International Journal of Theoretical Physics (2019) 58: 1326–1336
https://doi.org/10.1007/s10773-019-04025-7

The Security Analysis of Quantum B92 Protocol in Collective-Rotation Noise Channel

Leilei Li[1] · Jian Li[1] · Chaoyang Li[1] · Hengji Li[1] · Yuguang Yang[2] · Xiubo Chen[3]

Received: 17 August 2018 / Accepted: 24 January 2019 / Published online: 4 February 2019

Abstract
Quantum communication protocols should take the effect of noise into account in a real environment. To analyze the security of the quantum B92 protocol presented by Bennett in collective-rotation noise channel, an excellent model of noise analysis is proposed. In the security analysis, the eavesdropping can be detected with the increment of the qubits error rate (ber). When the level of noise less than 0.50, it will cause a larger bit error rate if the eavesdropper Eve wants to obtain the same amount of information. In our analysis, Eve can maximally get about 50% of the key from the communication when the noise level approximates to 0.5. We also presented a new idea in analyzing the protocol security in collective-rotation noise channel with the idea of the Markov process.

Keywords The quantum B92 protocol · Collective rotation noise · Security analysis · Qubit error rate · Information entropy

1 Introduction

Cryptography is the basis of information security, the task of cryptograph is to ensure that only the legitimate users like Alice and Bob can read the secret message in the secure communication, which the unauthorized users like Eve cannot read. The key is used to encrypt and decrypt information in cryptography. Quantum Cryptography, based on the quantum mechanics, which is definitely different from the classical digital cryptographic system, and has much higher performance of security.

✉ Jian Li
buptlijian@126.com

Leilei Li
lileilei258@qq.com

[1] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

[3] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China

Quantum communication and quantum Cryptography mainly includes quantum key distribution (QKD) [1, 18, 32] , quantum teleportation (QT) [21, 26], quantum secret sharing (QSS) [10, 14], quantum secure direct communication (QSDC) [11, 29, 30], etc. In 1984, C.H. Bennett presented the first QKD protocol, which called the BB84 protocol [3]. The BB84 protocol needs four states of particle, the sender Alice randomly sends one of them to the receiver Bob, Bob randomly choose a measurement basis to measure the particles. After measurements, Bob announce his measurement basis and Alice tell him which part is right. The right part can be used as the original keys. The BB84 protocol has been the most widely used QKD protocol since it was presented because the BB84 protocol doesn't need to store quantum states and it only uses the pure states. In 1992, Bennett creatively put forward a simplified version of BB84 with only two non-orthogonal states of QKD scheme, the most concise key distribution scheme is called B92 protocol [2]. Compared with the BB84 protocol, the B92 protocol doesn't need to public their measurement result through public channel because it only uses two non-orthogonal quantum particle, the receiver can determine the right qubit with the measurement basis and measurement result. The efficiency of B92 protocol is 25% in ideal environment, while BB84 protocol is 50%. But the B92 protocol represents the two-state quantum key distribution protocol, which required less experimental equipment and relatively more simple procedure, meanwhile considered with better prospects in secure communication. This protocol has received lots of attention since it was put forward [12, 13]. Since then, a lot of quantum information security processing methods have been advanced [5, 6, 8, 19, 22–25, 27, 31].

However, those analyses often ignored the effect of the environment noise, which cannot be neglected in practice [28]. The environmental noise must produce certain effect in the quantum state. We can use error correction coding or privacy amplification to restrain noise and interference, but if applied to a real communication environment, it is necessary to take into account the effect of noise. So the security analysis of the protocol is necessary. A quantum communication protocol has good robustness only if it has been proved security in a real environment.

This paper introduced an excellent model of collective rotation noise analysis with the idea of Markov process and applied the information theory to analyze the security of B92 protocol in the noise environment [7, 33]. The eavesdropper(Eve) can be detected all the time under a certain level of noise $\varepsilon \leq 0.50$. What's more, according to the average mutual information of the information theory [15], the range of information that Eve can attain is from 0.399 to 0.5. It can be concluded that the threshold of bit error rate is variable with the change of the level of environment noise ε, and when $\varepsilon \leq 0.50$, the B92 protocol is secure in the real noise environment, and Eve can only gets parts of qubits so that she can't read the keys transmitted in the quantum channel. Meaning Eve cannot get security messages encrypted by the quantum keys between Alice and Bob.

2 Related Works

2.1 Brief Introduction of Quantum B92 Protocol

Let's give a brief introduction of the B92 protocol which is presented by C.H. Bennett in 1992 [2]. The sender Alice randomly sends $|0\rangle$ or $|+\rangle$, where $|0\rangle$ represents 0 and $|+\rangle$ represents 1.

