Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels*

Kevin Garapo[1,†], Mhlambululi Mafu[2], and Francesco Petruccione[1,3]

[1] *Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X*54001 *Durban* 4000, *South Africa*
[2] *Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag* 16, *Palapye, Botswana*
[3] *National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa*

(Received 12 November 2015; revised manuscript received 3 March 2016; published online 31 May 2016)

We investigate the effect of collective-rotation noise on the security of the six-state quantum key distribution. We study the case where the eavesdropper, Eve, performs an intercept-resend attack on the quantum communication between Alice, the sender, and Bob, the receiver. We first derive the collective-rotation noise model for the six-state protocol and then parameterize the mutual information between Alice and Eve. We then derive quantum bit error rate for three intercept-resend attack scenarios. We observe that the six-state protocol is robust against intercept-resend attacks on collective rotation noise channels when the rotation angle is kept within certain bounds.

Keywords: six states, quantum key distribution, security, collective-rotation noise

PACS: 03.67.Dd **DOI:** 10.1088/1674-1056/25/7/070303

1. Introduction

Quantum key distribution (QKD) provides the only physically secure and proven method to exchange secret cryptographic keys between two parties, Alice and Bob,[1,2] through public communication channels. QKD guarantees that an eavesdropper, Eve, with full access to the communication channels and unbounded computational power is unable to extract useful information on secret keys exchanged.[2] Unlike the conjectured security of classical key distribution,[3,4] which rely on the implied difficulty of solving discrete logarithm and integer factorisation problems, the security of QKD is based on the fundamental laws of physics, for example, the no-cloning theorem[5] and the Heisenberg uncertainty principle.[6–8] This means that in principle QKD guarantees unconditional security in communication between legitimate users if perfectly implemented.[2]

Since Bennett and Brassard's pioneering work of the BB84 protocol,[1] several QKD protocols have been proposed,[9–12] reviewed and implemented.[13–28] Furthermore, these developments have led to commercialization of QKD.[29,30]

In security studies, the noise in the quantum channel requires scrutiny because an eavesdropper trying to avoid detection may disguise themselves as noise.[31] Precisely, the noise pattern of the channel can be controlled by an eavesdropper. A number of studies on the effect of noise on QKD have been published. For example, the security of the Bennett 1992 QKD against individual attack over a realistic channel,[32] and over a lossy and noisy channel.[33] Likewise, the effect of quantum noise on the achievable finite-key rates of the BB84 and the six-state protocols has also been presented in Ref. [34].

Photons are the best carriers of quantum information in current QKD set-ups and the majority of the commercial systems use optical fibre as the communication channel. However, optical fibres suffer from slow fluctuations in the birefringence, which can be modeled as collective noise.[31] Therefore, noise is highly unavoidable in the communication process. There are two main types of collective noise namely, collective-dephasing noise and collective-rotation noise. In general, noise poses a threat especially for QKD schemes that implement a polarization degree of freedom for encoding information. This is because the noise usually changes the fidelity of quantum states that carry quantum information and also allows an eavesdropper to disguise her disturbance as noise in the communication channel, thus reducing her detection probability. Only when the noise, i.e., error rates are acceptable can the legitimate parties use the quantum signals to generate a secret key. Otherwise, if the noise is too large, this results in a high error rate, therefore no secret key can be extracted. Collective noise is the noise that has the same effect on adjacent quantum systems. Several studies have been published on the effects of collective-dephasing and collective-rotation noises on quantum communication, see Refs. [35]–[39]. Given a qubit, collective-dephasing noise introduces phase in one of the two basis states. This phase, however, does not affect the statistics of measurement in the preparation basis. Collective-rotation noise, on the other hand, alters the

*Project supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.
†Corresponding author. E-mail: kevingarapo@gmail.com
© 2016 Chinese Physical Society and IOP Publishing Ltd

statistics by introducing a probability of inverting one basis state into the other.

The aim of this study is to demonstrate the security bounds for the six-state QKD protocol,[11] which was designed to be more resistant to noise, when collective-rotation noise is present in the transmission channel. This article is arranged as follows. In Section 2, we give a brief description of the operation of the six-state QKD protocol. In Sections 3 and 4, we describe the scheme for collective noise rotation and analyze the effect of the noise on the operation of the protocol. We conclude the article in Section 5.

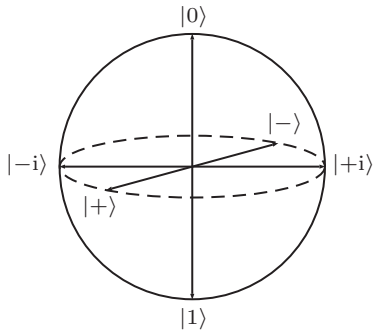


Fig. 1. The six states spanning the Bloch sphere.

