Simulating realistic effects on MDI-QKD

Vicente Gonzalez Bosca
Daniel Cano Reol, Veronica Fernandez Marmol
CSIC, C/ Serrano 144, Madrid, Spain
vicente.bosca@csic.es

Quantum Key Distribution (QKD) allows two parties to exchange a secret key with unconditional security by exploiting the principles of quantum mechanics [1]. However, one of the most critical problems is that imperfections in real instruments may allow attacks that compromise the security of the shared key. Several relevant attacks exploit the scenario where measurement devices are under partial or total control of a third party [2-3]. The Measurement Device Independent (MDI) protocol proposes a communication scheme that is secure even when the measurement devices are in the hands of a third party [4]. To do so, the two parties that wish to share a key become photon emitters (Alice and Bob), sending their respective encoded signals to a relay station where all the measurements occur (Charlie). After measurements are done, Charlie announces the results so Alice and Bob can distill a key and evaluate whether an eavesdropper has interfered in the communication. One can assume that Charlie is under complete control of a malicious third party and still ensure unconditional security. The security of MDI-QKD relies on the violation of a Bell inequality by Hong-Ou-Mandel interference (HOM), which requires Alice's and Bob's signals to be identical in frequency and arrive at Charlie at the same time. Even though MDI-QKD has proven to be immune to any side channel attack to the detectors, its efficiency is very sensitive to small deviations of the quantum states. In this study, we explore the impact of these deviations on the communication process, the Quantum Bit Error rate (QBER), and the key rate. To do so, we have created a realistic simulation of the protocol by including these imperfections in the detection probabilities. We have also considered other deficiencies such as polarization and phase mismatch, losses in the channel, limited efficiencies of the detector, and their dark counts. Thus, we use this realistic simulation to tune in the parameters of the protocol (width of the weak coherent pulses, intensities of the decoy states, emission frequency…) to increase the efficiency of secret key transmission. This simulation environment is also critical to set the requirements of the devices used in the implementation of the protocol.

References

[1] Heihu Xu et al., Rev. Mod. Phys. 92, 025002 (2020)
[2] Bing Qi et al., Quantum Information and Computation, vol. 7 (2007) pp. 073-082
[3] L. Lydersen et al., Nature Photonics 4, (2010) pp. 686-689
[4] Lo, H.-K., M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).

Figures

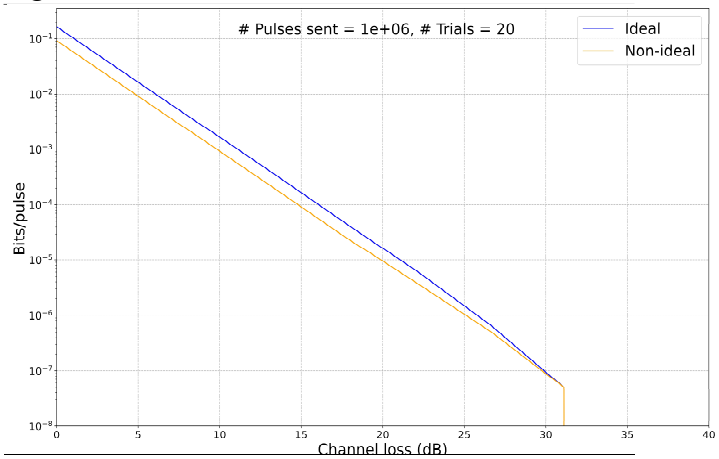

Figure 1: Bits/pulse VS. Channel loss of an ideal a non-ideal stochastic simulation of the MDI-QKD protocol. Imperfections include polarization and arrival times mismatch, fluctuations of laser frequency; efficiency and jitter of the detectors, and dark and solar counts. These flaws decrease the number of key bits generated with the same number of pulses sent, thus decreasing the key rate. The simulation allows to evaluate the impact of the different defects with respect to an ideal transmission scenario.