Alice sends the corresponding qubit to Bob through the quantum channel. As is known to all, there are two groups of basis, $Z\text{-}basis$: $B_Z = \{|0\rangle, |1\rangle\}$ and $X\text{-}basis$: $B_X = \{|+\rangle, |-\rangle\}$.

Table 1 The record of Bob with different basis and result

Basis	Result	Record
X	$\|-\rangle$	$\|0\rangle$
Z	$\|1\rangle$	$\|+\rangle$

After receiving the qubit, Bob uses B_Z or B_X to measure it. If the measurement result is $|1\rangle$ based on B_Z, Bob records. If the measurement result is $|-\rangle$ based on B_X, Bob records. Other measurement results are not taken into account. Just as Table 1 shows. Repeat the process until all qubits are transmitted.

This is a brief example of the quantum B92 protocol when Alice tries to send $|0\rangle$ to Bob.

1. Alice prepares the quantum state $|0\rangle$ and sends it to Bob.
2. After receiving the qubit from Alice, Bob randomly chooses $B_X = \{|+\rangle, |-\rangle\}$ or $B_Z = \{|0\rangle, |1\rangle\}$ to measure it.
   (a) Bob chooses B_X, he will receive $|+\rangle$ or $|-\rangle$ with the same probability.
   (b) Bob chooses B_Z, he always gets $|0\rangle$.
   (c) When Bob gets $|+\rangle$ with B_X, he cannot determine which qubit Alice sends. (Alice sends $|0\rangle$ or $|+\rangle$, Bob can still gets $|+\rangle$ with B_X).
   (d) When Bob gets $|-\rangle$ with B_X, he can determine the qubit that Alice sends. (Only Alice sends $|0\rangle$ can Bob gets $|-\rangle$ with B_X).
   (e) When Bob gets $|0\rangle$ with B_Z, he cannot determine which qubit Alice sends. (Alice sends $|0\rangle$ or $|+\rangle$, Bob can still gets $|0\rangle$ with B_Z).
3. Bob gets $|-\rangle$ with B_X, he can determine that Alice sends $|0\rangle$.
4. The B92 protocol ends successfully.

The recorded data is then converted to a sequence of 0 and 1. The sequence of 0 and 1 can be then used as the raw keys. To detect the eavesdropping behaviors, Alice and Bob contrast a little segment of the raw keys. If there is bit error, the channel is eavesdropped. Alice and Bob terminate communication and restart a new one.

Compared with BB84 protocol, B92 protocol doesn't need to public their measurement bases. It's easily to get that the efficiency of B92 protocol is 25% in ideal environment. That's to say, 75% of the particles in the B92 protocol will be abandoned, only 25% can be remained as the original key. So the B92 protocol is a simplified version of the BB84 protocol, and it has only half the efficiency of the BB84 protocol.

2.2 The Noise in B92 Protocol

The noise and eavesdropping can't be distinguished between each other. The qubits error rate *ber* may result from Alice to Bob, Alice to Eve and Eve to Bob.

In the original B92 protocol, the qubit error rate just results from the eavesdropping. So if there is a bit error, Alice and Bob think that there is an eavesdropper. But the bit error can be caused by not only eavesdropping behavior, but also noise. Meaning that the original B92 protocol can't be used in the noise environment. The mechanism to judge whether there exists eavesdropping in quantum noise channel needs to be improved for protecting the information.

An initial qubit error rate ber_0 can be set according to the noisy quantum channel. If the qubit error rate ber_i of quantum communication channel is larger than ber_0, it can be

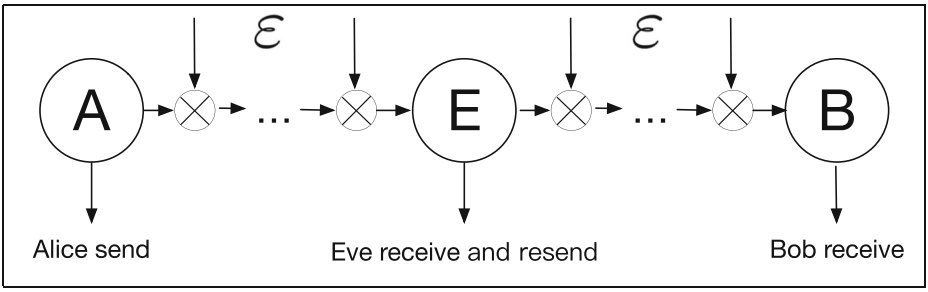

Fig. 1 The noise model based the idea of Markov process

determined that the quantum channel is not secure and exists eavesdropping, no matter what the reason is.

