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

U. Shrikant,1, 2, * R. Srikanth,1, † and Subhashish Banerjee3

1Poornaprajna Institute of Scientific Research, Bangalore - 562164, India
2Graduate Studies, Manipal University, Manipal-576104
3IIT Jodhpur, Rajasthan India

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. We indicate a specific attack model, where non-unital, quantum non-Markovianity of the added noise can improve the key rate. We show that this noise-induced advantage cannot be obtained by Alice and Bob by adding local classical noise to their post-measurement data.

I. 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 past three decades, a number of QKD protocols have been proposed (cf. the review [1]). Noise is especially detrimental to quantum information processing, given the fragility of quantum resources [2]. 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 [3–5]. Here, we shall refer to such user added noise as “trusted”. Note that this terminology differs from that used by [6], who in the context of continuous variable QKD protocols [7] 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 [8–10], though we may reasonably posit weaker manifestations of quantum non-Markovianity (cf. [11, 12]). Thus, it is intuitive to expect that quantum non-Markovianity can be helpful to information processing [13, 14], especially at low temperatures [15, 16]. However, this is by no means automatic (cf. e.g., [17]).

In an earlier work it was shown [13] 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 to Markovian noise in certain time ranges.

There do not seem many works that have explored this practically useful aspect. Notably, Ref. [5] shows that deliberately adding depolarizing noise increases secure key rate for BB84 [18] and for entanglement based six-state protocols [19, 20]. This was somewhat inspired from the work [4] 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 Section II, we introduce the protocol, which is the “ping-pong” communication protocol adapted for QKD. In Section III we discuss the phenomenologically motivated model of amplitude damping noise and describe how it can be added during the protocol. We consider in Section III A the first scenario involving a single-qubit noise, and in Section III B, the second scenario involving two-qubit incoherent noise. In section IV 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 Section V.

*Electronic address: shrik@poornaprajna.org
†Electronic address: srik@poornaprajna.org
‡Electronic address: subhashish@iitj.ac.in
by applying either Alice through a quantum channel, ideally assumed to be noiseless and lossless. Alice then encodes the travel qubit pair of photons entangled in the polarization degree of freedom, out of which he sends one photon (travel photon) to

determined the Holevo information between trusted party Alice and malicious Eve. In practice, the key rate may be as high as

corresponding to Alice’s operation

legs. In this attack, Eve includes two ancillary particles, the first (labelled photons to be in the maximally mixed state. Wojcik [22] proposed a strategy by attacking the onward and return

ahead with key distillation, or else they abort the protocol.

potential indicator of eavesdropper Eve’s presence. If QBER is found to be less than a threshold value, they proceed

rate (QBER) by sampling a fraction of the qubits transmitted. On them, Alice announces her encoded bit and Bob

which he distinguishes through a Bell measurement. As a security check, both parties compute the quantum bit error

is left with either of the two Bell states

for

announces the Bell state he detected. The fraction of cases where their records differ is an estimate of QBER, and a

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

After the end of the quantum round, Bob receives the final states $|\Psi\rangle_{\text{fin}} = \frac{1}{\sqrt{2}}(|012\rangle + |102\rangle)$, 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

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

(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.

III. NOISE ADVANTAGE

In general, it is known that noise can degrade the quantum information processing tasks, in particular QKD. In Ref. [13], 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 Section II. 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 \[ E_A^0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1 - \lambda(t)} \end{bmatrix}, \quad E_A^1 = \begin{bmatrix} 0 & \sqrt{\lambda(t)} \\ 0 & 0 \end{bmatrix}, \] where

\[ \lambda(t) = 1 - e^{-gt} \left( g l \sinh \left( \frac{lt}{2} \right) + \cosh \left( \frac{lt}{2} \right) \right)^2, \] with \( l = \sqrt{g^2 - 2\gamma g} \). Here, \( g \) is the spectral band width of the noise and \( \gamma \) 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 [24].

The above noise may be simulated in an all-optical setup [25–27] by associating the qubit to 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 [25], the authors of [28] propose an optical simulation of Markovian and non-Markovian AD. However, we consider the former approach for our case in this paper.

Below we analyze the protocol in Markov and non-Markov regimes, and compare improvement in the key rates.

**A. Case 1: Only travel qubit subjected to NMAD**

When the photon returns back to Bob, the state of the system \( h_{ty} \) 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 the Alice’s encodings \( j = 0 \) and \( j = 1 \) are:

\[ \rho^{j=0} = \frac{1}{2} \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & 1 - \lambda & \sqrt{1 - \lambda} & 0 \\ 0 & \sqrt{1 - \lambda} & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad \rho^{j=1} = \frac{1}{2} \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{1 - \lambda} \\ 0 & 0 & \frac{1}{\sqrt{1 - \lambda}} & 1 - \lambda \end{bmatrix}. \] (5)

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

\[ P_{000} = \frac{(\sqrt{1 - \lambda} + 1)^2}{8}; \quad P_{001} = \frac{(\sqrt{1 - \lambda} - 1)^2}{8}, \]
\[ P_{002} = P_{003} = P_{102} = P_{103} = \frac{\lambda}{8}; \quad P_{100} = P_{101} = \frac{1}{8}, \]
\[ P_{110} = P_{111} = \frac{(1 - \lambda)}{8}, \] (6)

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
FIG. 2: (Color online). 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 $\gamma$ 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).

$$I(A : B) = -\frac{1}{8} \left( -2\lambda + \left( \lambda - 2 \left( \sqrt{1 - \lambda} + 1 \right) \right) \log \left( \frac{-\lambda + 2\sqrt{1 - \lambda} + 2}{-\lambda + \sqrt{1 - \lambda} + 2} \right) 
+ (\lambda - 2) \log \left( \frac{\lambda - 2}{\lambda - \sqrt{1 - \lambda} - 2} \right) + (\lambda - 2) \log \left( \frac{\lambda - 2}{\lambda + \sqrt{1 - \lambda} - 2} \right) + \lambda \log \left( \frac{\lambda + 2\sqrt{1 - \lambda} - 2}{\lambda + \sqrt{1 - \lambda} - 2} \right) 
+ 2 \left( \sqrt{1 - \lambda} - 1 \right) \log \left( \frac{\lambda + 2\sqrt{1 - \lambda} - 2}{\lambda + \sqrt{1 - \lambda} - 2} \right) \right),$$

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 Figure 3.

