Quantum Inf Process (2013) 12:3207–3222
DOI 10.1007/s11128-013-0593-x

Fault tolerant quantum key distributions using entanglement swapping of GHZ states over collective-noise channels

Chun-Wei Yang · Tzonelih Hwang

Received: 23 March 2013 / Accepted: 20 May 2013 / Published online: 1 June 2013

Abstract This work proposes two fault tolerant quantum key distribution (QKD) protocols. Each of which is robust under one kind of collective noises: collective-dephasing noise and collective-rotation noise, respectively. Due to the use of the entanglement swapping of Greenberger–Horne–Zeilinger (GHZ) state as well as the decoy logical qubits, the new protocols provide the best qubit efficiency among the existing fault tolerant QKD protocols over the same collective-noise channel. The receiver simply performs two Bell measurements to obtain the raw key. Moreover, the proposed protocols are free from several well-known attacks and can also be secure over a lossy channel.

Keywords Collective noise · Entanglement swapping · GHZ state · Quantum cryptography · Quantum key distribution

1 Introduction

The quantum key distribution (QKD) is one of the most important research topics in quantum cryptography. In a QKD protocol, a secret key is determined by one communicant (Alice) and then distributed to the other communicant (Bob) through the transmission of quantum signals. Since the first QKD protocol presented by Bennett

C.-W. Yang · T. Hwang (✉)
Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, University Rd., Tainan City 70101, Taiwan, ROC
e-mail: hwangtl@ismail.csie.ncku.edu.tw

C.-W. Yang
e-mail: waywei.yang@gmail.com

and Brassard [1] in 1984 (also known as BB84), a variety of QKD protocols have been proposed [2–7].

However, in practice, quantum channels introduce noises (such as vibration, thermal fluctuation, and the imperfection of the fiber) to the communication qubits. And the noises influence both the correctness and efficiency of communication. Since qubits travel inside a time window which is shorter than the variation of the noise sources [8], these qubits will all be affected by the same noise, which is known as the collective noise.

The collective noise types are among the dominant noise sources in quantum communications. There are two types of collective noises: collective-dephasing noise and collective-rotation noise. The effects of these two types of noises are illustrated by the following transformations. When the polarization photons $|0\rangle$ and $|1\rangle$ undergo the transformations of collective-dephasing noise (or collective-rotation noise), they become: $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow e^{i\theta}|1\rangle$ (or $|0\rangle \rightarrow \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|1\rangle \rightarrow -\sin\theta|0\rangle + \cos\theta|1\rangle$ under the transformations of collective-rotation noise), where $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarization states respectively, and the fluctuation of the noise with time is represented by the parameter θ.

Decoherence-free subspaces (DFS) [9–12], which have the property of being invariant under collective noises, are frequently used to combat these types of noises. For instance, the Bell states $\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ are unchanged by propagating through a collective-dephasing noise channel [8]. On the other hand, the Bell states $\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ are unchanged by propagating through a collective-rotation noise channel [8]. Hence, these states can form two noiseless subspaces (i.e., DFS), one for each type of noise.

Several quantum protocols [8,13–25] have been developed to remove the effects of collective noises in QKD [8,13–18], quantum secret sharing (QSS) [19–22], quantum secure direct communication (QSDC) [23,24], and quantum dialogue (QD) [25]. In 2008, Li et al. [8] proposed two QKD protocols using DFS over two collective-noise channels, where a 1-bit key is transmitted via a 4-particle state. In 2009, Xiu et al. [15] presented two QKD protocols immune to collective noises also using DFS, where a two-bit key is transmitted via a 6-particle state. After that, Li et al. [16] presented two two-step QKD schemes against two kinds of collective noises, respectively. Li and Li [17] also used two-step communication strategy to design QKD over two collective-noise channels. However, these protocols [16,17] are insecure under Trojan horse attacks [26–30].

Different from the above schemes, this paper presents two QKD protocols based on entanglement swapping. By merely using two Bell measurements, two unrelated 3-particle Greenberger–Horne–Zeilinger (GHZ) states are able to build up an entanglement correlation. The entanglement swapping of these two 3-particle GHZ states allows two participants to share an entanglement relation of the Bell states even if the channels between them are subject to collective noises. In our proposed schemes, to generate a raw key, the participants only need to perform Bell measurement without performing any local unitary operations. Moreover, no classical information is required to negotiate the key except for the eavesdropping check. Compared

to the other related QKD protocols [8,15–17], our approach has the following advantages:

1. The proposed protocols are secure under several well-known attacks.
2. The proposed protocols can prevent the Trojan-horse attacks because one-step photon transmission is adopted.
3. The proposed protocols are robust over both kinds of collective-noise channels as well as a lossy quantum channel.
4. The qubit efficiency of our QKD protocols is the highest among the existing QKD protocols [8,15–17] due to the use of the decoy logical qubits.

The rest of this paper is organized as follows. Section 2 describes the preliminaries of this paper. Section 3 presents the fault tolerant QKD schemes. Section 4 gives an efficiency analysis on the proposed schemes. Section 5 analyzes the security of the proposed protocols. Finally, Sect. 6 summarizes our results.

2 Preliminaries

This section includes three subsections. Sections 2.1 and 2.2 give definitions to the logical qubits resistant to the collective-dephasing noise and the collective-rotation noise, respectively. Section 2.3 illustrates the entanglement swapping of GHZ states and GHZ-like states, respectively.

2.1 The logical qubit immune to collective-dephasing noise

In order to avoid the collective-dephasing noise, two logical qubits $\left|0_{dp}\right\rangle$ and $\left|1_{dp}\right\rangle$ can be constructed from two physical qubits $|0\rangle\,|1\rangle$ and $|1\rangle\,|0\rangle$, respectively, where the subscript "dp" indicates the logical qubit resistant to the collective-dephasing noise. The superpositions of $\left|0_{dp}\right\rangle$ and $\left|1_{dp}\right\rangle$, which can be denoted as $\left|+_{dp}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\right)$ $(= \frac{1}{\sqrt{2}}\left(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle\right))$ and $\left|-_{dp}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle - \left|1_{dp}\right\rangle\right)$ $(= \frac{1}{\sqrt{2}}\left(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle\right))$, are also immune to the collective-dephasing noise.

It is obvious that GHZ state $|G\rangle_{123} = \frac{1}{\sqrt{2}}\left(|0\rangle_1\,|10\rangle_{23} + |1\rangle_1\,|01\rangle_{23}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle_1\,\left|1_{dp}\right\rangle_{23} + |1\rangle_1\,\left|0_{dp}\right\rangle_{23}\right)$ is invariant when the 2*nd* and the 3*rd* qubits are transmitted through the collective-dephasing noise channel.

