RECAP: · PRG $\Rightarrow$ one-time comp. sec. SKE

· OWFs $\Rightarrow$ PRGs

one-way permutation

Let $f: \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a OWP

Then $G(s) = (f(s), h(s))$ where $h: \{0,1\} \to \{0,1\}$ is HARD-CORE for f, is a PRG with stretch $\ell = 1$.

To show this is not secure, we should show that f is not secure, by proving it is not a OWF with a counter-example (f^*) that breaks the definition

EX Show that the above PRG construction is not secure when f is ANY OWF.

Intuition: IF f is a function, then $f(s)$ may not be uniform for random $s \leftarrow\$ \{0,1\}^\lambda$.

Need to show that $\exists f^*$ a OWF for which above G can be broken efficiently.

e.g. let f be a OWF

concatenated

$$f^*(x) = f(x) \| 0$$

1) Show $G(s) = f^*(s) \| h^*(s)$ is not a PRG

2) Show f^* is a OWF.

THM OWFs $\Rightarrow$ PRGs (with $\ell = 1$)

Later: more efficient construction

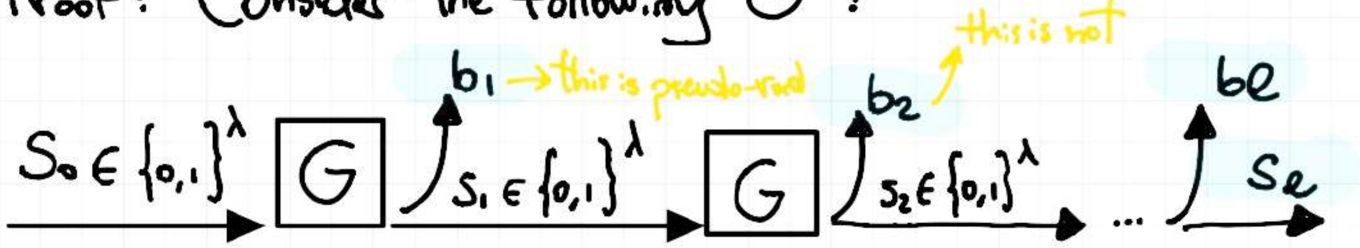
Now: $\ell = 1 \Rightarrow \ell = \text{poly}(\lambda)$

THM Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ be a PRG.

Then, for any $\ell = \text{poly}(\lambda)$ there is a PRG

$$G^\ell : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$$

Proof: Consider the following G^ℓ:



$S_0 \leftarrow \$ \{0,1\}^\lambda$; $\forall i \in [\ell] : G(S_{i-1}) = (s_i, b_i)$

Output: $b_1, b_2, \ldots, b_\ell, s_\ell$

↳ seed, ℓ is any poly

So: $G(s_{i-1}) = z_{i-1} \in \{0,1\}^{\lambda+1}$

$\stackrel{\text{DEF}}{=} s_i \| b_i \rightarrow \in \{0,1\}$

↳ $\in \{0,1\}^\lambda$

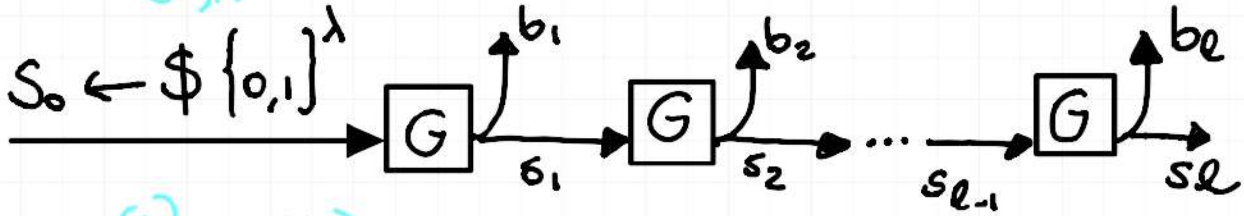
Formal proof requires the HYBRID ARGUMENT

