Quantum discord as a resource for quantum cryptography
- Supplementary Information -

Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, United Kingdom

KEYS FROM SEPARABLE GAUSSIAN STATES

Here we provide a simple example of device-dependent QKD protocol which is based on the distribution of a bipartite Gaussian state which is mixed and separable (not in a tensor-product, therefore having non-zero discord). We show that the key rates can be positive despite no entanglement being present. The reader not familiar with the formalism of bosonic systems and Gaussian states can find these concepts in Ref. [1], whose notation is here adopted ($\hbar = 2$ and unit vacuum noise).

Let us consider a continuous variable QKD protocol where Alice prepares two bosonic modes, A and a, in a separable Gaussian state ρ_{Aa}, with zero mean and covariance matrix (CM)

$$\mathbf{V}_{Aa} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \mu\mathbf{I} \end{pmatrix}, \tag{1}$$

where $\mu \geq 1$ and $\mathbf{G}$ is a diagonal correlation block which can be in one of the following forms

$$\mathbf{G} = \begin{pmatrix} g & \\ & g \end{pmatrix} := g\mathbf{I},\ \mathbf{G} = \begin{pmatrix} g & \\ & -g \end{pmatrix} := g\mathbf{Z}. \tag{2}$$

Here the parameter g must satisfy $|g| \leq \mu - 1$, so that $\mathbf{V}_{Aa}$ is both physical and separable [2]. Apart from the singular case $g = 0$, this symmetric Gaussian state has always non-zero discord, i.e., $D(A|a) = D(a|A) > 0$ [3].

Mode a is sent through the channel, where Eve performs a collective Gaussian attack, whose most general description can be found in Ref [4]. Assuming random permutations (so that quantum de Finetti applies), this is the most powerful attack against Gaussian protocols [1]. One of the canonical forms of this attack is the so-called ‘entangling cloner’ attack [1], where Eve uses a beam splitter with transmissivity τ to mix the incoming mode a with one mode e of an EPR state $\rho_{eE'}$ with CM

$$\mathbf{V}_{eE'} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix} := \mathbf{V}(\omega), \tag{3}$$

where $\omega \geq 1$. One output mode B is sent to Bob, while the other output mode E is stored in a quantum memory together with the retained mode E'. Such memory will be coherently detected at the end of the protocol.

In order to extract two correlated (complex) variables, X and Y, Alice and Bob heterodyne their local modes A and B. (Note that other protocols involving homodyne detection for one of the parties or even two homodynes may be considered as well.) One can easily check that Alice remotely prepares thermal states on mode a. In fact, by heterodyning mode A, the other mode a is collapsed in a Gaussian state $\rho_{a|X}$ with CM $\mathbf{V}_{a|X} = (1 + \varepsilon)\mathbf{I}$, where

$$\varepsilon := \mu - 1 - \frac{g^2}{\mu + 1} \geq 0 \tag{4}$$

quantifies the thermalization above the coherent state. This conditional thermal state is randomly displaced in the phase space according to a bivariate Gaussian distribution with variance $\mu - 1 - \varepsilon$ (so that the average input state on mode a is thermal with the correct CM $\mu\mathbf{I}$).

At the output of the channel, Bob’s average state is thermal with CM $\nu_B\mathbf{I}$, where

$$\nu_B := \tau\mu + (1 - \tau)\omega. \tag{5}$$

By propagating the conditional thermal state $\rho_{a|X}$, we also get Bob’s conditional state $\rho_{B|X}$, which is randomly displaced and has CM $\nu_{B|X}\mathbf{I}$, where

$$\nu_{B|X} := \tau(1 + \varepsilon) + (1 - \tau)\omega = \nu_B - \frac{\tau g^2}{\mu + 1}. \tag{6}$$

Therefore, we can easily compute Alice and Bob's mutual information, which is equal to

$$I(X,Y)=\log_2\frac{\nu_B+1}{\nu_{B|X}+1}. \tag{7}$$

The next step is the calculation of Eve's Holevo information on Alice's and Bob's variables. We derive the global state of Alice, Bob and Eve, which is pure Gaussian with zero mean and CM

$$\mathbf{V}_{ABEE'}=\begin{pmatrix} \mu\mathbf{I} & \sqrt{\tau}\mathbf{G} & -\sqrt{1-\tau}\mathbf{G} & \mathbf{0} \\ \sqrt{\tau}\mathbf{G} & \nu_B\mathbf{I} & \gamma\mathbf{I} & \delta\mathbf{Z} \\ -\sqrt{1-\tau}\mathbf{G} & \gamma\mathbf{I} & \nu_E\mathbf{I} & \kappa\mathbf{Z} \\ \mathbf{0} & \delta\mathbf{Z} & \kappa\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \tag{8}$$

where $\mathbf{0}$ is the 2×2 zero matrix, and

$$\nu_E := \tau\omega+(1-\tau)\mu, \tag{9}$$
$$\gamma := \sqrt{\tau(1-\tau)}(\omega-\mu), \tag{10}$$
$$\delta := \sqrt{1-\tau}\sqrt{\omega^2-1}, \tag{11}$$
$$\kappa := \sqrt{\tau(\omega^2-1)}. \tag{12}$$

