Quantum Information Processing (2020) 19:366
https://doi.org/10.1007/s11128-020-02874-4

Ping-pong quantum key distribution with trusted noise: non-Markovian advantage

Shrikant Utagi [1,2] · **R. Srikanth** [1] · **Subhashish Banerjee** [3]

Received: 20 April 2020 / Accepted: 18 September 2020 / Published online: 1 October 2020

Abstract
The ping-pong protocol adapted for quantum key distribution is studied in the trusted quantum noise scenario, wherein the legitimate parties can add noise locally. For a well-studied attack model, we show how non-unital, quantum non-Markovianity of the added noise can improve the key rate. We also point out that this noise-induced advantage cannot be obtained by Alice and Bob by adding local classical noise to their post-measurement data.

Keywords Ping-pong · Non-Markovianity · Quantum key distribution · Amplitude damping noise

1 Introduction

Quantum key distribution (QKD) protocols are known to offer information theoretic security of information, unlike their classical counterparts which can only offer computational security. Over the time, a number of QKD protocols have been proposed (cf. the review [1]), since their foundation was laid over three decades ago by Bennett and Brassard [2]. While QKD protocols typically involve the probabilistic generation of a secret key, [3] proposed a deterministic version thereof using entanglement in a two-way protocol (called the "ping-pong protocol," described below), but it turns

✉ R. Srikanth
srik@poornaprajna.org

Shrikant Utagi
shrik@poornaprajna.org

Subhashish Banerjee
subhashish@iitj.ac.in

1 Poornaprajna Institute of Scientific Research, Bengaluru 560080, India

2 Manipal Academy of Higher Education, Manipal 576104, India

3 Indian Institute of Technology, IIT-Jodhpur, Jodhpur, India

out that the idea can also be realized without entanglement [4]. Certain attacks or modifications to the ping-pong protocol were proposed in [5–8], which were analyzed in [9]. Subsequently, further modifications or attacks on the ping-pong protocol were studied by other authors [10–14].

Noise is especially detrimental to quantum information processing, given the fragility of quantum resources [15]. Yet, recently, there have been a few reports pointing out that the addition of classical or quantum noise by information sender Alice or receiver Bob can be advantageous to QKD [16–18]. Here, we shall refer to such user added noise as "trusted." Note that this terminology differs from that used by [19], who in the context of continuous variable QKD protocols [20] refer to noise that is security breaking as "untrusted" and noise that is merely key rate reducing as "trusted."

Quantum non-Markovianity of noise is the quantum analogue of classical memory effects and manifests itself through the backflow of quantum information or increase in the distinguishability of two states subjected to a noisy channel [21–23], though we may reasonably posit weaker manifestations of quantum non-Markovianity (cf. [24,25]). Thus, it is intuitive to expect that quantum non-Markovianity can be helpful to information processing [26,27], especially at low temperatures [28,29] . However, this is by no means automatic (cf. e.g., [30]).

In an earlier work, it was shown [26] that non-unital noise helps cryptographic security for QKD based on the ping-pong communication protocol for a specific attack, essentially because the noise turns out to be more detrimental for Eve than Alice and Bob. In this paper, we show that non-Markovianity can further boost the advantage given by the non-unitality of quantum channels under certain circumstances. As before, unital channels provide no advantage. We consider two different scenarios in which amplitude damping noise is deliberately applied by a legitimate party (Bob, specifically) before a Bell measurement, and study the increase in secure key rate. In both cases, we find that if the quantum noise is non-Markovian, then the secure key rate increases significantly in comparison with Markovian noise in certain time ranges.

There do not seem many works that have explored this practically useful aspect. Notably, Ref. [18] shows that deliberately adding depolarizing noise increases secure key rate for BB84 [2] and for entanglement-based six-state protocols [31,32]. This was somewhat inspired from the work [17] where for the six-state protocol, white noise added by the sender to the message qubit either prior to sending the qubit or prior to measurement on the qubit gives rise to an increased secure key rate in the sense we consider in this paper.

This paper is arranged as follows. In Sect. 2, we introduce the protocol, which is the "ping-pong" communication protocol adapted for QKD. In Sect. 3, we discuss the phenomenologically motivated model of amplitude damping noise and describe how it can be added during the protocol. We consider in Sect. 3.1 the first scenario involving a single-qubit noise and in Sect. 3.2 the second scenario involving two-qubit incoherent noise. In Sect. 4, we show that the noisy joint statistics cannot be simulated by locally adding classical randomness to the noiseless joint quantum statistics of the protocol. Then, we conclude in Sect. 6.

