Long-distance continuous-variable quantum key distribution with quantum scissors

Masoud Ghalaii,[1] Carlo Ottaviani,[2] Rupesh Kumar,[3] Stefano Pirandola,[2] and Mohsen Razavi[1]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, United Kingdom*
[2]*Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom*
[3]*Department of Physics, University of York, York YO10 5DD, United Kingdom*

(Dated: August 7, 2018)

The use of quantum scissors, as candidates for non-deterministic amplifiers, in continuous-variable quantum key distribution systems is investigated. Such devices rely on single-photon sources for their operation and as such, they do not necessarily preserve the Guassianity of the channel. Using exact analytical modeling for system components, we bound the secret key generation rate for the system that uses quantum scissors. We find that for non-zero values of excess noise such a system can reach longer distances than the system with no amplification. The prospect of using quantum scissors in continuous-variable quantum repeaters is therefore emboldened.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] addresses the problem of sharing secret keys between two users. Such keys can then be used for secure communications. While original QKD protocols [1–4] rely on encoding data in discrete quantum states, such as the polarization of single photons, one can also exploit continuous-variable QKD (CV QKD) protocols, in which data is encoded on the quadratures of the light [5–8]. In particular, the recent progress in CV QKD systems has placed them in a competitive position with their conventional discrete-variable counterparts [9, 10]. For instance, contrary to discrete-variable QKD protocols, which require single-photon detectors, CV QKD uses coherent measurement schemes, such as homodyne and/or heterodyne detection, to measure light quadratures, without relying on photon counting devices [11–13]. Moreover, CV QKD protocols can be the better choice over short distances [10]. Once it comes to long distances, however, CV QKD has its own challenges to compete with discrete-variable QKD [14]. This paper examines how the security distance can be enhanced in CV QKD systems by using realistic non-deterministic amplification [15].

One of the proposed solutions to improve the rate-versus-distance performance of CV QKD protocols is to use noiseless linear amplifiers (NLAs) [15, 16]. It is known that deterministic amplification cannot be noise free [17]. An NLA can only then work *probabilistically*. This inevitably reduces the key rate by a factor corresponding to the success rate of the NLA, which implies that, at short distances, the use of NLAs may not be beneficial. The key rate may, however, increase at long distances because of the improvement in the signal to noise ratio. That is, while the number of data points we can use for key extraction is less, the quality of the remaining points could be such high that a larger number of secret key bits can be extracted. This has been shown theoretically by treating the NLA as a probabilistic, but *noiseless*, black box and assuming that the NLA achieves its theoretically maximum possible success rate for all possible inputs [15].

The story can be quite different when we replace the above ideal NLA with realistic systems that offer NLA-like functionality. For instance, one of the most basic structures for an NLA is a quantum scissor (QS), which combines the incoming light with a single photon [18]. While under weak signal assumptions, a QS can be approximated as an NLA, more precise analysis reveals that its operation is not necessarily noiseless. This is particularly important because in many CV QKD protocols the transmitted signal does not have a fixed power, and realistic NLAs often treat different input signals differently. This is more or less true for other proposals that implement the NLA operation [19–24].

In this paper, we provide a realistic account of what a QS can offer within a CV QKD setup. In particular, using an exact model for the QS setup, we analyze the secret key rate of a Gaussian modulated protocol, whose receiver unit is equipped with a QS. One of the implications of our exact modeling for the QS is the inapplicability of standard key rate calculation techniques that rely on the Gaussianity of the output states. This will make the exact calculation of the key rate cumbersome. We manage this problem by using relevant bounds for certain components of the key rate. We find that by using the QS we can exchange secret keys over longer distances. Our work also provides insights into the practicality of the recent proposals for CV quantum repeaters [25, 26].

The manuscript is structured as follows. In Sec. II, we describe details of the proposed system. In Sec. III, by analyzing input-output characteristic functions of a single QS, we calculate the exact output state and success probability of the QS NLA in Ref. [18]. We further study the non-Gaussian behavior of the system. In Sec. IV, we present the key rate analysis of the CV QKD link with a single QS as part of its receiver. In Sec. V, we discuss the numerical results. Finally, Sec. VI concludes the paper.

II. SYSTEM DESCRIPTION

In this section, we describe our proposed setup for the QS-amplified CV QKD protocol. We assume that the sender, Alice (A), is connected to the receiver, Bob (B), via a quantum channel; see Fig. 1(a). The protocol runs along the same lines as proposed by Grosshans and Grangier in 2002 (GG02) [5, 6, 27, 28]. That is, in every round, Alice transmits a co-

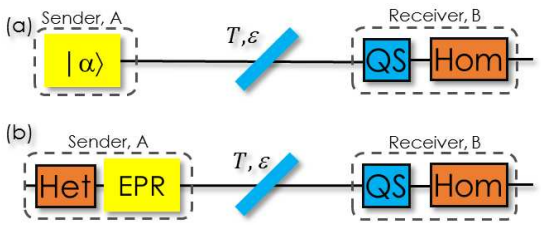

FIG. 1. (a) Schematic view of CV QKD link with an additional quantum scissor at the receiver. A beam splitter with transmittivity T characterizes the quantum channel, with excess noise at the input represented by ε. (b) Entanglement-based CV QKD protocol equivalent to (a). QS, Hom and Het boxes represent, respectively, a non-deterministic quantum scissor, the homodyne detection and heterodyne detection modules.

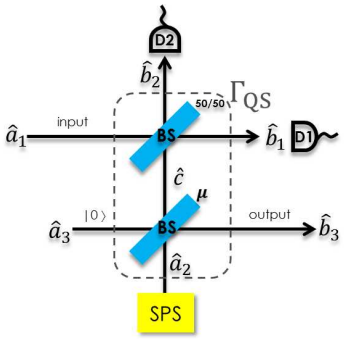

FIG. 2. The schematic diagram of a quantum scissor. Here, we assume that an on-demand ideal single-photon source (SPS) is in use, and that the single-photon detectors have unity efficiencies.

herent state $|\alpha\rangle$, where $\alpha = x_A + ip_A$, to Bob, with real parameters x_A and p_A being chosen randomly according to the following Gaussian probability density functions:

$$f_{X_A}(x_A) = \frac{e^{-\frac{x_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}} \quad \text{and} \quad f_{P_A}(p_A) = \frac{e^{-\frac{p_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}}, \quad (1)$$

where V_A is the modulation variance in the shot-noise units. At the receiver, however, we equip Bob with a single QS before the homodyne module used in GG02. Upon a successful QS operation, Bob randomly chooses to measure $\hat{x}_B = \hat{a}_B + \hat{a}_B^\dagger$ or $\hat{p}_B = (\hat{a}_B - \hat{a}_B^\dagger)/i$, where $\hat{a}_B$ represents the annihilation operator for the output mode of the QS. During the sifting stage, Bob would then publicly declare his measurement choices as well as the rounds in which the QS has been successful. Alternatively, one can use the equivalent entanglement-based (EB) scheme of Fig. 1(b), where Alice's source is replaced with an EPR source followed by heterodyne detection. In either case, we assume that Bob can reconstruct, in an error-free way, the phase reference for the local oscillator used in his homodyne detection. By using post-processing techniques, Alice and Bob extract a key from the subset of data for which the QS has been successful.

