Quantum private comparison via cavity QED

Tian-Yu Ye*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R.China

*E-mail: happyty@aliyun.com

Abstract: The first quantum private comparison (QPC) protocol via cavity quantum electrodynamics (QED) is proposed in this paper by making full use of the evolution law of atom via cavity QED, where the third party (TP) is allowed to misbehave on his own but cannot conspire with either of the two users. The proposed protocol adopts two-product atom states rather than entangled states as the initial quantum resource, and only needs single-atom measurements for two users. Both the unitary operations and the quantum entanglement swapping operation are not necessary for the proposed protocol. The proposed protocol can compare the equality of one bit from each user in each round comparison with one two-product atom state. The proposed protocol can resist both the outside attack and the participant attack. Particularly, it can prevent TP from knowing two users’ secrets. Furthermore, the qubit efficiency of the proposed protocol is as high as 50%.

Keywords: Quantum private comparison (QPC), cavity quantum electrodynamics (QED), third party (TP), product state, participant attack

1 Introduction

In the past two decades, quantum information processing had greatly aroused the interest of researchers throughout the world and gained considerable developments. Quantum cryptography, which was first proposed by Bennett and Brassard [1] in 1984, is the development outcome of quantum information processing in the realm of cryptography. It can attain unconditional security on the basis of quantum mechanics principles such as the Heisenberg uncertainty principle, the quantum no-cloning theorem and so on, and has greatly attracted the attentions of many researchers. Up to now, it has established many branches, such as quantum key distribution (QKD) [1-10], quantum secret sharing (QSS) [11-15], quantum secure direct communication (QSDC) [16-24], quantum dialogue (QD) [25-31], quantum teleportation (QT) [32-37] etc.

Quantum private comparison (QPC), which was first suggested by Yang et al. [38] in 2009, is another interesting branch of quantum cryptography. It aims to compare the equality of secrets from different users without leaking them out on the basis of quantum mechanics principles. As pointed out by Lo [39] that it is impossible to securely evaluate the equality function in a two-party scenario, QPC always requires some additional assumptions such as a third party (TP), etc. In recent years, QPC has been greatly developed so that different quantum states and different quantum technologies have been utilized to construct different kinds of QPC protocols. There are QPC protocols with single particles [40-43], Bell states [38,42,44-52], GHZ states [53-56], W states [52,57-58], cluster states [59-60], \( \chi \) -type entangled states [61-63]. There are QPC protocols requiring the unitary operations [38,40,43,45,53-54,57,59-60,62] and QPC protocols requiring the quantum entanglement swapping operation [44,50-52,55,61].

At present, the physical systems for realizing quantum information processing mainly include cavity quantum electrodynamics (QED), ion trap, nuclear magnetic resonance, quantum dot, superconducting system with Josephson effect, etc. [64] Many works, such as entanglement detection [65], Bell-state analysis [66-67], entanglement concentration [68-71], entanglement purification [72], entanglement generation [71,73-74] and quantum repeater [75], have been realized via these physical systems. Cavity QED can guarantee a high level of coherence so that it is an ideal candidate for the experiment of quantum information processing. [64] Cavity QED has become one of the most promising physical systems due to its unique contribution.

Based on the above analysis, following some ideas in the protocol of Ref.[46], we put forward the first QPC protocol via cavity QED by making full use of the evolution law of atom via cavity QED. Different from the standard semi-honest TP first proposed by Chen et al. [53], in our protocol, TP is assumed to be a more practical third party. That is, TP is allowed to misbehave on his own but cannot conspire with either of the two users. Similar to the protocol of Ref.[41], our protocol adopts product states rather than entangled states as the initial quantum resource. Unlike the protocols of Refs.[38,40,43,45,53-54,57,59-60,62], our protocol does not need the unitary operations. Unlike the protocols of Refs.[44,50-52,55,61], our protocol does not need the quantum entanglement swapping operation.

The rest of this paper is organized as follows. Sec.2 introduces the model of cavity QED. Sec.3 illustrates the QPC protocol via cavity QED. Sec.4 analyzes its correctness, security and qubit efficiency. Sec.5 discusses its comparison with some previous QPC protocols. Sec.6 gives the conclusion.

2 Model of cavity QED

Driven by a classical field, two identical two-level atoms can simultaneously interact with a single-mode cavity. The interaction Hamiltonian between the single-mode cavity and the atoms under the
rotating-wave approximation can be depicted as [73-74,76-77]

\[ H = \omega_0 S_i + \omega a^\dagger a + \sum_{j=1}^{L} \left[ \left( \alpha^2 S_j + a^\dagger S_j^+ S_j^\dagger \right) + \Omega \left( S_j^+ e^{-i\omega t} + S_j e^{i\omega t} \right) \right]. \] (1)

