International Journal of Theoretical Physics (2020) 59:1638–1643
https://doi.org/10.1007/s10773-020-04431-2

Multi-Party Quantum Summation within a *d*-Level Quantum System

Duan Ming-Yi[1]

Received: 8 December 2019 / Accepted: 26 February 2020 / Published online: 5 March 2020

Abstract
At present, there are some quantum summation protocols calculating the addition in a bit-by-bit way so that they are inefficient and unpractical in certain circumstances. In this paper, a secure multi-party quantum summation protocol within a *d*-level quantum system is constructed by using the qudit shifting operation, where the encoded photons are transmitted in a circular way. The proposed protocol can calculate the addition of modulo ***d*** in an integer-by-integer way rather than a bit-by-bit way. The security analysis result shows that the proposed protocol is secure against both the outside attack and the participant attack.

Keywords Multi-party quantum summation · *d*-level quantum system · Qudit shifting operation

1 Introduction

Secure multi-party summation is a sub-field of secure multi-party computation, and aims to obtain the correct summation result while keeping the inputs of parties secret. In the years of 2002 and 2003, Heinrich et al. studied quantum summation with an application to integration [1] and quantum Boolean summation with repetitions in the worst-average setting [2]. In 2006, Hillery et al. [3] constructed a secure multi-party quantum summation scheme with two-particle *N*-level entangled states which computes the summation in the voting procedure. In 2007, Du et al. [4] proposed a secure multi-party quantum summation scheme with non-orthogonal states, which can compute the addition modulo $n+1$. Here, n denotes the number of parties. In 2010, Chen et al. [5] suggested a secure multi-party quantum summation protocol based on three-photon GHZ states and single photons, which can only compute the addition modulo 2. In 2014, Zhang et al. [6]

✉ Duan Ming-Yi
duanmingyi2020@163.com

[1] College of Information and Engineering, Zhengzhou Institute of Technology, Zhengzhou 450044, People's Republic of China

designed a quantum summation protocol with single photons in both polarization and spatial-mode degrees of freedom, which can only compute the addition modulo 2. In 2015, Zhang et al. [7] put forward a three-party quantum summation protocol with six-qubit maximally entangled states, which can only compute the addition modulo 2. In 2016, Shi et al. [8] designed a quantum summation protocol based on quantum Fourier transform, controlled-not operation, oracle operation and inverse quantum Fourier transform, which computes the addition modulo N in an integer-by-integer way rather than a bit-by-bit way. In 2017, Shi and Zhang [9] put forward a common quantum solution to a class of particular two-party summation problems; Zhang et al. [10] constructed a multi-party quantum summation protocol without a trusted TP by using single particles, which can only compute the addition modulo 2.

Based on the above analysis, this paper concentrates on constructing a secure multi-party quantum summation protocol within a d-level quantum system by using the qudit shifting operation, where the addition of modulo d is computed in an integer-by-integer way rather than a bit-by-bit way.

The rest of this paper is arranged as follows: in Sect. 2, the multi-party quantum summation protocol within a d-level quantum system is proposed; in Sect. 3, the security of the proposed protocol is analyzed; and in Sect. 4, the conclusion is given.

2 The Multi-Party Quantum Summation Protocol within a d-Level Quantum System

The two common conjugate bases of a d-level quantum system, C_1 and C_2, are defined as.

$$C_1 = \{|k\rangle\}, \quad k = 0, 1, \cdots, d-1, \tag{1}$$

$$C_2 = \{F|k\rangle\} = \left\{ \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jk} |j\rangle \right\}, \ \omega = e^{\frac{2\pi i}{d}}, \ k = 0, 1, \cdots, d-1, \tag{2}$$

where F is the dth order discrete quantum Fourier transform, and $\omega = e^{\frac{2\pi i}{d}}$. Here, each element in the set C_1 is orthogonal to the others. Similarly, each element in the set C_2 is also orthogonal to the others.

One generalized unitary operation of a d-level quantum system is defined as

$$U_X = \sum_{u=0}^{d-1} |u \oplus 1\rangle\langle u,| \tag{3}$$

which represents the qudit shifting operation. Here, the symbol '$\oplus$' denotes the addition modulo d. Apparently, after the state $|r\rangle$ ($r \in \{0, 1, \ldots, d-1\}$) is performed with U_X k times, its state is changed into $|r \oplus k\rangle$.

There are n parties, $P_1, P_2, \cdots, P_n$. Assume that P_i has a random integer sequence of length N, $K_i = \left(k_i^1, k_i^2, \ldots, k_i^N\right)$, where $k_i^t \in \{0, 1, \ldots, d-1\}$, $i = 1, 2, \ldots, n$, $t = 1, 2, \ldots, N$. The proposed

multi-party quantum summation protocol within a d-level quantum system is made up of the following steps.

