CS120, Quantum Cryptography, Fall 2016

Homework # 7 **due: 10:29AM, November 22nd, 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)* **Establishing keys in the presence of a limited eavesdropper**
   Assume that Alice and Bob are connected by a classical authenticated channel. Your goal is to devise ways in which Alice and Bob can obtain a key in any of the situations below.

   (a) Suppose that Alice and Bob are connected by a classical channel such that Eve learns each bit with probability q, where we only know that $1/3 \leq q \leq 1/2$. Give a protocol that allows Alice and Bob to create an ϵ-secure key, where $\epsilon = 10^{-5}$. Explain why your protocol is secure. How many uses of the channel are required per bit of key produced?

   (b) Suppose now that Alice and Bob are connected by a classical channel on which Eve can intercept bits arbitrarily. However, Eve's memory is limited to $k = 1024$ bits. Give a protocol that allows Alice and Bob to create an ϵ-secure key where $\epsilon = 10^{-10}$. Explain why your protocol is secure.

2. *[Optional]* **Recursive information reconciliation**
Suppose that Alice and Bob have n-bit strings $X, Y \in \{0,1\}^n$ respectively such that for each $i \in \{1,\ldots,n\}$, $\Pr(X_i = Y_i) = p = 1 - \delta \in [1/3, 2/3]$.

   (a) Let $S \subseteq \{1,\ldots,n\}$ be a set of coordinates of size $|S| = k$. Evaluate $\Pr(x_S = y_S)$ and $\Pr(\oplus_{i\in S} x_i = \oplus_{i\in S} y_i)$, as a function of δ.

   (b) Using the previous question, find a lower bound on k which guarantees that $\Pr(x_S = y_S | \oplus_{i\in S} x_i = \oplus_{i\in S} y_i) \geq 1 - \delta/2$.

   (c) Explain how this idea can be used to implement an iterative scheme for information reconciliation *[Hint: use larger and larger alphabets].*

   (d) How efficient is your scheme? For some small $\varepsilon > 0$ (much smaller than δ), estimate the number of bits that Alice and Bob have to exchange before they find a subset T such that $\Pr(x_T = y_T) \geq 1 - \varepsilon$. How large is T?

3. *(5 points)* **Generating a key using an anonymous message board**

   (a) Alice and Bob's conversation takes place on an anonymous message board. That is, Eve can see the whole transcript but doesn't know which message came from which person. Find a protocol in which Alice and Bob exchange a total of two messages, which succeeds with probability at least one half, and when it succeeds, Alice and Bob share one bit of key which is uniformly random from the perspective of Alice.

   (b) Give an anonymous-message-board protocol to generate an n-bit private key which takes a linear number of rounds and has exponentially small failure rate. (*Hint: You'll need a Chernoff bound to control the error rate.*)

   (c) Eve sees the entire transcript of Alice and Bob's conversation, but in the lecture notes it is argued that key generation is impossible against an adversary who can overhear all communication. Why does that argument fail to apply here?

4. *(4 points)* **Information reconciliation via linear codes**

   (a) Suppose Alice and Bob have access to the the binary symmetric channel with error p: Bob receives each bit that Alice sends correctly with probability $(1-p)$. Consider the linear code generated by the parity check matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

   Using the information reconciliation scheme defined in the edX videos, with what probability does Alice and Bob succeed at distributing their key?

(b) What is the probability that a 7-bit message is transmitted correctly with no reconciliation? Compare this to the success probability of the previous part and to the success probability of the 3-bit scheme generated by the parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

(The three-bit scheme is analyzed in the edX lecture videos; you may quote those results.) Which schemes have success probabilities with the best leading order behavior? For $p \in \left(0, \frac{1}{2}\right)$, which scheme is best?

5. *(6 points)* **Cloning attacks**

In previous problems, we studied the ability of Alice and Bob to generate a key over a classical channel given some strict limitations on Eve's ability. Now we aim to analyze BB84 in the context of a limited Eve. In particular, Eve will be limited to intercepting Alice's message and attempting to copy it with one of the maps from HW2, problem 6.

