Quantum Information Processing (2022) 21:285
https://doi.org/10.1007/s11128-022-03638-y

Cryptanalysis of secure multiparty quantum summation

Xiao-Qiu Cai[1,2,3] · **Tian-Yin Wang**[2,3] · **Chun-Yan Wei**[1,2,3] · **Fei Gao**[1]

Received: 11 January 2022 / Accepted: 24 July 2022 / Published online: 13 August 2022

Abstract

Secure multiparty summation plays an important role in the field of secure communication. In this paper, we give a cryptanalysis of a generalized quantum protocol for secure multiparty summation and find a security leak, whereby a dishonest player can steal all the other players' shares and the summation of secrets without being found, which is in conflict with the security requirement for secure multiparty summation. Furthermore, we analyze the reason and present an improved version to deal with the security problem.

Keywords Secure multiparty computation · Secure multiparty summation · Participant attack · Secure multiparty quantum computation · Secure multiparty quantum summation.

1 Introduction

Secure multiparty computation is a fundamental cryptographic primitive, which allows n $(n \geq 3)$ participants to cooperatively compute a function value with their private inputs while keeping the privacy of their respective inputs [1]. Due to the speciality, secure multiparty computation has many applications such as private auctions, e-election, anonymous ranking and anonymous communication [2–10].

As a special case of secure multiparty computation, secure multiparty summation can enable n participants to jointly calculate a summation function $f(x_1, x_2, \ldots, x_n)$

✉ Tian-Yin Wang
wangtianyin79@163.com

Fei Gao
gaof@bupt.edu.cn

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] School of Mathematical Science, Luoyang Normal University, Luoyang 471934, China

[3] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China

without revealing any participant's secret x_i to the others for $i = 1, 2, \ldots, n$. Secure multiparty summation not only can be used to construct other secure multiparty computation protocols but also plays an important role in secret sharing, e-voting, and data mining, etc. [11, 12].

However, the security of classical secure multiparty summation protocols is generally based on the computation complexity assumption. With the fast development of quantum computing, it becomes more and more possible to break through them [13, 14]. Consequently, the concept of secure multiparty quantum summation was introduced in 2007 [15], whose security is based on the basic principles of quantum mechanics. Contributing to the superiority of information-theoretical security, secure multiparty quantum summation attracted much attention and various proposals were presented [16–24].

Recently, a novel secure multiparty quantum summation protocol (named SO-protocol hereafter) was reported by using linear secret sharing (LSS) and quantum Fourier transform (QFT), which reduces both the communication and computation complexity [25]. Furthermore, it is more flexible and practical compared with the existing protocols.

As we know, cryptographic design and cryptanalysis are two inherent directions of cryptography, which are opposite to but stimulate each other. Both are essential for the development of cryptography. This is also the case for quantum cryptography [26–30]. Nevertheless, the development of quantum cryptanalysis is relatively slow because the theory of quantum information remains still far from satisfactorily known, especially for secure multiparty quantum summation. In fact, it is a very difficult work to analyze secure multiparty quantum summation protocols' security because multiple participants are involved and the dishonest have many advantages (e.g., they know partial information legally and can avoid introducing errors by lying in the eavesdropping check) in contrast to external opponents. Consequently, participant attack is the most serious threat for secure multiparty quantum summation protocols' security, and few results have been obtained.

In this paper, we analyze the SO-protocol's security and propose a new participant attack, in which one dishonest player can steal all the other players' shares and the summation of secrets without being found. Therefore, the SO-protocol is not secure in the sense that it does not satisfy the security requirement for secure multiparty summation. Furthermore, we study how to solve the security loophole.

The remainder of this paper is organized as follows. In Sec. 2, we give a brief review of the SO-protocol. Then, the cryptanalysis of this protocol is given and a new participant attack is proposed in Sect. 3. In Sect. 4, we study the reason for the security problem and present an improved version to deal with it. Finally, a short conclusion of this paper is covered in Sect. 5.

2 The SO-protocol

We firstly give a brief description of the SO-protocol. In this protocol, n participants P_1, P_2, ..., and P_n are involved. Each participant P_i has a secret e_i for $i = 1, 2, \ldots, n$, and any k participants of them can jointly calculate the summation without revealing their respective secrets. This protocol consists of the following several steps [25].

