An Dynamic Protocol for the Quantum Secure Multi-party Summation Based On Commutative Encryption

Wen Liu[1,2(✉)] and Min-Yao Ma[3]

[1] School of Computer Science and Cybersecurity, Communication University of China, Beijing, China
lw_8206@163.com
[2] Key Laboratory of Convergent Media and Intelligent Technology, Communication University of China, Ministry of Education, Beijing, China
[3] Department of Mathematics and Computer Science, Guizhou Education University, Guiyang, China

Abstract. A dynamic protocol for the quantum secure multi-party summation based on commutative encryption is proposed. Without using the entangled character, joint measurement, n parties can encrypt their private information and privately get the summation of their private information using commutative encryption. Any m parties can dynamically participate and drop out the proposed protocol. Correctness analysis shows that the proposed protocol can be used to get the summation of their private information correctly. Security analysis shows that the proposed protocol can resist the general active attacks from an outside eavesdropper. And it can overcomes the problem of information leakage. In theory, our protocol can be used to build complex secure protocols for other multiparty computations and also lots of other important applications in distributed networks.

Keywords: Quantum secure multi-party summation · Dynamic · Commutative encryption · Correctness · Security

1 Introduction

Many quantum cryptographic protocols, such as quantum key distribution (QKD) [1–7], quantum secret sharing (QSS) [8–11], quantum stegonagraphy [12],

Supported by the National Natural Science Foundation of China (Grant No.61502437,Grant No.61773352); The China Scholarship Council(No.201707055033); The Fundamental Research Funds for the Central Universities (Grant No.2018CUCTJ017); The Science and Technology Program of Guizhou Province (No.QianKeHeJiChu[2016]1115); The Science and Technology Platform and Talent Team Project of Guizhou Province (No. QianKeHePingTaiRenCai [2017]5501; QianKeHePingTaiRenCai [2016]5609); The Youth Science and Technology Talent Program of Department of Education of Guizhou Province (No. QianJiaoHeKYZi[2016]220).

© Springer Nature Switzerland AG 2019
X. Sun et al. (Eds.): ICAIS 2019, LNCS 11632, pp. 537–547, 2019.
https://doi.org/10.1007/978-3-030-24274-9_49

private quantum computation [13], and so on, have been proposed to solve various secure problems.

Secure multi-party summation problem was introduced by Goldreich in [14] and it is a important problem in secure multi-party computation. In the problem of secure multi-party summation, we supposed that there are n parties $P_1, P_2, .., P_n$ and they want to correctly calculate a summation function using their private information $x_1, x_2, ..., x_n$. It is a fundamental primitive of secure multi-party computation and can be applied in secret sharing, electronic voting, secure sorting, data mining and so on.

Secure multi-party summation problem has been extended to the quantum field and some researchers have investigated this problem based on quantum states. In 2006, a multi-party summation protocol with the two-particle N-level entangled states was proposed by Hillery et al. [15]. In 2007, a secure quantum addition module $n + 1$ based on non-orthogonal single states was presented by Du et al. [16]. In 2010, a quantum summation protocol with the multi-particle entangled GHZ states was presented by Chen et al. [17]. Then, Zhang et al. employed single photons in both polarization and spatial-mode degrees of freedom to design a quantum summation protocol [18] and proposed a quantum summation protocol based on the genuinely maximally entangled six-qubit states [19]. In 2016, a quantum summation protocol based on quantum Fourier transform and CNOT gate operators was presented by Shi et al. [20]. In 2017, Liu et al. [21] used Pauli matrices operations to encode information and Hadamard matrix to extract information and present a quantum secure multi-party summation protocol.

In this paper, we proposed a dynamic secure multi-party quantum summation protocol based on commutative encryption. In our protocol, n parties can privately get the result of $x_1 + x_2 + ... + x_n$ using the rotation operations and single-state measurement, which are easier to be realized with current technologies. The participants can dynamically be added or deleted in our protocol and it is more flexible in practice. Compared to other previous protocols, our protocol is simple and the entangled character, joint measurement of quantum states are not needed. The security of the presented protocol is also proved to be secure against both outside and participant attacks.

