photonics

MDPI

Communication

Security of Bennett–Brassard 1984 Quantum-Key Distribution Under a Collective-Rotation Noise Channel

Mhlambululi Mafu [1,*], Comfort Sekga [2] and Makhamisa Senekane [3,4]

[1] Department of Physics, Case Western Reserve University, Cleveland, OH 44106, USA
[2] Department of Physics and Astronomy, Botswana International University of Science and Technology, Palapye P/ Bag 16, Botswana
[3] Institute for Intelligent Systems, University of Johannesburg, Johannesburg 2006, South Africa
[4] National Institute for Theoretical and Computational Sciences, Gauteng 2006, South Africa
* Correspondence: mhlambululi.mafu@case.edu

Abstract: The security analysis of the Ekert 1991 (E91), Bennett 1992 (B92), six-state protocol, Scarani–Acín–Ribordy–Gisin 2004 (SARG04) quantum key distribution (QKD) protocols, and their variants have been studied in the presence of collective-rotation noise channels. However, besides the Bennett–Brassard 1984 (BB84) being the first proposed, extensively studied, and essential protocol, its security proof under collective-rotation noise is still missing. Thus, we aim to close this gap in the literature. Consequently, we investigate how collective-rotation noise channels affect the security of the BB84 protocol. Mainly, we study scenarios where the eavesdropper, Eve, conducts an intercept-resend attack on the transmitted photons sent via a quantum communication channel shared by Alice and Bob. Notably, we distinguish the impact of collective-rotation noise and that of the eavesdropper. To achieve this, we provide rigorous, yet straightforward numerical calculations. First, we derive a model for the collective-rotation noise for the BB84 protocol and parametrize the mutual information shared between Alice and Eve. This is followed by deriving the quantum bit error rate (QBER) for two intercept-resend attack scenarios. In particular, we demonstrate that, for small rotation angles, one can extract a secure secret key under a collective-rotation noise channel when there is no eavesdropping. We observe that noise induced by rotation of 0.35 radians of the prepared quantum state results in a QBER of 11%, which corresponds to the lower bound on the tolerable error rate for the BB84 QKD protocol against general attacks. Moreover, a rotational angle of 0.53 radians yields a 25% QBER, which corresponds to the error rate bound due to the intercept-resend attack. Finally, we conclude that the BB84 protocol is robust against intercept-resend attacks on collective-rotation noise channels when the rotation angle is varied arbitrarily within particular bounds.

Keywords: BB84 protocol; security; collective-rotation noise; quantum-key distribution

Citation: Mafu, M.; Sekga, C.; Senekane, M. Security of Bennett–Brassard 1984 Quantum-Key Distribution Under a Collective-Rotation Noise Channel. *Photonics* **2022**, *9*, 941. https://doi.org/10.3390/photonics9120941

Received: 4 October 2022
Accepted: 1 December 2022
Published: 6 December 2022

1. Introduction

The quantum-key distribution (QKD) has become a mature field of quantum cryptography, which exploits the quantum mechanical principles to generate secret keys for secure communication between legitimate parties, Alice and Bob [1,2]. Since its inception, there has been remarkable progress and development, and it has turned fundamental physics into real-life applications for academia and industry [3]. In QKD implementations, photons have emerged as the trusted carriers of quantum information due to their high transmission speed and resilience against environmental decoherence. However, the field still faces some challenges due to channel imperfections and the effect of noise in the transmission channel [4–6]. Optical fibers have been used as a mode of transmission of these photons in most QKD commercial applications [7]. Unfortunately, optical fibers undergo some slow fluctuations in the birefringence, and this can be modeled as a collective-noise [8,9]. As a result, avoiding noise in the communication process is challenging. The primary types of collective-noises are collective-rotation and collective-dephasing noise [10].

Depending on the detection method required to recover information about the key encoded in the properties of light, QKD protocols fall into three classes [11]. For instance, the BB84, E91, BBM92, B92 [2], six-state [12,13], SARG04 [14], and decoy-state protocols [6,15] belong to a class of the so-called discrete-variable (DV) protocols, where one encodes information in the polarization pulses. This simulates actual single-photon states and requires single-photon detectors for their implementation. However, another class of continuous-variable (CV) protocols was proposed due to challenges in realizing actual single-photon sources and detectors [16]. In CV protocols, information is encoded in the quadratures of the quantized electromagnetic field, for example those of coherent or squeezed states [17,18]. Finally, due to other practical requirements, the class of distributed-phase-reference (DPR) protocols in which the coherence of sequential pulses plays an essential role in security was proposed [2]. The DPR class encodes information in the photon's arrival times or the phase between adjacent weak coherent pulses. Members of this family are the differential-phase-shift (DPS) protocol [19] and the coherent-one-way (COW) protocol [20,21]. These protocols are tolerant to photon number splitting (PNS) attacks. Concerning detection, the DV and DPR protocols use the single-photon detection technique, while the CV protocols utilize the homodyne or heterodyne detection technique [22,23].

On the other hand, device-independent (DI) QKD protocols have been proposed to address challenges relating to detector side-channel attacks, where the security is based on the violation of a parity–CHSH inequality [24–26]. However, the DI QKD schemes require loophole-free parity-CHSH experiments, which is not attainable with current technology [27]. Therefore, a more practical solution is measurement device-independent (MDI) QKD, which is inherently resistant to all side-channel attacks targeting the measurement device and removes all detection-related security loopholes [28,29]. Once more, despite these advances, it has been challenging to adopt QKD widely, and large-scale deployment will likely require chip-based devices for improved performance, miniaturization, and enhanced functionality [30–34]. Moreover, these integrated photonic chips offer numerous benefits such as low cost, low power consumption, and well-established batch fabrication techniques [35].

