COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

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.

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 semester will be dropped from your final grade.

Problems:

1. (6 points) **Superdense Coding.**
   In Homework 1, you were introduced to the idea of "quantum teleportation". By sending just two bits of classical information, Alice was able to "teleport" her single-qubit quantum state to Bob, provided they shared a pair of maximally entangled qubits to begin with.
   In this problem, Alice instead wants to share two classical bits with Bob, but she only has a quantum channel at her disposal, and she is only allowed to use it once (i.e. send only one single-qubit state). Can she succeed?

   (a) The first idea she has is to encode her two classical bits into her preparation of one of four states in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then send this qubit to Bob.
   Suppose that the a priori distribution of Alice's two classical bits is uniform. What is the maximum probability with which Bob can correctly guess both of Alice's two classical bits?

   (b) Suppose that Alice and Bob share a maximally entangled pair of qubits. Alice thinks that it is a good idea to start by performing one of four unitary transformations on the qubit in her possession depending on the value of the two classical bits that she wishes to communicate and send her qubit to Bob. What next? Help Alice (and Bob) devise a scheme that achieves the desired task with certainty.

(c) After all the thought that Alice and Bob put into coming up with a working scheme, they finally decide to employ it.
Unfortunately, the tireless eavesdropper Eve has heard of their new scheme, and as soon as Alice and Bob use it, she intercepts the qubit as it's sent from Alice to Bob. Can Eve recover information about the two confidential classical bits that Alice intended to share with Bob?

2. (6 points) **Secret sharing among three people.**
In class we saw how to share a classical secret between two people using an entangled state. In this problem we create a scheme that shares a classical secret among three people, Alice, Bob and Charlie. We encode the secret $b \in \{0,1\}$ in a GHZ-like state of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B |0\rangle_C + (-1)^b |1\rangle_A |1\rangle_B |1\rangle_C).$$

(a) Calculate the single-party reduced density matrices ρ_A, ρ_B, and ρ_C. Verify that no single one of Alice, Bob, and Charlie can recover the secret on their own.

(b) Calculate the two-party reduced densities ρ_{AB}, ρ_{BC}, and ρ_{AC}. Verify that no pair of Alice, Bob, and Charlie can recover the secret on their own.

(c) Suppose each of Alice, Bob, and Charlie is limited to the following operations:

- Local Hadamard operation on their qubit;
- Local measurement of their qubit in the computational basis $\{|0\rangle, |1\rangle\}$;
- Sending a (classical) measurement outcome to one of the other two players.

Devise a scheme by which they can together recover the secret b.

3. (8 points) **Inner product extractor.**

Define the inner product extractor $\mathrm{Ext}_{\mathrm{IP}} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ by $\mathrm{Ext}_{\mathrm{IP}}(x,y) = x \cdot y \mod 2$. Our goal is to show that this is a valid strong seeded extractor.

(a) Let

$$\mathcal{F} = \left\{ f_y : x \mapsto x \cdot y \mid y \in \{0,1\}^n \right\} \subseteq \left\{ f : \{0,1\}^n \to \{0,1\} \right\}.$$

Show that $\mathcal{F}$ is 2-universal.

Based on the work done in class, we already know that $\mathrm{Ext}_{\mathrm{IP}}$ is a (k,ε) extractor for any $k \geq 1 + 2\log(1/\varepsilon)$. The goal of this exercise is to give a different, more direct proof of this fact. In the following we consider a source of the form

$$\rho_{XE} = |\psi\rangle\langle\psi|_{XE}, \quad \text{where} \quad |\psi\rangle_{XE} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle_X |\psi_x\rangle_E .$$

Here, the $|\psi_x\rangle$ are normalized states (but not necessarily orthogonal), so that the marginal on X is uniform: $\rho_X = \frac{1}{2^n}\mathbb{I}_X$.

