Assisting Discrete-Modulation CV-QKD with Soft-Decoding Strategy in Reverse Reconciliation

Emanuele Parente[1], **Marco Origlia**[1,2], **Marco Secondini**[1]

1. *TeCIP Institute, Scuola Superiore Sant'Anna, Via G. Moruzzi 1, 56124, Pisa, Italy*
2. *National Council of Research (CNR-IEIIT), Pisa, Italy*

Abstract: We analyze a QAM-based continuous variable quantum key distribution protocol with a novel soft decoding technique under collective attacks, reverse reconciliation, uniform signaling and infinite key size.

Quantum key distribution (QKD) allows two remote authenticated parties to establish a theoretically-secure key under an unrestricted eavesdropper. QKD requires a quantum channel for the optical signals exchange and an authenticated classical channel for the reconciliation stage. Among various QKD schemes, continuous variable (CV-) QKD protocols can be realized with off-the-shelf classical telecom devices and detection techniques, making them advantageous for implementation over optical fibers. The benchmark is the GG02 protocol [1], based on the use of coherent Gaussian modulated (GM) states and enabling a simple theoretical framework for security proofs. On the other hand, the choice of a GM for on-field realizations introduces many practical difficulties at both the sender and the receiver side [2], making discrete modulation schemes preferable. Reconciliation is the main bottleneck in CV-QKD, limiting both the secret key rate (SKR) and the maximum transmission distance d_{max} [3]. In the asymptotic limit, its performance is quantified by the reconciliation efficiency ζ [4], with ideal value ζ=1.

In this work we study collective attacks with reverse reconciliation in the asymptotic regime of infinite key size, and we employ both the soft reconciliation scheme introduced in [5] based on the disclosure of additional parameters that do not reveal more information to the eavesdropper than the standard error-correction syndrome, and a hard reconciliation scheme in which the only information in Alice's hands is the knowledge of the transmitted sequence of symbols. Using the numerical bound introduced by Denis et al. [5], we analyze the transmission along a linear quantum channel, the latter characterized by a linear relation between the input and output quadratures, for different distances d and excess noise values ξ, and employ uniform signaling for 16QAM and 64QAM constellations, where the QAM format is adopted due to its efficient utilization of the available bandwidth [4]. Fig. 1 shows the maxima of the SKR, over the distance range [0.5 , 120] km with soft (ζ_{soft}), hard (ζ_{hard}) and ideal (ζ_{ideal}) reconciliation in the case of ξ = 0.03, 0.05 (shot noise units, SNU) for 16QAM (left) and 64QAM (right).

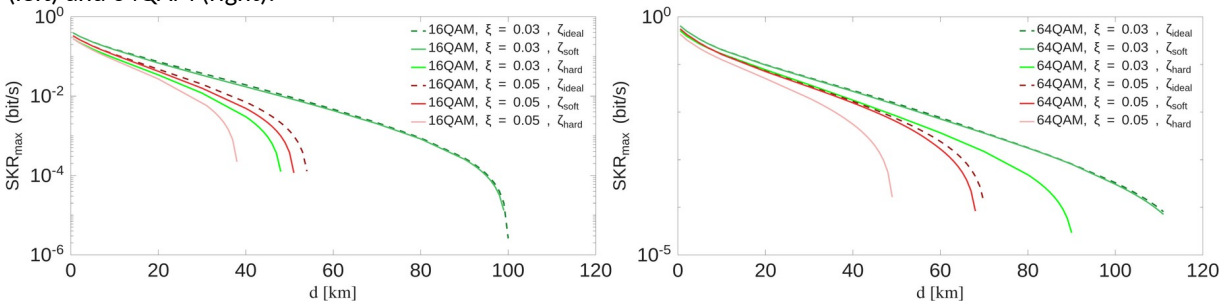

Fig. 1 Maxima of the SKR for U-16QAM (left) and U-64QAM (right) for ξ = 0.03, 0.05, in the range [0.5, 120] km, with soft, hard and ideal reconciliation.

Our soft reconciliation improves the performance of both 16QAM and 64QAM across all evaluated excess noise values; in particular, the soft reconciliation scheme allows ζ_{soft} to closely approach 1, enhancing the protocol's resilience to loss and noise. Compared to ζ_{hard}, the maximum transmission distance d_{max} increases with ζ_{soft} for both 16QAM and 64QAM with ξ = 0.03 and ξ = 0.05. Moreover, we can notice that, for 16QAM, our soft scheme with ξ = 0.05 outperforms the hard scheme with ξ = 0.03.

Example References

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

[2] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," Applied Physics Reviews, vol. 11, no. 1, 2024.

[3] A. Leverrier et al., "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A, vol. 77, no. 4, Apr. 2008.

[4] Origlia, Marco, and Marco Secondini. "Soft reverse reconciliation for discrete modulations." *2025 14th International ITG Conference on Systems, Communications and Coding (SCC)*. IEEE, 2025.

[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.