Various authors have recently studied the impact of collective-rotation noise on QKD protocols. For instance, Tamaki and Lütkenhaus (2004) presented the unconditional security proof for the B92 QKD protocol when implemented over a lossy and noisy channel [36]. Wang (2005) proposed a straightforward prepare-and-measure protocol for robust QKD implemented with photon polarization. The protocol demonstrated fault-tolerance against the collective random unitary channel noise [37]. Notably, there are numerous discussions about the impact of quantum noise on the achievable finite-key rates for the BB84 QKD protocol and the six-state QKD protocol [11,38]. Leveraging the polarization-based QKD protocol and a collective-noise channel, Zhang (2006) developed robust multiparty quantum secret sharing (QSS) using two collective-noise channels [39]. Furthermore, Li et al. [40] presented two efficient QKD schemes implemented using two collective-noise channels. Dong (2009) developed a deterministic secure quantum communication against collective-dephasing noise, which uses EPR pairs and auxiliary photons [41]; on the other hand, Xiu et al. presented a QKD protocol implemented using six photon states against collective-noise [42]. In 2010, Deng and Sheng demonstrated a scheme that operates deterministically and achieves an efficient quantum entanglement distribution over an arbitrary collective-noise channel [43]. Remarkably, the collective-noise leads to an additional advantage [44,45].

Furthermore, in 2011, Gu et al. [46] presented two robust quantum-secure direct communication schemes consisting of a quantum one-time pad over a collective-noise channel. Then, remarkably, Yang et al. [47] developed a fault-tolerant two-step quantum-secure direct communication protocol against collective-noises. After that, Wei et al. [48] presented two novel quantum-secure direct communication protocols using different collective-noise channels. Later, Yang and Hwang (2013) developed two quantum dialogue protocols, each robust against either the collective-dephasing noise or collective-rotation noise [10].

Moreover, Yu (2015) developed two fault-tolerant channel-encrypting quantum dialogue protocols resistant to collective-noise [49]. Additionally, using the Bell states, Yu (2015) proposed a scheme for quantum-secure direct dialogue protocols, adapted to both collective-dephasing noise and collective-rotation noise [50]. Furthermore, Jian et al. [51] presented the security proof of the SARG04 protocol under collective-rotation noise and established that the protocol was secure against a certain level of such noise. Then, Wu and Chen (2015) analyzed a multi-photon analysis for the three-stage quantum protocol under the collective-rotation noise model and demonstrated that a multi-photon system provides better error rate tolerance during transmission in a noisy environment [52]. Furthermore, Garapo et al. [53] investigated the influence of the intercept-resend attack on the six-state QKD over collective-rotation noise channels and found that the protocol was secure when the angle of rotation was restricted within certain bounds. This was followed by security analysis for the E91 protocol in the presence of a collective-rotation noise channel [54]. In 2019, Jian et al. [54] presented the B92 QKD security analysis under a collective-rotation noise channel based on the Markov process. Furthermore, Yang et al. [55] presented four three-party quantum secret sharing protocols resistant to both collective-dephasing noise and collective-rotation noise. He and Ma (2019) developed three multiparty protocols for direct communication using the collective-dephasing noise channels and the collective-rotation noise channels [56]. Furthermore, Chang et al. [57] presented a fault-tolerant controlled quantum dialogue against collective-noise. Notably, they demonstrated that, besides their protocols being free from information leakage, they were resistant to several attacks. This was followed by Zhao et al. [58], who developed a quantum private query protocol using a collective-dephasing noise channel. Using similar approaches, we provide the security analysis of the BB84 protocol in the presence of collective-rotation noise.

An essential task in QKD involves proving the unconditional security of a protocol [2]. This is important because a security result is expected to hold against all attacks allowed by quantum mechanics. During communication, Eve may deploy several eavesdropping strategies to attain secret key information. In theory, Eve's hacking techniques are categorized into three main classes: individual, collective, and coherent (or general) attacks [3]. A way to characterize how much information Eve acquired through these attacks or to establish security bounds is determined by evaluating the QBER. In most security proofs, the QBER is attributed to Eve's actions in the channel, but in real applications, the noise and eavesdropping activities contribute to the attained QBER. A rigorous security proof against all individual particle attacks, including intercept-resend attacks, even with practical signals, was given in [59]. The security proof bounds an eavesdropper's knowledge of the key by exploiting the average collision probability theory. While this security proof is of great importance for QKD, it lacks consideration of other practical imperfections in the quantum channel. For instance, the noise in the transmission channel is inevitable and has always been a menace to QKD since it leads to the deterioration of quantum states.

Therefore, in this paper, we consider a simple intercept and resend eavesdropping strategy in the presence of a collective-rotation noise transmission channel to demonstrate the security bounds for the BB84 QKD protocol. Besides this Introduction, which provides the background, we arrange the remainder of this paper as follows. In the next section, we introduce relevant theoretical knowledge, and in Section 2, we briefly describe the operation of the BB84 protocol. Then, Section 3 presents the procedure for the collective-noise rotation, while in Section 4, we analyze the influence of the noise and the intercept-resend attack on the BB84 QKD protocol. Finally, Section 5 concludes this work.

2. Operation of the BB84 Protocol

The BB84 QKD protocol belongs to a class of prepare and measure (P&M) protocols [2]. This protocol leverages the no-cloning theorem, which makes duplicating quantum states impossible. Thus, this hinders the eavesdropper from wiretapping the quantum communication channel or copying the quantum states, creating a key, and transmitting the original states to the receiver. Moreover, its security is based on the quantum measurement

principle, which states that a measurement of a quantum system causes it to collapse into an eigenstate of the operator corresponding to the measurement. Thus, an eavesdropper trying to learn (i.e., perform a measurement) the information being transmitted will result in her/his detection. The BB84 QKD protocol is implemented through the quantum and classical phases. Alice and Bob use quantum mechanical signals, measurements, and the quantum channel during the quantum phase. Moreover, this employs four quantum states, which constitute the two Pauli eigenbases, i.e., the canonical Z basis $\{|0\rangle, |1\rangle\}$ and the mutually unbiased X basis $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.

2.1. Preparation and Measurement

During the protocol operation, Alice prepares and sends signals to Bob, who measures them in a random sequence of Pauli bases, either the Z or X basis. Alice records her signal choices, while Bob records his basis choice, including the respective measurement outcomes. During the classical step, Alice and Bob utilize the authenticated public channel to conduct a classical communication protocol that employs a classical record of the quantum phase as the input.

