ONE-TIME SKE

We proved: PRG $\Rightarrow$ ONE-TIME SKE.
($|k| \ll |m|$.)

Now: OWF $\Rightarrow$ PRG.

Is there a construction of PRG from ANY OWF?

YES! But it's hard.

OWF

Q: What info $f(x)$ hides about x?

Hard to say.

Indeed: Let $f'(x) = x[1] \| f(x)$

↳ 1st bit of x

Ex: f' still OWF.

DEF We say $h : \{0,1\}^n \to \{0,1\}$ is HARD-CORE for f if OWF:

$$(f(x), h(x)) \approx_c (f(x), b)$$

$b \leftarrow \{0,1\}$; $x \leftarrow \{0,1\}^n$.

If such h would exist: WARM-UP

$$G(s) = f(s) \| h(s)$$

$$G : \{0,1\}^l \to \{0,1\}^{l+1} \quad (l = 1)$$

Is it secure? No! Not sure $f(s)$ ← OWF
UNIFORM vs SUNIFORM. $f(s) = 0 \| f(s)$.

What if f is a PERMUTATION (OWP).

$\Rightarrow$ OWP $\Rightarrow$ PRG !

FACT. OWF $\Rightarrow$ PRG.

Q: Is there h s.t. h HARD-CORE $\forall$ OWF f?

No: For every such h, $f'(x) = \underbrace{h(x)}\,||\,f(x)$ ← OWF

is still OWF, but h NOT HARD-CORE.

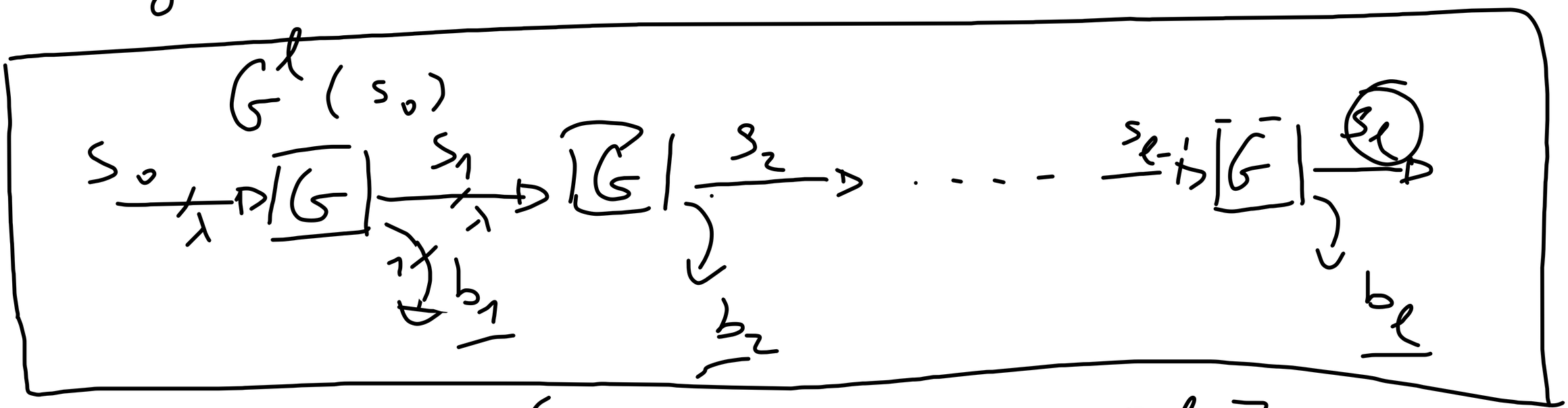
FACT $\forall$ OWF f $\exists$ OWF f', PREDICATE h that is HARD-CORE for f'.

$f: \{0,1\}^n \to \{0,1\}^n$; $f': \{0,1\}^{2n} \to \{0,1\}^{2n}$

$f'(x,r) = (r, f(x))$; $r, x \in \{0,1\}^n$ | $h(x,r) = \langle x, r \rangle \bmod 2$.

$= \sum_{i=1}^{n} x_i r_i \bmod 2$

Seq $G: \{0,1\}^\ell \to \{0,1\}^{\ell+1}$ a PRG.



$G(s_{i-1}) = (s_i, b_i) \quad \forall\, i \in [\ell]$

Output : $(b_1, \ldots, b_\ell, s_\ell)$

THM If G is secure, the above is also secure for every $\ell(\lambda) = \text{poly}(\lambda)$.

Proof. A new technique: HYBRID ARGUMENT.

