5
Decoherence can help quantum cryptographic security

5.1 Introduction

Cryptography helps secure information being communicated between legitimate users [Gisin et al., 2002; Srinatha et al., 2014] across a quantum communication channel [Sharma, 2016; Sharma et al., 2015, 2016b; Sharma and Sharma, 2014], which may be optical, open space or satellite-based [Wang et al., 2014; Sharma and Banerjee, 2017]. Since the seminal BB84 quantum key distribution (QKD) proposal [Bennett and Brassard, 1984], the idea that unconditional security of the distributed key can be obtained by using quantum resources has been extensively studied through more detailed security analyses and newer QKD protocols [Long and Liu, 2002], among them [Ekert, 1991; Bennett, 1992; Goldenberg and Vaidman, 1995; Lo and Chau, 1999; Scarani and Gisin, 2001; Lo et al., 2005a; Scarani et al., 2009]. See Refs. [Pathak, 2013] and [Shenoy-Hejamadi et al., 2017] and references therein.

A variant of QKD is one involving direct communication avoiding the step of key generation [Deng and Long, 2004a]. These protocols may be classified as QSDC (quantum secure direct communication) [Boström and Felbinger, 2002; Lucamarini and Mancini, 2005; Shukla et al., 2012] and DSQC (deterministic secure quantum communication) protocols. The difference is that, unlike DSQC protocols, QSDC protocols don't require any additional classical communication, except for checking eavesdropping. Other important cryptotasks under active investigation include quantum coin flipping [Pappa et al., 2011], quantum money [Amiri and Arrazola, 2017], quantum private query [Wei et al., 2017], quantum secure computation [Shi et al., 2016].

Environmental noise is ubiquitous in the real world, and is generally detrimental to quantum communication [Banerjee and Srikanth, 2008b; Srikanth and Banerjee, 2008; Banerjee and Ghosh, 2007b; Omkar et al., 2013]. In quantum key distribution, it is conservative to assume that all of the noise is due to an eavesdropper Eve, who replaces the noisy (and/or lossy) channel with an ideal one [Adhikari et al., 2015]. Eve is assumed to be as powerful as the laws of physics would allow. This determines the largest noise level that can be tolerated. In reality, we may expect that Eve, too, to be restricted by the noise. Alice, Bob and Eve may be assumed to be aware of this. As the legitimate and eavesdropping channels are not identical, this scenario of noise-restricted Eve gives rise to the interesting possibility that noise may be more disadvantageous for Eve than for Alice and Bob. Here we shall present a concrete instance of such a situation. This can be trivially ensured by making the eavesdropping channel more noisy than Alice's and Bob' communication channel. A more non-trivial scenario is one where the noisy channel acts directly only on the communication channel and not on the eavesdropping channel. On the other hand, Eve is assumed to be unable to replace the noisy channel of Alice and Bob with an ideal one. Our main result is the demonstration of a quantum key distribution (QKD) situation where non-unital noise can be beneficial to

the legitimate participants in this sense, whereas unital noise is detrimental to them. This can potentially form the basis for"trusted noise", wherein Alice and Bob add noise prior to classical post-processing to improve the protocol's security or performance. Interestingly, such an application of noise for QKD has been noted earlier. In particular, in an analysis of various QKD protocols, [Renner et al., 2005] shows that they can be made more robust against channel noise by the addition of noise by Alice or Bob to the measurement data prior to key reconciliation. Refs. [Pirandola et al., 2009; García-Patrón and Cerf, 2009] discuss adding noise to the signal to improve noise tolerance in the context of continuous-variable QKD over Gaussian channels. Interestingly, a somewhat similar favorable effect of noise on quantum information processing was noted in [Banerjee et al., 2008].
Secure direct communication (SDC) is a stronger form of secure communication than key distribution wherein message bits, rather than random key bits, are transmitted from sender Alice to receiver Bob. Since the proposal of the first quantum SDC protocol, namely the Ping-pong protocol [Boström and Felbinger, 2002], a number of other realizations of this theme have been proposed [Long et al., 2007; Wang et al., 2005a; Deng and Long, 2004b; Ting et al., 2005; Wang et al., 2005b; Li et al., 2005; Jin et al., 2006; Zhong-Xiao and Yun-Jie, 2007]. The Ping-Pong protocol's security, as well as its modified versions, have been extensively studied by various other authors [Wójcik, 2003; Han et al., 2014; Zawadzki, 2012c,b; Cai and Li, 2004b,a; Cai, 2006; Zawadzki and Miszczak, 2016; Li et al., 2012; Zawadzki, 2012a; Zhang et al., 2004; Wang et al., 2005a; Vasiliu, 2011; Chamoli and Bhandari, 2009]. A comprehensive review of some of the attacks and protective measures against them are discussed by the authors of the Ping-pong protocol Boström and Felbinger [2008].

