Single-state semiquantum private comparison based on Bell entangled states

Mao-Jie Geng, Ying Chen, Tian-Jie Xu, Tian-Yu Ye*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R.China
E-mail: happyyty@aliyun.com(T.Y.Ye)

Abstract: In this paper, a novel semiquantum private comparison (SQPC) protocol based on single kind of Bell entangled states is proposed, which allows two classical parties to judge the equality of their private inputs securely and correctly under the help of a semi-honest third party (TP) who possesses complete quantum capabilities. TP is allowed to misbehave on her own but cannot conspire with anyone else. Our protocol does not need to share secret keys among different participants in advance, and needs neither unitary operations nor quantum entanglement swapping. Moreover, our protocol only needs to prepare single kind of Bell entangled states as initial quantum resource. Detailed security analysis turns out that our protocol is secure against various outside and participant attacks. Compared with most of the existing SQPC protocols based on Bell entangled states, our protocol is more feasible in practice.

Keywords: Semiquantum cryptography; semiquantum private comparison; semi-honest third party; Bell entangled state

1 Introduction

Relying on the physical laws such as the quantum no-cloning theorem, the uncertainty principle etc., quantum cryptography has unconditional security in theory. In 1984, Bennett and Brassard [1] proposed the world's first quantum key distribution (QKD) protocol by using the polarization of single photons, which was always named as the BB84 protocol later. Starting with the BB84 protocol, quantum cryptography has gained a considerable development in recent years. Researchers have proposed different kinds of quantum cryptography protocols suitable for different application scenarios, such as quantum key distribution (QKD) [2-6], quantum secret sharing (QSS) [7-10], quantum secure direct communication (QSDC) [11-16], quantum identity authentication (QIA) [17,18], and so on. QKD protocols can be used to establish a private sequence of key bits between two remote communicants through the transmission of quantum signals. QSS permits different participants to share a secret privately in the way that only all of them cooperate together can they reconstruct it. QSDC protocols can be used to directly transmit a secret message from one party to the other party. QIA protocols can be used for authenticating whether the user's identity is legal or not. In 2009, Yang and Wen [19] proposed the first quantum private comparison (QPC) protocol, which can compare the equality of private inputs from two different users under the condition that none of them will be leaked out. Since then, scholars have
designed abundant QPC protocols with different quantum states, such as the ones with single particles [20,21], Bell states [22-24], GHZ states [25,26], cluster states [27], $\chi$-type entangled states [28], etc. The above QPC protocols require all users to have quantum capabilities, which may incur high costs in practice.

In 2007, Boyer et al. [29] proposed the first measure-resend semiquantum key distribution (SQKD) protocol by using the famous BB84 protocol, where it is not necessary for all users to have complete quantum capabilities. Subsequently, in 2009, Boyer et al. [30] further put forward the randomization-based SQKD protocol with single photons. At present, in the field of semiquantum cryptography, according to two representative works in Refs.[29,30], classical users are widely considered to be limited to the following operations: (a) sending or reflecting the qubits without interference; (b) measuring qubits in the classical basis $\{0,1\}$; (c) preparing the fresh qubits in the classical basis $\{0,1\}$; and (d) reordering the qubits through different delay lines.

Based on these settings, compared with the traditional quantum cryptography, semiquantum cryptography may effectively save quantum resource and quantum operations. The idea of semiquantum has been applied into various branches of quantum cryptography so that the corresponding semiquantum cryptography branches have been established, such as SQKD [29-33], semiquantum secret sharing (SQSS) [34-37], semiquantum key agreement (SQKA) [38-41], semiquantum controlled secure direct communication (SQCSDC) [41] and semiquantum dialogue (SQD) [41,42] etc.

In 2016, Chou et al. [43] introduced the concept of semiquantum into quantum private comparison (QPC) and put forward the first semiquantum private comparison (SQPC) protocol by using Bell entangled states and quantum entanglement swapping. In 2018, Thapliyal et al. [44] proposed a SQPC protocol based on Bell entangled states, which needs to share the secret key in advance among different participants by using SQKD and SQKA; Ye et al. [45] designed a SQPC protocol with measure-resend characteristics based on two-particle product states. In 2019, Yan et al. [39] constructed a randomization-based SQPC protocol based on Bell entangled states without pre-shared keys; Lin et al. [46] proposed a SQPC protocol with single photons, which allowed two classical participants to safely compare the equality of their private inputs under the help of an almost dishonest third party (TP); Yan et al. [47] put forward a SQPC scheme based on Greenberger-Horne-Zeilinger (GHZ) class states. In 2020, Jiang et al. [48] put forward two SQPC protocols with Bell entangled states, where the first protocol requires the classical users to measure the received particles and the second protocol doesn’t have this requirement. In 2021, Tsai et al. [49] and Xie et al. [50] pointed out that the first SQPC protocol in Ref.[48] has security loopholes. In order to solve these problems, Ref.[49] makes TP share a secret key with each
classical user in advance through SQKD, while Ref.[50] increases the quantum measurement capability for two classical users. In the same year, Yan et al. [51] put forward a SQPC protocol with three-particle G-like states; Ye et al. [52] proposed an efficient circular SQPC protocol based on single-particle states without using pre-shared key; Sun et al. [53] suggested a novel measure-resend SQPC scheme with pre-shared keys by using Bell entangled states. Note that each of the SQPC protocols in Refs.[43,44,48-50,53] needs to employ four kinds of Bell entangled states as initial quantum resource.

According to the above analysis, in this paper, in order to cut down the usage of initial quantum resource and quantum operations for Bell entangled states based SQPC, we propose a novel SQPC protocol based on single kind of Bell entangled states, which utilizes the entanglement correlation of Bell entangled states to skillfully compare the equality of two classical users’ private inputs. Compared with most of the existing SQPC protocol with Bell entangled states, our protocol is much easier to implement in practice, due to the following advantages: firstly, it only adopts one kind of Bell entangled states as initial quantum resource; secondly, it needn’t share private keys among different participants beforehand; and thirdly, it doesn’t need to employ quantum entanglement swapping.

The left parts of this paper are arranged as follows: Section 2 depicts the steps of the proposed single-state SQPC protocol based on single kind of Bell entangled states; Section 3 conducts the correctness analysis; Section 4 validates its security in detail; and finally, Section 5 gives the discussions and conclusions.

2 Protocol description

Suppose that Alice (Bob), who only possesses limited quantum capabilities, has a private message $M_A$ ($M_B$), where $M_A = \{M_A^1, M_A^2, \ldots, M_A^m\}$ ($M_B = \{M_B^1, M_B^2, \ldots, M_B^m\}$), $M_A^i \in \{0,1\}$ ($M_B^i \in \{0,1\}$), $i = 0,1,\ldots,m$. Alice and Bob want to know whether $M_A$ and $M_B$ are equal or not under the help of TP who possesses full quantum capabilities. According to Ref.[54], here, TP is assumed to be semi-honest, which means that she is allowed to misbehave on her own but cannot conspire with anyone else. In order to compare the equality of $M_A$ and $M_B$ securely without disclosing their genuine contents, Alice and Bob calculate the one-way hash function values of $M_A$ and $M_B$ to obtain $h(M_A)$ and $h(M_B)$ beforehand, respectively. Here, the one-way hash function $h(\cdot)$ can turn $\{0,1\}^m$ into $\{0,1\}^n$, where $m$ represents the length of the input bit string and $n$ denotes the length of the output bit string. With respect to initial quantum resource, we try to accomplish the above goal by using as few kinds of quantum states as possible. The proposed single-state SQPC protocol based on Bell entangled states can be depicted as follows, whose flow chart is shown in
Step 1: TP prepared \( N = 16n \) Bell entangled states all in the state of \( \left| \psi^+ \right\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \). Then, she divides the first particles and the second particles of the first \( 4n \) Bell entangled states into sequences \( T_1 \) and \( T_2 \), respectively. Similarly, she makes the two particles of the second \( 4n \) Bell entangled states to form sequences \( T_3 \) and \( T_4 \), respectively, and lets the two particles of the last \( 8n \) Bell entangled states to compose sequences \( T_5 \) and \( T_6 \), respectively. Finally, TP transmits the particles of sequence \( T_1 \) (or \( T_3 \)) to Alice (Bob) one by one. Note that after TP sends the first particle to Alice (Bob), she sends a particle only after receiving the previous one.

Step 2: After receiving each particle from TP, Alice (Bob) randomly selects one of the following two operations: measuring the received particle with the \( Z \) basis (i.e., \( \{ 0 \}, \{ 1 \} \)) and resending a fresh one to TP in the same state to the measurement result (this is called as the MEASURE mode); and returning the received particle to TP directly (this is called as the REFLECT mode). Alice (Bob) records the measurement results of corresponding particles in \( T_1 \) (or \( T_3 \)) which she (he) chose to MEASURE.

