# Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier

Rémi Blandino,[1,*] Anthony Leverrier,[2] Marco Barbieri,[1,†]
Jean Etesse,[1] Philippe Grangier,[1] and Rosa Tualle-Brouri[1,3]

[1] *Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France*
[2] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[3] *Institut Universitaire de France, 103 boulevard St. Michel, 75005, Paris, France*

We show that the maximum transmission distance of continuous-variable quantum key distribution in presence of a Gaussian noisy lossy channel can be arbitrarily increased using a heralded noiseless linear amplifier. We explicitly consider a protocol using amplitude and phase modulated coherent states with reverse reconciliation. Assuming that the secret key rate drops to zero for a line transmittance $T_{\rm lim}$, we find that a noiseless amplifier with amplitude gain $g$ can improve this value to $T_{\rm lim}/g^2$, corresponding to an increase in distance proportional to $\log g$. This work is presented in detail in [1].

Cryptography is certainly one of the most advanced applications of quantum technologies. Within this field, the most studied primitive is quantum key distribution (QKD), which is the art of distributing a secret key to two distant parties, Alice and Bob, in an untrusted environment controlled by an adversary, Eve [2]. The security of QKD lies on the idea that an adversary trying to acquire some information about the secret key will necessarily introduce some noise in the quantum communication between Alice and Bob. A consequence of this idea is that if the quantum channel is too lossy or noisy, then it cannot be used to distill a secret key. This limits the maximum transmission distance between the legitimate parties. Developing QKD protocols resistant to losses and noise is therefore of great practical importance.

Among QKD protocols, those encoding information in the amplitude and phase of coherent states [3, 4] have the advantage of only requiring off-the-shelf telecom components, as well as being compatible with wavelength-division multiplexing, making an interesting solution for robust implementations [5]. On the theoretical side, these continuous-variable (CV) protocols have been proven secure against arbitrary attacks provided that they are secure against collective attacks [6]. This latter condition is in particular met for all CV protocols without postselection for which Gaussian attacks are known to be optimal within collective attacks [7–10].

Protocols with postselection on the other hand [11, 12], where Alice and Bob only use part of their data to extract a secret key, can increase the robustness of QKD to losses and noise but at the price of more involved security proofs. In particular, their security is only established against Gaussian attacks [13, 14], or when an active symmetrization of the classical data is applied [15].

We consider the use of a heralded noiseless linear amplifier (NLA) [16–22] on the detection stage as a way to increase the robustness of CV QKD protocols against losses and noise. First, it should be noted that while amplifiers can effectively recover classical signals, they only offer limited advantages when working on quantum signals, as amplification is bound to preserve the original signal to noise ratio (SNR) [18, 23, 24]. This implies that ordinary linear amplifiers, as those realized by optical parametric processes [25], can only find limited applications in the context of QKD [26].

On the other hand, a *probabilistic* NLA can in principle amplify the amplitude of a coherent state while retaining the initial level of noise [16]. Thus, when only considering its successful runs, the NLA can compensate the effect of losses and could therefore be useful for quantum communication [27]. The availability of such a device has stimulated intense experimental activity over the past years, demonstrating the implementation of approximated versions [17–22], which have provided solid proof-of-principle. The question arises if these more sophisticated devices can deliver a compensation of losses with a success rate such that it may represent a useful tool for quantum cryptography. Here we address this problem, by investigating the advantages and limitations of the most general NLA device, without making assumptions on the particular realization.

We consider explicitly the case for the most common protocol for continuous-variable QKD, designed by Grosshans and Grangier (GG02) [3], in its version with reverse reconciliation [4]. In a prepare-and-measure (PM) scheme, Alice encodes information in the quadratures of coherent states which are then sent to Bob through the untrusted quantum channel of transmittance $T$, and input equivalent excess noise $\epsilon$. Alice chooses her preparation $|\alpha{=}x_{\rm A}{+}ip_{\rm A}\rangle$ from a Gaussian distribution for the two quadratures having zero mean and variance $V_{\rm A}$. Bob randomly decides whether to measure the $\hat{x}$ or the $\hat{p}$ quadrature, using homodyne detection. Alice and Bob finally extract a secret key from the correlated data by performing classical data processing and authenticated clas-

* remi.blandino@institutoptique.fr
† Current address: Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU, United Kingdom

sical communication. This protocol offers a simple experimental implementation [4, 28–30] and is secure against finite-size collective attacks [31] as well as arbitrary attacks in the asymptotic limit of arbitrary long keys [6].

