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

Michele N. Notarnicola and Stefano Olivares*
*Dipartimento di Fisica "Aldo Pontremoli," Università degli Studi di Milano, 20133 Milano, Italy and INFN, Sezione di Milano, 20133 Milano, Italy*

(Received 18 May 2023; revised 13 July 2023; accepted 18 July 2023; published 4 August 2023)

Noiseless linear amplifiers (NLAs) provide a powerful tool to achieve long-distance continuous-variable (CV) quantum key distribution (QKD) in the presence of realistic setups with nonunit reconciliation efficiency. We address a NLA-assisted CV QKD protocol implemented via realistic physical NLAs, namely, quantum scissors and single-photon catalysis, 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.

DOI: 10.1103/PhysRevA.108.022404

## I. INTRODUCTION

Quantum key distribution (QKD) [1] allows one 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 (CV) QKD for both theoretical and experimental reasons [2]. In the first proposal of a CV QKD scheme by Grosshans and Grangier [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 a 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 and the phase noise of the carrier signal introduce 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 slot, and prevent long-distance communication leading to a maximum transmission distance at which the KGR vanishes [10–12]. In the latest experimental realizations, high-loss CV QKD has been achieved up to maximum transmission distances ranging from 100 to 200 km [13–17].

A challenging task to face those issues is to modify the original protocol by implementing strategies allowing one 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 [18–20]. Indeed, an ideal probabilistic noiseless linear amplifier (NLA) with amplitude gain $g$ leads to an increase in the maximum transmission distance proportional to $\log g$ [21]. Nevertheless, any realistic physical NLA can only approximate the ideal amplifier for low-amplitude optical signals [18,22–30]. To avoid this limitation, measurement-based NLAs, performing virtual amplification based on classical data postselection, have also been proposed [31–33]. However, the low success probabilities of these operations [34,35] make physical NLAs still worthy of investigation. Recently, CV QKD employing quantum scissors (QS) [18] has been addressed, allowing one to achieve long-distance CV QKD for sufficiently low channel excess noise [36,37]. With the same goal, also single-photon catalysis (SPC) has been investigated [25,38]. In the QS scheme, a single photon is mixed with the vacuum at a beam splitter with transmissivity $\tau$. One of the output branches then impinges at a balanced beam splitter with the incoming signal, after which double conditional photodetection is performed. Differently from QS, in the SPC process a single photon interferes directly with the incoming signal at a beam splitter with transmissivity $\tau$ 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 present paper we investigate a CV QKD protocol assisted by these two schemes and consider a simplified realistic scenario where photodetection is replaced by on-off detection. We compute the KGRs for both strategies and compare them to the performance of the protocol assisted by the ideal NLA proposed in [21]. Moreover, we distinguish two alternative cases. In the first 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 second 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

*stefano.olivares@fisica.unimi.it

 

discuss the robustness in the presence of a quantum detection efficiency $\eta \leqslant 1$, showing that the detection efficiency only rescales the KGR without preventing long-distance communication.

The structure of the paper is as follows. In Sec. II we recall the main features of the Grosshans-Grangier (GG) protocol. 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. In Sec. V we summarize the results obtained and draw some conclusions.

## II. THE GG ORIGINAL PROTOCOL

We start by reviewing the CV QKD protocol proposed in [3–6] in its entanglement-based version, which provides a simplified theoretical analysis [39,40]. Here Alice and Bob share a two-mode squeezed vacuum (TMSV) state, namely, $|\mathrm{TMSV}\rangle\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle$, with $0 \leqslant \lambda \leqslant 1$. The TMSV is a two-mode Gaussian state [41,42] and can be completely described by the covariance matrix (CM) (see Appendixes A and B for details)

$$\Gamma_{\mathrm{TMSV}} = \begin{pmatrix} V\mathbb{1}_2 & Z\boldsymbol{\sigma}_z \\ Z\boldsymbol{\sigma}_z & V\mathbb{1}_2 \end{pmatrix}, \tag{1}$$

where $V = 1 + 2\lambda^2/(1-\lambda^2)$ is the TMSV variance, corresponding to the input modulation variance of the protocol, $Z = \sqrt{V^2-1}$, $\mathbb{1}_2 = \mathrm{diag}(1,1)$, and $\boldsymbol{\sigma}_z$ 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 kilometers and $\kappa \sim 0.2$ dB/km is the typical loss parameter for optical fibers at 1550 nm [43–45]. Moreover, a single-mode thermal bath of $n_\varepsilon = T\varepsilon/2(1-T)$ photons models the presence of an excess noise $\varepsilon$ 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 the CM [41,42]

$$\Gamma_{AB} = \begin{pmatrix} \Gamma_A & \Gamma_Z \\ \Gamma_Z^{\mathsf{T}} & \Gamma_B \end{pmatrix} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{T}Z\boldsymbol{\sigma}_z \\ \sqrt{T}Z\boldsymbol{\sigma}_z & T(V+\chi)\mathbb{1}_2 \end{pmatrix}. \tag{2}$$

Once received the signal, Bob implements a Gaussian measurement [39,40] 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 [42,46], when Alice and Bob perform detection on their own signals they get a bivariate Gaussian distribution $p_{A\,(B)}(x_{A\,(B)}, y_{A\,(B)})$ with zero mean and covariance $\Gamma_{A\,(B)} + \boldsymbol{\sigma}^{(\mathrm{m})}_{A\,(B)}$, where $\boldsymbol{\sigma}^{(\mathrm{m})}_A = \mathbb{1}_2$ is the CM of the heterodyne detection and

$$\boldsymbol{\sigma}^{(\mathrm{m})}_B = \lim_{z\to 0}\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \tag{3}$$

is the $2\times 2$ 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 $\Gamma_{AB} + (\boldsymbol{\sigma}^{(\mathrm{m})}_A \oplus \boldsymbol{\sigma}^{(\mathrm{m})}_B)$. The mutual information between Alice and Bob is then given by

$$\begin{aligned} I_{AB} &= H[p_A] + H[p_B] - H[p_{AB}] \\ &= \log_2\left(\sqrt{\frac{\det\left[\Gamma_A + \boldsymbol{\sigma}^{(\mathrm{m})}_A\right]\det\left[\Gamma_B + \boldsymbol{\sigma}^{(\mathrm{m})}_B\right]}{\det\left[\Gamma_{AB} + \left(\boldsymbol{\sigma}^{(\mathrm{m})}_A \oplus \boldsymbol{\sigma}^{(\mathrm{m})}_B\right)\right]}}\right), \end{aligned} \tag{4}$$

with $H[p] = -\int dx\, p(x)\log_2 p(x)$ 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 data set [7]. If the reconciliation efficiency is $0 \leqslant \beta \leqslant 1$, the KGR is written

$$K = \beta I_{AB} - \chi_{BE}, \tag{5}$$

where the Holevo information $\chi_{BE}$ represents the amount of information extracted by Eve [47] and can be computed starting from the CM (2) as

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

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{7}$$

and $d_{1\,(2)}$ are the symplectic eigenvalues of $\Gamma_{AB}$ [42,46], namely,

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

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)

$$\Gamma_{A|B} = \Gamma_A - \Gamma_Z\left(\Gamma_B + \boldsymbol{\sigma}^{(\mathrm{m})}_B\right)^{-1}\Gamma_Z^{\mathsf{T}}. \tag{9}$$

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 $\beta \sim 0.95$ [9,48,49] and the channel excess noise $\varepsilon$. 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. Specifically, Alice prepares the TMSV state with modulation variance $V$ and injects one mode into the thermal-loss channel. To mitigate the added noise $\chi$, Bob implements a NLA on his received pulse, before performing homodyne detection. Here

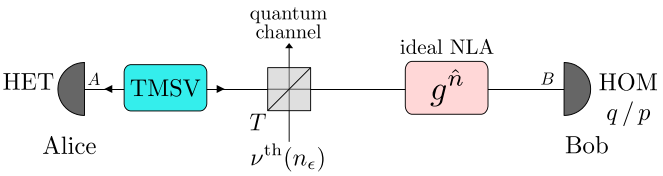


FIG. 1. Scheme of the CV QKD protocol assisted by the ideal NLA proposed in [21]. Here HET and HOM denote the heterodyne and homodyne detectors, respectively.

we consider Bob to employ either the ideal NLA proposed in [21] or feasible physical NLAs realized via QS or SPC.

