Computers, Materials & Continua CMC, vol.61, no.2, pp.877-887, 2019

Measure-Resend Semi-Quantum Private Comparison Scheme Using GHZ Class States

Lili Yan[1, *], Yan Chang[1], Shibin Zhang[1], Qirun Wang[2], Zhiwei Sheng[1] and Yuhua Sun[1]

Abstract: Quantum private comparison is an important topic in quantum cryptography. Recently, the idea of semi-quantumness has been often used in designing private comparison protocol, which allows some of the participants to remain classical. In this paper, we propose a semi quantum private comparison scheme based on Greenberge-Horne-Zeilinger (GHZ) class states, which allows two classical participants to compare the equality of their private secret with the help of a quantum third party (server). In the proposed protocol, server is semi-honest who will follow the protocol honestly, but he may try to learn additional information from the protocol execution. The classical participants' activities are restricted to either measuring a quantum state or reflecting it in the classical basis $\{|0\rangle, |1\rangle\}$. In addition, security and efficiency of the proposed schemes have been discussed.

Keywords: Quantum private comparison, semi-quantum protocol, semi-honest third party, GHZ class states.

1 Introduction

Since Bennett and Brassard proposed the first quantum key distribution (QKD) protocol [Bennett and Brassard (1984)], various facets of secure communication have been explored using quantum technology, such as QKD [Ekert (1991); Bennett (1992)], Quantum secret sharing (QSS) [Long and Liu (2002); Guo (2002); Karlsson, Koashi and Imoto (1999)], Quantum secure direct communication (QSDC) [Deng, Gui and Liu (2003); Deng and Gui (2004); Zhong, Liu and Xu (2018); Man and Xia (2004)] and quantum private comparison (QPC). The main goal of QPCs is to compare the equality of parties' private information in pubic without revealing their information. The first QPC protocol was proposed by Yang et al. [Yang and Wen (2009)] using Einstein-Podolsky-Rosen (EPR) pairs. Many QPC protocol have been proposed with different quantum states in recent years, such as single particles [Yang, Gao and Wen (2009); Chen, Su, Niu et al. (2014); Liu, Gao, Jia et al. (2013); Yang, Xia, Jia et al. (2012)], Bell states [Yang

[1] School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610000, China.

[2] School of Engineering and Technology, University of Hertfordshire, Hertford, UK.

[*] Corresponding Author: Lili Yan. Email: yanlili@cuit.edu.cn.

and Wen (2009); Liu, Wang and Cui (2012); Tseng, Lin and Hwang (2012); Wang, Xu and Yang (2013); Lin, Yang and Hwang (2014)], GHZ states [Chen, Xu, Niu et al. (2010); Liu and Wang (2012); Chang, Tsai and Hwang (2013)] and multiple particle state. A pioneering work of Lo [Lo (2007)] pointed out two-party secure QPC is not possible. This implies that to implement secure QPC, we must have a third party, who would assist the users to compare the equality of their secrets.

It is easy to find out that all above QPC protocols require all the participants to have quantum capabilities. That is, all the participants equip advance quantum devices such as qubit generating devices and quantum memory, unitary operation and so on. So, how much quantumness is needed for participants? Alternatively, whether all the participants are required to have quantum capabilities? However, such expensive quantum resources and operations cannot be afforded by all parties. In this case, it will be difficult to apply these protocols in real environments. In 2007, Boyer et al. [Boyer, Kenigsberg and Mor (2007)] proposed the first semi-quantum key distribution. There are two participants in Boyer et al.'s schemes. One is a powerful quantum operator and the other one has only classical capabilities. The classic party can either reflect the qubits without disturbed or perform measurement and prepare a new qubit in the classical basis $\{|0\rangle,|1\rangle\}$. In Boyer's protocol, it assumes that the classical party has access to a segment of the quantum channel that leads from the lab of the powerful quantum operator to the outside world and then goes back.