The idea is to take the construction and gradually change it

The two extremes for HYB are G^ℓ and uniform

$\mathrm{REAL}_{G^\ell, A}(\lambda)$

$S_0 \leftarrow \$ \{0,1\}^\lambda$

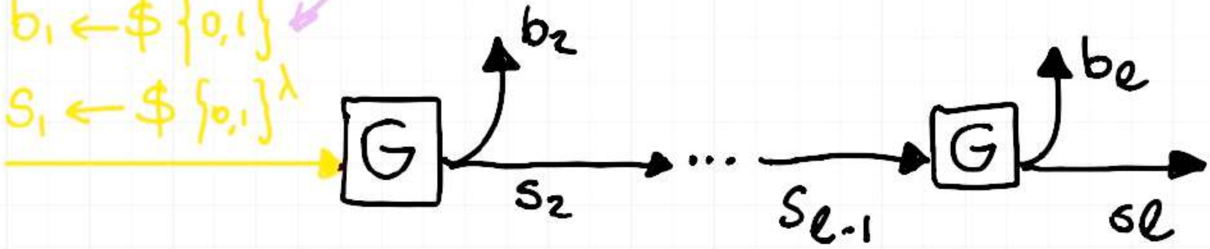


$\mathrm{HYB}^{(1)}_{G^\ell, A}(\lambda)$

these are truly random

$b_1 \leftarrow \$ \{0,1\}$

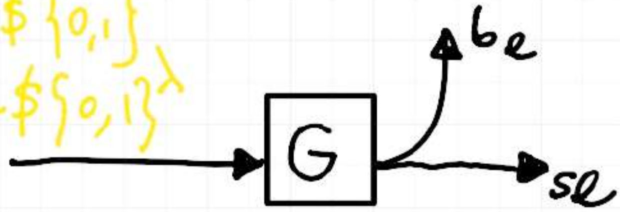
$s_1 \leftarrow \$ \{0,1\}^\lambda$



$\mathrm{HYB}^{(2)}_{G^\ell, A}(\lambda)$

$b_1 \leftarrow \$ \{0,1\}$ $b_2 \leftarrow \$ \{0,1\}$

$s_1 \leftarrow \$ \{0,1\}^\lambda$ $s_2 \leftarrow \$ \{0,1\}^\lambda$



$\mathrm{HYB}^{(\ell)}_{G^\ell, A}(\lambda)$

$b_1 \dots b_\ell \leftarrow \$ \{0,1\}$

$s_\ell \leftarrow \$ \{0,1\}^\lambda \quad \equiv U_{\lambda+\ell}$

We need to show that $\mathrm{HYB}^{(1)} \approx_c \mathrm{HYB}^{(\ell)}$

By the HYBRID argument, it suffices to show

$$\forall i \in [\ell] : \left\{\mathrm{HYB}^{(i)}_{G,A}\right\} \approx_c \left\{\mathrm{HYB}^{(i+1)}_{G,A}\right\}$$

Fix $i \in [\ell]$ and assume not $\exists$ PPT $\mathcal{A}$ such that

$$\left| \Pr\left[\mathrm{HYB}^{(i)}_{G,\mathcal{A}}(\lambda)=1\right] - \Pr\left[\mathrm{HYB}^{(i+1)}_{G,\mathcal{A}}(\lambda)=1\right] \right| \geq 1/poly(\lambda)$$

If this is true, $\exists$ PPT $\mathcal{A}'$ breaking G:

$\mathcal{A}(1^\lambda)$ $\qquad$ $\mathcal{A}'(1^\lambda)$ $\qquad$ $C'(1^\lambda)$

$\xleftarrow{\text{"START"}}$ $\qquad$ $\xleftarrow{z \in \{0,1\}^{\lambda+1}}$ z: $G(s)$, $s \leftarrow \$ \{0,1\}^\lambda$; $z \leftarrow \$ \{0,1\}^{\lambda+1}$

$b_1, \dots b_i \in \{0,1\}$

$z \stackrel{DEF}{=} s_{i+1} \| b_{i+1}$

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

$\xleftarrow{(b_1, \dots, b_\ell, s_\ell)}$

$\xrightarrow{b'}$ $\qquad$ $\xrightarrow{b'}$

Analysis: If $\mathcal{A}$ is PPT so is $\mathcal{A}'$

When $z = s_{i+1} \| b_{i+1}$ is random $\mathcal{A}$ obtains same TRANSCRIPT as $\mathrm{HYB}^{(i+1)}$.

When $z = s_{i+1} = b_{i+1} = G(s)$ for $s \leftarrow \$ \{0,1\}^\lambda$, $\mathcal{A}$ obtains same transcript as in $HYB^{(i)}$.

$$\Pr[\text{REAL}_{G,A'}(\lambda)=1] \overset{DEF}{=}$$

$$= \Pr[A'(1^\lambda, z)=1 : z = G(s); s \leftarrow \$ \{0,1\}^\lambda] =$$

$$= \Pr[\text{HYB}^{(i)}_{A,G}(\lambda)=1]$$

Also: $\Pr[\text{RAND}_{G,A}(\lambda)=1] = \Pr[A'(1^\lambda, z) : z \leftarrow \$ \{0,1\}^{\lambda+1}]$

$$= \Pr[\text{HYB}^{(i+1)}_{G,A}(\lambda)=1]$$

Remember: $\text{Enc}(K,m) = G(K) \oplus m$ is one-time secure with $|K| \ll |m|$