(1) For $i = 1, 2, \ldots, n$, P_i randomly chooses a vector $\overrightarrow{w_i} = (e_i, w_1, \ldots, w_v)^T$, and then calculates $M \times \overrightarrow{w_i} = (e_{i_1}, e_{i_2}, \ldots, e_{i_n})^T$, where M is defined in monotone span program (MSP) (please see Appendix B). Then, P_i sends the original share e_{i_j} to P_j for $j = 1, 2, \ldots, i-1, i+1, \ldots, n$ via a secure channel.

(2) When receiving all e_{j_i} $(j = 1, 2, \ldots, n, j \neq i)$ from other participants, each P_i $(i = 1, 2, \ldots, n)$ computes his share

$$H_i = \left(\sum_{j=1}^{n} e_{j_i}\right) \times \beta_{X_i} \mathtt{mod} d, \tag{1}$$

where d is a prime number, and β_{X_i} is the ith component of a vector $\overrightarrow{\beta_X}$ defined in Appendix B.

(3) The initiator (e.g., the first player P_1) prepares k single particles $\otimes_{i=1}^{k}|0\rangle_i$ and applies QFT operation on the first particle $|0\rangle_1$, i.e.,

$$|\Psi_1\rangle = \mathtt{QFT}|0\rangle_1 = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1. \tag{2}$$

(4) The initiator performs $(k-1)$ SUM operations on the particles $|0\rangle_1$ and $\otimes_{i=2}^{k}|0\rangle_i$, where $|0\rangle_1$ and $\otimes_{i=2}^{k}|0\rangle_i$ are control qudit and target qudits, respectively, and the SUM operation is defined as $\mathtt{SUM}(|\varphi\rangle, |\psi\rangle) = (|\varphi\rangle, |(\varphi+\psi)\mathtt{mod} d\rangle)$. After that, they evolve into the state

$$|\Psi_2\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1 |r\rangle_2 \cdots |r\rangle_k. \tag{3}$$

Finally, P_1 sends $|r\rangle_i$ to P_i for $i = 2, 3, \ldots, k$.

(5) For $i = 1, 2, \ldots, k$, P_i performs both QFT and Pauli operation $U_{H_i,0}$ on his particle $|r\rangle_i$. Then, $|\Psi_2\rangle$ evolves into the state

$$\begin{aligned} |\Psi_3\rangle &= (\otimes_{i=1}^{k} U_{H_i,0}\mathtt{QFT})|\Psi_2\rangle \\ &= d^{-\frac{k+1}{2}} \sum_{0 \le f_1, f_2, \ldots, f_k < d, f_1 + \cdots + f_k = 0 \ \mathtt{mod} d} |f_1 + H_1\rangle |f_2 \\ &\quad + H_2\rangle \cdots |f_k + H_k\rangle. \end{aligned} \tag{4}$$

(6) For $i = 1, 2, \ldots, k$, P_i uses computation basis to measure his particle $|f_i + H_i\rangle$, and then broadcasts the measurement outcome $f_i + H_i$. After collecting the other measurement outcome $f_j + H_j$ for $j = 1, 2, \ldots, i-1, i+1, \ldots, k$, P_i computes

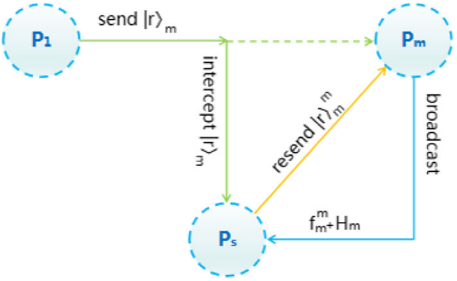

Fig. 1 Drawing of participant attack. When the initiator P_1 sends the particle $|r\rangle_m$ to P_m, the dishonest player P_s intercepts it and then sends a fake particle $|r\rangle_m^m$ to P_m. After receiving the measurement result $f_m^m + H_m$ broadcasted by P_m, P_s can obtain P_m's share H_m by simply computing

the summation

$$\begin{aligned}
&\sum_{j=1}^{k}(f_j + H_j)\mathtt{mod}d \\
&\quad= \sum_{j=1}^{k} f_j\mathtt{mod}d + \sum_{j=1}^{k} H_j\mathtt{mod}d \\
&\quad= 0 + \sum_{j=1}^{k} H_j\mathtt{mod}d \\
&\quad= \sum_{j=1}^{k} H_j\mathtt{mod}d.
\end{aligned} \tag{5}$$

