Entropy **2015**, *17*, 2919-2931; doi:10.3390/e17052919

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Three-Stage Quantum Cryptography Protocol under Collective-Rotation Noise

Linsen Wu [†] **and Yuhua Chen** [†,*]

Department of Electrical and Computer Engineering, N308 Engr. Bldg. 1, University of Houston, Houston, TX 77204-4005, USA; E-Mail: lwu6@uh.edu (L.W)

[†] These authors contributed equally to this work.

[*] Author to whom correspondence should be addressed; E-Mail: yuhuachen@uh.edu; Tel.: +1-713-743-4441.

Received: 31 March 2015 / Accepted: 4 May 2015 / Published: 7 May 2015

Abstract: Information security is increasingly important as society migrates to the information age. Classical cryptography widely used nowadays is based on computational complexity, which means that it assumes that solving some particular mathematical problems is hard on a classical computer. With the development of supercomputers and, potentially, quantum computers, classical cryptography has more and more potential risks. Quantum cryptography provides a solution which is based on the Heisenberg uncertainty principle and no-cloning theorem. While BB84-based quantum protocols are only secure when a single photon is used in communication, the three-stage quantum protocol is multi-photon tolerant. However, existing analyses assume perfect noiseless channels. In this paper, a multi-photon analysis is performed for the three-stage quantum protocol under the collective-rotation noise model. The analysis provides insights into the impact of the noise level on a three-stage quantum cryptography system.

Keywords: quantum cryptography; three-stage quantum protocol; multi-photon; collective-rotation noise

1. Introduction

The purpose of cryptography is to protect the secret message that is transmitted between the legitimate sender and the receiver from unauthorized reading or modification of the message. The task of cryptographers is to develop secure and reliable cryptographic protocols. Classical cryptography techniques such as symmetric cryptography and asymmetric cryptography are widely used. However, since classical cryptography is based on the complexity of computation, it is facing more and more challenges due to the development of supercomputers and, potentially, quantum computers.

The development of quantum cryptography provides a solution that is based on the Heisenberg Uncertainty Principle and No-Cloning Theorem. In 1984, Bennet and Brassard proposed the first quantum key distribution (QKD) protocol, which is known as the BB84 protocol [1]. In this protocol, two legitimate users can establish a secure channel by using quantum resources to generate an unconditionally secure key. After 1984, several variants [2–4] of BB84 protocols concentrated around QKD were proposed. In 1999, Buzek and Bertaiume proposed a protocol for quantum secret sharing (QSS) [5]. In the same year, a protocol for deterministic secure quantum communication (DSQC) was proposed by Shimizu and Imoto [6]. In a DSQC protocol, one bit of additional classical information transmission is required for each qubit; otherwise the receiver cannot read the correct secret message. Secure direct quantum communication does not require exchange of classical information for encryption or decryption of the message. A protocol that does not require such classical information exchange is named quantum secure direct communication (QSDC) [7,8]. In all QSDC and DSQC protocols, the secret message can be only transmitted one-way “from Alice to Bob”. In the year of 2004, the first quantum dialogue protocol was proposed by Nguyen using Bell states [9], which enables the bidirectional quantum communication that Alice and Bob can transmit and receive their messages simultaneously. This protocol is a modification of the Ping-Pong protocol which started with an initial state [7]. In 2006, Kak proposed the three-stage quantum cryptography protocol [10]. In this protocol, there is no need to have prior generation of keys and it does not need an initial state. Besides, multi-photons can be used to increase the stability and security of the transmission [11]. QSDC has been also extended to continuous-variable systems [12,13].

Most quantum protocols assume a noiseless channel. But in real applications and implementations, noise should be considered as it will have a critical impact on the performance of the transmission. The concept of collective noise on quantum cryptography was explained by Ball and Banaszek [14]. Several collective noise analyses have been performed on previous protocols. Authors of [15] proposed an efficient way for quantum key distribution over collective noise. An economical setup for faithful entanglement sharing against collective noise was presented in [16]. Paper [17] analyzed the security of the “Ping-Pong” protocol in a noisy environment. Two quantum dialogue protocols were proposed in [18], each of which is robust against one of the two kinds of collective noise: Collective-dephasing noise and collective-rotation noise. Furthermore, continuous-variable quantum cryptography with two-way quantum communication has shown to be very robust to the presence of noise [19–21].

In this paper, we analyze the effect of collective-rotation noise in a multi-photon system under the three-stage protocol. This work distinguishes itself from existing work in the following ways: The three-stage protocol is an interesting quantum protocol as it can be used either as QKD, or as QSDC. It maps information onto non-orthogonal polarization states of photons. In the simplest form, all communications in the three-stage protocol are performed using quantum channels. No classical information is exchanged between Alice and Bob. To the best of authors’ knowledge, this paper is the first one to analyze the three-stage protocol in a noisy environment. Lastly, the three-stage protocol is a multi-photon tolerant protocol, which means that the protocol is provably secure when more than single photons are used in communication. This is also the first paper to analyze the impact of noise on a multi-photon system, and should be instrumental to other potential multi-photon tolerant quantum protocols [22].

