Special Topics in Cryptography

Mohammad Mahmoody

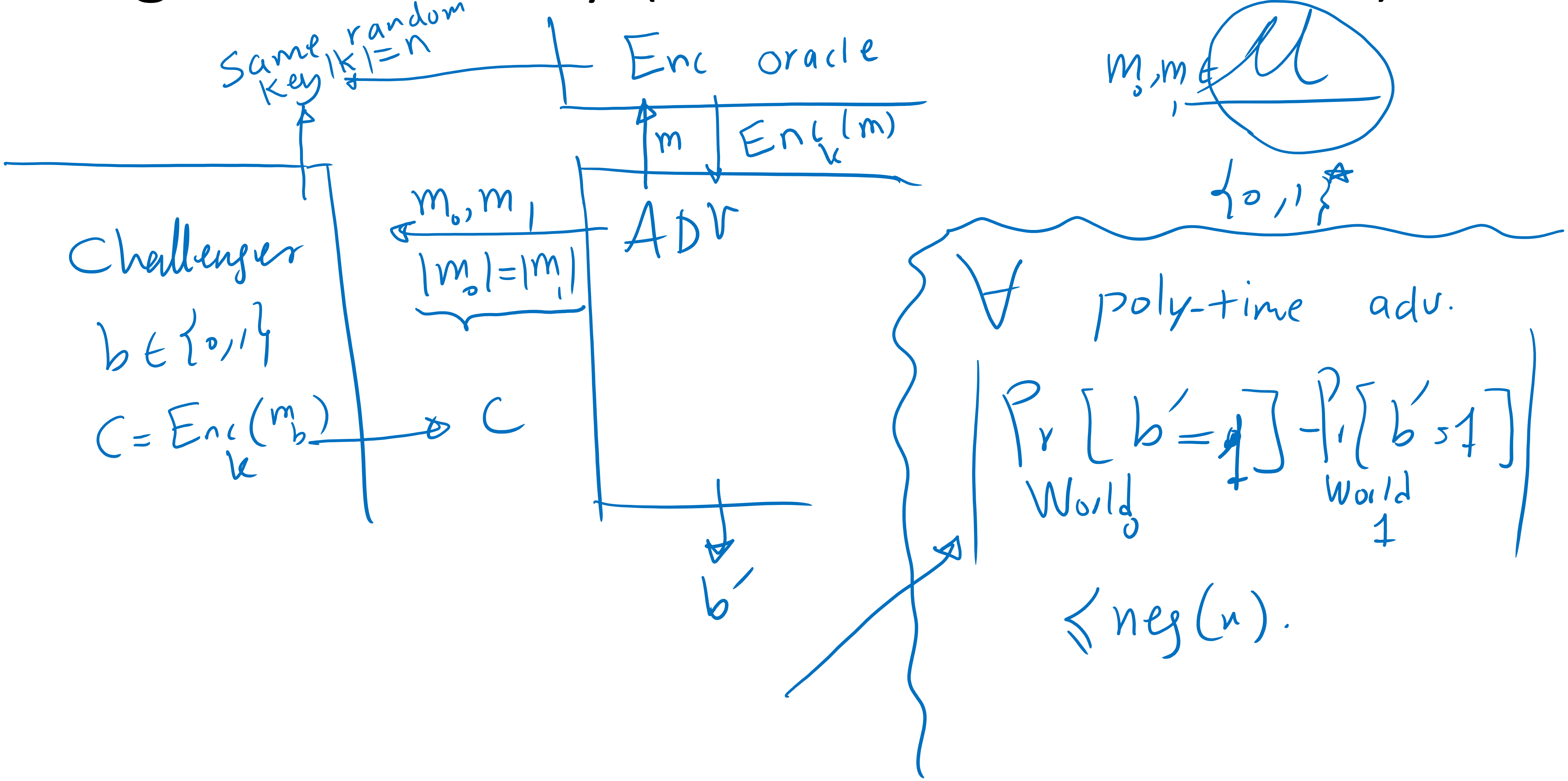
Last time

- How to make PRGs stretch more
- How to use Cryptographic Hash Functions to get PRGs
- Chosen plain-text security