### A. Ideal NLA

First, we assume Bob to employ an ideal NLA, as depicted in Fig. 1. The ideal NLA is a nondeterministic operation described by the self-adjoint operator $g^{\hat{n}}$, where $\hat{n}$ is the photon-number operator of the optical mode undergoing amplification and $g \geqslant 1$ is the amplifier gain [18]. As discussed in [21], this operation preserves Gaussianity; therefore the protocol in Fig. 1 is equivalent to a GG scheme with the parameters

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

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

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

provided

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

Without the last condition on the gain an unphysical unnormalizable state is obtained [18,21]. Equivalently, for a fixed gain Eq. (11) corresponds to a threshold of the transmissivity, namely,

$$T \leqslant T_{\text{th}} \equiv \frac{2}{(g^2-1)(V+\varepsilon-1)}, \tag{12}$$

preventing the use of the NLA protocol for distances $d \leqslant d_{\text{th}}^{(\text{id})} = (-10\log_{10} T_{\text{th}})/\kappa$. For $d > d_{\text{th}}^{(\text{id})}$, employing the ideal NLA is equivalent to considering an effective channel of increased transmissivity $T_{\text{id}} \geqslant T$. The resulting KGR then reads

$$\tilde{K}_{\text{id}}(V,g) = P_{\text{id}}(V,g)\big[\beta I_{AB}^{(\text{id})}(V,g) - \chi_{BE}^{(\text{id})}(V,g)\big], \tag{13}$$

where $P_{\text{id}}(V,g)$ is the success probability of the NLA and $I_{AB}^{(\text{id})}(V,g)$ and $\chi_{BE}^{(\text{id})}(V,g)$ are computed from Eqs. (4) and (6), respectively, with the modified parameters (10). Since $P_{\text{id}}(V,g) \leqslant 1/g^2$ [21], from now on we consider as a benchmark the KGR

$$K_{\text{id}}(V,g) = \frac{1}{g^2}\big[\beta I_{AB}^{(\text{id})}(V,g) - \chi_{BE}^{(\text{id})}(V,g)\big]. \tag{14}$$

The KGR (14) 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

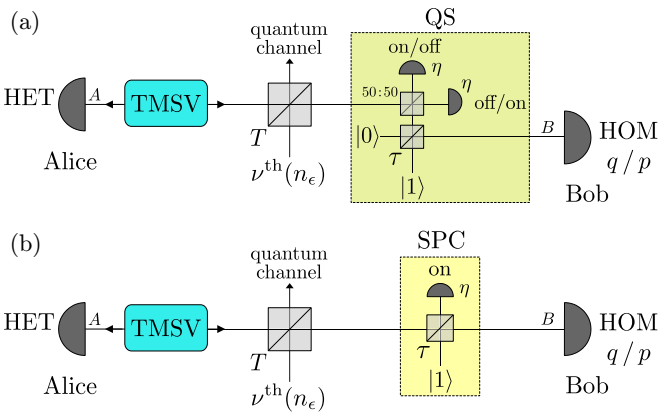


FIG. 2. Scheme of the CV QKD protocol assisted by the two physical NLAs discussed in the paper: strategy based on (a) quantum scissors and (b) single-photon catalysis.

will discuss two separate cases. In the first case we assume a fixed $g$ and optimize only the modulation variance, obtaining the KGR

$$K_{\text{id}}(g) = \max_V K_{\text{id}}(V,g), \tag{15}$$

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

$$K_{\text{id}} = \max_{V,g} K_{\text{id}}(V,g), \tag{16}$$

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 [36] [Fig. 2(a)], Bob prepares two ancillary modes in the Fock states $|1\rangle$ and $|0\rangle$, respectively. He mixes them at a beam splitter with transmissivity $\tau$ 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 output branches (see Appendix C for details), corresponding to the positive-operator-valued measurement $\{\Pi_{\text{off}}, \Pi_{\text{on}} = \mathbb{1} - \Pi_{\text{off}}\}$, where

$$\Pi_{\text{off}} = \sum_{k=0}^{\infty}(1-\eta)^k |k\rangle\langle k|, \tag{17}$$

with $\eta \leqslant 1$ the detection quantum efficiency. If one of the two detectors gives the outcome "on," Bob performs homodyne detection on the postselected output state. The value of $\tau$ fixes the gain associated with the NLA; that for low-amplitude coherent signals reads $g = \sqrt{(1-\tau)/\tau}$ [18]. Thus, to achieve the gain $g$ we set the transmissivity equal to

$$\tau_{\text{QS}}(g) = \frac{1}{1+g^2}. \tag{18}$$

In contrast, in the SPC scheme [Fig. 2(b)], Bob has a single ancillary mode excited in $|1\rangle$ impinging at a beam

splitter with transmissivity $\tau$ with the pulse received by Alice. He performs on-off detection on the reflected branch, conditioned on outcome "on," and homodynes the postselected state. The associated gain is $g = (1-2\tau)/\sqrt{\tau}$ [25], which can be inverted to find the transmissivity as a function of the gain

$$\tau_{\mathrm{SPC}}(g) = \tfrac{1}{8}(4 + g^2 - g\sqrt{8+g^2}). \tag{19}$$

In both cases, after the NLA Alice and Bob share a non-Gaussian state $\rho_{AB}^{(p)}$ $(p = \mathrm{QS}, \mathrm{SPC})$. However, since Bob's measurement is Gaussian, the security analysis of the NLA-assisted protocol can be based on the optimality of Gaussian attacks [50–52], which, in this scenario, maximize the amount of information extractable by Eve. Moreover, following Ref. [50], we consider the Gaussian lower bound on the mutual information, which 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

$$K_p(V,g) = P_p(V,g)\big[\beta I_{AB}^{(p)}(V,g) - \chi_{BE}^{(p)}(V,g)\big], \tag{20}$$

where $P_p(V,g)$ is the success probability associated with the $p$ 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 $K_p(V,g) \geqslant 0$ provides a sufficient condition to guarantee secure communication. Nevertheless, our results are in good agreement with other exact numerical approaches [36], proving the bound (20) 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)

$$\Gamma_{AB}^{(p)} = \begin{pmatrix} V_p(V,g)\mathbb{1}_2 & Z_p(V,g)\boldsymbol{\sigma}_z \\ Z_p(V,g)\boldsymbol{\sigma}_z & W_p(V,g)\mathbb{1}_2 \end{pmatrix}. \tag{21}$$

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 $\Gamma_{AB} \to \Gamma_{AB}^{(p)}$ and optimize Eq. (20) over the free parameters, obtaining the KGRs

$$K_p(g) = \max_V K_p(V,g) \quad (p = \mathrm{QS}, \mathrm{SPC}) \tag{22}$$

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

$$K_p = \max_{V,g} K_p(V,g) \quad (p = \mathrm{QS}, \mathrm{SPC}) \tag{23}$$

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

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 us to retrieve the results of the original 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 $0 \leqslant \tau \leqslant \frac{1}{2}$ for which the corresponding gain is $g \geqslant 0$, as shown in Appendix C.