2. Six-state QKD protocol

The six-state protocol[40] is a more generalized version of the BB84 protocol,[1] in which information is randomly encoded in three bases: $\{|0\rangle,|1\rangle\}$, $\{|+\rangle,|-\rangle\}$, and $\{|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$ bases, where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ and $|\pm\mathrm{i}\rangle = 1/\sqrt{2}(|0\rangle \pm \mathrm{i}|1\rangle)$. The six-state protocol is more symmetrical than the standard BB84 protocol because the three conjugate bases span the entire Bloch sphere, as shown in Fig. 1. The representation of the six states in the three conjugate bases is given in Table 1. Due to symmetry, other variants of the six-state protocol have been proposed and studied.[41–44] The six-state protocol belongs to the class of prepare and measure schemes. It can be implemented by modern optical techniques without the requirement of a quantum computer.

In the six-state protocol, Alice creates a random bit string and randomly selects one of the three bases, with equal probability $p = 1/3$, to encode each bit in the string. She sends the resultant qubit stream to Bob using a quantum channel. Bob randomly chooses, with probability $1/3$, the basis in which he measures the state of each qubit in the stream. Bob's observables are given by the following Pauli operators: σ_z, σ_x, and σ_y for the $\{|0\rangle,|1\rangle\}$, $\{|+\rangle,|-\rangle\}$, and $\{|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$ bases, respectively. Following Bob's measurements, Alice communicates the random basis selection through an authenticated classical channel. They both discard measurements where Bob used a different basis, in a process called sifting, and apply classical post-processing techniques on the remaining events to distil a secret key.

Table 1. Representation of the six states in the three bases.

State	Basis		
	$\{\|0\rangle,\|1\rangle\}$	$\{\|+\rangle,\|-\rangle\}$	$\{\|+\mathrm{i}\rangle,\|-\mathrm{i}\rangle\}$
$\|0\rangle$	$\|0\rangle$	$(\|+\rangle+\|-\rangle)/\sqrt{2}$	$(\|+\mathrm{i}\rangle+\|-\mathrm{i}\rangle)/\sqrt{2}$
$\|1\rangle$	$\|1\rangle$	$(\|+\rangle-\|-\rangle)/\sqrt{2}$	$+\mathrm{i}(\|+\mathrm{i}\rangle-\|-\mathrm{i}\rangle)/\sqrt{2}$
$\|+\rangle$	$(\|0\rangle+\|1\rangle)/\sqrt{2}$	$\|+\rangle$	$\exp(-\mathrm{i}\pi/4)(\|+\mathrm{i}\rangle+\mathrm{i}\|-\mathrm{i}\rangle)/\sqrt{2}$
$\|-\rangle$	$(\|0\rangle-\|1\rangle)/\sqrt{2}$	$\|-\rangle$	$\exp(\mathrm{i}\pi/4)(\|+\mathrm{i}\rangle-\mathrm{i}\|-\mathrm{i}\rangle)/\sqrt{2}$
$\|+\mathrm{i}\rangle$	$(\|0\rangle+\mathrm{i}\|1\rangle)/\sqrt{2}$	$\exp(\mathrm{i}\pi/4)(\|+\rangle-\mathrm{i}\|-\rangle)/\sqrt{2}$	$\|+\mathrm{i}\rangle$
$\|-\mathrm{i}\rangle$	$(\|0\rangle-\mathrm{i}\|1\rangle)/\sqrt{2}$	$\exp(-\mathrm{i}\pi/4)(\|+\rangle+\mathrm{i}\|-\rangle)/\sqrt{2}$	$\|-\mathrm{i}\rangle$

The six-state QKD protocol has been studied under various scenarios since its proposal. Based on the optimal mutual information between sender and eavesdropper, it has been shown that the six-state scheme is safer against eavesdropping on single qubits than the one based on two conjugate bases.[40] A study of optimal eavesdropping strategies for the six-state QKD protocol has been made and the results show that this scheme is more secure against symmetric attacks than protocols using two-dimensional states.[45] Furthermore, incoherent and coherent eavesdropping strategies on the six-state protocol have been classified, and for a disturbance of 1/6, the optimal incoherent eavesdropping strategy reduces to the universal quantum-cloning machine.[46,47] One of the most important tasks in QKD is to prove the unconditional security of a protocol, i.e., security bounds in the case where Eve has unlimited power over the quantum channel. The unconditional security proof of the standard six-state scheme using only one-way classical communications has been presented. In this proof it was shown that the six-state scheme could be made secure up to an error rate of 12.7%.[18] Later, using the technique of two-way entanglement purification, the security proof against the most general attack has been derived. Based on this tech-

