International Journal of Theoretical Physics (2020) 59:3079–3085
https://doi.org/10.1007/s10773-020-04554-6

Multi-Party Quantum Private Comparison with Qudit Shifting Operation

Duan Ming-Yi[1]

Received: 23 April 2020 / Accepted: 21 July 2020 / Published online: 15 August 2020

Abstract
In this paper, a multi-party quantum private comparison (MQPC) protocol is proposed based on the qudit shifting operation. The semi-honest third party (TP) prepares the initial particles and sends them to the first user. Then, each of n users encodes his private integers on the travelling particles with the qudit shifting operations and transmits them to the next user. Finally, the travelling particles are transmitted back to TP. The equality of the private integers from n users can be determined within one time execution of the protocol. It is verified that the proposed protocol is secure against both the outside attack and the participant attack. One user cannot obtain other users' private integers except for the case that their private integers are same. TP cannot know the private integers from n users except their comparison result.

Keywords Multi-party quantum private comparison (MQPC) · Circular transmission · Qudit shifting operation

1 Introduction

In 1982, Yao [1] introduced the millionaire problem, i.e., two millionaires want to know who is richer while keeping their genuine assets secret to each other. Since then, secure multi-party computation (SMPC) in classical cryptography began to arouse the interests of researchers, as it has important applications in many circumstances such as private bidding and auctions, secret ballot elections, e-commerce, data mining et al..

In 2009, Yang and Wen [2] put forward quantum private comparison (QPC) for the first time, in order to judge whether two inputs from two users are equal or not while keeping them secret through the quantum means. Since then, a lot of attentions from researchers have been focused on it. In the early development, numerous two-party QPC protocols [2–9] were

✉ Duan Ming-Yi
duanmingyi2020@163.com

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

designed through different quantum technologies. Later, researchers became more interested in constructing multi-party quantum private comparison (MQPC) protocols, as it can accomplish the comparison of equality among many users within one execution of protocol. Until now, numerous MQPC protocols [10–19] have been proposed through different quantum technologies. In 2013, Chang et al. [10] proposed the first MQPC protocol using GHZ class states. In 2014, Wang et al. [11] proposed a MQPC protocol with$n$-level entangled states. In 2015, Huang et al. [12] put forward a MQPC protocol with an almost-dishonest third party. In 2016, Ye [13] put forward a MQPC protocol based on entanglement swapping of Bell entangled states; Liu and Wang [14] suggested a dynamic MQPC protocol with single photons in both polarization and spatial-mode degrees of freedom; Huang et al. [15] designed a MQPC protocol with an almost-dishonest third party using GHZ states. In 2017, Hung et al. [16] constructed a MQPC protocol with almost dishonest third parties for strangers; Ji and Ye [17] put forward a MQPC protocol based on the entanglement swapping of d-level Cat states and d-level Bell states; Ye and Ji [18] proposed a novel MQPC protocol with scattered preparation and one-way convergent transmission of quantum states. In 2018, Ye and Ye [19] proposed a MQPC protocol of size relation with d-level single-particle states.

Based on the above analysis, inspired by the summation method of Ref. [20], this paper also concentrates on designing the MQPC protocol, by using the qudit shifting operation. The remaining part of this paper is arranged as follows: in Sect. 2, the MQPC protocol with qudit shifting operation is proposed; in Sect. 3, the security of the proposed MQPC protocol is validated; and finally, in Sect. 4, the conclusion are illustrated.

2 The Proposed MQPC Protocol with Qudit Shifting Operation

In a n-level quantum system, two common conjugate bases, C_1 and C_2, can be defined as.

$$C_1 = \{|k\rangle\}, \quad k = 0, 1, \ldots, \quad n-1\,, \tag{1}$$

$$C_2 = \{F|k\rangle\} = \left\{\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{jk}|j\rangle\right\}, \quad k = 0, 1, \ldots, \quad n-1\,, \tag{2}$$

where $\omega = e^{\frac{2\pi i}{n}}$ and F represents the nth order discrete quantum Fourier transform. Apparently, any two different elements in the set C_1 are mutually orthogonal. Likewise, any two different elements in the set C_2 are also mutually orthogonal. In addition, in a n-level quantum system, the qudit shifting operation can be defined as

$$U_v = \sum_{u=0}^{n-1}|u\oplus v\rangle\langle u|, \tag{3}$$

where the symbol '$\oplus$' denotes the addition modulo n.

