Quantum cryptography over non-Markovian channels

Kishore Thapliyal[a,*], Anirban Pathak[a,†], Subhashish Banerjee[b,‡]

[a]*Jaypee Institute of Information Technology, A 10, Sector-62, Noida, UP-201307, India*
[b]*Indian Institute of Technology Jodhpur, Rajasthan-342011, India*

A set of schemes for secure quantum communication are analyzed under the influence of non-Markovian channels. By comparing with the corresponding Markovian cases, it is seen that the average fidelity in all these schemes can be maintained for relatively longer periods of time. The effects of non-Markovian noise on a number of facets of quantum cryptography, such as quantum secure direct communication, deterministic secure quantum communication and their controlled counterparts, quantum dialogue, quantum key distribution, quantum key agreement, etc., have been extensively investigated. Specifically, a scheme for controlled quantum dialogue (CQD) is analyzed over damping, dephasing and depolarizing non-Markovian channels, and subsequently, the effect of these non-Markovian channels on the other schemes of secure quantum communication is deduced from the results obtained for CQD. The damped non-Markovian channel causes, a periodic revival in the fidelity; while fidelity is observed to be sustained under the influence of the dephasing non-Markovian channel. The depolarizing channel, as well as the other non-Markovian channels discussed here, show that the obtained average fidelity subjected to noisy environment depends on the strength of coupling between the quantum system with its surroundings and the number of rounds of quantum communication involved in a particular scheme.

PACS numbers: 03.67.Dd,03.67.Hk,42.50.Lc
Keywords: non-Markovian channel, depolarizing channel, quantum cryptography, secure quantum communication

I. INTRODUCTION

Quantum cryptography, after its inception in 1984 [1], has been flourishing over the last decade. The prime reason is the possibility of unconditional security, a task unachievable in the domain of classical physics. This fact and already available marketable products based on quantum cryptography have motivated further research in this field. To name a few, apart from the initial interest in quantum key distribution (QKD) [1–5], various schemes concerning direct communication (secure communication circumventing the need of a prior shared key) [6–11], quantum key agreement (QKA) [12], quantum secret sharing [13], have been proposed in the recent past (see [14] for details). Specifically, in the direct communication, the receiver may or may not require an additional classical information to decode the message sent by the sender; depending upon this, the protocol falls under the category of deterministic secure quantum communication (DSQC) [10] and quantum secure direct communication (QSDC) [6–9], respectively. There is another novel technique of direct communication, quantum dialogue (QD) [15], where both the users can send their information simultaneously, with no need of a prior shared key.

All these schemes for secure direct quantum communication, provide us a vast potential for extension and modification to design protocols required in various real life scenarios. One such important facet of quantum cryptography provides solutions for maintaining the hierarchy in offices or government, in terms of the information accessible to each user. Hierarchical quantum communication schemes are aimed to deal with these problems, when either only single sender holds all the information [16] or it is distributed among two of them [17]. We may consider another important scenario, where a controller supervises the communication among all the remaining users, and he can maintain his control by making sure that the communication is not accomplished without his consent [11, 18, 19]. Further, a scheme for quantum controlled communication based on a quantum cryptographic switch has been proposed recently, which allows the supervisor to control even the amount of information he wishes to share with the other users in a continuously varying degree [18, 19].

It would be worth summarizing that the security achieved in all the cryptographic schemes is based on the principle of splitting the whole information in many pieces, and the whole information can only be extracted if all the pieces are available simultaneously. Usually, one of the parties prepares an entangled state to be used as a quantum channel and shares it with all other parties in a secure way. By secure, we mean that a proper eavesdropping checking technique is employed, after inserting the decoy qubits with the entangled qubits to ensure the absence of Eve. Once this channel is shared the legitimate parties can securely share their secrets, either by teleportation or encoding their information using Pauli operations and sending the qubits to the receiver again in a secure manner. An interesting observation, we would like to exploit here, is that if we start with a controlled quantum dialogue (CQD) scheme, we can reduce it to almost all the schemes of secure quantum communication. This point is discussed in detail in the forthcoming sections.

The feasibility of implementation of various quantum communication schemes when subjected to noisy environment has been analyzed in the past. In particular, the schemes of QKD [20], QKA [20], controlled DSQC (CDSQC) [19], QSDC [20], CQD [18], QD [20], asymmetric QD (AQD) [21], con-

[*] Email: tkishore36@yahoo.com
[†] Email: anirban.pathak@gmail.com
[‡] Email: subhashish@iitj.ac.in

trolled bidirectional remote state preparation [22], among others, have been considered under the influence of both purely dephasing and damping noises. Most of these investigations (cf. [18–21]) were restricted to the domain of Markovian environments [23, 24], though, some attempts have been made to study the effects of non-Markovian environments on quantum communication schemes, such as teleportation [25, 26], densecoding [26] and entanglement swapping [27, 28]. The security of a QKD protocol has also been analyzed over non-Markovian depolarizing channel [29]. All these attempts (except Ref. [29]) to examine the usefulness of entangled states under the influence of non-Markovian environments were restricted to insecure quantum communication, where security is not required. However, in the secure quantum communication protocols, it becomes relevant to differentiate the disturbance caused due to eavesdropping and the effects of noise. This sets the motivation for this work, where we wish to analyze the effect of non-Markovian noisy environment considering the scenario when no eavesdropping has been attempted. This would provide a threshold of error due to disturbance from a non-Markovian environment; errors exceeding this could be attributed to the presence of an eavesdropper. Specifically, we would consider pure dephasing, damping and depolarizing interactions with a non-Markovian reservoir. Though entanglement can only be maintained for relatively longer time due to dephasing non-Markovian interaction [30], it can show revival under dissipative interactions [31]. As we are essentially using entangled states and entanglement revival could be an interesting feature to affect the feasibility of quantum cryptographic schemes, we would like to address the problem here.

Non-Markovian noise has been attracting a lot of interest from both quantum optics and quantum information communities, theoretically as well as experimentally. A paradigm for studying non-Markovian evolution is the quantum Brownian motion [32–34]. Specifically, degradation of purity and nonclassicality of Gaussian states have been studied under the effect of non-Markovian channels [35]. Dynamics of entanglement has been discussed in both discrete [31, 36–38] and continuous [39] variable channels. Recently, dynamics of multipartite entanglement and its protection have been addressed [40]. The additional problems due to non-Markovian noise in quantum error correction [41] and dynamical deocupling [42, 43] have also been discussed in the past. The non-Markovianity was also characterized from an information theoretic approach in terms of quantum Fisher information flow [44]. A number of beautiful experiments depicting non-Markovian nature of the system-reservoir interaction have been performed [45–47].

First, the Kraus operators of non-Markovian dissipative and dephasing noise models are discussed in a concise manner (in Section II). In Section III, we introduce, briefly, a CQD scheme (III A) using Bell states and based on the quantum cryptographic switch. Then, we study the effect of non-Markovian noise on the feasibility of the CQD scheme. To quantify the effect of noise, a distance-based measure known as fidelity has been calculated. Next, we reduce the scheme of CQD to design a CDSQC protocol (in Section III B), a QD protocol (in Section III C), a DSQC and QSDC protocols (in Section III D), a QKA protocol (in Section III E), and finally, two well known QKD protocols (in Section III F). The QKD protocols discussed here are well known as BB84 [1] and BBM [5] protocols. The feasibility of all these schemes under the action of non-Markovian channels are also analyzed. Finally, we conclude the paper in Section IV.