nique, it was shown that the six-state protocol could tolerate a bit error rate of 26.4%.[48] Moreover, the lower and upper bounds on the secret-key rate for six-state protocol use one-way classical communication.[15,16] The security bounds for the BB84 and the six-state protocols have been calculated using the smooth min-entropies obtained in Refs. [49] and [50]. Security bounds for the six-state protocol when implemented with finite resources under one-way post processing have been shown in Ref. [51]. An eavesdropping technique for the six-state protocol when Alice deliberately adds noise to the signal states before they leave her lab or in a realistic scenario where Eve cannot replace the noisy quantum channel by a noiseless one has been presented. It was found that addition of quantum noise makes quantum key distribution more robust against eavesdropping.[52]

3. Collective-rotation noise

The collective noise assumption states that if several qubits are transmitted simultaneously or they are close to each other spatially, the random unitaries or transformations of the noise on each qubit must be identical.[53] Various protocols have been studied under collective noise.[31,35–37] Recently, studies on the effect of counter-clockwise and clockwise collective-rotation noise on the security of quantum key distribution have been reported in Refs. [54] and [55], respectively. We analyze the effect of clockwise collective-rotation noise in the channel represented by the following unitary rotation matrix:

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

where θ is a rotation angle characterizing the effect of the noise.

Collective rotation noise transforms the six states in the protocol as follows:

$$\begin{aligned} |0\rangle &\to \cos\theta|0\rangle - \sin\theta|1\rangle \\ &= \frac{\cos\theta-\sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta+\sin\theta}{\sqrt{2}}|-\rangle \\ &= \frac{e^{i\theta}}{\sqrt{2}}(|+i\rangle + e^{-2i\theta}|-i\rangle), \end{aligned} \tag{2}$$

$$\begin{aligned} |1\rangle &\to \sin\theta|0\rangle + \cos\theta|1\rangle \\ &= \frac{\cos\theta+\sin\theta}{\sqrt{2}}|+\rangle + \frac{\sin\theta-\cos\theta}{\sqrt{2}}|-\rangle \\ &= -i\frac{e^{i\theta}}{\sqrt{2}}(|+i\rangle - e^{-2i\theta}|-i\rangle), \end{aligned} \tag{3}$$

$$\begin{aligned} |+\rangle &\to \frac{\cos\theta+\sin\theta}{\sqrt{2}}|0\rangle + \frac{\cos\theta-\sin\theta}{\sqrt{2}}|1\rangle \\ &= \cos\theta|+\rangle + \sin\theta|-\rangle \\ &= \frac{e^{i(\theta-\pi/4)}}{\sqrt{2}}(|+i\rangle + i\,e^{-2i\theta}|-i\rangle), \end{aligned} \tag{4}$$

$$\begin{aligned} |-\rangle &\to \frac{\cos\theta-\sin\theta}{\sqrt{2}}|0\rangle - \frac{\sin\theta+\cos\theta}{\sqrt{2}}|1\rangle \\ &= \cos\theta|-\rangle - \sin\theta|+\rangle \\ &= \frac{e^{i(\theta+\pi/4)}}{\sqrt{2}}(|+i\rangle - i\,e^{-2i\theta}|-i\rangle), \end{aligned} \tag{5}$$

$$\begin{aligned} |+i\rangle &\to \frac{e^{i\theta}}{\sqrt{2}}|0\rangle + i\frac{e^{i\theta}}{\sqrt{2}}|1\rangle \\ &= \frac{e^{i(\theta+\pi/4)}}{\sqrt{2}}(|+\rangle - i|-\rangle) = e^{i\theta}|+i\rangle, \end{aligned} \tag{6}$$

$$\begin{aligned} |-i\rangle &\to \frac{e^{-i\theta}}{\sqrt{2}}|0\rangle - i\frac{e^{-i\theta}}{\sqrt{2}}|1\rangle = \frac{e^{-i(\theta+\pi/4)}}{\sqrt{2}}(|+\rangle + i|-\rangle) \\ &= e^{-i\theta}|-i\rangle. \end{aligned} \tag{7}$$

