New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

Continuous-variable quantum key distribution over multispan links employing phase-insensitive and phase-sensitive amplifiers

To cite this article: M N Notarnicola *et al* 2024 *New J. Phys.* **26** 043015

IOP Publishing New J. Phys. 26 (2024) 043015 https://doi.org/10.1088/1367-2630/ad3774

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
29 September 2023

REVISED
18 March 2024

ACCEPTED FOR PUBLICATION
25 March 2024

PUBLISHED
18 April 2024

PAPER

Continuous-variable quantum key distribution over multispan links employing phase-insensitive and phase-sensitive amplifiers

M N Notarnicola[1], F Cieciuch[2] and M Jarzyna[3,*]

[1] Dipartimento di Fisica 'Aldo Pontremoli', Università degli Studi di Milano and INFN Sezione di Milano, via Celoria 16, I-20133 Milano, Italy
[2] Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warszawa, Poland
[3] Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warszawa, Poland
[*] Author to whom any correspondence should be addressed.

E-mail: m.jarzyna@cent.uw.edu.pl and michele.notarnicola@unimi.it

Keywords: continuous-variable quantum key distribution, multi-span links, optical amplifiers, wiretap channel

Abstract

Transmission losses through optical fibers are one of the main obstacles preventing both long-distance quantum communications and continuous-variable quantum key distribution. Optical amplification provides a tool to obtain, at least partially, signal restoration. In this work, we address a key distribution protocol over a multi-span link employing either phase-insensitive (PIA) or phase-sensitive (PSA) amplifiers, considering Gaussian modulation of coherent states followed by homodyne detection at the receiver's side. We perform the security analysis under both unconditional and conditional security frameworks by assuming in the latter case only a single span of the whole communication link to be untrusted. We compare the resulting key generation rate (KGR) for both kinds of amplified links with the no-amplifier protocol, identifying the enhancement introduced by optical amplification. We prove an increase in the KGR for the PSA link in the unconditional scenario and for both PSA and PIA in the conditional security setting depending on position of the attack and the measured quadrature.

1. Introduction

Thanks to the quantum key distribution (QKD) [1–3] it is possible to distill a random secure key between a sender (Alice) and a receiver (Bob), communicating via an untrusted quantum channel under the control of an eavesdropper (Eve). Generally speaking, QKD protocols may be divided into two branches: discrete-variable QKD, in which qubit states are exchanged [4–7], and continuous-variable QKD (CV-QKD), exploiting the quadratures of a quantum optical field [8, 9]. In particular, CV-QKD provides a powerful resource as it exploits coherent states of radiation and quadrature measurements [10], thus being compatible with both the modulation and detection systems already employed in standard fiber-optical communications [11].

The milestone of CV-QKD is represented by the GG02 protocol, originally proposed by Grosshans and Grangier [8, 9, 12–14], in which Alice generates coherent states by sampling a Gaussian distribution and Bob randomly implements a homodyne detection of one of the two orthogonal quadratures of the field. Later, a no-switching scheme where the single quadrature measurement is replaced by double homodyne detection has also been proposed [15]. The GG02 protocol has been widely analyzed in the *unconditional security* framework [9], exploiting the optimality of Gaussian attacks [16–18]. In this approach one considers the most general attack allowed by the laws of quantum mechanics, which requires the eavesdropper to possess a quantum computer-like machinery and perform any collective unitary and detection operations on many time slots. In practice, however, one can often restrict the attacks to a reasonable smaller class, either assuming a limited power by the eavesdropper or some level of trust in the infrastructure. For example, in satellite QKD a typical attack consists of detecting some part of the signal that is not captured by Bob's telescope [19]. Similarly, for the fiber based protocols it is reasonable to assume that an attack is performed on just a single section of the fiber and that attacker cannot easily gain access to the whole cable. For these reasons, more recently, the interest has been directed to the *conditional security* approach, in which every setup component is associated with a different trust level [20]. Moreover, towards a practical description, within the framework of conditional security there have also been included realistic assumptions on the feasible experimental setups, such as wiretap channels [21–23] and restricted eavesdropping [21].

Above all, in CV-QKD a crucial factor restricting security of long-distance secure communication is provided by channel losses. Indeed, a canonical model for optical fibers is provided by the thermal-loss channel, in which the channel transmissivity is exponentially decaying with the transmission distance [24–26]. To compensate transmission losses and restore the signal, one can employ optical amplifiers [27–29] and consider a multi-span link, that is, a periodic array of amplifiers connected by many independent thermal-loss channels. So far, multi-span links have been investigated with the intent of increasing channel capacity [30–33], showing that both phase-insensitive amplifiers (PIAs) [32] and phase-sensitive amplifiers (PSAs) [33] induce an exponential enhancement of the ultimate capacity being more appreciable for short-distance communication. In the context of CV-QKD heralded noiseless linear amplification [34–37] and quantum repeaters [38–40] have been widely considered. These provide innovative solutions, but are technologically challenging and far from a direct large-scale implementation. In contrast, the role of optical amplifiers has been investigated to compensate for detection imperfections [41], raising the question on their possible application to the channel losses mitigation task.

In this paper, we address the problem of performing CV-QKD over a multi-span link. We maintain the same modulation and detection schemes of GG02, that is, a Gaussian modulation of coherent states and homodyne detection, but replace the single thermal-loss channel of the original proposals with a multi-span link of M spans connected via either PIAs or PSAs. In particular we compare three different cases: a PIA link with random homodyne detection of one of the two orthogonal field quadratures and a PSA link with homodyne detection of either the amplified or de-amplified quadrature. We compute the key generation rate (KGR), i.e. the length of the secret key per unit time slot, in both the unconditional and the conditional security approaches. In the former scenario, we prove that unconditional security is improved in particular regimes only by PSA links followed by homodyne measurement of the de-amplified quadrature. On the other hand, we also address conditional security under restricted eavesdropping: we assume trusted amplifiers and only a single untrusted span among the whole M ones composing the link. This assumption provides a simplified picture to identify the more vulnerable points of the fiber link. We compare the three discussed cases and show that amplification is helpful if the untrusted node is placed either at the beginning or the end of the link, according to the particular employed amplifier and measured quadrature. In the unconditional security framework, we prove an increase in the KGR only for a PSA link where Bob homodynes the de-amplified quadrature and a lack of thereof for the measurement of the amplified quadrature. On the contrary, under conditional security assumption, we distinguish two different cases. For PIA or PSA link with homodyne measurement of the amplified quadrature, we obtain an enhancement of the KGR when Eve attacks one of the first spans, whereas for PSA links and measurement of the de-amplified quadrature, the enhancement appears when the attacked span is in the latter part of the link. Finally, we briefly discuss the case in which Alice and Bob achieve the ultimate capacity limits discussed in [30–33]. This provides us with the ultimate enhancement in the KGR brought by the links under investigation. We focus on the PIA link case and show that, even in this case, the advantages of PIA disappear as the location of attack nodes increases.

The structure of the paper is the following. In section 2 we present the structure of the multi-span links under investigation. Then, in sections 3 and 4 we perform the security analysis under unconditional and conditional security paradigms, respectively, assuming a single untrusted span. Thereafter, in section 5 we consider the ultimate limits obtained when Alice and Bob achieve the quantum channel capacity while in section 6 we speculate about the impact of PSAs at the modulation stage of the protocol to further enhance CVQKD. Finally, in section 7 we draw the final conclusions and summarize the obtained results.

2. Multi-span amplified links

In this work, we address the application of multi-span links employing optical amplifiers for CV-QKD. In particular, we employ the quantum amplifiers depicted in figure 1. We consider an incoming optical mode a, satisfying $[a, a^\dagger] = 1$, and its associated quadrature operators

$$q = \sigma_0 \left(a + a^\dagger\right) \quad \text{and} \quad p = \mathrm{i}\sigma_0 \left(a^\dagger - a\right) , \tag{1}$$

with $[q, p] = 2\mathrm{i}\sigma_0^2$ and σ_0^2 being the shot-noise variance [10]. Throughout the work we will always consider shot-noise units, namely $\sigma_0^2 = 1$. The goal is to amplify the mode a by a gain factor G. The PIA, see figure 1(a), is implemented by coupling mode a together with an ancillary mode b prepared in the vacuum state $|0\rangle$ and performing a two-mode squeezing operation, namely

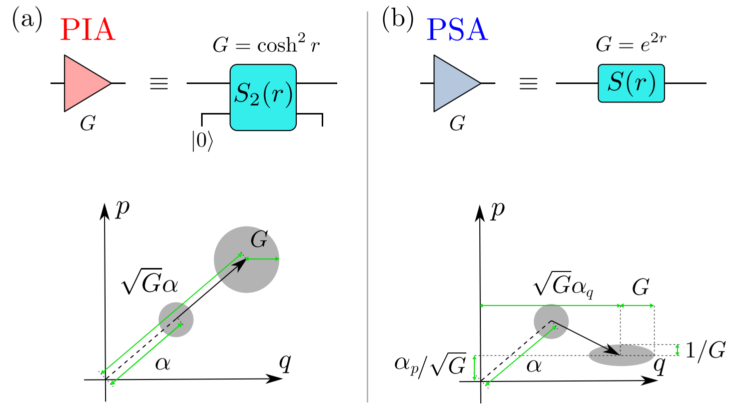

Figure 1. Schemes of the phase-insensitive amplifier (PIA) (a) and phase-sensitive amplifier (PSA) (b) employed throughout the paper. In both the cases the amplification gain G is related to the squeezing parameter r. The PIA applies the same amplification to both quadratures and introduces additional noise while PSA amplifies one of the quadratures and deamplifies the second rescaling the variances accordingly as seen on the example for a coherent state with amplitude $\alpha = \alpha_q + i\alpha_p$.

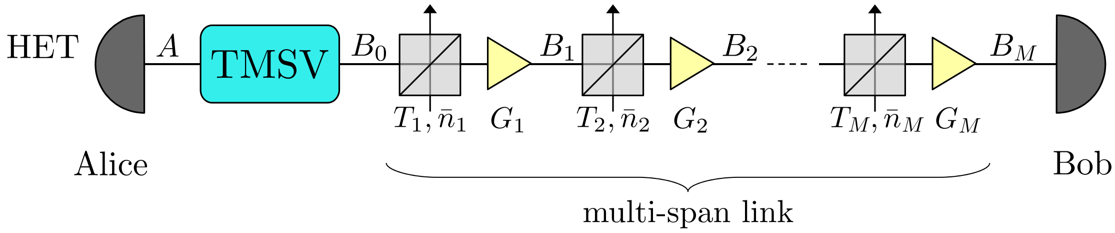

Figure 2. Scheme of the CV-QKD protocol discussed in the present paper. A two mode squeezed vacuum state (TMSV) is distributed between Alice and Bob. Alice performs a heterodyne measurement on her mode, whereas the mode sent to Bob travels through a loss-thermal channel modeled by a series of M beam splitters with transmissivities T_j and added mean thermal number of photons $\bar{n}_j$. In order to counteract losses the signal after each span B_j is amplified by either PIA or PSA with gain G_j. Finally, Bob performs a measurement which we assume to be either case I: a random homodyne detection of quadratures q/p, or homodyne detection of either q, IIa, or p, IIb.

$$S_2(r) = \exp\left[r\left(a^\dagger b^\dagger - ab\right)\right], \tag{2}$$

$r \geqslant 0$ being the squeezing parameter [28, 42]. The original input mode is then transformed into $a \to \sqrt{G}a + \sqrt{G-1}\,b$, with $G = \cosh^2 r$. Thereafter, we trace over mode b, ending up with an amplified signal but at the expense of introducing an ineludible added noise equal to $G-1$ on both quadratures variances. PIAs well describe also amplification by a laser medium without optical feedback from a cavity [28, 43], being of particular interest for systems working at high powers, whereas their application at the quantum level is more limited due to the introduced excess noise [27].

The issue of noise may be circumvented by employing PSAs, see figure 1(b), implemented via a unitary single-mode squeezing operation

$$S(r) = \exp\left\{\frac{r}{2}\left[\left(a^\dagger\right)^2 - a^2\right]\right\}, \tag{3}$$

$r \geqslant 0$ [28, 42]. PSA amplifies the quadrature q by a factor $\sqrt{G} = \exp(r) \geqslant 1$ at the expense of squeezing, i.e. de-amplifying, quadrature p by $1/\sqrt{G} \leqslant 1$. Consequently, the quadrature variances are also amplified and de-amplified by G and $1/G$, respectively. Crucially, the input commutation relations between the quadratures are preserved without introducing any further noise. Note also the important difference between PIA and PSA: the former is a noisy operation requiring the introduction of an additional light mode lost to the environment which, in principle, can be intercepted by a malicious party, whereas the latter amplification scenario assumes unitary evolution which does not leak any information, thus being always trusted.

