Lecture 4.

TODAY

* Pseudorandomness
* Private and Public-Key Encryption

Pseudo randomness

$$X = \{X_k\}_{k \in \mathbb{N}} \approx_c \quad Y = \{Y_k\}_{k \in \mathbb{N}}$$

iff

$\forall$ nu PPT adversaries $\mathcal{D}$,

$$\left| \Pr\left[\mathcal{D}_{x \leftarrow X_k}(x) = 1\right] - \Pr\left[\mathcal{D}_{y \leftarrow Y_k}(y) = 1\right] \right| = \text{negl}(k)$$

PSEUDORANDOM GENERATOR.

$$\boxed{PRG}(s) \longrightarrow s'$$

s: seed

$\hookrightarrow |s'| > |s|$

Intuitively: $PRG(s) \approx_c$ unif string of size s'.

Def. (PRG) A PRG is a function

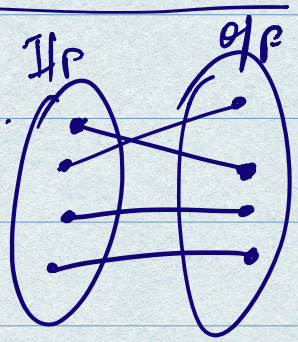
$$G = \{G_k\}_{k \in \mathbb{N}} \qquad G_k : \{0,1\}^k \to \{0,1\}^{m(k)}$$

such that

- $m(k) > k$ (poly(k))
- $G_k(s)_{s \xleftarrow{R} \{0,1\}^k} \approx_c U_{m(k)}$

Build a PRG.

$s \longrightarrow f(s)$



Let's that OWF is * length-preserving (size of output string = size of input string) and * injective.

This is called a one-way permutation.

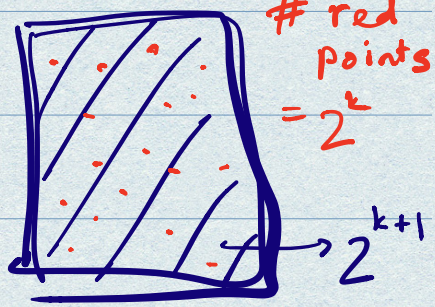
Take owp f; Define $G(s) = f(s)$.

NOT a PRG because it does not expand.

Define $G(s) = f(s) \| hcb(s)$.

Is this a PRG?

Yes.



$$\{G(s)\}_{s \xleftarrow{R} \{0,1\}^k} \neq U_{k+1}$$

Claim:

$$\{G(s)\}_{s \xleftarrow{R} \{0,1\}^k} \approx_c U_{k+1}$$

$\forall$ nu PPT adversary $\mathcal{D}$,

$$\left| \Pr_{s \xleftarrow{R} \{0,1\}^k} [\mathcal{D}(G(s)) = 1] - \Pr[\mathcal{D}(U_{k+1}) = 1] \right| < \text{negl}(k)$$

ASIDE → A hard-core predicate for all OWF's.

Every OWF admits a hard core bit

(Goldreich-Levin '89 thm; see proof in Ostrovsky Lecture Notes)

$$G(s) = f(s) \,||\, \underline{hcb(s)}$$

$$\approx_c f(s) \,||\, (\neg hcb(s))$$ H.W

By Def. of hcb,

$$\Pr_{s \xleftarrow{R} \{0,1\}^k}\left[A(f(s)) = hcb(s) \right] = \frac{1}{2} + negl(k)$$

H.W.

$$G(s) \approx_c \{ f(s) \,||\, \underline{uniform} \}_{s \xleftarrow{R} \{0,1\}^k}$$

$$= \{ uniform \,||\, uniform \}_{s \xleftarrow{R} \{0,1\}^k}$$

[Because $f(s)$ is a OWP]

Q: Build

$$G' = \{ G'_k : \{0,1\}^k \longrightarrow \{0,1\}^{k+2} \}_{k \in \mathbb{N}}$$

given $G = \{ G_k : \{0,1\}^k \longrightarrow \{0,1\}^{k+1} \}_{k \in \mathbb{N}}$

Ans: $G'_k(s) = G_{k+1}(G_k(s)) \approx_c G_{k+1}(U_{k+1}) \approx_c U_{k+2}$

$$G(s) = f(f(s)) \,||\, hcb(s) \,||\, hcb(f(s))_{s \leftarrow \{0,1\}^k}$$

$$\approx_c f(f(s)) \,||\, u_1 \,||\, hcb(f(s))_{s \leftarrow \{0,1\}^k}$$

$$= f(s') \,||\, u_1 \,||\, hcb(s')_{s' \leftarrow \{0,1\}^k}$$

$$\approx_c f(s') \,||\, u_1 \,||\, \bar{u}_1$$

$$= s'' \,||\, u_1 \,||\, \bar{u}_1$$

PSEUDORANDOM FUNCTION

A function family is a map.

F : Keys $\times$ Domain $\to$ Range.

$= \{0,1\}$

$\text{All}^{\text{Dom} \to \text{Range}}$: { Set of all functions that map elements in Dom to elements in Range }.

Exp^1

$g \xleftarrow{\$} \text{All}^{\text{Dom} \to \text{Range}}$

$b \leftarrow A^{g}$

Return b.

Exp^2

$K \leftarrow \text{Keys}(F)$

$b \leftarrow A^{F_K}$

Return b.

