Quantum Inf Process (2014) 13:239–247
DOI 10.1007/s11128-013-0645-2

Quantum private comparison of equality protocol without a third party

Jason Lin · Chun-Wei Yang · Tzonelih Hwang

Received: 6 January 2013 / Accepted: 19 September 2013 / Published online: 1 October 2013

Abstract This paper presents a novel quantum private comparison protocol that uses Einstein–Podolsky–Rosen pairs. The proposed protocol allows two parties to secretly compare their information without exposing their actual contents. The technique of entanglement swapping enables the comparison to be achieved without the help of a third party. Moreover, because the proposed protocol employs one-step transmission and decoy photons, it is secure against the various quantum attacks in existence thus far.

Keywords Einstein–Podolsky–Rosen pair · Entanglement swapping · Quantum private comparison · Quantum cryptography

1 Introduction

Ever since the first quantum key distribution (QKD) protocol was devised by Bennett and Brassard [1], numerous quantum cryptographic applications such as quantum teleportation (QT) [2,3], quantum secret sharing (QSS) [4–8], and quantum secure direct communication (QSDC) [9–12] have been proposed to cover various security loopholes. Recently, quantum private comparison (QPC) has gained popularity as another interesting branch of quantum cryptography. The goal of a QPC protocol is

J. Lin · C.-W. Yang · T. Hwang (✉)
Department of Computer Science and Information Engineering, National Cheng Kung University,
No. 1, University Rd., Tainan City 70101, Taiwan, ROC
e-mail: hwangtl@ismail.csie.ncku.edu.tw

J. Lin
e-mail: senya_lin@hotmail.com

C.-W. Yang
e-mail: waywei.yang@gmail.com

to privately compare two parties' undisclosed information for equality. Based on the properties of quantum mechanics, an equality comparison can be easily performed without any complex computation.

The private comparison concept was already a topic for discussion in conventional cryptography. Yao [13,14] proposed a protocol to solve the millionaires' problem, in which two millionaires (say Alice and Bob) are interested in knowing which of them is richer without revealing their actual wealth. On the basis of Yao's solution to the millionaires' problem, Boudot et al. [15] subsequently proposed a protocol to determine whether the two millionaires are equally rich. However, Lo [16] indicated that the equality function used to determine this cannot be securely evaluated in a two-party scenario. Therefore, some additional assumptions such as a semi-honest third party (TP) should be considered to successfully achieve a private comparison.

The pioneering works in QPC were first presented by Yang and Wen [17], Yang et al. [18] in 2009. Since then, many QPC schemes [19–30] have been proposed to improve both the security and the qubit efficiency. Thus far, these protocols have required a TP that is at least semi-honest to help the two parties, Alice and Bob, accomplish the comparison work. According to the definitions in [17–30], a legitimate TP should faithfully execute the protocol and preserve a record of all of the intermediate computations. He/she might try to infer the players' secrets from the record, but will not be corrupted by any external adversary.

Summarizing the ideas in [17–30], a secure QPC protocol should consider the following three principles. First, the two players should compare their secrets block-by-block instead of bit-by-bit in each round to avoid leaking the actual content. Second, the players' secrets should be well covered by a secret key to prevent TP from recognizing their bit values. Finally, to prevent any player from inferring the other player's secret, TP should announce only the comparison result (i.e., identical or different), instead of other details such as the positions of different bits.

It should be noted, however, that Lo in 1997 indicated that a QPC may not be possible with a two-party scenario under the technology of that time. With the advance in quantum mechanics, especially in the development of quantum entanglement swapping [31,32], this paper reconsiders this issue on constructing a two-party QPC using the entanglement swapping of Einstein–Podolsky–Rosen (EPR) pairs. Based on the property of entanglement swapping, each player's secret can be congenitally encrypted using a one-time-pad key, which provides unconditional security for any outside eavesdropper. Furthermore, since the published information is the computation result of the user's message hash codes and the measurement results by executing exclusive-OR operation, the security for any inside user relies on the one-time-pad encryption. On the other hand, because the proposed protocol adopts the one-step quantum transmission strategy, it can be immune to Trojan horse attacks [33–38] without requiring the installation of any optical filter devices.

