Int J Theor Phys (2014) 53:3191–3200
DOI 10.1007/s10773-014-2116-7

Quantum Private Comparison Based on Phase Encoding of Single Photons

Yan-Bing Li · Ying-Jie Ma · Sheng-Wei Xu · Wei Huang · Yan-shuo Zhang

Received: 23 January 2014 / Accepted: 21 March 2014 / Published online: 23 April 2014

Abstract In this paper, we propose a scheme for quantum private comparison using phase encoding. The analysis indicates that the scheme is secure, and can prevent some familiar attacks. With the use of error-correcting code (ECC), it achieves a limited fault tolerant quantum private comparison. The scheme is easy to be realized in current experiments.

Keywords Quantum private comparison · Phase encoding · Single photon · Error-correcting code

1 Introduction

Quantum cryptography allows higher security than classical cryptography as it is based on the laws of physics instead of some difficult mathematical problems. There are some quantum cryptography protocols been proposed, such as quantum key distribution (QKD) [1–6], quantum secret sharing (QSS) [7–12], quantum secure direct communication (QSDC) [13–17], quantum teleportation (QT) [18–21], and so on. Secure multiparty computation (SMPC) is an important and fundamental cryptographic protocol [22–29]. Unfortunately, it was shown by Mayers [24] and Lo-Chau [25] that deterministic two-party-setting computation was impossible, even with quantum means.

Y.-B. Li (✉)
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
e-mail: liyanbing1981@gmail.com

Y.-B. Li · Y.-J. Ma · S.-W. Xu · W. Huang · Y.-s. Zhang
Beijing Electronic Science and Technology Institute, Beijing, 100070, China

Y.-B. Li
Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208, USA

Quantum private comparison (QPC) is a interesting topic in quantum secure multiparty computation. It allows two distrustful parties, Alice and Bob, to determine whether their secret inputs are equal or not without disclosing their own secret information. In 2009, QPC was proposed by Yang et al. [30, 31] first. After these, some QPC schemes based on different states are proposed [32–41]. Since secure two-party-setting computation is impossible, a third party (TP) is needed in QPC to help Alice and Bob compare their private information. In some schemes, TP is required as at least a semi-honest participant. Recently, it was found that TP is not needed to be a semi-honest participant [40]. Hence, the QPC schemes presented previously have the following principles.

1. The QPC task is implemented with the help of a TP. TP will not be corrupted by others. He cannot learn any information about the players' respective private inputs by means of various active and passive attacks.
2. No matter whether TP will know the positions of different bit value in the compared information or not, he/she will not be able to know the actual bit value of the information.
3. All outsiders and the two players should only know the result of the comparison (i.e., identical or different), but not the positions of the different information.

In this paper, we will propose a new QPC scheme based on phase encoding of single photons, and prove that it is secure in the above principles. This scheme is easy to be realized in current experiments as only some simple devices are used. It also can prevent some familiar attacks in practical setting.

The rest of this paper is constructed as follows. Section 2 proposes the QPC scheme based on phase encoding of single photons. In Section 3, we analyze the protocol's correctness, security and the capability of fault-tolerate. Finally, a short conclusion is given in Section 4.

2 QPC Based on Phase Encoding of Single Photons

In this section, we give a QPC scheme based on phase encoding of single photons. Here are two participants, Alice and Bob, and a third party, Charlie who helps Alice and Bob to compare, but wants to know their private inputs by means of various active and passive attacks. Following the conclusions that a SMPC protocol should be insecure when less than a half of participants are honest [26], we suppose that TP should not be colluded by other dishonest parties.

Here, Alice and Bob have two private information M^A and M^B, respectively. The binary representations of M^A and M^B in F_{2^N} are $\left(m_1^A, m_2^A, \ldots, m_N^A\right)$, $\left(m_1^B, m_2^B, \ldots, m_N^B\right)$, where $m_i^A, m_i^B \in \{0, 1\}$; $M^A = \sum_{i=1}^{N} m_i^A \cdot 2^i$, $M^B = \sum_{i=1}^{N} m_i^B \cdot 2^i$.

