4 A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols

4.1 Introduction

In 1984, Bennett and Brassard proposed the first protocol for quantum key distribution (QKD), which is now known as BB84 protocol [Bennett and Brassard, 2014]. This pioneering work drew a considerable amount of attention from the scientific community, as it was shown to be unconditionally secure. A desired feature for all key distribution schemes is to provide the unconditional security to the distributed key, but it is known to be unachievable in the domain of classical cryptography. This interesting fact that unconditional security of the distributed key can be obtained by using quantum resources led to extensive studies on the protocols of secure quantum communication (see Ref. [Pathak, 2013] for further details). Initial studies were limited to QKD [Bennett and Brassard, 2014; Bennett, 1992; Ekert, 1991; Bennett, 1992; Goldenberg and Vaidman, 1995]. These initial studies on QKD brought out a number of facts which were further established later. Here, in the context of the present work, we wish to specially stress on a specific aspect. In 1991, Ekert proposed a protocol for QKD using entangled state which can be reduced to BB84 protocol (which uses single photon (qubit) states) under certain conditions [Ekert, 1991]. Later, Bennett introduced a single-photon-based scheme for QKD which requires only 2 states, now known as the B92 protocol [Bennett, 1992]. Soon BBM protocol [Bennett, 1992] was introduced, and it was found that BBM protocol may be viewed as an entangled-state-based analogue of the single-photon-based B92 protocol. Thus, these studies indicated that the security achieved by a single-photon-based scheme can also be achieved by a corresponding entangled-state-based scheme. As we have already mentioned, initial studies on quantum cryptography were limited to QKD [Bennett and Brassard, 2014; Bennett, 1992; Ekert, 1991; Bennett, 1992; Goldenberg and Vaidman, 1995]. Later, other aspects of secure quantum communication were investigated [Long and Liu, 2002]. For example, protocols were proposed for quantum secret sharing [Hillery et al., 1999], quantum key agreement (QKA) [Zhou et al., 2004; Shukla et al., 2014; Chong and Hwang, 2010], quantum dialogue (QD) [Nguyen, 2004; An, 2005; Shukla et al., 2013b; Shi et al., 2010; Yang and Hwang, 2013], quantum secure direct communication (QSDC) [Boström and Felbinger, 2002; Lucamarini and Mancini, 2005], and deterministic secure quantum communication (DSQC) [Jun et al., 2006; Li et al., 2006;

Yan and Zhang, 2004; Zhong-Xiao et al., 2005; Zhu et al., 2006; Hai-Jing and He-Shan, 2006; Yuan et al., 2011; Banerjee and Pathak, 2012]. For the purpose of the present study, all these schemes of secure quantum communication can be broadly divided in two classes: Class A: single-qubit-based schemes which do not use entangled states to implement the protocol, like BB84 protocol [Bennett and Brassard, 2014], B92 protocol [Bennett, 1992], LM05 protocol [Lucamarini and Mancini, 2005], and Class B: entangled-state-based protocols, which uses one or more entangled states to implement the protocol. Ekert protocol [Ekert, 1991], BBM protocol [Bennett, 1992], ping-pong (PP) protocol [Boström and Felbinger, 2002], are some of the protocols belonging to Class B. In fact, there exists a one to one map between the protocols of Class A and Class B. In principle, any task that can be implemented using single qubit states can also be implemented using an entangled-state-based scheme. Of course, device independent schemes can be realized only using the protocols of Class B. However, we do not wish to stress on that feature (device independence) here. Excluding ideas of device independence, it can be shown that the security provided by a scheme of Class A and the corresponding scheme of Class B is equivalent in the ideal situation, where noise is not present. To illustrate this point in Table 4.1, we have listed protocols of Class A and Class B for various tasks related to secure quantum communication. As we have already mentioned in an ideal situation, these schemes (i.e., any two schemes shown in the same row of Table 4.1) are equivalent as far as the ability to perform the cryptographic task in a secure manner is concerned. However, to the best of our knowledge this equivalence is not investigated in the realistic situation (i.e., in the presence of noise). Keeping this fact in mind, this chapter aims to perform a comparative study of the protocols for secure quantum communication under various noise models. Specifically, we wish to compare single-qubit-based protocols (protocols of Class A) with entangled-state-based protocols (Protocol of Class B) under various noise models. Here, it may be noted that although, such comparative study has not yet been performed for protocols of Class A and Class B mentioned above, a similar comparative study has been performed on conjugate-coding-based protocols of secure quantum communication and orthogonal-state-based protocols of secure quantum communication, which are equivalent in the ideal situation ([Shukla, 2015] and references therein), but not in noisy environment ([Sharma et al., 2016a] and references therein). Further, there are various equivalent but different decoy-qubit-based strategies (such as the BB84 subroutine, GV subroutine) for eavesdropping checking that are used in standard protocols of secure quantum communication. These subroutines are also known to be equivalent in a noise free environment, but a recent study has established that they are not equivalent in a noisy environment [Sharma et al., 2016a]. This recent observation has further motivated us to perform the present investigation and to systematically investigate the effect of different type of noises on various type of schemes of secure quantum communication.

There are several noise models [Nielsen and Chuang, 2002; Preskill, 1998]. Here, we will restrict ourselves to the study of the effects of amplitude damping (AD) channel, phase damping (PD) channel [Banerjee and Ghosh, 2007b; Omkar et al., 2013], collective noise and Pauli noise. Finally, we will also discuss squeezed generalized amplitude damping (SGAD) channel [Omkar et al., 2013; Srikanth and Banerjee, 2008; Banerjee and Srikanth, 2008b] and note that results for the generalized amplitude damping (GAD) channel as well as that for the AD channel can be obtained from the results computed for the SGAD channel. The motivation to study these noise models is that the AD noise model deals with an interaction of the quantum system with a zero temperature (vacuum) bath. An energy dissipation is involved in this noise model while not in PD. These two noise models can bring about the phenomena of entanglement decay and entanglement sudden-death [Huang and Zhu, 2007]. Here, as we wish to analyze the equivalence between a single-qubit-based scheme

Sr. No.	Quantum Cryptographic Task	Protocol from Class A	Protocol from Class B
1	QKD	B92 protocol [Bennett, 1992]	BBM protocol [Bennett, 1992]
2	QKA	Chong et al. protocol [Chong and Hwang, 2010]	Shukla et al. protocol [Shukla et al., 2014]
3	QSDC	LM05 protocol [Lucamarini and Mancini, 2005]	PP protocol [Boström and Felbinger, 2002]
4	QD	Shi et al. protocol [Shi et al., 2010]	Ba An protocol [Nguyen, 2004]

Table 4.1: Single-qubit-based and entangled-state-based protocols for various tasks related to secure quantum communication.

with an entanglement-based one, these two noise models become relevant. Collective noise is a coherent effect on all the qubits, viz., all the polarization encoded photons traveling through an optical fiber undergo the same birefringence [Bourennane et al., 2004]. The Pauli noise channels include various physically relevant cases, such as bit flip, phase flip, and depolarizing channels [Omkar et al., 2013; Chiuri et al., 2011; Fischer et al., 2001; Fern and Whaley, 2008]. SGAD channels are a generalization of the AD family of channels, which includes the GAD and involves the dissipative interaction with a non-zero temperature bath with non-vanishing squeezing [Srikanth and Banerjee, 2008]. The squeezing, being a quantum resource, provides an edge over GAD channels, which study a dissipative interaction with a finite temperature bath without squeezing [Srinatha et al., 2014; Thapliyal et al., 2015, 2016]. Hence, the choice of SGAD channel enables investigations into both non-zero as well as vanishing regimes of squeezing. The wide applicability of all these noise models sets our motivation to systematically study various schemes for secure quantum communication under noisy environment and to analyze their equivalence.

The effect of noise on various protocols of secure quantum communication has been performed. We have investigated the effect of amplitude damping, phase damping, squeezed generalized amplitude damping, Pauli noise as well as various collective noise models on the protocols of quantum key distribution, quantum key agreement, quantum secure direct communication and quantum dialogue. From each type of protocol of secure quantum communication, we have chosen two protocols for our comparative analysis: one based on single-qubit states and the other one on entangled states. This comparative analysis has revealed that single-qubit-based schemes are generally found to perform better in the presence of amplitude damping, phase damping, squeezed generalized amplitude damping noises, while entanglement-based protocols turn out to be preferable in the presence of collective noises. It is also observed that the effect of noise depends upon the number of rounds of quantum communication involved in a scheme of quantum communication. It is also observed that squeezing, a completely quantum mechanical resource present in the squeezed generalized amplitude channel can be used in a beneficial way as it may yield higher fidelity compared to the corresponding zero squeezing case.

The remaining part of the chapter [1] is organized as follows. In Section 4.2, we briefly discuss the noise models we are going to apply on the schemes mentioned in Table 4.1. The next section is dedicated to the method adopted to study the effect of noise models described in Section 4.2. In Section 4.4, we briefly describe the protocols listed in Table 4.1, and report the effect of various type of noises on these protocols with a clear aim to compare single-qubit-based scheme for a specific cryptographic task with the corresponding entangled-state-based scheme. Finally, we conclude in Section 4.5.

4.2 Different noise models

The most important and widely studied noise models are the AD, PD, collective and Pauli noise models. Apart from these, generalization of AD considering a dissipative interaction with a thermal and squeezed thermal bath have been studied as GAD and SGAD, respectively. Here, we describe only the SGAD channels as the effect of the GAD channel can be obtained as its limiting case for zero bath squeezing. Further, as the AD noise is a limiting case of GAD, it provides a consistency check of the obtained results under SGAD noise. Similarly, one can view PD noise as a special case of Pauli noise (for detail discussion, see [Omkar et al., 2013]), and thus the results obtained under PD noise can also be used to check the consistency of the results obtained under Pauli noise. In what follows, we will study the effect of all these noise models on the protocols of secure quantum communication that are listed in Table 4.1. The noise models we have opted to study in the present chapter are briefly described below.

4.2.1 AD noise model

The AD noise simulates the dissipative interaction of a quantum system with a vacuum bath. A perception about the importance of this noise model can be obtained easily if we consider the large number of theoretical and experimental works on this noise model reported in the recent past ([Sharma et al., 2016a; Huang and Zhu, 2007; Thapliyal et al., 2015; Kim et al., 2013; Turchette et al., 2000b; Myatt et al., 2000; Marques et al., 2015] and references therein). The Kraus operators of an AD channel are given by [Nielsen and Chuang, 2000; Preskill, 1998; Srikanth and Banerjee, 2008]

$$E_0=\left[\begin{array}{cc}1 & 0\\ 0 & \sqrt{1-\eta}\end{array}\right],\qquad E_1=\left[\begin{array}{cc}0 & \sqrt{\eta}\\ 0 & 0\end{array}\right],\tag{4.1}$$

where η $(0\leq\eta\leq1)$ is the probability of error or decoherence rate.

4.2.2 PD noise model

Similarly, Kraus operators for phase-damping noise model are [Nielsen and Chuang, 2000; Preskill, 1998; Omkar et al., 2013]

$$E_0=\sqrt{1-\eta}\left[\begin{array}{cc}1 & 0\\ 0 & 1\end{array}\right],\qquad E_1=\sqrt{\eta}\left[\begin{array}{cc}1 & 0\\ 0 & 0\end{array}\right],\qquad E_2=\sqrt{\eta}\left[\begin{array}{cc}0 & 0\\ 0 & 1\end{array}\right],\tag{4.2}$$

where η $(0\leq\eta\leq1)$ is the decoherence rate. This is another widely studied noise model. For instance, PD noise is discussed in Refs. ([Sharma et al., 2016a; Omkar et al., 2013; Banerjee and Srikanth, 2008b; Huang and Zhu, 2007; Turchette et al., 2000b; Myatt et al., 2000; Marques et al., 2015; Sharma et al., 2015; Kuang et al., 1997; Thapliyal and Pathak, 2015]

[1] This chapter is based on the publication [Sharma et al., 2016b; Sharma, 2016].

and references therein). This noise model is also experimentally simulated in Refs. [Turchette et al., 2000b; Marques et al., 2015]. Here, it would be apt to note that this particular noise model can be viewed as a special type of Pauli channel described in Sec. 4.2.4. However, PD noise deserves special attention because of the fact that it corresponds to quantum non-demolition interactions with the environment. Further, a large number of recent theoretical and experimental works indicate that it deserves special attention. Keeping these facts in mind, in what follows, we would investigate the effect of PD noise independently, and would subsequently use the obtained results for consistency check of the results obtained under Pauli noise.

4.2.3 Collective noises

A coherent effect of environment on all the travel qubits passing through a channel [Zanardi and Rasetti, 1997] can be studied using collective rotation (CR) and dephasing (CD) noise models. It is known that the singlet states are resistant to an arbitrary collective noise [Zanardi and Rasetti, 1997]. Recently, the effect of collective noise on various schemes of quantum communication has been studied [Yang and Hwang, 2013; Sharma et al., 2016a; Bourennane et al., 2004; Sheng and Deng, 2010; Boileau et al., 2004; Li et al., 2008]. Interestingly, these studies provided protocols for quantum communication, which use logical qubits to avoid the effect of collective noise (cf. [Yang and Hwang, 2013; Boileau et al., 2004; Li et al., 2008]). However, in the present chapter, we have not used logical qubits. Specifically, in what follows, we have studied the effect of collective noise on physical qubits. Before we proceed further let us briefly introduce CR and CD noise models.

