International Journal of Theoretical Physics (2021) 60:3711–3721
https://doi.org/10.1007/s10773-021-04932-8

Quantum Secure Multi-Party Summation Based on Grover's Search Algorithm

Xin Zhang[1] · Song Lin[1] · Gong-De Guo[1]

Received: 23 April 2021 / Accepted: 8 August 2021 / Published online: 1 September 2021

Abstract
In this paper, a quantum secure multi-party summation protocol is proposed based on some properties of Grover's search algorithm. In the protocol, each participant's secret input is encoded as a unitary operation on the travelling two-qubit state. With the help of a semi-honest third party, all participants can simultaneously obtain the summation result without disclosing their secret inputs. Only the preparation and measurement of single qubits are required, which makes the proposed protocol feasible using current technology. At last, we demonstrate the correctness and security of the protocol, which can resist various attacks from both external attackers and internal participants.

Keywords Quantum secure multi-party summation · Grover's search algorithm · Unambiguous state discrimination

1 Introduction

Quantum cryptography, which is regarded as the combination of quantum mechanics and classical cryptography, has attracted a lot of attention since Bennett and Brassard presented the first quantum key distribution protocol [1]. Different from the security of the classical cryptography which is based on the assumption of computation complexity, that of quantum cryptography relies on the quantum mechanics principles, e.g., no-cloning theorem, Heisenberg uncertainty principle, which make it unconditionally secure in theory. Consequently, in the past decades, many scholars have studied it, and proposed a lot of branches of quantum cryptography, such as quantum key distribution [1–3], quantum secret sharing [4–7], quantum private query [8–11], quantum multi-party computation [12–14], and so on.

Secure multi-party summation, as a vital research point of secure multi-party computation, can be used to construct complex security protocols for other multi-party computation. Thus, in the past few years, researchers have proposed a variety of quantum secure multi-party summation protocols using different strategies. In 2006, Hillery et al. [15] proposed the first multi-party summation protocol with the two-particle N-level entangled states,

✉ Song Lin
lins95@gmail.com

[1] College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350007, China

which can complete the summation of N participants in the voting process on the premise of ensuring the anonymity of participants. In 2010, based on multi-particle entangled states, Chen et al. [16] proposed another secure addition module 2. In 2016, Shi et al. [17] proposed a new protocol based on the quantum Fourier transform, which utilized $2m-$qubit entangled state as information carrier. Afterwards, a few quantum secure multi-party summation [18–20] has been proposed, in which various properties of quantum mechanics are exploited. However, these protocols encounter a problem in practical application, that is, it is difficult to prepare the information carriers (multi-particle entangled states) with current technology. To solve this problem, a novel quantum secure multi-party summation protocol with qubits is proposed, in which some properties of Grover's search algorithm is utilized. In the protocol, two-qubit states are used as the information carriers that are transmitted among the participants. For the signal particles, each participant encodes his secret input by performing the encoding operations that are used to transform the initial state into the target state in Grover's search algorithm. At last, according to the parity of the number of the unitary operations, a semi-honest third party selects one of two mutually unbiased bases to measure these single qubits. Based on the third party's announcement, participants can get the summation result of their secret inputs.

The rest of this paper is organized as follows. In Section 2, we introduce the essential preliminaries briefly. Then, we use the properties of Grover's search algorithm to design a protocol of quantum secure multi-party summation and give an example in Section 3. In Section 4, we demonstrate the proposed protocol is correct and secure. Finally, a brief conclusion is given in Section 5.

2 Preliminaries

Let us start with describing some notations which are used in this paper. For convenience, these notations are similar to Grover's search algorithm [21]. In the algorithm, there exists a data set with four items that is represented by a two-qubit state $|\widetilde{\varphi}_{uv}\rangle = (|0\rangle + (-1)^v|1\rangle)(|0\rangle + (-1)^u|1\rangle)$, $u, v \in \{0, 1\}$. Evidently, $|\widetilde{\varphi}_{00}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$. The target state is $|\varphi_{mn}\rangle = |mn\rangle$, $m, n \in \{0, 1\}$. Two specific unitary operations are required on $|\widetilde{\varphi}_{uv}\rangle$ to achieve the search task.

$$U_{xy} = I - 2|\varphi_{xy}\rangle\langle\varphi_{xy}|,\ V_{xy} = 2|\widetilde{\varphi}_{xy}\rangle\langle\widetilde{\varphi}_{xy}| - I, \tag{1}$$

where $x, y \in \{0, 1\}$. The first unitary operation U_{xy} causes the phase of the state $|xy\rangle$ to flip once, and its matrix is expressed as:

$$U_{xy} = \begin{pmatrix} (-1)^{\bar{x}\bar{y}} & & & \\ & (-1)^{\bar{x}y} & & \\ & & (-1)^{x\bar{y}} & \\ & & & (-1)^{xy} \end{pmatrix}, \tag{2}$$

where $\bar{x} = x \oplus 1$, $\bar{y} = y \oplus 1$, the symbol $\oplus$ denotes bitwise Exclusive OR. The second one V_{xy} causes the amplitude of the state $|xy\rangle$ to increase. Performing the above two unitary operations on $|\widetilde{\varphi}_{uv}\rangle$, we can find

$$V_{uv}U_{mn}|\widetilde{\varphi}_{uv}\rangle = |\varphi_{mn}\rangle. \tag{3}$$

Here, since the global phase has no effect on the results, it can be ignored in this paper, i.e., $\pm|\varphi_{mn}\rangle = |\varphi_{mn}\rangle$. The search target can be obtained by measuring with the basis $MB_Z = \{|0\rangle, |1\rangle\}$.