From this global CM, we extract Eve's reduced CM $\mathbf{V}_{EE'}:=\mathbf{V}_{\mathbf{E}}$ describing the two output modes $\mathbf{E}=EE'$ of the entangling cloner. This reduced CM has symplectic spectrum [1]

$$\nu_{\mathbf{E}}^{\pm}=\frac{\sqrt{\alpha^2+4\beta}\pm\alpha}{2}, \tag{13}$$

where

$$\alpha := (1-\tau)(\mu-\omega), \tag{14}$$
$$\beta := \tau+(1-\tau)\mu\omega. \tag{15}$$

The von Neumann entropy of Eve's average state is then given by

$$S(\mathbf{E})=h(\nu_{\mathbf{E}}^{+})+h(\nu_{\mathbf{E}}^{-}), \tag{16}$$

where

$$h(x):=\frac{x+1}{2}\log_2\frac{x+1}{2}-\frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{17}$$

By transforming the global CM under heterodyne detection [1], we compute Eve's conditional CMs. First, we derive Eve's CM conditioned to Bob's detection

$$\mathbf{V}_{\mathbf{E}|Y}=\mathbf{V}_{\mathbf{E}}-\frac{1}{\nu_B+1}\begin{pmatrix} \gamma^2\mathbf{I} & \gamma\delta\mathbf{Z} \\ \gamma\delta\mathbf{Z} & \delta^2\mathbf{I} \end{pmatrix}, \tag{18}$$

which has symplectic spectrum

$$\nu_{\mathbf{E}|Y}^{-}=1,\ \nu_{\mathbf{E}|Y}^{+}=\frac{\mu+\beta}{1+\mu\tau+(1-\tau)\omega}. \tag{19}$$

Then, Eve's CM conditioned to Alice's detection is

$$\mathbf{V}_{\mathbf{E}|X}=\mathbf{V}_{\mathbf{E}}-\frac{(1-\tau)g^2}{\mu+1}\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \tag{20}$$

and has symplectic spectrum

$$\nu_{\mathbf{E}|X}^{\pm}=\frac{\sqrt{\theta^2+4(\mu+1)\phi}\pm\theta}{2(\mu+1)}, \tag{21}$$

where

$$\theta := (1-\tau)g^2 - (\mu+1)\alpha, \tag{22}$$

$$\phi := (\mu+1)\beta - (1-\tau)\omega g^2. \tag{23}$$

From the previous conditional spectra, we compute Eve's conditional entropies

$$S(\mathbf{E}|X) = h(\nu^{+}_{\mathbf{E}|X}) + h(\nu^{-}_{\mathbf{E}|X}),\ S(\mathbf{E}|Y) = h(\nu^{+}_{\mathbf{E}|Y}), \tag{24}$$

and, therefore, we can derive the two Holevo quantities $I(\mathbf{E},X) = S(\mathbf{E}) - S(\mathbf{E}|X)$ and $I(\mathbf{E},Y) = S(\mathbf{E}) - S(\mathbf{E}|Y)$. By subtracting these from Alice and Bob's mutual information $I(X,Y)$, we finally get the two key rates in direct and reverse reconciliation, i.e., $K(Y|X)$ and $K(X|Y)$.

It is easy to check the existence of wide range of parameters for which these two rates are strictly positive, so that Alice and Bob can extract a secret key despite the absence of entanglement (at the input state ρ_{Aa} and, therefore, also at the output state ρ_{AB}). As an example, we may consider the maximum correlation value $g = \mu - 1$ for the separable Gaussian state ρ_{Aa}, and we may take the large modulation limit $\mu \rightarrow +\infty$, as typical in continuous variable QKD. In this case, we get the following asymptotical expression for Alice and Bob's mutual information

$$I(X,Y) \rightarrow \log_2 \frac{\tau\mu}{1+3\tau+(1-\tau)\omega} + O(\mu^{-1}), \tag{25}$$

and the following asymptotical spectra

$$\nu^{-}_{\mathbf{E}} \rightarrow (1-\tau)\mu + \tau\omega + O(\mu^{-1}), \tag{26}$$

$$\nu^{+}_{\mathbf{E}} \rightarrow \omega + O(\mu^{-1}), \tag{27}$$

$$\nu^{+}_{\mathbf{E}|Y} \rightarrow \frac{1+(1-\tau)\omega}{\tau} + O(\mu^{-1}), \tag{28}$$

$$\nu^{\pm}_{\mathbf{E}|X} \rightarrow \xi_{\pm} + O(\mu^{-1}), \tag{29}$$

where

$$\xi_{\pm} := \frac{\sqrt{(\omega+3)^2 + \tau^2(\omega-3)^2 - 2\tau(\omega^2+7)}}{2} \pm \frac{(1-\tau)(\omega-3)}{2}. \tag{30}$$

Then, using the expansion $h(x) \simeq \log_2(ex/2) + O(1/x)$ for large x, we can write the two asymptotical rates

$$K(Y|X) = R(\tau,\omega) + h(\xi_+) + h(\xi_-), \tag{31}$$

$$K(X|Y) = R(\tau,\omega) + h\left[\frac{1+(1-\tau)\omega}{\tau}\right], \tag{32}$$

where we have introduced the common term

$$R(\tau,\omega) := \log_2 \frac{2\tau}{e(1-\tau)[1+3\tau+(1-\tau)\omega]} - h(\omega). \tag{33}$$

As we can see from Fig. 1, there are wide regions of positivity for these rates.

