COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 4 **due: 11:59PM, December 16th, 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.

The goal of this problem set is to give a complete security proof of a bit commitment protocol in the bounded storage model. The first two exercises provide tools that are used in the last exercise, which is the main one. The results of the first two exercises can be assumed to solve the third. In particular, the second exercise is "bonus" and it is not required to solve it; if you wish you may use its result as a given.

Problems:

1. *(6 points)* **Approximate guessing**
   The leftover hash lemma allows us to bound the probability of exactly guessing an unknown string X, given access to a correlated quantum state in system E, as a function of the conditional min-entropy $H_{\min}(X|E)$. The bound that we obtain in (b) below will be used in the exercise on realizing bit commitment.

   For $X \in \{0,1\}^n$ and $0 \leq \delta < \frac{1}{2}$ we let $B^{\delta n}(X)$ denote the Hamming ball of radius δn around X, i.e. the set of all strings X' such that $|X \oplus X'|_H \leq \delta n$. Let $B^{\delta n} = |B^{\delta n}(X)|$, which does not depend on X. Let $\mathcal{F}$ be a 2-universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}$.

   (a) Let $X, \hat{X} \in \{0,1\}^n$ be arbitrary. Show that

   $$\mathop{\mathbf{Pr}}_{\substack{X' \leftarrow_U B^{\delta n}(\hat{X}) \\ F \leftarrow_U \mathcal{F}}} \left[F(X') = F(X)\right] = \frac{1}{2} + \frac{1}{2B^{\delta n}} 1_{\hat{X} \in B^{\delta n}(X)} \,.$$

(b) Use the leftover hash lemma to deduce that, if ρ_{XE} is an arbitrary quantum state and $\hat{X}$ a guess for X given the quantum state in E, then

$$\mathbf{Pr}\left[\hat{X} \in B^{\delta n}(X)\right] \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-1)+\log(B^{\delta n})+1} .$$

2. *(Bonus 4 points)* **An uncertainty relation**
Let ρ be an n-qubit density matrix. For $\theta \in \{0,1\}$ let $Q^\theta(\cdot)$ be the distribution on n-but strings that results from measuring each qubit of ρ in basis θ. The goal of this exercise is to show the following uncertainy relation: for any two sets $L^0, L^1 \subseteq \{0,1\}^n$ it holds that

$$Q^0(L^0) + Q^1(L^1) \leq \left(1 + \sqrt{2^{-n}|L^0| \cdot |L^1|}\right)^2 , \tag{1}$$

where for $\theta \in \{0,1\}$, $Q^\theta(L^\theta) := \sum_{x \in L^\theta} Q^\theta(x)$. To show this bound, we consider a purification $|\psi\rangle_{AB}$ of ρ_A and expand it as $|\psi\rangle_{AB} = \sum_x \alpha_x |x\rangle_A |\varphi_x\rangle_B$, where the $|\varphi_x\rangle_B$ have norm 1. This gives us that $Q^0(x) = |\alpha_x|^2$.

(a) Show that for any $z \in \{0,1\}^n$, $Q^1(z) = \| \sum_x 2^{-n/2}(-1)^{x\cdot z}\alpha_x |\varphi_x\rangle \|^2$.

(b) We decompose the summation in two parts, depending on whether $x \in L^0$ or $x \in S^0 = \overline{L^0}$. Let $p = Q^0(S^0)$ and

$$\xi_z = \frac{1}{\sqrt{p}} \left\| \sum_{x \in S^0} 2^{-n/2}(-1)^{x\cdot z}\alpha_x |\varphi_x\rangle \right\| .$$

Show that $\sum_z \xi_z^2 = 1$.

(c) Use the Cauchy-Schwarz inequality to show that

$$\left\| \sum_{x \in L^0} 2^{-n/2}(-1)^{x\cdot z}\alpha_x |\varphi_x\rangle \right\| \leq 2^{-n/2}\sqrt{|L^0|} .$$

(d) Starting from

$$Q^1(L^1) = \sum_{z \in L^1} Q^1(z) \leq \sum_{z \in L^1} \left(\sqrt{p}\xi_z + 2^{-n/2}\sqrt{|L^0|}\right)^2 ,$$

use the previous questions to show (1).

3. *(14 points)* **Bit commitment in the bounded storage model**
In class we gave a construction of an oblivious transfer protocol in the bounded storage model. We also saw that oblivious transfer implies bit commitment. In this problem we give a direct construction of a bit commitment protocol in the bounded storage model, with a different, quantitatively stronger analysis compared to class. Essentially, we replace the bound from the guessing game by the uncertainty relation proved in the previous problem.