(a) CR noise model

CR noise transforms $|0\rangle \rightarrow \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and $|1\rangle \rightarrow -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$. Here, θ is the noise parameter [Sharma et al., 2016a; Sheng and Deng, 2010; Boileau et al., 2004; Li et al., 2008]. Mathematically, a rotation operator acts on the quantum state of travel qubits corresponding to this transformation.

(b) CD noise model

CD noise leaves $|0\rangle$ unchanged while transforms $|1\rangle$ as $|1\rangle \rightarrow \exp(i\phi)\,|1\rangle$, where ϕ is the noise parameter [Sharma et al., 2016a; Sheng and Deng, 2010; Boileau et al., 2004; Li et al., 2008]. This is equivalent to a phase gate.

4.2.4 Pauli noise

The set of all Pauli channels is a tetrahedron. The phase flip and phase damping channels correspond to a proper subset of the Pauli channels. Depolarizing channels forms a 1-simplex embedded within the convex polytope representing the Pauli channels [Omkar et al., 2013]. Pauli noise [Omkar et al., 2013] is studied using operators $E_i = \sqrt{p_i}\sigma_i$, where $\sigma_0 = \mathbb{I}$, $\sigma_1 = X$, $\sigma_2 = iY$, and $\sigma_3 = Z$. Here, p_i corresponds to the probability with which a particular Pauli operation is applied [Chiuri et al., 2011; Fischer et al., 2001,?]. Corresponding expression for the depolarizing channel can be obtained with $p_i = \frac{p'}{3}$ for $i \in \{1, 2, 3\}$ and $p_0 = 1 - p'$. Specifically, it would mean that with a certain probability the state remains unchanged while with the remaining probability, it becomes completely mixed. Further, information regarding bit flip, phase flip and bit-phase flip channels can be obtained with $p_0 = 1 - p'$ and $p_i = p'$ for $i = 1, 3$ and 2, respectively. This kind of noise channel is studied for noise estimation [Chiuri et al., 2011], channel characterization [Fischer et al., 2001] and error correction [Fischer et al., 2001].

4.2.5 SGAD noise model

SGAD channel is a generalization of the AD and GAD channels and is characterized by the following Kraus operators [Omkar et al., 2013; Srikanth and Banerjee, 2008]

$$\begin{aligned}
E_0 &= \sqrt{Q}\left[\begin{array}{cc} 1 & 0 \\ 0 & \sqrt{1-\lambda\left(t\right)} \end{array}\right], \\
E_1 &= \sqrt{Q}\left[\begin{array}{cc} 0 & \sqrt{\lambda\left(t\right)} \\ 0 & 0 \end{array}\right], \\
E_2 &= \sqrt{1-Q}\left[\begin{array}{cc} \sqrt{1-\nu\left(t\right)} & 0 \\ 0 & \sqrt{1-\mu\left(t\right)} \end{array}\right], \\
E_3 &= \sqrt{1-Q}\left[\begin{array}{cc} 0 & \sqrt{\mu\left(t\right)}e^{-i\Phi(t)} \\ \sqrt{\nu\left(t\right)} & 0 \end{array}\right], \qquad (4.3)
\end{aligned}$$

here $\lambda\left(t\right)=\frac{1}{p}\left\{1-\left(1-p\right)\left[\mu\left(t\right)+\nu\left(t\right)\right]-\exp\left(-\gamma_0\left(2N+1\right)t\right)\right\},$
$\mu\left(t\right)=\frac{2N+1}{2N(1-p)}\frac{\sinh^2(\gamma_0 at/2)}{\sinh^2(\gamma_0(2N+1)t/2)}\exp\left(-\frac{\gamma_0}{2}\left(2N+1\right)t\right)$, and $\nu\left(t\right)=\frac{N}{(1-p)(2N+1)}\left\{1-\exp\left(-\gamma_0\left(2N+1\right)t\right)\right\}$. Here, γ_0 is the spontaneous emission rate, $a=\sinh\left(2r\right)\left(2N_{th}+1\right)$, and $N=N_{th}\left\{\cosh^2\left(r\right)+\sinh^2\left(r\right)\right\}+\sinh^2\left(r\right)$, where $N_{th}=1/\left\{\exp\left(\hbar\omega/k_BT\right)-1\right\}$ and $\Phi\left(t\right)$ is equal to the bath squeezing angle. The analytic expression for the parameter Q is quite involved, and can be obtained from Ref. [Srikanth and Banerjee, 2008]. The beauty of SGAD channel is that for zero bath squeezing (Φ), it reduces to GAD channel, which can further be reduced to zero temperature bath (AD channel), where Q becomes 1. Hereafter, we will avoid the time t in the argument of all the expressions under SGAD noise for simplicity of notations. Quasiprobability distributions and tomogram of the single and two qubit spin states under the SGAD channels have been studied recently in [Thapliyal et al., 2015, 2016]. The influence of SGAD noise on a quantum cryptographic switch was analyzed in [Srinatha et al., 2014].

4.3 Strategy for studying the effect of various noise models on the protocols of secure quantum communication

The effect of noise can be studied by using a distance-based measure, fidelity, between the final quantum state expected in the absence of noise and the final state obtained when one of the noise models discussed above is considered. To be precise, the strategy adopted in Ref. [Sharma et al., 2016a, 2015; Thapliyal and Pathak, 2015] will be used here. Before we discuss various protocols of secure quantum communication and the effect of noise on them, we will briefly summarize the strategy adopted for the task.

Consider an initial pure state $\rho=|\psi\rangle\langle\psi|$ which is to be evolved under a noisy environment. The evolution of the state after applying the Kraus operators characterizing a particular noise is $\rho_k=\underset{i}{\Sigma}E_i\rho E_i^{\dagger}$, where E_is are the Kraus operators for the chosen noise model under consideration. Specifically, the Kraus operators of AD, PD, SGAD and Pauli channels are given in Section 4.2.

Further, in case of the coherent effect of noise on all the qubits, i.e., collective noise, the transformed state is obtained as $\rho_k=U\rho U^{\dagger}$, where U is the unitary operation due to corresponding noise. The unitary operations for both collective noises are given in the previous section. Finally, fidelity, defined as

$$F=\langle\psi|\rho_k|\psi\rangle,$$

between the final state after the effect of noise ρ_k and pure initial state $|\psi\rangle$ is used as a measure of the effect of noise. It would be worth mentioning here that the fidelity expression used here has been used in Refs. ([Sharma et al., 2016a; Guan et al., 2014b; Li and Jin, 2016] and references therein). However, conventionally, an equivalent, but a slightly different definition of fidelity is used, and fidelity for two quantum states ρ and σ is defined as $F(\sigma,\rho) = Tr\sqrt{\sigma^{\frac{1}{2}}\rho\sigma^{\frac{1}{2}}}$.

In the current study, we have assumed that one of the noise models is studied at a time. Further, we have also considered that only the travel qubits are affected by the environment, while the qubits not traveling through the channel, i.e., home qubits remain unaffected.

4.4 Various aspects (protocols) of secure quantum communication and effect of noise on them

We briefly review two protocols for each type of secure quantum communication task (namely, QKD, QKA, QSDC and QD), and study the effect of the above described noise models on them. For this we chose one protocol from Class A and another one from Class B. Specifically, for a cryptographic task listed in the second column of Table 4.1, a protocol from Class A (B) is mentioned in the third (fourth) column. Here, we aim to compare the protocol mentioned in the third column of Table 4.1 with the protocol mentioned in the fourth column of the same row under different type of noise models. The purpose, is to investigate their equivalence when subjected to different noise models discussed in Section 4.2. Specifically, the strategy mentioned in the previous section is used here to perform the comparison by comparing fidelity. We obtain expressions of fidelity for the quantum states to be recovered at the end of each protocol. Further, we would like to mention that all the fidelity expressions reported here are obtained as an average fidelity for all possible choices of initial states and encoding on them. For example, if we consider Ba An protocol of QD where a predecided entangled state is used as initial state, then there will be 16 possible cases as Alice and Bob each can encode messages using 4 different operations. Similarly, for a single-qubit-based QD scheme there are 16 possible cases with 4 initial states and 2 possible encodings by each party. This is why for each type of QD average fidelity is obtained by computing fidelity for all cases and then averaging. A similar approach is adopted in the rest of the chapter to obtain average fidelity for various protocols.

4.4.1 QKD protocols and effect of noise on them

Here, as we compare a single-qubit-based scheme for QKD with a QKD scheme which requires an entangled state. Specifically, we opt for B92 protocol [Bennett, 1992] as an example of single-qubit-based QKD scheme and BBM protocol [Bennett, 1992] as its entangled state counterpart.

Entanglement is an important resource for various applications of quantum computation. Another important endeavor is to establish the role of entanglement in a practical implementation where a system of interest is affected by various kinds of noisy channels. Here, a single classical bit is used to send information under the influence of a noisy quantum channel. The entanglement content of quantum states is computed under noisy channels such as amplitude damping, phase damping, squeezed generalized amplitude damping, Pauli channels and various collective noise models on the protocols of quantum key distribution.

Entanglement plays a major role in quantum information theory [Nielsen and Chuang, 2000]. Entangled quantum states find many applications in the fields like quantum cryptography [Bennett et al., 1992], quantum computation [Prevedel et al., 2011; Deutsch, 1985], teleportation [Cubitt et al., 2010; Bennett et al., 1993b]. Entanglement properties are deployed in many areas as a resource to get effective results [Song and Xi, 2011]. There are a number of facets of entanglement such as concurrence [Mintert et al., 2005], distillable entanglement [Horodecki et al., 2009] and entanglement cost [Horodecki et al., 2009]. It is important to know the strength of entanglement in applications of quantum communication under noisy environment. We use 0 and 1 as classical information [Sharma and Sharma, 2014; Sharma and Panchariya, 2015] for transmission under noisy quantum channels, for e.g., amplitude damping and Pauli channels, for the scenario where Alice and Bob act as transmitter (sender) and receiver following the postulates of quantum physics to encrypt and decrypt the information being sent. The simulation results show the amount of average error probability to judge the effect of entanglement under noisy channels for the quality of quantum communication is done. The aim is to achieve error-free communication between Alice and Bob.

Quantum cryptography is based on the laws of quantum mechanics, with the use of optical fibers as a quantum channel and photons as an information carrier, it provides unconditional security against eavesdroppers for long distance communication. This can only be successful when very efficient quantum repeaters are deployed to maintain the strength of the quantum signals at the end of the receiver side.

Quantum key distribution (QKD) is one of the important techniques in the area of the secure communication network. It is based on key exchange phenomenon that is opposite to classical cryptography where key distribution is used for security. For symmetric key cryptosystems, the same secret key is required for both the users to perform encryption and decryption. This drawback is solved in public key cryptography but it is insecure because of various attacks [Girault and Pailles, 2007]. The Diffie-Hellman key exchange is a classical key exchange protocol but more complex to perform in polynomial time for some selected problems [Girault and Pailles, 2007; Diffie and Hellman, 1976]. All these methods are not unconditionally secure and data can be altered and duplicated by an eavesdropper, say, Eve in between the communication link at any point even without notice of the communicating parties. QKD is based on the No-Cloning theorem that is quantum mechanically and unconditionally secure and any changes in original data alerts the transmitter and receiver, hence providing high security from eavesdroppers [Wootters and Zurek, 1982; Dieks, 1982; Peres, 2006].

QKD simulation and error reconciliation is implemented by OptiSystem and other related software installed on a PC to obtain a high key rate for transmission of the quantum information. Field Programmable Gate Array (FPGA) is one of the efficient hardware used to perform practical QKD protocols. Features of FPGA include its simplicity for bit-wise operation, fast and parallel computing and large integrated RAM [Cui et al., 2013].