The structure of this paper is as follows: we propose a quantum dynamic multi-party summation protocol based on commutative encryption in Sect. 2; and we analyze the correctness and security of this protocol in Sect. 3. A brief discussion and the concluding summary are given in Sect. 4.

2 The Quantum Dynamic Secure Multi-party Summation Protocol based on Commutative Encryption

2.1 Quantum Commutative Encryption Scheme

Before presenting the protocol, we firstly give a description of the quantum commutative encryption scheme [22,23]. Note that binary data can be encoded

by using horizontal and vertical polarization (i.e., the horizontally polarized photon $|0\rangle$ represents zero in a binary representation and the vertically polarized photon $|1\rangle$ represents one). And, all transmitted polarized photons are encrypted before the transmission. The secret key is defined as a set of angles $K = \{\theta_i : 0 \leq \theta_i < \pi, i = 1, 2, 3, ..., n\}$ for an n-bit message, where the subscript indicates the position of the bit in the message where the encryption with the angle θ_i is applied, and the rotation operation as encryption (i.e., a process o f disguising to hide its original polarization). Let $E_K[M]$ be an encryption of data M with a secret key K. Then, in order to read the disguised photons correctly, the receiver must rotate the transmitted photon by the angle θ_i in the opposite direction of what the sender rotated. This operation is defined as decryption. Let $D_K[M]$ be an decryption of data M with a secret key K. These operations can be represented mathematically as shown below.

In the following discussion, without losing generality, we can assume that a message M is a single photon encoded as $M : |\psi_0\rangle = |0\rangle$ for simplicity. By using the Jones matrix representation, the rotation operation can be represented by the following matrix:

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

A sender encrypts the data qubit $|\psi\rangle$ with θ_A.(θ_A is randomly chosen and is shared between a sender and a receiver prior to the communication.)

$$\begin{aligned} E_K[M] = R(\theta_A)|0\rangle &= \begin{pmatrix} \cos\theta_A & \sin\theta_A \\ -\sin\theta_A & \cos\theta_A \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta_A \\ -\sin\theta_A \end{pmatrix} = \cos\theta_A|0\rangle - \sin\theta_A|1\rangle = |\psi_1\rangle \end{aligned} \tag{2}$$

The sender sends the superposition states $|\psi_1\rangle$ to a receiver.

Before the receiver measures the received photon, he needs to rotate the received photon by θ_A in the opposite direction o f what the sender rotated. This decryption can be represented as follows:

$$\begin{aligned} R(-\theta_A)|\psi_1\rangle &= \begin{pmatrix} \cos(-\theta_A) & \sin(-\theta_A) \\ -\sin(-\theta_A) & \cos(-\theta_A) \end{pmatrix} \begin{pmatrix} \cos\theta_A \\ -\sin\theta_A \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\theta_A + \sin^2\theta_A \\ \sin\theta_A.\cos\theta_A - \cos\theta_A.\sin\theta_A \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle. \end{aligned} \tag{3}$$

The main advantage of this encryption/decryption scheme is that a receiver does not have to decrypt a ciphertext in the same order as it was encrypted with different secret keys when data is encrypted more than once (e.g., i times) as follows.

$$\begin{aligned} E_{\theta_1}[E_{\theta_2}[...E_{\theta_{i-2}}[E_{\theta_{i-1}}[E_{\theta_i}[M]]]...]] &= E_{\theta_1}[E_{\theta_2}[...E_{\theta_{i-2}}[E_{\theta_{i-1}}[R(\theta_i).|\psi\rangle]]...]] \\ &= E_{\theta_1}[E_{\theta_2}[...E_{\theta_{i-2}}[R(\theta_{i-1}).R(\theta_i).|\psi\rangle]...]] \\ &= E_{\theta_1}[E_{\theta_2}[...E_{\theta_{i-2}}[R(\theta_{i-1}+\theta_i).|\psi\rangle]...]] \\ &= R(\theta_1+\theta_2+...+\theta_{i-2}+\theta_{i-1}+\theta_i).|\psi\rangle \end{aligned} \tag{4}$$

Evidently, the encrypted data are irrespective of the order of encryptions. Also, the commutative relation of decryptions is trivial. In short, even if a sender encrypts a message with K_1 and then encrypts it with K_2, a receiver can decrypt the ciphertext with K_1 and then decrypt it with K_2.