A general thing: Say I need to prove $X \approx_c Y$.

$$X \equiv H_0 \approx_c H_1 \overset{\not\in}{\approx_c} H_2 \cdots\cdots \approx_c H_{\ell-1} \approx_c H_\ell \equiv Y$$

$A \approx_c B$, $B \approx_c C \Rightarrow A \approx_c C$

For us: $X \equiv H_0 \equiv G^\ell(U_\lambda) \equiv G^\ell(s_0)$ for $s_0 \leftarrow\!\!\!\!\rightarrow \{0,1\}^\lambda$

$Y \equiv U_{\lambda+\ell} \equiv \left(z \leftarrow\!\!\!\!\rightarrow \{0,1\}^{\lambda+\ell}\right)$

H_i : $b_1, \dots, b_i \leftarrow\$ \{0,1\}$

$s_i \leftarrow\$ \{0,1\}^\lambda$

$(b_{i+1}, \dots, b_\ell, s_\ell) = G^{\ell - i}(s_i)$ $\quad i \in [0, \ell]$

$(b_{i+1}, s_{i+1}) = G(s_i)$

$(b_{i+2}, s_{i+2}) = G(s_{i+1})$

$\vdots$

$H_0 \equiv X$; $Y \equiv H_\ell$.

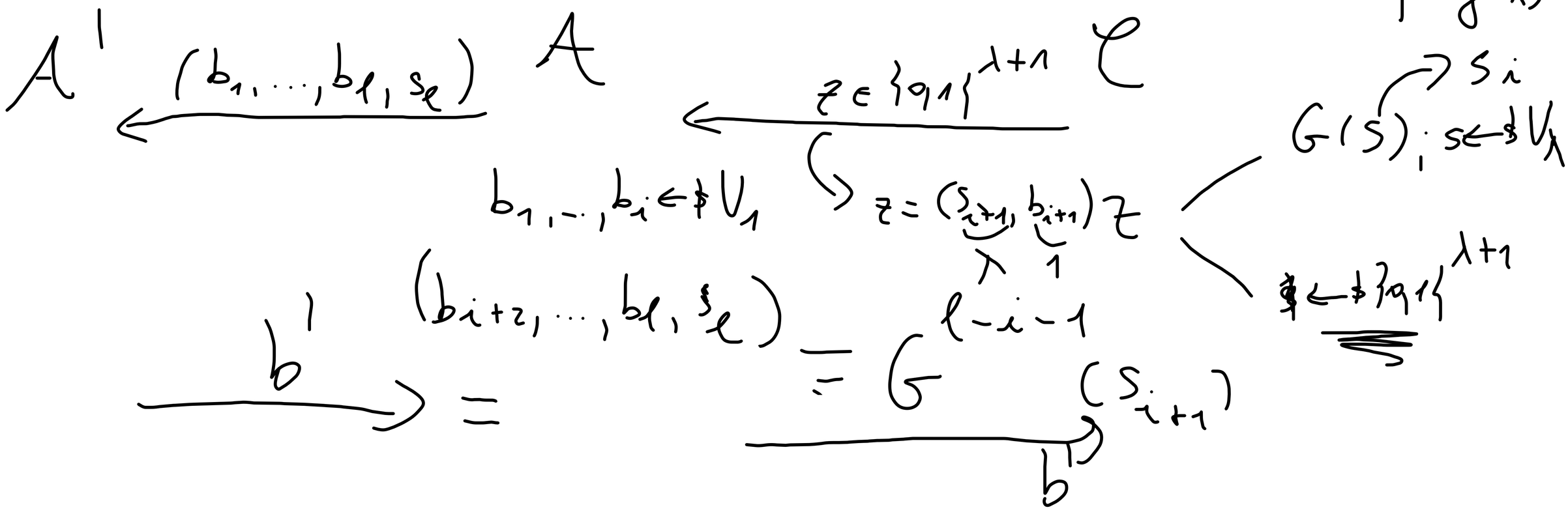
LEMMA $\forall\ i \in [0, \ell-1]$: $H_{i+1} \overset{c}{\sim} H_i$.

Proof. Fix i. Assume not: $\exists$ PPT A' s.t. $\left| \Pr[H_i(\lambda) = 1] - \Pr[H_{i+1}(\lambda) = 1] \right| \geq 1/\text{poly}(\lambda)$.

Or more precisely:

$$\left| \Pr\left[A^1(b_1,\dots,b_\ell, s_\ell) = 1 : (b_1,\dots,b_\ell, s_\ell) \leftarrow\$ H_i(\lambda) \right] \right.$$
$$\left. - \Pr\left[A^1(b_1 \dots b_\ell, s_\ell) = 1 : (b_1,\dots,b_\ell, s_\ell) \leftarrow\$ H_{i+1}(\lambda) \right] \right| \geq 1/\mathrm{poly}(\lambda)$$

Build PPT A against G:



By inspection:

- If $z = G(s)$ for $s \leftarrow\!\$ U_\lambda$, then

  $b_1, \dots, b_\ell, s_\ell$ are dist. acc. to $H_i(\lambda)$

- If $z \leftarrow\!\$ \{0,1\}^{\lambda+1}$, then

  $b_1, \dots, b_\ell, s_\ell$ are dist. acc. to $H_{i+1}(\lambda)$. ▨

$$\Rightarrow \left| \Pr[A(z)=1 : z = G(s); s \leftarrow\!\$ U_\lambda] - \Pr[A(z)=1 : z \leftarrow\!\$ U_{\lambda+1}] \right| \geq 1/\mathrm{poly}(\lambda).$$