2.2. Parameter Estimation

This is followed by a parameter estimation procedure, where Alice selects a fraction of her signal slots and broadcasts which signal she sent for these slots. Accordingly, Bob discloses his measurements on those signals and the respective outcome. Finally, they accept the decision if Alice and Bob, from their corresponding announcements, conclude that all the signals provided their correct deterministic outcomes whenever their basis choice coincided. If this happens, they proceed with the protocol or abort.

2.3. Sifting

In the sifting phase, the parties announce the polarization bases employed for the signal preparation and the remaining signals. Notably, Alice and Bob discard the data in which the polarization preparation and their measurement outcomes differed. Thus, the remaining data are called the "sifted data".

2.4. Key Map

At this stage, the parties form a secret key by mapping their event records of the sifted data in the secret key according to the following: $|0\rangle, |+\rangle \rightarrow 0$, and $|1\rangle, |-\rangle \rightarrow 1$. The binary string that results from this step constitutes a secret key.

2.5. Error Correction

At the end of the preceding step, Alice and Bob have a partially correlated pair of key strings created by executing the information reconciliation procedure. Alice sets her key as a reference key and performs a random hash function on her key string. She then shares her choice of the hash function, including the hash, with Bob. After that, Bob performs a hash function in his key string. The output hash of both parties must be compatible; otherwise, the protocol aborts. A fraction of information denoted by leak_{EC} is disclosed to Eve during the error-correction step.

2.6. Privacy Amplification

To eliminate Eve's knowledge about their secret key strings, Alice and Bob then extract an ℓ-bit key from their remaining error-corrected bit strings by applying privacy amplification. In doing so, Alice performs a random universal Class-2 hash function and publicly announces the results to Bob. Finally, Bob executes a similar hash function to distill a secret key of the same length as Alice.

3. Collective-Rotation Noise

Collective-noise assumes that, when numerous qubits are transmitted simultaneously or near each other at least spatially, then the random unitaries or transformations due to noise on each qubit should be identical [42,60,61]. Various studies have recently reported on the influence of counter-clockwise and clockwise collective-rotation noise on the security of QKD [51,62], respectively. Therefore, we analyze the impact of the clockwise collective-rotation noise in the channel, defined by the following unitary rotation matrix:

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

where θ represents the rotation angle that characterizes the effect of the noise. The collective-rotation noise changes the four BB84 states according to the following:

$$|0\rangle \rightarrow \cos\theta|0\rangle - \sin\theta|1\rangle = \frac{\cos\theta - \sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta + \sin\theta}{\sqrt{2}}|-\rangle, \tag{2}$$

$$|1\rangle \rightarrow \sin\theta|0\rangle + \cos\theta|1\rangle = \frac{\cos\theta + \sin\theta}{\sqrt{2}}|+\rangle + \frac{\sin\theta - \cos\theta}{\sqrt{2}}|-\rangle, \tag{3}$$

$$|+\rangle \rightarrow \frac{\cos\theta + \sin\theta}{\sqrt{2}}|0\rangle + \frac{\cos\theta - \sin\theta}{\sqrt{2}}|1\rangle = \cos\theta|+\rangle + \sin\theta|-\rangle, \tag{4}$$

$$|-\rangle \rightarrow \frac{\cos\theta - \sin\theta}{\sqrt{2}}|0\rangle - \frac{\sin\theta + \cos\theta}{\sqrt{2}}|1\rangle = \cos\theta|-\rangle - \sin\theta|+\rangle. \tag{5}$$

Notably, the collective-rotation noise introduces bit-flip errors in the following bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Thus, the weighted sum of the bit-flip errors results in the QBER, defined as the probability that a randomly selected qubit sent from Alice's lab arrives at Bob's side flipped. This can be represented as $|0\rangle$ as $|1\rangle$, $|+\rangle$ as $|-\rangle$, and vice versa. Based on Equations (2)–(5), the effect of noise is that it flips the states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ with probability $\sin^2\theta$. Therefore, if Alice selects and transmits each of the four states with a probability of $p = 1/4$, then the collective-rotation noise in the channel will result in a QBER of:

$$Q_0 = \frac{1}{4}(4\sin^2\theta) = \sin^2\theta. \tag{6}$$

The QBER is one of the essential QKD security parameters [2]. It gives the ratio of the number of bits in error to the total detected bits. Therefore, QBER provides the percentage of signals chosen by Alice and Bob for the same encoding, but where Bob got a measurement outcome that differs from that prepared by Alice [51].

4. Security Analysis of the Intercept-and-Resend Attack

Eve can perform an intercept-and-resend attack, one of the well-known attacks achieved through randomly measuring qubits that Alice sent in any of the two bases [63]. After that, Eve forwards to Bob the qubits prepared in states corresponding to her measurement outcomes [2]. For example, suppose we have an ordered set $S = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ of the possible states of the qubits; we can use the following probability transition matrix to represent the effect of Eve's actions:

$$P_{E|A} = \begin{pmatrix} \frac{\cos^2\theta}{2} & \frac{\sin^2\theta}{2} & \frac{1}{4}(1-\sin 2\theta) & \frac{1}{4}(\sin 2\theta + 1) \\ \frac{\sin^2\theta}{2} & \frac{\cos^2\theta}{2} & \frac{1}{4}(\sin 2\theta + 1) & \frac{1}{4}(1-\sin 2\theta) \\ \frac{1}{4}(\sin 2\theta + 1) & \frac{1}{4}(1-\sin 2\theta) & \frac{\cos^2\theta}{2} & \frac{\sin^2\theta}{2} \\ \frac{1}{4}(1-\sin 2\theta) & \frac{1}{4}(\sin 2\theta + 1) & \frac{\sin^2\theta}{2} & \frac{\cos^2\theta}{2} \end{pmatrix}, \tag{7}$$

where the matrix elements represent the conditional probabilities $p(e|a)$ obtained by Eve, given that Alice prepares a particular state. Notably, $p(a, e)$ denotes the joint probability

that Alice prepares a state $|\psi\rangle_A \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and Eve receives a state $|\psi\rangle_E \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, given as follows:

$$p(a,e) = p(e|a)p(a) = p(a|e)p(e), \tag{8}$$

where $p(a) = 1/4$ represents the probability that Alice prepares a state $|\psi\rangle_A \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, while $p(e) = 1/4$ denotes the probability that Eve acquires measurement outcomes that correspond to a state $|\psi\rangle_E \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Therefore, we can deduce that $p(a|e) = p(e|a)$. As a result, in Table 1, we summarize the results of the joint probabilities according to the following:

Table 1. A summary of joint probabilities when Alice prepares a particular state and Eve obtains measurement outcomes corresponding to each of the four states on qubits that Alice sent.

