Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 694798, 13 pages
http://dx.doi.org/10.1155/2014/694798

Research Article

Controlled Bidirectional Quantum Secure Direct Communication

Yao-Hsin Chou,[1] Yu-Ting Lin,[1] Guo-Jyun Zeng,[1] Fang-Jhu Lin,[1] and Chi-Yuan Chen[2]

[1] *Department of Computer Science and Information Engineering, National Chi Nan University, No. 1, University Road, Puli, Nantao 545, Taiwan*
[2] *Department of Computer Science and Information Engineering, National Ilan University, No. 1, Section 1, Shen-Lung Road, I-Lan 260, Taiwan*

Correspondence should be addressed to Chi-Yuan Chen; chiyuan.chen@ieee.org

Received 18 March 2014; Accepted 13 April 2014; Published 5 May 2014

Academic Editor: Han-Chieh Chao

We propose a novel protocol for controlled bidirectional quantum secure communication based on a *nonlocal swap* gate scheme. Our proposed protocol would be applied to a system in which a controller (supervisor/Charlie) controls the bidirectional communication with quantum information or secret messages between legitimate users (Alice and Bob). In this system, the legitimate users must obtain permission from the controller in order to exchange their respective quantum information or secret messages simultaneously; the controller is unable to obtain any quantum information or secret messages from the decoding process. Moreover, the presence of the controller also avoids the problem of one legitimate user receiving the quantum information or secret message before the other, and then refusing to help the other user decode the quantum information or secret message. Our proposed protocol is aimed at protecting against external and participant attacks on such a system, and the cost of transmitting quantum bits using our protocol is less than that achieved in other studies. Based on the *nonlocal swap* gate scheme, the legitimate users exchange their quantum information or secret messages without transmission in a public channel, thus protecting against eavesdroppers stealing the secret messages.

1. Introduction

There have been many ingenious applications of quantum information science through the combination of quantum communication and quantum cryptography [1, 2] since Bennett and Brassard [3] first proposed the original quantum key distribution (QKD) protocol in 1984, which is a way for two remote users to share a private key for encrypting or decrypting secret messages in a quantum channel. This was one of the most promising applications of quantum machine, and many more QKD protocols have since been presented [4–8].

The quantum secure direct communication (QSDC) protocol differs from the QKD protocols used to distribute private keys and has been proposed [9] for directly transmitting secret messages, without having to share a private key between two legitimate users beforehand. Moreover, Boström and Felbinger [10] presented a "Ping Pong" QSDC using Einstein-Podolsky-Rosen (EPR), but some researches [11–13] noted that the "Ping Pong" protocol is insecure for direct communication in a noisy quantum channel. Deng et al. [14] also presented a two-step QSDC protocol using EPR pairs, which is useful for QSDC protocols not sharing the private key first; quantum bits (qubits) carrying the secret messages are transmitted directly. Therefore, bidirectional QSDC (BQSDC) is a concept extended from QSDC protocols. Most QSDC protocols offer only one way communication, so that the secret message can only be transmitted from one legitimate user to the other. If two remote legitimate users want to exchange their respective secret messages using the QSDC protocol, they have to implement it twice. In this situation, one legitimate user can receive the secret message from the other, but fail to keep their promise to transmit their own message. Thus, BQSDC protocols must be designed in

such a way that two remote legitimate users transmit their respective secret messages simultaneously in one way communication. Nguyen [15] improved the ping pong protocol, and first proposed the BQSDC protocol (called quantum dialogue protocol) which enables two remote legitimate users to exchange secret messages. Other BQSDC protocols [15–17] are based on the QSDC protocols. Legitimate users must transmit the qubit with the secret message in the public channel under any local operation and classical communication (LOCC) in order to obtain the secret message from the other party; however, an eavesdropper could steal the qubits or attack the protocol without being discovered. To prevent an external eavesdropper extracting the secret messages, researchers developed BQSDC protocols that do not transmit encoded qubits [15]. In general, BQSDC protocols assume that participants are honest, so they are unable to protect against participant attacks by dishonest participants utilizing the order of measurement announce.

To prevent this asymmetric situation, we suggest that a fair third party should be involved to authenticate participants and prevent the above situation. In most one-way or bidirectional protocols, third parties are designed to identify the participants, so receivers must get permission from the third party to obtain the secret messages. In our proposed protocol, we call the fair third party the controller or supervisor (represented as Charlie). This controller not only provides authentication of legitimate users, but also prevents participant attacks in the QSDC protocol. In some applications, we need a powerful third-party to assist the process or provide costly equipment [18, 19]. We take a simple example of online shopping to explain why controller is needed [see Figure 1]. Assume the controller is the online shopping mall, Alice and Bob are users and the detailed steps are described as follows.

Step 1: Alice and Bob send registration request to the controller.

Step 2: controller authenticates them as members.

Step 3: controller transmits GHZ sequences to Alice and Bob.

Step 4: they check the channel security with classical bits transmitted.

Step 5: Alice and Bob exchange their quantum information with our protocol.

Most QSDC protocols claim that their protocol can safely transmit secret messages by qubits via a public channel; however, eavesdroppers can still steal or attack the qubits in transmission. Some researchers have taken advantage of entanglement swapping to design QSDC protocols that exclude the encoded qubit transmission process. Yan and Zhang [20] presented a scheme for QSDC based on teleportation without transmitting a qubit with a secret message. Using the teleportation scheme, the legitimate user can send an unknown quantum state through a quantum channel to another user. Before Yan's protocol, there were many QSDC protocols that just transmitted classical information instead of quantum information.

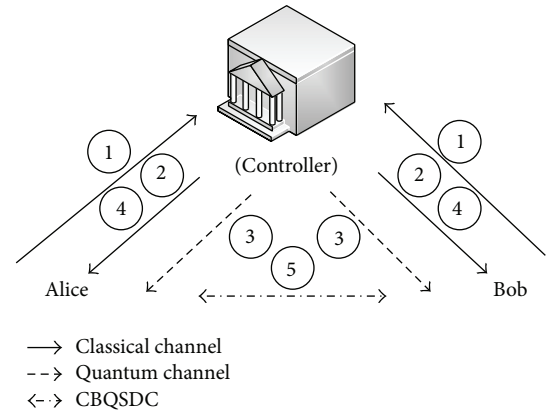

Figure 1: The demonstration of online shopping.

Due to the quantum property of noncloning [21], quantum information must be transmitted from the sender to the receiver using entanglement swapping [22]. In addition, it is far more difficult to produce quantum resources than classical ones. If we use quantum resources to send classical messages, we may sometimes find that the cost of the quantum resources is higher than that of the secret message itself. Overall, if the QSDC protocol can transmit quantum information, it is also able to transmit classical messages, but not vice versa. So it takes more effort to come up with a QSDC protocol that transmits quantum information than one that transmits classical information.

Therefore, we propose a novel protocol for controlled bidirectional QSDC based on a *nonlocal swap* gate scheme without transmitting the qubits carrying the secret message. Legitimate users can simultaneously exchange their respective quantum information or classical messages with each other, with the controller's permission. Our protocol has the ability to transmit quantum information, which is rare in QSDC protocols. This is advantageous because when we use quantum resources to transmit classical messages, sometimes the cost will be higher than the resource cost in using classical cryptography, which can achieve the same goal. Moreover, quantum information is noncloning. This means that an arbitrary quantum state cannot be reproduced if we do not know its actual state; this makes quantum information more secure than classical information. We prove that our scheme is reliable by analyzing the security; the analysis shows that our protocol can resist both internal and external attacks. Moreover, we ensure that it is impossible for one participant to quickly receive the other's message. Performance comparison is also provided, and our quantum resource costs are shown to be the lowest. [23] demonstrates that a *nonlocal swap* gate requires at least two EPR pairs. Our protocol uses 5 qubits to accomplish communication, and the supernumerary one qubit is used for the controller. Compared to other CQSDC protocols, the cost of our proposed protocol is the lowest.

In Section 2, we present works related to our protocol. In Section 3, we present the controlled bidirectional QSDC protocol based on the *nonlocal swap* gate. In Section 4,

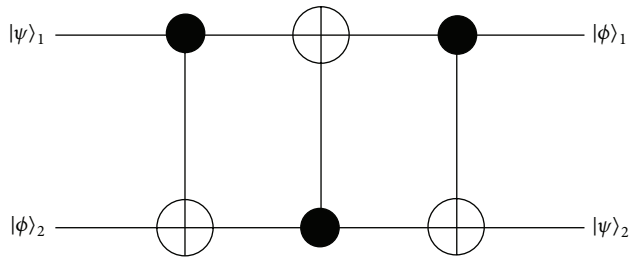

FIGURE 2: The *swap* gate cascades three quantum *Controlled-Not* gates.

we analyze the security of our protocol. In Section 5, we compare the performance of our protocol with previous QSDC protocols. Finally, Section 6 offers conclusions drawn from this paper.