Step 3: TP and Alice (Bob) cooperate together to check the transmission security of \( T_1 \) (or \( T_3 \)). Alice (Bob) tells TP the positions where she (he) chose to REFLECT. TP performs different operations on the received particles according to Alice’s (Bob’s) choices, as illustrated in Table 1.

For checking the error rate on the \( 2n \) REFLECT particles in \( T_1 \) (or \( T_3 \)), TP compares her Bell basis measurement results with her initial prepared states. Apparently, if there exists no Eve, TP’s measurement results should always be \( \left| \psi^+ \right\rangle \).
For checking the error rate on the $2n$ MEASURE particles in $T_3(T_3)$, TP randomly chooses $n$ ones among them, tells Alice (Bob) the chosen positions and requires Alice (Bob) to inform her of the corresponding measurement results. TP calculates the error rate by comparing her measurement results on them, her measurement results on the corresponding $n$ particles in $T_4(T_4)$ and Alice’s (Bob’s) measurement results on them. Apparently, if there exists no Eve, these three kinds of measurement results should be perfectly correlated.

If either the error rate on the REFLECT particles or the error rate on the MEASURE particles in $T_3(T_3)$ is unreasonably high, the protocol will be halted; otherwise, the protocol will be continued.

| Case | Alice (Bob) | TP |
|------|-------------|----|
| 1    | REFLECT    | Action 1 |
| 2    | MEASURE    | Action 2 |

- **Action 1**: TP performs the Bell basis measurements on the REFLECT particles in $T_3(T_3)$ and the corresponding particles in $T_4(T_4)$.
- **Action 2**: TP uses the $Z$ basis to measure the MEASURE particles in $T_3(T_3)$ and the corresponding particles in $T_4(T_4)$, respectively.

Step 4: TP drops out the $3n$ particles in $T_4(T_4)$ used for security check in Step 3. TP’s measurement results on the remaining $n$ particles in $T_4(T_4)$ are represented as $S_2 = \{S_2^1, S_2^2, \ldots, S_2^n\}$ ($S_4 = \{S_4^1, S_4^2, \ldots, S_4^n\}$). Alice’s (Bob’s) measurement results on these $n$ particles in $T_3(T_3)$ are represented as $S_1 = \{S_1^1, S_1^2, \ldots, S_1^n\}$ ($S_3 = \{S_3^1, S_3^2, \ldots, S_3^n\}$).

Step 5: TP transmits the particles of sequence $T_5(T_6)$ to Alice (Bob) one by one. Note that after TP sends the first particle to Alice (Bob), she sends a particle only after receiving the previous one.

After receiving each particle from TP, Alice (Bob) randomly selects one of the two operations, MEASURE and REFLECT. Then, Alice (Bob) tells TP the positions where she (he) chose to REFLECT. According to the choices of Alice and Bob, TP performs different operations on the received particles, as illustrated in Table 2. Case ①, Case ② and Case ③ are used for checking whether the transmissions of $T_5$ and $T_6$ are secure or not; and Case ④ is used for both the security check of the transmissions of $T_5$ and $T_6$ but also privacy comparison.

For the $2n$ positions where Case ① happens, TP compares her Bell basis measurement results with her initial prepared states. Apparently, if there exists no Eve, TP’s measurement results should always be $|\psi^+\rangle$.

For the $2n$ positions where Case ② happens, TP compares her $Z$ basis measurement results with Alice’s $Z$ basis measurement results. Apparently, if there exists no Eve, TP’s $Z$ basis
measurement results should always be opposite to Alice’s Z basis measurement results.

For the \(2n\) positions where Case ③ happens, TP compares her Z basis measurement results with Bob’s Z basis measurement results. Apparently, if there exists no Eve, TP’s Z basis measurement results should always be opposite to Bob’s Z basis measurement results.

For the \(2n\) positions where Case ④ happens, TP randomly chooses \(n\) ones among them, and tells Alice (Bob) the chosen positions. TP calculates the error rate by comparing her measurement results for the chosen positions and Alice’s (Bob’s) measurement results on them. Apparently, if there exists no Eve, these two kinds of measurement results should be identical.

If either of the error rates of Case ①, Case ②, Case ③ and Case ④ is unreasonably high, the protocol will be halted; otherwise, the protocol will be continued.

| Case | Alice  | Bob   | TP          |
|------|--------|-------|-------------|
| ①   | REFLECT| REFLECT| Action 1*   |
| ②   | MEASURE| REFLECT| Action 2*   |
| ③   | REFLECT| MEASURE| Action 3*   |
| ④   | MEASURE| MEASURE| Action 4*   |

Table 2  Alice’s actions on the particles in \(T_5\), Bob’s actions on the particles in \(T_6\) and TP’s corresponding actions

Action 1*: TP employs the Bell basis to measure the received particles in \(T_5\) and the corresponding received particles in \(T_6\);

Action 2*: TP measures the received particles in \(T_6\) with the Z basis, and requires Alice to inform her of the measurement results of corresponding particles in \(T_5\);

Action 3*: TP measures the received particles in \(T_5\) with the Z basis, and requires Bob to inform her of the measurement results of corresponding particles in \(T_6\);

Action 4*: TP measures the received particles in \(T_5\) (\(T_6\)) with the Z basis, and requires Alice (Bob) to inform her of the measurement results of particles in \(T_5\) (\(T_6\)).

Step 6: Alice (Bob) drops out the \(7n\) particles in \(T_5\) (\(T_6\)) used for security check in Step 5. In Case ④, Alice’s (Bob’s) measurement results on the remaining \(n\) particles in \(T_5\) (\(T_6\)), which are not used for security check, are represented as \(S_{\epsilon} = \{S_1 = S_{\epsilon}^1, S_2 = S_{\epsilon}^2, \ldots, S_n = S_{\epsilon}^n\}\) (\(S_{\epsilon} = \{S_{\epsilon}^1, S_{\epsilon}^2, \ldots, S_{\epsilon}^n\}\)). Alice (Bob) calculates \(R_{\epsilon} = h(M_A) \otimes S_{\epsilon}^1 \oplus S_{\epsilon}^j\) (\(R_{\epsilon} = h(M_B) \otimes S_{\epsilon}^j \oplus S_{\epsilon}^2\)), where \(\otimes\) is the bitwise XOR operation and \(j = 1, 2, \ldots, n\). Then, Alice (Bob) sends \(R_A\) (\(R_B\)) to TP, where \(R_A = \{R_{\epsilon}^1, R_{\epsilon}^2, \ldots, R_{\epsilon}^n\}\) (\(R_B = \{R_{\epsilon}^1, R_{\epsilon}^2, \ldots, R_{\epsilon}^n\}\)).

Step 7: After receiving \(R_A\) and \(R_B\), TP compute \(R_j = R_{\epsilon}^1 \oplus R_{\epsilon}^2 \oplus S_j^1 \oplus S_j^2\), where \(j = 1, 2, \ldots, n\).

Once \(R_j = 0\) is found, TP terminates the protocol, and tells Alice and Bob that \(M_A\) is not identical.
to $M_B$. Otherwise, TP tells Alice and Bob that $M_A$ is same to $M_B$.

3 Correctness analysis

In the proposed SQPC protocol, Alice and Bob's secret messages are $M_A = \{M_A^1, M_A^2, \ldots, M_A^m\}$ and $M_B = \{M_B^1, M_B^2, \ldots, M_B^m\}$, respectively; Alice and Bob intent to judge the equality of $M_A$ and $M_B$ with the help of a semi-honest TP. In order to protect the genuine contents of $M_A$ and $M_B$, the proposed protocol compares their hash values, $h(M_A)$ and $h(M_B)$, where $h(M_A) = [h^1(M_A) h^2(M_A) \ldots h^n(M_A)]$, $h(M_B) = [h^1(M_B) h^2(M_B) \ldots h^n(M_B)]$. Apparently, as the initial states prepared by TP are always in the state of $|\psi^+\rangle$, we have $S_i^j \oplus S_i^j = 1, S_i^j \oplus S_i^j = 1$ and $S_i^j \oplus S_i^j = 1, j = 1, 2, \ldots, n$. Because $R_i^j = h^i(M_A) \oplus S_i^j \oplus S_i^j$ and $R_i^j = h^i(M_B) \oplus S_i^j \oplus S_i^j$, it can be obtained that

$$R_i^j = R_i^j \oplus R_i^j \oplus S_i^j \oplus S_i^j$$
$$= [h^i(M_A) \oplus S_i^j \oplus S_i^j] \oplus [h^i(M_B) \oplus S_i^j \oplus S_i^j] \oplus S_i^j \oplus S_i^j$$
$$= h^i(M_A) \oplus h^i(M_B) \oplus 1. \quad (1)$$

According to Eq.(1), $R_i^j = 0$ indicates that $h^i(M_A) = h^i(M_B)$. Therefore, only when $R_i^j = 1$ stands for $j = 1, 2, \ldots, n$ can we have $M_A = M_B$.