Quantum scissors are the main building blocks in the NLA proposed by Ralph and Lund [18]. At the core of a QS, there is a partial Bell-state measurement (BSM) module, with a balanced beam splitter followed by two single-photon detectors, in the space spanned by number states $|0\rangle$ and $|1\rangle$. This BSM module is driven by an asymmetric entangled state $|\psi\rangle = \sqrt{\mu}|1\rangle_c|0\rangle_{b_3} + \sqrt{1-\mu}|0\rangle_c|1\rangle_{b_3}$, generated by a single photon that goes through a beam splitter with transmittance μ; see Fig. 2. For an input state in the $|0\rangle$-$|1\rangle$ space, the QS could then offer an asymmetric teleportation functionality, whenever the BSM operation is successful, i.e., when only one of D1 or D2 detector in Fig. 2 clicks. For instance, in the particular case of a weak coherent state input $|\alpha\rangle_{a_1} \approx |0\rangle_{a_1} + \alpha|1\rangle_{a_1}$, with $|\alpha| \ll 1$, a single click could come from the single-photon component in the entangled state $|\psi\rangle$ and/or the input state. In that case, the output state, after renormalization, can be approximated by $|0\rangle_{b_3} + \alpha g|1\rangle_{b_3} \approx |\alpha g\rangle_{b_3}$, for $|g\alpha| \ll 1$, where $g = \sqrt{(1-\mu)/\mu}$ represents the amplification gain of the QS.

Under these assumptions, the success probability for the QS operation is given by $P_{\rm succ}^{\rm RL}(\alpha) \approx \mu + (1-\mu)|\alpha|^2$. Note that, in the above description, the essential assumption for a QS to possibly operate as an NLA is that $|\alpha| \ll 1$.

There are two reservations in using the above asymptotic approach for analyzing a QS-based CV QKD system. First, note that the output state of a QS is always in the space spanned by single-photon and vacuum states. By approximating the output state as a coherent state, we are introducing some errors, which can affect the security of the system. More precisely, the transition from a coherent state to a single-photon state is a non-Gaussian one, whose effect must be carefully considered in the security analysis. Secondly, in the GG02 protocol, the coherent states are chosen randomly via Gaussian distributions; hence, the input states to the QS may not necessarily satisfy the assumption $|\alpha| \ll 1$.

In order to resolve the above issues, in our work, we find the *exact* output state and probability of success for an arbitrary coherent state at the input of a QS. This will be detailed in Sec. III. We then apply our findings to the key rate analysis of a QS-equipped CV QKD system. For simplicity, we assume that the required single-photon source (SPS) in the QS is ideal and on-demand. Single-photon detector efficiencies are also assumed to be unity. Our analysis can, nevertheless, be extended to account for the imperfections in the source and detectors.

III. QUANTUM SCISSORS: INPUT-OUTPUT RELATIONSHIP

In this section, we first obtain an exact input-output relationship for a QS driven by a coherent state. We use characteristic functions to model the input and output states. For a joint, M-mode, state $\hat{\rho}$, where each mode j is represented by an annihilation operator $\hat{a}_j$, the anti-normally ordered characteristic function is given by

$$\chi_{\rm A}^{\hat{\rho}}(\xi_1, \ldots, \xi_M) = \left\langle \bigotimes_{j=1}^{M} \hat{D}_{\rm A}(\hat{a}_j, \xi_j) \right\rangle_{\hat{\rho}}, \quad (2)$$

where $\langle\circ\rangle_{\hat{\rho}} \equiv \mathrm{Tr}[\hat{\rho}\circ]$ and $\hat{D}_{\rm A}(\hat{a},\xi) = e^{-\xi^*\hat{a}}e^{\xi\hat{a}^\dagger}$ is the anti-normally ordered displacement operator with ξ^* being the complex conjugate of the complex number $\xi = \xi_r + i\xi_i$, where ξ_r and ξ_i are real numbers. The density matrix $\hat{\rho}$ and its anti-normally ordered characteristic function are related via a Fourier-like transformation relationship as follows

$$\hat{\rho} = \int \frac{d^2\xi_1}{\pi}\cdots\int \frac{d^2\xi_M}{\pi}\chi^{\hat{\rho}}_{\rm A}(\xi_1,\ldots,\xi_M)\bigotimes_{j=1}^{M}\hat{D}_{\rm N}(\hat{b}_j,\xi_j), \tag{3}$$

where $\hat{D}_{\rm N}(\hat{a},\xi) = e^{\xi\hat{a}^\dagger}e^{-\xi^*\hat{a}}$ is the normally-ordered displacement operator and $\int d^2\xi = \int_{-\infty}^{+\infty} d\xi_r \int_{-\infty}^{+\infty} d\xi_i$.

In the following, we use the above formalization, to characterize a QS driven by an arbitrary coherent state.

A. Pre-measurement state

For the QS in Fig. 2, we can use the well-known relationships for beam splitters to relate the three input modes of the linear circuit, represented by $\hat{a}_1$, $\hat{a}_2$ and $\hat{a}_3$, to the three output modes, represented by $\hat{b}_1$, $\hat{b}_2$ and $\hat{b}_3$. In fact, we have $[\hat{b}_1\ \hat{b}_2\ \hat{b}_3]^{\rm T} = \Gamma_{\rm QS}[\hat{a}_1\ \hat{a}_2\ \hat{a}_3]^{\rm T}$, where

$$\Gamma_{\rm QS} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \sqrt{\mu} & -\sqrt{1-\mu} \\ -1 & \sqrt{\mu} & -\sqrt{1-\mu} \\ 0 & \sqrt{2(1-\mu)} & \sqrt{2\mu} \end{pmatrix}. \tag{4}$$

The output anti-normally ordered characteristic function can then be expressed in terms of the input one by

$$\begin{aligned}\chi^{\rm out}_{\rm A}(\xi_1,\xi_2,\xi_3) =& \langle\hat{D}_{\rm A}(\hat{b}_1,\xi_1)\hat{D}_{\rm A}(\hat{b}_2,\xi_2)\hat{D}_{\rm A}(\hat{b}_3,\xi_3)\rangle \\ =& \langle\hat{D}_{\rm A}(\hat{a}_1,\lambda_1)\hat{D}_{\rm A}(\hat{a}_2,\lambda_2)\hat{D}_{\rm A}(\hat{a}_3,\lambda_3)\rangle \\ =& \chi^{\rm in}_{\rm A}(\lambda_1,\lambda_2,\lambda_3),\end{aligned} \tag{5}$$

where $[\lambda_1\ \lambda_2\ \lambda_3]^{\rm T} = \Gamma^{\rm T}_{\rm QS}[\xi_1\ \xi_2\ \xi_3]^{\rm T}$ with $\Gamma^{\rm T}_{\rm QS}$ being the transpose of $\Gamma_{\rm QS}$. In above, we made use of the facts that $\hat{D}_{\rm A}(s\hat{a},\xi) = \hat{D}_{\rm A}(\hat{a},s\xi)$, where s is a real number, and $\langle\hat{D}_{\rm A}(\hat{a},\xi_1)\hat{D}_{\rm A}(\hat{a},\xi_2)\rangle = e^{\xi_1\xi_2^*}\langle\hat{D}_{\rm A}(\hat{a},\xi_1+\xi_2)\rangle$. Note that $\Gamma_{\rm QS}$ is unitary, i.e., $\Gamma^{\rm T}_{\rm QS} = \Gamma^{-1}_{\rm QS}$. Hence, we have $\sum_j|\xi_j|^2 = \sum_j|\lambda_j|^2$.