2. The Nonlocal SWAP Gate Scheme

The swap gate plays an important role in network design for qubit quantum computation. The quantum operation of the local swap gate [24, 25] permutes the state of two qubits; therefore, we propose that legitimate users can interchange their information with a swap gate as follows:

$$U_{\text{swap}}|\psi\rangle_1|\phi\rangle_2 = |\phi\rangle_1|\psi\rangle_2. \tag{1}$$

It can be represented by the following matrix:

$$U_{\text{swap}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2}$$

On the quantum circuit, this can be achieved by cascading three quantum *Controlled-NOT* (CNOT) gates [see Figure 2] for arbitrary qubit states $|\psi\rangle_1$ and $|\phi\rangle_2$ as follows:

$$C_{12}C_{21}C_{12}|\psi\rangle_1|\phi\rangle_2 = |\phi\rangle_1|\psi\rangle_2. \tag{3}$$

We define C_{ij} as a notation of a quantum CNOT gate. The first qubit i is a control bit, which performs the *NOT* operation on the second target qubit j only when the control qubit i is $|1\rangle$ as follows:

$$\begin{aligned} |\psi_1\rangle\,|\psi_2\rangle &\xrightarrow{C_{12}} |\psi_1\rangle\,|\psi_1 \oplus \psi_2\rangle \\ |\psi_1\rangle\,|\psi_2\rangle &\xrightarrow{C_{12}} |\psi_1 \oplus \psi_2\rangle\,|\psi_2\rangle\,, \end{aligned} \tag{4}$$

where $\oplus$ denotes addition modulo 2.

Because the framework of the bidirectional QSDC protocols is established on two remote legitimate users who want to exchange secret messages, we have to use the swap gate in a nonlocal manner. Fortunately, Barenco et al. [26] proposed a *nonlocal swap* gate scheme that can be used to construct a bidirectional QSDC protocol. We will introduce this *nonlocal swap* gate scheme below.

Suppose that two remote legitimate users, Alice and Bob, want to swap their respective unknown qubits $|\psi\rangle_0 = a|0\rangle + b|1\rangle$ and $|\psi\rangle_5 = c|0\rangle + d|1\rangle$ with each other. To accomplish this task, they have to share two quantum pairs previously with the same maximally entangled state $|\phi\rangle_{13} = (1/2)(|00\rangle + |11\rangle)$ and $|\phi\rangle_{24} = (1/2)(|00\rangle + |11\rangle)$. Therefore, there are three qubits 0, 1, and 2 given by Alice, and another qubits 3, 4, and 5 given by Bob. To interchange qubit 0 and qubit 5, Alice and Bob will perform the following protocol [see Figure 3].

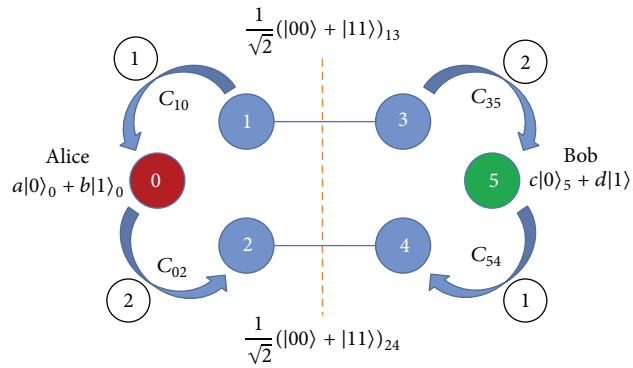

FIGURE 3: The demonstration of *nonlocal swap* gate scheme.

Step 1. Alice implements C_{10} (the CNOT gate on qubit 1 and qubit 0) and then C_{02} while Bob performs C_{54} and then C_{35}.

Step 2. After Alice measures her qubit 2 and Bob measures his qubit 4, they communicate the result to each other. If the results are the same, they go to Step 3, or Alice and Bob apply the *NOT* gate to the remaining qubits in their possession. The *NOT* gate can be presented by the following matrix:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5}$$

Step 3. Alice and Bob apply the rotation to qubit 1 and qubit 3, respectively. Consider the following:

$$\sqrt{\frac{1}{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{6}$$

Step 4. Alice measures her qubit 1 and Bob measures his qubit 3; they then communicate the result to each other. If the results are the same, the qubit state will have been swapped. Otherwise, Alice and Bob apply the unitary transformation

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{7}$$

to qubit 0 and qubit 5, respectively, with the disagreeing results. Finally, they successfully swap their quantum information to a different place.

This protocol not only successfully swaps quantum information to different places, but also simultaneously exchanges the quantum information. It is suitable for bidirectional QSDC protocol, but it cannot protect against one legitimate user deriving the quantum information from the other side first, and then not assisting the other side in decoding their quantum information. Therefore, we designed a new protocol with a controller in order to avoid an uncoordinated condition between the legitimate users based on Barenco's protocol.

3. Controlled Bidirectional Quantum Secure Direct Communication

Before introducing our protocol for controlled bidirectional QSDC based on a *nonlocal swap* gate [26], we need to define four Bell states and three-particle GHZ states in our protocol. The four Bell states are

$$\begin{aligned}
\left|\Phi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right)\\
\left|\Phi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{-}\rangle + |{-}{+}\rangle\right)\\
\left|\Psi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle - |{-}{-}\rangle\right)\\
\left|\Psi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{-}\rangle - |{-}{+}\rangle\right).
\end{aligned} \tag{8}$$

The eight GHZ states in a three-particle maximally entangled quantum system are as follows:

$$\begin{aligned}
\left|\Psi_{000}\right\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{+}\rangle + |{-}{-}\rangle\right) + |-\rangle\left(|{+}{-}\rangle + |{-}{+}\rangle\right)\right]\\
\left|\Psi_{001}\right\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{-}\rangle + |{-}{+}\rangle\right) + |-\rangle\left(|{-}{-}\rangle + |{+}{+}\rangle\right)\right]\\
\left|\Psi_{010}\right\rangle &= \frac{1}{\sqrt{2}}\left(|001\rangle + |110\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{+}\rangle - |{-}{-}\rangle\right) - |-\rangle\left(|{+}{-}\rangle - |{-}{+}\rangle\right)\right]\\
\left|\Psi_{011}\right\rangle &= \frac{1}{\sqrt{2}}\left(|001\rangle - |110\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{-}\rangle - |{-}{+}\rangle\right) - |-\rangle\left(|{+}{+}\rangle - |{-}{-}\rangle\right)\right]\\
\left|\Psi_{100}\right\rangle &= \frac{1}{\sqrt{2}}\left(|010\rangle + |101\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{+}\rangle - |{-}{-}\rangle\right) + |-\rangle\left(|{+}{-}\rangle - |{-}{+}\rangle\right)\right]\\
\left|\Psi_{101}\right\rangle &= \frac{1}{\sqrt{2}}\left(|010\rangle - |101\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{-}\rangle - |{-}{+}\rangle\right) + |-\rangle\left(|{+}{+}\rangle - |{-}{-}\rangle\right)\right]\\
\left|\Psi_{110}\right\rangle &= \frac{1}{\sqrt{2}}\left(|011\rangle + |100\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{+}\rangle + |{-}{-}\rangle\right) - |-\rangle\left(|{+}{-}\rangle + |{-}{+}\rangle\right)\right]\\
\left|\Psi_{111}\right\rangle &= \frac{1}{\sqrt{2}}\left(|011\rangle - |100\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left[|+\rangle\left(|{+}{-}\rangle + |{-}{+}\rangle\right) - |-\rangle\left(|{+}{+}\rangle + |{-}{-}\rangle\right)\right],
\end{aligned} \tag{9}$$

where $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$. Now, let us describe the CBQSDC protocol. Suppose that the two remote legitimate users, Alice and Bob, want to swap their respective unknown qubit to each other. To accomplish this, they must initially share one GHZ state and one EPR pair. To swap their qubits, Alice and Bob must have permission from Charlie (controller), according to the following protocol.

First, we have to detect whether an eavesdropper exists in the quantum channel and authenticate the legitimate users.

Step 1. The controller (supervisor) Charlie generates a group of N three-particle GHZ states randomly in one of the eight three-particle GHZ states ($|\Psi_{ijk}\rangle_{ABC}$, $i, j, k = 0, 1$) between legitimate users Alice and Bob. For a group of N three-particle GHZ states, Charlie keeps the sequence of particles C for himself and sends the sequence of particles A and the sequence of particles B to Alice and Bob, respectively.

