Quantum Inf Process (2017) 16:180
DOI 10.1007/s11128-017-1630-y

Quantum private comparison employing single-photon interference

Bin Liu[1,2] · Di Xiao[1] · Wei Huang[2] · Heng-Yue Jia[3] · Ting-Ting Song[4]

Received: 21 November 2016 / Accepted: 31 May 2017 / Published online: 8 June 2017
© Springer Science+Business Media New York 2017

Abstract As a typical quantum cryptographic task between distrustful participants, quantum private comparison (QPC) has attracted a lot of attention in recent years. Here we propose two QPC protocols employing single-photon interference, a typical and interesting technology for quantum communications. Compared with the previous QPC protocols employing normal single states or entangled states, the proposed protocols achieve lower communication complexity utilizing the characteristics of single-photon interference. And we also proved the security of the proposed protocols in theory.

Keywords Quantum private comparison · Quantum cryptography · Quantum information · Single-photon interference

1 Introduction

As we know, quantum mechanics has achieved huge success in many aspects of information processing, especially in cryptography. On one hand, the powerful computational capability of quantum computer is becoming a considerable and realistic threat to our privacies. The most famous instance is Shor's quantum algorithm of fac-

✉ Bin Liu
liubin31416@gmail.com

1 Post-Doctoral Research Center, College of Computer Science, Chongqing University, Chongqing 400044, China

2 Science and Technology on Communication Security Laboratory, Chengdu 610041, China

3 School of Information, Central University of Finance and Economics, Beijing 100081, China

4 Department of Computer Science, College of Information Science and Technology, Jinan University, Guangzhou 510632, China

torization which can break the widely used public-key cryptography RSA in a short period [1]. Meanwhile, advances in both theory and experiment on quantum computer have raced ahead recently [2]. On the other hand, quantum mechanics also brings us an entirely new approach to protect our privacies, quantum cryptography [3]. The security of quantum cryptographic protocols is based on physical principles such as Heisenberg uncertainty principle and quantum no-cloning theorem, making quantum cryptography more effective to counter the threats from quantum communication than classic cryptography. Since Bennett and Brassard designed the first quantum cryptographic protocol in 1984 [4], many quantum cryptographic protocols have been proposed in recent years.

Quantum cryptographic protocols may be broadly subdivided into two types. One is between mutual trusted participants, such as quantum key distribution (QKD) [4–9], quantum secure direct communication [10–14], quantum position verification [15–18] and so on. Such protocols aim to prevent the outside adversaries from cheating the participants or stealing their secrets. While the other is between participants who are not trust each other, such as quantum bit commitment [4], quantum coin flipping [19,20], quantum private query [21–24] and so on [25]. Such protocols mainly deal with the insider attacks, which are also called participant attacks, and outside attacks are always ignored since dishonest participants are more powerful than outside adversaries.

Quantum private comparison (QPC) is just an attractive kind of quantum cryptographic protocols between distrustful participants. In a QPC protocol, each of Alice and Bob owns a secret massage; they want to verify whether their secrets are identical, but do not want to reveal their own secret to the other if their secrets are different. Since Yang et al. designed the first QPC protocol in 2009 [26], people have achieved to design a variety of QPC protocols with different technologies of quantum communication, some of them employ entangled states [26–48], the other employ single-particle states [49,50].

As a kind of two-party secure computation, QPC cannot achieve unconditionally security just by the two participants themselves [51], and therefore, a third party (TP) is usually introduced. Of cause, the participants do not want TP to get their secrets. In fact, an unrestricted TP cannot help improve the security of QPC protocols, since if TP conspire with one of the participants, the protocol turns a two-party one, which has been proved insecure [51]. Therefore, some assumptions should be made on TP. In practice, assumptions on TP are quite different in different QPC protocols. Some protocols assume an *honest-but-curious* TP who would strictly follow the procedure of the protocol but try to gain the participants' secrets according to the records during the protocol [26–35,39,49]. Others assume an *almost-fully-dishonest* TP who would take more active approaches to steal the participants' secrets but would not conspire with any of them [36,37,40,46–48,50]. Obviously, the latter assumption is more propitious to the participants' privacies. However, the communication complexity of QPC protocols with an almost-fully-dishonest TP is always 2–3 times of that of QPC protocols with an honest-but-curious TP, since, to prevent TP's initiative attacks, the participants always need to share a sequence of entangled states (or a secret key) with the same length of the secret massages.

Note that QPC protocols are much different from quantum private query (QPQ) protocols, although there is only one word different literally. Firstly, their application

scenarios are different. In QPQ protocols, one party has a database of n secret data and the other wants to query one of them. While in QPC protocols, each of two parties has a secret massage and they want to know whether they are identical. Secondly, they are different in security assumptions. Neither of QPQ protocols and QPC protocols can achieve unconditional security. QPQ protocols adopt a compromise way that allows the user to get a little more information of the database and the database also can get some information about the user's querying position at risk of being found by the user. While QPC protocols always choose to introduce a third party to improve the security.

