The performance of typical QKD scheme under the condition of quantum measurement noise

Zhang Zhaolei1, Ma Zhiqiang2 and Shi Lei2*

1Air Traffic Control and Navigation College, Air Force Engineering University, 710076, China
2Information and Navigation College, Air Force Engineering University, 710076, China
*e-mail: youxiang_wangyi@126.com

Abstract. The performance of typical quantum key distribution protocol under the condition of quantum measurement noise has been explored in this paper. Additionally, the realization steps for quantum key distribution are presented. Based on the successful probability, the performance of quantum key distribution is studied. The results show that the total probability is not influenced by the phase factors, and this probability is relative with the amplitude parameters. The results about quantum key distribution protocol with measurement noise would be useful in the field of quantum communication.

1. Introduction
The quantum communication field has lots of research directions, for example, quantum teleportation, dense coding, and remote state preparation. Quantum key distribution (QKD) [1] is an important part of quantum communication, and is considered as an unconditional security communication scheme [2-5].

The first QKD protocol was proposed by Bennett et al[1]. For its potential applications, lots of research work has been performed, and some QKD protocols have been presented. Zhang et al[6] proposed the decoy-state Reference-frame-independent measurement-device independent QKD protocol with biased bases. For the purpose of removing the detector side channel attacks, Li et al[7] proposed a measurement-device-independent QKD protocol. Yin et al[8] proposed an efficient scheme of decoy state quantum key distribution with modified coherent state. Zhao et al[9] proposed a non-Gaussian post-selection method to emulate the photon sub-ttraction used in coherent-state continuous-variable QKD protocols the decoy-state Reference-frame-independent measurement-device independent QKD protocol with biased bases. Zhang et al[10] proposed a biased decoy-state scheme using heralded single-photon sources for the three-intensity measurement-device independent QKD.

It could be obtained that quantum measurement is necessary for quantum key distribution. Quantum measurement will be influenced by human beings and instruments inevitably. Thus, it is very useful to investigate the performance of quantum key distribution with quantum measurement noise. Based on the steps of quantum key distribution, and from the point of successful probability, the performance of quantum key distribution will be studied in this paper. The research results are useful for other quantum communication protocols.

This paper is structured as follows: In Section II, the original protocol of quantum key distribution would be stated. In Section III, measurement noise would be analyzed. Section IV will present the
processes of quantum key distribution with measurement noise. In Section V, the performance of quantum key distribution will be explored from the successful probability. A brief summary would be performed in Section VI.

2. Typical quantum key distribution protocol
In this section, the original protocol for quantum key distribution (QKD) based on quantum measurement would be stated. For this typical QKD protocol, the realization protocol could be generalized as follow

Step 1: Suppose that the sender Alice want to transmit safety some information to the receiver Bob. Therefore, Alice and Bob need to generate some random keys. First of all, Alice would create a string of binary numbers, and then prepare these numbers based on one of two quantum sets \{q0\} and \{q1\}, which can be expressed as follow

$$+ = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$$

$$- = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$$

The preparation principle of QKD protocol could be presented as follow

$$\begin{align*}
1 & |0\rangle, \\
0 & |1\rangle,
\end{align*}$$

Suppose that a string of binary numbers transmitted form Alice to Bob is ’1011011100’, and the quantum coding basis of Alice are ‘⊕⊗⊕⊕⊗⊗⊗⊗⊗ ⊕’. Thus, the corresponding quantum states can be presented as follow

$$|0\rangle |1\rangle |+\rangle |0\rangle |0\rangle |0\rangle |1\rangle |0\rangle$$

Then, Alice sends these quantum states to using quantum channel.

Step 2: When Bob obtains these quantum states from Alice, he can do the quantum measurement on these states based on \{q0||0\rangle, |1\rangle\} and \{q1||+, |−\rangle\}. Suppose that the measurement basis performed by Bob are ‘⊕⊗⊕⊕⊗⊗⊗⊗⊗ ⊕’. Hence, Bob can get the relative quantum states

$$|0\rangle |1\rangle \frac{1}{\sqrt{2}}|0\rangle \frac{1}{\sqrt{2}}|1\rangle |+\rangle \frac{1}{\sqrt{2}}|0\rangle \frac{1}{\sqrt{2}}|1\rangle |\rangle \frac{1}{\sqrt{2}}|1\rangle$$

Here, ’\frac{1}{\sqrt{2}}|0\rangle \frac{1}{\sqrt{2}}|1\rangle’ means Bob could get ’|0\rangle’ or ’|1\rangle’ with the probability of ’\frac{1}{2}’.