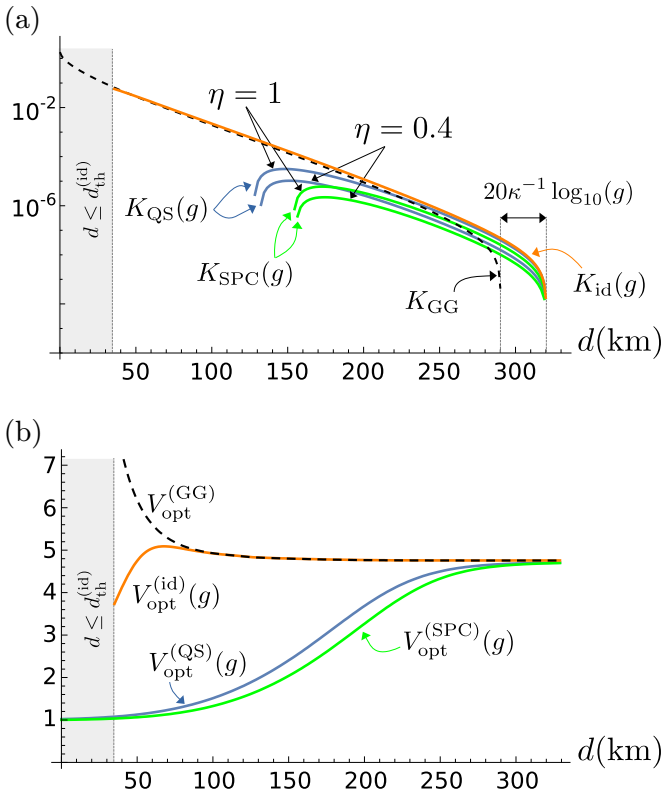


FIG. 3. (a) Logarithmic plot of the KGRs $K_p(g)$ for different values of the quantum efficiency $\eta$ and $K_{\mathrm{id}}(g)$ as functions of the distance $d$ in kilometers for $\beta = 0.95$, $\varepsilon = 0.03$, and $g = 2$. The dashed line is the KGR of the original protocol. (b) Plot of the optimized (input) modulations $V_{\mathrm{opt}}^{(p)}(g)$ and $V_{\mathrm{opt}}^{(\mathrm{id})}(g)$ as functions of the distance $d$ in kilometers for $\beta = 0.95$, $\varepsilon = 0.03$, $g = 2$, and $\eta = 1$. In both the plots, the shaded region represents the regime $d \leqslant d_{\mathrm{th}}^{(\mathrm{id})}$, where ideal NLAs generate an unphysical unnormalizable state (see the text for details).

## 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(a) for $\varepsilon > 0$. As emerges from the plot, 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 effective transmissivity in Eq. (10) is $T_{\mathrm{id}} \approx g^2 T$ [21]. 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 for the realistic

values of practical CV QKD systems where $0.4 \leqslant \eta \leqslant 0.6$ [10,40].

In fact, by expanding the CM (21) in the long-distance regime where $T \ll 1$ up to the first order in $T$, we have

$$V_p(V, g) = V + O(T), \tag{24a}$$

$$W_p(V, g) = g^2 T(V + \chi) + O(T^2), \tag{24b}$$

$$Z_p(V, g) = \sqrt{g^2 T} Z + O(T^{3/2}) \quad (p = \mathrm{QS}, \mathrm{SPC}), \tag{24c}$$

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

$$P_p(V, g) \approx P_p(g) = \eta \tau_p(g), \tag{25}$$

and, since $P_{\mathrm{SPC}}(g) \leqslant P_{\mathrm{QS}}(g)$, we have $K_{\mathrm{SPC}}(g) \leqslant K_{\mathrm{QS}}(g)$. In turn, a quantum efficiency $\eta \leqslant 1$ only reduces the success probability and rescales the KGR, without preventing long-distance secure communication. For completeness, we report the (input) optimized modulations in Fig. 3(b). Despite the different behavior at small distances, for large $d$ all the protocols converge to the same asymptotic value, not depending on $\varepsilon$. Numerical calculations have also shown that $V_{\mathrm{opt}}^{(p)}(g)$ does not depend on the quantum efficiency.

We note that in the short-distance regime, where $T \approx 1$ or, equivalently, $\kappa d \ll 1$, both physical NLAs are useless since we obtain negative KGR up to a threshold distance $d_{\mathrm{th}}^{(p)}$ ($p = \mathrm{QS}, \mathrm{SPC}$). In this regime, the CM (21) cannot be recast in the form of Eq. (2) and, as displayed in Fig. 4(a) for the QS case, both the mutual information $I_{AB}^{(p)}(g) = I_{AB}^{(p)}(V_{\mathrm{opt}}^{(p)}(g), g)$ and the Holevo information $\chi_{BE}^{(p)}(g) = \chi_{BE}^{(p)}(V_{\mathrm{opt}}^{(p)}(g), g)$ are lower than their GG counterparts $I_{AB}^{(\mathrm{GG})}$ and $\chi_{BE}^{(\mathrm{GG})}$, respectively. Moreover, for $\varepsilon > 0$ we have $I_{AB}^{(p)}(g) \leqslant \chi_{BE}^{(p)}(g)$, leading to a negative KGR which inhibits secure communication. This effect may be understood by considering the success probability $P_p(V, g)$ of the proposed physical NLAs, plotted in Fig. 4(b) for the QS case. Analogous considerations hold for SPC. When $P_p(V, g) > 1/g^2$ the $p$ scheme does not implement a true NLA [21,36], and the amplification process introduces an unavoidable noise on the quadrature variances, becoming a further resource for Eve's attack. Accordingly, for $\kappa d \ll 1$ the optimization procedure leads to low modulation variances $V_{\mathrm{opt}}^{(p)}(g) \approx 1$, resulting in lower mutual information with respect to the GG scheme and in a negative KGR. On the other hand, for $\kappa d \gg 1$, $V_{\mathrm{opt}}^{(p)} \approx V_{\mathrm{opt}}^{(\mathrm{GG})}$ and both $I_{AB}^{(p)}$ and $\chi_{BE}^{(p)}$ outperform the GG protocol. In turn, between the short- and long-distance regimes, we identify the threshold distance such that $K_p(g) \geqslant 0$ for $d \leqslant d_{\mathrm{th}}^{(p)}$.