Next, for the particular input state $|\alpha\rangle_{\hat{a}_1}|1\rangle_{\hat{a}_2}|0\rangle_{\hat{a}_3}$ the output characteristic function can be found as follows

$$\begin{aligned}\chi^{\rm out}_{\rm A}(\xi_1,\xi_2,\xi_3) =& \mathrm{Tr}\big[|\alpha\rangle_{\hat{a}_1}\langle\alpha|\otimes|1\rangle_{\hat{a}_2}\langle 1|\otimes|0\rangle_{\hat{a}_3}\langle 0| \\ & \hat{D}_{\rm A}(\hat{a}_1,\lambda_1)\hat{D}_{\rm A}(\hat{a}_2,\lambda_2)\hat{D}_{\rm A}(\hat{a}_3,\lambda_3)\big] \\ =& e^{-|\lambda_1|^2-|\lambda_2|^2-|\lambda_3|^2}e^{\bar{\alpha}\lambda_1-\alpha\bar{\lambda}_1}(1-|\lambda_2|^2),\end{aligned} \tag{6}$$

which can be re-written as the following:

$$\begin{aligned}\chi^{\rm out}_{\rm A}(\xi_1,\xi_2,\xi_3) =& e^{-|\xi_1|^2-|\xi_2|^2-|\xi_3|^2}e^{\sqrt{2}i\mathbb{I}m[\bar{\alpha}(\xi_1-\xi_2)]} \\ & \times(1-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{\frac{2(1-\mu)}{\mu}}\xi_3|^2),\end{aligned} \tag{7}$$

with $\mathbb{I}m[\xi]$ being the imaginary part of the complex number ξ. Using Eq. (3), the output state of the system is then given by

$$\begin{aligned}\hat{\rho}_{\rm out} = \int\frac{d^2\xi_1}{\pi}\int\frac{d^2\xi_2}{\pi}\int\frac{d^2\xi_3}{\pi}\chi^{\rm out}_{\rm A}(\xi_1,\xi_2,\xi_3) \\ \hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3).\end{aligned} \tag{8}$$

B. Post-selected state

Following Ref. [18], we consider a QS successful only if one detector in Fig. 2 clicks. In order to model such measurements we use the following non-resolving measurement operator

$$\hat{M} = (\mathbb{1} - |0\rangle_1\langle 0|)\otimes|0\rangle_2\langle 0|, \tag{9}$$

which corresponds to the case where detector D1 clicks while D2 does not. The post-selected state, $\hat{\rho}^{\rm PS}_{\rm out}$, is then given by [29]:

$$\begin{aligned}\hat{\rho}^{\rm PS}_{\rm out} =& \frac{\mathrm{Tr}_{\hat{b}_1\hat{b}_2}(\hat{M}\hat{\rho}_{\rm out})}{\mathrm{Tr}(\hat{M}\hat{\rho}_{\rm out})} \\ =& \frac{1}{P^{\rm PS}}\int\frac{d^2\xi_1}{\pi}\int\frac{d^2\xi_2}{\pi}\int\frac{d^2\xi_3}{\pi}\chi^{\rm out}_{\rm A}(\xi_1,\xi_2,\xi_3) \\ & \times[\pi\delta^2(\xi_1)-1]\hat{D}_{\rm N}(\hat{b}_3,\xi_3),\end{aligned} \tag{10}$$

where $\delta^2(\xi) = \delta(\xi_r)\delta(\xi_i)$ and $P^{\rm PS} = \mathrm{Tr}(\hat{M}\hat{\rho}_{\rm out})$ is the corresponding (success) probability to measurement $\hat{M}$, which will be calculated in Sec. III C. In Eq. (10), we used the identities $\langle 0|\hat{D}_{\rm N}(\hat{a},\xi)|0\rangle = 1$ and $\langle 1|\hat{D}_{\rm N}(\hat{a},\xi)|1\rangle = 1-|\xi|^2$.

Because the truncated post-measurement state lives in the qubit subspace spanned by number states $\{|0\rangle_{b_3},|1\rangle_{b_3}\}$, the output state has the form

$$\hat{\rho}^{\rm PS}_{\rm out} = \rho_{00}|0\rangle_{b_3}\langle 0| + \rho_{01}|0\rangle_{b_3}\langle 1| + \rho_{10}|1\rangle_{b_3}\langle 0| + \rho_{11}|1\rangle_{b_3}\langle 1|, \tag{11}$$

where $\rho_{jk} = {}_{b_3}\langle j|\hat{\rho}^{\rm PS}_{\rm out}|k\rangle_{b_3}$, for $j,k=0,1$. We then obtain

$$\begin{cases}\rho_{00}(\alpha) = e^{-\frac{|\alpha|^2}{2}}\frac{\mu}{2}(1+\frac{|\alpha|^2}{2})/P^{\rm PS} \\ \rho_{01}(\alpha) = \frac{\alpha^*}{2}e^{-\frac{|\alpha|^2}{2}}\sqrt{\mu(1-\mu)}/P^{\rm PS} \\ \rho_{10}(\alpha) = \frac{\alpha}{2}e^{-\frac{|\alpha|^2}{2}}\sqrt{\mu(1-\mu)}/P^{\rm PS} \\ \rho_{11}(\alpha) = e^{-\frac{|\alpha|^2}{2}}(1-\mu)(1-e^{-\frac{|\alpha|^2}{2}})/P^{\rm PS}.\end{cases} \tag{12}$$

We remark that in the case that detector D2 clicks and D1 does not, the QS is still considered successful. After working out the post-selected output state, we find that the result has the same form as in Eq. (11), but we only need to replace α with $-\alpha$ in Eq. (12). In practice, in a QKD setup, Bob can negate its measurement results whenever this happens. One can also use a unitary operation to correct the output state so that we always end up with Eq. (11) as the post-selected state.

We note that the post-measurement state is Hermitian and positive-semidefinite, as expected. In addition, in the limit of $|g\alpha| \ll 1$, we can verify that the post-selected state of the single QS approaches the weak coherent state $|g\alpha\rangle$.

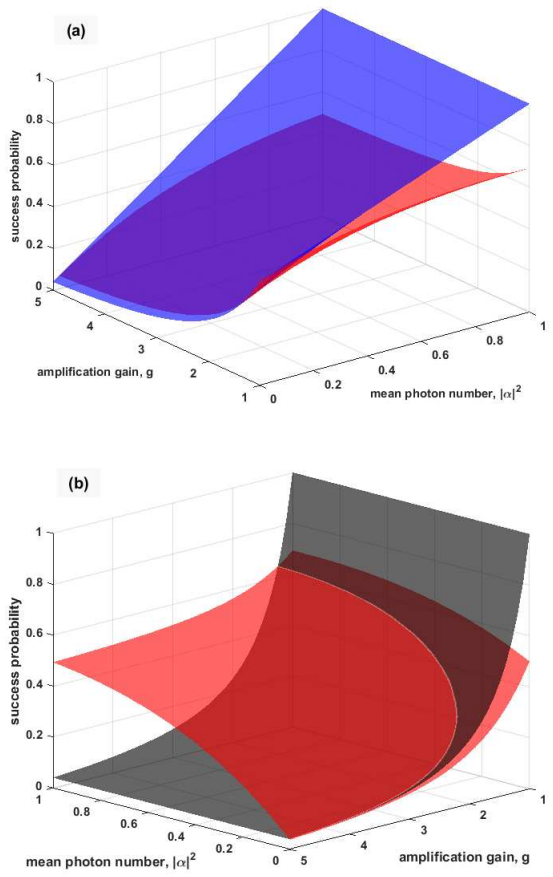

FIG. 3. (a) The exact success probability of a single QS (lower red), $P_{\rm succ}$, and that based on approximations in Ref. [18] (upper blue), $P^{\rm RL}_{\rm succ}$. (b) The exact success probability of a single QS (red), $P_{\rm succ}$, and that of an ideal NLA (grey), $1/g^2$, versus average photon number and amplification gain.