4 Security analysis

4.1 Outside attack

In the proposed SQPC protocol, TP sends $T_1( T_3 )$ to Alice (Bob) firstly, and then transmits $T_5$ and $T_6$ to Alice and Bob, respectively. As a result, an external eavesdropper, Eve, may try her best to obtain something useful during each transmission by launching some well-known attacks, such as the intercept-resend attack, the measure-resend attack and the entangle-measure attack, and so on. For clarity, we firstly analyze the security of transmission of $T_1( T_3 )$, and then validate the security of transmissions of $T_5$ and $T_6$.

Case 1: Eve attacks $T_1( T_3 )$ when it goes from TP to Alice (Bob)

In the proposed SQPC protocol, $T_1$, which is independent from $T_3$, essentially plays the same role to $T_3$. Thus, for simplicity, we only analyze the transmission security of $T_1$ from TP to Alice and back to TP.

(1) The intercept-resend attack
During the transmission of $T_1$ from TP to Alice and back to TP, Eve may try her best to obtain $S_1$ by launching the following attack: Eve may intercept the particles of $T_1$ from TP to Alice, and sends the fake particles she generated in the $Z$ basis beforehand to Alice. However, Eve will be inevitably detected due to the following two reasons: on one hand, the fake particles she prepared beforehand may be different from the genuine ones in $T_1$; and on the other hand, she does not know Alice’s operations, which are random in fact. Concretely speaking, when TP sends one particle of $T_1$ to Alice, Eve intercepts it and sends the prepared fake one to Alice. Without loss of generality, assume that the fake one prepared by herself is in the state of $|0\rangle$. As a result, if Alice chooses to MEASURE, her measurement result will be $|0\rangle$. After Alice tells TP her operation, TP uses the $Z$ basis to measure the corresponding particle in $T_2$ and obtains the measurement result randomly in one of the two states $|0\rangle$ and $|1\rangle$. Hence, if Alice chooses to MEASURE, Eve will be detected with the probability of $\frac{1}{2}$. If Alice chooses to REFLECT, TP will receive the fake particle.

After Alice tells TP her operation, TP measures the fake particle and the corresponding particle in $T_2$ with the Bell basis, and obtains the measurement result randomly in one of the four states $|\psi^-\rangle$, $|\phi^-\rangle$ and $|\phi^+\rangle$, where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. Hence, if Alice chooses to REFLECT, Eve will be detected with the probability of $\frac{3}{4}$. To sum up, when Eve launches this kind of attack on one particle of $T_1$, the probability that she will be discovered is $\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}$.

(2) The measure-resend attack

In order to obtain $S_1$, Eve may intercept the particles of $T_1$ sent from TP to Alice, measure them with the $Z$ basis and send the resulted states to Alice. However, this kind of attack from Eve will be inevitably discovered as Alice’s operations are random. Concretely speaking, after Eve’s measurement, the particle Eve sends to Alice is randomly in one of the two states $|0\rangle$ and $|1\rangle$.

Without loss of generality, assume that the particle after Eve’s measurement is in the state of $|0\rangle$. If Alice chooses to MEASURE, after she tells TP her operation, TP uses the $Z$ basis to measure the corresponding particle in $T_2$ and obtains the measurement result $|1\rangle$. Hence, if Alice chooses to MEASURE, Eve will be detected with the probability of 0. If Alice chooses to REFLECT, after she tells TP her operation, TP measures the received particle from Alice and the corresponding particle in $T_2$ with the Bell basis, and obtains the measurement result randomly in one of the two
states $|\psi^+\rangle$ and $|\psi^-\rangle$. Hence, if Alice chooses to REFLECT, Eve will be detected with the probability of $\frac{1}{2}$. To sum up, when Eve launches this kind of attack on one particle of $T_1$, the probability that she will be discovered is $\frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$.

(3) The entangle-measure attack

Eve may try to obtain something useful by entangling her auxiliary qubit with the transmitted qubit. Eve’s entangle-measure attack can be modeled with two unitary operations $\hat{E}$ and $\hat{F}$, where $\hat{E}$ attacks the qubit sent from TP to Alice, and $\hat{F}$ attacks the qubit returned from Alice to TP. Moreover, $\hat{E}$ and $\hat{F}$ share a common probe space with the initial state $|\epsilon\rangle_E$. Just as pointed out in Refs.[29,30], the shared probe permits Eve to attack the returned particles depending on the knowledge obtained from $\hat{E}$ (if Eve does not take advantage of this, the ‘shared probe’ can simply be regarded as the composite system comprised of two independent probes). Any attack where Eve would make $\hat{F}$ depend on a measurement after performing $\hat{E}$ can be realized by $\hat{E}$ and $\hat{F}$ with controlled gates. Eve’s entangle-measure attack on the particles of $T_1$ within the implementation of the protocol can be depicted as Fig.2.

![Fig.2](image)

Fig.2  Eve’s entangle-measure attack on the particles of $T_1$ with two unitaries $\hat{E}$ and $\hat{F}$

**Theorem 1.** Suppose that Eve performs attack $\{\hat{E}, \hat{F}\}$ on the particle from TP to Alice and back to TP. For this attack inducing no error in Step 3, the final state of Eve’s probe should be independent of not only Alice’s operation but also TP and Alice’s measurement results. As a result, Eve gets no information on the bits of $S_1$ and $S_2$.

**Proof.** The effect of $\hat{E}$ on the qubits $|0\rangle$ and $|1\rangle$ can be expressed as

$$\hat{E}(|0\rangle|\epsilon\rangle_E) = a_{00}|0\rangle|\epsilon_{00}\rangle + a_{01}|1\rangle|\epsilon_{01}\rangle,$$

(2)
\[ E(\hat{\psi}_{12}^+|\psi_E^+) = \alpha_{10}|0\rangle_2|\epsilon_{10}\rangle + \alpha_{11}|1\rangle_2|\epsilon_{11}\rangle, \quad (3) \]

where \(|\epsilon_{00}\rangle, |\epsilon_{01}\rangle, |\epsilon_{10}\rangle\) and \(|\epsilon_{11}\rangle\) are Eve’s probe states determined by \(E^+|\epsilon_{00}\rangle^2 + |\epsilon_{01}\rangle^2 = 1\) and \( |\epsilon_{10}\rangle^2 + |\epsilon_{11}\rangle^2 = 1\).

According to Stinespring dilation theorem, the global state of the composite system before Alice’s operation is

\[
\begin{bmatrix}
|\epsilon_{00}\rangle_1|\epsilon_{00}\rangle_2 + |\epsilon_{01}\rangle_1|\epsilon_{01}\rangle_2 + (|\epsilon_{10}\rangle_1|\epsilon_{10}\rangle_2 + |\epsilon_{11}\rangle_1|\epsilon_{11}\rangle_2)
\end{bmatrix} = \begin{bmatrix}
0_1\langle 0 |_{12} |\epsilon_{00}\rangle + \alpha_{10} |0_1\langle 0 |_{12} |\epsilon_{01}\rangle + \alpha_{11} |0_1\langle 0 |_{12} |\epsilon_{10}\rangle + \alpha_{11} |0_1\langle 0 |_{12} |\epsilon_{11}\rangle
\end{bmatrix},
\]

(4)

where the subscripts 1 and 2 represent the particles from \(T_1\) and \(T_2\), respectively.

(i) Firstly, consider the case that Alice chooses to MEASURE. As a result, the state of the composite system is collapsed into

\[ |0_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle) \]

if Alice’s measurement result is \(|0_1\rangle_1\); or

\[ |1_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle) \]

if Alice’s measurement result is \(|1_1\rangle_1\).