II. NON-MARKOVIAN NOISE MODELS

We briefly discuss below, a few non-Markovian models that are subsequently used to study the performance of various quantum cryptographic schemes. The dynamics of a system interacting with its surroundings can be expressed in terms of Kraus operators as

$$\rho\left(t\right)=\sum_{i}K_{i}\left(t\right)\rho\left(0\right)K_{i}^{\dagger}\left(t\right) \tag{1}$$

(see [48] for a review). Here, we use this approach to describe the dissipative and purely dephasing interactions with non-Markovian environments. The Kraus operators for the damping noise under non-Markovian effects are given by [31]

$$K_{0}=|0\rangle\langle0|+\sqrt{p}|1\rangle\langle1|,\qquad K_{1}=\sqrt{1-p}|0\rangle\langle1|, \tag{2}$$

where $p\equiv p\left(t\right)=\exp\left(-\Gamma t\right)\left\{\cos\left(\frac{dt}{2}\right)+\frac{\Gamma}{d}\sin\left(\frac{dt}{2}\right)\right\}^{2}$ with $d=\sqrt{2\gamma\Gamma-\Gamma^{2}}$. Here, Γ is the line width which depends on the reservoir correlation time $\tau_{r}\approx\Gamma^{-1}$; and γ is the coupling strength related to qubit relaxation time $\tau_{s}\approx\gamma^{-1}$. In the domain of large reservoir correlation time in comparison to qubit relaxation time, memory effects come into play. The memory effects are characteristic of non-Markovian nature of dissipation. Interestingly, taking $p=1-\eta$, the results obtained for amplitude damping noise under Markovian regime can be deduced, with η being the decoherence rate of amplitude damping channel.

Similarly, the Kraus operators for purely dephasing non-Markovian noise are [30]

$$K_{0}=|0\rangle\langle0|+p|1\rangle\langle1|,\qquad K_{1}=\sqrt{1-p^{2}}|1\rangle\langle1|, \tag{3}$$

where $p\equiv p\left(t\right)=\exp\left[-\frac{\gamma}{2}\left\{t+\frac{1}{\Gamma}\left(\exp\left(-\Gamma t\right)-1\right)\right\}\right]$. All the parameters have the same meaning as above. As in the case of dissipative noise, the result for the well known phase damping channel can be obtained from Eq. (3) by considering $p=\sqrt{1-\eta}$. In what follows, we consider an independent environment for each qubit as it travels through different channels; a similar assumption has been made in [49, 50].

Finally, a non-Markovian depolarizing channel can be described by the Kraus operators $K_{i}=\sqrt{\mathcal{P}_{i}}\sigma_{i}$, where $\sigma_{0}\equiv I$ and σ_{i}s are the three Pauli matrices. The $\mathcal{P}_{i}$s should remain positive to ensure the complete positivity for all values of $\frac{\gamma_{j}}{\Gamma_{j}}$ and are given by [51]

$$\mathcal{P}_{1}=\frac{1}{4}\left[1+\Omega_{1}-\Omega_{2}-\Omega_{3}\right],$$

$$\mathcal{P}_2 = \frac{1}{4}\left[1 - \Omega_1 + \Omega_2 - \Omega_3\right],$$

$$\mathcal{P}_3 = \frac{1}{4}\left[1 - \Omega_1 - \Omega_2 + \Omega_3\right],$$

and

$$\mathcal{P}_4 = \frac{1}{4}\left[1 + \Omega_1 + \Omega_2 + \Omega_3\right].$$

Here, $\Omega_i = \exp\left(-\frac{\Gamma t}{2}\right)\left[\cos\left(\frac{\Gamma d_i t}{2}\right) + \frac{1}{d_i}\sin\left(\frac{\Gamma d_i t}{2}\right)\right]$ with $d_i = \sqrt{16\left(\frac{\gamma_j^2}{\Gamma_j^2} + \frac{\gamma_k^2}{\Gamma_k^2}\right) - 1}$ for $i \neq j \neq k$ [51]. Further, γ is the coupling strength of the system and Γ is the noise bandwidth parameter. It should be noted that the Markovian case can be deduced from the above by taking $\Omega_i = \exp\left(-\frac{\gamma_i t}{2}\right)$ with $\gamma_i = \frac{4}{\Gamma}\left(\gamma_j^2 + \gamma_k^2\right)$ for $i \neq j \neq k$ [51].

III. EFFECT OF NON-MARKOVIANITY ON THE SECURE QUANTUM COMMUNICATION SCHEMES

In what follows, we consider a set of quantum cryptographic protocols and analyze the feasibility of their implementation over the above discussed non-Markovian channels. For all the one-way schemes for quantum cryptography that are discussed here, we consider Alice as the sender and Bob as the receiver, unless stated otherwise; whereas, Charlie is the third party supervising the protocol and referred to as the controller. However, for two-way schemes (e.g., QD, CQD), both Alice and Bob are considered to play dual roles of receiver and sender.

A. CQD

Let us start with a three party protocol for quantum cryptography, where two parties (Alice and Bob) wish to communicate simultaneously under the control of a third party (Charlie). In fact, all the controlled communication protocols work under an assumption that all the parties are semi-honest. Otherwise, Alice and Bob can share a quantum state of their own and circumvent Charlie's control. In literature, this is sometimes viewed as Alice and Bob lacking resources for state preparation, and consequently, they do not set up a quantum channel between them, rather they rely on Charlie to prepare it for them.

To begin with, we consider a CQD scheme recently proposed by some of the present authors [18]. Charlie prepares n copies of a Bell state and makes two strings S_A and S_B of all the first and second qubits. Subsequently, he sends both the strings to Bob, only after permuting S_B[1]. Bob will encode his message by using Pauli operations on the qubits in string S_A. Subsequently, Bob sends S_A to Alice, who returns it to him after encoding her secret message as Bob did. It is pre-decided that Pauli operations I, X, iY, and Z correspond to encoded bit values 00, 01, 10, and 11, respectively. Finally, Charlie discloses the permutation operator, and using this information Bob performs a Bell measurement on the partner qubits (Bell pairs). When Bob announces the measurement outcome, both Alice and Bob can extract each other's message using their own encoding information and the knowledge of initial Bell state prepared by Charlie. If the choice of Bell state prepared by Charlie is made public, it leads to some leakage, which is often considered to be an inherent characteristic of schemes for QD and its variants. However, such leakage can be circumvented if Charlie chooses the Bell state randomly and sends his choice to Alice and Bob by using a scheme of DSQC or QSDC [21]. In fact, the schemes of QD are the most efficient protocols without involving prior key generation.

Suppose Charlie started with the initial state $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \{|\psi^{\pm}\rangle, |\phi^{\pm}\rangle\}$, and $|\psi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$, $|\phi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$. The transformed density matrix over the noisy channel would become

$$\begin{aligned}\rho' = & \sum_{A_n,B_n}\sum_{i,j,k,l}\left(K_l\left(p_4\right)\otimes I\right)U_{A_n}\left(K_k\left(p_3\right)\otimes I\right)U_{B_n} \\ & \times \left(K_i\left(p_1\right)\otimes K_j\left(p_2\right)\right)\rho\left(\left(K_i\left(p_1\right)\otimes K_j\left(p_2\right)\right)\right)^{\dagger} \\ & \times \left(\left(K_l\left(p_4\right)\otimes I\right)U_{A_n}\left(K_k\left(p_3\right)\otimes I\right)U_{B_n}\right)^{\dagger},\end{aligned} \tag{4}$$

where K_is are the Kraus operators for a specific kind of noise discussed in the previous section and U_js are the Pauli operations by Alice and Bob with $j \in \{j_{00}, j_{01}, j_{10}, j_{11}\}$ for $\{I, X, iY, Z\}$. Here, we have used different values of p_is corresponding to each operation of the Kraus operator (from Eq. (2), (3) or the depolarizing channel) on the initial quantum state as the coupling strength during various rounds of the quantum communication is assumed to be different. It may be noted that the second summation in the right hand side of Eq. (4) ensures that the map is positive while the first summation corresponds to the average over all the possible encoding operations that Alice and Bob are allowed to perform. Thus, the fidelity that we are discussing here, and in the rest of the paper, is the average fidelity. Further, here, we have assumed that the qubits not traveling through a quantum channel are not affected by noise. There are various distance-based measures to quantify the effect of noise on the quantum state, such as trace distance, fidelity, and the Bures distance [53]. The fidelity of the transformed density matrix with the quantum state in the ideal situation (i.e., in the absence of noise) would be [48]

$$F = \langle\psi'|\rho'|\psi'\rangle, \tag{5}$$

where the expected quantum state $|\psi'\rangle = U_{A_n}U_{B_n}|\psi\rangle$.