3 The cryptanalysis

From the SO-protocol, it can be seen that when all the players in a qualified subset $X = \{P_1, P_2, \ldots, P_k\}$ of participants perform both the QFT and Pauli operation honestly, they can jointly calculate the summation $\sum_{j=1}^{k} H_j\mathtt{mod}d$ correctly by Eq. (5). However, as mentioned in [25], it is also required that no unqualified set can do it and nobody can gain access to a player's share in a (k, n) threshold secure multiparty quantum summation protocol at the same time. In the following, we will show that the SO-protocol does not satisfies these security requirements by a new participant attack, which is shown in Fig. 1.

From Eq. (5), it can be found that if a dishonest player P_s $(s \in \{2, \ldots, k\})$ can steal the other players' shares $H_1, \ldots, H_{s-1}, H_{s+1}, \ldots, H_k$, then he can compute the summation $\sum_{j=1}^{k} H_j\mathtt{mod}d$ easily. Specifically, this attack includes the following four steps.

(i) In Step (4), when the initiator P_1 sends the particle$|r\rangle_i$ to P_i for $i = 2, 3, \ldots, s-1, s+1, \ldots, k$, P_s intercepts them. Then, he chooses $k-1$ Pauli operations $U_{H_2^1,0}, U_{H_3^1,0}, \ldots, U_{H_k^1,0}$. After that, he performs QFT and $U_{H_i^1,0}$ on the corresponding particle $|r\rangle_i$ for $i = 2, 3, \ldots, k$ and keeps them in his quantum database.

(ii) For each player P_m $(m = 2, 3, \ldots, s-1, s+1, \ldots, k)$, similarly as the initiator P_1 does in Steps (3) and (4), P_s prepares k single particles $\otimes_{i=1}^{k}|0\rangle_i^m$ and applies QFT operation on the first particle $|0\rangle_1^m$, i.e.,

$$|\Psi_1^m\rangle = \mathtt{QFT}|0\rangle_1^m = \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}|r\rangle_1^m. \tag{6}$$

Then, he performs $(k-1)$ SUM operations on the particles $|0\rangle_1^m$ and $\otimes_{i=2}^k|0\rangle_i^m$, where $|0\rangle_1^m$ and $\otimes_{i=2}^k|0\rangle_i^m$ are control qudit and target qudits, respectively. Analogously, the state $|\Psi_1^m\rangle$ evolves into

$$|\Psi_2^m\rangle = \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}|r\rangle_1^m|r\rangle_2^m\cdots|r\rangle_k^m. \tag{7}$$

After that, he sends the particle $|r\rangle_m^m$ to P_m and keeps other particles in his quantum database. Finally, he also chooses $k-1$ Pauli operations $U_{H_1^m,0}, U_{H_2^m,0}, \ldots, U_{H_{m-1}^m,0}, U_{H_{m+1}^m,0}, \ldots, U_{H_k^m,0}$ and performs both QFT and $U_{H_i^m,0}$ on the corresponding particle $|r\rangle_i^m$ for $i = 1, 2, \ldots, m-1, m+1, \ldots, k$.

(iii) In Step (6), when all the other $k-1$ players broadcast their measurement results $f_1^1 + H_1, f_2^2 + H_2, \ldots, f_{s-1}^{s-1} + H_{s-1}, f_{s+1}^{s+1} + H_{s+1}, \ldots, f_k^k + H_k$, P_s uses computation basis to measure each particle $|r\rangle_i$ for $i = 2, 3, \ldots, k$, and each particle $|r\rangle_i^m$ for $i = 1, 2, \ldots, m-1, m+1, \ldots, k$ and $m = 2, 3, \ldots, k$. The measurement results are denoted as $H_i^1 + f_i^1$ for $|r\rangle_i$ and $H_i^m + f_i^m$ for $|r\rangle_i^m$, respectively. Then, he broadcasts his measurement result $f_s^s + H_s$.