The original Ping-pong protocol is based on two modes: the message mode during which a bit is transmitted deterministically, and control mode, to monitor eavesdropping. This structure is necessitated by the requirement for the protocol to perform as a scheme for SDC. Here, however, we will use a simplified version of the Ping-pong protocol (though it will still be called as such), which is suitable for key distribution, but in general not for SDC. This is done by dropping the control mode, and instead using a quantum bit error rate (QBER) analysis (which involves sacrficing some otherwise secret bits) for detecting eavesdropping.

For our purpose, it will suffice to consider the depolarizing and AD (amplitude damping) channels, representative of unital channels (those that map the identity operator to itself) and non-unital channels, respectively. Furthermore, the noise acts only on the communication channel and not directly on the eavesdropping channel, so that Eve is affected only by the interaction of her probes with the noisy communication channel, rather than noise acting on her probes directly. In this scenario, the semi-powerful Eve is able to deploy noiseless probes, but unable to replace Alice-Bob's noisy channel with a noiseless one.

In quantum key distribution, one conservatively assumes that the eavesdropper Eve is restricted only by physical laws, whereas the legitimate parties, namely the sender Alice and receiver Bob, are subject to realistic constraints, such as noise due to environment-induced decoherence. In practice, Eve too may be bound by the limits imposed by noise, which can give rise to the possibility that decoherence works to the advantage of the legitimate parties. A particular scenario of this type is one where Eve can't replace the noisy communication channel with an ideal one, but her eavesdropping channel itself remains noiseless. Here, we point out such a situation, where the security of the Ping-Pong protocol (modified to a key distribution scheme) against a noise-restricted adversary improves under a non-unital noisy channel, but deteriorates under unital channels. This highlights the surprising fact

that, contrary to the conventional expectation, noise can be helpful to quantum information processing. Furthermore, we point out that the measurement outcome data in the context of the non-unital channel can't be simulated by classical noise locally added by the legitimate users.

[1] The remaining work is divided as follows. In Section 5.2, we briefly review the Ping-Pong protocol reformulated as a QKD (rather than SDC) scheme, and an attacking strategy on it [Wójcik, 2003]. In Section 5.3, we introduce the noise scenario used in this work. In Sections 5.3.1 and 5.3.2, we study the performance of the (modified) Ping-Pong protocol in the presence of the AD and depolarizing channels, respectively, pointing out the (surprisingly) beneficial aspect of the former. The question of the simulation of the measurement outcome data under a noisy channel by the resource of local classical noise applied by the legitimate users, is considered in the concluding Section 5.4.

5.2 Eavesdropping on the Ping-Pong protocol

First, we briefly describe the (modified) Ping-Pong key distribution protocol, based on the original secure deterministic communication protocol [Boström and Felbinger, 2002]. In what follows, we use the notation where $|0\rangle$ and $|1\rangle$ represent the two polarization states H and V of a single photon, respectively, whilst $|2\rangle$ represents the vacuum state.

1. Bob transmits to Alice one half (the "travel qubit") of the Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

2. Alice encodes one bit of information by applying operation I (resp., Pauli σ_Z), corresponding to the bit value $a = 0$ (resp., $a = 1$).

3. She retransmits the travel qubit back to Bob.

4. The two-qubit state now left with Bob is ideally in one the Bell states $|\psi^\pm\rangle$, which is determined by Bob by a Bell-state measurement.

5. For a sufficiently large set of the (noisy) shared bits, Alice announces the encoded bit on some of the transmissions. The fraction of bits where Alice's and Bob's records differ determines the quantum bit error rate (QBER). If the QBER is below a threshold value, they proceed to distill a secret key. Else, they abort.

Wöjcik proposed an eavesdropping strategy on the original ping-pong protocol, which is now adapted for the modified Ping-pong protocol. The basic intuition of security in the Ping-pong protocol is that the travel qubit remains always in the maximally mixed state, irrespective of Alice's encoding. The subtlety of Wöjcik's attack is that by making the probe interact before and after the encoding, Eve is able to extract some information about the encoding. A brief description of the attack adapted to the above protocol is enumerated below.

1. Eve prepares two probes x and y in the state $|2\rangle_x|0\rangle_y$, where $|2\rangle$ is the vacuum state. Thus, the combined initial quantum state with Bob and Eve is $|\psi^{\text{initial}}\rangle = |\psi^+\rangle_{ht}|2\rangle_x|0\rangle_y$.

