ABSTRACT

CTIC workshop:
Quantum Information & Quantum Cryptography
October 19-23, 2015
Aarhus University, Denmark

Title: Security analysis for round-robin differential-phase-shift quantum key distribution

Xiongfeng Ma

In quantum key distribution (QKD), the information leakage due to eavesdropping is normally monitored by channel disturbance, such as bit errors. For instance, in Shor-Preskill security proof [PRL 85, 441 (2000).], the information leakage quantified by phase error rate is estimated by the bit error rate. Thus, the privacy amplification that removes leaked key information normally relies on the error rate. Recently, a round-robin differential-phase-shift (RRDPS) QKD protocol for which privacy amplification does not rely on channel disturbance was proposed [Nature 509, 475 (2014)], see also, its experimental demonstrations [PRL 114.180502 (2015); arXiv:1505.07914; arXiv:1505.07884; arXiv:1505.08142]. In the RRDPS QKD protocol, the information leakage is bounded by the state preparation stage. In security analysis, we present a tight bound on the key rate and employ a decoy-state method. The effects of background noise and misalignment are taken into account under practical conditions. By simulating a practical QKD system, we compare RRDPS QKD with the BB84 protocol. Details of the work can be found in [arXiv:1505.02481].

Joint work with Zhen Zhang, Xiao Yuan, Zhu Cao