Figure 1 shows the noise model between Alice and Bob with the eavesdropping behaviors. Based the idea of Hidden Markov Model, only three states can be observed, the noise can effect the quantum states any times (form 0 to ∞). To simplify analysis process, we can suppose that all the effect of noise can be summed up into once. In another word, the noise only effect the quantum states once between Alice to Eve and Eve to Bob. We only need two take the effect of noise into consider twice during the whole security analysis.

2.3 Brief Introduction of the Collective-Rotation Noise Channel

During the process of analyzing the security conveniently, an assumption can be reasonably proposed that the environmental noise is constant. Even if actually noise is variable, the maximum or average value of the noise can still be conducted. To ensure the security of the B92 protocol, we should take the maximum value into account.

The noise will produce the same effect on every particle in an ideally collective-rotation noise environment. From the features of collective rotation noise shown in [9, 17, 20] , the effect is making every particle left or right deflect θ angle. The effect of the collective rotation noise could read as the following unitary matrix U,

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

Under the collective rotation noise, the quantum states become:

$$\begin{aligned}
|0\rangle &\rightarrow \cos\theta|0\rangle + \sin\theta|1\rangle = \frac{\cos\theta+\sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta-\sin\theta}{\sqrt{2}}|-\rangle \\
|1\rangle &\rightarrow -\sin\theta|0\rangle + \cos\theta|1\rangle = \frac{\cos\theta-\sin\theta}{\sqrt{2}}|+\rangle - \frac{\cos\theta+\sin\theta}{\sqrt{2}}|-\rangle \\
|+\rangle &\rightarrow \frac{\cos\theta-\sin\theta}{\sqrt{2}}|0\rangle + \frac{\cos\theta+\sin\theta}{\sqrt{2}}|1\rangle = \cos\theta|+\rangle - \sin\theta|-\rangle \\
|-\rangle &\rightarrow \frac{\cos\theta+\sin\theta}{\sqrt{2}}|0\rangle - \frac{\cos\theta-\sin\theta}{\sqrt{2}}|1\rangle = \sin\theta|+\rangle + \cos\theta|-\rangle
\end{aligned} \tag{2}$$

As we all know, without noise and Eve's attack, Bob's records cannot go wrong. Therefore, the noise level ε can be defined as the average error rate of Bob's records under the circumstance where only noise appears but attacks don't. The value of ε will be given in the subsequent discussion.

Table 2 The result of Bob's receive. Where P is probability of sending, A is Alice and B is Bob

P	A/B	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\frac{1}{2}$	$\|0\rangle$	$\frac{\cos^2\theta}{4}$	$\frac{\sin^2\theta}{4}$	$\frac{1-\sin 2\theta}{8}$	$\frac{1+\sin 2\theta}{8}$
$\frac{1}{2}$	$\|+\rangle$	$\frac{1+\sin 2\theta}{8}$	$\frac{1-\sin 2\theta}{8}$	$\frac{\cos^2\theta}{4}$	$\frac{\sin^2\theta}{4}$

3 The Security Analysis of B92 Protocol in the Noise Environment

3.1 The Environment Noise Level ε Without Eavesdropper

Alice sends the quantum bit $|0\rangle$ and $|+\rangle$ with the probability of 50% separately, after the effect of the noise in the quantum channel. Let's analysis the probability when Alice sends $|0\rangle$ and Bob receivers $|0\rangle$.

the probability that Alice sends $|0\rangle$ is $\frac{1}{2}$.According to Formula 2, the probability that Bob receivers $|0\rangle$ is:

$$P = \frac{1}{2} \times \cos^2\theta \times \frac{1}{2} = \frac{\cos^2\theta}{4} \tag{3}$$

And other calculations are similar. The outcome of Bob's measurement is shown in Table 2.

Considering that there exists the discard of bits, When Alice sends $|0\rangle$ Bob receives $|1\rangle$ and Alice sends $|+\rangle$ Bob receives $|-\rangle$, means there is a bit error. Thus the raw key bit error rate ber_0 can be easily calculated:

$$ber_0 = (\frac{\sin^2\theta}{4} + \frac{\sin^2\theta}{4}) \times 2 = \sin^2\theta \tag{4}$$

That is to say, when there is no eavesdropping in the noisy channel, the qubit error rate which just result from the noise should be $ber_0 = \sin^2\theta$. According to the Sections 2.2 and 2.3, ε should be set to ber_0.

$$\varepsilon = ber_0 = \sin^2\theta \tag{5}$$

3.2 The Amount of Information Obtained by the Eavesdropper

In Ref [4] , the authors have proved that if the information that the receiver Bob gets from the sender Alice $I(A, B)$ is larger than the information that the eavesdropper Eve gets from Alice $I(A, E)$. The quantum communication is feasible. So we can compare the information entropy $I(A, B)$ with $I(A, E)$ to analysis the security of the quantum B92 protocol.