Here we design a QPC protocol with an almost-fully-dishonest TP based on single-photon interference.[1]

Utilizing this interesting and important technology, the proposed protocol achieves lower communication complexity compared with the similar QPC protocols, since TP only need to establish a secret parameter of the phase modulator with each participant, instead of a sequence of entangled states or a key. The rest of this paper is organized as follows. A QPC protocol employing single-photon interference is proposed and analyzed in Sect. 2. In Sect. 3, based on the first QPC protocol, we propose and analyze another QPC protocol which is more practical but a little compromised in communication complexity. A short conclusion and a brief discussion are given in Sect. 4.

2 The theoretical QPC protocol employing single-photon interference

2.1 The protocol

In a QPC protocol, two participants, Alice and Bob, verify whether their secrets, i.e., S_A and S_B, are identical. Since Alice and Bob do not want to reveal their secrets to each other when the secrets are different, an honest or semi-honest TP is necessary. Obviously, QPC protocols with a fully honest TP are trivial and unreasonable. As we have mentioned above, there are almost two kinds of TP in the previous QPC protocols. One is honest-but-curious TP who would honestly follow the legal procedure of the protocol but try to get the secrets by the records of the protocol. The other is almost-fully-dishonest TP who would try almost everything to steal the participant's secrets, the only restriction is that he would not conspire with any of the participants.

QPC protocols with an almost-fully-dishonest TP are more reasonable than ones with an honest-but-curious TP. However, in the previous QPC protocols with an almost-fully-dishonest TP [36,37,40,46–48,50], to prevent TP's active attacks, two participants always need to share sequences of additional entangled states or additional keys, both share the same length with the secret massages. Therefore, the communication complexity of the QPC protocols with an almost-fully-dishonest TP is always much higher. Interestingly, we find the technology of single-photon interference can

[1] Single-photon interference is a typical and important technology of quantum communication. Utilizing such technology, people designed many interesting protocols, for example, the first QKD protocol by orthogonal state encoding [6], the counterfactual QKD protocol where the secret is generated when no photons have been transmitted from one participant to the other [7], the QKD protocol without monitoring signal disturbance [8], and so on [24,52].

effectively reduce the communication complexity of the above protocols. To detect TP's dishonest behaviors, the participants only need to share a secret parameter of the phase modulator in the single-photon-interference-based protocol, which could be much shorter than their secret massages.

Now we propose a theoretical protocol employing single-photon interference, which is based on the direct idea using secret phase modulators instead of entangled states or keys. In other words, the structure of the following proposed protocol is similar with the previous QPC protocols with an almost-fully-dishonest TP [36,37,40,46–48,50]. The shortcomings of the following protocol is the difficulty in realization because of its dependence on quantum memory technology.

Suppose the length of the secret massage is n, the processes of the theoretical QPC protocol employing single-photon interference is as follows.

1. *Preparation* Alice, Bob and TP first set up an interference circuit as that in Fig. 1. Then Alice and Bob share a secret parameter of the phase modulator ϕ_{AB}. Similarly, TP and Alice (Bob) share ϕ_{TA} (ϕ_{TB}).
2. *Start* When the protocol starts, Alice sends $2n$ single-photon signals into the interference circuit from S in sequence.
3. *Detection* Alice and Bob restore all the received wave packets utilizing the quantum memory devices QM_A and QM_B. Then Bob selects n signals in random and let Alice send the corresponding wave packets to him by the blue path in Fig. 1. Thus, utilizing the blue circuit in Fig. 1, Bob can finish the interference on his side to check whether Alice or TP has cheated by sending fake signals to him. If all the n photons are detected at $D_{B_{00}}$ or $D_{B_{01}}$ and the above two detectors never respond simultaneously, they think all the parties are honest and continue to next step.
4. *Encoding* Alice and Bob send the remaining n pairs of wave packets back to the interference circuit in order, in the manner that the wave packets of the same pair would get BS_2 simultaneously. And for the ith wave packet, Alice sets PM_A at the phase $\phi_{\mathrm{AB}} + \phi_{\mathrm{TA}}$ ($\phi_{\mathrm{AB}} + \phi_{\mathrm{TA}} + \pi$) if the ith bit of her secret is 0 (1). Similarly, for the ith wave packet, Bob sets PM_B at the phase $\phi_{\mathrm{AB}} + \phi_{\mathrm{TB}}$ ($\phi_{\mathrm{AB}} + \phi_{\mathrm{TB}} + \pi$) if the ith bit of his secret is 0 (1).
5. *Comparison* TP use $\mathrm{PM}_{\mathrm{TA}}$ and $\mathrm{PM}_{\mathrm{TB}}$ modulate the wave packets from Alice by $-\phi_{\mathrm{TA}}$ and the wave packets from Bob by $-\phi_{\mathrm{TB}}$, respectively. Then the two ways of wave packets intervene at BM_2. If all the photons are detected at D_0, TP announces that their secrets are the same, otherwise, he announces they are different.