2. In the onward leg, Eve attacks the travel qubit by applying $Q_{txy} = SWAP_{tx}CPBS_{txy}H_y$,

[1] This chapter is based on [Sharma et al., 2018]

with CPBS being the controlled polarization beam splitter operation, given by:

$$\left.\begin{array}{l}|020\rangle\\|021\rangle\\|120\rangle\\|121\rangle\end{array}\right\} \xrightarrow{CPBS} \left\{\begin{array}{l}|002\rangle\\|021\rangle\\|120\rangle\\|112\rangle\end{array}\right. \tag{5.1}$$

3. After Alice has encoded her bit on the travel qubit and she returns it, Eve applies the operation Q_{txy}^{-1} on the travel qubit and forwards it to Bob.

Eve then obtains some information about Alice's encoding by measuring her probes. To see how the attack works, we note that after Bob has received back the attacked travel qubit, the final state of the Alice-Bob-Eve system is

$$|\psi^a\rangle_{htxy} = \frac{1}{\sqrt{2}}(|012a\rangle + |1020\rangle). \tag{5.2}$$

From this, one finds that the only non-vanishing probabilities P_{AEB} are

$$\begin{aligned} P_{000} &= \frac{1}{2} \\ P_{100} = P_{101} &= P_{110} = P_{111} = \frac{1}{8}. \end{aligned} \tag{5.3}$$

This corresponds to a QBER of $\sum_e (p_{0e1} + p_{1e0}) = \frac{1}{4}$. Using these, one may compute the mutual information between Alice and Bob, $I_{AB} \equiv H(A) - H(A|B)$, where $H(A)$ and $H(A|B)$ are the classical (Shannon) entropy associated with probability distribution $P(a)$ and the conditional probability distribution $P(a|b)$ [Nielsen and Chuang, 2010]. This is a measure of entropic correlation between Alice and Bob. Similarly, one defines the mutual information between Alice and Eve, given by $I_{AE} \equiv H(A) - H(A|E)$. From (5.3), one then finds that [Wójcik, 2003]

$$I_{AB} = I_{AE} = \frac{3}{4}\log_2\frac{4}{3} \approx 0.311. \tag{5.4}$$

Thus, the attack makes the protocol insecure, since security (with one-way communication) requires that $I_{AB} > I_{AE}$. This attack is not symmetric between $a = 0$ and $a = 1$, and [Wójcik, 2003] proposes another, symmetric attack. Ref. [Cai, 2004] discusses a number of other attacks on the Ping-pong protocol, showing it to be effectively robust against them. Thus, while the attack described is not known to be optimal, it represents a powerful and well-studied attack, and its performance under decoherence is likely to carry general implications of a wider nature, in particular the occurrence of the "trusted noise" scenario. Therefore, our present work is focused on studying this aspect of it. Furthermore, it is generally difficult to prove the security of a given QKD protocol against the most general (collective) attacks, though, specific protocols can be proposed where such security can be proven. Under the circumstances, a reasonable approach is to prove security against a non-general, but sufficiently powerful and sophisticated attack, which is the case here.

5.3 Quantum communication under a noisy environment

The action of noise manifesting as a completely positive (CP) map on a system's density operator, can be given a Kraus representation:

$$\phi(\rho) = \sum_i A_i \rho A_i^\dagger, \tag{5.5}$$

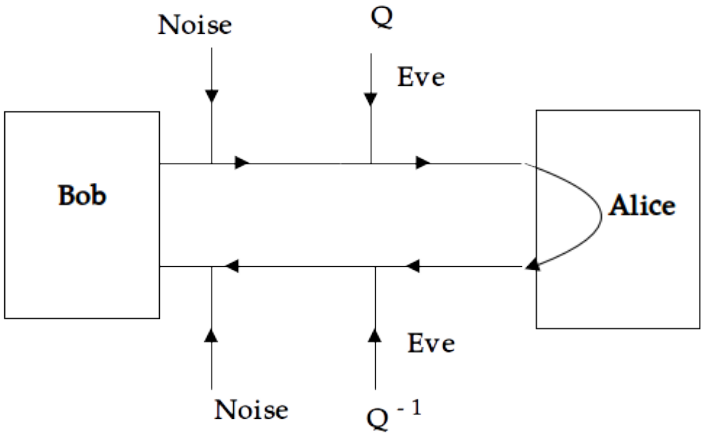

Figure 5.1: Scenario of noise and attack as used in this work: Bob transmits to Alice one half of a Bell state, on which Alice encodes her bit by applying either the operation I or σ_Z, before returning it to Bob. The action of noise is idealized as acting before Eve's action Q in the onward leg and after her action Q^{-1} in the return leg.