2.2 The logical qubit immune to collective-rotation noise

To combat the collective-rotation noise, two logical qubits can be defined as $|0_r\rangle = \left|\Phi^+\right\rangle (= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right))$ and $|1_r\rangle = \left|\Psi^-\right\rangle (= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right))$, respectively, where the subscript "r" indicates the logical qubit resistant to collective-rotation noise. Here, $\left|\Phi^+\right\rangle$ and $\left|\Psi^-\right\rangle$ are the only two of the four Bell states that will not change their states after rotating the qubits' phases. The superpositions of the two logical qubits, denoted as $|+_r\rangle = \frac{1}{\sqrt{2}}\left(|0_r\rangle + |1_r\rangle\right)$ $\left(= \frac{1}{\sqrt{2}}\left(\left|\Phi^+\right\rangle + \left|\Psi^-\right\rangle\right)\right)$ and

$|-_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle)$ $\left(=\frac{1}{\sqrt{2}}\left(\left|\Phi^+\right\rangle - \left|\Psi^-\right\rangle\right)\right)$, are also resistant to the collective-rotation noise.

It is obvious that GHZ-like state $|L\rangle_{123} = \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle + |111\rangle)_{123} = \frac{1}{\sqrt{2}}(|0\rangle_1 |1_r\rangle_{23} + |1\rangle_1 |0_r\rangle_{23})$ is invariant when the *2nd* and the *3rd* qubits are transmitted through the collective-rotation noise channel.

2.3 The entanglement swapping using GHZ states and GHZ-like states

In this section, we describe the process of the entanglement swapping using GHZ states and GHZ-like states, respectively. The entanglement swapping can be performed between two GHZ states as follows. Let us first prepare two GHZ states, $|G\rangle_{123} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{123}$ and $|G\rangle_{456} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{456}$, where the subscript i denotes the ith qubit of $|G\rangle_{123}$ and $|G\rangle_{456}$. These two GHZ states are individually entangled. That is, there is no entangled relationship between the 1*st* and the 4*th* qubits, the 2*nd* and the 5*th* qubits, or the 3*rd* and the 6*th* qubits, respectively. If, however, one performs the Bell measurements on the 2*nd* and the 5*th* qubits and also on the 3*rd* and the 6*th* qubits, respectively. Then, the 1*st* and the 4*th* qubits become a Bell state. That is, a correlation of entanglement is established between the 1*st* and the 4*th* qubits.

As an example, after performing the entanglement swapping between the two GHZ states $|G\rangle_{123} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{123}$ and $|G\rangle_{456} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{456}$, the state of $|G\rangle_{123} \otimes |G\rangle_{456}$ becomes the following.

$$
\begin{aligned}
&|G\rangle_{123} \otimes |G\rangle_{456} \\
&= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{123} \otimes \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{456} \\
&= \frac{1}{2\sqrt{2}} \begin{pmatrix} \left|\Phi^+\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56} + |01\rangle_{23}|01\rangle_{56}) \\ + \left|\Phi^-\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56} - |01\rangle_{23}|01\rangle_{56}) \\ + \left|\Psi^+\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56} + |01\rangle_{23}|10\rangle_{56}) \\ + \left|\Psi^-\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56} - |01\rangle_{23}|10\rangle_{56}) \end{pmatrix} \\
&= \frac{1}{2\sqrt{2}} \begin{pmatrix} \left|\Phi^+\right\rangle_{14} & \left(\left|\Phi^+\right\rangle_{25}\left|\Phi^+\right\rangle_{36} - \left|\Phi^-\right\rangle_{25}\left|\Phi^-\right\rangle_{36}\right) \\ + \left|\Phi^-\right\rangle_{14} & \left(\left|\Phi^+\right\rangle_{25}\left|\Phi^-\right\rangle_{36} - \left|\Phi^-\right\rangle_{25}\left|\Phi^+\right\rangle_{36}\right) \\ + \left|\Psi^+\right\rangle_{14} & \left(\left|\Psi^+\right\rangle_{25}\left|\Psi^+\right\rangle_{36} - \left|\Psi^-\right\rangle_{25}\left|\Psi^-\right\rangle_{36}\right) \\ + \left|\Psi^-\right\rangle_{14} & \left(\left|\Psi^+\right\rangle_{25}\left|\Psi^-\right\rangle_{36} - \left|\Psi^-\right\rangle_{25}\left|\Psi^+\right\rangle_{36}\right) \end{pmatrix}
\end{aligned} \tag{1}
$$

If Bell measurement results of the 2*nd* and the 5*th* qubits and the 3*rd* and the 6*th* qubits are $\left|\Phi^+\right\rangle_{25}\left|\Phi^+\right\rangle_{36}$ or $\left|\Phi^-\right\rangle_{25}\left|\Phi^-\right\rangle_{36}$, then the correlation of entanglement on the 1*st* and the 4*th* qubits is $\left|\Phi^+\right\rangle_{14}$. According to Eq. (1), one can easily infer the correlation of entanglement of the 1*st* and the 4*th* qubits based on the Bell measurement results of the 2*nd* and the 5*th* qubits and the 3*rd* and the 6*th* qubits.

Obviously, the entanglement swapping also can be done by using two GHZ-like states $|L\rangle_{123} = \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle + |111\rangle)_{123}$ and $|L\rangle_{456} = \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle + |111\rangle)_{456}$ as shown in Eq. (2).

$$
\begin{aligned}
&|L\rangle_{123} \otimes |L\rangle_{456} \\
&= \frac{1}{2}\left(|001\rangle - |010\rangle + |100\rangle + |111\rangle\right)_{123} \otimes \frac{1}{2}\left(|001\rangle - |010\rangle + |100\rangle + |111\rangle\right)_{456} \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\Psi^-\right\rangle_{23} + |1\rangle_1 \left|\Phi^+\right\rangle_{23}\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_4 \left|\Psi^-\right\rangle_{56} + |1\rangle_4 \left|\Phi^+\right\rangle_{56}\right) \\
&= \frac{1}{2\sqrt{2}} \begin{pmatrix} \left|\Phi^+\right\rangle_{14} & \left(\left|\Phi^+\right\rangle_{25}\left|\Phi^+\right\rangle_{36} + \left|\Psi^-\right\rangle_{25}\left|\Psi^-\right\rangle_{36}\right) \\ + \left|\Phi^-\right\rangle_{14} & \left(-\left|\Phi^-\right\rangle_{25}\left|\Phi^-\right\rangle_{36} - \left|\Psi^+\right\rangle_{25}\left|\Psi^+\right\rangle_{36}\right) \\ + \left|\Psi^+\right\rangle_{14} & \left(\left|\Phi^-\right\rangle_{25}\left|\Psi^+\right\rangle_{36} - \left|\Psi^+\right\rangle_{25}\left|\Phi^-\right\rangle_{36}\right) \\ + \left|\Psi^-\right\rangle_{14} & \left(-\left|\Phi^+\right\rangle_{25}\left|\Psi^-\right\rangle_{36} + \left|\Psi^-\right\rangle_{25}\left|\Phi^+\right\rangle_{36}\right) \end{pmatrix}
\end{aligned} \tag{2}
$$

3 Proposed quantum key distribution protocols

This section presents two QKD protocols. Each one is designed to be resistant to a particular type of collective noises.