The remaining part of the article is organized as follows: In Section 2, we briefly describe the three-stage protocol. In Section 3, we introduce the collective-rotation noise model and derive the mathematical model for the three-stage multi-photon protocol and show numerical results. Section 4 concludes the paper.

2. Three-Stage Quantum Cryptography

In the BB84 protocol and its many variants, each qubit is transmitted in one of four different states. In contrast, in the three-stage protocol, the qubit can be in an arbitrary quantum state during the transmission. The qubit remains in its quantum state in each stage. No classical information exchange is needed for the three-stage protocol. In comparison, in previous protocols, the classical information is exchanged after qubit transmission in one direction.

In the three-stage protocol, the qubit state $|X\rangle$ can be in one of the two orthogonal states, such as $|0\rangle$ and $|1\rangle$. Alternative orthogonal states, e.g., $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, can also be used. The orthogonal states of $|X\rangle$ represent 0 and 1 respectively. The orthogonal states, as well as details such as which state represents 1 and 0, are agreed upon prior to the transmission.

Alice and Bob will apply secret rotation operators $R_A(\alpha)$ and $R_B(\beta)$ on the qubit state $|X\rangle$. $R_A(\alpha)$ and $R_B(\beta)$ are commutative, which means $R_A(\alpha)R_B(\beta)|X\rangle = R_B(\beta)R_A(\alpha)|X\rangle$.

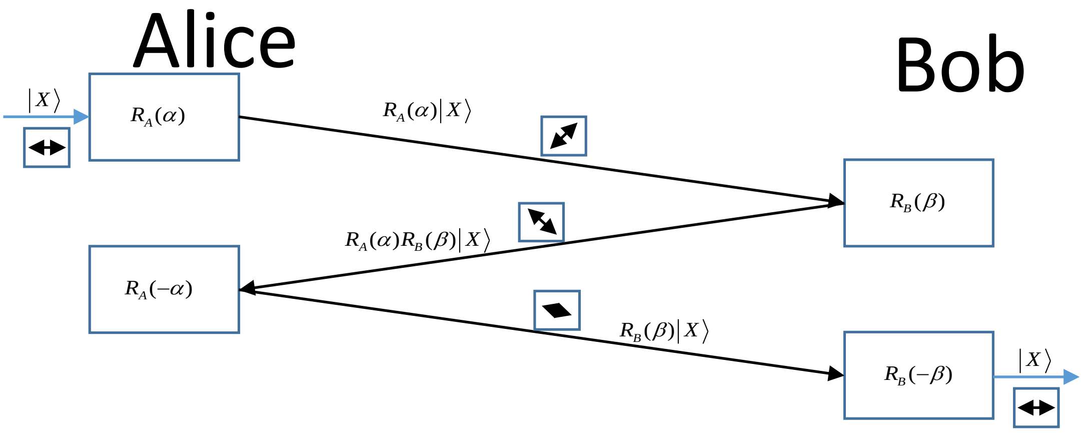

Figure 1. Schematic diagram of the three-stage protocol.

The summarized steps shown in Figure 1 are described as follows:

- Step 1: Alice applies a unitary operator $R_A(\alpha)$ on quantum information $|X\rangle$ and sends the qubit to Bob.
- Step 2: Bob applies another unitary operator $R_A(\beta)$ on the received qubit state $R_A(\alpha)|X\rangle$, thereby giving $R_B(\beta)R_A(\alpha)|X\rangle$ and sends it back to Alice. $R_A(\alpha)$ and $R_B(\beta)$ should be commutative transformations.

- Step 3: Alice applies $R_A(-\alpha)$ (transpose of complex conjugate of $R_A(\alpha)$) on the received qubit state to get $R_A(-\alpha)R_B(\beta)R_A(\alpha)|X\rangle = R_B(\beta)|X\rangle$ and sends it back to Bob.
- Step 4: Then Bob applies $R_B(-\beta)$ on $R_B(\beta)|X\rangle$ to get the information $|X\rangle$.

The angles of polarization rotation that both sides (Alice and Bob) select to apply to the information bits are arbitrary and independent values which vary from 0 to 180 degrees. The eavesdropper cannot obtain correct information without the knowledge of the correct polarization rotation. Moreover, both Alice and Bob do not need to exchange the encryption angle before the transmission. All they need to do is to apply their independent angle to the information (potentially, one unique rotation angle for each bit of information), and reverse the process independently. Then the receiver can recover the original information.

3. Collective-Rotation Noise Analysis

3.1. Collective-Rotation Noise Model

In this section, we analyze the effect of collective-rotation noise [14] on the three-stage protocol. In a real situation, the noise will fluctuate with time and space. In order to analyze conveniently, the environment noise is set as a constant using the maximum value of the noise as a upper bound to analyze the performance of the protocol under the collective-rotation noise model.