Using the property depicted in (3), Hsu [22] has proposed a quantum secret sharing protocol based on Grover's search algorithm in 2003. In this protocol, only when two participants combine their qubits and perform V_{uv} on their two-qubit state can they both determine the state $|\varphi_{mn}\rangle$. Subsequently, researchers have carried out a series of researches on quantum cryptographic protocols based on Grover's search algorithm [23–26]. Then, we further investigated the properties of these quantum states and operations, and drew some interesting results, which can be used to design the proposed quantum secure multi-party summation protocol.

Given two operators $U_{x_1y_1}$ and $U_{x_2y_2}$, where $x_1, y_1, x_2, y_2 \in \{0, 1\}$. Clearly, these operators are commutative. That is, $U_{x_2y_2}U_{x_1y_1} = U_{x_1y_1}U_{x_2y_2}$. In addition, if $x_1 = x_2$ and $y_1 = y_2$, we get $U_{x_1y_1}U_{x_1y_1} = I$, i.e.,

$$U^n_{x_1y_1} = U^{n(mod\ 2)}_{x_1y_1}. \tag{4}$$

Otherwise, we get

$$U_{x_2y_2}U_{x_1y_1} = X_{x_1\oplus x_2, y_1\oplus y_2}, \tag{5}$$

where,

$$X_{00} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, X_{01} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix},$$
$$X_{10} = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}, X_{11} = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix}. \tag{6}$$

So, we can obtain the result shown in (7) after these two operations on the quantum state $|\widetilde{\varphi}_{uv}\rangle$.

$$U_{x_2y_2}U_{x_1y_1}|\widetilde{\varphi}_{uv}\rangle = |\widetilde{\varphi}_{x_1\oplus x_2\oplus u, y_1\oplus y_2\oplus v}\rangle. \tag{7}$$

3 Quantum Secure Multi-Party Summation Protocol

Suppose that there is a semi-honest third party P_0, who may misbehave on his own but cannot conspire with anyone. There are N parties, $P_i(i = 1, 2, \cdots, N)$, who hold their own secret input D_i with length of $2n$. That is, $D_i = (d_{i,1}, d_{i,2}, \cdots, d_{i,2n})$, $d_{i,j} \in \{0, 1\}(j = 1, 2, \cdots, 2n)$. All participants want to obtain the summation of their secret inputs shown in (8), without revealing the genuine content of their secret inputs.

$$\oplus_{i=1}^N D_i = \{\oplus_{i=1}^N d_{i,1}, \oplus_{i=1}^N d_{i,2}, \cdots, \oplus_{i=1}^N d_{i,2n}\}, \tag{8}$$

where $\oplus_{i=1}^N d_{i,j} = d_{1,j} \oplus d_{2,j} \oplus \cdots \oplus d_{N,j}$. The detailed procedures of the proposed quantum secure multi-party summation can be described as follows.

Step 1: P_0 generates a random bit sequence S with length of $2n$. According to this bit sequence, he prepares an ordered sequence of two-qubit states Q_1, i.e.,

$$S = (s_1, s_2, \cdots, s_{2n}) \Longrightarrow Q_1 = (|\widetilde{\varphi}_{s_1,s_2}\rangle, |\widetilde{\varphi}_{s_3,s_4}\rangle, \cdots, |\widetilde{\varphi}_{s_{2n-1},s_{2n}}\rangle). \tag{9}$$

To ensure the security of particle transmission, P_0 prepares δ decoy particles which are randomly in one of the four BB84 states, and inserts them into the sequence Q_1 randomly to form a new sequence $\widetilde{Q}_1$. At last, P_0 sends the particle sequence $\widetilde{Q}_1$ to the next participant P_1.

Step 2: After confirming that P_1 has received the sequence $\widetilde{Q}_1$, P_0 checks the security of $\widetilde{Q}_1$'s transmission together with P_1. To be specific, according to the positions of decoy particles and their bases published by P_0, P_1 measures the corresponding decoy particles and tells P_0 the results. P_0 calculates the error rate by comparing the measurement results with the initial states of the decoy particles. If the error rate exceeds the predetermined threshold, they restart the protocol. Otherwise, they proceed to the next step.