For the practical implementation of QKD protocol, there are dedicated hardwares available like XILINX based SPARTAN v3 FPGA clocked at 24 MHz. It is similar to an embedded hardware [Sharma, 2014; Sharma and Panchariya, 2015] which includes all the necessary devices and components mounted on a single chip, where a clock is used for USB interfaced with PC, 1 Mbps counter value as the quantum key bits are decided by the divider circuit. Power section and PLL (Phase-Locked Loop) is monitored by controlled commands sent by FPGA. The gated avalanche photodiode (APD) needs a pulse generation of approximately 20 ns for a quantum channel, this pulse generation is generated by a digital

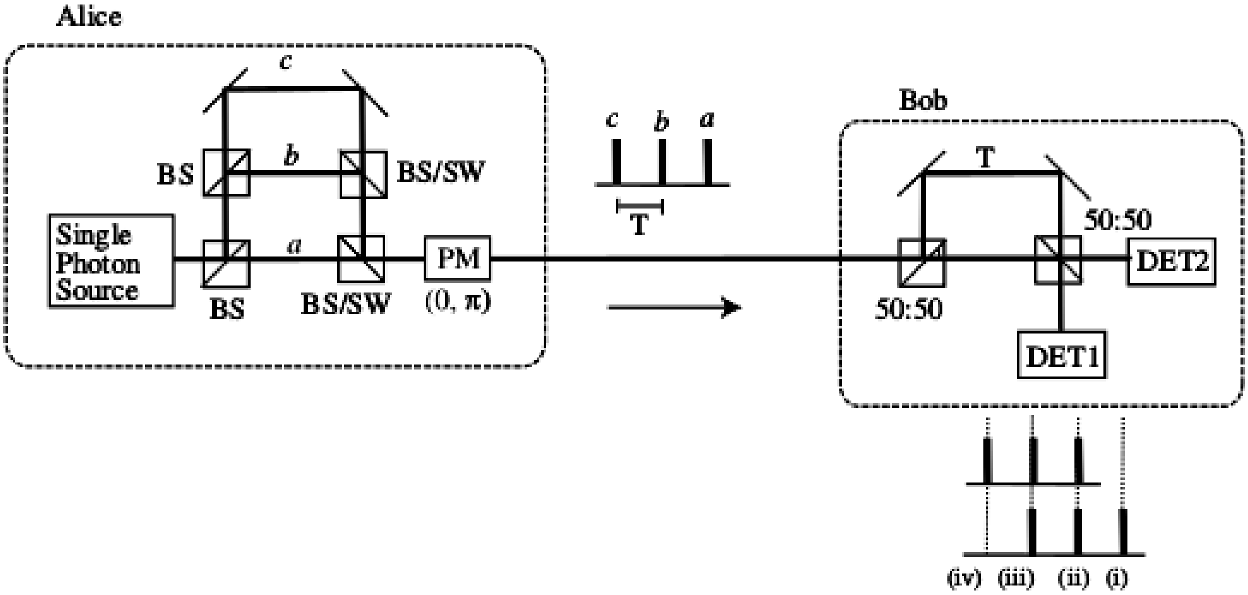

Figure 4.1: Block diagram of DPS (differential phase shift) QKD protocol [Inoue et al., 2002] .

clock manager (DCM). DCM is also responsible for the generation of 48 MHz clocks to regulate the functioning of the FPGA board. Static random-access memory (SRAM) on the FPGA hardware is an important building block used to store and process the data [Cui et al., 2013; Townsend et al., 1994].

Any eavesdropping attempt between the communicating parties perturbs the quantum information, hence as per No-Cloning theorem Eve's presence can be detected. The DPS QKD protocol is used for long-distance communication between the repeater nodes and practically less complex compared to other existing quantum communication systems. The DPS QKD system is functionally compatible with optical devices and networks because of its integrity with these devices hence it is an important component for the whole area of network security [Gyongyosi and Imre, 2012].

The DPS QKD system as shown in Fig. 4.1 [Inoue et al., 2002] uses optical-fiber as a quantum channel and both the sender and receiver communicate via weak coherent pulses with the encoding of logical bits in terms of relative phase of these pulses. Encoding and decoding of the logical bits are performed with two signals both at transmitter and receiver side. The working principle of DPS QKD system is similar to B92 protocol, the encoding and decoding of sent pulses depends on the relative phases, if these are in phase that means encoded and decoded as 0, if relative phase is π, the logical bit is 1. Moreover, some kind of security threats has to be considered because of weak coherent pulses (WCP) leave some of loop holes for eavesdroppers hence photon number splitting attack is the main concern of DPS QKD protocol [Gyongyosi and Imre, 2012].

(a) B92 protocol

A modified version of BB84 with less resources was proposed by Bennett in 1992 [Bennett, 1992]. Hence, the protocol is referred to as B92 protocol. The B92 scheme can be summarized in the following steps:

B92 1: Alice sends a random string of $|0\rangle$ and $|+\rangle$ to Bob, where $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$, and it is assumed that $|0\rangle$ and $|+\rangle$ correspond to bit values 0 and 1, respectively.
We can easily observe the modification from BB84 as, in BB84 a random string of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ was prepared.

B92 2: Bob measures the received qubits in either computational $\{|0\rangle, |1\rangle\}$ or diagonal $\{|+\rangle, |-\rangle\}$ basis randomly.
Here, Bob does not announce his choice of basis, which is in contrast to BB84.

B92 3: From his measurement outcome Bob keeps only the qubits with measurement outcome $|1\rangle$ or $|-\rangle$ and announces the same. Subsequently, Alice also discards the rest of the qubits. The reason behind discarding the measurement outcomes can be understood by noting that a contribution to measurement outputs $|0\rangle$ or $|+\rangle$ can be from both the initial states $|0\rangle$ and $|+\rangle$, due to which the measurement outcomes $|0\rangle$ or $|+\rangle$ can lead to a non-conclusive result. Therefore, only $|1\rangle$ or $|-\rangle$ outcomes are considered which correspond to Alice's bit values 1 and 0. Hence, these qubits can be used to generate a random symmetric key.

B92 4: Bob announces the measurement outcomes of a part of the generated string with the positions of the qubits for verification of eavesdropping. For the corresponding qubits Alice checks the measurement outcome with the initial state as $|0\rangle_A \rightarrow |-\rangle_B$ and $|+\rangle_A \rightarrow |1\rangle_B$. For the errors above a tolerable limit the protocol is discarded. Otherwise a secure and symmetric key can be generated between the two users.

The protocol described above can be studied under various noise models. When the qubit prepared by Alice travels to Bob under the effect of AD noise, the obtained fidelity is

$$F_{AD1}^{QKD} = \frac{1}{4}\left(\sqrt{1-\eta}+3\right). \tag{4.4}$$

Here, and in the remaining part of the chapter, required expressions of fidelity are provided using a notation of the form F_{ji}^{x}, where $j : j \in \{\mathrm{AD}, \mathrm{PD}, \mathrm{CR}, \mathrm{CD}, \mathrm{SGAD}, \mathrm{P}\}$ is the type of noise model; i is 1 and 2 for single-qubit-based and entanglement-based schemes, respectively; and x denotes the type of secure quantum communication, i.e., $x \in \{\text{QKD, QKA, QSDC, QD}\}$. Now, considering that travel qubits have propagated via a PD channel, we obtain

$$F_{PD1}^{QKD} = \frac{1}{4}\left(-\eta+4\right). \tag{4.5}$$

In the collective noisy environment, the obtained fidelity expressions are

$$F_{CD1}^{QKD} = \frac{1}{4}(\cos(\phi)+3), \tag{4.6}$$

and

$$F_{CR1}^{QKD} = \cos^2(\theta), \tag{4.7}$$

for CD and CR noise channels, respectively. The analytic expressions of fidelity under the effect of Pauli and SGAD channels are

$$F_{P1}^{QKD} = \frac{1}{2}(2p_1+p_2+p_4) \tag{4.8}$$

and

$$F_{SGAD1}^{QKD} = \frac{1}{4}\left(\sqrt{1-\mu}\sqrt{1-\nu} - 2\nu + Q\left(\sqrt{1-\lambda} - \sqrt{1-\mu}\sqrt{1-\nu} + 2\nu\right) - \sqrt{\mu}\sqrt{\nu}(Q-1)\cos(\Phi) + \tag{4.9}$$

respectively.

(b) BBM protocol

The BBM protocol [Bennett, 1992] is a variant of the Ekert protocol [Ekert, 1991], with reduced resources. Specifically, Ekert protocol uses three mutually unbiased bases (MUBs) to calculate the correlation function for detecting eavesdropping when the entanglement source was kept in between the two authenticated users Alice and Bob [Ekert, 1991]. In contrast, in BBM protocol, the source of entangled photon is given to Alice and the requirement of three MUBs are reduced to two [Bennett, 1992]. The protocol can be summarized as follows.

BBM 1: Alice prepares a string of the singlet state $|\phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ and sends the second qubit to Bob keeping the first qubit with herself.

BBM 2: Both Alice and Bob measure their qubits of shared quantum state in either computational $\{|0\rangle, |1\rangle\}$ or diagonal $\{|+\rangle, |-\rangle\}$ basis randomly. Both the users announce their choices of measurement basis, but not the measurement outcomes.

BBM 3: Both users decide to discard the measurement outcomes where their choices of measurement basis were different, as in all the remaining cases their measurement outcomes are supposed to be correlated.

BBM 4: Finally, both the users choose around half of the string of the undiscarded instances and announce corresponding measurement outcomes. If the error in the measurement outcomes is below certain tolerable limit both Alice and Bob can obtain a symmetric key using the outcomes of the measurements performed on the remaining qubits which are not used for eavesdropping check. In other words, a lack of correlation in the measurement outcomes is a signature of the presence of an adversary.

The entanglement-based protocol of QKD considered here, i.e., BBM scheme, under the AD, PD, CD and CR noises lead to the following fidelities expressions

$$F_{AD2}^{QKD} = \frac{1}{4}\left(-\eta + 2\sqrt{1-\eta} + 2\right), \tag{4.10}$$

$$F_{PD2}^{QKD} = \frac{1}{2}\left(-\eta + 2\right), \tag{4.11}$$

$$F_{CD2}^{QKD} = \cos^2\left(\frac{\phi}{2}\right), \tag{4.12}$$

and

$$F_{CR2}^{QKD} = \cos^2(\theta), \tag{4.13}$$

respectively. In case of Pauli channels, the fidelity only depends on the probability with which the state remains unchanged

$$F_{P2}^{QKD}=p_1. \tag{4.14}$$

Hence, a linear plot is expected. When the qubits travel under the dissipative SGAD channel, the compact form of fidelity is

$$F_{SGAD2}^{QKD}=\frac{1}{4}\left(2\sqrt{1-\mu}\sqrt{1-\nu}-\mu-\nu+Q\left(-\lambda+2\sqrt{1-\lambda}-2\sqrt{1-\mu}\sqrt{1-\nu}+\mu+\nu\right)+2\right). \tag{4.15}$$

Now, we will try to make a comparative analysis of the obtained fidelity expressions in the QKD protocols from the two classes. Interestingly, fidelity obtained for both the QKD schemes considered here is the same when the travel qubits are subjected to CR noise, as can be seen in Fig. 4.2 a. In the presence of another type of collective noise (namely CD noise), which is dephasing in nature, B92 is seen to perform better (cf. Fig. 4.2 b). Here, it is worth noting that the singlet state is decoherence free in an arbitrary collective noise when both the qubits of the singlet state travel through the noisy channel. However, when one of the qubits travel through the channel having collective noise, it gets affected by the noise and as a consequence, the singlet state also gets affected. This is what we observe here. We have shown only the decay in fidelity considering both the collective noises. This is because of the presence of inversion symmetry along certain points on the absicca (i.e., $\theta=\frac{\pi}{2}$ and $\phi=\pi$, respectively); the remaining plots are a re-trace of the ones depicted. However, in the plots of collective noise, applied to the protocols to follow, we have explicitly depicted we explicitly depict the region in the domain $\theta\in[0,\pi]$ and $\phi\in[0,2\pi]$ for CR and CD noises, respectively. This is so because in those cases, the behavior is more involved and it is instructive to see the parameter dependence in the entire domain.

Expressions of fidelity under Pauli noise reveal that for BBM protocol equally affected states will be obtained for bit-flip, phase-flip, bit-phase flip errors with certain probability. For the depolarizing channel the fidelity expression shows a similar nature. The same expression is obtained for B92 protocol with bit-phase flip error. Further, bit-flip and phase flip errors with equal probabilities affect the state in a similar manner as the expressions become equal in both the cases. The values are always higher than all others for the same amount of error, as shown in Fig. 4.2 c. The obtained fidelity in depolarizing channels can be seen to be intermediate between the last two. As mentioned in Sec. 4.2, the effect of phase damping noise can be extracted from the phase flip error. Specifically, a linear decay in fidelity under the phase damping noise for both B92 and BBM protocols can be deduced from the variation of fidelity due to phase flip error (cf. Fig. 4.2 c), and it can be observed that B92 protocol always performs better than BBM protocol.

From the expressions of fidelity under SGAD noise, the corresponding fidelities under AD and GAD channels can be obtained as limiting cases. When the travel qubits are subjected to AD noise (see smooth (blue) and dashed (red) lines in Fig. 4.2 d) we observe that B92 protocol performs better than BBM protocol at every instant of time. This fact observed here in the presence of AD and PD noises is consistent with some of our recent observations that single qubits perform better while traveling through AD and PD channels

[Sharma et al., 2016a]. In Fig. 4.2 d, we can also see the advantage obtained due to squeezing. Specifically, for non-zero squeezing we can obtain higher fidelity than that with a GAD noisy environment, for a longer time period. Further, it can also be observed that a state is more affected while traveling through a finite temperature bath than in a vacuum bath (AD).

4.4.2 QKA protocols and effect of noise on them

In realistic scenarios, it may be preferable that a single party does not control the whole key. In such scenarios QKD can be circumvented by a key agreement protocol, where all the parties can equally contribute in the final key. To be precise, QKA schemes are studied under two notions: weaker and stronger. In the weaker notion of QKA protocols, the final key is generated after negotiation between both the parties. If we follow this notion, then many of the QKD schemes can be viewed as QKA schemes, such as BB84, B92 and BBM discussed in the previous subsection. However, in the strong notion all the parties contribute equally to the final shared key. Many QKA schemes have been proposed in the past ([Zhou et al., 2004; Shukla et al., 2014; Chong and Hwang, 2010] and references therein).

(a) Single-qubit-based QKA protocol

A single-qubit-based quantum key agreement protocol given by Chong et al., in 2010 [Chong and Hwang, 2010] can be described in the following steps:

QKA1-1 Alice randomly prepares an n bit raw key K_A and a random string of 0 and 1.

QKA1-2 Alice prepares n qubits in such a way that for every 0 (1) in the key she prepares either $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$) depending upon the corresponding bit value in the random string 0 or 1, respectively. Finally, she sends all the qubits to Bob.

