# COM-440, Introduction to Quantum Cryptography, Fall 2025

## Homework # 4 Solutions

---

**Problems:**

1. **Approximate guessing**

   (a) By total probability

$$\begin{aligned}
&\Pr_{\substack{X' \leftarrow_U B^{\delta n}(\hat{X}) \\ F \leftarrow_U \mathcal{F}}} \left[F(X') = F(X)\right] \\
=&\Pr_{\substack{X' \leftarrow_U B^{\delta n}(\hat{X}) \\ F \leftarrow_U \mathcal{F}}} \left[F(X') = F(X) \wedge X' \neq X\right] + \Pr_{\substack{X' \leftarrow_U B^{\delta n}(\hat{X}) \\ F \leftarrow_U \mathcal{F}}} \left[F(X') = F(X) \wedge X' = X\right] \\
=&\frac{1}{2}(1 - \frac{1}{B^{\delta n}} 1_{\hat{X} \in B^{\delta n}(X)}) + \frac{1}{B^{\delta n}} 1_{\hat{X} \in B^{\delta n}(X)} \qquad \text{(By properties of } \mathcal{F}\text{)} \\
=&\frac{1}{2} + \frac{1}{2B^{\delta n}} 1_{\hat{X} \in B^{\delta n}(X)} \ .
\end{aligned}$$

   (b) By the leftover hash lemma, if $m = 1 \leq H_{\min}(H|E) - 2\log 1/\varepsilon$

$$D(\rho_{F(X)E}, \frac{1}{2}\mathbb{I} \otimes \rho_E) \leq \varepsilon \ .$$

   In other words,

$$D(\rho_{F(X)E}, \frac{1}{2}\mathbb{I} \otimes \rho_E) \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-1)} \ .$$

   Note that on the one hand, for $\frac{1}{2}\mathbb{I} \otimes \rho_E$, the probability that given the quantum state in $E$, an adversary can guess the first register with probability exactly $\frac{1}{2}$.
   On the other hand, for $\mathbb{I} \otimes \rho_E$, the probability that given the quantum state in $E$, an adversary can guess $F(X)$ with probability at least $\frac{1}{2} + \frac{1}{2B^{\delta n}} \mathbf{Pr}[\hat{X} \in B^{\delta n}(X)]$ by part (a), since the adversary can first guess $\hat{X}$, and then guess the first register using $F(X')$ for $X' \leftarrow_U B^{\delta n}(\hat{X})$.
   By the operation meaning of trace distance,

$$D(\rho_{f(X)E}, \frac{1}{2}\mathbb{I} \otimes \rho_E) \geq \frac{1}{2} + \frac{1}{2B^{\delta n}} \mathbf{Pr}[\hat{X} \in B^{\delta n}(X)] - \frac{1}{2} = \frac{1}{2B^{\delta n}} \mathbf{Pr}[\hat{X} \in B^{\delta n}(X)] \ .$$

   As a result, $\frac{1}{2B^{\delta n}} \mathbf{Pr}[\hat{X} \in B^{\delta n}(X)] \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-1)}$.
   Therefore, $\mathbf{Pr}[\hat{X} \in B^{\delta n}(X)] \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-1)+\log(B^{\delta n})+1}$.
   You may also use the stronger version of leftover hash lemma from Chapter 5.3.4, which would give the bound $\mathbf{Pr}[\hat{X} \in B^{\delta n}(X)] \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-1)+\log(B^{\delta n})}$.