3.1 Quantum key distribution over a collective-dephasing noise channel

Let Alice and Bob be two communicants in a QKD protocol, and the four Bell states $\left|\Phi^+\right\rangle, \left|\Phi^-\right\rangle, \left|\Psi^+\right\rangle$ and $\left|\Psi^-\right\rangle$ represent two-bit information "00", "01", "10" and "11", respectively. The proposed QKD protocol resistant to the collective-dephasing noise is described below (see also Fig. 1).

Step 1. Alice prepares a sequence of $2n$ GHZ states, $S = \{s_1, s_2, \ldots, s_{2n}\}$, where $s_i = \left\{q_1^i, q_2^i, q_3^i\right\}, i = 1, 2, \ldots, 2n$. Each GHZ state is in $|G\rangle = \frac{1}{\sqrt{2}}\left(|010\rangle + |101\rangle\right)_{123}$. She takes the second qubits and the third qubits from all GHZ states to form a new sequence $S_B = \left\{q_2^i, q_3^i\right\}$, and the first qubits to form the other sequence $S_A = \left\{q_1^i\right\}$, for $i = 1, 2, \ldots, 2n$. Alice also prepares m logical qubits from $\left\{\left|0_{dp}\right\rangle, \left|1_{dp}\right\rangle, \left|+_{dp}\right\rangle \text{ and } \left|-_{dp}\right\rangle\right\}$ as decoy logical qubits. She randomly inserts these decoy logical qubits into S_B to get S'_B and sends it to Bob.

Step 2. After confirming that Bob has received the sequence, Alice announces the positions, the measurement results and the measurement bases of the decoy logical qubits. Bob will then measure the corresponding check sets for eavesdropping check. If there is no eavesdropper, then the protocol will continue to the next step, otherwise they will terminate the protocol and start it again.

Step 3. Alice measures the qubits $\left\{q_1^{2j-1}, q_1^{2j}\right\}$, and Bob measures the qubits $\left\{q_2^{2j-1}, q_2^{2j}\right\}$ and $\left\{q_3^{2j-1}, q_3^{2j}\right\}$ with Bell measurements as shown in Eq. (1), for $j = 1, 2, \ldots, n$. Alice's measurement result (MR_A) of the Bell state represents two bits of the classical information. That is, "00" if the result is $\left|\Phi^+\right\rangle$; "01" if $\left|\Phi^-\right\rangle$; "10" if $\left|\Psi^+\right\rangle$; and "11" if $\left|\Psi^-\right\rangle$. Then, Bob can obtain Alice's raw key according to his measurement results (MR_B). That is, "00" if the result is $\left|\Phi^+\right\rangle\left|\Phi^+\right\rangle$ or $\left|\Phi^-\right\rangle\left|\Phi^-\right\rangle$; "01" if $\left|\Phi^+\right\rangle\left|\Phi^-\right\rangle$ or $\left|\Phi^-\right\rangle\left|\Phi^+\right\rangle$; "10" if $\left|\Psi^+\right\rangle\left|\Psi^+\right\rangle$ or $\left|\Psi^-\right\rangle\left|\Psi^-\right\rangle$; and "11" if $\left|\Psi^+\right\rangle\left|\Psi^-\right\rangle$ or $\left|\Psi^-\right\rangle\left|\Psi^+\right\rangle$. Finally, if the

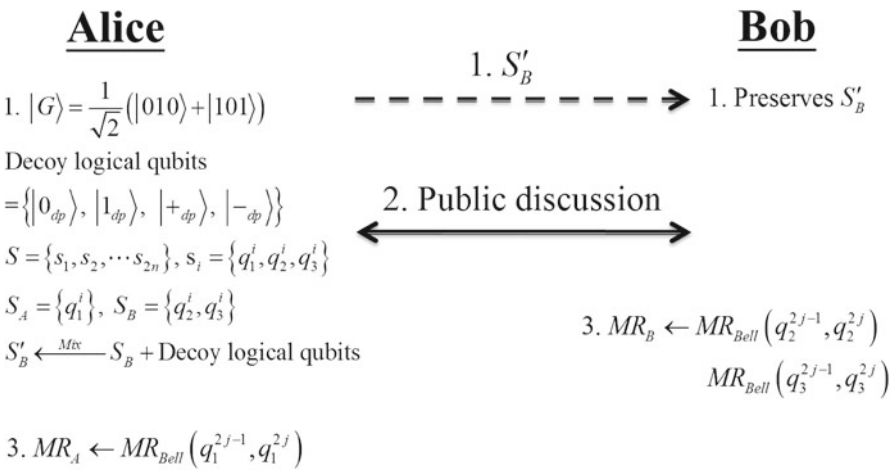

Fig. 1 The proposed QKD protocol

transmission between Alice and Bob is secure, then they can distil a private key with the privacy amplification process [31,32] on the raw key.

An eavesdropper who did not know in advance each decoy logical qubit's state and its position cannot retrieve Alice's raw key without being detected. Furthermore, since all qubits are transmitted in one step only, the proposed scheme is free from Trojan horse attacks. More details of the security analysis will be given in Sect. 5.

3.2 Quantum key distribution over a collective-rotation noise channel

Alternatively, for the QKD protocol over a collective-rotation noise channel, Alice can generate the GHZ-like state $|L\rangle = \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle + |111\rangle)_{123}$, and also prepare decoy logical qubits randomly chosen from $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ instead in Step 1 of the previous protocol. Furthermore, the entanglement swapping of the GHZ-like states can be distinguished by the Bell measurements as shown in Eq. (2). Following the same procedure in Sect. 3.1, by using the GHZ-like states, the proposed QKD protocol can be resistant to the collective-rotation noise.

4 Efficiency analysis

Table 1 compares several important features of fault tolerant QKDs including Li et al.'s scheme [8], Xiu et al.'s scheme [15], Li et al.'s scheme [16] and Li and Li's scheme [17] with the proposed schemes. Suppose that $\eta = \frac{c}{q}$ is the qubit efficiency of a quantum protocol, where c is the total number of shared classical bits and q is the total number of qubits generated in the protocols [24,30,33–36]. Let us assume that half of the qubits transmitted in the public discussion step of the protocol are used for detecting the presence of eavesdroppers, and half of the transmitted qubits are used to check for the Trojan horse attacks.