where the $A_i's$ must conform to the completeness constraint $\sum_i A_i^\dagger A_i = I$. In this work, we choose the simplified noise scenario depicted in Figure 5.1. In the onward leg, the noise first acts on the travel qubit, followed by Eve's attack Q on this qubit, and then by Alice's encoding operation. In the return leg, this sequence is time-reversed, so that Eve's second attack Q^{-1} is followed by the noise, before receipt of the travel qubit and decoding of the two-qubit state by Bob. In a noisy channel, suppose bits 0 and 1 correspond to noisy states $\rho^{a=0}$ and $\rho^{a=1}$. Then, the mutual information between Alice and Bob is upper-bounded by the Holevo bound:

$$\chi = S\left(\frac{\rho_{\rm ht}^{a=0} + \rho_{\rm ht}^{a=1}}{2}\right) - \frac{1}{2}\left[S\left(\rho_{\rm ht}^{a=0}\right) + S\left(\rho_{\rm ht}^{a=1}\right)\right], \tag{5.6}$$

where $S(\rho) \equiv -\mathrm{Tr}[\rho \log(\rho)]$ denotes the von-Neumann entropy. We next consider noisy conditions with Eve's above attack on the Ping-Pong QKD protocol, with the travel qubit subjected to the amplitude damping (AD) [Srikanth and Banerjee, 2007] and depolarizing channels.

5.3.1 Amplitude-Damping Noise

The Kraus operators for AD channel are [Srikanth and Banerjee, 2008]:

$$E_0^A = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix};\ E_1^A = \begin{bmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{bmatrix}, \tag{5.7}$$

where p is the noise parameter, sometimes called the decoherence rate, and $0 \leq p \leq 1$. The first attack of [Wójcik, 2003] (during the onward leg) makes the channel lossy and involves creating the vacuum state of the travel photon. This necessitates extending the qubit noise model (5.7) to that of a qutrit. There is no unique way to do this. We use the extension represented by the following Kraus operators:

$$E_0^A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sqrt{1-p} & 0 \\ 0 & 0 & 1 \end{bmatrix};\ E_1^A = \begin{bmatrix} 0 & \sqrt{p} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tag{5.8}$$

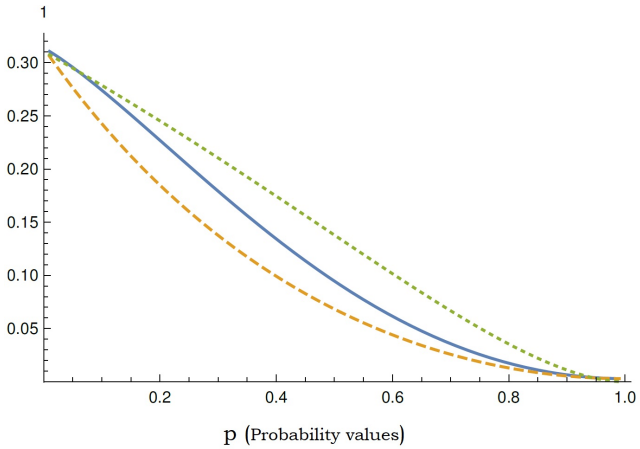

Figure 5.2: (Color online) Performance of the modified Ping-pong protocol under AD noise: The bold (blue), dashed (red) and dotted (green) plots represents I_{AB}, I_{AE} and the Holevo bound for Alice-Bob. That $I_{AB} > I_{AE}$ for $0 < p \leq 1$ implies that noise is beneficial to the legitimate users. In the noiseless limit, the Holevo bound coincides with I_{AB}, implying that the measurement strategy is optimal.

which essentially implements the AD noise Eq. (5.7) on the polarization Hilbert space and does nothing to the vacuum state. Here the vacuum state is taken to be the third dimension, denoted $|2\rangle$. When the photon returns back to Bob, the state of the system hty for either encoding 'a' can be shown to have support of dimensionality 4, spanned by the states $|010\rangle, |100\rangle, |011\rangle$ and $|000\rangle$, with the state of the x particle being $|2\rangle$, as in the noiseless attack case. The final states with Bob-Eve for the encodings $a = 0$ and $a = 1$ are:

$$\rho_{hty}^{a=0} = \frac{1}{2}\begin{pmatrix} (1-p)^2 & 1-p & 0 & 0 \\ 1-p & 1 & 0 & 0 \\ 0 & 0 & p(2-p) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$
$$\rho_{hty}^{a=1} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1-p \\ 0 & 0 & p(2-p) & 0 \\ 0 & 1-p & 0 & (1-p)^2 \end{pmatrix}. \tag{5.9}$$

From Eq. (5.9), we obtain the following joint probabilities p_{AEB}, in place of Eq. (5.3):

$$\begin{aligned} P_{000} &= \frac{1}{8}(2-p)^2 \\ P_{001} &= \frac{p^2}{8} \\ P_{002} &= P_{003} = P_{102} = P_{103} = \frac{1}{8}(2-p)p \\ P_{110} &= P_{111} = \frac{1}{8}(1-p)^2 \\ P_{010} &= P_{011} = P_{012} = P_{013} = 0 \\ P_{100} &= P_{101} = \frac{1}{8}, \end{aligned} \tag{5.10}$$

with all other joint probability terms vanishing. Note that in the presence of AD noise, Bob will also obtain outcomes $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ in his Bell state measurement, which corresponds to the outcome symbols 2 and 3 in Eq. (5.10).

