Exploring The Potential of Probabilistic Shaping Technique in Quantum Key Distribution Systems

Emanuele Parente[1], Michele Notarnicola[2,3], Stefano Olivares[2,3], Enrico Forestieri[1], Marco Secondini[1] and Luca Potì [1]

[1] *TeCIP Institute, Scuola Superiore Sant'Anna, Via G. Moruzzi 1, 56124, Pisa, Italy*
[2] *Dipartimento di Fisica "Aldo Pontremoli", Universit'a degli Studi di Milano, I-20133 Milano, Italy*
[3] *INFN, Sezione di Milano, I-20133 Milano, Italy*

[*] *opex@optica.org*

Abstract: We investigated the role of probabilistic shaping in the optimization of the secure key rate of a continuous variable quantum key distribution system with discrete modulation in both homodyne and heterodyne scheme.

1. Introduction

Quantum key distribution (QKD) is a branch of quantum cryptography offering a way to generate a one-time pad secure key among two remote authenticated parties, say Alice and Bob, despite the presence of a powerful adversary Eve [1]. In particular, the continuous variable (CV-QKD) family of QKD protocols results interesting in terms of high detection efficiency, low-costs implementation and high compatibility with existing telecom equipment [2].
The simplest CV-QKD protocol was introduced by Grosshans and Grangier in 2002 (GG02) and it employs Gaussian modulation (GM), since this choice maximizes the Mutual Information (MI) between Alice and Bob over a Gaussian channel (GC). However, the finite resolution of the analog-to-digital converter and the finite working input power of the laser bring some issue in its practical implementation: the need for a higher reconciliation efficiency made the discrete modulation formats gain interest in the scientific community [3]. In this regard, the quadrature-amplitude modulation (QAM) format gives nearly optimal performances in classical communication systems because of its high post-processing efficiency and since, if used together with the Probabilistic Amplitude Shaping (PAS) technique, it provides a solution in reducing the gap with the Shannon capacity of a GC [4]. In particular, QAM can open the way to implementation of CV-QKD systems with large modulation variance, solving the problem to work at extremely low Signal-to-Noise Ratio [5].
The performance of a QKD system can be evaluated in terms of the Secure Key Rate (SKR), measured in bit/s and representing the difference between the amount of information shared by Alice and Bob (MI) and that stolen by Eve, i.e. the Holevo Information (HI). In this paper we extend our previous work [6] in order to explore, theoretically, the possibilities offered by the combination of PAS technique and QAM in CV-QKD systems in the case of a pure-loss wiretap channel, for higher cardinality of the modulation alphabet and for both homodyne and heterodyne measurements.

2. Results

We will focus on the Collective Attacks case (Coll. Att.) and only the Reverse Reconciliation (RR) will be taken into account, as in this scheme the amount of information Alice gains about Bob is always higher then that in the hands of Eve for any transmittance value. [2]. The expression of the SKR in the RR picture is:

$$SNR^{(RR)}_{Coll.\ att.} = \xi I_{AB} - \chi_{BE} = \xi I_{AB} - \left[S(\rho_E) - \int p(x_B) S(\rho_{E|B}) dx_B \right] \tag{1}$$

where I_{AB} is the MI between Alice and Bob, χ_{BE} is the HI between Bob and Eve and ξ is the reconciliation efficiency (here fixed at 0.95). The goal of our research is not dealing with security proofs, but with what Alice can do at her best in order to limit Eve's possible information about the key. Therefore, we model the channel as a wiretap one[1] and show the effects on the SKR of a non-uniform samplings of the input symbols at different distances. Specifically, we employ a Maxwell-Boltzmann (MB) distribution as this is the one ensuring the maximization of the entropy of the source for a classical system affected by a maximum average power usage [7] and we use it

[1] In this scenario Eve can only gain information by collecting the fraction of signals that are lost along the channel, but she cannot alter the quantum nature of the signals.

to maximize the whole SKR expression in eq. (1) (for more details see [6]). We define: I) R as the ratio between the maxima of the optimized (PS) and uniform (U) 16 QAM and 64 QAM with respect to those obtained with a continuous modulation (CM); II) SKR_{max} the maxima for 16 QAM modulation with homodyne and heterodyne detection at different distances.