Table 1 Comparison of [8,15–17] and the proposed scheme

	Li et al.'s scheme [8]	Xiu et al.'s scheme [15]	Li et al.'s scheme [16]	Li and Li's scheme [17]	Proposed scheme
Quantum state	4-Particle state	6-Particle state	GHZ state	Bell state	GHZ state
Quantum communication	One way	One way	Two-step	Two-step	One way
Qubit efficiency (%)	12.5	16.67	8.33	6.25	20
Photon number splitter	No	No	Yes	Yes	No
Wavelength filter	No	No	Yes	Yes	No

In Li et al.'s scheme [8], Alice has to generate n 4-particle states, and each 4-particle state can carry one key bit. One round of public discussion is used in Li et al.'s QKD. Therefore, the qubit efficiency of Li et al.'s protocol is $\frac{n}{4n} \times \frac{1}{2} = \frac{1}{8} = 12.5\,\%$.

In Xiu et al.'s scheme [15], Alice has to generate n 6-particle states, and each 6-particle state can carry two key bits. One round of public discussion is used in Xiu et al.'s QKD. Therefore, the qubit efficiency of Xiu et al.'s protocol is $\frac{2n}{6n} \times \frac{1}{2} = \frac{1}{6} = 16.67\,\%$.

In Li et al.'s scheme [16], Alice has to generate nGHZ states, and each GHZ state can carry two key bits. Two rounds of public discussions are used in Li et al.'s QKD, and half of the transmitted qubits are used to check for the Trojan horse attacks. Therefore, the qubit efficiency of Li et al.'s protocol is $\frac{2n}{3n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{12} = 8.33\,\%$.

In Li and Li's scheme [17], Alice has to generate n Bell states, and each Bell state can carry one key bit. Two rounds of public discussions are used in Li and Li's QKD, and half of the transmitted qubits are used to check for the Trojan horse attacks. Therefore, the qubit efficiency of Li and Li's protocol is $\frac{n}{2n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16} = 6.25\,\%$.

In the proposed QKD protocol over a collective-dephasing noise channel, each two GHZ states can be used to encode two key bits. Since Alice has to prepare $2n$ GHZ states (i.e., $6n$ qubits) and $2n$ decoy logical qubits (i.e., $4n$ qubits), the qubit efficiency of the proposed QKD protocol is $\frac{2n}{6n+4n} = \frac{1}{5} = 20\,\%$. The same qubit efficiency with 20 % is calculated in the proposed QKD protocol over a collective-rotation noise channel by using GHZ-like states. Obviously, the qubit efficiency of our QKD protocol is the highest among the existing QKD protocols [8,15–17] due to the use of the decoy logical qubits.

5 Security analysis

This section analyzes two well-known attacks, the intercept-and-resend attack and the entanglement-and-measure attack, against the proposed protocols. Then, the situation of a lossy quantum channel is discussed to show that the proposed protocols are also secure under this case.

5.1 Security against intercept-and-resend attack

The eavesdropper, Eve, may try to intercept and measure the sequences S'_B in Step 1 of Sect. 3 to deduce Alice's raw key, and then send a bunch of forged logical qubits to Bob. However, according to Step 2 of Sect. 3, the decoy logical qubits are randomly inserted in the transmitted sequences S'_B. Thus, without knowing the positions of these decoy logical qubits in advance, some errors will later be detected during the public discussion if Eve launches the intercept-and-resend attack. For example, consider only one specific decoy logical qubit, $|0_L\rangle$ $(= \frac{1}{\sqrt{2}}(|+_L\rangle + |-_L\rangle))$ in S'_B, where subscript "L" denotes the logical state resistant to the collective noise. Then, when performing the intercept-and-resend attack, Eve has to forge the decoy logical qubit. Since four decoy logical qubits $|0_L\rangle, |1_L\rangle, |+_L\rangle$ and $|-_L\rangle$ are possible candidates for Eve to choose, if she chooses the right decoy logical qubit $|0_L\rangle$, she will pass the eavesdropping check. If, however, she chooses $|1_L\rangle$ as the decoy logical qubit, then she cannot pass the eavesdropping check. If, on the other hand, she chooses $|+_L\rangle$ and $|-_L\rangle$ as the decoy logical qubits of different basis, she will pass the eavesdropping check with a probability of $\frac{1}{2}$, where $|+_L\rangle = \frac{1}{\sqrt{2}}(|0_L\rangle + |1_L\rangle)$ and $|-_L\rangle = \frac{1}{\sqrt{2}}(|0_L\rangle - |1_L\rangle)$. In total, Eve has a probability of $\frac{1}{2}\left(= \frac{1}{4} + 2 \times \frac{1}{4} \times \frac{1}{2}\right)$ to pass the checking process for each decoy logical qubit. Thus, the detection rate can be computed as $1 - \left(\frac{1}{2}\right)^n$, if there are n decoy logical qubits. The detection probability would converge to 1 when n is large enough.

Without considering the public discussion in the proposed protocols, one can also evaluate the information which will be revealed by Eve through this attack based on the information theory [37]. In order to compute Alice's raw key, Eve has to perform the Bell measurement on each two logical qubits. Then, three possible situations could occur: (1) none of the logical qubits is a decoy; (2) one of the logical qubits is a decoy; (3) both logical qubits are decoys. The following analysis thus is based on these three cases.

(1) None of the logical qubits is decoy

Without loss of generality, consider a pair of GHZ states, $|G\rangle_{123} \otimes |G\rangle_{456}$, prepared by Alice in the protocol over a collective-dephasing noise channel. Since none of the logical qubits is a decoy, the logical qubits for Eve are the (2*nd*, 3*rd*) and the (5*th*, 6*th*) qubits of the original GHZ states, $|G\rangle_{123} \otimes |G\rangle_{456}$. After Eve performs the Bell measurement on both the (2*nd*, 5*th*) and the (3*rd*, 6*th*) qubits, the result will correspond to one of Bell measurement results of Alice as shown in Eq. (3). Based on Eq. (3), each result occurs with a probability of 25 % $(= \frac{1}{4})$. For example, if the measurement result of Eve is $\left\{\left|\Phi^+\right\rangle_{25}\left|\Phi^+\right\rangle_{36}, \left|\Phi^-\right\rangle_{25}\left|\Phi^-\right\rangle_{36}\right\}$ $\left(\left\{\left|\Phi^+\right\rangle_{25}\left|\Phi^-\right\rangle_{36}, \left|\Phi^-\right\rangle_{25}\left|\Phi^+\right\rangle_{36}\right\}, \left\{\left|\Psi^+\right\rangle_{25}\left|\Psi^+\right\rangle_{36}, \left|\Psi^-\right\rangle_{25}\left|\Psi^-\right\rangle_{36}\right\}\right.$, or $\left\{\left|\Psi^+\right\rangle_{25}\right.$ $\left.\left|\Psi^-\right\rangle_{36}, \left|\Psi^-\right\rangle_{25}\left|\Psi^+\right\rangle_{36}\right\}$), then Alice's measurement result is $\left|\Phi^+\right\rangle_{14}$ $(\left|\Phi^-\right\rangle_{14}, \left|\Psi^+\right\rangle_{14}$, or $\left|\Psi^-\right\rangle_{14}$), which implies the raw key is "00" ("01", "10", or "11"). Now suppose Shannon entropy, $E = -\sum_i \rho_i \log_2 \rho_i$, is introduced hereafter, where ρ_i is the probability distribution. The entropy E_1 can be computed as $E_1 = -4 \times \frac{1}{4} \log \frac{1}{4} = 2$.