To make calculation simplified, we can reasonably assume that the qubits only be affected by noise once during a transmission process. That is to say, before the man-in-middle eavesdropping happens, the noise has made the one-time all effects on every particle [15]. The eavesdropper Eve measures the qubits after the effect of the noise. The qubits state she gets after her measurement just as Bob in Table 2. Now let us analyze how much information Eve can maximally gain. According to the Von Neumann entropy, The information that can be extracted from this state can be given by average mutual information $I(A, E)$.

$$I(A, E) = H(A) - H(A|E) \tag{6}$$

Because the qubit is sent randomly by Alice, so $H(A) = 1$ and

$$H(A|E) = -\sum p(A, E) \log_2 p(A|E) \tag{7}$$

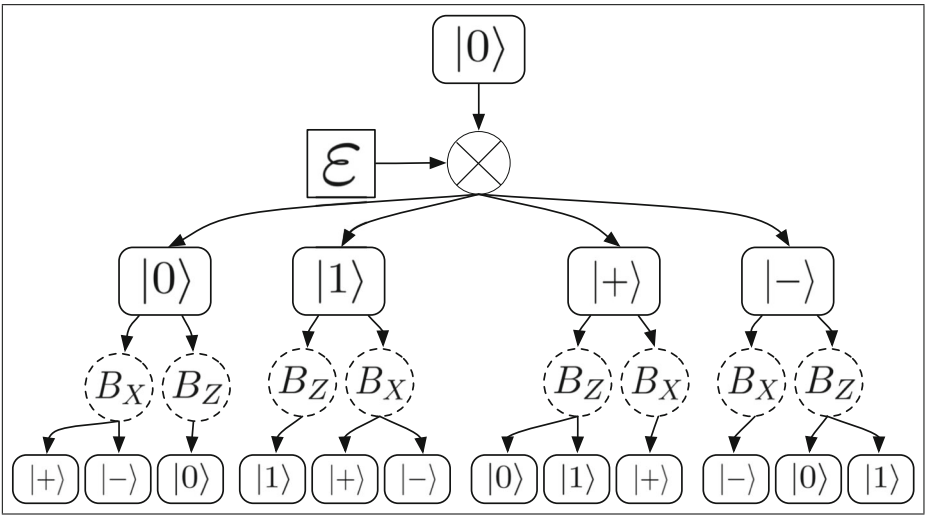

Fig. 2 The measurement results when Alice sends $|0\rangle$

According to Table 2, the noise level $\varepsilon = \sin^2\theta$ and $\xi = \cos^2\theta = 1-\varepsilon$, the maximal information Eve $I(A,E)$ can be rewritten [16]:

$$I(A,E) = 1 + \frac{\xi}{2}\log_2\xi + \frac{\varepsilon}{2}\log_2\varepsilon + \frac{1-2\sqrt{\varepsilon\xi}}{4}\log_2\frac{1-2\sqrt{\varepsilon\xi}}{2} + \frac{1+2\sqrt{\varepsilon\xi}}{4}\log_2\frac{1+2\sqrt{\varepsilon\xi}}{2} \tag{8}$$

The value of $I(A,E)$ is determined by ε and $\xi = 1-\varepsilon$. In another word, $I(A,E)$ is determined by the level of environment noisy ε. Once ε is determined, we can easily calculate $I(A,E)$

3.3 The Receiver'S Measurement Result in Noisy Environment

According to the Tables 1 and 2, we can conclude the measurement results in noisy environment. Figure 2 shows the measurement results when Alice sends $|0\rangle$.

From Fig. 2, we can easily calculate the probability distribution of the measurement results. For example, when Alice sends $|0\rangle$ and receiver's measurement result is also $|0\rangle$, the probability is $p_{|0\rangle\to|0\rangle}$:

$$\begin{aligned} p_{|0\rangle\to|0\rangle} &= \frac{\cos^2\theta}{4} + \frac{1-sin2\theta}{8}\times\frac{1}{2} + \frac{1+sin2\theta}{8}\times\frac{1}{2} \\ &= \frac{1}{8} + \frac{\cos^2\theta}{4} \end{aligned} \tag{9}$$

The rest of the situation is similar, so we can get the probability of receiver's measurement, just as Table 3 shows:

Table 3 The result of receiver's measurement. Where A is Alice and R is receiver (Bob or Eve)

A/R	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$\frac{1}{8}+\frac{\cos^2\theta}{4}$	$\frac{1}{8}+\frac{\sin^2\theta}{4}$	$\frac{1}{8}+\frac{1-\sin 2\theta}{8}$	$\frac{1}{8}+\frac{1+\sin 2\theta}{8}$
$\|+\rangle$	$\frac{1}{8}+\frac{1+\sin 2\theta}{8}$	$\frac{1}{8}+\frac{1-\sin 2\theta}{8}$	$\frac{1}{8}+\frac{\cos^2\theta}{4}$	$\frac{1}{8}+\frac{\sin^2\theta}{4}$

3.4 The Bit Error Rate Caused by Eavesdropping

Suppose Eve intercepts qubits from Alice, takes a measurement and resends the qubits to Bob. When Eve's measurement is $|1\rangle$ or $|-\rangle$, she has two choice: one is resending the measurement to Bob directly, the other is resending $|0\rangle$ and $|+\rangle$ with the same probability.

According to the Table 3, When Alice sends $|0\rangle$ and $|+\rangle$ with the same probability, we can calculate Eve's measurement result:

$$
\begin{aligned}
|0\rangle &: \frac{1}{2}\times\left(\frac{1}{8}+\frac{\cos^2\theta}{4}+\frac{1}{8}+\frac{1+\sin 2\theta}{8}\right)=\frac{3+2\cos^2\theta+\sin 2\theta}{16}=r_{|0\rangle}\\
|1\rangle &: \frac{1}{2}\times\left(\frac{1}{8}+\frac{\sin^2\theta}{4}+\frac{1}{8}+\frac{1-\sin 2\theta}{8}\right)=\frac{3+2\sin^2\theta-\sin 2\theta}{16}=r_{|1\rangle}\\
|+\rangle &: \frac{1}{2}\times\left(\frac{1}{8}+\frac{1-\sin 2\theta}{8}+\frac{1}{8}+\frac{\cos^2\theta}{4}\right)=\frac{3+2\cos^2\theta-\sin 2\theta}{16}=r_{|+\rangle}\\
|-\rangle &: \frac{1}{2}\times\left(\frac{1}{8}+\frac{1+\sin 2\theta}{8}+\frac{1}{8}+\frac{\sin^2\theta}{4}\right)=\frac{3+2\sin^2\theta+\sin 2\theta}{16}=r_{|-\rangle}
\end{aligned}
\tag{10}
$$

3.4.1 Eve Resends Her Measurement Directly

Eve chooses to resend her measurement directly, we can calculate the bit error rate ber_1 with the help of formula 5, 10 and Table 2.

$$
\begin{aligned}
ber_1 = 2\times\Bigg(& r_{|0\rangle}\times\left(\frac{\sin^2\theta}{4}+\frac{1+\sin 2\theta}{8}\right)\\
&+r_{|1\rangle}\times\left(\frac{\cos^2\theta}{4}+\frac{1-\sin 2\theta}{8}\right)\\
&+r_{|+\rangle}\times\left(\frac{1-\sin 2\theta}{8}+\frac{\sin^2\theta}{4}\right)\\
&+r_{|-\rangle}\times\left(\frac{1+\sin 2\theta}{8}+\frac{\cos^2\theta}{4}\right)\Bigg)\\
=\ & \frac{7+2\sin^2 2\theta}{16}=\frac{7+8\varepsilon(1-\varepsilon)}{16}
\end{aligned}
\tag{11}
$$

3.4.2 Eve Resends $|0\rangle$ or $|+\rangle$ Instead

When Eve's measurement result is $|0\rangle$ or $|+\rangle$, she doesn't know which qubit her receives. She can randomly resends $|0\rangle$ or $|+\rangle$ with the same probability. Suppose the probability

that Eve resends $|0\rangle$ is $p_{|0\rangle}$ and $p_{|+\rangle}$ is the probability of resending $|+\rangle$, $p_{|0\rangle} + p_{|+\rangle} = 1$. According to the formula 10 we can calculate they easily.

$$\begin{aligned} p_{|0\rangle} &= \frac{3 + 2\cos^2\theta + \sin 2\theta}{16} + \frac{1}{2} \times \left(\frac{3 + 2\sin^2\theta - \sin 2\theta}{16} + \frac{3 + 2\sin^2\theta + \sin 2\theta}{16} \right) \\ &= \frac{8 + \sin 2\theta}{16} \end{aligned} \tag{12}$$

$$\begin{aligned} p_{|+\rangle} &= \frac{3 + 2\cos^2\theta - \sin 2\theta}{16} + \frac{1}{2} \times \left(\frac{3 + 2\sin^2\theta + \sin 2\theta}{16} + \frac{3 + 2\sin^2\theta - \sin 2\theta}{16} \right) \\ &= \frac{8 - \sin 2\theta}{16} = 1 - p_{|0\rangle} \end{aligned} \tag{13}$$