Based on the collective-rotation noise model, each photon is deflected to either counterclockwise or clockwise by an angle of θ, with a probability of 1/2 respectively. For a random qubit state $|x\rangle$, clockwise deflection is denoted as $|x-\theta\rangle$ and counterclockwise deflection is denoted as $|x+\theta\rangle$. The state $|1\rangle$, $|x\rangle$, $|0\rangle$ and their corresponding deflection states are shown in Figure 2.

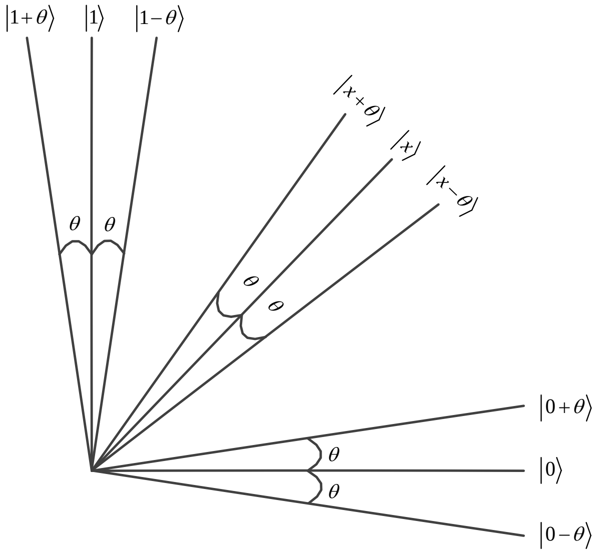

Figure 2. Collective-rotation model on qubit states $|1\rangle$, $|x\rangle$ and $|0\rangle$.

Parameter θ denotes the noise in the collective-rotation channel. In the following analysis, θ is considered as a constant for all three stages. However, the impact of different values of θ is analyzed.

Based on the value of information bit X , the initial qubit Alice prepares can be in one of the two states: $\left|0\right\rangle$ and $\left|1\right\rangle$. Without considering the rotation operator, let us first consider the case where $\left|0\right\rangle$ is sent. Because of the collective-rotation channel noise, the qubit $\left|0\right\rangle$ has a probability of 1/2 to become $\left|0+\theta\right\rangle$ and a probability of 1/2 to become $\left|0-\theta\right\rangle$, which can be written as

$$|0\rangle \to \begin{cases} |0+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle \\ |0-\theta\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle \end{cases} \tag{1}$$

The probability that qubit $\left|0\right\rangle$ is recognized as 0 is $1/2\cos^2\theta + 1/2\cos^2\theta = \cos^2\theta$ and the probability that qubit $\left|0\right\rangle$ is recognized as 1 is $1/2\sin^2\theta + 1/2(-\sin)^2\theta = \sin^2\theta$. The error rate is given by $\sin^2\theta$.

Let us consider the case where $\left|1\right\rangle$ is sent. Similarly, qubit $\left|1\right\rangle$ has a probability of 1/2 to become $\left|1+\theta\right\rangle$ and a probability of 1/2 to become $\left|1-\theta\right\rangle$, which can be written as

$$|1\rangle \to \begin{cases} |1+\theta\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle \\ |1-\theta\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle \end{cases} \tag{2}$$

So the probability that qubit $\left|1\right\rangle$ is recognized as 1 is $1/2\cos^2\theta + 1/2\cos^2\theta = \cos^2\theta$ and the probability that qubit $\left|1\right\rangle$ is recognized as 0 is $1/2(-\sin)^2\theta + 1/2\sin^2\theta = \sin^2\theta$. The error rate is therefore given by $\sin^2\theta$.

For each qubit sent in a noisy quantum channel, the qubit error rate σ_0 is

$$\sigma_0 = \frac{1}{2}\sin^2\theta + \frac{1}{2}\sin^2\theta = \sin^2\theta \tag{3}$$

3.2. A Single-Photon Analysis

In the three-stage protocol, a single photon is transmitted through the quantum channel three times between Alice and Bob, each of which is subject to collective-rotation noise. In this section, we analyze the state of the photon in each of the stages, and derive the error rate due to collective-rotation noise.

Based on the protocol described in Section 2, a rotation operator is applied to the qubit in each round to map the qubit to a non-orthogonal state. Therefore, the collective-rotation noise changes the non-orthogonal quantum state by either θ or $-\theta$, respectively. Since Alice and Bob will reverse their rotation operations eventually, the actual value of the rotation operator does not affect the results of the analysis. In order to make the derivation concise, the rotation operators are not shown in the derivation.

After the first stage, the deflection angle can be either θ or $-\theta$ with probability 1/2, as shown in Table 1.

Table 1. Probabilities of each angle after first round of transmission.

Deflection Angle	θ	$-\theta$
Probability	1/2	1/2

The states of the qubit can be written as

$$|0\rangle \to \begin{cases} |0+\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |0-\theta\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle \end{cases},\quad |1\rangle \to \begin{cases} |1+\theta\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \\ |1-\theta\rangle = \sin\theta\,|0\rangle + \cos\theta\,|1\rangle \end{cases}. \tag{4}$$

Because there are two possible deflection angles at the end of the first stage of transmission, there are three possible angles after the second stage, namely, 2θ, 0 and -2θ. The probabilities of the angles are shown in Table 2.