In this scheme, the single photon should be used with the technique block transmission, namely using an ordered particle sequence, which first proposed in Ref. [13]. They divide the N bits private information into some blocks including t bits, and fill the last block by some bits 0, then compare them one by one. When a pair of blocks are not identify, they know $M^A \neq M^B$ and stop the protocol. They accept $M^A = M^B$ only when all of these blocks are identify. The specific steps of the scheme are described as follows. And the schematic of the scheme is shown in Fig. 1.

1. Charlie prepares photons sequence $S = (s_1, s_1, \cdots, s_{n'})$ which is composed by n' single photons and passes each of them through 50 : 50 beam splitter

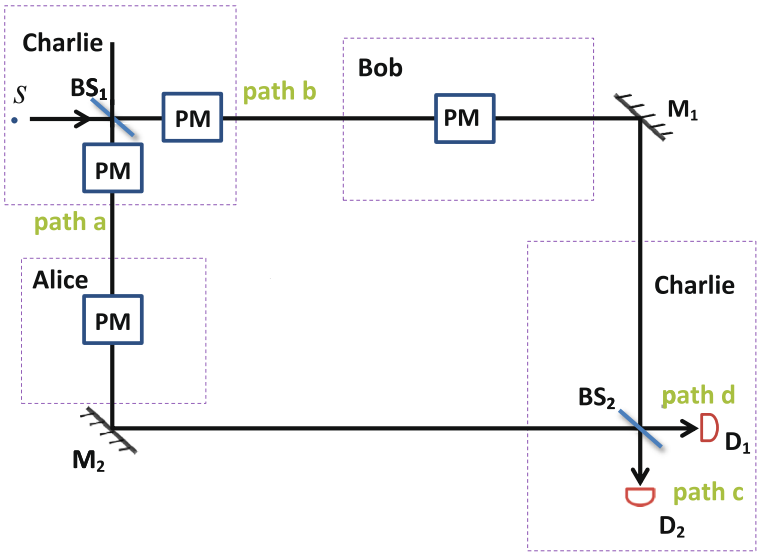

Fig. 1 The schematic of QPC based on phase encoding of single photon (*color online*)

BS_1. The jth photon is split to two pulse waves s_j^a and s_j^b. Then the state is

$$|\phi^0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + i|1\rangle_a|0\rangle_b), \tag{1}$$

where $|0\rangle$ denotes the vacuum state, the subscripts a and b represent the paths towards Alice's and Bob's sites, respectively.

2. To the jth photon, Charlie randomly choose a phase θ_j^C from the two basis sets of $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. Phase values 0 and $\pi/2$ represent $k_j^{*C} = 0$ and the other two represent $k_j^{*C} = 1$. Now Charlie has bits sequences $K^{*C} = \left(k_1^{*C}, k_1^{*C}, \cdots, k_{n'}^{*C}\right)$. He uses modulator introduce relative phase shift θ_j^C to the pulse wave s_j^a or s_j^b. The system state develops to

$$|\phi^1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_a|1\rangle_b + ie^{i\theta_j^C}|1\rangle_a|0\rangle_b\right), \quad or \tag{2a}$$

$$|\phi^1\rangle = \frac{1}{\sqrt{2}}\left(e^{i\theta_j^C}|0\rangle_a|1\rangle_b + i|1\rangle_a|0\rangle_b\right). \tag{2b}$$

Then he sends the two pulse waves sequences $S^A = \left(s_1^A, s_1^A, \cdots, s_{n'}^A\right)$, $S^B = \left(s_1^B, s_1^B, \cdots, s_{n'}^B\right)$ to Alice and Bob, respectively.