Alice Sends	**Eve Obtains**			
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$\cos^2\theta/8$	$\sin^2\theta/8$	$(1-\sin 2\theta)/16$	$(1+\sin 2\theta)/16$
$\|1\rangle$	$\sin^2\theta/8$	$\cos^2\theta/8$	$(1+\sin 2\theta)/16$	$(1-\sin 2\theta)/16$
$\|+\rangle$	$(1+\sin 2\theta)/16$	$(1-\sin 2\theta)/16$	$\cos^2\theta/8$	$\sin^2\theta/8$
$\|-\rangle$	$(1-\sin 2\theta)/16$	$(1+\sin 2\theta)/16$	$\sin^2\theta/8$	$\cos^2\theta/8$

We can use mutual information to measure the amount of information that Eve gains from each measurement. This is expressed as:

$$I(A:E) = H(A) - H(A|E), \tag{9}$$

where

$$H(A) = -\sum_{i=1}^{4} p(i)\log_2 p(i) = -\sum 4\Big(\frac{1}{4}\log_2\frac{1}{4}\Big) = -\log_2\frac{1}{4}, \tag{10}$$

and

$$\begin{aligned} H(A|E) &= -\sum_{a,e} p(a,e)\log_2 p(a|e) \\ &= -\Big(\frac{\cos^2\theta}{2}\log_2\frac{\cos^2\theta}{2} + \frac{\sin^2\theta}{2}\log_2\frac{\sin^2\theta}{2} + \frac{1-\sin 2\theta}{4}\log_2\frac{1-\sin 2\theta}{4} \\ &\quad + \frac{1+\sin 2\theta}{4}\log_2\frac{1+\sin 2\theta}{4}\Big). \end{aligned} \tag{11}$$

To simplify Equation (9), let $\varepsilon = \sin^2\theta$. This implies that ε takes values that belong to $[0,1]$. If we substitute ε into Equation (9), it yields the following form:

$$\begin{aligned} I(A:E) = &-\log_2\frac{1}{4} + \frac{1-\varepsilon}{2}\log_2\frac{1-\varepsilon}{2} + \frac{\varepsilon}{2}\log_2\frac{\varepsilon}{2} + \frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{4}\log_2\frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{4} \\ &+ \frac{1+2\sqrt{\varepsilon(1-\varepsilon)}}{4}\log_2\frac{1+2\sqrt{\varepsilon(1-\varepsilon)}}{4}. \end{aligned} \tag{12}$$

We now analyze two types of intercept-and-resend methods that Eve could engage. Firstly, Eve could break the quantum channel between Alice and Bob and slide her devices between the communicating parties, as shown in Figure 1a. As a result, we find that the

transition probability matrix, which describes the change between the states prepared by Eve and those obtained by Bob, can be shown to be:

$$P_{B|E} = \begin{pmatrix} \frac{\cos^2\phi}{2} & \frac{\sin^2\phi}{2} & \frac{1}{4}(1-\sin 2\phi) & \frac{1}{4}(\sin 2\phi+1) \\ \frac{\sin^2\phi}{2} & \frac{\cos^2\phi}{2} & \frac{1}{4}(\sin 2\phi+1) & \frac{1}{4}(1-\sin 2\phi) \\ \frac{1}{4}(\sin 2\phi+1) & \frac{1}{4}(1-\sin 2\phi) & \frac{\cos^2\phi}{2} & \frac{\sin^2\phi}{2} \\ \frac{1}{4}(1-\sin 2\phi) & \frac{1}{4}(\sin 2\phi+1) & \frac{\sin^2\phi}{2} & \frac{\cos^2\phi}{2} \end{pmatrix}. \quad (13)$$

The matrix $P_{A,B}$, which denotes the joint probabilities of Alice and Bob's states, can be calculated as follows:

$$P_{A,B} = \frac{1}{4} \times P_{E|A} \times P_{B|E}. \quad (14)$$

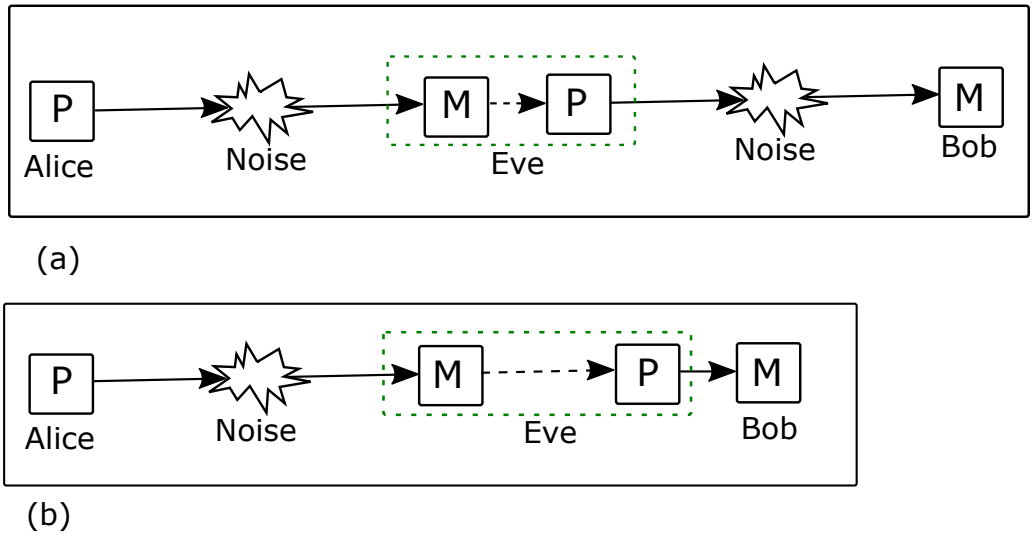

Figure 1. An illustration of the two intercept-and-resend attack strategies. The quantum channel is denoted by straight arrows, while dashed arrows depict lossless classical channels. (**a**) Eve breaks the quantum channel between Alice and Bob and places her devices between the two parties. (**b**) Eve places her preparation device at a location close to, possibly inside, Bob's lab and connects her measurement and preparation devices by a lossless classical channel. The letters P and M represent preparation and measurement devices, respectively.