Collective-rotation noise introduces bit-flip errors in the $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ bases, and phase in the $\{|+i\rangle,|-i\rangle\}$ basis. The weighted sum of the bit-flip errors gives the quantum bit error rate, which can be defined as the probability that a randomly selected qubit sent by Alice arrives flipped, that is, $|0\rangle$ as $|1\rangle$, $|+\rangle$ as $|-\rangle$, $|+i\rangle$ as $|-i\rangle$ and vice versa. According to Eqs. (2)–(7) the noise flips the states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ with probability $\sin^2\theta$ and $|+i\rangle$, $|-i\rangle$ with probability 0. As a result of Alice selecting and transmitting each of the six states with probability $p = 1/6$, the collective-rotation noise in the channel results in a quantum bit error rate given by

$$Q_0 = \frac{1}{6}(4\sin^2\theta) = \frac{2}{3}\sin^2\theta. \tag{8}$$

The QBER is an important parameter in quantum cryptography, it is used to investigate the security of QKD protocols. The QBER gives the ratio of signals for which Alice and Bob chose the same encoding but where Bob got a measurement outcome different from what Alice prepared.[2] It is customary to define a parameter $\varepsilon = Q_0$ as the channel noise level.[25] We, however, choose not to attach any operational definition but rather use $\varepsilon = Q_0 = 2/3\sin^2\theta$ to simplify expressions whenever it is convenient to do so. We note the periodic nature of Q_0.

4. Security analysis

To perform an intercept-resend attack,[56] Eve randomly measures qubits sent by Alice in any one of the three bases. She then forwards, to Bob, qubits prepared in states corresponding to her measurement outcomes.[2] Given an ordered set $S = \{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+i\rangle,|-i\rangle\}$ of the possible states of the qubits, the effect of Eve's actions can be represented by the following probability transition matrix:

$$P_{E|A}=\begin{pmatrix} \frac{\cos^2(\theta)}{3} & \frac{\sin^2(\theta)}{3} & \frac{1}{6}(1-\sin(2\theta)) & \frac{1}{6}(\sin(2\theta)+1) & \frac{1}{6} & \frac{1}{6} \\ \frac{\sin^2(\theta)}{3} & \frac{\cos^2(\theta)}{3} & \frac{1}{6}(\sin(2\theta)+1) & \frac{1}{6}(1-\sin(2\theta)) & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6}(\sin(2\theta)+1) & \frac{1}{6}(1-\sin(2\theta)) & \frac{\cos^2(\theta)}{3} & \frac{\sin^2(\theta)}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6}(1-\sin(2\theta)) & \frac{1}{6}(\sin(2\theta)+1) & \frac{\sin^2(\theta)}{3} & \frac{\cos^2(\theta)}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{3} \end{pmatrix}, \tag{9}$$

where the elements in the matrix can be interpreted as the conditional probabilities $p(e|a)$ that Eve obtains a certain state given that Alice prepares a certain state. The joint probability $p(a,e)$ that Alice prepares a state $|\psi\rangle_A \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$ and Eve obtains a state $|\psi\rangle_E \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$ is given by

$$p(a,e)=p(e|a)p(a)=p(a|e)p(e), \tag{10}$$

where $p(a)=1/6$ is the probability that Alice prepares a state $|\psi\rangle_A \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$ and $p(e)=1/6$ is the probability that Eve obtains measurement outcomes corresponding to a state $|\psi\rangle_E \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\mathrm{i}\rangle,|-\mathrm{i}\rangle\}$. It follows that $p(a|e)=p(e|a)$. The summary of the joint probabilities is given in Table 2. The amount of information Eve gains from each measurement is given by the mutual information

$$I(A:E)=H(A)-H(A|E), \tag{11}$$

where

$$H(A)=-\sum p(i)\log_2 p(i)=-\sum\frac{1}{6}\log_2\frac{1}{6}=-\log_2\frac{1}{6}, \tag{12}$$

and

$$\begin{aligned} &H(A|E)\\ &=-\sum_{a,e}p(a,e)\log_2 p(a|e)\\ &=-\left(\frac{2\cos^2\theta}{9}\log_2\frac{\cos^2\theta}{3}+\frac{2\sin^2\theta}{9}\log_2\frac{\sin^2\theta}{3}\right.\\ &\quad+\frac{1-\sin 2\theta}{9}\log_2\frac{1-\sin 2\theta}{6}+\frac{1+\sin 2\theta}{9}\log_2\frac{1+\sin 2\theta}{6}\\ &\quad\left.+\frac{4}{9}\log_2\frac{1}{6}+\frac{1}{9}\log_2\frac{1}{3}\right). \end{aligned} \tag{13}$$

Table 2. Summary of joint probabilities of Alice preparing certain states and Eve obtaining measurement outcomes corresponding to each of the six states on qubits sent by Alice.