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\\
&=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\\
&=\frac{1}{2\sqrt{2}}\begin{pmatrix}
\left|\Phi^{+}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\
+\left|\Phi^{-}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\
+\left|\Psi^{+}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\
+\left|\Psi^{-}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})
\end{pmatrix}\\
&=\frac{1}{2\sqrt{2}}\begin{pmatrix}
\left|\Phi^{+}\right\rangle_{14} & (\left|\Phi^{+}\right\rangle_{25}\left|\Phi^{+}\right\rangle_{36}-\left|\Phi^{-}\right\rangle_{25}\left|\Phi^{-}\right\rangle_{36})\\
+\left|\Phi^{-}\right\rangle_{14} & (\left|\Phi^{+}\right\rangle_{25}\left|\Phi^{-}\right\rangle_{36}-\left|\Phi^{-}\right\rangle_{25}\left|\Phi^{+}\right\rangle_{36})\\
+\left|\Psi^{+}\right\rangle_{14} & (\left|\Psi^{+}\right\rangle_{25}\left|\Psi^{+}\right\rangle_{36}-\left|\Psi^{-}\right\rangle_{25}\left|\Psi^{-}\right\rangle_{36})\\
+\left|\Psi^{-}\right\rangle_{14} & (\left|\Psi^{+}\right\rangle_{25}\left|\Psi^{-}\right\rangle_{36}-\left|\Psi^{-}\right\rangle_{25}\left|\Psi^{+}\right\rangle_{36})
\end{pmatrix}
\end{aligned}
\tag{3}
$$

(2) One of the logical qubit is a decoy

If one of the logical qubits intercepted by Eve is a decoy, the (7*th*, 8*th*) qubits, then the decoy one can be either in the state $|0_L\rangle = |01\rangle, |1_L\rangle = |10\rangle, |+_L\rangle = \left|\Psi^{+}\right\rangle$ or $|-_L\rangle = \left|\Psi^{-}\right\rangle$ with the same probability. Suppose the other logical qubit intercepted by Eve is the (2*nd*, 3*rd*) qubits of GHZ states $|G\rangle_{123}\otimes|G\rangle_{456}$. After Eve performs the Bell measurement on both the (2*nd*, 7*th*) and the (3*rd*, 8*th*) qubits, the result will correspond to one of Bell measurement results of Alice as shown in Eqs. (4), (5), (6) and (7), respectively. As in Eqs. (4) and (5), when the decoy is in $|0_L\rangle$ (or $|1_L\rangle$), the probability of getting each Alice's result is 6.25 % ($=\frac{1}{16}$). For instance, if the measurement result of Eve is $\left|\Phi^{+}\right\rangle_{27}\left|\Phi^{+}\right\rangle_{38}$ or $\left|\Phi^{-}\right\rangle_{27}\left|\Phi^{-}\right\rangle_{38}$, then Alice's measurement result is $\left|\Phi^{+}\right\rangle_{14}$ with 6.25 % probability. Conversely, when the decoy is in $|+_L\rangle$ (or $|-_L\rangle$), the probability of getting each Alice's result is 3.125 % ($=\frac{1}{32}$) as shown in Eqs. (6) and (7). For instance, if the measurement result of Eve is $\left|\Phi^{+}\right\rangle_{27}\left|\Phi^{+}\right\rangle_{38}$ or $\left|\Phi^{-}\right\rangle_{27}\left|\Phi^{-}\right\rangle_{38}$, then Alice's measurement result is $\left|\Phi^{+}\right\rangle_{14}$ with 3.125 % probability. Furthermore, since the original GHZ states are $|G\rangle_{123}\otimes|G\rangle_{456}$, there are only four situations in Eqs. (4) and (5), and eight situations in Eqs. (6) and (7), that are consistent to the entanglement swapping results of $|G\rangle_{123}\otimes|G\rangle_{456}$, in which Eve will obtain useful information. That is, if Alice's measurement result is $\left|\Phi^{+}\right\rangle_{14}$ ($\left|\Phi^{-}\right\rangle_{14}$, $\left|\Psi^{+}\right\rangle_{14}$, or $\left|\Psi^{-}\right\rangle_{14}$), then Eve's measurement result is $\left\{\left|\Phi^{+}\right\rangle_{27}\left|\Phi^{+}\right\rangle_{38},\left|\Phi^{-}\right\rangle_{27}\left|\Phi^{-}\right\rangle_{38}\right\}$ $\left(\left\{\left|\Phi^{+}\right\rangle_{27}\left|\Phi^{-}\right\rangle_{38},\left|\Phi^{-}\right\rangle_{27}\left|\Phi^{+}\right\rangle_{38}\right\},\left\{\left|\Psi^{+}\right\rangle_{27}\left|\Psi^{+}\right\rangle_{38},\left|\Psi^{-}\right\rangle_{27}\left|\Psi^{-}\right\rangle_{38}\right\}\right.$, or $\left.\left\{\left|\Psi^{+}\right\rangle_{27}\left|\Psi^{-}\right\rangle_{38},\left|\Psi^{-}\right\rangle_{27}\left|\Psi^{+}\right\rangle_{38}\right\}\right)$. Hence, the entropy E_2 can be computed as $E_2=\frac{1}{2}\left(-4\times\frac{1}{16}\log\frac{1}{16}\right)+\frac{1}{2}\left(-8\times\frac{1}{32}\log\frac{1}{32}\right)=1.125$.