Soon after, many researches based on the semi-quantum have been proposed, such as semi-quantum secret sharing (SQSS), semi-quantum key distribution (SQKD), semi-quantum secure direct communication (SQSDC) and semi-quantum private comparison (SQPC). Recently, Chou et al. [Chou, Hwang and Gu (2016)] put forward a SQPC protocol based on Bell states. But the protocol employs quantum entanglement swapping. Thapliyala et al. [Thapliyala, Sharmab and Pathak (2016)] proposed a SQPC protocol using Bell entangled states, and Lang [Lang (2018)] proposed a SQPC protocol using single photons. Ye et al. [Ye and Ye (2018)] designed a multi-user SQPC protocol based on two-particle product states. Moreover, two classical participants need to prepare a shared key before work in the SQPC protocols [Thapliyala, Sharmab and Pathak (2016); Lang (2018); Ye and Ye (2018)].

Traditionally, it is assumed that a classical party can only perform a restricted set of classical operations over a quantum channel. Specifically, a classical party can measure a qubit in the classical basis $\{|0\rangle,|1\rangle\}$, and reflect a qubit back without disturbance. Furthermore, the classical user does not require quantum memory. In the paper, we propose a two-party semi-quantum private comparison protocol based on GHZ states. There are three participants in the protocol, where server has all quantum powers, but Alice and Bob are classical. Alice and Bob compare the equality of their private secret with the help of server. Furthermore, server is semi-honest which means that he will follow the protocol honestly, but he may try to learn additional information from the protocol execution.

The rest of this paper is outlined as follows. In the next section, we give the description of the two-party semi-quantum private comparison protocol in detail. Section 3, we demonstrate the security and efficiency of our protocol. Finally, a conclusion is given in Section 4.

2 Protocol for two-party semi-quantum private comparison

In this section, we propose a two-party semi-quantum private comparison scheme. There are three participants in the protocol Alice, Bob and server. Alice and Bob are classic. They want to compare the equality of their private secret. Server is a semi-honest third party who may try to disclose the secret key during executing of the protocol, but he cannot public a fake result or collude with the participants.

Before giving our scheme, we first describe three-particle GHZ states which will be used in our protocol.

The three-particle GHZ states can be denoted as

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle) \quad |\psi_4\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle)$$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle) \quad |\psi_6\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$$

$$|\psi_7\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) \quad |\psi_8\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle)$$

It is assumed in the proposed protocol that the quantum channels is ideal (i.e., non-lossy and noiseless) and an authenticated classical channel is shared among all the legitimate participants. An adversary can eavesdrop a message communicated through this channel. Based on the scenario described above, the process of the proposed scheme will be described in steps as follows.

Step 1: Server prepares 4*n* GHZ states, each of which is $|\psi_i\rangle$, where i = 1 to 8. He extracts all the first particles in the GHZ states, and forms a sequence S_1 in order. The second particles form a sequence S_2 in order, and the third particles form a sequence S_3 in order.

Server keeps the sequence S_1, sends S_2 to Alice and S_3 to Bob. S_1, S_2 and S_3 contain N = 4*n* qubits.

Step 2: Upon receiving the particles from server, Alice and Bob can perform one of the following operations (Measure or Reflect).

Measure: Measures the particle in the classical basis $\{|0\rangle, |1\rangle\}$, and saves the measurement results.

Reflect: Reflects the qubits back without disturbance.

Step 3: eavesdropping checking

Server restores the returning qubits. Alice and Bob announce their operations on all qubits. In the same position of S_2 and S_3, only one of them perform a measurement, they need to announce the measurement result. If both of them perform a measurement, they must keep the measurement results confidential.

Based on the announcement of Alice and Bob, server begins to detect eavesdropping. If both Alice and Bob reflect the qubits, server will perform a GHZ measurement on the reflected particles with his own one (i.e., the original entangled GHZ state). In other word, if one of them measures the qubit, server will measure his own particle and the reflected particle in the classical basis. Finally, server checks his measurement results, if the error rate exceeds a pre-defined threshold, they proceed to the next step, otherwise terminate the protocol.