According to the Table 3, we can calculate the bit error rate ber_2 when Eve resend $|0\rangle$ or $|+\rangle$ instead $|1\rangle$ or $|-\rangle$.

$$\begin{aligned} ber_2 &= 2 \times \left(p_{|0\rangle} \times \left(\frac{1}{8} + \frac{\sin^2\theta}{4} \right) + p_{|1\rangle} \times \left(\frac{1}{8} + \frac{\sin^2\theta}{4} \right) \right) \\ &= \frac{1}{4} + \frac{1}{2}\sin^2\theta = \frac{1}{4} + \frac{1}{2}\varepsilon \end{aligned} \tag{14}$$

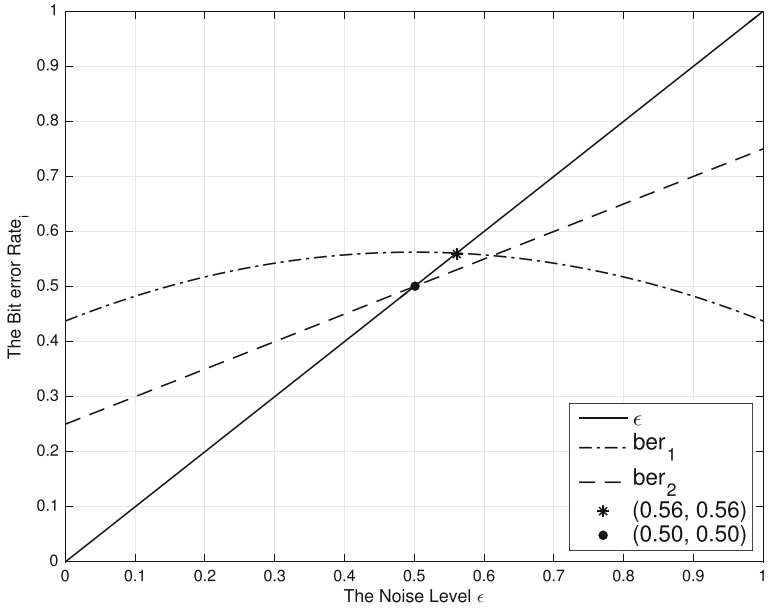

Fig. 3 The relationship between ε and ber_i. Where $ber_0(\varepsilon)$ is caused by environment noise; ber_1 is caused by Eve resends measurement directly to Bob; ber_2 is caused by Eve resends $|0\rangle$ or $|+\rangle$ instead wrong measurement results

3.5 Analyzing the Expression and Data

From Section 3.2 , the followings are known, the maximal information Eve can gain is $I(A, E)$ as Formula 8 shows, the qubit error rate $ber_0(\varepsilon)$, ber_1 and ber_2, as Fig. 3 shows:

As is known to all, Eve would choose a better way to avoid being detected, When the noise level $0.5 \leq \varepsilon \leq 0.56$, $ber_1 \geq ber_0 \geq ber_2$. Means The B92 protocol can still detect eavesdropping When Eve resends measurement result directly, but it cannot detect eavesdropping when Eve chooses to resend new qubits. So for Eve's eavesdropping, it's better to resend $|0\rangle$ or $|+\rangle$ (which is shown in ber_2) rather than resend measurement result directly (which is shown in ber_1).

When the noise level $\varepsilon \leq 0.5$, $ber_2 \geq ber_0$.This means the eavesdropping of Eve has been detected for the increment of qubit error rate. When $\varepsilon = 0$, there is no noise in the channel, in other words, the environment is ideally. The eavesdropping of Eve will also result in 25% of bit error rate, while the qubit error rate should be 0 without eavesdropping. When $\varepsilon \geq 0.5$, means that the environment of communication is too bad and the noise makes bits get wrong very much. So this environment should be avoided and the analysis of this makes no sense. In this paper we will not take into account.

Let's analyze how much information Eve can get from eavesdropping. The maximal information $I_{\max}$ can be depicted as the Fig. 4.

From Fig. 4, when $\varepsilon \to 0.5$, the maximal amount of information that Eve may get is $I_{\max} = 0.50$, while the minimal information is $I_{\min} = 0.399$ from her eavesdropping and measurement. When $\varepsilon \geq 0.5$, the environment of communication is too bad and we will not take into discussion.

