Universität Tübingen
Ángela Capel
Paul Gondolf

Sheet 9 — 13. July 2023

Quantum cryptography

Graded exercises

Problem 1. Consider the BB84 protocol, in which now we keep track of the disturbance created by the eavesdropper Eve:

$$|0\rangle \to |0\rangle |E_0\rangle \quad \text{and} \quad |1\rangle \to |1\rangle |E_1\rangle \ ,$$

where $\langle E_0 \mid E_1 \rangle = \alpha$. Then, she sends Alice's qubit to Bob, waits until Bob announces which of the two bases discussed on the lecture he's going to use, and then measures in that basis.

- Compute the bit error rate depending on α.
- Compute the probability that Eve obtains the private-key information.

Problem 2. Consider the so-called Eckert protocol: Alice and Bob share a state which has been tampered by Eve. Then, the joint state of Alice, Bob and Eve can be expressed as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle |E_0\rangle - |1,0\rangle |E_1\rangle) \,,$$

where $\langle E_0 \mid E_1 \rangle = \alpha$.

- Compute the bit error rate depending on α.
- Compute the probability that Eve obtains the private-key information.

Challenge exercises

Problem 3. Consider the protocol described on the previous exercise. In this problem, we will analyze both the information reconciliation and privacy amplification for this protocol.

- In information reconciliation, Alice picks k bits from her which are identical and announces the locations of these bits over the classical public channel. Subsequently, Bob (and Eve) perform a majority vote on their copies of the key. Calculate the bit error rate and the probability that Eve has the correct key as a function of k.
- Consider now a setting where Alice and Bob, through the information reconciliation step, have ensured that their keys are identical. However, Eve also has the key, but with probability p a bit in Eve's key is wrong. Alice and Bob now take q bits at random and generate a single bit of their new key by calculating the parity of these bits. Calculate the probability, per bit, that Eve has the new key.

Comment: Even though, in practice, the keys obtained in the first part of the exercise are not exactly the same, the error will be exponentially small in k; thus, we can assume they are identical.