Suppose that there are n users, $P_1, P_2, \cdots, P_n$, where P_i has a private integer X^i, $i = 1, 2, \ldots, n$. The binary representation of X^i in F_{2^L} is $\left(x^i_{L-1}, x^i_{L-2}, \ldots, x^i_0\right)$, where $x^i_j \in \{0, 1\}, j = 0, 1, \ldots, L-1$. They want to judge whether all of their private integers are equal or not under the help of the semi-honest TP. The proposed MQPC protocol with qudit shifting operation can be described as follows.

Step 1: TP and $P_i (i = 1, 2, \ldots, n)$ share a key sequence K^i of length L via a secure QKD protocol. Here, $K^i = \left(k^i_{L-1}, k^i_{L-2}, \ldots, k^i_0\right)$, where $k^i_j \in \{0, 1, \ldots, n-1\}, j = 0, 1, \ldots, L-1$.

Step 2: TP prepares a particle sequence S_0 which is composed of L n-level single photons $|r_0\rangle$, $|r_1\rangle$, …, $|r_{L-1}\rangle$, where $r_j \in \{0, 1, \ldots, n-1\}, j = 0, 1, \ldots, L-1$. For the sake of security check, TP also prepares δ n-level decoy single photons which are randomly chosen from the sets C_1 and C_2. Afterward, TP randomly inserts these decoy single photons into sequence S_0 and obtains a new sequence $S_0^{'}$. Finally, TP sends sequence $S_0^{'}$ to P_1.

Step 3: After P_1 receives sequence $S_0^{'}$, P_1 performs the security check together with TP to check whether the transmission of sequence $S_0^{'}$ is secure or not. TP tells P_1 the positions and the preparation basis of decoy single photons.P_1 measures the decoy single photons with the basis TP told and informs TP of his measurement outcomes. TP compares the measurement outcomes of decoy single photons with their initial prepared states. If the error rate is unreasonably high, the communication will be terminated; otherwise, it will be continued.

P_1 drops out the decoy single photons in sequence $S_0^{'}$ to restore sequence S_0. Then, P_1 encodes $x^1_j \oplus k^1_j (j = 0, 1, \ldots, L-1)$ on the jth particle in sequence S_0 by performing the qudit shifting operation $U_{x^1_j \oplus k^1_j}$ on it. As a result, the jth particle is changed into $\left|r_j \oplus x^1_j \oplus k^1_j\right\rangle$. Consequently, sequence S_0 is turned into sequence S_1, where $S_1 = \left[\left|r_0 \oplus x^1_0 \oplus k^1_0\right\rangle, \left|r_1 \oplus x^1_1 \oplus k^1_1\right\rangle, \ldots, \left|r_{L-1} \oplus x^1_{L-1} \oplus k^1_{L-1}\right\rangle\right]$.

For the sake of security check, P_1 prepares δ n-level decoy single photons which are randomly chosen from the sets C_1 and C_2. Afterward, P_1 randomly inserts these decoy single photons into sequence S_1 and obtains a new sequence $S_1^{'}$. Finally,P_1 sends sequence $S_1^{'}$ to P_2.

Step 4: For $i = 2, 3, \ldots, n-1$:

After P_i receives sequence $S_{i-1}^{'}$, P_i performs the security check together withP_{i-1} to check whether the transmission of sequence $S_{i-1}^{'}$ is secure or not. P_{i-1} tells $P_i$the positions and the preparation basis of decoy single photons. P_i measures the decoy single photons with the basis P_{i-1} told and informs P_{i-1} of his measurement outcomes.P_{i-1} compares the measurement outcomes of decoy single photons with their initial prepared states. If the error rate is unreasonably high, the communication will be terminated; otherwise, it will be continued.