The rest of this paper is organized as follows. Section 2 describes the proposed QPC protocol in details by using the entanglement swapping of two EPR pairs. Section 3 analyzes the security of the proposed scheme with all aspects of attacks. Finally, a brief conclusion will be given in Sect. 4.

2 The proposed two-party QPC protocol

In this section, first an observation to the entanglement swapping of two EPR pairs will be introduced. Then, based on the observed property, details of the newly proposed two-party QPC will be described in steps, in which the protocol can be done without a trusted TP.

2.1 The entanglement swapping of two EPR pairs

Entanglement swapping [31,32] is a physical phenomenon of quantum mechanics, which allows two or more independent entangled systems to build up entanglement to each other by switching their photons. In this paper, we only interest in the result of swapping two EPR pairs. For convenience, suppose that there are two unrelated parties: Alice and Bob. Each prepares an EPR pair in one of the four Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, respectively. Here, Alice's two particles of EPR pair are denoted as (A_1, A_2), and those for Bob's are denoted as (B_1, B_2). After Alice exchanges her particle (A_1) with Bob's particle (B_1), the entanglement swapping can be done by performing the Bell measurement on the particle pairs (B_1, A_2) and (A_1, B_2). The relationship of the two initial Bell states and the two measurement outcomes after swapping is displayed in Table 1. For example, if the two initial states are $\{|\Psi^+\rangle, |\Psi^+\rangle\}$, then the two measurement results of entanglement swapping will become one of the four sets $\{|\Phi^+\rangle, |\Phi^+\rangle\}$, $\{|\Phi^-\rangle, |\Phi^-\rangle\}$, $\{|\Psi^+\rangle, |\Psi^+\rangle\}$, or $\{|\Psi^-\rangle, |\Psi^-\rangle\}$, as depicted in Eq. (1).

$$\begin{aligned}
|\Psi^+\rangle_{A_1A_2} \otimes |\Psi^+\rangle_{B_1B_2} &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{A_1A_2} \otimes \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{B_1B_2} \\
&= \frac{1}{2}\left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle\right)_{A_1A_2B_1B_2} \\
&= \frac{1}{2}\left(|0101\rangle + |1100\rangle + |0011\rangle + |1010\rangle\right)_{B_1A_2A_1B_2} \\
&= \frac{1}{4}\begin{bmatrix} \left(|\Psi^+\rangle + |\Psi^-\rangle\right) & \left(|\Psi^+\rangle + |\Psi^-\rangle\right) \\ +\left(|\Phi^+\rangle - |\Phi^-\rangle\right) & \left(|\Phi^+\rangle + |\Phi^-\rangle\right) \\ +\left(|\Phi^+\rangle + |\Phi^-\rangle\right) & \left(|\Phi^+\rangle - |\Phi^-\rangle\right) \\ +\left(|\Psi^+\rangle - |\Psi^-\rangle\right) & \left(|\Psi^+\rangle - |\Psi^-\rangle\right) \end{bmatrix}_{B_1A_2A_1B_2} \\
&= \frac{1}{2}\left(|\Phi^+\rangle|\Phi^+\rangle - |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\right)_{B_1A_2A_1B_2}
\end{aligned} \tag{1}$$

Let the four Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$ represent the two bit of classical information "00", "01", "10", and "11", respectively. Suppose $\{IS_1, IS_2\}$ are the two-bit codes of two initial Bell states, and $\{MR_1, MR_2\}$ are the two-bit codes of two measured Bell states after entanglement swapping. According to Table 1, a special correlation can be found that $IS_1 \oplus MR_1 = IS_2 \oplus MR_2$. Since the result of MR_i can be one of the four possibilities of two-bit information, it can be regarded as a

Table 1 The comparative table of entanglement swapping two Bell states [39]