[1] Here, and in what follows, all the qubits traveling from one party to other are sent in a secure manner, i.e., to send a sequence of n travel qubits, an equal number of decoy qubits are inserted randomly in the original sequence of the travel qubits, and subsequently, these decoy qubits are measured to check the existence of eavesdropper(s). Various choices of decoy qubits and the corresponding principles of security are discussed in [52].

The fidelity of the quantum state transformed under the damping effect of non-Markovian environment is

$$F=\frac{1}{4}\left[1+2\sqrt{p_1p_2p_3p_4}+p_1p_3p_4\left(2p_2-1\right)+p_3p_4\left(1-p_2\right)\right], \tag{6}$$

when the initial quantum state prepared by Charlie is $|\psi^{\pm}\rangle$. As the choice of initial state is solely a decision of Charlie, an independent choice of the initial state, i.e., $|\phi^{\pm}\rangle$, would lead to the following expression of fidelity

$$F=\frac{1}{4}\left[1+2\sqrt{p_1p_2p_3p_4}+p_1p_3p_4+p_3p_4\left(p_2-1\right)\right]. \tag{7}$$

If the state prepared by Charlie were subjected to a non-Markovian dephasing noise, the fidelity would be

$$F=\frac{1}{2}\left[1+p_1p_2p_3p_4\right]. \tag{8}$$

It is interesting to see that the obtained fidelity is independent of the choice of the initial Bell state by Charlie. This is also seen in analogous scenarios of Markovian dephasing noise in [17, 18, 20, 21, 52] and references therein. If we now consider that the system has evolved under the effect of a depolarizing channel, then following the above prescription, the analytical expression for fidelity can be obtained as

$$F=\frac{1}{2}\left[1+\Omega_1^4+\Omega_2^4+\Omega_3^4\right]. \tag{9}$$

It is interesting to observe the appearance of fourth order terms in all the non-Markovian fidelities, a signature of four noisy channels acting on the, four, different rounds of quantum communication. It should be mentioned here that instead of sending both the strings to Bob, Charlie could have sent S_A to Alice and S_B to Bob. Subsequently, Alice would have sent S_A to Bob after encoding her message and Bob would have encoded his message before performing the measurement. The obtained fidelity expressions in this case turns out to be the same as that of the CDSQC protocol, discussed in the next subsection. The effect of noise in the case discussed here is more than that in the case of CDSQC. Making use of this observation, we analyze the scheme of CQD, described above, in detail as the results obtained in the following subsections can be reduced from it.

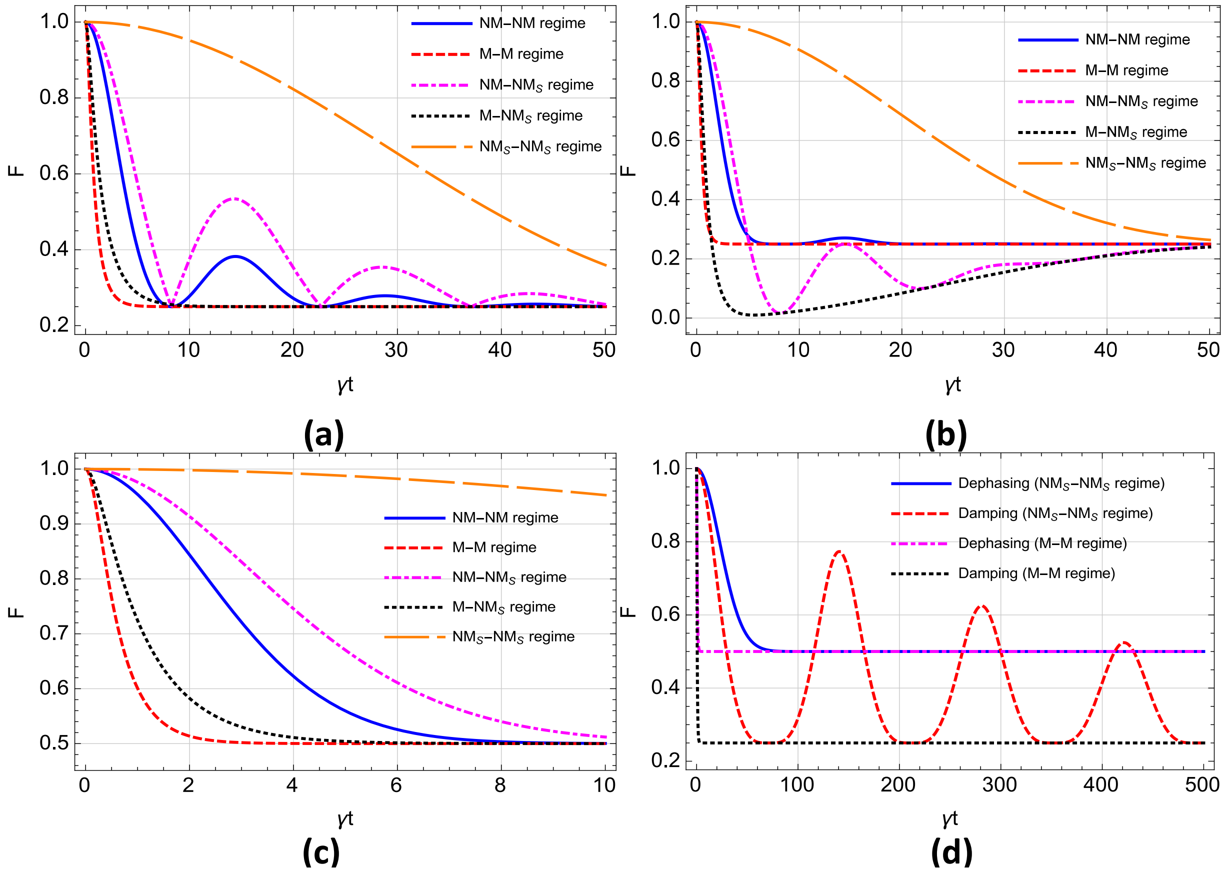
Now, we will discuss the fidelities for different scenarios depicted in Eqs. (6)-(9), for both Markovian and non-Markovian noises. The case of the non-Markovian damping/dephasing channels are also considered for strong and weak coupling regimes. Specifically, we obtain results in the strong and weak coupling regimes over non-Markovian damping channels $\Gamma=0.01\gamma$ and $\Gamma=0.1\gamma$, whereas for very high values, such as $\Gamma=5\gamma$, it is found to reduce to Markovian case. In the following figures, we have used the notation NM, M, and $\mathrm{NM_S}$, which correspond to the non-Markovian, Markovian, and non-Markovian (under strong coupling strengths) regimes of interactions, respectively.

A comparative analysis of the effects of non-Markovian (for both strong and weak couplings) and Markovian noise can be seen from Figs. 1-4. In this case, though four different coupling regimes are possible, one for each p_is, we have restricted ourselves, for simplicity, to the scenario of Charlie to Bob quantum channel having the same coupling strength for both the travel qubits. Similarly, Bob to Alice quantum channel has the same coupling strength as that for the other way round. We explicitly mention the two choices of regimes in Fig. 1. Specifically, Fig. 1 (a) and (b) show the effect of damping quantified by fidelity on the CQD scheme for different choices of initial Bell states, i.e., $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$, respectively. It is interesting to observe that when both the qubits undergo damping, either in Markovian or in strong coupling non-Markovian regimes, the choice of initial Bell states becomes irrelevant (see red (dashed) and orange (large dashed) curves in Fig. 1 (a) and (b)). However, this initial choice becomes considerably important for all the remaining cases, and $|\psi^{\pm}\rangle$ states are seen to be preferable as these states are less affected by non-Markovian damping noise than $|\phi^{\pm}\rangle$. Further, it is seen that, due to non-Markovian effects, the fidelity can be maintained for a relatively larger period of time (i.e., the quantum state decoheres slowly in non-Markovian environments in comparison to the corresponding Markovian environments), a feature that depends on the coupling strength (cf. Fig. 1 (a) and (b)). Another interesting characteristic of this kind of non-Markovian noise is periodicity [31] and the kinks present in Fig. 1 (a) and (b) are its signature. In Ref. [20] it was shown that the dilapidating influence of decoherence, due to Markovian damping, can be checked using squeezing. Here, it is seen that the same task can also be achieved by exploiting non-Markovianity.