Alice sends	Eve obtains					
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\mathrm{i}\rangle$	$\|-\mathrm{i}\rangle$
$\|0\rangle$	$(\cos^2\theta)/18$	$(\sin^2\theta)/18$	$(1-\sin 2\theta)/36$	$(1+\sin 2\theta)/36$	1/36	1/36
$\|1\rangle$	$(\sin^2\theta)/18$	$(\cos^2\theta)/18$	$(1+\sin 2\theta)/36$	$(1-\sin 2\theta)/36$	1/36	1/36
$\|+\rangle$	$(1+\sin 2\theta)/36$	$(1-\sin 2\theta)/36$	$(\cos^2\theta)/18$	$(\sin^2\theta)/18$	1/36	1/36
$\|-\rangle$	$(1-\sin 2\theta)/36$	$(1+\sin 2\theta)/36$	$(\sin^2\theta)/18$	$(\cos^2\theta)/18$	1/36	1/36
$\|+\mathrm{i}\rangle$	1/36	1/36	1/36	1/36	1/18	0
$\|-\mathrm{i}\rangle$	1/36	1/36	1/36	1/36	0	1/18

To simplify Eq. (11), we let $\varepsilon=2/3\sin^2\theta$; implying that ε can take values in the interval $[0,2/3]$. Substituting ε into Eq. (11), reduces the equation to the following:

$$\begin{aligned} &I(A:E)\\ &=-\frac{5}{9}\log_2\frac{1}{6}+\frac{1}{9}\log_2\frac{1}{3}+\frac{2-3\varepsilon}{9}\log_2\frac{2-3\varepsilon}{6}+\frac{\varepsilon}{3}\log_2\frac{\varepsilon}{2}\\ &\quad+\frac{1-\sqrt{3\varepsilon(2-3\varepsilon)}}{9}\log_2\frac{1-\sqrt{3\varepsilon(2-3\varepsilon)}}{6}\\ &\quad+\frac{1+\sqrt{3\varepsilon(2-3\varepsilon)}}{9}\log_2\frac{1+\sqrt{3\varepsilon(2-3\varepsilon)}}{6}. \end{aligned} \tag{14}$$

The variation of mutual information $I(A:E)$ with rotation angle θ is shown in Fig. 2.

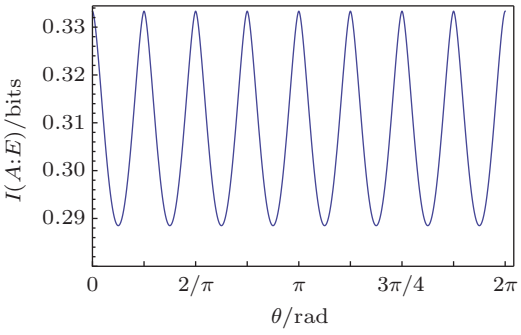


Fig. 2. (color online) Variation of the mutual information between Alice and Eve ($I(A:E)$) as a function of the collective-rotation angle θ.

We analyze the following two intercept-resend strategies that could be employed by Eve.

(I) Eve breaks the quantum channel between Alice and Bob and inserts both of her devices in between, as illustrated in Fig. 3(a).

(II) 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,[56] as illustrated in Fig. 3(b).

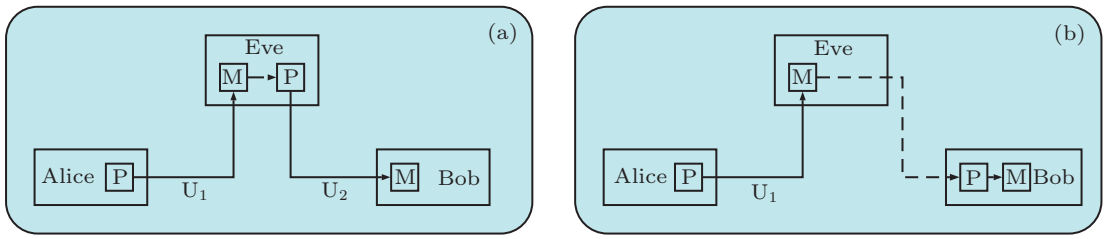


Fig. 3. (color online) Schematics of the two intercept-resend attack strategies. Quantum channels are represented by continuous arrows, while dashed arrows represent lossless classical channels. Letters P and M denote preparation and measurement devices, respectively. (a) Eve breaks the quantum channel between Alice and Bob and inserts both of her devices in between. (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 transition probability matrices describing the transition between the states prepared by Eve and the states obtained by Bob are given by

