COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 3 **due: 12:59PM, October 19th, 2025**

Ground rules:

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 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. If you use an AI tool to partially solve a question, or improve your write-up of a solution, then you should also mention it. All questions on the homework, including requests for clarifications or typos, should be directed to the Ed forum.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of an academic committee.

Each of the four problem set counts for 20% of the total homework grade. (Each of the two readings will count for 10% of the final homework grade.)

Revisions since the first posting are in blue.

Problems:

1. *(6 points)* **Information reconciliation via linear codes.** 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 $(1-p)$, and incorrectly with probability p. In other words, Alice has a uniformly random $X_A \in \{0,1\}^7$ and Bob has $X_B \in \{0,1\}^7$ such that each bit of X_B equals the same bit of X_A with probability $(1-p)$.

   (a) Consider the linear code generated by the parity check matrix

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

   Show that this code corrects a single error.

   (b) Using the information reconciliation scheme from class (described in the Chapter 6 notes), with what probability do Alice and Bob succeed in performing reconciliation on their strings (thus obtaining an identical 7-bit key)?

   (c) 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

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

Which scheme has success probability with the best leading order behavior? For $p \in \left(0, \frac{1}{2}\right)$, which scheme is best?

2. *(6 points)* **Establishing keys in the presence of a limited eavesdropper.** In all settings below, we 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. *[Hint: In both cases, start by evaluating $H_{\min}(X|E)$ where X is the string shared by Alice and Bob after transmission and E is Eve's (classical) information about it.]*

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

3. *(8 points)* **Cloning attacks NEED TO EDIT BASED ON PDF**
   In this problem we study the effectiveness of a simple cloning attack for the eavesdropper in the BB84 key distribution protocol. Recall that in the protocol Alice prepares N single-qubit states $|x_j\rangle_{\theta_j}$, for $j \in \{1, \ldots, N\}$ and random $x_j, \theta_j \in \{0, 1\}$, and sends each of these states 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 to Bob.

   For simplicity, first assume $N = 1$. Based on the results of HW2 Problem 6 (you may consult the solution available online), evaluate the following:

   (a) Suppose both Alice and Bob measure their qubit in the correct basis $\theta = \theta_1$. If $p = 0$, what is the probability that they get the same outcome (recall $\theta \in \{0, 1\}$ is chosen uniformly at random). Same question if $p = 1$. Same question for a general $0 < p < 1$.

   (b) Answer the same questions, where now Alice and Eve measure their qubit. What is the probability that they get the same outcome?

(c) What is the probability that all of Alice, Bob and Eve all obtain the same outcome, if they each measure their respective qubit in basis θ? (Answer for a general p.)

Let's continue with the BB84 protocol. We now consider a number of rounds $N = 4n$. Suppose that in $2n$ of the rounds (exactly), Alice and Bob happen to make the same 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.

(d) What is the expected number of errors (non-agreement of their measurement outcomes) that Alice and Bob will notice in the testing rounds T, as a function of p?

(e) Invert the previous bound: as a function of the fraction δ of errors detected in the testing rounds, what is a reasonable estimate $\hat{p}$ for p that Alice and Bob could come up with?

(f) Suppose Alice and Bob make a guess $\hat{p}$ for p based on the method from the previous question. Using question (b), deduce a bound on the min-entropy $H_{\min}(A|E)$ per round that they could estimate for the rounds in $K = R \backslash T$.

(g) Conclude: how many bits of key, as a function of p and N, can Alice and Bob reasonably hope to generate from the protocol? *[Hint: This is a subtle calculation. Alice and Bob will have to perform both information reconciliation and privacy amplification on the rounds in K. First, estimate the number of bits they will need to exchange to perform information reconciliation. Second, deduce a bound on the min-entropy of the resulting agreed-on string. Third, use the best privacy amplification method you know of to maximize the length of extracted key]*