The effect of noisy environment is independent of the initial Bell state over dephasing channel and the fidelity is observed to improve gradually with non-Markovian effects and coupling strength (cf. Fig. 1 (c)). Periodicity in the time variation of fidelity, when all interactions are (strong) non-Markovian is not visible in the time scale of Fig. 1 (a) and (b). For larger time scales, this can be observed in Fig. 1 (d), where fidelity over both the damping and dephasing non-Markovian channels is shown together. It can be seen that the fidelity under the effect of the damping noise decays faster than that over dephasing channel. At times, the fidelity over damping channel is observed to be much larger than that over dephasing channels, which remains constant at 1/2.

To analyze the effect of the coupling strength with varying time, we depict, in Fig. 2, a contour and a 3 dimensional plots. The ripple like plot (cf. the blue-colored surface plot in Fig. 2 (b)) shows that with decreasing coupling strength the amplitudes of the revived fidelity gradually become smaller. The same fact is also illustrated through a contour plot shown in Fig. 2 (a), where we can see that the area of the light-colored region reduces as we move from bottom to top. Physically, this corresponds to a transition from strong to weak coupling non-Markovian regime and finally into Markovian regime.

A similar analysis of the fidelity expression for the depolarizing channel is illustrated in Fig. 3. In Fig. 3 (a), homogeneous depolarizing noise is assumed $\gamma_i=\gamma\,\forall i\in\{1,2,3\}$, for which $\gamma\leq\left|\sqrt{\frac{1+(\pi/\log 3)^2}{32}}\right|$ to ensure that the dynamical map is completely positive [29, 51]. Interestingly, it can be



(a) **(b)**

(c) **(d)**

Figure 1: (Color online) The variation of the average fidelity obtained for CQD protocol with respect to the dimensionless quantity γt is depicted when the travel qubits undergo a damping or dephasing interaction with its surroundings. In (a) and (b), both the travel qubits may have different coupling strengths during their various rounds of travels under damping effects, which are characterized by $p_i \; : i \in \{1, 2, 3, 4\}$. The values of coupling strength for strong (weak) regime of non-Markovian effect is chosen as $\Gamma = 0.01\gamma$ ($\Gamma = 0.1\gamma$), and $\Gamma = 5\gamma$ for Markovian regime. In (a) and (b), the choice of initial Bell states by Charlie is $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$, respectively. (c) Shows similar cases over the dephasing channels. In (d), both purely dephasing and damping effects are shown together for strong non-Markovian and Markovian regimes.

seen from Fig. 3 (a) that the fidelity falls gradually with the parameter $\frac{\gamma}{\Gamma}$, which determines the fluctuation due to the depolarizing channel. However, it can be noted that for all the cases, the fidelity under non-Markovian environment is always greater than that for the corresponding Markovian case, till all the plots merge, with time, to a single value. Further, for the case of inhomogeneous fluctuations [29, 51], we observe revival in the fidelity in Fig. 3 (b). From Fig. 3, it can be summarized that non-Markovian depolarizing channel affects the system less than the corresponding Markovian channel.

The change in coupling strength controls the transition from non-Markovian to Markovian regime for both damping and depolarizing channels. This dependence has been illustrated in Fig. 4. Initial small changes in the value of coupling strength changes considerably the nature of the obtained fidelity, i.e., the periodicity and maximum value of fidelity after revival show ample changes for even a small change of coupling strength. However, for small values of the coupling strength, this change becomes less sensitive as reflected in the dense black lines corresponding to smaller values of coupling strengths.

A similar comparison of the effect of non-Markovian and Markovian depolarizing channels shows that the fidelity sustains for a longer period of time under the influence of a non-Markovian depolarizing channel, and is more sensitive to small changes in the noise parameter, which controls the fluctuation. For higher values of noise parameter, the variation due to small changes in noise parameters becomes negligible in both Markovian and non-Markovian depolarizing channels.

In the following subsections, we will deduce corresponding results for the remaining cryptographic tasks from the results obtained in this section for the fidelity (for the CQD scheme) over the various non-Markovian channels.

B. CDSQC

A protocol of CDSQC, based on quantum cryptographic switch, can be obtained from the CQD scheme discussed in the previous subsection, i.e., when only a single party encodes and sends his/her message in a secure manner via the quantum channel, which is decoded by the other party [11]. To be pre-

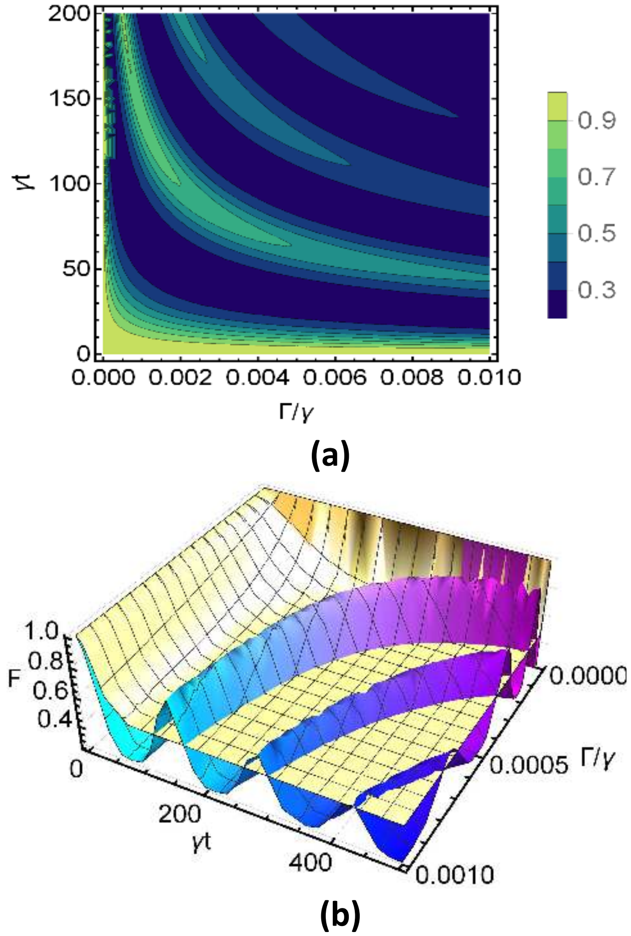


Figure 2: (Color online) The dependence of the obtained fidelity over the damping channel on the coupling strength and rescaled time is illustrated through a contour plot in (a). (b) depicts the variation of the fidelity for varying coupling strength and time for both purely dephasing and damping non-Markovian channels in light (yellow) and dark (blue) colored surface plots, respectively.

cise, Charlie initially follows the same steps as in Section III A but rather sends the two strings S_A and S_B to Alice and Bob, respectively. Alice encodes her message as usual and sends the encoded qubit to Bob, who decodes the secret by performing Bell state measurement on partner pairs with the help of Charlie [11].

The CDSQC scheme and the effect of noise can be summarized as follows

$$\rho' = \sum_{A_n}\sum_{i,j,l} \left(K_l\left(p_4\right)\otimes I\right) U_{A_n} \left(K_i\left(p_1\right)\otimes K_j\left(p_2\right)\right)\rho \\ \times \left(\left(K_l\left(p_4\right)\otimes I\right) U_{A_n} \left(K_i\left(p_1\right)\otimes K_j\left(p_2\right)\right)\right)^\dagger, \tag{10}$$

where all the parameters have the same meaning as in Section III A. It is interesting to observe that the transformed density matrix in Eq. (10) can be obtained from Eq. (4) just by considering $p_3 = 1$ and $U_{B_n} = I$. The fidelity can be calculated with the quantum state expected in the ideal situation, i.e., $|\psi'\rangle = U_{A_n}|\psi\rangle$.

