COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 2 **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. (4 points) **A Guessing Game.**
   Imagine that Alice and Eve play a guessing game where they share a two-qubit state ρ_{AE}. First, Alice produces a random bit $\theta \in \{0,1\}$, and she measures her qubit in the standard basis if $\theta = 0$ and in the Hadamard basis if $\theta = 1$. In both cases she obtains a bit $x \in \{0,1\}$ as measurement outcome. She then announces θ to Eve. Eve's goal is to guess the bit x. Imagine that $\rho_{AE} = |\text{EPR}\rangle\langle\text{EPR}|$, where as usual $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, so Alice and Eve share a maximally entangled pair of qubits. In this scenario we know that if Eve measures in the same basis as Alice she will get the same outcome and thus be able to guess x perfectly.

   (a) Suppose now that Alice wants to foil Eve so, before measuring, she first applies some unitary U_A to her qubit, and then measures. Of course Eve, being really smart, gets wind of this so she will know what unitary Alice has used before measuring. So they share the state

   $$|\Phi_U\rangle = (U_A \otimes \mathbf{1}_E)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   and Eve knows θ and U_A. In this scenario, what is Eve's optimal guessing probability, and what is a strategy that achieves it?

(b) Consider now a scenario in which Alice's strategy consists in choosing one out of three possible unitaries, according to a distribution that may depend on her choice of θ. The three unitaries are the same whether $\theta = 0$ or $\theta = 1$, and Eve knows what they are as well as the distribution used by Alice, but she does not learn which unitary Alice eventually selected. Provide a set of three unitaries that makes Eve's guessing probability the lowest possible. (You do not need to prove that your strategy is optimal.)

(c) Suppose we restrict Alice's set of possible unitaries to contain only two. Can she still make Eve's guessing probability as low as in part (b)?

2. (6 points) **Robustness of GHZ and W States, Part II.**
We return to the multi-qubit GHZ and W states introduced in the previous exercise. In class we learned to distinguish product states from (pure) entangled states by calculating the Schmidt rank of $|\Psi\rangle_{AB}$, i.e. the rank of the reduced state $\rho_A = \mathrm{Tr}_B |\Psi\rangle\langle\Psi|$. In particular ρ is pure if and only if $|\Psi\rangle$ has Schmidt rank 1. In the following, we denote by Tr_N the operation of tracing out only the last one out of N qubits.

(a) What are the ranks r_{GHZ} of $\mathrm{Tr}_N |GHZ_N\rangle\langle GHZ_N|$ and r_W of $\mathrm{Tr}_N |W_N\rangle\langle W_N|$, respectively? (Note that these are the Schmidt ranks of $|GHZ_N\rangle$ and $|W_N\rangle$ if we partition each of them between the first $N-1$ qubits and the last qubit.)

Let us now introduce a more discriminating (in fact, continuous) measure of the entanglement of a state $|\Psi\rangle_{AB}$: namely, the *purity* of the reduced state ρ_A given by $\mathrm{Tr}\rho_A^2$. First let's see how this works in practice with the extreme cases in d dimensions:

(b) What are the purities $\mathrm{Tr}(\rho^2)$ for $\rho = |0\rangle\langle 0|$ and the "maximally mixed" state $\rho = \frac{1}{d} id_d$, respectively?

(c) Is the purity of ρ_A higher or lower for more entangled states $|\Psi\rangle_{AB}$? Can you explain this in terms of the definition $\mathrm{Tr}(\rho_A^2)$?

Now consider again the behavior of the N-qubit GHZ and W states with one qubit discarded (i.e. traced out):

(d) What is the purity of $\mathrm{Tr}_N |GHZ_N\rangle\langle GHZ_N|$ in the limit $N \to \infty$?

(e) What is the purity of $\mathrm{Tr}_N |W_N\rangle\langle W_N|$ in the limit $N \to \infty$?

Discuss the implications for the "robustness" of multipartite entanglement under loss of one qubit in GHZ versus W states. What can we say about losses of more than one qubit?

3. **An optimal attack**
Let

$$N_1 = \frac{1}{\sqrt{12}} \begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad N_2 = \frac{1}{\sqrt{12}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 3 \end{pmatrix} .$$

(a) Show that (N_1, N_2) are valid Kraus operators in the definition of a quantum channel $\mathcal{N}(\rho) = N_1 \rho N_1^\dagger + N_2 \rho N_2^\dagger$ mapping one qubit to two qubits.

(b) Show that using $\mathcal{N}$, a quantum adversary succeeds in the CLONE security game for Wiesner's quantum money scheme with probability $\frac{3}{4}$.

4. *(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]*