International Journal of Theoretical Physics (2018) 57: 3389–3395
https://doi.org/10.1007/s10773-018-3852-x

Two-Party Quantum Private Comparison Using Single Photons

Hong-Ming Pan[1]

Abstract

Quantum private comparison (QPC) aims to determine whether two parties' private inputs are equal or not without leaking out their genuine contents. At present, there is seldom QPC protocol which uses single photons as quantum resource. In this paper, we are devoted to converting Zhang et al.'s three-party quantum summation (QS) protocol based on single photons (Int. J. Quantum Inf. **15**(2), 1750010, 2017) into the corresponding two-party QPC protocol with single photons. The correctness and the security of the proposed QPC protocol with single photons can be guaranteed. The proposed QPC protocol is naturally free from Trojan horse attacks because of its single directional particle transmission mode.

Keywords Quantum private comparison (QPC) · Quantum summation (QS) · Single photons · Correctness · Security

1 Introduction

Quantum private comparison (QPC), first suggested by Yang and Wen [1] in 2009, aims to determine whether two parties' private inputs are equal or not without leaking out their genuine contents. Since the first two-party QPC protocol [1] was proposed, QPC has quickly aroused the interests of researchers. As a result, a lot of two-party QPC protocols have been designed, such as the ones with single particles [2], product states [3, 4], Bell states [1, 5–9], GHZ states [10–12], W states [13, 14], cluster states [15, 16], χ-type entangled states [17–19], five-particle entangled states [20] and six-particle entangled states [21]. Besides the two-party QPC protocols, many multi-party QPC protocols [22–30] have also been suggested.

It is easy to find out that at present, there is seldom QPC protocol which uses single photons as quantum resource. Apparently, compared with an entangled state, single photon has some merits. For example, the preparation and the measurement of single photon are much easier than those of an entangled state. Therefore, it is worthy of designing a QPC protocol with single photons.

✉ Hong-Ming Pan
hmpan@zjgsu.edu.cn

[1] Hangzhou College of Commerce, Zhejiang Gongshang University, Hangzhou 310018, People's Republic of China

Based on the above analysis, in this paper, we are devoted to designing a novel two-party QPC protocol which uses single photons as quantum resource. After looking deeply into the three-party quantum summation (QS) protocol based on single photons proposed by Zhang et al. [31], we find out that Zhang et al.'s three-party QS protocol can be converted into the corresponding two-party QPC protocol with single photons. Therefore, in this paper, we concentrate on converting Zhang et al.'s three-party QS protocol into the corresponding two-party QPC protocol.

The rest of this paper is organized as follows: in Section 2, Zhanget al.'s three-party QS protocol is reviewed; in Section 3, the two-party QPC protocol with single photons is described and analyzed; and finally, conclusion is given in Section 4.

2 Review of Zhang et al.'s Three-Party QS Protocol

For integrity, in this section, we review Zhang et al.'s three-party QS protocol.

In Zhang et al.'s three-party QS protocol, there are three participants, P_1, P_2, P_3, each of whom has one secret bit. The secret bit from P_i is represented by m_i, where $i = 1, 2, 3$. The goal of this protocol is to guarantee the correctness of the summation result and keep the privacy of each participant's input. Three participants agree on beforehand that both $|0\rangle(|1\rangle)$ and $|+\rangle(|-\rangle)$ represent the classical bit 0 (1). Here, $|\pm\rangle = \frac{1}{2}(|0\rangle \pm |1\rangle)$. The quantum and classical channels are supposed to be authenticated, noiseless and lossless. Without loss of generality, suppose that P_1 prepares the initial quantum states. Zhang et al.'s three-party QS protocol is illustrated as follows.

Step 1: P_1 prepares $1 + d$ single photons $\{p_{1,1}, p_{1,2}, \ldots, p_{1,1+d}\}$ all in the state $|+\rangle$, and generates $(1 + d) \times 2$ single photons $\{p_{2,1}, p_{2,2}, \ldots, p_{2,1+d}\}$, $\{p_{3,1}, p_{3,2}, \ldots, p_{3,1+d}\}$ all in the state $|1\rangle$. Then, P_1 performs $(1 + d) \times 2$ controlled-not operations, which are denoted by CNOT_{ij}, $i \in \{1, 2, \ldots, 1 + d\}$, $j \in \{2, 3\}$. In the operation CNOT_{ij}, $p_{1,i}$ is the control qubit and $p_{j,i}$ is the target qubit. Afterward, P_1 performs the Hadamard gates on all photons. Finally, P_1 picks out photons $\left\{p_{1,1}, p_{1,2}, \ldots, p_{1,1+d}\right\}$ as the group G_1, photons $\{p_{2,1}, p_{2,2}, \ldots, p_{2,1+d}\}$ as the group G_2, and photons $\{p_{3,1}, p_{3,2}, \ldots, p_{3,1+d}\}$ as the group G_3.