(b) We first rule out perfect adversaries. Namely, suppose that $|\psi\rangle_{XE}$ is such that given any $y \in \{0,1\}^n$, there is a measurement $\{M_b^y\}$ on E that returns $x \cdot y$ with certainty, i.e. $\mathrm{Tr}(M_b^y \rho_x) = 1$ if $b = x \cdot y$ and 0 otherwise.

i. Show carefully that there is a unitary U acting on E, Y, and an additional single-qubit register A such that $U : |\psi_x\rangle_E |y\rangle_Y |0\rangle_A \mapsto |\psi_x\rangle_E |y\rangle_Y |x \cdot y\rangle_A$ for all x, y.

ii. Consider an additional register B, initialized in $|-\rangle_B$. Compute the effect of

$$U' := (U \otimes \mathbb{I}_B)^\dagger (\mathbb{I}_{EY} \otimes \mathrm{CNOT}_{A \to B})(U \otimes \mathbb{I}_B)$$

on $|\psi_x\rangle_E |y\rangle_Y |0\rangle_A |-\rangle_B$, where here $\mathrm{CNOT}_{A \to B}$ applies an X bit flip to B controlled on A being in state $|1\rangle$.

iii. Deduce that there is a unitary $V : |\psi_x\rangle_E |0\rangle_Y |0\rangle_A |0\rangle_B \mapsto |x\rangle_E |0\rangle_Y |0\rangle_A |0\rangle_B$ for all x (where we make sure that E is large enough so that we are able to write 'x' in it). Say how to construct V as a function of U' and any other building blocks you may need.

iv. State an upper bound on $H_{\min}(X|E)_\rho$ for this (i.e. the assumption in (b)(i)) to be possible.

(c) We now analyze the more delicate case where the adversary does not perfectly predict the inner product. Let

$$\rho_{ZYE} = \frac{1}{2^{2n}} \sum_{x,y} |x \cdot y\rangle\langle x \cdot y| \otimes |y\rangle\langle y| \otimes |\psi_x\rangle\langle\psi_x| \quad \text{and} \quad \varepsilon = \left\| \rho_{ZYE} - \frac{\mathbb{I}_Z}{2} \otimes \frac{\mathbb{I}_Y}{2^n} \otimes \rho^E \right\|_{tr} .$$

i. For $b \in \{0,1\}$ and $y \in \{0,1\}^n$ let $\sigma_{b,y} = \frac{1}{2^{2n}} \sum_{x:\ c \cdot y = b} |\psi_x\rangle\langle\psi_x|_E$. Show that for every y, there is a measurement $\{M_b^y\}_{b \in \{0,1\}}$ on E such that

$$\frac{1}{2^n} \sum_y \left(\frac{1}{2} \mathrm{Tr}(M_0^y \sigma_{0,y}) + \frac{1}{2} \mathrm{Tr}(M_1^y \rho_{1,y}) \right) \geq \delta \, ,$$

for some δ depending on ε that you will determine.

ii. Deduce that there is a unitary $U : |\psi_x\rangle |y\rangle |a\rangle \mapsto |\psi'_x\rangle |y\rangle (\alpha_{x,y} |a \oplus x \cdot y\rangle + \beta_{x,y} |a \oplus x \cdot y \oplus 1\rangle)$ for all x, y and $a \in \{0,1\}$, and where $2^{-2n} \sum_{x,y} |\alpha_{x,y}|^2 \geq \delta$. Here, $|\psi'_x\rangle$ may be different from $|\psi_x\rangle$ but it is still normalized.

iii. Let $|\psi_{ideal}\rangle = (-1)^{x \cdot y} |\psi_x\rangle |y\rangle |0\rangle |-\rangle$ be the "ideal" state obtained as in (b)(ii). Compute the *difference* between $|\psi_{ideal}\rangle$ and $U' |\psi_x\rangle |y\rangle |0\rangle |-\rangle$ and bound its norm as a function of α_{xy} and β_{xy}.

iv. Deduce a lower bound on k, as a function of n and ε, such that $\mathrm{Ext}_{\mathrm{IP}}$ is a (k, ε) strong extractor.