International Journal of Theoretical Physics (2021) 60:1686–1691
https://doi.org/10.1007/s10773-021-04790-4

Cryptanalysis and Improvement of Quantum Private Comparison without Classical Computation

Duan Ming-Yi[1]

Received: 10 January 2021 / Accepted: 22 March 2021 / Published online: 27 April 2021

Abstract
Recently, Lang suggested a quantum private comparison (QPC) without classical computation (Int J Theor Phys, 59(2020)2984). Lang claimed that this QPC protocol is secure against both the participant attack and the outside attack. It is pointed out in this paper that the third party (TP) can totally obtain the private binary sequences of two communicants by launching a special measurement attack; and moreover, an outside attacker can make this protocol fail by launching the disturbance attack. The corresponding methods are further put forward to overcome these drawbacks.

Keywords Quantum private comparison (QPC) · GHZ state · Controlled-not gate · Measurement attack · Disturbance attack

1 Introduction

In 2009, Yang and Wen [1] put forward the first quantum private comparison (QPC) protocol by using Bell entangled states. Hereafter, a lot of researchers focused their attentions on QPC so that numerous QPC protocols have been constructed [2–7]. It is apparent that there is always a classical computation process in most of existing QPC protocols, which outputs the comparison outcome of the private inputs of communicants. Recently, Lang [8] proposed the first fully quantum QPC protocol, which substitutes the classical exclusive-or operations with quantum controlled-not gates to implement comparison. Duan [9] pointed out the weaknesses of Ref. [8] and suggested the corresponding strategies to improve them. Subsequently, Lang [10] suggested another fully quantum QPC protocol without classical computation by using GHZ states. In Ref. [10], Lang claimed that his protocol is secure against both the participant attack and the outside attack. However, it is not the truth. In this paper, the security loopholes

✉ Duan Ming-Yi
duanmingyi2020@163.com

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

of the protocol of Ref. [10] is illustrated in detail, and the corresponding methods are further put forward to overcome these drawbacks.

The remaining part of this paper is arranged as follows: Sect.2 reviews Lang's QPC protocol without classical computation; Sect.3 points out the security loopholes of Lang's QPC protocol without classical computation; Sect.4 put forwards the corresponding improving methods; and finally, Sect.5 gives the conclusion.

2 Review of Lang's QPC Protocol without Classical Computation

It has been proven by Lang in Ref. [10] that

$$\boldsymbol{CNOT}|+\rangle|+\rangle = |+\rangle|+\rangle, \tag{1}$$

$$\boldsymbol{CNOT}|-\rangle|+\rangle = |-\rangle|+\rangle, \tag{2}$$

$$\boldsymbol{CNOT}|+\rangle|-\rangle = |-\rangle|-\rangle, \tag{3}$$

$$\boldsymbol{CNOT}|-\rangle|-\rangle = |+\rangle|-\rangle, \tag{4}$$

where $|\pm\rangle = \left(1/\sqrt{2}\right)(|0\rangle \pm |1\rangle)$, $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. Apparently, the above four equations imply that if both of two qubits are from $\{|+\rangle, |-\rangle\}$, the first qubit and the second qubit will serve as a target qubit and a control qubit, respectively. Therefore, it can be easily derived that

$$\boldsymbol{CNOT}|v\rangle|w\rangle = (|v\rangle \oplus |w\rangle)|w\rangle, \tag{5}$$

where $|v\rangle, |w\rangle \in \{|+\rangle, |-\rangle\}$, $|+\rangle \oplus |+\rangle = |+\rangle$, $|-\rangle \oplus |+\rangle = |-\rangle$, $|+\rangle \oplus |-\rangle = |-\rangle$, $|-\rangle \oplus |-\rangle = |+\rangle$.

