CS120, Quantum Cryptography, Fall 2016

Homework # 8 **due: 10:29AM, November 29th, 2016**

Ground rules:

Your homework should be submitted to the marked bins that will be by Annenberg 241.

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are strongly encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Some of the problems are inspired from problems available on EdX. You are not allowed to look up the EdX problems for hints (such as the multiple answers provided). Focus on the present pset!

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the quarter will be dropped from your final grade.

Place all your problems in the first (top) bin in the box by Annenberg 241. Start each problem on a new page, with your name clearly marked at the top of the page.

Problems:

1. (4 points) **Thinking adversarially.**
   Let's imagine that we are playing the role of the eavesdropper Eve. We observe two parties, Alice and Bob, trying to implement certain QKD protocols. Because QKD is hard, Alice and Bob might try to cut corners in the implementation of their protocols. Here are two suggested protocols that Alice and Bob might want to implement. For each of them, either prove security or provide an explicit attack for Eve.

   Protocol 1:
   Alice and Bob can communicate through a classical authenticated channel, and a quantum (non-authenticated) channel.

   - Alice generates bit strings $x, \theta \in \{0,1\}^n$ uniformly at random.
   - Alice prepares qubits $|x_i\rangle_{\theta_i}$ for $i = 1, .., n$ where $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$, $|1\rangle_1 = |-\rangle$, and sends them to Bob.
   - Alice announces the basis string θ.

- Bob measures the qubits he received according to the bases specified by the string θ and recovers x.

Protocol 2:

- Alice creates n EPR pairs and sends one half of each to Bob.
- She generates the string $\theta \in \{0,1\}$ and measures her half of each pair according to the corresponding bit of θ (standard basis for 0, Hadamard for 1)
- Bob generates a random string $\hat{\theta}$, and similarly measures his half of the EPR pairs. Then Bob announces over an authenticated channel that he received and measured his qubits.
- Alice and Bob announce θ and $\hat{\theta}$ over an authenticated channel.
- Alice and Bob use the measurement results they obtained for each $\theta_i = \hat{\theta}_i$ as their key.

2. (8 points) **BB'84 fails in the device-independent setting.**
Consider the purified variant of the BB'84 protocol. Suppose that Eve prepares the state ρ_{ABE} in the following form:

$$\rho_{ABE} = \sum_{x,z=0}^{1} |xz\rangle\langle xz|_A \otimes |xz\rangle\langle xz|_B \otimes |xz\rangle\langle xz|_E , \tag{1}$$

where $|xz\rangle$ is short-hand notation for $|x\rangle \otimes |z\rangle$. Note that here each of the systems A and B handed over to Alice and Bob respectively is made of two qubits. But suppose that they don't notice this - the qubits go directly into their respective measurement device.

Now suppose each of Alice and Bob's measurement device, instead of measuring a single qubit in the standard or Hadamard bases, as it is supposed to do, in fact performs the following:

- When the device is told to measure in the standard basis, it measures the first qubit of the two-qubit system associated with the device in (1) in the standard basis;
- When the device is told to measure in the Hadamard basis, it measures the *second* qubit of the two-qubit system associated with the device in (1) in the standard basis.

(a) Alice and Bob put blind faith in their hardware and attempt to implement BB'84. They want to check that their state is an EPR pair, so Alice asks her box to measure in the standard basis. The box returns a measurement outcome of 0. Determine the post-measurement state.

(b) After Alice's measurement, Bob asks his box to measure in the Hadamard basis. What measurement outcome will Bob receive? Suppose instead Bob had asked his box to measure in the standard basis. What measurement outcome would Bob have received?

(c) Suppose Bob did in fact the latter. Suppose that now Eve measures her first qubit in the standard basis. What measurement outcome does she receive?

(d) Suppose Alice and Bob run the BB'84 protocol, and, as per the usual, they look at all the rounds in which they made the same measurement as each other. They pick a random subset of half of those rounds and test whether they received the same output on all the rounds. What is the probability that they pass the test?

(e) Let T' be the set of rounds on which Alice and Bob made the same measurement but didn't perform a test. Let $\{\theta_j\}_{j\in T'}$ be the measurements they made and $\{x_j\}_{j\in T'}$ and $\{\hat{x}_j\}_{j\in T'}$ be the results they received. The θ_j have been communicated over the public channel. Eve wishes to learn the x_j. Which measurements should she make?