2. **An uncertainty relation**

(a) $Q^1(z)$ is the probability that we get the outcome $z$ when measuring each qubit in register $A$ of the state $|\psi\rangle_{AB}$ in the Hadamard basis. Therefore,

$$\begin{aligned} Q^1(z) &= \|(\langle z_1|_{\theta_1=1} \cdots \langle z_n|_{\theta_n=1})_A \cdot |\psi\rangle_{AB} \|^2 \\ &= \|2^{-n/2}( \sum_{x' \in \{0,1\}^n} (-1)^{x' \cdot z} \langle x'|)_A \cdot |\psi\rangle_{AB} \|^2 \\ &= \|2^{-n/2}( \sum_{x' \in \{0,1\}^n} (-1)^{x' \cdot z} \langle x'|)_A \cdot \sum_x \alpha_x |x\rangle_A |\varphi_x\rangle_B \|^2 \\ &= \| \sum_{x \in \{0,1\}^n} 2^{-n/2} (-1)^{x \cdot z} \alpha_x |\varphi_x\rangle \|^2 \ . \end{aligned}$$

(b) Since the unitary $H$ preserves the norm, we have that

$$\begin{aligned} \sum_z \xi_z^2 =& \sum_z \frac{1}{p} \Big\| \sum_{x \in S^0} 2^{-n/2} (-1)^{x \cdot z} \alpha_x |\varphi_x\rangle \Big\|^2 \\ =& \frac{1}{p} \Big\| \sum_z \sum_{x \in S^0} 2^{-n/2} (-1)^{x \cdot z} \alpha_x |z\rangle |\varphi_x\rangle \Big\|^2 \\ =& \frac{1}{p} \Big\| \sum_{x \in S^0} \alpha_x |x_1\rangle_{\theta_1=1} \cdots |x_n\rangle_{\theta_n=1} |\varphi_x\rangle \Big\|^2 \\ =& \frac{1}{p} \Big\| \sum_{x \in S^0} \alpha_x H|x_1\rangle_{\theta_1=1} \cdots H|x_n\rangle_{\theta_n=1} |\varphi_x\rangle \Big\|^2 \\ =& \frac{1}{p} \Big\| \sum_{x \in S^0} \alpha_x |x\rangle |\varphi_x\rangle \Big\|^2 \\ =& \frac{1}{p} \sum_{x \in S_0} |\alpha_x|^2 \\ =& 1 \ . \end{aligned}$$

(c) By the triangle inequality and the Cauchy-Schwarz inequality,

$$\begin{aligned} \Big\| \sum_{x \in L^0} 2^{-n/2} (-1)^{x \cdot z} \alpha_x |\varphi_x\rangle \Big\| &\leq \sum_{x \in L^0} \Big\| 2^{-n/2} (-1)^{x \cdot z} \alpha_x |\varphi_x\rangle \Big\| \\ &= 2^{-n/2} \sum_{x \in L^0} |\alpha_x| \\ &= 2^{-n/2} \sqrt{|L^0| \sum_{x \in L^0} |\alpha_x|^2} \\ &= 2^{-n/2} \sqrt{|L^0|} \ . \end{aligned}$$

(d) With the notation from previous part, we have that

$$Q^0(L^0) = 1 - Q^0(\overline{L^0}) = 1 - Q^0(S^0) = 1 - p \ .$$

Moreover,

$$\begin{aligned}
Q^1(L^1) &= \sum_{z \in L^1} Q^1(z) \\
&= \sum_{z \in L^1} \| \sum_{x \in \{0,1\}^n} 2^{-n/2}(-1)^{x \cdot z} \alpha_x \left|\varphi_x\right\rangle \|^2 \\
&= \sum_{z \in L^1} \left( \| \sum_{x \in S_0} 2^{-n/2}(-1)^{x \cdot z} \alpha_x \left|\varphi_x\right\rangle \| + \| \sum_{x \in L_0} 2^{-n/2}(-1)^{x \cdot z} \alpha_x \left|\varphi_x\right\rangle \| \right)^2 \\
&\qquad\qquad \text{(Triangle inequality)} \\
&\leq \sum_{z \in L^1} \left( \sqrt{p}\xi_z + 2^{-n/2}\sqrt{|L^0|} \right)^2 \qquad \text{(Part (c))} \\
&\leq \sum_{z \in L^1} p\xi_z^2 + 2^{-n}|L^0||L^1| + 2 \sum_{z \in L^1} \sqrt{p}\xi_z \cdot 2^{-n/2}\sqrt{|L^0|} \\
&\leq p + 2^{-n}|L^0||L^1| + 2 \sum_{z \in L^1} \xi_z \cdot 2^{-n/2}\sqrt{|L^0|} \qquad \text{(Part (b) and } p \leq 1\text{)}
\end{aligned}$$

