Reverse Reconciliation Softening for CV-QKD with Discrete Modulations

Marco Origlia[1,2,3], **Marco Secondini**[1]

1. Scuola Superiore Sant'Anna, Istituto di Telecomunicazioni, Ingegneria Informatica e Fotonica, via Moruzzi 1 - 56124 Pisa, Italy

2. Consiglio Nazionale delle Ricerche, Istituto di Elettronica, Ingegneria Informatica e Telecomunicazioni, via Caruso 16 - 56122 Pisa, Italy

3. Sma-RTy Italia SRL, via Alessandro Volta 16 - 20093 Cologno Monzese, Italy

Abstract: We propose a reverse reconciliation scheme for continuous-variable quantum key distribution using QAM constellations. To allow soft-decoding error correction on Alice's side, Bob shares soft information that is independent of his decision variables.

Information reconciliation is a crucial post-processing task in quantum key distribution (QKD) that takes place after the transmission of quantum states. In continuous variables (CV) QKD, soft information is readily available to Bob, who can use it to perform error correction in a so-called direct reconciliation (DR) scenario. However, reverse reconciliation (RR), in which Alice performs error correction, is usually preferred due to its superior performance compared to DR. For CV-QKD with continuous modulations, effective RR schemes [1, 2] are available. However, for discrete modulations, only RR schemes for BPSK and QPSK in AWGN channels have been studied [3]. In this work, we generalize such schemes to QAM modulations with higher order.

Fig. 1 (left) gives an overview of the proposed scheme. The core idea is that, upon reception of a channel output y, Bob takes the MAP decision $\hat{x}$ by locating which decision region y lays in, and he computes a soft metric, namely n, corresponding to the cumulative density function (CDF) of Y at y, conditioned to Y laying in such decision region. It is immediate to show that the distribution of n does not depend on $\hat{x}$, because it is always uniformly distributed in [0,1], therefore its public announcement does not reveal any information about Bob's received data when no information is known about the transmitted symbols. Conversely, Alice enjoys the advantage of knowing which symbol x was transmitted. She can compute a log-*a posteriori*-probability ratio (LAPPR) that accounts both for x and for n to initialize a soft decoder.

We assessed the feasibility of this scheme by Monte Carlo simulations, where the error correction procedure we apply on top of our scheme is an LDPC code: Bob computes the syndrome associated with the received symbol sequence and announces it publicly, then Alice feeds the syndrome and the computed LAPPRs to an LDPC decoder implementing the sum-product algorithm. We used a standard DVB/S2 LDPC code with rate ½ and blocklength 64800, and we tested our scheme on a PAM-4 modulation.

The gap between the performance of DR and hard-information-only RR is partially filled by our RR scheme, denoted with C_A in Fig. 1 (right). Performance can be further improved by scaling the LAPPR by a non-unitary coefficient α, suggesting that the proper scheme variations, currently under investigation, may lead to further performance improvements for RR with discrete modulations.

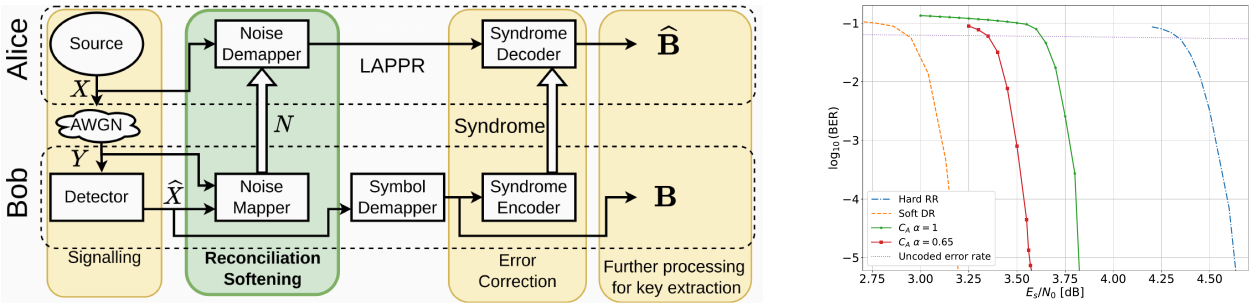

Fig. 1. (left) Overview of the soft RR scheme; (right) comparison of BER curves for a PAM-4 modulation with different schemes.

Example References

[1] A. Leverrier et al., "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A, **77** (2008).
[2] G. Van Assche, J. Cardinal, and N. Cerf, "Reconciliation of a quantum-distributed gaussian key," IEEE Trans. on Inf. Th., **50**, (2004).
[3] A. Leverrier, 'Theoretical study of continuous-variable quantum key distribution', p. 267.