3. Alice and Bob insert a filter in front of her devices to filter out the photon signal with an illegitimate wavelength. They select l orders for detecting multi-photons as follows. They split each of these waves with a beam splitter followed by measuring the two signals with detectors. In an ideal scenario, only one detector would click for a same order. If the multi-photon rate is unreasonably high, they abort the protocol.
4. To the ith pulse wave, Alice and Bob randomly choose θ_j^A and θ_j^B from the two basis sets of $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. Phase values 0 and $\pi/2$ represent k_j^{*A} or $k_j^{*B} = 1$ and the other two represent k_j^{*A} or $k_j^{*B} = 0$. They use phase modulators

to introduce relative phase shifts θ_j^A and θ_j^B to the pulse waves s_j^a and s_j^b, respectively. Now Alice and Bob have two bits sequences $K^{*A} = \left(k_1^{*A}, k_1^{*A}, \cdots, k_{n'}^{*A}\right)$ and $K^{*B} = \left(k_1^{*B}, k_1^{*B}, \cdots, k_{n'}^{*B}\right)$, respectively. The system state develops to

$$\begin{aligned} |\phi^2\rangle &= \frac{1}{\sqrt{2}}\left(e^{i\theta_j^B}|0\rangle_a|1\rangle_b + ie^{i(\theta_j^A+\theta_j^C)}|1\rangle_a|0\rangle_b\right) \\ &= \frac{e^{i\left(\theta_j^C+\theta_j^A\right)}}{\sqrt{2}}\left(e^{i(\theta_j^B-\theta_j^A-\theta_j^C)}|0\rangle_a|1\rangle_b + i|1\rangle_a|0\rangle_b\right), \quad or \end{aligned} \tag{3a}$$

$$\begin{aligned} |\phi^2\rangle &= \frac{1}{\sqrt{2}}\left(e^{i\left(\theta_j^B+\theta_j^C\right)}|0\rangle_a|1\rangle_b + i\left(e^{i\theta_j^A}|1\rangle_a|0\rangle_b\right)\right. \\ &= \frac{e^{i\theta_j^A}}{\sqrt{2}}\left(e^{i\left(\theta_j^B+\theta_j^C-\theta_j^A\right)}|0\rangle_a|1\rangle_b + i|1\rangle_a|0\rangle_b\right), \end{aligned} \tag{3b}$$

where the overall factor $e^{i\left(\theta_j^C+\theta_j^A\right)}$ and $e^{i\theta_j^A}$ could be omit. We denote the pulse waves after Alice and Bob's phase shifts as s_j^{*A} and s_j^{*B}.

Then they send the two pulse waves sequences $S^{*A} = \left(s_1^{*A}, s_1^{*A}, \cdots, s_{n'}^{*A}\right)$, $S^{*B} = \left(s_1^{*B}, s_1^{*B}, \cdots, s_{n'}^{*B}\right)$ back to Charlie.

5. The two pulse waves are combined at the second beam splitters BS_2. The system state develops to

$$|\phi^3\rangle = \frac{1}{\sqrt{2}}\left(\left(e^{i\left(\theta_j^B-\theta_j^A-\theta_j^C\right)}-1\right)|0\rangle_c|1\rangle_d + i\left(e^{i\left(\theta_j^B-\theta_j^A-\theta_j^C\right)}+1\right)|1\rangle_c|0\rangle_d\right) \; or \tag{4a}$$

$$|\phi^3\rangle = \frac{1}{\sqrt{2}}\left(\left(e^{i\left(\theta_j^B+\theta_j^C-\theta_j^A\right)}-1\right)|0\rangle_C|1\rangle_d + i\left(e^{i\left(\theta_j^B+\theta_j^C-\theta_j^A\right)}+1\right)|1\rangle_C|0\rangle_d\right), \tag{4b}$$

which means the detector D_1 will click with probability $\frac{1}{2}\left(1-\cos\left(\theta_j^B-\theta_j^A-\theta_j^C\right)\right)$ or $\frac{1}{2}\left(1-\cos\left(\theta_j^C+\theta_j^B-\theta_j^A\right)\right)$, the detector D_2 will click with probability $\frac{1}{2}\left(1+\cos\left(\theta_j^B-\theta_j^A-\theta_j^C\right)\right)$ or $\frac{1}{2}\left(1+\cos\left(\theta_j^C+\theta_j^B-\theta_j^A\right)\right)$.