Eve imposes \(\hat{F}\) on the particle sent back to TP. In order that Eve’s attacks on the MEASURE particle will not be discovered by TP and Alice in Step 3, the global state of the composite system should be

\[ \hat{F}\left[ |0_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle) \right] = |0_1\rangle_1|0_2\rangle_2|\epsilon_{00}\rangle, \quad (5) \]

if Alice’s measurement result is \(|0_1\rangle_1\); or

\[ \hat{F}\left[ |1_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle) \right] = |1_1\rangle_1|0_2\rangle_2|\epsilon_{01}\rangle. \quad (6) \]

(ii) Secondly, consider the case that Alice chooses to REFLECT. As a result, the state of the composite system is

\[ \frac{1}{\sqrt{2}} \left[ |0_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{11}\rangle) \right]. \]

Eve imposes \(\hat{F}\) on the particle sent back to TP. According to Eq.(5) and Eq.(6), it has

\[ \hat{F}\left[ E\left(\hat{\psi}_{12}^+|\psi_E^+\right) \right] = \frac{1}{\sqrt{2}} \hat{F}\left[ |0_1\rangle_1(0_1|0_2|\epsilon_{00}\rangle + \alpha_{10}|0_1\langle 0_2|\epsilon_{01}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{10}\rangle + \alpha_{11}|0_1\langle 0_2|\epsilon_{11}\rangle) \right] \]

\[ = \frac{1}{\sqrt{2}} \left[ |0_1\rangle_1|0_2\rangle_2|\epsilon_{00}\rangle + |1_1\rangle_1|0_2\rangle_2|\epsilon_{01}\rangle \right] \]

\[ = \frac{1}{2} \left[ |\psi^+\rangle_{12} + |\psi^-\rangle_{12} |\epsilon_{00}\rangle + \left( |\psi^+\rangle_{12} - |\psi^-\rangle_{12} \right) |\epsilon_{11}\rangle \right] \]
\[
\frac{1}{2} \left[ |\psi^+\rangle_{12} (|\varepsilon_0\rangle + |\varepsilon_1\rangle) + |\psi^-\rangle_{12} (|\varepsilon_0\rangle - |\varepsilon_1\rangle) \right].
\]  
(7)

In order that Eve’s attacks on the REFLECT particle will not be discovered by TP and Alice in Step 3, the probability of TP measuring a pair of particles in \(T_1\) and \(T_2\) in the result \(|\psi^+\rangle_{12}\) should be 1. Thus, it should establish

\[
|\varepsilon_0\rangle = |\varepsilon_1\rangle = |\varepsilon\rangle. 
\]  
(8)

Inserting Eq.(8) into Eq.(7) produces

\[
\hat{F} \left( \hat{E} \left( |\psi^+\rangle_{12} |\varepsilon\rangle_E \right) \right) = |\psi^+\rangle_{12} |\varepsilon\rangle. 
\]  
(9)

(iii) Inserting Eq.(8) into Eq.(5) and Eq.(6) produces

\[
\hat{F} \left[ \hat{F} \left( |0\rangle_1 (\alpha_{00} |0\rangle_2 |\varepsilon_{00}\rangle + \alpha_{01} |0\rangle_2 |\varepsilon_{01}\rangle) \right) \right] = |0\rangle_1 |1\rangle_2 |\varepsilon\rangle, 
\]  
(10)

and

\[
\hat{F} \left[ \hat{F} \left( |1\rangle_1 (\alpha_{01} |1\rangle_2 |\varepsilon_{01}\rangle + \alpha_{11} |1\rangle_2 |\varepsilon_{11}\rangle) \right) \right] = |1\rangle_1 |0\rangle_2 |\varepsilon\rangle, 
\]  
(11)

respectively.

According to Eq.(9), Eq.(10) and Eq.(11), in order not to be detected by TP and Alice, the final state of Eve’s probe should be independent from not only Alice’s operation but also the TP and Alice’s measurement results. As a result, Eve gets no information on the bits of \(S_1\) and \(S_2\).

(4) The Trojan horse attack

Because the particles of \(T_1\) are transmitted forth and back between TP and Alice, the Trojan horse attack from Eve should be taken into account. This attack mainly contains two types: the invisible photon eavesdropping attack [55] and the delay-photon Trojan horse attack [56,57]. In order to resist the invisible photon eavesdropping attack, a wavelength filter can be installed by Alice in front of her device to filter out the photon signal with an illegitimate wavelength [57,58]. To defeat the delay-photon Trojan horse attack, Alice needs to employ a photon number splitter (PNS: 50/50) to split each sample signal into two parts and measure the resulted signals with the correct measuring bases [57,58]. If the multiphoton rate is abnormally high, this attack will be detected.

Case 2: Eve attacks \(T_5\) and \(T_6\) when they go from TP to Alice and Bob

(1) The intercept-resend attack

In Step 5, TP transmits \(T_5\) and \(T_6\) to Alice and Bob, respectively. During these transmissions, Eve may try her best to obtain \(S_5\) and \(S_6\) by launching the following attack: Eve intercepts the two particles sent from TP to Alice and Bob, and sends two fake ones she prepared in the \(Z\) basis beforehand to Alice and Bob, respectively. However, Eve will be undoubtedly discovered for two facts: firstly, the fake particles she prepared beforehand may be different from the genuine ones in
$T_5$ and $T_6$; and secondly, Alice and Bob’s operations are random. Concretely speaking, when TP sends one particle of $T_5$ to Alice and one particle of $T_6$ to Bob, Eve intercepts them and sends the prepared fake ones to Alice and Bob, respectively. Firstly, assume that the two fake particles prepared by Eve are in the state of $|0\rangle|0\rangle (|1\rangle|1\rangle)$. As a result, if both Alice and Bob choose to REFLECT, TP will receive the two fake particles $|0\rangle|0\rangle (|1\rangle|1\rangle)$. After Alice and Bob tell TP their operations, TP measures the two fake particles $|0\rangle|0\rangle (|1\rangle|1\rangle)$ with the Bell basis, and obtains the measurement result randomly in one of the two states $|\psi^+\rangle$ and $|\psi^-\rangle$. Hence, if both Alice and Bob choose to REFLECT, Eve will be detected with the probability of 1. If Alice chooses to MEASURE and Bob chooses to REFLECT, after Alice and Bob tell TP their operations, TP will measure the fake particle $|0\rangle (|1\rangle)$ reflected by Bob with the $Z$ basis and require Alice to inform her of her measurement result. Hence, if Alice chooses to MEASURE and Bob chooses to REFLECT, Eve will be detected with the probability of 1. Similarly, if Alice chooses to REFLECT and Bob chooses to MEASURE, Eve will be also detected with the probability of 1. If both Alice and Bob choose to MEASURE, after Alice and Bob tell TP their operations, TP will measure the received particles with the $Z$ basis and obtain the result $|0\rangle|0\rangle (|1\rangle|1\rangle)$. So, if both Alice and Bob choose to MEASURE, Eve will be detected with the probability of 1. To sum up, when the two fake particles prepared by Eve are in the state of $|0\rangle|0\rangle (|1\rangle|1\rangle)$, Eve is detected with the probability of $\frac{\frac{1}{4} \times 1 + \frac{1}{4} \times 1 + \frac{1}{4} \times 1 + \frac{1}{4} \times 1 = 1}{1}$. Secondly, assume that the two fake particles prepared by Eve are in the state of $|0\rangle|1\rangle (|1\rangle|0\rangle)$. As a result, if both Alice and Bob choose to REFLECT, TP will receive the two fake particles $|0\rangle|1\rangle (|1\rangle|0\rangle)$. After Alice and Bob tell TP their operations, TP measures the two fake particles $|0\rangle|1\rangle (|1\rangle|0\rangle)$ with the Bell basis, and obtains the measurement result randomly in one of the two states $|\psi^+\rangle$ and $|\psi^-\rangle$. Hence, if both Alice and Bob choose to REFLECT, Eve will be detected with the probability of $\frac{1}{2}$. If Alice chooses to MEASURE and Bob chooses to REFLECT, after Alice and Bob tell TP their operations, TP will measure the fake particle $|1\rangle (|0\rangle)$ reflected by Bob with the $Z$ basis and require Alice to inform her of her measurement result. Hence, if Alice chooses to MEASURE and Bob chooses to REFLECT, Eve will be detected with the probability of 0. Similarly, if Alice chooses to REFLECT and Bob chooses to MEASURE, Eve
will be also detected with the probability of 0. If both Alice and Bob choose to MEASURE, after Alice and Bob tell TP their operations, TP will measure the received particles with the Z basis and obtain the result \( |0\rangle |1\rangle (|1\rangle |0\rangle) \). In this case, Eve will be detected with the probability of 0. To sum up, when the two fake particles prepared by TP are in the state of \( |0\rangle |1\rangle (|1\rangle |0\rangle) \), Eve is detected with the probability of 0. To sum up, when the two fake particles prepared by TP are in the state of \( |0\rangle |1\rangle (|1\rangle |0\rangle) \), Eve is detected with the probability of 0. To sum up, when the two fake particles prepared by TP are in the state of \( |0\rangle |1\rangle (|1\rangle |0\rangle) \), Eve is detected with the probability of 0.