Step 3: By deleting the decoy particles from $\tilde{Q}_1$, P_1 can get the sequence Q_1. Then, P_1 encodes his secret input D_1 on the sequence Q_1. Concretely, P_1 generates a random bit string $m_1 = \{m_{1,1}, m_{1,2}, \cdots, m_{1,n}\}$. If $m_{1,t} = 0$ $(t = 1, 2, \cdots, n)$, the private data $d_{1,2t-1}, d_{1,2t}$ is split to two parts, i.e., $d_{1,2t-1} = x_1^{1,2t-1} \oplus x_2^{1,2t-1}$, $d_{1,2t} = y_1^{1,2t} \oplus y_2^{1,2t}$. Then, P_1 performs $U_{x_1^{1,2t-1}, y_1^{1,2t}} U_{x_2^{1,2t-1}, y_2^{1,2t}}$ on the state $|\widetilde{\varphi}_{s_{2t-1},s_{2t}}\rangle$. Otherwise, P_1 directly performs $U_{d_{1,2t-1},d_{1,2t}}$ on $|\widetilde{\varphi}_{s_{2t-1},s_{2t}}\rangle$. The encoded sequence is denoted as Q_2. Finally, P_1 randomly selects δ decoy particles to insert into Q_2, and sends the new sequence $\widetilde{Q}_2$ to participant P_2.

Step $i + 2$ $(i = 2, 3, \cdots, N)$: When P_i has received the quantum state sequence $\widetilde{Q}_i$ from P_{i-1}, P_{i-1} checks the security of the particle transmission with P_i ,which is similar to Step 2. If the error rate exceeds the predetermined threshold, the protocol is restarted. Otherwise, P_i performs the encoding operations similar to Step 3 and sends the particle sequence $\widetilde{Q}_{i+1}$ to the next participant P_{i+1}. As for the last participant P_N, he sends the particle sequence $\widetilde{Q}_{N+1}$ to P_0.

Step $N + 3$: When P_0 has received the sequence $\widetilde{Q}_{N+1}$ from P_N, he performs eavesdropping detection with P_N. Then he gets Q_{N+1} after removing the decoy particles from $\widetilde{Q}_{N+1}$. Now, P_i $(i = 1, 2, \cdots, N)$ tells P_0 the bit string m_i. P_0 calculates $M_t = m_{1,t} \oplus m_{2,t} \oplus \cdots \oplus m_{N,t}$ $(t = 1, 2, \cdots, n)$. Then, P_0 executes different processes according to the value of M_t.

(1) When $M_t = 0$, P_0 measures the corresponding particles with basis $MB_X = \{|+\rangle, |-\rangle\}$ directly, and obtains the result $|\widetilde{\varphi}_{w_{2t-1},w_{2t}}\rangle$. P_0 calculates the summation:

$$A_{2t-1} = w_{2t-1} \oplus s_{2t-1}, A_{2t} = w_{2t} \oplus s_{2t}. \tag{10}$$

(2) When $M_t = 1$, P_0 performs the unitary operation $V_{s_{2t-1},s_{2t}}$ on the t-th two-qubit state. Then he measures these states with basis MB_Z, and obtains the result $|\varphi_{w_{2t-1},w_{2t}}\rangle$. P_0 calculates the summation:

$$A_{2t-1} = w_{2t-1}, A_{2t} = w_{2t}. \tag{11}$$

Finally, P_0 publishes the summation result $A = (A_1, A_2, \cdots, A_{N-1}, A_N)$. In this way, all participants can obtain the summation of their secret inputs.

To illustrate our protocol more clearly, a three-party case (i.e., $N = 3$) is taken as an example. For convenience, the eavesdropping detecting is ignored. In this case, there are three participants P_1, P_2, and P_3, who want to get the summation of their secret inputs with length of 8 (i.e., $n = 4$), $D_1 = 01101101$, $D_2 = 10100111$, $D_3 = 11010010$.

At first, P_0 generates an ordered two-qubit state sequence $Q_1 = (|\widetilde{\varphi}_{01}\rangle, |\widetilde{\varphi}_{01}\rangle, |\widetilde{\varphi}_{11}\rangle, |\widetilde{\varphi}_{00}\rangle)$, namely the bit string is $S = 01011100$. P_1 (P_2, P_3) applies his encoding operations on the signal particles, according to his secret input D_1 (D_2, D_3) and random bit string m_1 (m_2, m_3). The states are changed with the corresponding encoding operations, which are depicted in Table 1.