In particular, for a pure loss channel ($\omega = 1$), the previous asymptotical rates simplify to the following

$$K(Y|X) = \log_2 \frac{\tau}{e(1-\tau^2)} + h(3-2\tau), \tag{34}$$

which is positive for any $\tau > 0.693$, and

$$K(X|Y) = \log_2 \frac{\tau}{e(1-\tau^2)} + h\left(\frac{2}{\tau} - 1\right), \tag{35}$$

which is positive for any $\tau > 0.532$.

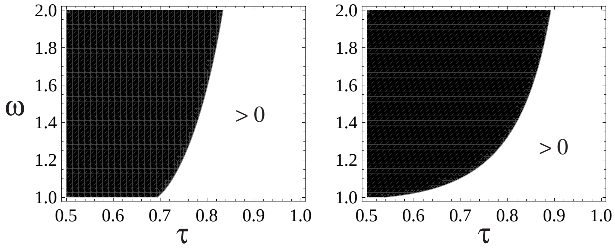

FIG. 1: *Left panel.* Rate $K(Y|X)$ in direct reconciliation, as a function of channel transmissivity τ and thermal variance ω. K is positive in the white area, while it is zero in the black area. *Right panel.* Rate $K(X|Y)$ in reverse reconciliation, as function of τ and ω. White area ($K > 0$) is wider at low ω.

DISCORD BOUND CAN BE TIGHT

Here we discuss a typical scenario where the optimal backward rate $K(\blacktriangleleft)$ of an ideal QKD protocol is exactly equal to the output discord $D(B|A)$ shared by Alice and Bob. This happens in continuous variable QKD, where reverse reconciliation is extremely important for its ability to beat the 3dB loss-limit affecting direct reconciliation [1]. (Other possible strategies include postselection [5, 6] and two-way quantum communication [7]).

Consider an ideal QKD protocol which is based on the distribution of an EPR state ρ_{Aa}, with CM $\mathbf{V}_{Aa} = \mathbf{V}(\mu)$ defined according to Eq. (3) with $\mu \geq 1$. By performing a rank-1 Gaussian POVM on mode A, Alice remotely prepares an ensemble of Gaussianly-modulated pure Gaussian states on the other mode a. For instance, heterodyne prepares coherent states, while homodyne prepares squeezed states. On average, mode a is described by a thermal state with CM $\mu\mathbf{I}$.

Suppose that signal mode a is subject to a pure-loss channel. This means that Eve is using a beam splitter of transmissivity τ mixing the signal mode with a vacuum mode e. At the output of the beam splitter, mode B is detected by Bob, while mode E is stored in a quantum memory coherently detected by Eve (this is a collective entangling cloner attack with $\omega = 1$).

Since the average state of mode a is thermal and mode e is in the vacuum, no entanglement can be present between the two output ports B and E of the beam splitter. This implies that their entanglement of formation must be zero $E_f(B, E) = 0$ and, therefore, the optimal backward rate $K(\blacktriangleleft)$ must be equal to the discord $D(B|A)$ of the Gaussian state ρ_{AB}. Since this output state has CM

$$\mathbf{V}_{AB} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\tau(\mu^2-1)}\mathbf{Z} \\ \sqrt{\tau(\mu^2-1)}\mathbf{Z} & (\tau\mu + 1 - \tau)\mathbf{I} \end{pmatrix}, \tag{36}$$

its discord is easy to compute and is equal to [8]

$$D(B|A) = h(\mu) - h[\tau + (1-\tau)\mu]. \tag{37}$$

For large modulation ($\mu \to +\infty$), we have the asymptotic expression

$$K(\blacktriangleleft) = D(B|A) = \log_2\left(\frac{1}{1-\tau}\right), \tag{38}$$

which is positive for any $0 < \tau < 1$. One can check that this rate can be achieved by heterodyne detections at Bob's side (and coherent detection at Alice's side).

[1] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N.J. Cerf, T.C. Ralph, J.H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[2] S. Pirandola, A. Serafini, and S. Lloyd, Phys. Rev. A **79**, 052327 (2009).
[3] S. Rahimi-Keshari, C.M. Caves, and T.C. Ralph, Phys. Rev. A **87**, 012119 (2013).
[4] S. Pirandola, S.L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[5] C. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[6] A.M. Lance, T. Symul, V. Sharma, C. Weedbrook, T.C. Ralph, and P.K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[7] S. Pirandola, S. Mancini, S. Lloyd, and S.L. Braunstein, Nature Phys. **4**, 726 (2008).
[8] S. Pirandola *et al.*, preprint arXiv:1309.2215.