

Long-distance continuous-variable quantum key distribution with feasible physical noiseless linear amplifiers

Michele N. Notarnicola^{1,2} and Stefano Olivares^{1,2,*}

¹*Dipartimento di Fisica “Aldo Pontremoli”, Università degli Studi di Milano, I-20133 Milano, Italy*

²*INFN, Sezione di Milano, I-20133 Milano, Italy*

(Dated: May 19, 2023)

Noiseless linear amplifiers (NLAs) provide a powerful tool to achieve long-distance continuous-variable quantum key distribution (CV-QKD) in the presence of realistic setups with non unit reconciliation efficiency. We address a NLA-assisted CV-QKD protocol implemented via realistic physical NLAs, namely, quantum scissors (QS) and single-photon catalysis (SPC), and compare their performance with respect to the ideal NLA $g^{\hat{n}}$. We investigate also the robustness of two schemes against inefficient conditional detection, and discuss the two alternative scenarios in which the gain associated with the NLA is either fixed or optimized.

I. INTRODUCTION

Quantum key distribution (QKD) [1] allows to share a common secure key between a sender and a receiver even in the presence of an untrusted channel that could be under the control of an eavesdropper. Within this framework, a promising role is played by continuous-variable QKD (CV-QKD) for both theoretical and experimental reasons [2]. In the first proposal of a CV-QKD scheme by Grosshans and Grangier (GG02) [3–7] information is encoded by the sender (Alice) on the quadratures of a quantized optical field with Gaussian modulation and then sent into a channel to the receiver (Bob) that performs either homodyne or heterodyne (double-homodyne) measurements. The key is then extracted after a reconciliation process, where one of the two parties publicly reveals part of the data: if such party is Alice the process is referred to as direct reconciliation, if the party is Bob we have reverse reconciliation. The security analysis of the reverse-reconciliation protocol guarantees a non null secure key rate for any transmission distance [3, 4, 7, 8].

In realistic conditions, however, the reconciliation procedure is not perfect and one can introduce a reconciliation efficiency, which depends on the particular code employed to extract the secure key [9]. Moreover, the presence of defects inside Alice’s Gaussian modulator as well as phase noise of the carrier signal introduce an excess noise [10]. Both these limitations crucially affect the key generation rate (KGR), i.e. the length of the secret key shared by Alice and Bob per unit time, and prevent long-distance communication leading to a maximum transmission distance at which the KGR vanishes [10, 11].

A challenging task to face those issues is to modify the original protocol by implementing strategies allowing to increase as much as possible the maximum transmission distance. An intriguing solution is provided by heralded noiseless linear amplification at the receiver’s side [12, 13]. Indeed, an ideal probabilistic noiseless linear amplifier (NLA) with amplitude gain g leads to an increase in the maximum transmission distance proportional to $\log g$ [14]. Nevertheless, any realistic

physical NLA can only approximate the ideal amplifier for low-amplitude optical signals [12, 15–23]. To avoid this limitation, measurement-based NLAs, performing virtual amplification based on classical data post-selection, have also been proposed [24–26]. However, the low success probabilities of these operations [27, 28] make physical NLAs still worth of investigation. Recently, CV-QKD employing quantum scissors (QS) [12] has been addressed, allowing to achieve long-distance CV-QKD for sufficiently low channel excess noise [29, 30]. To the same goal, also single-photon catalysis (SPC) has been investigated [18, 31]. In the QS scheme, a single photon is mixed with the vacuum at a beam splitter with transmissivity τ . One of the output branches then impinges at a balanced beam splitter with the incoming signal, after which double conditional photo-detection is performed. Differently from QS, in the SPC process a single photon interferes directly with the incoming signal at a beam splitter with transmissivity τ and then a single photon is retrieved at the end. Thus, SPC provides a simpler scheme and may represent a feasible alternative to QS for experimental realizations.

In the following paper we investigate a CV-QKD protocol assisted by these two schemes and consider a simplified realistic scenario, where photo-detection is replaced by on-off detection. We compute the KGRs for both the strategies and compare them to the performance of the protocol assisted by the ideal NLA proposed in [14]. Moreover, we distinguish two alternative cases. In the former, we fix the NLA gain g and show that also physical NLAs increase the maximum transmission distance by the same amount $\log g$ as the ideal amplifier. In the latter, we assume g to be a free parameter and optimize its value, obtaining that both physical and ideal NLAs achieve arbitrary long-distance CV-QKD. For the physical amplifiers, we also discuss the robustness in the presence of a quantum detection efficiency $\eta \leq 1$, showing that the detection efficiency only rescales the KGR without preventing long-distance communication.

The structure of the paper is the following. In Sec. II we recall the main features of the GG02 protocol. Then, in Sec. III we describe the NLA-assisted protocols for both the ideal and the physical amplifiers, namely, QS and SPC. In Sec. IV we perform the security analysis by comparing the KGRs of the protocols under investigation. Finally, in Sec. V we summarize the results obtained and draw some conclusions.

* stefano.olivares@fisica.unimi.it

II. THE GG02 ORIGINAL PROTOCOL

We start reviewing the CV-QKD protocol proposed in [3–6] in its entanglement-based (EB) version, which provides a simplified theoretical analysis [32, 33]. In the EB protocol, Alice and Bob share a two-mode squeezed vacuum (TMSV) state with variance $V > 1$, namely $|\text{TMSV}\rangle = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle|n\rangle$ with $\lambda = \sqrt{(V-1)/(V+1)}$ [34]. The TMSV is a two-mode Gaussian state [34, 35], completely described by the covariance matrix (CM) (see Appendices A and B for details)

$$\Gamma_{\text{TMSV}} = \begin{pmatrix} V \mathbb{1}_2 & Z \sigma_z \\ Z \sigma_z & V \mathbb{1}_2 \end{pmatrix}, \quad (1)$$

where $Z = \sqrt{V^2 - 1}$, $\mathbb{1}_2 = \text{Diag}(1, 1)$ and σ_z is the Pauli z -matrix. All quantities are expressed in shot noise units.

Now, Alice performs a heterodyne (i.e. double-homodyne) measurement on her beam, while the other one is sent to Bob through an untrusted communication channel, described by means of a thermal-loss channel. The channel has a transmissivity $T = 10^{-\kappa d/10}$, where d is the transmission distance in km and $\kappa \sim 0.2 \text{ dB/km}$ is the typical loss parameter for optical fibers at 1550 nm [36–38]. Moreover, a single-mode thermal bath of $n_\varepsilon = T\varepsilon/2(1-T)$ photons models the presence of an excess noise ε introduced by the realistic defects of Alice's modulation system [10]. Losses and imperfections affect the signal received by Bob that exhibits an added noise $\chi = (1-T)/T + \varepsilon$, leading to an overall thermal-loss channel. Therefore, the state shared between Alice and Bob is still Gaussian with CM [34, 35]:

$$\Gamma_{AB} = \begin{pmatrix} \Gamma_A & \Gamma_Z \\ \Gamma_Z^\top & \Gamma_B \end{pmatrix} = \begin{pmatrix} V \mathbb{1}_2 & \sqrt{T} Z \sigma_z \\ \sqrt{T} Z \sigma_z & T(V + \chi) \mathbb{1}_2 \end{pmatrix}. \quad (2)$$

Once received the signal, Bob implements a Gaussian measurement [32, 33] that here we assume to be homodyne detection of a quadrature randomly chosen between q and p , as in the original proposal [3, 4].

All the necessary information to perform the security analysis is contained in the CM (2). According to the Gaussian formalism [35, 39] when Alice and Bob perform detection on their own signals they get a bi-variate Gaussian distribution $p_{A(B)}(x_{A(B)}, y_{A(B)})$ with zero mean and covariance $\Gamma_{A(B)} + \sigma_{A(B)}^{(m)}$, where $\sigma_A^{(m)} = \mathbb{1}_2$ is the CM of the heterodyne detection and

$$\sigma_B^{(m)} = \lim_{z \rightarrow 0} \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \quad (3)$$

is the 2×2 CM associated with homodyne detection still in shot noise units (see Appendix B). Therefore, the joint measurement leads to the distribution $p_{AB}(x_A, y_A; x_B, y_B)$ with covariance $\Gamma_{AB} + (\sigma_A^{(m)} \oplus \sigma_B^{(m)})$. The mutual information between Alice and Bob is then given by:

$$\begin{aligned} I_{AB} &= H[p_A] + H[p_B] - H[p_{AB}] \\ &= \log_2 \left\{ \sqrt{\frac{\det[\Gamma_A + \sigma_A^{(m)}] \det[\Gamma_B + \sigma_B^{(m)}]}{\det[\Gamma_{AB} + (\sigma_A^{(m)} \oplus \sigma_B^{(m)})]}} \right\}, \quad (4) \end{aligned}$$

$H[p] = -\int dx p(x) \log_2 p(x)$ being the Shannon entropy of $p(x)$.

