Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation: Abstract

Aurélie Denys [1], Peter Brown [2], Anthony Leverrier [1]

[1] Inria Paris, France
[2] ENS Lyon, France

Quantum key distribution (QKD) enables two distant parties, a sender Alice and a receiver Bob, with access to a quantum channel and an authenticated classical channel, to establish a uniform shared secret key. Historically, QKD protocols relied on the exchange of discrete variables (DV) encoded for instance on the polarisation of single photons. Those protocols require single-photon detectors which are expensive and suffer from imperfections, as compared to the coherent detection devices used in continuous-variable (CV) QKD. However, the security proofs for CV QKD are less advanced. The only continuous-variable protocols whose full composable security proofs are well understood use a Gaussian modulation of coherent states. In such protocols, Alice needs to draw a random complex variable from a Gaussian distribution and send the corresponding coherent state to Bob. In practice, however, the number of coherent states available is necessarily finite and a perfect Gaussian distribution is thus impossible to achieve. Protocols using a discrete modulation of states are therefore more appealing. Some recent works [1, 2] enabled to compute numerical bounds on the asymptotic secret key rate for protocols with four states. However, because these approaches were computationally intensive, they could not be applied to modulations with more than a few states. In particular, the more relevant case of quadrature amplitude modulation (QAM), consisting of a grid of weighted coherent states lying on a grid in phase-space, could not be analysed using this method. We solve this problem here: we give an explicit analytical formula for the asymptotic secret key rate of any CV QKD protocol. This result opens the way towards the derivation of a full composable security proof in the finite size regime. It also enables to compare the performance of various protocols. In particular, our bound shows that constellations of 64 states are sufficient to get results similar to those obtained with a Gaussian modulation. Such constellations are therefore an attractive solution for the large-scale deployment of CV QKD.
See full version at https://doi.org/10.22331/q-2021-09-13-540.

---

[1] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X*, 9:021059 (2019).

[2] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X*, 9:041064 (2019).