Step 2. Once Alice and Bob confirm with Charlie that they have received the sequences of particles A and B, respectively, they have an order to choose the sufficiently random subset of A and B sequence for detecting an eavesdropper. First, Alice and Bob publish the positions of GHZ states which are used for detection in the quantum channel, and they require that Charlie announce the initial states of the corresponding GHZ states. Once Charlie has published the initial states, Alice and Bob measure the selected particles of sequences A and B using one of two measuring basis, Z-basis $|0\rangle, |1\rangle$ or X-basis $|+\rangle, |-\rangle$ randomly, and then announce the measuring bases and results for the selected particles of sequences A and B through a classical channel. According to the public information, the three parties (Alice, Bob, and Charlie) measure their corresponding particles of A sequence, B sequence, and C sequence using the same bases, respectively, and they will reveal their measurement results for analysis. According to the measurement results of the three parties, they can check whether the quantum channel is secure through the error rate. If the error rate is higher than the predetermined threshold, the communication must be terminated; otherwise, Alice, Bob, and Charlie go to the next step.

Step 3. After ensuring the security of the quantum channel, Charlie uses some of the remaining C particles to produce EPR pairs between Alice and Bob. Only Charlie measures some of the remaining C particles using X-basis, and gives the

position to Alice and Bob. The particles in the same positions of A sequence and B sequence will then be maximally entangled with each other between Alice and Bob. Consider the following:

$$
\begin{aligned}
|\Psi_{000}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|00\rangle + |11\rangle)|+\rangle + (|00\rangle - |11\rangle)|-\rangle]_{ABC} \\
|\Psi_{001}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|00\rangle - |11\rangle)|+\rangle + (|00\rangle + |11\rangle)|-\rangle]_{ABC} \\
|\Psi_{010}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|00\rangle + |11\rangle)|+\rangle - (|00\rangle - |11\rangle)|-\rangle]_{ABC} \\
|\Psi_{011}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|00\rangle - |11\rangle)|+\rangle - (|00\rangle + |11\rangle)|-\rangle]_{ABC} \\
|\Psi_{100}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|01\rangle + |10\rangle)|+\rangle + (|01\rangle - |10\rangle)|-\rangle]_{ABC} \\
|\Psi_{101}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|01\rangle - |10\rangle)|+\rangle + (|01\rangle + |10\rangle)|-\rangle]_{ABC} \\
|\Psi_{110}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|01\rangle + |10\rangle)|+\rangle - (|01\rangle - |10\rangle)|-\rangle]_{ABC} \\
|\Psi_{111}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle)_{ABC} \\
&= \frac{1}{\sqrt{2}}[(|01\rangle - |10\rangle)|+\rangle - (|01\rangle + |10\rangle)|-\rangle]_{ABC}.
\end{aligned}
\tag{10}
$$

Step 4. After the quantum channel is secure, Charlie prepares EPR pairs and GHZ states from the remaining C sequence to implement the protocol. To understand the process of our protocol easily, we will number the qubits [see Figure 4]. Assume that Charlie has already prepared an EPR pair $|\Phi^+\rangle_{25} = (1/\sqrt{2})(|00\rangle + |11\rangle)$ for Alice and Bob, and then a GHZ state $|\Psi_{000}\rangle_{134} = (1/\sqrt{2})(|000\rangle + |111\rangle)$ for Alice, Charlie, and Bob. Here, the GHZ state and EPR pair can be collocated randomly. Alice and Bob want to swap their

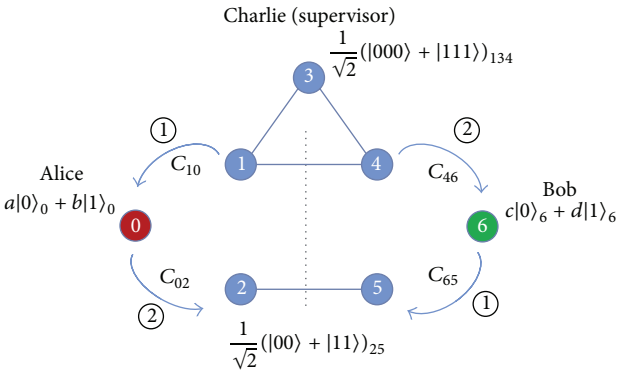

Figure 4: The scenario of our proposed protocol.

respective unknown qubits $|\psi\rangle_0 = a|0\rangle + b|1\rangle$ and $|\psi\rangle_6 = c|0\rangle + d|1\rangle$ with each other. Therefore, there are three qubits 0, 1, and 2 given by Alice, and the other three qubits 4, 5, and 6 are given by Bob. The remaining qubit 3 is for controller Charlie [see Figure 4]. The quantum system becomes

$$
\begin{aligned}
&|\psi\rangle_0 \otimes |\Psi_{000}\rangle_{134} \otimes |\Phi^+\rangle \otimes |\psi\rangle_6 \\
&= (a|0\rangle + b|1\rangle)_0 \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{134} \\
&\otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{25} \otimes (c|0\rangle + d|1\rangle)_6.
\end{aligned}
\tag{11}
$$

Step 5. After confirming these steps above, Alice implements C_{10} and then C_{02} while Bob performs C_{65} and then C_{46}.

Step 6. After Alice measures her qubit 2 and Bob measures his qubit 5, they communicate the results to each other and Charlie. If the results are the same, they go to the next step. Otherwise, Alice and Bob apply the *NOT* gate to the remaining qubits in their possession, as in Step 2 of the *nonlocal swap* gate scheme. Suppose that there is a $|0\rangle_2 \otimes |1\rangle_5$ difference between Alice and Bob's measurement results of qubits 2 and 5. Because there are two different results, Alice, Bob, and Charlie have to apply the X gate to their remaining qubits 0, 1, 3, 4, and 6. Here, Alice and Bob publish their measurement results of qubit 1 and 4 as $|0\rangle_1 \otimes |1\rangle_4$ and Charlie measures his qubit 3 as $|0\rangle_3$. The measurement result of qubit 3 cannot be published, but according to the results of qubits 1, 2, 4, and 5, Charlie will tell Alice and Bob to apply the Z gate to transfer their qubits 0 and 6 to obtain the correct qubit state $(c|0\rangle + d|1\rangle)_0$ and $(a|0\rangle + b|1\rangle)_6$. Consider the following:

$$
\begin{aligned}
&C_{46}C_{02}C_{65}C_{10}\left(|\psi\rangle_0 \otimes |\Psi_{000}\rangle_{134} \otimes |\Phi^+\rangle \otimes |\psi\rangle_6\right) \\
&= \frac{1}{2}\,[\,|00\rangle_{25}\,(ac\,|00000\rangle + ad\,|11110\rangle \\
&\qquad + bd\,|10001\rangle + bc\,|01111\rangle)_{01346} \\
&\quad + |01\rangle_{25}\,(ac\,|11111\rangle + ad\,|00001\rangle \\
&\qquad + bd\,|01110\rangle + bc\,|10000\rangle)_{01346}
\end{aligned}
$$

$$
\begin{aligned}
&+ |10\rangle_{25} (ac\,|11111\rangle + ad\,|00001\rangle \\
&\qquad + bd\,|01110\rangle + bc\,|10000\rangle)_{01346} \\
&+ |11\rangle_{25} (ac\,|00000\rangle + ad\,|11110\rangle \\
&\qquad + bd\,|10001\rangle + bc\,|01111\rangle)_{01346}]
\end{aligned} \tag{12}
$$

$$
\begin{aligned}
&|01\rangle_{25} (ac\,|11111\rangle + ad\,|00001\rangle \\
&\qquad + bd\,|01110\rangle + bc\,|10000\rangle)_{01346} \\
&\xrightarrow{X_{01346}} |01\rangle_{25} (ac\,|00000\rangle + ad\,|11110\rangle \\
&\qquad + bd\,|10001\rangle + bc\,|01111\rangle)_{01346}.
\end{aligned} \tag{13}
$$

Step 7. Alice, Bob, and Charlie apply the *Hadamard* gate to qubits 1, 4, and 3, respectively, as Step 3 of the *nonlocal swap* gate scheme.