Throughout this paper we will focus on a reverse reconciliation scheme, which has been proved to guarantee higher security than direct reconciliation [7, 8]. Furthermore, we will assume an eavesdropper (Eve) to be able to perform collective attacks, which represent the best possible kind of attacks in his power, at least in the asymptotic limit of an infinite dataset [7]. If the reconciliation efficiency is $0 \leq \beta \leq 1$, the KGR writes

$$K = \beta I_{AB} - \chi_{BE}, \quad (5)$$

where the Holevo information χ_{BE} represents the amount of information extracted by Eve [40] and can be computed starting from the CM (2) as:

$$\chi_{BE} = G\left(\frac{d_1 - 1}{2}\right) + G\left(\frac{d_2 - 1}{2}\right) - G\left(\frac{d_3 - 1}{2}\right), \quad (6)$$

where

$$G(x) = (x+1) \log_2(x+1) - x \log_2 x, \quad (7)$$

and $d_{1(2)}$ are the symplectic eigenvalues of Γ_{AB} [35, 39], namely

$$d_{1(2)} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4I_4}}{2}}, \quad (8)$$

with $I_{1(2)} = \det(\Gamma_{A(B)})$, $I_3 = \det(\Gamma_Z)$, $I_4 = \det(\Gamma_{AB})$ and $\Delta = I_1 + I_2 + 2I_3$. Finally, $d_3 = \sqrt{\det(\Gamma_{A|B})}$ with (see Appendix B):

$$\Gamma_{A|B} = \Gamma_A - \Gamma_Z \left[\Gamma_B + \sigma_B^{(m)} \right]^{-1} \Gamma_Z^\top. \quad (9)$$

In the following we will study the behavior of K as a function of the transmission distance d , optimizing over the modulation variance V for fixed reconciliation efficiency $\beta \sim 0.95$ [9, 41, 42] and the channel excess noise ε .

For the sake of clarity, we will review the results for the original protocol in the next section together with the NLA-assisted strategies under investigation.

III. NLA-ASSISTED CV-QKD

In this section we investigate the performance of the CV-QKD protocol presented in Sec. II assisted by a NLA. That is, Alice prepares the TMSV state with variance V and injects one mode into the thermal-loss channel. To mitigate the added noise χ , Bob implements a NLA on his received pulse, before performing homodyne detection.

Here we consider Bob to employ either the ideal NLA proposed in [14], or feasible physical NLAs realized via QS or SPC.

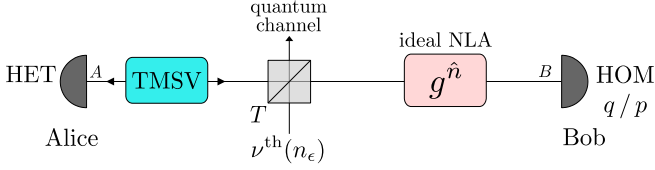


Figure 1. Scheme of the CV-QKD protocol assisted by the ideal NLA proposed in [14].

A. Ideal NLA

At first, we assume Bob to employ an ideal NLA, as depicted in Fig. 1. The ideal NLA is a non-deterministic operation described by the self-adjoint operator $g^{\hat{n}}$, \hat{n} being the photon-number operator of the optical mode undergoing amplification, and $g \geq 1$ is the amplifier gain [12]. As discussed in [14], this operation preserves Gaussianity, therefore the protocol in Fig. 1 is equivalent to a GG02 scheme with the following parameters:

$$V_{\text{id}} = V + \frac{T(g^2 - 1)Z^2}{2 - T(g^2 - 1)(V - 1 + \varepsilon)}, \quad (10a)$$

$$T_{\text{id}} = \frac{g^2 T}{1 + T(g^2 - 1)[T\varepsilon(g^2 - 1)(\varepsilon - 2)/4 - \varepsilon + 1]}, \quad (10b)$$

$$\varepsilon_{\text{id}} = \varepsilon - \frac{T\varepsilon}{2}(g^2 - 1)(\varepsilon - 2). \quad (10c)$$

Remarkably, employing the ideal NLA is equivalent to considering an effective channel of increased transmissivity $T_{\text{id}} \geq T$. Moreover, the physical request $V_{\text{id}} \geq V$ imposes a constraint on the gain, namely,

$$g \leq \sqrt{1 + \frac{2}{T(V + \varepsilon - 1)}}. \quad (11)$$

The resulting KGR then reads:

$$K_{\text{id}}(V, g) = P_{\text{id}}(V, g) \left[\beta I_{AB}^{(\text{id})}(V, g) - \chi_{BE}^{(\text{id})}(V, g) \right], \quad (12)$$

where $I_{AB}^{(\text{id})}(V, g)$ and $\chi_{BE}^{(\text{id})}(V, g)$ are computed from Eq.s (4) and (6), respectively, with the modified parameters (10). Instead, $P_{\text{id}}(V, g)$ is the success probability of the NLA, such that $P_{\text{id}}(V, g) \leq 1/g^2$ [14]. From now on, as a benchmark we will make the most optimistic choice $P_{\text{id}}(V, g) = 1/g^2$.

The KGR (12) depends on the two free parameters V and g that can be optimized. As discussed in the rest of the paper, the choice of the gain g will be a crucial task. Hence, we will discuss two separate cases. In the former case we assume a fixed g and optimize only the modulation variance, obtaining the KGR

$$K_{\text{id}}(g) = \max_V K_{\text{id}}(V, g), \quad (13)$$

and the corresponding distance-dependent modulation $V_{\text{opt}}^{(\text{id})}(g)$. In the latter case the optimization involves also the

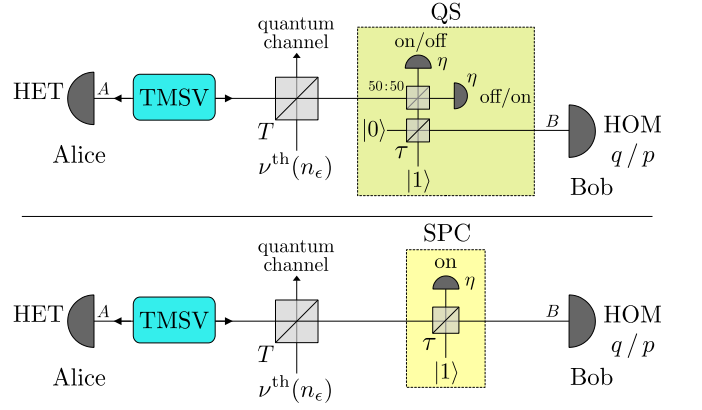


Figure 2. Scheme of the CV-QKD protocol assisted by the two physical NLAs discussed in the paper. (Top) Strategy based on quantum scissors (QS); (bottom) strategy based on single-photon catalysis (SPC).

gain, obtaining

$$K_{\text{id}} = \max_{V, g} K_{\text{id}}(V, g), \quad (14)$$

and the associated parameters $V_{\text{opt}}^{(\text{id})}$ and $g_{\text{opt}}^{(\text{id})}$.

B. Physical NLAs: QS and SPC

Here we consider the more realistic scenario in which Bob employs a physical NLA, realized via either QS or SPC and employing on-off detection rather than photon counting.

In the QS scheme proposed in [29] (Fig. 2, top panel), Bob prepares two ancillary modes in the Fock states $|1\rangle$ and $|0\rangle$, respectively. He mixes them at a beam splitter with transmissivity τ and lets the reflected signal interfere at a balanced beam splitter with the pulse received by Alice. Then, he performs conditional on-off detection on both the output branches (see Appendix C for details), corresponding to the positive-operator-valued measurement (POVM) $\{\Pi_{\text{off}}, \Pi_{\text{on}} = \mathbb{1} - \Pi_{\text{off}}\}$, where

$$\Pi_{\text{off}} = \sum_{k=0}^{\infty} (1 - \eta)^k |k\rangle\langle k|, \quad (15)$$

and $\eta \leq 1$ is the detection quantum efficiency. If one of the two detectors gives the outcome “on”, Bob performs homodyne detection on the post-selected output state. The value of τ fixes the gain associated with the NLA, that for low-amplitude coherent signals reads $g = \sqrt{(1 - \tau)/\tau}$ [12]. Thus, to achieve the gain g we set the transmissivity equal to

$$\tau_{\text{QS}}(g) = \frac{1}{1 + g^2}. \quad (16)$$

On the contrary, in the SPC scheme (Fig. 2, bottom panel), Bob has a single ancillary mode excited in $|1\rangle$ impinging at a beam splitter with transmissivity τ with the pulse received by Alice. He performs on-off detection on the reflected

branch, conditioning on outcome “on”, and homodynes the post-selected state. The associated gain is $g = (1 - 2\tau)/\sqrt{\tau}$ [18], which can be inverted to find the transmissivity as a function of the gain

$$\tau_{\text{SPC}}(g) = \frac{1}{8} \left(4 + g^2 - g\sqrt{8 + g^2} \right). \quad (17)$$

In both the cases, after the NLA Alice and Bob share a non-Gaussian state $\rho_{AB}^{(p)}$, $p = \text{QS, SPC}$. However, since Bob’s measurement is Gaussian, the security analysis of the NLA-assisted protocol can be based on the optimality of Gaussian attacks [43–45], which, in this scenario, maximize the amount of information extractable by Eve. Moreover, following Ref. [43], we consider the Gaussian lower bound on the mutual information, that is a consequence of the Gaussian (heterodyne) detection at Alice’s side. In turn, we can compute a *lower bound* of the exact KGR as:

$$K_p(V, g) = P_p(V, g) \left[\beta I_{AB}^{(p)}(V, g) - \chi_{BE}^{(p)}(V, g) \right], \quad (18)$$

where $P_p(V, g)$ is the success probability associated with the p -th NLA and $I_{AB}^{(p)}(V, g)$ and $\chi_{BE}^{(p)}(V, g)$ are the mutual information and the Holevo information, respectively, both computed for a Gaussian state having the same CM of $\rho_{AB}^{(p)}$. The condition $K_p(V, g) \geq 0$ provides a sufficient condition to guarantee secure communication. Nevertheless, our results are in good agreement with other exact numerical approaches [29], proving the bound (18) to be tight, especially in the long-distance regime $\kappa d \gg 1$.