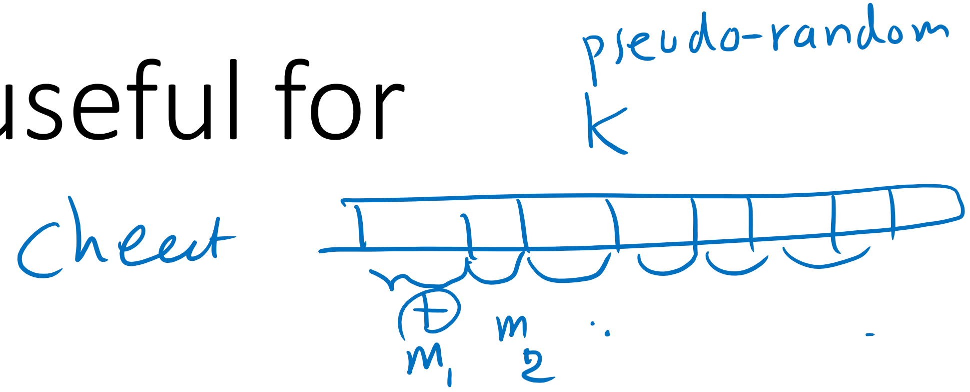
Today

- Pseudorandom Functions
- PRFs → CPA secure encryption
- Starting Authentication

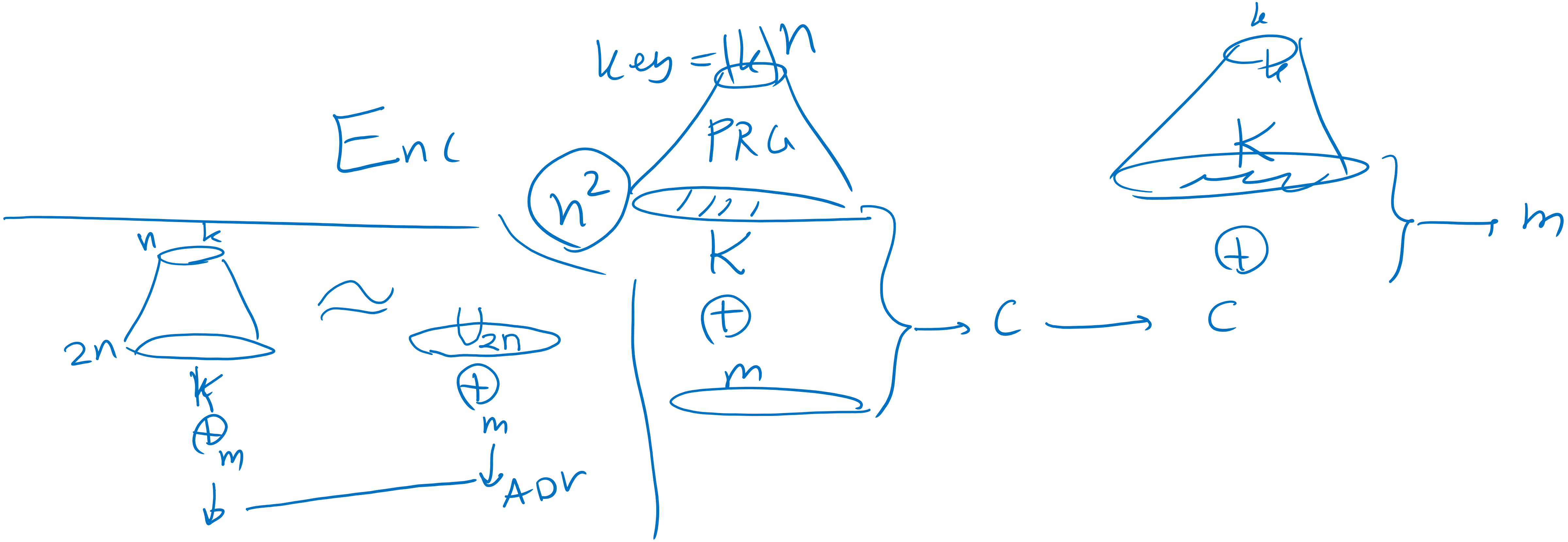
Recalling CPA Security (and Randomized Enc)



Recalling how PRGs were useful for single-message security



Relying on OTP's idea.