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\otimes|01\rangle_{78}\\
&=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\otimes|01\rangle_{78}\\
&=\frac{1}{2\sqrt{2}}\begin{pmatrix}
\left|\Phi^{+}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\
+\left|\Phi^{-}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\
+\left|\Psi^{+}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\
+\left|\Psi^{-}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})
\end{pmatrix}\otimes|01\rangle_{78}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{4\sqrt{2}}\{|\Phi^+\rangle_{14}[(|\Psi^+\rangle|\Psi^+\rangle+|\Psi^+\rangle|\Psi^-\rangle-|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|10\rangle_{56}\\
&\quad+(|\Phi^+\rangle|\Phi^+\rangle-|\Phi^+\rangle|\Phi^-\rangle+|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|01\rangle_{56}]\\
&\quad+|\Phi^-\rangle_{14}[(|\Psi^+\rangle|\Psi^+\rangle+|\Psi^+\rangle|\Psi^-\rangle-|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|10\rangle_{56}\\
&\quad-(|\Phi^+\rangle|\Phi^+\rangle-|\Phi^+\rangle|\Phi^-\rangle+|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|01\rangle_{56}]\\
&\quad+|\Psi^+\rangle_{14}[(|\Psi^+\rangle|\Psi^+\rangle+|\Psi^+\rangle|\Psi^-\rangle-|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|01\rangle_{56}\\
&\quad+(|\Phi^+\rangle|\Phi^+\rangle-|\Phi^+\rangle|\Phi^-\rangle+|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|10\rangle_{56}]\\
&\quad+|\Psi^-\rangle_{14}[(|\Psi^+\rangle|\Psi^+\rangle+|\Psi^+\rangle|\Psi^-\rangle-|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|01\rangle_{56}\\
&\quad-(|\Phi^+\rangle|\Phi^+\rangle-|\Phi^+\rangle|\Phi^-\rangle+|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|10\rangle_{56}]\} \qquad (4)
\end{aligned}
$$

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\otimes|10\rangle_{78}\\
&= \frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\otimes|10\rangle_{78}\\
&= \frac{1}{2\sqrt{2}}\begin{pmatrix}|\Phi^+\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\ +|\Phi^-\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\ +|\Psi^+\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\ +|\Psi^-\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})\end{pmatrix}\otimes|10\rangle_{78}\\
&= \frac{1}{4\sqrt{2}}\{|\Phi^+\rangle_{14}[(|\Phi^+\rangle|\Phi^+\rangle+|\Phi^+\rangle|\Phi^-\rangle-|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|10\rangle_{56}\\
&\quad+(|\Psi^+\rangle|\Psi^+\rangle-|\Psi^+\rangle|\Psi^-\rangle+|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|01\rangle_{56}]\\
&\quad+|\Phi^-\rangle_{14}[(|\Phi^+\rangle|\Phi^+\rangle+|\Phi^+\rangle|\Phi^-\rangle-|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|10\rangle_{56}\\
&\quad-(|\Psi^+\rangle|\Psi^+\rangle-|\Psi^+\rangle|\Psi^-\rangle+|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|01\rangle_{56}]\\
&\quad+|\Psi^+\rangle_{14}[(|\Phi^+\rangle|\Phi^+\rangle+|\Phi^+\rangle|\Phi^-\rangle-|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|01\rangle_{56}\\
&\quad+(|\Psi^+\rangle|\Psi^+\rangle-|\Psi^+\rangle|\Psi^-\rangle+|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|10\rangle_{56}]\\
&\quad+|\Psi^-\rangle_{14}[(|\Phi^+\rangle|\Phi^+\rangle+|\Phi^+\rangle|\Phi^-\rangle-|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)_{2738}|01\rangle_{56}\\
&\quad-(|\Psi^+\rangle|\Psi^+\rangle-|\Psi^+\rangle|\Psi^-\rangle+|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)_{2738}|10\rangle_{56}]\} \qquad (5)
\end{aligned}
$$

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\otimes|\Psi^+\rangle_{78}\\
&= \frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\otimes|\Psi^+\rangle_{78}\\
&= \frac{1}{2\sqrt{2}}\begin{pmatrix}|\Phi^+\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\ +|\Phi^-\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\ +|\Psi^+\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\ +|\Psi^-\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})\end{pmatrix}\otimes(|01\rangle+|10\rangle)_{78}\\
&= \frac{1}{8\sqrt{2}}\{|\Phi^+\rangle_{14}[[(|\Psi^+\rangle|\Psi^+\rangle+|\Psi^+\rangle|\Psi^-\rangle-|\Psi^-\rangle|\Psi^+\rangle-|\Psi^-\rangle|\Psi^-\rangle)\\
&\quad+(|\Phi^+\rangle|\Phi^+\rangle-|\Phi^+\rangle|\Phi^-\rangle+|\Phi^-\rangle|\Phi^+\rangle-|\Phi^-\rangle|\Phi^-\rangle)]_{2738}|10\rangle_{56}
\end{aligned}
$$

$$
\begin{aligned}
&+\left[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right.\\
&\left.+\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\right]_{2738}|01\rangle_{56}\Big]\\
&+\left|\Phi^{-}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&+\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\\
&-\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&+\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\Big]\\
&+\left|\Psi^{+}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&+\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\\
&+\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&+\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\Big]\\
&+\left|\Psi^{-}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&+\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\\
&-\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&+\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\Big]\Big\} \quad (6)
\end{aligned}
$$

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\otimes\left|\Psi^{-}\right\rangle_{78}\\
&=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\otimes\left|\Psi^{-}\right\rangle_{78}\\
&=\frac{1}{2\sqrt{2}}\begin{pmatrix}\left|\Phi^{+}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\ +\left|\Phi^{-}\right\rangle_{14} & (|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\ +\left|\Psi^{+}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\ +\left|\Psi^{-}\right\rangle_{14} & (|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})\end{pmatrix}\otimes(|01\rangle-|10\rangle)_{78}\\
&=\frac{1}{8\sqrt{2}}\Big\{\left|\Phi^{+}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\\
&-\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\Big]\\
&+\left|\Phi^{-}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\\
&-\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\Big]\\
&+\left|\Psi^{+}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\\
&+\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
&-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\Big]\\
&+\left|\Psi^{-}\right\rangle_{14}\Big[\Big[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\\
&-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\Big]_{2738}|01\rangle_{56}\\
&-\Big[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\\
&-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\Big]_{2738}|10\rangle_{56}\Big]\Big\} \quad (7)
\end{aligned}
$$