Table 1 Encoding operations on the sequence

$m_1 = \{0, 1, 1, 0\}$	$m_2 = \{0, 1, 0, 1\}$	$m_3 = \{1, 1, 0, 1\}$
$\lvert\widetilde{\varphi}_{01}\rangle \xrightarrow{01:U_{11}U_{10}} \lvert\widetilde{\varphi}_{00}\rangle$	$\xrightarrow{10:U_{11}U_{01}} \lvert\widetilde{\varphi}_{10}\rangle$	$\xrightarrow{11:U_{11}} U_{11}\lvert\widetilde{\varphi}_{10}\rangle$
$\lvert\widetilde{\varphi}_{01}\rangle \xrightarrow{10:U_{10}} U_{10}\lvert\widetilde{\varphi}_{01}\rangle$	$\xrightarrow{10:U_{10}} \lvert\widetilde{\varphi}_{01}\rangle$	$\xrightarrow{01:U_{01}} U_{01}\lvert\widetilde{\varphi}_{01}\rangle$
$\lvert\widetilde{\varphi}_{11}\rangle \xrightarrow{11:U_{11}} U_{11}\lvert\widetilde{\varphi}_{11}\rangle$	$\xrightarrow{01:U_{00}U_{01}} U_{10}\lvert\widetilde{\varphi}_{11}\rangle$	$\xrightarrow{00:U_{01}U_{01}} U_{10}\lvert\widetilde{\varphi}_{11}\rangle$
$\lvert\widetilde{\varphi}_{00}\rangle \xrightarrow{01:U_{00}U_{01}} \lvert\widetilde{\varphi}_{01}\rangle$	$\xrightarrow{11:U_{11}} U_{11}\lvert\widetilde{\varphi}_{01}\rangle$	$\xrightarrow{10:U_{10}} \lvert\widetilde{\varphi}_{00}\rangle$

At the end of the protocol, P_0 obtains states $U_{11}|\widetilde{\varphi}_{10}\rangle$, $U_{01}|\widetilde{\varphi}_{01}\rangle$, $U_{10}|\widetilde{\varphi}_{11}\rangle$, $|\widetilde{\varphi}_{00}\rangle$. According to the value of m_i declared by P_i, P_0 can calculate $M_1 = 1$, $M_2 = 1$, $M_3 = 1$, $M_4 = 0$. So he performs the operations $V_{01} \otimes V_{01} \otimes V_{11} \otimes I$ to get the states $|\varphi_{00}\rangle$, $|\varphi_{01}\rangle$, $|\varphi_{10}\rangle$, $|\widetilde{\varphi}_{00}\rangle$, and measures these particles in the basis MB_Z or MB_X. Finally, P_0 obtains the summation of their secret inputs $A = 00011000$, and knows $A = D_1 \oplus D_2 \oplus D_3$.

4 Analysis of the Protocol

In this section, we first discuss the correctness of the proposed protocol. Then, the security of this protocol is analyzed by considering the external attacks and some common internal attacks.

4.1 Correctness

For a secure multi-party summation protocol, it is correct, which means that all participants can obtain the summation of their secret inputs without disclosing any secrets. In the following, we will show the result of the protocol is the summation of their secret inputs.

Suppose one initial state of the signal particles is $|\widetilde{\varphi}_{s_{2t-1},s_{2t}}\rangle$, the encoding operation U_{xy} has been performed r times in Steps 3 to $N+2$, that is, $U_{x_r,y_r}U_{x_{r-1},y_{r-1}}\cdots U_{x_2,y_2}U_{x_1,y_1}$, where $x_i, y_i \in \{0,1\}$. According to the Step $N+3$, we know $M_t = r \pmod 2$. So, after these encoding operations, the signal particles are in the state $|\phi\rangle = U_{x_r,y_r}\cdots U_{x_1,y_1}|\widetilde{\varphi}_{s_{2t-1},s_{2t}}\rangle$. Due to the commutability of U_{xy}, we can get:

$$U_{x_r,y_r}\cdots U_{x_1,y_1} = \underbrace{U_{00}\cdots U_{00}}_{r_{00}}\underbrace{U_{01}\cdots U_{01}}_{r_{01}}\underbrace{U_{10}\cdots U_{10}}_{r_{10}}\underbrace{U_{11}\cdots U_{11}}_{r_{11}}, \tag{12}$$

where r_{xy} is the frequency of U_{xy}, and $r_{00} + r_{01} + r_{10} + r_{11} = r$. Based on (4), we get $U_{x_i,y_i}^{r_{xy}} = U_{x_i,y_i}^{a_{xy}}$, where $a_{xy} = r_{xy} \pmod 2$. Thus, (12) can be abbreviated as:

$$U_{x_r,y_r}U_{x_{r-1},y_{r-1}}\cdots U_{x_2,y_2}U_{x_1,y_1} = U_{00}^{a_{00}}U_{01}^{a_{01}}U_{10}^{a_{10}}U_{11}^{a_{11}}. \tag{13}$$

Obviously, if r is even, $M_t = a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 0$. Otherwise, $M_t = a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 1$. Next, we will discuss these two cases.

(1) $M_t = 0$, i.e., $a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 0$.