2.2 Correctness

Now we show the proposed protocol can work effectively when two participants and TP are all honest. To verify the correctness of the proposed protocol, we only need to consider the n single-photon signals remained in Step 4. When the signals have been sent into the interference circuit in Step 2. Each of them is first split into two wave packets by BS_1. Then Alice and Bob modulate the phase of one of the wave packets, respectively, to encode their secrets. At last, the two wave packets interfere at BS_2 after TP has modulated their phases. Next, we will take the kth signal as the example to prove the correctness of the protocol.

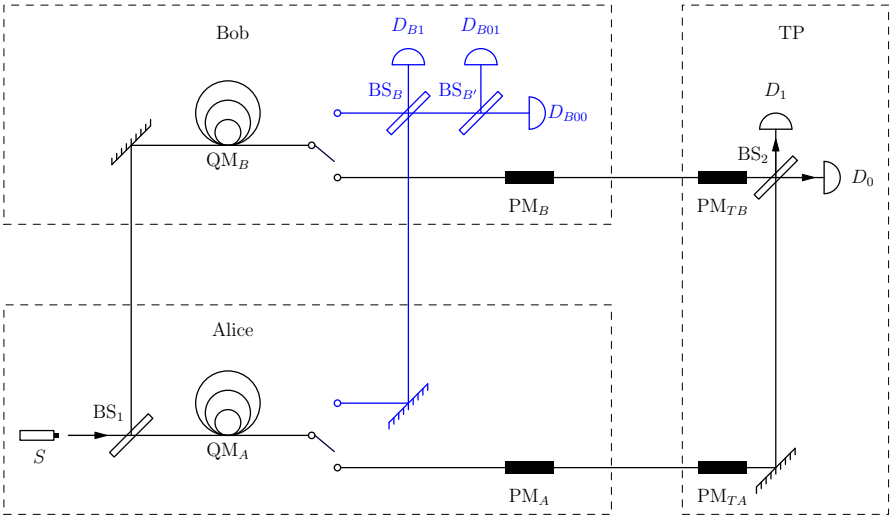

Fig. 1 The interference circuit used in the theoretical protocol. S is a single-photon source. All the beam splitters (i.e., BS_1, BS_2, BS_B, and $BS_{B'}$) are in the same type, which transmit and reflect the light with the probability 50 and 50%, respectively. QM_A and QM_B are quantum memory devices which can restore the wave packets and help the participants select specific wave packets back to the appointed path. PM_A and PM_B are adjustable phase modulators while PM_{TA} and PM_{TB} are fixed ones. And at the end of each path, there is always a photon detector to measure the position of the photons

In Step 2, after passing through BS_1, the sole photon of the ith signal might either be in the wave packet in the upper circuit, or be in the wave packet in the below circuit. We represent the two possible path of the photon as $|u\rangle$ and $|b\rangle$, respectively. Thus, the position state of the photon after it goes through BS_1 can be denoted as

$$|P\rangle_{BS_1} = \frac{1}{\sqrt{2}}(\mathbf{i}|u\rangle + |b\rangle). \tag{1}$$

Note that the reflection always adds a phase $\pi/2$ to the wave packet, which is represented by $\mathbf{i}$ in the above equation. And for the sake of simplicity, we ignore the reflections except BS_1 and BS_2 in the following analysis, and this is reasonable because of the symmetry of the circuit.

Suppose the ith bit of Alice's secret is A_i and the ith bit of Bob's secret is B_i. In Step 4, Alice (Bob) modulates the upper (below) wave packet by $\phi_{\mathrm{AB}} + \phi_{\mathrm{TA}} + A_i\pi$ ($\phi_{\mathrm{AB}} + \phi_{\mathrm{TB}} + B_i\pi$). Thus, after Alice and Bob modulated the two wave packets, the position state turns into

$$\begin{aligned} |P\rangle_{PM_{\mathrm{AB}}} &= \frac{1}{\sqrt{2}}\left(\mathbf{i}\mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TA}}+A_i\pi)}|u\rangle + \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+B_i\pi)}|b\rangle\right) \\ &= \frac{\mathbf{e}^{\mathbf{i}\phi_{\mathrm{AB}}}}{\sqrt{2}}\left(\mathbf{i}\mathbf{e}^{\mathbf{i}(\phi_{\mathrm{TA}}+A_i\pi)}|u\rangle + \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{TB}}+B_i\pi)}|b\rangle\right). \end{aligned} \tag{2}$$

