

## Theorem 2 (Lecture 6)

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

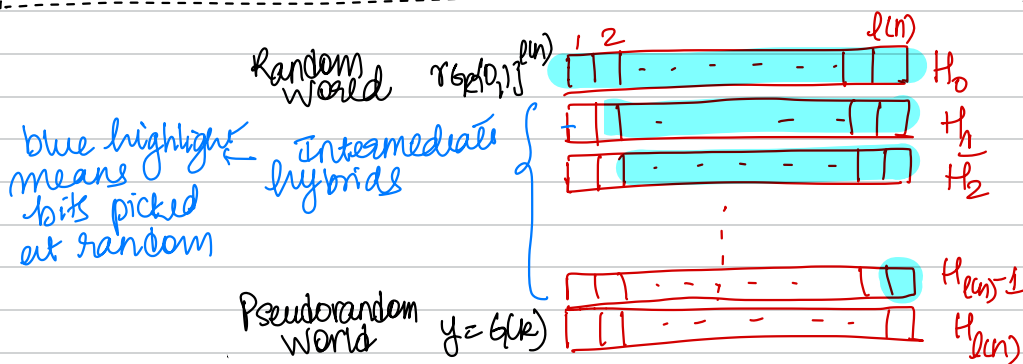
Proof

Assume to the contrary that  $G$  is not pseudorandom

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

$$\textcircled{\text{I}} \quad |\Pr[\text{Eve}^{\text{PS}}(H_0) = 1] - \Pr[\text{Eve}^{\text{PS}}(H_{\text{len}}) = 1]| > \delta$$

non-negligible



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

Challenger<sup>NBU</sup>

$k \leftarrow \{0,1\}^n$   
 $y = G(k)$

$\text{Eve}^{\text{NBU}}$

$i^* \leftarrow \{1, \dots, \text{len}\}$

compute  $y'$  as:

$\textcircled{1} \forall j=1, 2, \dots, i^*$

$y'_j = y_j$

output

$b$  if  $b' \neq 1$

$\bar{b}$  if  $b' = 0$

$\textcircled{2} \forall i^*+1 \leq j \leq \text{len}$

$y'_j \leftarrow \{0,1\}$  (let  $y_{i^*+1} = b$ )

$y'$   
 $\leftarrow b'$

$\text{Eve}^{\text{PS}}$

guess for  $(i^*+1)$ th bit

$\textcircled{\text{II}}$

Analyzing Eve<sup>NBU</sup>'s success probability in (I):

$$\begin{aligned}
 & \Pr_{y \leftarrow G(k)} [\text{Eve}^{\text{NBU}}(y_1, y_2, \dots, y_{\ell n}^*) = y_{\ell n+1}^*] \\
 = & \Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_{\ell n}^* \text{ b } \dots) = 1 \mid \text{b} = y_{\ell n+1}^*] \cdot \Pr[\text{b} = y_{\ell n+1}^*] \\
 & + \Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_{\ell n}^* \text{ b } \dots) = 0 \mid \text{b} \neq y_{\ell n+1}^*] \cdot \Pr[\text{b} \neq y_{\ell n+1}^*] \\
 = & \frac{1}{2} \cdot \frac{1}{\ell n} \sum_{i=1}^{\ell n} \Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_i, y_{i+1}, \dots) = 1] + \Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_{\ell n}, y_{\ell n+1}) = 0] \\
 = & \frac{1}{2} + \frac{1}{2 \ell n} \sum_{i=1}^{\ell n} \underbrace{\Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_i, y_{i+1}, \dots) = 1]}_{\text{Pr} [\text{Eve}^{\text{PS}}(H_{i+1}) = 1]} - \underbrace{\Pr [\text{Eve}^{\text{PS}}(y_1, y_2, \dots, y_{\ell n}, y_{\ell n+1}) = 1]}_{\text{Pr} [\text{Eve}^{\text{PS}}(H_{\ell n}) = 1]} \\
 & \quad (\because i+1 \text{ pseudorandom, then random}) \quad (\text{Simulator reason}) \\
 = & \frac{1}{2} + \frac{1}{2 \ell n} \sum_{i=0}^{\ell n-1} \Pr [\text{Eve}^{\text{PS}}(H_{i+1}) = 1] - \Pr [\text{Eve}^{\text{PS}}(H_{\ell n}) = 1] \\
 & \quad \text{things cancel out and you get } \downarrow \\
 = & \frac{1}{2} + \frac{1}{2 \ell n} \Pr [\text{Eve}^{\text{PS}}(H_{\ell n}) = 1] - \Pr [\text{Eve}^{\text{PS}}(H_0) = 1] \\
 > & \frac{1}{2} + \frac{\epsilon}{2 \ell n} \quad (\text{by assumption (I)})
 \end{aligned}$$