Given the previous considerations, in figure 2 we present the protocol discussed in the paper. We start from the GG02 scheme in its entanglement-based version [8, 9, 12–14]. That is, Alice has a two-mode squeezed vacuum state (TMSV) with variance $V > 1$, namely

$$|\mathrm{TMSV}\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle, \tag{4}$$

where $\lambda = \sqrt{(V-1)/(V+1)}$ and $|n\rangle$ being the Fock state with n photons [10]. She injects the second branch into the quantum channel while performing heterodyne detection, equivalent to double homodyne, on the remaining mode, such that the conditional state sent to Bob is a coherent state. Ultimately, Bob performs a homodyne measurement on the received pulses, which in the former version of GG02 consists of a random homodyne detection of either q or p quadratures [8, 14].

Unlike in the standard GG02 protocol, the quantum channel discussed in this work consists of a multi-span link with M spans alternated by optical amplifiers. Each span $j = 1,\dots,M$ is modeled as an independent thermal-loss channel with transmissivity $T_j \leqslant 1$ and excess noise $\epsilon_j \geqslant 0$. More precisely, the optical mode entering the jth link is mixed at a beam splitter with transmissivity T_j with a thermal state having $\bar{n}_j = T_j\epsilon_j/[2(1-T_j)]$ mean number of photons [10]. Thereafter, the radiation undergoes optical amplification, either phase-insensitive or phase-sensitive, before being injected into the $(j+1)$-th span. For simplicity, here we assume both identical and equally spaced amplifiers, such that all spans have the same transmissivity $T_j = T$, added thermal noise $\bar{n}_j = \bar{n}_T$ and amplification gain $G_j = G$. Note, however, that this choice may not be the optimal arrangement [32]. Then, if the total transmission distance is L, two neighboring amplifiers are spaced by L/M and we have

$$T = 10^{-\kappa L/(10M)}\,, \tag{5}$$

$\kappa = 0.2$ dB/km being the typical loss rate of standard optical fibers [24–26]. Moreover, we assume the added thermal photons in each span to be equal to

$$\bar{n}_T = \frac{T^M\epsilon}{2\,(1-T^M)}\,. \tag{6}$$

With these choices, in the absence of optical amplification, that is $G = 1$, we retrieve the standard GG02 scenario, that is a single-span thermal-loss channel with total transmissivity $T_\mathrm{n} = T^M$ and added noise $N_\mathrm{n} = (1-T_\mathrm{n})/T_\mathrm{n} + \epsilon$, $\epsilon \geqslant 0$ being the total excess noise [9, 14].

Starting from the scheme in figure 2, we address three different cases, differing from one another by both the employed amplifier and the measurement implemented by Bob:

- Case I: PIA link and random homodyne detection of quadratures q/p,
- Case IIa: PSA link and homodyne detection of quadrature q, namely the anti-squeezed quadrature,
- Case IIb: PSA link and homodyne detection of quadrature p, namely the squeezed quadrature.

Note that the presence of a PSA link makes the channel phase-sensitive, thus differentiating the behavior of quadratures q and p. Therefore, in the presence of PSAs Bob may perform homodyne detection of a single quadrature for those experimental runs dedicated to key extraction, while homodyning both q and p for the channel evaluation stage, in order to fully characterize the quantum channel [9].

In the following, we compute the KGR for all three cases under both unconditional and conditional security scenarios. To perform the analysis, we adopt the notation introduced in figure 2. At first Alice has two optical modes A and B_0 excited in the TMSV state (4). Then, the mode B_0 is injected into the sequence of M spans. We denote by B_j the optical mode coming out from the jth span and subsequently amplified by the jth amplifier. Finally, we refer to the last output mode as $B = B_M$. We start by computing the mutual information shared between Alice and Bob, addressing the cases I and IIp, $\mathrm{p} = \mathrm{a},\mathrm{b}$, separately. The whole analysis is carried out following the Gaussian formalism, briefly reminded in appendix A.

2.1. Case I : PIA link

The initial state before injection into the channel is a TMSV in modes A and B_0, completely characterized by its covariance matrix (CM)

$$\boldsymbol{\sigma}_{AB_0} = \begin{pmatrix} V\mathbb{1}_2 & Z\boldsymbol{\sigma}_z \\ Z\boldsymbol{\sigma}_z & V\mathbb{1}_2 \end{pmatrix}, \tag{7}$$

where $Z = \sqrt{V^2-1}$, $\mathbb{1}_2$ is a 2×2 identity matrix and $\boldsymbol{\sigma}_z$ is the Pauli z-matrix.

The mode B_0 is injected into the noisy channel, which may be modeled via a sequence of Gaussian completely-positive (CP) maps as derived in appendix B. More specifically, each node is described by a Gaussian CP map associated with the matrices $X^{(\mathrm{I})} = \sqrt{GT}\mathbb{1}_2$ and $Y^{(\mathrm{I})} = [G(1-T)(1+2\bar{n}) + (G-1)]\mathbb{1}_2$, such that the bipartite state on modes AB_j after the j-th span is a Gaussian state with associated CM $\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_j} = (\mathbb{1}_2 \oplus X^{(\mathrm{I})})\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{j-1}}(\mathbb{1}_2 \oplus X^{(\mathrm{I})})^\intercal + (\mathbf{0} \oplus Y^{(\mathrm{I})})$, $\mathbf{0}$ being the null 2×2 matrix. Accordingly, after M nodes applying PIA the state shared between Alice and Bob is still Gaussian with CM

$$\boldsymbol{\sigma}_{AB}^{(\mathrm{I})} = \begin{pmatrix} \boldsymbol{\sigma}_A^{(\mathrm{I})} & \boldsymbol{\sigma}_Z^{(\mathrm{I})} \\ \boldsymbol{\sigma}_Z^{(\mathrm{I})\intercal} & \boldsymbol{\sigma}_B^{(\mathrm{I})} \end{pmatrix} = \begin{pmatrix} a^{(M)}\,\mathbb{1}_2 & z^{(M)}\boldsymbol{\sigma}_z \\ z^{(M)}\boldsymbol{\sigma}_z & b^{(M)}\,\mathbb{1}_2 \end{pmatrix}, \tag{8}$$

where

$$a^{(M)} = V, \tag{9a}$$

$$b^{(M)} = T^{(M)}\left[V + N^{(M)}\right], \tag{9b}$$

$$z^{(M)} = \sqrt{T^{(M)}}\,Z, \tag{9c}$$

and

$$T^{(M)} = (GT)^M, \tag{10a}$$

$$N^{(M)} = \frac{1}{(GT)^{M-1}}\,\frac{1-(GT)^M}{1-GT}\,[N + N_G], \tag{10b}$$

$N = (1-T)(1+2\bar{n}_T)/T$ being the added noise introduced after the passage though a single span due to the channel thermal noise, while $N_G = (G-1)/(GT)$ is the added noise due to the PIA. Consequently, compared to the scenario in the absence of amplifiers, the PIA link is equivalent to a thermal-loss channel with increased transmissivity $T^{(M)} \geqslant T_{\mathrm{n}}$, but also increased added noise $N^{(M)} \geqslant N_{\mathrm{n}}$.

After transmission, Alice performs heterodyne detection on her mode, associated with the CM $\boldsymbol{\sigma}_{\mathrm{het}} = \mathbb{1}_2$, while Bob implements a homodyne detection of either quadrature q or p, referred to as sub-cases a and b, and described by the CMs

$$\boldsymbol{\sigma}_{\mathrm{a}} = \lim_{z\to 0}\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix} \quad \text{and} \quad \boldsymbol{\sigma}_{\mathrm{b}} = \lim_{z\to \infty}\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}, \tag{11}$$

respectively. Due to the symmetry of (8), the resulting statistics for both quadrtures are identical, therefore, we can safely assume that Bob always measures the quadrature q. In turn, the mutual information between Alice and Bob may be obtained directly from (8) as [37]:

$$I_{AB}^{(\mathrm{I})}(V,G) = \frac{1}{2}\log_2\left\{\frac{\det\left[\boldsymbol{\sigma}_A^{(\mathrm{I})} + \boldsymbol{\sigma}_{\mathrm{het}}\right]\det\left[\boldsymbol{\sigma}_B^{(\mathrm{I})} + \boldsymbol{\sigma}_{\mathrm{a}}\right]}{\det\left[\boldsymbol{\sigma}_{AB}^{(\mathrm{I})} + (\boldsymbol{\sigma}_{\mathrm{het}} \oplus \boldsymbol{\sigma}_{\mathrm{a}})\right]}\right\}, \tag{12}$$

where we highlighted the dependence on the free parameters V and G.

2.2. Case II : PSA link

For cases IIp, p = a, b, we follow analogous procedure as in the previous subsection. Now, each node is modeled by a Gaussian CP map with matrices $X^{(\mathrm{II})}$ and $Y^{(\mathrm{II})}$, see appendix B. The shared state on modes AB_j has CM $\boldsymbol{\sigma}_{AB_j}^{(\mathrm{II})} = (\mathbb{1}_2 \oplus X^{(\mathrm{II})})\boldsymbol{\sigma}_{AB_{j-1}}^{(\mathrm{II})}(\mathbb{1}_2 \oplus X^{(\mathrm{II})})^{\intercal} + (\mathbf{0} \oplus Y^{(\mathrm{II})})$, thus ultimately we obtain the CM of the state shared between Alice and Bob as:

$$\boldsymbol{\sigma}_{AB}^{(\mathrm{II})} = \begin{pmatrix} \boldsymbol{\sigma}_A^{(\mathrm{II})} & \boldsymbol{\sigma}_Z^{(\mathrm{II})} \\ \boldsymbol{\sigma}_Z^{(\mathrm{II})\intercal} & \boldsymbol{\sigma}_B^{(\mathrm{II})} \end{pmatrix} = \begin{pmatrix} a^{(M)} & 0 & z_1^{(M)} & 0 \\ 0 & a^{(M)} & 0 & -z_2^{(M)} \\ z_1^{(M)} & 0 & b_1^{(M)} & 0 \\ 0 & -z_2^{(M)} & 0 & b_2^{(M)} \end{pmatrix}, \tag{13}$$

where

$$b_{1(2)}^{(M)} = T_{1(2)}^{(M)}\left[V + N_{1(2)}^{(M)}\right], \tag{14a}$$

$$z_{1(2)}^{(M)} = \sqrt{T_{1(2)}^{(M)}}\,Z, \tag{14b}$$

and

$$T_1^{(M)} = (GT)^M, \qquad T_2^{(M)} = \left(G^{-1}T\right)^M, \tag{15a}$$

$$N_1^{(M)} = \frac{1}{(GT)^{M-1}} \frac{1-(GT)^M}{1-GT} N, \tag{15b}$$

$$N_2^{(M)} = \frac{1}{(G^{-1}T)^{M-1}} \frac{1-(G^{-1}T)^M}{1-G^{-1}T} N, \tag{15c}$$

with $N = (1-T)(1+2\bar{n}_T)/T$.

Unlike case I, the PSA link is a phase-sensitive channel. Indeed, in the presence of PSA, quadrature q exhibits an increased transmissivity $T_1^{(M)} \geqslant T_{\rm n}$ and reduced added noise $N_1^{(M)} \leqslant N_{\rm n}$, whereas quadrature p shows a reduced transmissivity $T_2^{(M)} \leqslant T_{\rm n}$ with increased added noise $N_2^{(M)} \geqslant N_{\rm n}$. As we discuss in the following, under appropriate conditions this allows Bob to hide behind the increased noise to reduce the amount of information intercepted by an eventual eavesdropper. The mutual information for the two sub-cases $\rm p = a, b$ then reads:

$$I_{AB}^{(\rm IIp)}(V,G) = \frac{1}{2}\log_2 \left\{ \frac{\det\left[\boldsymbol{\sigma}_A^{(\rm II)} + \boldsymbol{\sigma}_{\rm het}\right] \det\left[\boldsymbol{\sigma}_B^{(\rm II)} + \boldsymbol{\sigma}_{\rm p}\right]}{\det\left[\boldsymbol{\sigma}_{AB}^{(\rm II)} + \left(\boldsymbol{\sigma}_{\rm het} \oplus \boldsymbol{\sigma}_{\rm p}\right)\right]} \right\}. \tag{16}$$

In the next sections, we will perform a security analysis of the above protocols by considering both the cases of unconditional security, where the entire channel is untrusted, and conditional security, assuming that only a single span is untrusted and may be intercepted by Eve. In both scenarios, we take as a benchmark the security of the associated protocol in the absence of optical amplifiers, referred to as the 'no-amplifier protocol', in which we assume Bob to perform a random homodyne measurement of either quadrature q or p as in GG02. The results of the standard no-amplifier protocol can be retrieved from both cases I and II by fixing $G = 1$.