In our analysis, Eve can get 50% of the original keys, but she doesn't know which parts her gets. Even if partial key is leaked, Eve cannot decrypt with an incomplete key. In another word, the B92 protocol is security in the collective-rotation noise channel when $\varepsilon \leq 0.50$.

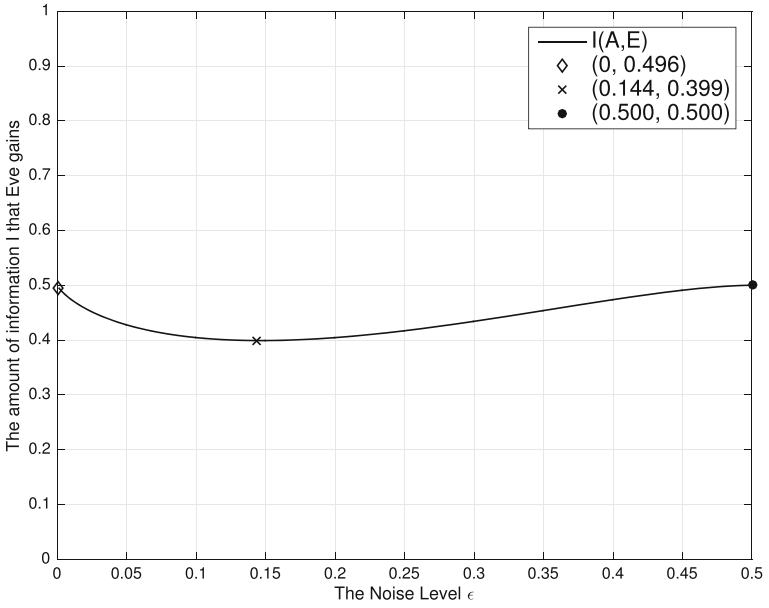

Fig. 4 The relation between ε and I

4 Conclusions

From the analysis of Fig. 3, when the noise in the environment is determined, the qubit error rate will be on the increment as the noise level increases. When $\varepsilon < 0.50$, Eve's eavesdropping will cause the increment of the ber_i, $(i = 1, 2)$ which should be equal as ber_0, Alice and Bob can multiple detect the bit error rate and get the average value to ensure the environmental noise level ber_0, means it is impossible to get the quantum keys without being detected. From Fig. 4 The maximal information Eve can get from her eavesdropping and measurement is $I_{\max} = 0.5$, that is to say, Eve can only get about 50% of the common key bits kept by Alice and Bob but the eavesdropping has been detected and what Eve gets is the incomplete keys, the parts of quantum keys that Eve gets will be useless. She cannot get the security message communicated between Alice and Bob with the incomplete quantum keys.

It's concluded that the quantum key distribution(QKD) protocol called B92 is secure in the noise environment. In other words, the protocol can protect the quantum keys transmitted in the channel. Eve can only get parts of quantum key bits, and she unable to get the security message between Alice and Bob. This result will give new idea for the application of the quantum B92 protocol in communication and information processing with the environmental noise.

Our method also presented a new idea in analyzing the protocol security in Collective-Rotation noise channel. In our method, we found the mathematical relationship between the bit error rate cause by eavesdropping $ber_i (i = 1, 2)$ and the bit error rate caused by environment noise ε. Once the ε is determined, We can easily get the value of ber_i. In our analysis, when ε less than a certain value(this value is 0.50 in the B92 protocol), the threshold to detect eavesdropper can be set higher than the level of environment noise ε, proving that the QKD protocol has a better ability to tolerate noise, making it easy to application to the actual environment.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No.U1636106, No.61472048 and No.61572053).

References

1. Allati, A.E., Baz, M.E., Hassouni, Y.: Quantum key distribution via tripartite coherent states. Quantum Inf. Process. **10**(5), 589–602 (2011)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992)
3. Bennett, C.H., Brassard, G.: An update on quantum cryptography. Lect. Notes Comput. Sci. **196**, 475–480 (1984)
4. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
5. Chang, Y., Zhang, S.B., Zhu, J.M.: Comment on "flexible protocol for quantum private query based on b92 protocol". Quantum Inf. Process. **16**(3), 86 (2017)
6. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on bb84. Opt. Commun. **283**(6), 1192–1195 (2010)
7. Dong, H., Li, D., Xiu, X., Gao, Y.: A deterministic secure quantum communication protocol through a collective rotation noise channel. Int. J. Quantum Inf. **8**(08), 1389–1395 (2010)