C. Probability of success

The probability of success for measurement $\hat{M}$, $P^{\rm PS}$, is given by

$$\begin{aligned} P^{\rm PS} =& {\rm Tr}(\hat{M}\hat{\rho}_{\rm out}) \\ =& \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \chi^{\rm out}_{\rm A}(\xi_1,\xi_2,0)[\pi\delta^2(\xi_1)-1]. \end{aligned} \quad (13)$$

By substituting Eq. (7) into the above expression, we obtain

$$\begin{aligned} P_{\rm succ}(\alpha) &= 2P^{\rm PS}(\alpha) \\ &= \big[2-\mu(1-\frac{|\alpha|^2}{2})\big]e^{-|\alpha|^2/2} - 2(1-\mu)e^{-|\alpha|^2}, \end{aligned} \quad (14)$$

where $P_{\rm succ}(\alpha)$ is the total probability of success for the QS module, i.e., when either of D1 or D2 detector clicks. As expected, $P_{\rm succ}(\alpha)$ approaches, to first-order approximation, to $P^{\rm RL}_{\rm succ}(\alpha) = \mu + (1-\mu)|\alpha|^2 = (1+|g\alpha|^2)/(1+g^2)$, when $|\alpha| \ll 1$. This approximation is, however, invalid even when we slightly deviate from the condition on $|\alpha|$, as can be seen in Fig. 3(a). Here, we have plotted the exact probability of success, $P_{\rm succ}(\alpha)$, versus $|\alpha|^2$ and g, and compared it with the asymptotic value obtained by Ralph and Lund, $P^{\rm RL}_{\rm succ}(\alpha)$. It can be seen that the exact probability of success is always lower than the asymptotic value, and the difference is visible at all values of g. The success probability also increases with the decrease in g. For $|\alpha| \ll 1$, the success probability approaches its maximum possible value of $1/g^2$ [17]. But, again, as can be seen in Fig. 3(b), we quickly deviate from this ideal regime when $|\alpha|$ increases. This indicates that we cannot operate at maximum possible success probability for all possible inputs, as assumed in Ref. [15], if we use a QS as an NLA.

In Fig. 3(b), the maximum possible success probability, $1/g^2$, divides the plot into two regions. There is a region in which the success probability is above the maximum possible for an NLA. This implies that the QS operation should be very noisy in this region, hence breaking the assumption on the noise-free operation of the NLA. If we want to work in the region that $P_{\rm succ}(\alpha) < 1/g^2$, we will then have to deal with limitations on the maximum gain that we can choose for the range of input states we may expect. This indicates a trade-off between the amount of noise that the QS may add to the signal versus its gain and success probability. We will later address this issue, in the context of CV QKD, in our numerical results when we optimize the secret key generation rate over system parameters.

D. Non-Gaussian behavior of the QS

Before calculating the secret key generation rate of a QS-equipped CV QKD system, it is necessary to better understand the nature of a quantum channel that includes a QS module. This is important because majority of results on the secret key rate of CV QKD systems rely on Gaussian characteristics of the channel [27, 30]. This is not, however, the case for a QS module as we see in this section.

In order to examine the non-Gaussian behavior of the QS output, let us focus on the distribution of homodyne measurement results on quadrature $\hat{x}_B$. Let us also consider a loss-less noise-free channel, which provides an input coherent state $|\alpha\rangle$, with $\alpha = x_A + ip_A$ as distributed by Eq. (1), at the QS port $\hat{a}_1$. The case of lossy and noisy channels will be considered in Appendix A. The probability distribution for obtaining a real number x_B after measuring $\hat{x}_B$, conditional on the transmission of $|\alpha\rangle$ and the success of the QS, is then given by

$$\begin{aligned} f_{X_B}(x_B|\alpha) &= {\rm Tr}[|x_B\rangle\langle x_B|\hat{\rho}^{\rm PS}_{\rm out}(\alpha)] \\ &= \big[\rho_{00}(\alpha) + \sqrt{2}\big(\rho_{01}(\alpha)+\rho^*_{01}(\alpha)\big)x_B \\ &\quad + 2\rho_{11}(\alpha)x_B^2\big]\frac{e^{-x_B^2}}{\sqrt{\pi}}, \end{aligned} \quad (15)$$

where $\hat{x}_B|x_B\rangle = x_B|x_B\rangle$. In above, we substituted $\hat{\rho}^{\rm PS}_{\rm out}(\alpha)$ from Eq. (11). Now, by averaging over all possible input

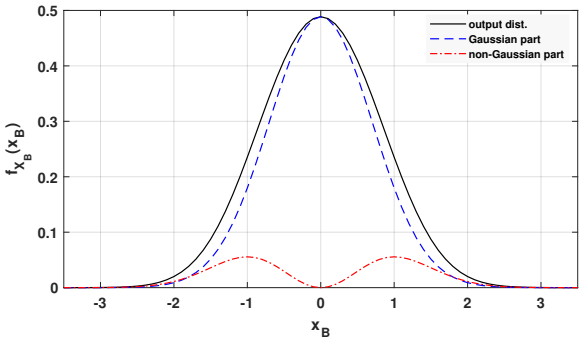

FIG. 4. The output distribution at the receiver side (solid-black), which comprises Gaussian (dashed blue) and non-Gaussian (dot-dashed red) parts. Here, $g = 3$ and $V_A = 0.04$.

states, we obtain

$$f_{X_B}(x_B) = \int dx_A \int dp_A \; f_{X_A}(x_A) f_{P_A}(p_A) f_{X_B}(x_B|\alpha). \tag{16}$$

In the above expression, because $f_{X_A}(x_A)$ and $f_{P_A}(p_A)$ have zero-mean Gaussian distributions, the term $\rho_{01}(\alpha) + \rho_{01}^*(\alpha)$ is averaged out after the integration in Eq. (16). The expression for $f_{X_B}(x_B)$ will then have two components: one is a Gaussian term in x_B proportional to the average of $\rho_{00}(\alpha)$, and the other is a non-Gaussian term proportional to the average of $\rho_{11}(\alpha)$. Figure 4 shows the contribution of each of these components in making $f_{X_B}(x_B)$ for $g = 3$ and $V_A = 0.04$. We notice that even for such a small modulation variance, which corresponds mostly to small values of $|\alpha|$, the non-Gaussian term is quite distinct. Higher amplification gains could even result in more deviation from a Gaussian state. This non-Gaussian behavior would have ramifications on the key rate analysis of a QS-based system as we see next.

IV. SECRET KEY RATE ANALYSIS

In this section, we use the results in Sec. III to determine the secret key rate of the GG02 protocol when Bob uses a single QS before his homodyne measurement. We find the secret key rate in a nominal operation condition when no eavesdropper is present. We assume a thermal loss channel with trasmissivity T, modeled by a beam splitter, and an excess noise, ε, at the input of the channel. The secret key rate of CV QKD protocols in the asymptotic limit of infinitely many signals is given by

$$K = \beta I_{\rm AB} - \chi_{\rm BE}, \tag{17}$$

where β, $I_{\rm AB}$, $\chi_{\rm BE}$ are, respectively, the reconciliation efficiency, the mutual information between Alice and Bob, and eavesdroppers accessible information when reverse reconciliation is used.