Finally, in Fig. 5 we plot the maximum tolerable excess noise (MTEN) $\varepsilon_{\mathrm{max}}$ as a function of the distance $d$: It represents the maximum value of $\varepsilon$ still leading to a positive KGR. For the original protocol, $\varepsilon_{\mathrm{max}}$ is a decreasing function of $d$. The behavior is rather different for the NLA-assisted protocols. In the presence of ideal NLA the MTEN $\varepsilon_{\mathrm{max}}^{(\mathrm{id})}(g)$ for $d \lesssim 40$ km is lower than in the original protocol due to the limitation imposed by (11). However, for larger distances we have $\varepsilon_{\mathrm{max}}^{(\mathrm{id})}(g) > \varepsilon_{\mathrm{max}}$. In contrast, the MTEN associated with the physical NLAs, namely, $\varepsilon_{\mathrm{max}}^{(p)}(g)$, is not a monotonic function of $d$; it is an increasing function of $d$ approaching $\varepsilon_{\mathrm{max}}^{(\mathrm{id})}$. A quantum efficiency $\eta \leqslant 1$ does not affect the value of $\varepsilon_{\mathrm{max}}^{(p)}$, consistently with the previous discussion. As a consequence, for fixed $g$, in the long-distance regime the physical NLAs guarantee the same performance of the ideal NLA.

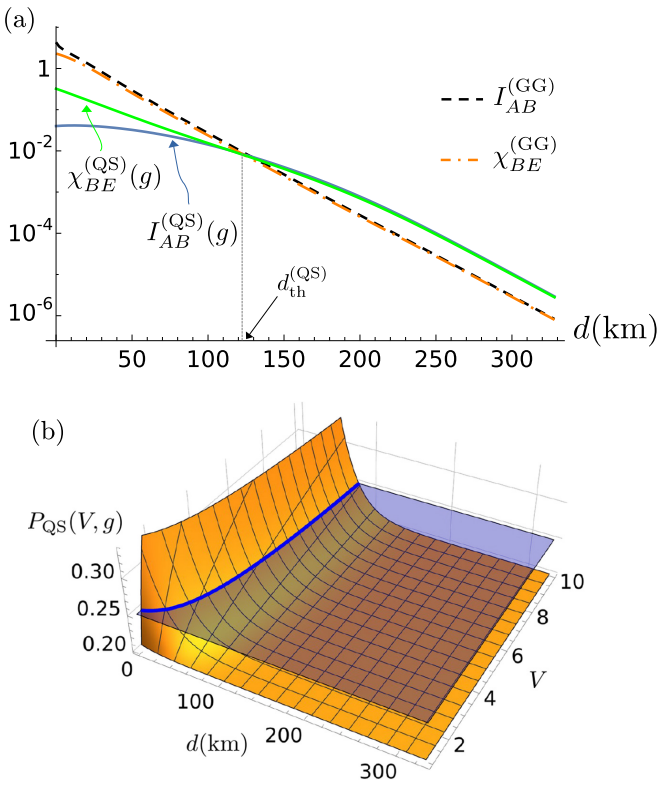


FIG. 4. (a) Logarithmic plot of $I_{AB}^{(\mathrm{QS})}(g)$ and $\chi_{BE}^{(\mathrm{QS})}(g)$ (solid lines), $I_{AB}^{(\mathrm{GG})}$ (dashed line), and $\chi_{BE}^{(\mathrm{GG})}$ (dash-dotted line) as functions of the distance $d$ in kilometers. (b) Plot of the success probability $P_{\mathrm{QS}}(V, g)$ as a function of the distance $d$ and the modulation variance $V$. The horizontal plane refers to the value $1/g^2$: When $P_{\mathrm{QS}}(V, g) > 1/g^2$, the QS do not perform noiseless amplification. In both figures we set $\beta = 0.95$, $\varepsilon = 0.03$, $g = 2$, and $\eta = 1$.

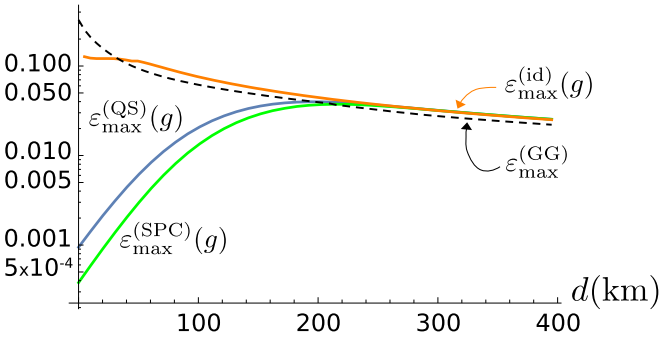


FIG. 5. Logarithmic plot of the maximum tolerable excess noise $\varepsilon_{\mathrm{max}}^{(\mathrm{id})}(g)$ and $\varepsilon_{\mathrm{max}}^{(p)}(g)$ ($p = \mathrm{QS}, \mathrm{SPC}$) as a function of the distance $d$ in kilometers for $g = 2$, $\eta = 1$, and $\beta = 0.95$. The black dashed line corresponds to the $\varepsilon_{\mathrm{max}}$ of the original protocol.

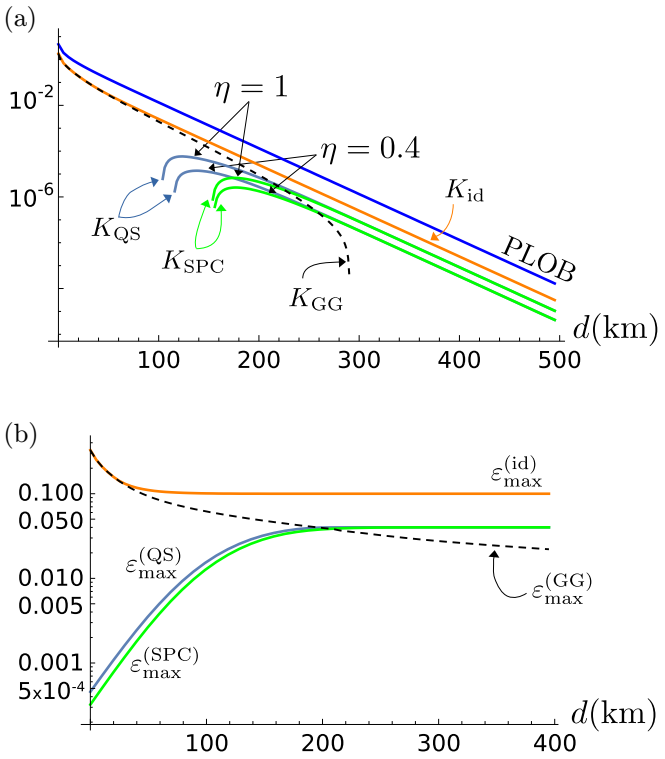


FIG. 6. (a) Logarithmic plot of the KGRs $K_p$ ($p = \mathrm{QS}, \mathrm{SPC}$) and $K_{\rm id}$ as functions of the distance $d$ in kilometers for different values of the quantum efficiency $\eta$, $\varepsilon = 0.03$, and $\beta = 0.95$ and with optimized gain $g$. The dashed line is the KGR of the original protocol and the upper line is the PLOB bound (26). (b) Logarithmic plot of the maximum tolerable excess noises $\varepsilon_{\rm max}^{\rm (id)}$ and $\varepsilon_{\rm max}^{(p)}$ ($p = \mathrm{QS}, \mathrm{SPC}$) as functions of the distance $d$ in kilometers for $\eta = 1$ and $\beta = 0.95$. The black dashed line corresponds to the $\varepsilon_{\rm max}$ of the original protocol.