QKA1-3 Bob also prepares an n bit raw key K_B. Now, to encode this key he applies I (iY) on the received qubits for 0 (1).

QKA1-4 Bob selects a random sequence from the qubits as verification string and announces the positions of the corresponding qubits. He also announces his raw key.

QKA1-5 Alice can extract a final key as $K = K_A \oplus K_B$ from her and Bob's keys. Subsequently, she broadcasts the obtained values corresponding to the qubits Bob had chosen as verification string along with the information of basis chosen for each qubit in QKA1-2.

QKA1-6 Using the information of the basis chosen Bob can also extract the final key K. If the obtained values for Alice and Bob have errors below a tolerable limit they share an unconditionally secure quantum key.

If the single-qubit-based QKA scheme described above is implemented using a quantum channel having AD noise then we obtain

$$F_{AD1}^{QKA} = \frac{1}{4}\left(-\eta + \sqrt{1-\eta} + 3\right), \tag{4.16}$$

whereas under PD noise we have

$$F_{PD1}^{QKA} = \frac{1}{4}\left(\eta^2 - 2\eta + 4\right). \tag{4.17}$$

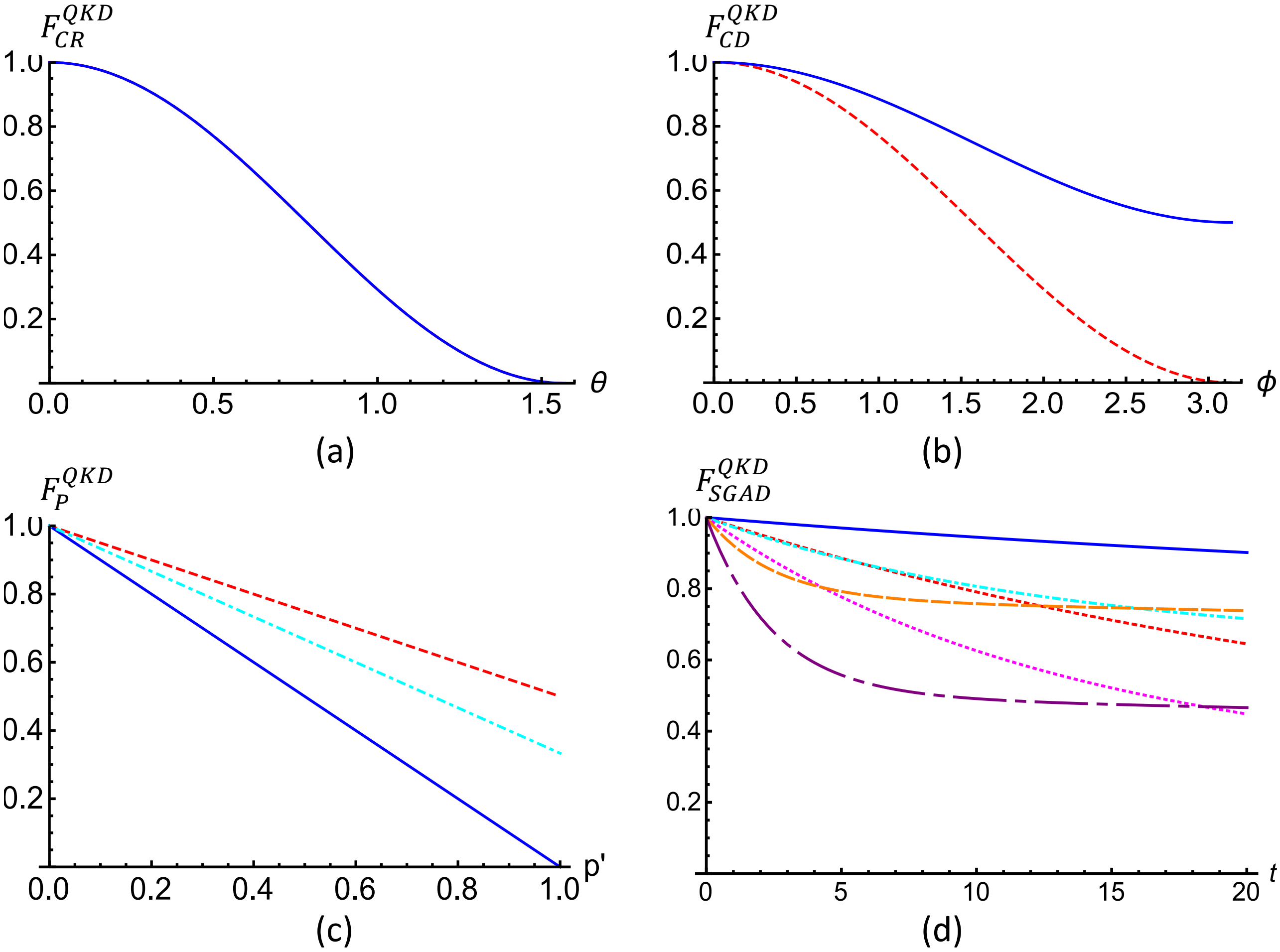

Figure 4.2: QKD in CR and CD noises is shown in (a) and (b), respectively. For CR noise both B92 and BBM protocols have the same fidelity (in (a)). The smooth (blue) and dashed (red) lines in (b) correspond to B92 and BBM protocols, respectively. In (c), the smooth (blue) line corresponds to the fidelity variation with probability of bit-phase flip error for B92 protocol. This same curve also illustrates the dependence of fidelity on probability in all four possible cases discussed in the text for BBM protocol. The dashed (red) and dotted dashed (cyan) lines show fidelity variation in B92 scheme with bit/phase flip error and depolarizing channel, respectively. The smooth (blue) and dashed (red) lines also demonstrate fidelity variation when B92 and BBM protocols are subjected to phase damping noise. (d) demonstrates the effect of AD (in smooth (blue) and dashed (red) lines); GAD (in dotted dashed (cyan) and dotted (magenta) lines) with temperature $T = 1$; and SGAD (in large dashed (orange) and large dotted dashed (purple) lines) with $T = 1$ and squeezing parameters $r = 1$ and $\Phi = \frac{\pi}{8}$ for B92 and BBM protocols, respectively.

On the effect of CD noise the fidelity becomes

$$F_{CD1}^{QKA} = \frac{1}{4}(\cos(\phi_1) + 3), \tag{4.18}$$

while under the influence of CR noise it is

$$F_{CR1}^{QKA} = \cos^2(\theta_1). \tag{4.19}$$

In case the travel particles go through a Pauli channel the obtained fidelity is

$$F_{P1}^{QKA} = \frac{1}{2}(2p_1 + p_2 + p_4). \tag{4.20}$$

For an interaction with a squeezed thermal bath, the fidelity depends on various parameters as

$$F_{SGAD1}^{QKA} = \frac{1}{4}\left(\sqrt{1-\mu}\sqrt{1-\nu} - \mu - \nu + Q\left(-\lambda + \sqrt{1-\lambda} - \sqrt{1-\mu}\sqrt{1-\nu} + \mu + \nu\right) - \sqrt{\mu}\sqrt{\nu}(Q - \right. \tag{4.21}$$

(b) Entangled-state-based QKA protocol

There are various protocols of quantum key agreement that exploit entanglement. Here, we wish to summarize a protocol proposed by Shukla et al. in 2014 [Shukla et al., 2014].

QKA2-1 Alice prepares $|\psi^+\rangle^{\otimes n}$, where $|\psi^+\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. She also prepares a raw key K_A of n bits. She prepares a string of all the first particles to be sent to Bob keeping all the second qubits with herself.

QKA2-2 Alice prepares $\frac{n}{2}$ Bell states $|\psi^+\rangle^{\otimes \frac{n}{2}}$ as decoy qubits and concatenates them with the string of the first particles of the Bell states and sends the $2n$ qubits to Bob after applying a permutation operator Π_{2n}.

QKA2-3 After an authentic acknowledgment of the receipt of all the qubits Alice announces the positions of the decoy qubits, i.e., information of Π_n. Using this information Bob performs a Bell state measurement on partner pairs and calculates error rate. It would be relevant to mention that the decoy-qubit-based security achieved here with GV subroutine can be equivalently done by BB84 subroutine where single qubit decoy qubits are used. They decide to proceed if error rates are below a certain value.

QKA2-4 Bob also prepares a raw key K_B. Further, on the remaining qubits Bob encodes his raw key by applying I or X operations for 0 and 1, respectively. Subsequently, he prepares $\frac{n}{2}$ Bell states as decoy qubits and permutes the string of $2n$ qubits by permutation operator Π'_{2n} after concatenating the decoy and encoded qubits. Finally, he sends them to Alice.

QKA2-5 Bob informs the coordinates of the decoy qubits using which Alice computes the error rate. From this they choose whether to proceed or not.

QKA2-6 Alice announces her key publicly from which Bob can generate the final key $K = K_A \oplus K_B$.

QKA2-7 Bob announces the permutation operator to rearrange the particles in the encoded string with Alice. Using this Alice performs a Bell state measurement on the partner pairs of home and travel qubits. The measurement outcome would reveal Bob's key to Alice.

QKA2-8 Alice can also obtain the final shared, unconditionally secure, quantum key K.

The fidelity expression for the entanglement-based QKA scheme when subjected to AD and PD noise are

$$F_{AD2}^{QKA} = \frac{1}{4}(\eta - 2)^2 \tag{4.22}$$

and

$$F_{PD2}^{QKA} = \frac{1}{2}\left(\eta^2 - 2\eta + 2\right), \tag{4.23}$$

respectively. The quantum state evolves under the collective noise such that the obtained fidelity with the expected pure state is

$$F_{CD2}^{QKA} = \frac{1}{2}\left\{\cos(\phi_1)\cos(\phi_2) + 1\right\}, \tag{4.24}$$

and

$$F_{CR2}^{QKA} = \frac{1}{2}\left\{\cos^2(\theta_1 - \theta_2) + \cos^2(\theta_1 + \theta_2)\right\}, \tag{4.25}$$

for CD and CR noise, respectively. Here, it may be noted that the two noise parameters ϕ_i and θ_i correspond to each round of the travel qubit. The Pauli channels have a symmetric expression for fidelity, given by

$$F_{P2}^{QKA} = p_1^2 + p_2^2 + p_3^2 + p_4^2. \tag{4.26}$$

The closed form analytic expression of fidelity, under the SGAD channel, for the above described QKA scheme [Shukla et al., 2014] is

$$\begin{aligned} F_{SGAD2}^{QKA} &= \tfrac{1}{4}\Big\{Q^2\left(\lambda^2 - 2\lambda(\mu+\nu+1) - 2\left(2\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu} + \mu + \nu - 2\right) + \mu^2 + 5\mu\nu + \nu^2\right) \\ &+ \mu^2 + \mu(5\nu - 4) + (\nu - 2)^2 + \mu\nu(Q-1)^2\cos(2\Phi) \\ &+ 2Q\left(\lambda(\mu+\nu-1) + 2\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu} - \mu^2 + \mu(3-5\nu) - (\nu-3)\nu - 2\right)\Big\}. \end{aligned} \tag{4.27}$$

For QKA schemes two way quantum communication is involved unlike QKD protocols in the previous section, where only sender to receiver communication is involved. Here and in what follows, we explicitly depict the behavior of fidelity of various schemes under AD and PD noise channels, which as noise channels, are subsets of the SGAD and Pauli channels, respectively. However, as mentioned above, there exists a large literature, both theoretical as well as experimental, discussing the impact of the AD and PD noises on various aspects of cryptography. We thus feel justified in discussing the effect of AD and PD noises, separately and use the obtained results for consistency check of the results obtained under SGAD and Pauli noise channels. In both single-qubit-based and entangled-state-based QKA schemes fidelity falls gradually with an increase in decoherence rate η when subjected to AD and PD noisy environments of identical strength (cf. Fig. 4.3 a and b). Similar to the QKD scheme, single-qubit-based schemes perform better than the entangled-state-based ones in both these noisy channels. Further, this similarity between the single-qubit-based QKD and QKA schemes for collective noises, is depicted in the corresponding curves shown in Figs. 4.2 a and b and Figs. 4.3 c and d. However, the entangled-state-based QKA scheme is seen to benefit under collective noise as fidelity for the entangled-state-based QKA scheme is more than that of single-qubit-based protocol, under the assumption of the same noise strength in both rounds of the travel qubit. This fact can be attributed to different choices of Bell state in entanglement-based QKD and QKA protocols.

Further, as discussed in the previous section, the collective noise parameter remains the same for all the qubits traveling through a channel at a particular time, but can have a different value at any other time. The effect of two different values of noise parameters, of the collective noises, on the fidelity of the obtained state can be studied by showing either 3 dimensional variation or contour plots. Fig. 4.4 a and b (c and d) show both these kinds of plots for QKA scheme subjected to CR (CD) noise. Hereafter, we will stick to the contour plots to illustrate the effect of two parameters. Interestingly, it can be observed that it is possible to obtain states with unit or null fidelity for some values of noise parameters.

