Quantum Information Processing (2022) 21:127
https://doi.org/10.1007/s11128-022-03460-6

Security analysis and improvement of a semi-quantum private comparison protocol with three-particle G-like states

Qin Li[1] · Peishan Li[1] · Li Xie[1] · Lingli Chen[1] · Junyu Quan[2]

Received: 4 September 2021 / Accepted: 12 February 2022 / Published online: 30 March 2022

Abstract

Semi-quantum private comparison (SQPC) allows two parties with limited quantum capability to compare their private secrets for equality with the assistance of a quantum third party (TP). Recently, Yan et al. presented an efficient SQPC protocol by using three-particle G-like states as the resource state (Quantum Inf Process 20(6): 17, 2021). However, we discover a design flaw in the protocol and show how it can make the protocol vulnerable to the double CNOT attack, through which a malicious participant can acquire each secret bit of the other honest party with probability $1/2$ without being detected. Then, we propose an improved SQPC protocol and show that it can be secure against similar types of attack that can be avoided in the original SQPC protocol and also the double CNOT attack.

Keywords Quantum private comparison · Semi-quantum private comparison · Double CNOT attack

1 Introduction

Quantum cryptography is a combination of quantum physics and cryptography and has been extensively investigated [1,2]. It has inherent advantages compared with classical cryptography, since its security is based on quantum mechanical principles instead of unproven mathematical assumptions [3]. Bennett and Brassard proposed the first quantum cryptography protocol in 1984 [4], which was proved to be unconditionally secure. Subsequently, a lot of quantum cryptographic protocols have been designed to solve various problems, such as quantum key distribution (QKD) [5–7], quantum

✉ Junyu Quan
quanli91@qq.com

[1] School of Cyberspace Security, Xiangtan University, Xiangtan 411105, China

[2] School of Mathematics and Computational Science, Xiangtan University, Xiangtan 411105, China

secret sharing (QSS) [8,9], quantum encryption [10,11], and quantum private query [12,13]. Quantum private comparison (QPC) has also gained a lot of attention, as it can allow participants who do not trust each other to compare whether their private information is equal without leaking them. The first QPC protocol was proposed by Yang *et al* by using Bell states and decoy states [14]. Later, Chen et al proposed an efficient QPC protocol based on three-particle GHZ states [15]. Subsequently, some other QPC protocols are proposed to be suitable for different environments [16–28].

However, almost all these proposed QPC protocols required participants to have full quantum capabilities. In fact, quantum resources are still relatively scarce and many participants often do not have enough quantum capability at present. It is an issue that needs to be solved to reduce the quantum capabilities of participants. Boyer et al. first put forward the notion of “semi-quantum” in 2007 [29], where one participant is “classical" and the other is quantum. A “classical” participant indicates that one can only perform four operations described below: (1) preparing qubits in the computational basis $\{|0\rangle, |1\rangle\}$, (2) measuring qubits in the computational basis, (3) reordering qubits, and (4) sending and receiving qubits. Semi-quantum technology also can be applied to QPC [30–34]. Chou *et al* introduced the first semi-quantum private comparison (SQPC) protocol in 2016, which does not require participants to have sufficient quantum capabilities [30]. With the assistance of a third-party TP, two players can check whether their secret inputs are equal by using decoy photons and two-particle entangled states. Other similar SQPC protocols also have been proposed by the combined use of QPC and semi-quantum technology [31–33]. But the efficiency of qubits in the existing SQPC protocols is low [30,33]. Recently, Yan *et al.* presented a SQPC protocol with three-particle G-like states [35], which obtains higher efficiency than the previously proposed SQPC protocols [31–33]. We observe there is a design weakness in their protocol. It can make the protocol vulnerable to the double CNOT attack, by which a malicious participant is possible to get secret information of another honest participant without being caught. Furthermore, we improve the SQPC protocol given by Yan et al. to avoid this attack.

The remainder of the paper can be organized below. Section 2 is a general overview of Yan *et al.*’s SQPC protocol [35]. Cryptanalysis on Yan *et al.*’s SQPC protocol is made in Sect. 3. Section 4 gives an improved SQPC protocol. Section 5 makes security analysis on the proposed SQPC protocol. The final section makes a conclusion of this paper.

2 Review of Yan et al.’s SQPC protocol

Yan et al.’s SQPC protocol [35] is briefly reviewed in this part. Let two classical participants share a key sequence K_{AB} through a semiquantum key distribution [36] and have their own private messages X and Y, where each key bit $K^i_{AB} \in \{0, 1\}$, $X = \sum_{i=1}^{n} x_i 2^{i-1}$, $Y = \sum_{i=1}^{n} y_i 2^{i-1}$, and $x_i, y_i \in \{0, 1\}$. The equality of their secrets X and Y must be compared securely without revealing their true value to each other and a semi-honest TP. Note that, a semi-honest TP means that he may attempt to obtain the secrets of the participants by collecting related information during the

Table 1 Actions on the qubits for participants in Yan et al.'s protocol [35]

Case	Alice's action	Bob's action	TP's action	TP obtains information	TP computes data
1	R	R	Action 1	N/A	N/A
2	R	M	Action 2	MB_i and RB_i	PB_i=$MB_i \oplus RB_i$=$K^i_{AB} \oplus y_i$
3	M	R	Action 2	MA_i and RA_i	PA_i=$MA_i \oplus RA_i$=$K^i_{AB} \oplus x_i$
4	M	M	Action 3	MA_i, RA_i, MB_i, and RB_i	PA_i=$MA_i \oplus RA_i$=$K^i_{AB} \oplus x_i$ PB_i=$MB_i \oplus RB_i$=$K^i_{AB} \oplus y_i$

Note that Action 1: TP performs the three-qubit joint measurement on his own qubit, the qubit sent by Alice, and the qubit sent by Bob to check eavesdropping;
Action 2: TP performs the Bell measurement on his own qubit and the qubit returned by the participant who chose R to check eavesdropping as well as the Z basis measurement on the qubit returned by the participant who chose M;
Action 3: TP measures his own qubit, the qubit sent by Alice, and the qubit sent by Bob all in the Z basis

implementation process, but he has to follow the specified steps and cannot collude with any participant. The specific steps in the protocol are given as follows.

Step 1 Quantum user TP generates $2n$ G-like states in the form of $|\psi\rangle_{TAB}$ which can be written as

$$\begin{aligned}|\psi\rangle_{TAB} &= \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{TAB}\\ &= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{TA}|0\rangle_B + |\phi^+\rangle_{TA}|1\rangle_B)\\ &= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{TB}|0\rangle_A + |\phi^+\rangle_{TB}|1\rangle_A),\end{aligned} \tag{1}$$

where $|\phi^+\rangle$, $|\phi^-\rangle$, $|\varphi^+\rangle$ and $|\varphi^-\rangle$ are the four Bell states and the subscripts 'T', 'A', and 'B' indicate that the qubits will be held by TP, Alice, and Bob, respectively. All the first qubis of these states form the sequence S_T, the second qubits of them form the sequence S_A, and the third qubits of them constitute the sequence S_B. Then he sends S_A to Alice, S_B to Bob, and keeps S_T by himself.

Step 2 For each received qubit, Alice (or Bob) randomly chooses to reflect the qubit to TP without doing anything else (called action R) or makes a measurement in the $\{|0\rangle, |1\rangle\}$ basis to obtain MA_i (or MB_i) and computes $RA_i = MA_i \oplus K^i_{AB} \oplus x_i$ ($RB_i = MB_i \oplus K^i_{AB} \oplus y_i$) (called action M). Note that and $1 \leq i \leq n$, $MA = \{MA_1, MA_2, ..., MA_n\}$, $RA = \{RA_1, RA_2, ..., RA_n\}$, $MB = \{MB_1, MB_2, ..., MB_n\}$, and $RB = \{RB_1, RB_2, ..., RB_n\}$.