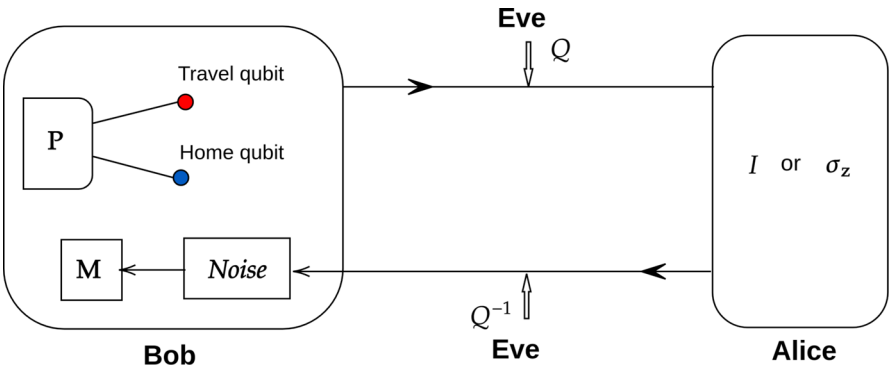

Fig. 1 General scheme of the ping-pong protocol [3]: Bob prepares an entangled qubit pair in polarization degrees of freedom, and transmits the travel qubit to Alice and retains the home qubit. All channel noise is conservatively assumed to be due to Eve's attack. In addition, Bob adds noise to the qubit(s) prior to his measurements. The same layout is used when the protocol is adapted for QKD, except that the control mode is dropped (cf. text) (Color online)

2 The basic protocol and the optimal individual attack

The ping-pong protocol, adapted as a scheme for QKD, runs as follows: Bob prepares the Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, in particular pair of photons entangled in the polarization degree of freedom, out of which he sends one photon (travel photon) to Alice through a quantum channel, ideally assumed to be noiseless and lossless. Alice then encodes the travel qubit by applying either I or σ_z with probability $\frac{1}{2}$, and sends it back to Bob. Once the travel qubit returns to Bob, he is left with either of the two Bell states $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, corresponding to the bit 0 or 1 encoded by Alice, which he distinguishes through a Bell measurement.

In the original ping-pong quantum direct communication protocol, the security requires alternating between the above message mode and a control mode, wherein Alice measures the travel qubit for error checking, and does not return it. Here, for the requirement of QKD, we drop the control mode and consider only the message mode. As a security check, both parties compute the quantum bit error rate (QBER) by sampling a fraction of the qubits transmitted. On them, Alice announces her encoded bit and Bob announces the Bell state he detected. The fraction of cases where their records differ is an estimate of QBER and a potential indicator of eavesdropper Eve's presence. If QBER is found to be less than a threshold value, they proceed ahead with key distillation, or else they abort the protocol.

The interesting aspect of the ping-pong protocol is that in the ideal case, Eve only finds the onward and return photons to be in the maximally mixed state. Wojcik [5] proposed a strategy by attacking the onward and return legs. In this attack, Eve includes two ancillary particles: the first (labeled x) prepared in a vacuum state, denoted $|2\rangle$, and the other (labeled y) in the state denoted $|y\rangle = |0\rangle$. Then the composite initial state is $|\Psi\rangle_{\text{htxy}}^{\text{initial}} = |\psi^+\rangle|2\rangle_x|0\rangle_y$, where h and t are labels for "home" and "travel" qubit states, respectively. In the onward leg, Eve attacks the travel qubit by applying

the operation given by:

$$Q_{txy}: \begin{matrix} |020\rangle \\ |021\rangle \\ |120\rangle \\ |121\rangle \end{matrix} \Bigg\} \longrightarrow \begin{cases} |002\rangle + |201\rangle \\ |002\rangle - |201\rangle \\ |210\rangle + |112\rangle \\ |210\rangle - |112\rangle \end{cases} \tag{1}$$

with CPBS denoting the "controlled polarization beam splitter" operation. On the return leg (after Alice's encoding action), Eve applies the operation Q_{txy}^{-1} on the travel qubit and forwards it to Bob.