Step 1. P_1 generates $2(N+\delta)$ d-level single photons. Here, $N+\delta$ single photons are in the set of $V_1 = \{|r\rangle\}_{r=0}^{d-1}$ and denoted as $S = (|r_1\rangle, |r_2\rangle, \ldots, |r_{N+\delta}\rangle)$, where $r_j \in \{0, 1, \ldots, d-1\}, j = 1, 2, \ldots, N+\delta$. The other $N+\delta$single photons are in the set of $V_2 = \{F|r\rangle\}_{r=0}^{d-1}$ and denoted as $T = (|v_1\rangle, |v_2\rangle, \ldots, |v_{N+\delta}\rangle)$, where $j = 1, 2, \ldots, N+\delta$. Finally, P_1 mixes sequences S and T randomly to form a new sequence S', and sends it to P_2.

Step 2. After P_2 receives S', P_2 performs a random times of U_X on each photon of sequence S'. Then, P_2 reorders the photons of sequence S' and sends them together to P_3. Afterward, each of P_3, P_4, $\cdots$, P_n does the similar thing as P_2 one after another. After all photons return back to P_1, P_1 only needs to perform the operation of a random times of U_X.

After each of $P_2, P_3, \ldots, P_n$ tells P_1 the orders of photons in their respective hand,P_1 restores all photons in his hand to the original orders. Here, x_i^j is used to denote the times of U_X P_i performs on the jth photon of sequence S, where $x_i^j \in \{0, 1, \ldots, d-1\}$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, N+\delta$. And y_i^j is used to denote the times of U_X P_i performs on the jth photon of sequence T, where $y_i^j \in \{0, 1, \ldots, d-1\}$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, N+\delta$. After the encoding operations of $P_2, P_3, \ldots, P_n, P_1$, the photons of sequence S are changed into.

$$\left(\left|r_1 \oplus x_1^1 \oplus x_2^1 \oplus \ldots \oplus x_n^1\right\rangle, \left|r_2 \oplus x_1^2 \oplus x_2^2 \oplus \ldots \oplus x_n^2\right\rangle, \ldots, \left|r_{N+\delta} \oplus x_1^{N+\delta} \oplus x_2^{N+\delta} \oplus \ldots \oplus x_n^{N+\delta}\right\rangle\right),$$

which is denoted as $\left(\left|r_1'\right\rangle, \left|r_2'\right\rangle, \ldots, \left|r_{N+\delta}'\right\rangle\right)$, while the photons of sequence T are kept unchanged, according to Theorem 1 of Ref. [11].

Step 3. In order to check whether the communication is secure or not, P_1 uses the basis V_2 to measure each photon of sequence T. If there is no Eve on the line, the state of each photon will be kept unchanged.

In addition, P_1 randomly chooses δ photons from sequence S to check the security of communication with $P_2, P_3, \ldots, P_n$as follows: (1) P_1 uses the basis V_1 to measure these δ photons, and tells $P_2, P_3, \ldots, P_n$ their positions; (2) each of $P_2, P_3, \ldots, P_n$ publishes his encoding operations of these δ photons and their corresponding orders after his reordering operation; (3) P_1 checks whether his measurement result of each of these δ photons is corresponding to the encoding operations of $P_2, P_3, \ldots, P_n$ and himself.

If the quantum channel is verified to be secure after the above two kinds of security checks, the check photons will be dropped and the communication will be continued; otherwise, it will be terminated and started from Step 1.

Step 4. P_1 uses the basis V_1 to measure the left N photons in sequence S. The measurement results are denoted as $R = \left(r_1', r_2', \ldots, r_N'\right)$, where r_t' is the measurement result of the tth photon among these N photons, and $t = 1, 2, \ldots, N$. Let k_i^t denote the times of U_X P_i has performed on the tth photons among these N photons, where $k_i^t \in \{0, 1, \ldots, d-1\}$, $i = 1, 2, \ldots, n$, $t = 1, 2, \ldots, N$. Finally, P_1 obtains the summation results of random integer sequences from all parties by calculating

$$\begin{aligned}\left(r_t^{'}-r_t\right)\mathrm{mod}d &= \left(r_t\oplus k_1^t\oplus k_2^t\oplus\ldots\oplus k_n^t-r_t\right)\mathrm{mod}d\\ &= \left[\left(r_t+\sum_{i=1}^{n}k_i^t\right)\mathrm{mod}d-r_t\right]\mathrm{mod}d\\ &= \left(r_t+\sum_{i=1}^{n}k_i^t-r_t\right)\mathrm{mod}d\\ &= \left(\sum_{i=1}^{n}k_i^t\right)\mathrm{mod}d\\ &= k_1^t\oplus k_2^t\oplus\ldots\oplus k_n^t, t=1,2,\ldots,N.\end{aligned} \tag{4}$$

Finally, P_1 publishes the summation results to the other parties.

For clarity, the flow chart of the proposed protocol is given in Fig.1.

3 Security Analysis

In this subsection, the security of the proposed protocol against both the outside attack and the participant attack is analyzed.

