Last Lecture

Security Definition

① Security against the presence of eav

$\wedge$

② Security .... eav for multiple messages

$\wedge$

③ Chosen-plaintext attack (CPA) security

$\parallel$

④ CPA for multiple messages

② $\Rightarrow$ Enc is either stateful
or randomized

This Lecture

Construct CPA-secure encryption

New primitives:

PRF
PRP

New Primitive: Pseudorandom Function (PRF)

PRF $f: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$ $\quad f_{key}: \{0,1\}^n \to \{0,1\}^n$

$n = n(\lambda)$ $\quad m = m(\lambda)$

is a keyed function $f(key, x)$ $\quad f_{key}(x)$

- poly-time computable
- "If key is uniformly sampled the f_{key} looks like a random function under oracle access"

$$\forall \text{p.p.t. } D \quad \Pr_{key}\left[D^{f_{key}(\cdot)}(1^\lambda) \to 1\right] - \Pr_{F:\{0,1\}^n \to \{0,1\}^n}\left[D^{F(\cdot)}(1^\lambda) \to 1\right] \le negl(\lambda)$$

New Primitive : Pseudorandom Permutation (PRP

PRP $f : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ $\qquad f_{key} : \{0,1\}^n \to \{0,1\}^n$

$n = n(\lambda)$

is a keyed ~~function~~ permutation $f(key, x)$ $\quad f_{key}$ is a permutation

- poly-time computable, $f^{-1}(key, x)$ is poly-time computable
- Security

$\forall$ p.p.t. D
$$\left| \Pr_{key}\left[D^{f_{key}(\cdot)}(1^\lambda) \to 1 \right] - \Pr_{\substack{F : \{0,1\}^n \to \{0,1\}^n \\ \text{permutation}}}\left[D^{F(\cdot)}(1^\lambda) \to 1 \right] \right| \leq negl(\lambda)$$

New Primitive: Strong PRP

PRP ≈ block cipher

PRP $f: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ $\qquad f_{key}: \{0,1\}^n \to \{0,1\}^n$

$n = n(\lambda)$

is a keyed ~~function~~ permutation $f(key, x)$ $\qquad f_{key}$ is a permutation

- poly-time computable, $f^{-1}(key, x)$ is poly-time computable
- Security

$\forall$ p.p.t. D

$$\Pr_{key}\left[D^{f_{key}(\cdot),\, f^{-1}_{key}(\cdot)}(1^\lambda) \to 1\right] - \Pr_{\substack{F:\{0,1\}^n \to \{0,1\}^n \\ \text{permutation}}}\left[D^{F(\cdot),\, F^{-1}(\cdot)}(1^\lambda) \to 1\right] \le negl(\lambda)$$

Encryption Scheme for $n(\lambda)$-bit messages

$\Pi = (Gen, Enc, Dec)$

$Gen(1^\lambda)$: sample $k \leftarrow \{0,1\}^\lambda$

$Enc(k, m)$: sample $r \leftarrow \{0,1\}^n$

output $ct = (r, f(k,r) \oplus m)$

$Dec(k, ct=(r,c))$: output $f(k,r) \oplus c$

$PrivK^{CPA}_{\Pi,A} \leq \frac{1}{2} + negl(n)$

(assume $n(\lambda) \geq \lambda$)

$\Pi' = (Gen', Enc', Dec')$

$Gen'(1^\lambda)$: sample $F: \{0,1\}^n \to \{0,1\}^n$

$Enc'(F, m)$: sample $r \leftarrow \{0,1\}^n$

output $ct = (r, F(r) \oplus m)$

$Dec'(F, ct=(r,c))$

output $F(r) \oplus c$

$\forall$ p.p.t A

$$PrivK^{CPA}_{\Pi',A}(\lambda) \leq \frac{1}{2} + \frac{poly(\lambda)}{2^\lambda}$$

$$\text{Distinguisher}^{H(\cdot)} \quad \begin{cases} f_k(\cdot) \text{ for random } k \xleftarrow{\$} \{0,1\}^\lambda \\ F : \{0,1\}^n \to \{0,1\}^n \end{cases}$$