3. Unconditional security

At first, we analyze the performance of the discussed protocol under the unconditional security approach, where the whole transmission line is supposed to be attacked by Eve. In this framework, all elements of the multi-span link are assumed to be untrusted and the most powerful attack is the so-called purification attack [9, 14]. That is, Eve intercepts all the lost photons, and collects modes associated with the channel noise and purifies the final state shared between Alice and Bob, such that the tripartite system ABE is pure [9]. Under these conditions employing PIAs is useless because Eve would have access also to their purification, denoted by mode b in figure 1(a), and extract more information with respect to the no-amplifier protocol. In contrast, case II is still worth of interest due to the unitarity of phase-sensitive amplification.

Considering reverse reconciliation [9, 14], for the cases IIp, $\rm p = a, b$, the KGR is given by

$$K_u^{(\rm IIp)}(V,G) = \beta I_{AB}^{(\rm IIp)}(V,G) - \chi_{BE}^{(\rm IIp)}(V,G), \tag{17}$$

where $\beta \leqslant 1$ is the reconciliation efficiency and $\chi_{BE}^{(\rm IIp)}(V,G) = S_E - S_{E|B}^{(\rm p)}$ is the Holevo information between Bob and Eve [44], S_E and $S_{E|B}^{(\rm p)}$ being the Von Neumann entropies of Eve's overall state and Eve's conditional state after Bob's measurement, respectively. Due to the purification attack and the fact that Bob's measurement is represented by a 1-rank operator, we have $S_E = S_{AB}$ and $S_{E|B}^{(\rm p)} = S_{A|B}^{(\rm p)}$, where S_{AB} and $S_{A|B}^{(\rm p)}$ are the Von Neumann entropies of Alice and Bob's bipartite state and Alice's conditional state, respectively. These two latter quantities can be retrieved from the CM (13), leading to:

$$\chi_{BE}^{(\rm IIp)}(V,G) = h(d_1) + h(d_2) - h\left(d_3^{(\rm p)}\right), \tag{18}$$

where

$$h(x) = \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right), \tag{19}$$

d_1 and d_2 are the symplectic eigenvalues of (13) and $d_3^{(\rm p)} = \sqrt{\det\left[\boldsymbol{\sigma}_{A|B}^{(\rm IIp)}\right]}$, with

$$\boldsymbol{\sigma}_{A|B}^{(\rm IIp)} = \boldsymbol{\sigma}_A^{(\rm II)} - \boldsymbol{\sigma}_Z^{(\rm II)}\left[\boldsymbol{\sigma}_B^{(\rm II)} + \boldsymbol{\sigma}_{\rm p}\right]^{-1} \boldsymbol{\sigma}_Z^{(\rm II)\mathsf{T}}. \tag{20}$$

In particular, we have:

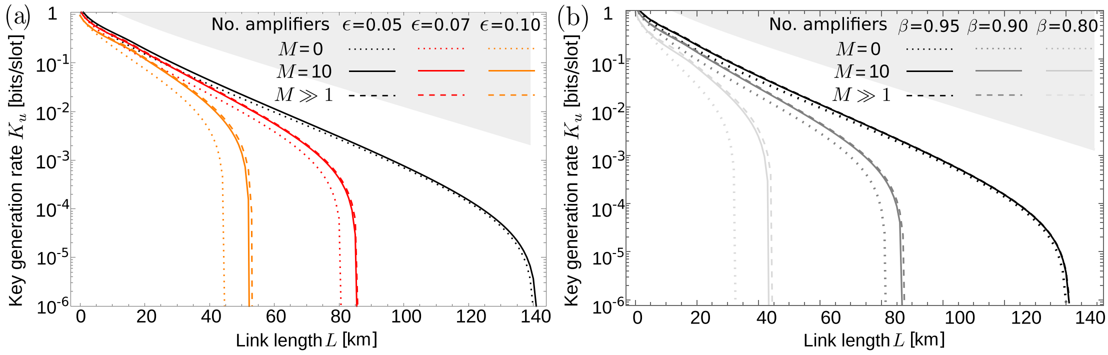

Figure 3. (a) Optimized KGR as a function of the transmission link length L for different level of external noise and number of amplifiers M, with fixed reconciliation efficiency $\beta = 0.95$. (b) Optimized KGR as a function of L for different values of reconciliation efficiency and number of amplifiers M, with fixed channel excess noise $\epsilon = 0.05$. The enhancement introduced by PSAs is accentuated for lower β. The case $M = 0$ refers to the no-amplifier protocol. The gray shaded area represents KGR greater than the PLOB bound.

$$d_3^{(\mathrm{a(b)})} = V\sqrt{1 - \frac{Z^2}{V\left[V + N_{1(2)}^{(M)}\right]}} \,. \tag{21}$$

Finally, we perform optimization over the free parameters—modulation variance V and gain G—obtaining

$$K_u^{(\mathrm{IIp})} = \max_{V,G} K_u^{(\mathrm{IIp})}\left(V,G\right), \qquad (\mathrm{p} = \mathrm{a},\mathrm{b}) \,, \tag{22}$$

subject to the set of constraints $b_1^{(j)} \leqslant V$, see equation (14*a*), i.e.

$$T_1^{(j)}\left[V + N_1^{(j)}\right] \leqslant V, \quad (j = 1,\ldots,M) \,, \tag{23}$$

assuring that throughout the channel the squeezing operation does not amplify the variances of the quadratures, proportional to the total optical power, over their input values [32, 33]. This conditions arises from a physical requirement that realistic optical fibers cannot support propagation of pulses with arbitrarily high energy without damaging the optical infrastructure or the emergence of unwanted nonlinear effects. Therefore, it is reasonable to impose a condition on the gain of the PSA, such that energy of the amplified signal after each span is not larger than the input one. Furthermore, since we assume all amplifiers to be characterized by the same gain , it suffices to verify condition (23) for $j = 1$, satisfied if $b_1^{(1)} \leqslant V$, namely

$$G \leqslant G_{\max}^{(\mathrm{II})} \equiv \frac{V}{1 + T\left(V + \epsilon - 1\right)} \,. \tag{24}$$

In this security paradigm, the no-amplifier protocol is described by a single-span quantum channel with transmissivity T_n and added noise N_n, which coincides with the GG02 protocol. The benchmark key rate $K_u^{(\mathrm{n})}$ is obtained by optimizing the unamplified KGR over the modulation variance V:

$$K_u^{(\mathrm{n})} = \max_{V} K_u^{(\mathrm{IIp})}\left(V, G = 1\right) . \tag{25}$$

The obtained numerical results suggest that the optimized gain for case IIa is equal to $G_u^{(\mathrm{IIa})} \equiv 1$ for all L, therefore $K_u^{(\mathrm{IIa})} \equiv K_u^{(\mathrm{n})}$ and measuring the anti-squeezed quadrature q does not increase the key rate of the discussed protocol. On the contrary, the case IIb improves the security for large values of excess noise ϵ, as depicted in figure 3(a). In this case, PSA links offer a higher KGR and, remarkably, increase the achievable maximum transmission distance, although the enhancement is relevant only for large excess noise, namely $\epsilon \gtrsim 0.05$ [45, 46]. Furthermore, as shown in figure 3(b), at fixed excess noise ϵ, the KGR increase induced by PSAs becomes larger for lower values of the reconciliation efficiency β. For the sake of completeness, in figure 3 we also show the PLOB bound [55]:

$$K_{\mathrm{PLOB}} = -\log_2\left[\left(1 - T_\mathrm{n}\right) T_\mathrm{n}^{\bar{n}_T}\right] - h\left(1 + 2\bar{n}_T\right) , \tag{26}$$

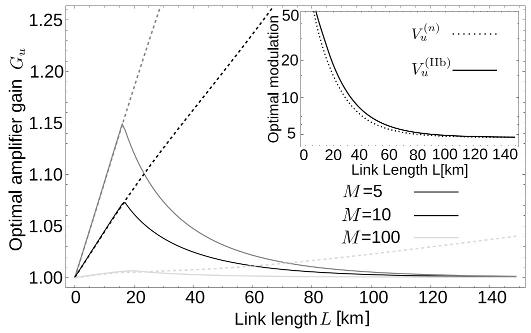

Figure 4. Optimal amplifier gain $G_u^{(\mathrm{IIb})}$ as a function of link length L for different number of amplifiers M. The dashed lines represent the maximum attainable gain $G_{\max}^{(\mathrm{II})}$ computed with the optimized modulation $V_u^{(\mathrm{IIb})}$, presented in the inset. We set $\epsilon = 0.05$ and $\beta = 0.95$.

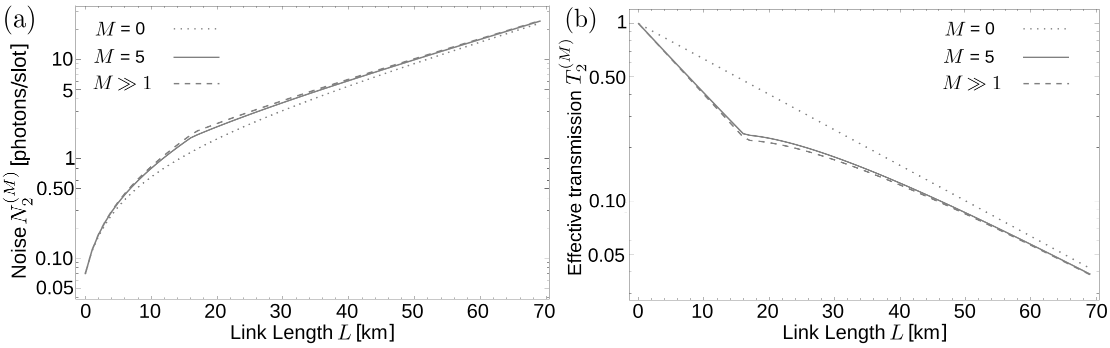

Figure 5. Noise (a) and effective link transmission (b) as a function of link length for different number of amplifiers M for $\epsilon = 0.05$ and $\beta = 0.95$. The case $M = 0$ refers to the no-amplifier protocol.

representing the secret-key capacity of the channel, namely the maximum KGR achievable with the considered thermal-loss channel.

The optimized gain $G_u^{(\mathrm{IIb})}$ obtained from the maximization procedure is plotted in figure 4. For small link lengths L, constraint (24) leads to $G_u^{(\mathrm{IIb})} = G_{\max}^{(\mathrm{II})}$ and the gain increases with link length, whereas for larger L it becomes a decreasing function approaching 1 asymptotically. Moreover, $G_u^{(\mathrm{IIb})}$ decreases with the number of spans M, as expected. Finally, the optimized modulation $V_u^{(\mathrm{IIb})}$ is a decreasing function of the link length such that $V_u^{(\mathrm{IIb})} \geqslant V_u^{(\mathrm{n})}$, where $V_u^{(\mathrm{n})}$ is the optimized modulation of the no-amplifier protocol.

The physical explanation of the previous results is the following. When measuring the squeezed quadrature p, Bob observes a higher added noise with respect to the standard protocol, that is, $N_2^{(M)} \geqslant N_{\mathrm{n}}$, and a reduced effective transmissivity $T_2^{(M)} \leqslant T_{\mathrm{n}}$, as depicted in figure 5. In turn, the mutual information between Alice and Bob is reduced, but at the same time also Eve's Holevo information is reduced since the conditional entropy $S_{E|B}^{(\mathrm{b})}$ becomes larger, according to (21). The tradeoff between the two types of information leads to the the existence of an optimized gain for which the Holevo information is reduced more than the mutual information, eventually resulting in a higher KGR obtained by 'hiding' behind the noise.