Step 3 When all qubits arrive, TP informs the participants Alice and Bob and they will reveal their choices in step 2. Based on the selections made by Alice and Bob in step 2, there are four cases and TP performs different operations as indicated in Table 1.

If case 1 happens, TP makes the joint measurement on his own qubit, the qubit sent by Alice, and the qubit sent by Bob in the G-like basis for eavesdropping. If there does not exist an eavesdropper, TP's measurement result should be $|\psi\rangle_{TAB}$. Otherwise TP terminates the protocol.

When cases 2 and 3 occur, the Bell measurement is done by TP with his own qubit and the qubit returned by Alice or Bob to detect eavesdroppers. If the measurement result is $|\phi^+\rangle$ or $|\varphi^+\rangle$, the protocol continues, otherwise it terminates. TP can obtain MB_i or MA_i according to the Bell measurement results and Eq. (1). Then TP measures the qubit sent by the participant who chose the operation M in the Z basis to get RB_i or RA_i. Finally, TP computes $PB_i = RB_i \oplus MB_i = (MB_i \oplus K_{AB}^i \oplus y_i) \oplus MB_i = K_{AB}^i \oplus y_i$ or $PA_i = RA_i \oplus MA_i = (MA_i \oplus K_{AB}^i \oplus x_i) \oplus MA_i = K_{AB}^i \oplus x_i$.

For case 4, Alice and Bob publish the values of MA_i and MB_i. TP measures his own qubit in the Z basis. If the measurement result is not the same as the expected result according to Eq. (1), MA_i, and MB_i, he terminates the protocol. Otherwise, he measures the qubits sent by Alice and Bob both in the Z basis to get RA_i and RB_i. Then he computes $PA_i = RA_i \oplus MA_i = K_{AB}^i \oplus x_i$ and $PB_i = RB_i \oplus MB_i = K_{AB}^i \oplus y_i$.

Step 4 TP computes $P_i = PA_i \oplus PB_i = K_{AB}^i \oplus x_i \oplus K_{AB}^i \oplus y_i = x_i \oplus y_i$. If the value of P_i is not zero, TP declares $X \neq Y$ and terminates the protocol; otherwise TP sets $i = i + 1$ and restarts the operation till $i = n$. If $x_i \oplus y_i = 0$ for each i, TP declares $X = Y$ and stops the protocol.

3 Cryptanalysis of Yan et al.'s SQPC protocol

In the following, we show Yan et al.'s SQPC protocol [35] is insecure, as the secret of honest participant can be learned by a malicious participant by performing the double CNOT attack without being caught.

Here Bob is assumed to be a curious participant and wants to obtain Alice's secret. In step 1, TP prepares states $|\psi\rangle_{TAB}$ and sends the qubit sequence S_A to Alice, S_B to Bob, and keeps S_T. When TP sends each qubit in S_A to Alice, the attacker Bob intercepts it and performs the first CNOT gate on it and his ancillary qubit which is in the state of $|0\rangle$. Then the state of the whole system is

$$\begin{aligned}|\psi\rangle_1 &= CNOT_{AE} \otimes I_{TB}(|\psi\rangle_{TAB} \otimes |0\rangle_E) \\ &= \frac{1}{2}(|0010\rangle + |0101\rangle + |1000\rangle + |1111\rangle)_{TABE}.\end{aligned} \tag{2}$$

Similarly, the subscripts 'T,' 'A,' and 'B' indicate the qubits held by TP, Alice, and Bob, and 'E' indicates an ancillary qubit generated by Bob. When Alice receives the qubit from TP, she chooses R or M at random. When Alice sends the qubit to TP, Bob once again intercepts it and performs the second CNOT gate on it and his ancillary qubit, where the intercepted one is used as the control qubit and his own ancillary qubit is used as the target qubit. Since both Alice and Bob can randomly choose R or M, there are four different cases to be considered.

(a) If both Alice and Bob chose R, the whole state after Bob implements the second CNOT gates can be written as

$$\begin{aligned}|\psi\rangle_2 &= (CNOT_{AE}\otimes I_{TB})(CNOT_{AE}\otimes I_{TB})(|\psi\rangle_{TAB}\otimes|0\rangle_E)\\ &= \frac{1}{2}(|0010\rangle+|0100\rangle+|1000\rangle+|1110\rangle)_{TABE}\\ &= |\psi\rangle_{TAB}\otimes|0\rangle_E.\end{aligned} \tag{3}$$

Obviously, TP cannot detect Bob's eavesdropping in this case since the state $|\psi\rangle_{TAB}$ remains unchanged. But Bob cannot get any valuable information since the state of the ancillary qubit is always $|0\rangle$.

(b) If Alice chose R and Bob chose M, Bob measures the received qubit from TP and generates a new quantum state $|B\rangle$ to be sent to TP, where $|B\rangle\in\{|0\rangle_{B'},|1\rangle_{B'}\}$. According to Eq. (2), the state of the system collapses to $(|0101\rangle+|1000\rangle)_{TABE}$ or $(|0010\rangle+|1111\rangle)_{TABE}$. At the same time, Bob performs the second CNOT gate on his own ancillary qubit and Alice's qubit. The state of the whole system is changed as

$$\begin{aligned}|\psi\rangle_3 &= CNOT_{AE}\otimes I_{TBB'}[\frac{1}{\sqrt{2}}(|0101\rangle+|1000\rangle)_{TABE}\otimes|0\rangle_{B'}]\\ &= \frac{1}{\sqrt{2}}(|0100\rangle+|1000\rangle)_{TABE}\otimes|0\rangle_{B'}\\ &= |\varphi^+\rangle_{TA}|00\rangle_{BE}\otimes|0\rangle_{B'}\end{aligned} \tag{4}$$

or

$$\begin{aligned}|\psi\rangle_4 &= CNOT_{AE}\otimes I_{TBB'}[\frac{1}{\sqrt{2}}(|0010\rangle+|1111\rangle)_{TABE}\otimes|1\rangle_{B'}]\\ &= \frac{1}{\sqrt{2}}(|0010\rangle+|1110\rangle)_{TABE}\otimes|1\rangle_{B'}\\ &= |\phi^+\rangle_{TA}|10\rangle_{BE}\otimes|1\rangle_{B'}.\end{aligned} \tag{5}$$

Then, TP measures the qubit sent by Alice and his own qubit in the Bell basis for eavesdropping. According to Eqs. (4) and (5), Bob can pass eavesdropping. But he also cannot get Alice's secret information since the state of his ancillary qubit is still $|0\rangle$.