Thus, in our approach it suffices to compute the CM $\Gamma_{AB}^{(p)}$ associated with $\rho_{AB}^{(p)}$ to perform the security analysis. Straightforward calculations lead to (see Appendix C)

$$\Gamma_{AB}^{(p)} = \begin{pmatrix} V_p(V, g) \mathbb{1}_2 & Z_p(V, g) \sigma_z \\ Z_p(V, g) \sigma_z & W_p(V, g) \mathbb{1}_2 \end{pmatrix}. \quad (19)$$

The expressions of $P_p(V, g)$, $V_p(V, g)$, $W_p(V, g)$ and $Z_p(V, g)$ are clumsy and thus only reported in Appendix C. We compute the mutual information and the Holevo information following the procedure described in Sec. II by substituting $\Gamma_{AB} \rightarrow \Gamma_{AB}^{(p)}$ and optimize Eq. (18) over the free parameters, obtaining the KGRs

$$K_p(g) = \max_V K_p(V, g), \quad (p = \text{QS, SPC}), \quad (20)$$

for a fixed g , together with the corresponding modulation $V_{\text{opt}}^{(p)}(g)$, and

$$K_p = \max_{V, g} K_p(V, g), \quad (p = \text{QS, SPC}), \quad (21)$$

if g can be optimized too, with the associated optimized parameters $V_{\text{opt}}^{(p)}$ and $g_{\text{opt}}^{(p)}$.

We note that in the SPC scheme there always exists a local maximum for $\tau = 1$, in which case the SPC performs as the identity operator, allowing to retrieve the results of the original

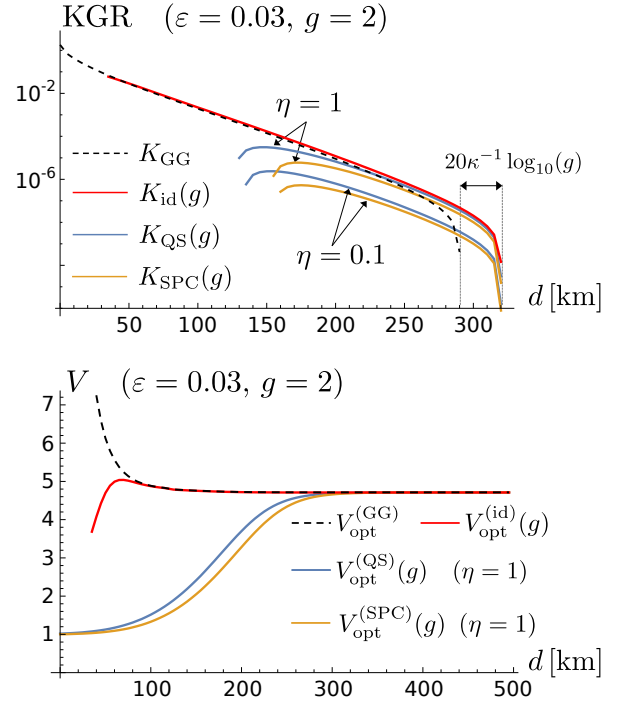


Figure 3. (Top) Log plot of the KGRs $K_p(g)$ and $K_{\text{id}}(g)$ as a function of the distance d , expressed in km. The dashed line is the KGR of the original protocol. (Bottom) Plot of the optimized modulations $V_{\text{opt}}^{(p)}(g)$ and $K_{\text{opt}}^{(\text{id})}(g)$ as a function of the distance d , expressed in km. In both the pictures we set $\beta = 0.95$, $\epsilon = 0.03$, $g = 2$ and $\eta = 1$.

protocol. However, for a more fair comparison with the QS, in the optimization procedure we have neglected this point and restricted maximization over the interval $0 \leq \tau \leq 1/2$ for which the corresponding gain is $g \geq 0$, as shown in Appendix C.

IV. SECURITY ANALYSIS

In this section we compare the KGRs of all the schemes under investigation, for the two cases of fixed or optimized gain.

A. KGR with fixed gain g

For a fixed g , the optimized KGRs are depicted in Fig. 3 (top panel) for $\epsilon > 0$. As emerges from the plot, both the ideal and physical NLAs are useless at small distances d . Indeed, the ideal amplifier prevents short-distance communication since condition (11) is violated for high transmissivity $T \lesssim 1$. Instead, for the physical NLAs $p = \text{QS, SPC}$ we have $K_p < 0$ up to a threshold distance. On the contrary, NLAs are fundamental in the long-distance regime, as for large d all the NLA-assisted protocols beat the KGR (5) of the original protocol. The ideal NLA increases the maximum transmission distance by the amount $(20 \log_{10} g)/\kappa$, since for $T \ll 1$ the

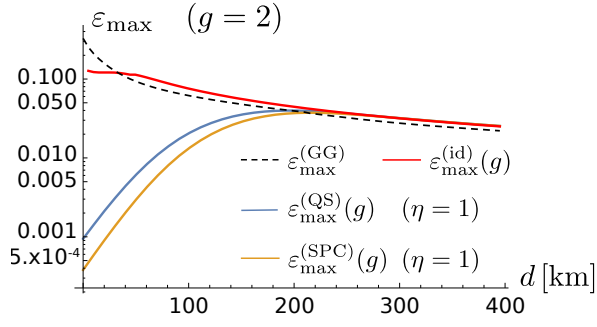


Figure 4. Log plot of the maximum tolerable excess noise $\varepsilon_{\max}^{(\text{id})}(g)$ and $\varepsilon_{\max}^{(p)}(g)$, $p = \text{QS, SPC}$, as a function of the distance d , expressed in km. The black dashed line corresponds to the ε_{\max} of the original protocol. We set $\beta = 0.95$ and $\eta = 1$.

effective transmissivity in Eq. (10) is $\approx g^2 T$ [14]. Remarkably, also the physical NLA-assisted protocols achieve the same maximum transmission distance. Moreover, the presence of inefficient conditional detection reduces the value of the KGRs, still maintaining the same increase in distance even if $\eta = 0.1$.

In fact, by expanding the CM (19) in the long-distance regime where $T \ll 1$ up to the first order in T , we have:

$$V_p(V, g) = V + O(T), \quad (22a)$$

$$W_p(V, g) = g^2 T (V + \chi) + O(T^2), \quad (22b)$$

$$Z_p(V, g) = \sqrt{g^2 T} Z + O(T^{3/2}), \quad (p = \text{QS, SPC}), \quad (22c)$$

corresponding to the CM of a GG02 scheme with transmissivity $g^2 T$, consistently with the ideal case. Moreover, the success probabilities read

$$P_p(V, g) \approx P_p(g) = \eta \tau_p(g), \quad (23)$$

and, being $P_{\text{SPC}}(g) \leq P_{\text{QS}}(g)$, we have $K_{\text{SPC}}(g) \leq K_{\text{QS}}(g)$. In turn, a quantum efficiency $\eta \leq 1$ only reduces the success probability and rescales the KGR, without preventing long-distance secure communication. On the contrary, in the short-distance regime where $T \approx 1$ or, equivalently, $\kappa d \ll 1$, the CM (19) does not get the form of Eq. (2) and the KGR turns out to be negative, inhibiting secure communication.

For completeness, we report the optimized modulations in the bottom panel of Fig. 3. Despite the different behaviour at small distances, for large d all the protocols converge to the same asymptotic value, not depending on ε . Numerical calculations have also shown that $V_{\text{opt}}^{(p)}(g)$ does not depend on the quantum efficiency.