In light of this, the advantage introduced by PSAs shall increase with the number of spans M. In particular, we may obtain the maximum increase in KGR in the continuous-amplification limit, $M \gg 1$. Since $T^M = T_{\mathrm{n}}$ is fixed, in this limit, up to a leading order in M, we have that $T \approx 1$, $1 - T \approx -\ln T = -(\ln T_{\mathrm{n}})/M$ and $G^M = G_\infty$. Consequently, the effective transmissivities and added noises read

$$T_1^{(\infty)} = G_\infty T_{\mathrm{n}}\,, \qquad T_2^{(\infty)} = G_\infty^{-1} T_{\mathrm{n}}\,, \tag{27a}$$

$$N_1^{(\infty)} = \frac{1 - G_\infty T_{\mathrm{n}}}{G_\infty T_{\mathrm{n}}} \frac{\ln T_{\mathrm{n}}}{\ln (G_\infty T_{\mathrm{n}})} (1 + 2\bar{n}_T)\,, \tag{27b}$$

$$N_2^{(\infty)} = \frac{1 - T_{\mathrm{n}}/G_\infty}{T_{\mathrm{n}}/G_\infty} \frac{\ln T_{\mathrm{n}}}{\ln (T_{\mathrm{n}}/G_\infty)} (1 + 2\bar{n}_T)\,, \tag{27c}$$

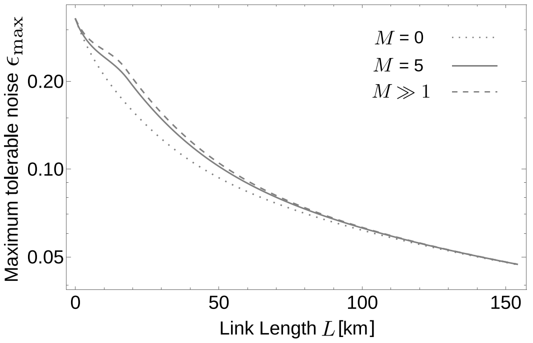

Figure 6. Maximum tolerable noise as a function of the link length for different number of amplifiers M for $\beta = 0.95$. The case $M = 0$ refers to the no-amplifier protocol.

and we obtain the KGR by (22). These channel parameters, calculated for the resulting optimized gain G_∞, are plotted in figure 5. Note also that even a few spans allow one to approach the continuous amplification limit.

Finally, we calculate the maximum tolerable excess noise $\epsilon_{\max}^{(\mathrm{IIb})}$ as a function of the transmission distance, reported in figure 6. It represents the maximum acceptable amount of noise to maintain a positive KGR. Consistently with the previous results, the exploitation of PSAs increases the maximum tolerable excess noise with respect to the no-amplifier scheme in the metropolitan-distance regime, as $\epsilon_{\max}^{(\mathrm{IIb})} \geqslant \epsilon_{\max}^{(\mathrm{n})}$. As expected, the advantage introduced increases with the number of nodes.

4. Conditional security under restricted eavesdropping: only one untrusted span

We now discuss the second instance under investigation, the restricted eavesdropping case. In this scenario we assume Eve to attack only a single span of the link, whilst all the remaining ones as well as the employed amplifiers are considered to be trusted, thus letting our analysis to belong to the conditional security framework. In turn, only a fraction $1/M$ of the whole fiber link is untrusted. The scheme for the eavesdropping strategy under investigation is depicted in figure 7. Across the whole channel, only the kth link, $k = 1,\ldots,M$, is untrusted and may be attacked via entangling cloner attack by Eve [9, 21], performing active eavesdropping. That is, Eve hides herself behind the thermal noise $\bar{n}_k = \bar{n}_T$, equal to (6), by generating a TMSV state with variance $V_\epsilon = 1 + 2\bar{n}_T$ on two modes $\boldsymbol{E} = (E_1, E_2)$ and injecting mode E_1 into the second input port of the beam splitter modeling the k-th span, retrieving the reflected output state. In this way she gets undetected by Alice and Bob, as performing partial trace over modes $\boldsymbol{E}$ introduces an additive thermal noise with exactly $\bar{n}_T$ mean number of photons. In order to perform the security analysis under the above paradigm we shall compute the quantum state in Eve's possession after the entangling cloner attack. We proceed as follows, starting with the case I.

Since all nodes $j = 1,\ldots,k-1$ are trusted, the quantum state shared by Alice and Bob injected into the k-th span is in the form (8), namely:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{k-1}} = \begin{pmatrix} a^{(k-1)}\,\mathbb{1}_2 & z^{(k-1)}\,\boldsymbol{\sigma}_z \\ z^{(k-1)}\,\boldsymbol{\sigma}_z & b^{(k-1)}\,\mathbb{1}_2 \end{pmatrix}. \tag{28}$$

Instead, the CM of Eve's initial TMSV state reads:

$$\boldsymbol{\sigma}_{\boldsymbol{E}} = \begin{pmatrix} V_\epsilon\,\mathbb{1}_2 & Z_\epsilon\,\boldsymbol{\sigma}_z \\ Z_\epsilon\,\boldsymbol{\sigma}_z & V_\epsilon\,\mathbb{1}_2 \end{pmatrix}, \tag{29}$$

with $Z_\epsilon = \sqrt{V_\epsilon^2 - 1}$. After the interference at the beam splitter, the joint quantum state of Alice, Bob and Eve is described by the CM:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_k\boldsymbol{E}} = S\left(\boldsymbol{\sigma}^{(\mathrm{I})}_{AB_{k-1}} \oplus \boldsymbol{\sigma}_{\boldsymbol{E}}\right) S^{\mathrm{T}}, \tag{30}$$

where

$$S = \mathbb{1}_2 \oplus S_{\mathrm{BS}} \oplus \mathbb{1}_2\,, \tag{31}$$

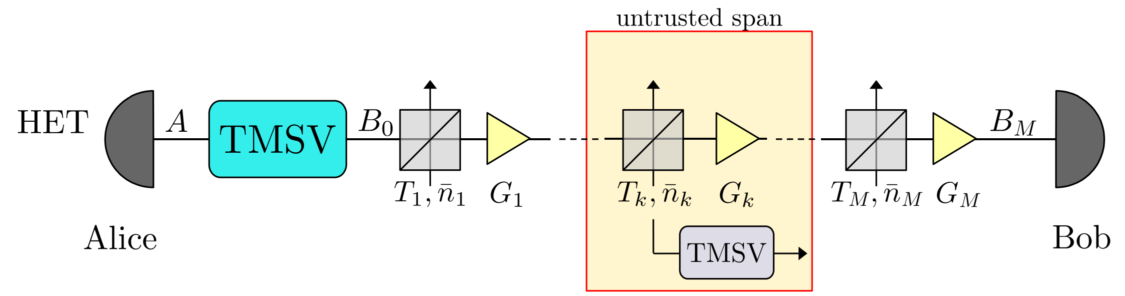

Figure 7. Scheme of the CV-QKD protocol under restricted eavesdropping. All the amplifiers are trusted and Eve is allowed to attack only the k-th span, $k = 1, \dots, M$, via active eavesdropping, that is by injecting one arm of a TMSV state into the span, hiding herself behind the introduced excess noise.

and

$$S_{\mathrm{BS}} = \begin{pmatrix} \sqrt{T}\mathbb{1}_2 & \sqrt{1-T}\mathbb{1}_2 \\ -\sqrt{1-T}\mathbb{1}_2 & \sqrt{T}\mathbb{1}_2 \end{pmatrix} \tag{32}$$

is the symplectic matrix associated with the beam splitter operation [42, 47].

Thereafter, we let the transmitted signal pass through the remaining $M-k$ spans, applying the techniques described in appendix B. Ultimately, the tripartite joint state after the channel is associated with the CM:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{ABE} = \begin{pmatrix} \boldsymbol{\sigma}^{(\mathrm{I})}_{AB} & \boldsymbol{\sigma}^{(\mathrm{I})}_{C} \\ \boldsymbol{\sigma}^{(\mathrm{I})\mathsf{T}}_{C} & \boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} \end{pmatrix}, \tag{33}$$

with the $\boldsymbol{\sigma}^{(\mathrm{I})}_{AB}$ in equation (8) and

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} = \begin{pmatrix} \left[(1-T)\,b^{(k-1)} + TV_\epsilon\right]\mathbb{1}_2 & \sqrt{TZ_\epsilon}\,\boldsymbol{\sigma}_z \\ \sqrt{TZ_\epsilon}\,\boldsymbol{\sigma}_z & V_\epsilon\,\mathbb{1}_2 \end{pmatrix}, \tag{34}$$

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{C} = \left(\begin{array}{c} \boldsymbol{\sigma}^{(\mathrm{I})}_{A\boldsymbol{E}} \\ \hdashline \boldsymbol{\sigma}^{(\mathrm{I})}_{B\boldsymbol{E}} \end{array}\right) = \left(\begin{array}{cc} c^{(1)}\,\boldsymbol{\sigma}_z & \mathbf{0} \\ \hdashline c^{(2)}\,\mathbb{1}_2 & c^{(3)}\,\boldsymbol{\sigma}_z \end{array}\right), \tag{35}$$

being the CM of Eve's overall state and the correlation matrix between Alice and Bob and Eve, respectively, with

$$c^{(1)} = -\sqrt{1-T}\,z^{(k-1)}, \tag{36a}$$

$$c^{(2)} = \sqrt{(GT)^{M-k+1}(1-T)}\left[V_\epsilon - b^{(k-1)}\right], \tag{36b}$$

$$c^{(3)} = \sqrt{(GT)^{M-k}\,G\,(1-T)\,Z_\epsilon}\,. \tag{36c}$$

Subsequently, after Bob's measurement Eve is left with the conditional state associated with:

$$\boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}|B} = \boldsymbol{\sigma}^{(\mathrm{I})}_{\boldsymbol{E}} - \boldsymbol{\sigma}^{(\mathrm{I})\mathsf{T}}_{B\boldsymbol{E}}\left[\boldsymbol{\sigma}^{(\mathrm{I})}_{B} + \boldsymbol{\sigma}_{\mathrm{a}}\right]^{-1}\boldsymbol{\sigma}^{(\mathrm{I})}_{B\boldsymbol{E}}\,. \tag{37}$$

Similarly as in the unconditional security case, the KGR resulting from the present conditional security analysis is given by the difference between the appropriately rescaled Alice and Bob's mutual information $I^{(\mathrm{I})}_{AB}(V,G)$ and the Holevo information between Eve and Bob $\chi^{(\mathrm{I})}_{BE}(V,G)$:

$$K^{(\mathrm{I})}_{c}(V,G) = \beta I^{(\mathrm{I})}_{AB}(V,G) - \chi^{(\mathrm{I})}_{BE}(V,G)\,, \tag{38}$$

where β denotes the reconciliation efficiency. The Holevo information can be written as

$$\chi^{(\mathrm{I})}_{BE}(V,G) = S^{(\mathrm{I})}_{E} - S^{(\mathrm{I})}_{E|B} = h\left(d^{(\mathrm{I})}_1\right) + h\left(d^{(\mathrm{I})}_2\right) - h\left(d^{(\mathrm{I})}_3\right) - h\left(d^{(\mathrm{I})}_4\right), \tag{39}$$

where $h(x)$ is the function in (19) and $d^{(\mathrm{I})}_{1(2)}$ and $d^{(\mathrm{I})}_{3(4)}$ are symplectic eigenvalues of the CMs (34) and (37), respectively. The resulting optimized KGR is equal to:

$$K^{(\mathrm{I})}_{c} = \max_{V,G} K^{(\mathrm{I})}_{c}(V,G)\,, \tag{40}$$

subject to the constraints of maximum power in the link $T^{(j)}[V+N^{(j)}] \leqslant V$ for all $j=1,\ldots,M$, or, equivalently,

$$G \leqslant G_{\max}^{(\mathrm{I})} \equiv \frac{1+V}{2+T(V+\epsilon-1)}\,. \tag{41}$$

The same procedure may be followed to derive the key rate of case II, identifying the corresponding CMs $\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})}$ and $\boldsymbol{\sigma}_{\boldsymbol{E}|B}^{(\mathrm{IIp})}$, the latter depending on the particular quadrature measured by Bob. The resulting expressions are cumbersome, and we only report them in C. The corresponding KGR can be written as:

$$K_c^{(\mathrm{IIp})}(V,G) = \beta I_{AB}^{(\mathrm{IIp})}(V,G) - \chi_{BE}^{(\mathrm{IIp})}(V,G)\,, \quad (\mathrm{p}=\mathrm{a},\mathrm{b})\,, \tag{42}$$

with the mutual information $I_{AB}^{(\mathrm{IIp})}(V,G)$ given in (16) and the Holevo information equal to

$$\begin{aligned}\chi_{BE}^{(\mathrm{IIp})}(V,G) &= S_E^{(\mathrm{II})} - S_{E|B}^{(\mathrm{IIp})}\\ &= h\left(d_1^{(\mathrm{II})}\right) + h\left(d_2^{(\mathrm{II})}\right) - h\left(d_3^{(\mathrm{IIp})}\right) - h\left(d_4^{(\mathrm{IIp})}\right)\,,\end{aligned} \tag{43}$$

$d_{1(2)}^{(\mathrm{II})}$ and $d_{3(4)}^{(\mathrm{IIp})}$ being the symplectic eigenvalues of $\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})}$ and $\boldsymbol{\sigma}_{\boldsymbol{E}|B}^{(\mathrm{IIp})}$, respectively. Finally, one obtains

$$K_c^{(\mathrm{IIp})} = \max_{V,G} K_c^{(\mathrm{IIp})}(V,G)\,, \tag{44}$$

subject to the constraint (24).