Recall that in the BB84 protocol Alice first generates random $x_j, \theta_j \in \{0, 1\}$, and then sends N single-qubit states $|x_j\rangle_{\theta_j}$, for $j \in \{1, \ldots, N\}$, to Bob.

Now suppose the eavesdropper Eve intercepts each of the states sent by Alice, and does the following:

(i) With probability $1-p$, she applies the cloning map T_1 from Problem 6(a) in HW2. She keeps the second qubit and forwards the first qubit to Bob.

(ii) With probability p, she applies the cloning map T_2 from Problem 6(b) in HW2. She keeps the second qubit, traces out (i.e. ignores) the third qubit, and forwards the first qubit to Bob.

For simplicity, assume $N = 1$. Based on the results of HW2 Problem 6 (you may consult the solution available online), evaluate the following. (In the solutions to HW2 it is proven that the map T_2 is equivalent to the map T_3; you should use whichever form you find most convenient.)

(a) Suppose Bob correctly guesses $\theta = \theta_1$ and measures his qubit in the corresponding basis. What is the probability that his measurement outcome is equal to $x = x_1$? First compute this for the case $p = 0$. Next compute the probability for $p = 1$; call this value q_B for future reference. Finally, extend this to give the success probability as a function of the probability p.

(b) Suppose Eve does the same, guessing θ correctly and measuring in the corresponding basis. As in part (a), compute her probability of success when $p = 0$, $p = 1$, and for general p. For future reference, let q_E be the value when $p = 1$.

(c) What is the probability that Bob and Eve's outcomes agree with each other and are correct? Give your answer as a function of p. *(Hint: This is related to the success probabilities of T_1 and T_2 as cloning maps.)*

6. *(6 points)* **BB84 against a cloning attack.**
Let's continue the previous problem with the BB84 protocol. Alice and Bob know that Eve will implement a cloning attack, but they do not know p ahead of time. They will try to generate a key independent from Eve which is as long as possible. We will informally estimate the length of the key produced. (It is possible but more difficult to show that with high probability, Alice and Bob produce a key which is mostly independent from Eve and has almost our estimated length.)

We now consider a number of rounds $N = 4n$. Suppose that in $2n$ of the rounds (exactly), Bob happens to make the right basis choice; call these the agreement rounds, $R \subseteq \{1, \ldots, N\}$. They select exactly n of these rounds for testing; call these rounds the testing rounds, $T \subseteq R$. You may assume all rounds behave the same.

(a) We say that Bob succeeds in round j if his measurement outcome against $|x_j\rangle_{\theta_j}$ is equal to x_j. If Bob does not succeed, we say there is an error. What is the expected number of errors that Alice and Bob will notice in the testing rounds T, as a function of q_B and p?

(b) Now suppose that Alice and Bob detect δn errors in the testing rounds. They should expect to also see approximately δn errors in the untested agreement rounds $R \setminus T$. They perform information reconciliation on Alice's bits $\{x_j\}$ and Bob's measurement outcomes to generate a common key $k_A = k_B$. How many bits do they need to exchange in order to perform the reconciliation, as a function of δ and n? (You may assume there are indeed at most δn errors.)

(c) Now we'll invert the bound from (a). What is Alice and Bob's best guess $\hat{p}$ for p, as a function of q_B and δ?

(d) Suppose Alice and Bob make a guess $\hat{p}$ for p based on the method from the previous question. Deduce a bound on the min-entropy $H_{\min}(A|E)$ per round that they could estimate for the rounds in $K = R \setminus T$. Give their estimate as a function of q_E, q_B, δ.

(e) Finally Alice and Bob apply privacy amplification to their reconciled string. They start with the min-entropy guarantee computed in (d) and leak as many bits as computed in (b) to Eve. Using the best privacy amplification method you know (e.g. as seen in class), how much private key can they extract? Express your answer as a function of δ, q_E, q_B, n.

(f) Estimate δ in terms of p as in part (a). Using your values of q_E and q_B from problem 5, how much key can they expect to extract as a function of p and n?