COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 3 **due: 11:59PM, November 18th, 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. Suppose that Alice selects 7 bits uniformly at random, $X_A \in \{0,1\}^7$, and sends them to Bob. Then, 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: for any codeword $c \in \ker H$ and any error $e \in \{0,1\}^7$ of Hamming weight 1, c can be uniquely recovered from $c+e$ (in other words, there are no c, c' and errors e, e' such that $c+e = c'+e'$.

   (b) Using the information reconciliation scheme from class (described in the Chapter 6 notes), with what probability (as a function of p) do Alice and Bob succeed in performing reconciliation on their strings (thus obtaining an identical 7-bit key)? *[Note that information reconciliation can use a noiseless authenticated channel to exchange the syndrome information]*

(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 for each bit sent on the channel, Eve learns it with probability exactly q, and with probability (1-q) Eve receives a uniformly random bit.[1] Furthermore, 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 $\epsilon = 2^{-128}$. Explain why your protocol is secure. How many uses of the channel are required per bit of key produced? *[Hint: You may assume that the seed for the strong seeded randomness extractor is sent over a perfect authenticated channel. However, don't forget to account for the information that this leaks to Eve: think about what is the seed length of the 2-universal hash function you use.]*

   (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 $b = 1024$ bits. (Bob always receives the correct bit.) Give a protocol that allows Alice and Bob to create an ϵ-secure key where $\epsilon = 2^{-256}$. Explain why your protocol is secure.

3. *(8 points)* **Min-entropy from the matching outcomes bound**
   This problem investigates a direct method to lower bound Alice and Bob's key extraction rate based on the probability that the matching-outcomes test succeeds. If we assume that the adversary Eve prepares n identical and uncorrelated copies of the tripartite state $|\Psi_{ABE}\rangle$ and sends the qubits A to Alice and B to Bob, then as shown in the notes the key extraction rate can be asymptotically lower-bounded by the min-entropy $H_{\min}(X|E\Theta)$ per round, where X is the outcome of Alice's measurement on her qubit. The goal of this problem is to prove a lower bound on this quantity.

[1] This sentence clarifies the original wording. If you took another interpretation of what the channel does, it is ok, as long as you are clear what interpretation you use for the entropy calculation.

Recall that if Alice measures her qubit in the standard basis, and the resulting post-measurement state on her qubit and Eve's system E is a classical-quantum (cq) state

$$\rho_{XE} = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_E^{Z,0} + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_E^{Z,1},$$

then since X consists of a single bit as we saw in class the optimal guessing probability $P_{guess}(X|E,\Theta=0)$ such that

$$H_{\min}(X|E,\Theta=0) = -\log P_{guess}(X|E,\Theta=0)$$

is given by the optimal distinguishing measurement, for which $P_{guess}(X|E,\Theta=0) = \frac{1}{2} + \frac{1}{2}\|\rho_E^{Z,0} - \rho_E^{Z,1}\|_{tr}$.

The same reasoning holds for any other choice of Alice's basis, notably the Hadamard basis $\{|+\rangle, |-\rangle\}$. In the BB'84 protocol Alice chooses with probability 1/2 one of the two bases in which to measure her qubit. If we denote by $P_{guess}(X|E,\Theta=0)$ and $P_{guess}(X|E,\Theta=1)$ the optimal guessing probabilities for Alice measuring in the standard ($\Theta=0$) and Hadamard ($\Theta=1$) bases respectively, the desired lower bound is given by

$$H_{\min}(X|E\Theta) = -\log\left[\frac{1}{2}P_{guess}(X|E,\Theta=0) + \frac{1}{2}P_{guess}(X|E,\Theta=1)\right]. \qquad (1)$$

(a) Suppose Alice and Bob share a pure EPR pair $|\mathrm{EPR}\rangle$, uncorrelated with Eve's system: $\rho_{ABE} = |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{AB} \otimes \rho_E$. What is $H_{\min}(X|E\Theta)$?

(b) Now consider the general case, where $|\Psi_{ABE}\rangle$ is an arbitrary state prepared by Eve. Let p be the probability that this state succeeds in the matching outcomes test, when Alice and Bob both measure in the same basis Θ chosen at random. Give coefficients a, b, c such that

$$p = a\,\langle\Psi_{ABE}|\, X_A \otimes X_B \otimes \mathbb{I}_E\,|\Psi_{ABE}\rangle + b\,\langle\Psi_{ABE}|\, Z_A \otimes Z_B \otimes \mathbb{I}_E\,|\Psi_{ABE}\rangle + c,$$

where X, Z are the Pauli observables $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z = |+\rangle\langle -| + |-\rangle\langle +|$.

(c) By expanding the qubit A in the computational basis, the state $|\Psi_{ABE}\rangle$ can be expressed as $|\Psi_{ABE}\rangle = |0\rangle\otimes|u_0\rangle_{BE} + |1\rangle\otimes|u_1\rangle_{BE}$, with $\|\,|u_0\rangle_{BE}\,\|^2 + \|\,|u_1\rangle_{BE}\,\|^2 = 1$. Give coefficients a', b' such that $\langle\Psi_{ABE}|\, X_A \otimes X_B \otimes \mathbb{I}_E\,|\Psi_{ABE}\rangle = a'\,\Re(\langle u_0|\, X_B \otimes \mathbb{I}_E\,|u_1\rangle) + b'$.

A similar equality can be obtained for $\langle\Psi_{ABE}|\, Z_A \otimes Z_B \otimes \mathbb{I}_E\,|\Psi_{ABE}\rangle$.

Suppose Alice measures her qubit in the computational basis: the post-measurement state on A and E (tracing out B) can be written as $\rho_{AE}^Z = |0\rangle\langle 0|_A \otimes \sigma_E^{Z,0} + |1\rangle\langle 1|_A \otimes \sigma_E^{Z,1}$. Similarly, if Alice measures in the Hadamard basis we may write the post-measurement state as $\rho_{AE}^X = |+\rangle\langle +|_A \otimes \sigma_E^{X,+} + |-\rangle\langle -|_A \otimes \sigma_E^{X,-}$.

(d) Use the previous two questions to determine coefficients α, β such that

$$2p - 1 \leq \alpha F(\sigma_E^{X,0}, \sigma_E^{X,1}) + \beta F(\sigma_E^{Z,+}, \sigma_E^{Z,-})$$

where F denotes the fidelity. *[Hint: observe that $|u_0\rangle_{BE}$ and $|u_1\rangle_{BE}$ considered in the previous question are purifications of $\sigma_E^{Z,0}$ and $\sigma_E^{Z,1}$ respectively, and use Uhlmann's theorem]*

(e) Recall the inequality $\|\rho - \sigma\|_{tr} \leq \sqrt{1 - F(\rho, \sigma)^2}$. Using also the definition of $H_{\min}(X|E\Theta)$ in (1), what is the best lower bound on $H_{\min}(X|E\Theta)$ as a function of p that you can get?