Differently from section 3, in this scenario the no-amplifier protocol is equivalent to the case of a wiretap channel under restricted eavesdropping, in which Eve has access only to a portion $1/M$ of the fiber link [21]. That is, we may model the channel as an asymmetric three-span channel composed of three beam splitters with effective transmissivities $T_l = T^{k-1}$, $T_k = T$ and $T_r = T^{M-k}$, and thermal noise $\bar{n}_l = \bar{n}_k = \bar{n}_r = \bar{n}_T$, respectively, in which only the central span is attacked by Eve via entangling-cloner attack. The benchmark key rate $K_c^{(\mathrm{n})}$ is then equal to:

$$K_c^{(\mathrm{n})} = \max_{V} K_c^{(\mathrm{I})}(V, G=1)\,. \tag{45}$$

In the next subsections, we show the obtained results, by comparing directly cases I and IIa, in which the amplified quadrature is probed by Bob and, thereafter, by discussing case IIb, where Bob detects the de-amplified quadrature.

4.1. Cases I and IIa : measuring the amplified quadrature

For both the discussed cases I and II, plots of the KGR $K_c^{(\mathrm{q})}$, $\mathrm{q}=\mathrm{I},\mathrm{IIa}$, are presented in figure 8 for links with $M=5$ (a) or $M=10$ (b) amplifiers and different positions $k=1,\ldots,N$ of the untrusted span, and compared to $K_c^{(\mathrm{n})}$ for no-amplifier protocol. We underline that the results for $M=5$ and $M=10$ can be only qualitatively compared, as we keep the assumption that only one span is untrusted and, in turn, by increasing M Eve becomes more and more restricted.

In general, one can observe that, when Bob measures the amplified quadrature, both PIAs and PSAs improve the KGR with respect to the no-amplifier protocol only if Eve attacks one of the first spans of the fiber-link. The case $k=1$, where the first span is the untrusted one, represents the best-case scenario, where the key rate is increased by several orders of magnitude. Indeed, in this scenario the signal intercepted by Eve has not been amplified yet. Thus, Eve's overall state, described by the CM $\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{q})}$, is independent of the gain G and the only effect of amplification is the reduction of the conditional entropy $S_{E|B}^{(\mathrm{q})}$ appearing in the Holevo information equations (39) and (43). On the other hand, for $k\geqslant 2$, amplifying Bob's received signal also increases Eve's overall entropy $S_E^{(\mathrm{q})}$. In turn, the benefits of optical amplification are more and more reduced with increasing k. To better quantify this effect, we compute the ratio:

$$\mathcal{R}^{(\mathrm{q})} = \frac{K_c^{(\mathrm{q})}}{K_c^{(\mathrm{n})}}\,, \qquad (\mathrm{q}=\mathrm{I},\mathrm{IIa})\,, \tag{46}$$

which is presented in figures 8(c) and (d). All ratios are initially equal to 1 up to a threshold distance, that is, $\mathcal{R}^{(\mathrm{q})}=1$ if $L\leqslant L_{\min}^{(\mathrm{q})}$, thereafter for $k\geqslant 2$ they reach a maximum and then decrease towards an asymptotic value. Moreover, the key ratio $\mathcal{R}^{(\mathrm{q})}$ decreases with increasing k and there exists a threshold value k_{th} such that for $k\geqslant k_{\mathrm{th}}^{(\mathrm{q})}$ we have $\mathcal{R}^{(\mathrm{q})}\equiv 1$. Therefore, if Eve attacks a span located further, $k\geqslant k_{\mathrm{th}}^{(\mathrm{q})}$, employing signal

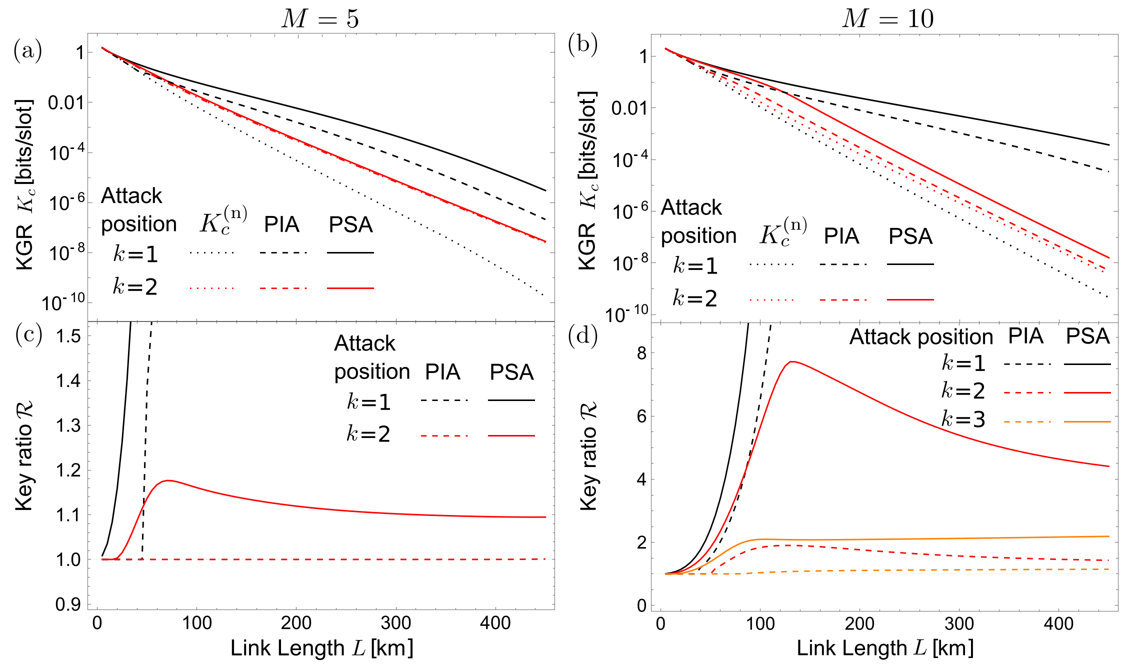

Figure 8. Optimized KGR and key ratio for cases I and IIa as a function of the transmission link length L for different locations of the eavesdropper for $M = 5$ (a) and (c) and $M = 10$ (b) and (d) respectively. We set $\epsilon = 0.05$ and $\beta = 0.95$.

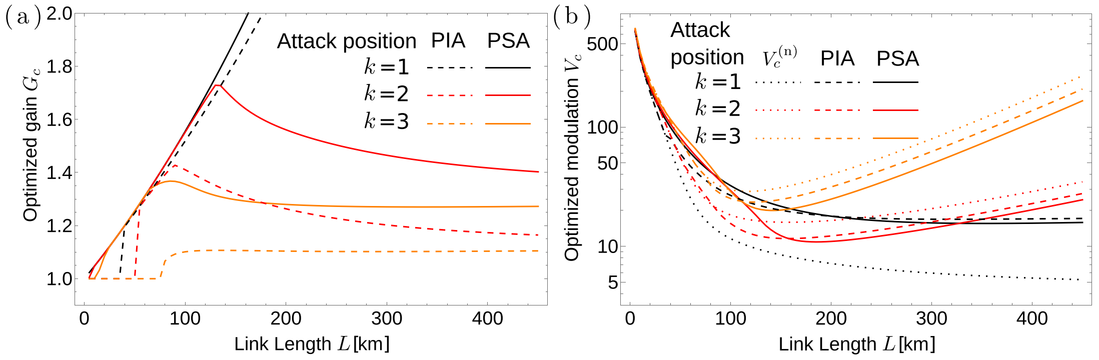

Figure 9. Optimal amplifier gain (a) and modulation (b) for cases I and IIa as a function of the link length L for different locations of the untrusted span k for $M = 10$, $\epsilon = 0.05$ and $\beta = 0.95$.

amplification is no longer beneficial. For link parameters values $\kappa = 0.2$ dB/km, $\epsilon = 0.05$ and $\beta = 0.95$ one obtains $k_{\text{th}}^{(\text{I})} = 2$ and $k_{\text{th}}^{(\text{IIa})} = 3$ for $M = 5$, while for $M = 10$ one gets $k_{\text{th}}^{(\text{I})} = 5$ and $k_{\text{th}}^{(\text{IIa})} = 8$. Importantly, note that the performance of PIA links is always lower than PSA ones, as $\mathcal{R}^{(\text{I})} \leqslant \mathcal{R}^{(\text{IIa})}$, $d_{\text{min}}^{(\text{I})} \leqslant d_{\text{min}}^{(\text{IIa})}$ and $k_{\text{th}}^{(\text{I})} \leqslant k_{\text{th}}^{(\text{IIa})}$. This is a direct consequence of the additional noise introduced by the phase-insensitive amplification process.

The optimized gain $G_c^{(\text{q})}$ and modulation $V_c^{(\text{q})}$, q = I, IIa, are depicted in figures 9(a) and (b), respectively. Consistent with the results from the previous paragraph, it is optimal to not amplify the signal, i.e. $G_c^{(\text{q})} = 1$, for short distances $L \leqslant L_{\text{min}}^{(\text{q})}$. For longer link lengths the optimal gain initially increases with L, following constraints (24) and (41), and then ultimately decreases towards an asymptotic value. The optimal gain $G_c^{(\text{q})}$ also decreases with k, similarly to the key ratio. On the other hand, the behavior of optimal modulation $V_c^{(\text{q})}$ is quite peculiar. For $k = 1$ it is a monotonous decreasing function of the transmission distance L, as obtained in section 3. The presence of optical amplifiers increases the modulation value with respect to the no-amplifier protocol, as $V_c^{(\text{q})} \geqslant V_c^{(\text{n})}$. On the contrary, when $k \geqslant 2$ the situation is completely different and in the long-distance regime the optimized modulation turns out to be an increasing function of L. In fact, if Eve attacks one of the last spans of the communication link she intercepts a weak pulse, therefore it is possible to safely increase the input modulation variance without preventing secure communication between Alice and Bob.

When the amplified quadrature is measured, the effective transmissivity probed by Bob, namely $T^{(M)}$ and $T_1^{(M)}$ for cases I and IIa respectively, is larger with respect to the no-amplifier protocol, $T^{(M)}, T_1^{(M)} \geqslant T_\mathrm{n}$. This leads to an increase of both mutual information between Alice and Bob, and, at the same time, Holevo information on Eve's side. This is because for $k \geqslant 2$ she also receives an amplified signal. In turn, when performing optimization over the free parameters, there emerges a tradeoff between these two types of information, resulting in the key rates shown in figure 8. In particular, for short-distance communication, $L \leqslant L_\mathrm{min}^{(\mathrm{q})}$, one obtains that optical amplification is useless, $G_c^{(\mathrm{q})} = 1$. The difference between cases I and IIa is due to the different impact of the added noise. In fact, for case IIa the added noise is rescaled with respect to the no-amplifier protocol, $N_1^{(M)} \leqslant N_\mathrm{n}$, whilst for case I the noise is increased because of the additive contribution N_G due to phase-insensitive amplification, $N^{(M)} \geqslant N_\mathrm{n}$. In the latter case the (incoherent) added contribution N_G detriments the mutual information between Alice and Bob, being less than its counterpart of case IIa. Ultimately, this leads to a reduced performance of PIA links with respect to PSA ones.