Due to this observation, the fidelity of the quantum states affected by the non-Markovian noise, for the CDSQC scheme can be obtained from the corresponding CQD expressions by taking $p_3 = 1$, in Eqs. (6)-(8). Interestingly, for the case of the depolarizing channel, the fidelity can be shown to be

$$F = \frac{1}{2}\left[1+\Omega_1^3+\Omega_2^3+\Omega_3^3\right], \tag{11}$$

where the presence of cubic terms manifests the fact that the number of rounds of quantum communication involved in this scheme is less than that for the scheme discussed in the previous subsection. Specifically, the scheme for CDSQC requires three rounds of quantum communication, while the scheme for CQD requires four rounds.

The qubit traveling through the noisy channel may have different coupling strength during each round of travel. Here,

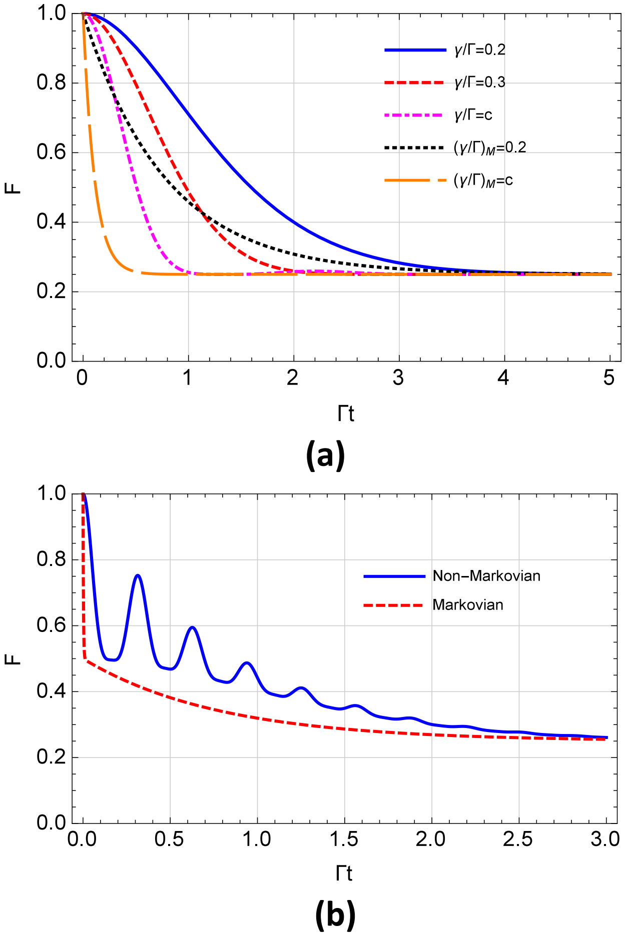


Figure 3: (Color online) (a) The effect of non-Markovian depolarizing channel on the CQD scheme has been illustrated for different values of the dimensionless quantity $\frac{\gamma}{\Gamma}$ indicated in the plot. (a) shows the case of homogeneous non-Markovian depolarizing channel (i.e., $\frac{\gamma_i}{\Gamma_i} = \frac{\gamma}{\Gamma}\forall i \in \{1,2,3\}$). (b) illustrates a comparison between inhomogeneous case of non-Markovian and Markovian depolarizing channels. In (a), the constant $c = \Gamma\left|\sqrt{\frac{1+(\pi/\log 3)^2}{32}}\right|$, which is the maximum value ensuring completely positive map for all times for the homogeneous case; in (b), the noise parameters are $\frac{\gamma_3}{\Gamma_3} = 5$, $\frac{\gamma_i}{\Gamma_i} = 0.2$ for $i \in \{1,2\}$.

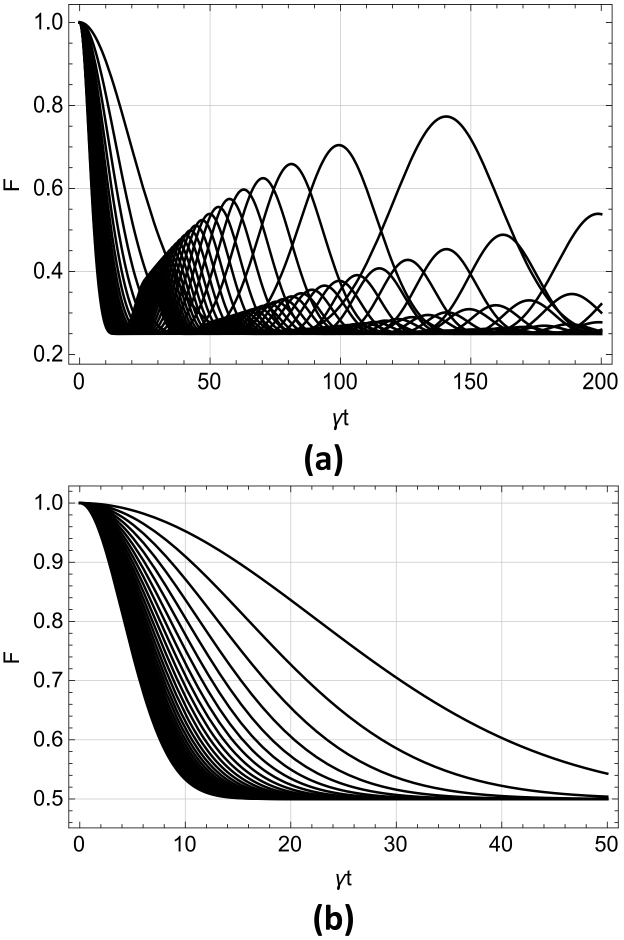


Figure 4: The effect of a change in the coupling strength on the fidelity is illustrated here with a set of plots for damping and dephasing non-Markovian noise in (a) and (b), respectively. Specifically, the parameter of the coupling strength Γ/γ varies from 0.001 to 0.03 in steps of 0.001 in both the plots.

we wish to emphasize this point with the help of three possible coupling strengths for three noisy channels acting on the travel qubits. The observations made above for the extreme cases, i.e., the qubits traveling through either non-Markovian channels with strong coupling or Markovian channels all the time, remain valid here as well. Nevertheless, it cannot be conjectured that the more the number of non-Markovian channels, the higher the fidelity. In particular, the large dot-dashed (purple) curve in Fig. 5 (a) and (b) establishes that even lower fidelity is observed with lesser number of Markovian channels acting on the travel qubits. In fact, Fig. 5 (b) shows that the obtained fidelity for parity 1 Bell states (i.e., $|\phi^{\pm}\rangle$) is less for all the cases when various noise channels had different coupling strengths than that for the case of the travel qubits subjected to noisy channels with the same coupling strength. However, no such nature is visible in Fig. 5 (c) for dephasing channels. It is worth stressing here that out of the three possible choices for different coupling regimes corresponding to each p_i, we have emphasized only on the interesting cases and mentioned them accordingly in Fig. 5.

Interestingly, the fidelity in the CDSQC protocol falls below the corresponding Markovian value, under the influence of the non-Markovian depolarizing channel, when all three noise parameters have different values (cf. Fig. 5 (d)). This nature can be attributed to the presence of cubic terms in the fidelity, Eq. (11).