$$D_{K_1}[D_{K_2}[E_{K_2}[E_{K_1}[M]]]] = D_{K_1}[D_{K_2}[E_{K_1}[E_{K_2}[M]]]] = M \tag{5}$$

Another notable feature o f this encryption scheme is that the original message (plaintext) in the encrypted data (ciphertext) can be modified without decrypting the ciphertext if the plaintext is known. For example, let us assume that the plaintext is a single bit, say, logic-one(i.e.,$M = |1\rangle$). Now, Alice encrypts it as $E_\theta[M] = R(\theta).|1\rangle = \sin\theta\,|0\rangle + \cos\theta\,|1\rangle$. If Alice wants to change the plaintext from logic-one to logic-zero after encryption, Alice rotates the quantum state by 90 degrees(i.e., $\pi/2$ radians).

$$\begin{aligned} R(\pi/2).E_\theta[|1\rangle] &= R(\pi/2).R(\theta)\,|1\rangle = R(\pi/2+\theta)\,|1\rangle \\ &= \begin{pmatrix} \cos(\pi/2+\theta) & \sin(\pi/2+\theta) \\ -\sin(\pi/2+\theta) & \cos(\pi/2+\theta) \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} -\sin(\theta) & \cos(\theta) \\ -\cos(\theta) & -\sin(\theta) \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos(\theta) \\ -\sin(\theta) \end{pmatrix} \\ &= \cos(\theta)\,|0\rangle - \sin(\theta)\,|1\rangle = R(\theta).|0\rangle = E_\theta[|0\rangle] \end{aligned} \tag{6}$$

By using this technique, receivers can perform exclusive-OR (XOR) operations between the encrypted states and classical bits without decrypting if the receiver needs it for some applications. For instance, suppose the input is 1, we have $K_2 = \pi/2$, then

$$\begin{aligned} E_{\pi/2}E_{K_1}\,|0\rangle &= E_{K_1}R(\pi/2)\,|0\rangle = E_{K_1}\,|1\rangle = E_{K_1}\,|1\oplus 0\rangle \\ E_{\pi/2}E_{K_1}\,|1\rangle &= E_{K_1}R(\pi/2)\,|1\rangle = E_{K_1}\,|1\rangle = E_{K_1}\,|1\oplus 1\rangle \end{aligned} \tag{7}$$

where $\oplus$ denotes the addition module 2.

2.2 The Basic Scheme

Supposed that there are n parties, $P_1, P_2, ..., P_n$, where P_j has a secret sequence $I_j = (I_j^1, I_j^2, ..., I_j^L)(j = 1, 2, ..., n)$. They can calculate the summation $\oplus\sum_{j=1}^{n} I_j$, where $\sum\oplus$ denotes the addition module 2. In this case, one player, suppose that the player P_1 can act as TP. The detail of our quantum dynamic secure multiparty summation protocol is described as follows:

(1) P_1 randomly generates a secret key $\theta_1 = \theta_1^1\theta_1^2, ..., \theta_1^L$, where $\theta_1^1\theta_1^2, ..., \theta_1^L$. It prepares a L-length sequence of photons $\left|\psi_1^1\right\rangle\left|\psi_1^2\right\rangle, ..., \left|\psi_1^L\right\rangle$ according to its secret sequence I_1, if $I_1^i = 0$, $\left|\psi_1^i\right\rangle = |0\rangle$; if $I_1^i = 1$, $\left|\psi_1^i\right\rangle = |1\rangle$. P_1 uses θ_1 to encrypt $\left|\psi_1^1\right\rangle\left|\psi_1^2\right\rangle, ..., \left|\psi_1^L\right\rangle$ and gets the result states $R(\theta_1^1)\left|\psi_1^1\right\rangle \otimes ... \otimes R(\theta_1^L)\left|\psi_1^L\right\rangle$, where $R(\theta_1^i)(i = 1, 2, ..., L)$ is the rotation operation.