In our proposed setup, since the QS operation is non-deterministic, the whole key rate formula should be multiplied by the *average* success probability of the QS, $\overline{P}_{\rm succ}$, where the averaging is performed over all possible inputs. Therefore, the secret key rate reads

$$K_{\rm QS} \geq \overline{P}_{\rm succ}(\beta I^{\star}_{\rm AB} - \chi^{\star}_{\rm BE}), \tag{18}$$

where '$\star$' indicates that the mutual and Holevo information terms are calculated for the post-selected data when the QS is successful. The measurement results corresponding to unsuccessful QS events will be discarded at the sifting stage.

The fact that we only use the post-selected data for key extraction implies that we have to account for the non-Gaussianity of the QS output states. Unfortunately, the non-Gaussian behavior of the QS makes conventional methods for key rate calculation inapplicable. In order to take the non-Gaussian effects into account, we calculate the exact mutual information by directly using the conditional distribution of the QS output. Ideally one could also look for the exact calculation of the Holevo information term as well. But, this turns out to be extremely cumbersome. Instead, in this paper, we find an upper bound for the Holevo information term by finding the covariance matrix (CM) of the actual channel and then calculate the Holevo information for a Gaussian channel with the same CM. The reason is that Gaussian collective attacks for a given CM is proven optimal in the sense that they maximize the Holevo quantity [30]; hence, providing a lower bound on the key rate.

In the following, we provide more detail on how each of the terms in Eq. (18) can be calculated.

A. Mutual information

The mutual information between two random variables X_A and X_B, corresponding, respectively, to post-selected data on Alice and Bob side, is, by definition, the difference between the entropy function $H(X_B)$ and the conditional entropy $H(X_B|X_A)$ [31]:

$$I^{\star}_{\rm AB} = H(X_B) - H(X_B|X_A), \tag{19}$$

where

$$H(X_B) = -\int dx_B \; f_{X_B}(x_B) \log_2 f_{X_B}(x_B), \tag{20}$$

and

$$H(X_B|X_A) = -\int dx_A f_{X_A}(x_A) \times \int dx_B f_{X_B}(x_B|x_A) \log_2 f_{X_B}(x_B|x_A), \tag{21}$$

with

$$f_{X_B}(x_B|x_A) = \int dp_A f_{P_A}(p_A) f_{X_B}(x_B|x_A + ip_A). \tag{22}$$

In above, $f_{X_B}(x_B|x_A + ip_A)$ and $f_{X_B}(x_B)$ can, respectively, be obtained from Eqs. (15) and (16), after making the necessary adjustments to account for channel loss and the excess

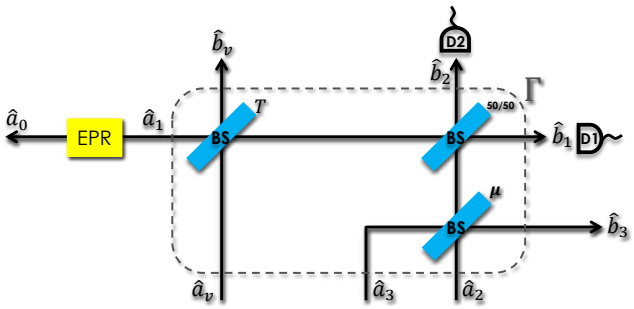

FIG. 5. QS-amplified EB CV QKD scheme. The quantum channel and the QS are considered as a combined system with input modes $\hat{a}_1 - \hat{a}_3$ and $\hat{a}_v$ and three output modes $\hat{b}_1 - \hat{b}_3$ and $\hat{b}_v$. The transformation matrix of the system is given by Eq. (23).

noise; see Appendix A for details. In our work, we numerically carry out the above integrals for a given set of parameters.

B. Holevo information

In order to calculate the Holevo information term, $\chi^{\star}_{\rm BE}$, we use the EB description of the protocol, where one part of an EPR state travels through the quantum channel and amplified by a QS, while the other is measured by Alice; see Fig. 5. In order to upper bound $\chi^{\star}_{\rm BE}$, what we need is then the CM of Alice-Bob bipartite state. We will then first derive the exact post-selected joint state, from which the CM parameters can be obtained.

We use a similar approach to Sec. III in using characteristic functions to find a relationship between Alice and Bob states when the QS is successful. As shown in Fig. 5, we also account for the effect of the quantum channel in our calculations. Note that the dashed box in Fig. 5 is a linear optics circuit, for which input-output relationships can be obtained. In particular, considering the input modes represented by $\mathcal{A}^T = [\hat{a}_1\ \hat{a}_2\ \hat{a}_3\ \hat{a}_v]$ and output modes $\mathcal{B}^T = [\hat{b}_1\ \hat{b}_2\ \hat{b}_3\ \hat{b}_v]$, we find $\mathcal{B} = \Gamma\mathcal{A}$, where the transformation matrix

$$\Gamma = \begin{pmatrix} \sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & \sqrt{\frac{1-T}{2}} \\ -\sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & -\sqrt{\frac{1-T}{2}} \\ 0 & \sqrt{1-\mu} & \sqrt{\mu} & 0 \\ -\sqrt{1-T} & 0 & 0 & \sqrt{T} \end{pmatrix} \tag{23}$$

is a unitary matrix.

By using Eq. (2) and the transformation matrix Γ, we can now write the full output anti-normally ordered characteristic function, including $\hat{a}_0$ mode, in terms of the input one by $\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_v) = \chi^{\rm in}_{\rm A}(\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_v)$, where

$$[\lambda_0\ \lambda_1\ \lambda_2\ \lambda_3\ \lambda_v]^T = \begin{pmatrix} 1 & 0 \\ 0 & \Gamma^T \end{pmatrix} [\xi_0\ \xi_1\ \xi_2\ \xi_3\ \xi_v]^T, \tag{24}$$

with $\sum_j |\lambda_j|^2 = \sum_j |\xi_j|^2$ and

$$\chi^{\rm in}_{\rm A}(\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_v) = \chi^{\rm EPR}_{\rm A}(\lambda_0,\lambda_1) \times \chi^{\rm in}_{\rm A}(\lambda_2,\lambda_3,\lambda_v), \tag{25}$$

where $\chi^{\rm EPR}_{\rm A}(\lambda_0,\lambda_1) = \exp\{-\delta^2(|\lambda_0|^2 + |\lambda_1|^2) - 2\mathbb{R}e(\delta\gamma\lambda_0^*\lambda_1^*)\}$ is the anti-normally ordered characteristic function of the EPR state with parameters δ and $\gamma = \sqrt{\delta^2-1}$, $\mathbb{R}e[\xi]$ being the real part of the complex number ξ, and $\chi^{\rm in}_{\rm A}(\lambda_2,\lambda_3,\lambda_v)$ is calculated for an input state $|1\rangle_{\hat{a}_2}|0\rangle_{\hat{a}_3}|0\rangle_{\hat{a}_v}$. Putting all this together, we then find the pre-measurement anti-normally ordered characteristic function for modes $\hat{a}_0$, $\hat{b}_1$, $\hat{b}_2$, $\hat{b}_3$, and $\hat{b}_v$ as follows:

$$\begin{aligned} \chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_v) = {} & e^{-\delta^2|\xi_0|^2} e^{-\omega\mathbb{R}e\left(\xi_0^*(\xi_1^*-\xi_2^*)\right)} \\ & \times e^{-\frac{\delta^2 T}{2}|\xi_1-\xi_2-\sqrt{2}\tau\xi_v|^2} e^{-\frac{1-T}{2}|\xi_1-\xi_2+\frac{\sqrt{2}}{\tau}\xi_v|^2} \\ & \times e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2} e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2} \\ & \times \left(1-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2\right), \end{aligned} \tag{26}$$

where $g = \sqrt{(1-\mu)/\mu}$, $\tau = \sqrt{(1-T)/T}$, and $\omega = 2\delta\gamma\sqrt{T/2}$. Note that we account for the effect of excess noise by adjusting the effective modulation variance as described in Appendix A.

