CC-07-01

Tight and general security proofs for quantum key distribution

Thomas Van Himbeeck

Inria Paris

Abstract

Quantum Key Distribution is one of the most mature quantum protocols. This technological advancement comes with a need for new security proofs that work with realistic devices and perform well in the finite-size regime, where the users exchange a large but finite set of messages. In recent years, we have seen a new generation of proof techniques utilizing ideas from convex optimization or information theory. In this talk, I will present these new ideas and review some challenges and opportunities for the future work.