4.2. Case IIb : measuring the de-amplified quadrature

The KGR $K_c^{(\mathrm{IIb})}$ for the Bob's measurement of the de-amplified quadrature, IIb, is depicted in figure 10 for links with $M = 5$ (a) or $M = 10$ (b) amplifiers and different positions $k = 1, \ldots, M$ of the untrusted span, together with the key ratio

$$\mathcal{R}^{(\mathrm{IIb})} = \frac{K_c^{(\mathrm{IIb})}}{K_c^{(\mathrm{n})}} \,. \tag{47}$$

The scenario is reversed with respect to the previous section. Indeed, when Bob probes the squeezed (i.e. de-amplified) quadrature, PSA links improve the resulting KGR if Eve attacks one of the last spans of the channel. The best-case scenario is provided by $k = M$, in which the KGR increases by more than an order of magnitude. Consequently, and in contrast to the results from section 4.1, one observes enhancement in the key ratio $\mathcal{R}^{(\mathrm{IIb})}$ with increasing k. In this scenario the PSA becomes useless if Eve attacks the first span for all M, namely $\mathcal{R}^{(\mathrm{IIb})} \equiv 1$, since in this case she intercepts the pulse before all amplifiers and therefore, de-amplifying the signal only reduces the mutual information between Alice and Bob, maintaining a higher Holevo information at Eve's side. On the other hand, for $k \geqslant 2$, de-amplifying Bob's signal also reduces Eve's extracted information, thus leading to $\mathcal{R}^{(\mathrm{IIb})} \geqslant 1$. In particular, there exists a threshold attack location $k_\mathrm{th}^{(\mathrm{IIb})}$ such that for $k \leqslant k_\mathrm{th}^{(\mathrm{IIb})}$ one has $\mathcal{R}^{(\mathrm{IIb})} \equiv 1$, being equal to $k_\mathrm{th}^{(\mathrm{IIb})} = 1$ for $M = 5$ and $k_\mathrm{th}^{(\mathrm{IIb})} = 2$ for $M = 10$. For eavesdropping performed on a span located further within the link $k \geqslant k_\mathrm{th}^{(\mathrm{IIb})}$ all key ratios exhibit a maximum and then decrease towards an asymptotic value, equal to 1 for locations closer to the threshold value or greater than 1 for those placed further, implying an improvement of security in the long-distance regime brought by the PSA link.

Note, that the absence of PSA advantage for $k = 1$ does not stand in contradiction with it existence in the unconditional security framework discussed in section 3, where Eve is assumed to collect the reflected pulses from all spans. This is because de-amplification reduces the accessible information contained in the signals lost after the second span, eventually resulting in an enhancement of the KGR.

In figures 11(a) and (b), one can see the optimized gain $G_c^{(\mathrm{IIb})}$ and modulation $V_c^{(\mathrm{IIb})}$, respectively. We see that amplification is not beneficial, $G_c^{(\mathrm{IIb})} \equiv 1$, for eavesdropping performed on initial spans $k \leqslant k_\mathrm{th}^{(\mathrm{IIb})}$, whereas for attacks on latter spans the optimal gain increases with the link length following constraint (24), until finally decreasing towards an asymptotic value. In accordance with the previous results, one needs to employ the stronger optimal amplification the further the eavesdropped span is located. The optimized modulation increases with respect to the no-amplifier protocol $V_c^{(\mathrm{IIb})} \geqslant V_c^{(\mathrm{n})}$. Similarly to the results obtained in section 4.1, it is a decreasing function of the link length if the attack is performed on the first span, whilst it becomes non-monotonous for $k \geqslant 2$, increasing in the long-distance regime.

The physical meaning of these results is analogous to these obtained in section 3. Indeed, the case IIb is associated with a reduced transmissivity with respect to the no-amplifier protocol, $T_2^{(M)} \leqslant T_\mathrm{n}$, and amplified added noise $N_2^{(M)} \geqslant N_\mathrm{n}$. Therefore, for $k \geqslant 2$ by employing PSAs Bob accepts to reduce the extracted mutual information, in order to increase the conditional entropy $S_{E|B}^{(\mathrm{IIb})}$, resulting in a lower Holevo information between Eve and himself. The tradeoff between these two quantities is such that for $k \geqslant k_\mathrm{th}^{(\mathrm{IIb})}$ one has $G_c^{(\mathrm{IIb})} \geqslant 1$ and PSA links increase the obtained KGR.

4.3. On the relevance of multi-span links

The above analysis under the conditional security paradigm opens up an intriguing question about the possible use cases of a multi-span configuration. In fact, since in the considered scenario most of the links are

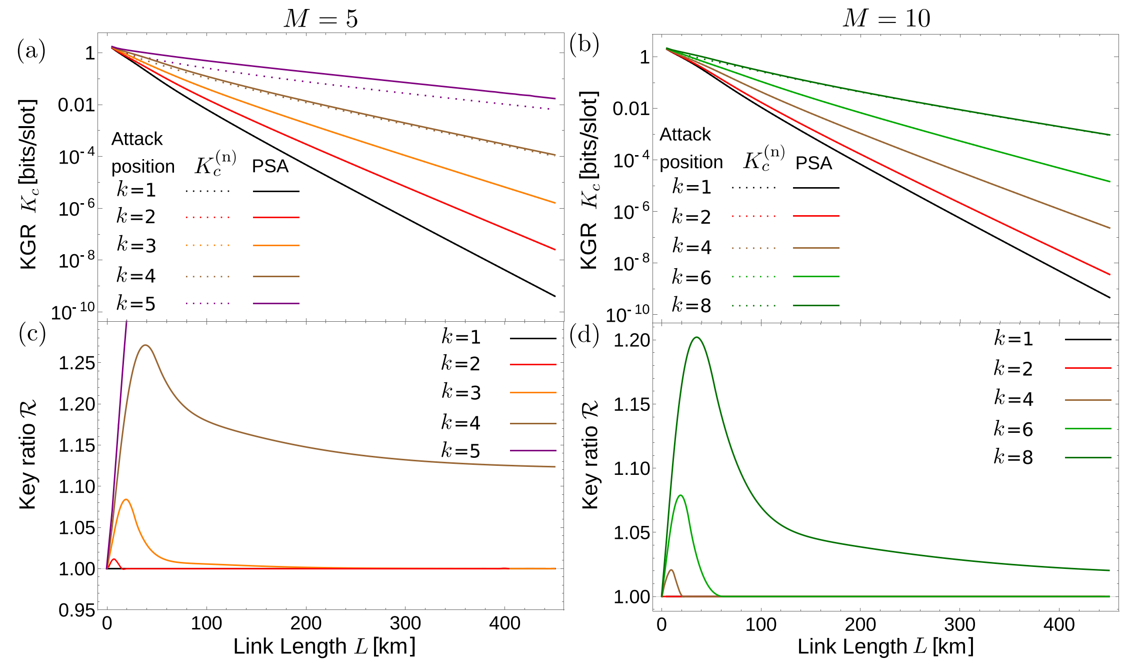

Figure 10. Optimized KGR and key ratio for case IIb as a function of the transmission link length L for different locations of the eavesdropper for $M = 5$ (a) and (c) and $M = 10$ (b) and (d) respectively. We set $\epsilon = 0.05$ and $\beta = 0.95$.

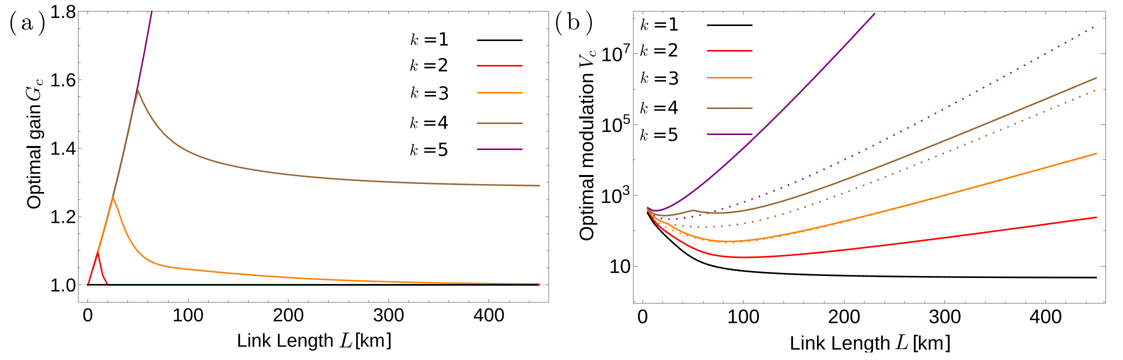

Figure 11. Optimal amplifier gain (a) and modulation (b) for case IIb as a function of the link length L for different locations of the untrusted span k for $M = 10$, $\epsilon = 0.05$ and $\beta = 0.95$.

trusted nodes, an alternative choice would be instead to insert classical-like repeaters after each span and establish keys separately between neighboring nodes. At the quantum limit, a classical repeater would be described as an intercept-resend system, performing double homodyne detection on the received signal and preparing a coherent pulse with amplitude equal to the obtained outcome.

In principle, establishing keys between subsequent nodes would significantly reduce the impact of channel losses at the cost of introducing additional excess noise due to probabilistic nature of the quadrature measurement. However, from a practical point of view, this configuration would be unfeasible in real networks, as classical-repeater nodes are expensive and, thus, cannot be placed at every few km. A further solution may be the adoption of quantum repeaters [38–40], which represent an intriguing strategy from a theoretical point of view, but rather an unpractical one with current state-of-the-art technology. In fact, quantum repeaters for CV systems employ probabilistic noiseless linear amplifiers as a fundamental building block, and, thus, require the presence of a quantum memory, not yet available with the current optical communication technologies [48, 49].

In turn, employing either classical or quantum repeaters can lead to a much higher key rate at the cost of making infrastructure complicated and expensive. On the contrary, optical amplifiers like PIA and PSA are much cheaper and manageable than repeaters and provide a feasible tool to enhance communication between the nodes.

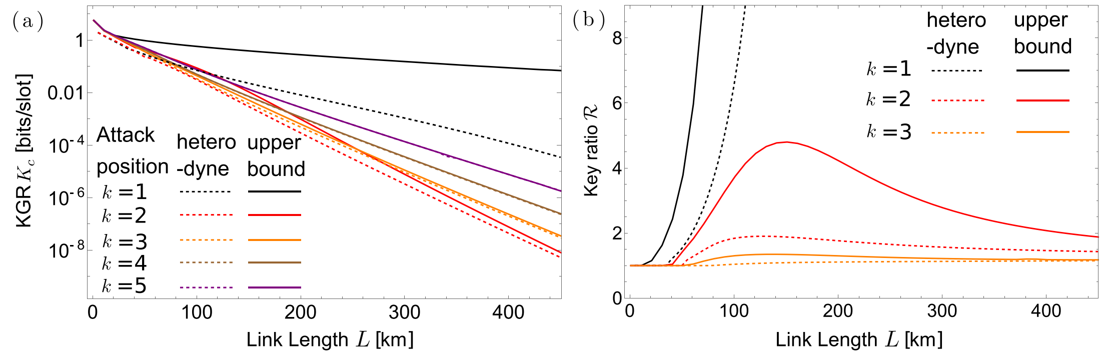

Figure 12. Upper bound on KGR (a) and corresponding key ratio (b) for PIA as a function of link length for $M = 10$ nodes, $\epsilon = 0.05$ and $\beta = 0.95$.

5. Ultimate key rate limits

In the analysis above, we considered the entanglement-based CV-QKD protocol where Alice and Bob perform heterodyne and homodyne detection, respectively, which in the prepare-and-measure picture is equivalent to considering coherent-state encoding followed by quadrature detection [8, 9, 12]. In turn, the resulting mutual information depends only on the signal-to-noise ratio, according to the Shannon-Hartley theorem [56], as derived in (12) and (16). However, from the perspective of quantum communication, we may also consider the fundamental quantum limit, namely the Holevo information between Alice and Bob [44]. This ultimate capacity provides an upper bound on the achievable mutual information which has been also investigated for multi-span links employing either PIAs or PSAs [32, 33].

We embed this approach within the CV-QKD framework by considering an equivalent protocol to that of figures 2 and 7, in which Bob still performs the homodyne measurement of quadratures q and p, but Alice replaces her heterodyne detection with the proper measurement achieving the Holevo bound. In this way, we compute the Holevo information χ_{AB} by interpreting Bob's measurement as a state-preparation process. Ultimately, we obtain an upper bound on the KGR which allows to highlight the ultimate limits on KGR of multi-span links. For the sake of simplicity, here we will discuss only the case of a PIA link under restricted eavesdropping with the same assumptions as in section 4, namely a single untrusted span.