(iv) After collecting the measurement result $f_m^m + H_m$ for $m = 1, 2, \ldots, s-1, s+1, \ldots, k$, P_s can obtain all the other players' shares $H_1, H_2, \ldots, H_{s-1}, H_{s+1}, \ldots, H_k$ by computing

$$H_1 = [(f_1^1 + H_1) + (f_2^1 + \cdots + f_k^1)]\mathtt{mod}d \tag{8}$$

and

$$\begin{aligned} H_m = [(f_m^m + H_m) + (f_1^m + \cdots + f_{m-1}^m \\ + f_{m+1}^m + \cdots + f_k^m)]\mathtt{mod}d \end{aligned} \tag{9}$$

for $m = 2, 3, \ldots, s-1, s+1, \ldots, k$. Then, he can gain access to the shares' summation $\sum_{j=1}^k H_j\mathtt{mod}d$ easily.

Therefore, although each original share is sent via a secure channel, this attack is possible because they are not necessary to compute the summation $\sum_{j=1}^k H_j\mathtt{mod}d$. Now we give a detailed explanation.

Firstly, we show that P_s can steal the initiator P_1's share H_1 by this attack. It can be found that after both P_1's and P_s's operations on the state $|\Psi_2\rangle$ in Step (i), it will evolve into

$$\begin{aligned} &|\Psi_3^1\rangle \\ &= U_{H_1,0}\mathtt{QFT}\otimes U_{H_2^1,0}\mathtt{QFT}\otimes\cdots\otimes U_{H_k^1,0}\mathtt{QFT}|\Psi_2\rangle \end{aligned}$$

$$= d^{-\frac{k+1}{2}} \sum_{0\le f_1^1, f_2^1, \ldots, f_k^1 < d, f_1^1+\cdots+f_k^1=0 \bmod d} |f_1^1 + H_1\rangle |f_2^1 + H_2^1\rangle \cdots |f_k^1 + H_k^1\rangle. \tag{10}$$

Because P_s knows both H_i^1 and the measurement outcome $f_i^1+H_i^1$ for $i = 2, 3, \ldots, k$, he can get f_i^1 for $i = 2, 3, \ldots, k$. Furthermore,

$$f_1^1 + f_2^1 + \cdots + f_k^1 = 0 \,\mathtt{mod} d. \tag{11}$$

Accordingly, when the initiator P_1 broadcasts his measurement outcome $f_1^1 + H_1$, P_s can gain access to his share H_1 by computing

$$\begin{aligned}
&[(f_1^1 + H_1) + (f_2^1 + \cdots + f_k^1)]\mathtt{mod} d \\
&\quad = [H_1 + (f_1^1 + f_2^1 + \cdots + f_k^1)]\mathtt{mod} d \\
&\quad = (H_1 + 0)\, \mathtt{mod} d \\
&\quad = H_1 \mathtt{mod} d \\
&\quad = H_1.
\end{aligned} \tag{12}$$

Secondly, we show that P_s can steal P_m's share H_m for $m = 2, 3, \ldots, s-1, s+1 \ldots, k$ by this attack. Analogously, after P_m's and P_s's operations on the state $|\Psi_2^m\rangle$, it will evolve into

$$\begin{aligned}
&|\Psi_3^m\rangle \\
&= U_{H_1^m,0}\mathtt{QFT} \otimes \cdots \otimes U_{H_{m-1}^m,0}\mathtt{QFT} \otimes U_{H_m,0}\mathtt{QFT} \\
&\quad \otimes U_{H_{m+1}^m,0}\mathtt{QFT} \cdots \otimes U_{H_k^m,0}\mathtt{QFT}|\Psi_2^m\rangle \\
&= d^{-\frac{k+1}{2}} \sum_{0\le f_1^m, f_2^m, \ldots, f_k^m < d, f_1^m+\cdots+f_k^m=0 \bmod d} |f_1^m \\
&\quad +H_1^m\rangle \cdots |f_{m-1}^m + H_{m-1}^m\rangle |f_m^m + H_m\rangle |f_{m+1}^m \\
&\quad +H_{m+1}^m\rangle \cdots |f_k^m + H_k^m\rangle.
\end{aligned} \tag{13}$$