Recall that in bit commitment, Alice (the *sender*) has an input $b \in \{0,1\}$, while Bob (the *receiver*) has no input. There are two phases, the *commit* and the *open* phases, as follows:

(i) Bob selects $x, \theta \in \{0,1\}^n$ uniformly at random and sends the qubits $|x_1\rangle_{\theta_1}, \ldots, |x_n\rangle_{\theta_n}$ to Alice.

(ii) To commit to b, Alice measures all qubits in basis $\theta' = b$, obtaining an n-bit string $\hat{x} \in \{0,1\}^n$.

(iii) To open the commitment, Alice sends b and $\hat{x}$ to Bob.

(iv) Bob checks that $x_i = \hat{x}_i$ whenever $\theta_i = b$, and accepts and returns b if and only if this is the case.

(a) Show that this protocol is correct.

(b) To show that the protocol is hiding, first introduce a version of the protocol where at the first step Bob sends half-EPR pairs to Alice. Write out the protocol step-by-step (following the same format as above), modifying the player's actions as appropriate (in particular, specify when and how Bob measures his half-EPR pairs.

(c) Argue that, if Bob is honest, a dishonest Alice cannot distinguish if she is playing with Bob that executes the protocol above, or your version with EPR pairs from the previous question.

(d) Show that the protocol above is perfectly hiding.

Next we will show that the protocol is ε-binding, for an ε depending on n to be determined, as long as dishonest Alice does not have too much quantum memory. To model this, introduce a parameter $0 \leq \gamma < \frac{1}{2}$ and assume that, at step (ii), Alice is forced to perform a measurement on her quantum memory that leaves her with a quantum state of at most γn qubits, stored in register E, and a classical outcome y of arbitrary size, stored in register Y. Our goal is to show that for such Alice the ε-binding property holds, i.e. if we let p_b be the probability that such Alice successfully opens $b \in \{0,1\}$ then $p_0 + p_1 \leq 1 + \varepsilon$.

Towards this we define a few quantities. Let $\kappa > 0$ be such that $\gamma + \kappa < \frac{1}{2}$. Conditioned on the classical y obtained as a result of the forced measurement at the beginning of step (ii), let $Q^\theta(\cdot)$ be the distribution that would result from measuring Bob's half-EPR pairs, in the EPR-pair version of the protocol, in basis $\theta \in \{0,1\}$.[1] Let $S^\theta = \{x \in \{0,1\}^n : Q^\theta(x) \leq 2^{-(\gamma+\kappa)n}\}$ (S for "small"), $L^\theta = \overline{S^\theta}$ and $q^\theta = Q^\theta(S^\theta)$ the total probability of "small" strings.

(e) Show that, by definition of the min-entropy, if X is a random variable with distribution Q^θ then

$$H_{\min}(X|E, Y = y, \Theta = \theta, X \in S^\theta) \geq \kappa n + \log(q^\theta) \ .$$

[1] To understand this, suppose for example that at step (ii) dishonest Alice measures everything in the computational basis and obtains a string x'. Then, $Q^0(x) = 1$ if $x = x'$ and 0 otherwise, and $Q^1(z) = 2^{-n}$ for every z ; because Bob's half-EPR pairs are projected to $|x'\rangle_0$ as a result of Alice's measurement.

To make the $H_{\min}(\cdot)$ term precise, define an appropriate quantum state as follows. First let $\rho_{X\Theta YE}$ be the density matrix that represents the (classical) distribution on Bob's side ($X \in \{0,1\}^n$ is the result of measuring Bob's EPR pairs in basis $\Theta \in \{0,1\}$), the classical outcome Y obtained from the (forced) measurement of Alice's half EPR pairs, and E the at most γn qubits that Alice was allowed to keep. Then, for some fixed values y and θ we condition on $Y = y$, $\Theta = \theta$ and $X \in S^\theta$, i.e. we restrict those classical random variables to the prescribed values and renormalize the density matrix.

(f) Suppose that $q^\theta \geq 2^{-\varepsilon n/2}$, and assume δ chosen small enough that $B^{\delta n} \leq 2^{(\kappa-\varepsilon)n/2}$. Let $\hat{X}$ be any "guess" produced from y, θ and the quantum state in E. Show that

$$\mathbf{Pr}(\hat{X} \in B^{\delta n}(X) | X \in S^\theta) \leq 2^{-\frac{\varepsilon}{4}n+\frac{3}{2}} .$$

(g) If $\hat{X} \notin B^{\delta n}(X)$, what is the probability that honest Bob accepts?

(h) Deduce a bound of the form $p_b \leq 1 - q^b + f(n)$, where f is a function depending on ε, δ that goes to 0 as $n \to \infty$ (as long as both $\varepsilon, \delta > 0$).

(i) Use (1) from the previous problem to obtain a lower bound on $q^0 + q^1$ and deduce the binding condition, i.e. a bound of the form $p_0 + p_1 \leq 1 + \mathrm{negl}(n)$.