Step 4: After ensuring that there is no eavesdropping, Alice and Bob discard the decoy photons. For the remaining qubits, Alice and Bob perform a measurement in the same positon of S_2 and S_3. They can use them measurement results r_A and r_B (each of n bit length) to compare their private secret.

To ensure that Alice and Bob secretly compare their information without exposing their actual contents, Alice and Bob employ the one-way hash function [Damgard (1990)] (i.e., $h() : \{0,1\}^m \to \{0,1\}^n$, where m denotes the length of the inputted data, and n denotes the length of the hash code) on their binary representation of secret message M_A and M_B to obtain two hash codes $h(M_A)$ and $h(M_B)$, each of n bit length. Finally, they compute the $R_A = r_A \oplus h(M_A)$ and $R_B = r_B \oplus h(M_B)$. Finally, Alice and Bob publish R_A and R_B to server, where R_A and R_B contain n bit.

Step 5: Server generates a classical bit string C of n-bits corresponding to the choice of the initial GHZ states, for the ith GHZ state being $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\psi_4\rangle (|\psi_5\rangle, |\psi_6\rangle, |\psi_7\rangle, |\psi_8\rangle)$ he generates ith bit value in C as 0 (1). Server computes R, which is now exclusive-OR result of R_A, R_B and C as $R = C \oplus R_A \oplus R_B$. The bit value 0 (1) of R^i corresponds to the same (different) values of $h(M_A)^i$ and $h(M_B)^i$. Thus, if server found out that $R^i = 0$ for all, he will public 0, otherwise public 1.

The process of the proposed protocol is shown in Fig. 1, and Tab. 1 demonstrates the detailed process, where the parameters "M" and "R" denote measurement and reflection, "GHZ" denotes GHZ measurement.

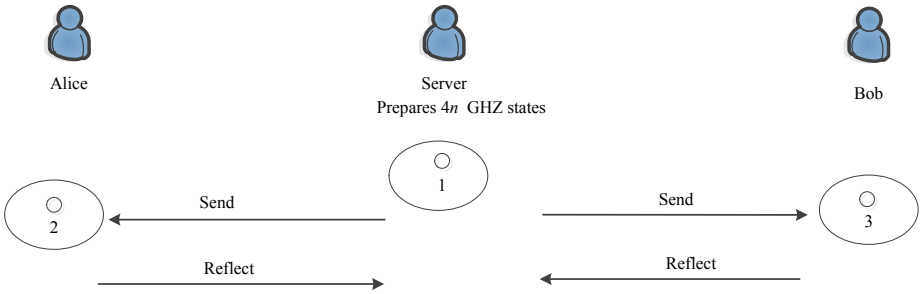

Figure 1: The process of the proposed protocol

Table 1: The detailed process of the proposed protocol

	Alice's operation	Bob's operator	Server's operator	$r_A^i \oplus r_B^i$	C
$\|\psi_1\rangle,\|\psi_2\rangle,\|\psi_3\rangle,\|\psi_4\rangle$	M	M		0	0
	R	R	GHZ		
	M(announce measurement result)	R	M		
	R	M(announce measurement result)	M		
$\|\psi_5\rangle,\|\psi_6\rangle,\|\psi_7\rangle,\|\psi_8\rangle$	M	M		1	1
	R	R	GHZ		
	M(announce measurement result)	R	M		
	R	M(announce measurement result)	M		

Here it is important to note that Alice and Bob cannot announce the measurement results when both of them perform measurement operation in the same position.

3 Security and efficiency analysis

In this section, we first analyze the security of the eavesdropping detection to show that the proposed protocol can avoid the outside attacks. Therefore, the efficiency of the protocol is analyzed.

3.1 The detection probability of eavesdropping information

Now, let us analyze the efficiency of the eavesdropping detection in the proposed protocol. If there is an outside eavesdropper (Eve) who attempts to derive the session key. She can only use the chance of the transmission of S_2 and S_3 to steal qubits, Eve performs the unitary attack operation $\hat{E}$ on the composed system firstly, and then Alice, Bob and server perform the corresponding operation on these qubits. All the transmitted particles are sent together before eavesdropping is detected. Because Eve does not know which particles are used to detect eavesdropping, she can only perform the same attack operation on all the particles. As for Eve, the state of qubits is distinguishable from the complete mixture, so all qubits are considered in either of the states |0> or |1> with an equal probability p=0.5.

