Quantum Cryptography (spring 2022) Dominique Unruh

Exercise Sheet 06

Out: 2022-04-18 Due: 2022-04-26

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:

$$\begin{aligned} |\Psi_{00}\rangle &:= |0\rangle \\ |\Psi_{10}\rangle &:= |1\rangle \\ |\Psi_{01}\rangle &:= |+\rangle \\ |\Psi_{11}\rangle &:= |-\rangle \end{aligned}$$

  (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 receives ABORT, they abort.

(a)

Knowlets:	QKDIntro, QKDSecDef ProblemID: BadQKDBreak
Time:	
Difficulty:	

Break the protocol.

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 ρ_E describing Eve's state can be omitted from all formulas).

(a)

Knowlets:	QKDSecDef ProblemID: EveAdvReal
Time:	
Difficulty:	

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

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

(for the particular Eve described above)?

3 Bell test, doing the "impossible"

Let $|\beta_{ab}\rangle$ for $a, b \in \{0,1\}$ be the Bell states, and let

$$\begin{aligned} P_{bf} &:= |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|, \\ P_{pf} &:= |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|. \end{aligned}$$

(Remember that $\{P_{bf}, 1 - P_{bf}\}$ and $\{P_{pf}, 1 - P_{pf}\}$ are the measurements that Alice and Bob need to perform on their qubit pairs during the Bell test.)

Note that in both cases below, experiment (ii) can be implemented even if the two qubits are in different locations and only classical communication is possible between these locations. This allows to replace the Bell test from the lecture by a procedure that can actually be implemented.

(a)

Knowlets:	BellTest, DensityM ProblemID: BellTestComp
Time:	
Difficulty:	

Consider the following two experiments on a two qubit system.

(i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{bf}, P_{no} := 1 - P_{bf}\}$. Then the qubits are destroyed.

(ii) The two qubits are individually measured in the computational basis $\{|0\rangle, |1\rangle\}$. If the results are equal, output *yes*, otherwise output *no*. Then the qubits are destroyed.

Show that both experiments are equivalent. That is, show that for any two-qubit state $\rho \in S(\mathbb{C}^4)$, we have that the probability for getting outcome *yes* is the same. (Usually, one would have to also show that the post-measurement state is the same. But since here the qubits are destroyed, this is trivially the case.)

Hint: Let P_{00}, P_{11} be the two projectors corresponding to both measuring 0 and both measuring 1, respectively, in the second experiment. Then the probability of *yes* in the second experiment is $\operatorname{tr} P_{00}\rho + \operatorname{tr} P_{11}\rho = \operatorname{tr}(P_{00} + P_{11})\rho$.

(b)

Knowlets:	BellTest, DensityM ProblemID: BellTestDiag
Time:	
Difficulty:	

Consider the following two experiments on a two qubit system.

(i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{pf}, P_{no} := 1 - P_{pf}\}$. Then the qubits are destroyed.

(ii) The two qubits are individually measured in the diagonal basis $\{|+\rangle, |-\rangle\}$ with $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. If the results are equal, output *yes*, otherwise output *no*. Then the qubits are destroyed.

Show that both experiments are equivalent.