(c) If Alice chose M and Bob chose R, Alice measures the received qubit from TP and produces the corresponding quantum state $|A\rangle$ which is sent to TP, where $|A\rangle\in\{|0\rangle_{A'},|1\rangle_{A'}\}$. Similar to case (b), the state of the system collapses to $(|0010\rangle+|1000\rangle)_{TABE}$ or $(|0101\rangle+|1111\rangle)_{TABE}$ according to Eq. (2). If Alice prepares $|0\rangle_{A'}$, the state of the whole system after Bob carries out the second CNOT gate is

$$\begin{aligned}|\psi\rangle_5 &= CNOT_{A'E}\otimes I_{TAB}\left[|0\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0010\rangle+|1000\rangle)_{TABE}\right]\\ &= \left[|0\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0010\rangle+|1000\rangle)_{TABE}\right]\end{aligned} \tag{6}$$

or

$$\begin{aligned}|\psi\rangle_6 &= CNOT_{A'E}\otimes I_{TAB}\left[|0\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0101\rangle+|1111\rangle)_{TABE}\right]\\ &=\left[|0\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0101\rangle+|1111\rangle)_{TABE}\right].\end{aligned} \tag{7}$$

Similarly, if Alice prepares $|1\rangle_{A'}$, the entire state after Bob performs the second CNOT gate should be

$$\begin{aligned}|\psi\rangle_7 &= CNOT_{A'E}\otimes I_{TAB}\left[|1\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0010\rangle+|1000\rangle)_{TABE}\right]\\ &=\left[|1\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0011\rangle+|1001\rangle)_{TABE}\right]\end{aligned} \tag{8}$$

or

$$\begin{aligned}|\psi\rangle_8 &= CNOT_{A'E}\otimes I_{TAB}\left[|1\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0101\rangle+|1111\rangle)_{TABE}\right]\\ &=\left[|1\rangle_{A'}\otimes\frac{1}{\sqrt{2}}(|0100\rangle+|1110\rangle)_{TABE}\right].\end{aligned} \tag{9}$$

In order to escape being detected, Bob should reflect his true qubit to TP. But Bob can perform the Z basis measurement on his ancillary qubit to learn some information. According to Eqs. (6), (7), (8), and (9), if the result is $|0\rangle$, Bob can know $MA_i\oplus RA_i=0$; else he knows $MA_i\oplus RA_i=1$. Thus, Bob is able to obtain one bit of Alice's secret information $x_i=P_i\oplus K_{AB}^i=MA_i\oplus RA_i\oplus K_{AB}^i$.

(d) If both Alice and Bob chose M, they must publish the measurement results MA_i and MB_i. The state of the system may collapse to $|0010\rangle_{TABE}$, $|0101\rangle_{TABE}$, $|1000\rangle_{TABE}$ or $|1111\rangle_{TABE}$ after Alice and Bob perform the measurements. Then Bob performs the second CNOT gate on the qubit returned by Alice and his ancillary qubit and the state of the whole system is changed to $|0\rangle_{A'}|0010\rangle_{TABE}|B\rangle$, $|0\rangle_{A'}|0101\rangle_{TABE}|B\rangle$, $|0\rangle_{A'}|1000\rangle_{TABE}|B\rangle$, $|0\rangle_{A'}|1111\rangle_{TABE}|B\rangle$, $|1\rangle_{A'}|0011\rangle_{TABE}|B\rangle$, $|1\rangle_{A'}|0100\rangle_{TABE}|B\rangle$, $|1\rangle_{A'}|1001\rangle_{TABE}|B\rangle$, or $|1\rangle_{A'}|1110\rangle_{TABE}|B\rangle$. Since the state of qubit owned by TP has not changed, Bob's attack will not be discovered. Then Bob measures his ancillary qubit in the Z basis, obtaining $|0\rangle$ or $|1\rangle$ with probability $1/2$. Since the value of MA_i is published, Bob can easily get Alice's secret bit x_i. For example, suppose the measurement result of Bob's ancillary qubit is 0, that is, MB_i is 0, and MA_i that Alice publishes is also 0. Then Bob knows the state of the whole system after he does the second CNOT gate should be $|0\rangle_{A'}|1000\rangle_{TABE}|B\rangle$ and thus learns the value of RA_i is 0. Then he can compute $x_i=RA_i\oplus MA_i\oplus K_{AB}^i$ to get Alice's secret x_i.

In terms of the above analysis, we can deduce that in cases (c) and (d), since the qubits returned to TP after measuring by Alice are not the same as those sent by TP, the participant Bob who is a malicious one can get Alice's secret without being detected by performing the double CNOT attack. Hence, the private information of the honest

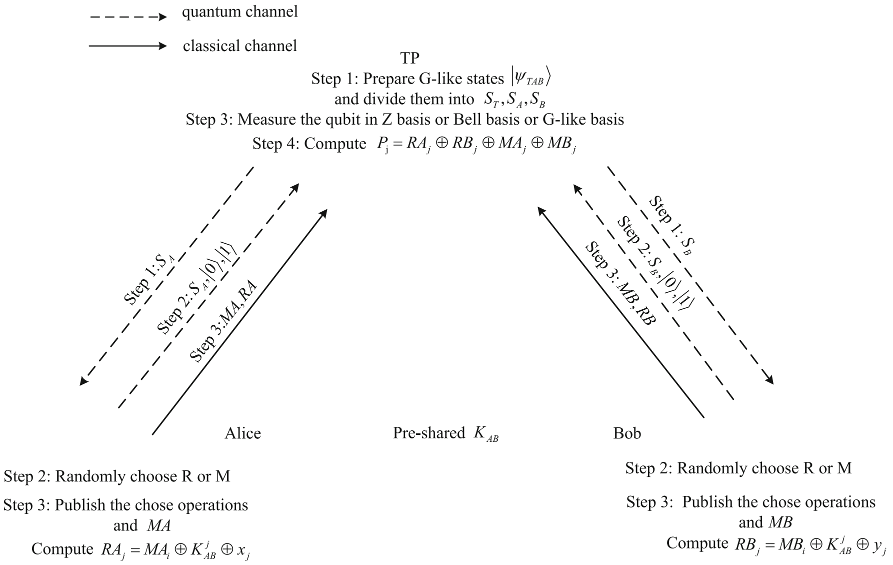
quantum channel
classical channel
TP
Step 1: Prepare G-like states $|\psi_{TAB}\rangle$
and divide them into S_T, S_A, S_B
Step 3: Measure the qubit in Z basis or Bell basis or G-like basis
Step 4: Compute $P_j = RA_j \oplus RB_j \oplus MA_j \oplus MB_j$
Step 1: S_A
Step 2: S_A, $|0\rangle$, $|1\rangle$
Step 3: MA, RA
Step 1: S_B
Step 2: S_B, $|0\rangle$, $|1\rangle$
Step 3: MB, RB
Alice
Pre-shared K_{AB}
Bob
Step 2: Randomly choose R or M
Step 3: Publish the chose operations and MA
Compute $RA_j = MA_i \oplus K_{AB}^j \oplus x_j$
Step 2: Randomly choose R or M
Step 3: Publish the chose operations and MB
Compute $RB_j = MB_i \oplus K_{AB}^j \oplus y_j$

Fig. 1 Processes involved in the improved SQPC protocol. Note that, Alice and Bob only disclose the value of RA and RB when they both choose M in step 3

participant can be acquired by the malicious participant using the double CNOT attack with a probability of 1/2.

4 The proposed improved SQPC protocol

In the following, we improve Yan et al.'s SQPC protocol [35] to be secure against various types of attack like the original protocol and also the double CNOT attack.

In the improved protocol, two classical participants Alice and Bob share a n-bit key sequence K_{AB} through an efficient mediated quantum key distribution protocol [37], Alice has the secret X, and Bob has the secret Y. Let K_{AB}^i, x_i, and y_i be the i-th bit of K_{AB}, X, and Y, respectively, where $K_{AB}^i, x_i, y_i \in \{0, 1\}$ and $1 \leq i \leq n$. TP is a semi-honest third party to help Alice and Bob to complete their secret comparison. The basic processes of the improved protocol are depicted in Fig. 1 and a detailed description of it is given as follows.