Generally speaking, suppose there is a group of decoy photons in GHZ states $|\psi_1\rangle$. And we assume that after the attack operation $\hat{E}$ is performed, the state |0> and |1> become

$$|\varphi_0'\rangle = \hat{E}\otimes|0x>=\alpha|0x_0>+\beta|1x_1> \tag{1}$$

$$|\varphi_1'\rangle = \hat{E}\otimes|1x>=m|0y_0>+n|1y_1> \tag{2}$$

where $|x_i>$ and $|y_i>$ are the pure ancillary states determined by $\hat{E}$ uniquely, and $|\alpha|^2+|\beta|^2=1$, $|m|^2+|n|^2=1$. (3)

Then let us compute the detection probability. After attacked by Eve, the state of the composed system becomes

$$|\psi\rangle_{Eve} = \frac{1}{\sqrt{2}}[|0>\otimes(\hat{E}\otimes\hat{E}|0x0x>)+|1>\otimes(\hat{E}\otimes\hat{E}|1x1x>)]$$

$$=\frac{1}{\sqrt{2}}[|0>\otimes(\alpha|0x_0>+\beta|1x_1>)\otimes(\alpha|0x_0>+\beta|1x_1>)$$

$$+|1>\otimes(m|0y_0>+n|1y_1>)\otimes(m|0y_0>+n|1y_1>)]$$

$$=\frac{1}{\sqrt{2}}(\alpha^2|00x_00x_0>+\alpha\beta|00x_01x_1>+\alpha\beta|01x_10x_0>+\beta^2|01x_11x_1>$$

$$+m^2|10y_00y_0>+mn|10y_01y_1>+mn|11y_10y_0>+n^2|11y_11y_1>) \tag{4}$$

Obviously, when Alice, Bob and server perform measurement on the decoy photons, the probability without an eavesdropper is

$$p|\psi\rangle=\frac{1}{2}(|\alpha^2|^2+|n^2|^2) \tag{5}$$

So the lower bound of the detection probability is

$$d=1-p|\psi\rangle=1-\frac{1}{2}(|\alpha^2|^2+|n^2|^2) \tag{6}$$

Suppose $|\alpha|^2=a$ and $|n|^2=b$, where a and b are positive real numbers, and $a = b = 1$. Then

$$d=1-p|\psi\rangle=1-\frac{1}{2}(|\alpha^2|^2+|n^2|^2)=1-\frac{1}{2}(a^2+b^2) \tag{7}$$

In the case of $p_0 = p_1$=0.5, the maximal amount of information is equal to the Shannon entropy of a binary channel [Gisin, Ribordy and Tittel et al. (2002)],

$$I=-a\log_2 a-(1-a)\log_2(1-a)=H(a) \tag{8}$$

After some simple mathematical calculations, we can get $d=1-a^2$ (9)

The maximum I is $I(d)=H(\sqrt{1-d})$ (10)

The above results show that if Eve wants to obtain the full information (I=1), the probabilities of the eavesdropping detection is d=0.75. When Eve gains the information, the detection probability is shown in Fig. 2.