(f) Let X be the classical key generated by Alice and Bob. What is $H_{\min}(X \mid E)$, where E is Eve's system?

3. (3 points) **Commuting observables are compatible.**
Consider $X \otimes X$ and $Z \otimes Z$. Each of these is a 4×4 Hermitian matrix which squares to identity, so it has ± 1 eigenvalues. Moreover, since $X \otimes X$ and $Z \otimes Z$ mutually commute, they have a simultaneous eigenbasis. It turns out that it consists of the Bell states

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right); \quad |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right);$$
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right); \quad |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

(a) Suppose we measure an arbitrary two-qubit state $|\phi\rangle$ using the observable $X \otimes X$ and obtain the outcome -1. To which two-dimensional eigenspace does the post-measurement state belong? (Specify the subspace using two of the Bell states above.) Next, we measure the observable $Z \otimes Z$ and obtain outcome 1. What is post-measurement state $|\phi'\rangle$?

(b) Suppose that instead we performed the measurement $-Y \otimes Y = (X \otimes X)(Z \otimes Z)$ directly, and the post-measurement state had nonzero overlap with $|\phi'\rangle$. What measurement outcome would we have obtained?

(c) What do you deduce about about the relationship between the outcomes of measuring commuting observables A and B with the outcome of measuring the observable AB directly?

4. (9 points) **A coherent attack on a nonlocal game.**
In video 7.5-2 on EdX, you saw a nonlocal game where a coherent attack allowed the players to do just as well when playing two parallel copies of the game as they did when playing just one copy.

Now we'll see another example of a game with such an attack, and we'll prove that this attack is the best strategy for the game even in the quantum setting.

(a) We begin by describing the single-shot game. Eve starts by generating a pair $(s,t) \in \{(0,0),(0,1),(1,0)\}$ uniformly at random. She gives s to Alice and t to Bob. Alice and Bob generate output bits $a, b \in \{0,1\}$, respectively. They win if $a \vee s \neq b \vee t$. As a warm-up, consider the strategy in which $a = s$ and $b = t$. What is the winning probability? Which inputs cause Alice and Bob to lose?

(b) In the two-parallel version $G^{(2)}$ of the game we just described, Eve picks two strings $(s_0,t_0),(s_1,t_1)$ from $\{(0,0),(0,1),(1,0)\}$ independently and uniformly at random. She gives (s_0,s_1) to Alice, (t_0,t_1) to Bob, and demands outputs $(a_0,a_1),(b_0,b_1)$ from Alice and Bob. They win if $a_0 \vee s_0 \neq b_0 \vee t_0$ and $a_1 \vee s_1 \neq b_1 \vee t_1$.

Describe a deterministic strategy for Alice and Bob that achieves a winning probability of $2/3$.

(c) Suppose Alice and Bob have a valid strategy for the two-parallel game which wins with probability ω_c. Describe a strategy for them to win the one-shot game with probability at least w_c. This proves that the optimal success probability in the one-shot game is an upper bound for the optimal success probability in the two-parallel game.

(d) Now we will find an upper bound on the success probability of the one-shot game, assuming that Alice and Bob may use shared entanglement in addition to classical resources.

The most general strategy that Alice and Bob can take is as follows. They each have two ± 1-eigenvalue-observables A_0, A_1, B_0, B_1. They share a joint state $|\psi\rangle$. Alice measures $|\psi\rangle$ on A_s, Bob measures on B_t, and they each output 0 if they measured a 1 and 1 if they measured a -1.

In general, if X is an observable, then $\langle\psi| X |\psi\rangle$ is equal to the probability of measuring a 1 minus the probability of measuring -1.

Let $M = -\frac{1}{3}A_0B_0 + \frac{1}{3}A_0 + \frac{1}{3}B_0$. Prove that the probability that Alice and Bob win the game is $\frac{1}{2} + \frac{1}{2}\langle\psi| M |\psi\rangle$.

(e) Prove that $M^2 = \frac{1}{3}\mathbb{I} - \frac{2}{3}M$.

(f) The answer to the last is the characteristic polynomial of M (indeed, it is the unique monic quadratic satisfied by M). Use it to solve for the largest eigenvalue $\lambda_{\max}$ of M.

(g) Now use the facts that $p_{\text{win}} \leq \frac{1}{2} + \frac{1}{2}\langle\psi| M |\psi\rangle$ and $\langle\psi| M |\psi\rangle \leq \lambda_{\max}$ to find the tightest possible upper bound on p_{win}.