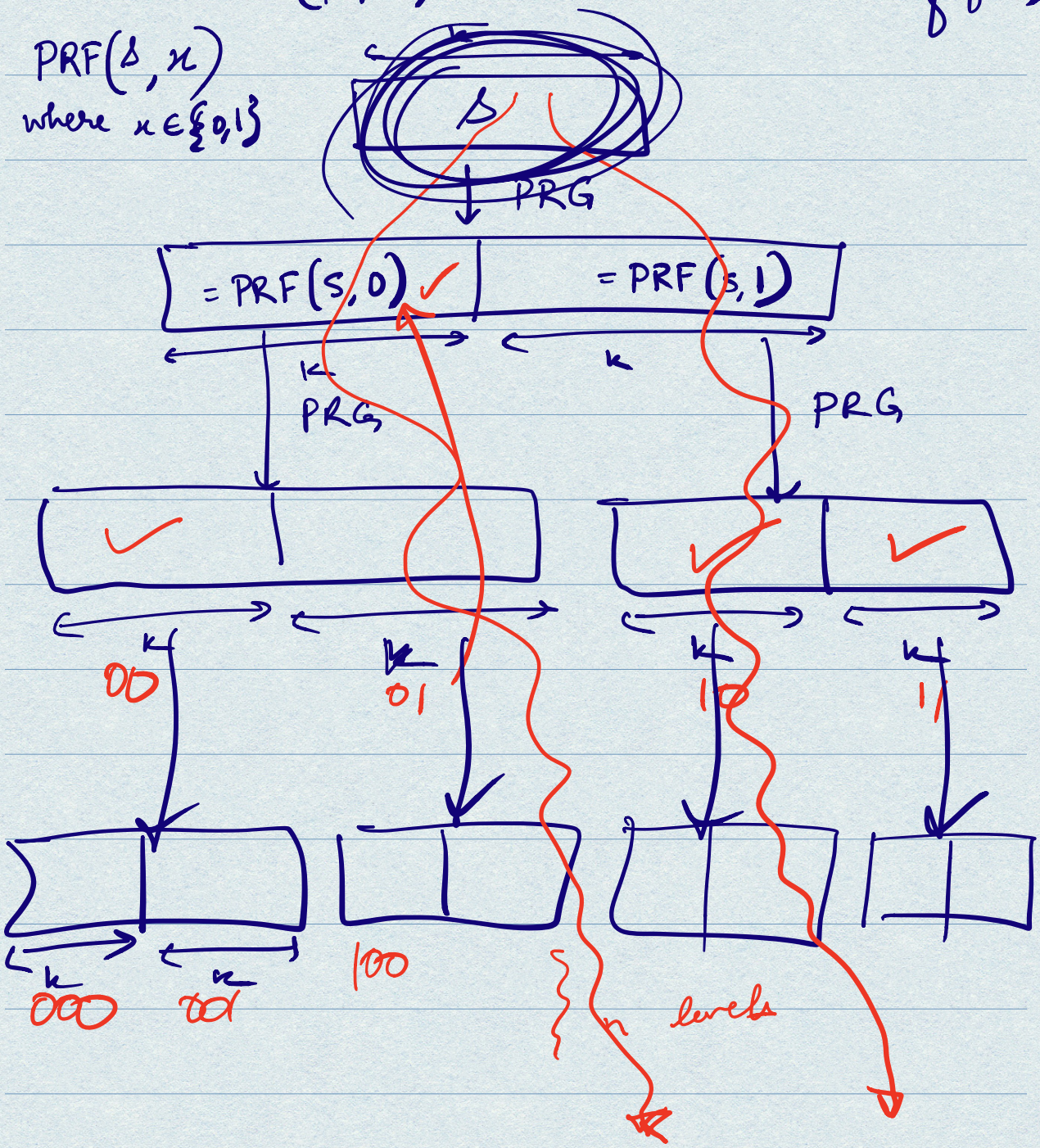
F_K : should have an efficient description

$G: \{0,1\}^k \rightarrow \{0,1\}^{2k}$

$PRF(s, 0)$:= Output the first half of $G(k)$

$PRF(s, 1)$:= " second half of $G(k)$

$PRF(s, x)$ where $x \in \{0,1\}^*$



ENCRYPTION SCHEMES

$(KeyGen, Enc, Dec)$

$KeyGen(1^k; r_g) \rightarrow (ek, dk)$

$Enc(ek, m; r_{enc}) \rightarrow c$

$Dec(dk, c) \rightarrow m$

CORRECTNESS

$$\Pr_{(ek, dk) \xleftarrow{R} KeyGen(1^k)}[Dec(dk, Enc(ek, m)) = m]$$

$= 1$ [perfect correction]

or $\geq 1 - negl(k)$ [statistical correctness]

SECURITY.

EXTRA: INSIGHTS ON HARD CORE BITS.

Given $f : \{0,1\}^k \to \{0,1\}^k$

Define $g : \{0,1\}^{2k} \to \{0,1\}^{2k}$ as:

$$g(x) = f(x_1) \,||\, x_2$$

where $x = \underbrace{x_1}_{k} \,||\, \underbrace{x_2}_{k}$

1. g is a OWF.
2. $HCB(x) = \langle x_1, x_2 \rangle \bmod 2$.

$\forall$ nu PPT $\mathcal{A}$

$$\boxed{GL}\ \Pr[\mathcal{A}(g(x)) = HCB(x)] \leq \frac{1}{2} + \text{negl}(k)$$

$\mathcal{A}(g(x))$ outputs $\langle x_1, x_2 \rangle \bmod 2$ -

- $100\ldots0$ $x_1[1]$
- $010\ldots0$ $x_1[2]$
- ⋮