Int J Theor Phys (2016) 55:2969–2976
DOI 10.1007/s10773-016-2929-7

Multi-Party Quantum Private Comparison Protocol with an Almost-Dishonest Third Party using GHZ States

Sheng-Liang Huang[1] · Tzonelih Hwang[1] · Prosanta Gope[1]

Received: 22 October 2015 / Accepted: 16 January 2016 / Published online: 27 January 2016

Abstract This article proposes an innovative quantum private comparison (QPC) protocol for *n* users using GHZ states, where an almost-dishonest third party (TP) is introduced to assist the participants for comparing their secrets. It is argued that as compared to the existing QPC protocols our proposed scheme has some considerable advantages. First, in the existing QPC protocols, the TP can only to determine whether all participants' secrets are equal or not. Instead of that, in our proposed scheme a TP can even compare the secrets between any subsects of users. Second, since our proposed scheme is based on GHZ state; hence it can ensure higher efficiency as compared to other existing multi-party QPC protocols on d-dimension photons.

Keywords Quantum private comparison · Almost-dishonest · 2-dimensional photon

1 Introduction

Quantum private comparison (QPC) is an imperative branch of secure multiparty computing, which allows two participants to determine whether their secrets happened to be equal or not, and at the same time their inputs can be kept in secret. The first pioneering work in QPC was proposed by Yang et al. [2], where the secrets of two parties can be compared with the Einstein-Podolsky-Rosen (EPR) pairs, and its security was guaranteed with the concept of the inclusion of decoy photons in the quantum sequence and the one-way hash function, which utilizes to encipher their own secrets by both of the players. Moreover, to

✉ Tzonelih Hwang
hwangtl@csie.ncku.edu.tw

Sheng-Liang Huang
thanatos116@gmail.com

Prosanta Gope
prosanta.nitdgp@gmail.com

[1] Tainan City, Taiwan, Taiwan, Republic of China

resist some special attacks in their round trip transmissions, a number of special optical filters are inserted in every round, which decreases the qubit efficiency. Hereafter, Chen et al. [3] proposed a QPC protocol using a triplet Greenberger-Horne-Zeilinger (GHZ) states. In their protocol, to construct a secure equality function in a two-party scheme, a semi-honest TP was introduced, where TP might try to steal the players' private inputs, which makes the protocol insecure.

Subsequently, few more interesting QPC protocols have been proposed, where all comparison are between two parties. Examples of them include, Tseng et al.'s [4] QPC protocol without any entangled EPR pairs and Liu et al. [5–9] proposed QPC protocols which are based on the GHZ states, triplet W states and the χ-type genuine four particle entangled states. Besides, there are some QPC protocols [14–17], which have been proposed with the concept of d-dimensional photon. However, because of the requirement of the highly-constrained equipment, 2-dimensional photon is considered to be more practical than the d-dimensional one.

In 2013, the first multi-party QPC was proposed by Chang et al. [1], where, if there are $n$parties, each of them have a private information, then $n$parties can determine their $n$secrets are equal or not. Now, like [3], and [5–9] in this case also, a semi-honest TP is involved to help the participants, which we consider as a strong assumption, because, in the real world, TP may not be semi-honest always. Here, by semi-honest TP we mean that the TP has to execute the protocol loyally and announce the result of the comparison faithfully. If TP wants to obtain the two participants' secret information, he/she might be able to do that by using the records of all intermediate transmissions and computations of the participants to reveal the private information. Till date, there are two kinds of definitions for the semi-honest TP. One is similar to the definition, used in [1], and [5–9]. On the other hand, the other definition of the semi-honest TP is that, except colluding with the participants, TP may try to perform several possible attacks for disclosing the secret information of the participants. There are some existing QPC protocols [14–17], where the second definition of the semi-honest TP is used. Even though, the capabilities of the TP in two different definitions are dissimilar. However, they are represented with the same designation, i.e. semi-honest, which may confuse a reader (especially a beginner). In this article, at first we resolve this issue by designating the TP used in [14–17], as almost-dishonest [18, 19]. Subsequently, we propose a quantum private comparison (QPC) protocol for n users using GHZ states, where an almost-dishonest third party (TP) will support the participants for comparing their secrets. As compared to the existing QPC protocols our proposed scheme has some notable advantages. Firstly, in the existing QPC protocols, a TP only to determine whether all participants' secrets are equal or not, instead in our proposed QPC protocol, a TP can even compare the secrets between any subsects of users. Secondly, since our proposed QPC protocol is based on GHZ state; hence it can ensure higher efficiency as compared to other existing multi-party QPC protocols on dimension photons [14–17], where capability of the TP is similar as ours.