6. Alice, Bob and Charlie take turns to check whether the other two participants are honest or not. First, Alice selects a detecting photon and announces its order, let Bob announce his bit k_j^{*B}, Charlie announce his bit k_j^{*C} and which detector clicked. Second, Bob selects a detecting photon and announces its order, let Alice announce his bit k_j^{*A}, Charlie announce his bit k_j^{*C} and which detector clicked. Third, Charlie selects a detecting photon and announces its order, let Alice and Bob announce their bit k_j^{*A} and k_j^{*B}. Then they come into another round of detecting process, till l' photons has been detected. They check dishonest participants with the following two restrains: In the two cases of (i) detector D_1 clicked and $k_i^{*C} = 1$ and (ii) detector D_2 clicked and $k_j^{*C} = 0$, it should be $k_j^{*A} = k_j^B$ with certainly; In the other two cases of (iii) detector D_1 clicked and $k_i^{*C} = 0$ and (iv) detector D_2 clicked and $k_i^{*C} = 1$, it should be $k_j^{*A} = k_j^{*B}$ with probability $1/3$ and $k_j^{*A} \neq k_j^{*B}$ with probability $2/3$. If all the checks passed, they go to the next step.

7. To the remaining $m - l - l'$ orders, Charlie announces which orders are in the cases (iii) and (iv). In a half of these orders, Alice announces her bit k_j^{*A} following by Bob announces his bit k_j^{*B}. In the other half of these orders, Bob announces his bit k_j^{*B} following by Alice announces her bit k_j^{*A}. Same to the check process in step 5, it should be $k_j^{*A} = k_j^{*B}$ with probability 1/3 and $k_j^{*A} \neq k_j^{*B}$ with probability 2/3. If all the checks passed, they go to the next step.
8. We suppose the amount of the remaining orders is n. By eliminating the announced bits, Alice, Bob and Charlie still keep secret bit sequences $K^A = \left(k_1^A, k_2^A, \ldots, k_n^A\right)$, $K^B = \left(k_1^B, k_2^B, \ldots, k_n^B\right)$ and $K^C = \left(k_1^C, k_2^C, \ldots, k_n^C\right)$ orderly in bit sequences K^{*A}, K^{*B} and K^{*C}, respectively.
9. Alice, Bob and Charlie select a $[n, t]$ error-correcting code [42] which could use n bits codeword to encode t bits word by using generator matrix $G(x^t)$ and could correct t' codeword error bits using the error-correcting function $D(y^n)$.
10. Alice chooses a bits word $R^A = \left(r_1^A, r_2^A, \ldots, r_t^A\right)$ and calculates the corresponding bits codeword $W^A = \left(w_1^A, w_2^A, \ldots, w_n^A\right)$, i.e.,

$$W^A = R^A \cdot G, \quad and \quad R^A = W^A \cdot D. \tag{5}$$

Then she obtains bit string $P^A = \left(p_1^A, p_2^A, \ldots, p_t^A\right)$ by calculating $p_j^A = r_j^A \oplus m_j^A$, bit string $Q^A = \left(q_1^A, q_2^A, \ldots, q_n^A\right)$ by calculating $q_j^A = w_j^A \oplus k_j^A$. After these, she announces P^A and Q^A to Charlie.