Finally, in Fig. 4 we plot the maximum tolerable excess noise (MTEN) ε_{\max} as a function of the distance d : it represents the maximum value of ε still leading to a positive KGR. For the original protocol, ε_{\max} is a decreasing function of d . The behaviour is rather different for the NLA-assisted protocols. In the presence of ideal NLA the MTEN $\varepsilon_{\max}^{(\text{id})}(g)$ for $d \lesssim 40$ km is lower than the original protocol due to the limitation imposed by (11). However, for larger distances we

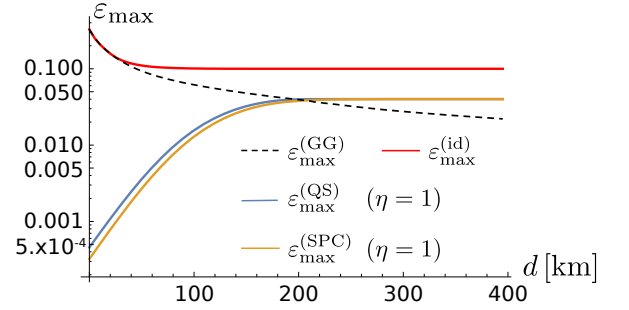
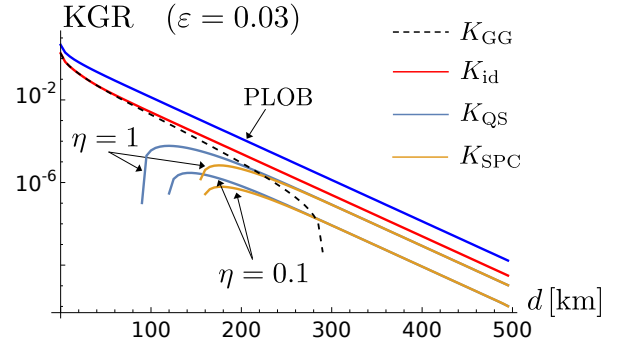


Figure 5. (Top) Log plot of the KGRs K_p , $p = \text{QS, SPC}$, and K_{id} as a function of the distance d , expressed in km, for different values of the quantum efficiency and $\varepsilon = 0.03$. The dashed line is the KGR of the original protocol and the blue line is the PLOB bound (24). (Bottom) Log plot of the maximum tolerable excess noises $\varepsilon_{\max}^{(\text{id})}$ and $\varepsilon_{\max}^{(p)}$, $p = \text{QS, SPC}$, as a function of the distance d , expressed in km, for $\eta = 1$. The black dashed line corresponds to the ε_{\max} of the original protocol. In both the pictures we set $\beta = 0.95$.

have $\varepsilon_{\max}^{(\text{id})}(g) > \varepsilon_{\max}$. On the contrary, the MTEN associated with the physical NLAs, namely $\varepsilon_{\max}^{(p)}(g)$, is not a monotonous function of d : it is an increasing function of d approaching $\varepsilon_{\max}^{(\text{id})}$. A quantum efficiency $\eta \leq 1$ does not affect the value of $\varepsilon_{\max}^{(p)}$, consistently with the previous discussions. As a consequence, for fixed g , in the long-distance regime the physical NLAs guarantee the same performance of the ideal NLA.

B. KGR with optimized gain g

The situation is rather different if we can also optimize the gain g associated with the NLAs, as reported in Fig. 5 (top panel). All the NLA-assisted protocols allow to reach arbitrary large distances, but the ideal amplifier outperforms the physical ones. As before, a quantum efficiency still rescales the KGR. However, differently from Sec. IV A, in the long distance regime $\kappa d \gg 1$, K_{QS} and K_{SPC} are almost identical, proving SPC as a feasible alternative to QS.

We also remark that in the long-distance regime both K_{id} and K_p , $p = \text{QS, SPC}$, are proportional to the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [46]

$$K_{\max} = -\log_2 [(1-T)T^{n\varepsilon}] - G(n\varepsilon), \quad (24)$$

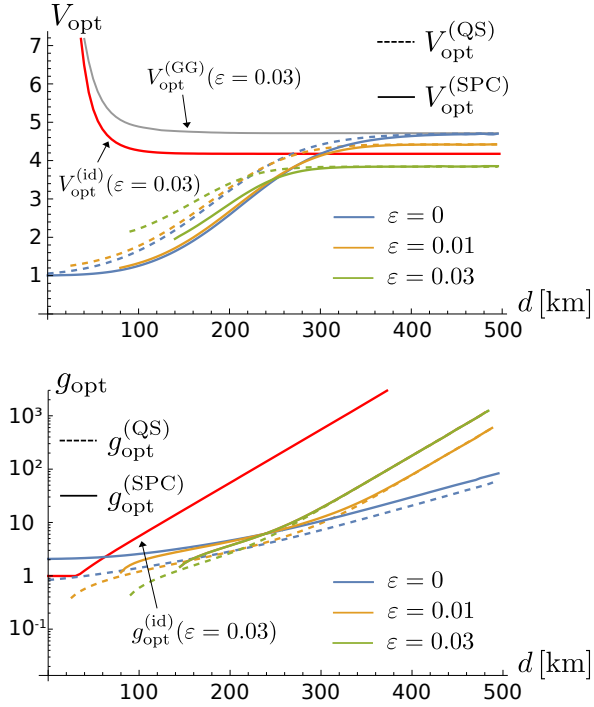


Figure 6. Plot of $V_{\text{opt}}^{(p)}$ (top) and \log plot of $g_{\text{opt}}^{(p)}$ (bottom), $p = \text{QS, SPC}$, as a function of the distance d , expressed in km, for different values of excess noise ϵ . The gray and red line represent the optimized modulation for the original and the ideal NLA-assisted protocols, respectively, for $\epsilon = 0.03$. The plots have been performed only for the distances such that $K_p > 0$, $p = \text{QS, SPC}$. We set $\beta = 0.95$ and $\eta = 1$.

which represents the maximum KGR achievable with the considered repeaterless thermal-loss channel, thus resulting in nearly optimal strategies.

Furthermore, in Fig. 6 we report the optimized parameters $V_{\text{opt}}^{(p)}$ and $g_{\text{opt}}^{(p)}$. The modulation $V_{\text{opt}}^{(p)}$ has a different behavior with respect to Sec. IV A, being an ϵ -dependent growing function of d . On the contrary, the modulations of the original and the ideal NLA-assisted protocols are decreasing functions of d converging to an asymptotic value not depending on ϵ , as for the case of fixed g . Instead, the optimized gains $g_{\text{opt}}^{(\text{id})}$ and $g_{\text{opt}}^{(p)}$ grow exponentially with d in the long-distance regime. However, if $\epsilon = 0$ this exponential scaling is not reached yet for the physical NLAs within the considered range of distances $d \leq 500$ km.

Finally, in the bottom panel of Fig. 5 we plot the MTENs as a function of d . Differently from Sec. IV A, the MTEN associated with the physical NLAs, namely $\epsilon_{\text{max}}^{(p)}$, do not achieve the performance of the ideal one, $\epsilon_{\text{max}}^{(\text{id})}$. Actually, both these MTENs outperform the original protocol and saturate to a value ϵ_{∞} as $\kappa d \gg 1$. However, the saturation value of the physical NLAs, namely $\epsilon_{\infty}^{(p)} \approx 0.04$, is lower than the ideal NLA one, that is $\epsilon_{\infty}^{(\text{id})} \approx 0.1$ (see Fig. 5). The numerical results also show that a quantum efficiency $\eta \leq 1$ does not affect the value of $\epsilon_{\infty}^{(p)}$, consistently with the previous findings.

The difference between ideal and physical NLAs emerges by expanding the CM (19) in the long-distance regime $T \ll 1$ up to the first order, keeping all the contributions of $O(g^2 T)$, due to the fact that $g_{\text{opt}}^{(p)} \gg 1$, and neglecting the other terms:

$$V_p(V, g) \approx V + \delta V_p, \quad (25a)$$

$$W_p(V, g) \approx T_p [V_p(V, g) + \chi_p], \quad (25b)$$

$$Z_p(V, g) \approx \frac{T_p}{\sqrt{g^2 T}} Z, \quad (p = \text{QS, SPC}), \quad (25c)$$

where $\delta V_p = T_p Z^2 / 2$. T_p represents the effective transmissivity

$$T_p = \frac{g^2 T}{1 + g^2 T (V + \epsilon - 1) / 2}, \quad (26)$$

while $\chi_p = (1 - T_p) / T_p + \epsilon_p$, with the effective excess noise

$$\epsilon_p = \epsilon - \delta V_p. \quad (27)$$

Employing a physical NLA is then equivalent to considering an effective channel of higher transmissivity $T_p \geq T$ and lower excess noise $\epsilon_p \leq \epsilon$. Nevertheless, the correspondence with a GG02 protocol does not occur anymore, as the correlation term $Z_p(V, g)$ does not coincide with the one expected for a GG02 scheme, namely,

$$Z_p^{(\text{GG})}(V, g) = \sqrt{T_p [V_p(V, g)^2 - 1]}, \quad (28)$$

but rather

$$Z_p(V, g) \leq Z_p^{(\text{GG})}(V, g), \quad (29)$$

as depicted in Fig. 7 (top panel). We have $Z_p(V, g) \approx Z_p^{(\text{GG})}(V, g)$ only if $g^2 T \ll 1$. As a consequence, the analogy with the ideal-NLA assisted protocol in Eq. (10) is broken.