For the single-qubit-based scheme, the analytic expressions for fidelities are the same for all three types of Pauli channels (i.e., for bit flip, phase flip and bit-phase flip channels). The expressions of fidelity for bit flip and phase flip channels are also the same for the entangled-state-based protocol, but for bit-phase flip error, we obtain a different expression for fidelity, and it is observed that the obtained value of fidelity is smaller compared to the corresponding values for bit flip and phase flip errors. Fig. 4.3 e shows variations of fidelity in all these error channels, where an increase in fidelity for entanglement-based QKA schemes can be attributed to the presence of quadratic terms in the fidelity expression. The variation of fidelity in Fig. 4.3 f considering a dissipative interaction via SGAD channel for both kinds of QKA schemes reemphasize the facts established by their QKD counterparts (cf. Fig. 4.2 d). Specifically, with increase in temperature, dissipation increases, causing decay in the fidelity of the recovered state. Also, squeezing turns out to be a useful resource here, as observed from the increased fidelity of the SGAD plots compared to their GAD (without squeezing) counterparts after a certian evolution period.

4.4.3 QSDC protocols and effect of noise on them

Quantum secure communication not necessarily involves a key generation or key agreement. There are direct communication protocols avoiding key generation and such protocols are referred to as the protocols for secure direct quantum communication. These protocols can be broadly categorized as QSDC and DSQC protocols depending upon the requirement of additional classical communication for decoding of the information. QSDC protocols do

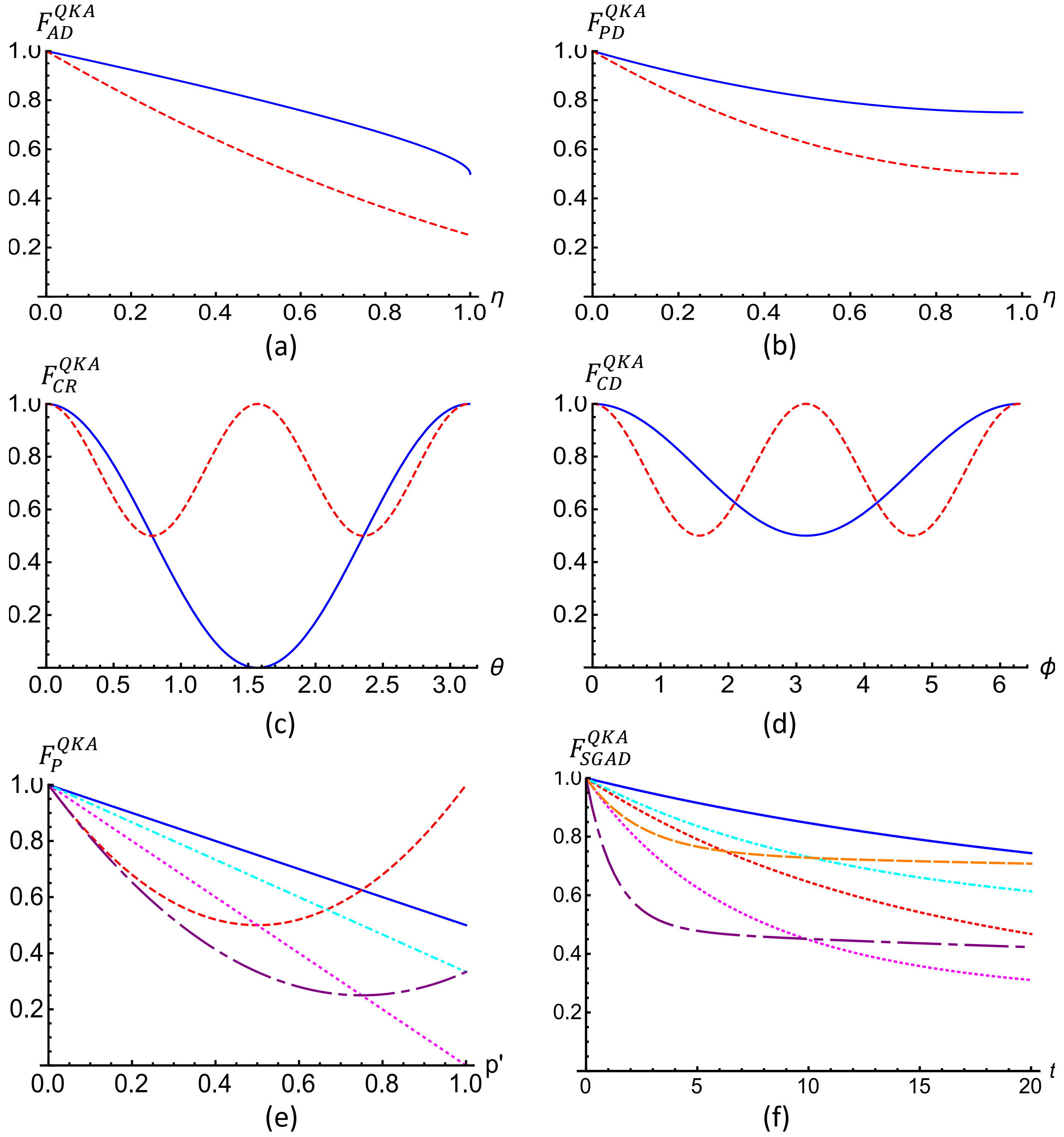

Figure 4.3: (a)-(d) illustrates the fidelity obtained for QKA protocols when subjected to AD, PD, CR and CD noises, respectively. The smooth (blue) and dashed (red) lines correspond to single-qubit-based and entangled-state-based QKA protocols, respectively. For CR and CD noises it is assumed that the noise parameter is same for both the directions of travel of the qubit (i.e., Alice to Bob and Bob to Alice). In (e), the effect of bit flip error on single-qubit-based QKA and entangled-state-based QKA protocols are shown using smooth (blue) and dashed (red) lines, respectively. In the same plot, dotted dashed (cyan) and large dotted dashed (purple) lines correspond to the effect of depolarizing channel on Shi et al.'s and Shukla et al.'s QKA schemes, respecetively; and the dotted (magenta) line illustrates the effect of bit-phase flip error on the single-qubit-based QKA scheme. (f) corresponds to the effect of AD in smooth (blue) and dashed (red) lines; GAD in dotted dashed (cyan) and dotted (magenta) lines with $T = 1$; and SGAD in large dashed (orange) and large dotted dashed (purple) lines with $T = 1$ and squeezing parameters $r = 1$ and $\Phi = \frac{\pi}{8}$ for single-qubit-based and entangled-state-based QKA protocols, respectively.

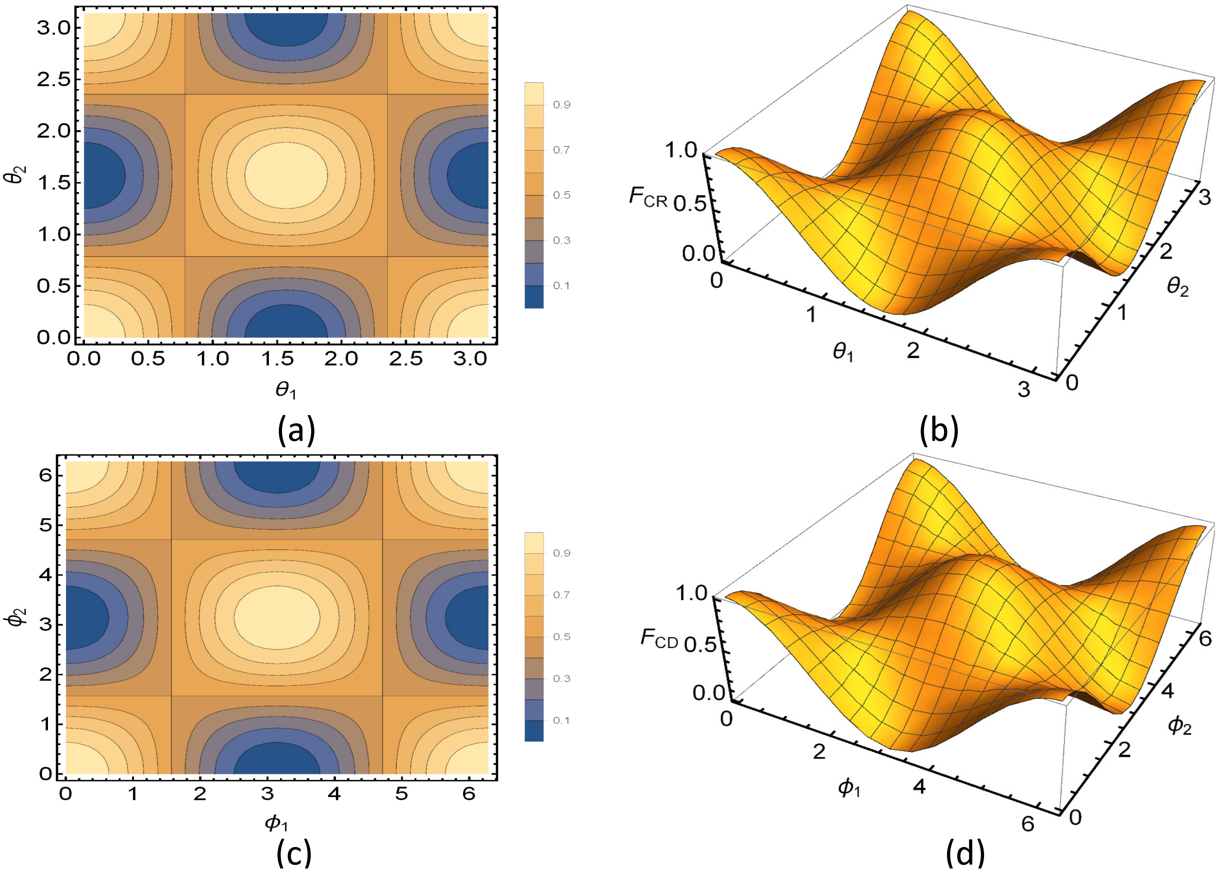

Figure 4.4: Contour and 3D variation of fidelity of entangled-state-based QKA protocol is shown in CR and CD noises. Specifically, in (a) and (c) the contour plots under the effect of CR and CD noise are shown. Corresponding 3D plots can be seen in (b) and (d), respectively. The same plots are obtained for PP protocol as well. A detailed discussion follows in Subsection 4.4.3.

not require any additional classical communication other than that involved in eavesdropping checking, while DSQC protocols do. Here, we wish to discuss two QSDC protocols and compare them in the presence of noise.

(a) LM05 protocol

A QSDC protocol without using entanglement was proposed by Lucamarini and Mancini in 2005 which is now known as LM05 protocol [Lucamarini and Mancini, 2005]. The protocol can be briefly describe in the following steps:

LM1 Bob (receiver) prepares a random string of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and sends it to Alice.

LM2 Alice chooses randomly half of the received qubits as a verification string (to be used as decoy qubits) and performs eavesdropping checking on these qubits. Specifically, Alice measures all the qubits in the verification string in MUBs $\{0, 1\}$ or $\{+, -\}$ randomly. Then she announces the choice of basis with the position of qubits. Based on this, Bob announces the qubits where he has chosen the same basis to prepare the initial state. Depending on this, the measurement outcomes of Alice are expected to be the same with the state prepared by Bob in the absence of any attempt of eavesdropping. For errors below a tolerable limit they proceed to the next step, else they start afresh.

LM3 To encode her message on half of the remaining qubits Alice applies operator I (iY) for sending 0 (1). Subsequently, she returns the encoded qubits to Bob. Here, it would be nice to mention that using such a scheme, for both choices of encoding, a particular initial state will transform into orthogonal states. Consequently, at Bobs end, a message can be easily decoded by measuring the state in the basis it was prepared.

LM4 Alice announces the coordinates of the qubits she had not encoded on (as she wished to use them as decoy qubits for Alice to Bob communication). Bob measures corresponding qubits in the basis he had prepared them initially to check the presence of Eve for Alice to Bob travel of the encoded particles. The same task can also be achieved by Alice encoding on all the remaining qubits after eavesdropping in LM2, while she prepares additional string of equal number of qubits in $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ randomly for eavesdropping checking in this step.

LM5 Only if Bob is convinced of the absence of Eve, he decodes the message sent by Alice by measuring the qubits in the same basis he had prepared them in LM1, otherwise they abort the protocol.