From the above probabilities P_{AEB}, one derives the mutual information between Alice and Bob and that between Alice and Eve, to be

$$\begin{aligned} I(A:B) = \frac{1}{8}\Bigg[& p\left(p\log\left(\frac{p^2}{2p^2-2p+2}\right) + p\log\left(\frac{8(p-2)^2}{(p-3)p+3}\right) + (p-2)\log\left(\frac{(p-2)p+2}{(p-1)p+1}\right)\right. \\ & \left. + (p-2)\log\left(\frac{p-1}{(p-3)p+3}+1\right)\right) - 2p(p+2)\log(2) - 4(p-1)\log\left(\frac{(p-2)^2}{2((p-3)p+3)}\right. \\ & + 2\log\left(\frac{(p-2)p+2}{(p-1)p+1}\right) + 2\log\left(\frac{p-1}{(p-3)p+3}+1\right) + 4\Bigg], \end{aligned} \tag{5.11}$$

and

$$\begin{aligned} I(A:E) = \frac{1}{8}\Bigg(& 6 + 2\log\left(\frac{1}{-p^2+2p+3}\right) \\ & + (1-(p-2)p)\log\left(\frac{(p-2)p-1}{(p-3)(p+1)}\right)\Bigg), \end{aligned} \tag{5.12}$$

respectively. These two quantities are depicted as a function of noise p in Figure 5.2. This shows that under the AD channel, there is a positive key rate $\kappa \equiv I_{AB} - I_{AE}$ for finite noise. It is as if the symmetry existing between Bob and Eve in terms of information gained, is broken by the noise, to the advantage of Alice and Bob. This is a surprising result, and implies that Alice and Bob will find this type of noise beneficial in this eavesdropping scenario.

If Alice and Bob are employing the original Ping-pong strategy and the eavesdropper is known to employ the above attack, then in the noise range $0 < p < 1$, Alice and Bob know that they can extract a finite secret key, after suitable privacy amplification.

From Eq. (5.9) one obtains the reduced density operators for the particles ht:

$$\begin{aligned} \rho_{ht}^{a=0} &= \tfrac{1}{2}\begin{pmatrix} (1-p)^2 & 1-p & 0 \\ 1-p & 1 & 0 \\ 0 & 0 & p(2-p) \end{pmatrix}; \\ \rho_{ht}^{a=1} &= \tfrac{1}{2}\begin{pmatrix} (1-p)^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p(2-p) \end{pmatrix}. \end{aligned} \tag{5.13}$$

in the basis $\{|01\rangle, |10\rangle, |00\rangle\}$. The maximum information Bob can receive is upper-bounded by the Holevo quantity (5.6). To obtain this, we note that the eigenvalues λ_j^0, λ_j^1 and λ_j^{01} for the density operators $\rho_{ht}^{a=0}, \rho_{ht}^{a=1}$ and their equal average, are:

$$\begin{aligned} \lambda_j^0 &= \left\{0, -\frac{1}{2}(p-2)p, \frac{1}{2}((p-2)p+2)\right\} \\ \lambda_j^1 &= \left\{\frac{1}{2}, \frac{1}{2}(p-1)^2, -\frac{1}{2}(p-2)p\right\} \\ \lambda_j^{01} &= \left\{\frac{(2-p)}{2}p, \frac{1}{4}\left((p-2)p \pm \sqrt{(p-2)p(p-1)^2+1}+2\right)\right\} \end{aligned} \tag{5.14}$$

The Holevo bound (5.6) is thus given by:

$$\chi_{AD} = h\left[\lambda_j^{01}\right] - \frac{1}{2}\left(h\left[\lambda_j^{0}\right] + h\left[\lambda_j^{1}\right]\right), \tag{5.15}$$

where $h\left[\lambda_j^{\alpha}\right] = -\sum_{j=0}^{2} \lambda_j^{\alpha} \log_2\left(\lambda_j^{\alpha}\right)$. The quantity χ_{AD} is plotted in Figure 5.2.

That the Holevo bound exceeding I_{AB} here suggests that Bob's Bell state measurement strategy, although guaranteeing a positive key rate, is sub-optimal. Note that it is indeed optimal in the noiseless case.