Now, the optimization procedure described above leads to exponential gains $g_{\text{opt}}^{(\text{id})}$ and $g_{\text{opt}}^{(p)}$ for the ideal and physical NLAs, respectively, such that the product $g^2 T$ is kept constant for $\kappa d \gg 1$. Consequently, the effective transmissivities T_{id} and T_p saturate, as shown in the bottom panel Fig. 7. In turn, also the mutual information and the Holevo information saturate and the corresponding KGRs (14) and (21) turn out to be proportional only to the success probability of the NLAs:

$$K_{\text{id}} \propto P_{\text{id}} = \frac{T}{(g_{\text{opt}}^{(\text{id})})^2 T}, \quad (30)$$

with $P_{\text{id}} = P_{\text{id}}(V_{\text{opt}}^{(\text{id})}, g_{\text{opt}}^{(\text{id})})$, and

$$K_p \propto P_p \approx \frac{\eta T}{2 T_p} \left[1 + T_p (V_p + \chi_p) \right], \quad (31)$$

with $P_p = P_p(V_{\text{opt}}^{(p)}, g_{\text{opt}}^{(p)})$ and $V_p = V_p(V_{\text{opt}}^{(p)}, g_{\text{opt}}^{(p)})$, decreasing linearly with T and thus guaranteeing $K_p > 0$ for $\kappa d \gg 1$. The same linear scaling is achieved by the PLOB bound if $T \ll 1$:

$$K_{\text{max}} \approx T \frac{2 - \epsilon [1 - \ln(\epsilon/2)]}{2 \ln 2}, \quad (32)$$

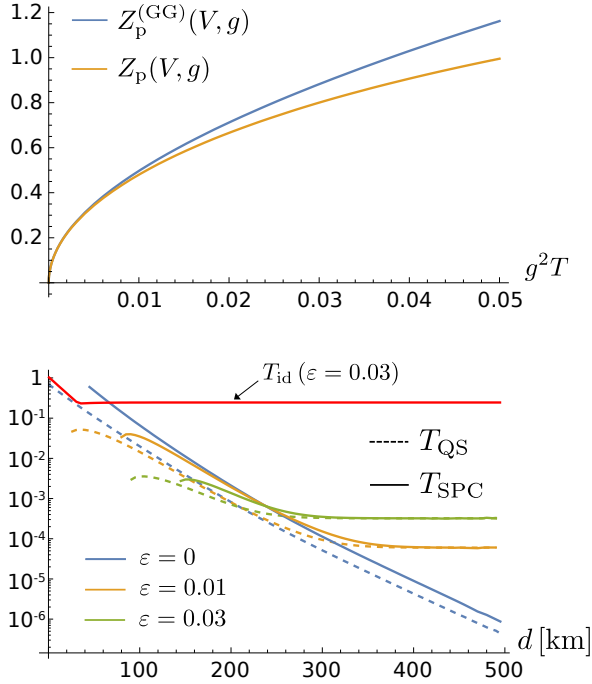


Figure 7. (Top) Plot of $Z_p(V, g)$ and $Z_p^{(GG)}(V, g)$, $p = \text{QS, SPC}$, as a function of $g^2 T$ for $\varepsilon = 0.03$ and $V = 4$. (Bottom) Log plot of the effective transmissivity T_p , $p = \text{QS, SPC}$, as a function of the distance d , expressed in km, for different values of excess noise ε . The plot have been performed only for the distances such that $K_p > 0$. In both the pictures we set $\beta = 0.95$ and $\eta = 1$.

which proves both all the NLA-assisted protocols to be nearly optimal. Furthermore, as in Sec. IV A a quantum efficiency $\eta \leq 1$ only rescales the KGR and does not introduce any maximum transmission distance.

Moreover, the saturation value of T_p determines the difference between ideal and physical NLAs. Indeed, if ε_p is small we have $T_p \ll 1$ and the physical NLA-assisted protocols approximate a GG02 protocol with the effective channel parameters T_p and ε_p . By increasing the excess noise further, we have $T_p \ll 1$ and $Z_p(V, g) \leq Z_p^{(GG)}(V, g)$, the state shared between Alice and Bob is less correlated and the protocol deviates more and more from GG02. This implies the reduced asymptotic maximum tolerable excess noise with respect to the ideal case.

V. CONCLUSIONS

In this paper we have addressed the exploitation of NLAs to achieve long-distance CV-QKD in the presence of a non-unit reconciliation efficiency and a non-null excess noise of the channel. We have considered both the ideal amplifier and two approximated physical realizations, namely, QS and SPC, in the presence of inefficient conditional on-off detection. We have discussed two alternative scenarios of either fixed or optimized NLA gain and showed that in the former case em-

ploying a NLA increases the maximum transmission distance by $(20 \log_{10} g)/\kappa$, whereas in the latter one NLAs allow to reach arbitrary large distances, provided the excess noise of the channel to be sufficiently low. Furthermore, we have proved both the physical NLA-assisted protocols to be robust if $\eta \leq 1$, showing that the quantum efficiency only rescales the KGR without preventing long-distance communication.

The results obtained offer a further strategy to overcome the practical limitations in CV-QKD and quantifies the degradation of performance produced by inefficient conditional detection. Moreover, they provide new perspectives for the applications of NLAs in realistic conditions for both one-way communication and end-to-end communication over quantum repeater chains [47–49].

ACKNOWLEDGEMENTS

This work has been partially supported by MAECI, Project No. PGR06314 “ENYGMA” and by University of Milan, Project No. RV-PSR-SOE-2020-SOLIV “S-O PhoQuLis”.

Appendix A: Brief review of the phase-space formalism

As discussed in the main text, to perform the analysis of the continuous-variable quantum key distribution (CV-QKD) protocol we exploit the phase-space formalism [35, 39]. We consider a n -mode bosonic system, described by the bosonic operators a_k satisfying the canonical commutation relations $[a_k, a_l] = 0$, $[a_k, a_l^\dagger] = \delta_{kl}$, and by the quadrature operators

$$q_k = a_k + a_k^\dagger \quad \text{and} \quad p_k = i(a_k^\dagger - a_k), \quad (\text{A1})$$

such that $[q_k, p_l] = 2i\delta_{kl}$. All quantities are expressed in shot noise units. A more compact notation is obtained by introducing the vector operators $\mathbf{a} = (a_1, a_2, \dots, a_n)^\top$ and $\mathbf{r} = (q_1, p_1, q_2, p_2, \dots, q_n, p_n)^\top$.

1. Quantum states

According to Glauber’s formula [35, 39], any n -mode quantum state of radiation ρ writes:

$$\rho = \int \frac{d^2 \alpha}{\pi^n} \chi(\alpha) D_{\mathbf{a}}(\alpha)^\dagger, \quad (\text{A2})$$

where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)^\top \in \mathbb{C}^n$ and

$$D_{\mathbf{a}}(\alpha) = \bigotimes_{k=1}^n D_{a_k}(\alpha_k), \quad (\text{A3})$$

where $D_{a_k}(\alpha_k)$ is the displacement operator acting on mode a_k , namely,

$$D_{a_k}(\alpha_k) = \exp(\alpha_k a_k^\dagger - \alpha_k^* a_k). \quad (\text{A4})$$

Some useful properties of the displacement operator are reported below:

$$D_{\mathbf{a}}(\alpha_1)D_{\mathbf{a}}(\alpha_2) = D_{\mathbf{a}}(\alpha_1 + \alpha_2), \quad \alpha_1, \alpha_2 \in \mathbb{C}^n, \quad (\text{A5a})$$

$$D_{\xi\mathbf{a}}(\alpha) = D_{\mathbf{a}}(\xi\alpha), \quad \xi \in \mathbb{R}, \quad (\text{A5b})$$

$$\text{Tr}[D_{\mathbf{a}}(\alpha)] = \pi^n \delta^{(n)}(\alpha), \quad (\text{A5c})$$

$\delta^{(n)}(\alpha)$ being the complex n -mode Dirac delta distribution.

Finally, the function

$$\chi(\alpha) = \text{Tr}[\rho D_{\mathbf{a}}(\alpha)] \quad (\text{A6})$$

is the characteristic function associated with ρ . In particular, a quantum state ρ_G exhibiting a Gaussian characteristic function is said to be a *Gaussian state*, namely,

$$\chi(\alpha) = \exp\left[-\frac{1}{2}\tilde{\alpha}^\top \sigma \tilde{\alpha} - i\tilde{\alpha}^\top \mathbf{X}\right], \quad (\text{A7})$$

where $\tilde{\alpha} = (\text{Re}\alpha_1, \text{Im}\alpha_1, \text{Re}\alpha_2, \text{Im}\alpha_2, \dots, \text{Re}\alpha_n, \text{Im}\alpha_n) \in \mathbb{R}^{2n}$,

$$\mathbf{X} = \text{Tr}[\rho_G \mathbf{r}] \quad (\text{A8})$$

is the first moment vector and

$$\sigma = \frac{1}{2} \text{Tr}\left[\rho_G \{(\mathbf{r} - \mathbf{X}), (\mathbf{r} - \mathbf{X})^\top\}\right] \quad (\text{A9})$$

is the $2n \times 2n$ covariance matrix (CM) where $\{A, B\} = AB + BA$ is the anti-commutator of A and B . Thus, a Gaussian state is completely characterized by its prime moments and its covariance matrix.