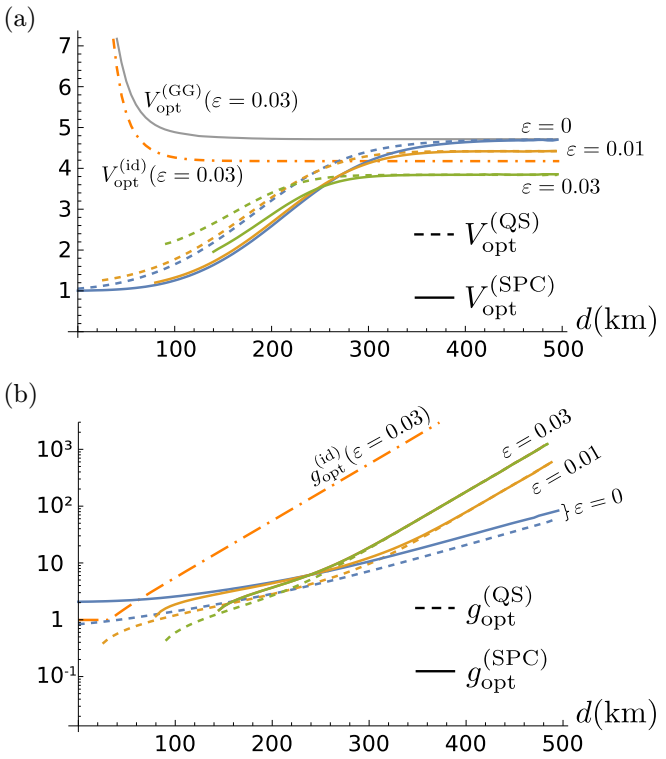


FIG. 7. (a) Plot of $V_{\rm opt}^{(p)}$ ($p = \mathrm{QS}, \mathrm{SPC}$) as a function of the distance $d$ in kilometers for different values of excess noise $\varepsilon$. The upper gray and the dash-dotted lines represent the optimized modulation for the original and the ideal NLA-assisted protocols, respectively, for $\varepsilon = 0.03$. (b) Logarithmic plot of $g_{\rm opt}^{(p)}$ ($p = \mathrm{QS}, \mathrm{SPC}$) as a function of the distance $d$ in kilometers for different values of excess noise $\varepsilon$. The plots have been performed only for distances such that $K_p > 0$ ($p = \mathrm{QS}, \mathrm{SPC}$). We set $\beta = 0.95$ and $\eta = 1$.

### 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. 6(a). First, in the short-distance regime the physical NLAs still exhibit a threshold distance to obtain a positive KGR, differently from the ideal amplifier. Second, all the NLA-assisted protocols allow us 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 $\kappa d \gg 1$, $K_{\rm QS}$ and $K_{\rm SPC}$ are almost identical, proving SPC as a feasible alternative to QS. We also remark that in the long-distance regime both $K_{\rm id}$ and $K_p$ ($p = \mathrm{QS}, \mathrm{SPC}$) are proportional to the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [53]

$$K_{\rm max} = -\log_2[(1-T)T^{n_\varepsilon}] - G(n_\varepsilon), \tag{26}$$

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

Furthermore, in Fig. 7 we report the optimized parameters $V_{\rm opt}^{(p)}$ and $g_{\rm opt}^{(p)}$. The modulation $V_{\rm opt}^{(p)}$ has a different behavior with respect to Sec. IV A, being an $\varepsilon$-dependent growing function of $d$. In contrast, the modulations of the original and the ideal NLA-assisted protocols are decreasing functions of $d$ converging to an asymptotic value not depending on $\varepsilon$, as for the case of fixed $g$. Instead, the optimized gains $g_{\rm opt}^{\rm (id)}$ and $g_{\rm opt}^{(p)}$ grow exponentially with $d$ in the long-distance regime. However, if $\varepsilon = 0$ this exponential scaling is not reached yet for the physical NLAs within the considered range of distances $d \leqslant 500$ km.

Finally, in Fig. 6(b) we plot the MTENs as a function of $d$. Differently from Sec. IV A, the MTEN associated with the physical NLAs, namely, $\varepsilon_{\rm max}^{(p)}$, do not achieve the performance of the ideal one $\varepsilon_{\rm max}^{\rm (id)}$. Actually, both these MTENs outperform the original protocol and saturate to a value $\varepsilon_\infty$ as $\kappa d \gg 1$. However, the saturation value of the physical NLAs, namely, $\varepsilon_\infty^{(p)} \approx 0.04$, is lower than the ideal NLA one, that is, $\varepsilon_\infty^{\rm (id)} \approx 0.1$ (see Fig. 6). The numerical results also show that a quantum efficiency $\eta \leqslant 1$ does not affect the value of $\varepsilon_\infty^{(p)}$, consistently with the previous findings.

The difference between ideal and physical NLAs emerges by expanding the CM (21) 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 $g_{\rm opt}^{(p)} \gg 1$, and neglecting the other terms

$$V_p(V, g) \approx V + \delta V_p, \tag{27a}$$

$$W_p(V, g) \approx T_p[V_p(V, g) + \chi_p], \tag{27b}$$

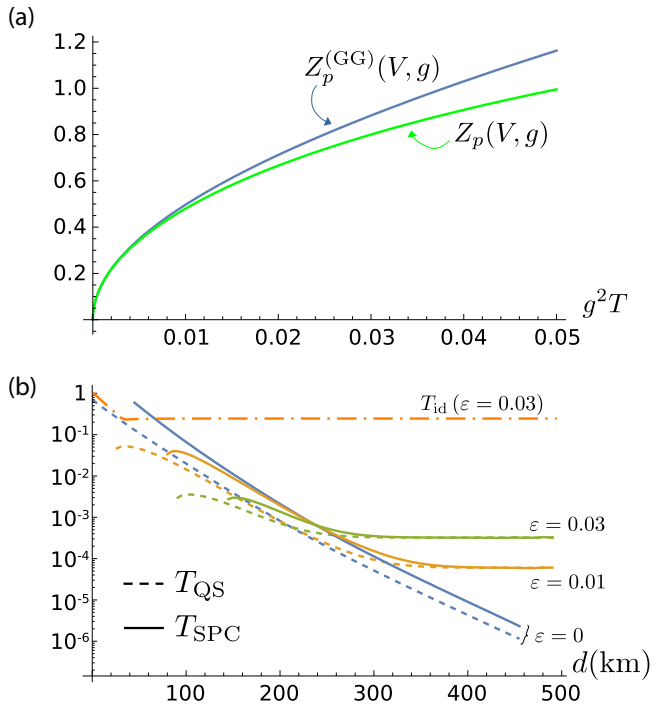


FIG. 8. (a) Plot of $Z_p(V,g)$ and $Z_p^{(\mathrm{GG})}(V,g)$ ($p=\mathrm{QS},\mathrm{SPC}$) as functions of $g^2T$ for $\varepsilon=0.03$ and $V=4$. (b) Logarithmic plot of the effective transmissivity $T_p$ ($p=\mathrm{QS},\mathrm{SPC}$) as a function of the distance $d$ in kilometers for different values of excess noise $\varepsilon$. The plot is only for distances such that $K_p>0$. In both figures we set $\beta=0.95$ and $\eta=1$.