Step 8. Alice and Bob measure their respective qubits 1 and qubit 4, and publish the results for Charlie. Once the results from Alice and Bob are published, Charlie measures his qubit 3 before telling Alice and Bob the unitary operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ to transfer their qubit 0 and qubit 6, which leads to successful swapping as follows:

$$
|01\rangle_{25} \otimes \frac{1}{2\sqrt{2}} \begin{bmatrix}
|000\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|001\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|010\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|011\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|100\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|101\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|110\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|111\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6
\end{bmatrix}. \tag{14}
$$

Our protocol not only simultaneously exchanges quantum information $\{\alpha|0\rangle + \beta|1\rangle, (1/\sqrt{2})(|0\rangle \pm |1\rangle), |0\rangle, |1\rangle\}$ but also interchanges classical secret messages 0, 1 for each user. The legitimate users first define that $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ represents classical bit "0," and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ represents classical bit "1," then the legitimate users prepare the qubit states $|+\rangle$ and $|-\rangle$ as their secret messages to implement all of the above steps. After transferring their respective qubit states, they use the X-basis to measure their respective qubit 0 and qubit 6. Finally, they successfully swap the secret messages. Here, Alice and Bob publishes their measurement results of qubits 1 and 4 as $|0\rangle_1 \otimes |1\rangle_4$, and Charlie measures his qubit 3 as $|0\rangle_3$. The measurement result of qubit 3 cannot be published, but according to the results of qubits 1, 2, 4, and 5, Charlie will tell Alice and Bob to apply the Z gate to transfer their qubits 0 and 6 to obtain the correct qubit state $(c|0\rangle + d|1\rangle)_0$ and $(a|0\rangle + b|1\rangle)_6$. Our protocol can, therefore, simultaneously exchange a combination of quantum information and classical secret messages.

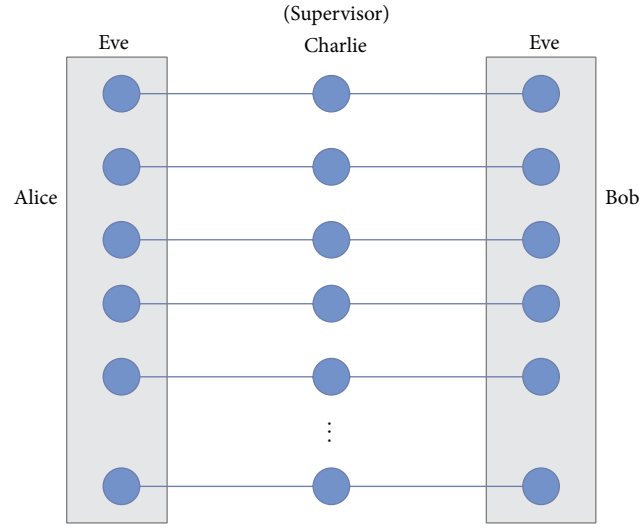

Figure 5: The scenario of Eve intercepts sequences.

4. Security Analysis

Most bidirectional QSDC protocols discuss the security of external attack from an eavesdropper (Eve), but seldom or never discuss the honesty between the legitimate users and the controller. They [15–17, 27] all have to assume that the legitimate users are honest and reliable, and then cooperate to decode the classical secret messages from each other. However, there is a problem involving the honesty of the legitimate users, which arises if one of the legitimate users receives the quantum information or secret message from the other first, and then does not cooperate to help the other decode the quantum information or secret message. Thus, we will analyze the security for external attacks from Eve on the two parties, and internal problems from the legitimate users. Furthermore, there are some attacks that use the imperfect quantum equipment to get illegal secret information, like the Trojan horse attack [28, 29], but when the technology of manufacturing quantum resource becomes more mature, this kind of attacks would be prevented.

External Attack. To check the security of the quantum channel, we have to suppose that the eavesdropper intends to steal the quantum information or classical messages via the quantum channel. There are ways for Eve to conduct this kind of attack. We introduce how Eve would attack our protocol, and show that these attacks do not allow Eve access to any information about the secret messages.

(1) The Man in the Middle Attack by Eve. We suppose that Eve prepares some EPR pairs with the intent to steal secret messages by the *nonlocal swap* gate scheme [see Figure 7]. When Charlie (controller) sends the sequence of A particles and B particles to Alice and Bob, Eve intercepts the A sequence and B sequence and keeps some of them [see Figure 5]. Eve then inserts one of the particles of each EPR pair prepared by herself back to the A sequence and B sequence, and sends A' sequence and B' sequence (A' and

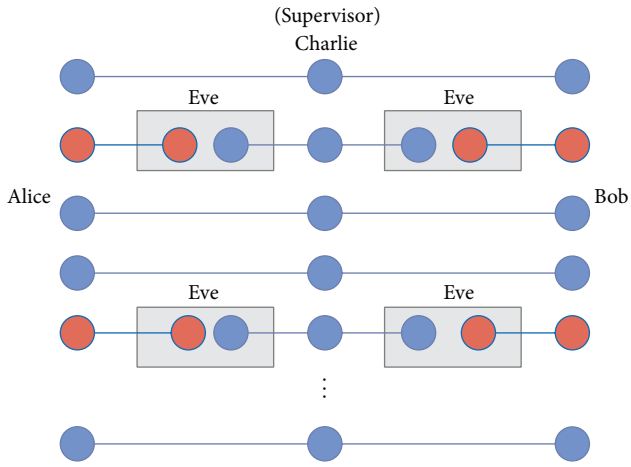

Figure 6: The scenario of Eve inserts EPR pairs.

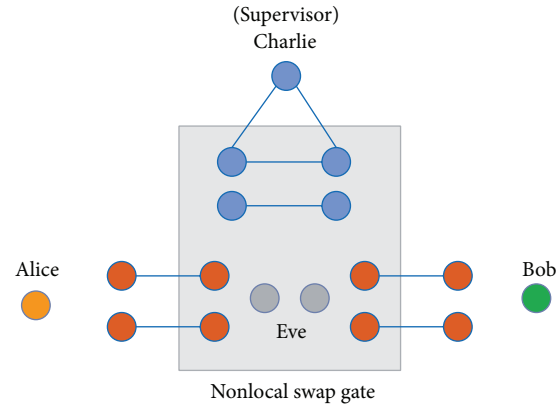

Figure 7: The scenario of Eve steals secret message by the *nonlocal swap* gate scheme.

B' sequences represent the sequences that contain Eve's EPR pairs.) to Alice and Bob [see Figure 6]. If Eve is not detected and her EPR pairs are the quantum resources for legitimate users to exchange their secret message, she can obtain the secret messages from Alice and Bob. Since the quantum resources are kept between the legitimate users and Eve, Eve can mimic Alice and Bob's actions in order to obtain the secret messages.

However, Eve would be found out in the quantum channel. The following shows the error detection rate that the controller and legitimate users find an eavesdropper in the quantum channel, and the calculation of Eve's success rate. After Alice and Bob confirm with Charlie that they have received all the sequences of particles A' and B' (A' and B' sequence represent the sequences that contain Eve's EPR pairs), respectively, they have an order to choose the sufficiently random subset of A and B sequence for detecting an eavesdropper. Assume that Eve inserts the $2k_e$ EPR pairs (Eve has to use two EPR pairs to replace a GHZ state) [see Figure 8]. The legitimate users now have k_e/N probability (Charlie prepares a group of N three-particle GHZ states) to choose Eve's EPR pairs. If one of the legitimate users chooses the particle that is one of the EPR pairs from Eve for a channel check, the legitimate users have 3/4 probability of finding the error. Assume that Alice chooses the GHZ state $(1/\sqrt{2})(|000\rangle + |111\rangle)_{ABC}$ that has the two EPR pairs $(1/\sqrt{2})(|00\rangle + |11\rangle)_{A_1A_2}$ and $(1/\sqrt{2})(|00\rangle + |11\rangle)_{B_1B_2}$ inserted, and Alice keeps the qubit A_1 and Bob keeps the qubit B_1, then Eve keeps the qubits A, B, A_2, and B_2 [see Figure 8].

If Alice (Bob) measures the qubit A_1 (B_1) using Z-basis, the measurement result will have a 1/2 probability of collapsing to $|00\rangle_{A_1A_2}$ ($|00\rangle_{B_1B_2}$) or $|11\rangle_{A_1A_2}$ ($|11\rangle_{B_1B_2}$), and the GHZ state also has a 1/2 probability of collapsing to $|000\rangle_{ABC}$ or $|111\rangle_{ABC}$. When the qubits A_1, C, and B_1 are $|0\rangle$ or $|1\rangle$, Eve has a $(1/4)((1/2) \times (1/2))$ probability of not being found. In other words, if Alice (Bob) measures the qubit A_1 (B_1) using X-basis, the measurement result will have a 1/2 probability of collapsing to $|++\rangle_{A_1A_2}$ ($|++\rangle_{B_1B_2}$) or $|--\rangle_{A_1A_2}$ ($|--\rangle_{B_1B_2}$), and the GHZ state also has a 1/4 probability of collapsing to $|+++\rangle_{ABC}$, $|+--\rangle_{ABC}$, $|-++\rangle_{ABC}$, and $|--+\rangle_{ABC}$. When the qubits A_1, C, and B_1 are $|+\rangle$ or $|-\rangle$, Eve has a (1/4) ((1/2) × (1/2)) probability of not being found.