Step 1 TP generates $4n$ G-like states in the form of $|\psi\rangle_{TAB}$ which can be written as

$$\begin{aligned} |\psi\rangle_{TAB} &= \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{TAB} \\ &= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{TA}|0\rangle_B + |\phi^+\rangle_{TA}|1\rangle_B) \\ &= \frac{1}{\sqrt{2}}(|\varphi^+\rangle_{TB}|0\rangle_A + |\phi^+\rangle_{TB}|1\rangle_A), \end{aligned} \tag{10}$$

Table 2 Actions on the qubits for participants in the proposed protocol

Case	Alice's action	Bob's action	TP's action
1	*R*	*R*	To implement the G-like basis joint measurement on his own qubit and the qubits sent by Alice and Bob
2	*R*	*M*	To implement the measurement on the qubit sent by Alice and his own qubit in the Bell basis and compare the result with that Bob reveals
3	*M*	*R*	To implement the measurement on the qubit sent by Bob and his own qubit in the Bell basis and compare the result with that Alice reveals
4	*M*	*M*	To implement the *Z* basis measurements on his own qubit and the qubits sent by Alice and Bob

where $|\phi^+\rangle$, $|\phi^-\rangle$, $|\varphi^+\rangle$ and $|\varphi^-\rangle$ are the four Bell states. TP divides them into three sequences S_T, S_A, and S_B. Then he transmits the sequence S_A to Alice, S_B to Bob, and keeps S_T.

Step 2 Alice and Bob choose one of the following two operations at random after receiving each qubit: (1) returning the qubit to TP directly (called action R), and (2) measuring the received qubit in the Z basis and preparing a new qubit according to the measurement result and sending it to TP (called action M). Let the binary sequence $MA = \{MA_1, MA_2, ..., MA_{2n}\}$ (or $MB = \{MB_1, MB_2, ..., MB_{2n}\}$) be made up of the measurement results and $MA_i \in \{0, 1\}$ (or $MB_i \in \{0, 1\}$) be the ith bit of MA (or MB). Note that different from Yan et al.'s SQPC protocol [35], here participants need to resend the qubit to the TP in the state corresponding to the measurement result. For instance, the participant should generate $|0\rangle$ and send it to TP if the measurement result is 0. It can ensure that the attacker cannot distinguish which actions the participants chose.

Step 3 If TP has received all the qubits, Alice and Bob broadcast their choices in step 2. There are four cases and TP performs different actions according to the choices that Alice and Bob made as described in Table 2.

In case 1 where both Alice and Bob chose R, TP makes a joint measurement on the qubit sent by Alice and Bob, and his own qubit in the G-like basis for eavesdropping detection. TP's measurement result should be $|\psi\rangle_{TAB}$, otherwise there may exist an eavesdropper and the protocol is terminated.

In cases 2 and 3 where one participant chose R and the other participant chose M, TP measures his own qubit and the directly returned qubit by the participant who chose R in the Bell basis. In addition, the participant who chose M reveals the value of MA_i or MB_i. If the Bell measurement result corresponds to the state $|\phi^+\rangle$ or $|\varphi^+\rangle$, TP continues the protocol, else he terminates it.

In case 4 where both Alice and Bob chose M, TP measures the qubits returned by Alice and Bob in the Z basis to obtain MA_i and MB_i. Then, TP makes the Z basis measurement on his own qubit. If the measurement result differs from the expected result based on Eq. (10), MA_i, and MB_i, TP terminates the protocol. Then, Alice calculates $RA_j = MA_i \oplus K_{AB}^j \oplus x_j$, where $i \in (1, 2, ..., n)$ and $j \in (1, 2, ..., n)$. Bob also calculates $RB_j = MB_i \oplus K_{AB}^j \oplus y_j$. Then Alice and Bob broadcast the value of RA_j and RB_j, respectively.

Step 4 TP computes $P_j = RA_j \oplus RB_j \oplus MA_i \oplus MB_i = (MA_i \oplus K_{AB}^j \oplus x_j) \oplus (MB_i \oplus K_{AB}^j \oplus y_j) \oplus MA_i \oplus MB_i = x_j \oplus y_j$. If $P_j \neq 0$, TP will publish $X \neq Y$, which means Alice and Bob have unequal secrets. Otherwise, TP repeats the comparisons till all the results have been obtained. If $P_j = 0$ for all the comparisons, TP can conclude that Alice's secret is the same as Bob's secret and he will announce $X = Y$.

5 Security analysis

In the improved SQPC protocol, since a key sequence K_{AB} is pre-shared among the participants, who know more information than the external eavesdropper, the probability of successful attack by the participants is significantly higher than that of the outside eavesdropper. Therefore, we focus on analyzing the security of the protocol in the worst case where a participant is considered as an attacker. For instance, Bob is assumed to be dishonest and may try to obtain Alice's secret through some types of attacks, such as the intercept-resend attack, the measure-resend attack, the double CNOT attack, and the entangle-measure attack. In addition, TP's attack is also analyzed.

5.1 Intercept-resend attack

A malicious attacker Bob may launch the intercept-resend attack to steal some valuable information from Alice. The specific operations are as follows. Bob intercepts the qubit sequence S_A in step 1 and stores them. Then Bob sends his prepared fake qubits in the state of $|0\rangle$ or $|1\rangle$ to Alice at random. Subsequently, Bob intercepts Alice's qubits once more and delivers the stored qubit sequence S_A to TP. This kind of attack Bob will be discovered in step 3 with a certain probability and the detail analysis is in the following. If the participants chose to reflect the qubit directly in step 2, TP will measure his own qubit and the directly reflected qubits in the G-like basis or the Bell basis for eavesdropping. Since the qubit sequence S_A and S_B do not change, Bob's attack will not be discovered. Similarly, if both Alice and Bob chose to measure the qubits, TP measures the qubits sent by Alice and Bob in the Z basis to get the values of MA_i and MB_i. Due to Bob's attack, TP may acquire MA_i which may not be equal to that Alice got with probability 1/2. But Bob learns the value of MA_i that Alice got and may obtain the secret qubit of Alice without being caught. But if Alice chose to measure the qubit and Bob chose to reflect the qubit, TP detects eavesdropping by performing the Bell basis measurement on the qubits returned by Bob and his own qubit. Since the qubit that Alice performed the measurement on was replaced by that Bob prepared, Bob can be discovered by TP and Alice with probability 1/2. Consequently, the probability that Bob may be detected in the four cases is $P = 1 - (3/4 + 1/4 \times 1/2)^N = 1 - (7/8)^N$. When N is large enough, P is close to 1.

5.2 Measure-resend attack

The measure-resend attack here means that Bob intercepts the qubit sequence S_A sent by the TP and performs the Z basis measurement, generates the new qubit in the corresponding state according to the measurement result and sends it to Alice. In step 3, for case 3, TP measures the qubit sent by Bob and his own qubit in the Bell basis for eavesdropping. Since the qubit that Alice performed the measurement was the same as that Bob prepared, Bob cannot be discovered by TP. Similarly, in case 4, Bob's attack does not change the qubit owned by TP and thus he is undetectable. Bob also can figure out Alice's secret exactly. However, in cases 1, TP performs the G-like basis measurement on the returned qubits and his own qubit to check detection. Since Bob's attack destroyed the initial G-like state, the probability of him being detected is 1/2. Similarly, in case 2, TP measures the qubit sent by Alice and his own qubit in the Bell basis for eavesdropping detection. Based on Eq. (10), TP must obtain $|\varphi^+\rangle$ or $|\phi^+\rangle$ with equal probability. But Bob replaced the qubits sent by TP with the qubits generated by himself, his attack also will be detected with probability 1/2. To sum up, the total probability of Bob being detected in four cases is $P = 1 - (1/4 \times 1/2 + 1/4 \times 1/2 + 1/2)^N = 1 - (3/4)^N$ and it is close to 1 if N is large enough.