Suppose that Alice owns the private binary sequence $A = (a_{L-1}\ldots a_1 a_0)$ while Bob has the private binary sequence $B = (b_{L-1}\ldots b_1 b_0)$, where a_j, $b_j \in \{0, 1\}, j \in \{0, 1, \ldots, L-1\}$. If $|+\rangle$ and $|-\rangle$ denote the classical bits 0 and 1, respectively, the quantum counterparts of A and B will be $QA = (qa_{L-1}, \ldots, qa_1, qa_0)$ and $QB = (qb_{L-1}, \ldots, qb_1, qb_0)$, respectively, where qa_j, $qb_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Lang's QPC protocol without classical computation is composed of the following steps.

- **Step 1:** The semi-honest TP generates LGHZ states $|GHZ\rangle = \left(1/\sqrt{2}\right)(|000\rangle + |111\rangle) = (1/2)\,(|++\rangle + |--\rangle)\,|+\rangle + (1/2)\,(|+-\rangle + |-+\rangle)\,|-\rangle$. TP picks out the first, the second and the third particles of these LGHZ states to make up sequences SA, SB and ST, respectively. Afterward, TP generates two sets of decoy photons DA and DB, which are randomly chosen from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, TP randomly mixes DA

with SA to compose the new sequence SA^*, and DB with SB to compose the new sequence SB^*. Finally, TP measures ST with the X basis to obtain the measurement results $MT = \{mt_{L-1}, \ldots, mt_1, mt_0\}$, where the X basis is $\{|+\rangle, |-\rangle\}$, $mt_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$, and transmits SA^* and SB^* to Alice and Bob, respectively. Obviously, the decoy photon technology [11, 12] is used to guarantee the transmission security of SA^* and SB^*.

- **Step 2:** After confirming that Alice (Bob) has received SA^* (SB^*), TP tells Alice (Bob) the positions and the measuring bases of decoy photons in SA^* (SB^*). Then, Alice (Bob) uses the correct measuring bases to measure the decoy photons in SA^* (SB^*) and tells TP her (his) measurement results. Afterward, TP judges whether the quantum channel is secure or not. If the error rate is small enough, the protocol will be continued; otherwise, it will be terminated.
- **Step 3:** Alice (Bob) discards the decoy photons in SA^*(SB^*) to restore SA (SB). Alice measures SA with the X basis to obtain the measurement results $SA' = \{sa_{L-1}, \ldots, sa_1, sa_0\}$, where $sa_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. As a result, SB is collapsed into $\{sb_{L-1}, \ldots, sb_1, sb_0\}$, where $sb_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Then, Alice preforms the controlled-not gate $G0$ on two particles sa_j and qa_j which act as the target and control qubits, respectively. Bob preforms the controlled-not gate $G1$ on two particles sb_j and qb_j which act as the target and control qubits, respectively. As a result, $RA = \{ra_{L-1}, \ldots, ra_1, ra_0\}$ and $RB = \{rb_{L-1}, \ldots, rb_1, rb_0\}$ are derived by Alice and Bob, respectively, where $ra_j = sa_j \oplus qa_j \in \{|+\rangle, -\rangle\}, rb_j = sb_j \oplus qb_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Finally, Alice and Bob send RA and RB to TP, respectively.
- **Step 4:** TP preforms the controlled-not gate $G2$ on two particles rb_j and ra_j which act as the control and target qubits, respectively. As a result, ra_j is changed into $rt_j = ra_j \oplus rb_j$, where $rt_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Then, TP preforms the controlled-not gate $G3$ on two particles rt_j and mt_j which act as the target and control qubits, respectively. As a result, rt_j is changed into $r_j = rt_j \oplus mt_j = ra_j \oplus rb_j \oplus mt_j = sa_j \oplus qa_j \oplus sb_j \oplus qb_j \oplus mt_j$, where $r_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$.
- **Step 5:** TP measures the particle r_j with the X basis. If TP discovers one r_j in the state of $|-\rangle$, she will terminate the protocol immediately and announce that A and B are not equal; otherwise, she will terminate the protocol and announce that A and B are identical.