This protocol can be reformulated in an entanglement-based version (EB), in terms of entanglement distribution between Alice and Bob [32]: the two parties initially share a two-mode squeezed vacuum state $|\lambda\rangle=\sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle$, with $\lambda<1$. Alice performs an heterodyne measurement on her mode, which projects the other mode on a coherent state. The outcome of Alice's measurement is random, but with a probability distribution depending on $\lambda$. Although the EB version does not correspond to the actual implementation, it is equivalent to the PM version from a security point of view, and it provides a more powerful description for establishing security proofs against collective attacks through the covariance matrix of the state shared by Alice and Bob before their respective measurements.

Let us now consider the use of a NLA in the GG02 protocol. In this modified version of the protocol, Alice and Bob implement GG02 as usual but Bob adds a NLA to his detection stage, before his homodyne detection, which is assumed to be perfect. Then, only the events corresponding to a successful amplification will be used to extract a secret key. This scheme is therefore very similar to protocols with postselection. As usual, the security analysis is performed in the EB version. Here, we also restrict ourselves to the case of a Gaussian quantum channel, that is Eve is limited to perform Gaussian attacks. Since the secure key rate of the protocol depends only on the covariance matrix of Alice and Bob, it is sufficient to compute it in presence of the NLA.

Our calculation of the secret key rate with the amplifier is based on an effective system for which the security proofs are well established. Since the output of the NLA remains in the Gaussian regime, we can look for equivalent parameters of an EPR state sent through a Gaussian noisy channel. We show that the covariance matrix of the amplified state is equal to the covariance matrix of an equivalent system with an EPR parameter $\zeta$, sent through a channel of transmittance $\eta$ and excess noise $\epsilon^g$, without using the NLA (Fig. 1). The secret key rate with the NLA is then obtained by multiplying the secret key rate for successful amplifications by the success probability of the amplification. An upper bound for the success probability is derived, however the results do not depend on its precise value.

In presence of excess noise, the secret key rate against Gaussian collective attacks always becomes negative for a certain distance of transmission. We find a regime in which the NLA leads to an improvement of the maximum transmission distance attainable on a noisy and lossy Gaussian channel, by increasing the tolerable losses by an equivalent of $20\log_{10} g$ dB (Fig. 2 and 3). We also show that for given losses, the protocol is more robust against excess noise (Fig. 3).

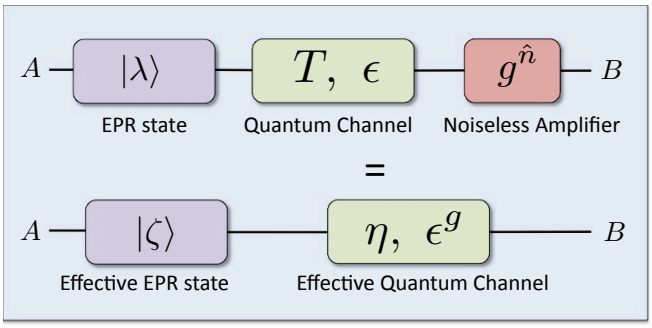


Figure 1. Equivalent channel and squeezing: a state $|\lambda\rangle$ sent through a Gaussian channel of transmittance $T$ and excess noise $\epsilon$, followed by a successful amplification, has the same Alice-Bob covariance matrix than a state $|\zeta\rangle$ sent through a Gaussian channel of transmittance $\eta$ and excess noise $\epsilon^g$, without the NLA.

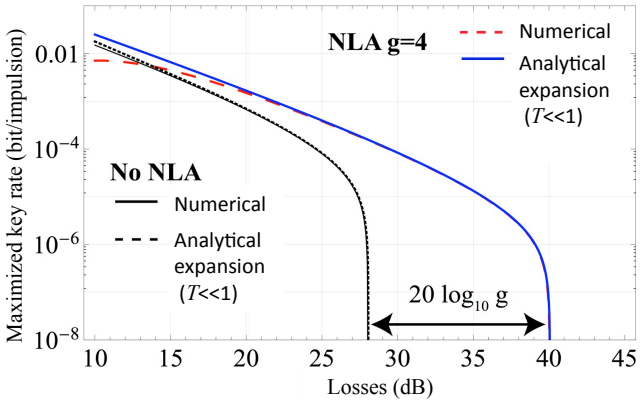


Figure 2. Maximized secret key rate as a function of the losses in dB. The secret key rate with the NLA is very optimistic due to the chosen success probability, and hence its curve gives only information on its positivity. The other parameters are excess noise $\epsilon$=0.05, and reconciliation efficiency $\beta$=0.95 [33].