There are two different scenarios. One is $a_{00} = a_{01} = a_{10} = a_{11} = 1$ or 0. Due to the property of $U_{00}U_{01}U_{10}U_{11} = I$, we get the final state $|\phi\rangle = |\widetilde{\varphi}_{s_{2t-1},s_{2t}}\rangle$. The other is that any two of $a_{00}, a_{01}, a_{10}, a_{11}$ are 1. Namely, there are two operations performed odd times and two operations with even times. In terms of (5), we get

$$U_{00}^{a_{00}}U_{01}^{a_{01}}U_{10}^{a_{10}}U_{11}^{a_{11}} = (-1)^{a_{00}}X_{a_{10}\oplus a_{11},a_{01}\oplus a_{11}}. \tag{14}$$

To sum up, when $a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 0$, we get the final state $|\phi\rangle$:

$$\begin{aligned} |\phi\rangle &= (-1)^{a_{00}} X_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}} |\widetilde{\varphi}_{s_{2t-1}, s_{2t}}\rangle \\ &= |\widetilde{\varphi}_{a_{10}\oplus a_{11}\oplus s_{2t-1}, a_{01}\oplus a_{11}\oplus s_{2t}}\rangle. \end{aligned} \tag{15}$$

At the end of this protocol, we know, when $M_t = 0$, the unitary operation U_{xy} of the t-th two-qubit state $|\widetilde{\varphi}_{s_{2t-1}, s_{2t}}\rangle$ is even times. According to (15), we can obtain the result $|\phi\rangle = |\widetilde{\varphi}_{w_{2t-1}, w_{2t}}\rangle$, which is in $\{|++\rangle, |-+\rangle, |+-\rangle, |--\rangle\}$. Finally, P_0 measures the state with MB_X to gain the summation. Clearly, in terms of (10) and (16), we know the summation is $A_j = \oplus_{i=1}^{N} D_{i,j}$ $(j = 1, 2, \cdots, 2n)$.

$$\begin{aligned} w_{2t-1} &= a_{10} \oplus a_{11} \oplus s_{2t-1} = d_{1,2t-1} \oplus d_{2,2t-1} \oplus \cdots \oplus d_{N,2t-1} \oplus s_{2t-1}, \\ w_{2t} &= a_{01} \oplus a_{11} \oplus s_{2t} = d_{1,2t} \oplus d_{2,2t} \oplus \cdots \oplus d_{N,2t} \oplus s_{2t}. \end{aligned} \tag{16}$$

(2) $M_t = 1$, i.e., $a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 1$.

There are two scenarios to consider as well. On the one hand, only one of $a_{00}, a_{01}, a_{10}, a_{11}$ is 1. That is, only one of the four operations performs odd, (13) can be rewritten as $U_{00}^{a_{00}} U_{01}^{a_{01}} U_{10}^{a_{10}} U_{11}^{a_{11}} = U_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}}$. On the other hand, any three of $a_{00}, a_{01}, a_{10}, a_{11}$ are 1. That is, three of the four operations perform odd, (13) can be rewritten as $U_{00}^{a_{00}} U_{01}^{a_{01}} U_{10}^{a_{10}} U_{11}^{a_{11}} = -U_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}}$.

Overall, when $a_{00} \oplus a_{01} \oplus a_{10} \oplus a_{11} = 1$, the encoding operation sequence of U_{xy} can be abbreviated as:

$$U_{00}^{a_{00}} U_{01}^{a_{01}} U_{10}^{a_{10}} U_{11}^{a_{11}} = \pm U_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}}. \tag{17}$$

In our protocol, when $M_t = 1$, P_0 has to perform operation $V_{s_{2t-1}, s_{2t}}$ on the quantum state $|\widetilde{\varphi}_{s_{2t-1}, s_{2t}}\rangle$ in Step $N+3$. According to the Grover's search algorithm, the following results are obtained:

$$|\phi\rangle = \pm V_{s_{2t-1}, s_{2t}} U_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}} |\widetilde{\varphi}_{s_{2t-1}, s_{2t}}\rangle = |\varphi_{a_{10}\oplus a_{11}, a_{01}\oplus a_{11}}\rangle. \tag{18}$$

Contrast with $M_t = 0$, the unitary operation U_{xy} of the t-th two-qubit state $|\widetilde{\varphi}_{s_{2t-1}, s_{2t}}\rangle$ is odd. According to (18), We obtain the result $|\phi\rangle = |\varphi_{w_{2t-1}, w_{2t}}\rangle$, which is in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Finally, P_0 measures the state with MB_Z to gain the summation. Evidently, from (11) and (19), we know the summation is $A_j = \oplus_{i=1}^{N} D_{i,j}$ $(j = 1, 2, \cdots, 2n)$.

$$\begin{aligned} w_{2t-1} &= a_{10} \oplus a_{11} = d_{1,2t-1} \oplus d_{2,2t-1} \oplus \cdots \oplus d_{N,2t-1}, \\ w_{2t} &= a_{01} \oplus a_{11} = d_{1,2t} \oplus d_{2,2t} \oplus \cdots \oplus d_{N,2t}. \end{aligned} \tag{19}$$

Consequently, taking the above two circumstances into consideration, the protocol we proposed is correct.

