Security proof of discrete-modulated continuous-variable quantum key distribution

Antonio Acín

ICFO-The Institute of Photonic Sciences, 08860 Castelldefels (Barcelona), Spain

antonio.acin@icfo.eu

Continuous variable quantum key distribution with discrete modulation has the potential to provide information-theoretic security using widely available optical elements and existing telecom infrastructure. While their implementation is significantly simpler than that for protocols based on Gaussian modulation, proving their finite-size security against coherent attacks poses a challenge. We consider protocols in which, contrary to previous approaches, all the information is discretized. This allows using standard techniques developed in the discrete-variable scenario to prove the security of these protocols, with no significant loss in the key rate. We discuss several variants of these protocols and their security, the theoretical and implementation challenges and how the use of post-selection may open promising avenues to address them.

References

[1] S. Bäuml, C. Pascual García, V. Wright, O. Fawzi, A. Acín, arXiv:2303.09255.

Figures

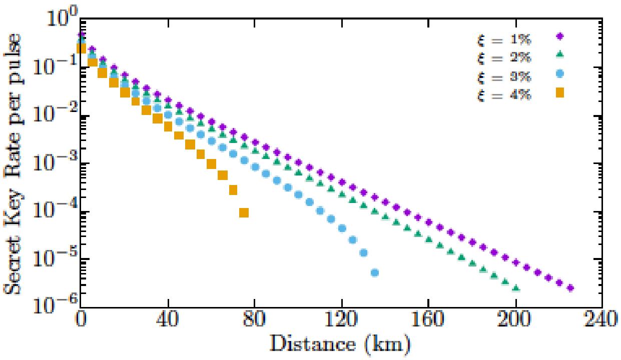

Figure 1: Asymptotic secret key generation rate in terms of distances D and excess noise.