In Step 5, TP first modulates the two wave packets with $-\phi_{\mathrm{TA}}$ and $-\phi_{\mathrm{TB}}$, respectively, and the position states becomes

$$|P\rangle_{PM_{TP}} = \frac{\mathbf{e}^{\mathbf{i}\phi_{\mathrm{AB}}}}{\sqrt{2}}\left(\mathbf{i}\mathbf{e}^{\mathbf{i}(A_i\pi)}|u\rangle + \mathbf{e}^{\mathbf{i}(B_i\pi)}|b\rangle\right). \tag{3}$$

Similarly, after the two wave packets passing through BS_2 simultaneously, the photon might be detected by either D_0 or D_1, and we denote the above two position states as $|0\rangle$ and $|1\rangle$, respectively. Thus, after the two modulated wave packets interfere at BS_2, the position state turns into

$$\begin{aligned}|P\rangle_{\mathrm{BS}_2} &= \frac{\mathbf{e}^{\mathbf{i}\phi_{\mathrm{AB}}}}{2}\left[\mathbf{i}\mathbf{e}^{\mathbf{i}(A_i\pi)}(|0\rangle + \mathbf{i}|1\rangle) + \mathbf{e}^{\mathbf{i}(B_i\pi)}(\mathbf{i}|0\rangle + |1\rangle\right] \\ &= \frac{\mathbf{e}^{\mathbf{i}\phi_{\mathrm{AB}}}}{2}\left[\mathbf{i}(\mathbf{e}^{\mathbf{i}(A_i\pi)} + \mathbf{e}^{\mathbf{i}(B_i\pi)})|0\rangle + (\mathbf{e}^{\mathbf{i}(B_i\pi)} - \mathbf{e}^{\mathbf{i}(A_i\pi)})|1\rangle\right].\end{aligned} \tag{4}$$

As shown in Eq. (4), if Alice's secret bit is the same with Bob's (i.e., A_i=B_i), Eq. (4) turns into

$$|P\rangle_{\mathrm{BS}_2} = \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+(A_i+1/2)\pi)}|0\rangle, \tag{5}$$

which means D_0 always responds. Otherwise, Eq. (4) turns into

$$|P\rangle_{\mathrm{BS}_2} = \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+B_i\pi)}|1\rangle, \tag{6}$$

which means D_1 responds if $A_i \neq B_i$.

To summarize, if Alice's secret is the same with Bob's, D_0 always responds and D_1 never; and once D_1 responds, it implies that Alice and Bob own the different secrets. Therefore, the proposed protocol is correct.

2.3 Security

Now we analyze the security of the proposed protocol in two aspects, the security against dishonest participant and against dishonest TP.

2.3.1 Security against dishonest participants

For the security against dishonest participants, we first show that if the signals are prepared as what they should be, none of Alice or Bob can steal the other's secret, then we show that the eavesdropping detection in Step 3 can force Alice to prepare the signals legally. Note that the signals are prepared by Alice, so Bob cannot interfere them before Alice's encoding operations have finished.

In fact, the security against dishonest participants is guaranteed by the secret parameters ϕ_{TA} and ϕ_{TB}. Without loss of generality, we suppose Alice is the dishonest

participant. If the signals are prepared legally and have not been interfered by adversaries, after Bob's encoding operation, the state of the signal is

$$|P_{B_i}\rangle = \frac{1}{\sqrt{2}}\left(\mathbf{i}|u\rangle + \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+B_i\pi)}|b\rangle\right). \tag{7}$$

Since B_i could be either 0 or 1 equiprobably, in Alice's view, the above state is

$$\begin{aligned}|P_B\rangle &= \frac{1}{2}(|P_0\rangle\langle P_0| + |P_1\rangle\langle P_1|)\\ &= \frac{1}{4}\left(|u\rangle\langle u| + |b\rangle\langle b| + \mathbf{ie}^{-\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}})}|u\rangle\langle b| - \mathbf{ie}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}})}|u\rangle\langle b|\right)\\ &\quad+\frac{1}{4}\left(|u\rangle\langle u| + |b\rangle\langle b| + \mathbf{ie}^{-\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+\pi)}|u\rangle\langle b| - \mathbf{ie}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+\pi)}|u\rangle\langle b|\right)\\ &= \frac{1}{2}(|u\rangle\langle u| + |b\rangle\langle b|),\end{aligned} \tag{8}$$

which is in the maximum mixed state. Considering l signals collectively, the joint state of them is

$$\begin{aligned}|P_B\rangle^{\otimes l} &= \frac{1}{2^l}(|u\ldots uu\rangle\langle u\ldots uu| + |u\ldots ub\rangle\langle u\ldots ub| + \ldots + |b\ldots bb\rangle\langle b\ldots bb|)\\ &= \frac{1}{2^l}\sum_{k=1}^{2^l}(|k\rangle\langle k|),\end{aligned} \tag{9}$$

which is still in the maximum mixed state. Therefore, whatever measurement Alice preforms on it, the result is totally random. And, without any information about ϕ_{TB}, Alice cannot get any precise information about Bob's secret from the above measurement results. Worse more, such reckless attacks would lead to the failure of the protocol, i.e., TP would get a wrong comparison result of their secrets. As analyzed above, if the signals are prepares as what they should be, rational participants would not attack the protocol since they cannot get any useful information about the other's secret, but only disturbing the comparison result.