Here, \[S_i = (1/2) \sum_{j=1}^{L} \left( |e_j\rangle \langle e_j| - |g_j\rangle \langle g_j| \right), \]

\[S_j^+ = |e_j\rangle \langle g_j|, \quad \text{and} \quad S_j^\dagger = |g_j\rangle \langle e_j|, \]

where \[|e_j\rangle \quad \text{and} \quad |g_j\rangle\]

are the ground and excited states of the \[j^{\text{th}} \]

atom, respectively. \[g\] is the atom-cavity coupling strength. \[\alpha \quad \text{and} \quad \alpha^2\]

are the annihilation and creation operators for the cavity mode, respectively. \[\omega_0, \omega, \omega^2 \quad \text{and} \quad \Omega \quad \text{are the atomic transition frequency, the cavity frequency, the classical field frequency and the Rabi frequency, respectively.} \]

\[t\]

is the interaction time. Given that \[\omega = \omega_0\], the evolution operator of the system in the interaction picture can be expressed as [73-74,76-77]

\[U(t) = e^{-iH_0 t} e^{-iH_1 t}, \] (2)

where \[H_0 = \sum_{j=1}^{L} \left( S_j^+ S_j^\dagger + S_j S_j^\dagger \right), \]

and \[H_1\]

is the effective Hamiltonian. Considering the large detuning case \[\delta \gg g\]

( \[\delta\]

is the detuning between \[\omega_0 \quad \text{and} \quad \omega_2\]

and the strong driving regime \[\Omega \gg \delta, g\]

, there is no energy exchange between the atomic system and the cavity. As a result, the effects of cavity decay and thermal field are erased. Consequently, the effective interaction Hamiltonian \[H_e\]

in the interaction picture can be described as [73-74,76-77]

\[H_e = (1/2) \sum_{j=1}^{L} \left( |e_j\rangle \langle e_j| + |g_j\rangle \langle g_j| \right) + \sum_{i,j \neq j} \left( S_i^+ S_j^\dagger + S_j^+ S_i^\dagger + H.C. \right), \] (3)

where \[\lambda = g^2 / 2\delta. \]

When two atoms are sent into the above cavity simultaneously, driven by a classical field, they interact with it. If the interaction time and the Rabi frequency are made to satisfy \[\lambda t = \pi / 4\]

and \[\Omega t = \pi, \]

two atoms will have the following evolution:

\[|gg\rangle_\mu \rightarrow \frac{\sqrt{2}}{2} e^{-i\omega t / 4} \left( |gg\rangle_\mu - i|ee\rangle_\mu \right), \]

\[|ge\rangle_\mu \rightarrow \frac{\sqrt{2}}{2} e^{-i\omega t / 4} \left( |ge\rangle_\mu - i|eg\rangle_\mu \right), \]

\[|eg\rangle_\mu \rightarrow \frac{\sqrt{2}}{2} e^{-i\omega t / 4} \left( |eg\rangle_\mu - i|ge\rangle_\mu \right), \]

\[|ee\rangle_\mu \rightarrow \frac{\sqrt{2}}{2} e^{-i\omega t / 4} \left( |ee\rangle_\mu - i|gg\rangle_\mu \right). \] (4-7)

3 QPC protocol via cavity QED

Two users, Alice and Bob, want to know whether their secrets are equal or not under the help of TP, who is allowed to misbehave on his own but cannot conspire with either of them. Assume that \[X \quad \text{and} \quad Y\]

are Alice and Bob’s secrets, respectively, where \[X = \sum_{j=1}^{L} x_j 2^j, \quad Y = \sum_{j=1}^{L} y_j 2^j, \quad x_j, y_j \in \{0,1\}. \]

Alice and Bob share two common key sequences \[K_A \quad \text{and} \quad K_B\]

individual with length \(L\) through the QKD protocols [1-10] beforehand. Here, \[K_A, K_B \in \{0,1\}\]

, where \[K_{ij}^A\]

is the \(i^{\text{th}}\) bit of \(K_A\), \(K_{ij}^B\]

is the \(i^{\text{th}}\) bit of \(K_B\), and 

\[i = 1,2,\ldots,L. \]

The QPC protocol via cavity QED is constructed as follows:

Step 1: Alice (Bob) divides the binary representation of \(X\) (\(Y\)) into \(L\) groups \(G_1^A, G_2^A, \ldots, G_L^A, \quad G_1^B, G_2^B, \ldots, G_L^B\), where each group contains one binary bit.

Step 2: TP prepares a quantum state sequence composed of \(L\) product states, each of which is randomly in one of the four states \([|gg\rangle, |ge\rangle, |eg\rangle, |ee\rangle]\). This quantum state sequence is denoted as \(S = \left[ S_1^A S_1^B, S_2^A S_2^B, \ldots, S_L^A S_L^B \right]\). Here, the subscripts \(a, b\) represent two atoms in one product state, while the superscripts \(1, 2, \ldots, L\) denote the orders of product states in \(S\).

Step 3: TP sends \(S_i^A S_i^B\) \((i = 1,2,\ldots,L)\) into the single-mode cavity described above. Driven by a classical field, the two atoms \(S_i^A\) and \(S_i^B\) simultaneously interact with the single-mode cavity. TP chooses the Rabi
frequency and the interaction time to satisfy $\Omega = \pi$ and $\lambda t = \pi/4$. As a result, $S'_1 S'_2$ will undergo the evolution as shown in formulas (4-7). Obviously, $S'_1$ and $S'_2$ become entangled together after the evolution. After they fly out the single-mode cavity, TP picks up $S'_1$ and $S'_2$ to form sequences $S_a$ and $S_b$, respectively. That is, $S_a = \left[ S'_1, S'_2, \ldots, S'_{l_a} \right]$ and $S_b = \left[ S'_1, S'_2, \ldots, S'_{l_b} \right]$.