P_1 prepares $L^{'}$ particles, which are randomly chosen from four photon states $|+y\rangle, |-y\rangle, |+\rangle, |-\rangle$ and randomly inserts the sequences $S_1^{'}$ of $L^{'}$ particles into

the result states $R(\theta_1^1)\left|\psi_1^1\right\rangle \otimes ... \otimes R(\theta_1^L)\left|\psi_1^L\right\rangle$ to form a new states sequence S_1. P_1 records the insert positions sequence Po_1 and sends S_1 to P_2.

For $j = 2, ..., n$:

(2) After receiving S_{j-1}, P_{j-1} and P_j perform the eavesdropping check. P_{j-1} announces the insert positions Po_{j-1} and the measuring bases of $S_{j-1}^{'}$. If the insert particle is $|+y\rangle$ or $|-y\rangle$, the measuring basis is $|+y\rangle$ or $|-y\rangle$ basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then P_j chooses the $L^{'}$ particles from S_{j-1} according to the insert positions Po_{j-1} and measures these particles according to the measuring bases. P_{j-1} and P_j can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in S_{j-1} and continue to the next step.

(3) P_j performs the commutative encryption on the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{K=2}^{j-1}\right.$ $I_k^1 \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ according to his secret sequence I_j: if $I_j^i = 0$, the encryption key $\theta_j^i = 0$; if $I_j^i = 1$, the encryption key $\theta_j^i = \pi/2$.

After performing the commutative encryption, the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{K=2}^{j-1}\right.$ $I_k^1 \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ become $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle$.

P_j prepares $L^{'}$ particles, which are randomly chosen from four photon states $|+y\rangle, |-y\rangle, |+\rangle, |-\rangle$ and randomly inserts the sequences $S_j^{'}$ of $L^{'}$ particles into the result states $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$ to form a new states sequence S_1. P_j records the insert positions sequence Po_j and sends S_j to P_{j+1}(if $j = n$, P_n send S_n to P_1).

(4) When P_1 has received the photons from P_n, he first does eavesdropping check with P_n. If there is no eavesdropper, he gets photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L\right\rangle)$ and uses the secret key $\theta_1 = \theta_1^1\theta_1^2, ..., \theta_1^L$ to decrypt these photons $R(-\theta_1^1)R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1\right\rangle), ..., R(-\theta_1^L)R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L\right\rangle)$. P_1 measures $\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1\right\rangle, ..., \left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L\right\rangle$ and gets the summation of n parties' secret information.

2.3 Add Participants

We assume m participants $P_{n+1}, ..., P_{n+m}$ want to join the old n participants $P_1, P_2, ..., P_n$ before the step(4) of the basic protocol. Each participant of $P_{n+1}, ..., P_{n+m}$ has a secret sequence $I_j = (I_j^1, I_j^2, ..., I_j^L)(j = n+1, n+2, ..., n+m)$. The protocol of adding participants is described as follows:

For $j = n+1, ..., n+m$:

(1) After receiving S_{j-1}, P_{j-1} and P_j perform the eavesdropping check.

(2) P_j performs the commutative encryption on the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ according to his secret sequence I_j: if $I_j^i = 0$, the encryption key $\theta_j^i = 0$; if $I_j^i = 1$, the encryption key $\theta_j^i = \pi/2$.

After performing the commutative encryption, the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ become $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$.

P_j prepares L' particles, which are randomly chosen from four photon states $|+y\rangle, |-y\rangle, |+\rangle, |-\rangle$ and randomly inserts the sequences S_j' of L' particles into the result states $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$ to form a new states sequence S_1. P_j records the insert positions sequence Po_j and sends S_j to P_{j+1}(if $j = n+m$, P_{n+m} send S_{n+m} to P_1).

(3) When P_1 has received the photons from P_{n+m}, he first does eavesdropping check with P_{n+m}. If there is no eavesdropper, he gets photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n+m} I_k^L\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n+m} I_k^L\right\rangle)$ and uses the secret key $\theta_1 = \theta_1^1\theta_1^2, ..., \theta_1^L$ to decrypt these photons:$R(-\theta_1^1)R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n+m} I_k^1\right\rangle), ..., R(-\theta_1^L)R(\theta_1^L)\ (\left|\psi_1^L \oplus \bigoplus_{k=2}^{n+m} I_k^L\right\rangle)$. P_1 measures $\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n+m} I_k^1\right\rangle, ..., \left|\psi_1^L \oplus \bigoplus_{k=2}^{n+m} I_k^L\right\rangle$ and gets the summation of $n+m$ parties' secret information.