**B. 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:

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

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

$$P_{000} = \frac{1 - \lambda}{2},$$
$$P_{002} = P_{003} = P_{102} = P_{103} = \frac{\lambda}{4},$$
$$P_{100} = P_{101} = \frac{1 - \lambda}{8},$$
$$P_{110} = P_{111} = \frac{1 - \lambda}{8}. \tag{10}$$
FIG. 3: (Color online) 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 $\gamma$ 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).

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

$$I(A : B) = \frac{3}{4}(1 - \lambda) \log \left(\frac{4}{3}\right) = 0.31(1 - \lambda),$$

$$I(A : E) = 1 + \frac{1}{2} \log \left(\frac{2}{\lambda + 3}\right) + \frac{1}{4}(\lambda + 1) \log \left(\frac{\lambda + 1}{\lambda + 3}\right).$$

(11)

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

For both the cases above, 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.

IV. ON THE CLASSICAL SIMULATION OF THE QUANTUM ADVANTAGE

In Ref. [3] 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 Sections III A and III B. That is adding classical noise locally on the part of Bob or even Alice cannot reproduce the 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 $P_{AEB}^{002}$, $P_{AEB}^{012}$ and $P_{AEB}^{112}$ of joint probabilities (10) from the noiseless data (2). Let $a_{jk}$ define the probability with which Alice uses a pseudo-random 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):

$$P_{012}' = P_{110}^{AEB} a_{10}b_{02} + P_{111}^{AEB} a_{10}b_{12} = 0$$

$$= \frac{a_{10}}{8}(b_{02} + b_{12}) = 0,$$

(12)
\[ P_{AB}^{AE'B'} = P_{110}^{AEB} a_{11} b_{02} + P_{111}^{AEB} a_{11} b_{12} = 0 \]
\[ = \frac{a_{11}}{8} (b_{02} + b_{12}) = 0, \]  
(13)

and
\[ P_{0'02'}^{AE'B'} = P_{000}^{AEB} a_{00} b_{02} + P_{100}^{AEB} a_{10} b_{02} + P_{101}^{AEB} a_{10} b_{12} \]
\[ = \frac{a_{00} b_{02}}{2} + \frac{a_{10}}{8} (b_{02} + b_{12}) = \frac{\lambda}{4}. \]  
(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),
\[ a_{00} b_{02} = \frac{\lambda}{2} \]  
(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 Eq. (12) and (13), necessarily \( b_{02} + b_{12} = 0 \). Again from Eq. (14) and (15), observe that \( b_{02} > 0 \). Hence, we arrive at a contradiction again. It follows that Alice and Bob can not unilaterally simulate the quantum advantage due to the NMAD channel by adding uncorrelated local classical noise to their measurement data.

V. 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 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. This is because of the fact that, as shown in our previous work [13], unital noise favors Eve in this scenario. 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
\[ \rho_{\text{id}} = \mathcal{E}_{\text{GAD}}[I] = \begin{pmatrix} 1 - 2p\lambda + \lambda & 0 \\ 0 & (2p - 1)\lambda + 1 \end{pmatrix}, \]  
(16)

where \( p \in \{0, \frac{1}{2}\} \) and \( \mathcal{E}_{\text{GAD}} \) is given in the Appendix. Note that the trace distance (TD) between \( \rho_{\text{id}} \) 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.

Acknowledgments

US acknowledges financial support of the Govt. of India DST-SERB grant EMR/2016/004019. SB and RS acknowledge the support from Interdisciplinary Cyber Physical Systems (ICPS) programme of the Department of Science and Technology (DST), India, Grant No.: DST/ICPS/QuST/Theme-1/2019/6. US thanks Ashutosh Singh and S. Omkar for helpful discussions.

[1] Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna. Quantum cryptography: Key distribution and beyond. Quanta, 6(1):1–47, 2017.
[2] Subhashish Banerjee. Open quantum systems: Dynamics of Nonclassical Evolution. Springer Nature, Singapore., 2018.
[3] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A, 72:012332, Jul 2005.
The action of a GAD channel 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

$$A_1 = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}; \quad A_2 = \sqrt{1-p} \begin{pmatrix} 0 & \sqrt{\lambda} \\ \sqrt{\lambda} & 0 \end{pmatrix}; \quad A_3 = \sqrt{p} \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}; \quad A_4 = \sqrt{p} \begin{pmatrix} \sqrt{1-\lambda} & 0 \\ 0 & 1 \end{pmatrix}.$$ (17)

where $p \in \{0, \frac{1}{2}\}$ and $\lambda \in \{0, 1\}$. 

**GAD channel**

The action of a GAD channel 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

$$A_1 = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}; \quad A_2 = \sqrt{1-p} \begin{pmatrix} 0 & \sqrt{\lambda} \\ \sqrt{\lambda} & 0 \end{pmatrix}; \quad A_3 = \sqrt{p} \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}; \quad A_4 = \sqrt{p} \begin{pmatrix} \sqrt{1-\lambda} & 0 \\ 0 & 1 \end{pmatrix}.$$ (17)

where $p \in \{0, \frac{1}{2}\}$ and $\lambda \in \{0, 1\}$.