11. Bob chooses a t bits word $R^B = \left(r_1^B, r_2^B, \ldots, r_t^B\right)$ and calculates the corresponding bits codeword $W^B = \left(w_1^B, w_2^B, \ldots, w_n^B\right)$, i.e.,

$$W^B = R^B \cdot G, \text{ and } R^B = W^B \cdot D. \tag{6}$$

Then he obtains bit string $P^B = \left(p_1^B, p_2^B, \ldots, p_t^B\right)$ by calculating $p_j^B = r_j^B \oplus m_j^B$, bit string $Q^B = \left(q_1^B, q_2^B, \ldots, q_n^B\right)$ by calculating $q_j^B = w_j^B \oplus k_j^B$. After these, he announces P^B and Q^B to Charlie.

12. Charlie obtains bit string $W^C = \left(w_1^C, w_2^C, \ldots, w_n^C\right)$ by calculating $w_j^C = q_j^A \oplus q_j^B \oplus k_j^C$. Then he uses the check matrix H of the $[n, t]$ error-correcting code to check whether the number of error bits exceeds the threshold t'. If it does, Charlie aborts the protocol and restarts from Step 1. Otherwise, he obtains t bits string R^C by decoding W^C with error-correcting function $D(W^C) = W^C \cdot D$. He obtains $R'^C = \left(r'^C_1, r'^C_2, \ldots, r'^C_t\right)$ by calculating $r'^C_j = p_j^A \oplus p_j^B$. If *one* or more bits are different between R^C and R'^C, Charlie announces $X \neq Y$. Otherwise, he announces $X = Y$.

3 Analysis

3.1 Correctness

For simpleness, we first prove that the protocol is correct in ideal scenario. Then we prove that the effect of limited noise will be removed by ECC in practical scenario.

3.1.1 Correctness in Ideal Scenario

Since there are $l + l' + \frac{3(m-l-l')}{4} = \frac{3m+l+l'}{4}$ single photons used as detecting states which are not used in final comparison, we only consider the other n decoding single photons. In the protocol, up to step 8, it should be that

$$K^C = K^A \tilde{\oplus} K^B, \tag{7}$$

where $\tilde{\oplus}$ denotes that one bit string bitwise XOR another bit string.[1] Obliviously, Charlie, Alice and Bob share some randomly bits from which one can know the other two parties' bitwise XOR value.

At step 12, it should be that

$$\begin{aligned} W^C &= Q^A \tilde{\oplus} Q^B \tilde{\oplus} K^C \\ &= (W^A \tilde{\oplus} K^A) \tilde{\oplus} (W^B \oplus K^B) \tilde{\oplus} K^C \\ &= W^A \tilde{\oplus} W^B. \end{aligned} \tag{8}$$

Based on (5) and (6), we know that

$$\begin{aligned} R^A \tilde{\oplus} R^B &= (W^A \tilde{\oplus} W^B) \cdot D \\ &= W^C \cdot D. \end{aligned} \tag{9}$$

Since $R^C = W^C \cdot G$, it should be that $R^C = R^A \tilde{\oplus} R^B$.

After these, we consider the other bits string R'^C which Charlie obtains at step 12 too. We know that

$$\begin{aligned} R'^C &= P^A \tilde{\oplus} P^B \\ &= (R^A \tilde{\oplus} M^A) \tilde{\oplus} (R^B \tilde{\oplus} M^B). \end{aligned} \tag{10}$$

When $M^A = M^B$, it should be that

$$R'^C = R^A \tilde{\oplus} R^B. \tag{11}$$

Otherwise, when $M^A \neq M^B$, it should be that

$$R'^C \neq R^A \tilde{\oplus} R^B. \tag{12}$$

In other words, Charlie knows whether $M^A = M^B$ or not by comparing R^C and R'^C.

Therefore, the presented protocol is correct in an ideal scenario. We analyze it in practical scenario as follows.