The overview of the above two external attacks: Charlie prepares N GHZ states for detecting an eavesdropper and quantum resources. Eve prepares $2k_e$ EPR pairs to insert into the A and B sequences. The legitimate users randomly choose m GHZ states together for detecting quantum channels. Therefore, when the legitimate users choose one of N GHZ states, Eve has a $((k_e/N) \times (1/4) + ((N - k_e)/N) \times 100\%)$ probability of not being found in the quantum channel. However, if the legitimate users choose m number of N GHZ states for detecting quantum channels, the error detection rate is $1 - ((k_e/N) \times (1/4) + ((N - k_e)/N) \times 100\%)^m$ for the legitimate users, and the controller finds Eve in the quantum channel regardless of whether the measuring basis is X-basis or Z-basis.

Figures 9 and 10 display the relation between the three parameters m, k_e, and N. In Figure 9, we display five percentages of k_e in N GHZ states corresponding to the error detection rate and the number of detecting GHZ states. The legitimate users can depend on the error detection rate to decide how many m GHZ states must be used to detect an eavesdropper. For example, suppose that Charlie prepares 100 GHZ states; then, Eve uses 100 EPR pairs to replace 50 GHZ states for the legitimate users. According to the line of 50% N in Figure 9, the legitimate users only choose 10 GHZ states for detecting an eavesdropper, the legitimate users and controller find the eavesdropper with a 99.0905% probability. When the legitimate users increase the number of GHZ states for detecting an eavesdropper to 29, there is a 99.9999% probability of the legitimate users and controller finding the eavesdropper. Therefore, the higher the number of GHZ states that are replaced, the fewer detecting GHZ states that are required by the legitimate users to find the eavesdropper.

Figure 10 illustrates that the legitimate users detect the eavesdropper with a 100% probability corresponding to the number of detecting GHZ states and percentage of replaced GHZ states. As in Figure 10, the higher the number of GHZ

$$|\Psi_{000}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}}[|+\rangle(|++\rangle + |--\rangle) + |-\rangle(|+-\rangle + |-+\rangle)]$$

$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

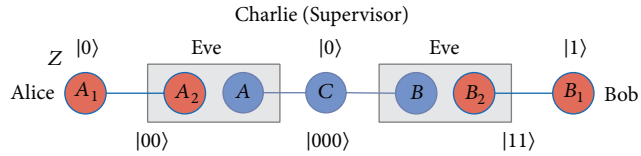

Figure 8: The scenario of external attack in which the legitimate users and controller measure the qubits A_1, C, and B_1.

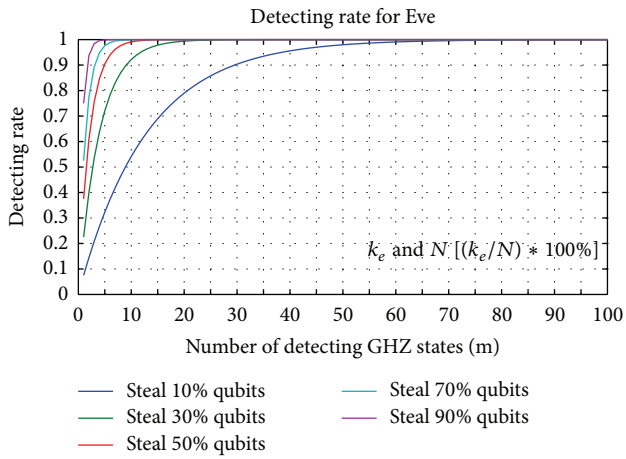

Figure 9: The different percentages of k_e in N GHZ states corresponding to the error detection rate and the number of detecting GHZ states. (k_e: the number of GHZ states replaced by Eve's EPR pairs; N: the number of GHZ states which are prepared from Charlie).

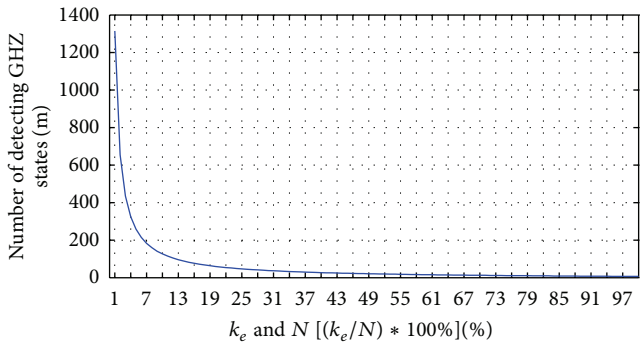

Figure 10: The legitimate users detect eavesdropper with 100% probability corresponding to the number of detecting GHZ states and percentage of replaced GHZ states.

states that are replaced, the fewer detecting GHZ states that are required by the legitimate users to find the eavesdropper. Conversely, the legitimate users need to consume more detecting GHZ states to detect the quantum channels when Eve replaces fewer GHZ states to be EPR pairs.

(2) The Teleportation Attack [30]. Some QSDC protocols examine the security of quantum channel only after photons transmission are all finished, and then this kind of attack will get benefits from this type of transmission. Once photons are transmitted, our proposed protocol will check the error rate to ensure that the quantum channel is secure, so this attack is invalid to our protocol.

(3) The Correlation-Elicitation [31–33]. This kind of attack does *control-not* gate twice on two photons to steal one bit information and cause information leakage problem. Because our protocol uses *nonlocal swap* gate to exchange users' message, no secret information is transmitted during photons distribution, so our protocol can resist this attack.

(4) The Forcible Measurement Attack [34]. This attack measures photons during transmission to get secret message, but like the former attack, in this proposed protocol, transmitted photons are without carrying message, so this attack is invalid to our protocol.

Participant Attack. We focus on two sources of participant attack: attacks from the controller and attacks from the legitimate users. First, we discuss how the controller might steal the secret message, and the situation in which one of the legitimate users is dishonest.

(1) The Man in the Middle Attack by Charlie. We suppose that Charlie prepares some additional EPR pairs with the intent of stealing the secret messages by the *nonlocal swap* gate scheme [see Figure 12]. Before Charlie sends the sequence of A particles and B particles to Alice and Bob, he inserts $2k_c$ EPR pairs to replace k_c GHZ states [see Figure 11]. After this, Charlie sends A' sequence and B' sequence (A' and B' sequences represent the sequences that contain Charlie's attack EPR pairs) to Alice and Bob. If Charlie is not detected, and his EPR pairs are used as the quantum resources for the legitimate users to exchange their secret message, he can obtain the secret message from Alice and Bob. Since the quantum resources are kept between the legitimate users and the controller, he can mimic Alice and Bob's actions in order to obtain the secret message.

However, the evil Charlie would be found out in the quantum channel. Let us show you the error detection rate that the legitimate users find the errors in the quantum

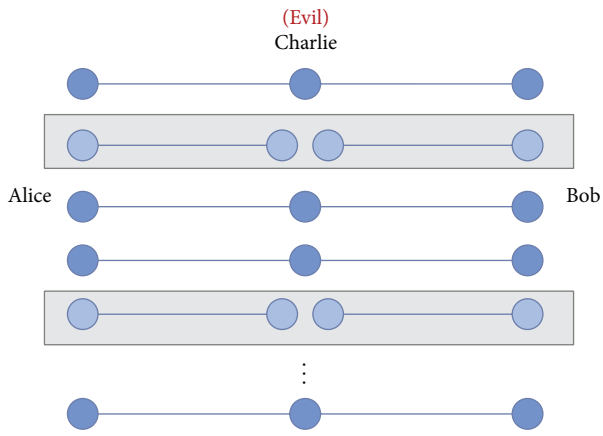

Figure 11: The scenario of participant attack in which Charlie (controller) inserts his EPR pairs to replace GHZ states.

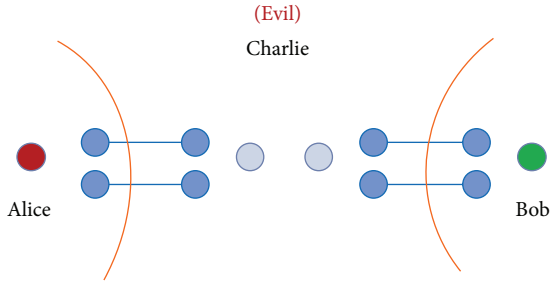

Figure 12: The scenario of participant attack 1 in which Charlie (controller) steals the secret messages by the *nonlocal swap* gate scheme.

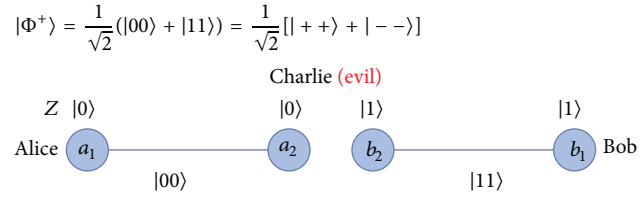

Figure 13: The scenario of participant attack 1 in which Charlie (controller) steals the secret messages by the *nonlocal swap* gate scheme.