A useful lemma for indistinguishability

Lemma 1

$\forall$: Starting point $X_n \underset{c}{\approx} Y_n$: $\forall$ poly-time adv. A $\exists$ neg ε.

computationally ind.

$$\left| \Pr_{x \leftarrow X_n}[A(x)=1] - \Pr_{y \leftarrow Y_n}[A(y)=1] \right| \le neg(n).$$

Conclusion: for all $\boxed{\text{poly-time}}$ Z (potentially randomized)

then $\underbrace{[Z(X_n)]}_{X_n'} \underset{c}{\approx} \underbrace{[Z(Y_n)]}_{Y_n'}$

if B breaks $X_n' \approx Y_n'$

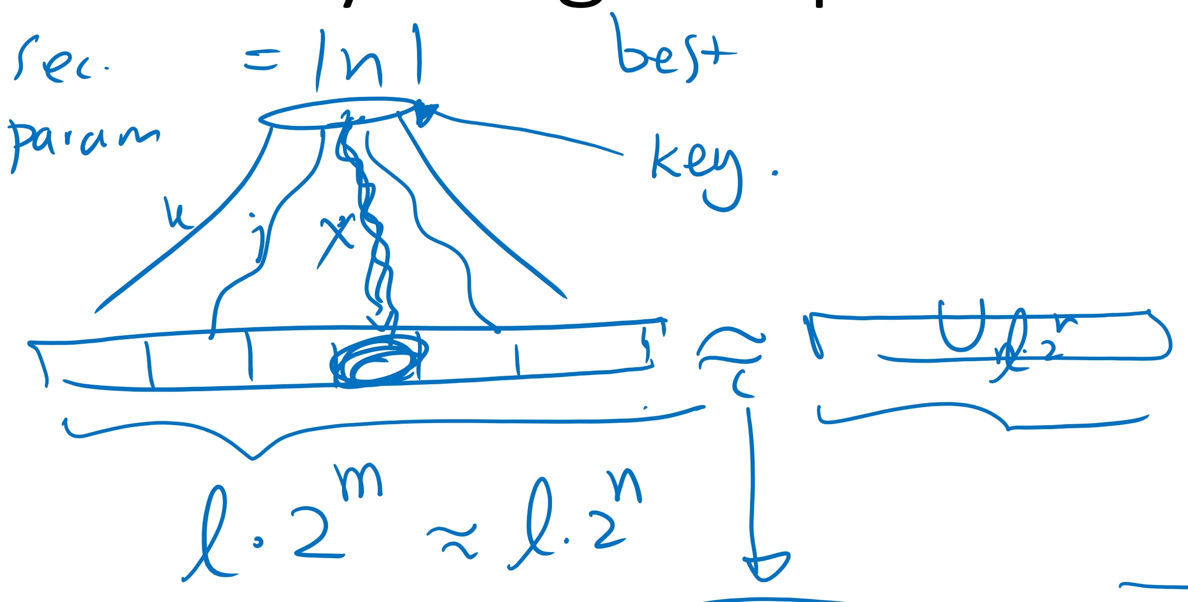
Y_n, X_n : randomized inputs.

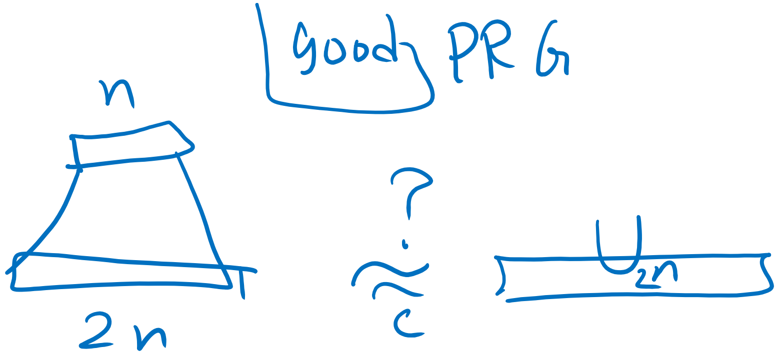
X_n', Y_n' : outputs.