P_i drops out the decoy single photons in sequence $S_{i-1}^{'}$ to restore sequence S_{i-1}. Then, P_i encodes $x^i_j \oplus k^i_j (j = 0, 1, \ldots, L-1)$ on the jth particle by performing the qudit shifting operation $U_{x^i_j \oplus k^i_j}$ on it. As a result, the jth particle is changed into $\left|r_j \oplus x^1_j \oplus k^1_j \oplus x^2_j \oplus k^2_j \oplus \ldots \oplus x^i_j \oplus k^i_j\right\rangle$. Consequently, sequence S_{i-1} is turned into sequence S_i, where $S_i = \left[\left|r_0 \oplus x^1_0 \oplus k^1_0 \oplus x^2_0 \oplus k^2_0 \oplus \ldots \oplus x^i_0 \oplus k^i_0\right\rangle, \left|r_1 \oplus x^1_1 \oplus k^1_1 \oplus x^2_1 \oplus k^2_1 \oplus \ldots \oplus x^i_1 \oplus k^i_1\right\rangle, \ldots, \left|r_{L-1} \oplus x^1_{L-1} \oplus k^1_{L-1} \oplus x^2_{L-1} \oplus k^2_{L-1} \oplus \ldots \oplus x^i_{L-1} \oplus k^i_{L-1}\right\rangle\right]$.

For the sake of security check, P_i prepares δ n-level decoy single photons which are randomly chosen from the sets C_1 and C_2. Afterward, P_i randomly inserts these decoy single photons into sequence S_i and obtains a new sequence $S_i^{'}$. Finally,P_i sends sequence $S_i^{'}$ to P_{i+1}.

Step 5: After P_n receives sequence S'_{n-1}, P_n performs the security check together with P_{n-1} to check whether the transmission of sequence S'_{n-1} is secure or not. P_{n-1} tells P_n the positions and the preparation basis of decoy single photons. P_n measures the decoy single photons with the basis P_{n-1} told and informs P_{n-1} of his measurement outcomes. P_{n-1} compares the measurement outcomes of decoy single photons with their initial prepared states. If the error rate is unreasonably high, the communication will be terminated; otherwise, it will be continued.

P_n drops out the decoy single photons in sequence S'_{n-1} to restore sequence S_{n-1}. Then, P_n encodes $x_j^n \oplus k_j^n (j = 0, 1, \ldots, L-1)$ on the jth particle by performing the qudit shifting operation $U_{x_j^n \oplus k_j^n}$ on it. As a result, the jth particle is changed into $\left| r_j \oplus x_j^1 \oplus k_j^1 \oplus x_j^2 \oplus k_j^2 \oplus \ldots \oplus x_j^n \oplus k_j^n \right\rangle$. Consequently, sequence S_{n-1} is turned into sequence S_n, where $S_i = [|r_0 \oplus x_0^1 \oplus k_0^1 \oplus x_0^2 \oplus k_0^2 \oplus \ldots \oplus x_0^n \oplus k_0^n\rangle \ , |r_1 \oplus x_1^1 \oplus k_1^1 \oplus x_1^2 \oplus k_1^2 \oplus \ldots \oplus x_1^n \oplus k_1^n\rangle , \ldots, |r_{L-1} \oplus x_{L-1}^1 \oplus k_{L-1}^1 \oplus x_{L-1}^2 \oplus k_{L-1}^2 \oplus \ldots \oplus x_{L-1}^n \oplus k_{L-1}^n\rangle]$.

For the sake of security check, P_n prepares δ n-level decoy single photons which are randomly chosen from the sets C_1 and C_2. Afterward, P_n randomly inserts these decoy single photons into sequence S_n and obtains a new sequence S'_n. Finally, P_n sends sequence S'_n to TP.

Step 6: After TP receives sequence S'_n, TP performs the security check together with P_n to check whether the transmission of sequence S'_n is secure or not. P_n tells TP the positions and the preparation basis of decoy single photons.TP measures the decoy single photons with the basis P_n told and informs P_n of his measurement outcomes. P_n compares the measurement outcomes of decoy single photons with their initial prepared states. If the error rate is unreasonably high, the communication will be terminated; otherwise, it will be continued.

TP drops out the decoy single photons in sequence S'_n to restore sequence S_n. Then TP measures the particles in sequence S_n with the basis C_1 and obtains the measurement results $R = \left(r'_0, r'_1, \ldots, r'_{L-1}\right)$, where r'_j is the measurement result of the jth particle and $j = 0, 1, \ldots, L-1$. Afterward, TP calculates

$$\begin{aligned} &\left(r'_j \oplus (n - r_j) - k_j^1 \oplus k_j^2 \oplus \ldots \oplus k_j^n\right) \bmod n \\ &= x_j^1 \oplus x_j^2 \oplus \ldots \oplus x_j^n, \quad j = 0, 1, \ldots, L-1 \end{aligned} . \tag{4}$$

If $x_j^1 \oplus x_j^2 \oplus \ldots \oplus x_j^n = 0$ for all j, all $X^i (i = 1, 2, \ldots, n)$ should be same; otherwise, not all X^i are same. Finally, TP publicly informs P_1, P_2, $\cdots$, P_n of the comparison result.