5.3 Double CNOT attack

In step 1, TP generates $|\psi\rangle_{TAB}$ and divides these qubits into three sequences S_T, S_A, and S_B. Then he sends S_A to Alice, S_B to Bob, and keeps S_T. Bob intercepts each qubit sent by TP to Alice and performs the first CNOT gate on it and his ancillary qubit $|0\rangle$, the state of the whole system is

$$\begin{aligned}|\psi\rangle_1 &= CNOT_{AE} \otimes I_{TB}(|\psi\rangle_{TAB} \otimes |0\rangle_E)\\ &= \frac{1}{2}(|0010\rangle + |0101\rangle + |1000\rangle + |1111\rangle)_{TABE}.\end{aligned} \tag{11}$$

In step 2, when Alice receives each qubit, she chooses R or M at random. Bob intercepts the qubit returned from Alice and implements the second CNOT gate on it and his ancillary qubit. According to different choices made by Alice and Bob, there are the following four situations.

Case 1 When both Alice and Bob chose R, the entire state after Bob implements the second CNOT gate can be written as

$$\begin{aligned}|\psi\rangle_2 &= (CNOT_{AE} \otimes I_{TB})(CNOT_{AE} \otimes I_{TB})(|\psi\rangle_{TAB} \otimes |0\rangle_E)\\ &= \frac{1}{2}(|0010\rangle + |0100\rangle + |1000\rangle + |1110\rangle)_{TABE}.\end{aligned} \tag{12}$$

In this case, the state $|\psi\rangle_{TAB}$ is not changed by executing the CNOT gate operation twice. It is simple to determine that the ancillary qubit is always $|0\rangle$, implying that Bob is unable to gain any meaningful information.

Case 2 When Alice chose R and Bob chose M, Bob measures the received qubit from TP and generates a new qubit $|B\rangle$ to be sent to TP, where $|B\rangle \in \{|0\rangle_{B'}, |1\rangle_{B'}\}$. According to Eq. (11), $|\psi\rangle_1$ collapses to $(|0101\rangle + |1000\rangle)_{TABE}$ or $(|0010\rangle + |1111\rangle)_{TABE}$. Then Bob performs the second CNOT gate operation on his own ancillary qubit and Alice's qubit. The state of the whole system is changed as

$$\begin{aligned}|\psi\rangle_3 &= CNOT_{AE} \otimes I_{TBB'}\left[\frac{1}{\sqrt{2}}(|0101\rangle + |1000\rangle)_{TABE} \otimes |0\rangle_{B'}\right]\\ &= \frac{1}{\sqrt{2}}(|0100\rangle + |1000\rangle)_{TABE} \otimes |0\rangle_{B'}\\ &= |\varphi^+\rangle_{TA}|00\rangle_{BE} \otimes |0\rangle_{B'}\end{aligned} \tag{13}$$

or

$$\begin{aligned}|\psi\rangle_4 &= CNOT_{AE} \otimes I_{TBB'}\left[\frac{1}{\sqrt{2}}(|0010\rangle + |1111\rangle)_{TABE} \otimes |1\rangle_{B'}\right]\\ &= \frac{1}{\sqrt{2}}(|0010\rangle + |1110\rangle)_{TABE} \otimes |1\rangle_{B'}\\ &= |\phi^+\rangle_{TA}|10\rangle_{BE} \otimes |1\rangle_{B'}.\end{aligned} \tag{14}$$

TP measures the qubit returned from Alice and his own qubit in the Bell basis for eavesdropping. According to Eqs. (13) and (14), Bob can pass the detection as Bob's ancillary bit is always $|0\rangle$ and he does not get any information of Alice from the ancillary qubit.

Case 3 When Alice selected M and Bob selected R, Alice measures the received qubit from TP in the Z basis and generates $|A\rangle$ according to the measurement to be sent to TP, where $|A\rangle \in \{|0\rangle_{A'}, |1\rangle_{A'}\}$. Similar to case 2, $|\psi\rangle_1$ collapses to $(|0010\rangle + |1000\rangle)_{TABE}$ or $(|0101\rangle + |1111\rangle)_{TABE}$. Bob intercepts $|A\rangle$ and performs the second CNOT gate operation on it and his ancillary qubit again. If Alice prepares $|0\rangle_{A'}$, the state of the whole system after Bob carries out the second CNOT gate is

$$\begin{aligned}|\psi\rangle_5 &= CNOT_{A'E} \otimes I_{TAB}\left[|0\rangle_{A'} \otimes \frac{1}{\sqrt{2}}(|0010\rangle + |1000\rangle)_{TABE}\right]\\ &= \left[|0\rangle_{A'} \otimes \frac{1}{\sqrt{2}}(|0010\rangle + |1000\rangle)_{TABE}\right],\end{aligned} \tag{15}$$

but if Alice prepares $|1\rangle_{A'}$, the state of the entire system should be

$$\begin{aligned}|\psi\rangle_6 &= CNOT_{A'E} \otimes I_{TAB}\left[|1\rangle_{A'} \otimes \frac{1}{\sqrt{2}}(|0101\rangle + |1111\rangle)_{TABE}\right]\\ &= \left[|1\rangle_{A'} \otimes \frac{1}{\sqrt{2}}(|0100\rangle + |1110\rangle)_{TABE}\right].\end{aligned} \tag{16}$$

TP performs the Bell basis measurement on the qubit returned from Bob and his own qubit for eavesdropping. From Eqs. (15, 16), Alice makes a measurement and produces qubit $|A\rangle$ that is consistent with the initial state sent by TP to Alice. At this time, Bob measures his ancillary qubit in the Z basis and the result is always $|0\rangle$. Thus, he cannot distinguish Alice's choice and get her secret in this case.

Case 4 When both Alice and Bob selected M, the state of the system $|\psi\rangle_1$ will collapse to $|0010\rangle_{TABE}$, $|0101\rangle_{TABE}$, $|1000\rangle_{TABE}$ or $|1111\rangle_{TABE}$. Then Bob performs the second CNOT gate and the state of the whole system should be $|0\rangle_{A'}|0010\rangle_{TABE}|1\rangle_{B'}$, $|1\rangle_{A'}|0100\rangle_{TABE}|0\rangle_{B'}$, $|0\rangle_{A'}|1000\rangle_{TABE}|0\rangle_{B'}$, or $|1\rangle_{A'}$ $|1110\rangle_{TABE}|1\rangle_{B'}$. Since Bob's attack does not change the state of qubit owned by TP, Bob's attack will not be discovered. In addition, Alice measures the qubit sent by the TP and generates the same qubit as the measurement result back to the TP. Therefore, Bob still cannot get any valuable information of Alice as his ancillary qubit is always $|0\rangle$.

5.4 Entangle-measure attack

The entangle-measure attack means that Bob measures his ancillary qubits which are entangled with the qubits transmitted between Alice and TP by performing unitary operations to extract Alice's secret information. Bob may perform two unitary operations, U_1 and U_2. The U_1 operation is performed when Bob entangles his ancillary qubit with the qubit sent by TP to Alice. Similarly, the U_2 operation is made on the intercepted qubit that Alice returns to TP and the ancillary qubit. The U_1 can be described as

$$\begin{aligned} U_1(|e\rangle_E|0\rangle) &= a_0|g_0\rangle_E|0\rangle + a_1|g_1\rangle_E|1\rangle \\ U_1(|e\rangle_E|1\rangle) &= b_0|h_0\rangle_E|0\rangle + b_1|h_1\rangle_E|1\rangle, \end{aligned} \tag{17}$$

where $|a_0|^2 + |a_1|^2 = 1$, $|b_0|^2 + |b_1|^2 = 1$, $|e\rangle_E$ is an ancillary qubit of Bob, and $\{|g_0\rangle, |g_1\rangle, |h_0\rangle, |h_1\rangle\}$ are arbitrary states that are not necessarily orthogonal. Then U_2 can be described as