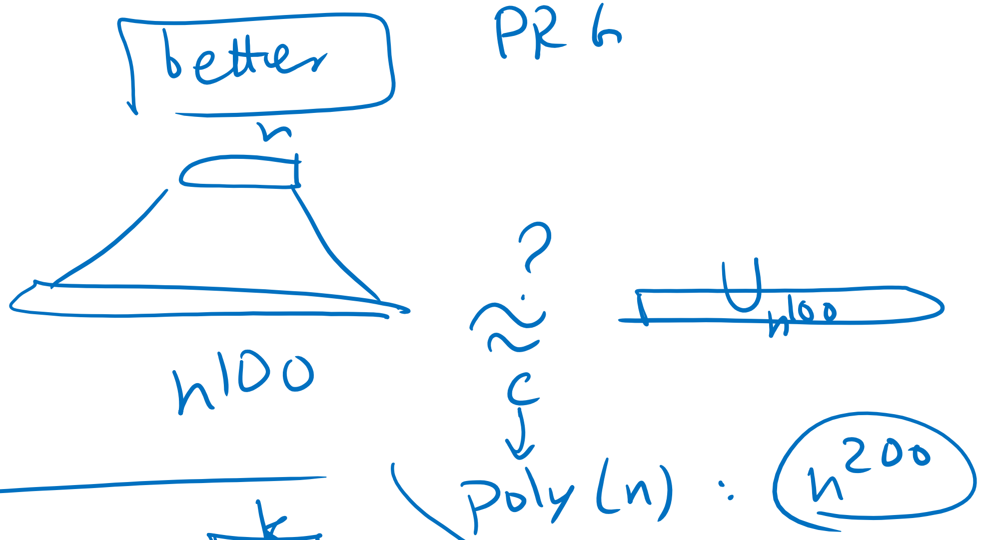
$$\boxed{X_n' \underset{c}{\approx} Y_n'}$$

: outputs are also indistinguishable

Pseudo Random Functions: A very long-output PRG



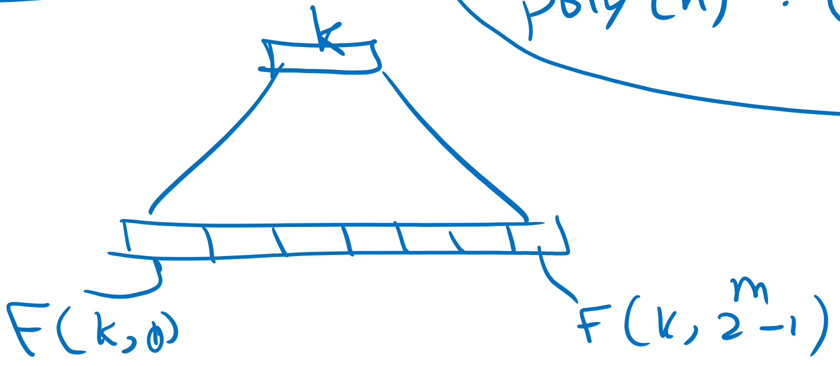




$F(k, x) \to \{0,1\}^{\ell}$ → output length

k: n-bit

x: m-bit



Pseudo-Random Functions (other definition)

3rd :

$F(k, x) \to \{0,1\}^\ell$

k: n-bits.

$x \in \{0,1\}^*$

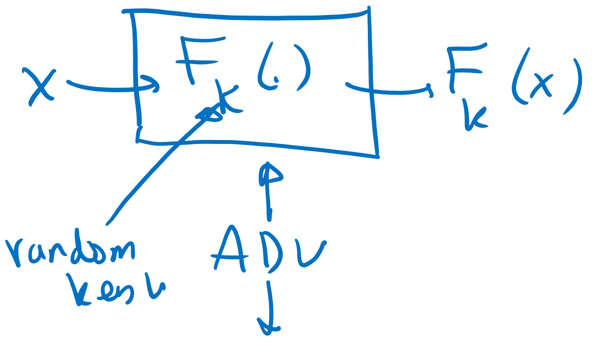
DEFINITION 3.25 *Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. F is a* pseudorandom function *if for all probabilistic polynomial-time distinguishers D, there is a negligible function* negl *such that:*

$$\left| \Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \right| \leq \mathsf{negl}(n),$$

where the first probability is taken over uniform choice of $k \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \mathsf{Func}_n$ and the randomness of D.

Our Version (1)

$F(k, x) \to y$, with k: n, x: m, y: ℓ-bits



F is PRF if for all poly-Time A ...