For security check, TP prepares two sets of sample single atoms $D_a$ and $D_b$ randomly in one of the four states $\{|g\}, \{|e\}, \{|+\}, \{|-\} \rangle$. Here, $|\pm\rangle = \frac{1}{\sqrt{2}} (|g\rangle \pm |e\rangle)$ is denoted as Z basis while $\{|\pm\rangle, \{|\mp\rangle \rangle$ is denoted as X basis. Then, TP randomly inserts $D_a (D_b)$ into $S_a (S_b)$ to form a new sequence $S'_a (S'_b)$. Finally, TP sends $S'_a (S'_b)$ to Alice (Bob).

After confirming that Alice (Bob) has received $S'_a (S'_b)$, TP tells Alice (Bob) the positions and the preparation basis of sample single atoms from $D_a (D_b)$. Then, Alice (Bob) measures the sample single atoms in $S'_a (S'_b)$ with the basis TP told and tells TP her (his) measurement results. By comparing the initial states of sample single atoms in $S'_a (S'_b)$ with Alice’s (Bob’s) measurement results, TP can judge whether the quantum channel is secure or not during the transmission of $S'_a (S'_b)$. If the error rate is unreasonably high, the communication is stopped; otherwise, Alice (Bob) drops out the sample single atoms in $S'_a (S'_b)$ to recover $S_a (S_b)$, and goes to the next step.

**Step 4:** For the $i^\text{th}$ ($i$ from 1 to $L$) round comparison, Alice (Bob) measures atom $S'_a (S'_b)$ with Z basis. The measurement result of $S'_a (S'_b)$ is coded with one classical bit which is represented by $M'_1 (M'_2)$. Concretely speaking, if the measurement result of $S'_a (S'_b)$ is $|g\rangle$, $M'_1 (M'_2)$ will be 0; otherwise, if the measurement result of $S'_a (S'_b)$ is $|e\rangle$, $M'_1 (M'_2)$ will be 1. Then, Alice (Bob) computes $R'_a = G'_a \oplus M'_1 \oplus K'_a$ ($R'_b = G'_b \oplus M'_2 \oplus K'_b$). Here, $\oplus$ is the module 2 operation. Finally, Alice (Bob) tells TP $R'_a (R'_b)$ publicly.

**Step 5:** TP transforms $S'_a S'_b$ prepared in Step 2 into one classical bit $M'_i$ according to its initial state. Concretely speaking, if the initial state of $S'_a S'_b$ is $|g\rangle |g\rangle$ or $|e\rangle |e\rangle$, $M'_i$ will be 0; otherwise, if the initial state of $S'_a S'_b$ is $|g\rangle |e\rangle$ or $|e\rangle |g\rangle$, $M'_i$ will be 1. That is, $M'_i$ represents the parity of $S'_a$ and $S'_b$ prepared by TP. Then, TP computes $R' = R'_a \oplus R'_b \oplus M'_i$, and tells $R'$ to Alice and Bob publicly.

**Step 6:** After receiving $R'$, both Alice and Bob compute $R' = R' \oplus K'_a \oplus K'_b$. They terminate the protocol and conclude that $X = Y$ as long as they find out that $R' \neq 0$; otherwise, they set $i = i + 1$ and repeat the protocol from step 4. If they find out that $R' = 0$ for all $i$ in the end, they will conclude that $X = Y$.

Now it concludes the description of our protocol. For clarity, we further give out the flow chart of our protocol in Fig.1, taking $S'_a S'_b$ for example.

It should be emphasized that in this kind of dissipative system, the effects of cavity decay and thermal field are of great concerns. In order to erase the effects of cavity decay and thermal field, we need use the large detuning case and the strong driving regime. That is, $\delta$ should be chosen to satisfy $\delta \gg g$, and $\Omega$ should be chosen to satisfy $\Omega \gg \delta, g$. In this way, there is no energy exchange between the atomic system and the cavity. In addition, in order to make our protocol work well, formulas (4-7) should be established first. Therefore, both of $\lambda t = \pi/4$ and $\Omega t = \pi$ should be also satisfied.

### 4 Analysis

In this section, we analyze our protocol on three aspects including the correctness of its output, the security and the qubit efficiency.

#### 4.1 Correctness

In our protocol, under the help of TP, Alice and Bob compare the equality of $G'_a$ and $G'_b$ in the $i^\text{th}$ round comparison by using the evolution law of $S'_a S'_b$ via cavity QED. Here, $G'_a$ is the $i^\text{th}$ bit of Alice’s secret $X$, $G'_b$ is the $i^\text{th}$ bit of Bob’s secret $Y$, and $S'_a S'_b$ is the $i^\text{th}$ product state in $S$ prepared by TP. For convenience, we use $IS'$ to denote the initial state of $S'_a S'_b$ prepared by TP. Accordingly, $M'_i$ is the one-bit classical code of $IS'$. According to the description of our protocol, it is apparent that $M'_i$ is the one-bit classical code of the $Z$ basis measurement result of $S'_a$ after evolution in cavity QED, and $M'_i$ is the one-bit classical code of the $Z$
basis measurement result of $S'_i$ after evolution in cavity QED. Moreover, it follows that $R'_i = G'_i \oplus M'_i \oplus K'_i$, $R'_b = G'_b \oplus M'_b \oplus K'_b$, $R' = R'_i \oplus R'_b \oplus M'_1$, and $R'' = R' \oplus K'_i \oplus K'_b$, where $K'_i$ is the $i$th bit of $K'_i$, and $K'_b$ is the $b$th bit of $K'_b$. The relationships of these essential variables in our protocol are further shown in Table 1.