Table 2. Probabilities of each angle after second round of transmission.

Deflection Angle	2θ	0	-2θ
Probability	1/4	1/2	1/4

The possible qubit states can be written as

$$|0\rangle \to \begin{cases} |0+2\theta\rangle = \cos 2\theta\,|0\rangle + \sin 2\theta\,|1\rangle \\ |0+0\rangle = |0\rangle \\ |0-2\theta\rangle = \cos 2\theta\,|0\rangle - \sin 2\theta\,|1\rangle \end{cases},\quad |1\rangle \to \begin{cases} |1+2\theta\rangle = -\sin 2\theta\,|0\rangle + \cos 2\theta\,|1\rangle \\ |1+0\rangle = |1\rangle \\ |1-2\theta\rangle = \sin 2\theta\,|0\rangle + \cos 2\theta\,|1\rangle \end{cases}. \tag{5}$$

After the third stage, there are four possible angles: 3θ, θ, $-\theta$ and -3θ. The probabilities of the angles are show in Table 3.

Table 3. Probabilities of each angle after third round of transmission.

Deflection Angle	3θ	θ	$-\theta$	-3θ
Probability	1/8	3/8	3/8	1/8

The possible qubit states can be written as

$$|0\rangle \to \begin{cases} |0+3\theta\rangle = \cos 3\theta\,|0\rangle + \sin 3\theta\,|1\rangle \\ |0+\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |0-\theta\rangle = \cos\theta\,|0\rangle - \sin\theta\,|1\rangle \\ |0-3\theta\rangle = \cos 3\theta\,|0\rangle - \sin 3\theta\,|1\rangle \end{cases},\quad |1\rangle \to \begin{cases} |1+3\theta\rangle = -\sin 3\theta\,|0\rangle + \cos 3\theta\,|1\rangle \\ |1+\theta\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \\ |1-\theta\rangle = \sin\theta\,|0\rangle + \cos\theta\,|1\rangle \\ |1-3\theta\rangle = \sin 3\theta\,|0\rangle + \cos 3\theta\,|1\rangle \end{cases}. \tag{6}$$

Because each case in (6) occurs with probability $1/8$, we can derive the mean error probability as

$$\varepsilon_0 = \frac{1}{8}\sin^2 3\theta + \frac{3}{8}\sin^2\theta + \frac{3}{8}\sin^2(-\theta) + \frac{1}{8}\sin^2(-3\theta) = \frac{1}{4}\sin^2\theta + \frac{3}{4}\sin^2 3\theta \tag{7}$$

3.3. Multi-Photon Analysis

Since the three-stage protocol is multi-photon tolerant [11], multiple photons can be transmitted simultaneously to indicate one bit of information to improve the success rate of the transmission.

We assume each photon is independent from each other and all photons transmitted at the same time are affected by the same collective-rotation noise. As discussed in Section 3.2, the probability that a single photon is recognized as incorrect information is ε_0, which is the mean error rate for a single photon transmitted in the noisy channel, as shown in Equation (7). The probability that a single photon is recognized correctly is

$$\overline{\varepsilon_0} = 1 - \varepsilon_0 \tag{8}$$

We also assume that the channel is lossless. Therefore, all photons sent by Alice reach the photon detector on Bob's side. Bob will register a correct bit if a majority number of photons reach the correct photon detector. In the case of a tie, we assume that there is 50% of chance to register a correct bit. Let the total number of photons used in transmitting one bit be N, where $N = 2k+1, k \geq 0$ or $N = 2k+2, k \geq 0$. Note that we purposely use the notation $2k+2$ to indicate that an even number of photons are used in the communication, instead of the standard notation of $2k$. This allows us to establish a relationship between the even and odd numbers of photons under the same value of k. First, we derive the error rate under the odd number and the even number of photons, respectively.

Case 1: $N = 2k+1, k \geq 0$.

In this situation, odd number photons are sent simultaneously. If more than k photons reach the correct photon detector, Bob will receive the correct bit (either 0 or 1) sent by Alice.

Let i be the number of photons that reach the correct photon detector. The probability of this event is

$$\rho_i^{\text{odd}} = C_{2k+1}^{i} (\varepsilon_0)^i (\overline{\varepsilon_0})^{2k+1-i} \tag{9}$$

So the overall error rate ε^{odd} is

$$\varepsilon^{\text{odd}} = \sum_{i=k+1}^{i=2k+1} \rho_i^{\text{odd}} = \sum_{i=k+1}^{i=2k+1} C_{2k+1}^{i} (\varepsilon_0)^i (1-\varepsilon_0)^{2k+1-i} \tag{10}$$

Using the results from Equation (7), the overall error rate ε_{odd} can be re-written as

$$\varepsilon^{\text{odd}} = \sum_{i=k+1}^{i=2k+1} C_{2k+1}^{i} (\frac{1}{4}\sin^2\theta + \frac{3}{4}\sin^2 3\theta)^i (1 - \frac{1}{4}\sin^2\theta - \frac{3}{4}\sin^2 3\theta)^{2k+1-i} \tag{11}$$

Case 2: $N = 2k+2, k \geq 0$.

