International Journal of Theoretical Physics (2021) 60:4030–4036
https://doi.org/10.1007/s10773-021-04937-3

# Quantum Private Comparison Using Single Bell State

Yan-Feng Lang [1]

Received: 18 May 2021 / Accepted: 11 August 2021 / Published online: 12 October 2021


**Abstract**
Quantum private comparison (QPC) can tell us whether two users' private data are equal or not by quantum technology without disclosing privacy to each other. There are many QPC protocols with diverse procedures and a wide variety of quantum resources. If two forms of quantum states or above are used in a QPC protocol, there will be a need of multiple devices or methods to generate these quantum states, which could bring about some lurking unfavourable effects such as inefficiency and high costs in application. In order to improve the QPC efficiency and reduce costs, a design principle to develop QPC protocols is put forward as a reference in this paper. Also, to take Bell states for example, a QPC protocol with a single Bell state as quantum resource is presented. The protocol is not only simple yet efficient and easy to apply but also of low costs. The analyses show its correctness so it could behave as an alternative way to exercise QPC.

**Keywords** Quantum private comparison · States-generation switching · Semi-honest third party · Single bell state

## 1 Introduction

Quantum private comparison (QPC) aims at determining whether two customers' secrets are equal or not without disclosing privacy to each other by quantum technology. At present, there are a large number of QPC protocols [1–41], which employ diverse procedures and a wide variety of quantum resources. In a safe premise, an advisable idea is to make procedures as simple as possible and make the preparation of the used quantum resources as easy as can be. If the idea is kept as a design principle in developing QPC protocols, we will get a more efficient and practical one. To demonstrate the design principle, this study will take Bell states for example in what follows.

As we know, among quantum resources, such as two-particle product states, Bell states, W states, GHZ states, cluster states, $\chi$-type entangled states, five-particle entangled states, six-

✉ Yan-Feng Lang
langyf@aliyun.com

[1] School of Electrical Engineering, Zhejiang University of Water Resources and Electric Power, Hangzhou 310018, People's Republic of China

particle entangled states, and multi-level quantum system, Bell states are a common and useful one. There are four Bell states: $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, where $|\phi^\pm\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$. They have found application in diverse QPC protocols [9–18]. If we focus narrowly on their usage of Bell states, it can be seen that they have used at least two forms of Bell states.

Although the usage of diverse Bell states might increase the qubit efficiency, which is defined as the ratio of the number of compared classical bits to the total number of photons used in comparison [12], it should reduce working efficiency and increase running costs. The reason goes as follows. Various Bell states mean the requirement of multiple states-producing devices or ways. That is to say, different devices, working modes, input particles or whatever will be switched to generate different kinds of quantum states. This is called as states-generation switching in the paper. It would be rather frequent and abundant in a QPC process, which could reduce working efficiency and increase running costs.

If the proposed design principle is used as a reference to design QPC protocols, the used quantum states will be as single as may be and thus states-generation switching can be also avoided as much as possible. In this way, the qubit efficiency might be lowered. However, once a quantum state can be mass produced, its number and the qubit efficiency are not the first things to consider, for to prepare two states of a kind is generally far easier than to do two states of two kinds. For example, to produce two $|\phi^+\rangle$ Bell states is much easier than to prepare two different Bell states $|\phi^+\rangle$ and $|\psi^+\rangle$ when you have the ability to generate a $|\phi^+\rangle$ Bell state. Therefore, for some cases, you would mind quantum states' forms, not their numbers. In other words, the states' singleness, not the qubit efficiency, would be one of the first considerations in developing QPC protocols.

According to the above discussion, there should be a QPC protocol implemented using a single Bell state, say $|\phi^+\rangle$. However, such a protocol is hard to see yet. As mentioned earlier, existent Bell-based QPC protocols generally utilized two forms of theirs or over. Thus, the paper will utilize a single Bell state to design a novel QPC protocol, where the single Bell state $|\phi^+\rangle$ or $|\phi^-\rangle$ will be used. It would improve efficiency and reduce use costs without states-generation switching.

As Lo [42] dealt with, it is impossible to design a secure equality function in a two-party scenario, so a semi-honest third party (TP) will take part in the presented protocol. Its correctness and security will be validated.

The paper is organized as follows. The proposed protocol is described in Section 2. Its correctness and security are analysed in Section 3. Conclusions are drawn in Section 4.