After the end of the quantum round, Bob receives the final states $|\Psi\rangle_{\text{fin}} = \frac{1}{\sqrt{2}}(|012j\rangle + |1020\rangle)$, with $j \in \{0, 1\}$, corresponding to Alice's operation $\hat{O}_j \in \{I, Z\}$. The joint probabilities of Alice, Eve and Bob, P_{AEB}, are found to be

$$P_{000} = \frac{1}{2}; \quad P_{1jk} = \frac{1}{8}, \tag{2}$$

for $j, k \in \{0, 1\}$.

The secure (or secret) key rate for this individual attack on each travel by Eve is lower bounded by $k_{\min} = I(A : B) - \chi(A : E)$, where $I(A : B)$ is the mutual information between the trusted parties Alice and Bob, and $\chi(A : E)$ is the Holevo information between trusted party Alice and malicious Eve. In practice, the key rate may be as high as determined $k_{\max} = I(A : B) - I(A : E)$. For the noiseless case of (2) , it turns out that $I(A : B) = I(A : E) = \chi(A : E) \approx 0.31$ implying that the key rate vanishes and that Eve's attack strategy is indeed optimal for this protocol.

3 Noise advantage

In general, it is known that noise can degrade the quantum information processing tasks, in particular QKD. In Ref. [26], we pointed out the surprising fact of advantage that noise can bestow on QKD. Here, we extend that analysis, by including the role of memory in the quantum dynamics. Because the noise brings an advantage, we can visualize the scenario wherein Bob (or Alice) deliberately adds such beneficial noise to the particles.

We consider two scenarios, wherein Bob, before making Bell measurements on the entangled pair of particles, but after receiving the travel qubit, introduces noise into the system. In the first case, he subjects the travel qubit alone to an optical setup that simulates AD. In the second case, he subjects both the photons to noisy devices in the above manner. In both scenarios, Eve is still assumed to act according to the attack described in Sect. 2. Note that we may also assume that the noise occurs naturally because of Bob's noisy devices, and he merely takes advantage of it.

For the noisy dynamics introduced by Bob, we consider a non-Markovian amplitude damping (NMAD) channel, modeled by damped Jaynes–Cummings model with

operator-sum representation given by the Kraus operators [33]

$$E_0^A = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda(t)} \end{bmatrix}; \; E_1^A = \begin{bmatrix} 0 & \sqrt{\lambda(t)} \\ 0 & 0 \end{bmatrix}, \tag{3}$$

where

$$\lambda(t) = 1 - e^{-gt}\left(\frac{g}{l}\sinh\left[\frac{lt}{2}\right] + \cosh\left[\frac{lt}{2}\right]\right)^2, \tag{4}$$

with $l = \sqrt{g^2 - 2\gamma g}$. Here, g is the spectral band width of the noise and γ is the system–environment coupling strength. One readily sees that the system exhibits Markovian and non-Markovian evolution when $2\gamma \ll g$ and $2\gamma \gg g$, respectively [34].

The above noise may be simulated in an all-optical setup [35–37] by associating the qubit with polarization degrees and the reservoir to the path degrees. With a suitable mapping of the parameters of JC model to the parameters of the optical setup, one may obtain Markovian and non-Markovian effects experimentally. Interestingly, similar to [35], the authors of [38] propose an optical simulation of Markovian and non-Markovian AD. However, we consider the former approach for our case in this paper.

3.1 Case 1: Only travel qubit subjected to NMAD

When the photon returns back to Bob, the state of the system hty for either encoding "j" can be shown to have support of dimensionality 4, spanned by the states $|000\rangle$, $|010\rangle$, $|100\rangle$ and $|011\rangle$, with the state of the x particle being $|2\rangle$, as in the noiseless attack case.

After receiving the returned noisy travel qubit, Bob further subjects it to the damping noise, described by Eq. (3). Accordingly, the final states with Bob for Alice's encodings $j = 0$ and $j = 1$ are:

$$\rho^{j=0} := \frac{1}{2}\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & \sqrt{1-\lambda} & 0 \\ 0 & \sqrt{1-\lambda} & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \; \rho^{j=1} := \frac{1}{2}\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{1-\lambda} \\ 0 & 0 & \sqrt{1-\lambda} & 1-\lambda \end{pmatrix}. \tag{5}$$