Having obtained the characteristic function, we can find the corresponding output density matrix using Eq. (3). Then, by tracing out the output mode $\hat{b}_v$ and also performing photon-detection measurements on modes $\hat{b}_1$ and $\hat{b}_2$—by introducing the same measurement operator as in Eq. (9)—we find the resultant joint state of $\hat{a}_0$ and $\hat{b}_3$ modes in the case of having a successful event.

Appendix B provides the detailed calculations of the post-measurement density matrix, and the corresponding CM parameters. It turns out that the CM of the shared bipartite state between Alice and Bob has the form

$$\gamma_{\rm AB} = \begin{pmatrix} a\mathbb{1} & c\sigma_{\rm z} \\ c\sigma_{\rm z} & b\mathbb{1} \end{pmatrix}, \tag{27}$$

where $\mathbb{1} = \mathrm{diag}(1,1)$ and $\sigma_{\rm z} = \mathrm{diag}(1,-1)$ with

$$
\begin{aligned}
a &= -1 - \frac{2}{(g^2+1)\overline{P}_{\rm succ}}\Big(\frac{4\delta^2[\gamma^2 T-(2F+1)][(2F+1)g^2+2F]-4\delta^2\gamma^2 T}{(2F+1)^3} - \frac{\delta^2 g^2(\gamma^2 T-2F)}{2F^2}\Big),\\
b &= -1 - \frac{2}{(g^2+1)\overline{P}_{\rm succ}}\Big(-\frac{4[g^2(2F+1)+2F]}{(2F+1)^2} - \frac{4g^2}{2F+1} + \frac{2g^2}{F}\Big),\\
c &= \frac{8\delta\gamma g\sqrt{T}}{(g^2+1)(2F+1)^2\overline{P}_{\rm succ}},
\end{aligned}
\tag{28}
$$

and

$$
F = \frac{1-T+\delta^2 T}{2} \quad \text{and} \quad \overline{P}_{\rm succ} = \frac{2}{g^2+1}\Big(\frac{2[(2F+1)g^2+2F]}{(2F+1)^2} - \frac{g^2}{2F}\Big).
$$

It is interesting to make the following observation. If the EPR state is assumed totally uncorrelated, which happens when its squeezing parameter goes to zero, both parts of the state are left with vacuum states. Thus, if the QS is successful, the output state of mode $\hat{b}_3$ should be a vacuum state as well. This means that the CM of the end-to-end state is identity [8]. We verify that in the case of having a totally uncorrelated EPR state, corresponding to $\delta = 1$ and $\gamma = 0$, the expressions above will indeed result in the identity matrix; that is, we obtain $a = b = 1$ and $c = 0$.

Now that the CM is known, we can upper bound the Holevo information by using Eq. (B13).

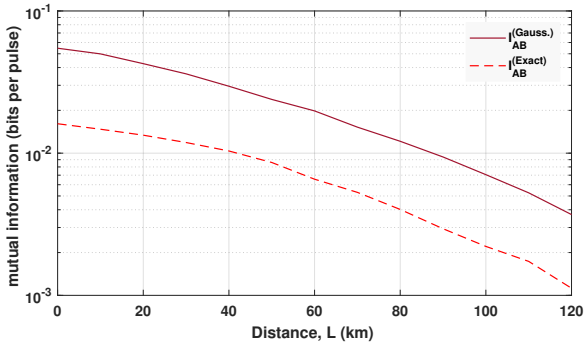

FIG. 6. The exact mutual information function (dashed) as compared to its Gaussian approximation (solid) versus distance at $\varepsilon = 0$. All other parameters have been optimized.

V. NUMERICAL RESULTS

In this section, we present numerical simulations of the secret key rate of the QS-amplified GG02 protocol and compare it with that of the conventional one. We find the maximum value for the lower bound in Eq. (18) by optimizing, at each distance, the modulation variance, V_A, or, equivalently, the parameter δ in the EB scenario, as well as the QS parameter, μ, which specifies the QS amplification gain. We also account for the excess noise which, as discussed in Appendix A, can be included in the modulation variance. We assume that the quantum channel between the sender and receiver is an optical fiber with loss factor α, whose transmittance is given by $T = 10^{-\alpha L/10}$, where L is the channel length and the loss factor is $\alpha = 0.2$ dB/km corresponding to standard optical fibers. Also, we assume $\beta = 1$ and that ideal homodyne detection, with no electronic noise, is performed at the receiver.

We first highlight the importance of accounting for the non-Gaussian behavior of the QS by comparing the difference between the exact value of the mutual information function $I^{\star}_{\rm AB}$, given by Eq. (19), and that obtained by Gaussian approximation, $I^{\rm G}_{\rm AB}$, in Eq. (B14). Figure 6 shows both curves, versus distance, at no excess noise. It is clear that the Gaussian approximation would have overestimated the mutual info between Alice and Bob at all distances considered, and that could have resulted in wrong bounds for the key rate of QS-based systems.

Figure 7 shows the optimized secret key rates of both conventional and the QS-assisted GG02 protocol versus distance in two scenarios: with and without excess noise. In the case of no excess noise, it can be seen that the no-QS curve stays above the QS-assisted system at all distances considered. The slope of the QS-based system is, however, almost half of the no-QS system, especially at short to mid range distances, which resembles a repeater behavior. By introducing a fixed excess noise of 0.002 at the receiver, the QS-based system offers a clear rate advantage over distances greater than 80 km, and can reach a security distance of around 120 km. This is a promising result in the sense that one extend the range of CV QKD systems by nearly 50% using a simple QS module. More importantly, the better rate-versus-distance scaling of the QS-assisted system makes it a potential candidate for CV repeater setups [25].

As can be seen in Fig. 7, QS-equipped receivers may not support high key rates at short distances. There are over two orders of magnitude difference between the no-QS and QS-based curves at $L = 0$. This is attributed to multiple factors. First, the trade-off between the choice of modulation variance and noise level in the system, would require us to use very small values of V_A at short distances, as otherwise, the QS will not operate at its low-noise regime. For instance, at $L = 0$, the optimum value of V_A for the QS-based system is 0.05. A no-

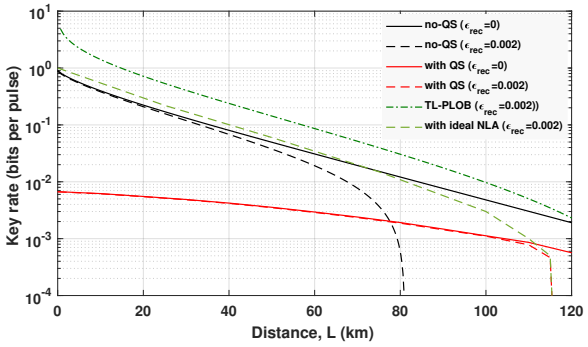

FIG. 7. The optimized secret key rate for the QS-amplified CV QKD protocol versus distance, as compared to the rate of conventional GG02, the upper bound for a thermal-loss channel (TL-PLOB) at a mean thermal photon number of $\varepsilon_{\rm rec}/(2(1-T))$, and the rate obtained by an ideal NLA.