Table 1 The total processes of QKD protocol.

| Random number | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
|---------------|---|---|---|---|---|---|---|---|---|---|
| Alice | | | | | | | | | | |
| Bob | | | | | | | | | | |

2
### Table 1

| Key | 0 | 0 | - | - | 0 | 1 | 0 | 0 |

Step 3: For the purpose of quantum key distribution, Alice and Bob tell each other of the preparation or measurement basis. If and only if the preparation basis is equal to the relative measurement basis, Bob could obtain the binary number from Alice. According to Eqs. (4) and (5), Alice and Bob can determine a string of binary number ‘100100’, and this can be used as the key number. The total processes of this typical quantum key distribution protocol can be presented as Table 1.

### 3. Quantum measurement noise

From Section II, it can be obtained that quantum key distribution (QKD) cannot be performed without quantum measurement. Thus, quantum measurement would be influenced by human beings and instruments inevitably for quantum information processing. The type of measurement noise on quantum key distribution would be discussed in this section.

Based on the protocol statement of Section II, one can get that two kinds of quantum measurement are necessary for quantum key distribution protocol, and they can be expressed as Eq. (1), which are single-qubit projective measurements. In the realization of quantum key distribution, because of quantum noise, the measurements could be performed as follow

\[
\otimes \left\{ \left| 0 \right\rangle \rightarrow \otimes \left| 0 \right\rangle = \cos \frac{\theta_1}{2} \left| 0 \right\rangle + e^{i\phi} \sin \frac{\theta_1}{2} \left| 1 \right\rangle \right.
\]

\[
|\psi\rangle = \cos \frac{\theta_2}{2} |0\rangle + e^{i\phi} \sin \frac{\theta_2}{2} |1\rangle
\]

\[
|\psi\rangle = \cos \frac{\theta_2}{2} |0\rangle + e^{i\phi} \sin \frac{\theta_2}{2} |1\rangle
\]

Here the amplitude factors \( \theta_1 \) and \( \theta_2 \) are in the value region \([0, \pi]\), the phase parameters \( \phi \) and \( \phi' \) are in the value region \([0, 2\pi]\). If and only if \( \theta_1 = \theta_2 = \phi = \phi' = 0 \), the measurement states \( \{|\psi\rangle, |\varphi\rangle\} \) would become to \( \{|0\rangle, |1\rangle\} \) and \( \{|\psi\rangle, |\varphi\rangle\} \), respectively. Based on Eqs. (1) and (6), it could be obtained that

\[
|0\rangle = \cos \frac{\theta_2}{2} |\psi\rangle + e^{i\phi} \sin \frac{\theta_2}{2} |\varphi\rangle
\]

\[
|1\rangle = \cos \frac{\theta_2}{2} |\psi\rangle - e^{i\phi} \sin \frac{\theta_2}{2} |\varphi\rangle
\]

When the quantum measurement basis \( \{|0\rangle, |1\rangle\} \) have the amplitude factor \( \theta_1 \) and phase parameter \( \phi \), i.e., the quantum measurement operators is \( \{|\psi\rangle, |\varphi\rangle\} \), for the preparation states \( \{|0\rangle, |1\rangle\} \), the states after the measurement and the corresponding probabilities could be presented as follow

\[
|\psi\rangle = \cos \frac{\theta_2}{2} |\psi\rangle + e^{i\phi} \sin \frac{\theta_2}{2} |\varphi\rangle
\]

\[
|\varphi\rangle = \cos \frac{\theta_2}{2} |\psi\rangle - e^{i\phi} \sin \frac{\theta_2}{2} |\varphi\rangle
\]

\[
\mathcal{P}_\psi = \cos^2 \frac{\theta_2}{2} \quad \mathcal{P}_\varphi = \sin^2 \frac{\theta_2}{2}
\]
\[ |\psi^{-}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle), \quad |\psi^{+}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
\[ p_{\psi^{-}} = \cos^{2} \theta = \frac{1}{2}, \quad p_{\psi^{+}} = \sin^{2} \theta = \frac{1}{2} \]