C. QD

A CQD scheme can be viewed as a QD scheme under the supervision of a controller. Therefore, a QD scheme can be easily derived from the CQD scheme if we consider the scenario that one of the two communicating parties (i.e., either Alice or Bob) prepares and measures the quantum state, while both the parties encode their secret on the same qubits. This QD scheme, which is obtained as a result of reduction from the CQD scheme described above, can be easily recognized to be equivalent to the first QD protocol proposed by Ba An [15]. The effect of noise on this scheme for QD can be obtained by considering $p_1 = p_2 = 1$ in all the expressions of Section III A. This would imply that the initial state is prepared by one of the communicating parties (say, Bob). Then the transformed density matrix and the fidelity expressions over non-Markovian channels can be deduced from Eqs. (4)-(8). Here, it is important to note that the effect of noise is independent of the choice of initial Bell state by Charlie/Bob in all the schemes other than CQD and CDSQC. Similarly, under the effect of depolarizing channels, the expression of fidelity turns out to be

$$F = \frac{1}{2}\left[1 + \Omega_1^2 + \Omega_2^2 + \Omega_3^2\right], \tag{12}$$

due to two rounds of quantum communication of a travel qubit.

D. QSDC/DSQC

As mentioned beforehand in Section III B, a CDSQC scheme can be viewed as a CQD scheme, where only one party is allowed to encode. In the same way, a QSDC scheme (say, a Ping Pong protocol [6]) can be viewed as a scheme for QD [15], where one party (say Bob) is restricted to encode Identity only. Therefore, all the expressions of the fidelity for a QSDC scheme are exactly the same as those for the scheme of QD.

A DSQC scheme can be reduced from the above mentioned protocols if Bob incorporates information splitting in two quantum pieces and sends them one after the other in two different rounds of Bob to Alice communication [14]. Specifically, Bob prepares two strings as in Section III C and sends the first string to Alice. He subsequently sends the second string to Alice only if the first quantum part is received by Alice undisturbed. The effect of non-Markovian noisy environment on this DSQC scheme can be obtained from the corresponding expressions for the CQD scheme obtained in Sec.

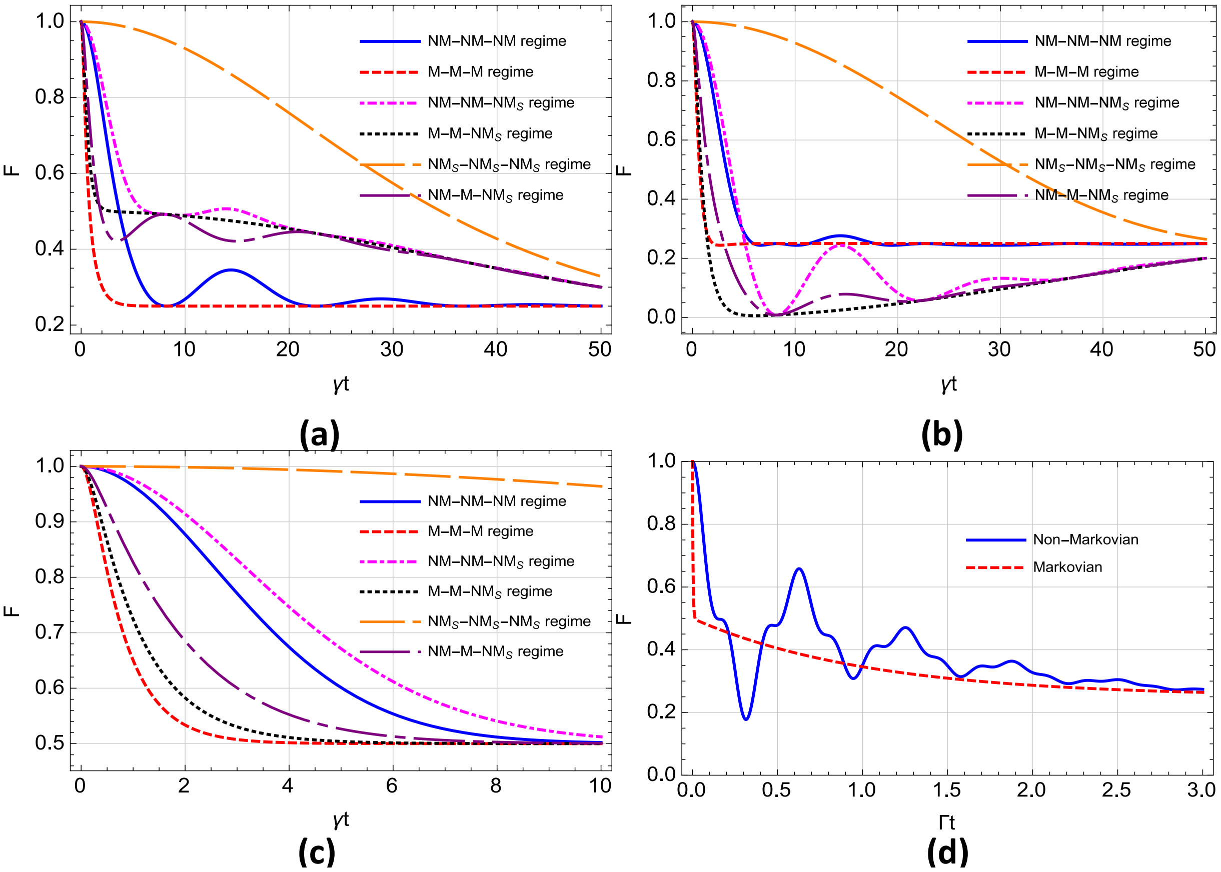


Figure 5: (Color online) The dependence of the average fidelity obtained for the CDSQC protocol on the coupling strength is illustrated through its variation with the dimensionless quantity γt, when the travel qubits undergo damping (in (a) and (b)) or dephasing (in (c)) interaction with their ambient surroundings. In (a) and (b), the initial state chosen by Charlie was $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$, respectively. Here, we have chosen different values of all the coupling constants in various regimes, i.e., non-Markovian with strong and weak couplings as well as for the Markovian case. All the values of coupling strengths corresponding to various regimes are the same as used in the previous plots. In (d), time variation of the fidelity for the CDSQC protocol over a depolarizing channel is shown corresponding to the values used in Fig. 3 (b).

III A, if we consider $p_1 = p_4 = 1$ and $p_2 = p_3'$ in Eqs. (6)-(8). Here, p_3' is used to show the effect of noise on the second qubit traveling from Bob to Alice in the first round. In fact, it turns out to be exactly similar to what is obtained for the QSDC scheme. Interestingly, in case of depolarizing noise, all the expressions for fidelity are found to be the same for QD, QSDC and DSQC schemes. For the convenience of discussion for the DSQC scheme, we have chosen Bob (Alice) as the sender (receiver).

So far, we have discussed quantum communication schemes where prior key generation is circumvented by proper use of quantum resources. We may now proceed to key generation schemes and investigate the effect of non-Markovian environment on them.

E. QKA

A QKA scheme provides equal power to all the parties taking part in the key generation process, and does not allow members of a proper subset of the set of all users to solely decide the final key. Here, we consider a completely orthogonal QKA scheme proposed in [12]. In this QKA protocol, a party (say Alice) sends her raw key to another party (say Bob) by using a QSDC protocol, while the other party publicly announces his key. The security of the final key is achieved by the unconditional security of Alice's transmission of raw key using quantum resources (i.e., from the security of the QSDC/DSQC scheme used by Alice and Bob for Alice to Bob communication). Specifically, Alice transmits a key k_A to Bob in a secure manner, whereas Bob announces his key k_B, publicly, and for all future communication they use a key $k_{AB} = k_A \oplus k_B$, where $\oplus$ denotes a bitwise XOR operation. Although, Eve knows k_B, she cannot obtain any information about k_{AB} as she knows nothing about k_A. Thus, the security of k_{AB} depends on the security of k_A. In other words, unconditional security of the QSDC scheme involved here would ensure the security of the protocol for QKA. Interestingly, in Ref. [20], the present authors had already shown that the effect of noise on this scheme is identical to the QSDC scheme discussed in the previous Section III D. Since the observations made there remain valid here, we do not discuss it in further detail.

F. QKD

Any discussion on quantum cryptography remains incomplete without discussing a protocol that changed the course of cryptography by establishing the feasibility of unconditional security. In this section, we discuss two QKD protocols, which can be viewed as the variants of the same scheme, differing only in the measurement procedure. Specifically, the BB84 [1] and BBM [5] QKD protocols are discussed here. Before we proceed further, it would be apt to note that in contrast to the fidelity expressions obtained in the earlier sections (which were average over all the encoding operations), for QKD protocols, the average fidelity is obtained over all possible equally probable measurement outcomes.