Two initial Bell states	Two Bell states after entanglement swapping
$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Phi^+\rangle), (\vert\Phi^-\rangle, \vert\Phi^-\rangle) \\ (\vert\Psi^+\rangle, \vert\Psi^+\rangle), (\vert\Psi^-\rangle, \vert\Psi^-\rangle) \end{bmatrix}_{A_1A_2B_1B_2}$	$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Phi^+\rangle), (\vert\Phi^-\rangle, \vert\Phi^-\rangle) \\ (\vert\Psi^+\rangle, \vert\Psi^+\rangle), (\vert\Psi^-\rangle, \vert\Psi^-\rangle) \end{bmatrix}_{B_1A_2A_1B_2}$
$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Phi^-\rangle), (\vert\Phi^-\rangle, \vert\Phi^+\rangle) \\ (\vert\Psi^+\rangle, \vert\Psi^-\rangle), (\vert\Psi^-\rangle, \vert\Psi^+\rangle) \end{bmatrix}_{A_1A_2B_1B_2}$	$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Phi^-\rangle), (\vert\Phi^-\rangle, \vert\Phi^+\rangle) \\ (\vert\Psi^+\rangle, \vert\Psi^-\rangle), (\vert\Psi^-\rangle, \vert\Psi^+\rangle) \end{bmatrix}_{B_1A_2A_1B_2}$
$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Psi^+\rangle), (\vert\Phi^-\rangle, \vert\Psi^-\rangle) \\ (\vert\Psi^+\rangle, \vert\Phi^+\rangle), (\vert\Psi^-\rangle, \vert\Phi^-\rangle) \end{bmatrix}_{A_1A_2B_1B_2}$	$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Psi^+\rangle), (\vert\Phi^-\rangle, \vert\Psi^-\rangle) \\ (\vert\Psi^+\rangle, \vert\Phi^+\rangle), (\vert\Psi^-\rangle, \vert\Phi^-\rangle) \end{bmatrix}_{B_1A_2A_1B_2}$
$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Psi^-\rangle), (\vert\Phi^-\rangle, \vert\Psi^+\rangle) \\ (\vert\Psi^+\rangle, \vert\Phi^-\rangle), (\vert\Psi^-\rangle, \vert\Phi^+\rangle) \end{bmatrix}_{A_1A_2B_1B_2}$	$\begin{bmatrix} (\vert\Phi^+\rangle, \vert\Psi^-\rangle), (\vert\Phi^-\rangle, \vert\Psi^+\rangle) \\ (\vert\Psi^+\rangle, \vert\Phi^-\rangle), (\vert\Psi^-\rangle, \vert\Phi^+\rangle) \end{bmatrix}_{B_1A_2A_1B_2}$

one-time-pad key to encrypt its corresponding initial state IS_i. Furthermore, if the two initial Bell states are identical, then the two measurement results after entanglement swapping will also be the same. This feature can be used in designing a QPC protocol, which will be described in the following subsection.

2.2 The proposed QPC protocol using EPR pairs

This subsection gives description of the proposed two-party QPC protocol based on EPR pairs. Suppose two parties (say Alice and Bob) want to make contrast on the equality of their document. Both parties are able to generate EPR pairs in four Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, and single photon in four types of qubit $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. To be noted, the four Bell states can be identified by Bell measurement, and the orthogonal state $\{|0\rangle, |1\rangle\}$ $(\{|+\rangle, |-\rangle\})$ can be distinguished by Z-basis measurement (X-basis measurement). Alice and Bob compare the length of their private information. If their private information has the same length, then the proposed protocol can be depicted in steps as follows.

Step 1. Alice (Bob) prepares a sequence of EPR pairs $S_A (S_B)$ according to each two bit of her secret message $M_A (M_B)$, where “00” is $|\Phi^+\rangle$,“01” is $|\Phi^-\rangle$, “10” is $|\Psi^+\rangle$, and “11” is $|\Psi^-\rangle$. She (he) divides these EPR pairs into two sequences S_{A_1} and $S_{A_2} (S_{B_1}$ and $S_{B_2})$, which include the 1st and the 2nd particles of all states, respectively.

Step 2. Alice (Bob) mixes S_{A_1} (S_{B_1}) with some decoy photons D_A (D_B) for each particle randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to form a new sequence $S^*_{A_1}$ $(S^*_{B_1})$ and then sends it to Bob (Alice) via a quantum channel.

