

⑤ Prove that  $f(s) : \{0,1\}^n \rightarrow \{0,1\}^n$  OWP  
 $h(s) : \{0,1\}^n \rightarrow \{0,1\}$  HARD-CORE PREDICATE

PRG  $G(s) = f(s) \| h(s)$  is secure

[2]: P. 269

**THEOREM 7.6** Let  $f$  be a one-way permutation and let  $hc$  be a hard-core predicate of  $f$ . Then,  $G(s) \stackrel{\text{def}}{=} f(s) \| hc(s)$  is a pseudorandom generator with expansion factor  $\ell(n) = n + 1$ .

**Theorem 5.** OWP with a HC bit  $\Rightarrow$  PRG.

*Proof.* Let  $f : \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$  be a OWP, and let  $h : \{0,1\}^\lambda \rightarrow \{0,1\}$  be its HC bit. We claim that  $G : \{0,1\}^\lambda \rightarrow \{0,1\}^{\lambda+1}$  where  $G(x) = (f(x), h(x))$  is a PRG.

Assume that  $G$  is not a PRG. Then, there exists a PPT  $A$  such that

$$|Pr_{x \leftarrow \{0,1\}^\lambda}^{GAME} [1 \leftarrow A(G(x))] - Pr_{y \leftarrow \{0,1\}^{\lambda+s(\lambda)}}^{H \times B'} [1 \leftarrow A(y)]| \geq \varepsilon(\lambda)$$

(A can distinguish between PRG output and a random string of same length)

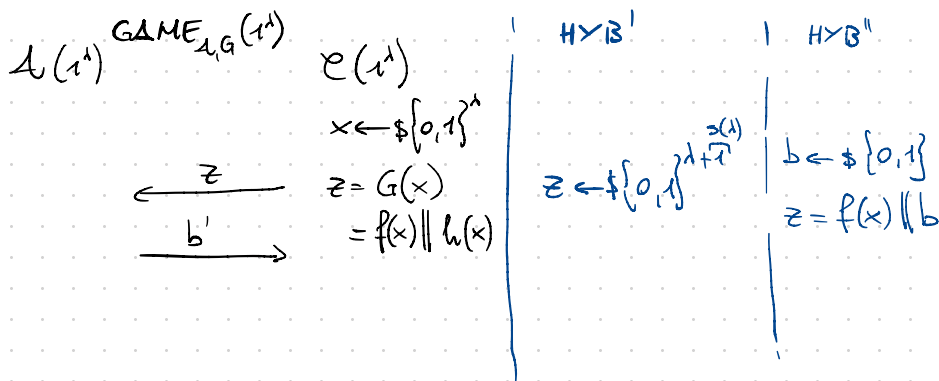
where  $\varepsilon$  is non-negligible. Note that

$$Pr_{y \leftarrow \{0,1\}^{\lambda+s(\lambda)}}^{H \times B''} [1 \leftarrow A(y)] = Pr_{x \leftarrow \{0,1\}^\lambda, b \leftarrow \{0,1\}} [1 \leftarrow A(f(x), b)]$$

$f(x)$  is uniformly distributed when  $x$  is uniform  
 since  $f$  is a permutation, so we have

$$|Pr_{x \leftarrow \{0,1\}^\lambda} [1 \leftarrow A(f(x), h(x))] - Pr_{x \leftarrow \{0,1\}^\lambda, b \leftarrow \{0,1\}} [1 \leftarrow A(f(x), b)]| \geq \varepsilon(\lambda).$$

This directly contradicts the definition of a HC bit. Thus,  $G$  must be a PRG.  $\square$



for  $G(x)$  to be a SECURE PRG we have

$$\{ \text{GAME}_{A,G}^{\text{PRG}}(1^n) \} \approx_c \{ H \times B'(1^n) \}$$

and that

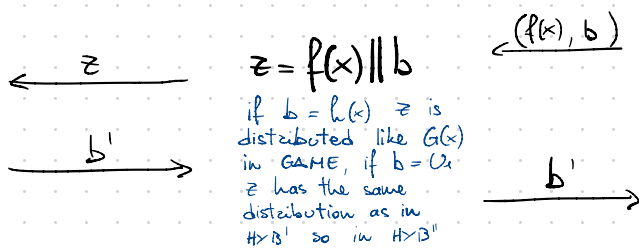
$$\{ H \times B'(1^n) \} = \{ H \times B''(1^n) \} \text{ because } f(x) \text{ OWP}$$

so truly uniformly distributed

By CONTRADICTION we assume  $\exists$  ~~PT~~  $A$  which breaks PRG security (distinguish with  $P_2 > \text{negl}$  between  $\text{GAME}$  and  $H \times B'$  and so between  $\text{GAME}$  and  $H \times B''$ ), then we can build  $A'$  by REDUCTION which breaks HC  $h(x)$

$A$

$A'$



$\mathcal{E}_{\text{HC}}$

$$x \leftarrow \{0,1\}^n$$

$f(x)$  OWP

$$b \leftarrow \begin{cases} h(x) \text{ HC} \\ U_1 \in \{0,1\} \end{cases}$$

$A$  w.p.  $> \text{negl}(n)$  can distinguish between  $z = G(x) = f(x) \parallel h(x)$  and  $z = f(x) \parallel b = U_n$  and with the same  $P_2 > \text{negl}(n)$

$A$  can distinguish between  $(f(x), h(x))$  and  $(f(x), U_1)$

$$\Rightarrow (f(x), h(x)) \not\approx_c (f(x), U_1)$$

$$\Rightarrow h(x) \text{ NOT HC for } f(x)$$

$$\Rightarrow G \text{ must be a PRG}$$