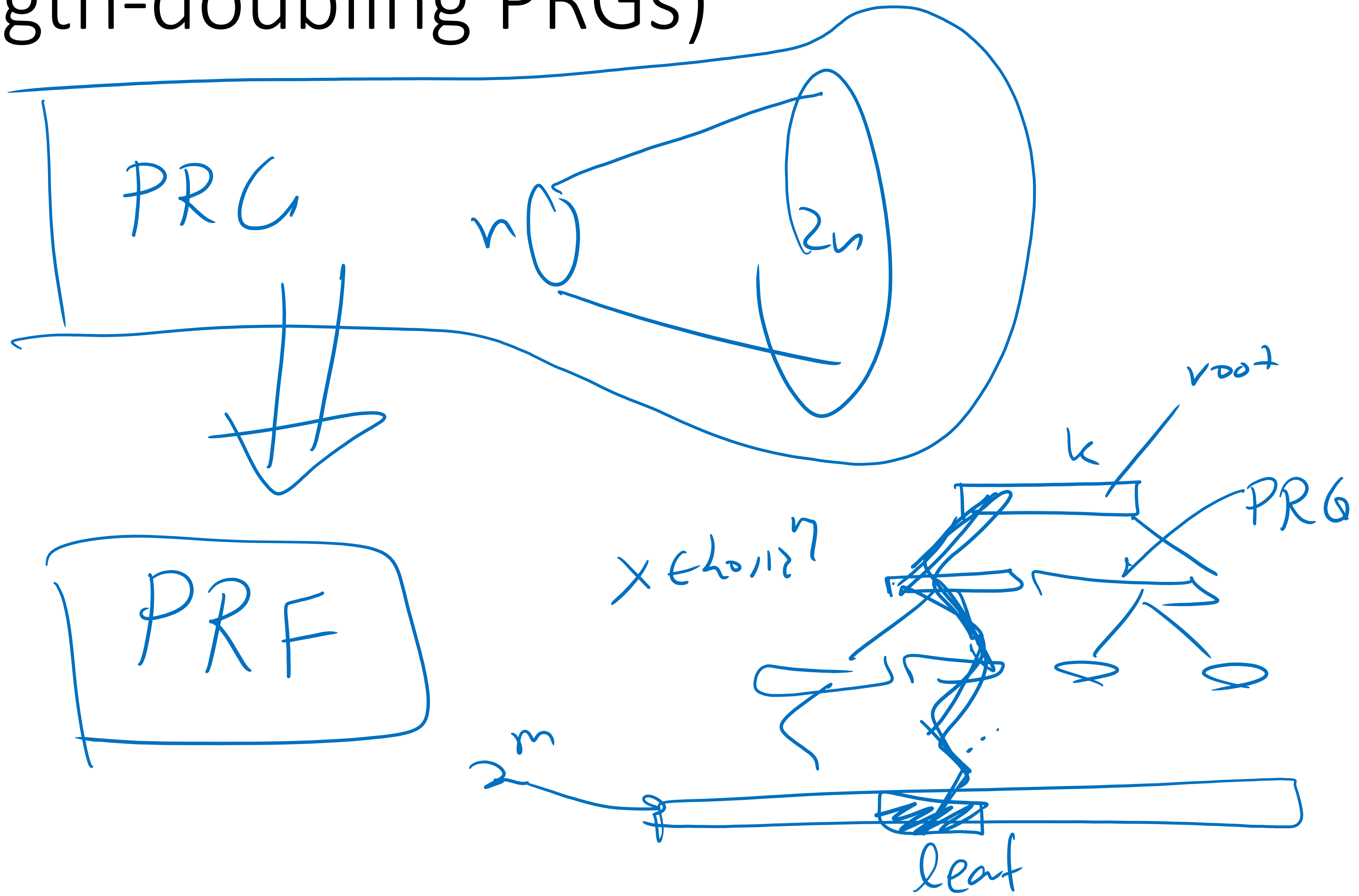
//

F is poly(n) time computable

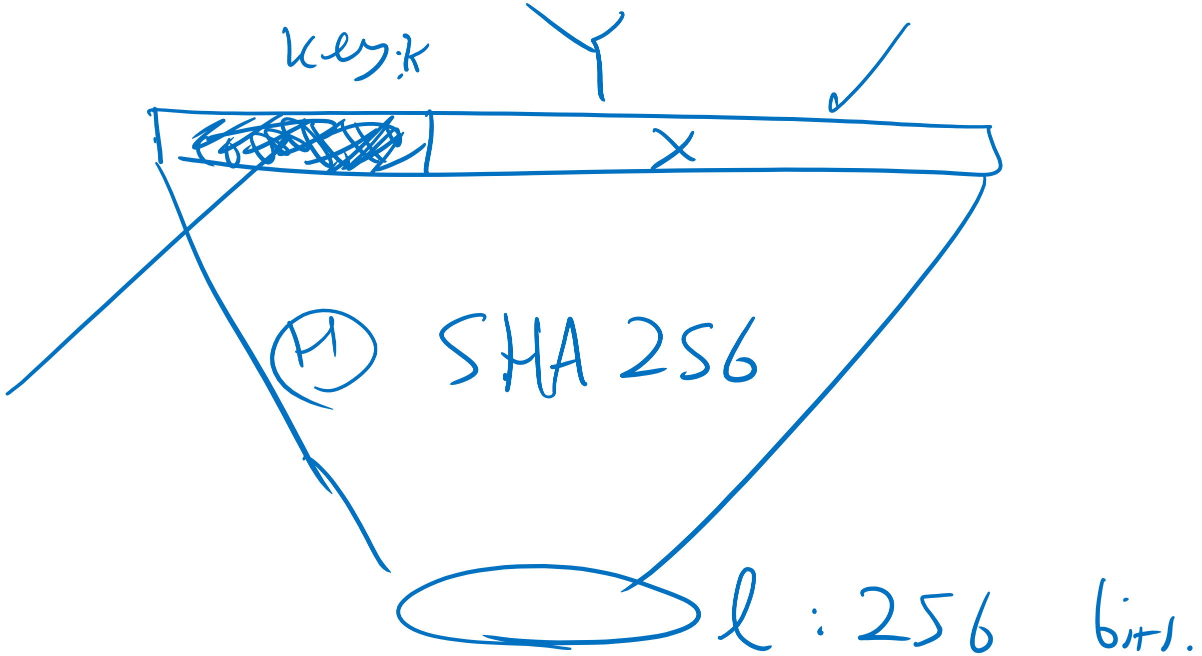
$$\left| \Pr\left[A^{F_k(\cdot)}(n) = 1\right] - \Pr\left[A^{Rand(\cdot)}(n) = 1\right] \right| < neg(n) := \varepsilon(n)$$

$\ell(\cancel{n})$, $m(\cancel{n})$

How to Obtain Pseudorandom Functions?
(1: using length-doubling PRGs)



How to Obtain Pseudorandom Functions? (2: again using hash functions)



$F(k, x) \in \{0,1\}^{\ell}$ $\in 256$

$k \in \{0,1\}^{n}$ ← given n 100