3.1.2 Correctness in Practical Scenario

In practical scenario, noise might appear in all of quantum preparation setups, quantum channel and measurement equipments. Here we only consider their effect on the encoding states (i.e., the noise appear in the courses of obtaining K^C) as the detecting photons will be discarded and not effect the correctness of comparison.

[1] In an ideal scenario, Charlie can obtain the comparison result with K^C if Alice and Bob use their private information M^A and M^B to replace K^A and K^B respectively. However, in the presented protocol, some bits in K^{*A} and K^{*B} (which K^A and K^B come form) are used randomly to detect cheats which happen in non-ideal scenario. So Alice and Bob do not know which bits in K^{*A} and K^{*B} will become K^A and K^B ultimately. Consequently, they cannot use their private information to replace K^A and K^B.

We denote the noise appear in the courses of obtaining K^C as $O = (o_1, o_2, \ldots, o_n)$, where $o_i = 0$ or 1 representing error is existent or not in k_i. So Charlie obtains bit string K'^C as

$$\begin{aligned} K'^C &= K^C \tilde{\oplus} O \\ &= (R^A \tilde{\oplus} R^B) \cdot G. \end{aligned} \tag{13}$$

Then (8) is replaced with

$$W'^C = W^A \tilde{\oplus} W^B \tilde{\oplus} O. \tag{14}$$

When the error rate does not exceed a rational threshold, i.e., the number of 1 in bit string O does not exceed t', we have

$$\begin{aligned} R^A \tilde{\oplus} R^B &= (W^A \tilde{\oplus} W^B \tilde{\oplus} O) \cdot D \\ &= W^C \cdot D. \end{aligned} \tag{15}$$

replacing (9). Subsequently, noise will not effect (10)–(12). Namely, the present protocol is correct in practical scenario when noise has not exceed the used ECC's ability.

3.2 Security

In QPC, every participant has more resources than outsider. With these resources, a dishonest participant has more strategies to cheat besides the strategies which outsider can perform. So the term "participant attack" [43–48] has attracted much attention in the cryptanalysis of quantum cryptography and should be paid more attention to. From the conclusions of QSMPC, we know that it should be insecure when less than a half of participants are honest [26]. Since QPC is a instance of QSMPC, it can only guarantee the secure when there is only one dishonest participant. So we will only analyze the attacks performed by Alice, Bob, and Charlie respectively, but not two colluded participants.

3.2.1 Alice's (Bob's) Attacks

In the proposed protocol, Alice's position are equal to Bob's completely. So we could only analyze the case that a dishonest Alice cheats Bob's private information. Before the step 11, what Bob announced is about the detecting states which are not useful to extract Bob's private information. And in the step 12, Charlie only announces the comparison result. So Alice must pay attention on the messages P^B and Q^B Bob announced at step 11. If Alice knows K^B which is corresponding to Bob's operations performed on the encoding states at step 3, she can extract Bob's private information from P^B and Q^B as $P^B = R^B \tilde{\oplus} M^B$, $Q^B = W^B \tilde{\oplus} K^B$ and (6).

Since the encoding states travel between Charlie and Alice, Charlie and Bob respectively in the protocol, the Trojan horse attacks [49, 50] should be considered. With Trojan horse attacks, Alice might use invisible photon eavesdropping or delay-photon eavesdropping to cheat. Since a filter could filter out the photon signal with an illegitimate wavelength, invisible photon eavesdropping is prevented. With the use of multi-photon detection, enough number of delay-photon eavesdropping is prevented. If a few of bits in K^B are extracted by Alice, she only can recover a few bits of W^B. When the number of correct bits in W^B is less than t, R^B cannot be recovered with the error-correcting function correctly. Then the delay-photon eavesdropping is invalid.