Note that by the Cauchy-Schwarz inequality, $\sum_{z \in L^1} \xi_z \leq \sqrt{|L_1| \sum_{z \in L^1} \xi_z^2} \leq \sqrt{|L_1|}$. Combining the above equations, we obtain $Q^0(L^0) + Q^1(L^1) \leq \left(1 + \sqrt{2^{-n}|L^0| \cdot |L^1|}\right)^2$.

3. **Bit commitment in the bounded storage model**

(a) This is not hard to verify.

(b) The scheme is perfect hiding because when Bob is dishonest and Alice is honest, in the commitment phase, Bob sends (part of) a state of his choice, and Alice measures all the qubits she receives in basis $b$. The partial density matrix of the state on Bob's side does not change when Alice makes a measurement on the state on her side. Therefore, the partial density matrix of the state on Bob's side when $b = 0$ is the same as the partial density matrix of the state on Bob's side when $b = 1$. Therefore, the scheme is perfect hiding.

(c) The EPR-pair version of the protocol works as follows:

(i) Bob prepares $n$ EPR pairs on registers $A_i, B_i$ for $i \in [n]$, and sends the states on registers $A_1, ..., A_n$ 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 selects $\theta \in \{0,1\}^n$ uniformly at random, and measures the register $B_i$ in $\theta_i$ basis to obtain $x_i$ for each $i \in [n]$.

(v) 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.

(d) For a dishonest Alice, since she does not have access to the registers $B_1, ..., B_n$, she cannot distinguish the measurements on the registers $B_1, ..., B_n$ (step (iv) in the above protocol) are performed as described above, or are performed after step (i) in the above protocol. It is not hard to see that if the measurements are performed after step (i), then it is the same as the original protocol. Therefore, dishonest Alice cannot distinguish the original protocol and the EPR-pair version of the protocol.

(e) For $x \in S^\theta$,

$$\mathop{\mathbf{Pr}}_{X \leftarrow Q^\theta}(X = x | X \in S^\theta) = \mathop{\mathbf{Pr}}_{X \leftarrow Q^\theta}(X = x) / \mathop{\mathbf{Pr}}_{X \leftarrow Q^\theta}(X \in S^\theta) = \mathop{\mathbf{Pr}}_{X \leftarrow Q^\theta}(X = x)/q^\theta \ .$$

By the definition of $S^\theta$, we can continue the equation to get

$$\mathop{\mathbf{Pr}}_{X \leftarrow Q^\theta}(X = x | X \in S^\theta) \leq 2^{-(\gamma+\kappa)n}/q^\theta \ .$$

Therefore,

$$\begin{aligned} & H_{\min}(X|Y = y, \Theta = \theta, X \in S^\theta) \\ =& \max_x \log \frac{1}{\mathbf{Pr}_{X \leftarrow Q^\theta}(X = x | X \in S^\theta)} \\ \geq& (\gamma + \kappa)n + \log(q^\theta) \ . \end{aligned}$$

Since $E$ has size at most $\gamma n$, by the property of conditional min-entropy,

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

(f) This follows from part (e) and part (b) of Problem 1.

$$\begin{aligned} \mathbf{Pr}(\hat{X} \in B^{\delta n}(X) | X \in S^\theta) \leq& 2^{-\frac{1}{2}(H_{\min}(X|E')-1)+\log(B^{\delta n})+1} \\ \leq& 2^{-\frac{1}{2}(\kappa n+\log(q^\theta)-1)+\log(B^{\delta n})+1} \\ \leq& 2^{-\frac{1}{2}(\kappa n-\varepsilon n/2-1)+(\kappa-\varepsilon)n/2+1} \\ \leq& 2^{-\frac{\varepsilon}{4}n+\frac{3}{2}} \ , \end{aligned}$$

where $E' = (E, Y = y, \Theta = \theta, X \in S^\theta)$.