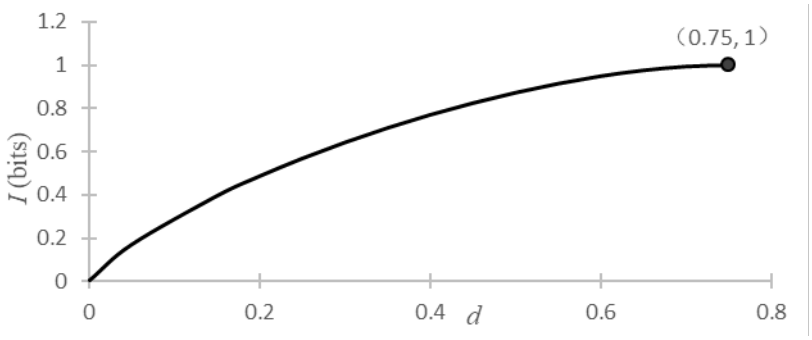

Figure 2: Detection probability of eavesdropping information

3.2 Intercept-measure-resend attack

In the proposed protocol, Alice and Bob randomly perform measurement and reflected operation. Without knowing the position of these operation, Eve will be detected inevitably if Eve performs a projective measurement on them.

Supposed server prepares Bell states $|\psi_1\rangle$, and send the first and second photon to Alice and Bob, respectively. If Eve intercepts this qubit and performs a measurement on it in the basis $\{|0\rangle,|1\rangle\}$, $|\psi_1\rangle$ will collapsed into $|000\rangle$ or $|111\rangle$. Eve retransmits this result state to Alice and Bob. Accordingly the protocol, Alice and Bob choose randomly either Measurement or Reflected. If one of Alice and Bob decides to Measurement, Eve induces no error. In view of $|000\rangle = \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_2\rangle)(|11>= \frac{1}{\sqrt{2}}(|\psi_1\rangle - |\psi_2\rangle))$, if both Alice and Bob decide to Reflected, server performs GHZ basis measurement and obtains $|\psi_1\rangle$ or $|\psi_2\rangle$ each with probability of 1/2. Thus, the error rate introduced by Eve is 50%. Therefore, the probability for Eve to pass the security checking is $\frac{7}{8} = \frac{3}{4}\times 1 + \frac{1}{4}\times\frac{1}{2}$. And Eve only can obtain the valuable information when both Alice and Bob perform measurement operation, the probability is 1/4. Thus, the probability for Eve to pass the security checking and obtain the valuable information is $\frac{7}{32} = \frac{1}{4}\times\frac{7}{8}$, for Eve's intercept-measure-resend attack, the probability of being detected is $d = 1-(\frac{7}{32})^n$. This probability is approximate to 1, if n is large enough.

3.3 Flip attack

When the sequence S_2 and S_3 are transmitted from server to Alice and Bob, Eve can cause Alice and Bob to obtain the wrong bit value of the message by flipping some particles in

the sequence. Suppose server prepares GHZ states $|\psi_1\rangle$, and sends the first and second photon to Alice and Bob respectively. Eve intercepts and flips the qubit. Accordingly the protocol, Alice and Bob choose randomly either measurement or reflected operation. If both Alice and Bob decide to measure, Eve induces no error. If one of them decides to reflect, server can find the flip attack with the help of the announcement of Alice and Bob. Thus, the error rate introduced by Eve is 100%.

Therefore, the probability for Eve to pass the security checking is $\frac{1}{4}$. Thus, for *n* encoded message qubits, the probability of being detected is $d = 1-(\frac{1}{4})^n$. With the increase of *n*, the probability of Eve being detected is also increasing.

3.4 Man-in-the-middle attack

If Eve captures the qubit from server to Alice and Bob. She prepares another Bell state $|\phi_e\rangle$, sends them to Alice and Bob. Then Eve also catches that qubits back to server. Because we just send back the reflected qubits, and the order of the reflected particle sequence is completely secret to Eve. Even if Eve catches these qubits, she also cannot obtain any secret information.

3.5 Trojan horse attack

Since the proposed protocol is a two-way communication protocol, Eve may implement a Trojan horse attack to get the secret message. In order to resist the attack, a photon number splitter (PNS) and a wavelength filter could be added before Alice and Bob's devices [Cai (2006); Li, Deng and Zhou (2006); Deng, Li, Zhou et al. (2005)].