$$\begin{aligned} U_2(|g_0\rangle_E|0\rangle) &= c_0|i_0\rangle_E|0\rangle + c_1|i_1\rangle_E|1\rangle \\ U_2(|g_0\rangle_E|1\rangle) &= d_0|j_0\rangle_E|0\rangle + d_1|j_1\rangle_E|1\rangle \\ U_2(|g_1\rangle_E|0\rangle) &= e_0|k_0\rangle_E|0\rangle + e_1|k_1\rangle_E|1\rangle \\ U_2(|g_1\rangle_E|1\rangle) &= f_0|m_0\rangle_E|0\rangle + f_1|m_1\rangle_E|1\rangle \\ U_2(|h_0\rangle_E|0\rangle) &= l_0|n_0\rangle_E|0\rangle + l_1|n_1\rangle_E|1\rangle \\ U_2(|h_0\rangle_E|1\rangle) &= p_0|v_0\rangle_E|0\rangle + p_1|v_1\rangle_E|1\rangle \\ U_2(|h_1\rangle_E|0\rangle) &= s_0|w_0\rangle_E|0\rangle + s_1|w_1\rangle_E|1\rangle \\ U_2(|h_1\rangle_E|1\rangle) &= t_0|o_0\rangle_E|0\rangle + t_1|o_1\rangle_E|1\rangle, \end{aligned} \tag{18}$$

where $|c_0|^2 + |c_1|^2 = 1$, $|d_0|^2 + |d_1|^2 = 1$, $|e_0|^2 + |e_1|^2 = 1$, $|f_0|^2 + |f_1|^2 = 1$, $|l_0|^2 + |l_1|^2 = 1$, $|p_0|^2 + |p_1|^2 = 1$, $|s_0|^2 + |s_1|^2 = 1$, $|t_0|^2 + |t_1|^2 = 1$, and $\{|i_0\rangle, |i_1\rangle\}$, $\{|j_0\rangle, |j_1\rangle\}$, $\{|k_0\rangle, |k_1\rangle\}$, $\{|m_0\rangle, |m_1\rangle\}$, $\{|n_0\rangle, |n_1\rangle\}$, $\{|v_0\rangle, |v_1\rangle\}$, $\{|w_0\rangle, |w_1\rangle\}$, $\{|o_0\rangle, |o_1\rangle\}$ are arbitrary states and not necessarily orthogonal. In step 1, TP generates $|\psi\rangle_{TAB}$ and distributes these qubits into three sequences S_T, S_A, and S_B.

S_T is owned by TP, S_A is sent to Alice and S_B is sent to Bob. The state of the quantum system after Bob performs U_1 operation on a qubit in S_A and his own ancillary qubit becomes

$$\begin{aligned}|\Psi\rangle_1 =&(U_1 \otimes I_{TB})(|e\rangle_E|\psi\rangle_{TAB})\\ =&\frac{1}{2}(a_0|g_0\rangle|001\rangle + a_1|g_1\rangle|011\rangle + b_0|h_0\rangle|000\rangle + b_1|h_1\rangle|010\rangle\\ &+ a_0|g_0\rangle|100\rangle + a_1|g_1\rangle|110\rangle + b_0|h_0\rangle|101\rangle + b_1|h_1\rangle|111\rangle)_{ETAB}.\end{aligned} \tag{19}$$

In step 2, after receiving each qubit, Alice and Bob randomly choose R or M and send the operated qubits to TP. Then Bob performs the U_2 operation on the qubit returned by Alice and his ancillary qubit.

If both Alice and Bob select M, the state $|\Psi\rangle_1$ collapses to $|\psi\rangle_1$, $|\psi\rangle_2$, $|\psi\rangle_3$ or $|\psi\rangle_4$ with equal probability, where $|\psi\rangle_1 = [(a_0|g_0\rangle|0\rangle + b_0|h_0\rangle|1\rangle)|01\rangle]_{ETAB}$, $|\psi\rangle_2 = [(b_1|h_1\rangle|0\rangle + a_1|g_1\rangle|1\rangle)|10\rangle]_{ETAB}$, $|\psi\rangle_3 = [(a_0|g_0\rangle|1\rangle + b_0|h_0\rangle|0\rangle)|00\rangle]_{ETAB}$, and $|\psi\rangle_4 = [a_1|g_1\rangle|0\rangle+b_1|h_1\rangle|1\rangle)|11\rangle]_{ETAB}$. For example, if Alice's measurement result is $|0\rangle$ and Bob's measurement result is $|1\rangle$, the state of the system collapses to $|\psi\rangle_1$. Now the state of the qubit held by TP can be described by the following reduced density operator

$$\begin{aligned}\rho^T =&tr_{EAB}(|\psi\rangle_{11}\langle\psi|)\\ =&tr_E(a_0|g_0\rangle|0\rangle\langle 0|\langle g_0|a_0^*) + tr_E(b_0|h_0\rangle|1\rangle\langle 1|\langle h_0|b_0^*)\\ =&|a_0|^2|0\rangle\langle 0| + |b_0|^2|1\rangle\langle 1|.\end{aligned} \tag{20}$$

When TP measures his qubit in the Z basis, he should get $|0\rangle$ with certainty according to Eq. (11). Thus, we can obtain

$$\begin{aligned}P(|0\rangle) =&|a_0|^2 = 1,\\ P(|1\rangle) =&|b_0|^2 = 0.\end{aligned} \tag{21}$$

Based on Eqs. (20, 21), we can deduce

$$a_0 = 1, b_0 = 0. \tag{22}$$

Similarly, if the state collapses to $|\psi\rangle_2$, $|\psi\rangle_3$ or $|\psi\rangle_4$, we can get

$$a_1 = 0, b_1 = 1. \tag{23}$$

Thus, the operation U_1 can be rewritten as

$$\begin{aligned}U_1(|e\rangle_E|0\rangle) = a_0|g_0\rangle_E|0\rangle\\ U_1(|e\rangle_E|1\rangle) = b_1|h_1\rangle_E|1\rangle,\end{aligned} \tag{24}$$

and the operation U_2 can be rewritten as

$$\begin{aligned} U_2(|g_0\rangle_E|0\rangle) &= c_0|i_0\rangle_E|0\rangle + c_1|i_1\rangle_E|1\rangle \\ U_2(|g_0\rangle_E|1\rangle) &= d_0|j_0\rangle_E|0\rangle + d_1|j_1\rangle_E|1\rangle \\ U_2(|h_1\rangle_E|0\rangle) &= s_0|w_0\rangle_E|0\rangle + s_1|w_1\rangle_E|1\rangle \\ U_2(|h_1\rangle_E|1\rangle) &= t_0|o_0\rangle_E|0\rangle + t_1|o_1\rangle_E|1\rangle, \end{aligned} \tag{25}$$

where $|c_0|^2 + |c_1|^2 = 1$, $|d_0|^2 + |d_1|^2 = 1$, $|s_0|^2 + |s_1|^2 = 1$, $|t_0|^2 + |t_1|^2 = 1$, and $\{|i_0\rangle, |i_1\rangle\}$, $\{|j_0\rangle, |j_1\rangle\}$, $\{|w_0\rangle, |w_1\rangle\}$, $\{|o_0\rangle, |o_1\rangle\}$ are arbitrary states that are not necessarily orthogonal. After Bob performs a unitary operation U_1 on a qubit in S_A and his ancillary qubit, the entire system's state should be

$$\begin{aligned} |\Psi\rangle_2 =&(U_1 \otimes I_{TB})(|e\rangle_E|\psi\rangle_{TAB}) \\ =&\frac{1}{2}(a_0|g_0\rangle|001\rangle + b_1|h_1\rangle|010\rangle + a_0|g_0\rangle|100\rangle + b_1|h_1\rangle|111\rangle)_{ETAB}. \end{aligned} \tag{26}$$