$$P_{B|E}=\begin{pmatrix} \frac{\cos^2(\phi)}{3} & \frac{\sin^2(\phi)}{3} & \frac{1}{6}(1-\sin(2\phi)) & \frac{1}{6}(\sin(2\phi)+1) & \frac{1}{6} & \frac{1}{6} \\ \frac{\sin^2(\phi)}{3} & \frac{\cos^2(\phi)}{3} & \frac{1}{6}(\sin(2\phi)+1) & \frac{1}{6}(1-\sin(2\phi)) & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6}(\sin(2\phi)+1) & \frac{1}{6}(1-\sin(2\phi)) & \frac{\cos^2(\phi)}{3} & \frac{\sin^2(\phi)}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6}(1-\sin(2\phi)) & \frac{1}{6}(\sin(2\phi)+1) & \frac{\sin^2(\phi)}{3} & \frac{\cos^2(\phi)}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{3} \end{pmatrix}, \tag{15}$$

and

$$P_{B|E}=\begin{pmatrix} \frac{1}{3} & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ 0 & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & 0 & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{3} \end{pmatrix}, \tag{16}$$

respectively. The matrix $P_{A,B}$ of the joint probabilities of Alice and Bob's states is obtained as follows:

$$P_{A,B}=\frac{1}{6}\times P_{E|A}\times P_{B|E}. \tag{17}$$

The summary of the joint probabilities is given in Table 3. For strategy (I), the elements in Table 3 are given by

$$a=\frac{\cos^2\theta}{18}\times\frac{\cos^2\phi}{3}+\frac{\sin^2\theta}{18}\times\frac{\sin^2\phi}{3}+\frac{1-\sin 2\theta}{36}\times\frac{1+\sin 2\phi}{6}+\frac{1+\sin 2\theta}{36}\times\frac{1-\sin 2\phi}{6}+\frac{1}{108}, \tag{18}$$

$$b=\frac{\cos^2\theta}{18}\times\frac{\sin^2\phi}{3}+\frac{\sin^2\theta}{18}\times\frac{\cos^2\phi}{3}+\frac{1-\sin 2\theta}{36}\times\frac{1-\sin 2\phi}{6}+\frac{1+\sin 2\theta}{36}\times\frac{1+\sin 2\phi}{6}+\frac{1}{108}, \tag{19}$$

$$c=\frac{\cos^2\theta}{18}\times\frac{1-\sin 2\phi}{6}+\frac{\sin^2\theta}{18}\times\frac{1+\sin 2\phi}{6}+\frac{1-\sin 2\theta}{36}\times\frac{\cos^2\phi}{3}+\frac{1+\sin 2\theta}{36}\times\frac{\sin^2\phi}{3}+\frac{1}{108}, \tag{20}$$

$$d=\frac{\cos^2\theta}{18}\times\frac{1+\sin 2\phi}{6}+\frac{\sin^2\theta}{18}\times\frac{1-\sin 2\phi}{6}+\frac{1-\sin 2\theta}{36}\times\frac{\sin^2\phi}{3}+\frac{1+\sin 2\theta}{36}\times\frac{\cos^2\phi}{3}+\frac{1}{108}, \tag{21}$$

$$g=\frac{1}{36},\quad h=\frac{1}{36},\quad i=\frac{1}{27},\quad j=\frac{1}{54}. \tag{22}$$

Table 3. Summary of the joint probabilities of Alice preparing certain states and Bob obtaining measurement outcomes corresponding to each of the six states, given an intercept-resent attack by Eve.

Eve sends	Bob receives					
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\mathrm{i}\rangle$	$\|-\mathrm{i}\rangle$
$\|0\rangle$	$(\cos^2\phi)/3$	$(\sin^2\phi)/3$	$(1-\sin 2\phi)/6$	$(1+\sin 2\phi)/6$	1/6	1/6
$\|1\rangle$	$(\sin^2\phi)/3$	$(\cos^2\phi)/3$	$(1+\sin 2\phi)/6$	$(1-\sin 2\phi)/6$	1/6	1/6
$\|+\rangle$	$(1+\sin 2\phi)/6$	$(1-\sin 2\phi)/6$	$(\cos^2\phi)/3$	$(\sin^2\phi)/3$	1/6	1/6
$\|-\rangle$	$(1-\sin 2\phi)/6$	$(1+\sin 2\phi)/6$	$(\sin^2\phi)/3$	$(\cos^2\phi)/3$	1/6	1/6
$\|+\mathrm{i}\rangle$	1/6	1/6	1/6	1/6	1/3	0
$\|-\mathrm{i}\rangle$	1/6	1/6	1/6	1/6	0	1/3
Alice sends	Bob receives					
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\mathrm{i}\rangle$	$\|-\mathrm{i}\rangle$
$\|0\rangle$	a	b	c	d	h	h
$\|1\rangle$	b	a	d	c	h	h
$\|+\rangle$	d	c	a	b	h	h
$\|-\rangle$	c	d	b	a	h	h
$\|+\mathrm{i}\rangle$	g	g	g	g	i	j
$\|-\mathrm{i}\rangle$	g	g	g	g	j	i

The terms c, d, g, and h in Table 3 go to zero during sifting. Therefore, the quantum bit error rate Q, after sifting, is given by

$$Q = \frac{4b+2j}{4(a+b)+2(i+j)} = \frac{4-\cos 2(\theta+\phi)}{9}. \tag{23}$$

The variation of the quantum bit error rate Q with rotation angles θ and ϕ is shown in Fig. 4.