Besides Trojan horse attacks, some other attacks [44–48] also could be used to cheat information from traveling states, such as intercept-resend attack, measurement-resend

attack, and entanglement-measure attack [30, 31]. In these attacks, Alice first performs some operations on S^B before step 3, such as entangles photons, replaces photon, then performs some measurements before it comes back to Charlie. However, these attacks will be detected by Charlie's detection based on Alice and Bob's announcements at step 6. In fact, the states used in this protocol is the four states which are similar as the four BB84 states. When $\theta = \left\{0, \frac{\pi}{2}, \frac{\pi}{4}, \frac{3\pi}{4}\right\}$, the states $\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + ie^{i\theta}|1\rangle|0\rangle\right)$ are corresponding to BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ respectively. Without the knowledge of the detecting photons' positions, Charlie and Bob's phase shifts, Alice might measure detecting states in incorrect bases. Then she will be detected for that the detecting states have been disturbed.

Therefore, the proposed protocol can resist all well known attacks performed by Alice and Bob.

3.2.2 Charlie's Attacks

Now we consider the case that a dishonest Charlie cheats Alice and Bob's private information. For extracting Alice and Bob's private information, Charlie needs only cheat one of K^A and K^B as he know the value of $K^C = K^A \tilde{\oplus} K^B$. So we only analyze the case that Charlie cheat Alice's private information.

Similarly to the analysis in the above subsection, the two Trojan horse attacks will be prevented by Alice and Bob's filter of illegitimate wavelength and the multi-photons detection.

In the other attacks, if Charlie cheats K^A, he first performs some operations on S^A at step 2, such as entangles photons, replaces photon, then performs some measurements on S^{*A} as it was sent back to him. However, all of these attacks will be detected by the check process in which he is required to announce k_j^C and the clicked detector first. Without the knowledge of the positions of detecting states, k_j^A and k_j^B before cheating, Charlie cannot make sure the detecting states' bases. Then his any dishonest measurements or operations will disturb the detecting states. Subsequently, he will be detected.

Therefore, the proposed protocol can resist all well known attacks performed by Charlie.

3.3 The Capability of Limited Fault-Tolerate

In the presented scheme, ECC are used to prevent the limited noise which appears in non-ideal scenario, including quantum preparation setups, quantum channel and measurement equipments.

However, ECC's capability of error-correcting is limited, so the protocol is appropriate for the scenario where the noise is limited. In the protocol, the error rate of noise must be less than t'/n, otherwise, the scheme should be restarted. Then the participants should use another error-correcting code which has higher error-correcting capability to utilize the scheme.

4 Conclusion

In this paper, we propose a quantum private comparison scheme based on phase encoding. The analysis indicates that the scheme is secure which can prevent some familiar attacks. And this scheme is easy to be realized in current experiments as only some simple devices are used.