P_s knows both H_i^m and the measurement outcome $f_i^m + H_i^m$ for $i = 1, 2, \ldots, m-1, m+1, \ldots, k$, and hence he can get f_i^m for $i = 1, 2, \ldots, m-1, m+1, \ldots, k$. Moreover,

$$f_1^m + f_2^m + \cdots + f_k^m = 0 \,\mathtt{mod} d. \tag{14}$$

Consequently, after P_m broadcasts his measurement result $f_m^m + H_m$, P_s can gain access to P_m's share H_m by computing

$$\begin{aligned}
&[(f_m^m + H_m) \;+\; (f_1^m + \cdots + f_{m-1}^m + f_{m+1}^m + \\
&\qquad \cdots + f_k^m)]\mathtt{mod} d
\end{aligned}$$

$$\begin{aligned} &= [H_m + (f_1^m + f_2^m + \cdots + f_k^m)]\mathrm{mod}d \\ &= (H_m + 0)\ \mathrm{mod}d \\ &= H_m\mathrm{mod}d \\ &= H_m. \end{aligned} \tag{15}$$

Finally, P_s can compute the summation $\sum_{j=1}^{k} H_j\mathrm{mod}d$ easily after getting all the other $k-1$ shares $H_1, H_2, \ldots, H_{s-1}, H_{s+1}, \ldots, H_k$. Furthermore, it is clear that P_m ($m \in \{2, 3, \ldots, s-1, s+1 \ldots, k\}$) has no way to discriminate the real state $|r\rangle_m$ sent by P_1 and the fake state $|r\rangle_m^m$ forged by P_s in the SO-protocol. Therefore, the other $k-1$ players $P_1, P_2, \ldots, P_{s-1}, P_{s+1}, \ldots, P_k$ cannot find this deception and will compute a false summation

$$\begin{aligned} &[(f_1^1 + H_1) + (f_s^s + H_s) + \sum_{j=2, j\neq s}^{k} (f_j^j + H_j)]\mathrm{mod}d \\ &= \left(\sum_{j=1}^{k} H_j + \sum_{j=1}^{k} f_j^j\right)\mathrm{mod}d \\ &\neq \sum_{j=1}^{k} H_j\mathrm{mod}d \end{aligned} \tag{16}$$

for

$$\sum_{j=1}^{k} f_j^j \neq 0\ \mathrm{mod}d. \tag{17}$$

By simple analysis, it can be found that if the initiator P_1 is dishonest, then he also can steal the other players' shares $H_2, H_3, \ldots, H_k$ and the summation $\sum_{j=1}^{k} H_j\mathrm{mod}d$ by this attack.

So far, we have shown that an unqualified set can compute the summation $\sum_{j=1}^{k} H_j\mathrm{mod}d$ by the way of stealing all the other players' shares in the SO-protocol, which is obviously in conflict with the security requirement for secure multiparty summation.

4 The improvement and analysis

Now we analyze the reason for the security loophole. From the participant attack in Sec. 3, it can be seen that there are two reasons for its success. One is that the player P_s can intercept the particle $|r\rangle_i$ for $i = 2, 3, \ldots, s-1, s+1, \ldots, k$, and then sends a fake one $|r\rangle_i^i$ to P_i instead of the real one without being found. The other is that the correlation among k particles shown in Eqs. (10) and (13). Nevertheless, the correlation is the base of calculating the summation $\sum_{j=1}^{k} H_j\mathrm{mod}d$, which means this way is not possible by changing it. Therefore, we can improve the SO-protocol to resist the presented participant attack by guaranteeing the security of quantum channel between the initiator P_1 and each player P_i $(i = 2, 3, \ldots, k)$, which is described as follows.

(A) The previous three steps are the same as that in the SO-protocol.

(B) In Step (4), after the initiator P_1 performs $(k-1)$ SUM operations on the particles $|0\rangle_1$ and $\otimes_{i=2}^{k}|0\rangle_i$, he prepares $\lambda(k-1)$ decoy particles, which are randomly chosen from $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, |\widehat{0}\rangle, |\widehat{1}\rangle, \ldots, |\widehat{d-1}\rangle\}$, where

$$\begin{aligned}|\widehat{j}\rangle &= \texttt{QFT}|j\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1} e^{2\pi ijr/d}|r\rangle \end{aligned} \tag{18}$$

for $j = 0, 1, 2, \ldots, d-1$. After that, for $i = 2, 3, \ldots, k$, he selects λ decoy particles and inserts the particle $|r\rangle_i$ in them. Finally, P_1 sends them to P_i.