From Eq. (5), we obtain the following joint probabilities P_{AEB}:

$$\begin{aligned} P_{000} &= \frac{(\sqrt{1-\lambda}+1)^2}{8}; \quad P_{001} = \frac{(\sqrt{1-\lambda}-1)^2}{8}, \\ P_{002} &= P_{003} = P_{102} = P_{103} = \frac{\lambda}{8}; \quad P_{100} = P_{101} = \frac{1}{8}, \\ P_{110} &= P_{111} = \frac{(1-\lambda)}{8}, \end{aligned} \tag{6}$$

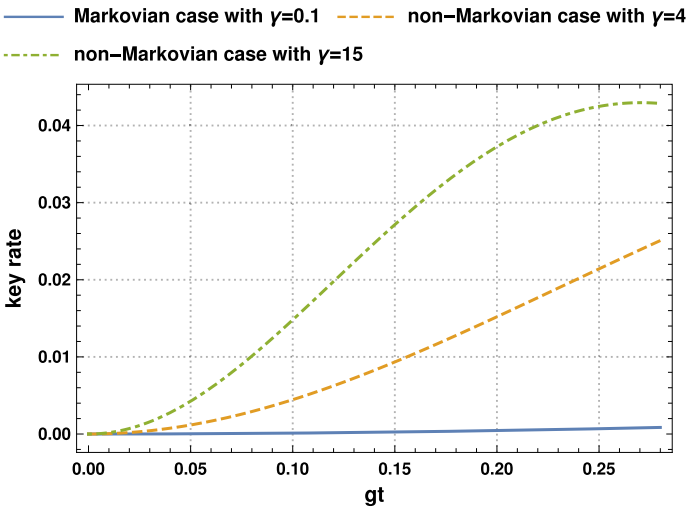

Fig. 2 Plot of secure key rate as a function of the dimensionless time gt, for the Case 1, where the travel qubit alone is subject to NMAD. Here, γ is the coupling strength and $g := 1$ in all the cases. In the considered time range, non-Markovian noise provides improvement in the key rate as seen for the cases of $\gamma = 4$ (dashed, orange curve) and $\gamma = 15$ (dot dashed, green curve), as opposed to the Markovian case with $\gamma = 0.1$ (bold, blue curve) (Color online)

with all other joint probability terms vanishing. Note that in the presence of amplitude damping noise, Bob will also obtain outcomes $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ in his Bell state measurement, which corresponds to the outcome symbols 2 and 3 in Eq. (6).

The probabilities Eq. (6) imply the mutual information between Alice and Bob is

$$\begin{aligned} I(A:B) = -\frac{1}{8}\Bigg(&-2\lambda + \left(\lambda - 2\left(\sqrt{1-\lambda}+1\right)\right)\log\left(\frac{-\lambda+2\sqrt{1-\lambda}+2}{-\lambda+\sqrt{1-\lambda}+2}\right) \\ &+(\lambda-2)\log\left(\frac{\lambda-2}{\lambda-\sqrt{1-\lambda}-2}\right) + (\lambda-2)\log\left(\frac{\lambda-2}{\lambda+\sqrt{1-\lambda}-2}\right) \\ &+\lambda\log\left(\frac{\lambda+2\sqrt{1-\lambda}-2}{\lambda+\sqrt{1-\lambda}-2}\right) + 2\left(\sqrt{1-\lambda}-1\right)\log\left(\frac{\lambda+2\sqrt{1-\lambda}-2}{\lambda+\sqrt{1-\lambda}-2}\right)\Bigg), \end{aligned} \tag{7}$$

while that between Alice and Eve:

$$I(A:E) = \frac{2\log\left(\frac{2}{\lambda+3}\right) + (\lambda+1)\log\left(\frac{\lambda+1}{\lambda+3}\right) + \log(16)}{\log(16)}. \tag{8}$$

A plot of the key rate $\kappa \equiv I_{AB} - I_{AE}$ *w.r.t* (dimensionless) time is given in Fig. 2.

