| **Quantum Cryptography (spring 2020)** | Dominique Unruh |
|---|---|
| **Exercise Sheet 6** | |
| Out: 2020-04-10 | Due: 2020-04-22 |

# Problem 1: Quantum Key Exchange

Alice and Bob perform the following quantum key distribution protocol:

- Alice chooses random bits $a_1, \dots, a_n \in \{0,1\}$ and $b_1, \dots, b_n \in \{0,1\}$. For $i = 1, \dots, n$, Alice prepares $|\Psi_i\rangle := |\Psi_{a_i b_i}\rangle$ according to the following table:

| | |
|---|---|
| $\lvert\Psi_{00}\rangle$ | $\lvert 0\rangle$ |
| $\lvert\Psi_{10}\rangle$ | $\lvert 1\rangle$ |
| $\lvert\Psi_{01}\rangle$ | $\lvert +\rangle$ |
| $\lvert\Psi_{11}\rangle$ | $\lvert -\rangle$ |

  (In other words, $b_i$ specifies the basis in which $a_i$ is encoded.)

- Then Alice sends $|\Psi_1\rangle \otimes \dots \otimes |\Psi_n\rangle$ to Bob (over an insecure quantum channel that is under the control of the adversary Eve).

- When Bob has received all the $n$ qubits, he acknowledges receipt over an authenticated (but public, i.e., not secret) channel.

- After getting the acknowledgement from Bob, Alice sends all bits $b_i$ to Bob, and for checking, she also sends $a_i$ to Bob for $i = 1, \dots, \frac{n}{2}$ (we assume $n$ to be even).

- Then Bob measures each of the qubits he received in the basis given by the $b_i$. Let the outcomes be $\tilde{a}_i$.

- Bob checks whether $a_i = \tilde{a}_i$ for all $i = 1, \dots, \frac{n}{2}$. If so, he sends OK to Alice over the authenticated channel and outputs the key $\tilde{a}_{\frac{n}{2}+1} \dots \tilde{a}_n$, otherwise he sends ABORT and aborts.

- When Alice receives OK, she outputs the key $a_{\frac{n}{2}+1} \dots a_n$. If she receives ABORT, she aborts.

(a) Break the protocol.

(b) Argue how the protocol security could be improved. (But do not try to prove it!)

## Problem 2: Eve's advantage

Assume that in a (bad) QKD protocol, some adversary Eve succeeds in doing the following: The protocol aborts with probability $\frac{2}{3}$. In the cases where the protocol does not abort, the key that is chosen is always $0\dots0$ ($n$ bits, $n > 2$). For simplicity, assume that Eve's state is empty after the protocol execution (that is, Eve's quantum state consists of zero qubits, and density operators $\rho_E$ describing Eve's state can be omitted from all formulas).

(a) Describe the state $\rho_{ABE}^{\mathrm{Real}}$. What is the value of

$$\mathrm{TD}(\rho_{ABE}^{\mathrm{Real}}, S_{\mathrm{Ideal}}) := \max_{\rho_{ABE}^{\mathrm{Ideal}} \in S_{\mathrm{Ideal}}} \mathrm{TD}(\rho_{ABE}^{\mathrm{Real}}, \rho_{ABE}^{\mathrm{Ideal}})$$

(for the particular Eve described above)?

(b) Show that the protocol is not $\varepsilon$-secure for $\varepsilon = \frac{1}{4}$.