

Exercise Sheet 06

Out: 2023-03-20

Due: 2023-03-27

1 Quantum key exchange, bad protocol

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:

$$|\Psi_{00}\rangle := |0\rangle$$

$$|\Psi_{10}\rangle := |1\rangle$$

$$|\Psi_{01}\rangle := |+\rangle$$

$$|\Psi_{11}\rangle := |-\rangle$$

(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, they acknowledge 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, Alice 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 they 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, they send OK to Alice over the authenticated channel and outputs the key $\tilde{a}_{\frac{n}{2}+1} \dots \tilde{a}_n$, otherwise they send ABORT and abort.
- When Alice receives OK, they output the key $a_{\frac{n}{2}+1} \dots a_n$. If they receive ABORT, they abort.

(a)	Knowlets:	QKDIntro, QKDSecDef	ProblemID: BadQKDBreak
	Time:		
	Difficulty:		

Break the protocol.

(b)	Knowlets:	QKDIntro, QKDSecDef	ProblemID: BadQKDFix
	Time:		
	Difficulty:		

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

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 $0 \dots 0$ (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 ρ_E describing Eve's state can be omitted from all formulas).

(a)	Knowlets:	QKDSecDef	ProblemID: EveAdvReal
	Time:		
	Difficulty:		

Describe the state ρ_{ABE}^{Real} . What is the value of

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

(for the particular Eve described above)?

(b)	Knowlets:	QKDSecDef	ProblemID: EveAdvInsec
	Time:		
	Difficulty:		

Show that the protocol is not ε -secure where $\varepsilon := \frac{1}{4}$.