5.3.2 Depolarizing noise

Consider the travel qubit subjected to depolarizing noise. This noise is characterized by the transformation $\rho \longrightarrow p\frac{\mathbb{I}}{2} + (1-p)\rho$ [Nielsen and Chuang, 2000; Omkar et al., 2013], for which the Kraus operators are:

$$\begin{aligned} D_0 &= \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, D_1 = \sqrt{\frac{p}{3}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \\ D_2 &= \sqrt{\frac{p}{3}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, D_3 = \sqrt{\frac{p}{3}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \end{aligned} \tag{5.16}$$

where $p = (1 - \exp^{-\frac{\tau t}{2}})$, τ being the decay factor. Here we shall use the extension of Eq. (5.16) given by:

$$\begin{aligned} D_0 &= \sqrt{1-p}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, D_1 = \sqrt{\frac{p}{3}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \\ D_2 &= \sqrt{\frac{p}{3}}\begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, D_3 = \sqrt{\frac{p}{3}}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned} \tag{5.17}$$

which essentially implements a depolarizing noise on the polarization Hilbert space and does nothing to the vacuum state. When the photon returns back to Bob, as per the scenario of Figure 5.1, with the noise given by the depolarizing channel, the state of the system hty for either encoding a can be shown to have support of dimensionality 8, spanned by the states $|jkl\rangle$, with $j, k, l \in \{0, 1\}$, and the state of the x particle being $|2\rangle$ as in the noiseless attack

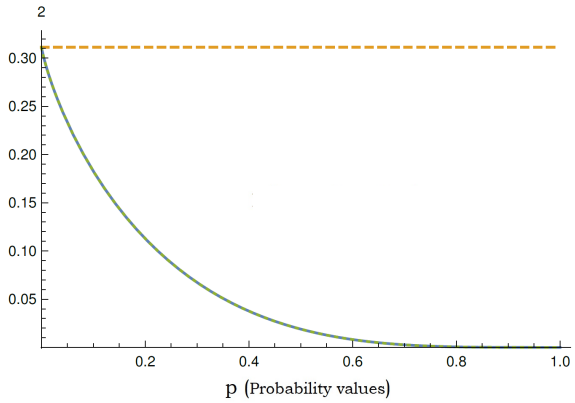

Figure 5.3: (Color online) Performance of the Ping-pong QKD protocol under depolarizing noise: The bold (black) and dashed (red) plots represent I_{AB} and I_{AE} with the Holevo bound for Alice-Bob coinciding with I_{AB}. As a function of noise parameter p, I_{AE} remains constant at the noiseless value of 0.311, because Eve's attack strategy is indifferent to unital noise. That I_{AB} equals the Holevo bound implies that Bob's Bell state measurement in the modified Ping-pong protocol is already optimal.

case. The final states with Bob-Eve for the encodings $a = 0$ and $a = 1$ are:

$$\rho^0 = \frac{1}{2}\begin{pmatrix} \frac{p(4-p)}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{(p-2)^2}{4} & 0 & (p-1)^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (p-1)^2 & 0 & \frac{(p-2)^2}{4} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{p(4-p)}{4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix};$$

$$\rho^1 = \frac{1}{2}\begin{pmatrix} \frac{p(2-p)}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{p(2-p)}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{p^2}{4} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{(p-2)^2}{4} & (p-1)^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & (p-1)^2 & \frac{(p-2)^2}{4} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{p^2}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{p(2-p)}{4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{p(2-p)}{4} \end{pmatrix}. \tag{5.18}$$

From Eq. (5.18), we obtain the following joint probabilities P_{AEB}, in place of Eq. (5.3):

$$\begin{aligned} P_{000} &= \frac{1}{2} + \frac{3p}{8}(p-2) \\ P_{001} &= P_{002} = P_{003} = \frac{p}{8}(2-p) \\ P_{010} &= P_{011} = P_{012} = P_{013} = 0 \\ P_{100} &= P_{101} = P_{110} = P_{111} = \frac{1}{8} + \frac{p}{16}(p-2) \\ P_{102} &= P_{103} = P_{112} = P_{113} = \frac{p}{16}(2-p) \end{aligned} \tag{5.19}$$

with all other joint probability terms vanishing. As with AD noise, here again Bob will also obtain outcomes $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ in his Bell state measurement, which correspond to the outcome symbols 2 and 3 in Eq. (5.19). From the above probabilities P_{AEB} , one finds the mutual information between Alice and Bob to be

$$\begin{aligned} I_{AB}(p) = \frac{1}{36}\Bigg[& 9\log\left(\frac{4}{9}p(2p-3)+1\right) \\ & + 8p(2p-3)\coth^{-1}\left(\frac{9}{(3-4p)^2}\right) \\ & + 6\left(4p^2-6p+3\right)\log\left(\frac{3}{4}-\frac{9}{64p(2p-3)+108}\right) \\ & + (4p(2p-3)+9)\log\left(\frac{36}{16p(2p-3)+27}+4\right)\Bigg]. \end{aligned} \tag{5.20}$$