3.2 Case 2: Both the qubits are subject to NMAD

After receiving the returned noisy travel qubit, Bob subjects both qubits individually to NMAD, described by Eq. (3). Accordingly, the final states with Bob for the Alice's encodings $j = 0$ and $j = 1$ are:

$$\rho_{hty}^{(j=0)} = \frac{1}{2}\begin{pmatrix} 2\lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & 1-\lambda & 0 \\ 0 & 1-\lambda & 1-\lambda & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \quad \rho_{hty}^{(j=1)} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1-\lambda & 1-\lambda & 0 \\ 0 & 1-\lambda & 1-\lambda & 0 \\ 0 & 0 & 0 & 2\lambda \end{pmatrix}. \quad (9)$$

From Eq. (9), we obtain the following joint probabilities P_{AEB}, as follows:

$$\begin{aligned} P_{000} &= \frac{1-\lambda}{2}, \\ P_{002} &= P_{003} = P_{102} = P_{103} = \frac{\lambda}{4}, \\ P_{100} &= P_{101} = \frac{1-\lambda}{8}, \\ P_{110} &= P_{111} = \frac{1-\lambda}{8}, \end{aligned} \quad (10)$$

with all other joint probability terms vanishing.

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

$$\begin{aligned} I(A:B) &= \frac{3}{4}(1-\lambda)\log\left(\frac{4}{3}\right) = 0.31(1-\lambda), \\ I(A:E) &= 1 + \frac{1}{2}\log\left(\frac{2}{\lambda+3}\right) + \frac{1}{4}(\lambda+1)\log\left(\frac{\lambda+1}{\lambda+3}\right). \end{aligned} \quad (11)$$

The key rate $\kappa \equiv I_{AB} - I_{AE}$ is shown in Fig. (3).

For both the above cases, from Eqs. (5) and (9), one can calculate the Holevo bound for Alice–Bob by tracing out Eve's systems x, y. It is found that mutual information between Alice and Bob $I(A:B)$ is always lesser than the Alice–Bob Holevo bound suggesting that Bob's measurement strategy is sub-optimal. However, the Holevo bound between Eve's states for Alice's encoding $j \in \{0, 1\}$ equals $I(A:E)$, with or without added noise, suggests that Eve's attack strategy in indeed optimal.

4 On the classical simulation of the quantum advantage

In Ref. [16], it was shown that adding classical noise to measurement data by a trusted party can improve information security. In contrast, here we show that this is not possible for the cases of quantum advantage reported in Sects. 3.1 and 3.2. That is adding classical noise locally on the part of Bob or even Alice cannot reproduce the

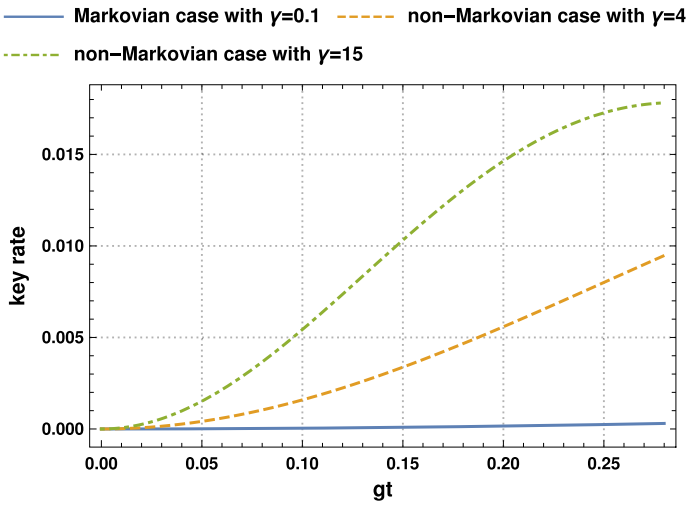

Fig. 3 Plot of secure key rate with respect to the dimensionless time gt, for the Case 2, where the both travel and home qubits are subject to NMAD noise. Here, γ is the coupling strength and $g := 1$ in all the cases. In the considered time range, non-Markovian noise provides improvement in the key rate as seen for the cases of $\gamma = 4$ (dashed, orange curve) and $\gamma = 15$ (dot dashed, green curve), as opposed to the Markovian case with $\gamma = 0.1$ (bold, blue curve) (Color online)

benefit of adding the quantum noise. This non-simulability of the quantum advantage may be attributed to the fact that in the regime where the quantum noise is beneficial, it leaves the Bell pair entangled, and thus, the resulting joint probability statistics cannot be captured by local classical noise.