Without the key SHA256 is NOT a PRF.

How to use PRFs to encrypt CPA securely?

W.l.o.g: enough to only encrypt $\mathcal{M} = \{0,1\}^{\ell}$

Claim: $Enc(k, x)$:

if Enc is CPA-secure for a fixed block $\longrightarrow$ it is CPA secure for $\{0,1\}^*$ if we do it this way.

$X = (\underbrace{x_1}_{\ell\text{-bit}}, x_2, \ldots, \underbrace{x_k}_{\ell\text{-bit}})$

$y_i \leftarrow$ fresh $Enc(k, x_i)$

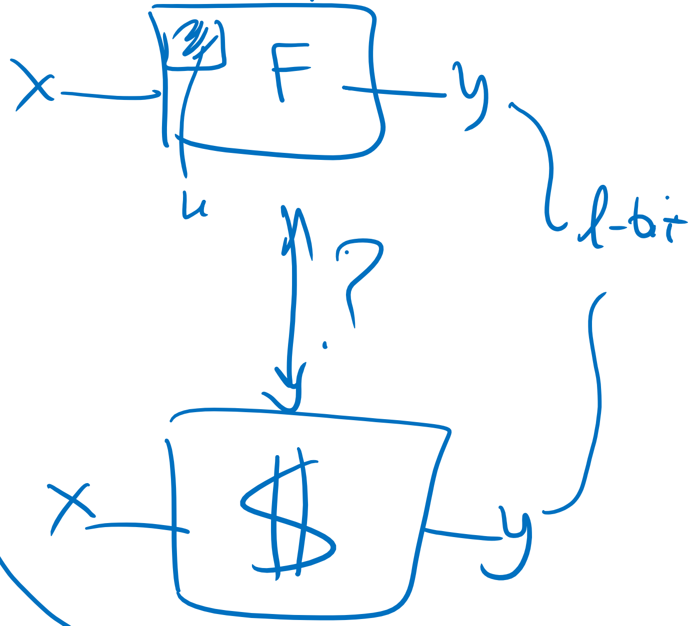
~~Out~~ put $(y_1 — y_k) = y$

needs a proof: (Book proves it!)