According to formulas (4-7) or Table 1, it is easy to get that $M'_i \oplus M'_b \oplus M'_j = 0$. Consequently, we obtain

\begin{align*}
R' &= R' \oplus K'_i \oplus K'_b \\
&= \left( (G'_i \oplus M'_i \oplus K'_i) \oplus (G'_b \oplus M'_b \oplus K'_b) \right) \oplus K'_i \oplus K'_b \\
&= \left( G'_i \oplus G'_b \right) \oplus \left( M'_i \oplus M'_b \oplus M'_j \right) \\
&= G'_i \oplus G'_b. 
\end{align*}

(8)

According to formula (8), if $R' = 0$, we will get that $G'_i = G'_b$; otherwise, we will get that $G'_i \neq G'_b$. It can be concluded now that the correctness of the output of our protocol is validated.

Note that similar to the QPC protocol of Ref.[46], our protocol utilizes the parity of two atoms to accomplish the equality comparison of private secrets. Concretely speaking, in the $i$th round comparison, $G'_i$ is encrypted with $M'_i$ and $K'_i$ to derive $R'_i$, and $G'_b$ is encrypted with $M'_b$ and $K'_b$ to derive $R'_b$. Here, $M'_i$, $K'_i$, $M'_b$ and $K'_b$ play the role of one-time-pad key. After doing the calculations of $R' = R'_i \oplus R'_b \oplus M'_j$ and $R'' = R' \oplus K'_i \oplus K'_b$, we get the XOR value of $G'_i$ and $G'_b$, as shown in formula (8).

As a result, the equality comparison result of $G'_i$ and $G'_b$ can be easily obtained. It is obvious that formula (8) relies deeply on the XOR relation of $M'_i$, $M'_b$ and $M'_j$, i.e., $M'_i \oplus M'_b \oplus M'_j = 0$. Actually, $M'_i \oplus M'_b$ essentially implies the parity of two atoms $S'_i$ and $S'_j$ after evolution via cavity QED, while $M'_j$ represents the parity of $S'_i$ and $S'_j$ before evolution via cavity QED. According to formulas (4-7), the parity of $S'_i$ and $S'_j$ keeps unchanged during the evolution via cavity QED so that $M'_i \oplus M'_b \oplus M'_j = 0$ is easily established, which guarantees the correctness of the equality comparison result of $G'_i$ and $G'_b$. It can be concluded now that the parity of two atoms $S'_i$ and $S'_j$ is utilized to accomplish the equality comparison of $G'_i$ and $G'_b$.

Accordingly, in the whole equality comparison process of $G'_i$ and $G'_b$, our protocol employs neither the unitary operations nor the quantum entanglement swapping operation.

4.2 Security

4.2.1 Outside attack

We analyze the outside attack according to each step of our protocol.

As for steps 1, 2 and 6, an outside eavesdropper has no chance to launch an attack, since there is not any quantum transmission or classical transmission in these steps.

As for step 3, there are quantum transmissions as TP sends $S'_i$ ($S'_j$) to Alice (Bob). An outside eavesdropper may try to obtain the two users’ secrets by performing the intercept-resend attack, the measure-resend attack, the entangle-measure attack, etc. Fortunately, the sample single atoms randomly in one of the four states $\{|g\rangle, |e\rangle, |+\rangle, |-\rangle\}$ are used to detect the outside attack. This security check method is equivalent to the decoy photon technology [78-79], which has been validated in detail in Refs.[28-29]. Note that the decoy photon technology can be regarded as a variant of the BB84 security check method [1], which has also been validated in Ref.[80]. Therefore, the attacks from an outside eavesdropper are invalid in this step.

As for step 4, Alice (Bob) tells TP $R'_i$ ($R'_b$) publicly. Apparently, $G'_i$ ($G'_b$) is encrypted with $K'_i$ ($K'_b$) in this step. However, an outside eavesdropper has no knowledge about $K'_i$ ($K'_b$). In this case, she still has no access to $G'_i$ ($G'_b$), even though she hears $R'_i$ ($R'_b$) from Alice (Bob).

As for step 5, TP tells $R'$ to Alice and Bob publicly. It can be derived that

\begin{align*}
R' &= R'_i \oplus R'_b \oplus M'_j \\
&= \left( (G'_i \oplus M'_i \oplus K'_i) \oplus (G'_b \oplus M'_b \oplus K'_b) \right) \oplus M'_j \\
&= \left( G'_i \oplus K'_i \right) \oplus \left( G'_b \oplus K'_b \right). 
\end{align*}

(9)

Even though she hears $R'$ from TP, an outside eavesdropper still cannot extract anything useful.
about $G'_a$ or $G'_b$ in this step, as she has no access to $K'_a$ and $K'_b$.

It can be concluded now that our protocol has a high level of security towards the outside attack.

4.2.2 Participant attack

Participant attack is a kind of attack from a dishonest participant. As suggested by Gao et al. [81], participant attack is generally more powerful than outside attack so that it should be paid more attention to. Two cases of participant attack including the attack from a dishonest user and the attack from TP are analyzed here.