Next, we will show that Alice has to prepare the legal signals in order to pass Bob's detection in Step 3. Since the reflection ratio of both Bob's beam splitter BS_B and TP's beam splitter BS_2 are 50%, the reflection ratio of BS_1 must also be 50%, otherwise, the interference result would not be determinate, so that Alice would fail to pass Bob's detection and TP would get an incorrect comparison result. Therefore, the only left opportunity for her is cheating at the source, i.e., sending multi-photon signals instead single-photon signals. Suppose Alice sends a two-photon signal into the circuit, the position state after Bob's encoding operation is [compared with Eq. (7)]

$$\begin{aligned}|P'_{B_i}\rangle = |P_{B_i}\rangle^{\otimes 2} &= \left[\frac{1}{\sqrt{2}}\left(\mathbf{i}|u\rangle + \mathbf{e}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+B_i\pi)}|b\rangle\right)\right]^{\otimes 2}\\ &= \frac{1}{2}\left(-|uu\rangle + \mathbf{ie}^{\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+B_i\pi)}(|ub\rangle + |bu\rangle) + \mathbf{e}^{\mathbf{2i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}}+B_i\pi)}|bb\rangle\right).\end{aligned} \tag{10}$$

And in Alice's view, it is [compared with Eq. (8)]

$$|P_B\rangle = \frac{1}{4}[|uu\rangle\langle uu| + |bb\rangle\langle bb| + (|ub\rangle + |bu\rangle)(\langle ub| + \langle bu|) - \mathbf{e}^{-2\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}})}|uu\rangle\langle bb| - \mathbf{e}^{2\mathbf{i}(\phi_{\mathrm{AB}}+\phi_{\mathrm{TB}})}|bb\rangle\langle uu|], \tag{11}$$

which contains the information about ϕ_{TB}. In fact, the more photons the signal has, the more information about ϕ_{TB} is contained in the state after Bob's encoding operation. Therefore, this multi-photon attack strategy is effective to steal the value of ϕ_{TB} and further steal the secret of Bob. Fortunately, with the help of $\mathrm{BS}_{B'}$, Bob can detect this attack by simultaneous responses of $D_{B_{00}}$ and $D_{B_{01}}$. And it is easy to calculate that the simultaneous response rate is $1-(1/2)^{l-1}$ for an l-photon signal.

By now, we have proven the security of the proposed protocol against dishonest participants.

2.3.2 Security against dishonest TP

Similar with the situation for Alice to steal Bob's secret, TP faces the same difficulties in stealing the participants' secrets. As we have analyzed above, without any information about ϕ_{AB}, TP's direct attack on Alice's secret would get nothing about Alice's secret but only disturb the comparison result. And since the signal is prepared by Alice, it is useless for TP to steal Alice's secret directly. As for Bob, TP can intercept and capture the legal signal Alice sent to Bob and resends a fake signal he prepared. Similarly, it is useless to send single-photon signals, and therefore, the only effective attack strategy for TP is sending multi-photon signals to Bob in order to get the value of ϕ_{AB} first. However, similar with Alice's multi-photon attack strategy, Bob would find this dishonest actions by simultaneous responses of $D_{B_{00}}$ and $D_{B_{01}}$.

By now, we have analyzed the correctness and the security of the proposed protocol. Although the proposed protocol performs well in security and efficiency, in the sense that the participants only need to share three private parameters instead of three secret keys or sequences of entangled states, there are two main disadvantages. One is the difficulty in realization because of the using of quantum memory, actually the storage for the wave packages, which is very difficult with today's technologies. Generally in cryptography, the outsider attacker would not be considered in protocols between participants without mutual trust. However, because of the specific nature of quantum mechanics, especially the single-photon interference signals, the outsider attacks becomes a real problem in the proposed protocol. To be specific, the participants cannot verify the correctness of the comparison result while outside attackers are concerned. In next section, we will propose a practical QPC protocol employing single-photon interference, which solves the above two problems with a little compromise on efficiency.

3 The practical QPC protocol employing single-photon interference

In this section, we present a practical QPC protocol employing single-photon interference, where no quantum memory devices are required. The main idea is that Alice and Bob compare the hash functions of their secrets, and let TP perform part of the detections. To describe to processes more detailedly, we introduce more parameters and to facilitate the readers, we list them together in Table 1. The detailed process of the practical QPC protocol employing single-photon interference is as follows.