$$Z_p(V,g)\approx\frac{T_p}{\sqrt{g^2T}}Z,\quad (p=\mathrm{QS},\mathrm{SPC}),\tag{27c}$$

where $\delta V_p=T_pZ^2/2$, $T_p$ represents the effective transmissivity

$$T_p=\frac{g^2T}{1+g^2T(V+\varepsilon-1)/2},\tag{28}$$

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

$$\varepsilon_p=\varepsilon-\delta V_p.\tag{29}$$

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

$$Z_p^{(\mathrm{GG})}(V,g)=\sqrt{T_p[V_p(V,g)^2-1]},\tag{30}$$

but rather

$$Z_p(V,g)\leqslant Z_p^{(\mathrm{GG})}(V,g),\tag{31}$$

as depicted in Fig. 8(a). We have $Z_p(V,g)\approx Z_p^{(\mathrm{GG})}(V,g)$ only if $g^2T\ll1$. 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 $g_{\mathrm{opt}}^{(\mathrm{id})}$ and $g_{\mathrm{opt}}^{(p)}$ for the ideal and physical NLAs, respectively, such that the product $g^2T$ is kept constant for $\kappa d\gg1$. Consequently, the effective transmissivities $T_{\mathrm{id}}$ and $T_p$ saturate, as shown in Fig. 8(b). In turn, also the mutual information and the Holevo information saturate and the corresponding KGRs (16) and (23) turn out to be proportional only to the success probability of the NLAs, namely,

$$K_{\mathrm{id}}\propto\frac{1}{(g_{\mathrm{opt}}^{(\mathrm{id})})^2}\propto T\tag{32}$$

and

$$K_p\propto P_p\approx\frac{\eta T}{2T_p}[1+T_p(V_p+\chi_p)],\tag{33}$$

with $P_p=P_p(V_{\mathrm{opt}}^{(p)},g_{\mathrm{opt}}^{(p)})$ and $V_p=V_p(V_{\mathrm{opt}}^{(p)},g_{\mathrm{opt}}^{(p)})$, decreasing linearly with $T$ and thus guaranteeing $K_p>0$ for $\kappa d\gg1$. The same linear scaling is achieved by the PLOB bound if $T\ll1$,

$$K_{\max}\approx T\frac{2-\varepsilon[1-\ln(\varepsilon/2)]}{2\ln2},\tag{34}$$

which proves both NLA-assisted protocols to be nearly optimal. Furthermore, as in Sec. IV A, a quantum efficiency $\eta\leqslant1$ 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 $\varepsilon_p$ is small we have $T_p\ll1$ and the physical NLA-assisted protocols approximate a GG protocol with the effective channel parameters $T_p$ and $\varepsilon_p$. By increasing the excess noise further, we have $T_p\ll1$ and $Z_p(V,g)\leqslant Z_p^{(\mathrm{GG})}(V,g)$ and the state shared between Alice and Bob is less correlated and the protocol deviates more and more from GG. This implies the reduced asymptotic maximum tolerable excess noise with respect to the ideal case.

## V. CONCLUSION

In this paper we have addressed the exploitation of NLAs to achieve long-distance CV QKD in the presence of a nonunit 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, employing a NLA increases the maximum transmission distance by $20\log_{10}g/\kappa$, whereas in the latter NLAs allow us to reach arbitrary large distances, provided the excess noise of the channel is sufficiently low. Furthermore, we have proved both physical NLA-assisted protocols to be robust if $\eta\leqslant1$, 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 [54–56].

## ACKNOWLEDGMENTS

We thank M. G. A. Paris for useful comments. This work was partially supported by the Ministry of Foreign Affairs and International Cooperation (MAECI) through Project ENYGMA, No. PGR06314, and by University of Milan through Project S-O PhoQuLis, No. RV-PSR-SOE-2020-SOLIV.


## 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 protocol we exploit the phase-space formalism [42,46]. We consider an $n$-mode bosonic system, described by the bosonic operators $a_k$ satisfying the canonical commutation relations $[a_k, a_l] = 0$ and $[a_k, a_l^\dagger] = \delta_{kl}$ and by the quadrature operators

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

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

### 1. Quantum states

According to Glauber's formula [42,46], any $n$-mode quantum state of radiation $\rho$ is written

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

where $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^\mathsf{T} \in \mathbb{C}^n$ and

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

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

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

Some useful properties of the displacement operator are

$$D_{\mathbf{a}}(\boldsymbol{\alpha}_1) D_{\mathbf{a}}(\boldsymbol{\alpha}_2) = D_{\mathbf{a}}(\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2), \quad \boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \in \mathbb{C}^n, \tag{A5a}$$

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

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

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

Finally, the function

$$\chi(\boldsymbol{\alpha}) = \mathrm{Tr}[\rho D_{\mathbf{a}}(\boldsymbol{\alpha})] \tag{A6}$$

is the characteristic function associated with $\rho$. In particular, a quantum state $\rho_G$ exhibiting a Gaussian characteristic function is said to be a Gaussian state, namely,

$$\chi(\boldsymbol{\alpha}) = \exp\left(-\tfrac{1}{2}\tilde{\boldsymbol{\alpha}}^\mathsf{T} \boldsymbol{\sigma} \tilde{\boldsymbol{\alpha}} - i\tilde{\boldsymbol{\alpha}}^\mathsf{T} \mathbf{X}\right), \tag{A7}$$

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

$$\mathbf{X} = \mathrm{Tr}(\rho_G \mathbf{r}) \tag{A8}$$

is the first moment vector, and

$$\boldsymbol{\sigma} = \tfrac{1}{2}\mathrm{Tr}[\rho_G\{(\mathbf{r} - \mathbf{X}), (\mathbf{r} - \mathbf{X})^\mathsf{T}\}] \tag{A9}$$

is the $2n \times 2n$ covariance matrix (CM) where $\{A, B\} = AB + BA$ is the anticommutator 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 $\mathcal{O}_1$ and $\mathcal{O}_2$ acting on the Hilbert space of $n$ modes the trace rule holds:

$$\mathrm{Tr}(\mathcal{O}_1 \mathcal{O}_2) = \int \frac{d^2\boldsymbol{\alpha}}{\pi^n} \chi_{\mathcal{O}_1}(\boldsymbol{\alpha}) \chi_{\mathcal{O}_2}(-\boldsymbol{\alpha}). \tag{A10}$$

Here $\chi_{\mathcal{O}_{1\,(2)}}(\alpha)$ is the characteristic function of $\mathcal{O}_{1\,(2)}$. As an example, for a single radiation mode $a$, we choose $\mathcal{O}_1 = D_a(\alpha)$ and $\mathcal{O}_2 = q_a^2 = (a + a^\dagger)^2$ and obtain [36]

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

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 $n_A$ an $n_B$ modes, respectively. In the vector notation we have $\mathbf{a} = (\mathbf{a}_A, \mathbf{a}_B)$. We consider a bipartite quantum state $\rho_{AB}$ with characteristic functions $\chi_{AB}(\boldsymbol{\alpha}) = \chi_{AB}(\boldsymbol{\alpha}_A, \boldsymbol{\alpha}_B)$. We now perform a quantum measurement on subsystem $B$, described my means of the positive-operator-valued measurement (POVM) $\{\Pi_{\mathbf{r}_m}\}_{\mathbf{r}_m}$, whose effects are associated with the characteristic function $\chi_{\mathbf{r}_m}(\boldsymbol{\alpha}_B)$. By applying the trace rule, the conditional state on $A$ reads