Case 1: the attack from a dishonest user

In our protocol, Alice’s role is similar to Bob’s. Without loss of generality, Alice is assumed to be the dishonest user who wants to obtain the secret of the other user.

In step 3, Alice may want to intercept $S'_a$ TP sends to Bob. However, as she has no knowledge about the positions and the preparation basis of sample single atoms from $D_a$, she will inevitably leave her trace and be caught as an outside attacker if she launches this attack.

In step 4, Alice may hear $R'_b$ from Bob. $S'_a$ and $S'_b$ become entangled together after the evolution via cavity QED in step 3. Since Alice does not know the initial product state of $S'_aS'_b$ prepared by TP in step 2, she has no knowledge about the entangled state composed by $S'_a$ and $S'_b$ after the evolution. According to formulas (4-7), she cannot correctly deduce $M'_a$ from $M'_b$. The only thing she can do is to randomly guess the true value of $M'_b$. Because $G'_b$ is encrypted with $M'_b$, she cannot know $G'_a$ at all.

In step 5, Alice hears $R'$ from TP. According to formula (8), she can obtain $G'_b$ by computing $R' \oplus G'_a$. However, our protocol has to be terminated as long as Alice and Bob find out that $R' \neq 0$ for certain $i$. Therefore, Alice can know all the $G'_a$, where $R' = 0$ has been derived and only obtain at most 1 bit of the $G'_a$, where $R' \neq 0$ has been derived.

Case 2: the attack from TP

In our protocol, TP is allowed to try his best to obtain the secrets from two users without conspiring with either of Alice and Bob.

In step 4, Alice (Bob) tells TP $R'_a$ ($R'_b$) publicly. Since TP has no access to $K'_a$ ($K'_b$), he still cannot extract $G'_a$ ($G'_b$) from $R'_a$ ($R'_b$).

In step 5, both Alice and Bob do not tell TP $R'$. However, once the protocol is terminated by Alice and Bob in the middle, TP naturally knows that $X \neq Y$. This case happens with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$. Or if the protocol is not terminated by Alice and Bob until $G'_a$ and $G'_b$ are compared, TP has to randomly guess the comparison result between $X$ and $Y$. This case happens with the probability of $\left(\frac{1}{2}\right)^{L-1}$. It can be concluded that TP knows the exact comparison result between $X$ and $Y$ (i.e., $X \neq Y$) with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$.

4.3 Qubit efficiency

The qubit efficiency $\eta_q$ here is defined as $\eta_q = \frac{n_c}{n_q}$, where $n_c$ and $n_q$ are the number of compared classical bits and the number of consumed qubits in each round comparison, respectively [14-15]. In our protocol, one two-atom product state can be used to compare one classical bit from each user. Therefore, the qubit efficiency of our protocol is 50%.

5 Discussion

We discuss the comparison between our protocol and some previous QPC protocols [38,41,46,52-53,58,60] in this section. The comparison result is summarized in Table 2. Here, the symbol $n$ is the comparison times on the condition that Alice and Bob’s secrets are identical.

From Table 2, we can conclude that the advantage of our protocol lies in having the following features simultaneously:

1. It employs two-particle product states as the initial quantum resource, which are much easier to prepare than entangled states;
2. It only needs to perform single-atom measurements, which are easier to accomplish than Bell state measurements;
(3) It does not require the unitary operations or the quantum entanglement swapping operation;
(4) It can be automatically halted once Alice and Bob discover the inequality of their secrets in the
middle, which means that not all the secrets are necessary to be compared when their secrets are not
identical;
(5) It has a high qubit efficiency equal to 50%.

It should be emphasized that our protocol needs the use of QKD method to guarantee the security, just
as analyzed in Sec.4.2. Likewise, the QPC protocol of Ref.[38] uses the hash function to guarantee the
security. In fact, the QPC protocol in Ref.[53] is not secure, since Alice and Bob can perform the
intercept-resend attack to obtain each other’s secret without being discovered, just as pointed out by Ref.[54].
The QPC protocol in Ref.[46] is also not secure when TP is a more practical third party who tries his best to
extract useful information about two users’ secrets with active attacks, just as pointed out by Refs.[47–49].
When TP is a more practical third party than the one assumed, the QPC protocols in Refs.[53,60] have the
similar security loophole induced by TP to that in Ref.[46] indicated above. Actually, in this case, the QKD
method can be utilized to guarantee the security of the QPC protocols in Refs.[46,53,60].

In addition, different from the QPC protocols in Refs.[38,41,46,52–53,58,60], our protocol is realized
via cavity QED, thus it can make full use of the evolution law of atom via cavity QED. Actually, our
protocol is the first QPC protocol via cavity QED.

6 Conclusion
In this paper, by making full use of the evolution law of atom via cavity QED, we propose the first QPC
protocol via cavity QED. Here, TP is allowed to misbehave on his own but cannot conspire with either of the
two users. Our protocol adopts two-atom product states rather than entangled states as the initial quantum
resource, and only needs single-atom measurements for two users. It needs neither the unitary operations nor
the quantum entanglement swapping operation. It can compare the equality of one bit from each user in each
round comparison with one two-atom product state. It can resist both the outside attack and the participant
attack. Particularly, it can prevent TP from knowing two users’ secrets. Moreover, its qubit efficiency is as
high as 50%.