2.4 Delete Participants

Without loss of generality, we assume the original participants are $P_1, P_2, ..., P_n$, and m participants $P_2, P_3, ..., P_m + 1$ want to leave. The protocol of deleting participants is described as follows:

(1) Before P_1 decrypts photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L\right\rangle)$, $P_2, P_3, ..., P_m + 1$ can leave the protocol.

For $j = 2, 3, ..., m+1$:

(2) P_j performs the commutative encryption on the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \oplus \bigoplus_{k=2}^{j-1} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ according to his secret sequence I_j(if $I_j^i = 0$, the encryption key $\theta_j^i = 0$; if $I_j^i = 1$, the encryption key $\theta_j^i = \pi/2$).

After performing the commutative encryption, the photons $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \oplus \bigoplus_{k=2}^{j-1} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ become $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$.

P_j prepares L' particles, which are randomly chosen from four photon states $|+y\rangle, |-y\rangle, |+\rangle, |-\rangle$ and randomly inserts the sequences S_j' of L' particles into the result states $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle)$ to form a new states sequence S_j. P_j records the insert positions sequence Po_j and sends S_j to P_{j+1}(if $j = m+1$, $P_m + 1$ send S_j to P_1).

P_{j+1} has received the photons from P_j, he also needs to do the eavesdropping check like the eavesdropping check in the basic scheme.

(3) P_1 decrypts $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \bigoplus_{k=2}^{m+1} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \bigoplus_{k=2}^{m+1} I_k^L\right\rangle)$ and gets the summation of $n - m$ parties' secret information.

3 Analysis

3.1 Correctness Analysis

In the step(1) of our basic protocol, P_1 gets $E_{\theta_1}(\left|\varphi_1^1\right\rangle \left|\varphi_1^2\right\rangle, ..., \left|\varphi_1^L\right\rangle) = R(\theta_1^1)\left|\psi_1^1\right\rangle \otimes ... \otimes R(\theta_1^L)\left|\psi_1^L\right\rangle$. P_1 sends the encrypted states to P_2.

$P_2, P_3, ..., P_n$ choose the encryption key according to their secret sequences and sequentially execute the commutative encryption on the encrypted states of P_1. After $P_2, P_3, ..., P_n$ sequentially perform the commutative encryption, they get the new states $R(\theta_n^1)R(\theta_{n-1}^1)...R(\theta_2^1)R(\theta_1^1)(\left|\psi_1^1\right\rangle) \otimes ... \otimes R(\theta_n^L)R(\theta_{n-1}^L)... R(\theta_2^L)R(\theta_1^L)(\left|\psi_1^L\right\rangle)$.

If there is no eavesdropper between these parties, the new states according to Eq. (7) become as follows:

$$\begin{aligned}
&R(\theta_n^1)R(\theta_{n-1}^1)...R(\theta_2^1)R(\theta_1^1)(\left|\psi_1^1\right\rangle) \otimes ... \otimes R(\theta_n^L)R(\theta_{n-1}^L)...R(\theta_2^L)R(\theta_1^L)(\left|\psi_1^L\right\rangle) \\
&= R(\theta_n^1)R(\theta_{n-1}^1)...R(\theta_1^1)(\left|\psi_1^1 \oplus I_2^1\right\rangle) \otimes ... \otimes R(\theta_n^L)R(\theta_{n-1}^L)...R(\theta_1^L)(\left|\psi_1^L \oplus I_2^L\right\rangle) \\
&= R(\theta_1^1)(\left|\psi_1^1 \oplus I_2^1 \oplus ... \oplus I_{n-1}^1 \oplus I_n^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus I_2^L ... \oplus I_{n-1}^L \oplus I_n^L\right\rangle) \\
&= R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L\right\rangle)
\end{aligned} \tag{8}$$

When P_1 checks the eavesdropper, he can use his secret key to decrypt and measure the new states. Then he can get $\bigoplus_{k=1}^{n} I_k^1, ..., \bigoplus_{k=1}^{n} I_k^L$.