In Table 2, we summarize the joint probabilities, and based on this strategy, elements in the table are provided as:

$$a = \frac{\cos^2\theta}{8} \times \frac{\cos^2\phi}{2} + \frac{\sin^2\theta}{8} \times \frac{\sin^2\phi}{2} + \frac{1-\sin 2\theta}{16} \times \frac{1+\sin 2\phi}{4} + \frac{1+\sin 2\theta}{16} \times \frac{1-\sin 2\phi}{4}, \quad (15)$$

$$b = \frac{\cos^2\theta}{8} \times \frac{\sin^2\phi}{2} + \frac{\sin^2\theta}{8} \times \frac{\cos^2\phi}{2} + \frac{1-\sin 2\theta}{16} \times \frac{1-\sin 2\phi}{4} + \frac{1+\sin 2\theta}{16} \times \frac{1+\sin 2\phi}{4}, \quad (16)$$

$$c = \frac{\cos^2\theta}{8} \times \frac{1-\sin 2\phi}{4} + \frac{\sin^2\theta}{8} \times \frac{1+\sin 2\phi}{4} + \frac{1-\sin 2\theta}{16} \times \frac{\cos^2\phi}{2} + \frac{1+\sin 2\theta}{16} \times \frac{\sin^2\phi}{2}, \quad (17)$$

$$d = \frac{\cos^2\theta}{8} \times \frac{1+\sin 2\phi}{4} + \frac{\sin^2\theta}{8} \times \frac{1-\sin 2\phi}{4} + \frac{1-\sin 2\theta}{16} \times \frac{\sin^2\phi}{2} + \frac{1+\sin 2\theta}{16} \times \frac{\cos^2\phi}{2}. \quad (18)$$

During the sifting stage, the terms c and d in Table 2 reduce to zero. Accordingly, Q, after sifting, becomes:

$$Q = \frac{b}{a+b} = \frac{2-\cos 2(\theta+\phi)}{4}. \quad (19)$$

However, in the case where $\theta = \phi$, which means that the level of noise in both channels is equal, then Q becomes

$$Q_1 = \frac{1 + 2\sin^2 2\theta}{4}. \tag{20}$$

As the second eavesdropping strategy that Eve could deploy, the preparation device is placed near, or even where possible, inside Bob's lab. After that, Eve links the measurement and preparation devices using a lossless classical channel [63]. This is shown in Figure 1b. The matrix describing conditional probabilities to prepare particular states by Eve and the measurements obtained by Bob is given by

$$P_{B|E} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \end{pmatrix}. \tag{21}$$

Table 2. A summary of joint probabilities for states prepared by Alice and Bob's measurement outcomes corresponding to each of the four states when given Eve's intercept-and-resend attack.

Eve Sends	**Bob Obtains**			
	$\|\mathbf{0}\rangle$	$\|\mathbf{1}\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$(\cos^2\phi)/2$	$(\sin^2\phi)/2$	$(1-\sin 2\phi)/4$	$(1+\sin 2\phi)/2$
$\|1\rangle$	$(\sin^2\phi)/2$	$(\cos^2\phi)/2$	$(1+\sin 2\phi)/4$	$(1-\sin 2\phi)/4$
$\|+\rangle$	$(1+\sin 2\phi)/4$	$(1-\sin 2\phi)/4$	$(\cos^2\phi)/2$	$(\sin^2\phi)/2$
$\|-\rangle$	$(1-\sin 2\phi)/4$	$(1+\sin 2\phi)/4$	$(\sin^2\phi)/2$	$(\cos^2\phi)/2$
Alice Sends	**Bob Receives**			
	$\|\mathbf{0}\rangle$	$\|\mathbf{1}\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	a	b	c	d
$\|1\rangle$	b	a	d	c
$\|+\rangle$	d	c	a	b
$\|-\rangle$	c	d	b	a

Suppose Eve performs the attack presented in this strategy; this allows her to minimize her quantum "footprint" by replacing the collective-rotation noise channel with a lossless classical channel. However, this strategy fails to enhance her odds of going undetected. This is depicted in Figure 2. To find Q_2, first, we evaluate the elements a – d in Table 2 by employing Equation (14). The matrices $P_{E|A}$ and $P_{B|E}$ come from Equations (7) and (21), respectively. As a result, the terms a – d are evaluated to be:

$$a = \frac{1 + 2\cos^2\theta}{32}, \tag{22}$$

$$b = \frac{1 + 2\sin^2\theta}{32}, \tag{23}$$

$$c = \frac{2 - \sin 2\theta}{32}, \tag{24}$$

$$d = \frac{2 + \sin 2\theta}{32}. \tag{25}$$

We note that the terms c and d disappear during sifting. Thus, Q_2 becomes:

$$Q_2 = \frac{1 + 2\sin^2\theta}{4}. \tag{26}$$

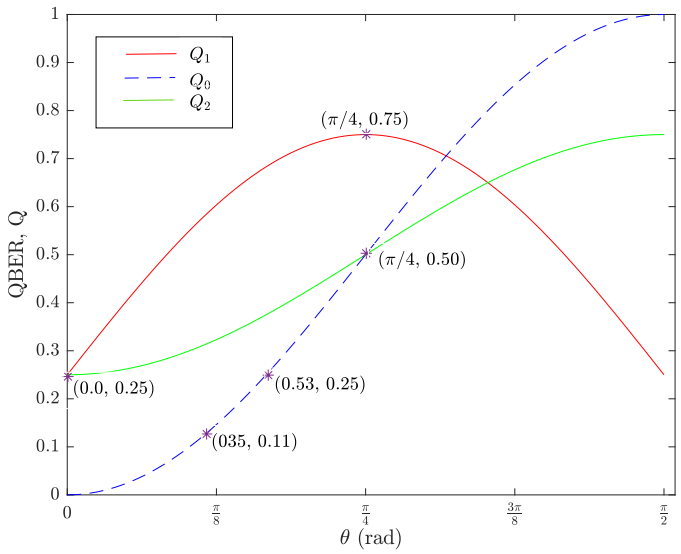

Figure 2. Comparison of the variation of the quantum bit error rate Q with the rotation angle θ for the case where there is no eavesdropping (Q_0), the case where the eavesdropper performs the attack outlined in the strategy shown in Figure 1a (Q_1), and the case where the eavesdropper performs the attack outlined in the strategy shown in Figure 1b (Q_2).

Figure 2 illustrates the relationship between the QBER and rotational noise in the channel. It can be observed from Figure 2 that, when rotational angle $\theta \leq \frac{\pi}{4}$, $Q_1 > Q_2$, Eve's eavesdropping results in a more significant bit error rate and she will be detected. We observe that, in a noise-free environment (i.e., $\theta = 0$), Eve will induce a 25% QBER. This corresponds to the well-known error bound for the BB84 protocol under the simple intercept-resend attack. The results also indicate that QBER Q_1 reaches a maximum for every rotation angle $\theta = n\pi + \frac{\pi}{4}$ (where n is an integer), and this corresponds to noise, which will flip the prepared quantum states into a state in the opposite basis (phase flip error). Furthermore, for curve Q_1, we note that, for every $\theta = n\frac{\pi}{2}$, the QBER is at its lowest value. Finally, we observe that when Eve intercepts the qubits and prepares them at the site closer to Bob's measurement station, represented by the curve Q_2, the noise in the channel does not heavily contribute to the QBER. Thus, according to the curve Q_2, for every rotation angle $\theta = n\pi + \frac{\pi}{2}$, the QBER is at its maximum and reaches its lowest at every $\theta = n\pi$. Moreover, it is observed that for Q_1, the maximum QBER is reached at $\frac{\pi}{4}$, which occurs before Q_2 reaches its maximum QBER at $\theta = \frac{\pi}{2}$. Therefore, any noise induced by rotational angles $\frac{\pi}{4} < \theta < \frac{5\pi}{4}$ results in a decrease in the QBER in Q_1 due to the periodic nature of the function. The slow increase in the QBER in Q_1 compared to Q_1 can be attributed to the fact that in case Q_2, the quantum states prepared by Eve do not experience any noise in the channel before reaching Bob, as illustrated by Figure 1b. However, when $\theta = \frac{\pi}{4}$, the case that results in phase flip errors, the QBER is at 50%, i.e., half of the sifted key bits will be erroneous. Furthermore, from Figure 2, we observe that a noise induced by the rotation of the prepared quantum state by an angle of 0.35 radians will cause a QBER of 11%, and this corresponds to the lower bound on the tolerable error rate for the BB84 protocol against general attacks. Furthermore, a rotational angle of 0.53 radians will cause a 25% QBER, a value corresponding to the bound on the error rate brought about by the intercept-resend attack.

In Figure 3, we investigate the amount of information Eve can gain from her intercept-resend strategy. Our results show that the maximum information that Eve can acquire is 0.5 bits, which occurs at a noise level of 0.5 and in a noise-free environment (i.e., at $\varepsilon = 0$). Furthermore, we observe that Alice randomly sends $H(A) = 2$ bits of information; this implies Eve gains utmost 25% of the information Alice sends to Bob. Thus, this confirms that Eve can obtain a minimum of 0.4 bits of information at a 12% noise level.

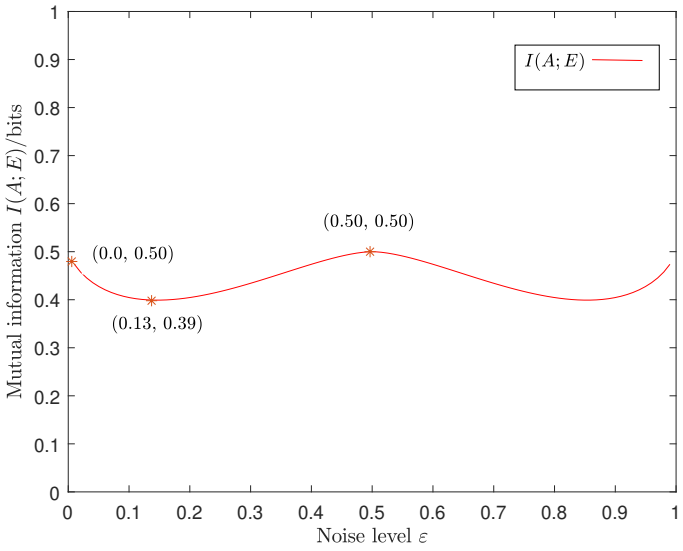

Figure 3. Variation of the mutual information between Alice and Eve *I(A:E)* as a function of the collective-rotation noise ε.