TABLE I. Optimized values for modulation variance and amplification gain at zero excess noise.

Distance (km)	Optimized modulation variance	Optimized gain
0	0.05	1.02
50	0.20	1.36
100	0.45	1.53

QS system with such a low value of V_A also offers a low key rate of 3.52×10^{-2}, which is comparable to what we obtain for the QS-based system. Other factors are the success probability, which at $L=0$ is around 0.5, and it almost linearly goes down to around 0.2 at 120 km. One other factor is also the fact that the QS is not entirely noise free. The additional noise by the QS would bring the rate at $L=0$ to around 0.01 per pulse.

The post-selection mechanism in the QS is the key to obtaining higher key rates at long distances. At long distances, the channel loss naturally prepares low-intensity inputs to the QS, which allows us to use larger values of V_A, as shown in Table I. That would also enable us to use slightly higher gains without necessarily increasing the QS noise. A higher-than unity gain for the post-selected states would then offer a better signal-to-noise ratio at long distances, which allows us to achieve positive secret key rates at longer distances. It is noteworthy that, at $\varepsilon_{\rm rec}=0.002$, the maximum security distance that can be achieved by using an ideal NLA, as in Ref. [15], is almost the same as we have achieved with the QS. This implies that within certain regions the QS module can offer a performance close to ideal NLA devices, which matches our findings in Sec. III. Note that the plots in Ref. [15] are obtained for fixed values of amplification gain and modulation variance $g=4$ and $V_A=3.5$, respectively), where no optimization is performed. The ideal NLA curve in Fig. 7 is, however, gained after optimizing the secret key rate given in Ref. [15].

Figure 7 also shows that our QS-amplified system cannot beat the existing upper bounds for repeaterless systems [32]. Here, we have used the bound given in Eq. (23) of Ref. [32] for a thermal-loss channel as a benchmark (labelled TL-PLOB in Fig. 7). This curve has been obtained at an equivalent mean thermal photon number, $\bar{n}$, to our receiver excess noise. That is, we have used $\bar{n}=\varepsilon_{\rm rec}/(2(1-T))$. As expected, the QS-based system cannot outperform this bound. This again indicates that one would need a CV repeater setup in order to beat such bounds by CV QKD.

VI. CONCLUSIONS AND DISCUSSION

In this work, we studied the performance of the GG02 protocol where the received signal was amplified by a quantum scissor. We first obtained the exact output state and success probability of the QS under study, which was latter used in calculating the secret key generation rate of the system. We showed that the QS would turn a Gaussian input state into a non-Gaussian one. That would make the conventional techniques to estimating the key rate not directly applicable to our case. We instead directly calculated the mutual information by working out the probability distribution function of the quadratures after the QS. Also, in order to upper bound the leaked information to Eve, we obtained the exact covariance matrix of the bipartite state shared between sender and receiver labs. We then found the Holevo information corresponding to a Gaussian channel with the same covariance matrix. We optimized the key rate over input modulation variance and amplification gain. Our results showed that the QS-enhanced key rate can tolerate more excess noise than the no-QS system. This implied that we could reach longer distances, up to 120 km with existing technologies, by using a QS at the receiver module.

There are certain practical aspects that one should consider before using quantum scissors in CV QKD. One assumption that we make throughout our paper is that on-demand single-photon sources are available for our scheme. There are two practical issues, in this regard, that affect the performance of the QS-based system. The first is the rate at which single-photons are generated. The success rate of such sources directly affect the key rate achievable. Secondly, we should be cautious about the purity of the single-photon source output. Multiple-photon components, in particular, could be damaging to the performance of the QS. The good news is that the current available technology for quantum-dot sources has made a substantial progress to meet both above requirements. In particualr, quantum dot sources with efficiencies over 80% and second-order coherence values <0.004 have already been demonstrated [33, 34]. The second issue is the reliance on single-photon detectors, which will make CV QKD systems, in terms of requirements, as pricy as their discrete-variable counterparts. But, paying such prices may be unavoidable if one wants to have long-distance CV QKD and/or CV repeaters. Our study would, in particular, be highly relevant to analyzing the performance of recently proposed CV quantum repeaters [25], which rely on a similar building block. Finally, note that while the original NLA proposal by Ralph and Lund relies on multiple QS modules, in our scheme, we find using one QS optimal as it minimizes the noise while we can adjust

the signal level by optimizing the modulation variance.

ACKNOWLEDGMENTS

The authors acknowledge partial support from the White Rose Research Studentship and the UK EPSRC Grant No. EP/M013472/1. All data generated in this paper can be reproduced by the provided methodology and equations.

Appendix A: Channel loss and excess noise

In order to calculate the exact conditional and marginal entropy functions in Eqs. (20)–(22), the following procedure should be followed:

Channel transmittance (T). The state that reaches the QS is attenuated because of the channel transmittance; hence, in Eqs. (15) and (16): $(x_A, p_A) \to (\sqrt{T}x_A, \sqrt{T}p_A)$.

Channel excess noise (ε). A thermal excess noise that is added at the channel input can be modeled by an independent Gaussian distribution. In the prepare and measure scheme, that implies that the effective modulation variance of the system should change from V_A to $V_A + \varepsilon$. This is because the sum of two independent Gaussian distributions is another Gaussian distribution with a variance equal to the sum of their variances [31]. In the EB scheme, we find the corresponding parameter δ in our EPR state, which gives the same output statistics for the signal that goes to Bob, when Alice does a heterodyne measurement on her state. It then turns out that to get an identical output state we should satisfy $\delta = \sqrt{(V+1)/2}$, where $V = V_A + \varepsilon + 1$.

Note that in our simulation, following the experimental results in Ref. [9], we assume that the noise level, $\varepsilon_{\rm rec}$, is measured at the receiver. We estimate the excess noise at the transmitter side by $\varepsilon = \varepsilon_{\rm rec}/T$.

Appendix B: Covariance matrix

Having obtained the output anti-normally ordered characteristic function of Eq. (26), we use Eq. (3) to find the corresponding output state:

$$\hat{\rho}^{\rm out}_{0123v} = \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\frac{d^2\xi_v}{\pi}\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_v)\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3)\hat{D}_{\rm N}(\hat{b}_v,\xi_v). \quad \text{(B1)}$$