In the protocol of adding participants, there are m participants want to join the quantum dynamic secure multi-party summation protocol. They performs the commutative encryption on $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ according to his secret sequence I_j, the new states according to Eq. (7) become as follows:

$$\begin{aligned}
&R(\theta_{n+m}^1)...R(\theta_{n+1}^1)R(\theta_n^1)...R(\theta_1^1)(\left|\psi_1^1\right\rangle) \otimes ... \otimes R(\theta_{n+m}^L)...R(\theta_{n+1}^L)R(\theta_n^L)...R(\theta_1^L)(\left|\psi_1^L\right\rangle) \\
&= R(\theta_{n+m}^1)...R(\theta_1^1)(\left|\psi_1^1 \oplus I_2^1\right\rangle) \otimes ... \otimes R(\theta_{n+m}^L)...R(\theta_1^L)(\left|\psi_1^L \oplus I_2^L\right\rangle) \\
&= R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n+m} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n+m} I_k^L\right\rangle)
\end{aligned} \tag{9}$$

When P_1 checks the eavesdropper, he can use his secret key to decrypt and measure the new states. Then he can get $\bigoplus_{k=1}^{n+m} I_k^1, ..., \bigoplus_{k=1}^{n+m} I_k^L$.

In the protocol of deleting participants, m participants want to leave the quantum dynamic secure multi-party summation protocol. They performs the commutative encryption on $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j-1} I_k^L\right\rangle)$ according to his secret sequence I_j, the new states according to Eq. (7) become as follows:

$$\begin{aligned}
&R(\theta_{m+1}^1)...R(\theta_2^1)R(\theta_n^1)...R(\theta_1^1)(\left|\psi_1^1\right\rangle) \otimes ... \otimes R(\theta_{m+1}^L)...R(\theta_2^L)R(\theta_n^L)...R(\theta_1^L)(\left|\psi_1^L\right\rangle) \\
&= R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{n} I_k^1 \oplus \bigoplus_{k=2}^{m+1} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{n} I_k^L \oplus \bigoplus_{k=2}^{m+1} I_k^L\right\rangle) \\
&= R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=m+2}^{n} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=m+2}^{n} I_k^L\right\rangle)
\end{aligned} \tag{10}$$

When P_1 checks the eavesdropper, he can use his secret key to decrypt and measure the new states. Then he can get $I_1^1 \oplus \bigoplus_{k=m+2}^{n} I_k^1, ..., I_1^L \oplus \bigoplus_{k=m+2}^{n} I_k^L$.

3.2 Security Analysis

Firstly, we show that the outside attack is invalid to our protocol. Secondly, we show that the n parties can not get any information about the private information of others.

3.3 Outside Attack

We analyze the possibility of the outside eavesdropper to get information about $I_1, I_2, ..., I_n$ in every step of protocol. In the basic scheme, the chance of attack from the outside eavesdropper is to attack the quantum channel in Step (1)(3). In Step (1)(3), the outside eavesdropper can attack the quantum channel when P_i sent $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$ to P_{i+1}. Because of the use of nonorthogonal decoy photons, we performed eavesdropper checking process in Step (2)(4) and several kinds of outside attacks, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack, were detected with nonzero probability. Anyone who do not know the insert positions and bases of decoy particles cannot distinguish the decoy particles and the signal particles. For some special attacks, such as the photon-number-splitting (PNS) attack, the decoy-photon Trojan horse attack and the invisible photon Trojan horse attack, participants can defeat these attacks by using some beam splitters to split the sampling signals chosen for eavesdropping check before their operations and inserting filters in front of their devices to filter out the photon signal with an illegitimate wavelength. So, our quantum protocol is robust against outside attack.

3.4 Participant Attack

The term "participant attack", which emphasizes that the attacks from dishonest users are generally more powerful and should be paid more attention to, is first proposed by Gao et al. in Ref. [24] and has attracted much attention in the cryptanalysis of quantum cryptography [25–30]. We analyze the possibility of the n parties to get information about $I_1, I_2, ..., I_n$ in our protocol. We firstly analyze the case that P_i wants to learn the private information of other $n-1$ parties. Secondly, we analyze the case that P_1 wants to learn the private information of $P_2, ..., P_n$.