Consider that Alice and Bob try to locally (i.e., with no communication whatsoever) reproduce P_{002}^{AEB}, P_{012}^{AEB} and P_{112}^{AEB} of joint probabilities (10) from the noiseless data (2). Let a_{jk} define the probability with which Alice uses a pseudorandom number generator (PRNG) to make a transition from a bit value of A in the noiseless data (2) to a bit value of A' in the noisy data (10), where A' is the bit value locally reproduced by Alice. Similarly, we define the probability b_{jk} for Bob's local transitions using a PRNG to produce a bit value of B'. Consider the case of reproducing the following joint probabilities from Eqs. (2) and (10):

$$\begin{aligned} P_{0'12'}^{A'EB'} &= P_{110}^{AEB} a_{10} b_{02} + P_{111}^{AEB} a_{10} b_{12} = 0 \\ &= \frac{a_{10}}{8}(b_{02} + b_{12}) = 0, \end{aligned} \tag{12}$$

$$\begin{aligned} P_{1'12'}^{A'EB'} &= P_{110}^{AEB} a_{11}.b_{02} + P_{111}^{AEB} a_{11} b_{12} = 0 \\ &= \frac{a_{11}}{8}(b_{02} + b_{12}) = 0, \end{aligned} \tag{13}$$

and

$$P_{0'02'}^{A'EB'} = P_{000}^{AEB} a_{00} b_{02} + P_{100}^{AEB} a_{10} b_{02} + P_{101}^{AEB} a_{10} b_{12}$$

$$= \frac{a_{00}b_{02}}{2} + \frac{a_{10}}{8}(b_{02} + b_{12}) = \frac{\lambda}{4}. \tag{14}$$

From Eq. (12), it is implied that either $a_{10} = 0$ or $b_{02} + b_{12} = 0$ or both are zero. Note that since $\sum_k a_{jk} = 1, a_{11} = 1$. This implies that if $a_{10} = 0$ then, from Eq. (13), necessarily $b_{02} + b_{12} = 0$.

Now, from Eqs. (12) and (14),

$$a_{00}.b_{02} = \frac{\lambda}{2} \tag{15}$$

which implies that $a_{00} \neq 0$ and $b_{02} \neq 0$. Hence, we arrive at a contradiction that $b_{02} + b_{12} \neq 0$.

Now consider that $a_{10} \neq 0$ and $a_{11} \neq 0$. Then from Eqs. (12) and (13), necessarily $b_{02} + b_{12} = 0$. Again from Eqs. (14) and (15), observe that $b_{02} > 0$. Hence, we arrive at a contradiction again. It follows that Alice and Bob cannot unilaterally simulate the quantum advantage due to the NMAD channel by adding uncorrelated local classical noise to their measurement data.

5 Effect of temperature

A generalized amplitude damping (GAD) channel models the effect of temperature of the bath along with damping on the qubit state. As in our previous work [26], here we find that unital noise favors Eve in this scenario. We show below that an increase in temperature leads to an increase in the unitality of the channel, and correspondingly to a greater disadvantage for Alice and Bob. One way to understand this effect is as follows. A qubit channel $\mathcal{E}$ is unital if $\mathcal{E}[I] = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Now, one may compute

$$\rho_{\text{id}} = \mathcal{E}^{\text{GAD}}[I] = \begin{pmatrix} 1 - 2p\lambda + \lambda & 0 \\ 0 & (2p-1)\lambda + 1 \end{pmatrix}, \tag{16}$$

where $p \in \{0, \frac{1}{2}\}$. The action of a GAD channel $\mathcal{E}^{\text{GAD}}$ on a qubit is given by the quantum operation representation $\mathcal{E}[\rho] = \sum_k A_k \rho A_k^\dagger$, where the A_k are the Kraus operator, which for GAD take the form

$$A_1 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}; \qquad A_2 = \sqrt{1-p}\begin{pmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{pmatrix};$$
$$A_3 = \sqrt{p}\begin{pmatrix} 0 & 0 \\ \sqrt{\lambda} & 0 \end{pmatrix}; \qquad A_4 = \sqrt{p}\begin{pmatrix} \sqrt{1-\lambda} & 0 \\ 0 & 1 \end{pmatrix}, \tag{17}$$

where the noise mixing $p \in \{0, \frac{1}{2}\}$ and the damping parameter $\lambda \in \{0, 1\}$.

Note that the trace distance (TD) between ρ_{id} and I evaluates to $(2p-1)\lambda$, so that as $p \to \frac{1}{2}$, the TD $\to 0$, i.e., $\rho_{\text{id}} \to I$. Therefore, increasing temperature enhances the unital part of the noise.