8. Etengu, R., Abbou, F.M., Wong, H.Y., Abid, A., Nortiza, N., Setharaman, A.: Performance comparison of bb84 and b92 satellite-based free space quantum optical communication systems in the presence of channel effects. J. Opt. Commun. **32**(1), 37–47 (2011)
9. Fu-Guo, D., Xi-Han, L., Chun-Yan, L., Ping, Z., Hong-Yu, Z.: Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel. Chin. Phys. **16**(2), 277 (2007)
10. Hsu, J.L., Chong, S.K., Hwang, T., Tsai, C.W.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**(1), 331–344 (2013)
11. Hwang, T., Luo, Y.P., Yang, C.W., Lin, T.H.: Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants. Quantum Inf. Process. **13**(4), 925–933 (2014)
12. Jian, L., Na, L., Li, L.L., Tao, W.: One step quantum key distribution based on epr entanglement. Sci. Rep. **6**, 28767 (2016)
13. Jian, L., Yang, Y.G., Chen, X.B., Zhou, Y.H., Shi, W.M.: Practical quantum private database queries based on passive round-robin differential phase-shift quantum key distribution. Sci. Rep. **6**, 31738 (2016)
14. Jiang, Y., Zhang, S., Yang, F., Chang, Y., Zhang, H.: Quantum secret sharing protocol and its modeling checking. Laser and Optoelectronics Progress **54**(12), 122704 (2017)
15. Li, J., Chen, Y.H., Pan, Z.S., Sun, F.Q., Li, N., Li, L.L.: Security analysis of bb84 protocol in the collective-rotation noise channel. Acta Physica Sinica Chinese Edition **65**(3), 030302 (2016)
16. Li, L., Li, H., Li, C., Chen, X., Chang, Y., Yang, Y., Li, J.: The security analysis of e91 protocol in collective-rotation noise channel. Int. J. Distrib. Sens. Netw. **14**(5), 1550147718778192 (2018)
17. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
18. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050 (1999)
19. Matsumoto, R.: Improved asymptotic key rate of the b92 protocol. In: IEEE international symposium on information theory proceedings, pp. 351–353 (2014)
20. Niu, H.C., Ren, B.C., Wang, T.J., Hua, M., Deng, F.G.: Faithful entanglement sharing for quantum communication against collective noise. Int. J. Theor. Phys. **51**(8), 2346–2352 (2012)
21. Pan, J.W., Bouwmeester, D.: Experimental quantum teleportation. Nature **390**(390), 575 (1997)
22. Quan, Z.: Modification of b92 protocol and the proof of its unconditional security. Acta Phys. Sin. **51**(7), 1446–1447 (2002)
23. Quan, Z., ChaoJing, T., ShenQiang, Z.: Modification of b92 protocol and the proof of its unconditional security. Acta Phys. Sin. **51**(7), 1446–1447 (2002)
24. Stojanovic, A.D., Ramos, R.V., Matavulj, P.S.: Authenticated b92 qkd protocol employing synchronized optical chaotic systems. Opt. Quant. Electron. **48**(5), 1–7 (2016)
25. Su, B.B., Zhou, Y.Y., Zhou, X.J.: B92 protocol analysis related to the same basis eavesdropping. In: IEEE international conference on cloud computing and big data analysis, pp. 189–192 (2016)
26. Valivarthi, R., Puigibert, M.L.G., Zhou, Q., Aguilar, G.H., Verma, V.B., Marsili, F., Shaw, M.D., Nam, S.W., Oblak, D., Tittel, W.: Quantum teleportation across a metropolitan fibre network. Natare Photonics **10**, 676–680 (2016)
27. Wan, L., Huang, Y., Huang, C.: Quantum noise theory for phonon transport through nanostructures. Physica B Condensed Matter **510**, 22–28 (2017)
28. Wang, X.B.: Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys. Rev. A **72**(5), 762–776 (2004)
29. Yang, C.W., Hwang, T.: Improved qsdc protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
30. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Revisiting the security of secure direct communication based on ping-pong protocol[quantum inf. process. 8, 347 (2009)]. Quantum Inf. Process. **10**(3), 317–323 (2011)
31. Zhiyong, Z., Yanbo, W., Min, H., Jian, W.: Intercept-resent eavesdropping in polarization-drift quantum cryptography. Chinese Journal of Quantum Electronics **33**(1), 44–50 (2016)
32. Zhou, X.Y., Zhang, C.H., Zhang, C.M., Wang, Q.: Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources. Phys. Rev. A **96**(5), 052337 (2017)
33. Zou, M., Zhang, G.: Information investigation for b92 protocol in quantum cryptography. Proc Spie **5631**, 181–191 (2005)