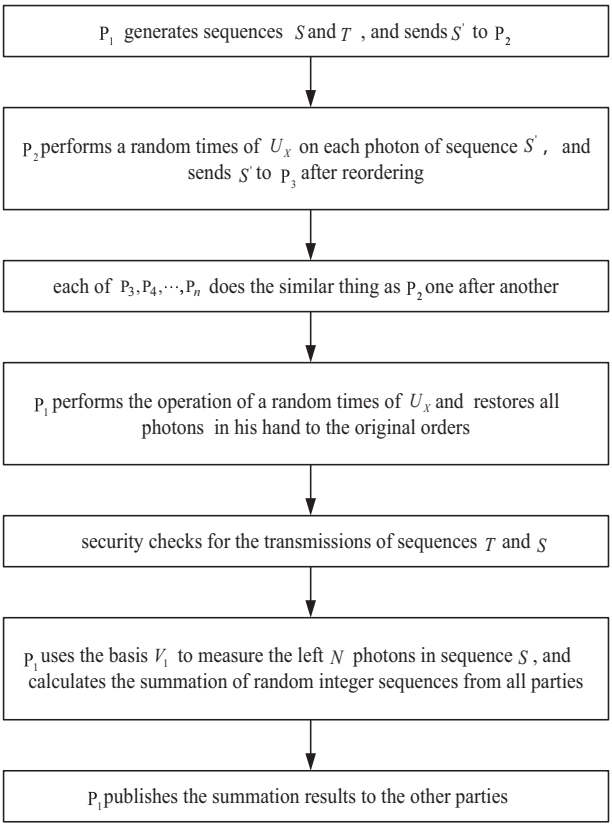

Fig. 1 The flow chart of the proposed protocol

(i) Outside attack

In the proposed protocol, P_i transmits all photons to P_{i+1}. An outside attacker, Eve, may launch her attack during the transmission process, such as the intercept-resend attack, the measure-resend attack and the entangle-measure attack et al. However, Eve doesn't know the genuine positions of the $N+\delta$ check photons from sequence T and the δ check photons from sequence S. As a result, Eve's attack will inevitably leave her trace on the check photons and be detected.

(ii) Participant attack

Two kinds of participant attack need be analyzed, i.e., the participant attack from one malicious party and the colluding attack from two or more malicious parties.

(a) The participant attack from one malicious party

As for the participant attack from the malicious P_j, if P_j attacks the photons from P_i to $P_{i+1}(i \neq j)$, due to having no knowledge about the genuine positions of the $N+\delta$ check photons from sequence T and the δ check photons from sequence S, she will inevitably be caught as an outside attacker.

(b) The colluding attack from two or more malicious parties

In the proposed protocol, P_1 is not allowed to collude with other parties. If the other $n-1$ parties collude together, they can easily obtain the private integers of P_1 from the summation results. Thus, it cannot resist the colluding attack from $n-1$ parties.

Next, whether the proposed protocol can resist the colluding attack from $n-2$ parties is analyzed. Without loss of generality, assume that P_2, …, P_{i-1}, P_{i+1}, …, P_n collude together to get the private integers of P_1 and P_i. If P_2, …, P_{i-1}, P_{i+1}, …, P_n attack the particles from P_i to P_{i+1}, due to having no knowledge about the genuine positions of the $N+\delta$ check photons from sequence T and the δ check photons from sequence S , they will inevitably be caught as an outside attacker.

4 Conclusion

To sum up, in this paper, a secure multi-party quantum summation protocol within a d-level quantum system is constructed by using the qudit shifting operation. The encoded photons are transmitted in a circular way. The proposed protocol can calculate the addition of modulo d in an integer-by-integer way rather than a bit-by-bit way. The security analysis result shows that the proposed protocol is secure against both the outside attack and the participant attack.

References

1. Heinrich, S.: Quantum summation with an application to integration. J. Complex. **18**, 1–50 (2002)
2. Heinrich, S., Kwas, M., Wozniakowski, H.: Quantum Boolean summation with repetitions in the worst-average setting. 2003, arXiv:quant-ph/0311036

3. Hillery, M., Ziman, M., Buzek, V., Bielikova, M.: Towards quantum-based privacy and voting. Phys. Lett. A. **349**, 75 (2006)
4. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**(11), 6214–6219 (2007)
5. 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**(11), 2793–2804 (2010)
6. Zhang, C., Sun, Z.W., Huang, Y., Long, D.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)
7. Zhang, C., Sun, Z.W., Huang, X.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
8. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
9. Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. Quantum Inf. Process. **16**, 225 (2017)
10. Zhang, C., Situ, H.Z., Huang, Q., Yang, P.: Multi-party quantum summation without a trusted third party based on single particles. Int J Quantum Inf. **15**(2), 1750010 (2017)
11. Ye, C.Q., Ye, T.Y.: Circular multi-party quantum private comparison with *n*-level single-particle states. Int. J. Theor. Phys. **58**(4), 1282–1294 (2019)