(C) When confirming that P_i has received $|r\rangle_i$ and λ decoy particles, P_1 tells P_i these decoy particles' initial states and positions. For each decoy particle, P_i chooses the corresponding basis to measure it, i.e., if the state of decoy particle is in the set $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$, he uses Z-basis to measure it; otherwise, he uses X-basis to measure it, where Z-basis=$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ and X-basis=$\{|\widehat{0}\rangle, |\widehat{1}\rangle, \ldots, |\widehat{d-1}\rangle\}$. After that, P_i computes the error rate p_e, if it is more than the preset threshold, this protocol is aborted; otherwise, it continues.

(D) Similarly as that in Step (5), for $i = 1, 2, \ldots, k$, P_i performs both QFT and Pauli operation $U_{H_i,0}$ on his particle $|r\rangle_i$. Then, the state $|\Psi_2\rangle$ evolves into

$$\begin{aligned}|\Psi_3\rangle &= (\otimes_{i=1}^{k} U_{H_i,0}\texttt{QFT})|\Psi_2\rangle \\ &= d^{-\frac{k+1}{2}} \sum_{0\le f_1, f_2, \ldots, f_k < d,\, f_1+\cdots+f_k=0 \bmod d} |f_1 + H_1\rangle \\ &\quad |f_2 + H_2\rangle \cdots |f_k + H_k\rangle. \end{aligned} \tag{19}$$

(E) In Step (6), when all the measurement outcomes $f_1 + H_1, f_2 + H_2, \ldots, f_k + H_k$ are broadcasted, every player P_i can compute the summation

$$\begin{aligned}&\sum_{j=1}^{k}(f_j + H_j)\bmod d \\ &= \sum_{j=1}^{k} f_j \bmod d + \sum_{j=1}^{k} H_j \bmod d \\ &= 0 + \sum_{j=1}^{k} H_j \bmod d\end{aligned}$$

$$= \sum_{j=1}^{k} H_j \mathtt{mod} d. \tag{20}$$

In Step (C), the dishonest player P_s has no way to discriminate the encoding particle $|r\rangle_i$ and λ decoy particles. Therefore, if he randomly chooses only one from them, then the probability p_{r_i} that he chooses the right one is $\frac{1}{1+\lambda}$. Of course, if he chooses more particles from them, then the probability p_{r_i} that he chooses the right one will become larger, but the probability p_{d_i} that this deception will be detected will also become larger. Concretely, assume that P_s intercepts δ ($\delta \leq \lambda + 1$) particles from the encoding particle $|r\rangle_i$ and λ decoy particles, by simply computation, it can be obtained that $p_{r_i} = \frac{\delta}{1+\lambda}$ and

$$\begin{aligned} p_{d_i} &= \frac{\delta}{1+\lambda}(1 - \frac{1}{d^{\delta-1}}) + (1 - \frac{\delta}{1+\lambda})(1 - \frac{1}{d^{\delta}}) \\ &= 1 - \frac{1}{d^{\delta}}[\frac{\delta(d-1)}{1+\lambda} + 1], \end{aligned} \tag{21}$$

which is exponentially close to 1 with the increase of δ. Furthermore, if the dishonest player P_s wants to gain access to P_i's share H_i, these δ particles he randomly chooses must contain the encoding particle $|r\rangle_i$, while his deception cannot be found by P_i. Consequently, the probability p_{s_i} that P_s succeed to gain access to P_i's share is

$$\begin{aligned} p_{s_i} &= \frac{\delta}{1+\lambda} \times \frac{1}{d^{\delta-1}} \\ &= \frac{\delta}{d^{\delta-1}(1+\lambda)}, \end{aligned} \tag{22}$$

which does not become large with the increase of δ. Obviously, the probability p_{suc} that P_s can obtain all the shares' summation become more small, i.e.,

$$\begin{aligned} p_{suc} &= \prod_{j \neq s} p_{s_j} \\ &= \left(\frac{\delta}{d^{\delta-1}(1+\lambda)}\right)^{k-1}, \end{aligned} \tag{23}$$

which is exponentially close to 0 and therefore can be negligible.