Therefore, the rest of the article is organized as follows. In Section 2, we present our proposed scheme. Security of the proposed scheme is analyzed in Section 3. Finally, the concluding remarks are given in Section 4.

2 Proposed Scheme

This section comprises of our proposed QPC protocol with almost-dishonest TP. To do so, here at first we make a specific way for choosing the initial states, which helps the participants to check that whether their particles generated by TP are entangled or not. In other words, if TP generates any fake states like single photons, which may benefit TP to comprehend the secrets of the participants. Now, in order to prevent TP to do such things, our approach for selecting the initial states helps the participants to verify that whether the initial states generated by TP are phony or not.

Considering the GHZ states are described as follows:

$K^m = \frac{1}{\sqrt{2}}\left(|S_m\rangle + |\overline{S_m}\rangle\right), K^n = \frac{1}{\sqrt{2}}\left(|S_n\rangle - |\overline{S_n}\rangle\right)$, where $m, n = 1, 2, 3, ..., 2^{N-1}$, $|S_m\rangle, |S_n\rangle = |q_1, q_2, ..., q_N\rangle, |\overline{S_m}\rangle + |\overline{S_n}\rangle = |\overline{q_1, q_2, ..., q_N}\rangle, q_1 = 0, q_2, q_3, ..., q_N \in \{0, 1\}$. Here, N denotes the number of participants to compare the equality of their secrets.

In order to resist TP from preparing any fake initial states, here we selects the set of 2^{N-1} initial states (*IS*) Ψ^i, where $i = 1, 2, 3, ..., 2^{N-1}$, In which, 2^{N-2} are chosen from K^m and the rest 2^{N-2} from K^n where $m \neq n$, and for every $m \neq n \Rightarrow |S_m\rangle \neq |S_n\rangle$. In other words, exactly equal number initial states should be chosen from K^m and K^n. Otherwise, any unequal ratio may cause information leakage problem.

Ψ^i can be represented in Z-basis as follows:

$\Psi^i = \frac{1}{\sqrt{2}}\left(|q_1, q_2, ..., q_N\rangle + (-1)^{\Delta}|\overline{q_1, q_2, ..., q_N}\rangle\right)$ where Δ is either 0 or 1

Now, for verifying the initial states, the participants need two conjugate bases to check the entanglement between their particles. So, we convert the above initial states in X-basis, which can be denoted as follows:

$\Psi^i = \frac{1}{\sqrt{2}}\left(|q_1, q_2, ..., q_N\rangle + (-1)^{\Delta}|\overline{q_1, q_2, ..., q_N}\rangle\right) = \frac{1}{\sqrt{2^{N-1}}}(-1)^{\delta}|x_1, x_2, ..., x_N, \rangle$, $x_i \in \{+, -\}$ and $n(-)\begin{cases} even, if\, \Delta = 0 \\ odd, if\, \Delta = 1 \end{cases}$, where $\delta = \sum_{\{j|x_j=-\}} q_j$ (mod2) means the sum of all the q_j mod 2 if j satisfy that $x_j = -$ and in that case $n\,(-)$ represents the total number of '$-$'.

Protocol Steps:

1. TP selects a set of initial states $\left\{\Psi^1, \Psi^2, ..., \Psi^{2^{N-1}}\right\}$ according to the above rule and publishes to all the participants. Hereafter, during each execution of the protocol, TP can randomly choose GHZ state from the set of initial states to establish the sequence of initial state IS_{TP}.
2. Now, TP sends the sequence of ith photon, p_i with some decoy photons to the participant i and similarly, sends the sequence of $(i+1)th$ photons p_{i+1} with the decoy photons to the participant $i+1$ and so on.
3. Hereafter, TP needs to do the public discussion with every participant for informing the corresponding positions and bases of the decoy photons. Based on that, every participant can check their decoy photons. In that case, if the error rate is smaller than the threshold value, then execution of the protocol will be continued, otherwise, the execution of the protocol will be aborted.
4. Next, all the participants require to choose some positions of p in order to check that whether TP cheats with the initial states or not. To do so, at first they need to discuss for choosing some positions, and ask TP to announce the initial states about those corresponding positions. After that, they also need to discuss for selecting the identical basis from Z basis $\{|0\rangle, |1\rangle\}$ or X basis $\{|+\rangle, |-\rangle\}$ (where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$) and use the bases to measure the corresponding positions of p. In that case, if the error rate is smaller than a threshold value, then the execution of the protocol will be continued, or the protocol is required to be aborted. Conceive that, after dropping those checked photons, we have p' photons.

