Security proofs on Quantum key distribution

Winter break 2021

1 Course information

- Lecture dates: 01 - 05 March 2021. Evaluation: 10 March 2021
- Total activities: 30h
- Pre-requisite: basic knowledge of quantum information is assumed.

Lecturer: Gláucia Murta
Teaching assistant: Federico Grasselli

2 Preliminary Schedule

- Monday - March 01:
  - 10:30 - 13:00: Lesson 1
  - 14:30 - 16:00: Lesson 2
- Tuesday - March 02:
  - 10:30 - 13:00: Lesson 3
  - 14:30 - 16:00: Lesson 4
- Wednesday - March 03:
  - 10:30 - 13:00: Lesson 5
  - 14:30 - 16:00: Lesson 5/Group work (preparation of evaluation activity)
- Thursday - March 04:
  - 10:30 - 13:00: Lesson 6
  - 14:30 - 16:00: Lesson 6/Group work (preparation of evaluation activity)
- Friday - March 05:
  - 10:30 - 13:00: Lesson 7
  - 14:30 - 16:00: Lesson 7/Group work (preparation of evaluation activity)
- Wednesday - March 10:
  - 10:30 - 13:00: Evaluation: Project presentation by students - part I
  - 14:30 - 16:00: Evaluation: Project presentation by students - part II

3 Content

Lesson 1: Basic concepts

- Defining the task: key distribution.
- The BB84 protocol.
- Entanglement based version.
- Prepare-and-measure and entanglement based equivalence.
- Eavesdropper type of attack: individual, collective, coherent.

Lesson 2: Tools for the security analysis

- Diamond norm, trace distance.
- Shannon entropy, von Neumann entropy. Conditional entropy
- Guessing probability and min-entropy
- Other entropies of interest (collision entropy and Rényi α-entropies)
- Smooth min-entropy and operational interpretation
- Some properties of these entropies.

Lesson 3: Security of quantum key distribution

- Security definition: correctness, secrecy and completeness.
- Composable security.
- Leftover hashing lemma.

Lesson 4: Security of the BB84 protocol I

- Discussion: earlier proofs based on entanglement distillation. Devetak-Winter formula.
- Security proof against collective attacks (technique: asymptotic equipartition property).
- QBERs and Reduction to Bell-diagonal states.

Exercise: calculate the maximum QBER tolerated (in the asymptotic limit) in an implementation where the maximally entangled state undergoes depolarizing noise.

Lesson 5: Security of the BB84 protocol II

- Security proof against coherent attacks (techniques: de Finetti, and uncertainty relation).
- Other protocols (six state protocol, high dimensional QKD).

Lesson 6: Hacking the BB84 protocol

- What if the source is not perfect?
- Assumptions on prepare-and-measure vs entanglement based protocols.
- The decoy states method.

Lesson 7: Hacking the entanglement based version

- What if the detectors are not perfect?
- An example (Blind detectors)
- MDI QKD
- DIQKD

4 Evaluation

The evaluation will be done with a group project consisting of a report + 30 min presentation about a 'case study' (selected paper on hacking QKD or QKD implementation).

- In groups of 2-3 students, choose one paper among the provided list. The group may also suggest a paper outside of the list if they wish.
- The goal of the project is to identify the concepts learned in the course in an implementation. In particular, the group may try to answer to the following questions:
  - Identify the QKD protocol that is being implemented (BB84, six state, high dimensional,...? prepare-and-measure, entang. based,...?)
  - What are the parameters? (QBER, other noise parameters)
  - Which assumptions are present in the security proof of this protocol?
  - How are the qubits and measurements modelled in the platform of the experiment
  - How the protocol was hacked?
  - Which assumptions were not being matched?