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

where

$$\chi_{A|\mathbf{r}_m}(\boldsymbol{\alpha}_A) = \int \frac{d^2\boldsymbol{\alpha}_B}{\pi^{n_B}} \chi_{AB}(\boldsymbol{\alpha}_A, \boldsymbol{\alpha}_B)\chi_{\mathbf{r}_m}(-\boldsymbol{\alpha}_B) \tag{A13}$$

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

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

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

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\sigma}_A & \boldsymbol{\sigma}_{AB} \\ \boldsymbol{\sigma}_{AB}^\mathsf{T} & \boldsymbol{\sigma}_B \end{pmatrix}. \tag{A15}$$

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 $\boldsymbol{\sigma}_m$. Then the conditional state $\rho_{A|\mathbf{r}_m}$ is still a Gaussian state with CM $\boldsymbol{\sigma}_{A|\mathbf{r}_m}$ and first moment vector $\mathbf{X}_{A|\mathbf{r}_m}$ given by [42,46]

$$\boldsymbol{\sigma}_{A|\mathbf{r}_m} = \boldsymbol{\sigma}_A - \boldsymbol{\sigma}_{AB}(\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_m)^{-1}\boldsymbol{\sigma}_{AB}^{\mathsf{T}} \tag{A16}$$

and

$$\mathbf{X}_{A|\mathbf{r}_m} = \mathbf{X}_A + \boldsymbol{\sigma}_{AB}(\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_m)^{-1}(\mathbf{r}_m - \mathbf{X}_B), \tag{A17}$$

respectively.

## APPENDIX B: SECURITY PROOF OF THE GG PROTOCOL

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

$$K = \beta I_{AB} - \chi_{BE}, \tag{B1}$$

with $\beta$ 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 $\mathcal{N}(\mu, \boldsymbol{\sigma})$ with prime moments $\mu$ and CM $\boldsymbol{\sigma}$,

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

is equal to

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

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

$$\chi_{BE} = S_E - S_{E|B}, \tag{B4}$$

which 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 $\rho_{ABE}$ shared by Alice, Bob, and Eve is pure [39,40]. As a consequence, we have

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

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $d_{1\,(2)}$ are the symplectic eigenvalues of $\Gamma_{AB}$ [42,46]. 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 and thus

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

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

$$\Gamma_{A|B} = \Gamma_A - \Gamma_Z\left(\Gamma_B + \boldsymbol{\sigma}_B^{(\mathrm{m})}\right)^{-1}\Gamma_Z^{\mathsf{T}}, \tag{B7}$$

which is independent of the particular outcome obtained.

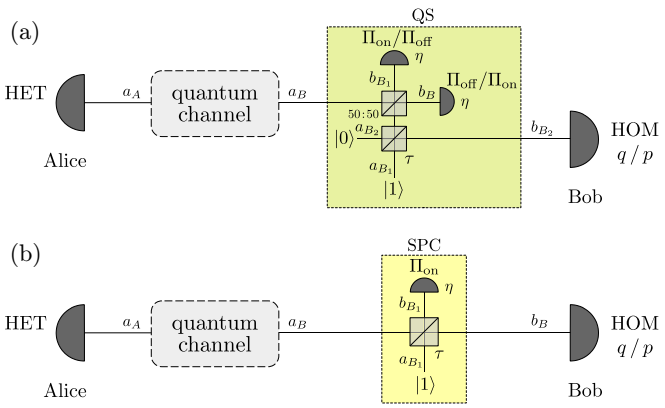


FIG. 9. Schematic representation of the two physical NLA-assisted protocol discussed in the paper: strategy based on (a) quantum scissors and (b) single-photon catalysis.

## APPENDIX C: EMPLOYING QUANTUM SCISSORS AND SINGLE-PHOTON CATALYSIS

As discussed in the main text, we perform the security analysis by exploiting the optimality of Gaussian attacks [50–52]. If Alice and Bob share a non-Gaussian state $\rho$, a lower bound of the exact KGR is obtained by considering a Gaussian protocol in which they share the Gaussian state $\rho_{\mathrm{G}}$ with the same CM of $\rho$. In this Appendix we derive the CM for both the physical noiseless linear amplifiers discussed in the paper, namely, the quantum scissors and the single-photon catalysis. To do so, we exploit the input-output formalism and the phase-space representation of quantum states.

### 1. Quantum scissors

By following the notation introduced in Fig. 9(a), the protocol employing QS works as follows [36]. 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 $\mathbf{a} = (a_A, a_B, a_{B_1}, a_{B_2})^{\mathsf{T}}$, where $a_A$ and $a_B$ are the modes shared by Alice and Bob after the channel and $a_{B_1}$ and $a_{B_2}$ are the modes exploited locally by Bob for the QS. The global input state reads

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

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

$$\chi_{\mathbf{a}}(\boldsymbol{\alpha}) = \chi_{\mathrm{G}}(\alpha_A, \alpha_B)(1 - |\alpha_{B_1}|^2)e^{-(|\alpha_{B_1}|^2 + |\alpha_{B_2}|^2)/2}, \tag{C2}$$

with $\chi_{\mathrm{G}}(\alpha_A, \alpha_B)$ 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 $\mathbf{b} = (b_A, b_B, b_{B_1}, b_{B_2})^{\mathsf{T}} = \mathscr{M}_{\mathrm{QS}}\mathbf{a}$, where

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

with $\tau = \tau_{\rm QS}(g) = (1+g^2)^{-1}$. The output state then is written

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

where, exploiting the properties in Eq. (A5), $\chi_{\mathbf{b}}(\boldsymbol{\beta}) = \chi_{\mathbf{a}}(\mathscr{M}_{\rm QS}^{\mathsf{T}}\boldsymbol{\alpha})$.

Finally, Bob performs on-off detection on modes $b_B, b_{B_1}$, corresponding to the POVM $\{\Pi_{\rm off}, \Pi_{\rm on} = \mathbb{1} - \Pi_{\rm off}\}$, with associated characteristic functions [46,57]

$$\chi_{\rm off}(\alpha) = \frac{1}{\eta} e^{-[(2-\eta)/2\eta]|\alpha|^2}, \tag{C5a}$$

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

The amplification is successful if one of the two detectors gives the outcome "on" [18,36]. In the following we assume to retrieve the couple (on and off), respectively for modes $b_B$ and $b_{B_1}$. The postselected state is then equal to

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

where

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

and

$$\tilde{P}_{\rm QS} = {\rm Tr}\left( \int \frac{d^2\beta_A}{\pi} \frac{d^2\beta_{B_2}}{\pi} \chi_{\rm QS}(\beta_A, \beta_{B_2}) D_{b_A}(\beta_A)^\dagger D_{b_{B_2}}(\beta_{B_2})^\dagger \right) = \chi_{\rm QS}(0,0) = 2\frac{8\eta\tau + (w-1)(3+w)(1+\eta\tau)}{(1+w)^2(3+w)^2} \tag{C8}$$

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 and on); thus the global success probability of the QS-based NLA is $P_{\rm QS} = 2\tilde{P}_{\rm QS}$.