5. Hereafter, the participant i will measure p' with Z basis and gets the measurement result MR_i and calculates $C_i = MR_i \oplus S_i$ then sends C_i to TP.
6. Now, based on the result of $C_i \oplus C_j$, TP can comprehend that whether each two of them are equal or not. Because, $C_i \oplus C_j = MR_i \oplus S_i \oplus MR_j \oplus S_j$, and TP knows $MR_i \oplus MR_j$ which reveals by the corresponding initial states.

Example

In order to clarify our proposed scheme in detail, here we give an example. Conceive that, there are three participants namely, Alice, Bob and Charlie with secrets $S_A = 4$, $S_B = 4$ and $S_C = 2$, want to compare their secrets and there is a third party denoted as TP, who is almost-dishonest can help them. TP chooses $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$, $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$ and $\frac{1}{\sqrt{2}}(|100\rangle - |011\rangle)$ from three-particle GHZ states according to the above rule as the set of initial states which is used for this round. Then, TP publishes the initial states of the above four states to all the participants. At the same time, TP generates five three-particle GHZ states $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$, $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ as the initial states. After that, TP sends the first, second and third photons of all sequences with decoy photons to Alice, Bob and Charlie, respectively. When all the participants receive the photons, TP announces the positions and measurement bases of the decoy photons. Then, every participant discusses with TP to check whether there exists any eavesdropper or not. If there is no eavesdropper, then all the participants discuss together to choose the positions one and three and ask TP to announce the initial states.

So, TP announces the initial state of position one with $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$ and position three with $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Then, all the participants decide to use X basis to measure position one and Z basis to measure position three. Hereafter, they measure the corresponding photons and publish the measurement results and eventually check whether the states are correct or not. If so, then all the participants drop the checked photons and measure the remaining photons with Z-basis. Here, we assume Alice, Bob and Charlie get the measurement results MR_A, MR_B and MR_C with 001, 101, and 001. (Because the remaining states is $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.) Then, they XOR the secrets $S_A = 4$, $S_B = 4$ and $S_C = 2$ with the MR_A, MR_B and MR_C, respectively and eventually get $C_A = 101$, $C_B = 001$ and $C_C = 011$. Subsequently, they send them to TP. After receiving C_A, C_B and C_C, since TP knows $MR_A \oplus MR_B = 100$, hence, TP can compare Alice's and Bob's secrets by $C_A \oplus C_B \oplus MR_A \oplus MR_B = 101 \oplus 001 \oplus 100 = 000$. Then TP can comprehend that S_A is the same as S_B. On the other hand, since $C_A \oplus C_B \oplus MR_A \oplus MR_B = 101 \oplus 011 \oplus 000 = 110$, so, TP can know that S_A is not the same as S_C.

3 Security Analysis and Comparison

In this section, at first we will demonstrate that our proposed scheme holds several imperative security properties, which are indeed essential to offer a secure QPC protocol. Then, in order to manifest the advantages of our proposed scheme, we compare the performance of our proposed scheme with respect to [1–3].

3.1 Outsider Attack

After TP sent all the particles to each participant, every participant needs to do the public discussion to check whether any outside attacker exists or not. In that case, at first, TP will announce the positions and measurement bases of all the decoy photons to each participant. Then, each participant can get the measurement results by measuring the corresponding decoy photons. After that, every participant needs to publish the measurement results to TP and then TP can verify the measurement results sent from the participants to determine whether there exists any outside attacker or not.