On the other hand, it follows from Eq. (5.19) that

$$\begin{aligned} & P_{AE=00} = \frac{1}{2}; P_{AE=01} = 0 \\ & P_{AE=10} = P_{AE=11} = \frac{1}{4}, \end{aligned} \tag{5.21}$$

i.e., P_{AE} is independent of the noise parameter. Consequently, $I_{AE}(p)$ is just the noiseless value of $\frac{1}{8}\log\left(\frac{64}{27}\right)$. Figure (5.3) shows that under the depolarizing channel, there is no positive key rate $\kappa \equiv I_{AB} - I_{AE}$ for finite noise, essentially because I_{AE} remains constant, being unaffected by the depolarizing noise (as explained above), whereas I_{AB} drops with the noise level. Therefore, this channel, in contrast to the AD channel, offers no advantage to Alice and Bob in our scenario. A similar disadvantageous behavior holds for dephasing and other unital noisy channels, which may be understood generally as follows. In our scenario, the noise acts *before* the first attack by Eve (see Figure 5.1), and the second instance of noise (in the backward trip of the particle) acts *after* Eve's second attack. Therefore, the second instance of noise doesn't affect I_{AE} (though, in general, it will affect I_{AB}). As to the onward trip of the particle, the travel qubit, as seen by Eve, is initially in a maximally mixed state $\frac{I}{2}$. Depolarizing noise or any other unital channel $\mathcal{C}_U$ is characterized by the property

$$\mathcal{C}_U : \frac{I}{2} \mapsto \frac{I}{2}, \tag{5.22}$$

i.e., it maps the state $\frac{I}{2}$ to itself. Thus, this state of the travel qubit remains unaffected, and hence Eve's correlation with Alice is indifferent to the noise. It is worth noting here that if the unital noise acts after Eve's first intervention (rather than before, see Figure 5.1), then I_{AE} is not expected to be invariant under the noise, since Eve's action can deviate the state of the particle from $\frac{I}{2}$. From Eq. (5.18) one obtains the reduced density operators for the state of particles ht

$$\rho_{ht}^{a=0} = \frac{1}{4}\begin{pmatrix} (2-q)q & 0 & 0 & 0 \\ 0 & ((q-2)q+2) & 2(q-1)^2 & 0 \\ 0 & 2(q-1)^2 & (q-2)q+2 & 0 \\ 0 & 0 & 0 & (2-q)q \end{pmatrix};$$

$$\rho_{ht}^{a=1} = \frac{1}{4}\begin{pmatrix} (2-q)q & 0 & 0 & 0 \\ 0 & (q-2)q+2 & 0 & 0 \\ 0 & 0 & (q-2)q+2 & 0 \\ 0 & 0 & 0 & (2-q)q \end{pmatrix}.$$

As with Eq. (5.14), the maximum information Bob can receive is upper-bounded by the Holevo quantity (5.6). To derive this, we obtain the eigenvalues λ_j^0, λ_j^1 and λ_j^{01} for the density operators $\rho_{ht}^{a=0}, \rho_{ht}^{a=1}$ and their equal average, which are found to be:

$$\begin{aligned}
\lambda_j^0 &= \tfrac{1}{4}\left\{(2-p)p, (2-p)p, (2-p)p, 3(p-2)p+4\right\}, \\
\lambda_j^1 &= \tfrac{1}{4}\left\{(2-p)p, (2-p)p, (p-2)p+2, (p-2)p+2\right\}, \\
\lambda_j^{01} &= \tfrac{1}{4}\left\{1, (2-p)p, (2-p)p, 2(p-2)p+3\right\}.
\end{aligned}$$

Using this, the Holevo bound χ_{DP} under the depolarizing channel can be found in a manner similar to Eq. (5.15). Interestingly χ_{DP} is found to coincide with I_{AB}. This coincidence suggests that the Bell state measurement strategy by Bob is indeed optimal, unlike in the case of the AD channel.