Moreover, for any pair of generic operators O_1 and O_2 acting on the Hilbert space of n modes the *trace rule* holds:

$$\text{Tr}[O_1 O_2] = \int \frac{d^2\alpha}{\pi^n} \chi_{O_1}(\alpha) \chi_{O_2}(-\alpha), \quad (\text{A10})$$

$\chi_{O_{1(2)}}(\alpha)$ being the characteristic function of $O_{1(2)}$, respectively. As an example, for a single radiation mode a , we choose $O_1 = D_a(\alpha)$ and $O_2 = q_a^2 = (a + a^\dagger)^2$ and obtain [29]:

$$\text{Tr}[D_a(\alpha) q_a^2] = e^{-(x^2+y^2)/2} \left[\pi \delta^{(2)}(\alpha) + 2\pi y \delta(x) \frac{d}{dy} \delta(y) - \pi \delta(x) \frac{d^2}{dy^2} \delta(y) \right], \quad (\text{A11})$$

where $\alpha = x + iy$ and $\delta(x)$ is the Dirac delta distribution.

2. Conditional measurements

In the paper we also discuss the case of conditional measurements. We consider a bipartite system AB , where subsystems A and B are composed of n_A and n_B modes, respectively. In the vector notation we have $\mathbf{a} = (\mathbf{a}_A, \mathbf{a}_B)$. We consider a bipartite quantum state ρ_{AB} with characteristic functions $\chi_{AB}(\alpha) = \chi_{AB}(\alpha_A, \alpha_B)$. We now perform a quantum measurement on subsystem B , described by means of the positive-operator-valued measurement (POVM) $\{\Pi_{\mathbf{r}_m}\}_{\mathbf{r}_m}$, whose effects are associated with the characteristic function $\chi_{\mathbf{r}_m}(\alpha_B)$. By applying the trace rule, the conditional state on A reads:

$$\begin{aligned} \rho_{A|\mathbf{r}_m} &= \frac{1}{p(\mathbf{r}_m)} \text{Tr}_B[\rho_{AB}(\mathbb{1}_A \otimes \Pi_{\mathbf{r}_m})] \\ &\equiv \frac{1}{p(\mathbf{r}_m)} \int \frac{d^2\alpha_A}{\pi^{n_A}} \chi_{A|\mathbf{r}_m}(\alpha_A) D_{\mathbf{a}_A}(\alpha_A)^\dagger, \end{aligned} \quad (\text{A12})$$

where:

$$\chi_{A|\mathbf{r}_m}(\alpha_A) = \int \frac{d^2\alpha_B}{\pi^{n_B}} \chi_{AB}(\alpha_A, \alpha_B) \chi_{\mathbf{r}_m}(-\alpha_B), \quad (\text{A13})$$

and $p(\mathbf{r}_m)$ is the detection probability:

$$\begin{aligned} p(\mathbf{r}_m) &= \text{Tr}_{AB}[\rho_{AB}(\mathbb{1}_A \otimes \Pi_{\mathbf{r}_m})] \\ &= \text{Tr}_A \left[\int \frac{d^2\alpha_A}{\pi^{n_A}} \chi_{A|\mathbf{r}_m}(\alpha_A) D_{\mathbf{a}_A} \right] = \chi_{A|\mathbf{r}_m}(\mathbf{0}). \end{aligned} \quad (\text{A14})$$

An interesting result is obtained for Gaussian states and Gaussian measurements. We now assume ρ_{AB} to be a Gaussian state with prime moments $\mathbf{X} = (\mathbf{X}_A, \mathbf{X}_B)$ and CM (written in block form)

$$\sigma = \begin{pmatrix} \sigma_A & \sigma_{AB} \\ \sigma_{AB}^\top & \sigma_B \end{pmatrix}. \quad (\text{A15})$$

Moreover, we consider a Gaussian POVM $\{\Pi_{\mathbf{r}_m}\}_{\mathbf{r}_m}$, that is a POVM whose effects have a Gaussian characteristic function with prime moments \mathbf{r}_m and CM σ_m . Then, the conditional state $\rho_{A|\mathbf{r}_m}$ is still a Gaussian state with CM $\sigma_{A|\mathbf{r}_m}$ and first moment vector $\mathbf{X}_{A|\mathbf{r}_m}$ given by [35, 39]:

$$\sigma_{A|\mathbf{r}_m} = \sigma_A - \sigma_{AB}(\sigma_B + \sigma_m)^{-1} \sigma_{AB}^\top, \quad (\text{A16})$$

and

$$\mathbf{X}_{A|\mathbf{r}_m} = \mathbf{X}_A + \sigma_{AB}(\sigma_B + \sigma_m)^{-1}(\mathbf{r}_m - \mathbf{X}_B), \quad (\text{A17})$$

respectively.

Appendix B: Security proof of the GG02 protocol

To perform the security analysis of the GG02 protocol in a reverse reconciliation scheme, we shall compute the KGR:

$$K = \beta I_{AB} - \chi_{BE}, \quad (\text{B1})$$

β being the reconciliation efficiency.

The mutual information I_{AB} gets the final expression reported in Eq. (4), as the Shannon entropy of a multivariate n -dimensional Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\sigma})$ with prime moments $\boldsymbol{\mu}$ and CM $\boldsymbol{\sigma}$:

$$\mathcal{G}(\mathbf{x}) = \frac{\exp\left[-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^T \boldsymbol{\sigma}^{-1}(\mathbf{x}-\boldsymbol{\mu})\right]}{(2\pi)^{n/2} \sqrt{\det(\boldsymbol{\sigma})}} \quad (\text{B2})$$

is equal to

$$\begin{aligned} H[\mathcal{G}] &= - \int d\mathbf{x} \mathcal{G}(\mathbf{x}) \log_2[\mathcal{G}(\mathbf{x})] \\ &= \frac{1}{2} \{ n \log_2(2\pi e) + \log_2[\det(\boldsymbol{\sigma})] \}. \end{aligned} \quad (\text{B3})$$

The amount of information extracted by Eve is given by the Holevo information

$$\chi_{BE} = S_E - S_{E|B}, \quad (\text{B4})$$

that can be evaluated as follows. We assume Eve to purify the system AB shared between Alice and Bob, that is we assume her to collect the fraction of the signal lost due to both the presence of the excess noise and the propagation into the channel such that the global quantum state ρ_{ABE} shared by Alice, Bob and Eve is pure [32, 33]. As a consequence, we have

$$S_E = S_{AB} = G\left(\frac{d_1-1}{2}\right) + G\left(\frac{d_2-1}{2}\right), \quad (\text{B5})$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $d_{1(2)}$ are the symplectic eigenvalues of Γ_{AB} [35, 39]. Furthermore, when Bob gets the outcome x_B from homodyne detection and reveals its value, the system AE shared between Alice and Eve becomes pure, thus

$$S_{E|B} = S_{A|B} = G\left(\frac{d_3-1}{2}\right), \quad (\text{B6})$$

where $d_3 = \sqrt{\det(\Gamma_{A|B})}$ and

$$\Gamma_{A|B} = \Gamma_A - \Gamma_Z \left[\Gamma_B + \boldsymbol{\sigma}_B^{(m)} \right]^{-1} \Gamma_Z^T, \quad (\text{B7})$$

which is independent of the particular outcome obtained.

Appendix C: Employing quantum scissors (QS) and single-photon catalysis (SPC)

As discussed in the main text, we perform the security analysis by exploiting the optimality of Gaussian attacks [43–45].

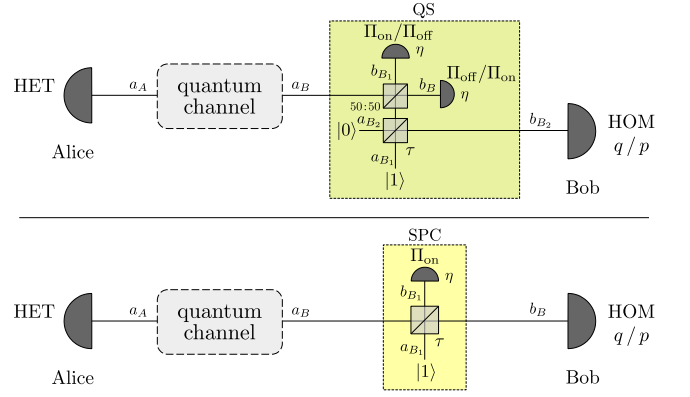


Figure 8. Schematic representation of the two physical NLA-assisted protocol discussed in the paper. (Top) Strategy based on quantum scissors (QS); (bottom) strategy based on single-photon catalysis (SPC).

If Alice and Bob share a non-Gaussian state ρ , a lower bound of the exact KGR is obtained by considering a Gaussian protocol in which they share the Gaussian state ρ_G with the same CM of ρ . In this section we derive the CM for both the physical noiseless linear amplifiers (NLAs) discussed in the paper, namely the quantum scissors (QS) and the single-photon catalysis (SPC). To do so, we exploit the input-output formalism and the phase-space representation of quantum states.