Case 1: P_i wants to learn the private information of other $n-1$ parties.

In our protocol, P_i can get $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$. The secret key θ_1 is randomly chosen by P_1. Without the secret key, P_i cannot decrypt and measure these phones. So P_i cannot infer any information about the private information of other $n-1$ parties.

Case 2: P_1 wants to learn the private information of $P_2, ..., P_n$.

In our protocol, P_1 knows the secret key θ_1 and also gets phones $R(\theta_1^1)(\left|\psi_1^1 \oplus \bigoplus_{k=2}^{j} I_k^1\right\rangle) \otimes ... \otimes R(\theta_1^L)(\left|\psi_1^L \oplus \bigoplus_{k=2}^{j} I_k^L\right\rangle)$. P_1 decrypts and measures these photons.

Although he can get the summation of n parties' secret information, he cannot exactly know $I_i (i = 1, 2, ..., L)$. So P_1 cannot infer any information about the private information of $P_2, ..., P_n$.

4 Discussion and Conclusions

In summary, we have put forward a dynamic quantum protocol to compute secure multiparty summation. In our protocol, n parties use the commutative encryption to encrypt the photons which include the private information of $P_1, P_2, ..., P_n$. And P_1 decrypts and measures the photons to get $\overset{n}{\underset{k=1}{\oplus}} I_k^1, ..., \overset{n}{\underset{k=1}{\oplus}} I_k^L$. Any m parties can participate and quit this protocol. Our protocol can not only withstand outside attacks, but also preserve the privacy of $P_1, P_2, ..., P_n$'s information. Furthermore, our quantum summation protocol can be generalized to compute lots of secure multiparty numerical computations.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **67**, 557–559 (1992)
4. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**, 042315 (2003)
5. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution without alternative measurements and rotations. Phys. Lett. A **349**, 53–58 (2006)
6. Guo, F.Z., Gao, F., Wen, Q.Y., Zhu, F.C.: A two-step channel-encrypting quantum key distribution protocol. Int. J. Quantum Inf. **8**, 1013–1022 (2010)
7. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution by constructiong nonorthogonal states with Bell states. Int. J. Mod. Phys. B **24**, 4611–4618 (2010)
8. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 052307 (1999)
9. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**, 162–168 (2004)
10. Deng, F.G., Zhou, H.Y., Long, G.L.: Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys. Lett. A **337**, 329–334 (2005)
11. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**, 3647–3651 (2009)
12. Qu, Z., Zhu, T., Wang, J., Wang, X.: A novel quantum stegonagraphy based on brown states. CMC Comput. Mater. Continua **56**(1), 47–59 (2018)
13. Liu, W., Chen, Z., Liu, J., Su, Z., Chi, L.: Full-blind delegating private quantum computation. CMC Comput. Mater. Continua **56**(2), 211–223 (2018)

14. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, p. 218. ACM, New York (1987)
15. Hillery, M., Ziman, M., Buek, V., Bielikov, M.: Phys. Lett. A **349**(1–4), 75 (2006)
16. Du, J.Z., Chen, X.B., Wen, Q.X., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin-Ch. Ed. **56**, 6214–6219 (2007)
17. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793–2804 (2010)
18. Zhang, C., Sun, Z.-W., Huang, X.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
19. Zhang, C., Sun, Z., Huang, Y.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933–941 (2014)
20. Shi, R., Yi, M., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
21. Jakobi, M., et al.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**(2), 022301 (2011)
22. Kanamori, Y.: Quantum encryption and authentication protocols. Ph.D thesis, University of Alabama in Huntsville (2006)
23. Sun, Z., Huang, J., Wang, P.: Efficient multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. **15**, 2101 (2016)
24. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
25. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secretsharing protocol. Phys. Rev. A **76**, 062324 (2007)
26. Lin, S., Gao, F., Guo, F.Z., et al.: Comment on multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **76**, 036301 (2007)
27. Lin, S., Wen, Q.Y., Gao, F., et al.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553 (2008)
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. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
30. Guo, F.Z., Qin, S.J., Gao, F., et al.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)