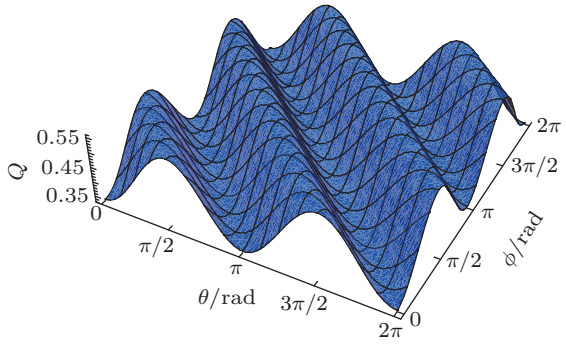


Fig. 4. (color online) Quantum bit error rate Q as a function of θ and ϕ.

In the special case where $\theta = \phi$, i.e., the noise in both channels is equal, the quantum bit error rate Q reduces to

$$Q_1 = \frac{3+2\sin^2 2\theta}{9}. \tag{24}$$

By performing an attack outlined in strategy (II), Eve attempts to minimise her quantum "footprint" by substituting collective-rotation noise channel with a lossless classical channel. It turns out that the strategy does not improve her odds of not being detected, as shown in Fig. 5. To derive the quantum bit error rate Q_2, we first compute the elements a–j in Table 3 using Eq. (17), where the matrices $P_{E|A}$ and $P_{B|E}$ are obtained from Eqs. (9) and (16), respectively. The elements g–j equate to the ones given in Eq. (22). However, the terms a–d evaluate to the following:

$$a = \frac{1+\cos^2\theta}{54}, \tag{25}$$

$$b = \frac{1+\sin^2\theta}{54}, \tag{26}$$

$$c = \frac{3-\sin 2\theta}{108}, \tag{27}$$

$$d = \frac{3+\sin 2\theta}{108}. \tag{28}$$

The terms c, d, g, and h vanish during sifting. Therefore, the quantum bit error rate Q_2 is given by

$$Q_2 = \frac{3+2\sin^2\theta}{9}. \tag{29}$$

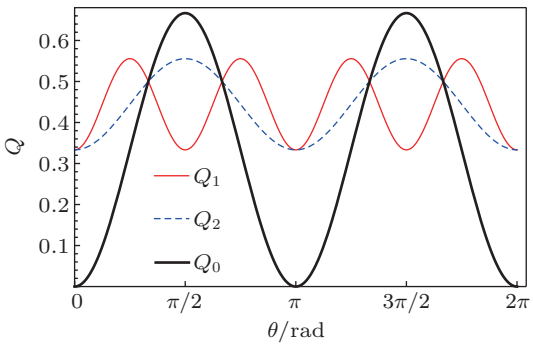


Fig. 5. (color online) Comparison of the variation of the quantum bit error rate Q with the rotation angle θ for the case where there is no eavesdropping (Q_0), the case where the eavesdropper performs the attack outlined in strategy (I) (Q_1) and the case where the eavesdropper performs the attack outlined in strategy (II) (Q_2).

Alice and Bob attribute quantum bit error rate above a predetermined value to eavesdropping. From Fig. 5, a quantum bit error rate above 0.3333 indicates the possibility of eavesdropping, rendering the channel unsafe for cryptographic purposes. In practice, the channel quantum bit error rate is

kept far below this threshold because the overall quantum bit error rate budget has to take into account all sources of error. For unconditional security this budget is capped at 12.6%, see Ref. [18] for the unconditional security proof of the six-state protocol, further suggesting that only collective-rotation noise channels with rotation angle (in radians)

$$\theta = n\pi \pm \delta, \tag{30}$$

where n is an integer and $\delta < 0.450$ radians, are suitable for six-state quantum cryptography.

5. Conclusion

We have demonstrated how the six-state QKD protocol responds to collective-rotation noise. From the analysis, we note that the six-state protocol is robust against collective-rotation noise for small rotation angles. We attribute this result to the symmetry of the protocol. We also note that the third basis $\{|+\mathrm{i}\rangle, |-\mathrm{i}\rangle\}$ is rotation invariant under collective-rotation noise thus reducing the quantum bit error rate. We recommend the six-state protocol for QKD implementations where collective-rotation noise is dominant in the communication channel.

