CC-04-07

Finite-key security of continuous-variable quantum key distribution

Masato Koashi

Univ. of Tokyo

Abstract

The security of quantum key distribution is often proved in the asymptotic regime, but in order to establish security for an actual implementation, one needs to prove it in the finite-key regime where the communication time is finite. Although a conventional approach to the security using phase errors in qubits excels in dealing with finite-size statistics, the use of qubits limited its use to discrete-variable QKD protocols with photon detectors until recently. Here I will explain how we can apply this approach to a two-state continuous-variable QKD protocol with homodyne/heterodyne detection to prove its finite-key security against general attacks.