Step 3. After confirming that Bob (Alice) has received the quantum sequence $S^*_{A_1}$ $(S^*_{B_1})$, Alice (Bob) announces the positions and the measurement bases of D_A (D_B) to Bob (Alice). Subsequently, Bob (Alice) extracts the particles in D_A (D_B) from $S^*_{A_1}$ $(S^*_{B_1})$ and performs the corresponding bases on them to obtain the measurement results R_{D_A} (R_{D_B}). The presence of eavesdropper can be discussed between Alice and Bob by analyzing the error rate of R_{D_A} (R_{D_B}). If there is no eavesdropper, then the protocol continues to the next step. Otherwise, Alice (Bob) aborts the protocol and restarts from Step 1.

Step 4. Alice and Bob perform Bell measurement on ($S^i_{B_1}$, $S^i_{A_2}$) and ($S^i_{A_1}$, $S^i_{B_2}$) to derive two bunches of measurement results MR_A and MR_B, respectively, where i represents the ith set of EPR pair. They transform the result string MR_A (MR_B) into a binary string C_A (C_B) of M bit length and then employ the one-way hash function [40] (i.e., $H : \{0, 1\}^N \rightarrow \{0, 1\}^M$, where N denotes the length of the inputted data, and M denotes the length of the hash code) on their secret message (M_A and M_B) to obtain two hash codes, h_A and h_B, each of M bit length (i.e., $h_A = H(M_A)$ and $h_B = H(M_B)$). Finally, they compute the exclusive-OR result R_A (R_B) of h_A and C_A (h_B and C_B) (i.e., $R_A = h_A \oplus C_A$ and $R_B = h_B \oplus C_B$).

Step 5. Alice (Bob) sends R_A (R_B) to Bob (Alice) via an authenticated classical channel. Later, they can compute the exclusive-OR result R_C of R_A and R_B (i.e., $R_C = R_A \oplus R_B$). If R_C is all bit "0", then the compared secrets of the two parties are identical. Otherwise, Alice's and Bob's secret message are regarded as different. (i.e., one or more classical bits in are "1").

In the proposed QPC protocol, even if the compared secrets fall within a range of value (e.g., wealth or bid), the measurement results after entanglement swapping will cover the secret with a one-time-pad key, which is conform to the unconditional security. More specifically, it is difficult for a malicious insider (say Alice) to acquire the other party Bob's secret content M_B from $R_B = h_B \oplus C_B$, C_A, and M_A. Furthermore, the difficulty for an insider (say Alice) to retrieve the other participant Bob's encrypted secret M_B is based on the security of the one-time-pad encryption. It should be noted that abiding by the protocol means the two participants must help themselves successfully accomplish the protocol. That is, they are responsible for the correct result (i.e., R_A and R_B) of the protocol in Step 5.

According to [19,23], the function $\eta_E = \frac{q_\mathrm{s}}{q_\mathrm{t}}$ has been used to evaluate the qubit efficiency, where q_s denotes the compared classical bits, and q_t denotes the total generated photons without the decoy photons. Since two EPR pairs can compare two bit of secret among two parties, the qubit efficiency can be computed as 50 % (i.e., $\eta_E = \frac{2}{4} = 50\,\%$), which is equivalent to the most efficient scheme proposed by Tseng et al. [23]. However, the proposed QPC does not require any semi-honest TP to complete the work.

3 Security analysis

This section analyzes the security of the proposed QPC protocol. Suppose an eavesdropper Eve intends to steal the secret message of the two participants. He/she can play the role of an outside unknown adversary or an inside malicious user. Fortunately, the protocol is demonstrated to be secure against three types of quantum attack: the Trojan horse attacks, the intercept–resend attack, and the Entangle-measure attack in Sects. 3.1, 3.2, and 3.3, respectively.

3.1 Trojan horse attacks

There are two kinds of Trojan horse attack: the IPE attack [33–35] and the delay-photon attack [36,37]. In general, the IPE attack can be prevented by installing a wavelength optical device that filters out the invisible photons. As for the delay-photon attack, the receiver can pick up a portion of the photons and split each particle by a photon number splitter (PNS). If there is an unreasonable high rate of multi-photon signal, then the presence of the delay-photon attack is detected. However, these quantum equipments would consume a great amount of transmitted photons. Therefore, in the proposed QPC protocol, all photons are sent one time only to the receiver, which can make it free from the Trojan horse attacks without any optical filter devices.