5. Conclusions

We demonstrated the security of the BB84 QKD protocol under the collective-rotation noise channel by studying scenarios where the eavesdropper, Eve, conducts an intercept-resend attack on the transmitted photons sent via a quantum communication channel shared by Alice and Bob. Notably, we distinguished the impact of collective-rotation noise and that of the eavesdropper. From the analysis, we observed that, for small rotation angles, one can extract a secure secret key under a collective-rotation noise channel when there is no eavesdropping. For instance, in a noise-free environment ($\theta = 0$), Eve will induce a 25% QBER, corresponding to the well-known error bound for the BB84 protocol under the simple intercept-resend attack. However, when both eavesdropping and noise exist in the channel, the QBER obtained would always be greater than the 25% error threshold for the intercept-resend attack. Hence, no secret key can be distilled by the legitimate parties. In addition, the BB84 protocol experiences the worst QBER Q_1 for every rotation angle $\theta = n\pi + \frac{\pi}{4}$. Notably, this corresponds to noise that will flip the prepared quantum states into a state on the opposite basis (i.e., a phase flip error). Thus, Q_1 reaches its lowest level at every $\theta = n\frac{\pi}{2}$. However, when $\theta = \frac{\pi}{4}$, the case that results in phase flip errors, the QBER is at 50%, meaning that half of the sifted key bits will be erroneous. Most significantly, we observed that noise induced by a rotation of 0.35 radians of the prepared quantum state will cause a QBER of 11%. This phenomenon corresponds to the lower bound on the tolerable error rate for the BB84 QKD protocol against general attacks. Finally, a rotational angle of 0.53 radians produces a 25% QBER, which corresponds to the bound on the error rate brought about by the intercept-resend attack.

Author Contributions: Conceptualization, M.M. and C.S.; methodology, M.M and C.S.; software, C.S.; validation, M.M. and C.S.; writing—original draft preparation, M.M.; writing—review and editing, C.S., M.M., and M.S.; visualization, C.S.; supervision, M.M.; project administration, M.M.; funding acquisition, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
3. Pirola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236.
4. Scarani, V.; Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. *Theor. Comput. Sci.* **2014**, *560*, 27–32. [CrossRef]
5. Kumar, A.; Garhwal, S. State-of-the-art survey of quantum cryptography. *Arch. Comput. Methods Eng.* **2021**, *28*, 1–38. [CrossRef]
6. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
7. Zoller, P.; Beth, T.; Binosi, D.; Blatt, R.; Briegel, H.; Bruss, D.; Calarco, T.; Cirac, J.I.; Deutsch, D.; Eisert, J.; et al. Quantum information processing and communication. *Eur. Phys. J. D.* **2005**, *36*, 203–228. [CrossRef]
8. Śliwczyński, Ł.; Krehlik, P.; Lipiński, M. Optical fibers in time and frequency transfer. *Meas. Sci. Technol.* **2010**, *21*, 075302. [CrossRef]
9. Ngabireng, C.; Ambomo, S.; Dinda, P.T.; Moubissi, A. Loss effects in the spectra of polarization modulational instability in weakly birefringent optical fibers. *J. Opt.* **2011**, *13*, 085201. [CrossRef]
10. Yang, C.W.; Hwang, T. Quantum dialogue protocols immune to collective noise. *Quantum Inf. Process.* **2013**, *12*, 2131–2142. [CrossRef]
11. Mertz, M.; Kampermann, H.; Shadman, Z.; Bruß, D. Quantum key distribution with finite resources: Taking advantage of quantum noise. *Phys. Rev. A* **2013**, *87*, 042312. [CrossRef]
12. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **1998**, *81*, 3018. [CrossRef]
13. Senekane, M.; Mafu, M.; Petruccione, F. Six-state symmetric quantum key distribution protocol. *J. Quant. Inf. Sci.* **2015**, *5*, 33. [CrossRef]
14. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 57901. [CrossRef]
15. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]
16. Ralph, T.C. Continuous variable quantum cryptography. *Phys. Rev. A* **1999**, *61*, 010303. [CrossRef]
17. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **2000**, *61*, 022309. [CrossRef]
18. Aguiar, L.D.S.; Borelli, L.F.; Roversi, J.A.; Vidiella-Barranco, A. Performance analysis of continuous-variable quantum key distribution using non-Gaussian states. *Quantum Inf. Process.* **2022**, *21*, 1–15. [CrossRef]
19. Inoue, K.; Waks, E.; Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **2002**, *89*, 037902. [CrossRef]
20. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
21. Mafu, M.; Marais, A.; Petruccione, F. A necessary condition for the security of coherent-one-way quantum key distribution protocol. *Appl. Math. Inf. Sci.* **2014**, *8*, 2769. [CrossRef]
22. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
23. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hübel, H. Continuous-Variable quantum key distribution with gaussian modulation—The theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1870011. [CrossRef]
24. Pironio, S.; Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Scarani, V. Device-independent quantum key distribution secure against collective attacks. *N. J. Phys.* **2009**, *11*, 045021. [CrossRef]
25. Woodhead, E.; Acín, A.; Pironio, S. Device-independent quantum key distribution with asymmetric CHSH inequalities. *Quantum* **2021**, *5*, 443. [CrossRef]
26. Zhao, W.; Shi, R.; Ruan, X.; Guo, Y.; Mao, Y.; Feng, Y. Monte Carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel. *Quantum Inf. Process.* **2022**, *21*, 1–14. [CrossRef]
27. Curty, M.; Xu, F.; Cui, W.; Lim, C.C.W.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 1–7. [CrossRef]
28. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
29. Zhou, Y.H.; Qin, S.F.; Shi, W.M.; Yang, Y.G. Measurement-device-independent continuous variable semi-quantum key distribution protocol. *Quant. Inf. Process.* **2022**, *21*, 1–21. [CrossRef]
30. Sibson, P.; Erven, C.; Godfrey, M.; Miki, S.; Yamashita, T.; Fujiwara, M.; Thompson, M.G. Chip-based quantum key distribution. *Nat. Comm.* **2017**, *8*, 1–6. [CrossRef] [PubMed]
31. Semenenko, H.; Sibson, P.; Hart, A.; Thompson, M.G.; Rarity, J.G.; Erven, C. Chip-based measurement-device-independent quantum key distribution. *Optica* **2020**, *7*, 238–242. [CrossRef]
32. Kwek, L.C.; Cao, L.; Luo, W.; Wang, Y.; Sun, S.; Wang, X.; Liu, A.Q. Chip-based quantum key distribution. *AAPPS Bull.* **2021**, *31*, 1–8. [CrossRef]