3 Security Analysis

In this section, the security against the outside attack and the participant attack is validated in detail, respectively.

(i) **The outside attack**

In the proposed protocol, the particles are transmitted in a circular way, i.e., from TP to P_1, P_i to $P_{i+1}(i = 1, 2, \ldots, n-1)$ and P_n back to TP. During the transmission from one party to another party, an outside attacker, Eve, may launch her attack to steal something useful about the private integers, such as the intercept-resend attack, the measure-resend attack and the entangle-measure attack. Fortunately, the proposed protocol employs the decoy photon technology to guarantee the security of particle transmission. Because Eve is unaware of the genuine positions of decoy photons in the transmitted sequence, she will inevitably leave her trace on them so that she will be detected undoubtedly.

(ii) **The participant attack**

In the proposed protocol, it is assumed that TP can not cooperate with any of users. Here, the participant attack from TP, the participant attack from one dishonest user and the participant attack from two or more dishonest users are validated in detail, respectively.

a) **The participant attack from TP**

TP sends her jth fake particle $|g_j\rangle$ to P_t, where $g_j \in \{0, 1, \ldots, n-1\}$, $t = 1, 2, \ldots, n$. After P_t finishes his encoding, the jth fake particle is turned into $\left|g_j \oplus x_j^t \oplus k_j^t\right\rangle$. Then,TP intercepts the transmitted sequence sent from $P_t$and measures its particles with the basis C_1. However, she still cannot decode out x_j^t, since she has no knowledge about the genuine position of the jth fake particle in the transmitted sequence. Moreover, this kind of attack from TP can be detected by the security check between P_{t-1} and P_t.

b) **The participant attack from one dishonest user**

Assume that P_t is the dishonest user, where $t = 1, 2, \ldots, n$.

After the security check with P_{t-1}, P_t measures the jth $(j = 0, 1, \ldots, L-1)$particle $\left|r_j \oplus x_j^1 \oplus k_j^1 \oplus x_j^2 \oplus k_j^2 \oplus \ldots \oplus x_j^{t-1} \oplus k_j^{t-1}\right\rangle$ with the basis C_1. However, he only obtains the value of $r_j \oplus x_j^1 \oplus k_j^1 \oplus x_j^2 \oplus k_j^2 \oplus \ldots \oplus x_j^{t-1} \oplus k_j^{t-1}$. He even has no idea about the value of $x_j^1 \oplus x_j^2 \oplus \ldots \oplus x_j^{t-1}$, as he is unaware of $k_j^1, k_j^2, \ldots, k_j^{t-1}$ and r_j.

Secondly, $P_t$sends his jth fake particle $|f_j\rangle$ to P_{t+1}, where $f_j \in \{0, 1, \ldots, n-1\}$. After P_{t+1} finishes his encoding, the jth fake particle is turned into $\left|f_j \oplus x_j^{t+1} \oplus k_j^{t+1}\right\rangle$. Then, P_t intercepts the transmitted sequence sent from P_{t+1} and measures its particles with the basis C_1. However, he still cannot decode out x_j^{t+1}, since he has no knowledge about the genuine position of the jth fake particle in the transmitted sequence and the value of k_j^{t+1}.

In addition, P_t may launch his attack on the particles transmitted from one party to another party. However, since he is unaware of the genuine positions of decoy photons in the transmitted sequence, he will inevitably leave his trace on them so that he will be detected undoubtedly as an outside eavesdropper.

c) **The participant attack from two or more dishonest users**

Case 1: The participant attack from two dishonest users

In the proposed protocol, two dishonet users P_t and P_{t+2} may cooperate to steal the private integer of P_{t+1} in the following way, where $t = 1, 2, \ldots, n-2$. After encoding his private integer, P_t measures the jth ($j = 0, 1, \ldots, L-1$) particle $\left|r_j \oplus x_j^1 \oplus k_j^1 \oplus x_j^2 \oplus k_j^2 \oplus \ldots \oplus x_j^t \oplus k_j^t\right\rangle$ with the basis C_1 and sends the same state to P_{t+1}. After the encoding of P_{t+1}, the jth particle is changed into $\left|r_j \oplus x_j^1 \oplus k_j^1 \oplus x_j^2 \oplus k_j^2 \oplus \ldots \oplus x_j^t \oplus k_j^t \oplus x_j^{t+1} \oplus k_j^{t+1}\right\rangle$. Then, after receiving the jth particle, P_{t+2} also measures it with the basis C_1. Finally, P_t and P_{t+2} can cooperate to decode out the value of $x_j^{t+1} \oplus k_j^{t+1}$ according to their measurement results. However, neither P_t or P_{t+2} knows the value of k_j^{t+1}, so they still cannot decode out x_j^{t+1}.