(a) *Preparation* Alice, Bob, and TP set up an interference circuit as that in Fig. 2, and share some necessary parameters and information in Table 1.
(b) *Start* At the beginning of the protocol, Alice first sends a high-lights signal into the circuits from S, as a starting signal. Then she sends single-photon signals into the circuits with the frequency f.
(c) *Encoding* We denote the moment that Bob receives the high-lights signal as T_B and the moment Alice receives it at the position PM_A as T_A. If the ith bit in h_A is A_i, Alice sets PM_A at $\phi_{\mathrm{AB}} + \phi_{\mathrm{TA}} + A_i \times \pi$ during the period $(T_A + i/f - 1/(2f), T_A + i/f + 1/(2f))$ to encoding A_i in the signal. Similarly, if the ith bit in h_B is B_i, Bob sets PM_B at $\phi_{\mathrm{AB}} + \phi_{\mathrm{TB}} + B_i \times \pi$ during the period $(T_B + i/f - 1/(2f), T_B + i/f + 1/(2f))$ to encoding B_i in the signal.
(d) *First detection* After encoding B_i in the signal, Bob has a choice to choose a detection mode with the probability c. When the detection mode is chosen, Bob transfers the ith signal into the detection circuit as shown in Fig. 2 to detect whether the signal has more than one photons. If more photons are detected, Bob announces the fact and they abandon the protocol. Otherwise, Bob publish i, TP ignores the result of the ith signal, Alice and Bob append A_i to h_A and B_i to h_B, respectively.
(e) *Second detection* At right part of the circuit, TP sets up a phase modulator with the fixed phase $-\phi_{\mathrm{TA}}$ ($-\phi_{\mathrm{TB}}$) at Alice's (Bob's) light path. The two wave packets intervene at the beam splitter BS_2. For each signal, TP has a choice to choose a

Table 1 Necessary parameters and information the participants shared in advance

Notation	What the notation denotes
f	The frequency of the operations in the protocol, for example, the frequency that Alice sends single-photon signals into the circuits and the frequency that Alice and Bob shift their phase modulator
c	The parameter for the detection rate, and generally $c \leq 0.5$
H	A hash function shared by Alice and Bob
l	The length of the outcome of H
K_{AB}	A secret key shared by Alice and Bob, with the length of $c \times l$
ϕ_{TA}	A secret parameter of the phase modulator shared by TP and Alice
ϕ_{TB}	A secret parameter of the phase modulator shared by TP and Bob
ϕ_{AB}	A secret parameter of the phase modulator shared by Alice and Bob
h_A	$h_A = H(S_A)$, which is only known by Alice, here S_A is Alice's secret
h_B	$h_B = H(S_B)$, which is only known by Bob, here S_B is Bob's secret

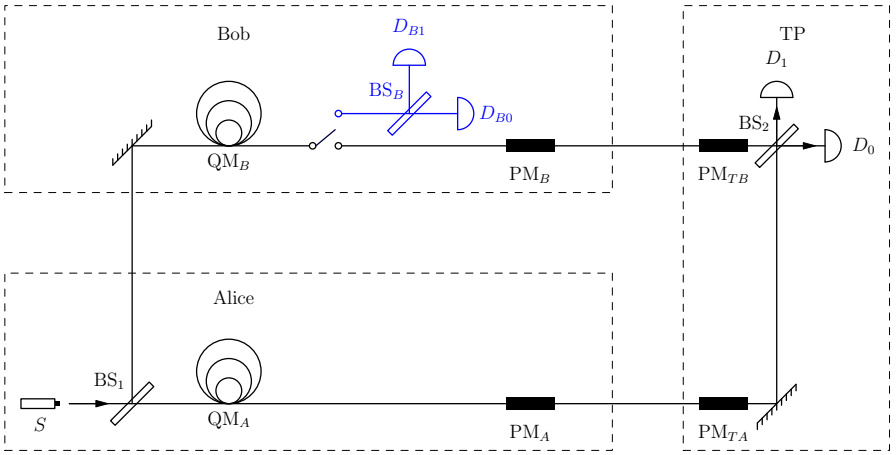

Fig. 2 The interference circuit used in the practical protocol. Each device is the same with the device labeled by the same symbol in Fig. 1. Note that Alice and Bob need no quantum memory devices here and Bob's detection operation becomes much easier, just sending the signal into BS_B to check whether it has more than one photon

detection mode with the probability c. When the detection mode is chosen, TP publishes the result that which of D_0 and D_1 has responded. Then TP randomly decides that Alice sends the ith bit in $h(A)$ to Bob or Bob send the ith bit in $h(B)$ to Alice. Note that the above $(c \times l)$-bit communication is encrypted by K_{AB}. Then the two participant check whether the result is right. If they finds an error in the second detection, they abandon the protocol.