## 2 The Proposed QPC Protocol

Two classical customers Alice and Bob are going to exercise QPC for their private data or the respective binary representations $A = (a_{N-1}...a_1a_0)$ and $B = (b_{N-1}...b_1b_0)$, where $a_j$, $b_j \in \{0, 1\}$, $j \in \{0, 1, ..., N-1\}$, $2^{N-1} \le \max\{A, B\} < 2^N$. Based on the three-party scenario described above, the process of the proposed QPC protocol can be described as follows.

Step 1: TP generates 3 $N$ $|\phi^+\rangle$Bell states, where $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, and divides the first $N$ ones into two sequences *T0* and *T1*, the second $N$ into *T2* and *T3*, and the last $N$ into *T4* and *T5*. In order to detect eavesdropping, TP generates two sets of decoy photons *DA* and *DB*, each randomly chosen from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$,

where $|+\rangle = \left(1/\sqrt{2}\right)(|0\rangle + |1\rangle)$ and $|-\rangle = \left(1/\sqrt{2}\right)(|0\rangle - |1\rangle)$. Here, $Z$ basis and $X$ basis are used to denote the measuring basis of $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$, respectively. TP randomly inserts $DA$ into $T0$ and $T4$, composing one new quantum sequence $SA$, and $DB$ into $T2$ and $T5$, forming $SB$, which are sent to Alice and Bob, respectively. TP measures $T1$ and $T3$ along $Z$ basis. If the measuring result is $|0\rangle/|1\rangle$, its corresponding classical bit is labelled as 0/1. We can obtain the measure bits $T1 = (t1_{N-1}...t1_1t1_0)$, $T3 = (t3_{N-1}...t3_1t3_0)$, where $t1_j$, $t3_j \in \{0, 1\}$, $j \in \{0, 1, ..., N-1\}$.

Step 2: Once the sequences $SA$ and $SB$ all reach Alice and Bob, respectively, TP will announce the decoy photons' positions and measuring bases. By them, Alice and Bob perform the corresponding measure and response its results to TP. It verifies these measure outcomes to check whether there are eavesdroppers in the quantum channels or not. If the detected error rate exceeds a predetermined threshold, this communication will be aborted and the protocol will be restarted. Otherwise, it goes on to Step 3.

Step 3: Alice (Bob) discards the decoy photons in $SA$ ($SB$) to restore the sequences $T0$ and $T4$ ($T2$ and $T5$), and measures them along $Z$ basis. And then, Alice (Bob) can get the measure bits $T0 = (t0_{N-1}...t0_1t0_0)$, $T4 = (t4_{N-1}...t4_1t4_0)$ ($T2 = (t2_{N-1}...t2_1t2_0)$, $T5 = (t5_{N-1}...t5_1t5_0)$), where $t0_j$, $t2_j$, $t4_j$, $t5_j \in \{0, 1\}$, $j \in \{0, 1, ..., N-1\}$. Alice and Bob perform the bit-wise exclusive-OR operations $ra_j = t0_j \oplus a_j \oplus t4_j$ and $rb_j = t2_j \oplus b_j \oplus t5_j$, respectively, where $ra_j$, $rb_j \in \{0, 1\}$, $RA = (ra_{N-1}...ra_1ra_0)$, $RB = (rb_{N-1}...rb_1rb_0)$, $j \in \{0, 1, ..., N-1\}$. The binary numbers $RA$ and $RB$ are announced to TP using classical channels.

Step 4: After getting $RA$ and $RB$, TP computes $r_j = ra_j \oplus t1_j \oplus rb_j \oplus t3_j$, with $RA$, $RB$, $T1$, and $T3$, where $r_j \in \{0, 1\}$, $R = (r_{N-1}...r_1r_0)$, $j \in \{0, 1, ..., N-1\}$. Once the computation outcome $r_j$ is 1, TP announces the inequality of the customers' private data and terminates its work. Otherwise, TP resumes calculating $r_j$ until the subscript $j = 0$, that is, all the bits of $RA$, $RB$, $T1$, and $T3$ have been calculated; the computation ends up $r_0 = 0$. At this time, it announces that the two participants' private data are identical.

From the steps above, we can deduce the comparisons with previous Bell-based QPC protocols, which are shown in Table 1.

