Security of quantum key distribution with imperfect devices

Hoi-Kwong Lo
Dept. of Electrical & Computer Engineering
University of Toronto
10 King's College Road
Toronto, Ontario
CANADA M5S 3G4

Abstract

We prove the security of the Bennett-Brassard (BB84) quantum key distribution protocol in the case where the source and detector are under the limited control of an adversary. Our proof applies when both the source and the detector have small basis-dependent flaws, as is typical in practical implementations of the protocol. We estimate the key generation rate in some special cases: sources that emit weak coherent states, detectors with basis-dependent efficiency, and misaligned sources and detectors.