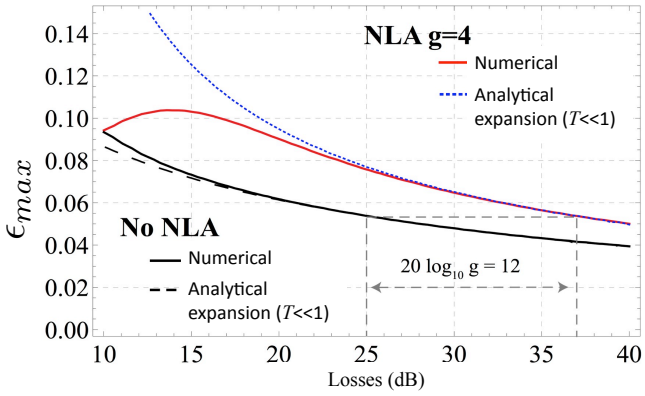


Figure 3. Maximal excess noise for which the secret key rate is positive, as a function of the losses in dB. The curves do not depend on the probability of success chosen for the NLA. The reconciliation efficiency is $\beta$=0.95 [33].

We perform series expansion of the key rate in first order in $T$, which gives us analytical formulae showing our main result. We also perform numerical studies of the full expressions, which are in excellent agreement with the series expansion.

Because of the non-deterministic nature of the NLA, the security proofs considered here are similar to those concerning protocols with postselection, that is, they hold against Gaussian attacks, or collective attacks provided an additional symmetrization of the classical data is performed.

Our approach could also find applications in other quantum communication protocols involving an EPR state sent through a quantum channel, followed by a noiseless amplifier. In particular, it could be applied to other CV QKD protocols, for instance protocols using squeezed states, or protocols using an heterodyne detection


[1] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, arXiv:1205.0959 (2012).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] F. Grosshans and P. Grangier, Physical Review Letters **88**, 057902 (2002).

[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[5] N. J. Cerf and P. Grangier, Journal of the Optical Society of America B **24**, 324 (2007).

[6] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[7] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

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

[9] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).

[10] A. Leverrier and P. Grangier, Physical Review A **81**, 062314 (2010).

[11] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[12] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[13] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[14] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[15] A. Leverrier, Phys. Rev. A **85**, 022339 (2012).

[16] T. C. Ralph and A. P. Lund, arXiv:0809.0326 (2008), quantum Communication Measurement and Computing Proceedings of 9th International Conference, Ed. A.Lvovsky, 155-160 (AIP, New York 2009).

[17] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Physical Review Letters **104**, 123603 (2010).

[18] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, Physical Review A **83**, 063801 (2011).

[19] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, Laser Physics Letters **8**, 411 (2011).

[20] A. Zavatta, J. Fiurasek, and M. Bellini, Nat Photon **5**, 52 (2011).

[21] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nature Photonics **4**, 316 (2010).

[22] M. A. Usuga, C. R. MÃ$\frac{1}{4}$ller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nature Physics **6**, 767 (2010).

[23] C. M. Caves, Physical Review D **26**, 1817 (1982).

[24] J. A. Levenson, I. Abram, T. Rivera, and P. Grangier, Journal of the Optical Society of America B **10**, 2233 (1993).

[25] R. Loudon, *The quantum theory of light* (Oxford University Press, 2000).

[26] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Journal of Physics B: Atomic, Molecular and Optical Physics **42**, 114014 (2009).

[27] T. C. Ralph, Physical Review A **84**, 022339 (2011).

[28] 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).

[29] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New Journal of Physics **11**, 045023 (2009).

[30] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, *et al.*, arXiv:1201.3744 (2012).

[31] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[32] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Info. Comput. **3**, 535 (2003).

[33] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).