(2) The measure-resend attack

In order to obtain \( S_2 (S_6) \), Eve may intercept the particles of \( T_5 (T_6) \) sent from TP to Alice (Bob), measure them with the Z basis and send the resulted states to Alice (Bob). However, this kind of attack from Eve will be detected undoubtedly as Alice and Bob’s operations are random. Concretely speaking, after Eve’s measurement, the Bell state prepared by TP is collapsed randomly into one of the two states \( |01\rangle \) and \( |10\rangle \). Without loss of generality, assume that the Bell state from TP after Eve’s measurement is collapsed into \( |01\rangle \). If both Alice and Bob choose to REFLECT, after Alice and Bob tell TP their operations, TP will measure the particles \( |01\rangle \) with the Bell basis and obtain \( \psi^+ \) or \( \psi^- \) with equal probability. As a result, if both Alice and Bob choose to REFLECT, Eve will be detected with the probability of \( \frac{1}{2} \). If Alice chooses to MEASURE and Bob chooses to REFLECT, after Alice and Bob tell TP their operations, TP will measure the particle \( |1\rangle \) reflected by Bob with the Z basis and require Alice to inform her of her measurement result. Hence, if Alice chooses to MEASURE and Bob chooses to REFLECT, Eve will be detected with the probability of 0. Similarly, if Alice chooses to REFLECT and Bob chooses to MEASURE, Eve will be also discovered with the probability of 0. If both Alice and Bob choose to MEASURE, after Alice and Bob tell TP their operations, TP will measure the received particles with the Z basis. Therefore, if both Alice and Bob choose to MEASURE, Eve will be detected with the probability of 0. To sum up, when Eve launches this kind of attack on one particle of \( T_5 \) and one particle of \( T_6 \), the probability that she will be discovered is

\[
\frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times 0 + \frac{1}{4} \times 0 + \frac{1}{4} \times 0 = \frac{1}{8}.
\]

(3) The entangle-measure attack

Eve’s entangle-measure attack on the particles of \( T_5 \) and \( T_6 \) can be modeled as two unitaries: \( U_E \) attacking particles from TP to Alice and Bob and \( U_F \) attacking particles back from Alice and Bob to TP, where \( U_E \) and \( U_F \) share a common probe space with initial state \( |\xi\rangle \). As pointed out in
Refs.\cite{29,30}, the shared probe permits Eve to attack the returned particles relying on the knowledge obtained by $U_E$ (if Eve does not utilize this fact, the ‘shared probe’ can simply be considered as the composite system composed by two independent probes). Any attack where Eve would make $U_F$ rely on a measurement after implementing $U_E$ can be accomplished by $U_E$ and $U_F$ with controlled gates. Eve’s entangle-measure attack on the particles of $T_5$ and $T_6$ within the implementation of the protocol can be described as Fig. 3.

![Diagram](image_url)

**Fig. 3**  Eve’s entangle-measure attack on the particles of $T_5$ and $T_6$ with two unitaries $U_E$ and $U_F$

**Theorem 2.** Suppose that Eve performs attack $(U_E, U_F)$ on the particles from TP to Alice and Bob and back to TP. For this attack inducing no error in Step 5, the final state of Eve’s probe should be independent of not only Alice and Bob’s operations but also their measurement results. As a result, Eve gets no information on the bits of $S_5$ and $S_6$.

**Proof.** The effect of $U_E$ on the qubits $\ket{0}$ and $\ket{1}$ can be expressed as

\[
U_E \left( \begin{array}{c} \beta_0 \ket{0} + \beta_1 \ket{1} \\ \xi_E \end{array} \right) = \beta_0 \ket{0} \xi_0 + \beta_1 \ket{1} \xi_1 ,
\]

(12)

\[
U_E \left( \begin{array}{c} \beta_{00} \ket{0} + \beta_{01} \ket{1} \\ \xi_E \end{array} \right) = \beta_{00} \ket{0} \xi_{00} + \beta_{01} \ket{1} \xi_{01} ,
\]

(13)

where $\ket{\xi_0}$, $\ket{\xi_1}$, $\ket{\xi_{00}}$ and $\ket{\xi_{01}}$ are Eve’s probe states determined by $U_E$, $|\beta_{00}|^2 + |\beta_{01}|^2 = 1$ and $|\beta_{10}|^2 + |\beta_{11}|^2 = 1$.

According to Stinespring dilation theorem, the global state of the composite system before Alice and Bob’s operations is

\[
U_E \left( \begin{array}{c} \beta_{00} \ket{0} + \beta_{01} \ket{1} \\ \xi_E \end{array} \right) = U_E \left[ \frac{1}{\sqrt{2}} \left( \ket{0} \ket{\xi_0} + \ket{1} \ket{\xi_1} \right) \right]
\]

\[
= \frac{1}{\sqrt{2}} \left( \beta_{00} \ket{0} \xi_{00} + \beta_{01} \ket{1} \xi_{01} \right) \left( \beta_{10} \ket{0} \xi_{10} + \beta_{11} \ket{1} \xi_{11} \right)
\]

\[
+ \left( \beta_{00} \ket{0} \xi_{00} + \beta_{01} \ket{1} \xi_{01} \right) \left( \beta_{10} \ket{0} \xi_{10} + \beta_{11} \ket{1} \xi_{11} \right)
\]

\[
+ \left( \beta_{00} \ket{0} \xi_{00} + \beta_{01} \ket{1} \xi_{01} \right) \left( \beta_{10} \ket{0} \xi_{10} + \beta_{11} \ket{1} \xi_{11} \right)
\]

14
\[
\frac{1}{\sqrt{2}} \left[ |0\rangle_5 |0\rangle_6 (\beta_{00} \beta_{10} |\tilde{\xi}_{00}\rangle |\tilde{\xi}_{10}\rangle + \beta_{10} \beta_{00} |\tilde{\xi}_{10}\rangle |\tilde{\xi}_{00}\rangle) \\
+ |0\rangle_5 |1\rangle_6 (\beta_{00} \beta_{11} |\tilde{\xi}_{00}\rangle |\tilde{\xi}_{11}\rangle + \beta_{11} \beta_{00} |\tilde{\xi}_{11}\rangle |\tilde{\xi}_{00}\rangle) \\
+ |1\rangle_5 |0\rangle_6 (\beta_{01} \beta_{10} |\tilde{\xi}_{01}\rangle |\tilde{\xi}_{10}\rangle + \beta_{10} \beta_{01} |\tilde{\xi}_{10}\rangle |\tilde{\xi}_{01}\rangle) \\
+ |1\rangle_5 |1\rangle_6 (\beta_{01} \beta_{11} |\tilde{\xi}_{01}\rangle |\tilde{\xi}_{11}\rangle + \beta_{11} \beta_{01} |\tilde{\xi}_{11}\rangle |\tilde{\xi}_{01}\rangle) \right]
= |0\rangle_5 |0\rangle_6 |\theta_{00}\rangle + |0\rangle_5 |1\rangle_6 |\theta_{01}\rangle + |1\rangle_5 |0\rangle_6 |\theta_{10}\rangle + |1\rangle_5 |1\rangle_6 |\theta_{11}\rangle.
\]

where the subscripts 5 and 6 represent the particles from $T_5$ and $T_6$, respectively, and

\[
|\theta_{00}\rangle = \frac{1}{\sqrt{2}} (\beta_{00} \beta_{10} |\tilde{\xi}_{00}\rangle |\tilde{\xi}_{10}\rangle + \beta_{10} \beta_{00} |\tilde{\xi}_{10}\rangle |\tilde{\xi}_{00}\rangle),
\]

\[
|\theta_{01}\rangle = \frac{1}{\sqrt{2}} (\beta_{00} \beta_{11} |\tilde{\xi}_{00}\rangle |\tilde{\xi}_{11}\rangle + \beta_{11} \beta_{00} |\tilde{\xi}_{11}\rangle |\tilde{\xi}_{00}\rangle),
\]

\[
|\theta_{10}\rangle = \frac{1}{\sqrt{2}} (\beta_{01} \beta_{10} |\tilde{\xi}_{01}\rangle |\tilde{\xi}_{10}\rangle + \beta_{10} \beta_{01} |\tilde{\xi}_{10}\rangle |\tilde{\xi}_{01}\rangle),
\]

\[
|\theta_{11}\rangle = \frac{1}{\sqrt{2}} (\beta_{01} \beta_{11} |\tilde{\xi}_{01}\rangle |\tilde{\xi}_{11}\rangle + \beta_{11} \beta_{01} |\tilde{\xi}_{11}\rangle |\tilde{\xi}_{01}\rangle).
\]

When Alice and Bob receive the particles from TP, they choose either to MEASURE or to REFLECT. After that, Eve performs $U_F$ on the particles sent back to TP.

(i) Firstly, consider the case that both Alice and Bob choose to MEASURE. As a result, the state of the composite system is collapsed into $|x\rangle_5 |y\rangle_6 |\theta_{xy}\rangle$, where $x, y \in \{0, 1\}$. For Eve not being detectable in Step 5, $U_F$ should satisfy

\[
U_F \left( |x\rangle_5 |y\rangle_6 |\theta_{xy}\rangle \right) = |x\rangle_5 |y\rangle_6 |\gamma_{xy}\rangle,
\]

which means that $U_F$ cannot alter the state of particles from Alice and Bob. Otherwise, Eve is discovered with a non-zero probability.