References

[1] Bennett C and Brassard G 1984 *Quantum Cryptography: Public Key Distribution and Coin Tossing*, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* Vol. 175 (Bangalore, India)

[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Diffie W and Hellman M E 1976 *IEEE Trans. Inform. Theory* **22** 644

[4] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120

[5] Wootters W K and Zurek W H 1982 *Nature* **299** 802

[6] Heisenberg W 1927 *Zeitschrift für Physik* **43** 172

[7] Busch P, Heinonen T and Lahti P 2007 *Phys. Rep.* **452** 155

[8] Nielsen M and Chuang I 2002 *Quantum Computation and Quantum Information*

[9] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

[10] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[11] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[12] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[13] Mayers D 1996 *Quantum Key Distribution and String Oblivious Transfer in Noisy Channels*, *Advances in Cryptology-CRYPTO'*96 (Springer) pp. 343–357

[14] Devetak I and Winter A 2005 *Distillation of Secret Key and Entanglement from Quantum States*, *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* Vol. 461 (The Royal Society) pp. 207–235

[15] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 80501

[16] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 12332

[17] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[18] Lo H K 2001 *Quantum Inf. Comput.* **1** 81

[19] Tamaki K, Koashi M and Imoto N 2003 *Phys. Rev. Lett.* **90** 167904

[20] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[21] Hughes R J, Morgan G L and Peterson C G 2000 *J. Mod. Opt.* **47** 533

[22] Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes J, *et al.* 2009 *New J. Phys.* **11** 075001

[23] Mirza A and Petruccione F 2010 *JOSA B* **27** A185

[24] Namekata N, Takesue H, Honjo T, Tokura Y and Inoue S 2011 *Opt. Express* **19** 10632

[25] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, *et al.* 2011 *Opt. Express* **19** 10387

[26] Stucki D, Legré M, Buntschu F, Clausen B, Felber N, Gisin N, Henzen L, Junod P, Litzistorf G, Monbaron P, *et al.* 2011 *New J. Phys.* **13** 123001

[27] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[28] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326

[29] http://www.idquantique.com

[30] http://www.magiqtech.com

[31] Xiu X M, Dong L, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 4171

[32] Tamaki K, Koashi M and Imoto N 2003 *Phys. Rev. A* **67** 032310

[33] Tamaki K and Lütkenhaus N 2004 *Phys. Rev. A* **69** 032316

[34] Mertz M, Kampermann H, Shadman Z and Bruß D 2013 *Phys. Rev. A* **87** 042312

[35] Wang X B 2005 *Phys. Rev. A* **72** 050304

[36] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321

[37] Gu B, Pei S, Song B and Zhong K 2009 *Science in China Series G: Physics, Mechanics and Astronomy* **52** 1913

[38] Dong L, Xiu X M, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 1688

[39] Yang C W and Hwang T 2012 *Int. J. Theor. Phys.* **51** 3941

[40] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018

[41] Phoenix S J, Barnett S M and Chefles A 2000 *J. Mod. Opt.* **47** 507

[42] Boileau J, Tamaki K, Batuwantudawe J, Laflamme R and Renes J 2005 *Phys. Rev. Lett.* **94** 40503

[43] Mafu M, Garapo K and Petruccione F 2014 *Phys. Rev. A* **90** 032308

[44] Senekane M, Mafu M and Petruccione F 2015 *J. Quantum Inf. Sci.* **5** 33

[45] Bruß D and Macchiavello C 2002 *Phys. Rev. Lett.* **88** 127901

[46] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev. A* **59** 4238

[47] Bourennane M, Karlsson A and Björk G 2001 *Phys. Rev. A* **64** 012306

[48] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theory* **49** 457

[49] Renner R 2008 *Inte. J. Quantum Inf.* **6** 1

[50] Cai R and Scarani V 2009 *New J. Phys.* **11** 045024

[51] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[52] Shadman Z, Kampermann H, Meyer T and Bruss D 2009 *Int. J. Quantum Inf.* **07** 297

[53] Żukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287

[54] Li J, Chen Y H, Pan Z S, Sun F Q, Li N and Li L L 2016 *Acta Phys. Sin.* **65** 30302 (in Chinese)

[55] Li J, Pan Z, Zheng J, Sun F, Ye X and Yuan K 2015 *Chin. J. Electron.* **24** 689

[56] Curty M and Lütkenhaus N 2005 *Phys. Rev. A* **71** 062301