Theorem 2 (Lecture 6)

If G is next-bit unpredictable, then G is pseudorandom

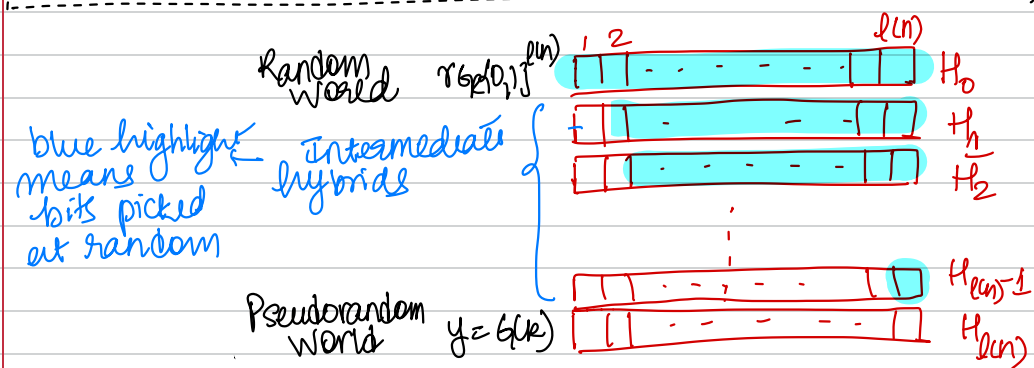
Proof

Assume to the contrary that G is not pseudorandom

$\Rightarrow \exists$ PPT Eve^{PS} such that

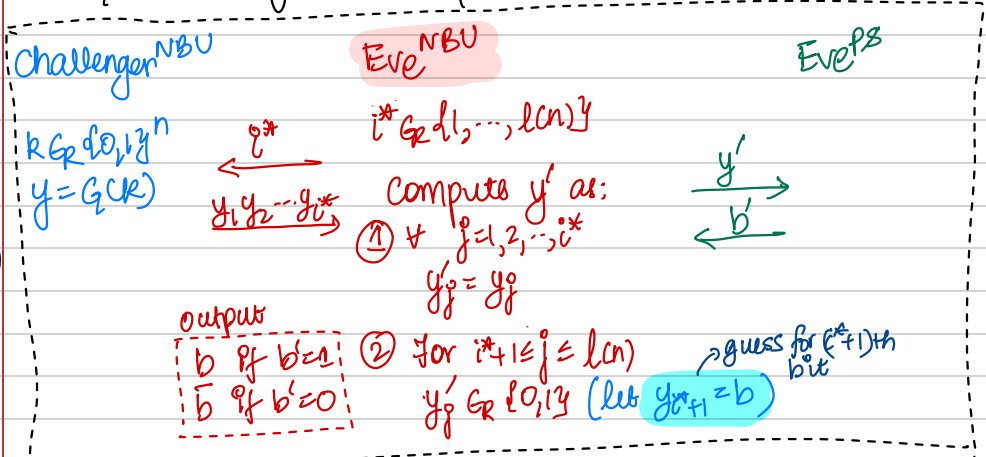
(I) $$\left| Pr[Eve^{PS}(H_0) = 1] - Pr[Eve^{PS}(H_{\ell(n)}) = 1] \right| > \delta$$

δ ↓ non-negligible



Now, let's define the predictor Eve^{NBU}

(II)



Analyzing Eve^{NBU}'s success probability in (II):

$$\Pr_{y \leftarrow G(k)}[\text{Eve}^{\text{NBU}}(y_1, y_2, \cdots, y_{\ell(n)}^*) = y_{i+1}^*]$$

$$= \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i^* b \cdots) = 1 \mid b = y_{i+1}^*] \cdot \Pr[b = y_{i+1}^*] + \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i^* b \cdots) = 0 \mid b \neq y_{i+1}^*] \cdot \Pr[b \neq y_{i+1}^*]$$

$$= \frac{1}{2} \cdot \frac{1}{\ell(n)} \sum_{i=1}^{\ell(n)} \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i y_{i+1} \cdots) = 1] + \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i \bar{y}_{i+1} \cdots) = 0]$$

$$= \frac{1}{2} + \frac{1}{2\ell(n)} \sum_{i=1}^{\ell(n)} \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i y_{i+1} \cdots) = 1] - \Pr[\text{Eve}^{PS}(y_1 y_2 \cdots y_i \bar{y}_{i+1} \cdots) = 1]$$

$\Pr[\text{Eve}^{PS}(H_{i+1}^{\ell(n)}) = 1]$ ($\because$ $i+1$ pseudorandom, then random)

$\Pr[\text{Eve}^{PS}(H_i^{\ell(n)}) = 1]$ (simulates reason)

$$= \frac{1}{2} + \frac{1}{2\ell(n)} \sum_{i=0}^{\ell(n)-1} \Pr[\text{Eve}^{PS}(H_{i+1}^{\ell(n)}) = 1] - \Pr[\text{Eve}^{PS}(H_i^{\ell(n)}) = 1]$$

things cancel out and you get ↓

$$= \frac{1}{2} + \frac{1}{2\ell(n)} \Pr[\text{Eve}^{PS}(H_{\ell(n)}^{\ell(n)}) = 1] - \Pr[\text{Eve}^{PS}(H_0^{\ell(n)}) = 1]$$

$$> \frac{1}{2} + \frac{\delta}{2\ell(n)}$$ (by assumption (I))

■