In this situation, even number photons are sent simultaneously. If more than $k+1$ photons reach the correct photon detector, the receiver will receive the correct bit. In the case of a tie, where $k+1$ photons reach the correct detector and $k+1$ photons reach the wrong detector, we assume that the system will randomly choose between 1 or 0 with probability 1/2.

Suppose the number of photons that reach the correct photon detector is *i*. The probability of this event is

$$\rho_i^{\text{even}} = C_{2k+2}^{i} (\varepsilon_0)^i (\overline{\varepsilon_0})^{2k-i} \tag{12}$$

The overall error rate $\varepsilon^{\text{even}}$ is

$$\varepsilon^{\text{even}} = \frac{1}{2}\rho_{k+1} + \sum_{i=k+2}^{i=2k+2} \rho_i^{\text{even}} = \frac{1}{2} C_{2k+2}^{k+1} (\varepsilon_0)^{k+1} (1-\varepsilon_0)^{k+1} + \sum_{i=k+2}^{i=2k+2} C_{2k+2}^{i} (\varepsilon_0)^i (1-\varepsilon_0)^{2k+2-i} \tag{13}$$

It can be re-written as

$$\begin{aligned} \varepsilon^{\text{even}} = {} & \frac{1}{2} C_{2k+2}^{k+1} (\frac{1}{4}\sin^2\theta + \frac{3}{4}\sin^2 3\theta)^{k+1} (1 - \frac{1}{4}\sin^2\theta - \frac{3}{4}\sin^2 3\theta)^{k+1} \\ & + \sum_{i=k+2}^{i=2k+2} C_{2k+2}^{i} (\frac{1}{4}\sin^2\theta + \frac{3}{4}\sin^2 3\theta)^i (1 - \frac{1}{4}\sin^2\theta - \frac{3}{4}\sin^2 3\theta)^{2k+2-i}. \end{aligned} \tag{14}$$

Mathematically, Equation (10) is equivalent to Equation (13) when they have the same value of k, which means that sending $2k+1$ photons has the same mean error rate as sending $2k+2$ photons. It is counter-intuitive. We briefly show the mathematical proof and explain the physical meaning.

Suppose the mean error rate of sending an odd number of $2k+1$ photons is ε_{2k+1}. Suppose we add one more photon to make it even. We are interested in determining if having one more photon joining the transmission will affect the error rate. Denote the mean error rate of sending $2k+2$ photons ε_{2k+2}.

To understand the effect of the added photon, we first exam the possible outcomes from the previous $2k+1$ photons. Denote the number of photons reaching the correct photon detector N^{c}, and denote the number of photons reaching the wrong photon detector N^{w}. Based on our assumption, the information bit is correctly detected if $N^{\mathrm{c}} > N^{\mathrm{w}}$; or if $N^{\mathrm{c}} = N^{\mathrm{w}}$, there is 50% chance the information is correctly detected. We discuss the following possibilities.

(1) More than $k+1$ photons out of the $2k+1$ photons hit the correct photon detector ($N^{\mathrm{c}} \geq k+2$). In this case, it does not matter whether the added photon hits the correct or the wrong detector. In either cases, $N^{\mathrm{w}} \leq k$. Therefore, $N^{\mathrm{c}} > N^{\mathrm{w}}$. The information bit is detected correctly.

(2) More than $k+1$ photons out of the $2k+1$ photons hit the wrong photon detector ($N^{\mathrm{w}} \geq k+2$). In this case, it again does not matter whether the added photon hits the correct or the wrong detector. In this case, the total number of photons reaching the correct detector $N^{\mathrm{c}} \leq k$. Therefore, $N^{\mathrm{w}} > N^{\mathrm{c}}$. The information bit is detected incorrectly.

(3) Out of $2k+1$ photons, $k+1$photons reach the correct detector and k photons reach the wrong detector. In this case, there are two possibilities. If the added photon reaches the correct detector, this will make $N^{\mathrm{c}} = k+2$, and $N^{\mathrm{w}} = k$. Therefore, $N^{\mathrm{c}} > N^{\mathrm{w}}$ and the information bit is detected correctly. On the other hand, if the added photon reaches the wrong detector, we have $N^{\mathrm{c}} = N^{\mathrm{w}} = k+1$. Based on the assumption, the probability to detect a correct information bit is $1/2$.

(4) Out of $2k+1$ photons, k photons reach the correct detector and $k+1$ photons reach the wrong detector. In this case, there are also two possibilities. If the added photon reaches the wrong detector, this will make $N^{\mathrm{w}} = k+2$, and $N^{\mathrm{c}} = k$. Therefore, $N^{\mathrm{W}} > N^{\mathrm{C}}$ and the information bit is detected incorrectly. If the added photon reaches the correct detector, this will make $N^{\mathrm{c}} = k+1$, and $N^{\mathrm{w}} = k+1$. Therefore, $N^{\mathrm{c}} = N^{\mathrm{w}}$ and the probability of detecting a correct information bit is $1/2$.