As a result, the improved version can resist the above participant attack by guaranteeing the security of quantum channel between the trusted initiator and each player.

Compared to the SO-protocol, the improved version increases the computation and communication cost with $(k-1)\lambda$ decoy particles+k verification+$(k-1)\lambda$ measurement operations. Nevertheless, it retains the SO-protocol's advantages such as universality and is secure against both participant attacks and external attacks.

5 Conclusion

Participant attack is a special internal attack on many cryptographic protocols, especially on multiparty cases, which is so powerful that the main security task of cryptographic protocols is to resist such attacks. We not only propose a valid participant attack on the SO-protocol but also give a possible way to improve the protocol against both attacks from internal participants and external opponents. The proposed participant attack and corresponding solution can be applied to similar protocols with some modifications, and therefore, we hope this work shed some light on the next development of secure multiparty quantum computation.

Acknowledgements We are grateful to the anonymous reviewers for helpful comments. This work was supported by the National Natural Science Foundation of China (Grant Nos. 62172196, 61976024, 61972048, 61602232, 61902166), the Guangxi Key Laboratory of Trusted Software (Grant No. KX202040), the Postgraduate Education Reform Project of Henan Province (Grant No.2019-SJGLX094Y), the Key Scientific Research Project in Universities of Henan Province (Grant No. 21A110017), the Natural Science Foundation of Henan Province (Grant No. 212300410062) and the Youth Key Teacher Project of Luoyang Normal University.

Declarations

The authors have no relevant financial or non-financial interests to disclose, and this manuscript has no associated data.

Appendix A Access structure

Given a set of participants $P = \{P_1, P_2, \ldots, P_n\}$, an access structure $\alpha \subseteq 2^{|P|}$ is such a qualified set of participants that if $X \in \alpha$ and $X \subseteq Y \subseteq P$, then $Y \in \alpha$. The set of unqualified participants is called an adversary structure ζ [25].

Appendix B Monotone span program

The MSP consists of four tuples $(F, M, \eta, \overrightarrow{\sigma})$, where F is a finite field, M is a $u \times v$ matrix over F, $\eta : \{1, 2, \ldots, u\} \to P$ is a surjective mapping, and $\overrightarrow{\sigma}$ is a target vector such that $\overrightarrow{\sigma} = (1, 0, \ldots, 0)^T \in F^v$. If $(F, M, \eta, \overrightarrow{\sigma})$ is a MSP for access structure α, then it must satisfy: If $X \in \alpha$, there exists a vector $\overrightarrow{\beta_X} \in F^k$ such that $M_X^T \overrightarrow{\beta_X} = \overrightarrow{\sigma}$; otherwise, if $X \in \zeta$, there exists a vector $\overrightarrow{u} = (u_1, u_2, \ldots, u_v)^T \in F^v$ such that $M_X \overrightarrow{u} = \overrightarrow{0} \in F^k$ with $u_1 = 1$, where k denotes the number of participants in X, and M_X denotes the ith row of M such that $\eta(i) \in X$ [25].

Appendix C Linear secret sharing

The LSS scheme consists of two phases: secret distribution phase and reconstruction phase [25].

Distribution phase: The dealer selects a random vector $\overrightarrow{w} = (e, w_2, \ldots, w_v)^T$ and computes $\overrightarrow{e} = M\overrightarrow{w} = (e_1, e_2, \ldots, e_n)^T$, where e is a secret. Then, it sends e_z to player $\eta(z)$ by a secure channel.