3.2 Intercept–resend attack

In the proposed QPC protocol, there are some decoy photons hidden in random positions of the transmitted photon sequences $S^*_{A_1}$ and $S^*_{B_1}$. If Eve chooses the wrong polarized basis to measure and resend these particles, she will cause an error to each decoy photon with a probability of $\frac{1}{4}$. Hence, the probability of detecting Eve's attack from the public discussion is $1-\left(\frac{3}{4}\right)^n$, where n is the total number of decoy photons. When n is large enough, the detection rate of eavesdropping check will approach to 1.

3.3 Entangle-measure attack

Eve may also try to retrieve some useful information from the transmitted photon sequence by performing the entangle-measure attack. She first prepares some ancillas $E=\{|E_1\rangle, |E_2\rangle, \ldots, |E_{2N}\rangle\}$ and then entangles them with the transmitted sequence by performing a unitary operation U_E, in which $U_E^\dagger U_E = U_E U_E^\dagger = I$. However, the effect of Eve's operation on the decoy photons will cause the following possible results:

$$\begin{aligned}
U_E\big|0\big\rangle\big|E_i\big\rangle &= \alpha\big|0\big\rangle\big|e_{00}\big\rangle + \beta\big|1\big\rangle\big|e_{01}\big\rangle \\
U_E\big|1\big\rangle\big|E_i\big\rangle &= \gamma\big|0\big\rangle\big|e_{10}\big\rangle + \delta\big|1\big\rangle\big|e_{11}\big\rangle \\
U_E\big|+\big\rangle\big|E_i\big\rangle &= \frac{1}{2}\begin{bmatrix} \big|+\big\rangle\big(\alpha\big|e_{00}\big\rangle + \beta\big|e_{01}\big\rangle + \gamma\big|e_{10}\big\rangle + \delta\big|e_{11}\big\rangle\big) \\ +\big|-\big\rangle\big(\alpha\big|e_{00}\big\rangle - \beta\big|e_{01}\big\rangle + \gamma\big|e_{10}\big\rangle - \delta\big|e_{11}\big\rangle\big) \end{bmatrix} \\
U_E\big|-\big\rangle\big|E_i\big\rangle &= \frac{1}{2}\begin{bmatrix} \big|+\big\rangle\big(\alpha\big|e_{00}\big\rangle + \beta\big|e_{01}\big\rangle - \gamma\big|e_{10}\big\rangle - \delta\big|e_{11}\big\rangle\big) \\ +\big|-\big\rangle\big(\alpha\big|e_{00}\big\rangle - \beta\big|e_{01}\big\rangle - \gamma\big|e_{10}\big\rangle + \delta\big|e_{11}\big\rangle\big) \end{bmatrix}
\end{aligned}$$

To be noted, $|E_i\rangle$ is the initial state of Eve's ancilla, and $|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle$ are the four distinguishable quantum states, where the relationship of the coefficients is $|\alpha^2|+|\beta^2| = |\gamma^2|+|\delta^2| = 1$. Apparently, if the decoy photon is $|0\rangle$ or $|1\rangle$, Eve has to let $\beta=\gamma=0$ to pass the eavesdropping check. On the contrary, if the decoy photon is $|+\rangle$ or $|-\rangle$, Eve has to let $\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \gamma|e_{10}\rangle - \delta|e_{11}\rangle = \alpha|e_{00}\rangle + \beta|e_{01}\rangle - \gamma|e_{10}\rangle - \delta|e_{11}\rangle = \vec{0}$ to escape from the detection, where $\vec{0}$ denotes a zero vector. If the above two situations are all conformed, then Eve's attack will be successfully undetectable during the public discussion.

Nevertheless, since $\beta = \gamma = 0$ leads to the result of $\alpha|e_{00}\rangle - \delta|e_{11}\rangle = \vec{0}$, it implies a contradictory relationship that $\alpha|e_{00}\rangle = \delta|e_{11}\rangle$; thus, Eve is unable to identify $\alpha|e_{00}\rangle$ from $\delta|e_{11}\rangle$ in such case. Hence, she cannot obtain any useful information by measuring these ancillas. On the other hand, if Eve tries to make the ancillas distinguishable (i.e., $\alpha|e_{00}\rangle \neq \delta|e_{11}\rangle$), the states of the decoy photons will be disturbed and end up being detected in the public discussion.

