Optimal realistic attacks in continuous-variable quantum key distribution

Nedasadat Hosseinidehaj[1], Nathan Walk[2,3], and Timothy C. Ralph[1,2]

[1]Centre for Quantum Computation and Communication Technology,
School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia.

[2]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany.

[3]Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom.

Abstract

In quantum cryptography we typically assume that opponents can carry out all physical operations, thus granting capabilities far in excess of present technology. Assuming more realistic capabilities is an attractive prospect, but can only be justified with a rigorous framework that relates adversarial restrictions to security. We investigate limitations on the eavesdropper's (Eve's) ability to make coherent attacks on the security of continuous-variable quantum key distribution (CV-QKD). We show that when the decoherence is greater than some threshold, Eve's best strategy reduces to an individual attack, significantly improving performance in terms of both key rate and maximum transmission distance.

CV-QKD is a promising avenue for high speed, secure communication, using cheap, efficient components that are compatible with existing telecommunications infrastructure. However, establishing composable security against arbitrary attacks has been extremely challenging. A general security proof that can certify rates approaching the asymptotic (in n, the number of exchanged signals) limit has only recently appeared [2] and in practical instances this result yields modest rates over short distances. We address this problem by exploiting the fact that making the most powerful attacks represents an extreme challenge for Eve, requiring a quantum memory and many multi-mode, coherent operations. Without these resources, Eve is forced to measure her quantum state immediately in a so-called individual attack. We model Eve's equipment as being decohered by a thermal channel of varying transmissivity, τ, and, constructing the optimal hybrid eavesdropping strategy, bound the aysmptotic and finite-size key rates as a function of τ (Fig. 1, left). We also find decoherence thresholds beyond which Eve's optimal strategy is always an individual attack, and we show a substantial improvement in the key rate and maximum transmission distance for realistic parameters (Fig. 1, right).

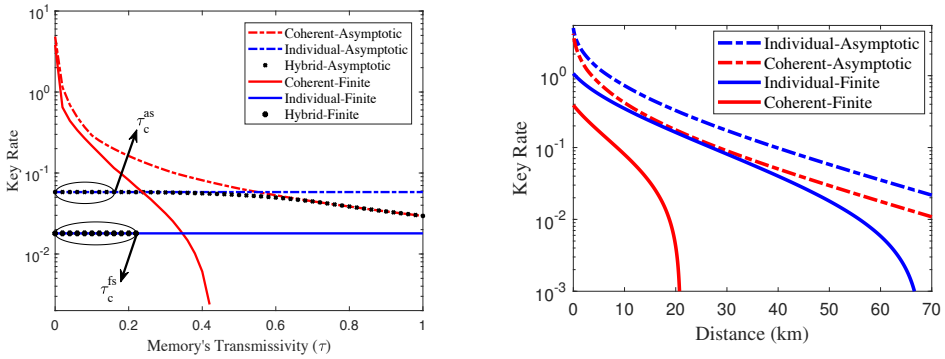

Figure 1: Left: finite-size and asymptotic key rate as a function of memory transmissivity, τ, for individual, coherent, and hybrid attacks. System parameters are based on experimental implementations as explained in [1]. Regions where individual attacks are optimal are marked with ellipses. Right: finite-size and asymptotic key rates as a function of channel distance (assuming 0.2dB loss/kilometer) for individual and coherent attacks.

[1] N. Hosseinidehaj, N. Walk, & T. C. Ralph, *Optimal realistic attacks in continuous-variable quantum key distribution*, arXiv:1811:05562 (2018).

[2] A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, Phys. Rev. Lett. **118,** 200501 (2017)