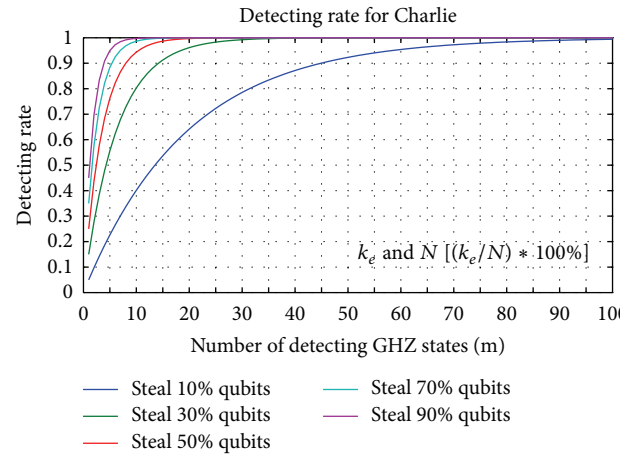

Figure 14: The different percentages of k_c in N GHZ states corresponding to the error detection rate and the number of detecting GHZ states. (k_c: the number of GHZ states replaced by Charlie's EPR pairs. N: the number of GHZ states which are prepared from Charlie).

channel and calculate the evil Charlie's successful rate. After Alice and Bob confirm with the evil Charlie that they have received all the sequences of particles A' and B' (A' and B' sequences are represented in a sequence that has contain Charlie's EPR pairs, respectively, they have an order to choose the random enough subset of A and B sequence for checking quantum channel security. Assume that the evil Charlie inserts the $2k_c$ EPR pairs, then the legitimate users have k_c/N probability (Charlie prepares a group of N three-particles GHZ states.) to choose the evil Charlie's EPR pairs. If one of the legitimate users chooses the particle that is one of the EPR pairs from the evil Charlie for the channel check, the legitimate users have 1/2 probability to find the error. Assume that Alice chooses one of the A' particles that is one of the EPR pairs $(1/\sqrt{2})(|00\rangle+|11\rangle)_{a_1a_2}$ and the corresponding particle in B' sequence that is EPR pair $(1/\sqrt{2})(|00\rangle+|11\rangle)_{b_1b_2}$. Here, Alice keeps the qubit a_1 and Bob keeps the qubit b_1, and then the evil Charlie keeps the qubits a_2 and b_2 [see Figure 13].

However, Charlie would be found out in the quantum channel. The following shows the error detection rate of the legitimate users finding the errors in the quantum channel, and the calculation of Charlie's attack success rate. After Alice and Bob confirm with Charlie that they have received all the sequences of particles A' and B', respectively, they have an order to choose the sufficiently random subset of A and B sequence for checking the quantum channel security. Assume that Charlie inserts the $2k_c$ EPR pairs; then, the legitimate users have a k_c/N probability (Charlie prepares a group of N three-particle GHZ states) of choosing Charlie's EPR pairs. If one of the legitimate users chooses the particle that is one of the EPR pairs from Charlie for the channel check, the legitimate users have a 1/2 probability of finding the error. Assume that Alice chooses one of the A' particles that is one of the EPR pairs $(1/\sqrt{2})(|00\rangle+|11\rangle)_{a_1a_2}$ and the corresponding particle in B' sequence that is EPR pair $(1/\sqrt{2})(|00\rangle+|11\rangle)_{b_1b_2}$. Here, Alice keeps the qubit a_1 and Bob keeps the qubit b_1, and then Charlie keeps the qubits a_2 and b_2 [see Figure 13].

If Alice (Bob) measures the qubit a_1 (b_1) using Z-basis, the measurement result will have a 1/2 probability of collapsing into $|00\rangle_{a_1a_2}$ ($|00\rangle_{b_1b_2}$) or $|11\rangle_{a_1a_2}$ ($|11\rangle_{b_1b_2}$. There are two choices for Charlie to publish his quantum state. If the two EPR pairs share the same measurement results, Charlie will not be found out. Conversely, Charlie has a 1/2 probability of failure. In other words, if Alice (Bob) measures the qubit a_1 (b_1) using X-basis, the measurement result will have a 1/2 probability of collapsing into $|++\rangle_{a_1a_2}$ ($|++\rangle_{b_1b_2}$) or $|--\rangle_{a_1a_2}$ ($|--\rangle_{b_1b_2}$). When the qubits a_1 and b_1 are $|+\rangle$ or $|1\rangle$, Charlie has a 1/2 probability of not being found out.

The overview of participant attack 1: Charlie prepares N GHZ states that include $2k_c$ EPR pairs inserted into

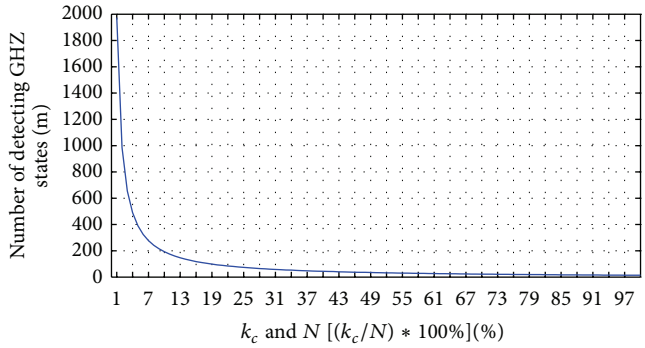

FIGURE 15: The legitimate users ensure quantum channel security with 100% probability corresponding to the number of detecting GHZ states and percentage of replaced GHZ states.

the A and B sequences for detecting eavesdroppers and quantum resources. The legitimate users randomly choose m GHZ states together for detecting quantum channels. Therefore, when the legitimate users choose one of N GHZ states, Charlie has a $((k_c/N) \times (1/2) + ((N - k_c)/N) \times 100\%)$ probability of not being found in the quantum channel. However, if the legitimate users choose m number of the N GHZ states for detecting quantum channels, the error detection rate is $1 - ((k_c/N) \times (1/2) + ((N - k_c)/N) \times 100\%)^m$ for the legitimate users and controller; Charlie is found in the quantum channel regardless of whether the measuring basis is X-basis or Z-basis.

Figures 14 and 15 display the relation between the three parameters m, k_c, and N. In Figure 14, we display five percentages of k_c in N GHZ states corresponding to the error detection rate and the number of detecting GHZ states. The legitimate users can depend on the error detection rate to decide how many m GHZ states must be used to ensure the quantum channel security. For example, suppose that Charlie prepares 100 GHZ states that include 100 EPR pairs to replace 50 GHZ states for the legitimate users. According to the line of 50% N in Figure 14, the legitimate users choose 17 GHZ states for checking the quantum channel, finding the error in the quantum channel with 99.2483% probability. When the legitimate users increase the number of GHZ states for checking the quantum channel to 51, there is a 100% probability of the legitimate users finding the error in the quantum channel. Therefore, the higher the number of GHZ states replaced, the fewer detecting GHZ states are required by the legitimate users to find the error in the quantum channel.

Figure 15 illustrates that the legitimate users ensure the quantum channel security with 100% probability corresponding to the number of detecting GHZ states and percentage of the replaced GHZ states. As with Figure 15, the higher the number of GHZ states replaced, the fewer detecting GHZ states required by the legitimate users to find the eavesdropper. Conversely, the legitimate users need to consume more detecting GHZ states to detect the quantum channels when Charlie replaces fewer GHZ states to be EPR pairs.

(2) Dishonest Condition between Legitimate Users. Some QSDC protocols may exhibit conditions that allow one of the legitimate users to derive the quantum information or secret message from the other one first, without assisting the other one in decoding the quantum information or secret message. The dishonest user may publish an incorrect measurement result, giving the other one an incorrect secret message, while they themselves obtain the correct secret message.

In our protocol, only the controller knows the initial GHZ state and EPR pairs, so the legitimate users are unable to know how to use the unitary operation to transfer their qubit state correctly. In addition, neither user has priority in obtaining the secret message in our protocol, as both receive the secret message from the other simultaneously.