4.2 Security

In a quantum secure multi-party summation protocol, the participants are not all honest, which means their attacks should be considered. Moreover, since the participant takes part in the execution of the protocol, he generally has more powerful than Eve. Thus, in addition to the external attacks, the security of the proposed protocol under three common internal attacks, which are performed by different dishonest participants respectively, are analyzed in this section.

4.2.1 External Attack

Suppose there is an external attacker, Eve, whose goal is to steal the secret information of one participant P_i $(i = 1, 2, \cdots, N)$. According to the publicly available messages m_i and A_i, Eve has no access to any information about D_i. So she has to attack the travelling particle sequence $\widetilde{Q}_{i+1}$, which is sent from P_i to P_{i+1}. This attack can be intercept-resend attack, measurement-resend attack and entanglement-measurement attack, etc. However, in our protocol, some decoy particles are added, and these particles are randomly in one of the four BB84 states. Clearly, the method of eavesdropping detection with decoy particles is derived from the BB84 protocol, which has proved to be unconditionally security in theory. That is, as long as Eve tries to attack the travelling particles in the process of particle transmission, it will be detected because she does not know the positions and measurement bases of these decoy particles. Therefore, the proposed protocol is secure against this external attack.

4.2.2 A Dishonest Participant's Attack

N participants P_i $(i = 1, 2, \cdots, N)$ play the same roles in the proposed protocol. So, without loss of generality, we can assume that the participant P_i is dishonest, denoting as P_i^*, who tries to steal the secret input of P_{i+1}. He can send a false particle sequence F to P_{i+1}. P_{i+1} performs the encoding operation on F according to his secret input, then adds δ decoy particles and gets the particle string $\widetilde{F}$. After that, P_{i+1} sends it to P_{i+2}. At this point, P_i^* attacks this particle sequence $\widetilde{F}$ to distinguish the encoding operations. However, since he does not know the locations of the decoy particles, his attack behavior will inevitably introduce errors as Eve, which will be inevitably discovered by the eavesdropping detection process between P_{i+1} and P_{i+2}. Thus, such an attack would be null and void for our protocol.

4.2.3 Multiple Dishonest Participants' Collusion Attack

In this attack, there are two or more participants who cooperate to steal secret inputs of honest participants. At first, a special case is considered, which $N-1$ participants conspire. Obviously, they can infer the secret input of the remaining honest participant based on the summation result published by P_0. Similarly, if $N-k$ participants conspire, they can easily get the summation of other k participants' secret inputs. Therefore, these situations are trivial. Now, we will discuss some non-trivial cases. For example, in a four-party protocol, P_1 and P_3 are dishonest participants, who are denoted as P_1^* and P_3^*, they clearly have easy access to the summation of P_2 and P_4. The key point is whether they are able to eavesdrop the information about P_2's or P_4's secret input. Obviously, P_1^* and P_3^* conspire to steal P_2's secret input more easily than P_4's. Thus, the case, in which, P_1^* and P_3^* conspire to attack P_2, is discussed as follows.

First of all, let us consider a simple attack strategy. P_1^* receives the quantum state sent by P_0, then he chooses the basis MB_X to obtain the initial state, and infers the classical bit sequence S. Then the secret input of P_1^* is encoded into the particle sequence $\widetilde{Q}_2$ and sent to P_2. P_2 receives the particle sequence and checks the security of the transmission. The sequence $\widetilde{Q}_3$ is obtained after the corresponding encoding operations and the addition of the decoy particles. P_3^* detects eavesdropping with P_2, discarding the decoy particles to get Q_3. After that, he performs the operation $V_{s_{2t-1},s_{2t}}$ according to the classical bit sequence S, and measures with MB_Z or MB_X. However, P_2 will announce whether the secret is not

Table 2 Encoding operations for different secret inputs

input	encoding operation	
	not split ($m_{2,t}=1$)	split ($m_{2,t}=0$)
00	U_{00}	$U_{00}U_{00}, U_{01}U_{01}, U_{10}U_{10}, U_{11}U_{11}$
01	U_{01}	$U_{00}U_{01}, U_{10}U_{11}$
10	U_{10}	$U_{00}U_{10}, U_{01}U_{11}$
11	U_{11}	$U_{00}U_{11}, U_{10}U_{01}$

split ($m_{2,t}=1$) or split ($m_{2,t}=0$) until P_0 receive the sequence $\widetilde{Q}_5$. Therefore, even they know the correct sequence S, they cannot infer the parity of the encoding operations by all participants. Namely, they cannot know whether the odd or even numbers of operations U_{xy} are carried out in the process of the protocol. Therefore, the correct measurement basis cannot be selected to get the correct results. Moreover, even they know $M_t=\oplus_i m_{i,t}$, they cannot know whether the $m_{1,t}$ and $m_{4,t}$ are 0 or 1, but only the summation of them.