(ii) Secondly, consider the case that Alice chooses to MEASURE and Bob chooses to REFLECT. As a result, the state of the composite system is collapsed into $|0\rangle_5 |0\rangle_6 |\theta_{00}\rangle + |0\rangle_5 |1\rangle_6 |\theta_{01}\rangle$ if Alice’s measurement result is $|0\rangle_5$ or $|1\rangle_5 |0\rangle_6 |\theta_{10}\rangle + |1\rangle_5 |1\rangle_6 |\theta_{11}\rangle$ if Alice’s measurement result is $|1\rangle_5$.

Assume that Alice’s measurement result is $|0\rangle_5$. After Eve imposes $U_F$ on the particles sent back to TP, due to Eq.(19), the state of the composite system is evolved into

\[
U_F \left( |0\rangle_5 |0\rangle_6 |\theta_{00}\rangle + |0\rangle_5 |1\rangle_6 |\theta_{01}\rangle \right) = |0\rangle_5 |0\rangle_6 |\gamma_{00}\rangle + |0\rangle_5 |1\rangle_6 |\gamma_{01}\rangle.
\]

For Eve not being detectable in Step 5, the probability of TP measuring the particle reflected by Bob in the result $|0\rangle_6$ should be 0. Hence, it has
\[ |\gamma_{00}\rangle = 0. \]  

On the other hand, assume that Alice’s measurement result is \( |1\rangle_5 \). After Eve imposes \( U_F \) on the particles sent back to TP, due to Eq.(19), the state of the composite system is evolved into

\[ U_F \left( |1\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) = |1\rangle_5 |0\rangle_6 |\gamma_{10}\rangle + |1\rangle_5 |1\rangle_6 |\gamma_{11}\rangle. \]  

For Eve not being detectable in Step 5, the probability of TP measuring the particle reflected by Bob in the result \( |1\rangle_6 \) should be 0. Hence, it has

\[ |\gamma_{11}\rangle = 0. \]  

(iii) Thirdly, consider the case that Alice chooses to REFLECT and Bob chooses to MEASURE. As a result, the state of the composite system is collapsed into

\[ |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle \] if Bob’s measurement result is \( |0\rangle_6 \) or

\[ |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \] if Bob’s measurement result is \( |1\rangle_6 \).

Assume that Bob’s measurement result is \( |0\rangle_6 \). After Eve imposes \( U_F \) on the particles sent back to TP, due to Eq.(19), the state of the composite system is evolved into

\[ U_F \left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle \right) = |0\rangle_5 |0\rangle_6 |\gamma_{00}\rangle + |1\rangle_5 |0\rangle_6 |\gamma_{10}\rangle. \]  

For Eve not being detectable in Step 5, the probability of TP measuring the particle reflected by Alice in the result \( |0\rangle_5 \) should be 0. This automatically stands after Eq.(21) is inserted into Eq.(24).

On the other hand, assume that Bob’s measurement result is \( |1\rangle_6 \). After Eve imposes \( U_F \) on the particles sent back to TP, due to Eq.(19), the state of the composite system is evolved into

\[ U_F \left( |0\rangle_5 |1\rangle_6 |\varphi_{00}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) = |0\rangle_5 |1\rangle_6 |\gamma_{01}\rangle + |1\rangle_5 |1\rangle_6 |\gamma_{11}\rangle. \]  

For Eve not being detectable in Step 5, the probability of TP measuring the particle reflected by Alice in the result \( |1\rangle_5 \) should be 0. This automatically stands after Eq.(23) is inserted into Eq.(25).

(iv) Fourthly, consider the case that both Alice and Bob choose to REFLECT. As a result, the state of the composite system is

\[ |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle. \]  

After Eve imposes \( U_F \) on the particles sent back to TP, due to Eq.(19), the state of the composite system is evolved into

\[ U_F \left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) =

\[ |0\rangle_5 |0\rangle_6 |\gamma_{00}\rangle + |0\rangle_5 |1\rangle_6 |\gamma_{01}\rangle + |1\rangle_5 |0\rangle_6 |\gamma_{10}\rangle + |1\rangle_5 |1\rangle_6 |\gamma_{11}\rangle. \]  

16
After Eq. (21) and Eq. (23) are inserted into Eq. (26), it can be obtained that
\[
U_F\left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right)
\]
\[
= |0\rangle_5 |1\rangle_6 |\gamma_{01}\rangle + |1\rangle_5 |0\rangle_6 |\gamma_{10}\rangle
\]
\[
= \frac{1}{\sqrt{2}}\left( |\psi^+\rangle_{56} + |\psi^-\rangle_{56} \right) |\gamma_{01}\rangle + \frac{1}{\sqrt{2}}\left( |\psi^+\rangle_{56} - |\psi^-\rangle_{56} \right) |\gamma_{10}\rangle
\]
\[
= \frac{1}{\sqrt{2}} |\psi^+\rangle_{56} (|\gamma_{01}\rangle + |\gamma_{10}\rangle) + \frac{1}{\sqrt{2}} |\psi^-\rangle_{56} (|\gamma_{01}\rangle - |\gamma_{10}\rangle). \tag{27}
\]
For Eve not being detectable in Step 5, the probability of TP measuring the particles reflected by Alice and Bob in the result $|\psi^+\rangle_{56}$ should be 1. Therefore, according to Eq. (27), it has
\[
|\gamma_{01}\rangle = |\gamma_{10}\rangle = |\gamma\rangle. \tag{28}
\]
Inserting Eq. (28) into Eq. (27) produces
\[
U_F\left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) = \sqrt{2} |\psi^+\rangle_{56} |\gamma\rangle. \tag{29}
\]
(v) Applying Eq. (28) into Eq. (19) produces
\[
U_F\left( |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle \right) = |0\rangle_5 |1\rangle_6 |\gamma\rangle. \tag{30}
\]
\[
U_F\left( |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle \right) = |1\rangle_5 |0\rangle_6 |\gamma\rangle. \tag{31}
\]
Applying Eq. (21) and Eq. (28) into Eq. (20) produces
\[
U_F\left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle \right) = |0\rangle_5 |1\rangle_6 |\gamma\rangle. \tag{32}
\]
Applying Eq. (23) and Eq. (28) into Eq. (22) produces
\[
U_F\left( |1\rangle_5 |0\rangle_6 |\varphi_{10}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) = |1\rangle_5 |0\rangle_6 |\gamma\rangle. \tag{33}
\]
Applying Eq. (21) and Eq. (28) into Eq. (24) produces
\[
U_F\left( |0\rangle_5 |0\rangle_6 |\varphi_{00}\rangle + |1\rangle_5 |0\rangle_6 |\varphi_{01}\rangle \right) = |1\rangle_5 |0\rangle_6 |\gamma\rangle. \tag{34}
\]
Applying Eq. (23) and Eq. (28) into Eq. (25) produces
\[
U_F\left( |0\rangle_5 |1\rangle_6 |\varphi_{01}\rangle + |1\rangle_5 |1\rangle_6 |\varphi_{11}\rangle \right) = |0\rangle_5 |1\rangle_6 |\gamma\rangle. \tag{35}
\]
According to Eqs. (29-35), it can be concluded that for Eve not inducing an error in Step 5, the final state of Eve’s probe should be independent of not only Alice and Bob’s operations but also their measurement results. As a result, Eve gets no information on the bits of $S_5$ and $S_6$.

(4) The Trojan horse attack

Because the particles of $T_5$ ($T_6$) goes a round trip between TP and Alice (Bob), the Trojan horse attack from Eve should be taken into account. For the sake of overcoming the invisible photon eavesdropping attack, Alice (Bob) can install a wavelength filter in front of her (his) device
to delete the illegal photon signal [57,58]. For the sake of defeating the delay-photon Trojan horse attack, Alice (Bob) can measure the resulted signals with the correct measuring bases after utilizing a photon number splitter (PNS: 50/50) to divide each sample signal into two parts [57,58]. If the multiphoton rate is unreasonably high, this attack will be discovered.

4.2 Participant attack

In 2007, Gao et al. [59] pointed out for the first time that the attack launched by a dishonest participant is always more powerful than that from an outside eavesdropper and should be paid special attention to. With respect to the proposed protocol, we need to consider the participant attack from Alice or Bob and that from the semi-honest TP.

1) The participant attack from Alice or Bob

In the proposed protocol, Alice plays the same role to Bob. Without loss of generality, we only consider the case that Bob, who is supposed to have complete quantum abilities, is dishonest.

In the proposed protocol, Bob naturally knows \(S_3\) and \(S_8\). Moreover, according to the entanglement correlation of two qubits within one Bell entangled state, Bob can deduce \(S_4\) and \(S_5\) from \(S_3\) and \(S_6\), respectively. As \(h(M_A)\) is encrypted with \(S_1\) and \(S_5\), in order to deduce \(h(M_A)\) from \(R_A\), Bob should further know \(S_1\). However, Bob cannot get \(S_1\) by cooperating with TP who knows \(S_2\). In addition, Bob may try his best to get \(S_1\) by launching some active attacks on the particles of \(T_i\). However, he will be inevitably discovered as an external eavesdropper, since Alice’s operations are random, just as analyzed above. In conclusion, Bob has no chance to obtain \(h(M_A)\), let alone \(M_A\).