Moreover, if one of the legitimate users deliberately announces an incorrect result to the controller, the controller will consequently give both legitimate users an erroneous unitary operation to transfer their qubit states, resulting in both users simultaneously receiving erroneous quantum information or secret messages. Assume that the measurement results of qubits 1, 2, 4, and 5 are $|0\rangle_1$, $|0\rangle_2$, $|1\rangle_4$, and $|1\rangle_5$, Charlie depends on their measurement result and his qubit 3 result $|0\rangle_3$ to deduce that Alice and Bob need to apply the Z gate to transfer their qubit 0 $(c|0\rangle_0 - d|1\rangle_0)$ and qubit 6 $(a|0\rangle_6 - b|1\rangle_6)$. Charlie will announce the unitary operation (Z gate) for the legitimate users to transfer their qubits 0 and 6 as the correct results $(c|0\rangle_0 + d|1\rangle_0)$ and $(a|0\rangle_6 + b|1\rangle_6)$ that the legitimate users want to send to each other as follows:

$$
\begin{aligned}
&H_{134}C_{46}C_{02}C_{65}C_{10}(a\,|0\rangle + b\,|1\rangle)_0 \\
&\quad \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{134} \otimes (c\,|0\rangle + d\,|1\rangle)_6 \longrightarrow |01\rangle_{25} \\
&\quad \otimes \frac{1}{2\sqrt{2}} \begin{bmatrix}
|000\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|001\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|010\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|011\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|100\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6 + \\
|101\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|110\rangle_{134}(c\,|0\rangle + d\,|1\rangle)_0(a\,|0\rangle + b\,|1\rangle)_6 + \\
|111\rangle_{134}(c\,|0\rangle - d\,|1\rangle)_0(a\,|0\rangle - b\,|1\rangle)_6
\end{bmatrix}.
\end{aligned}
\tag{15}
$$

However, a situation may arise in which one of the legitimate users publishes an incorrect measurement result and lets the other gain the wrong secret message, while themselves obtaining the correct secret message. Assume Bob is dishonest and deliberately publishes the wrong measurement result of qubit 4 $|0\rangle_4$ for Alice and Charlie [see Figure 16]. Charlie depends on the incorrect measurement result to tell the legitimate users to apply the wrong gate (I gate) to transfer their qubits. The result is that Alice cannot receive the correct secret message from Bob, while Bob hopes to receive the correct secret message from Alice.

However, can Bob depend on the measurement results of qubits 1, 2, 4, and 5 to deduce what unitary operation he

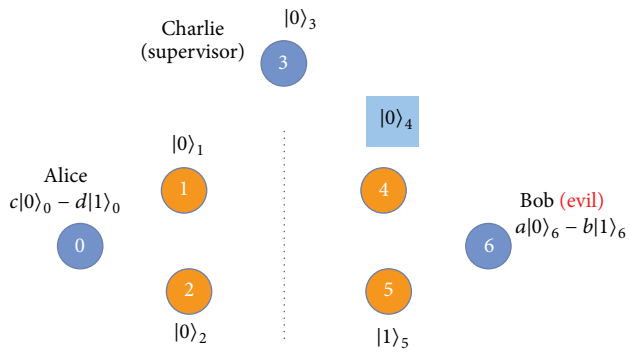

FIGURE 16: Bob publishes an incorrect measurement result of qubit 4.

needs to perform on qubit 6 to obtain Alice's secret message successfully? The answer is no; only Charlie knows the initial state of quantum resources, so only Charlie knows the unitary operation to transfer the legitimate users' qubits 0 and 6. The unitary operations are not only I and Z gates, but also X and Y gates. The unitary operations follow different quantum resources (a GHZ state and an EPR pair) and have different applications. Even if Bob knows the unitary operation of only I and Z gates, and the measurement results of qubits 1, 2, 4, and 5, he still does not know the measurement result of Charlie's qubit 3. Bob has a 1/2 probability of correctly guessing that the measurement result of qubit 3 is $|0\rangle_3$ or $|1\rangle_3$. This means that Bob has a 1/2 probability of guessing the correct unitary operation gate by himself to obtain Alice's secret message. In other words, if Bob repeats the action i times, his failure rate would be $1-(1/2)^i$. Therefore, according to the game theory presented by Nash Jr. [35], in order for the legitimate users to obtain the quantum information from each other, being honest to each other serves them best.

Our protocol not only defends against external attack (man in the middle attack), but also protects against legitimate users lying to the controller and guards against the controller stealing the secret message from the legitimate users by himself. Furthermore, with our protocol employed, since there is no transmission between the legitimate users, Eve has no opportunity to steal the secret message from the quantum channel.

5. Performance Comparison

We analyse the performance of the four protocols: Gao2005 [36], Dong2011 [37], Man2006 [38], and Dong2008 [39] and compare it with our protocol. There are two controlled one direction QSDC protocols and two controlled bidirectional QSDC protocols to be compared with our protocol. We briefly introduce these protocols and our protocol below.

Gao2005 is a controlled one direction QSDC scheme using GHZ state and teleportation. This protocol requires a GHZ-like state (three entangled qubits) to transmit quantum information and classical messages. In addition, Charlie publishes his result by one classical bit, and Alice announces her result by two classical bits, so the cost of Gao2005 is 3 qubits and 3 classical bits for one direction work. Here, the classical bits are used to communicate with each other in the classical channel. If the users want to exchange messages in Gao2005, they need to perform the protocol twice, so the cost is multiplied by two, consisting of 6 qubits and 6 classical bits. However, in Gao2005, the legitimate users receive the secret messages in order, rather than simultaneously, and this protocol cannot protect against the dishonesty of one user (participant attack (2)). Dong2011 presented a controlled one direction QSDC based on teleportation similar to Gao2005 above. The cost and security of Dong2011 are the same as those of Gao2005. The only difference between Gao2005 and Dong2011 is the type of secret message. Moreover, Gao2005 can transmit any unknown qubits, but Dong2011 can change the type of the secret message to pure states. Dong2011 is no more flexible than Gao2005 in transmitting legitimate users' secret messages. Hence, the contribution of Dong2011 is dubious.

Our protocol is a controlled bidirectional QSDC protocol with a GHZ state and an EPR pair. The legitimate users need to publish their respective measurement results by two classical bits, and the controller needs to tell the legitimate users how to transfer their qubit by two classical bits. The cost of our protocol is 5 qubits and 5 classical bits. The legitimate users receive the secret messages from each other simultaneously, and they can transmit any unknown quantum bit to each other. The security of our protocol is more reliable than that of the above protocols because there are no transmitted qubits carrying the secret messages between the legitimate users and the controller. Our protocol not only protects against external attack, but also prevents one legitimate user from being dishonest to the other. Furthermore, Collins et al. [23] note that the apparatus implementing the swap gate must use two EPR pairs as an internal nonlocal resource. Based on the *nonlocal swap* gate, the minimal quantum resource is 4 qubits. Our protocol, however, is a controlled bidirectional QSDC protocol that needs to add one qubit for the controller to control it. Therefore, our protocol has a minimal quantum resource cost (5 qubits) that can exchange any unknown qubit to each other.

According to Table 1, the cost of our protocol is one less qubit than that of Gao2005, because Gao's protocol uses one GHZ-like state (3 qubits) for work and 3 classical bits for public results at a time. In order to compare our protocol with the controlled bidirectional QSDC protocol, we have to work twice with the CQSDC protocol. The CQSDC protocols and our protocol can all transmit the quantum bits and classical bits to each other, but in terms of security, Gao2005 and Dong2011 are vulnerable to participant attack 2 between legitimate users, and they cannot transmit secret messages simultaneously.

Next, we choose two controlled bidirectional QSDC protocols, Man2006 and Dong2008, for comparison with our protocol. Man2006 shares a GHZ state for a controller and two legitimate users. If the legitimate users want to exchange their secret messages, they perform the unitary operation (one unitary operation can be represented by two classical bits) on their qubit and send it back to the controller. The controller will publish his GHZ measurement

Table 1: Comparison of CQSDC and CBQSDC protocols with our protocol.

	Scheme				
	Gao2005	Dong2011	Man2006	Dong2008	Ours
Protocol type	CQSDC	CQSDC	CBQSDC	CBQSDC	CBQSDC
Resource cost of two directional transmission	6 Q and 6 C	6 Q and 6 C	6 Q and 6 C	6 Q and 6 C	5 Q and 6 C
Secret message type	C/Q	C/Q	C	C	C/Q
Received classical bits	1 C	1 C	2 C	2 C	1 C
Received quantum bits	1 Q	1 Q	0	0	1 Q
Controller	Yes	Yes	Yes	Yes	Yes
Classical message exchange	Yes	Yes	Yes	Yes	Yes
Quantum information exchange	Yes	Yes	No	No	Yes
No transmission	Yes	Yes	No	Yes	Yes
Honest condition between legitimate users	No	No	No	No	Yes

C: classical bits; Q: quantum bits.

result to allow the two legitimate users to decode the secret messages from each other. Finally, the cost of Man2006 is three qubits and three classical bits for one time. However, Man2006 cannot transmit quantum information, and is vulnerable to participant attack 2. Because the secret message is made up of classical bits, the cost of the secret message might be lower than the quantum resources in Man2006. In terms of security of Man2006, it is vulnerable to attack by eavesdroppers stealing the qubits carrying the secret message in the transmissions between the legitimate users and the controller. Dong2008 is a controlled bidirectional QSDC protocol, in which legitimate users exchange their secret messages using entanglement swapping with two GHZ states. The controller first measures his two particles and publishes their measurement results by 2 classical bits. The legitimate users then need to Bell-measure their two particles and publish their Bell-measurement results by 2 classical bits, respectively. The cost of Dong2008 is 6 quantum bits and 6 classical bits for the legitimate users to exchange their secret messages at a time. Even though there are no transmissions with qubits carrying secret messages in Dong2008, it is also vulnerable to participant attack 2. In addition, since Dong2008 only transmits classical bits, the cost of sending the secret messages may be lower than the quantum resources of Man2006.