Since, the outside attacker does not know the positions and measurement bases of the decoy photons, some well-known attacks such as intercept-resend attack [10], correlation-elicitation attack [11], and entanglement-measure attack [12] can be detected via the checking mechanism [13]. For example, if Eve measures a decoy photon $|0\rangle$ or $|1\rangle$ with Z basis $\{|0\rangle, |1\rangle\}$, she can pass the public discussion. However, if Eve measures a decoy photon $|+\rangle$ or $|-\rangle$ with Z basis $\{|0\rangle, |1\rangle\}$, she will have the probability of 50 % to be detected. Obviously, Eve has a probability of 50 % to choose the wrong basis for measurement. Therefore, the detection rate for each decoy photons is 25 % (50 %×50 %). For l decoy photons (where l is large enough), the detection rate is $1 - (3/4)^l$ which is close to 1 if l is large enough. Furthermore, since quantum bits are transmitted only once in the proposed protocol, the Trojan horse attack can be automatically prevented. Therefore, the proposed protocol is free from any outsider attack.

Table 1 The comparison of the proposed protocol to the other QPC protocols

	Yang et al.'s [2]	Cheng et al.'s [3]	Chang et al.'s [1]	Our protocol
Quantum state	Bell state	Triplet GHZ state	m-particle GHZ class state	m-particle GHZ class state
Devices for Trojan horse attack	Yes	No	No	No
Operators for users	Unitatry operator	Single photon measurement	Single photon measurement	Single photon measurement
Quantum measurement for TP	No	Yes	No	No
Qubit efficiency	$\frac{nm}{4(m+l)(n-1)}$ $\sim \frac{nm}{4n(m+l)(n-1)}$	$\frac{nm}{(3m+2l)(n-1)}$ $\sim \frac{n}{n(3m+2l)(n-1)}$	$\frac{nm}{n(m+1)}$	$\frac{nm}{2n(m+1)}$
Number of times of protocol execution	$n-1 \sim \frac{n(n-1)}{2}$	$n-1 \sim \frac{n(n-1)}{2}$	1	1
TP	Dishonest (information leakage)	Semi-honest	Semi-honest	Almost-dishonest

Table 2 The comparison of the proposed protocol to the other almost dishonest based QPC protocols

Parameters	[14]	[15-A]	[15-b]	[16]	[17]	Proposed scheme
Environment	Multi-party compare equality (all users)	Multi-party compare equality (all users)	Multi-party compare equality (all users)	Multi-party compare size (Any two users)	Two-party compare size	Multi-party compare equality (Any two users)
Quantum state	$\|W\rangle = \frac{1}{2}(\|0000\rangle + \|1111\rangle + \|2222\rangle + \|3333\rangle)$	$\|W\rangle = \frac{1}{2}(\|0000\rangle + \|1111\rangle + \|2222\rangle + \|3333\rangle)$	$\|W\rangle = \frac{1}{2}(\|0000\rangle + \|1111\rangle + \|2222\rangle + \|3333\rangle)$	$\|\Psi^0_{130}\rangle = \frac{1}{2}(\|0130\rangle + \|1201\rangle + \|2312\rangle + \|3023\rangle)$	d-dimensional Single photon	$\frac{1}{\sqrt{2}}(\|q_1q_2...q_n\rangle + \|\overline{\|q_1q_2...q_n\rangle}), q_i \in \{0, 1\}$ $(n - GHZ)$
Devices for Trojan horse attack	Yes	No	Yes	No	Yes	No
Users generate photon	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon (a)	No
Operators for users	$\prod$	No	U_x	No	$\prod$	No
Quantum measurements for users	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon (B)	Single photon
Operators for TP	NO	NO	NO	NO	$\prod$	NO
Quantum measurements for TP	d-dimensional Single photon	d-dimensional Single photon	d-dimensional Single photon	No	d-dimensional Single photon	No
Qubit efficiency	$\frac{m}{3nm}$	$\frac{m}{6nm}$	$\frac{m}{(5+n)m}$	$\frac{m}{2nm}$	$\frac{m}{6m}$	$\frac{nm}{2n(m+1)}$
Number of times to compare all users	1	1	1	1	$n - 1$	1
Number of times to compare any two users	No	No	No	1	$n - 1 \sim \frac{n(n-1)}{2n}$	1
Honesty Level of TP	Semi-hones	Almost-dishonest	Almost-dishonest	Almost-dishonest	Almost-dishonest	Almost-dishonest
Shared Key Requirement	No	No	TP-all users share m-bits	all users share m-bits	Alice – Bob share 2m-bits	No

3.2 Insider Attack

In this sub-section, we consider two cases of insider attacks. The first case discusses how to resist for a user to obtain the other user's private information. The second case discusses the possibility for TP from stealing each user's information.

