



Last time, PRG definition

$$\text{GAME}_{G,A}^{\text{PRG}}(\lambda, b)$$

$A \xrightarrow{2} \mathcal{C}_{\text{PRG}}$   
 $\xrightarrow{b' \in \{0,1\}^{\lambda}}$   
 $b = 0; z \in G(s); s \leftarrow U_{\lambda}$   
 $b = 1; z \leftarrow U_{\lambda+R}$

$$\text{GAME}_{G,A}^{\text{PRG}}(\lambda, 0) \stackrel{c}{=} \text{GAME}_{G,A}^{\text{PRG}}(\lambda, 1)$$

$\forall \text{PPT } A$   
 $|P_A[\text{GAME}(\lambda, 0) = 1] - P_A[\text{GAME}(\lambda, 1) = 1]| < \text{neg}(\lambda)$

We want to show:

- OWF  $\Rightarrow$  PRG
- PRG  $\Rightarrow$  SKE (beating Shannon)

① PRG  $\Rightarrow$  SKE

assuming  $G: \{0,1\}^{\lambda} \rightarrow \{0,1\}^{\lambda+R}$

simple  $\Pi = (\text{ENC}, \text{DEC})$  for  $K = \{0,1\}^{\lambda}$ ,  $\mathcal{M} = \{0,1\}^{\lambda+R}$

$\text{ENC}(k, m) = G(k) \oplus m$   
 $\text{DEC}(k, c) = c \oplus G(k) \oplus m$

Secure SKE against PPT A?

$$\text{GAME}_{\Pi, A}^{\text{SKE}}(\lambda, b)$$

$A \xrightarrow{m_0, m_1 \in \mathcal{M}} \mathcal{C}_{\text{SKE}}$   
 $\xrightarrow{c} k \leftarrow U_{\lambda}$   
 $\xrightarrow{b'}$

$c = \text{Enc}(k, m_i)$   
 $b = 0 \rightarrow \text{decrypt } m_0$   
 $b = 1 \rightarrow \text{encrypt } m_1$

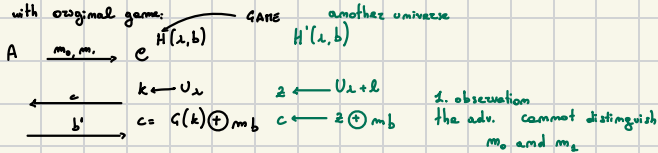
DEF.  $\Pi$  is ONE TIME SECURE if  $\text{GAME}_{\Pi, A}^{\text{SKE}}(\lambda, 0) \stackrel{c}{=} \text{GAME}_{\Pi, A}^{\text{SKE}}(\lambda, 1)$

Why is it good?

- For secure SKE it should be HARD to:
- get the key from  $c$ , but  $\text{ENC}(k, m) = m$   $\rightarrow$  stupid encryption
  - get  $m$  from  $c$
  - get first bit of  $m$  from  $c$   $\rightarrow$  Adversary choose the messages
  - get ANY info of  $m$ !

**THM** if  $G$  is a PRG, then: above  $\Pi$  is ONE TIME SECURE

**PROOF** We start with original game:



Need to show:  $H(\lambda, 0) \approx_c H(\lambda, 1)$

**LEMMA:**  $H'(\lambda, 0) = H'(\lambda, 1)$

Follows by PERFECT SECRECY

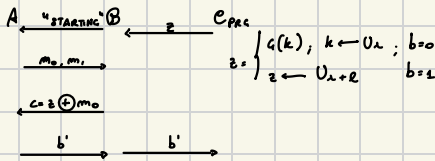
**LEMMA:**  $\forall b \in \{0, 1\}, H(\lambda, b) \approx_c H'(\lambda, b)$

**PROOF.** by reduction. fix  $b=0$  and assume not

$\exists$  PPT A s.t.

$$|P_z[H(\lambda, b) = a] - P_z[H'(\lambda, b) = a]| \geq \epsilon / \text{negl}(\lambda)$$

$\exists$  PPT B "breaking" G



$$P_z[B \text{ output } b' = 1 : z = G(s); s \leftarrow U_\lambda]$$

$$= P_z[\text{GAME PRG}(\lambda, 0) = 1]$$

$$= P_z[A \text{ output } b' = 1 : c = G(s) \oplus m_0]$$

$$= P_z[H(\lambda, 0) = 1]$$

$$P_z[H'(\lambda, 0) = 1] = P_z[\text{GAME PRG}(\lambda, 1) = 1]$$

$$\Rightarrow P_z[\text{GAME PRG}_{G, B}(\lambda, 0) = 1] - P_z[\text{GAME PRG}_{G, B}(\lambda, 1) = 1] \geq \frac{\epsilon}{\text{negl}(\lambda)}$$

So A can't exist. ■

$$\Rightarrow H(\lambda, 0) \approx_c H'(\lambda, 0) \equiv H'(\lambda, 1) \approx_c H(\lambda, 1) \quad \blacksquare$$

(by triangle inequality)