1. Quantum scissors (QS)

By following the notation introduced in Fig. 8 (top panel), the protocol employing QS works as follows [29]. Alice prepares the TMSV and injects one mode into the thermal-loss channel, thereafter Bob performs the QS protocol on the received beam. The input modes are $\mathbf{a} = (a_A, a_B, a_{B_1}, a_{B_2})^T$, where a_A, a_B are the modes shared by Alice and Bob after the channel whereas a_{B_1}, a_{B_2} are the modes exploited locally by Bob for the QS. The global input state reads:

$$\rho_{\mathbf{a}} = \int \frac{d^2\alpha}{\pi^4} \chi_{\mathbf{a}}(\alpha) D_{\mathbf{a}}(\alpha)^\dagger, \quad (\text{C1})$$

where $\boldsymbol{\alpha} = (\alpha_A, \alpha_B, \alpha_{B_1}, \alpha_{B_2})^T$ and

$$\chi_{\mathbf{a}}(\boldsymbol{\alpha}) = \chi_G(\alpha_A, \alpha_B) \times (1 - |\alpha_{B_1}|^2) e^{-(|\alpha_{B_1}|^2 + |\alpha_{B_2}|^2)/2}, \quad (\text{C2})$$

$\chi_G(\alpha_A, \alpha_B)$ being the Gaussian characteristic function in Eq. (A7) with null prime moments and the CM (2).

The output modes after the mode mixing operations performed by Bob are $\mathbf{b} = (b_A, b_B, b_{B_1}, b_{B_2})^T = \mathcal{M}_{\text{QS}} \mathbf{a}$, where

$$\mathcal{M}_{\text{QS}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \sqrt{\tau/2} & -\sqrt{(1-\tau)/2} \\ 0 & -\frac{1}{\sqrt{2}} & \sqrt{\tau/2} & -\sqrt{(1-\tau)/2} \\ 0 & 0 & \sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix}, \quad (\text{C3})$$

with $\tau = \tau_{\text{QS}}(g) = (1 + g^2)^{-1}$. The output state then writes:

$$\rho_{\mathbf{b}} = \int \frac{d^2\beta}{\pi^4} \chi_{\mathbf{b}}(\beta) D_{\mathbf{b}}(\beta)^\dagger, \quad (\text{C4})$$

where, exploiting the properties in Eq. (A5), $\chi_{\mathbf{b}}(\beta) = \chi_{\mathbf{a}}(\mathcal{M}_{\text{QS}}^\top \alpha)$.

Finally, Bob performs on-off detection on modes b_B, b_{B_1} , corresponding to the positive-operator-valued measurement (POVM) $\{\Pi_{\text{off}}, \Pi_{\text{on}} = \mathbb{1} - \Pi_{\text{off}}\}$, with associated characteristic functions [39, 50]

$$\chi_{\text{off}}(\alpha) = \frac{1}{\eta} e^{-\frac{2-\eta}{2\eta} |\alpha|^2} \quad (\text{C5a})$$

$$\chi_{\text{on}}(\alpha) = \pi \delta^{(2)}(\alpha) - \chi_{\text{off}}(\alpha). \quad (\text{C5b})$$

The amplification is successful if one of the two detectors gives the outcome ‘‘on’’ [12, 29]. In the following we assume to retrieve the couple (on,off), respectively for modes b_B, b_{B_1} . The post-selected state then equals to:

$$\rho_{\text{QS}} = \frac{1}{\tilde{P}_{\text{QS}}} \int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_{B_2}}{\pi} \chi_{\text{QS}}(\beta_A, \beta_{B_2}) D_{b_A}(\beta_A)^\dagger D_{b_{B_2}}(\beta_{B_2})^\dagger, \quad (\text{C6})$$

where

$$\chi_{\text{QS}}(\beta_A, \beta_{B_2}) = \int \frac{d^2\beta_B}{\pi} \frac{d^2\beta_{B_1}}{\pi} \chi_{\mathbf{b}}(\beta) \chi_{\text{on}}(-\beta_B) \chi_{\text{off}}(-\beta_{B_1}), \quad (\text{C7})$$

and

$$\begin{aligned} \tilde{P}_{\text{QS}} &= \text{Tr} \left[\int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_{B_2}}{\pi} \chi_{\text{QS}}(\beta_A, \beta_{B_2}) D_{b_A}(\beta_A)^\dagger D_{b_{B_2}}(\beta_{B_2})^\dagger \right] \\ &= \chi_{\text{QS}}(0, 0) = 2 \frac{8\eta\tau + (w-1)(3+w)(1+\eta\tau)}{(1+w)^2(3+w)^2} \end{aligned} \quad (\text{C8})$$

is the success probability of this conditional operation, with $w = 1 + \eta T(V + \varepsilon - 1)$. The same results hold if Bob gets the pair (off,on), thus the global success probability of the QS-based NLA is $P_{\text{QS}} = 2\tilde{P}_{\text{QS}}$.

Finally, we compute the CM associated with the state ρ_{QS} . By exploiting Eq. (A11), we have:

$$V_{\text{QS}} = \text{Tr} [\rho_{\text{QS}} q_{b_A}^2] = -1 - \frac{\mathcal{V}_{\text{QS}}}{\tilde{P}_{\text{QS}}}, \quad (\text{C9a})$$

$$W_{\text{QS}} = \text{Tr} [\rho_{\text{QS}} q_{b_{B_2}}^2] = -1 - \frac{\mathcal{W}_{\text{QS}}}{\tilde{P}_{\text{QS}}}, \quad (\text{C9b})$$

$$Z_{\text{QS}} = \text{Tr} [\rho_{\text{QS}} q_{b_A} q_{b_{B_2}}] = -\frac{\mathcal{Z}_{\text{QS}}}{\tilde{P}_{\text{QS}}}, \quad (\text{C9c})$$

where

$$\begin{aligned} \mathcal{V}_{\text{QS}} &= \left[\frac{d^2}{dy^2} \left(e^{-y^2/2} \chi_{\text{QS}}(iy, 0) \right) \right]_{y=0} \\ &= 2(V+1) \left[\frac{(2 + \eta T \varepsilon)(1 - \eta \tau)}{(1+w)^2} - \frac{8(3+w) + 2\eta T \varepsilon(3+w - 4\eta \tau) + 4\eta \tau(w-5)}{(3+w)^3} \right], \end{aligned} \quad (\text{C10a})$$

$$\mathcal{W}_{\text{QS}} = \left[\frac{d^2}{dv^2} \left(e^{-v^2/2} \chi_{\text{QS}}(0, iv) \right) \right]_{v=0} = -4 \frac{8\eta\tau + (w-1)(3+w)[2 - (1-\eta)\tau]}{(1+w)(3+w)^2}, \quad (\text{C10b})$$

$$\mathcal{Z}_{\text{QS}} = \left[\frac{d^2}{dydv} \left(e^{-(y^2-v^2)/2} \chi_{\text{QS}}(iy, iv) \right) \right]_{y=0, v=0} = \sqrt{TZ} \frac{8\eta\sqrt{\tau(1-\tau)}}{(3+w)^2}. \quad (\text{C10c})$$

Accordingly, the CM writes:

$$\Gamma_{AB}^{(\text{QS})} = \begin{pmatrix} V_{\text{QS}} \mathbb{1}_2 & Z_{\text{QS}} \sigma_z \\ Z_{\text{QS}} \sigma_z & W_{\text{QS}} \mathbb{1}_2 \end{pmatrix}. \quad (\text{C11})$$

2. Single-photon catalysis (SPC)

For SPC we follow the analogous procedure of the previous subsection. The input modes depicted in the bottom panel

of Fig. 8 are $\mathbf{a} = (a_A, a_B, a_{B_1})^\top$, where a_A, a_B are the modes shared by Alice and Bob after the channel and a_{B_1} is Bob’s ancillary mode. The global input state reads:

$$\rho_{\mathbf{a}} = \int \frac{d^2\alpha}{\pi^3} \chi_{\mathbf{a}}(\alpha) D_{\mathbf{a}}(\alpha)^\dagger, \quad (\text{C12})$$

where $\alpha = (\alpha_A, \alpha_B, \alpha_{B_1})^\top$ and

$$\chi_{\mathbf{a}}(\alpha) = \chi_{\text{G}}(\alpha_A, \alpha_B) \times e^{-|\alpha_{B_1}|^2/2} (1 - |\alpha_{B_1}|^2), \quad (\text{C13})$$

$\chi_G(\alpha_A, \alpha_B)$ being the Gaussian characteristic function in Eq. (A7) with null prime moments and the CM (2).