For case I, the ultimate KGR reads:

$$\widetilde{K}_c^{(\mathrm{I})} = \max_{V,G} \left[\beta \chi_{AB}^{(\mathrm{I})}(V,G) - \chi_{BE}^{(\mathrm{I})}(V,G)\right], \tag{48}$$

with the $\chi_{BE}^{(\mathrm{I})}$ in (39) and $\chi_{AB}^{(\mathrm{I})}$ being the Holevo capacity [32] retrievable from (8):

$$\chi_{AB}^{(\mathrm{I})}(V,G) = S_A^{(\mathrm{I})} - S_{A|B}^{(\mathrm{I})} = h\left(\tilde{d}_1\right) - h\left(\tilde{d}_2\right), \tag{49}$$

where $h(x)$ is the function in (19), $\tilde{d}_1 = \sqrt{\det\left[\boldsymbol{\sigma}_A^{(\mathrm{I})}\right]} = V$ and $\tilde{d}_2 = \sqrt{\det\left[\boldsymbol{\sigma}_{A|B}^{(\mathrm{I})}\right]}$, where

$$\boldsymbol{\sigma}_{A|B}^{(\mathrm{I})} = \boldsymbol{\sigma}_A^{(\mathrm{I})} - \boldsymbol{\sigma}_Z^{(\mathrm{I})}\left[\boldsymbol{\sigma}_B^{(\mathrm{I})} + \boldsymbol{\sigma}_{\mathrm{a}}\right]^{-1} \boldsymbol{\sigma}_Z^{(\mathrm{I})\mathsf{T}}. \tag{50}$$

The maximization procedure is, once again, subject to constraint (41).

It is seen in figure 12(a) that there is a considerable gap between the upper bound $\widetilde{K}_c^{(\mathrm{I})}$ and the performance of heterodyne receiver $K_c^{(\mathrm{I})}$ for few attacks performed on few initial nodes. For further spans, the difference disappears, as indicated by the key ratios $\mathcal{R}$ with respect to the associated no-amplifier protocol, depicted in figure 12(b). This means that, even in the best theoretical scenario, the advantage originating from PIA vanishes for attacks on further parts of the link. A possible remedy may be to employ PSA but obtaining the ultimate bound in such a scenario requires considerable effort since the resulting quantum channel is phase sensitive [33, 57].

6. Comparison with squeezed-state protocols

Throughout the paper we proved that optical amplification provides a powerful tool to mitigate transmission losses and enhance secure communications under different frameworks. In particular, in the unconditional

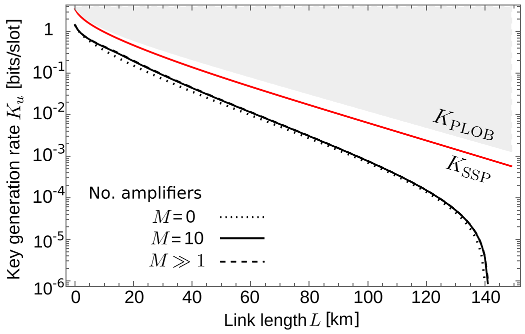

Figure 13. Optimized KGR $K_u^{(\mathrm{IIb})}$ as a function of the transmission link length L for different number of amplifiers M, compared to the KGR K_{SSP} achieved by the squeezed-state protocol and the PLOB bound (26). We set the values $\epsilon = 0.05$ and $\beta = 0.95$. The gray shaded area represents KGR higher than the ultimate PLOB bound. It is worth noticing that the amount of squeezing required to attain the performance of the SSP is large, ranging from 20 to 10 dB depending on the link length, whereas in the PSA-link scenario the optimized gain is close to 1, see figure 4.

case main advantages are found using PSAs, namely single-mode squeezers, to perform signal restoration after each transmission link.

However, from a more general viewpoint one may ask whether squeezing would be beneficial to enhance also other stages of CVQKD protocols. As an example, a squeezer can be employed directly at the modulation stage before the injection into the lossy channel, by letting Alice generate a single-mode squeezed vacuum state and, then, displace it by a random amplitude drawn from a Gaussian distribution. We refer to this alternative scheme as the squeezed-state protocol (SSP), which has been widely studied in literature as a possible alternative to coherent-state protocols like GG02 [50–54]. In turn, a natural question arises if the employment of PSAs would be more powerful either to amplify the signal throughout the channel or at the transmitter during the signal generation. Note, however, that these two schemes deal with different types of resources meaning their comparison may not be completely fair. In particular, in SSP squeezing is a part of input modulation whereas for the amplified link it is used during the propagation. Nevertheless, it is still worth of investigation to provide a complete picture on the role of PSAs for CVQKD.

The theoretical entanglement-based description of the SSP is the following. As for the coherent-state protocol, Alice generates the TMSV (4) with variance $V > 1$ and injects its second branch into a thermal-loss channel with transmissivity T and background thermal noise $\bar{n}_T$ equal to (6). However, now Alice performs a homodyne measurement of q on the first branch, instead of heterodyne detection, which projects state (4) onto a displaced squeezed state $D(\gamma)S(-r)|0\rangle$, with $\gamma = \sqrt{V^2 - 1}x/V$, x being the outcome of Alice's detection, and $\exp(2r) = V$. This procedure corresponds to the Gaussian modulation of a vacuum state squeezed in quadrature q. In turn, Bob performs homodyne measurement of the squeezed quadrature on the received pulse. Given this scenario, we compute the resulting KGR K_{SSP}, optimized over the input variance V, that now contains the contributions of both initial squeezing and signal modulation. Plots of K_{SSP} together with $K_u^{(\mathrm{IIb})}$ are reported in figure 13.

It is seen that the SSP outperforms the coherent-state protocol employing a PSA link, being close to the PLOB bound in the short-distance regime, as already discussed in [50]. One of the reasons behind this result is that performing squeezing before modulation preserves the signal amplitude injected into the channel, whereas squeezing after transmission reduces both the variance and the mean value of quadrature q, with the overall effect of reducing the effective transmissivity, $T_2^{(M)} \leqslant T_{\mathrm{n}}$. Thus, adopting squeezing at the modulation stage provides an additional resource. However, the two compared strategies are not mutually exclusive, therefore even in the presence of the SSP one can also utilize PSAs throughout the link to further improve the final KGR. Note also that in order to approach the performance seen in figure 13 the SSP requires large squeezing, of the order of $20 - 10$ dB, depending on the link length. In contrast, the optimal gain of PSA in the amplified link scenario is close to 1, as evidenced in figure 4, which is much less demanding experimentally.

7. Conclusions

In this paper we have addressed the exploitation of multi-span amplified links for CV-QKD. In particular, we have discussed three cases: PIA link with random homodyne detection of q/p quadratures and PSA link with measurement of either quadrature q or p. In the unconditional security approach we showed that the KGR is improved with respect to the standard no-amplifier protocol only for the scenario in which Bob measures the de-amplified quadrature. This enhancement is noticeable especially in the presence of large excess noise, $\epsilon \gtrsim 0.05$.

We have also investigated the KGR in the conditional security framework, by assuming that all amplifiers and spans except one are trusted. We showed that the position of the untrusted span greatly affects the potential enhancement offered by amplification. In particular, for the cases with PIA and random homodyne measurement and with PSA and measurement of the amplified quadrature one observes an enhancement in the KGR only if one of the first spans is attacked, namely $k \leqslant k_{\rm th}^{(\rm q)}$, whereas for case with PSA and detection of the de-amplified quadrature the improvement is present if the attacked span is in the latter part of the link, $k \geqslant k_{\rm th}^{(\rm IIb)}$. Finally, we have addressed the case in which Alice and Bob achieve the Holevo capacity, thus providing an upper bound for the security, highlighting the ultimate enhancement that may be brought by PIA links.

The results of the paper present a detailed analysis of the improvement and the limits offered by optical amplifiers for quantum secure communications under realistic assumptions and pave the way for future developments in the framework of conditional security CV-QKD. In particular, the advantage given by PSA, being a phase-sensitive operation, may be potentially further boosted by employing squeezed states [50–54, 58].

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

This Project has received funding from the European Union's Horizon Europe research and innovation programme under the project 'Quantum Security Networks Partnership' (QSNP, Grant Agreement No 101114043).

Appendix A. Brief review of the Gaussian formalism

As discussed in the main text, we exploit the Gaussian formalism to perform the security analysis [42, 47]. Here we present the main tools to retrieve the obtained results. We consider a n-mode bosonic system, described by bosonic annihilation 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

$$q_k = \sigma_0 \left(a_k + a_k^\dagger\right) \quad \text{and} \quad p_k = \mathrm{i}\sigma_0 \left(a_k^\dagger - a_k\right), \tag{A.1}$$

such that $[q_k, p_l] = 2\mathrm{i}\sigma_0^2 \delta_{kl}$, where we adopt shot-noise units, $\sigma_0^2 = 1$. A more compact notation is obtained by introducing the vectorial operator $\hat{\mathbf{r}} = (q_1, p_1, q_2, p_2, \ldots, q_n, p_n)^\intercal$.

A Gaussian state ρ_G is a quantum state associated with a Gaussian Wigner function

$$W[\rho_G](\mathbf{r}) = \frac{1}{(2\pi)^n \sqrt{\det(\boldsymbol{\sigma})}} \exp\left[-\frac{1}{2}(\mathbf{r} - \mathbf{R})^\intercal \boldsymbol{\sigma}^{-1} (\mathbf{r} - \mathbf{R})\right], \tag{A.2}$$

where $\mathbf{r}^\intercal = (x_1, y_1, x_2, y_2, \ldots, x_n, y_n) \in \mathbb{R}^{2n}$, and

$$\mathbf{R} = \mathrm{Tr}[\rho_G \hat{\mathbf{r}}] \tag{A.3}$$

is the first moment vector and

$$\boldsymbol{\sigma} = \frac{1}{2}\mathrm{Tr}\left[\rho_G \left\{(\hat{\mathbf{r}} - \mathbf{X}), (\hat{\mathbf{r}} - \mathbf{X})^\intercal\right\}\right] \tag{A.4}$$

is the $2n \times 2n$ 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 CM.

Gaussian dynamics, i.e. unitary evolution generated by bilinear Hamiltonians, is associated with a symplectic matrix S such that if the input state is Gaussian the evolved state is still Gaussian with [42, 47]:

$$\mathbf{R} \to S\mathbf{R} \quad \text{and} \quad \boldsymbol{\sigma} \to S\boldsymbol{\sigma}S^\intercal. \tag{A.5}$$

On the contrary, Gaussian CP maps are associated with a pair of matrices X and Y such that the evolved state is characterized by:

$$\mathbf{R} \to X\mathbf{R} \quad \text{and} \quad \boldsymbol{\sigma} \to X\boldsymbol{\sigma} X^{\mathsf{T}} + Y, \tag{A.6}$$

where $Y + \mathrm{i}\Omega \geqslant \mathrm{i}X\Omega X^{\mathsf{T}}$, Ω being the $2n\times 2n$ symplectic form [42, 47].

Finally, we discuss the case of conditional dynamics. In the paper, we consider a bipartite system AB, where subsystems A and B are composed of n_A an n_B modes, respectively. We consider a Gaussian state ρ_{AB} with prime moments $\mathbf{R} = (\mathbf{R}_A, \mathbf{R}_B)$ and CM (written in block form)

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\sigma}_A & \boldsymbol{\sigma}_C \\ \boldsymbol{\sigma}_C^{\mathsf{T}} & \boldsymbol{\sigma}_B \end{pmatrix}. \tag{A.7}$$

We now perform a Gaussian measurement on subsystem B associated with the CM $\boldsymbol{\sigma}_m$, obtaining outcome $\mathbf{r}_m \in \mathbb{R}^{2n_B}$. Then, the conditional state $\rho_{A|\mathbf{r}_m}$ on mode A is still a Gaussian state with CM $\boldsymbol{\sigma}_{A|\mathbf{r}_m}$ and first moment vector $\mathbf{R}_{A|\mathbf{r}_m}$ given by:

$$\boldsymbol{\sigma}_{A|\mathbf{r}_m} = \boldsymbol{\sigma}_A - \boldsymbol{\sigma}_C \left(\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_m\right)^{-1} \boldsymbol{\sigma}_C^{\mathsf{T}}, \tag{A.8}$$

and

$$\mathbf{R}_{A|\mathbf{r}_m} = \mathbf{R}_A + \boldsymbol{\sigma}_{AB} \left(\boldsymbol{\sigma}_B + \boldsymbol{\sigma}_m\right)^{-1} \left(\mathbf{r}_m - \mathbf{R}_B\right), \tag{A.9}$$

respectively [42, 47].