If Alice selected M and Bob selected R, Alice measures the qubit sent by TP, generates a new qubit $|0\rangle_{A'}$ or $|1\rangle_{A'}$ according to the result, and the state of the system $|\Psi\rangle_2$ collapses to $(|001\rangle + |100\rangle)_{TAB}$ or $(|010\rangle + |111\rangle)_{TAB}$. Suppose Alice prepares $|0\rangle_{A'}$, the state of the whole system after Bob implements the operation U_2 should be

$$\begin{aligned} |\Psi\rangle_3 &= (U_2 \otimes I_{TAB})(a_0|g_0\rangle|0\rangle|001\rangle + a_0|g_0\rangle|0\rangle|100\rangle)_{EA'TAB} \\ &= (a_0c_0|i_0\rangle|0\rangle|0\rangle|01\rangle + a_0c_1|i_1\rangle|1\rangle|0\rangle|01\rangle + a_0c_0|i_0\rangle|0\rangle|0\rangle|10\rangle \\ &\quad +a_0c_1|i_1\rangle|1\rangle|0\rangle|10\rangle)_{EA'ATB} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} a_0c_0|i_0\rangle|0\rangle|0\rangle(|\varphi^+\rangle + |\varphi^-\rangle) + a_0c_1|i_1\rangle|1\rangle|0\rangle(|\varphi^+\rangle + |\varphi^-\rangle) \\ +a_0c_0|i_0\rangle|0\rangle|0\rangle(|\varphi^+\rangle - |\varphi^-\rangle) + a_0c_1|i_1\rangle|1\rangle|0\rangle(|\varphi^+\rangle - |\varphi^-\rangle) \end{bmatrix}_{EA'ATB} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^+\rangle + a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^-\rangle \\ +a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^+\rangle + a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^-\rangle \\ +a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^+\rangle - a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^-\rangle \\ +a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^+\rangle - a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^-\rangle \end{pmatrix}_{EA'ATB} . \end{aligned} \tag{27}$$

In this case, the state of the qubit held by TP and the qubit sent back by Bob is

$$\begin{aligned} \rho^{TB} &= tr_{EA'A}(|\Psi\rangle_{33}\langle\Psi|) \\ &= \frac{1}{2}\begin{bmatrix} tr_{EA'A}(a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^+\rangle\langle\varphi^+|\langle i_0|\langle 0|\langle 0|a_0^*c_0^*) + tr_{EA'A}(a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^-\rangle \\ \langle\varphi^-|\langle i_0|\langle 0|\langle 0|a_0^*c_0^*) + tr_{EA'A}(a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^+\rangle\langle\varphi^+|\langle i_1|\langle 1|\langle 0|a_0^*c_1^*) \\ +tr_{EA'A}(a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^-\rangle\langle\varphi^-|\langle i_1|\langle 1|\langle 0|a_0^*c_1^*) + tr_{EA'A}((a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^+\rangle \\ \langle\varphi^+|\langle i_0|\langle 0|\langle 0|a_0^*c_0^*) - tr_{EA'A}(a_0c_0|i_0\rangle|0\rangle|0\rangle|\varphi^-\rangle\langle\varphi^-|\langle i_0|\langle 0|\langle 0|a_0^*c_0^*) \\ +tr_{EA'A}(a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^+\rangle\langle\varphi^+|\langle i_1|\langle 1|\langle 0|a_0^*c_1^*) - tr_{EA'A}(a_0c_1|i_1\rangle|1\rangle|0\rangle|\varphi^-\rangle \\ \langle\varphi^-|\langle i_1|\langle 1|\langle 0|a_0^*c_1^*) \end{bmatrix} \\ &= \frac{1}{2}\begin{bmatrix} (|a_0c_0|^2 + |a_0c_1|^2 + |a_0c_0|^2 + |a_0c_1|^2)|\varphi^+\rangle\langle\varphi^+| \\ +(|a_0c_0|^2 + |a_0c_1|^2 - |a_0c_0|^2 - |a_0c_1|^2)|\varphi^-\rangle\langle\varphi^-| \end{bmatrix}. \end{aligned} \tag{28}$$

TP checks whether there is eavesdropping at this time by performing the Bell basis measurement on the qubit returned by Bob and his own qubit. Only when TP gets $|\phi^-\rangle$ or $|\varphi^-\rangle$ with probability 0 and $|\phi^+\rangle$ or $|\varphi^+\rangle$ with probability 1/2, Bob's attack cannot be detected. Therefore, the equation below must hold true

$$\begin{aligned} P(|\varphi^-\rangle) =& \frac{1}{2}\left(|a_0c_0|^2+|a_0c_1|^2-|a_0c_0|^2-|a_0c_1|^2\right)=0, \\ P(|\varphi^+\rangle) =& \frac{1}{2}\left(|a_0c_0|^2+|a_0c_1|^2+|a_0c_0|^2+|a_0c_1|^2\right)=\frac{1}{2}. \end{aligned} \tag{29}$$

In terms of Eqs. (22, 23), it can be deduced that

$$|c_0|^2+|c_1|^2=\frac{1}{2}. \tag{30}$$

Similarly, if Alice prepares $|1\rangle_{A'}$, the state of the whole system after Bob implements the operation U_2 should be

$$\begin{aligned} |\Psi\rangle_4 &= (U_2\otimes I_{TAB})(b_1|h_1\rangle|1\rangle|010\rangle+b_1|h_1\rangle|1\rangle|111\rangle)_{EA'TAB} \\ &= (b_1t_0|o_0\rangle|0\rangle|1\rangle|00\rangle+b_1t_1|o_1\rangle|1\rangle|1\rangle|00\rangle+b_1t_0|o_0\rangle|0\rangle|1\rangle|11\rangle \\ &\quad +b_1t_1|o_1\rangle|1\rangle|1\rangle|11\rangle)_{EA'ATB} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} b_1t_0|o_0\rangle|0\rangle|1\rangle(|\phi^+\rangle+|\phi^-\rangle)+b_1t_1|o_1|1\rangle|1\rangle(|\phi^+\rangle+|\phi^-\rangle) \\ +b_1t_0|o_0\rangle|0\rangle|1\rangle(|\phi^+\rangle-|\phi^-\rangle)+b_1t_1|o_1\rangle|1\rangle|1\rangle(|\phi^+\rangle-|\phi^-\rangle) \end{bmatrix}_{EA'ATB} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^+\rangle+b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^-\rangle \\ +b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^+\rangle+b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^-\rangle \\ +b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^+\rangle-b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^-\rangle \\ +b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^+\rangle-b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^-\rangle \end{pmatrix}_{EA'ATB}. \end{aligned} \tag{31}$$