Acknowledgements
The author would like to thank the anonymous reviewers for their valuable comments that help enhancing the
quality of this paper. Funding by the National Natural Science Foundation of China (Grant No.61402407) is
gratefully acknowledged.

Compliance with ethical standards
Conflict of interest: The authors declare that they have no conflict of interest.

Reference
[1] Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. Proc. IEEE Int. Conf.
Computers, Systems and Signal Processing, 1984, 175–179
[2] Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys Rev Lett. 1991, 67(6):661–663
[3] Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell theorem. Phys Rev Lett., 1992, 68:557–559
[4] Cabello, A.: Quantum key distribution in the Holevo limit. Phys Rev Lett. 2000, 85:5635
[5] Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68:
042315
[6] Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A, 2004,
70:012311
[7] Su, X.L.: Applying Gaussian quantum discord to quantum key distribution.Chn Sci Bull, 2014, 59(11):1083–1090
[8] Zhang, C.M., Song, X.T, Treeviriyanupab, P., et al.: Delayed error verification in quantum key distribution. Chin Sci Bull,
2014, 59(23): 2825–2828
[9] Quan, D.X., Zhu,C.H., Liu,S.Q., Pei, C.X.:A long-distance quantum key distribution scheme based on pre-detection of optical
pulse with auxiliary state. Chin Phys B, 2015, 24:050309
[10] Zhang, C.M., Li, M., Yin, Z.Q., et al.: Decoy-state measurement-device-independent quantum key distribution with
mismatched-basis statistics. Sci China-Phys Mech Astron, 2015, 58: 590301
[11] Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys Rev A, 1999, 59:1829–1834
[12] Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59:
162–168
[13] Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69:
052307
[14] Lin, J., Hwang, T.: An enhancement on Shi et al.’s multiparty quantum secret sharing protocol. Opt Commun, 2011, 284 (5):
1468–1471
[15] Chen, J.H., Lee, K.C., Hwang, T.: The enhancement of Zhou et al.’s quantum secret sharing protocol. Int J Mod Phy C,
1999, 10(10):1531-1535
[16] Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002,65:
032302
[17] Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89:187902
[18] Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen
data block. Phys Rev A, 2003, 68:042317
[19] Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
[20] Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71:044305

[21] Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253(1-3): 15-20; Wang, C., Deng, F.G., Long, G.L.: Erratum to “Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state”. Opt Commun, 2006, 262(1): 134

[22] Chang, Y., Zhang, S., Han, G.H.: Robust quantum secure direct communication and authentication protocol against decoherence noise based on six-qubit DF state. Chin Phys B, 2015,24:050307

[23] Zou, X.F., Qiu, D.W.: Three-step semi-quantum secure direct communication protocol. Sci China-Phys Mech Astron, 2014, 57(9):1696-1702

[24] Chang, Y., Xu, C.X., Zhang, S.B., et al.: Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. Chin Sci Bull, 2014, 59(21):2541-2546

[25] Zhang, Z.J., Man, Z.X.: Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. 2004, http://arxiv.org/pdf/quant-ph/0403215.pdf

[26] Zhang, Z.J., Man, Z.X.: Secure bidirectional quantum communication protocol without quantum channel. 2004, http://arxiv.org/pdf/quant-ph/0403217.pdf

[27] Nguyen, B.A.: Quantum dialogue. Phys Lett A, 2004, 328(1):6-10

[28] Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin Phys Lett, 2007, 24(1):19

[29] Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin Phys Lett, 2013, 30(4):040305

[30] Zheng, C., Long, G.F.: Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. Sci China-Phys Mech Astron, 2014, 57(7): 1238-1243

[31] Ye, T.Y.: Fault tolerant channel-encrypting quantum dialogue against collective noise. Sci China-Phys Mech Astron, 2015, 58(4):040301

[32] Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett,1993,70:1895-1899

[33] Gorbachev, V.N., Trubilko, A.I.; Rodichkina, A.A.: Can the states of the W-class be suitable for teleportation? Phys Lett A, 2003,314:267-271

[34] Zhang, Z.J., Zhong, X.M.: Many-agent controlled teleportation of multi-qubit quantum information. Phys Lett A,2005,341: 55-59

[35] Dong, J., Teng, J.F.: Controlled teleportation of an arbitrary n-qubit state using nonmaximally entangled GHZ states. Eur Phys J D,2006,49:129-134

[36] Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: Centrally controlled quantum teleportation. Opt Commun, 2010,283:4802-4809

[37] Heo, J., Hong, C.H., Lim, J. I., Yang, H.J.: Bidirectional quantum teleportation of unknown photons using path-polarization intra-particle hybrid entanglement and controlled-unity gates via cross-Kerr nonlinearity. Chin Phys B, 2015,24:050304

[38] Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. Phys J A : Math Theor, 2009, 42 : 055305 ; Yang, Y. G. ; Wen, Q. Y. : Corrigendum : An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. Phys J A : Math Theor, 2010, 43 : 209801

[39] Lo, H.K.: Insecurity of quantum secure computations. Phys Rev A, 1997, 56(2):1154

[40] Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr, 2009, 80:065002

[41] Yang, Y.G., Xia, J., Jia, X., Shi, L., Zhang, H.: New quantum private comparison protocol without entanglement. Int J Quantum Inf, 2012,10:1250065

