COM-440, Introduction to Quantum Cryptography, Fall 2025

Midterm **October 30th, 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.

The total points value of the problems is 25 points. Your midterm grade will be the *minimum* of your total points number and *20*. This means that we do not expect you to solve all problems. Instead, we encourage you to spend the first 5-10 minutes looking at all problems and deciding which ones to attempt. Your goal is to collect as close to 20 points as possible in total, not necessarily to solve all questions.

Problems:

1. (6 points) **Superdense Coding.**
   In this problem, Alice wants to send two classical bits to 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, 2pts) 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, 2pts) 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, 2pts) 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, 2pts) 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, 2pts) 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, 2pts) 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. (3 points) **Quantum money security variant.**

Recall that in Wiesner's quantum money scheme, a bill is $(\$, |\psi_\$\rangle = |x_1\rangle_{\theta_1} \cdots |x_n\rangle_{\theta_n})$ where $x, \theta \in \{0,1\}^n$ and $|x\rangle_\theta = H^\theta |x\rangle$ and $\$ \in \{0,1\}^n$ is a serial number. The tuple $(\$, (x, \theta))$ is generated uniformly at random by the bank and kept in its private database, while $(\$, |\psi_\$\rangle)$ is given to the user. Verification is performed by measuring in the correct bases θ and accepting if and only if all outcomes match x.

In class we considered the security of Wiesner's quantum money under two different variants of the security game. In the first variant, the challenger gives a randomly generated bill $(\$, |\psi_\$\rangle)$ to the user, who is tasked with creating two quantum states both passing verification together with the same serial number $\$$. In the second variant, the user is additionally allowed to query a *verification oracle* that verifies the bill and returns it in case it was deemed valid. We saw that Wiesner's money is secure under the first variant (the adversary success probability is at most $(3/4)^n$), but not under the second due to the Elitzur-Vaidman bomb tester "attack" (the adversary success probability can be made $1 - \varepsilon$ for any $\varepsilon > 0$).

Consider a third variant where in the security game, the user is allowed to submit any bill for verification, *but* the only information they get as feedback is a single bit: whether the bill passed verification or not. The bill submitted to verification is not returned to the user. However, the adversary gets this feedback whether verification passed or not, i.e. they are not sent to jail even in case verification failed.

Do you think that Wiesner's scheme is secure under this third variant of the security game? Argue carefully your answer: if you believe the scheme is secure, provide a

security proof or a reduction to the first variant ; if you believe it is insecure then sketch an attack.

4. (10 points) **Inner product extractor.**

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

(a, 1pt) Let

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

Is the family $\mathcal{F}$ 2-universal? *[Recall the definition: $\mathcal{F}$ is 2 universal if, for every $x \neq x'$ and every z, z', $\mathbf{Pr}_{f \leftarrow_U \mathcal{F}}[f(x) = z \wedge f(x') = z'] = 2^{-2m}$ in case functions in f have range $\{0,1\}^m$.]*

The goal of this exercise is to give a direct, self-contained proof that $\mathrm{Ext}_{\mathrm{IP}}$ is a (k, ε) extractor, for a certain range of k depending on ε that we will determine at the end. 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: $\rho_X = \frac{1}{2^n}\mathbb{I}_X$. We also let $\rho_x = |\psi_x\rangle\langle\psi_x|$ and $\rho^E = 2^{-n}\sum_x \rho_x$.

(b) We first rule out perfect adversaries. For $b \in \{0,1\}$ and $y \in \{0,1\}^n$ let

$$\sigma_{b,y} = \frac{1}{2^{n-1}} \sum_{x:\ x \cdot y = b} \rho_x \ . \tag{1}$$

(i, 1pt) Suppose that for some y, it holds that

$$\|\sigma_{0,y} - \sigma_{2,y}\|_{tr} = 1 \ . \tag{2}$$

Show that there is a projection P_y such that $\mathrm{Tr}(P_y \sigma_{0,y}) = 1$ and $\mathrm{Tr}(P_y \sigma_{1,y}) = 0$.

(ii, 1pt) Suppose that the condition from the previous question is satisfied for all y. Show 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 (U should not depend on specific x, y, but it of course depends on the definition of $|\psi\rangle_{XE}$).

(iii, 1pt) 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 $|1\rangle$.

(iv, 1pt) Deduce that there is a unitary $V : |\psi_x\rangle_E |0\rangle_Y |0\rangle_A |0\rangle_B \mapsto |\psi_x\rangle_E |x\rangle_Y |0\rangle_A |0\rangle_B$ for all x. Say how to construct V as a function of U' and any other building blocks you may need.

(v, 1pt) State an upper bound on $H_{\min}(X|E)_\rho$ for this (i.e. the assumption (2) for all y) 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, 1pt) Recall the definition of $\sigma_{b,y}$ in (1). Show that for every y, there is a measurement $\{M_b^y\}_{b\in\{0,1\}}$ on E such that

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

for some δ depending on ε that you will determine.

(ii, 1pt) Deduce that there is a unitary

$$U \ : \ |\psi_x\rangle |y\rangle |0\rangle \ \mapsto \ \alpha_{x,y} |\psi'_{x,y}\rangle |y\rangle |x \cdot y\rangle + \beta_{x,y} |\psi''_{x,y}\rangle |y\rangle |(x \cdot y) \oplus 1\rangle$$

for all x, y, where $2^{-2n} \sum_{x,y} |\alpha_{x,y}|^2 \geq \frac{1}{2} + \delta$. Here, $|\psi'_{x,y}\rangle$ and $|\psi''_{x,y}\rangle$ may be different from $|\psi_x\rangle$ but each of them is still required to have norm 1.

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

(iv, 1pt) 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.