3 Security Loopholes of Lang's QPC Protocol without Classical Computation

3.1 The Disturbance Attack of an Outside Attacker

In Lang's QPC protocol without classical computation, Alice and Bob need to send RA and RB to TP, respectively. However, both RA and RB are sent to TP without any protection effort. If an outside attacker launches the disturbance attack, i.e., permuting the orders of particles of RA or RB, TP will inevitably obtain the wrong comparison result of A and B in the end. In this case, this protocol fails.

3.2 The Measurement Attack of TP

In the realm of QPC, Chen et al. [2] defined the first kind of semi-honest TP, i.e., TP executes the protocol loyally, keeps a record of all its intermediate computations and might try to steal

the users' private information from the record, but cannot be corrupted by others. Yang et al. [13] defined the second kind of semi-honest TP, i.e., TP is allowed to misbehave on her own but cannot conspire with others. It is well known that Yang et al.'s definition of semi-honest TP is much more reasonable in reality than Chen et al.'s definition of semi-honest TP. Lang's QPC protocol without classical computation is secure towards Chen et al.'s definition of semi-honest TP. However, it is unsecure towards Yang et al.'s definition of semi-honest TP. In the following, this point will be illustrated in detail.

In order to steal Alice and Bob's private binary sequences without being discovered, TP takes the following extra actions: (1) in Step 1, before randomly mixing DA (DB) with SA (SB), TP measures SA (SB) with the X basis to know the state of sa_j (sb_j), where $j \in \{0, 1, \ldots, L-1\}$; (2) in Step 4, after receiving RA (RB) from Alice (Bob), TP measures ra_j (rb_j) with the X basis to know its state, where $j \in \{0, 1, \ldots, L-1\}$. Then, TP decodes out qa_j (qb_j) by calculating $sa_j \oplus ra_j$ ($sb_j \oplus rb_j$), where $j \in \{0, 1, \ldots, L-1\}$. In this way, TP can totally know $A(B)$ without being discovered.

4 Improvement of Lang's QPC Protocol without Classical Computation

In order to resist the disturbance attack of an outside attacker and the measurement attack of TP, Lang's original QPC protocol without classical computation is changed into the following one.

- **Step 1:** The semi-honest TP generates$L+\delta$GHZ states $|GHZ\rangle = \left({}^{1}/_{\sqrt{2}}\right)(|000\rangle + |111\rangle) = (1/2)(|++\rangle + |--\rangle)|+\rangle + (1/2)(|+-\rangle + |-+\rangle)|-\rangle$. TP picks out the first, the second and the third particles of these $L+\delta$GHZ states to make up sequences SA, SB and ST, respectively. Afterward, TP generates two sets of decoy photons DA and DB, which are randomly chosen from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, TP randomly mixes DA with $SA$to compose the new sequence SA^*, and DB with SB to compose the new sequence SB^*. Finally, TP measures ST with the X basis to obtain the measurement results $MT = \{mt_{L-1}, \ldots, mt_1, mt_0\}$, where $mt_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$, and transmits SA^* and SB^* to Alice and Bob, respectively. Obviously, the decoy photon technology [11, 12] is used to guarantee the transmission security of SA^* and SB^*.
- **Step 2:** After confirming that Alice (Bob) has received SA^* (SB^*), TP tells Alice (Bob) the positions and the measuring bases of decoy photons in SA^* (SB^*). Then, Alice (Bob) uses the correct measuring bases to measure the decoy photons in SA^* (SB^*) and tells TP her (his) measurement results. Afterward, TP judges whether the quantum channel is secure or not. If the error rate is small enough, the protocol will be continued; otherwise, it will be terminated.
- **Step 3:** Alice (Bob) discards the decoy photons in SA^* (SB^*). Then, Alice and Bob randomly select δGHZ states from $L+\delta$ones to check the authenticity of GHZ states prepared by TP in Step 1 as follows. (1) Alice randomly chooses the Z-basis ($|0\rangle, |1\rangle$)or the X basis to measure the particles of these δGHZ states in her hand; (2) Alice tells Bob and TP her measurement basis for these δGHZ states; (3) Bob and TP use the measurement basis same to Alice's to measure the corresponding particles in their respective hands: (4) TP tells Alice and Bob her measurement results of the particles of these

δGHZ states in her hand; (5) Alice and Bob judges the authenticity of GHZ states prepared by TP in Step 1 by comparing their measurement results with TP's measurement results. If the error rate is small enough, the protocol will be continued; otherwise, it will be terminated.