Similar to the measurement basis \(|\{0\},|1\rangle\rangle\), if there are the amplitude factor \(\theta\) and phase parameter \(\phi\) for \(|\{+\},|\rangle\rangle\), this basis would become to \(|\{\phi\},|\phi\rangle\rangle\). For \(|\{+\},|\rangle\rangle\), the states after the measurement and the probabilities could be presented as follow

\[ |\phi^{+}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\phi}|1\rangle), \quad |\phi^{-}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - e^{i\phi}|1\rangle) \]
\[ p_{\phi^{+}} = \cos^{2} \frac{\theta}{2}, \quad p_{\phi^{-}} = \sin^{2} \frac{\theta}{2} \]

and

\[ |\phi^{-}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - e^{-i\phi}|1\rangle), \quad |\phi^{+}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{-i\phi}|1\rangle) \]
\[ p_{\phi^{-}} = \cos^{2} \frac{\theta}{2}, \quad p_{\phi^{+}} = \sin^{2} \frac{\theta}{2} \]

4. QKD Scheme with measurement noise

Based on Section III, we can obtain the expression of quantum measurement noise on quantum key distribution. The section would present the quantum key distribution protocol with quantum measurement noise. This protocol has three processes, and can be generalized as follow

Process 1: According to the string of binary numbers transmitted from the sender Alice to the receiver Bob, Alice would code quantum states respect with the coding basis \(|\{0\},|1\rangle\rangle\) and \(|\{\phi\},|\rangle\rangle\), then transmit these states to Bob. The string of binary numbers is set as Eq. (3). This process is same as Step 1 of Section II.

Process 2: For the quantum states, Bob want to measure these states based on the coding basis \(|\{0\},|1\rangle\rangle\) and \(|\{\phi\},|\rangle\rangle\). However, influenced by the measurement noise, the real measurement states performed by Bob would become to \(|\{\psi\},|\rangle\rangle\) and \(|\{\phi\},|\rangle\rangle\), shown as Eq. (5). The realization steps of this quantum key distribution protocol with measurement noise can be presented as Table 2. The parameters \(p_{\psi^{-}}, p_{\psi^{+}}, p_{\phi^{-}}, p_{\phi^{+}}\) are presented as Eqs. (7-10).

| Random number | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
|---------------|---|---|---|---|---|---|---|
| Alice         | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |
|               | 0 | 1 | 1 | 0 | 0 | 1 | 0 |

| Bob           | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |
|               | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |
|               | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |
|               | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |

Table 2: The realization steps of this QKD protocol with measurement noise.
Process 3: For the realization of creating quantum key, the coding basis performed by Alice and the measurement basis by Bob would be compared. If and only if these basis are same, the quantum keys may be generated.

5. The QKD performance

This section would study the performance of quantum key distribution protocol under the condition of quantum measurement noise. It should be emphasized that the successful probability is an important parameter for quantum key distribution. Based on Section IV, we can obtain the states after quantum measurement performed by the receiver Bob and the corresponding probabilities. The measurement results can be presented as Table 3.

Table 3 The after-measurement states and the probabilities.

| Original states | Measurement basis | Probabilities | States after measurement |
|----------------|------------------|---------------|-------------------------|
| | | \( \cos^2 \theta/2 \) | \( |\psi\rangle \) |
| \( |0\rangle \) | \( \{ |\psi\rangle, |\psi_\perp\rangle \} \) | \( \sin^2 \theta/2 \) | \( |\psi_\perp\rangle \) |
| \( |1\rangle \) | \( \{ |\psi\rangle, |\psi_\perp\rangle \} \) | \( \sin^2 \theta/2 \) | \( |\psi\rangle \) |
| \( \{ |\phi\rangle, |\phi_\perp\rangle \} \) | \( \cos^2 \theta/2 \) | \( |\phi\rangle \) |
| \( |+\rangle \) | \( \{ |\phi\rangle, |\phi_\perp\rangle \} \) | \( \sin^2 \theta/2 \) | \( |\phi_\perp\rangle \) |
| \( |-\rangle \) | \( \{ |\phi\rangle, |\phi_\perp\rangle \} \) | \( \cos^2 \theta/2 \) | \( |\phi_\perp\rangle \) |

