Lecture 10: Examples of Hybrid Arguments
We are interested in showing the other direction of the proof 
(2) \(\implies\) (1)

We consider the contrapositive: 
\(\neg(1) \implies \neg(2)\)

\(\neg(1)\) is equivalent to: There exists an efficient adversary \(A^*\) 
and constant \(c\) such that

\[
Pr[A^*(G(U_{\{0,1\}^n})) = 1] - Pr[A^*(U_{\{0,1\}^{n+\ell}}) = 1] > 1/n^c
\]

Our aim is to show \(\neg(2)\): This is equivalent to constructing an 
efficient adversary \(\tilde{A}\), and showing the existence of 
\(\tilde{i} \in \{1, \ldots, n + \ell\}\) and constant \(d\) such that the distribution 
\(G(u_{\{0,1\}^n})_{\leq \tilde{i}}\) is not next-bit unpredictable and the advantage 
of distinguishing is at least \(1/n^d\)
Consider $Y_1 \ldots Y_{n+\ell} = G(U_{\{0,1\}^n})$ and $U_1 \ldots U_{n+\ell} = U_{\{0,1\}^{n+\ell}}$

For $i \in \{0, 1, \ldots, n + \ell\}$, let $X^{(i)}$ be the distribution:

$$(Y_1, \ldots, Y_{n+\ell-i}, U_{n+\ell-i+1}, \ldots, U_{n+\ell})$$

Note that: $X^{(0)} = Y_1 \ldots Y_{n+\ell}$ and $X^{(n+\ell)} = U_1 \ldots U_{n+\ell}$

We know that $\Pr[A^*(X^{(0)}) = 1] - \Pr[A^*(X^{(n+\ell)}) = 1] \geq 1/n^c$

So, there exists $i^* \in \{1, \ldots, n + \ell\}$ such that

$$\Pr[A^*(X^{(i^*-1)}) = 1] - \Pr[A^*(X^{(i^*)} = 1)] \geq \frac{1}{n^c(n + \ell)}$$

The last step is known as the “Hybrid-argument.” Prove:

Using triangle inequality prove the conclusion made in the previous step.
Let us take a closer look at $X^{(i^*-1)}$ and $X^{(i^*)}$ distributions

$$X^{(i^*-1)} = (Y_1, \ldots, Y_{n+\ell-i^*}, Y_{n+\ell-i^*+1}, U_{n+\ell-i^*+2}, \ldots, U_{n+\ell})$$

$$X^{(i^*)} = (Y_1, \ldots, Y_{n+\ell-i^*}, U_{n+\ell-i^*+1}, U_{n+\ell-i^*+2}, \ldots, U_{n+\ell})$$

The only thing that changes is the $(n+\ell-i^*+1)$-th entry

Our adversary $\tilde{A}$ will predict the $(n+\ell-i^*+1)$-th bit

So, we choose $\tilde{i} = (n+\ell-i^*+1)$

Note that $A^*$ outputs 1 with higher probability when the $\tilde{i}$-th bit is sampled according to $Y_{\tilde{i}}$ instead of $U_{\tilde{i}}$. We want to leverage this advantage in the next-bit unpredictability experiment

Recall the next-bit unpredictability experiment for $i = \tilde{i}$. The adversary receives $\alpha \sim Y_1, \ldots, Y_{n+\ell-i^*}$. If $b = 0$ we have $\beta \sim Y_{n+\ell-i^*+1}$, otherwise (if $b = 1$) we have $\beta \sim U_{\{0,1\}}$
(2) \implies (1)

- Code of \( \widetilde{A} \) on input \((\alpha, \beta)\)
  - Sample \( u_{i+1} \ldots u_{n+\ell} \sim U_{\{0,1\}^{n+\ell-i}} \)
  - Let \( c = \widetilde{A}^*(\alpha, \beta, u_{i+1} \ldots u_{n+\ell}) \)
  - If \( c = 1 \), set \( \widetilde{b} = 0 \); otherwise \( \widetilde{b} = 1 \)
  - Return \( \widetilde{b} \)

- Prove: The advantage of \( \widetilde{b} = b \) is \( > \frac{1}{2n^c(n+\ell)} \).

- Set \( d \) such that \( \frac{1}{2n^c(n+\ell)} \geq \frac{1}{n^d} \). This completes the proof.
One-bit Stretch PRG implies PRG

**Definition (One-bit Stretch PRG)**

A family of function $G_n : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ is called a one-bit stretch PRG if there exists a negligible function $\varepsilon(n)$ such that:

$$G(U_{\{0,1\}^n}) \approx^{(c)} U_{\{0,1\}^{n+1}}$$

Prove using hybrid argument that the function $F_n : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\ell}$ defined below:

$$F_n(s) = G_{n+\ell-1}(\cdots G_{n+1}(G_n(s))\cdots)$$

is a PRG with indistinguishability $\varepsilon(n) + \varepsilon(n+1) + \cdots + \varepsilon(n+\ell-1)$
One-bit Stretch PRG implies PRG

Let $H_n: \{0, 1\}^n \rightarrow \{0, 1\}^{n + \ell}$ be a function defined by the following algorithm: $H_n(s)$ is calculated as follows

- $s^{(0)} = s$
- For $i \in \{1, \ldots, n + \ell\}$: Let $G_n(s^{(i-1)}) = (s^{(i)}, b_i)$, where $s^{(i)} \in \{0, 1\}^n$ and $b_i \in \{0, 1\}$
- Output $(b_1, \ldots, b_{n+\ell})$

Prove using hybrid argument that $H_n$ is a PRG with indistinguishability $(n + \ell)\varepsilon(n)$

Think: How to use this PRG to construct encryption scheme for multiple arbitrary length messages (assume that the sender and the receiver can maintain an $n$-bit secret state)