(3) Both logical qubits are decoys

If both logical qubits are decoys, then their measurement results are independent with the entanglement swapping. Remember that the original GHZ states prepared by Alice are $|G\rangle_{123}\otimes|G\rangle_{456}$. Alice performs the Bell measurement on the ($1st$, $4th$) qubits, the probability of getting the measurement result $\left|\Phi^{+}\right\rangle$ ($\left|\Phi^{-}\right\rangle$, $\left|\Psi^{+}\right\rangle$, or $\left|\Psi^{-}\right\rangle$) is 25 % ($=\frac{1}{4}$). In order to obtain the corresponding Bell measurement results with Alice, Eve performs the Bell measurement on both decoys (D_1, D_4) and (D_2, D_3) qubits, the probability of getting the measurement result $\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle$ or $\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle$ is $\frac{1}{4}\left(=\frac{1}{16}\left(\frac{1}{4}\times 8+\frac{1}{8}\times 16\right)\right)$ as shown in Eqs. (8) and (9). Hence, Eve can obtain the correct product state $\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle$ or $\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle$ with a probability of $\frac{1}{16}\left(=\frac{1}{4}\times\frac{1}{4}\right)$. Therefore, the entropy E_3 can be computed as $E_3=-4\times\frac{1}{16}\log\frac{1}{16}=1$.

$$
\begin{aligned}
|01\rangle_{D_1D_2}\otimes|01\rangle_{D_3D_4}&=\frac{1}{2}\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right.\\
&\quad\left.+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)_{D_1D_3D_2D_4}\\
|01\rangle_{D_1D_2}\otimes|10\rangle_{D_3D_4}&=\frac{1}{2}\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle\right.\\
&\quad\left.-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)_{D_1D_3D_2D_4}\\
|10\rangle_{D_1D_2}\otimes|10\rangle_{D_3D_4}&=\frac{1}{2}\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle\right.\\
&\quad\left.+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)_{D_1D_3D_2D_4}\\
|10\rangle_{D_1D_2}\otimes|01\rangle_{D_3D_4}&=\frac{1}{2}\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle\right.\\
&\quad\left.+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)_{D_1D_3D_2D_4}\\
\left|\Psi^{+}\right\rangle_{D_1D_2}\otimes\left|\Psi^{+}\right\rangle_{D_3D_4}&=\frac{1}{2}\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle\right.\\
&\quad\left.+\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)_{D_1D_3D_2D_4}\\
\left|\Psi^{+}\right\rangle_{D_1D_2}\otimes\left|\Psi^{-}\right\rangle_{D_3D_4}&=\frac{1}{2}\left(-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right.\\
&\quad\left.+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle\right)_{D_1D_3D_2D_4}\\
\left|\Psi^{-}\right\rangle_{D_1D_2}\otimes\left|\Psi^{+}\right\rangle_{D_3D_4}&=\frac{1}{2}\left(-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right.\\
&\quad\left.+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle\right)_{D_1D_3D_2D_4}
\end{aligned}
$$

$$
\begin{aligned}
\left|\Psi^{-}\right\rangle_{D_1D_2}\otimes\left|\Psi^{-}\right\rangle_{D_3D_4} &= \frac{1}{2}\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle\right. \\
&\quad \left.+\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)_{D_1D_3D_2D_4} \qquad (8)\\
|01\rangle_{D_1D_2}\otimes\left|\Psi^{+}\right\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right. \\
&\quad +\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle\right. \\
&\quad \left.\left.-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
|01\rangle_{D_1D_2}\otimes\left|\Psi^{-}\right\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle\right.\right. \\
&\quad \left.-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle\right. \\
&\quad \left.\left.+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
|10\rangle_{D_1D_2}\otimes\left|\Psi^{+}\right\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle\right.\right. \\
&\quad \left.-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)+\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
|10\rangle_{D_1D_2}\otimes\left|\Psi^{-}\right\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle\right.\right. \\
&\quad \left.-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
\left|\Psi^{+}\right\rangle_{D_1D_2}\otimes|01\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right.\right. \\
&\quad \left.+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)+\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
\left|\Psi^{+}\right\rangle_{D_1D_2}\otimes|10\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle\right.\right. \\
&\quad \left.+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)+\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
\left|\Psi^{-}\right\rangle_{D_1D_2}\otimes|01\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle+\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle\right.\right. \\
&\quad \left.-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)-\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle+\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \\
\left|\Psi^{-}\right\rangle_{D_1D_2}\otimes|10\rangle_{D_3D_4} &= \frac{1}{2\sqrt{2}}\left[\left(\left|\Psi^{+}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{+}\right\rangle\left|\Psi^{-}\right\rangle\right.\right. \\
&\quad \left.+\left|\Psi^{-}\right\rangle\left|\Psi^{+}\right\rangle-\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle\right)-\left(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Phi^{+}\right\rangle\left|\Phi^{-}\right\rangle\right. \\
&\quad \left.\left.-\left|\Phi^{-}\right\rangle\left|\Phi^{+}\right\rangle-\left|\Phi^{-}\right\rangle\left|\Phi^{-}\right\rangle\right)\right]_{D_1D_3D_2D_4} \qquad (9)
\end{aligned}
$$

Based on the above three situations, if Eve intercepts two logical qubits, then she can obtain the combinations of two states with either (logical qubit, logical qubit), (logical qubit, decoy), (decoy, logical qubit) or (decoy, decoy). Thus, the probability for three situations is $\frac{1}{4}$, $\frac{1}{2}$ and $\frac{1}{4}$, respectively. To summarize, the entire entropy E_T ($= \frac{1}{4} \times E_1 + \frac{1}{2} \times E_2 + \frac{1}{4} \times E_3 = 1.3125$) can be computed, i.e., Eve can reveal 1.3125 bits by performing the intercept-resend attack. However, this attack will eventually be detected in the public discussion of decoy logical qubits. Even if the eavesdropper passes the public discussion, one can still perform the privacy amplification process [31,32] on the transmitted information to avoid the information leakage problem.

5.2 Security against entangle-and-measure attack

In this attack, we assume that Eve has unlimited computing power and technology except for being limited by the laws of quantum mechanics [20,38,39]. In order to capture the transmitted information, Eve prepares some auxiliary qubits, and then she intercepts S'_B and entangles these auxiliary qubits with the intercepted S'_B by performing unitary operation U_E, where U_E satisfies $U_E^{\dagger} U_E = U_E U_E^{\dagger} = I$. Eve measures these auxiliary qubits in hope that she can obtain useful information. In the proposed schemes, however, once Eve makes the auxiliary qubits to obtain useful information about the decoy logical qubits, she will disturb the decoy logical qubits and being detected in the public discussion. Thus, the proposed protocols are free from the entangle-and-measure attack. A similar analysis is described in [24].

5.3 Security under a lossy quantum channel

This subsection shows that the proposed protocols are also secure under a lossy channel, i.e., the quantum channel between Alice and Bob is lossy. We also assume that Eve has the capability of establishing an ideal channel with any user. In order to derive Alice's raw key, Eve intercepts the logical qubits transmitted from Alice to Bob, retains some logical qubits (e.g. y logical qubits) to herself, as if these y qubits have been lost in a lossy channel, and sends the substitute y logical qubits to Bob through an ideal channel. If the intercepted logical qubits are not decoy logical qubits, then Eve can measure the logical qubits in Bell basis. The measurement result will correspond to Alice's key bits.

