

Renato Renner. *Security proofs in quantum cryptography.*

In this course, I will introduce the main quantum information-theoretic concepts and techniques needed to analyze the security of quantum cryptographic schemes. In particular, I will demonstrate how these techniques can be combined to get a full-fledged security proof for quantum key distribution (QKD).

- Security definitions and their operational meaning
- Single-shot information measures; smooth entropies
- De Finetti-type theorems
- Privacy amplification and its fully quantum generalization, called state merging