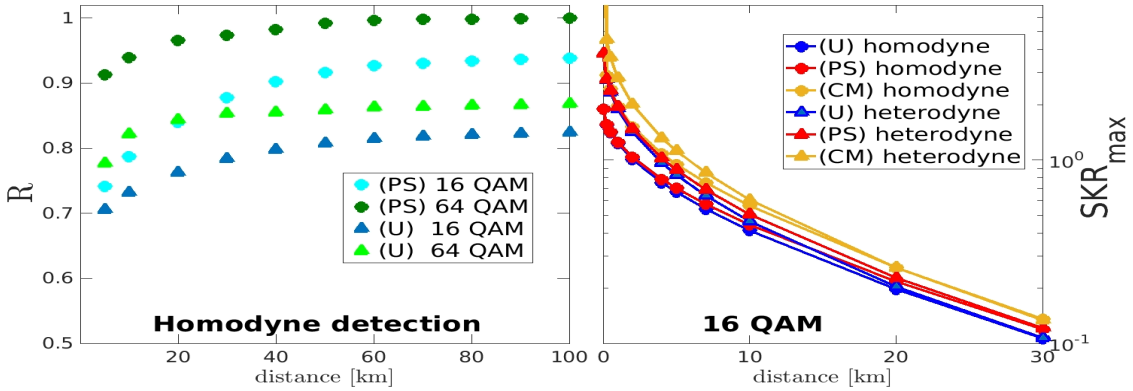

Fig. 1. R for (PS) and (U) 16 QAM, (PS) and (U) 64 QAM in homodyne scheme (left); SKR_{max} maxima for 16 QAM in homodyne and heterodyne detection (right).

The advantage given by the use of MB highlights in the long-distance regime (i.e. where the threat of Eve grows). This gain results more important for larger QAM constellation, as a consequence of the availability of a larger statistical ensemble: (PS) - 64 QAM at 20 *km* outcasts the long-distance performance of (PS) - 16 QAM, being able to reach already 95% of the (CM) limit (left graph). From the graph on the right side we notice that, with respect to the homodyne, doing heterodyne gives better results only at small distances: this is due to the trade-off between the increase of accessible information bits and the halving of the number of signal photons in heterodyne detection [2]. However, as the distances become shorter, the SKR_{max} becomes more and more constrained by the cardinality of the constellation.

3. Acknowledgement

This work was supported in part by the by PNRR MUR project PE0000023-NQSTI, by the National Operational Programme on Research and Innovation 2014–2020 - FSE REACT EU “Azione IV.5 Dottorati su tematiche Green”, and by the Quantum Pathfinder project funded by Scuola Superiore Sant’Anna.

4. Conclusions

The combined use of MB and QAM in CV-QKD system is able to reduce substantially the gap with the (CM) of GG02 protocol both in homodyne and heterodyne cases. In particular, at long distances the 64-QAM format is more convenient and it approaches the (CM) limit, while at small distances heterodyne detection performs better.

References

1. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.
2. Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.
3. Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical review letters*, 102(18):180504, 2009.
4. François Roumestan, Amirhossein Ghazisaeidi, Jérémie Renaudier, Luis Trigo Vidarte, Anthony Leverrier, Eleni Diamanti, and Philippe Grangier. Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution. *arXiv preprint arXiv:2207.11702*, 2022.
5. Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, 2021.
6. Michele N Notarnicola, Stefano Olivares, Enrico Forestieri, Emanuele Parente, Luca Potì, and Marco Secondini. Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel. *IEEE Transactions on Communications*, 2023.
7. Frank R Kschischang and Subbarayan Pasupathy. Optimal nonuniform signaling for gaussian channels. *IEEE Transactions on Information Theory*, 39(3):913–929, 1993.