
- [19] Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. PHYSICAL REVIEW A **75**(1), 8 (2007) https://doi.org/10.1103/PhysRevA.75.012333
- [20] Wu, W.-Q., Xie, M.-Z.: Quantum secure multi-party summation using single photons. ENTROPY **25**(4), 18 (2023) https://doi.org/10.3390/e25040590
- [21] Hu, J.-L., Ye, T.-Y.: Three-party secure semiquantum summation without entanglement among quantum user and classical users. International Journal of Theoretical Physics **61**(6), 170 (2022) https://doi.org/10.1007/s10773-022-05158-y
- [22] Ye, T.-Y., Xu, T.-J.: A lightweight three-user secure quantum summation protocol without a third party based on single-particle states. Quantum Information Processing 21(9), 309 (2022) https://doi.org/10.1007/s11128-022-03652-0
- [23] Zhang, C., Razavi, M., Sun, Z., Huang, Q., Situ, H.: Multi-party quantum summation based on quantum teleportation. ENTROPY 21(7), 16 (2019) https://doi.org/10.3390/e21070719
- [24] Ji, Z., Zhang, H., Wang, H., Wu, F., Jia, J., Wu, W.: Quantum protocols for secure multi-party summation. Quantum Information Processing 18(6), 168 (2019) https://doi.org/10.1007/s11128-018-2141-1
- [25] Zhi-Gang, G.: Improvement of quantum protocols for secure multi-party summation. International Journal of Theoretical Physics **59**(10), 3086–3092 (2020) https://doi.org/10.1007/s10773-020-04555-5
- [26] Zhang, C., Long, Y., Li, Q.: Quantum summation using d-level entanglement swapping. Quantum Information Processing 20(4) (2021) https://doi.org/10. 1007/s11128-021-03072-6
- [27] Wang, Y., Hu, P., Xu, Q.: Quantum secure multi-party summation based on entanglement swapping. Quantum Information Processing **20**(10) (2021) https://doi.org/10.1007/s11128-021-03262-2
- [28] Yang, H.-Y., Ye, T.-Y.: Secure multi-party quantum summation based on quantum fourier transform. Quantum Information Processing 17(6), 129 (2018) https://doi.org/10.1007/s11128-018-1890-1
- [29] Wu, W., Ma, X.: Multi-party quantum summation without a third party based

- on d-dimensional bell states. Quantum Information Processing $\bf 20(6),\,200$ (2021) https://doi.org/10.1007/s11128-021-03142-9
- [30] Liu, B., Xiao, D., Jia, H.-Y., Liu, R.-Z.: Collusive attacks to "circle-type" multiparty quantum key agreement protocols. Quantum Information Processing $\bf 15(5)$, 2113-2124 (2016) https://doi.org/10.1007/s11128-016-1264-5
- [31] Gao, F., Qin, S.J., Wen, Q.Y.: A simple participant attack on the bradler-dusek protocol. QUANTUM INFORMATION & COMPUTATION **7**(4), 329–334 (2007)