The mean error rate ε_{2k+2} can be written as

$$\begin{aligned}\varepsilon_{2k+2} &= (\frac{1}{2}\rho_k^{\mathrm{odd}} + \rho_{k+1}^{\mathrm{odd}} \ldots + \rho_{2k+1}^{\mathrm{odd}})\varepsilon_0 + (\frac{1}{2}\rho_{k+1}^{\mathrm{odd}} + \ldots \rho_{2k+1}^{\mathrm{odd}})\overline{\varepsilon_0} \\ &= \frac{1}{2}\rho_k^{\mathrm{odd}}\varepsilon_0 + \rho_{k+1}^{\mathrm{odd}}\varepsilon_0 + \frac{1}{2}\rho_{k+1}^{\mathrm{odd}}\overline{\varepsilon_0} + \rho_{k+2}^{\mathrm{odd}} + \ldots + \rho_{2k+1}^{\mathrm{odd}}.\end{aligned} \tag{15}$$

From Equation (9), it is clear that

$$\rho_k^{\mathrm{odd}} = \frac{\overline{\varepsilon_0}}{\varepsilon_0}\rho_{k+1}^{\mathrm{odd}} \tag{16}$$

Therefore,

$$\begin{aligned}&\frac{1}{2}\rho_{k}^{\text{odd}}\varepsilon_0+\rho_{k+1}^{\text{odd}}\varepsilon_0+\frac{1}{2}\rho_{k+1}^{\text{odd}}\overline{\varepsilon_0}\\&=\frac{1}{2}\frac{\overline{\varepsilon_0}}{\varepsilon_0}\rho_{k+1}^{\text{odd}}\varepsilon_0+\rho_{k+1}^{\text{odd}}\varepsilon_0+\frac{1}{2}\rho_{k+1}^{\text{odd}}\overline{\varepsilon_0}\\&=\frac{1}{2}\rho_{k+1}^{\text{odd}}\overline{\varepsilon_0}+\rho_{k+1}^{\text{odd}}\varepsilon_0+\frac{1}{2}\rho_{k+1}^{\text{odd}}\overline{\varepsilon_0}\\&=\rho_{k+1}^{\text{odd}}.\end{aligned}\tag{17}$$

So ε_{2k+2} will be written as

$$\varepsilon_{2k+2}=\rho_{(k+1)odd}+\rho_{(k+2)odd}+\ldots+\rho_{(2k+1)odd}=\sum_{i=k+1}^{i=2k+1}\rho_i=\varepsilon_{2k+1}\tag{18}$$

We have proved that the error rate of using $2k+1$ photons is the same as that of using $2k+2$ photons under the same value of k. The physical meaning can be found in the possible scenarios above. Essentially, the $(2k+2)-th$ photon either makes no contribution to the final outcome, or contributes to a tie situation. Therefore, it has no overall impact on the mean error rate. This only applies to the pair of photon numbers that share the same value of k. As k increases, the mean error rate will drop, which is demonstrated in Section 3.4.

In this section, the error rate of multi-photon transmission in three-stage protocol is analyzed under the collective-rotation noise model. The relationship between the error rate and the deflection angle is established. Numerical results will be shown in the following section.

3.4. Numerical Results

In this section, we present the numerical results of the three-stage protocol under the collective-rotation noise model. The error rate of a single photon and the error rate of multiple photons are plotted in Figure 3. We only plot the results for odd number photons as we have proved that the corresponding even number of photons with the same value of k produce the same error rate. From the figure we can see that the mean error rate increases as the deflection angle increases. In a multi-photon system, when the photons are influenced under the same deflection angle, increasing the number of photons used in transmission will decrease the mean error rate.

The achievable bit error rate is important to a quantum cryptography system. From Figure 3, we can see that if the target bit error rate is 0.1, it is not achievable under $\theta=15°$ collective-rotation noise, even with 15 photons. If the target bit error rate is 0.2, under $\theta=15°$ collective-rotation noise, it is achievable with 15 photons. If a single photon is used, the error rate will get close to 0.4 when the deflection angle is 15°. Increasing from 1 photon to 3 photons, the system can much better cope with collective-rotation noise. Likewise, under $\theta=10°$ collective-rotation noise, the error rate decreases from 0.2 to 0.1.