Case 1 Participant attack

Suppose, there is a user, Alice, who is basically a dishonest user, attempts to obtain the other user's (Bob) private information. If Alice tries to intercept the transmitted photons from TP to Bob, she will be detected as an outside attacker as described in Section 3.1 Thus, the only possible way for Alice to do is to use her particles to extract Bob's measurement result or infer $MR_A \oplus MR_B$. However, without knowing the initial states of the GHZ class states, it is impossible for her to do so.

Case 2 Almost-dishonest TP attack

Now, we consider TP who is an almost-dishonest entity, where TP has to help each participant to accomplish the protocol but TP cannot collude with the participants. However, TP may share the fake states in order to get the useful messages (information of participants). Fortunately, in our proposed QPC protocol, all the participants will come across with the verification process (in Step 4) to check whether TP shares the correct states with them or not.

Now, TP may also try to acquire useful information from the relation of the initial states and the returned value C_i sent from each participant. According to the Step 6, the returned value is $C_i = MR_i \oplus S_i$, that means, if TP can know the value of MR_i, then, he can get the secret of S_i However, according to the initial states, TP can know the relation between two participants but cannot know the value about MR_i. Hence, TP cannot comprehend the secret from any participant.

3.3 Comparison

Now, in order to manifest the advantages of the proposed scheme, here we compare our proposed scheme with the recently proposed QPC protocols [1–3] (shown in Table 1). From Table 1, it is clear that the performance of the proposed scheme is quite similar to [1]. However, in [1], TP was assumed to be semi-honest, which may not be true always, wherein our proposed scheme TP can be almost-dishonest, that specifies that the security resistance of our proposed scheme is much higher as compared to [1–3].

To benchmark the performance of the proposed scheme more clearly, now we compare the proposed QPC protocol with respect to some recently proposed QPC protocols [14–17], where the TP is considered as an almost dishonest participant. From Table 2, it is clear that, since our proposed QPC protocol is based on the 2-diamentional photon rather than the d-dimensional one. Hence, our proposed scheme is more practical as compared to [14–17]. It should be noted that there are two protocols presented in [15], accordingly, we present them as [15-A] and [15-B].

4 Conclusion

In this article, we have presented a new multi-party quantum private comparison protocol with an almost-dishonest TP based on GHZ states. In order to do that, here have introduced some constraints for selecting the initial states, which helps the participants to check that whether their particles generated by the almost-dishonest TP are entangled or not. Finally, security analysis shows that our proposed scheme can resist several imperative attacks like insider and outsider attacks etc. Hence, the proposed scheme can be quite useful for the n-party secrets comparison.

References

1. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process **12**, 1077–1088 (2013)
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. Tseng, H.-Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process **11**, 373–384 (2011)
5. Liu, W., Wang, Y.-B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
6. 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)
7. 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 (2011)
8. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**, 583–588 (2012)
9. 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)
10. Gao, F., Guo, F.-Z., Wen, Q.-Y., Zhu, F.-C.: Comment on "Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection". Phys. Rev. Lett. **101**, 208901 (2008)
11. Gao, F., Lin, S., Wen, Q.-Y., Zhu, F.-C.: A Special eavesdropping on One-Sender versus N -Receiver QSDC Protocol. Chin. Phys. Lett. **25**, 1561 (2008)
12. Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Info. Comput. **7**, 329–334 (2007)
13. Cai, Q.-Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
14. 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)
15. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with n-level entangled states. Quantum Inf. Process. **13**, 2370–2389 (2014)
16. 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**, 2343–2352 (2014)
17. Yu, C.H., Guo, G.D., Lin, S.: Quantum private comparison with d-level single-particle states. Phys. Scr. **88**, 065013 (2013)
18. Huang, S., Hwang, T., Gope, P.: Multi-party Quantum Private Comparison with an Almost-dishonest Third Party. Quantum Inf. Process. (2015). doi:10.1007/s11128-015-1104-z
19. Chang, C.-H., Hwang, T., Gope, P.: An Efficient Quantum Private Comparison of Equality over Collective-Noise Channels. Int. J. Theor. Phys. (2015). doi:10.1007/s10773-015-2851-4