Next, let us consider a more general attack strategy. P_1^* intercepts the signal particles, and sends a pseudo-particle sequence $\widetilde{Q}_2^*$. Each pair of particles in $\widetilde{Q}_2^*$ is:

$$|\alpha\rangle=|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle. \tag{20}$$

P_1^* continues to execute the protocol and sends $\widetilde{Q}_2^*$ to P_2. P_2 continues Step 2, splits the secret input or not according to $m_{2,t}$, encodes them into $\widetilde{Q}_2^*$ to get a new particle string $\widetilde{Q}_3^*$. At last, he sends it to P_3^*. P_3^* and P_2 pass the eavesdropping detection, then P_3^* measures the particle sequence and distinguishes what kind of encoding operations P_2 has carried out. Because the operations carried out in the encoding process are U_{xy}, which are determined by the secret inputs, there are different operations for different secret inputs shown in Table 2. P_2's different operations on quantum state $|\alpha\rangle$ result in different quantum states, as shown in Table 3.

Obviously, in order to distinguish the operations of P_2, we need to distinguish the above encoded quantum states. However, this is impossible, since we have found some interesting relationship between the encoded quantum states. Performing the encoding operation $U_{10}U_{11}$ for 01 to get $|\alpha_{01}^0\rangle$, we find that

$$|\alpha_{01}^0\rangle=|\alpha_{00}^0\rangle-|\alpha_{00}^1\rangle-|\alpha_{01}^1\rangle \text{ or } -|\alpha_{01}^0\rangle=|\alpha_{00}^0\rangle-|\alpha_{10}^1\rangle-|\alpha_{11}^1\rangle. \tag{21}$$

Table 3 Effects of different encoding operations on the pseudo-particle sequence

input	encoding operation	quantum state
00	U_{00}	$|\alpha_{00}^1\rangle=-|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle$
	$U_{00}U_{00}, U_{01}U_{01}, U_{10}U_{10}, U_{11}U_{11}$	$|\alpha_{00}^0\rangle=|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle$
01	U_{01}	$|\alpha_{01}^1\rangle=|00\rangle|u_{00}\rangle-|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle$
	$U_{10}U_{11}(-U_{00}U_{01})$	$|\alpha_{01}^0\rangle=|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle-|10\rangle|u_{10}\rangle-|11\rangle|u_{11}\rangle$
10	U_{10}	$|\alpha_{10}^1\rangle=|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle-|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle$
	$U_{01}U_{11}(-U_{00}U_{10})$	$|\alpha_{10}^0\rangle=|00\rangle|u_{00}\rangle-|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle-|11\rangle|u_{11}\rangle$
11	U_{11}	$|\alpha_{11}^1\rangle=|00\rangle|u_{00}\rangle+|01\rangle|u_{01}\rangle+|10\rangle|u_{10}\rangle-|11\rangle|u_{11}\rangle$
	$U_{10}U_{01}(-U_{00}U_{11})$	$|\alpha_{11}^0\rangle=|00\rangle|u_{00}\rangle-|01\rangle|u_{01}\rangle-|10\rangle|u_{10}\rangle+|11\rangle|u_{11}\rangle$

In addition, we also find that

$$|\alpha_{10}^{0}\rangle = |\alpha_{00}^{0}\rangle - |\alpha_{00}^{1}\rangle - |\alpha_{10}^{1}\rangle \text{ or } -|\alpha_{10}^{0}\rangle = |\alpha_{00}^{0}\rangle - |\alpha_{01}^{1}\rangle - |\alpha_{11}^{1}\rangle,$$
$$|\alpha_{11}^{0}\rangle = |\alpha_{00}^{0}\rangle - |\alpha_{00}^{1}\rangle - |\alpha_{11}^{1}\rangle \text{ or } -|\alpha_{11}^{0}\rangle = |\alpha_{00}^{0}\rangle - |\alpha_{01}^{1}\rangle - |\alpha_{10}^{1}\rangle. \tag{22}$$

Apparently, the quantum states obtained by different secret inputs after different encoding operations are linearly correlated. The necessary and sufficient condition for a configuration proposed by Chefles and Barnett [27] to be deterministically distinguished is linear independent, so the quantum states after these operations cannot be deterministically distinguished. Therefore, even P_1^* and P_3^* collusive attack P_2, P_2's secret input cannot be judged since the quantum states after operations are linearly correlated.

Thus, these participants' attacks are failure in the protocol.

4.2.4 The Semi-Honest Third Party's Attack

Since the third party P_0 is semi-honest, he also attempts to obtain a participant P_i's secret input. Furthermore, the role of P_0 in the protocol is different from other participants, he needs to prepare the initial states and send them to the next participant P_1. However, he is semi-honest, he cannot conspire with others. To be convenient, suppose P_0 wants to get the information of P_1's secret input. Since the encoding of secret input is realized by operation U_{xy}, P_0 must know what kind of operation that P_1 has carried out. Then P_0 will intercept the particles $\widetilde{Q}_2$ emitted by P_1, but in the eavesdropping detection between P_1 and P_2, he will be detected as Eve as well. So the protocol is safe for such attack.

From the above analyses, it is shown that the protocol is secure against both external and internal attacks, which means no one can access a participant's secret input without being detected.