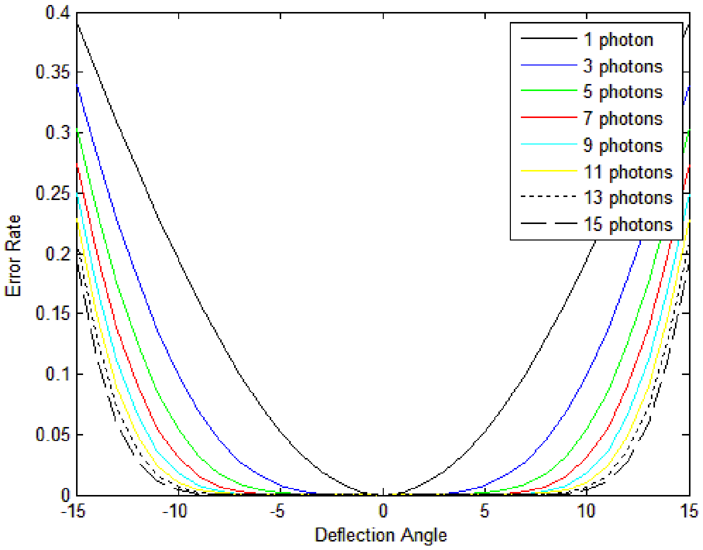

Figure 3. Error rate *versus* deflection angle in multi-photon system with odd numbers.

The error rate *versus* the numbers of photons with different deflection angles is plotted in Figures 4–6. By increasing the number of photons, the error rate decreases rapidly and gets close to 0 at some point. Under collective-rotation noise $\theta = 5°$, the bit error rate gets close to 0 at 7 photons. Under $\theta = 10°$, the bit error rate is close to 0 at 15 photons. When collective-rotation noise $\theta = 15°$, it might be too noisy for the quantum cryptography system. Even with 15 photons, it has an error rate close to 0.2.

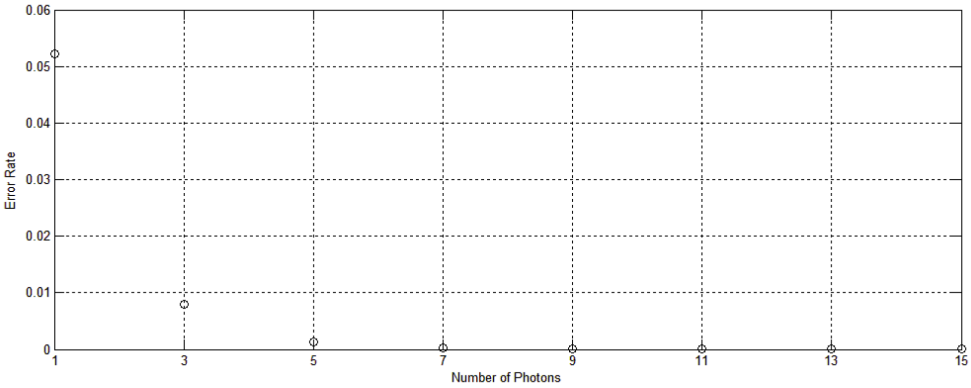

Figure 4. Error rate *versus* number of photons when deflection angle is 5°.

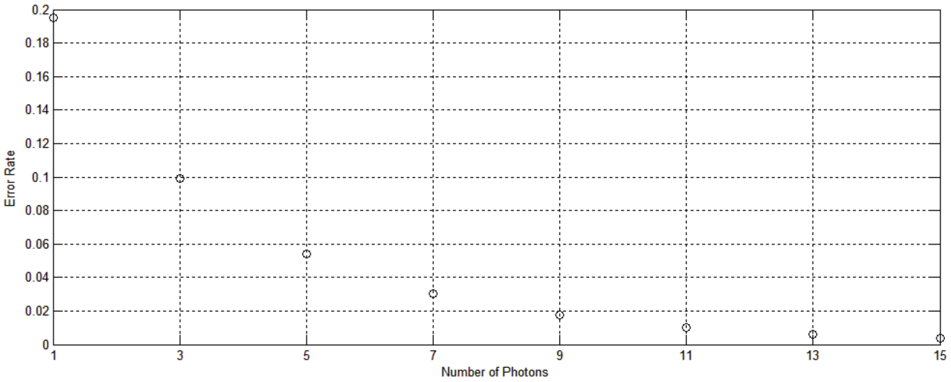

Figure 5. Error rate *versus* number of photons when deflection angle is 10°.

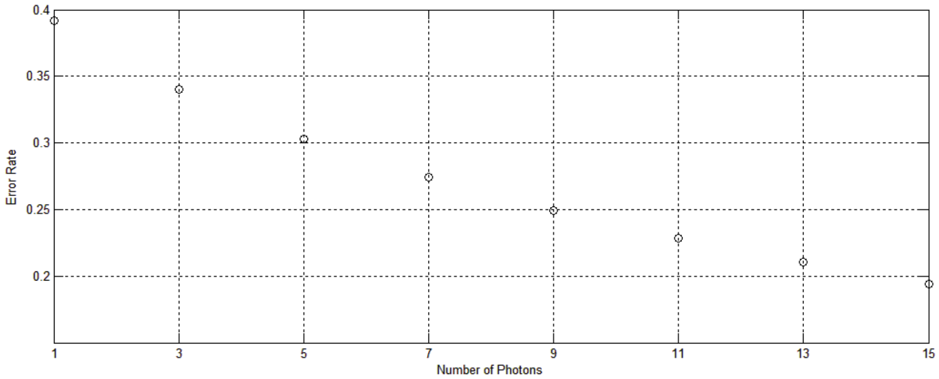

Figure 6. Error rate *versus* number of photons when deflection angle is 15°.