## 3 Analyses

### 3.1 Correctness

In the steps above, the expression $r_j = ra_j \oplus t1_j \oplus rb_j \oplus t3_j = r_j = t0_j \oplus a_j \oplus t4_j \oplus t1_j \oplus t2_j \oplus b_j \oplus t5_j \oplus t3_j$ holds. Once measured by Alice, Bob and TP, the Bell state $|\phi^+\rangle = 1/\sqrt{2}$

**Table 1** Comparisons with previous Bell-based QPC protocols

| Items | Bell-based QPCs [9–18] | This work |
|---|---|---|
| Bell-states forms | two forms or above | only a single form |
| Bell-generating devices or ways | at least two | one |
| States-generation switching | Yes | No |
| Production cost | High | Low |
| Production efficiency | Low | High |
| Practicability | Low | High |

$(|00\rangle + |11\rangle)$ will collapse to one of the two states $\{|00\rangle, |11\rangle\}$. Whether it is $|00\rangle$ or $|11\rangle$, these equations below will be right: $t0_j = t1_j$, $t2_j = t3_j$, $t4_j = t5_j$. Therefore, $r_j = a_j \oplus b_j$. According to the exclusive-OR operation, as long as $r_j = 1$, it indicates that $a_j$ is not equal to $b_j$; if all the $r_j = 0$, this means $a_j = b_j$. So the presented protocol can function correctly.

### 3.2 Security Analysis

The security of the protocol will be analysed from outsider attacks and insider attacks.

#### 3.2.1 Outsider Attack

There is no place for outsiders to attack in all the steps above except Step 1, where the qubit transmissions through the quantum channels are prone to outsider attacks. In Step 1, the sequences *SA* and *SB* containing decoy photons are transmitted in the way of quantum data block [43]; the decoy photon technique [44–45] also delivers the security of the qubit transmissions, which can be regarded as a variation of the eavesdropping check method of the BB84 protocol, proven to be unconditionally secure by Ref. [46].

In Step 3, for the announced number *RA* (*RB*) is encrypted by the one-time values *T0* and *T4* (*T2* and *T5*), which are only known to TP and Bob (TP and Alice), respectively, the private data will not be revealed to anyone. In Step 4, the announced $r_j = 1$ does not include any private data at all.

In short, the presented protocol can be resistant to outsider attacks.

#### 3.2.2 Insider Attack

There are two cases of insider attacks to discuss. One is a possibility for one party to get the other's private data. The other is a probability for TP to retrieve two parties' private data.

**Two Participants' Attack** Since Alice's role is equal to Bob's, only one case is discussed that Alice will try to know Bob's private data. The only way for Alice is to use the photons sent to her, i.e. the sequences *T0* and *T4*, by which she will just know *T1* and *T5* according to the properties of Bell states. However, *RB* is encrypted by Bob's *T2*, which is one-time values for, measured along *Z* basis, Bob's photon will collapse to $|0\rangle(|1\rangle)$ with probability of 50%. Because Bob can't release his own *T2* to Alice and also she is not able to deduce *T2* through TP's *T3* for the semi-honest TP cannot cooperate with any participant, Alice has no idea of *T2* and *T3*. Therefore, it is impossible for Alice to obtain Bob's private data *B* via her own photons.

If Alice tries to intercept the transmitted particles from TP to Bob, she will be found as an outside eavesdropper as described in the previous section. Therefore, no matter what Alice does, she cannot get Bob's private data.

In one word, one party can obtain nothing about the other's secrets.

**TP's Attack** In the proposed protocol, TP is semi-honest. This means that it faithfully prepares Bell states, follows the processes, and will not be corrupted by all outside eavesdroppers. Therefore, it can cheat only using the bits *T1* and *T3*. According to the properties of Bell states, TP can infer *T0* and *T2* but cannot know the one-time states *T4* and *T5*. And, *RA* and *RB* are also encrypted by Alice's *T4* and Bob's *T5*, respectively. Thus, it cannot deduce Alice and

Bob's private data $A$ and $B$ from $RA$ and $RB$. It obtains only the bit $r_j$, namely the QPC result. This means TP cannot get any information about the two participants' privacy. Hence, the proposed protocol can oppose TP's attack.

## 4 Conclusions

In order to better usability and reduce use costs, the paper introduces a design principle for QPC protocols at first. By the design principle, it can be inferred that the singleness of the used quantum resources would mean QPC's usability to some extent for there being no states-generation switching will avail of high efficiency and low costs. To take Bell states for example, the paper implemented a QPC protocol with a single Bell state, the analyses of which shows that it performs a correct QPC function securely. Moreover, the protocol used steps as few as possible; its quantum resource is only a single Bell state, namely $|\phi^+\rangle$. So, it can be much easier to handle than those with at least two Bell states. All these manifest that the presented design principle is not only feasible but also beneficial.

**Acknowledgements** The author Lang Yan-Feng thanks Daughter Lang Duo-Zi for her support on this work. Funding by Research Project of Department of Water Resources of Zhejiang Province (Grant No.RC2075) is gratefully acknowledged.

