Achieving CV-QKD GG02 Performance with QAM modulation and Probabilistic Shaping in a Linear Quantum Channel Scenario

Emanuele Parente[1], Michele Notarnicola[2,3], Stefano Olivares[2,3], Enrico Forestieri[1], Luca Potì[4], Marco Secondini[1]

1. TeCIP Institute, Scuola Superiore Sant'Anna, Via G. Moruzzi 1, 56124, Pisa, Italy

2. Dipartimento di Fisica "Aldo Pontremoli", Università degli Studi di Milano, I-20133 Milano, Italy

3. INFN, Sezione di Milano, I-20133 Milano, Italy

4. Photonic Networks and Technologies Laboratory, CNIT, Via G. Moruzzi 1, 56124, Pisa, Italy

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 a linear quantum channel.

Quantum key distribution (QKD) guarantees the generation of a one-time pad secure key among two remote authenticated parties despite the presence of a powerful adversary. In particular, continuous variable (CV-) QKD protocols have recently gained increasing attention due to their ability to operate with standard optical devices employed for classical communications, avoiding the use of single-photon sources and detectors. The ideal benchmark protocol for CV-QKD is GG02, where coherent states extracted according to a Gaussian distribution are used [1]. Gaussian variables provide a straightforward theoretical framework for security analysis but are hard to manipulate in practice. This is where discrete modulation formats come in, being based on simple and practical modulation schemes that can be seamlessly integrated with modern fiber optic communication devices. Among them, QAM ensures a good use of the available bandwidth, a high reconciliation efficiency [2], and it can be conveniently combined with probabilistic amplitude shaping (PAS), a technique in which the coherent states are drawn from a Maxwell–Boltzmann (MB) distribution to increase the information rate for a fixed launch power [3]. However, the security proofs for CV-QKD with QAM are less advanced than those for GG02.

Here we extend our previous work on the wiretap channel [4] and consider the more general security scenario of a linear quantum channel: using the numerical bound for the asymptotic secure key rate (SKR) introduced by Denis et al. [5], we compare, for different values of excess noise (ξ) and up to 300 km, the performance of a homodyne QAM-based CV-QKD protocol with either uniform (U) or PAS signaling with that of homodyne GG02. Fig. 1 illustrates (left) the maximum SKR and (right) the maximum tolerable excess noise ξ_{max} as functions of distance for U-QAM and PAS-QAM with various alphabet sizes, as well as for GG02 .

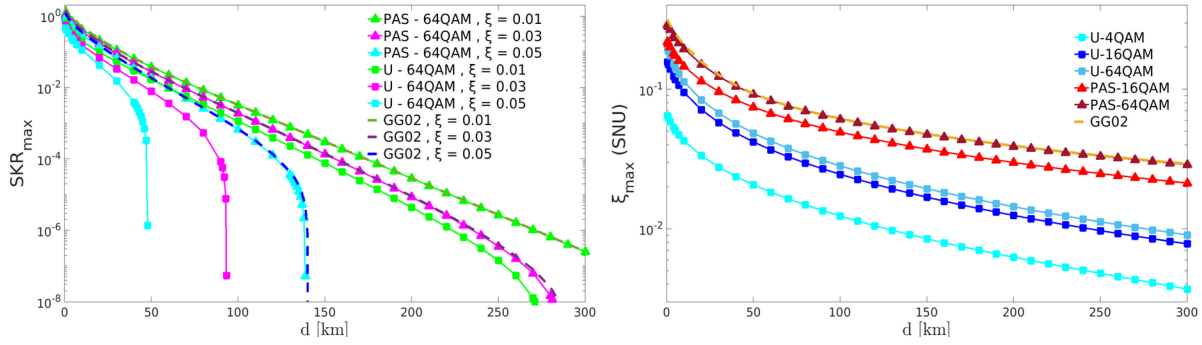

Fig. 1 (Left) Maximum SKR for various excess-noise levels and (right) maximum tolerable excess noise for GG02, U-QAM, PAS-QAM.

MB-distributed PAS-QAM proves to be an effective and practical approach for CV-QKD, especially in the long-range regime. Beyond 40 km, PAS-64QAM practically achieves the same performance and excess-noise tolerance as ideal GG02. At any distance, PAS significantly improves QAM performance compared to a uniform distribution, with the simpler PAS-16QAM outperforming the more complex U-64QAM and showing greater robustness to excess noise.

References

[1] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. Physical review letters, 88(5):057902, 2002.

[2] E. Kaur, S. Guha, and M. M. Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. Physical Review A, 103(1):012412, 2021.

[3] F. R. Kschischang and S. Pasupathy. Optimal nonuniform signaling for gaussian channels. IEEE Transactions on Information Theory, 39(3):913–929, 1993.

[4] M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini. Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel. IEEE Transactions on Communications, 2023.

[5] A. Denys, P. Brown, and A. Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum, 5:540, 2021.