But not two-time secure! In fact, assume A knows a pair $(\bar{m}, \bar{c})$ under key K, and aims at "breaking" target cyphertext $c = G(K) \oplus m$ for unknown $m \in \mathcal{M}$.

$$\bar{c} = G(K) \oplus \bar{m}$$

$$\Rightarrow \bar{c} \oplus c = \bar{m} \oplus m$$

$$\Rightarrow (\bar{m} \oplus m) \oplus \bar{m} = m$$ → it is not two-time secure!

<u>GOAL</u>: Have better (i.e. stronger) definitions!

We want to model an enc that can reuse the same key and still be secure

CPA security: CHOSEN-PLAINTEXT ATTACKS security

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

$A(1^\lambda)$ $\qquad$ $C(1^\lambda)$

poly(λ) $\quad$ $m_i \in \mathcal{M}$ $\longrightarrow$ repeats this a number of times

$\longleftarrow$ c_i

$m_0^*, m_1^* \in \mathcal{M}$ $\longrightarrow$ $\quad k \leftarrow \$ \mathcal{K}$

$c = Enc(k, m_b)$

$\longleftarrow$ c^* $\quad c_i = Enc(k, m_i)$

poly(λ) $\quad$ $m_i \in \mathcal{M}$ $\longrightarrow$

$\longleftarrow$ c_i

$\longrightarrow$ b'

<u>DEF</u>: We say Π is CPA secure if

$\forall$ PPT A, it holds

$$\left\{\text{GAME}^{CPA}_{\Pi,A}(\lambda,0)\right\}_{\lambda\in\mathbb{N}} \approx_c \left\{\text{GAME}^{CPA}_{\Pi,A}(\lambda,1)\right\}_{\lambda\in\mathbb{N}}$$

Remember: this means $\forall$ PPT A $\exists\, \varepsilon(\lambda) = negl(\lambda)$ s.t.

$$\left|\Pr\left[\text{GAME}^{CPA}_{\Pi,A}(\lambda,0)=1\right] - \Pr\left[\text{GAME}^{CPA}_{\Pi,A}(\lambda,1)=1\right]\right| \leq \varepsilon(\lambda)$$

We change the GAME just a tiny bit...

$$\mathrm{GAME}^{\mathrm{CPA}}_{\Pi,\mathcal{A}}(\lambda, b)$$

repeats this a number of times

$\mathcal{A}(1^\lambda)$ $\qquad\qquad$ $\mathcal{C}(1^\lambda)$

poly(λ)

$m_i \in \mathcal{M}$ $\longrightarrow$

$\longleftarrow$ c_i

$\qquad\qquad$ $k \leftarrow\$ \mathcal{K}$

$m_0^*, m_1^* \in \mathcal{M}$ $\longrightarrow$

$\longleftarrow$ c^* $\qquad$ $c^* \leftarrow\$ \mathrm{Enc}(k, m_b)$

$\qquad\qquad$ $c_i \leftarrow\$ \mathrm{Enc}(k, m_i)$

poly(λ)

$m_i \in \mathcal{M}$ $\longrightarrow$

$\longleftarrow$ c_i $\qquad$ $c_i = \mathrm{Enc}(k, m_i, r_i)$

b' $\longrightarrow$ $\qquad$ $r_i \leftarrow\$ \{0,1\}^\lambda$

randomness

<u>OBSERVATION</u>: No DETERMINISTIC SKE Π can be CPA-secure

$\Rightarrow \Pi$ needs to be randomized!

PSEUDORANDOM FUNCTION

Let $\mathcal{F} = \left\{ F_k : \{0,1\}^{n(\lambda)} \to \{0,1\}^{\ell(\lambda)} \right\}_{k \in \mathbb{N}}$ be a family of functions.

Intuition: For randomly chosen $k \in \{0,1\}^\lambda$, then

F_k looks like a random function R

$$R : \{0,1\}^n \to \{0,1\}^\ell$$

x_1 $\quad \underbrace{0.....0}_{n \text{ bits}}$ $\quad y_1 \leftarrow \$ \{0,1\}^\ell$

x_2 $\quad 0.... 1$ $\quad y_2 \leftarrow \$ \{0,1\}^\ell$

$\vdots$

$\quad 1.... 1$ $\quad y_{2^n} \leftarrow \$ \{0,1\}^\ell$

Every combination of $n \to \ell$ bits can be represented by their truth table, so the truth table is chosen at random