3.6 Server's attack

Our proposed protocol is considered in semi-honest model. Server may try to learn additional information from the protocol execution. In the protocol, server knows the state of GHZ states and Alice and Bob's operations on each qubit. From these information, server can only correctly obtain Alice and Bob's measurement results with probability $\frac{1}{2}$. If the length of the secret message is *n*, server will have a probability of $\frac{1}{2^n}$ to get secret message. When the length of the secret message is large enough, the probability that server correctly obtains Alice and Bob's secret message is negligible. Thus, the protocol is unconditionally secure against the server.

3.7 Efficiency analysis

Performance of a quantum protocol can be characterized using qubit efficiency [Cabello (2000)], $\xi = \frac{c}{q+b}$, where *c* is the number of secret bits received by the legal receiver, *q*

denotes the number of transmitted qubits, and b is the number of classical bits for decoding of the message (classical communications used for checking of eavesdropping are not counted). In our protocol, in order to make the Alice and Bob obtain n bits message, server should prepare $4n$ GHZ states photons and send $4n$ photons to Alice and Bob, respectively. Then Alice and Bob reflect $2n$ photons back to server. In addition, $2n$ classical bits are needed for Alice and Bob to inform server their operations on photons, n classical bits are needed for Alice and Bob to public R_A and R_B . Therefore, total $q=4n+4n+2n+2n = 12n$, $b=2n+n+n+n= 5n$, $c=n$. Thus the efficiency of the proposed protocol would be $\xi = \frac{n}{17n}$, which is 5.88%.

4 Conclusion

In the paper, a two-party semi-quantum private comparison scheme is proposed based on GHZ states. In the protocol, Alice and Bob are classical, they are restricted to either measuring a quantum state or reflecting it in the classical basis $\{|0\rangle, |1\rangle\}$. Compared with the previous SQPC protocols, the advantage of our protocol lies in that the classical participants only send the reflected qubits back to server, it avoids measurement results leakage, and it also does not need the pre-shared key and quantum entanglement swapping. According to the security analysis, the protocol can resist the outside attacks and semi-honest server attack. It can be used to solve a real application problems, because end users are expected to be classical in reality. Therefore, our proposed protocol is more practical and feasible with current technique.

Acknowledgement: The work was supported by the National Natural Science Foundation of China (Grant No. 61572086), Major Project of Education Department in Sichuan (Grant No. 18ZA0109), and Web Culture Project Sponsored by the Humanities and Social Science Research Base of the Sichuan Provincial Education Department (Grant No. WLWH18-22).

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175-179.

Bennett, C. H. (1992): Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, vol. 68, no, 21, pp. 3121-3124.

Boyer, M.; Kenigsberg, D.; Mor, T. (2007): Quantum key distribution with classical Bob. *Physical Review Letters*, vol. 99, no. 14, 140501.

Cabello, A. (2000): Quantum key distribution in the Holevo limit. *Physical Review Letters*, vol. 85, 5635.

Cai, Q. Y. (2006): Eavesdropping on the two-way quantum communication protocols with invisible photons. *Physics Letters A*, vol. 351, no. 1-2, pp. 23-25.

Chang, Y. J.; Tsai, C. W.; Hwang, T. (2013): Multi-user private comparison protocol using GHZ class states. *Quantum Information Process*, vol. 12, no. 2, pp. 1077-1088.

Chen, X. B.; Su, Y.; Niu, X. X.; Yang, Y. X. (2014): Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. *Quantum Information Process*, vol. 13, no. 1, pp. 101-112.

Chen, X. B.; Xu, G.; Niu, X. X.; Wen, Q. Y.; Yang, Y. X. (2010): An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. *Optics Communications*, vol. 283, no. 7, pp. 1561-1565.

Chou, W. H.; Hwang, T.; Gu, J. (2016): Semi-quantum private comparison protocol under an almost-dishonest third party. http://arxiv.org/pdf/quant-ph/160707961.pdf.

Damgard, I. B. (1990): A design principle for hash functions. *Advances in Cryptology*, vol. 89, no. 435, pp. 416-427.

Deng, F. G.; Gui, L. L.; Liu, X. S. (2003): Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physics Letters A*, vol. 68, no. 4, pp. 113-114.