In the BBM protocol [5], Alice prepares n Bell states and sends all the first qubits to Bob, and both of them measure the qubits of the shared Bell states randomly in computational ($\{|0\rangle, |1\rangle\}$) and diagonal ($\{|+\rangle, |-\rangle\}$) basis. Using the outcome of these measurements, they finally obtain an unconditionally secure quantum key for those cases where both Alice and Bob perform measurement using the same basis.

The BB84 protocol can also be viewed along the same lines, where Alice first measures her qubit (i.e., second qubit) of each Bell state randomly either in computational or diagonal basis and then sends the other qubit to Bob. Finally, they can obtain a key by using the measurement outcomes of half of those cases, where they have chosen the same basis. The other half of the cases should be used for eavesdropping check. Specifically, when Alice and Bob have performed measurement in the same basis, in the absence of Eve, their measurement outcomes should match and a mismatch would indicate the presence of Eve.

Interestingly, for the BBM protocol, the effect of noise can be considered by taking $p_1 = p_2 = p_4 = 1$ in Eqs. (6)-(8). Similarly, the effect of depolarizing channel reduces the fidelity to

$$F = \frac{1}{2}\left[1 + \Omega_1 + \Omega_2 + \Omega_3\right]. \qquad (13)$$

A similar study for the BB84 protocol results in the following fidelity over damping non-Markovian channels

$$F = \frac{1}{4}\left[2 + \sqrt{p_3} + p_3\right], \qquad (14)$$

while, for the dephasing channel the fidelity is

$$F = \frac{1}{4}\left[3 + p_3\right]. \qquad (15)$$

Further, the fidelity when the travel qubit is subjected to a depolarizing channel is

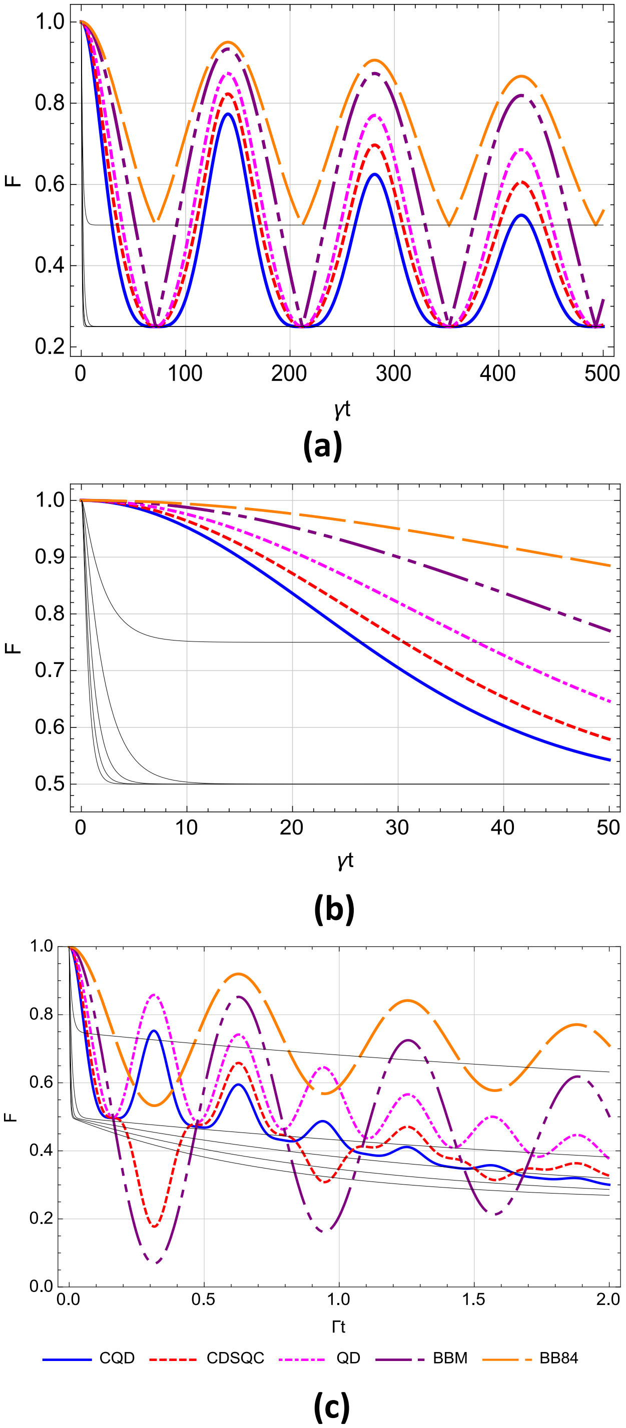
$$F = \frac{1}{2}\left[2 + \Omega_1 + \Omega_3\right]. \qquad (16)$$

Additionally, the present results can also be used to deduce the fidelity for a few other quantum cryptographic schemes, which will reflect quantitatively the effect of non-Markovian channels on the corresponding scheme. For example, the effect of noise on Ekert's QKD protocol [2] can also be deduced from the results in Sec. III A, by taking $p_3 = p_4 = 1$ as the source of entanglement is between both the parties, and both the entangled qubits travel to Alice and Bob from there. Similarly, the feasibility of the B92 protocol [3] can also be analyzed over the non-Markovian channels in analogy with the study for BB84 protocol by only considering two of the four single qubit states (one each chosen from computational and diagonal basis).

Finally, we perform a comparative study for the fidelity obtained in each cryptographic scheme to reveal the general nature of the effect of non-Markovian channels on all these schemes (shown in Fig. 6). Interestingly, the effect of noise depends on the number of rounds a qubit is required to travel through the noisy channel. This fact is consistent with the recent observations on a set of Markovian channels [20]. Specifically, in the CQD scheme, one qubit travels from Charlie to Bob, while another qubit travels from Charlie-Bob-Alice-Bob. Therefore, the maximum number of rounds of travels in the set of secure quantum communication schemes discussed here is four for CQD scheme, which decreases to three for CDSQC. It further reduces to two for QD, QSDC, DSQC, and QKA schemes. The same fidelity for all these schemes further establish this point. Finally, BBM and BB84 QKD protocols require only one round of quantum communication. In fact, BBM and BB84 protocols use entangled and single qubit states, respectively, to accomplish the same task. Out of these two schemes, the BB84 QKD scheme is least affected by noise as it uses single qubit states, which were shown to be less affected due to Markovian channels in [20].

In Fig. 6 (a) and (b), the fidelity variation over non-Markovian channels due to the strong coupling of the travel qubits with the environment is depicted. Similarly, the effect of different noise parameters corresponding to depolarizing channel is shown in Fig. 6 (c). Also shown is the effect of Markovian environment on the fidelity in all three cases, depicted by thin smooth (black) lines. For all cases of Markovian dynamics, the observation that the effect of noise depends on the rounds of quantum communication remains valid.

From Fig. 6 (a), the revival in the fidelity over non-Markovian damping channel is seen to decrease with an increase in the number of travel qubits. Similarly, the fidelity falls with increasing rounds of quantum communication when subjected to dephasing non-Markovian channel, as shown in Fig. 6 (b). Out of the set of fidelities, over the depolarizing channel, those having odd power terms, such as for the CDSQC and QKD protocols, show fidelity less than that for the corresponding Markovian case. Otherwise, in all the remaining cases, the fidelity over non-Markovian channels is more than that for the corresponding Markovian channels (cf. Fig. 6 (c)).



(a)

(b)

(c)

Figure 6: (Color online) A comparative analysis of all the quantum cryptographic schemes discussed so far over the non-Markovian channels. Each line in all three plots corresponds to the different cryptographic scheme mentioned in the plot legend at the bottom of the figure. The light black lines in all three plots represent the corresponding Markovian cases, and the black lines from bottom to top show the average fidelity for CQD, CDSQC, QD, BBM QKD, and BB84 QKD protocols. The fidelity obtained for QSDC, DSQC, and QKA schemes is exactly the same as that of the QD protocol.