Case 2: The participant attack from more than two dishonest users

Here, we consider the case that more than two dishonet users conclude. The most powerful case is that $n-1$ users conclude to steal the remaining user's private integer. Without loss of generality, suppose that $P_1, P_2, \ldots, P_t, P_{t+2}, \ldots, P_{n-1}, P_n$ cooperate to steal the private integer of P_{t+1}, where $t = 1, 2, \ldots, n$. If they launch the attack same to that of Case 1, due to having no knowledge about the value of $k_j^{t+1} (j = 0, 1, \ldots, L-1)$, they will cannot decode out x_j^{t+1}. In addition, they may deduce the value of x_j^{t+1} from the comparison result. Although they can easily calculate the value of $x_j^1 \oplus x_j^2 \oplus \ldots \oplus x_j^t \oplus x_j^{t+2} \ldots \oplus x_j^{n-1} \oplus x_j^n$, the compasion result of $X^1, X^2, \ldots, X^n$ is still helpless for them to know the value of x_j^{t+1}.

4 Conclusion

To sum up, in this paper, a MQPC protocol is proposed based on the qudit shifting operation. The semi-honest TP prepares the initial particles and sends them to the first user. Then, each of n users encodes his private integers on the travelling particles with the qudit shifting operations and transmits them to the next user. Finally, the travelling particles are transmitted back to TP. The equality of the private integers from n users can be determined within one time execution of the protocol. It is verified that the proposed protocol is secure against both the outside attack and the participant attack. One user cannot obtain other users' private integers except for the case that their private integers are same. TP cannot know the private integers from n users except their comparison result.

References

1. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Washington, DC, USA, 1982, pp.160
2. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A: Math. Theor. **42**, 055305 (2009)
3. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1561–1565 (2010)
4. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**, 065002 (2009)

5. Yang, Y.G., Xia, J., Jia, X., Shi, L., Zhang, H.: New quantum private comparison protocol without entanglement. Int. J. Quantum Inf. **10**, 1250065 (2012)
6. Liu, B., Gao, F., Jia, H.Y., Huang, W., Zhang, W.W., Wen, Q.Y.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. **12**, 887–897 (2013)
7. Li, Y.B., Ma, Y.J., Xu, S.W., Huang, W., Zhang, Y.S.: Quantum private comparison based on phase encoding of single photons. Int. J. Theor. Phys. **53**, 3191–3200 (2014)
8. Li, J., Zhou, H.F., Jia, L., Zhang, T.T.: An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping. Int. J. Theor. Phys. **53**(7), 2167–2176 (2014)
9. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**, 711–715 (2016)
10. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**, 1077–1088 (2013)
11. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with*n*-level entangled states. Quantum Inf. Process. **13**, 2375–2389 (2014)
12. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum Inf. Process. **14**, 4225–4235 (2015)
13. Ye, T.Y.: Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states. Commun. Theor. Phys. **66**(3), 280–290 (2016)
14. Liu, W., Wang, Y.B.: Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **55**, 5307–5317 (2016)
15. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. **55**, 2969–2976 (2016)
16. Hung, S.M., Hwang, S.L., Hwang, T., Kao, S.H.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process. **16**(2), 36 (2017)
17. Ji, Z.X., Ye, T.Y.: Multi-party quantum private comparison based on the entanglement swapping of*d*-level Cat states and *d*-level Bell states. Quantum Inf. Process. **16**(7), 177 (2017)
18. Ye, T.Y., Ji, Z.X.: Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci. China Phys. Mech. Astron. **60**(9), 090312 (2017)
19. Ye, C.Q., Ye, T.Y.: Multi-party quantum private comparison of size relation with*d*-level single-particle states. Quantum Inf. Process. **17**(10), 252 (2018)
20. Duan, M.Y.: Multi-party quantum summation within a d-level quantum system. Int. J. Theor. Phys. **59**, 1638–1643 (2020)