The output modes after the mode mixing operation performed by Bob are $\mathbf{b} = (b_A, b_B, b_{B_1})^T = \mathcal{M}_{\text{SPC}} \mathbf{a}$, where

$$\mathcal{M}_{\text{SPC}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\tau} & \sqrt{1-\tau} \\ 0 & -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix}, \quad (\text{C14})$$

with $\tau = \tau_{\text{SPC}}(g) = (4 + g^2 - g\sqrt{8 + g^2})/8$. The output state then writes:

$$\rho_{\mathbf{b}} = \int \frac{d^2\beta}{\pi^3} \chi_{\mathbf{b}}(\beta) D_{\mathbf{b}}(\beta)^\dagger, \quad (\text{C15})$$

where

$$\chi_{\mathbf{b}}(\beta) = \chi_{\mathbf{a}}(\mathcal{M}_{\text{SPC}}^T \alpha). \quad (\text{C16})$$

After the conditional on-off detection on mode b_{B_1} , the post-selected state reads:

$$\rho_{\text{SPC}} = \frac{1}{P_{\text{SPC}}} \int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_B}{\pi} \chi_{\text{SPC}}(\beta_A, \beta_B) D_{b_A}(\beta_A)^\dagger D_{b_B}(\beta_B)^\dagger, \quad (\text{C17})$$

where

$$\chi_{\text{SPC}}(\beta_A, \beta_B) = \int \frac{d^2\beta_{B_1}}{\pi} \chi_{\mathbf{b}}(\beta) \chi_{\text{on}}(-\beta_{B_1}), \quad (\text{C18})$$

and

$$\begin{aligned} P_{\text{SPC}} &= \text{Tr} \left[\int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_B}{\pi} \chi_{\text{SPC}}(\beta_A, \beta_B) D_{b_A}(\beta_A)^\dagger D_{b_B}(\beta_B)^\dagger \right] \\ &= \chi_{\text{SPC}}(0, 0) = 1 - \frac{4(1 - \eta\tau) + 2(w-1)(1-\tau)}{[2 + (w-1)(1-\tau)]^2} \end{aligned} \quad (\text{C19})$$

is the success probability of the SPC, and we introduced the quantity $w = 1 + \eta T(V + \varepsilon - 1)$.

The CM associated with the state ρ_{SPC} reads:

$$\Gamma_{AB}^{(\text{SPC})} = \begin{pmatrix} V_{\text{SPC}} \mathbb{1}_2 & Z_{\text{SPC}} \sigma_z \\ Z_{\text{SPC}} \sigma_z & W_{\text{SPC}} \mathbb{1}_2 \end{pmatrix}. \quad (\text{C20})$$

As for QS, we have:

$$V_{\text{SPC}} = \text{Tr} [\rho_{\text{QS}} q_{b_A}^2] = -1 - \frac{\mathcal{V}_{\text{SPC}}}{P_{\text{SPC}}}, \quad (\text{C21})$$

$$W_{\text{SPC}} = \text{Tr} [\rho_{\text{QS}} q_{b_B}^2] = -1 - \frac{\mathcal{W}_{\text{SPC}}}{P_{\text{SPC}}}, \quad (\text{C22})$$

$$Z_{\text{SPC}} = \text{Tr} [\rho_{\text{QS}} q_{b_A} q_{b_B}] = -\frac{\mathcal{Z}_{\text{SPC}}}{P_{\text{SPC}}}, \quad (\text{C23})$$

and

$$\begin{aligned} \mathcal{V}_{\text{SPC}} &= \left[\frac{d^2}{dy^2} \left(e^{-y^2/2} \chi_{\text{SPC}}(iy, 0) \right) \right]_{y=0} \\ &= -(V+1) \left[1 - 2 \frac{4 + \eta T \varepsilon (1-\tau)(1+q-4\eta\tau) + 2(1+\eta\tau)(q-1) - 4\eta\tau}{(1+q)^3} \right], \end{aligned} \quad (\text{C24a})$$

$$\begin{aligned} \mathcal{W}_{\text{SPC}} &= \left[\frac{d^2}{dv^2} \left(e^{-v^2/2} \chi_{\text{SPC}}(0, iv) \right) \right]_{v=0} \\ &= -4 - \tau(r-3) + 4 \frac{(q-1)^2 + (r-1)(q-1)(\eta+\tau) + 2\tau(r-1) - 2\eta\tau(q-1) + 2(w-1)(4-4\tau-\tau^2)}{(1+q)^3}, \end{aligned} \quad (\text{C24b})$$

$$\mathcal{Z}_{\text{SPC}} = \left[\frac{d^2}{dydv} \left(e^{-(y^2-v^2)/2} \chi_{\text{SPC}}(iy, iv) \right) \right]_{y=0, v=0} = \sqrt{\tau T Z} \left[1 - 4 \frac{2 + (1+\eta)(q-1) + 2\eta(1-2\tau)}{(1+q)^3} \right], \quad (\text{C24c})$$

with $q = 1 + \eta T(1-\tau)(V + \varepsilon - 1)$ and $r = 1 + T(V + \varepsilon - 1)$.

- [1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **747**, 513

- (2005).
[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

- [4] F. Grosshans et al., *Nature* **421**, 238 (2003).
- [5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [6] F. Grosshans et al., *Quantum Inf. Comput.* **3**, 535 (2003).
- [7] F. Grosshans, *Phys. Rev. Lett.* **94**, 020504 (2005).
- [8] S. Pirandola et al., *Adv. Opt. Photon.* **12**, 1012 (2020).
- [9] M. Bloch, A. Thangaraj, S. W. McLaughlin and J.-M. Merolla, in *Proc. IEEE Information Theory Workshop*, 2006, pp. 1179–1183.
- [10] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri and P. Grangier, *Phys. Rev. A* **72**, 050303(R) (2005).
- [11] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor and P. Grangier, *Phys. Rev. A* **77**, 042325, (2008).
- [12] T. C. Ralph and A. P. Lund, in *Proc. AIP Conf. Proc.*, 2009, vol. 1110, pp. 155–160.
- [13] T. C. Ralph, *Phys. Rev. A* **84**, 022339 (2011).
- [14] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier and R. Tualle-Brouri, *Phys. Rev. A* **86**, 012327 (2012).
- [15] J. Fiurášek, *Phys. Rev. A* **80**, 053822 (2009).
- [16] G.-Y. Xiang et al., *Nat. Photonics* **4**, 316 (2010).
- [17] N. A. McMahon, A. P. Lund and T. C. Ralph, *Phys. Rev. A* **89**, 023846 (2014).
- [18] S. Zhang and X. Zhang, *Phys. Rev. A* **97**, 043830 (2018).
- [19] M. S. Winnel, N. Hosseinidehaj and T. C. Ralph, *Phys. Rev. A* **102**, 063715 (2020).
- [20] J. Fiurášek, *Opt. Express* **30**, 1466 (2022).
- [21] J. J. Guanzon, M. S. Winnel, A. P. Lund and T. C. Ralph, *Phys. Rev. Lett.* **128**, 160501 (2022).
- [22] J. Fiurášek, *Phys. Rev. A* **105**, 062425 (2022).
- [23] J. J. Guanzon, M. S. Winnel, A. P. Lund and T. C. Ralph, *arXiv:2211.08035* (2022).
- [24] H. M. Chrzanowski et al., *Nat. Photonics* **8**, 333 (2014).
- [25] J. Fiurášek and N. J. Cerf, *Phys. Rev. A* **86**, 060302(R) (2012).
- [26] N. Walk, T. C. Ralph, T. Symul and P. K. Lam, *Phys. Rev. A* **87**, 020303(R) (2013).
- [27] J. Bernu et al., *J. Phys. B - At. Mol. Opt.* **47**, 215503 (2014).
- [28] J. Zhao, J. Y. Haw, T. Symul, P. K. Lam and S. M. Assad, *Phys. Rev. A* **96**, 012319 (2017).
- [29] M. Ghalaii et al., *IEEE J. Sel. Top. Quantum Electron.* **26**, 1 (2020).
- [30] M. Ghalaii et al., *IEEE J. Sel. Areas Commun.* **38**, 506 (2020).
- [31] L. Hu, M. Al-amri, Z. Liao and M. S. Zubairy, *Phys. Rev. A* **102**, 012608 (2020).
- [32] R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **102**, 130501 (2009).
- [33] J. Lodewyck et al., *Phys. Rev. A* **76**, 042305 (2007).
- [34] S. Olivares, *Phys. Lett. A* **418**, 127720 (2021).
- [35] S. Olivares, *Eur. Phys. J. Spec. Top.* **203**, 3 (2012).
- [36] A. Yoshizawa and H. Tsuchida, *Appl. Phys. Lett.* **85**, 2457 (2004).
- [37] X. Li, P. L. Voss, J. E. Sharping and P. Kumar, *Phys. Rev. Lett.* **94**, 053601 (2005).
- [38] M. V. Larsen et al., *npj Quantum Inf.* **5**, 46 (2019).
- [39] A. Ferraro, S. Olivares and M. G. A. Paris, *Gaussian States in quantum information* (Bibliopolis Napoli, 2005).
- [40] A. S. Holevo, *IEEE Trans. Inf. Theory* **44**, 269 (1998).
- [41] A. Leverrier and P. Grangier, *Phys. Rev. Lett.* **102**, 180504 (2009).
- [42] P. Jouguet, S. Kunz-Jacques and A. Leverrier, *Phys. Rev. A* **84**, 062317 (2011).
- [43] M. Navascués, F. Grosshans and A. Acín, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [44] A. Leverrier, PhD Thesis, Télécom ParisTech, 2009.
- [45] R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [46] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, *Nat. Commun.* **8**, 1 (2017).
- [47] F. Furrer and W. J. Munro, *Phys. Rev. A* **98**, 032335 (2018).
- [48] S. Pirandola, *Commun. Phys.* **2**, 1 (2019).
- [49] J. Dias, M. S. Winnel, N. Hosseinidehaj and T. C. Ralph, *Phys. Rev. A* **102**, 052425 (2020).
- [50] S. Olivares and M. G. Paris, *J. Opt. B Quantum Semiclassical Opt.* **7**, S616 (2005).