- **Step 4:** Alice (Bob) discards the particles of δGHZ states in $SA^*(SB^*)$ to obtain$SA'(SB')$. Alice measures SA' with the X basis to obtain the measurement results $\{sa_{L-1}, \ldots, sa_1, sa_0\}$, where $sa_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. As a result, SB' is collapsed into $\{sb_{L-1}, \ldots, sb_1, sb_0\}$, where $sb_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Then, Alice preforms the controlled-not gate $G0$ on two particles sa_j and qa_j which act as the target and control qubits, respectively. Bob preforms the controlled-not gate $G1$on two particles sb_j and qb_j which act as the target and control qubits, respectively. As a result, $RA = \{ra_{L-1}, \ldots, ra_1, ra_0\}$ and $RB = \{rb_{L-1}, \ldots, rb_1, rb_0\}$ are derived by Alice and Bob, respectively, where $ra_j = sa_j \oplus qa_j \in \{|+\rangle, |-\rangle\}, rb_j = sb_j \oplus qb_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Finally, Alice (Bob) sends RA (RB) to TP with the decoy photon technology.
- **Step 5:** Alice (Bob) checks the transmission security of RA (RB) with TP by using the method similar to that of Step 2.
- **Step 6:** TP preforms the controlled-not gate $G2$ on two particles rb_j and ra_j which act as the control and target qubits, respectively. As a result, ra_j is changed into $rt_j = ra_j \oplus rb_j$, where $rt_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$. Then, TP preforms the controlled-not gate $G3$ on two particles rt_j and mt_j which act as the target and control qubits, respectively. As a result, rt_j is changed into $r_j = rt_j \oplus mt_j = ra_j \oplus rb_j \oplus mt_j = sa_j \oplus qa_j \oplus sb_j \oplus qb_j \oplus mt_j$, where $r_j \in \{|+\rangle, |-\rangle\}, j \in \{0, 1, \ldots, L-1\}$.
- **Step 7:** TP measures the particle r_j with the X basis. If TP discovers one r_j in the state of $|-\rangle$, she will terminate the protocol immediately and announce that A and B are not equal; otherwise, she will terminate the protocol and announce that A and B are identical.

In the improved QPC protocol, the decoy photon technology is adopted to protect the transmissions of RA (RB) from Alice (Bob) to TP. If an outside attacker launches the disturbance attack described in Sect.3, she will inevitably leave her trace on the decoy photons so that she will be discovered undoubtedly by the eavesdropping check processes of Step 5. In addition, if TP launches the measurement attack described in Sect.3, TP's attack will inevitably be detected by the check processes of Step 3.

5 Conclusion

In summary, this paper points out the security loopholes of Lang's QPC protocol without classical computation firstly, i.e., TP can totally obtain the private binary sequences of two communicants by launching a special measurement attack and an outside attacker can make it fail by launching the disturbance attack, and then put forwards the corresponding methods to overcome these drawbacks.

Declarations

Conflict of Interest The author declares that he has no conflicts 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. 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)
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. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**, 1077–1088 (2013)
5. 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)
6. 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 and Astron. **60**(9), 090312 (2017)
7. 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)
8. Lang, Y.F.: Quantum gate-based quantum private comparison. Int. J. Theor. Phys. **59**, 833–840 (2020)
9. Duan, M.Y.: Cryptanalysis and improvement of quantum gate-based quantum private comparison. Int. J. Theor. Phys. **60**(1), 195–199 (2021)
10. Lang, Y.F.: Quantum private comparison without classical computation. Int. J. Theor. Phys. **59**, 2984–2992 (2020)
11. 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 (2005)
12. 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 (2006)
13. 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)