6 Discussions and conclusions

We consider a QKD based on the ping-pong communication protocol, with a non-unital non-Markovian noise deliberately added by the legitimate party before measurement and prior to key distillation. The noise used is the non-Markovian amplitude damping (NMAD). We show that adding this noise improves the security, when Eve uses an optimal individual attack. Conservatively, all the channel noise is attributed to Eve's attack. Within a noise parameter range, non-Markovianity is shown to boost the key rate. We considered two cases. In one, Bob adds noise only to the travel qubit, while in the other, noise it is added to both the travel and home qubits. The former is shown to lead to a higher key rate than the latter in the considered range of time. This provides a cautionary indication that the benefits of non-Markovianity of the noise are conditional and depend on the full context considered. We also studied a non-Markovian generalized amplitude damping (GAD) noise in this context, but in this case we found that temperature tends to diminish the quantum advantage.

In the matter of local classical non-simulability of the quantum advantage of the considered non-Markovian noise, it is important to stress that the model of classical noise considered in Sect. 4 is Markovian, in that at each round the random bit assignment depends only on the measurement outcomes of the current round, and does not require memory of the data from previous rounds. This is a non-trivial assumption, but one that is natural in the current scenario, where the Bell pair used in each round is uncorrelated with any other pair, and furthermore, we restrict Eve to attacks on individual qubits. This ensures that the measurement probabilities in each round are independent. Therefore, one expects that classical memory across rounds is not advantageous for the simulation. It is an interesting question whether non-Markovian classical noise can perform better than Markovian classical noise, if one or both of the above assumptions are relaxed. That is, the protocol may involve Bob's travel qubits being entangled across the rounds and/or Eve launching a joint or collective attack on multiple travel qubits.

Here, it may be pointed out that the quantum noise models given by Eqs. (3) and (4) are considered non-Markovian despite being applied to individual rounds of the protocol. The reason is that the memory in this context is with respect to an external environment, rather than preceding rounds of the protocol. In particular, quantum non-Markovianity arises when the dynamics of the system–environment correlation makes the system's intermediate map (or, propagator) to deviate from complete positivity. [21].

Acknowledgements SU and RS acknowledge financial support of the Government of India DST-SERB grant EMR/2016/004019. SU also thanks the Admar Mutt Education Foundation (AMEF), Bengaluru, Karnataka, India, for partial financial support. SB and RS acknowledge the support from Interdisciplinary Cyber Physical Systems (ICPS) program of the Department of Science and Technology (DST), India, Grants

No.: DST/ICPS/QuST/Theme-1/2019/6 and DST/ICPS/QuST/Theme-1/2019/14, respectively. US thanks Ashutosh Singh and S. Omkar for helpful discussions.

References

1. Shenoy-Hejamadi, A., Pathak, A., Radhakrishna, S.: Quantum cryptography: key distribution and beyond. Quanta **6**(1), 1–47 (2017)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10–12 December 1984, pp. 175–179
3. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
4. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**(14), 140501 (2005)
5. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**(15), 157901 (2003)
6. Cai, Q.-Y., Li, B.-W.: Improving the capacity of the boström-felbinger protocol. Phys. Rev. A **69**(5), 054301 (2004)
7. Cai, Q.-Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23 (2006)
8. Zhang, Z., Man, Z., Li, Y.: Improving wójcik's eavesdropping attack on the ping-pong protocol. Phys. Lett. A **333**(1), 46–50 (2004)
9. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A **372**(22), 3953–3956 (2008)
10. Vasiliu, E.V.: Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. **10**(2), 189–202 (2011)
11. Zawadzki, P.: Security of ping-pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. **11**, 1–12 (2012)
12. Zawadzki, P.: Improving security of the ping-pong protocol. Quantum Inf. Process. **12**(1), 149–155 (2012)
13. Li, J., Song, D.J., Guo, X.J., JING, B.: An improved security detection strategy based on w state in "ping-pong" protocol. Chin. J. Electron. **21**, 117–120 (2012)
14. Han, Y.-G., Yin, Z.-Q., Li, H.-W., Chen, W., Wang, S., Guo, G.-C., Han, Z.-F.: Security of modified ping-pong protocol in noisy and lossy channel. Sci. Rep. **4**, 4936 (2014)
15. Banerjee, S.: Open Quantum Systems. Springer, Berlin (2018)
16. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A **72**, 012332 (2005)
17. Shadman, Z., Kampermann, H., Meyer, T., Bruß, D.: Optimal eavesdropping on noisy states in quantum key distribution. Int. J. Quantum Inf. **07**(01), 297–306 (2009)
18. Mertz, M., Kampermann, H., Shadman, Z., Bruß, D.: Quantum key distribution with finite resources: taking advantage of quantum noise. Phys. Rev. A **87**, 042312 (2013)
19. Usenko, Vladyslav C., Filip, Radim: Trusted noise in continuous-variable quantum key distribution: a threat and a defense. Entropy **18**(1), (2016)
20. García-Patrón, R., Cerf, N.J.: Continuous-variable quantum key distribution protocols over noisy channels. Phys. Rev. Lett. **102**, 130501 (2009)
21. Rivas, A., Huelga, S.F., Plenio, M.B.: Quantum non-Markovianity: characterization, quantification and detection. Rep. Prog. Phys. **77**(9), 094001 (2014)
22. Pradeep Kumar, N., Banerjee, S., Srikanth, R., Jagadish, V., Petruccione, F.: Non-Markovian evolution: a quantum walk perspective. Open Syst. Inf. Dyn. **25**(03), 1850014 (2018)
23. Li, L., Hall, M.J.W., Wiseman, H.M.: Concepts of quantum non-Markovianity: a hierarchy. Phys. Rep. **759**, 1–51 (2018)
24. Shrikant, U, Srikanth, R., Banerjee, Subhashish: On a concept of quantum non-Markovianity weaker than cp-indivisibility. arXiv:1911.04162
25. Pollock, F.A., Rodríguez-Rosario, C., Frauenheim, T., Paternostro, M., Modi, K.: Operational Markov condition for quantum processes. Phys. Rev. Lett. **120**, 040405 (2018)