Step 2: P_1 prepares two groups of decoy photons randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, P_1 picks out one group of decoy photons and randomly inserts these decoy photons into G_2 (G_3) to form a new group $G'_2(G'_3)$. Finally, P_1 sends $G'_2(G'_3)$ to $P_2(P_3)$, and keeps G_1 in his hand.

Step 3: After confirming the receipt of G'_2 from P_2, P_1 publishes the positions of decoy photons in $G'_2$and asks P_2 to measure them with the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$. After P_2 announces his measurement results, P_1 calculates the error rate by comparing the initial states of decoy photons with the measurement results from P_2. If the error rate is greater than the threshold value, the communication will be terminated and restarted from Step 1; otherwise, P_2 will drop out the decoy photons to recover G_2, and the protocol will be continued.

In the meanwhile, P_1 checks the transmission security of G'_3 with P_3 in the similar way.

Step 4: P_2 and P_3 collaborate to check whether P_1 generated the true single photons and performed the proper operations as described in Step 1 in the following way.

P_2 and P_3 randomly choose d photons in the same positions of G_2 and G_3, and require P_1 to choose d photons in the same positions of G_1. Then, P_2 and P_3 ask P_1 to measure the chosen d photons randomly with the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$. After P_1 publishes his measurement results, P_2 and P_3 use the same basis as that used by P_1 to measure their corresponding photons. Finally, P_2 and P_3 compare the correlations of their three's measurement results to check whether P_1 is honest or not. If P_1 is dishonest, the communication will be terminated and restarted from Step 1; otherwise, the communication will be continued.

Step 5: After dropping out the d photons used for checking, $P_i (i = 1, 2, 3)$ measures the photon in his hand with the basis $\{|0\rangle, |1\rangle\}$ and obtains his private key k_i. Then, P_i calculates the ciphertext $c_i = m_i \oplus k_i$ and publishes it. As a result, P_i obtains the summation of their three's inputs by calculating $c_1 \oplus c_2 \oplus c_3$. Here, $\oplus$ is the addition modulo 2.

3 The Proposed Two-Party QPC Protocol with Single Photons

In this section, we convert Zhang et al.'s three-party QS protocol into the corresponding two-party QPC protocol.

In 1997, Lo [32] pointed out that it is impossible to evaluate the equality function securely in a two-party scenario. Therefore, in the realm of QPC, a third party (TP) is always needed. Suppose that there are two parties, Alice and Bob, each of whom has one secret bit. The secret bit from Alice (Bob) is represented by $m_a (m_b)$. Alice and Bob want to determine whether m_a is equal to m_b or not without leaking out their genuine contents. The proposed two-party QPC protocol is consisted of the following steps:

Step 1: TP prepares $1 + d$ single photons $\{p_{1,1}, p_{1,2}, \ldots, p_{1,1+d}\}$ all in the state $|+\rangle$, and generates $(1 + d) \times 2$ single photons $\{p_{2,1}, p_{2,2}, \ldots, p_{2,1+d}\}$, $\{p_{3,1}, p_{3,2}, \ldots, p_{3,1+d}\}$ all in the state $|1\rangle$. Then, TP performs $(1 + d) \times 2$ controlled-not operations, which are denoted by $\mathrm{CNOT}_{ij}, i \in \{1, 2, \ldots, 1 + d\}, j \in \{2, 3\}$. In the operation CNOT_{ij}, $p_{1,i}$ is the control qubit and $p_{j,i}$ is the target qubit. Afterward, TP performs the Hadamard gates on all photons. Finally, TP picks out photons $\{p_{1,1}, p_{1,2}, \ldots, p_{1,1+d}\}$ as the group G_1, photons $\{p_{2,1}, p_{2,2}, \ldots, p_{2,1+d}\}$ as the group G_2, and photons $\{p_{3,1}, p_{3,2}, \ldots, p_{3,1+d}\}$ as the group G_3.

Step 2: TP prepares two groups of decoy photons randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, TP picks out one group of decoy photons and randomly inserts these decoy photons into $G_2(G_3)$ to form a new group $G_2'(G_3')$. Finally, TP sends $G_2'(G_3')$ to Alice (Bob), and keeps G_1 in his hand.

Step 3: After confirming the receipt of G_2' from Alice, TP publishes the positions of decoy photons in G_2' and asks Alice to measure them with the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$. After Alice announces her measurement results, TP calculates the error rate by comparing the initial states of decoy photons with the measurement results of Alice. If the error rate is greater than the threshold value, the communication will be terminated and restarted from Step 1; otherwise, Alice will drop out the decoy photons to recover G_2, and the protocol will be continued.