Acknowledgements This work is supported by NSFC (Grant Nos. 61300181, 61272057, 61202434, 61170270, 61100203, 61121061, 61370188, and 61103210), Beijing Natural Science Foundation (Grant No. 4122054), Beijing Higher Education Young Elite Teacher Project, China scholarship council.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE, New York (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
3. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239–1243 (1995)
4. Koashi, M., Imoto, N.: Quantum cryptography based on split transmission of one-bit information in two steps phys. Rev. Lett. **79**, 2383–2386 (1997)
5. Guo, G.C., Shi, B.S.: Quantum cryptography based on interaction-free measurement. Phys. Lett. A **256**, 109–112 (1999)
6. Yuen, H.P.: Anonymous key quantum cryptography and unconditionally secure quantum bit commitment. In: Tombesi, P., Hirota, O. (eds.) Proceedings of QCMC00, Capri, 2001. Plenum Press, New York (2001)
7. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
8. Hillery, M., Buzěk, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
9. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
10. Wang, T.Y., Wen, Q.Y.: Security of a kind of quantum secret sharing with single photons. Quantum Inf. Comput. **11**(5–6), 0434–0443 (2011)
11. Hwang, T., Hwang, C.C., Yang, C.W., Li, C.M.: Revisiting Deng et al. multiparty quantum secret sharing protocol. Int. J. Theor. Phys. **50**, 2790–2798 (2011)
12. Shi, R., Huang, L.s., Yang, W., Zhong, H.: Efficient symmetric five-party quantum state sharing of an arbitrary m-qubit state. Int. J. Theor. Phys. **50**, 3329–3336 (2011)
13. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
14. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
15. Long, G.L., Deng, F.G., Wang, C., Li, X.H., Wen, K., Wang, W.y.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China **2**(3), 251–272 (2007)
16. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with χ-type entangled states. Phys. Rev. A **78**, 064304 (2008)
17. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Revisiting the security of secure direct communication based on ping-pong protocol. Quantum Inf. Process. **10**(3), 317–323 (2011)
18. Bennett, C.H., Brassard, G., Crépeau, 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**, 1895–1899 (1993)
19. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature (London) **390**, 575–579 (1997)
20. Jung, E., Hwang, M.R., Park, D., Son, J.W., Tamaryan, S.: Mixed-state entanglement and quantum teleportation through noisy channels. J. Phys. A Math. Theor. **41**, 385302 (2008)
21. Cao, H.J., Wang, H.S., Li, P.F., Song, H.S.: Teleportation of a 3-dimensional GHZ state. Int. J. Theor. Phys. **51**, 1448–1452 (2012)
22. Yao, A.C.: Protocols for secure computation. In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, pp. 160–164. IEEE Computer Society, Washington, DC (1982)
23. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: Annual ACM Symposium on Theory of Computing, pp. 218–229. ACM, New York, NY (1987)
24. Mayers, D.: Unconditional secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997)

25. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**, 3410–3413 (1997)
26. Damgård, I., Nielsen, J.B.: Scalable and unconditionally secure multiparty computation. In: Lecture Notes in Computer Science, vol. 4622, pp. 572–590. Springer, Berlin/Heidelberg (2007)
27. Wang, T.Y., Wen, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process **11**(2), 455–463 (2012)
28. Li, Y.B., Wen, Q.Y., Qin, S.: Improved secure multiparty computation with a dishonest majority via quantum means. Int. J. Theor. Phys. **52**(1), 199–205 (2013)
29. Li, Y.B., Wen, Q.Y., Qin, S.J., Guo, F.Z., Sun, Y.: Practical quantum all-or-nothing oblivious transfer protocol. Quantum Inf. Process **13**, 131–139 (2014)
30. 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)
31. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**, 065002 (2009)
32. 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)
33. 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**, 2412–2414 (2011)
34. 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)
35. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process **11**(2), 373–384 (2012)
36. Jia, H.Y., Wen, Q.Y., Li, Y.B., Gao, F.: Quantum private comparison using genuine four-particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
37. Li, Y.B., Wen, Q.Y., Gao, F., Jia, H.Y., Sun, Y.: Information leak in Liu et al.'s quantum private comparison and a new protocol. Eur. Phys. J. D **66**, 110 (2012)
38. Liu, W., Wang, Y.B., Tao, J.Z., Cao, Y.Z.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**, 69–77 (2012)
39. 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**(6), 1953–1960 (2012)
40. 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**(2), 877–885 (2013)
41. Li, Y.B., Wen, Q.Y., Li, Z.C., Qin, S.J., Yang, Y.T.: Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. Quantum Inf. Process. **13**, 141–149 (2014)
42. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland Mathematical Lib (1977)
43. Gao, F., Qin, S., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329–334 (2007)
44. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
45. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "Quantum exam". Phys. Lett. A **360**, 748–750. [Phys. Lett. A **350**, 174 (2006)]
46. 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)
47. Guo, F.Z., Qin, S.J., Gao, F., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)
48. Li, Y.B., Wen, Q.Y., Qin, S.: Comment on: "Secure multiparty computation with a dishonest majority via quantum means". Phys. Rev. A **84**, 016301 (2011)
49. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
50. 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**, 044302 (2005)