## References

1. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
2. 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**(2), 887–897 (2013)
3. Chen, X.B., Su, Y., Niu, X.X., Yang, Y.X.: Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. Quantum Inf. Process. **13**(1), 101–112 (2014)
4. Sun, Z.W., Yu, J.P., Wang, P., Xu, L.L., Wu, C.H.: Quantum private comparison with a malicious third party. Quantum Inf. Process. **14**(6), 2125–2133 (2015)
5. Lang, Y.-F.: Semi-quantum private comparison using single photons. Int. J. Theor. Phys. **57**(10), 3048–3055 (2018)
6. Ye, T.-Y., Ye, C.-Q.: Measure-resend semi-quantum private comparison without entanglement. Int. J. Theor. Phys. **57**(12), 3819–3834 (2018)
7. Yang, Y.G., Xia, J., Jia, X., Shi, L., Zhang, H.: New quantum private comparison protocol without entanglement. Int. J. Quant. Inform. **10**(6), 1250065 (2012)
8. Ye, T.Y.: Quantum private comparison via cavity QED. Commun. Theor. Phys. **67**(2), 147–156 (2017)
9. 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**(5), 055305 (2009)
10. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
11. Zi, W., Guo, F.Z., Luo, Y., Cao, S.H., Wen, Q.Y.: Quantum private comparison protocol with the random rotation. Int. J. Theor. Phys. **52**(9), 3212–3219 (2013)
12. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
13. Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int. J. Quant. Inform. **11**(4), 1350039 (2013)
14. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semihonest third party. Quantum Inf. Process. **12**(2), 877–885 (2013)

15. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**(5), 1981–1990 (2013)
16. Lin, J., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **13**(2), 239–247 (2014)
17. Zhang, B., Liu, X.T., Wang, J., Tang, C.J.: Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **14**(12), 4593–4600 (2015)
18. Lang, Y.-F.: Quantum gate-based quantum private comparison. Int. J. Theor. Phys. **59**(3), 833–840 (2020)
19. Lang, Y.-F.: Quantum private comparison without classical computation. Int. J. Theor. Phys. **59**(9), 2984–2992 (2020)
20. 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)
21. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**(12), 3160–3163 (2011)
22. Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W states. Int. J. Theor. Phys. **53**(5), 1723–1729 (2014)
23. 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**(7), 1561–1565 (2010)
24. 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**(9), 2412–2414 (2011)
25. Li, Y.B., Wang, T.Y., Chen, H.Y., Li, M.D., Yang, Y.T.: Fault-tolerate quantum private comparison based on GHZ states and ECC. Int. J. Theor. Phys. **52**(8), 2818–2825 (2013)
26. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**(2), 1077–1088 (2013)
27. 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. Quant. Inform. **10**(4), 1250045 (2012)
28. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**(1), 212–218 (2013)
29. 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**(1), 69–77 (2012)
30. Liu,W.,Wang, Y.B., Jiang, Z.T., Cao, Y.Z., Cui, W.: New quantum private comparison protocol usingχ-type state. Int. J. Theor. Phys. 51(6), 1953–1960 (2012)
31. Lin, S., Guo, G.D., Liu, X.F.: Quantum private comparison of equality with χ-type entangled states. Int. J. Theor. Phys. **52**(11), 4185–4194 (2013)
32. 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)
33. 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)
34. Ji, Z.X., Zhang, H.G., Fan, P.R.: Two-party quantum private comparison protocol with maximally entangled seven-qubit state. Mod. Phys. Lett. A. **34**(28), 1–179 (2019)
35. 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**(4), 1085–1091 (2014)
36. Luo, Q.B., Yang, G.W., She, K., Niu, W.N., Wang, Y.Q.: Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. **13**(10), 2343–2352 (2014)
37. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with n-level entangled states. Quantum Inf. Process. **13**(11), 2375–2389 (2014)
38. 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)
39. 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)
40. Lang, Y.-F.: Improvement of multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping. Int. J. Theor. Phys. **59**(9), 2773–2780 (2020)
41. Chou, W.H., Hwang, T., Gu, J.: Semi-quantum private comparison protocol under an almost-dishonest third party. http://arxiv.org/pdf/quant-ph/160707961.pdf
42. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A. **56**(2), 1154–1162 (1997)
43. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A. **65**, 032302 (2002)
44. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with bell states and local unitary operations. Chin. Phys. Lett. **22**(5), 1049–1052 (2005)

45. Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**(11), 2896–2899 (2006)
46. Shor P. W., Preskill J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85(2), 441–444(2000)