By coupling collective noise information with the number of photons used in transmission, the system can be tuned to an operating point where Eve's siphoning of photons can be detected by the change of the bit error rate from the expected values. For example, under collective-rotation noise $\theta = 10°$, if seven photons are used to transmit the information, the expected bit error rate is 0.03. If three to four photons get lost (Eve needs to steal at least three photons to obtain information), the bit error rate will increase dramatically to 0.1, which is a significant change for the system. This will allow Alice and Bob to abort the transmission. At this operating point, the system is very sensitive to the loss of photons, therefore, can be used to detect Eve's disturbance of the system.

4. Conclusions

In this paper, a multi-photon analysis is performed for the three-stage quantum protocol under the collective-rotation noise model. The analysis provides insights into the impact of the noise level on a three-stage quantum cryptography system. We show that a multi-photon system provides better error rate tolerance during the transmission in a noisy environment. The analysis on the mean error rate can provide better support on hardware equipment design. Also, the system can detect Eve's siphoning by the change of the bit error rate, which increases the robustness of the system. The results are also applicable to other multi-photon tolerant quantum cryptography protocols.

Acknowledgments

This research is partially supported by the National Science Foundation (NSF) under Grant 1117148.

Author Contributions

The authors contributed equally to this work. Both authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Bennett, H.C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Ekert, K.A. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663.
3. Bennett, H.C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *75*, 3121–3124.
4. Goldenberg, L.; Vaidman, L. Quantum Cryptography Based on Orthogonal States. *Phys. Rev. Lett.* **1995**, *67*, 1239–1243.
5. Hillery, M.; Bužek, V.; Bertaiume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, doi:10.1103/PhysRevA.59.1829.
6. Shimizu, K.; Imoto, N. Communication channels secured from eavesdropping via transmission of photonic Bell states. *Phys. Rev. A* **1999**, *60*, doi:10.1103/PhysRevA.60.157.
7. Bostrom, K.; Felbinger, T. Deterministic Secure Direct Communication Using Entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902.
8. Lucamarini, M.; Mancini, S. Secure Deterministic Communication without Entanglement. *Phys. Rev. Lett.* **2005**, *94*, 140501.
9. Nguyen, A.B. Quantum dialogue. *Phys. Lett. A* **2004**, *328*, 6–10.
10. Kak, S. A Three-Stage Quantum Cryptography Protocol. *Found. Phys. Lett.* **2006**, *19*, 293–296.
11. Mandal, S.; Macdonald, G.; El Rifai, M.; Punekar, N.; Zamani, F.; Chen, Y.; Kak, S.; Verma, P.K.; Huck, R.C.; Sluss, J. Multi-Photon Implementation of Three-Stage Quantum Cryptography Protocol. In Proceedings of Information Networking (ICOIN), Bangkok, Thailand, 28–30 January 2013; pp. 6–11.
12. Pirandola, S.; Braunstein, S.L.; Mancini, S.; Lloyd, S. Quantum direct communication with continuous variables. *Eur. Lett.* **2008**, *84*, 20013.
13. Pirandola, S.; Braunstein, S.L.; Lloyd, S.; Mancini, S. Confidential direct communications: A quantum approach using continuous variables. *IEEE J. Sel. Top. Quantum Electron.* **2009**, *15*, 1570–1580.
14. Ball, L.J.; Banaszek, K. Potential for Quantum Cryptography over Collective Noise Channels. In Proceedings of AIP Conference Proceedings, Glasgow, UK, 25–29 July 2004; pp. 295–298.
15. Li, X.; Deng, F.; Zhou, H. Efficient quantum key distribution over a collective noise channel. *Phys. Rev. A* **2008**, *78*, 022321.
16. Niu, H.; Ren, B.; Wang, T.; Hua, M.; Deng, F. Faithful Entanglement Sharing for Quantum Communication against Collective Noise. *Int. J. Theor. Phys.* **2012**, *51*, 2346–2352.
17. Li, J.; Li, L.; Jin, H.; Li, R. Security analysis of the "Ping–Pong" quantum communication protocol in the presence of collective-rotation noise. *Phys. Lett. A* **2013**, *377*, 2729–2734.
18. Yang, C.; Hwang, T. Quantum dialogue protocols immune to collective noise. *Quantum Inf. Process.* **2013**, *12*, 2131–2142.
19. Pirandola, S.; Braunstein, S.L.; Lloyd, S.; Mancini, S. Continuous Variable Quantum Cryptography using Two-Way Quantum Communication. *Nat. Phys.* **2008**, *4*, 726–730.

20. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Security of two-way quantum cryptography against asymmetric Gaussian attacks. In Proceeding of the SPIE Conference "Quantum Communications and Quantum Imaging VI", San Diego, CA, USA, 5 May 2008; Volume 7092.
21. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309.
22. Nikolopoulos, M.G. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A* **2008**, *77*, 032348.