Man2006, Dong2008, and our protocol are controlled bidirectional QSDC protocols. As shown in Table 1, the cost of our protocol's quantum resources is higher than that of Man2006, but Man2006 cannot transmit any unknown qubits. The users can exchange two classical bits at a time in Man2006 and Dong2008, which is one bit more than our protocol. However, classical bits are cheaper than qubits. Our protocol, therefore, is more efficient than the above protocols. Man2006 and Dong2008 are also vulnerable to participant attack 2. In summary, our protocol is more efficient than other protocols, and provides the security for the legitimate users to exchange their secret messages with minimal quantum resources.

6. Conclusion

In this paper, we proposed a controlled bidirectional quantum secure direct communication using a *nonlocal swap* gate to simultaneously exchange quantum information or classical messages without transmitting the qubits carrying the secret messages. The legitimate users must have permission from a controller to exchange their respective quantum information or secret messages. Our protocol not only protects against external attack, but also against participant attack. In addition, our protocol uses minimal quantum resources for legitimate users to transmit any unknown qubits in controlled bidirectional QSDC protocols. It is secure against eavesdropping attacks, and the controller has no access to the quantum information or secret messages in our protocol. Therefore, our design of a novel CBQSDC protocol based on a *nonlocal swap* gate is quite secure, reliable, and confidential.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was partly funded by the National Science Council of the ROC under Grants NSC 100-2221-E-260-038 and NSC 101-2221-E-260-033.

References

[1] Y.-H. Chou, C.-Y. Chen, H.-C. Chao, J. H. Park, and R.-K. Fan, "Quantum entanglement and non-locality based secure computation for future communication," *IET Information Security*, vol. 5, no. 1, pp. 69–79, 2011.

[2] Y.-H. Chou, C.-Y. Chen, R.-K. Fan, H.-C. Chao, and F.-J. Lin, "Enhanced multiparty quantum secret sharing of classical messages by using entanglement swapping," *IET Information Security*, vol. 6, no. 2, pp. 84–92, 2012.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[5] A. Cabello, "Quantum key distribution without alternative measurements," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 61, no. 5, Article ID 052312, 4 pages, 2000.

[6] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states," *Physical Review Letters*, vol. 75, no. 7, pp. 1239–1243, 1995.

[7] W. Y. Hwang, I. G. Koh, and Y. D. Han, "Quantum cryptography without public announcement of bases," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 244, no. 6, pp. 489–494, 1998.

[8] T. Hwang, K.-C. Lee, and C.-M. Li, "Provably secure three-party authenticated quantum key distribution protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 71–80, 2007.

[9] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *Acta Physica Polonica A*, vol. 101, no. 3, pp. 357–368, 2002.

[10] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, no. 18, Article ID 187902, 4 pages, 2002.

[11] Q.-Y. Cai, "The "ping-pong" protocol can be attacked without eavesdropping," *Physical Review Letters*, vol. 91, no. 10, Article ID 109801, 1 page, 2003.

[12] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 351, no. 1-2, pp. 23–25, 2006.

[13] A. Wójcik, "Eavesdropping on the "ping-pong" quantum communication protocol," *Physical Review Letters*, vol. 90, no. 15, Article ID 157901, 4 pages, 2003.

[14] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 68, no. 4, Article ID 042317, 6 pages, 2003.

[15] B. A. Nguyen, "Quantum dialogue," *Physics Letters A*, vol. 328, no. 1, pp. 6–10, 2004.

[16] X.-R. Jin, X. Ji, Y.-Q. Zhang et al., "Three-party quantum secure direct communication based on GHZ states," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 354, no. 1-2, pp. 67–70, 2006.

[17] Y. Xia, C.-B. Fu, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um, "Quantum dialogue by using the GHZ state," *Journal of the Korean Physical Society*, vol. 48, no. 1, pp. 24–27, 2006.

[18] J. C. R. Tseng and G.-J. Hwang, "Development of an intelligent internet shopping agent based on a novel personalization approach," *Journal of Internet Technology*, vol. 6, no. 4, pp. 477–485, 2005.

[19] I. Anagnostopoulos, "Improving the precision of third-party results by monitoring browsing behaviour and evolution in internet search engine caches," *Journal of Internet Technology*, vol. 11, no. 1, pp. 11–24, 2010.

[20] F. L. Yan and X. Q. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *European Physical Journal B: Condensed Matter and Complex Systems*, vol. 41, no. 1, pp. 75–78, 2004.

[21] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[22] C.-Y. Chen, Y.-H. Chou, and H.-C. Chao, "Distributed quantum entanglement sharing model for high-performance real-time system," *Soft Computing*, vol. 16, no. 3, pp. 427–435, 2012.

[23] D. Collins, N. Linden, and S. Popescu, "Nonlocal content of quantum operations," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 64, no. 3, Article ID 032302, 7 pages, 2001.

[24] N. Linden, H. Barjat, E. Kupče, and R. Freeman, "How to exchange information between two coupled nuclear spins: the universal SWAP operation," *Chemical Physics Letters*, vol. 307, no. 3-4, pp. 198–204, 1999.

[25] Z. L. Mádi, R. Brüschweiler, and R. R. Ernst, "One- and two-dimensional ensemble quantum computing in spin Liouville space," *The Journal of Chemical Physics*, vol. 109, no. 24, pp. 10603–10611, 1998.

[26] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, "Conditional quantum dynamics and logic gates," *Physical Review Letters*, vol. 74, no. 20, pp. 4083–4086, 1995.

[27] Y. Chen, Z.-X. Man, and Y.-J. Xia, "Quantum bidirectional secure direct communication via entanglement swapping," *Chinese Physics Letters*, vol. 24, no. 1, pp. 19–22, 2007.

[28] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[29] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojanhorse attacks on quantum-key-distribution systems," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 73, no. 2, Article ID 022320, 6 pages, 2006.

[30] F. Gao, Q.-Y. Wen, and F.-C. Zhu, "Teleportation attack on the QSDC protocol with a random basis and order," *Chinese Physics B*, vol. 17, no. 9, pp. 3189–3193, 2008.

[31] F. Gao, Q.-Y. Wen, and F.-C. Zhu, "Comment on: "quantum exam" [Phys. Lett. A 350 (2006) 174]," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 360, no. 6, pp. 748–750, 2007.

[32] S.-J. Qin, F. Gao, F.-Z. Guo, and Q.-Y. Wen, "Comment on "two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair"," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 82, no. 3, Article ID 036301, 3 pages, 2010.

[33] L.-Y. Wang, X.-B. Chen, G. Xu, and Y.-X. Yang, "Information leakage in three-party simultaneous quantum secure direct communication with EPR pairs," *Optics Communications*, vol. 284, no. 7, pp. 1719–1720, 2011.

[34] F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, "Forcible-measurement attack on quantum secure direct communication protocol with cluster state," *Chinese Physics Letters*, vol. 25, no. 8, pp. 2766–2769, 2008.

[35] J. F. Nash Jr., "The bargaining problem," *Econometrica*, vol. 18, no. 2, pp. 155–162, 1950.

[36] T. Gao, F.-L. Yan, and Z.-X. Wang, "Controlled quantum teleportation and secure direct communication," *Chinese Physics*, vol. 14, no. 5, pp. 893–897, 2005.

[37] L. Dong, X.-M. Xiu, Y.-J. Gao, Y.-P. Ren, and H.-W. Liu, "Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement," *Optics Communications*, vol. 284, no. 3, pp. 905–908, 2011.

[38] Z.-X. Man and Y.-J. Xia, "Controlled bidirectional quantum direct communication by using a GHZ state," *Chinese Physics Letters*, vol. 23, no. 7, pp. 1680–1682, 2006.

[39] L. Dong, X.-M. Xiu, Y.-J. Gao, and F. Chi, "A controlled quantum dialogue protocol in the network using entanglement swapping," *Optics Communications*, vol. 281, no. 24, pp. 6135–6138, 2008.