You may also use a stronger version of part (b) of Problem 1, which would give the bound $\mathbf{Pr}(\hat{X} \in B^{\delta n}(X) | X \in S^\theta) \leq 2^{-\frac{\varepsilon}{4}n+\frac{1}{2}}$.

(g) If $\hat{X} \notin B^{\delta n}(X)$, there are at least $\delta n$ positions at which $\hat{X}$ and $X$ differ. For each position, the honest Bob chooses to measure in basis $\theta$ with $1/2$ probability. The honest Bob accepts only if on the $\delta n$ positions, Bob measures it in basis $1-\theta$. Therefore, honest Bob accepts with probability at most $2^{-\delta n}$.

(h) We choose $f(n) = \max(2^{-\frac{\varepsilon}{4}n+\frac{3}{2}} + 2^{-\delta n}, 2^{-\varepsilon n/2})$. It's clear that $f$ goes to 0 as $n \to \infty$ (as long as both $\varepsilon, \delta > 0$).
$p_b = \mathbf{Pr}[\text{Bob accept } b \wedge \hat{X} \notin B^{\delta n}(X)] + \mathbf{Pr}[\text{Bob accept } b \wedge \hat{X} \in B^{\delta n}(X)]$. We bound each probability separately as follows:

$$\mathbf{Pr}[\text{Bob accept } b \wedge \hat{X} \notin B^{\delta n}(X)] \leq \mathbf{Pr}[\text{Bob accept } b | \hat{X} \notin B^{\delta n}(X)] \leq 2^{-\delta n} \ ,$$

by part (g).

$$\begin{aligned}
&\mathbf{Pr}[\text{Bob accept } b \wedge \hat{X} \in B^{\delta n}(X)] \\
=&\mathbf{Pr}[\hat{X} \in B^{\delta n}(X) \wedge X \in S^b] + \mathbf{Pr}[\hat{X} \in B^{\delta n}(X) \wedge X \notin S^b] \\
\leq&\mathbf{Pr}[\hat{X} \in B^{\delta n}(X) | X \in S^b] + \mathbf{Pr}[X \notin S^b] \\
=&\mathbf{Pr}[\hat{X} \in B^{\delta n}(X) | X \in S^b] + 1 - q^b \ .
\end{aligned}$$

By part (f), if $q^b \geq 2^{-\varepsilon n/2}$, $\mathbf{Pr}[\hat{X} \in B^{\delta n}(X) | X \in S^b] \leq 2^{-\frac{\varepsilon}{4}n+\frac{3}{2}}$ and therefore, combining the above equations, we obtain $p_b \leq 1 - q^b + f(n)$.
On the other hand, if $q^b \leq 2^{-\varepsilon n/2}$, it's easy to see that $p_b \leq 1 \leq 1 - q^b + f(n)$.
Thus $p_b \leq 1 - q^b + f(n)$ in both cases.
A common mistake is forgetting the assumption of part (f) when invoking it.

(i) By Problem 2, $(1-q^0) + (1-q^1) = Q^0(L^0) + Q^1(L^1) \leq \left(1 + \sqrt{2^{-n}|L^0| \cdot |L^1|}\right)^2$.
Since $L^\theta = \{x \in \{0,1\}^n : Q^\theta(x) > 2^{-(\gamma+\kappa)n}\}$ and $\sum_{x \in \{0,1\}^n} Q^\theta(x) = 1$, we have that $|L^\theta| \leq 2^{(\gamma+\kappa)n}$. Hence $(1-q^0) + (1-q^1) \leq (1 + 2^{-n(\frac{1}{2}-\gamma-\kappa)})^2 = 1 + \text{negl}(n)$, i.e. $q^0 + q^1 \geq 1 - \text{negl}(n)$.
Then by part (h), $p_0 + p_1 \leq (1-q^0) + \text{negl}(n) + (1-q^1) + \text{negl}(n) \leq 1 + \text{negl}(n)$.