(f) *Comparison* Ignoring the deleted signals in the first detection, if D_1 never responds during the whole process, TP can get the conclusion that Alice and Bob own the same secret. Otherwise, once D_1 detects a photon, it implies that Alice's and Bob's secrets are different. Then TP publishes the comparison result.

Note that in Step e and f, once TP or the participants confirm that the two secrets are different, the protocol is finished and they terminate the protocol.

The main difference between the two protocols above is the detection strategy. In the first protocol, the detection process and the encoding process is separated, i.e., first detection and afterward encoding. Consequently, Alice and Bob must restore the signals used to encoding their secret till the detection has finished, which makes the first protocol difficult to achieve. To avoid the use of quantum memory technology, we use interleaved the processes of detection and encoding instead in the second protocol, making the second protocol easier to realize. However, to protect the participants' privacies, the participants must share a secret key with half length of the massage to be encoded.

Now we briefly analyze the security and the efficiency of the second protocol. Similarly as in the first protocol, Alice or TP cannot steal the value of ϕ_{TB} or ϕ_{AB} by sending Bob multi-photon signals because of the first detection performed by Bob in Step d. And the second detection performed by the three parties together can force Alice to send the legal signals into the circuit and prevent TP from disturbing the

signal Alice sends to Bob. The only disadvantage of this detection is that Alice and Bob have to reveal some information about their secrets to each other to finish the detection. To solve this problem, Alice and Bob compare the hash functions of their secret instead of the secret directly, and preshare a secret key to encrypt the massage in the second detection. Due to the two protection measures, the revealed information can be reduced to a negligible level.

For the efficiency, the only added communications in the second protocol is the $(c \times l)$-bit key K_{AB}, ignoring the hash function. In the second protocol, Alice first sends n signals into the circuit. As to the first detection, about $c \times n$ signals are required to be added for the first n signals, then about $c^2 \times n$ signals are required for the new $c \times n$ signals. And Alice totally send

$$\sum_{i=0}^{+\infty} c^i \times n = \frac{n}{1-c}. \tag{12}$$

Usually we take $c = 1/2$, therefore, the total number of the signals Alice sends into the circuit is $2n$ in this situation, the same with that in the first protocol.

4 Conclusions

In this paper, we propose two QPC protocols utilizing a famous and important quantum communication technology, single-photon interference. In one hand, we have proposed the first QPC protocol based on single-photon interference, which allows two participants to compare their secrets privately in the single-photon interference circuit. One the other hand, compared with QPC protocols employing normal particles, the proposed protocols has significant advantages in communication efficiency, especially the photon efficiency, since the participants need not to generated several secret keys with the same length of their massages or sequences of entangled states. And we also analyzed the security and the efficiency of the proposed protocols.

Acknowledgements This work is supported by the National Postdoctoral Program for Innovative Talents under Grant No. BX201600199, China Postdoctoral Science Foundation funded project under Grant No. 2017M612912, the Fundamental Research Funds for the Central Universities under Grant Nos. 0216005202066, Sichuan Youth Science and Technology Foundation under Grant No. 2017JQ0045, National Natural Science Foundation of China under Grant Nos. 61572089, 61309029, 61502200, the Natural Science Foundation of Guangdong Province under Grant No. 2014A030310245.

References

1. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring, In: Proceedings of 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, pp. 124–134 (1994)
2. "Quantum Chaos: After a Failed Speed Test, the D-Wave Debate Continues". Scientific American. 2014-06-19
3. Gisin, N., Ribordy, G.G., Tittle, W.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002)