In the meanwhile, TP checks the transmission security of G_3' with Bob in the similar way.

Step 4: Alice and Bob collaborate to check whether TP generated the true single photons and performed the proper operations as described in Step 1 in the following way. Alice and Bob randomly choose d photons in the same positions of G_2 and G_3, and require TP to choose d photons in the same positions of G_1. Then, Alice and Bob ask TP to measure the chosen d photons randomly with the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$. After TP publishes his measurement results, Alice and Bob use the same basis as that used by TP to measure their corresponding photons. Finally, Alice and Bob compare the correlations of their three's measurement results to check whether TP is honest or not. If TP is dishonest, the communication will be terminated and restarted from Step 1; otherwise, the communication will be continued.

Step 5: After dropping out the d photons used for checking, Alice (Bob) measures the photon in her (his) hand with the basis $\{|0\rangle, |1\rangle\}$ and obtains her (his) private key $k_a(k_b)$. Similarly, TP can obtain his private key k_t. Then, Alice (Bob) calculates the ciphertext $c_a = m_a \oplus k_a (c_b = m_b \oplus k_b)$ and publishes it. Afterward, TP calculates $s = c_a \oplus c_b \oplus k_t$. Finally, if $s = 0$, TP will publish to Alice and Bob that $m_a = m_b$; otherwise, TP will publish to Alice and Bob that $m_a \neq m_b$.

For clarity, the flow chart of the proposed two-party QPC protocol is further given in Fig. 1.

We further point out the differences between the proposed two-party QPC protocol and Zhang et al.'s three-party QS protocol. In the former, we use TP, Alice and Bob to replace P_1, P_2 and P_3 of the latter, respectively. Moreover, in the former, TP has no secret bit to encrypt with his private key k_t while in the latter, P_1 needs to calculate the ciphertext $c_1 = m_1 \oplus k_1$.

Correctness In the following, we will show that the correctness of the comparison between m_a and m_b can be guaranteed.

After TP performs $(1 + d) \times 2$ controlled-not operations in Step 1, the particles $\{p_{1,j}, p_{2,j}, p_{3,j}\}$ will form an entangled state

$$|\phi_j\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle), \tag{1}$$

where $j \in \{1, 2, \ldots, 1 + d\}$. After the operations of Hadamard gates in Step 1, $|\phi_j\rangle$ will become

$$|\phi'_j\rangle = \frac{1}{2}(|000\rangle + |011\rangle - |101\rangle - |110\rangle). \tag{2}$$

In Step 5, TP, Alice and Bob measure their respective particle of $|\phi'_j\rangle$ with the basis $\{|0\rangle, |1\rangle\}$ and obtain the private keys k_t, k_a and k_b, respectively. Obviously, we have

$$k_a \oplus k_b \oplus k_t = 0. \tag{3}$$

As a result, it can be obtained that

$$s = c_a \oplus c_b \oplus k_t = (m_a \oplus k_a) \oplus (m_b \oplus k_b) \oplus k_t = m_a \oplus m_b. \tag{4}$$

Therefore, if $s = 0$, we will have $m_a = m_b$; otherwise, we will have $m_a \neq m_b$.

Security In Zhang et al.'s three-party QS protocol, the security against the outside attacks and the security against the participant attacks (including the individual attack from P_2 or P_3 and the individual attack from P_1) have been validated in detail. It is straightforward that the proposed two-party QPC protocol is also secure against the outside attacks and the