The effect of the AD noise on the single-qubit-based QSDC protocol (LM05 protocol) opted here, LM05, can be deduced from the fidelity expression

$$F_{AD1}^{QSDC} = \frac{1}{4}\left(\eta^2 - 3\eta + 4\right). \tag{4.28}$$

The corresponding expression under the effect of PD noise is

$$F_{PD1}^{QSDC} = \frac{1}{4}\left(\eta^2 - 2\eta + 4\right). \tag{4.29}$$

Similar to the entanglement-based QKA scheme, two rounds of quantum communication is involved here, due to which the expressions of fidelity under CD noise

$$F_{CD1}^{QSDC}=\frac{1}{4}(\cos(\phi_1)\cos(\phi_2)+3), \tag{4.30}$$

and that for CR noise

$$F_{CR1}^{QSDC}=\cos^2(\theta_1+\theta_2), \tag{4.31}$$

involve two noise parameters (ϕ_1, ϕ_2 or θ_1, θ_2) each. As usual, the fidelity expression for Pauli channels with four parameters is

$$F_{P1}^{QSDC}=p_1^2+p_2^2+p_3^2+p_4^2+(p_1+p_3)(p_2+p_4). \tag{4.32}$$

The presence of quadratic terms is signature of two rounds of quantum communication. When the travel qubits undergo a dissipative interaction characterized by the SGAD channel, the fidelity is obtained as

$$\begin{array}{rcl} F_{SGAD1}^{QSDC} & = & \frac{1}{8}\left\{2\left((\nu-3)\nu+Q^2\left(-2\lambda\nu+(\lambda-1)\lambda+\nu^2-\nu+2\right)+2(\nu-1)Q(\lambda-\nu+1)+4\right)\right. \\ & - & 4\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu}Q^2+\mu(Q-1)(-7\nu+Q(-4\lambda+7\nu-2) \\ & + & 4\sqrt{\mu}\sqrt{\nu}(Q-1)\cos(\Phi)\left(-\sqrt{1-\mu}\sqrt{1-\nu}-\sqrt{1-\lambda}Q+\sqrt{1-\mu}\sqrt{1-\nu}Q\right) \\ & + & \left.\nu(Q-1)\cos(2\Phi)+6)+4\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu}Q+2\mu^2(Q-1)^2\right\}. \end{array} \tag{4.33}$$

(b) Ping-pong protocol

The Ping-Pong protocol [Boström and Felbinger, 2002] is a secure direct communication protocol, based on Einstein-Podolsky-Rosen (EPR) pairs [Bennett and Wiesner, 1992]. Its security is studied by [Zawadzki, 2013]. It has two operation modes. One is message mode and other is control mode. In message mode, the legitimate users exchange the information and presence of Eve in between the line is detected in control mode. The control mode is also responsible to check whether the authenticated users are using local operations and classical communication (LOCC) for sharing the qubits of the same entangled pair.

In earlier original work of Ping-Pong protocol, only one classical bit per communication was used and the security issues were described incoherent attacks. Hence, this is the control mode which finds out that Eve introduces some errors in her eavesdropping attempts.

There are numerous proposed research work in Ping-Pong protocol that claims about its capacity and security using dense coding [Wang et al., 2005a; Vasiliu, 2011; Zawadzki, 2012c; Chamoli and Bhandari, 2009; Zawadzki, 2013].

Precisely, LM05 protocol is a single-qubit-based counterpart of PP protocol. The PP protocol works as follows:

PP1 Bob prepares $|\psi^+\rangle^{\otimes n}$, where $|\psi^+\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then he sends all the first particles to Alice keeping all the second qubits with himself.

PP2 Alice forms a verification string by randomly choosing a set of $\frac{n}{2}$ qubits to perform BB84 subroutine as was done in LM2. Specifically, Alice measures the qubits randomly in $\{0, 1\}$ or $\{+, -\}$ basis and announces the choice of basis. Bob also measures his qubits in the same basis. In the absence of Eve, their measurement outcomes are expected to be correlated. In the absence of such a correlation they discard the protocol and return to PP1, otherwise they proceed.

PP3 Out of half of the remaining qubits Alice randomly makes two sets of equal number of qubits. One set for encoding her message and another set for eavesdropping check for Alice to Bob communication. To encode 1 Alice applies X gate before sending the qubit to Bob, and for sending 0 she returns the qubit unchanged.

PP4 Alice informs the coordinates of verification string and Bob performs BB84 subroutine to compute the error rate.

PP5 For low error rates, Bob performs Bell state-measurement on the partner pairs to decode the message sent by Alice.

The analytical expressions of fidelity in the case of the PP protocol exactly match those for entanglement-based QKA scheme [Shukla et al., 2014]. Specifically, if Alice sends random bits instead of her message in the PP protocol, it will reduce to a QKD protocol. Now, suppose that Alice shares her key in a secure manner using this modified PP scheme and Bob announces his key with a prior agreement to obtain the final key by performing an Ex-OR operation between their individual keys. Then, the QKA scheme [Shukla et al., 2014] can be viewed as a modified PP scheme with the same amount of quantum communication involved. Hence, the effect of noise is expected to be the same in PP and Shukla et al.'s QKA scheme. Therefore, we avoid repetition of the expressions and carry on with the discussion regarding the comparison between LM05 and PP protocols under noisy environments.

Both the QSDC protocols when subjected to noise are affected to different extent. Precisely, as observed in the protocols discussed so far, the single-qubit-based schemes have been found to be more efficient as compared to entangled-state-based schemes in AD and PD noisy channels. This is also observed here in Figs. 4.5 a and b. Under the assumption of the same noise parameter for CD and CR noise for Alice to Bob and Bob to Alice travel of the qubits, PP protocol is affected by the CR and CD noise in a manner similar to the entangled-state-based QKA protocol. In fact, in the entangled-state-based QKA scheme one of the parties sends the raw key by PP type QSDC while the other party announces it. Therefore, the effect of noise is the same as in PP protocol. The single-qubit-based scheme has different nature in Fig. 4.5 c and d as compared to the corresponding QKD and QKA protocols. This can be attributed to the two way quantum communication associated in this scheme, unlike the last two cases where it was unidirectional. Further, in the presence of CD noise, the benefit of bidirectional communication can be easily observed as the observed fidelity is more than the previous cases. The single qubits (in LM05) perform better when subjected to CD noise, but suffer more under the influence of CR noise. In Fig. 4.6, we have not shown the contour plots for the fidelity for PP protocol under collective noise as the expressions are exactly the same as that illustrated through Fig. 4.4 for Shukla et al's QKA scheme. The contour plots also show that very low fidelity is also possible for some particular values of noise parameters during the two directions of transmission. Further, under the effect of CD noise, a similar nature of the fidelity variation under LM05 and PP protocols can be observed in Fig. 4.6. However, a closer look reveals that under CD noise fidelity obtained for LM05 protocol is more than that obtained for PP protocol, indicating that for CD noise, single-qubit-based LM05 protocol performs better than the corresponding entangled-state-based PP protocol.

The expressions of fidelity under Pauli noise reveal that the fidelity for PP protocol in bit, phase and bit-phase flip is the same as the fidelity for bit-phase flip errors for equal probability of error in LM05 protocol. In this case the fidelity resurrects to 1 for maximum probability of error. Quite a similar nature is observed for fidelity under bit flip and phase flip errors in LM05 scheme though it remains less than that of the corresponding values in the PP protocol. Similarly, under the influence of the depolarizing channel the fidelity fails to revive but remains always more for LM05 protocol.

The advantage of squeezing, a purely quantum resource, can be observed in Fig. 4.5 f, where in the presence of squeezing after an appreciable amount of time, fidelity higher than the corresponding case of zero squeezing can be observed. Specifically, higher fidelity under SGAD channel relative to AD channel shows that coherence can be sustained using squeezing that would have been lost due to the presence of non-zero temperature.

4.4.4 Quantum dialogue protocols and effect of noise on them

One of the most efficient secure quantum communication schemes is the quantum dialogue (QD). In this scheme both the legitimate parties encode their information on the same qubits and at the end of the protocol each party can deduce the others message. The first QD scheme was proposed by Ba An using Bell states in 2004 [Nguyen, 2004]. Recently, Yang and Hwang proposed a QD scheme immune to the collective noise using logical qubits [Yang and Hwang, 2013]. Here, we consider two QD protocols for analyzing their performance when subjected to noisy environments.

(a) Single-qubit-based QD protocol

A modified QD protocol using only single qubit states and MUBs was proposed by Shi et al. in 2010 [Shi et al., 2010]. Shi et al. protocol can be described in the following steps:

QD 1 Bob prepares a sequence of $2n$ single qubits randomly in $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis. He prepares two copies of n qubits, i.e., two adjacent photons are in the same quantum state. For example, Bob prepares a string of single qubits as $\{(|0\rangle, |0\rangle), (|+\rangle, |+\rangle), (|-\rangle, |-\rangle), (|$ and out of each pair, one qubit will be used for encoding while the other one will be used to send the initial state information. He also prepares some additional decoy qubits to be used for eavesdropping check in each round of communication. Finally, he sends all the $2n$ qubits after inserting decoy qubits randomly in them to Alice.

QD 2 Bob and Alice perform security checking for the received qubits. Specifically, Bob will announce positions of the decoy qubits he chooses for this round of communication and Alice announces her choice of measuring basis and corresponding outcome. Using that Bob determines the error rate and decides whether to proceed or call off the protocol.

QD 3 With the help of Bob, Alice can separate three sequences: the first one of decoy qubits, and two sequences of one copy of initial states each. Out of these three sequences she encodes her message on the second sequence using I (iY) operation for sending bit

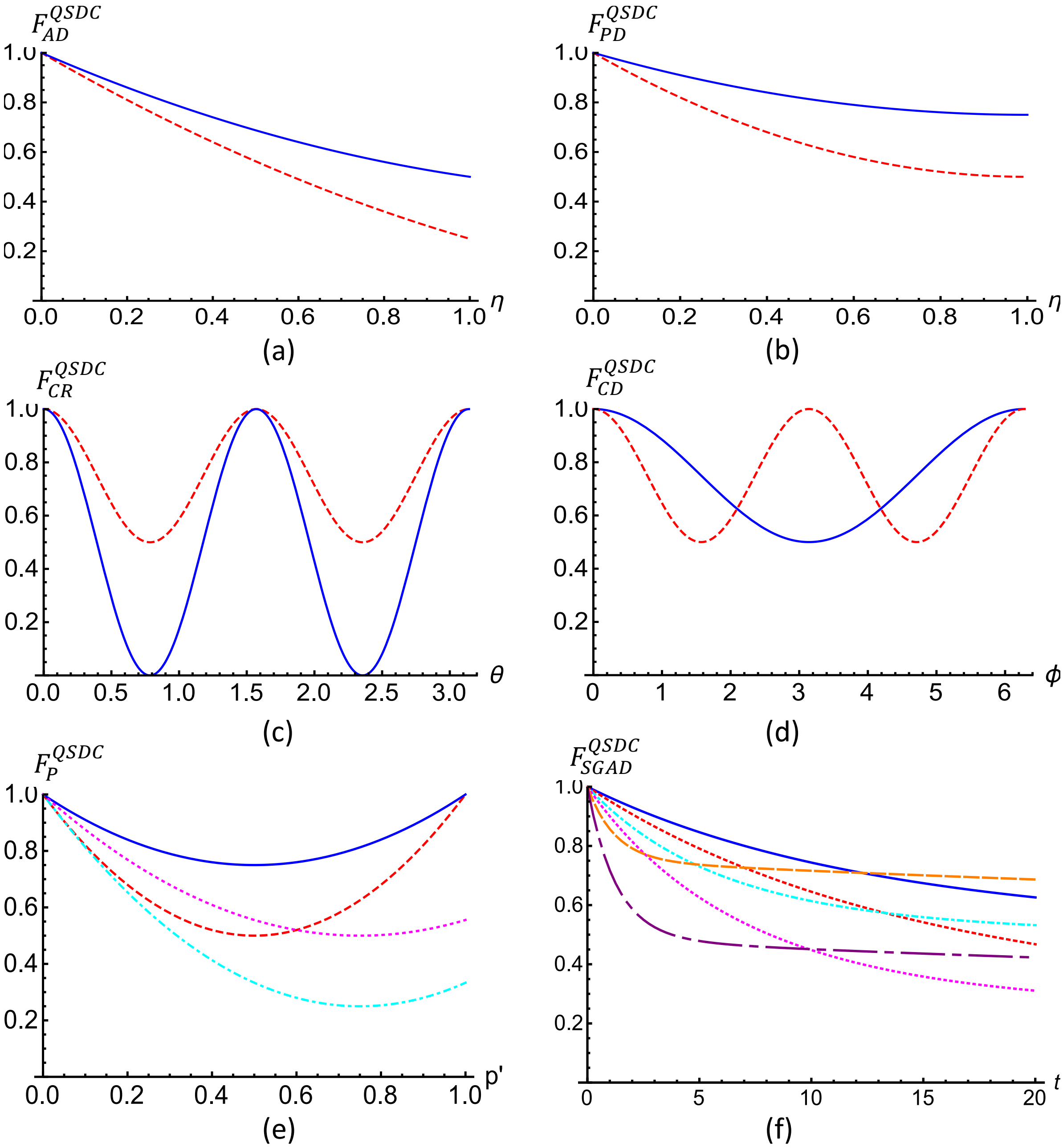

Figure 4.5: QSDC under AD, PD, CR and CD noises are depicted in (a), (b), (c) and (d), respectively. The smooth (blue) and dashed (red) lines correspond to LM05 and PP protocols, respectively. For CR and CD noises it is assumed that the noise parameter is same for both the directions of travel of the qubit (i.e., Alice to Bob and Bob to Alice). In (e), the fidelity under the depolarizing channel for LM05 and PP protocols are shown in dotted (magenta) and dotted dashed (cyan) lines, respectively. In all the remaining cases of PP and bit phase flip for LM05 the red line illustrates the fall and revival in fidelity. Lastly, the blue line corresponds to the fidelity in bit flip and phase flip errors in LM05 scheme. (f) illustrates the effect of AD (i.e., an interaction with a zero temperature and squeezing bath) in smooth (blue) and dashed (red) lines; GAD (i.e., an interaction with a non-zero temperature and zero squeezing bath) in dotted dashed (cyan) and dotted (magenta) lines with $T = 1$; and SGAD (finite temperature and squeezing bath) in large dashed (orange) and large dotted dashed (purple) lines with $T = 1$ and squeezing parameters $r = 1$ and $\Phi = \frac{\pi}{8}$ for LM05 and PP protocols, respectively.

