Quantum Privacy Amplification

Nicolas Gisin (nicolas.gisin@physics.unige.ch)
University of Geneva
Group of Applied Physics
20, rue de l'École de Médecine
CH-1211 Geneva 4
Switzerland

Abstract.

In quantum cryptographic protocols, once the qubits (or qudits) have been distributed to the partners, the information may be processed either classically (i.e. perform measurements and process the classical data) or quantum mechanically (i.e. entanglement distillation). If the used quantum communication channel is noisy, both the classical and the quantum processing may provide secrecy, provided the noise is not too large, i.e. below some thresholds. In this talk, I will address the question of comparing these classical and quantum thresholds. Protocols using 1-way and 2-way classical communication will both be considered.