IV. CONCLUSION

The present study on the effect of a set of non-Markovian channels on various schemes for secure quantum communication tasks led to a number of interesting results. Specifically, we have considered here a damping, a purely dephasing and a depolarizing non-Markovian channel to analyze the feasibility of some quantum cryptographic schemes evolving under the influence of the non-Markovian environments. We have started with a CQD scheme, based on a quantum cryptographic switch that uses Bell states. Later, this scheme is modified to deduce the results for other quantum cryptographic tasks, such as, CDSQC, QSDC, DSQC. Apart from these direct communication schemes, the effect of non-Markovian noise on some protocols of QKD and QKA is also analyzed.

It has been established that the effect of non-Markovian noise depends on the number of rounds of the travel qubits. We have observed that the BB84 QKD scheme is least affected due to non-Markovian channels, while the CQD scheme shows a maximum fall in the fidelity. In fact, from the results obtained here one can also show that the AQD scheme [21] will have the same effect as that on the QD protocol if the number of travel qubits is kept unchanged. This fact is consistent with the results obtained here, that the fidelity for QSDC, DSQC, and QKA schemes are exactly the same as that for the QD protocol. In the recent past, we have established that squeezing is a useful quantum resource for quantum cryptography as it can help to stop decoherence. Here, we have shown that non-Markovianity can also be used to accomplish a similar task.

Interestingly, the effect of noise on the CQD and CDSQC schemes is found to depend on Chalie's initial choice of the Bell state, while it is independent of this in all the remaining schemes. Finally, our analysis has also revealed that the fidelity obtained in the case of damping and dephasing channels depends on the coupling strength. We hope these results would bring out the importance and utility of the non-Markovian behavior in the understanding of quantum cryptographic protocols from the perspective of their practical implementation.

Acknowledgment: AP and KT thank Defense Research & Development Organization (DRDO), India for the support provided through the project number ERIP/ER/1403163/M/01/1603. SB acknowledges support by the project number 03(1369)/16/EMR-II funded by Council of Scientific and Industrial Research, New Delhi.

[1] C. H. Bennett and G. Brassard, In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India 175 (1984).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[6] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[7] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[8] G. l. Long, F. G. Deng, C. Wang, X. H. Li, K. Wen, and W. Y. Wang, Front. Phys. China **2**, 251 (2007).
[9] C. Shukla, A. Banerjee, and A. Pathak, Int. J. Theor. Phys. **52**, 1914 (2013).
[10] A. Banerjee and A. Pathak, Phys. Lett. A **376**, 2944 (2012).
[11] A. Pathak, Quantum Inf. Process. **14**, 2195 (2015).
[12] C. Shukla, N. Alam, and A. Pathak, Quantum Inf. Process. **13**, 2391 (2014).
[13] M. Hillery, V. Bužek, and A. Bertaiume, Phys. Rev. A **59**, 1829 (1999).
[14] A. Pathak, *Elements of Quantum Computation and Quantum Communication* (CRC Press, Boca Raton, USA 2013).
[15] N. B. An, Phys. Lett. A **328**, 6 (2004).
[16] C. Shukla and A. Pathak, Phys. Lett. A **377**, 1337 (2013).
[17] C. Shukla, K. Thapliyal, and A. Pathak, arXiv:1605.07399 (2016).
[18] K. Thapliyal and A. Pathak, Quantum Inf. Process. **14**, 2599 (2015).
[19] N. Srinatha, S. Omkar, R. Srikanth, S. Banerjee, and A. Pathak, Quantum Inf. Process. **13**, 59 (2014).
[20] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, Quantum Inf. Process.DOI 10.1007/s11128-016-1396-7 (2016).
[21] A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, and P. K. Panigrahi, arXiv:1605.08363 (2016).
[22] V. Sharma, C. Shukla, S. Banerjee, and A. Pathak, Quantum Inf. Process. **14**, 3441 (2015).
[23] S. Banerjee and R. Ghosh, J. Phys. A: Math. Theo. **40**, 13735 (2007).
[24] R. Srikanth and S. Banerjee, Phys. Rev. A **77**, 012318 (2008); S. Omkar, R. Srikanth, and S. Banerjee, Quantum Inf. Process. **12**, 3725 (2013).
[25] X. Hao and S. Zhu, Int. J. Quantum Inf. **10**, 1250051 (2012).
[26] Y. Yeo, J. H. An, and C. H. Oh, Phys. Rev. A **82**, 032340 (2010).
[27] J. W. Jun, Euro. Phys. J. D **67**, 1 (2013).
[28] J. W. Jun, J. Korean Phys. Soc. **60**, 550 (2012).
[29] P. Huang, J. Zhu, G. He, and G. Zeng, J. Phys. B: At. Mol. Opt. Phys. **45**, 135501 (2012).
[30] T. Yu and J. H. Eberly, Opt. Commun. **283**, 676 (2010).
[31] B. Bellomo, R. L. Franco, and G. Compagno, Phys. Rev. Lett. **99**, 160502 (2007).
[32] H. Grabert, P. Schramm, and G. L. Ingold, Phys. Rep. **168**, 115 (1988).
[33] S. Banerjee and R. Ghosh, Phys. Rev. E **67**, 056120 (2003).
[34] S. Banerjee and R. Ghosh, Phys. Rev. A **62**, 042105 (2000).
[35] M. Ban, J. Phys. A: Math. Gen. **39**, 1927 (2006).
[36] J. Piilo, S. Maniscalco, K. Härkönen, and K. A. Suominen, Phys. Rev. Lett. **100**, 180402 (2008).
[37] S. Maniscalco and F. Petruccione, Phys. Rev. A **73**, 012111 (2006).
[38] J. P. Paz and A. J. Roncaglia, Phys. Rev. Lett. **100**, 220401 (2008).
[39] J. H. An and W. M. Zhang, Phys. Rev. A **76**, 042127 (2007).
[40] A. Nourmandipour, M. K. Tavassoly, and M. Rafiee, Phys. Rev. A **93**, 022327 (2016).
[41] E. Novais, E. R. Mucciolo, and H. U. Baranger, Phys. Rev. A **78**, 012314 (2008).
[42] K. Shiokawa and B. L. Hu, Quantum Inf. Process. **6**, 55 (2007).
[43] P. Chen, Phys. Rev. A **75**, 062301 (2007).
[44] X. M. Lu, X. Wang, and C. P. Sun, Phys. Rev. A **82**, 042103 (2010).
[45] J. S. Xu, C. F. Li, M. Gong, X. B. Zou, C. H. Shi, G. Chen, and G. C. Guo, Phys. Rev. Lett. **104**, 100502 (2010).
[46] B. H. Liu, L. Li, Y. F. Huang, C. F. Li, G. C. Guo, E. M. Laine, H. P. Breuer, and J. Piilo, Nat. Phys. **7**, 931 (2011).
[47] A. Orieux, A. d'Arrigo, G. Ferranti, R. L. Franco, G. Benenti, E. Paladino, and P. Mataloni, Sci. Rep. **5**, 8575 (2015).
[48] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, Rev. Mod. Phys. **86**, 1203 (2014).
[49] J. Dajka, M. Mierzejewski, and J. Łuczka, Phys. Rev. A **77**, 042316 (2008).
[50] X. Cao and H. Zheng, Phys. Rev. A **77**, 022320 (2008).
[51] S. Daffer, K. Wódkiewicz, J. D. Cresser, and J. K. McIver, Phys. Rev. A **70**, 010304 (2004).
[52] R. D. Sharma, K. Thapliyal, A. Pathak, A. K. Pan, and A. De, Quantum Inf. Process. **15**, 1703 (2016).
[53] A. Miranowicz, K. Bartkiewicz, A. Pathak, J. Peřina Jr., Y. N. Chen, and F. Nori, Phys. Rev. A **91**, 042309 (2015).