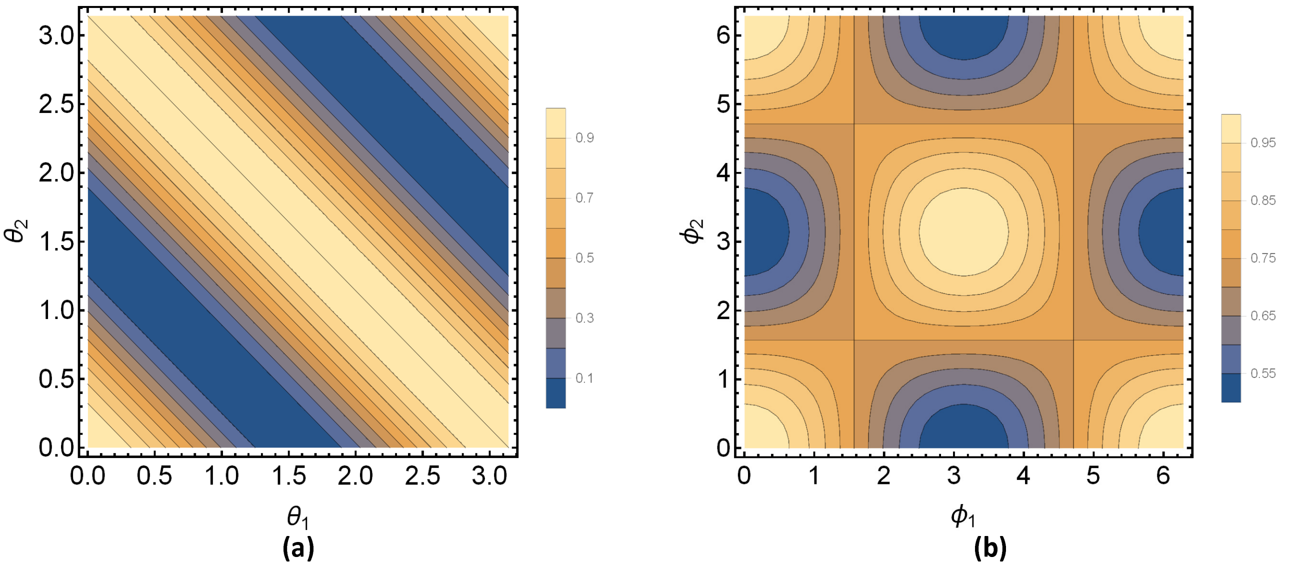

Figure 4.6: Contour plots of fidelity of LM05 protocol when subjected to CR and CD noises in (a) and (b), respectively.

value 0 (1). Subsequently, she encodes a checking message on the decoy qubits using the same scheme and concatenates these two encoded sequences. Finally, she sends this concatenated sequence after randomizing to Bob while keeping the last sequence with herself.

QD 4 After receiving authenticated receipt of all the qubits from Bob, Alice will announce the positions of the decoy qubits and being aware of the preparation basis he decodes the message and announces it publicly. With this checking message Alice decides whether to go to the next step or start afresh.

QD 5 If they decide to proceed, Bob also encodes on the received qubits after rearranging them using the same encoding scheme as Alice. Subsequently, he performs measurement on all these qubits in the basis in which they were prepared and announces the measurement outcomes. From the measurement outcomes, Bob gains the knowledge of Alice's encoding as he knows his encoding apart from the initial and final state. Further, the measurement outcomes also reveal the choice of the basis used for preparation of the states. Using this information Alice measures the third sequence, she had kept with herself in QD 3, in a suitable basis and learns the initial state of Bob. From the information of the initial and final states, Alice can extract the message of Bob by using her knowledge of her encoding.

The fidelity expression of single-qubit-based QD scheme under AD channel contains cubic terms

$$F_{AD1}^{QD}=\frac{1}{8}\left(-2\eta^{3}+5\eta^{2}-\left(\sqrt{1-\eta}+7\right)\eta+2\left(\sqrt{1-\eta}+3\right)\right), \tag{4.34}$$

which signify bidirectional quantum communication apart from a QSDC to inform Bob about the initial state. This fact can also be observed in PD noise

$$F_{PD1}^{QD} = \frac{1}{8}\left(-\eta^3 + 4\eta^2 - 6\eta + 8\right). \tag{4.35}$$

For the two rounds of communication under collective noisy channels, characterized by two noise parameters, the fidelity for CD is

$$F_{CD1}^{QD} = \frac{1}{8}\left(\cos^2(\phi_1)\cos(\phi_2) + \cos(\phi_1)(\cos(\phi_2) + 1) + 5\right), \tag{4.36}$$

and for CR noise is

$$F_{CR1}^{QD} = \cos^2(\theta_1)\cos^2(\theta_1 + \theta_2). \tag{4.37}$$

Similarly, all the qubits traveling through a Pauli channel give rise to the fidelity as a function of various parameters, as

$$\begin{array}{rcl} F_{P1}^{QD} & = & \frac{1}{2}\left\{2p_1^3 + 3p_1^2(p_2 + p_4) + 2p_1\left(2p_2^2 + p_2p_3 + p_3^2 + p_3p_4 + 2p_4^2\right)\right. \\ & & \left. +p_2^3 + p_2^2p_4 + p_2\left(p_3^2 + 4p_3p_4 + p_4^2\right) + p_4\left(p_3^2 + p_4^2\right)\right\}. \end{array} \tag{4.38}$$

$$\begin{array}{l} F_{SGAD1}^{QD} = \frac{1}{16}\left\{Q^3\left(-4\lambda^3 + 4(3\mu + \nu)\lambda^2 - 2\left(6\mu^2 + 4\nu\mu + 2\nu^2 + \sqrt{1-\lambda} - 3\sqrt{1-\mu}\sqrt{1-\nu}\right)\lambda\right.\right. \\ \qquad\qquad -6\sqrt{1-\lambda}\mu + 9\sqrt{1-\lambda}\mu\nu - 6\sqrt{1-\lambda}\nu - 5\sqrt{1-\mu}\mu\sqrt{1-\nu}\nu + 2\sqrt{1-\mu}\sqrt{1-\nu}\nu \\ + 4(\mu + \nu)\left(\mu^2 + \nu^2\right) + 8\sqrt{1-\lambda} + 2\sqrt{1-\mu}\mu\sqrt{1-\nu} - 8\sqrt{1-\mu}\sqrt{1-\nu}\Big) \\ -Q^2\left(12\mu^3 + 2(6\nu - 5)\mu^2 + 3\left(\nu\left(4\nu + 6\sqrt{1-\lambda} - 5\sqrt{1-\mu}\sqrt{1-\nu} - 5\right) + 2\sqrt{1-\mu}\sqrt{1-\nu}\right)\mu\right. \\ +2\left(-6\sqrt{1-\lambda}\mu + \mu + \nu + 2\sqrt{1-\lambda}\left(\sqrt{1-\mu}\sqrt{1-\nu} - 3\nu\right) + 6\sqrt{1-\lambda} - 6\sqrt{1-\mu}\sqrt{1-\nu} - 2\right) \\ +2\nu\left(\nu(6\nu - 5) + 3\sqrt{1-\mu}\sqrt{1-\nu}\right) + 2\lambda\left(6\nu - 2\left(2\nu^2 + 4\mu\nu + \mu(6\mu - 5)\right) + 3\sqrt{1-\mu}\sqrt{1-\nu} + 1\right) \\ + 2\lambda^2(6\mu + 2\nu - 5)\Big)\Big) + \left(3\left(\nu\left(4\nu + 3\sqrt{1-\lambda} - 5\sqrt{1-\mu}\sqrt{1-\nu} - 10\right) + 2\sqrt{1-\mu}\sqrt{1-\nu}\right)\mu\right. \\ +12\mu^3 + 2\left(\left(8 - 3\sqrt{1-\lambda}\right)\mu + 8\nu + \sqrt{1-\lambda}\left(2\sqrt{1-\mu}\sqrt{1-\nu} - 3\nu\right) + 4\sqrt{1-\lambda} - 4\sqrt{1-\mu}\sqrt{1-\nu} - 2\right) \\ \left.\left. + 4(3\nu - 5)\mu^2 - 4\lambda\left(3\mu^2 + (2\nu - 5)\mu + (\nu - 3)\nu + 3\right) + 2\nu\left(2\nu(3\nu - 5) + 3\sqrt{1-\mu}\sqrt{1-\nu}\right)\right)\right\}. \end{array} \tag{4.39}$$

(b) Ba An protocol of QD

In the originally proposed Ba An's QD scheme, both parties can communicate simultaneously using Bell states [Nguyen, 2004; An, 2005; Shukla et al., 2013b]. The protocol can be summarized in the following steps:

QD:BA 1 Bob prepares $|\psi^+\rangle^{\otimes n}$: $|\psi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. He encodes his message on the first qubit (travel qubit) and keeps the second qubit with himself as home qubit. To encode his message he uses dense coding, i.e., he applies unitary operations I, X, iY and Z to encode 00, 01, 10 and 11, respectively.

QD:BA 2 Bob sends all the first qubits to Alice and confirms their receipt.

QD:BA 3 Alice also encodes on the travel qubit using the same rule as was used by Bob and sends them back to Bob. Bob performs a Bell measurement on the partner particles (Bell measurement is done on a qubit from the sequence of home qubits and another qubit from the sequence of travel qubits, which was initially entangled with the chosen home qubit).

QD:BA 4 After Alice's disclosure Bob comes to know whether it was message mode (MM) or control mode (CM)[2]. Bob announces his measurement outcome in the MM using which both Alice and Bob can learn each others message. While in CM Alice announces her encoding which Bob uses for eavesdropping checking.

In the original Ba An's QD scheme, when subjected to AD and PD noise, the fidelity can be seen to be

$$F^{QD}_{AD2} = \frac{1}{4}(\eta - 2)^2, \tag{4.40}$$

and

$$F^{QD}_{PD2} = \frac{1}{2}\left(\eta^2 - 2\eta + 2\right), \tag{4.41}$$

respectively. The presence of quadratic terms is a signature of bidirectional quantum communication involved. Under the coherent effect of CD noise on the travel qubits, we obtain

$$F^{QD}_{CD2} = \frac{1}{2}\left\{\cos(\phi_1)\cos(\phi_2) + 1\right\}, \tag{4.42}$$

and for CR noise the fidelity is found to be

$$F^{QD}_{CR2} = \frac{1}{2}\left\{\cos^2(\theta_1 - \theta_2) + \cos^2(\theta_1 + \theta_2)\right\}. \tag{4.43}$$

When the travel qubit is transmitted through a Pauli channel the fidelity is the same as that obtained in case of PP protocol. The analytic expression of fidelity for Ba An protocol of QD, when subjected to SGAD noise is

$$\begin{array}{rcl} F^{QD}_{SGAD2} & = & \frac{1}{4}\left\{Q^2\left(\lambda^2 - 2\lambda(\mu+\nu+1) - 2\left(2\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu} + \mu + \nu - 2\right) + \mu^2 + 5\mu\nu + \nu^2\right.\right. \\ & + & \mu^2 + \mu(5\nu - 4) + (\nu - 2)^2 + \mu\nu(Q-1)^2\cos(2\Phi) \\ & + & \left.2Q\left(\lambda(\mu+\nu-1) + 2\sqrt{1-\lambda}\sqrt{1-\mu}\sqrt{1-\nu} - \mu^2 + \mu(3 - 5\nu) - (\nu-3)\nu - 2\right)\right\}. \end{array} \tag{4.44}$$

When both the protocols of QD are subjected to AD noise the fidelity obtained for the entangled-state-based protocol is comparable of that of the single-qubit-based one. This

[2] In fact, a random choice of MM or CM mode by Alice provides security in the protocol. In CM mode, both the legitimate parties opt to check eavesdropping while in MM mode they proceed with the communication.

is in contrast with the earlier observations reported in the present work, where single-qubit-based schemes were found to be preferable in cases of AD and PD noise models. Though, in the large decoherence limits the single-qubit-based QD turns out to be a suitable candidate (cf. Fig. 4.7 a). It is worth commenting here that the decay in the fidelity of single-qubit-based QD scheme when compared with the corresponding QSDC protocol (as they are of the same order in entanglement-based schemes) can be attributed to an extra single qubit traveling through the noisy channel in step QD 1. However, under the effect of PD channels, the observation established from the previous three secure quantum communication schemes (namely, QKD, QKA and QSDC protocols) remains valid (cf. Fig. 4.7 b), in other words, it is observed that the single-qubit-based schemes perform better in PD channels. When Ba An protocol of QD is subjected to collective noise the same nature of fidelity variation as was observed in PP protocol is observed if the same noise parameters are used in to and fro travel of the qubits. However, in the single-qubit-based QD scheme a different nature from LM05 protocol is observed. Interestingly, a close look at Figs. 4.5 c (d), and Fig. 4.7 c (d) reveals that compared to LM05 protocol, an extra dip is observed at $\theta = \frac{\pi}{2}$ (where for LM05 fidelity was obtained to be unity). This dip was observed in single-qubit-based QKA scheme, too (cf. Fig. 4.3 c). This point further establishes the fact that the fidelity of single-qubit-based QD schemes decays, when subjected to AD noise. The contour plots shown in Fig. 4.8 also demonstrate that the single-qubit-based QD scheme has a different nature of fidelity variation compared to that in LM05 protcol, while in entangled-state-based protocol it remains similar to that observed in PP.