4. 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, Bangalore, pp. 175–179 (1984)
5. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
6. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239–1243 (1995)
7. Noh, T.-G.: Counterfactual quantum cryptography. Phys. Rev. Lett. **103**, 230501 (2009)
8. Sasaki, T., Yamamoto, Y., Koashi, M.: Practical quantumkey distribution protocol without monitoring signal disturbance. Nature **509**, 475–479 (2014)
9. Liu, B., Gao, F., Qin, S.-J., et al.: Choice of measurement as the secret. Phys. Rev. A **89**, 042318 (2014)
10. Long, G.-L., Liu, X.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
11. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**, 042315 (2003)
12. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
13. Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state. Opt. Commun. **283**, 192 (2010)
14. Huang, W., Wen, Q.-Y., Jia, H.-Y., Qin, S.-J., Gao, F.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B **21**(10), 100308 (2012)
15. Malaney, R.A.: Location-dependent communications using quantum entanglement. Phys. Rev. A **81**, 042319 (2010)
16. Buhrman, H., et al.: Position-based quantum cryptography: impossibility and constructions. In: Rogaway P. (ed.) CRYPTO 2011. *LNCS*, vol. 6841, pp. 429–446. Springer, Heidelberg (2011). Full version is arXiv:1009.2490v4 [quant-ph]
17. Brassard, G.: The conundrum of secure positioning. Nature **479**, 307 (2011)
18. Gao, F., Liu, B., Wen, Q.-Y.: Quantum position verification in bounded-attack-frequency model. Sci. China Phys. Mech. Astron. **59**, 110331 (2016)
19. Nayak, A.: Bit-commitment-based quantum coin flipping. Phys. Rev. A **67**, 012304–012314 (2003)
20. Barrett, J., Massar, S.: Quantum coin tossing and bit-string generation in the presence of noise. Phys. Rev. A **69**(2), 577–580 (2004)
21. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries. Phys. Rev. Lett. **100**, 230502 (2008)
22. Jakobi, M., Simon, C., Gisin, N., et al.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**, 022301 (2011)
23. Gao, F., Liu, B., Huang, W., Wen, Q.Y.: Postprocessing of the oblivious key in quantum private query. IEEE J. Sel. Top. Quantum Electron. **21**(3), 6600111 (2015)
24. Liu, B., Gao, F., Huang, W., et al.: QKD-based quantum private query without a failure probability. Sci. China Phys. Mech. Astron. **58**, 100301 (2015)
25. Liu, B., Gao, F., Huang, W., Li, D., Wen, Q.-Y.: Controlling the key by choosing the detection bits in quantum cryptographic protocols. Sci. China Inf. Sci. **58**(11), 112110 (2015)
26. 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)
27. Yang, Y.-G., Cao, W.-F., Wen, Q.Y.: Secure quantum private comparison. Phsy. Scr. **80**, 065002 (2009)
28. 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**, 1161–1165 (2009)
29. 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)
30. Tseng, H.-Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
31. Chang, C.-H., Hwang, T., Gope, P.: An efficient quantum private comparison of equality over collective-noise channels. Int. J. Theor. Phys. **55**(4), 2125-38 (2016)
32. Chen, X.-B., Dou, Z., Xu, G., Wang, C., Yang, Y.X.: A class of protocols for quantum private comparison based on the symmetry of states. Quantum Inf. Process. **13**(1), 85–100 (2014)
33. 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. **13**(1), 101–112 (2014)

34. Guo, F.-Z., Gao, F., Qin, S.-J., Zhang, J., Wen, X.-Y.: Quantum private comparison protocol based on entanglement swapping of d-level Bell states. Quantum Inf. Process. **12**(8), 2793–2802 (2013)
35. He, G.P.: Comment on quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **14**(6), 2301–2305 (2015)
36. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum Inf. Process. **14**(11), 4225–4235 (2015)
37. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. **55**(6), 2969–2976 (2016)
38. Huang, W., Wen, Q.-Y., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. **56**(9), 1670–1678 (2013)
39. Ji, S., F., Wang, W.J., Liu, Yuan, X.M.: Twice-Hadamard-CNOT attack on Li et al.'s fault-tolerant quantum private comparison and the improved scheme. Front. Phys. **10**(2), 192–197 (2015)
40. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**(6), 711–715 (2016)
41. Li, J., Jia, L., Zhou, H.F., Zhang, T.T.: Secure quantum private comparison protocol based on the entanglement swapping between three-particle W-class state and bell state. Int. J. Theor. Phys. **55**(3), 1710–1718 (2016)
42. Li, Y.B., Ma, Y.J., Xu, S.W., Huang, W., Zhang, Y.S.: Quantum private comparison based on phase encoding of single photons. Int. J. Theor. Phys. **53**(9), 3191–3200 (2014)
43. 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)
44. Li, Y.B., Wang, T.Y., Chen, H.Y., Li, M.D., Yang, Y.T.: Fault-tolerate quantum private comparison based on GHZ states and ECC. Int. J. Theor. Phys. **52**(8), 2818–2825 (2013)
45. Lin, J.S., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. **13**(2), 239–247 (2014)
46. Lin, S., Guo, G.D., Liu, X.F.: Quantum private comparison of equality with χ-type entangled states. Int. J. Theor. Phys. **52**(11), 4185–4194 (2013)
47. Lin, S., Sun, Y., Liu, X.F., Yao, Z.Q.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process. **12**(1), 559–568 (2013)
48. 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**(4), 1085–1091 (2014)
49. 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)
50. He, G.P.: Simple quantum protocols for the millionaire problem with a semi-honest third party. Int J Quantum Inf. **11**(02), 289–300 (2013)
51. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS 82), Washington, DC (1982)
52. Xu, S.W., Sun, Y., Lin, S.: Quantum private query based on single-photon interference. Quantum Inf. Process. **15**(8), 3301–3310 (2016)