26. Sharma, V., Shrikant, U., Srikanth, R.: Decoherence can help quantum cryptographic security. Quantum Inf. Process. **17**(88), 207 (2018)
27. Thapliyal, K., Pathak, A., Banerjee, S.: Quantum cryptography over non-Markovian channels. Quantum Inf. Process. **16**(5), 115 (2017)
28. Weiss, U.: Quantum Dissipative Systems. World Scientific, Singapore (2008)
29. de Vega, I., Alonso, D.: Dynamics of non-Markovian open quantum systems. Rev. Mod. Phys. **89**, 015001 (2017)
30. Rossi, M.A.C., Cattaneo, M., Paris, M.G.A., Maniscalco, S.: Non-Markovianity is not a resource for quantum spatial search on a star graph subject to generalized percolation. Quantum Measurements Quantum Metrol. **5**(1), 40–49 (2018)
31. Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. **81**, 3018–3021 (1998)
32. Bruß, D., Lütkenhaus, N.: Quantum key distribution: from principles to practicalities. Appl. Algebra Eng. Commun. Comput. **10**(4), 383–399 (2000)
33. Srikanth, R., Banerjee, S.: Squeezed generalized amplitude damping channel. Phys. Rev. A **77**(1), 012318 (2008)
34. Breuer, H.-P., Laine, E.-M., Piilo, J., Vacchini, B.: Colloquium: non-Markovian dynamics in open quantum systems. Rev. Modern Phys. **88**(2), 021002 (2016)
35. Passos, M.H.M., Concha Obando, P., Balthazar, W.F., Paula, F.M., Huguenin, J.A.O., Sarandy, M.S.: Non-Markovianity through quantum coherence in an all-optical setup. Opt. Lett. **44**(10), 2478–2481 (2019)
36. Salles, A., de Melo, F., Almeida, M.P., Hor-Meyll, M., Walborn, S.P., Souto Ribeiro, P.H., Davidovich, L.: Experimental investigation of the dynamics of entanglement: sudden death, complementarity, and continuous monitoring of the environment. Phys. Rev. A **78**, 022322 (2008)
37. Fanchini, F.F., Karpat, G., Çakmak, B., Castelano, L.K., Aguilar, G.H., Jiménez Farías, O., Walborn, S.P., Souto Ribeiro, P.H., De Oliveira, M.C.: Non-Markovianity through accessible information Non-Markovianity through accessible information. Phys. Rev. Lett. **112**(21), 210402 (2014)
38. Yugra, Y., De Zela, F., Cuevas, Á.: Coherence-based measurement of non-Markovian dynamics in an open quantum system. Phys. Rev. A **101**(1), 013822 (2020)