The expression of fidelity under Pauli noise shows that for Ba An protocol of QD it is the same as in PP protocol. However, the presence of cubic terms in the expressions of fidelity for single-qubit-based QD is a signature of the nature observed in Fig. 4.7 e, i.e., the descent for very low and high error probabilities. For the bit/phase flip error the single-qubit-based scheme remains the preferred choice, but for very high probability of errors it should be avoided. A similar nature is also observed under the influence of a depolarizing channel. For bit-phase flip error, fidelity indicates better performance of entanglement-based scheme as compared to their single-particle counterparts.

Under a dissipative interaction with a non-zero temperature bath, a behavior similar to that observed under an AD channel is seen. However, due to the non-zero squeezing, single-qubit-based QD scheme turns out to be a better candidate. Fig. 4.7 f further reiterates the facts observed in Fig. 4.7 a-d, i.e., the obtained nature in the case of Ba An protocol of QD is the same as in PP protocol; and in single-qubit-based scheme, it can be explained as a compound effect of single-qubit-based QKA and QSDC protocols.

4.5 Conclusion

The comparative study of single-qubit-based and entangled-state-based schemes of secure quantum communication performed in the present work has lead to a number of interesting conclusions. Firstly, the equivalence observed in the ideal noiseless scenario is lost in more practical scenarios where noise is present. Next, it is observed that it is not possible to say unambiguously that in a noisy environment entangled-state-based protocols perform better than the single-qubit-based protocols or vice versa. In fact, it depends on the nature of the noise present in the channel. Specifically, single-qubit-based schemes are generally found to be the suitable choice in the presence of AD and/or PD noises, while entanglement-based protocols turn out to be preferable in the presence of collective noise. As SGAD and GAD channels are generalizations of the AD channel, conclusions similar to that

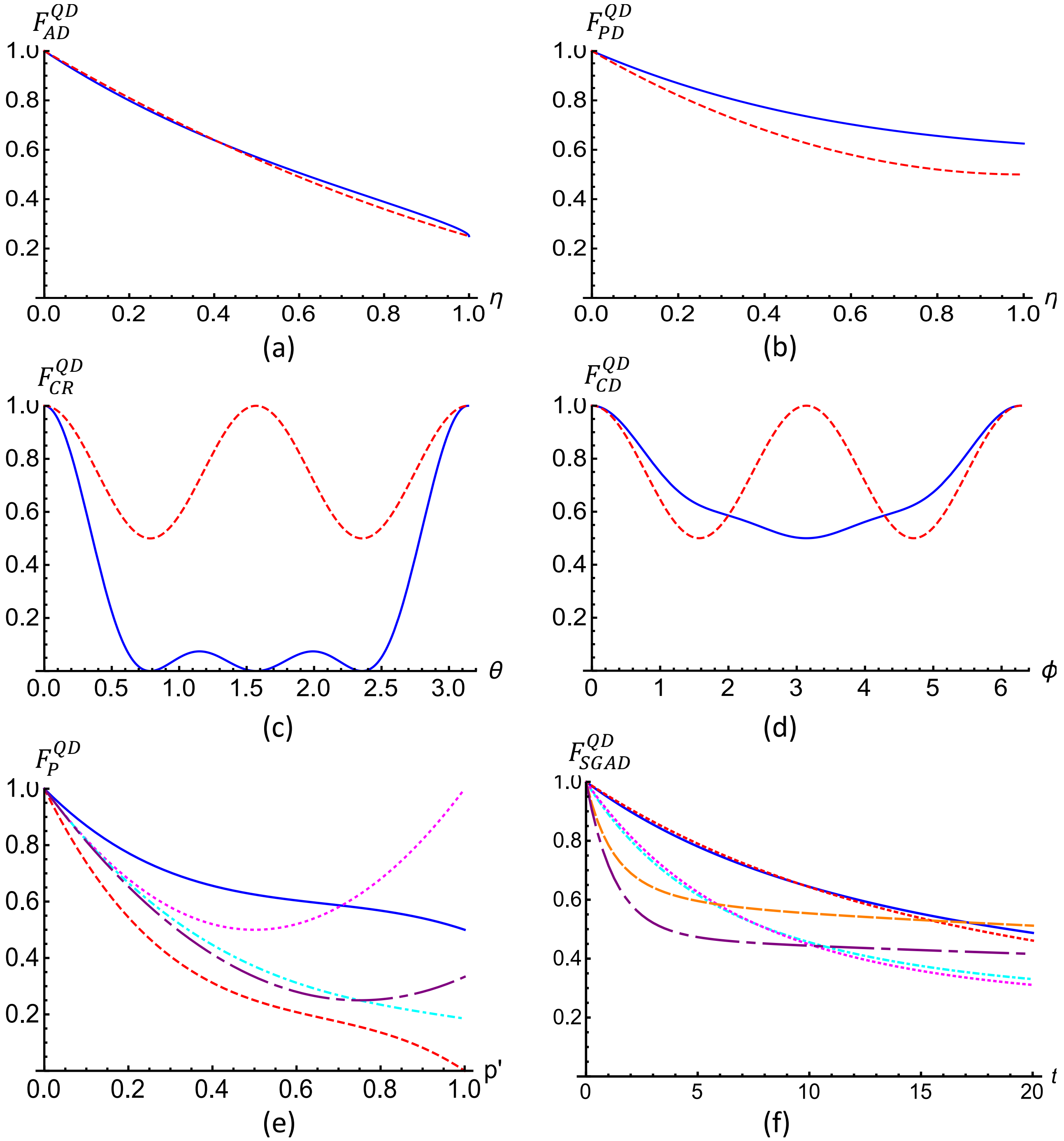

Figure 4.7: QD protocols are analyzed under AD, PD, CR and CD noises in (a)-(d), respectively. The smooth (blue) and dashed (red) lines correspond to the single-qubit-based and Ba An's QD protocols, respectively. For CR and CD noises it is assumed that the noise parameter is same for both the directions of travel of the qubit (i.e., Alice to Bob and Bob to Alice). In (e), bit/phase flip is shown together for the single-qubit-based QD and Ba An protocol of QD in smooth (blue) and dotted (magenta) lines, respectively. For Ba An protocol of QD bit phase flip errors matches exactly with the previous case. However, for single-qubit-based scheme, it is shown in dashed (red) line. Under the depolarizing channel the fidelity variation for the single-qubit-based scheme and Ba An protocol of QD is demonstrated by dotted dashed (cyan) and large dotted dashed (purple) lines, respectively. (f) corresponds to the effect of AD (i.e., an interaction with a zero temperature and squeezing bath) in smooth (blue) and dashed (red) lines; GAD (i.e., an interaction with a non-zero temperature and zero squeezing bath) in dotted dashed (cyan) and dotted (magenta) lines with $T = 1$; and SGAD (finite temperature and squeezing bath) in large dashed (orange) and large dotted dashed (purple) lines with $T = 1$ and squeezing parameters $r = 1$ and $\Phi = \frac{\pi}{8}$ for the single-qubit-based and Ba An's QD protocols, respectively.

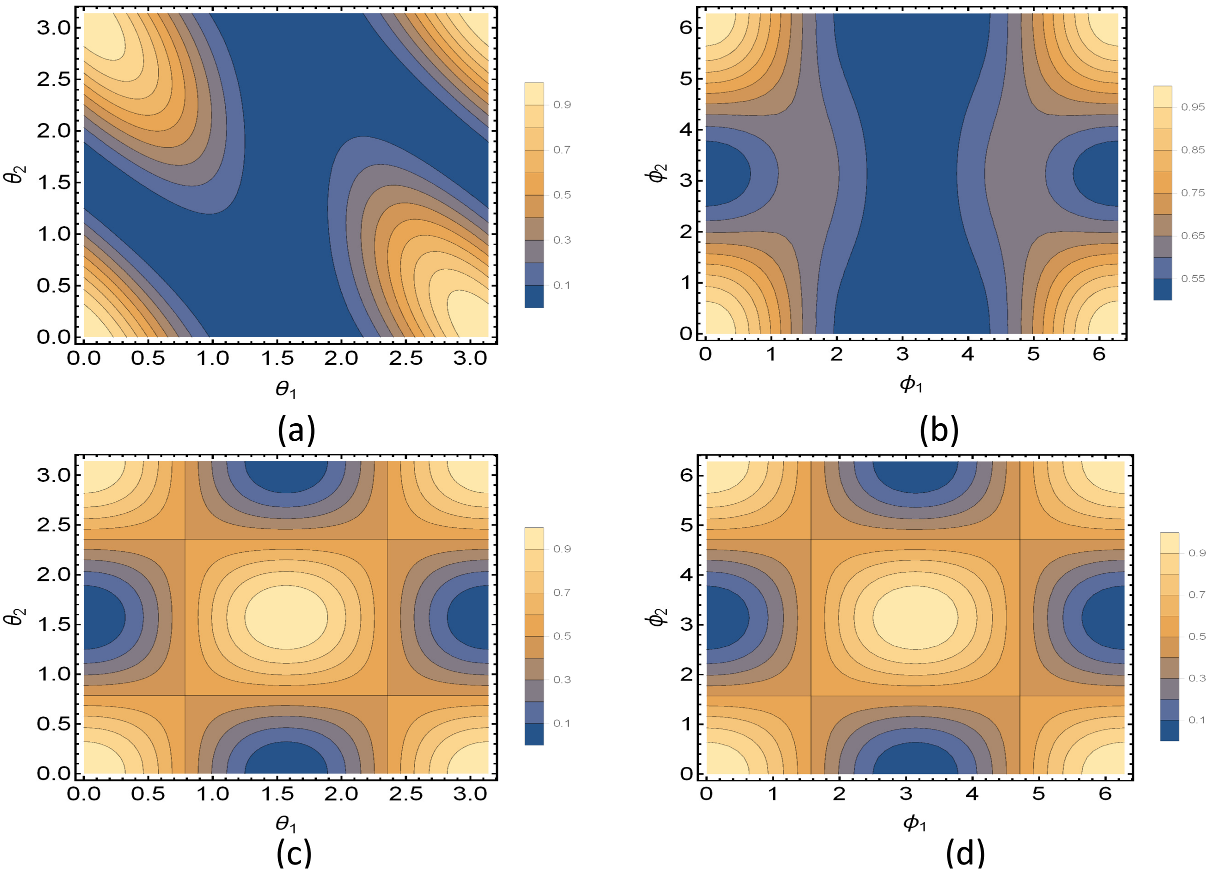

Figure 4.8: Contour plots illustrating the variation of fidelity of the single-qubit-based Shi et al. protocol and entangled-state-based Ba An protocol of QD in CR and CD noises, respectively.

for the AD channel are also applicable to them. However, with an increase in temperature, fidelity is seen to decay. Squeezing is seen to play the role of a beneficial quantum resource, in a host of scenarios, in practical quantum communication. Also, it is observed that the effect of noise depends upon the number of rounds (how many times a travel qubit travels through the noisy channel) of quantum communication involved. For instance, QKD protocols are least affected by noise, while QD protocols are most affected as in QKD protocols a travel qubit travels only once through the noisy channel, whereas in Ba An protocol of QD, it travels twice through the noisy channel. Further, the single-qubit-based QD scheme involves three rounds of communication as it requires Alice to Bob and Bob to Alice transmission of qubits and an additional Alice to Bob travel of equal number of qubits. As a consequence, single-qubit-based QD scheme is found to be the most affected among the four different single-qubit-based schemes for secure quantum communication discussed in this chapter.

The DPS (Differential Phase Shift) QKD protocol, in its practical application, is capable of communicating the quantum information between the quantum repeater nodes for long distance by deploying optical fiber as a quantum channel. This is because of its high key rates and ease of practical implementation. But, the various attacks must be considered for DPS QKD protocol for security issues. Similar to B92 protocol, in DPS QKD protocol, Alice also randomly prepares the quantum states and sends two non-orthogonal states to Bob, opposite to B92 protocol, in DPS QKD protocol, we need not to use a bright reference pulse but requires a weak coherent pulse (WCP) with less than one average number of photon, hence practically easy and simple to perform as compared to B92 protocol.

The quantum noise generated due to the fiber imperfections could provide a large amount of noise, so it is the main concern to deal with such noise while considering optical fibers for transmission of quantum information. Proper care should be taken when modulation speed is 40 Gb/s and above because it may severely degrade the quantum signal strength. Hence, We need a practical quantum communication system which is flexible, easily implementable and efficient with low communication complexity.

We conclude by noting that the comparison between two different types of resources (single qubits and entangled qubits), used for different quantum cryptographic tasks, does not show any specific advantage of entanglement based schemes unless we consider device independence. This is an interesting observation, as we know that entanglement can offer an advantage in some quantum communication tasks. For example, teleportation and dense coding cannot be performed without entanglement. Thus, the use of entanglement is justified in the implementation of protocols of dense coding and teleportation. However, for the quantum cryptographic tasks described here, one may circumvent the use of entanglement, which is a physically more expensive quantum resource compared to single qubits. Specifically, if the communication is done via a well characterized quantum channel, where it is known that the noise acts independently on each qubit, then entanglement-based protocols are not required for the implementation of any cryptographic task considered here. In other words, in such situations, we can work with a less expensive quantum resource (single qubit). This summarizes the practical relevance of the present work. Further, keeping this relevance in mind, we expect that the present observation will help experimentalists to select appropriate protocols and resources based on the characteristics of the quantum channel (nature of noise present in the quantum channel) used.