5 Conclusion

In Grover's search algorithm, a product state of two qubits can be converted to a special target state through applying two specific unitary operations. Moreover, if the unitary operation is executed one more time, the target state will become another superposition state. Obviously, since these states are non-orthogonal, they cannot be perfect discriminated. Based on it, a new quantum secure multi-party summation with qubits is proposed in this paper. At first, two qubits, the initial state of the Grover's search algorithm, are prepared by a semi-honest third party who may misbehave on his own but cannot conspire with other participants. Then, the signal particles are transmitted among all participants who respectively performs the unitary operations representing their secret inputs. Finally, according to the parity of the number of the encoding operations, the third party measures the traveling particles in different bases and obtains the summation. In this way, all participants achieve secure summation task with the aid of this semi-honest third party. By discussing the case under external attacks and some common internal attacks, it is shown that the proposed protocol is secure, which is based on some results of Grover's search algorithm and quantum state discrimination. In addition, instead of multi-particle entangled states, only qubits are used as the information carriers, which makes the proposed protocol more feasible using current technology.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grants No. 61772134 and No. 61976053), the Natural Science Foundation of Fujian Province (Grant No. 2018J01776), the Probability and Statistics: Theory and Application (Grant No. IRTL1704), and the Program for New Century Excellent Talents in Fujian Province University.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing [C]. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, Bangalore (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem [J]. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography [J]. Rev. Modern Phys. **74**, 145 (2002)
4. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing [J]. Phys. Rev. A **59**, 1829–1834 (1999)
5. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting [J]. Phys. Rev. A **59**, 162–168 (1999)
6. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes [J]. Phys. Rev. A **69**, 052307 (2004)
7. Zhang, K.J., Zhang, X., Jia, H.Y., Zhang, L.: A new n-party quantum secret sharing model based on multiparty entangled states [J]. Quantum Inf. Process **18**, 81 (2019)
8. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries [J]. Phys. Rev. Lett. **100**, 230502 (2008)
9. Jakobi, M., Simon, C., et al.: Practical private database queries based on a quantum-key-distribution protocol [J]. Phys. Rev. A **83**, 022301 (2011)
10. Gao, F., Qin, S.J., Huang, W., Wen, Q.Y.: Quantum private query: A new kind of practical quantum cryptographic protocol [J]. Sci. China Phys. Mechan. Astron. **62**, 070301 (2019)
11. Wei, C.Y., Cai, X.Q., Wang, T.Y., Qin, S.J., Gao, F., Wen, Q.Y.: Error tolerance bound in QKD-based quantum private query [J]. IEEE J. Select. Areas Commun. **38**, 517–527 (2020)
12. Goldreich, O., Micali, S., Wigderson, A.: How to play ANY mental game [C]. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC'87), 218. New York, NY, USA (1987)
13. Lo, H.K.: Insecurity of quantum secure computations [J]. Phys. Rev. A **56**, 1154–1162 (1997)
14. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority[C]. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06), pp. 249-260. IEEE, New York (2006)
15. Hillery, M., Ziman, M., Buzek, V., Bielikova, M.: Towards quantum-based privacy and voting [J]. Phys. Lett. A **349**, 75 (2006)
16. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation [J]. Int. J. Theor. Phys. **49**, 2793–2804 (2010)
17. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication [J]. Sci. Rep. **6**, 19655 (2016)
18. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum fourier transform [J]. Quantum Inf. Process **17**, 129 (2018)
19. Lv, S.X., Jiao, X.F., Zhou, P.: Multiparty quantum computation for summation and multiplication with mutually unbiased bases [J]. Int. J. Theor. Phys. **58**, 2872–2882 (2019)
20. Sutradhar, K., Om, H.: Hybrid quantum protocols for secure multiparty summation and multiplication [J]. Sci. Rep. **10**, 1–9 (2020)
21. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack [J]. Phys. Rev. Lett. **79**, 325 (1997)
22. Hsu, L.Y.: Quantum secret-sharing protocol based on Grover's algorithm [J]. Phys. Rev. A **68**, 022306 (2003)
23. Cao, H., Ma, W.P.: Multiparty quantum key agreement based on quantum search algorithm [J]. Sci. Rep. **7**, 45046 (2017)
24. Hao, L., Li, J.L., Long, G.L.: Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. Sci. China Phys. Mechan. Astron. **53**, 491–495 (2010)
25. Wang, C., Hao, L., Song, S.Y., Long, G.L.: Quantum direct communication based on quantum search algorithm [J]. Int. J. Theor. Phys. **8**, 443–450 (2010)

26. Zhang, W.W., Li, D., Song, T.T., Li, Y.B.: Quantum private comparison based on quantum search algorithm [J]. Int. J. Theor. Phys. **52**, 1466–1473 (2013)
27. Chefles, A., Barnett, S.M.: Optimum unambiguous discrimination between linearly independent symmetric states [J]. Phys. Lett. A **250**, 223–229 (1998)