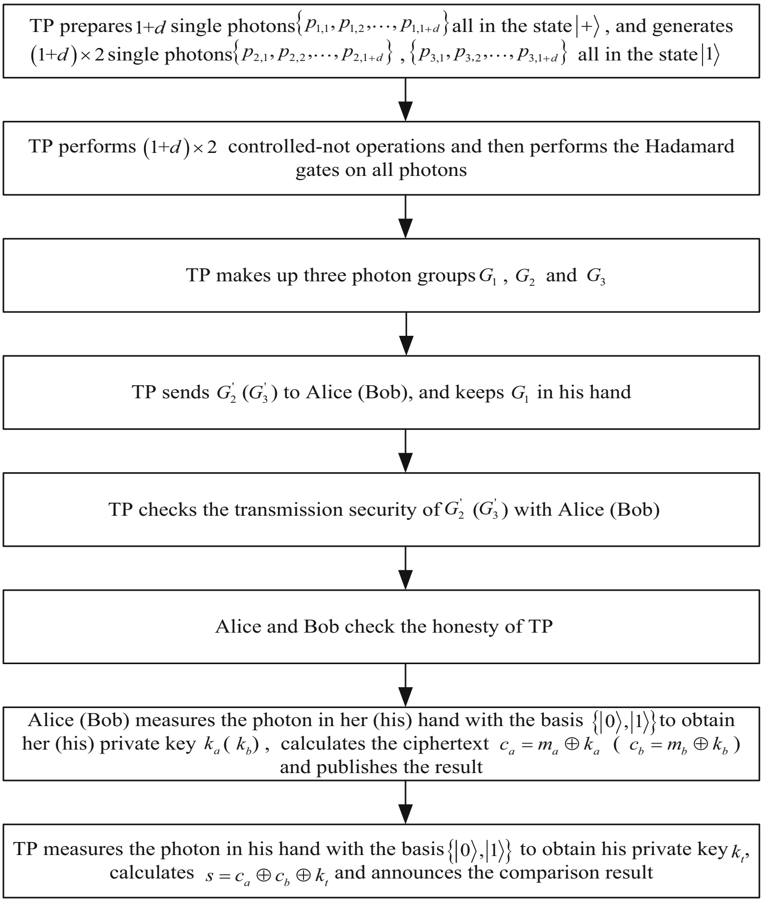

Fig. 1 The flow chart of the proposed two-party QPC protocol

participant attacks (including the individual attack from Alice or Bob and the individual attack from TP) .

Qubit Efficiency Here, we calculate the qubit efficiency after ignoring the eavesdropping check processes. The qubit efficiency η is defined as $\eta = \frac{r_c}{r_q}$, where r_c is the number of the compared classical bits and n_q is the number of consumed qubits [33]. In the proposed two-party QPC protocol, one $|+\rangle$ and two $|1\rangle$s can be used to compare one secret bit from each party, hence its qubit efficiency is 33.3%.

4 Conclusion

To sum up, in this paper, inspired by Zhang et al.'s three-party QS protocol based on single photons, we propose the corresponding two-party QPC protocol with single photons. The proposed QPC protocol uses single photons as the initial quantum resource rather than quantum entangled states. Moreover, the correctness and the security of the proposed QPC protocol can be guaranteed. The proposed QPC protocol transmits the particles in a single directional way, so it is naturally free from Trojan horse attacks.

Compliance with Ethical Standards

Conflict of interest The author declares that he has no conflict of interest.

References

1. 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)
2. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**, 065002 (2009)
3. 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)
4. Ye, T.Y.: Quantum private comparison via cavity QED. Commun. Theor. Phys. **67**(2), 147–156 (2017)
5. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**, 583–588 (2012)
6. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**, 373–384 (2012)
7. Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int. J. Quantum Inf. **11**, 1350039 (2013)
8. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf. Process. **12**, 877–885 (2013)
9. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**, 1981–1990 (2013)
10. 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 (2010)
11. Lin, J., Tseng, H.Y., Hwang, T.: Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Opt. Commun. **284**, 2412–2414 (2011)
12. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
13. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**, 3160–3163 (2011)
14. Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W States. Int. J. Theor. Phys. **53**(5), 1723–1729 (2014)
15. Xu, G.A., Chen, X.B., Wei, Z.H., Li, M.J., Yang, Y.X.: An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. Int. J. Quantum Inf. **10**, 1250045 (2012)
16. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**, 212–218 (2013)
17. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**, 69–77 (2012)
18. Jia, H.Y., Wen, Q.Y., Li, Y.B., Cao, F.: Quantum private comparison using genuine four-particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
19. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z., Cui, W.: New quantum private comparison protocol using χ -type state. Int. J. Theor. Phys. **51**, 1953–1960 (2012)
20. Ye, T.Y., Ji, Z.X.: Two-party quantum private comparison with five-qubit entangled states. Int. J. Theor. Phys. **56**(5), 1517–1529 (2017)
21. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**(6), 711–715 (2016)
22. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**, 1077–1088 (2013)
23. 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)
24. Liu, W., Wang, Y.B., Wang, X.M.: Multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping. Int. J. Theor. Phys. **53**, 1085–1091 (2014)

25. Liu, W., Wang, Y.B., Wang, X.M.: Quantum multi-party private comparison protocol using d -dimensional Bell states. Int. J. Theor. Phys. **54**, 1830–1839 (2015)
26. 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)
27. 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)
28. 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)
29. 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)
30. 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)
31. 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)
32. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
33. Chen, J.H., Lee, K.C., Hwang, T.: The enhancement of Zhou et al.'s quantum secret sharing protocol. Int. J. Mod. Phys. C **20**(10), 1531–1535 (1999)