Suppose that the sender Alice and the receiver Bob want to create \( n \) bits of classical information. There are \( n_1 \) bits of classical information based on the basis \( \{ \oplus |0\rangle, |1\rangle \} \), and \( n_2 \) bits of classical information based on the states \( \{ \oplus |+\rangle, |-\rangle \} \). It should be emphasized that the successful probability for one-bit based on \( \{ \oplus |0\rangle, |1\rangle \} \) can be expressed as follow

\[
p_{[|0\rangle, |1\rangle]} = \cos^2 \frac{\theta}{2}
\] (11)

Similar to the measurement states \( \{ \oplus |+\rangle, |-\rangle \} \), the successful probability for one-bit could be presented as follow

\[
p_{[|\phi\rangle, |\phi_\perp\rangle]} = \cos^2 \frac{\theta}{2}
\] (12)

Therefore, the total successful probability for \( n \)-bit classical information can be obtained as follow

\[
p_{\text{total}} = \left( \cos^2 \frac{\theta_1}{2} \right)^{n_1} \left( \cos^2 \frac{\theta_2}{2} \right)^{n_2}
\] (13)

From Eq. (13), we can find that the total probability is not influenced by the phase noise factors, and this probability is relative with the amplitude noise factors \( \theta_1 \) and \( \theta_2 \). Based on statistical
probability, when the number \( n \) count up to infinity, \( n_1 \) and \( n_2 \) are equal to \( n/2 \). Thus, Eq. (13) can be rewritten as follow

\[
p_{\text{total}} \rightarrow \infty = \left( \cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \right)^r
\]

(14)

If and only if \( \theta_1 = \theta_2 = 0 \), the measurement states \( \{ |\psi\rangle, |\psi_1\rangle \} \) and \( \{ |\phi\rangle, |\phi_1\rangle \} \) would become to \( \{ |0\rangle, |1\rangle \} \) and \( \{ |+\rangle, |–\rangle \} \) expressed as Eq. (1), and the total probability equal to 100%. This result about the successful probability is equal to the original quantum key distribution protocol.

6. Conclusion
Quantum key distribution is one of the most improtant directions for quantum communication. In this paper, we explored the measurement noise influence on quantum key distribution. The mathematical expressions for measurement noise are presented, the performance of quantum key distribution is studied. It should be emphasized that the probability and the classical information are irrelevant with the error of phase parameter. From Eqs. (11-14), it can be obtained that the total successful probability will not be influenced by the phase noise parameters, and this probability is only relative with the amplitude noise factors. Moreover, the total successful probability would equal to one when the errors of amplitude factor are zero. The research results are useful for other quantum communication protocols.

Acknowledgment
This work is supported by the Program for National Natural Science Foundation of China (Grant Nos. 61971436 and 61803382).

References
[1] Bennett, C. H. and Brassard, G.: Quantum Cryptography : Public key distribution and coin tossing. Proc. Of IEEE International Conference on Computers, Systems, and Signal processing 1984:175-179.
[2] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the bb84 quantum key distribution protocol. Physical Review Letters, 85(2), 441-444.
[3] Lo, H. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410):2050-2056.
[4] Gottesman D , Lo H K , Lütkenhaus, Norbert, et al. Security of quantum key distribution with imperfect devices[J]. Quant.inf.comput, 2002.
[5] Portmann C , Renner R . Cryptographic security of quantum key distribution[J]. International Journal of Quantum Information, 2014, 6(1):1-127.
[6] C.M. Zhang, G.C. Guo, M. Li, et al. Measurement-device-independent quantum key distribution with modified coherent state[J]. journal of lightwave technology, 2017, 35(20):4574-4578.
[7] M. Li, C.M. Zhang, Z.Q. Yin, et al. Measurement-device-independent quantum key distribution with modified coherent state.[J]. Optics Letters, 2014, 39(4):880.
[8] Yin Z Q, Han Z F, Sun F W, et al. Decoy state quantum key distribution with modified coherent state[J]. Physical Review A, 2007, 76(1):014304.
[9] Zhao Y , Zhang Y , Li Z , et al. Improvement of two-way continuous-variable quantum key distribution with virtual photon subtraction[J]. Quantum Information Processing, 2017, 16(8):184.
[10] Zhang C H , Zhang C M , Guo G C , et al. Biased three-intensity decoy-state scheme on the measurement-device-independent quantum key distribution using heralded single-photon sources[J]. Optics Express, 2018, 26(4):4219.