33. Zhao, P.; Zhou, L.; Zhong, W.; Sheng, Y.B. Faithful entanglement distribution using quantum multiplexing in noisy channel. *Eur. Lett.* **2021**, *135*, 40001. [CrossRef]
34. Liu, Q.; Huang, Y.; Du, Y.; Zhao, Z.; Geng, M.; Zhang, Z.; Wei, K. Advances in chip-based quantum key distribution. *Entropy* **2022**, *24*, 1334. [CrossRef]
35. Orieux, A.; Diamanti, E. Recent advances on integrated quantum communications. *J. Opt.* **2016**, *18*, 083002. [CrossRef]
36. Tamaki, K.; Lütkenhaus, N. Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A* **2004**, *69*, 032316. [CrossRef]
37. Wang, X.B. Fault tolerant quantum key distribution protocol with collective random unitary noise. *Phys. Rev. A* **2005**, *72*, 050304. [CrossRef]
38. Grasselli, F.; Kampermann, H.; Bruß, D. Finite-key effects in multipartite quantum key distribution protocols. *N. J. Phys.* **2018**, *20*, 113014. [CrossRef]
39. Zhang, Z.J. Robust multiparty quantum secret key sharing over two collective-noise channels. *Phys. A: Stat. Mech. Appl.* **2006**, *361*, 233–238. [CrossRef]
40. Li, X.H.; Deng, F.G.; Zhou, H.Y. Efficient quantum key distribution over a collective noise channel. *Phys. Rev. A* **2008**, *78*, 022321. [CrossRef]
41. Dong, L.; Xiu, X.M.; Gao, Y.J.; Chi, F. Deterministic secure quantum communication against collective-dephasing noise by using EPR pairs and auxiliary photons. *Opt. Commun.* **2009**, *282*, 1688–1690. [CrossRef]
42. Xiu, X.M.; Dong, L.; Gao, Y.J.; Chi, F. Quantum key distribution protocols with six-photon states against collective noise. *Opt. Commun.* **2009**, *282*, 4171–4174. [CrossRef]
43. Sheng, Y.B.; Deng, F.G. Efficient quantum entanglement distribution over an arbitrary collective-noise channel. *Phys. Rev. A* **2010**, *81*, 042332. [CrossRef]
44. Dong, H.K.; Dong, L.; Xiu, X.M.; Gao, Y.J. A deterministic secure quantum communication protocol through a collective rotation noise channel. *Int. J. Quantum Inf.* **2010**, *8*, 1389–1395. [CrossRef]
45. Huang, W.; Wen, Q.; Liu, B.; Gao, F.; Sun, Y. Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. *Sci. China Phys. Mech.* **2013**, *56*, 1670–1678. [CrossRef]
46. Gu, B.; Zhang, C.; Cheng, G.; Huang, Y. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. *Sci. China Physics, Mech. Astron.* **2011**, *54*, 942–947. [CrossRef]
47. Yang, C.; Tsai, C.; Hwang, T. Fault tolerant two-step quantum secure direct communication protocol against collective noises. *Sci. China Phys. Mech.* **2011**, *54*, 496–501. [CrossRef]
48. Wei, H.; Qiao-Yan, W.; Heng-Yue, J.; Su-Juan, Q.; Fei, G. Fault tolerant quantum secure direct communication with quantum encryption against collective noise. *Chin. Phys. B* **2012**, *21*, 100308.
49. Ye, T. Fault tolerant channel-encrypting quantum dialogue against collective noise. *Sci. China Phys. Mech.* **2015**, *58*, 1–10. [CrossRef]
50. Ye, T.Y. Quantum secure direct dialogue over collective noise channels based on logical Bell states. *Quantum Inf. Process.* **2015**, *14*, 1487–1499. [CrossRef]
51. Li, J.; Pan, Z.; Zheng, J.; Sun, F.; Ye, X.; Yuan, K. The security analysis of quantum SAGR04 protocol in collective-rotation noise channel. *Chin. J. Electron.* **2015**, *24*, 689–693. [CrossRef]
52. Wu, L.; Chen, Y. Three stage quantum cryptography protocol under collective-rotation noise. *Entropy* **2015**, *17*, 2919–2931. [CrossRef]
53. Garapo, K.; Mafu, M.; Petruccione, F. Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. *Chin. Phys. B* **2016**, *25*, 070303. [CrossRef]
54. Li, L.; Li, J.; Li, C.; Li, H.; Yang, Y.; Chen, X. The security analysis of quantum B92 protocol in collective-rotation noise channel. *Int. J. Theor. Phys.* **2019**, *58*, 1326–1336. [CrossRef]
55. Yang, Y.G.; Gao, S.; Li, D.; Zhou, Y.H.; Shi, W.M. Three-party quantum secret sharing against collective noise. *Quantum Inf. Process.* **2019**, *18*, 1–11. [CrossRef]
56. He, Y.F.; Ma, W.P. Multiparty quantum secure direct communication immune to collective noise. *Quantum Inf. Process.* **2019**, *18*, 1–11. [CrossRef]
57. Chang, L.W.; Zhang, Y.Q.; Tian, X.X.; Qian, Y.H.; Zheng, S.H. Fault tolerant controlled quantum dialogue against collective noise. *Chin. Phys. B* **2020**, *29*, 010304. [CrossRef]
58. Zhao, J.; Zhang, W.; Ma, Y.; Zhang, X.; Ma, H. Development of quantum private queries protocol on collective-dephasing noise channel. *Appl. Sci.* **2020**, *10*, 1935. [CrossRef]
59. Waks, E.; Zeevi, A.; Yamamoto, Y. Security of quantum key distribution with entangled photons against individual attacks. *Phys. Rev. A* **2002**, *65*, 052310. [CrossRef]
60. Żukowski, M.; Zeilinger, A.; Horne, M.A.; Ekert, A.K. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **1993**, *71*, 4287–4290. [CrossRef]
61. Gu, B.; Pei, S.; Song, B.; Zhong, K. Deterministic secure quantum communication over a collective-noise channel. *Sci. China Phys. Mech.* **2009**, *52*, 1913–1918. [CrossRef]

62. 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 Phys. Sin.* **2016**, *65*, 30302.
63. Curty, M.; Lütkenhaus, N. Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses. *Phys. Rev. A* **2005**, *71*, 062301. [CrossRef]