Error Correction and Multidimensional Reconciliation in CV-QKD

Lucien Martial[1,2], Alexis Rosio[2], Eleni Diamanti[2], Adrien Cassagne[2] and Baptiste Gouraud[1]
[1]*Exail, F-25000, Besançon, France*
[2]*LIP6, Quantum Information, Sorbonne Université, CNRS, F-75005 Paris, France*

Quantum key distribution (QKD) enables two parties to establish a secret key with information-theoretic security (ITS), guaranteeing security against adversaries with unlimited computational power based on the laws of quantum physics.

In continuous-variable QKD (CV-QKD), information is encoded in the quadratures of coherent optical states, enabling implementations based on mature telecommunications technology with low-cost, high-performance optical components while avoiding single-photon detectors. However, these advantages come with increased complexity in classical post-processing, particularly at high loss. At long distances, CV-QKD operates at low signal-to-noise ratios (SNRs), where quantum vacuum noise dominates. Multidimensional reconciliation addresses this challenge by transforming the physical Gaussian channel into a virtual binary-input additive white Gaussian noise (BIAWGN) channel, enabling the use of modern binary error-correcting codes.

In this low-SNR regime, efficient error-correcting codes are essential to approach the Shannon capacity while maintaining a sufficiently high decoded information rate.

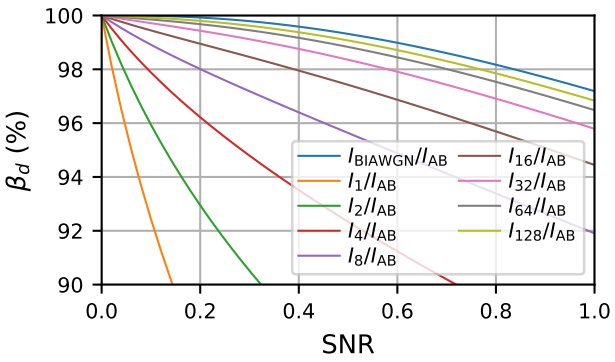


FIGURE 1 – Intrinsic reconciliation efficiency of the virtual channel as a function of the SNR. I_d denotes the channel capacity, with the numerical value indicating the dimension of the reconciliation. I_{AB} represents the quantum channel.

We first introduce the basic concepts of error-correcting codes, focusing on linear and Low Density Parity Check (LDPC) codes, and then describe multidimensional reconciliation and its transformation into a virtual BIAWGN channel. We investigate reconciliation dimensions beyond 8 [1] (see Figure 1) and introduce HDIRAC [2], an open-source implementation of state-of-the-art reconciliation approaches integrated with AFF3CT [3]. The resulting framework enables reproducible simulation and comparison of reconciliation strategies using open-source LDPC matrices representative of the current state of the art [4]. We evaluate several high-dimensional configurations and identify significant performance variations between reconciliation dimensions and schemes, including previously unreported behaviours.

[1] L. Martial *et al.*, "Multidimensional Reconciliation in Continuous-Variable QKD : Review, Coding Schemes, and Open Source Simulation," arXiv :2606.02323 (2026).
[2] HDirac v1.0.0 (2026). `https://github.com/aff3ct/HDirac`.
[3] A. Cassagne *et al.*, "AFF3CT : A Fast Forward Error Correction Toolbox !", SoftwareX **10**, 100345 (2019). doi :10.1016/j.softx.2019.100345.
[4] E. E. Cil and L. Schmalen, "An open-source library for information reconciliation in continuous-variable QKD," QCRYPT (2024). `https://arxiv.org/abs/2408.00569`.