5.4 Conclusion and discussions

It is generally accepted that noise is detrimental to quantum information processing, in particular quantum cryptography. Here we identify, counter to this expectation, a scenario of "trusted noise", where noise can play a helpful role. In quantum key distribution, proofs of unconditional security assume that the eavesdropper Eve is restricted only by physical laws, and that all the noise is due to her attack. We consider a more realistic scenario, where Eve too is bound by limits imposed by noise due to environment-induced decoherence. We show how this can work to the advantage of legitimate parties, when noise affects the eavesdropper more than the legitimate parties. Now, an easy version of this scenario would have been one, where noise universally affects not just the legitimate parties, but also Eve. Therefore, the nontrivial aspect is that the noise only affects the communication channel and not the eavesdropping channel directly. Eve's limitation is her inability to replace the noisy communication channel between Alice and Bob by an noiseless one. In the particular situation considered here, the security of the Ping-Pong protocol (modified to a key distribution scheme) against a noise-restricted adversary is shown to improve under a non-unital decoherence, but to deteriorate under unital decoherence. In light of [Renner et al., 2005; Pirandola et al., 2009; García-Patrón and Cerf, 2009], we may ask whether the AD statistics Eq. (5.10) can be produced using only local uncorrelated classical noise added by Alice and Bob, starting from the noiseless case Eq. (5.3). We now answer the question in the negative. Alice's most general noise can be modelled by a combination of a conditional probability distribution $P^A(x|y)$ (used with probability α) and a random coin toss φ^A (used with probability $1-\alpha$), while that for Bob by a combination of a conditional probability distribution $P^B(x|y)$ (used with probability β) and a random coin toss φ^B (used with probability $1-\beta$). Further, let $P^A(0|0) = g$, $P^A(0|1) = h$ and $P^B(0|0) = a, P^B(1|0) = b, P^B(2|0) = c, P^B(3|0) = 1-a-b-c$; and $P^B(0|1) = d, P^B(1|1) = e, P^B(2|1) = f, P^B(3|1) = 1-d-e-f$. Applying the noise unilaterally on her side, Alice can't reproduce Eq. (5.10) because of the occurence of symbols 2 and 3 on Bob's side. Suppose Bob alone applies his local noise. Then, one finds that $P^B_{101} = P^B_{110} = \frac{a+d}{8}$, which stands in contradiction with the data in Eq. (5.10). Thus, we must consider whether both Alice and Bob applying local noise independently can reproduce the required statistics. In the above, P_j^A denotes the jth component of the joint probability distribution obtained by Alice's application of her local classical noise to the classical outcome data of Eq. (5.3); analogously for P_j^B in the case of Bob. Without loss of generality, suppose Alice applies her local noise first, and then Bob. We shall use the notation where the jth component after Bob also has applied his local classical noisy channel to the classical data

P_j^A is denoted $P_j^{A\to B}$. Then, from Eq. (5.3), we obtain:

$$P_{010}^A = \frac{\alpha h}{8} + \frac{(1-\alpha)r}{8}. \tag{5.23}$$

This must, in view of the vanishing of this component in Eq. (5.10), implying

$$\alpha = 0, \quad r = 0 \tag{5.24a}$$
$$\alpha = 1, \quad h = 0. \tag{5.24b}$$

If P_{010}^A doesn't vanish, then we must have $p^B(0|0) = 0$, to ensure that under the transformation induced by Bob's play, the final $P_{010}^{A\to B}$ vanishes. This would mean that $p^B(1|0)$ or $p^B(2|0)$ or $p^B(3|0)$ should be non-vanishing. But this, in turn, would mean that $P_{011}^{A\to B}$ or $P_{012}^{A\to B}$ or $P_{013}^{A\to B}$ should be non-vanishing, in contradiction with the corresponding requirement in data Eq. (5.10). Thus, we are led to conditions Eq. (5.24). To see why condition Eq. (5.24a) won't work out, we note that it would imply that $P_{000}^A = \frac{\alpha}{2}\left(g + \frac{h}{4}\right) + (1-\alpha)r\frac{5}{8} \equiv 0$ as well as $p_{001}^A = \frac{\alpha h}{8} + (1-\alpha)\frac{r}{8} \equiv 0$. But, this would imply that

$$\begin{aligned} P_{000}^{A\to B} &= \beta(aP_{000}^A + dP_{001}^A) + (1-\beta)q(p_{000}^A + P_{001}^A) \\ &= 0, \end{aligned} \tag{5.25}$$

contradicting the fact that this component is non-vanishing in the AD statistics Eq. (5.10). To see why condition Eq. (5.24b) also won't work out, we note that it would imply that

$$\begin{aligned} P_{000}^{A\to B} &= \frac{g}{2}(\beta a + (1-\beta)q), \\ P_{100}^{A\to B} &= \frac{g}{8}(\beta a + (1-\beta)q), \end{aligned} \tag{5.26}$$

implying that these two components differ by a factor 4, contradicting the additional noise dependence seen in Eq. (5.10). In conclusion, the advantage provided by the quantum AD channel can't be simulated locally (without any classical communication) by the legitimate parties, acting on the noiseless (but eavesdropped) outcome statistics. This may be attributed to the fundamentally quantum nature of the disturbance introduced into the noisy channel through Eve's intervention.