However, the proposed protocols are secure against this kind of attack because Alice and Bob use the received logical qubits to do the public discussion and to share the raw key. The probability to detect 1-qubit modification is 50 % (the same as Sect. 5.1). The detection probability is $1 - \left(\frac{1}{2}\right)^y$, if y-qubit is substituted. While y is large enough, the detection probability is approximately 100 %. Thus, our protocols are still secure under this case. If there are only a few qubits being disturbed, then classical error correction codes and message authentication codes can be applied. However, this is not the focus of this paper.

6 Conclusion

This paper proposes two QKD protocols which are resistant to one kind of collective noises: the collective-dephasing noise and the collective-rotation noise, respectively. Moreover, the security analysis shows that the proposed protocols can avoid several well-known attacks and are still secure under the lossy quantum channel. Based on Bell measurements, an entanglement can be constructed from two independent GHZ state systems. Furthermore, by applying the decoy logical qubits and the entanglement swapping on constructing QKD protocols, the qubit efficiency of the proposed schemes can reach 20 %, which provides the best qubit efficiency among the existing QKD protocols.

Acknowledgments We would like to thank the anonymous reviewers for their very valuable comments, which greatly enhanced the clarity of this paper. We would also like to thank the National Science Council of Republic of China, for thefinancial support of this research under Contract No. NSC 100-2221-E-006-152-MY3.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Presented at the Proceedings of IEEE International Conference on Computers Systems and Signal Processing. Bangalore, India (1984)
2. Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with potential 100 % qubit efficiency. IET Inf. Secur. **1**(1), 43–45 (2007)
3. Shih, H.C., Lee, K.C., Hwang, T.: New efficient three-party quantum key distribution protocols. IEEE J. Sel. Top Quantum **15**(6), 1602–1606 (2009)
4. Hwang, T., Lee, K.C., Li, C.M.: Provably secure three-party authenticated quantum key distribution protocols. IEEE Trans. Depend. Secur. **4**(1), 71–80 (2007)
5. Hwang, T., Hwang, C.C., Tsai, C.W.: Quantum key distribution protocol using dense coding of three-qubit W state. Euro. Phys. J. D **61**(3), 785–790 (2011)
6. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**(11), 2097–2100 (2004)
7. Zhang, Z.J., Man, Z.X., Shi, S.H.: An efficient multiparty quantum key distribution scheme. Int. J. Quantum Inf. **3**(3), 555–560 (2005)
8. 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)
9. Zanardi, P., Rasetti, M.: Noiseless quantum codes. Phys. Rev. Lett. **79**(17), 3306 (1997)
10. Knill, E., Laflamme, R., Viola, L.: Theory of quantum error correction for general noise. Phys. Rev. Lett. **84**(11), 2525 (2000)
11. Kwiat, P.G., Berglund, A.J., Altepeter, J.B., White, A.G.: Experimental verification of decoherence-free subspaces. Science **290**(5491), 498–501 (2000)
12. Kempe, J., Bacon, D., Lidar, D., Whaley, K.: Theory of decoherence-free fault-tolerant universal quantum computation. Phys. Rev. A **63**(4), 042307 (2001)
13. Boileau, J.C., Gottesman, D., Laflamme, R., Poulin, D., Spekkens, R.W.: Robust polarization-based quantum key distribution over a collective-noise channel. Phys. Rev. Lett. **92**(1), 017901 (2004)
14. Sun, Y., Wen, Q.Y., Gao, F., Zhu, F.C.: Robust variations of the Bennett–Brassard 1984 protocol against collective noise. Phys. Rev. A **80**(3), 032321 (2009)
15. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: Quantum key distribution protocols with six-photon states against collective noise. Opt. Commun. **282**(20), 4171–4174 (2009)
16. Li, X.H., Zhao, B.K., Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Fault tolerant quantum key distribution based on quantum dense coding with collective noise. Int. J. Quantum Inf. **7**(8), 1479–1489 (2009)
17. Li, C.Y., Li, Y.S.: Fault-tolerate quantum key distribution over a collective-noise channel. Int. J. Quantum Inf. **8**(7), 1101–1109 (2010)

18. Cabello, A.: Six-qubit permutation-based decoherence-free orthogonal basis. Phys. Rev. A **75**(2), 020301 (2007)
19. Zhang, Z.J.: Robust multiparty quantum secret key sharing over two collective-noise channels. Phys. A **361**(1), 233–238 (2006)
20. Sun, Y., Wen, Q.Y., Zhu, F.C.: Improving the multiparty quantum secret sharing over two collective-noise channels against insider attack. Opt. Commun. **283**(1), 181–183 (2010)
21. Gu, B., Mu, L.L., Ding, L.G., Zhang, C.Y., Li, C.Q.: Fault tolerant three-party quantum secret sharing against collective noise. Opt. Commun. **283**(15), 3099–3103 (2010)
22. Yang, C.-W., Tsai, C.-W., Hwang, T.: Thwarting intercept-and-resend attack on Zhang's quantum secret sharing using collective rotation noises. Quantum Inf. Process. **11**(1), 113–122 (2012)
23. Yang, C.-W., Tsai, C.-W., Hwang, T.: Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci. China Phys. **54**(3), 496–501 (2011)
24. Yang, C.-W., Hwang, T.: Improved QSDC protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
25. Yang, C.-W., Hwang, T.: Quantum dialogue protocols immune to collective noise. Quantum Inf. Process. **12**(6), 2131–2131 (2013)
26. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
27. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
28. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack (vol 72, art no 044302, 2005). Phys. Rev. A **73**(4), 049901 (2006)
29. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
30. Yang, C.-W., Hwang, T., Luo, Y.-P.: Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf. Process. **12**(1), 109–117 (2013)
31. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
32. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
33. Lin, J., Hwang, T.: An enhancement on Shi et al'.s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)
34. Lin, J., Tseng, H.-Y., Hwang, T.: Intercept-resend attacks on Chen et al'.s quantum private comparison protocol and the improvements. Opt. Commun. **284**(9), 2412–2414 (2011)
35. Chong, S.-K., Tsai, C.-W., Hwang, T.: Improvement on "quantum key agreement protocol with maximally entangled states". Int. J. Theor. Phys. **50**(6), 1793–1802 (2011)
36. Hwang, T., Hwang, C.-C., Yang, C.-W., Li, C.-M.: Revisiting Deng et al'.s multiparty quantum secret sharing protocol. Int. J. Theor. Phys. **50**(9), 2790–2798 (2011)
37. Shannon, C.E.: Communication theory of secrecy system. Bell Syst. Tech. J. **28**, 656–715 (1949)
38. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
39. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)