In this case, ρ^{TB} should be

$$\begin{aligned} \rho^{TB} &= tr_{EA'A}(|\Psi\rangle_{44}\langle\Psi|) \\ &= \frac{1}{2}\begin{bmatrix} tr_{EA'A}(b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^+\rangle\langle\phi^+|\langle o_0|\langle 0|\langle 1|b_1^*t_0^*)+tr_{EA'A}(b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^-\rangle \\ \langle\phi^-|\langle o_0|\langle 0|\langle 1|b_1^*t_0^*)+tr_{EA'A}(b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^+\rangle\langle\phi^+|\langle o_1|\langle 1|\langle 1|b_1^*t_1^*) \\ +tr_{EA'A}(b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^-\rangle\langle\phi^-|\langle o_1|\langle 1|\langle 1|b_1^*t_1^*+tr_{EA'A}(b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^+\rangle \\ \langle\phi^+|\langle o_0|\langle 0|\langle 1|b_1^*t_0^*)-tr_{EA'A}(b_1t_0|o_0\rangle|0\rangle|1\rangle|\phi^-\rangle\langle\phi^-|\langle o_0|\langle 0|\langle 1|b_1^*t_0^*) \\ +tr_{EA'A}(b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^+\rangle\langle\phi^+|\langle o_1|\langle 1|\langle 1|b_1^*t_1^*)-tr_{EA'A}(b_1t_1|o_1\rangle|1\rangle|1\rangle|\phi^-\rangle \\ \langle\phi^-|\langle o_1|\langle 1|\langle 1|b_1^*t_1^*) \end{bmatrix} \\ &= \frac{1}{2}\begin{bmatrix} (|b_1t_0|^2+|b_1t_1|^2+|b_1t_0|^2+|b_1t_1|^2)|\phi^+\rangle\langle\phi^+| \\ +(|b_1t_0|^2+|b_1t_1|^2-|b_1t_0|^2-|b_1t_1|^2)|\phi^-\rangle\langle\phi^-| \end{bmatrix}. \end{aligned} \tag{32}$$

TP measures his qubit and Bob's qubit in the Bell basis to detect eavesdropping. When TP obtains $|\phi^-\rangle$ or $|\varphi^-\rangle$ with the probability of 0 and acquires $|\phi^+\rangle$ or $|\varphi^+\rangle$ with the probability of 1 after the measurement, Bob's attack cannot be discovered.

As a result, Eq. (33) must be correct

$$\begin{aligned} P(|\phi^-\rangle) =& \frac{1}{2}(|b_1t_0|^2 + |b_1t_1|^2 - |b_1t_0|^2 - |b_1t_1|^2) = 0, \\ P(|\phi^+\rangle) =& \frac{1}{2}(|b_1t_0|^2 + |b_1t_1|^2 + |b_1t_0|^2 + |b_1t_1|^2) = \frac{1}{2}. \end{aligned} \tag{33}$$

In terms of Eqs. (22, 23), we can get

$$|t_0|^2 + |t_1|^2 = \frac{1}{2}. \tag{34}$$

According to Eq. (24), it can be inferred that after U_1 operation, Bob's ancillary qubits and Alice's qubits are independent and have no entanglement relationship, thus Bob cannot get Alice's information by measuring $|g_0\rangle$ or $|h_1\rangle$. Based on Eqs. (30, 34), it is obvious they contradict with the initial assumptions $|c_0|^2 + |c_1|^2 = 1$ and $|t_0|^2 + |t_1|^2 = 1$ and such U_2 operation does not exist if Bob does not want to be detected. Then we can conclude that the proposed improved protocol is robust against the entangle-measure attack.

5.5 TP attack

Although the semi-honest TP cannot be allowed to collaborate with any participant, he may gather as much information about both participants as possible for learning the secrets of Alice or Bob. In step 3, TP can obtain MA_i and MB_i according to measuring the qubit returned by Alice and Bob. In step 4, Alice and Bob publish RA_j and RB_j, respectively. TP compares $P_j = RA_j \oplus RB_j \oplus MA_i \oplus MB_i = x_j \oplus y_j$. Even though he obtains MA_i, MB_i, RA_j and RB_j, the secrets of participants are still unknown to him since TP has no knowledge about the K_{AB} shared by two participants.

6 Conclusion

In this paper, the SQPC protocol proposed by Yan et al [35] has been shown to be vulnerable to the double CNOT attack, by which a malicious attacker is possible to steal one of the honest participant's secret bits without being detected. To effectively resist the double CNOT attack, an improved protocol has been put forward with no need to strengthen the ability of participants. In addition, the proposed improved protocol has also been proved to be secure against some typical attacks such as intercept-resend attack, measure-resend attack, and entangle-measure attack. But standard security analysis of semi-quantum protocols remains challenging and deserves further investigation.

Acknowledgements This work was supported by the Key Project of Hunan Province Education Department (Grant No. 20A471), the Joint Funds of the National Natural Science Foundation of China and China

General Technology Research Institute (Grant No. U1736113), and the Natural Science Foundation of Hunan Province (Grant No. 2018JJ2403).

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
3. Mayers, D.: Unconditional security in quantum cryptography. J. ACM (JACM) **48**(3), 351–406 (2001)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984)
5. Cabello, A.: Quantum key distribution in the holevo limit. Phys. Rev. Lett. **85**(26), 5635 (2000)
6. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
7. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321 (2008)
8. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
9. Grice, W.P., Qi, B.: Quantum secret sharing using weak coherent states. Phys. Rev. A **100**(2), 022339 (2019)
10. Boykin, P.O., Vwani, R.: Optimal encryption of quantum bits. Phys. Rev. A **67**(4), 042317 (2003)
11. Liu, J., Li, Q., Quan, J., Wang, C., Shi, J., Situ, H.: Efficient quantum homomorphic encryption scheme with flexible evaluators and its simulation. Des. Codes Cryptogr., pp 1–15 (2022)
12. Jakobi, M., Simon, C., Gisin, N., Bancal, J.D., Branciard, C., Walenta, N., Zbinden, H.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**(2), 022301 (2011)
13. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**(4), 042318 (2016)
14. 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)
15. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**(7), 1561–1565 (2010)
16. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**(12), 3160–3163 (2011)
17. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
18. Liu, W., Wang, Y.B., Wei, C.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**(4), 583–583 (2012)
19. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**(1), 212–218 (2013)
20. 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)
21. 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)
22. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**(5), 1981–1990 (2013)
23. Huang, S., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum Inf. Process. **14**(11), 1–11 (2015)
24. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. **55**(6), 2969–2976 (2016)
25. Liu, W., Wang, Y.B., Wang, X.M.: Quantum multi-party private comparison protocol using d-dimensional Bell states. Int. J. Theor. Phys. **54**(6), 1830–1839 (2015)
26. Ye, T.Y.: Quantum private comparison via cavity QED. Commun. Theor. Phys. **67**(2), 147 (2017)

27. Hung, S.M., Hwang, S.L., Hwang, T., Kao, S.H.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process. **16**(2), 36 (2017)
28. Ye, C.Q., Ye, T.Y.: Circular multi-party quantum private comparison with n-level single-particle states. Int. J. Theor. Phys. **58**(4), 1282–1294 (2019)
29. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**(14), 140510 (2007)
30. Chou, W.H., Hwang, T., Gu, J.: Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv preprint arXiv:1607.07961 (2016)
31. Thapliyal, K., Sharma, R.D., Pathak, A.: Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int. J. Quantum Inf. **16**(5), 1850047 (2016)
32. Lang, Y.F.: Semi-quantum private comparison using single photons. Int. J. Theor. Phys. **57**(10), 1–8 (2018)
33. Lin, P.H., Hwang, T., Tsai, C.W.: Efficient semi-quantum private comparison using single photons. Quantum Inf. Process. **18**(7), 207 (2019)
34. Xie, L., Li, Q., Yu, F., Luo, X.P., Zhang, C.: Cryptanalysis and improvement of a semi-quantum private comparison protocol based on Bell states. Quantum Inf. Process. **20**(7), 244 (2021)
35. Yan, L., Zhang, S., Chang, Y., Wan, G., Yang, F.: Semi-quantum private comparison protocol with three-particle G-like states. Quantum Inf. Process. **20**(1), 17 (2021)
36. Krawec, W.O.: Mediated semiquantum key distribution. Phys. Rev. A **91**(3), 032323 (2015)
37. Chen, L., Li, Q., Liu, C., Peng, Y., Yu, F.: Efficient mediated semi-quantum key distribution. Phys. A **582**, 126265 (2021)