We have $F(k, x) \Rightarrow y \leftarrow$ ℓ-bit.

k: n-bit
x: arbitrary length

F: is PRF:



Goal: $\text{Enc}(k, m; r) \rightarrow c$

k: n bit
r: ℓ-bit

$\text{Dec}(k, c) \longrightarrow m$

---

① $\text{Enc}(k, m) = F(k, m)$? Dec?

② $\text{Enc}(k, m) = F(k, m) \oplus m$

③ $\text{Enc}(k, m) = F(k, 1234) \oplus m$, $\text{Dec}(k, c) = F(k, 1234) \oplus c$

How to use PRFs to encrypt?

Recall: it has to be a randomized encryption!

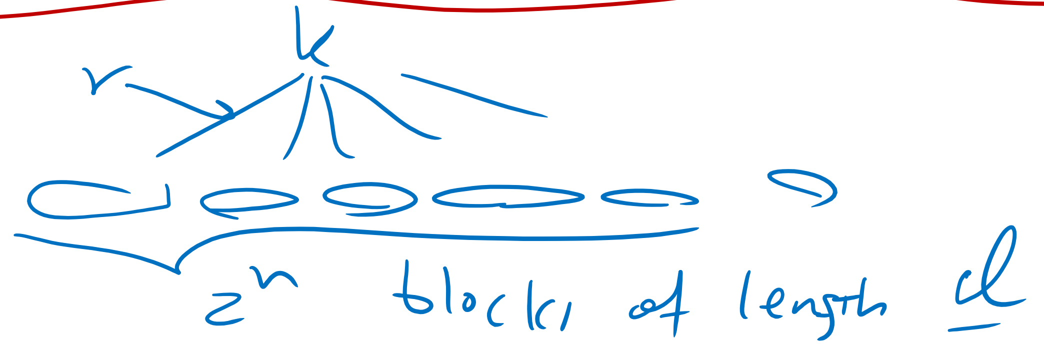
Pick it at length n

4th: $\mathrm{Enc}(k, m, r) = \underbrace{[F(k,r) \oplus m, r]}_{c}$

~~$\mathrm{Dec}(k, c) = F(k,r) \oplus c = m$~~

$\mathrm{Dec}(k, c) :=$ $c = [\alpha, r]$

$F(k,r) \oplus \alpha = m$



Pseudo-Random Functions → CPA Secure Encryption

- PRF $F_k(x)$: For a randomly chosen k no poly-time distinguisher A can distinguish if it is "talking to" $F_k(\cdot)$ or a truly random function $R(\cdot)$

- Construction of CPA secure encryption using PRF $F_k(\cdot)$:
  1. Generate random key k and use it as the key to the PRF
  2. To encrypt message m of length ℓ_{output} take $c = [r, m \oplus F_k(r)]$ for random r
  3. To decrypt $c = [r, y]$ take $m = y \oplus F_k(r)$

$R(\cdot)$ random function

$Enc(k,m) = (r, F_k(r) \oplus m)$

Proof of Security:

Real 0

$Enc^F(k,\cdot)$

m

m_0, m_1

Chal

ADV

$Enc^F(m_0)$

b

Ideal 0: Substite F with R

$Enc_k(m) = (r, R(r) \oplus m)$

m

m_0, m_1

ADV

$\widetilde{Enc}(m_0) = (r, r' \oplus m)$

Ideal 1: Substite F wit $R(\cdot)$

ADV

Real 1

like Real 0

$Enc(m_1)$

b

$P_0 = Pr[b=1]$

q_0

q_1

$Pr[b=1] \stackrel{?}{=} P_1$

PRF property of F

r is large.

if all r's are different → same experiment!

if $|P_0 - q_0| \geq \varepsilon$ → we can make this into an attack against security of PRF!