4 Conclusion

Based on the entanglement swapping of two EPR pairs, this paper provides a way to compare the quantum secrets of two legitimate parties without any help from a TP. The proposed QPC scheme has adopted the one-step quantum transmission strategy and the decoy state photons to prevent various types of eavesdropping attacks. Since the participants' encrypted secrets are protected by the entanglement swapping and the one-time-pad encryption, it provides unconditional security for outside attackers and inside attackers. Moreover, to extend such arbitrator-free QPC to a multiparty scenario, and then to construct more practical applications like quantum auction and quantum voting based on these QPC's might be a promising issue in quantum cryptography.

Acknowledgments We would like to thank the anonymous reviewers for their very valuable comments, which greatly enhanced the clarity of this paper. We would also like to thank the National Science Council of Republic of China, for the financial support of this research under Contract No. NSC 100-2221-E-006-152-MY3.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984)
2. Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)
3. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**(6660), 575–579 (1997)
4. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
5. Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication. Phys. Lett. A **342**(1–2), 60–66 (2005)
6. Zhang, Z.J.: Multiparty secret sharing of quantum information via cavity QED. Opt. Commun. **261**(1), 199–202 (2006)
7. Zhang, Z.J.: Robust multiparty quantum secret key sharing over two collective-noise channels. Phys. A **361**(1), 233–238 (2006)
8. Hwang, T., Hwang, C.-C., Yang, C.-W., Li, C.-M.: Revisiting Deng et al.'s multiparty quantum secret sharing protocol. Int. J. Theor. Phys. **50**(9), 2790–2798 (2011)
9. Deng, F.-G., Long, G., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
10. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)

11. Yang, C.-W., Tsai, C.-W., Hwang, T.: Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci. China Phys. **54**(3), 496–501 (2011)
12. Yang, C.-W., Hwang, T.: Improved QSDC protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
13. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (1982)
14. Yao, A.C.-C.: How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science (1986)
15. Boudot, F., Schoenmakers, B., Traoré, J.: A fair and efficient solution to the socialist millionaires' problem. Discret Appl. Math. **111**(1–2), 23–36 (2001)
16. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
17. 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)
18. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scripta **80**(6), 065002 (2009)
19. 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)
20. 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)
21. 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)
22. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys **57**(4), 583–588 (2012)
23. Tseng, H.-Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
24. 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)
25. 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**(4) (2012)
26. 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)
27. 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)
28. 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)
29. 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. doi:10.1007/s11128-012-0505-5 (2012)
30. Li, Y.-B., Qin, S.-J., Yuan, Z., Huang, W., Sun, Y.: Quantum private comparison against decoherence noise. Quantum Inf. Process. **12**(6), 2191–2205 (2013)
31. Pan, J.W., Bouwmeester, D., Weinfurter, H., Zeilinger, A.: Experimental entanglement swapping: entangling photons that never interacted. Phys. Rev. Lett. **80**(18), 3891–3894 (1998)
32. Zukowski, M., Zeilinger, A., Horne, M.A., Ekert, A.K.: Event-ready-detectors Bell experiment via entanglement swapping. Phys. Rev. Lett. **71**(26), 4287–4290 (1993)
33. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
34. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
35. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack (vol 72, art no 044302, 2005). Phys. Rev. A **73**(4), 049901 (2006)
36. Deng, F.G., Zhou, P., Li, X.H., Li, C.Y., Zhou, H.Y.: Robustness of two-way quantum communication protocols against Trojan horse attack. Quantum Phys. arXiv:quant-ph/0508168v1 (2005)
37. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
38. Yang, C.-W., Hwang, T., Luo, Y.-P.: Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf. Process. **12**(1), 109–117 (2013)

39. Lin, J., Hwang, T.: An enhancement on Shi et al.'s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)
40. Damgard, I.B.: A design principle for hash functions. Adv Cryptol. **89**(435), 416–427 (1990)