[42] 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,2014,13:101-112

[43] Jia, J., 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,2013,12:887-897

[44] Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun Theor Phys,2012,57:583-588

[45] Li, W., Guo, F.Z., Luo, Y., Cao, S.H., Wen, Q.Y.: Quantum private comparison protocol with the random rotation. Int J Theor Phys, 2013,52:3212-3219

[46] Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf Process, 2012,11:373-384

[47] Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int J Quantum Inf, 2013, 11:1350039

[48] Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf. Process. 2013, 12:877-885

[49] Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process, 2013, 12:1981-1990

[50] Lin, J., Yang, C.W., Hwang, T.: Quantum private comparison of equality protocol without a third party. Quantum Inf Process, 2014,13:239-247

[51] Zhang, B., Liu, X.T., Wang, J., Tang, C.J.: Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party. Quantum Inf Process, 2015, 14:4593-4600

[52] Li, J., Zhou, H.F., Jia, L., Zhang, T.T.: An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping. Int J Theor Phys, 2014,53(7):2167-2176

[53] 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, 2010,283:1561

[54] Lin, J., Tseng, H.Y., Hwang, T.: Intercept-resend attacks on Chen et al.’s quantum private comparison protocol and the improvements. Opt. Commun, 2011,284:2412-2414

[55] Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int J Theor Phys, 2012, 51: 3596-3604

[56] Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf
[57] Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt Commun, 2011, 284(2):3160-3163
[58] Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W States. Int J Theor Phys, 2014, 53(5):1723-1729
[59] Xu, G.A., Chen, X.B., Wei, Z.H., Li, M.J., Yang, Y.X.: An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. Int J Quantum Inf, 2012, 10:1250045
[60] Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int J Theor Phys, 2013, 52:212-218
[61] Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with X-type state. Int J Theor Phys, 2012, 51:69-77
[62] Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z., Cui, W.: New quantum private comparison protocol using X-type state. Int J Theor Phys, 2012, 51:1953-1960
[63] Lin, S., Guo, G.D., Liu, X.F.: Quantum private comparison of equality with X-type entangled states. Int J Theor Phys, 2013, 52:4185-4194
[64] Shu, J.: Quantum state preparation and quantum information processing in cavity QED. Heifei: University of science and technology of China, 2007, 19-20
[65] Zhou, L., Sheng, Y.B.: Detection of nonlocal atomic entanglement assisted by single photons. Phys Rev A, 2014, 90:024301
[66] Zhou, L., Sheng, Y.B.: Complete logic Bell-state analysis assisted with photonic Faraday rotation. Phys Rev A, 2015, 92:042314
[67] Wang, T.J., Wang, C.: Complete hyperentangled-Bell-state analysis for photonic qubits assisted by a three-level Lambda-type system. Sci Rep, 2016, 6:19497
[68] Sheng, Y.B., Zhou, L., Wang, L., Zhao, S.M.: Efficient entanglement concentration for quantum dot and optical microcavities systems. Quant. Inf. Process., 2013, 12:1885-1895
[69] Sheng, Y.B., Liu, J., Zhao, S.Y., Liu, L.: Multiparticle entanglement concentration for nitrogen-vacancy center and microtoroidal resonator system. Chin Sci Bull, 2013, 58:3570-3513
[70] Cao, C., Ding, H., Li, Y., Wang, T.J., Mi, S.C., Zhang, R., Wang, C.: Efficient multiparticle entanglement concentration protocol for nitrogen-vacancy center and microresonator coupled systems. Quant Inf Process, 2015, 14:1265-1277
[71] Cao, C., Wang, T.J., Zhang, R., Wang, C.: Cluster state entanglement generation and concentration on nitrogen-vacancy centers in decoherence-free subspace. Laser Phys Lett, 2015, 12:0306001
[72] Sheng, Y.B., Zhao, S.Y., Liu, J., Zhou, L.: Atomic entanglement purification using photonic Faraday rotation. Quant Inf Process, 2014, 13:881-893
[73] Zheng, S.B., Guo, G.C.: Efficient scheme for two-atom entanglement and quantum information processing in cavity QED. Phys Rev Lett, 2000, 85:2392-2395
[74] Zheng, S.B.: Generation of entangled states for many multilevel atoms in a thermal cavity and ions in thermal motion. Phys Rev A, 2003, 68:035801
[75] Li, T., Deng, F.G.: Heralded high-efficiency quantum repeater with atomic ensembles assisted by faithful single-photon transmission. Sci Rep, 2015, 5:15610
[76] Shan, C.J., Liu, J.B., Chen, T., Liu, T.K., Huang, Y.X., Li, H.: Controlled quantum secure direct communication with local separate measurements in cavity QED. Int J Theor Phys, 2010, 49:334-342
[77] Shan, C.J., Liu, J.B., Cheng W.W., Liu, T.K., Huang, Y.X., Li, H.: Bidirectional quantum secure direct communication in driven cavity QED. Mod Phys Lett B, 2009, 23:3225-3234
[78] Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin Phys Lett, 2005, 22(5):1049
[79] Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. Chin Phys Lett, 2006, 23(11):2896
[80] Shor P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85(2):441
[81] Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf Comput, 2007, 7:329
Appendix:

(a) TP prepares quantum product state $S_0 S_0$ as the quantum carrier. Here, the solid ellipse denotes an participant, while the solid rectangle denotes the quantum state preparation operation; (b) TP sends atom $S_0$ into cavity QED for evolution, and transmits it to Alice (Bob) after it flies out cavity QED. Here, the solid circle denotes cavity QED, while the solid line with an arrow denotes the quantum state transmission operation; (c) Alice (Bob) measures atom $S_0$ with $Z$ basis, computes $R'_i$ ($K'_i$) and sends $R'_i$ ($K'_i$) to TP. Here, the dotted rectangle, the dotted circle and the dotted line with an arrow denote the quantum measurement operation with $Z$ basis, the classical computation operation and the classical information transmission operation, respectively; (d) TP computes $R'$, and sends $R'$ to Alice and Bob; (e) Alice and Bob compute $R'$. 

Table 1  The relationships of essential variables in the proposed QPC protocol

\[ K'_i = G'_i \otimes M'_i \otimes K'_0, \quad R'_i = G'_i \otimes M'_i \otimes R'_0, \quad R'' = R'_i \otimes R'' \otimes K'_i \otimes K'_0. \]
| \( |ee\rangle \) | 0 | \( |eg\rangle \) | 0 | \( |ge\rangle \) | 1 | \( |eg\rangle \) | 1 | \( |ee\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 |
| 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 |
| \( |ee\rangle \) | 1 | \( |ge\rangle \) | 0 | \( |ge\rangle \) | 1 | \( |eg\rangle \) | 1 | \( |ee\rangle \) | 1 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 |
| 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 |
| 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 |
| \( |ee\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 |
| 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 |
| 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 |
| \( |ee\rangle \) | 1 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 |
| 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 |
| 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 |
| \( |ee\rangle \) | 1 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 | \( |gg\rangle \) | 0 |
| 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 |
| 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 |
| 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 | 1,1 |
Table 2: Comparison between our protocol and some previous QPC protocols

| Initial quantum resource | Bell entangled states | Two-particle product state | Bell entangled states | Four-particle W entangled states and Bell entangled states | Bell entangled states | Four-particle W entangled states | Three-particle GHZ entangled states | Four-particle cluster entangled states | Two-atom product state |
|--------------------------|-----------------------|----------------------------|----------------------|-------------------------------------------------|----------------------|--------------------------------|---------------------------------|---------------------------------|-----------------------|
| Ref.[38]                 | Yes                   | No                         | Yes                  | No                                              | Yes                  | No                             | Yes                             | No                              | Yes                   |
| Ref.[41]                 | Yes                   | No                         | Yes                  | No                                              | Yes                  | No                             | Yes                             | No                              | Yes                   |
| Ref.[46]                 | Yes                   | No                         | Yes                  | No                                              | Yes                  | No                             | Yes                             | No                              | Yes                   |
| Ref.[52]                 | No                    | No                         | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                             | No                              | Yes                   |
| Ref.[53]                 | No                    | No                         | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                             | No                              | Yes                   |
| Ref.[58]                 | No                    | Yes                        | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                             | No                              | Yes                   |
| Ref.[60]                 | No                    | No                         | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                  | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                             | No                              | Yes                   |
| Our protocol             | Yes                   | No                         | Yes                  | No                                              | Yes                  | No                             | Yes                             | No                              | Yes                   |

| Quantum measurement (except that for security check) | Bell state measurements | single-particle measurements | single-particle measurements | Bell state measurements | single-particle measurements | single-particle measurements | Single-atom measurements |
|------------------------------------------------------|--------------------------|-------------------------------|-----------------------------|-------------------------|-------------------------------|-----------------------------|---------------------------|
| Ref.[38]                 | No                       | Yes                           | No                           | No                       | Yes                           | No                           | No                        |
| Ref.[41]                 | Yes                      | No                            | No                           | No                       | Yes                           | No                           | No                        |
| Ref.[46]                 | Yes                      | No                            | Yes                          | No                       | Yes                           | No                           | Yes                       |
| Ref.[52]                 | No                       | No                            | Yes                          | No                       | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                       |
| Ref.[53]                 | No                       | Yes                            | Yes                          | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                           | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                       |
| Ref.[58]                 | No                       | Yes                            | Yes                          | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                           | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                       |
| Ref.[60]                 | No                       | No                             | Yes                          | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                           | Yes (with the probability of $1 - \left(\frac{1}{2}\right)^{L-1}$) | Yes                       |
| Our protocol             | Yes                      | No                             | Yes                          | No                       | Yes                           | No                           | Yes                       |

| Use of QKD method | No (Use of Hash function instead) | Yes | No | Yes | No | Yes | No | Yes |
|-------------------|-----------------------------------|-----|----|-----|----|-----|----|-----|
| Use of unitary operations | Yes | No | No | No | Yes | No | Yes | No |
| Use of entanglement swapping TP's knowledge about the comparison result | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Bit number compared each round | $L$ | 1 | 1 | $L$ | 1 | 1 | $L$ | 1 |
| Comparison times $n$ | 1 | $L$ | $L$ | 1 | $L$ | $L$ | 1 | $L$ |
| Qubit efficiency $\eta_1$ | 25% | 50% | 50% | 33% | 33% | 33% | 25% | 50% |