Deng, F. G.; Gui, L. L. (2004): Secure direct communication with a quantum one-time pad. *Physics*, vol. 69, no. 5, pp.521-524.

Deng, F. G.; Li, X. H.; Zhou, H. Y.; Zhang, Z. J. (2005): Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Physics Letters A*, vol. 72, no. 4, 044302.

Ekert, A. K. (1991): Quantum cryptography based on Bell's theorem. *Physical Review Letters*, vol. 67, pp. 661-663.

Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. (2002): Quantum cryptography. *Reviews of Modern Phys*ics, vol. 74, no. 1, pp. 145-795.

Guo, G. (2002): Quantum secret sharing. Quantum Optics in Computing and Communications. *International Society for Optics and Photonics*, pp. 101-105.

Karlsson, A.; Koashi, M.; Imoto, N. (1999): Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, vol. 59, no. 1, pp. 162-168.

Lang, Y. F. (2018): Semi-quantum private comparison using single photons. *International Journal of Theoretical Physics*, vol. 57, pp. 3048-3055.

Li, X. H.; Deng, F. G.; Zhou, H. Y. (2006): Improving the security of secure direct communication based on the secret transmitting order of particles. *Physical Review A*, vol. 74, no. 5, 054302.

Lin, J.; Yang, C. W.; Hwang, T. (2014): Quantum private comparison of equality protocol without a third party. *Quantum Information Process*, vol. 13, no. 2, pp. 239-247.

Liu, B.; Gao, F.; Jia, H. Y.; Huang, W.; Zhang, W. W. et al. (2013): Efficient quantum private comparison employing single photons and collective detection. *Quantum Information Process*, vol. 12, no. 2, pp. 887-897.

Liu, W.; Wang, Y. B. (2012): Quantum private comparison based on GHZ entangled states. *International Journal of Theoretical Physics*, vol. 51, no. 11, pp. 3596-3604.

Liu, W.; Wang, Y. B.; Cui, W. (2012): Quantum private comparison protocol based on Bell entangled states. *Communications in Theoretical Physics*, vol. 57, no. 4, pp. 583-588.

Lo, H. K. (2007): Insecurity of quantum secure computations. *Physical Review A*, vol. 56, no. 2, pp. 1154-1162.

Long, G. L.; Liu, X. S. (2002): Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, vol. 65, no. 3, pp. 032302.

Man, Z. X.; Xia, Y. J. (2004): Improvement of security of three-party quantum secure direct communication based on GHZ states. *Chinese Physics Lettetters*, vol. 24, no. 1, pp. 15-18.

Thapliyala, K.; Sharmab, R. D.; Pathak, A. (2016): Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. http://arxiv.org/pdf/quant-ph/160800101.pdf.

Tseng, H. Y.; Lin, J.; Hwang, T. (2012): New quantum private comparison protocol using EPR pairs. *Quantum Information Process*, vol. 11, no. 2, pp. 373-384.

Wang, C.; Xu, G.; Yang, Y. X. (2013): Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. *International Journal of Quantum Information*, vol. 11, no. 4, pp. 1350039.

Yang, Y. G.; Gao, W. F.; Wen, Q. Y. (2009): Secure quantum private comparison. *Physica Scripta*, vol. 80, no. 6, pp. 065002.

Yang, Y. G.; Wen, Q. Y. (2009): An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 5, pp. 055305.

Yang, Y. G.; Xia, J.; Jia, X.; Shi, L; Zhang, H. (2012): New quantum private comparison protocol without entanglement. *International Journal of Quantum Information*, vol. 10, no. 6, pp. 1250065.

Ye, T. Y.; Ye, C. Q. (2018): Measure-resend semi-quantum private comparison without entanglement. *International Journal of Theoretical Physics*, vol. 57, pp. 3819-3834.

Zhong, J. F.; Liu, Z. H.; Xu, J. (2018): Analysis and improvement of an efficient controlled quantum secure direct communication and authentication protocol. *Computers, Materials & Continua*, vol. 57, no. 3, pp. 621-633.