Appendix B. Derivation of the Gaussian CP map for the multi-span link

In the paper we discuss CV-QKD over multi-span links composed of either PIAs or PSAs connected via a sequence of thermal-loss (TL) channels. In the following we report the structure of the quantum CP maps associated with each of these components.

A thermal-loss channel with transmissivity $T \leqslant 1$ and thermal noise $\bar{n}_T$ is described via a Gaussian CP map associated with the matrices [42]:

$$X_{\mathrm{TL}} = \sqrt{T}\mathbb{1}_2 \quad \text{and} \quad Y_{\mathrm{TL}} = (1-T)(1+2\bar{n}_T)\mathbb{1}_2, \tag{B.1}$$

$\mathbb{1}_2$ being the 2×2 identity matrix.

As regards optical amplification, PIA are descripted by the Gaussian CP map [42]:

$$X_{\mathrm{PIA}} = \sqrt{G}\mathbb{1}_2 \quad \text{and} \quad Y_{\mathrm{PIA}} = (G-1)\mathbb{1}_2. \tag{B.2}$$

$G \geqslant 1$ being the amplification gain, whilst PSA are unitary maps, thus completely described by the symplectic matrix [47]:

$$S_{\mathrm{PSA}} = \begin{pmatrix} G^{1/2} & 0 \\ 0 & G^{-1/2} \end{pmatrix}. \tag{B.3}$$

Thus, for case I, namely in the presence of a PIA link, each span is given by the composition of the two Gaussian CP maps described by equations (B.1) and (B.2), resulting in a overall Gaussian CP map defined by the matrices:

$$\begin{aligned} X^{(\mathrm{I})} &= X_{\mathrm{PIA}} X_{\mathrm{TL}} = \sqrt{GT}\mathbb{1}_2, \\ Y^{(\mathrm{I})} &= X_{\mathrm{PIA}} Y_{\mathrm{TL}} X_{\mathrm{PIA}}^{\mathsf{T}} + Y_{\mathrm{PIA}} \\ &= \left[G(1-T)(1+2\bar{n}_T) + (G-1)\right]\mathbb{1}_2. \end{aligned} \tag{B.4}$$

Otherwise, for case II, namely PSA link, each span is the composition of the CP map (B.1) and the symplectic evolution (B.3), resulting in the overall Gaussian CP map associated with $X^{(\mathrm{II})} = S_{\mathrm{PSA}} X_{\mathrm{TL}}$ and $Y^{(\mathrm{II})} = S_{\mathrm{PSA}} Y_{\mathrm{TL}} S_{\mathrm{PSA}}^{\mathsf{T}}$, namely:

$$X^{(\mathrm{II})} = \begin{pmatrix} \sqrt{GT} & 0 \\ 0 & \sqrt{G^{-1}T} \end{pmatrix}, \tag{B.5}$$

and

$$Y^{(\mathrm{II})} = \begin{pmatrix} G(1-T)(1+2\bar{n}_T) & 0 \\ 0 & G^{-1}(1-T)(1+2\bar{n}_T) \end{pmatrix}. \tag{B.6}$$

We remark that in the main text we consider a two-mode state AB, where only branch B undergoes a Gaussian evolution. Thus, according to the Gaussian formalism, the bipartite map will be associated with the matrices $X_{AB} = \mathbb{1}_2 \oplus X_{\mathrm{p}}$ and $Y_{AB} = \mathbf{0} \oplus Y_{\mathrm{p}}$ for $\mathrm{p} = \mathrm{I}, \mathrm{II}$.

Appendix C. Conditional security analysis for case II

The key rate for cases IIp, $\mathrm{p} = \mathrm{a}, \mathrm{b}$, may be computed by following the same procedure described in section 4, leading to the joint state of the three parties:

$$\boldsymbol{\sigma}_{AB\boldsymbol{E}}^{(\mathrm{II})} = \begin{pmatrix} \boldsymbol{\sigma}_{AB}^{(\mathrm{II})} & \boldsymbol{\sigma}_{C}^{(\mathrm{II})} \\ \boldsymbol{\sigma}_{C}^{(\mathrm{II})\mathsf{T}} & \boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})} \end{pmatrix}, \tag{C.1}$$

with the $\boldsymbol{\sigma}_{AB}^{(\mathrm{II})}$ in equation (13) and

$$\boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})} = \begin{pmatrix} e_1 & 0 & \sqrt{T} Z_\epsilon & 0 \\ 0 & e_2 & 0 & -\sqrt{T} Z_\epsilon \\ \sqrt{T} Z_\epsilon & 0 & V_\epsilon & 0 \\ 0 & -\sqrt{T} Z_\epsilon & 0 & V_\epsilon \end{pmatrix}, \tag{C.2}$$

with

$$\boldsymbol{\sigma}_{C}^{(\mathrm{II})} = \begin{pmatrix} \boldsymbol{\sigma}_{A\boldsymbol{E}}^{(\mathrm{II})} \\ \hdashline \boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})} \end{pmatrix} = \left(\begin{array}{cccc} c_1^{(1)} & 0 & 0 & 0 \\ 0 & -c_2^{(1)} & 0 & 0 \\ \hdashline c_1^{(2)} & 0 & c_1^{(3)} & 0 \\ 0 & c_2^{(2)} & 0 & -c_2^{(3)} \end{array}\right), \tag{C.3}$$

$$e_{1(2)} = \left[(1-T)\, b_{1(2)}^{(k-1)} + T V_\epsilon\right], \tag{C.4a}$$

$$c_{1(2)}^{(1)} = -\sqrt{1-T}\, z_{1(2)}^{(k-1)}, \tag{C.4b}$$

$$c_1^{(2)} = \sqrt{(GT)^{M-k+1}(1-T)}\left[V_\epsilon - b_1^{(k-1)}\right], \tag{C.4c}$$

$$c_2^{(2)} = \sqrt{(G^{-1}T)^{M-k+1}(1-T)}\left[V_\epsilon - b_2^{(k-1)}\right], \tag{C.4d}$$

$$c_1^{(3)} = \sqrt{(GT)^{M-k}\, G(1-T)}\, Z_\epsilon, \tag{C.4e}$$

$$c_2^{(3)} = \sqrt{(G^{-1}T)^{M-k}\, G^{-1}(1-T)}\, Z_\epsilon. \tag{C.4f}$$

Finally, Eve's conditional CM reads:

$$\boldsymbol{\sigma}_{\boldsymbol{E}|B}^{(\mathrm{IIp})} = \boldsymbol{\sigma}_{\boldsymbol{E}}^{(\mathrm{II})} - \boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})\mathsf{T}} \left[\boldsymbol{\sigma}_{B}^{(\mathrm{II})} + \boldsymbol{\sigma}_{\mathrm{p}}\right]^{-1} \boldsymbol{\sigma}_{B\boldsymbol{E}}^{(\mathrm{II})}, \quad (\mathrm{p} = \mathrm{a}, \mathrm{b}). \tag{C.5}$$

ORCID iDs

M N Notarnicola https://orcid.org/0000-0002-7492-6143
M Jarzyna https://orcid.org/0000-0001-9989-1648

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Pirandola S *et al* 2020 *Adv. Opt. Photon.* **12** 1012–236
[4] Bennet C and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* vol 175 pp 175–9

[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[6] Wang S *et al* 2022 *Nat. Photon.* **16** 154–61

[7] Fan-Yuan G-J *et al* 2022 *Optica* **9** 812–23

[8] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[9] Laudenbach F, Pacher C, Fung C-H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P and Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011

[10] Olivares S 2021 *Phys. Lett.* A **418** 127720

[11] Agrawal G P 2002 *Fiber-Optic Communications Systems* (Wiley)

[12] Grosshans F, Van Assche G, Wenger J, Tualle-Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[13] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 *Quantum Inf. Comput.* **3** 535

[14] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504

[15] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Koy Lam P 2004 *Phys. Rev. Lett.* **93** 170504

[16] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[17] Leverrier A 2009 Theoretical study of continuous-variable quantum key distribution *PhD Thesis* Télécom ParisTech

[18] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[19] Pirandola S 2021 *Phys. Rev. Res.* **3** 013279

[20] Pirandola S 2021 *Phys. Rev. Res.* **3** 043014

[21] Pan Z, Seshadreesan K P, Clark W, Adcock M R, Djordjevic I B, Shapiro J H and Guha S 2020 *Phys. Rev. Appl.* **14** 024044

[22] Banaszek K, Jachura M, Kolenderski P and Lasota M 2021 *Opt. Express* **29** 43091–103

[23] Notarnicola M N, Olivares S, Forestieri E, Parente E, Potì L and Secondini M 2024 *IEEE Trans. Commun.* **72** 375–86

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

[25] Lodewyck J *et al* 2007 *Phys. Rev.* A **76** 042305

[26] Banaszek K, Kunz L, Jachura M and Jarzyna M 2020 *J. Lightwave Technol.* **38** 2741–54

[27] Caves C M 1982 *Phys. Rev.* D **26** 1817

[28] Bachor H-A and Ralph T C 2019 *A Guide to Experiments in Quantum Optics* (Wiley)

[29] Notarnicola M N, Genoni M G, Cialdi S, Paris M G A and Olivares S 2022 *J. Opt. Soc. Am.* B **39** 1059–67

[30] Yariv A 1990 *Opt. Lett.* **15** 1064–6

[31] Antonelli C, Mecozzi A, Shtaif M and Winzer P J 2014 *J. Light. Technol.* **32** 1853–60

[32] Jarzyna M, Garcia-Patron R and Banaszek K 2019 *2019 45th European Conf. on Optical Communication* (*ECOC*) pp 1–4

[33] Łukanowski K, Banaszek K and Jarzyna M 2023 *J. Light Technol.* **41** 5017–25

[34] Ralph T C and Lund A P 2009 *Proc. AIP Conf. Proc.* **1110** 155–60

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

[36] Ghalaii M, Ottaviani C, Kumar R, Pirandola S and Razavi M 2020 *J. Sel. Top. Quantum Electron.* **26** 1

[37] Notarnicola M N and Olivares S 2023 *Phys. Rev.* A **108** 022404

[38] Furrer F and Munro W J 2018 *Phys. Rev.* A **98** 032335

[39] Pirandola S 2019 *Commun. Phys.* **2** 1

[40] Dias J, Winnel M S, Hosseinidehaj N and Ralph T C 2020 *Phys. Rev.* A **102** 052425

[41] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 114014

[42] Serafini A 2017 *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press)

[43] Di Nicola J M 2018 *Nucl. Fusion* **59** 3

[44] Holevo A S 1998 *IEEE Trans. Inf. Theory* **44** 269–73

[45] Roumestan F, Ghazisaeidi A, Renaudier J, Vidarte L T, Diamanti E and Grangier P 2021 *European Conf. on Optical Communication (ECOC)* (IEEE) pp 1–4

[46] Roumestan F, Ghazisaeidi A, Renaudier J, Vidarte L T, Diamanti E and Grangier P 2022 Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution (arXiv:2207.11702 [quant-ph])

[47] Ferraro A, Olivares S and Paris M G A 2005 *Gaussian States in Quantum Information* (Bibliopolis Napoli)

[48] Wallucks A, Marinković I, Hensen B, Stockill R and Gröblacher S 2020 *Nat. Phys.* **16** 772–7

[49] Bersin E *et al* 2024 *PRX Quantum* **5** 010303

[50] Usenko V C and Filip R 2011 *New J. Phys.* **13** 113007

[51] Usenko V C and Grosshans F 2015 *Phys. Rev.* A **92** 062337

[52] Usenko V C 2018 *Phys. Rev.* A **98** 032321

[53] Usenko V C and Oruganti A N 2020 *43rd Int. Conf. on Telecommunications and Signal Processing* pp 421–5

[54] Derkach I, Usenko V C and Filip R 2020 *New J. Phys.* **22** 053006

[55] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1

[56] Essiambre R-J, Kramer G, Winzer P J, Foschini G J and Goebel B 2010 *J. Lightwave Technol.* **28** 662–701

[57] Schafer J, Karpov E, Pilyavets O V and Cerf N J 2016 Classical capacity of phase-sensitive Gaussian quantum channels (arXiv:1609.04119 [quant-ph])

[58] Gottesman D and Preskill J 2001 *Phys. Rev.* A **63** 022309