Finally, we compute the CM associated with the state $\rho_{\rm QS}$. By exploiting Eq. (A11), we have

$$V_{\rm QS} = {\rm Tr}\left(\rho_{\rm QS} q_{b_A}^2\right) = -1 - \frac{\mathscr{V}_{\rm QS}}{\tilde{P}_{\rm QS}}, \tag{C9a}$$

$$W_{\rm QS} = {\rm Tr}\left(\rho_{\rm QS} q_{b_{B_2}}^2\right) = -1 - \frac{\mathscr{W}_{\rm QS}}{\tilde{P}_{\rm QS}}, \tag{C9b}$$

$$Z_{\rm QS} = {\rm Tr}\left(\rho_{\rm QS} q_{b_A} q_{b_{B_2}}\right) = -\frac{\mathscr{Z}_{\rm QS}}{\tilde{P}_{\rm QS}}, \tag{C9c}$$

where

$$\mathscr{V}_{\rm QS} = \left(\frac{d^2}{dy^2}[e^{-y^2/2}\chi_{\rm QS}(iy,0)]\right)_{y=0} = 2(V+1)\left(\frac{(2+\eta T\varepsilon)(1-\eta\tau)}{(1+w)^2} - \frac{8(3+w) + 2\eta T\varepsilon(3+w-4\eta\tau) + 4\eta\tau(w-5)}{(3+w)^3}\right), \tag{C10a}$$

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

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

Accordingly, the CM is written

$$\Gamma_{AB}^{\rm (QS)} = \begin{pmatrix} V_{\rm QS}\mathbb{1}_2 & Z_{\rm QS}\boldsymbol{\sigma}_z \\ Z_{\rm QS}\boldsymbol{\sigma}_z & W_{\rm QS}\mathbb{1}_2 \end{pmatrix}. \tag{C11}$$

### 2. Single-photon catalysis

For SPC we follow the analogous procedure of the preceding section. The input modes depicted in Fig. 9(b) are $\mathbf{a} = (a_A, a_B, a_{B_1})^{\mathsf{T}}$, where $a_A$ and $a_B$ 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

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

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

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

with $\chi_{\rm G}(\alpha_A, \alpha_B)$ 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 $\mathbf{b} = (b_A, b_B, b_{B_1})^{\mathsf{T}} = \mathscr{M}_{\rm SPC}\mathbf{a}$, where

$$\mathscr{M}_{\rm SPC} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\tau} & \sqrt{1-\tau} \\ 0 & -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix}, \tag{C14}$$

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

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

where

$$\chi_{\mathbf{b}}(\boldsymbol{\beta}) = \chi_{\mathbf{a}}\left(\mathscr{M}_{\rm SPC}^{\mathsf{T}}\boldsymbol{\alpha}\right). \tag{C16}$$

After the conditional on-off detection on mode $b_{B_1}$, the postselected state reads

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

where

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

and

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

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 $\rho_{\mathrm{SPC}}$ reads

$$\Gamma_{AB}^{(\mathrm{SPC})}=\begin{pmatrix}V_{\mathrm{SPC}}\mathbb{1}_2 & Z_{\mathrm{SPC}}\boldsymbol{\sigma}_z\\ Z_{\mathrm{SPC}}\boldsymbol{\sigma}_z & W_{\mathrm{SPC}}\mathbb{1}_2\end{pmatrix}. \tag{C20}$$

As for QS, we have

$$V_{\mathrm{SPC}}=\mathrm{Tr}\left(\rho_{\mathrm{QS}}q_{b_A}^2\right)=-1-\frac{\mathcal{V}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}}, \tag{C21}$$

$$W_{\mathrm{SPC}}=\mathrm{Tr}\left(\rho_{\mathrm{QS}}q_{b_B}^2\right)=-1-\frac{\mathcal{W}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}}, \tag{C22}$$

$$Z_{\mathrm{SPC}}=\mathrm{Tr}(\rho_{\mathrm{QS}}q_{b_A}q_{b_B})=-\frac{\mathcal{Z}_{\mathrm{SPC}}}{P_{\mathrm{SPC}}} \tag{C23}$$

and

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

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

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

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. **77**, 513 (2005).

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

[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **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, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[7] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).

[8] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photon. **12**, 1012 (2020).

[9] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, *Proceedings of the IEEE International Symposium on Information Theory, Seattle, 2006* (IEEE, Piscataway, 2006), pp. 1179–1183.

[10] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303(R) (2005).

[11] M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini, arXiv:2211.05688.

[12] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).

[13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[14] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Phys. Rev. Lett. **125**, 010502 (2020).

[15] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, Opt. Lett. **48**, 1766 (2023).

[16] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, arXiv:2302.02391.

[17] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, arXiv:2305.08156.

[18] T. C. Ralph and A. P. Lund, in *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing, Calgary, 2008*, edited by A. Lvovsky, AIP Conf. Proc. No. 1110 (AIP, Melville, 2009), pp. 155–160.

[19] T. C. Ralph, Phys. Rev. A **84**, 022339 (2011).

[20] H. Adnane, B. Teklu, and M. G. A. Paris, J. Opt. Soc. Am. B **36**, 2938 (2019).

[21] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[22] J. Fiurášek, Phys. Rev. A **80**, 053822 (2009).
[23] G.-Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).
[24] N. A. McMahon, A. P. Lund, and T. C. Ralph, Phys. Rev. A **89**, 023846 (2014).
[25] S. Zhang and X. Zhang, Phys. Rev. A **97**, 043830 (2018).
[26] M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, Phys. Rev. A **102**, 063715 (2020).
[27] J. Fiurášek, Opt. Express **30**, 1466 (2022).
[28] J. J. Guanzon, M. S. Winnel, A. P. Lund, and T. C. Ralph, Phys. Rev. Lett. **128**, 160501 (2022).
[29] J. Fiurášek, Phys. Rev. A **105**, 062425 (2022).
[30] J. J. Guanzon, M. S. Winnel, A. P. Lund, and T. C. Ralph, arXiv:2211.08035.
[31] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Nat. Photon. **8**, 333 (2014).
[32] J. Fiurášek and N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).
[33] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Phys. Rev. A **87**, 020303(R) (2013).
[34] J. Bernu, S. Armstrong, T. Symul, T. C. Ralph, and P. K. Lam, J. Phys. B **47**, 215503 (2014).
[35] J. Zhao, J. Y. Haw, T. Symul, P. K. Lam, and S. M. Assad, Phys. Rev. A **96**, 012319 (2017).
[36] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, IEEE J. Sel. Top. Quantum Electron. **26**, 1 (2020).
[37] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, IEEE J. Sel. Areas Commun. **38**, 506 (2020).
[38] L. Hu, M. Al-amri, Z. Liao, and M. S. Zubairy, Phys. Rev. A **102**, 012608 (2020).
[39] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[40] 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).
[41] S. Olivares, Phys. Lett. A **418**, 127720 (2021).
[42] S. Olivares, Eur. Phys. J. Spec. Top. **203**, 3 (2012).
[43] A. Yoshizawa and H. Tsuchida, Appl. Phys. Lett. **85**, 2457 (2004).
[44] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, Phys. Rev. Lett. **94**, 053601 (2005).
[45] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, npj Quantum Inf. **5**, 46 (2019).
[46] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).
[47] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[48] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[49] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[50] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[51] A. Leverrier, Ph.D. thesis, Télécom ParisTech, 2009.
[52] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[53] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[54] F. Furrer and W. J. Munro, Phys. Rev. A **98**, 032335 (2018).
[55] S. Pirandola, Commun. Phys. **2**, 51 (2019).
[56] J. Dias, M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, Phys. Rev. A **102**, 052425 (2020).
[57] S. Olivares and M. G. Paris, J. Opt. B **7**, S616 (2005).