In the following, we show how the shared state between Alice and Bob is found step-by-step. We first trace out mode b_v, see Fig. 5, to obtain

$$\hat{\rho}^{\rm out}_{0123} = \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,0)\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3), \quad \text{(B2)}$$

where we use $\mathrm{Tr}[\hat{D}_{\rm N}(a,\xi)] = \pi\delta^2(\xi)$. Next, by defining the measurement operator $\hat{M} = (I - |0\rangle_{b_1}\langle 0|) \otimes |0\rangle_{b_2}\langle 0|$, modes $\hat{b}_1$ and $\hat{b}_2$ are measured. The post-selected state is

$$\hat{\rho}^{\rm PS}_{03} = \frac{\mathrm{Tr}_{12}[\hat{M}\hat{\rho}^{\rm out}_{0123}]}{\mathrm{Tr}[\hat{M}\hat{\rho}^{\rm out}_{0123}]} =: \frac{\hat{\sigma}^{\rm PS}_{03}}{P^{\rm PS}_{\rm EB}}, \quad \text{(B3)}$$

where

$$\begin{aligned}\hat{\sigma}^{\rm PS}_{03} &= \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\left[\int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,0)\big(\pi\delta^2(\xi_1)-1\big)\right]\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_3,\xi_3)\\ &= \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,\xi_3)\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_3,\xi_3) \quad \text{(B4)}\end{aligned}$$

with the following definition

$$\widetilde{\chi}_{\rm A}(\xi_0,\xi_3) := \int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,0)\big(\pi\delta^2(\xi_1)-1\big), \quad \text{(B5)}$$

and $P_{\rm EB}^{\rm PS}=\overline{P}_{\rm succ}/2$ is the corresponding success probability to measurement $\hat{M}$:

$$P_{\rm EB}^{\rm PS}=\int\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_{\rm A}^{\rm out}(0,\xi_1,\xi_2,0,0)\big(\pi\delta^2(\xi_1)-1\big)=\widetilde{\chi}_{\rm A}(0,0). \tag{B6}$$

Now, we find the CM for $\hat{\rho}_{03}^{\rm PS}$. In doing so, we need to work out the triplet (a,b,c) of the corresponding CM as follows. By definition, assuming that $\hat{x}_0$ is the X quadrature of mode $\hat{a}_0$, we have

$$a=\langle\hat{x}_0^2\rangle_{\hat{\rho}_{03}}=\frac{\langle\hat{x}_0^2\rangle_{\hat{\sigma}_{03}}}{P_{\rm EB}^{\rm PS}}=\frac{{\rm Tr}[\hat{x}_0^2\hat{\sigma}_{03}]}{P_{\rm EB}^{\rm PS}}, \tag{B7}$$

where

$$\begin{aligned}{\rm Tr}[\hat{x}_0^2\hat{\sigma}_{03}]&=\int\frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,\xi_3)\times{\rm Tr}[\hat{x}_0^2\hat{D}_{\rm N}(\hat{a}_0,\xi_0)]\times{\rm Tr}[\hat{D}_{\rm N}(\hat{b}_3,\xi_3)]\\&=\int\frac{d^2\xi_0}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,0)\times{\rm Tr}[\hat{x}_0^2\hat{D}_{\rm N}(\hat{a}_0,\xi_0)].\end{aligned} \tag{B8}$$

Assuming that $\xi_0=x+iy$, one can show that ${\rm Tr}[\hat{x}_0^2\hat{D}_{\rm N}(\hat{a}_0,\xi_0)]=\pi\delta^2(\xi_0)+2\pi y\delta(x)\frac{d}{dy}\delta(y)-\pi\delta(x)\frac{d^2}{dy^2}\delta(y)$; thus,

$${\rm Tr}[\hat{x}_0^2\hat{\sigma}_{03}]=-\widetilde{\chi}_{\rm A}(0,0)-\frac{d^2}{dy^2}\widetilde{\chi}_{\rm A}(0,y,\xi_3=0)\Big|_{y=0}, \tag{B9}$$

where we use the identity $\int dz f(z)\frac{d}{dz}\delta(z)=-\int dz\frac{d}{dz}f(z)\delta(z)$. Therefore,

$$a=-1-\frac{\frac{d^2}{dy^2}\widetilde{\chi}_{\rm A}(0,y,\xi_3=0)\Big|_{y=0}}{\widetilde{\chi}_{\rm A}(0,0)}. \tag{B10}$$

In a similar way, assuming $\xi_0=x+iy$ and $\xi_3=u+iv$, we show that

$$b=\frac{{\rm Tr}[\hat{x}_3^2\hat{\sigma}_{03}]}{\widetilde{\chi}_{\rm A}(0,0)}=-1-\frac{\frac{d^2}{dv^2}\widetilde{\chi}_{\rm A}(\xi_0=0,0,v)\Big|_{v=0}}{\widetilde{\chi}_{\rm A}(0,0)} \tag{B11}$$

and

$$c=\frac{{\rm Tr}[\hat{x}_0\hat{x}_3\hat{\sigma}_{03}]}{\widetilde{\chi}_{\rm A}(0,0)}=\frac{\frac{d}{dv}\Big[\frac{d}{dy}\widetilde{\chi}_{\rm A}(0,y,0,v)\Big|_{y=0}\Big]\Big|_{v=0}}{\widetilde{\chi}_{\rm A}(0,0)}. \tag{B12}$$

Having the integrals in Eq. (B5) taken, we are able to calculate the triplet (a,b,c), thus the CM. Using MAPLE, we obtain the closed form expressions as summarized in Eq. (28).

Having the triplet (a,b,c), $\chi_{\rm BE}^{\star}$ is upper bounded by:

$$\chi_{\rm BE}^{\rm G}=g(\Lambda_1)+g(\Lambda_2)-g(\Lambda_3), \tag{B13}$$

where

$$g(x)=(\frac{x+1}{2})\log_2(\frac{x+1}{2})-\frac{x-1}{2}\log_2\frac{x-1}{2}$$

and

$$\Lambda_{1/2}=\sqrt{\frac{1}{2}\big(A\pm\sqrt{A^2-4B^2}\big)}=\frac{\sqrt{(a+b)^2-4c^2}\pm(b-a)}{2},\quad\Lambda_3=\sqrt{\frac{aB}{b}}=\sqrt{\frac{a(ab-c^2)}{b}},$$

with $A=a^2+b^2-2c^2$ and $B=ab-c^2$. Note that Eq. (B13) is valid when we neglect the electronic noise at the receiver as we have assumed in our numerical results. Also, mutual information can be calculated form the covariance matrix, if we wish to use the Gaussian approximation, by

$$I_{\rm AB}^{\rm G}=\frac{1}{2}\log_2\frac{ab}{ab-c^2}. \tag{B14}$$

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, Bangalore, India, 1984) pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[7] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[9] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[10] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[11] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).
[12] H. Yonezawa, S. L. Braunstein, and A. Furusawa, Phys. Rev. Lett. **99**, 110503 (2007).
[13] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. ichi Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photon. **7**, 982 (2013).
[14] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[15] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).
[16] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, J. Phys. B: At. Mol. Opt. Phys. **47**, 035501 (2014).
[17] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves, Phys. Rev. A **88**, 033852 (2013).
[18] T. C. Ralph and A. P. Lund, AIP Conference Proceedings **1110**, 155 (2009).
[19] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, Phys. Rev. Lett. **111**, 213601 (2013).
[20] J. Fiurášek, Phys. Rev. A **80**, 053822 (2009).
[21] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2009).
[22] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).
[23] R. J. Donaldson, R. J. Collins, E. Eleftheriadou, S. M. Barnett, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **114**, 120505 (2015).
[24] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, Laser Phys. Lett. **8**, 411 (2011).
[25] J. Dias and T. C. Ralph, Phys. Rev. A **95**, 022312 (2017).
[26] F. Furrer and W. J. Munro, arXiv:1611.02795.
[27] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[28] R. Kumar, H. Qin, and R. Allaume, New J. of Phys. **17**, 043027 (2015).
[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[30] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[31] T. M. Cover and J. A. Thomas, *Elements of Information Theory-Second Edition* (John Wiley and Sons, New Jersey, 2006).
[32] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[33] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, Nat. Photon. **8**, 224 (2014).
[34] A. J. Shields, Nat. Photon. **1**, 215 (2007).