2) The participant attack from TP

The semi-honest TP may try her best to obtain \(M_A\) and \(M_B\) without colluding with Alice or Bob. In the proposed protocol, TP can know \(S_1, S_2, S_3, S_4, S_5\) and \(S_6\). Hence, TP can easily deduce \(h(M_A)\) and \(h(M_B)\) from \(R_A\) and \(R_B\), respectively. However, TP still cannot know \(M_A\) and \(M_B\), which is guaranteed by the one-way property of hash function.

5 Discussions and conclusions

In this part, we compare the proposed protocol with the existing SQPC protocols based on Bell entangled states in Refs.[39,43,44,48-50,53]. The detailed comparison results are shown in Table 3. Here, the qubit efficiency is defined as [60] \(\eta = \frac{b}{q + c}\), where \(b, q\) and \(c\) represent the number of compared private bits, the number of consumed qubits and the number of classical bits involved in classical communication, respectively. Note that the classical resources required for eavesdropping detection are not considered here.

In our protocol, Alice and Bob successfully compare their respective \(n\) bits of hash values, so it has \(b = n\). TP needs to prepare \(N = 16n\) initial Bell entangled states and distribute \(T_1(T_3)\) and \(T_5\)
(Tₖ) to Alice (Bob). Then, Alice (Bob) needs to prepare 2n and 4n new qubits when she (he) chooses to MEASURE the received qubits in T₁ (T₃) and T₃ (T₆), respectively. As a result, it has
\[
q = 16n \times 2 + 2n \times 2 + 4n \times 2 = 44n .
\]
Alice (Bob) needs to send Rₐ (Rₖ) to TP. Hence, it has c = 2n.
Therefore, the qubit efficiency of our protocol is
\[
\eta = \frac{n}{44n + 2n} = \frac{1}{46} .
\]

In the protocol of Ref.[39], Alice and Bob successfully compare their respective n bits of hash values, so it has b = n. Serve needs to prepare 4n initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, Alice (Bob) saves the measurement results or reflects the received qubits back without disturbance. As a result, it has q = 4n \times 2 = 8n. Alice (Bob) needs to send Rₐ (Rₖ) to Bob (Alice). Hence, it has c = 2n. Therefore, the qubit efficiency of the protocol of Ref.[39] is
\[
\eta = \frac{n}{8n + 2n} = \frac{1}{10} .
\]

In the protocol of Ref.[43], Alice and Bob successfully compare their respective n private bits, so it has b = n. TP needs to prepare two sequences of Bell states, each of whose length is 16n, and distribute the first particles of two sequences to Alice and Bob, respectively. Then, when Alice (Bob) chooses to MEASURE the received qubits, she (he) replaces the measurement results with the freshly prepared qubits. As a result, it has q = 16n \times 2 + 8n \times 2 = 80n. Alice (Bob) needs to send Rₐ (Rₖ) to TP. Hence, it has c = 2n. Therefore, the qubit efficiency of the protocol of Ref.[43] is
\[
\eta = \frac{n}{80n + 2n} = \frac{1}{82} .
\]

In the protocol of Ref.[44], Alice and Bob successfully compare their respective n private bits, so it has b = n. TP needs to prepare 8n initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, when Alice (Bob) chooses to MEASURE the received qubits, she (he) replaces the measurement results with the freshly prepared qubits. In addition, the protocol needs to employ the SQKD protocol in Ref.[31] to generate the n-bit pre-shared key Kₐₖ, which consumes 24n qubits, and the SQKA protocol in Ref.[41] to generate the n-bit pre-shared keys, Kₐₙ and Kₖₗ, which consumes 10n qubits in total. As a result, it has q = 8n \times 2 + 4n \times 2 + 24n + 10n = 58n. Alice (Bob) needs to send Cₐ (Cₖ) to TP. Hence, it has c = 2n. Therefore, the qubit efficiency of the protocol of Ref.[44] is
\[
\eta = \frac{n}{58n + 2n} = \frac{1}{60} .
\]

In the second protocol of Ref.[48], Alice and Bob successfully compare their respective n private bits, so it has b = n. TP needs to prepare 2n initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, when Alice (Bob) chooses to flip the received qubits, she (he) replaces the measurement results with the freshly prepared opposite qubits. In addition, the protocol needs to employ the SQKD protocol in Ref.[31] to generate the n-bit pre-shared key K , which consumes 24n qubits. As a result, it has q = 2n \times 2 + n \times 2 + 24n = 30n. Alice (Bob) needs to send Mₐ (Mₖ) to TP. Hence, it has c = 2n. Therefore, the qubit efficiency of
the protocol of the second protocol of Ref.[48] is \( \eta = \frac{n}{30n + 2n} = \frac{1}{32} \).

In the protocol of Ref.[49], Alice and Bob successfully compare their respective \( n \) private bits, so it has \( b = n \). TP needs to prepare \( 2n \) initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, when Alice (Bob) chooses to SIFT, she (he) generates fresh qubits and sends them to TP. In addition, the protocol uses the SQKD protocol in Ref.[29] to generate two \( n \)-bit pre-shared keys, \( K_{TA} \) and \( K_{TB} \), which consumes \( 16n \) qubits in total, and the SQKD protocol in Ref.[31] to generate the \( n \)-bit pre-shared key \( K \), which consumes \( 24n \) qubits. As a result, it has \( q = 2n \times 2 + n \times 2 + 16n + 24n = 46n \). Alice (Bob) needs to publish \( R_A \) (\( R_B \)) to TP. Hence, it has \( c = 2n \). Therefore, the qubit efficiency of the protocol of Ref.[49] is
\[
\eta = \frac{n}{46n + 2n} = \frac{1}{48}.
\]

In the protocol of Ref.[50], Alice and Bob successfully compare their respective \( n \) private bits, so it has \( b = n \). TP needs to prepare \( 3n \) initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, when Alice (Bob) chooses to SIFT, she (he) generates fresh qubits and sends them to TP. When Alice (Bob) chooses to DETECT, she (he) generates fresh trap qubits and sends them to TP. In addition, the protocol uses the SQKD protocol in Ref.[31] to generate the \( n \)-bit pre-shared key \( K \), which consumes \( 24n \) qubits. As a result, it has \( q = 3n \times 2 + n \times 2 + n \times 2 + 24n = 34n \). Alice (Bob) needs to publish \( R_A \oplus R'_A \) (\( R_B \oplus R'_B \)) to TP. Hence, it has \( c = 2n \). Therefore, the qubit efficiency of the protocol of Ref.[50] is
\[
\eta = \frac{n}{34n + 2n} = \frac{1}{36}.
\]

In the protocol of Ref.[53], Alice and Bob successfully compare their respective \( n \) private bits, so it has \( b = n \). TP needs to prepare \( 2n \) initial Bell entangled states and distribute the first and second particles to Alice and Bob, respectively. Then, when Alice (Bob) chooses to Measure the received qubits, she (he) generates fresh qubits and sends them to TP. In addition, this protocol needs to utilize the SQKD protocol in Ref.[31] to generate the \( 2n \)-bit pre-shared key \( K_{AB} \), which consumes \( 48n \) qubits. As a result, it has \( q = 2n \times 2 + n \times 2 + 48n = 54n \). Alice (Bob) needs to publish \( K_{AB} \) to TP. Hence, it has \( c = 4n \). Therefore, the qubit efficiency of the protocol of Ref.[53] is
\[
\eta = \frac{n}{54n + 4n} = \frac{1}{58}.
\]

In addition, Ref.[43] needs quantum entanglement swapping technology, which may be difficult to implement in practice. Fortunately, our protocol does not need quantum entanglement swapping technology. Moreover, each of the SQPC protocols in Refs.[43,44,48-50,53] needs to prepare four kinds of Bell entangled states as initial quantum resource. Fortunately, our protocol only needs to generate one kind of Bell entangled states. It is naturally that preparing the same kind of Bell entangled states repeatedly is easier in practice than generating different types of Bell entangled states. Hence, our protocol is easier to implement in practice than the SQPC protocols in
Table 3  Comparison results of our SQPC protocol and the previous SQPC protocols with Bell entangled states

| Feature          | Randomization-based | Measure-resend | Measure-resend | Measure-randomization-resend | Discard-resend | Measure-resend | Measure-resend | Measure-resend |
|------------------|---------------------|----------------|----------------|-------------------------------|----------------|----------------|----------------|----------------|
| Types of Bell entangled states | Single | Four | Four | Four | Four | Four | Four | Single |
| Usage of SQKD or SQKA | No | No | Yes | Yes | Yes | Yes | Yes | No |
| Usage of quantum entanglement swapping | No | Yes | No | No | No | No | No | No |
| Usage of unitary operations | No | No | No | No | No | No | No | No |
| TP’s knowledge about the comparison result | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Qubit efficiency | $\frac{1}{10}$ | $\frac{1}{82}$ | $\frac{1}{60}$ | $\frac{1}{32}$ | $\frac{1}{48}$ | $\frac{1}{36}$ | $\frac{1}{58}$ | $\frac{1}{46}$ |

In conclusion, in this paper, a novel SQPC protocol based on single kind of Bell entangled states is proposed, which utilizes the entanglement correlation of Bell entangled states to skillfully compare the equality of private inputs from two classical users. Our protocol can resist a variety of outside and participant attacks. Our protocol only employs one kind of Bell entangled states as initial quantum resource and doesn’t need to share private keys among different participants in
advance. Moreover, it needs neither unitary operations nor quantum entanglement swapping. Therefore, compared with most of the existing SQPC protocol with Bell entangled states, our protocol has better practical implementation feasibility.

