Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors

M. Ghalaii[1], **R. Kumar**[2], **C. Ottaviani**[3], **S. Pirandola**[3] **and M. Razavi**[1]

1. School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK
2. Department of Physics, University of York, York YO10 5DD, UK
3. Department of Computer Science, University of York, York YO10 5GH, UK

The recent progress in continuous-variable quantum key distribution (CV-QKD) systems has placed them in a competitive position with their conventional discrete-variable counterparts [1]. In particular, CV-QKD might be a better choice over short distances. When it comes to long distances, however, the story is different. One of the proposed solutions to improve the rate-versus-distance performance of CV systems is to use noiseless linear amplifiers (NLAs) [2]. A realistic analysis that accounts for non-idealities of existing NLAs is, however, missing. One of the most well-known NLAs is based on quantum scissors (QSs) [3], whose ideal operation relies on the assumption that an input coherent state would be mapped, probabilistically, to an amplified coherent state. This would preserve the Gaussianity of the channel. In this study, we calculate the secret key rate of the GG02 protocol [4] enhanced by a single QS, see Fig. 1(a), by properly modeling the QS operation. We remove the Gaussian assumption in the QS modeling and find regimes of operation where QS-assisted GG02 offers advantages over the conventional GG02 system. We show that the rate enhancement is achieved after a certain cross-over distances. Remarkably, our rate is able to nearly reach the ultimate repeater-less bound for QKD, known as the PLOB bound [5], by a proper setting of the QS parameters.

Our QS-amplified GG02 system is described as follows. The sender sends Gaussian modulated coherent states with variance V_A to the receiver through a quantum channel of length L. The receiver first amplifies the states using a QS and then measures randomly either of the quadratures using a homodyne detector; Fig. 1(a). The QS is considered successful if only one of its detectors clicks. By finding the exact output state of the QS—using characteristic-function relationships—we are able to estimate the effective gain and the excess noise that the QS produces; hence, being able to give an accurate estimate of the key rate.

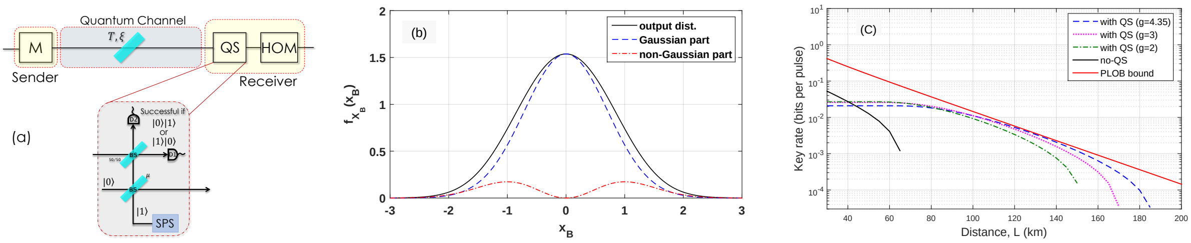

Fig. 1. (a) A CV-QKD link with an additional QS at the receiver. (b) Output distribution at the receiver side, which comprises Gaussian (dashed blue) and non-Gaussian (dot-dashed red) parts. The plots are for $\mu = 0.2$ and $V_A = 0.05$. (c) The secret key rate for no-QS and QS-based systems, at different gain values $g = \sqrt{(1-\mu)/\mu}$, as compared to the PLOB bound.

Note that because of removing the Gaussian assumption, the output state is no longer a coherent state; thus, the QS operation cannot be noiseless and the generated noise will be detrimental to the performance of the GG02 protocol. Moreover, the output distribution becomes non-Gaussian, see Fig. 1(b), which makes the conventional methods for evaluation of the key rate insufficient. In order to find a lower bound on the key rate we have to calculate the relevant Holevo and mutual information functions in a non-Gaussian setup. In our case, we find the exact values for the mutual information between Alice and Bob, and use a Gaussian approximation approach to come close to the upper bound of the Holevo information term in the key rate. Figure 1(c) shows that, after a certain distance, the QS-based system outperforms the no-QS one and its rate approaches the fundamental rate-loss scaling given by PLOB bound in long distances. There also seems to be an optimum gain for each given distance. We note that the single-photon source in our analysis is assumed to be ideal. Nevertheless, with recent progress in quantum-dot sources, it is expected that the QS-based system can offer enhancement in realistic setups as well. Our study would be highly relevant in analyzing the performance of recently proposed CV quantum repeaters [6], which rely on a similar building block. This study is partly funded by the White Rose Research Studentship and the UK Quantum Communications Hub EPSRC Grant EP/M013472/1.

References

[1] P. Jouguet, *et al.*, Nature Photonics **7**, 378 (2013).
[2] R. Blandino, *et al.*, Phys. Rev. A **86**, 012327 (2012).
[3] T. C. Ralph and A. P. Lund, arXiv:0809.0326
[4] F. Grosshans, *et al.*, Nature **421**, 238 (2003).
[5] S. Pirandola, , *et al.*, Nature Communications **8**, 15043 (2017).
[6] J. Dias and T. C. Ralph, arXiv:1505.03626