

PRP-PRF Switching Lemma

Thm Perms ($\{0,1\}^n$) and Funcs ($\{0,1\}^n \rightarrow \{0,1\}^n$) are $(\infty, q, \frac{q^2}{2^{n+1}})$ indistinguishable

Proof: Consider programs P and R. Only can distinguish P and R if "bad = true", which only occurs if R outputs a collision.

$$\text{Adv } A \leq \Pr[\text{bad} = \text{true}] = \Pr[\text{collision}] \leq \frac{q^2}{2^{n+1}}$$

	R: query	output	$\Pr[c]$
$\Pr[y_1 \text{ collides}] = \frac{2}{2^n} \Pr[y_1, y_2 \text{ don't collide}]$	x_1	y_1	$\frac{1}{2^n}$
$= \frac{1}{2^n} \Pr[y_1, y_2 \text{ do collide}]$	x_2	y_2	$\frac{1}{2^n}$
$\leq \frac{2}{2^n}$	\vdots	\vdots	\vdots
	x_q	y_q	$\frac{1}{2^n}$

$$\Pr[\text{collision}] \leq 0 + \frac{1}{2^n} + \frac{2}{2^n} + \frac{3}{2^n} + \dots + \frac{q-1}{2^n}$$

$$\leq \frac{q(q-1)}{2 \cdot 2^n} \leq \frac{q^2}{2^{n+1}}$$

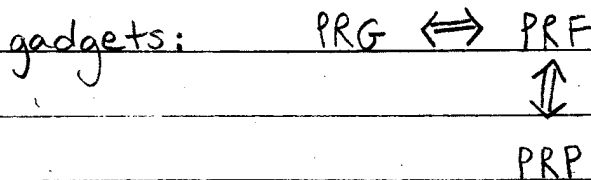
PRF

PRP

$F \sim \text{Funcs} \sim \text{Perms} \sim P$

Is a PRP a PRF? Yes, by transitivity

Is a PRF a PRP? No, but it does meet requirements



Block Cipher Design and Analysis

- Most block ciphers have

- some linear stuff
- some non-linear stuff

AES $L \cdot (x \oplus k_1, \dots, x_{16} \oplus k_{16})$

linear: $L, \oplus k_i$

non-linear: $y \rightarrow \frac{1}{y}$

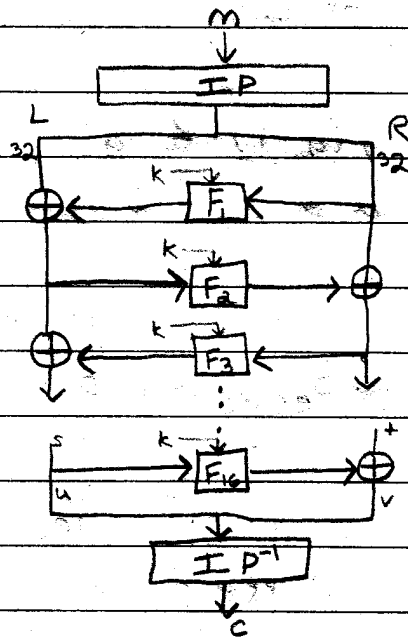
DES

key = $\{0, 1\}^{56}$

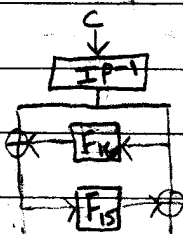
IP = initial permutation (shuffle bits)

$M = C = \{0, 1\}^{64}$

structure:
Feistel
Network



To decrypt,



Def. P is a PRP if

$$\text{Adv. } A = |P_r [A^{P_k} = 1] - P_r [A^{\pi} = 1]| \leq \epsilon$$

CPA \rightarrow chosen plaintext attack

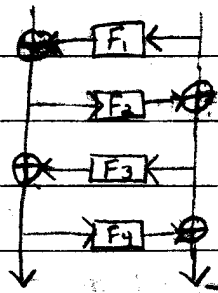
CCA \rightarrow chosen ciphertext attack

$$\text{Adv. } A = |P_r [A^{P_k, P_k^{-1}} = 1] - P_r [A^{\pi, \pi^{-1}} = 1]| \leq \epsilon$$

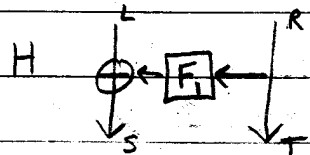
CCA secure \Rightarrow CPA secure

Thm. (PRF \Rightarrow PRP) If F is a (t, q, ϵ) PRF, then H :

$$F_k : \{0, 1\}^n \rightarrow \{0, 1\}^n$$



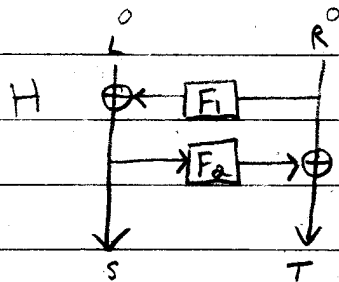
is a $(t - O(q), q, \frac{\epsilon}{2^{m-1}} + 4\epsilon)$ CCA PRP



Attack: pick L, R randomly:

$$(S, T) = \mathcal{O}(L, R)$$

return $T = R$

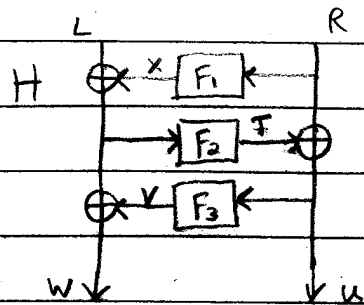


Attack: pick L, R randomly:

$$(S, T) = \mathcal{O}(L, R)$$

pick $L' \neq L$: $(S', T') = \mathcal{O}(L', R)$

return $(L', R) = (L' \oplus S)$



Attack: pick L, R randomly

$$(W, U) = \sigma(L, R)$$

pick $W' \neq W$

$$(L', R') = \sigma^{-1}(W', U)$$

$$(W'', U'') = \sigma(L' \oplus W \oplus W', R')$$

$$\text{return } (R' \oplus U'') = (R \oplus U)$$

$$T = R \oplus U$$

$$X \oplus V = L \oplus W$$

$$S = L \oplus X$$

$$= W \oplus V$$

$$S' = W' \oplus V'$$

$$= W' \oplus V$$

$$= W' \oplus W \oplus W \oplus V$$

$$= W' \oplus W \oplus S$$

$$S'' = L' \oplus W \oplus W' \oplus X'$$

$$= L' \oplus S' \oplus S \oplus W \oplus W' \oplus X'$$

$$= L' \oplus S \oplus S' \oplus X'$$

$$= L' \oplus S \oplus L' \oplus X' \oplus X'$$

$$= S \Rightarrow T'' = T$$