Reconstruction phase: The authenticated set X of players can recover the secret e by computing

$$\begin{aligned}\overrightarrow{e_X} \cdot \overrightarrow{\beta_X} &= (M_X \overrightarrow{w})^T \cdot \overrightarrow{\beta_X} \\ &= \overrightarrow{w}^T \cdot (M_X^T \overrightarrow{\beta_X}) \\ &= \overrightarrow{w}^T \cdot \overrightarrow{\sigma} \\ &= e.\end{aligned}$$

References

1. Yao, A.C.: Protocols for secure computations. In: SFCS'08. 23rd Annual Symposium on. IEEE, pp. 160-164, IEEE Press, (1982)
2. Cheng, S.T., Wang, C.Y.: Quantum switching and quantum merge sorting. IEEE Trans. Circuits Syst. I-Reg. Papers **53**, 316–325 (2006)
3. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Economical quantum anonymous transmissions. J. Phys. B: At. Mol. Opt. Phys. **43**, 245501 (2010)
4. Shu, H., Yu, R., Jiang, W., et al.: Efficient implementation of k-nearest neighbor classifier using vote count circuit. IEEE Trans. Circuits Syst. II-Exp. Briefs **61**, 448–452 (2014)
5. Huang, W., Wen, Q.Y., Liu, B., et al.: Quantum anonymous ranking. Phys. Rev. A **89**, 032325 (2014)
6. Kong, B.Y., Yoo, H., Park, I.C.: Efficient sorting architecture for successive-cancellation-list decoding of polar codes. IEEE Trans. Circuits Syst. II-Exp. Briefs **63**, 673–677 (2016)
7. Lin, S., Guo, G.D., Huang, F., et al.: Quantum anonymous ranking based on the Chinese remainder theorem. Phys. Rev. A **93**, 012318 (2016)
8. 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 Trans. Comput. **67**, 2–8 (2018)
9. Gao, F., Qin, S.J., Huang, W., et al.: Quantum private query: a new kind of practical quantum cryptographic protocols. Sci. China-Phys. Mech. Astron. **62**, 070301 (2019)
10. Wei, C.Y., Cai, X.Q., Wang, T.Y., et al.: Error tolerance bound in QKD-based quantum private query. IEEE J. Sel. Areas in Commun. **38**, 517–527 (2020)
11. Clifton, C., Kantarcioglu, M., Vaidya, J., et al.: Tools for privacy preserving distributed data mining. ACM Sigkdd Explor. Newsl. **4**, 28–34 (2002)
12. Du, W., Atallah., M. J.: Secure multi-party computation problems and their applications: a review and open problems. In: Proceedings of the 2001 Workshop on New Security Paradigms, ACM, pp.13-22, (2001)
13. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)
14. Zhong, H.S., Wang, H., Deng, Y.H., et al.: Quantum computational advantage using photons. Science **370**, 1460–1463 (2020)
15. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**, 012333 (2007)
16. Du, J.Z., Chen, X.B., Wen, Q.Y.: Secure multiparty quantum summation. Acta Phys. Sin. **56**, 6214 (2007)
17. 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**, 2793–2804 (2010)
18. Zhang, C., Sun, Z.W., Huang, X., et al.: Three-party quantum summation without a trusted third party. Int. J. Quant. Inf. **13**, 1550011 (2015)
19. Shi, R.H., Mu, Y., Zhong, H., et al.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)

20. Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. Quant. Inf. Process. **16**, 225 (2017)
21. 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**, 1750010 (2017)
22. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quant. Inf. Process. **17**, 129 (2018)
23. Ji, Z.X., Zhang, H.G., Wang, H.Z., et al.: Quantum protocols for secure multi-party summation. Quant. Inf. Process. **18**, 168 (2019)
24. Zhang, C., Razavi, M., Sun, Z.W., et al.: Improvements on Secure multi-party quantum summation based on quantum Fourier transform. Quant. Inf. Process. **18**, 336 (2019)
25. Sutradhar, K., Om, H.: A generalized quantum protocol for secure multiparty summation. IEEE Trans. Circuites Syst. II-Exp. Briefs **67**, 2978–2982 (2020)
26. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
27. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quant. Inf. & Comput **7**, 329–334 (2007)
28. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comment on experimental demonstration of a quantum protocol for Byzantine agreement and liar detection. Phys. Rev. Lett **101**, 208901 (2008)
29. Cai, X.Q., Wang, T.Y., Wei, et al.: Cryptanalysis of multiparty quantum digital signatures. Quant. Inf. Process **18**, 252 (2019)
30. Chen, Y.A., Zhang, Q., Chen, T.Y., et al.: An integrated space-to-ground quantum communication network over 4600 kilometres. Nature **589**, 214–219 (2021)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.