Acknowledgments

Funding by the National Natural Science Foundation of China (Grant No.62071430 and No.61871347), the Fundamental Research Funds for the Provincial Universities of Zhejiang (Grant No.JRK21002) and Zhejiang Gongshang University, Zhejiang Provincial Key Laboratory of New Network Standards and Technologies (No. 2013E10012) is gratefully acknowledged.

Reference

[1] Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. IEEE International Conference on Computers, Systems, and Signal Processing, pp.175-179 (1984)
[2] Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67(6):661-663 (1991)
[3] Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell theorem. Phys. Rev. Lett. 68:557-559 (1992)
[4] Lo, H.K., Ma, X.F., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94(23): 230504 (2005)
[5] Hwang, T., Hwang, C.C., Tsai, C.W.: Quantum key distribution protocol using dense coding of three-qubit W state. Eur. Phys. J. D 61(3):785-790 (2011)
[6] Zhang, C.M., Song, X.T., Treeviriyanupab, P., et al.: Delayed error verification in quantum key distribution. Chin. Sci. Bull. 59(23):2825-2828 (2014)
[7] Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 59:162-168 (1999)
[8] Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. J. Phys. A: Gen. Phys. 39(45):14089-14099(2007).
[9] Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. 282(17):3647-3651(2009)
[10] Hao, L., Wang, C., Long G.L.: Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration. Opt. Commun. 284:3639-3642 (2011)
[11] Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65: 032302 (2002)
[12] Chen, X.B., Wen, Q.Y., Guo, F.Z., Sun, Y., Xu, G., Zhu, F.C.: Controlled quantum secure direct communication with W state. Int. J. Quant. Inform. 6(4):899-906 (2008)
[13] 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. 59(21):2541-2546 (2014)
[14] Zhang, W., Ding, D.S., Sheng, Y.B., et al. Quantum secure direct communication with quantum memory. Phys. Rev. Lett. 118(22):220501 (2017)
[15] Peng, H., Niu, Z.R., et al. Measurement-device-independent quantum communication without encryption. Sci. Bull. 63(20):1345-1350 (2018)
[16] Qi, R.Y., Long, G.L., Sun, Z., et al.: Implementation and security analysis of practical quantum secure direct communication. Light-Sci. Appl. 8(1):183-190 (2019)
[17] Hong, C.H., Heo, J., Jang J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Inf. Process. 16: 236 (2017)
[18] Liu, B., Gao, Z.F., Xiao, D., et al.: Quantum identity authentication in the orthogonal-state-encoding QKD system. Quantum Inf. Process. 18:137 (2019)
[19] Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A: Math. Theor. 42(5):055305 (2009)
[20] 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)
[21] Li, Y.B., Ma, Y.J., Xu, S.W., et al.: Quantum private comparison based on phase encoding of single photons. Int. J. Theor. Phys. 53:3191-3200 (2014)
[22] Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. 57(4):583-588 (2012)
[23] Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. 11:373-384 (2012)
[24] Lang, Y.F.: Quantum private comparison using single Bell state. Int. J. Theor. Phys. https://doi.org/10.1007/s10773-021-04937-3 (2021)
[25] Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process.12(2):1077-1088 (2013)
[26] Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. 51:3596-3604 (2012)
[27] Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. 52(1):212-218 (2013)
[28] 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)
[29] Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. 99(14):140501 (2007)
[30] Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A 79(3):032341 (2009)
[31] Krawec, W.O.: Mediated semiquantum key distribution. Phys. Rev. A 91(3):032323 (2015)
[32] Zou, X.F., Qiu, D.W., Zhang, S.Y., Mateus, P.: Semiquantum key distribution without invoking the classical party’s measurement capability. Quantum Inf. Process.14(8):2981-2996 (2015)
[33] Zhu, K.N., Zhou, N.R., Wang, Y.Q. et al.: Semi-quantum key distribution protocols with GHZ states. Int J Theor Phys 57, 3621–3631 (2018)
[34] Li, Q., Chan, W.H., Long, D.Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A 82(2), 022303 (2010)
[35] Wang, J., Zhang, S., Zhang, Q., Tang, C.J.: Semiquantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. 10(05):1250050 (2012)
[36] Yang, C.W., Hwang, T.: Efficient key construction on semi-quantum secret sharing protocols.
[37] Xie, C., Li, L.Z., Qiu, D.W.: A novel semi-quantum secret sharing scheme of specific bits. Int. J. Theor. Phys. 54(10):3819-3824 (2015)

[38] Liu, W.J., Chen, Z.Y., Ji, S., et al.: Multi-party semi-quantum key agreement with delegating quantum computation. Int. J. Theor. Phys. 56:3164-3174 (2017)

[39] Yan, L.L., Zhang, S.B., Chang, Y., et al.: Semi-quantum key agreement and private comparison protocols using Bell states. Int. J. Theor. Phys. 58:3852-3862 (2019)

[40] Zhou, N.R., Zhu, K.N., Wang, Y.Q.: Three-party semi-quantum key agreement protocol. Int. J. Theor. Phys. 59:663-676 (2020)

[41] Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process. 16:295 (2017)

[42] Ye, T.Y., Ye, C.Q.: Semi-quantum dialogue based on single photons. Int. J. Theor. Phys. 57(5):1440-1454 (2018)

[43] Chou, W.H., Hwang, T., Gu, J.: Semi-quantum private comparison protocol under an almost-dishonest third party. https://arxiv.org/abs/1607.07961 (2016)

[44] Thapliyal, K., Sharma, R.D., Pathak, A.: Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Inter. J. Quant. Inf. 16(5): 1850047 (2018)

[45] Ye, T.Y., Ye, C.Q.: Measure-resend semi-quantum private comparison without entanglement. Int. J. Theor. Phys. 57(12):3819-3834 (2018)

[46] Lin, P.H., Hwang, T., Tsai, C.W.: Efficient semi-quantum private comparison using single photons. Quantum Inf. Process. 18:207 (2019)

[47] Yan, L.L., Chang, Y., Zhang, S.B., et al.: Measure-resend semi-quantum private comparison scheme using GHZ class states. Comput. Mater. Con. 61(2):877-887 (2019)

[48] Jiang, L.Z.: Semi-quantum private comparison based on Bell states. Quantum Inf. Process. 19:180 (2020)

[49] Tsai, C.W., Lin, J., Yang, C.W.: Cryptanalysis and improvement in semi-quantum private comparison based on Bell states. Quantum Inf. Process. 20:120 (2021)

[50] Xie, L., Li, Q., Yu, F. Lou, X.P., Zhang, C.: Cryptanalysis and improvement of a semi-quantum private comparison protocol based on Bell states. Quantum Inf. Process. 20:244 (2021)

[51] Yan, L.L., Zhang, S.B., Chang, Y., Wan, G.G., Yang, F.: Semi-quantum private comparison protocol with three-particle G-like states. Quantum Inf. Process. 20:17, (2021)

[52] Ye, C.Q., Li, J., Chen, X.B. Yuan. T.: Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. Quantum Inf. Process. 20:262 (2021)

[53] Sun, Y.H., Yan, L.L., Sun, Z.B., Zhang, S.B., Lu, J.Z.: A novel semi-quantum private comparison scheme using bell entangle states. Comput. Mater. Con. 66(3):2385-2395 (2021)

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

[55] Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A 351(1-2):23-25 (2006)

[56] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys.74(1): 145-195(2002)

[57] Deng, F.G., Zhou, P., Li, X.H., et al.: Robustness of two-way quantum communication
protocols against Trojan horse attack. https://arxiv.org/abs/quant-ph/0508168 (2005)

[58] Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74:054302 (2006)

[59] Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on theBradler-Dusek protocol. Quantum Inf. Comput. 7:329 (2007)

[60] Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. 85:5635 (2000)