Emulate $\mathrm{PrivK}^{CPA}_{A,\pi}$ or $\mathrm{PrivK}^{CPA}_{A,\pi'}$

A

challenger

no Gen

$Enc(m) = (r, H(r) \oplus m)$

$Dec(r, c) = H(r) \oplus c$

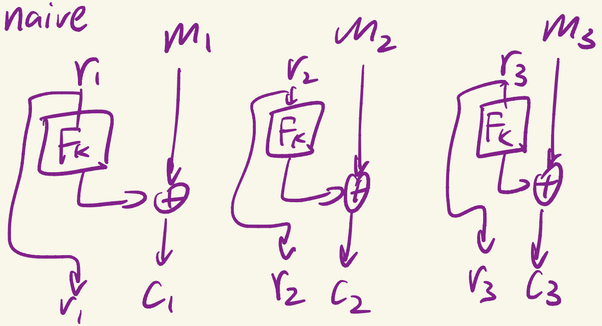
Distinguisher output 1 iff A wins Game

Modes of Block Cipher

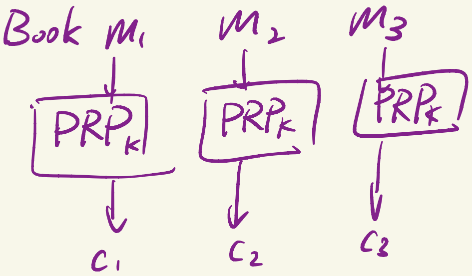
assume PRF & PRP
$f: \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$

Encryption Scheme for longer msgs

1) naive

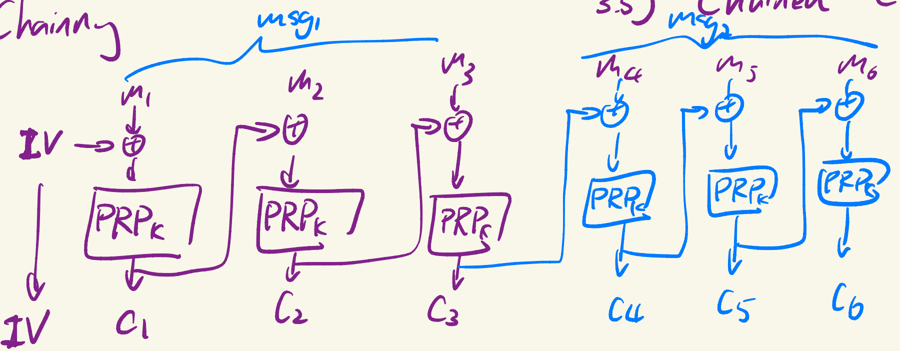


2) Electronic Code Book (ECB)



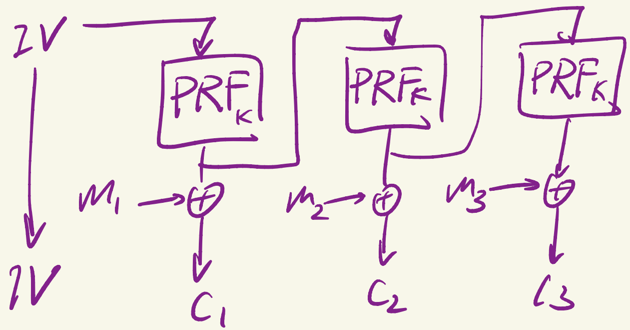
3) Cipher Block Chaining (CBC)

3.5) Chained CBC (stateful)

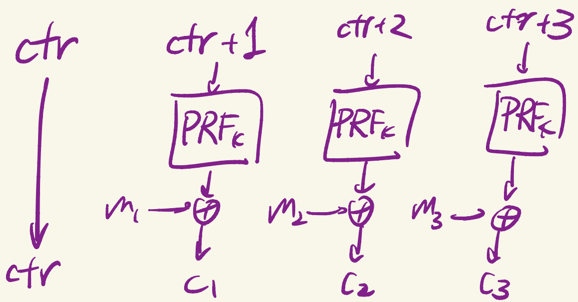


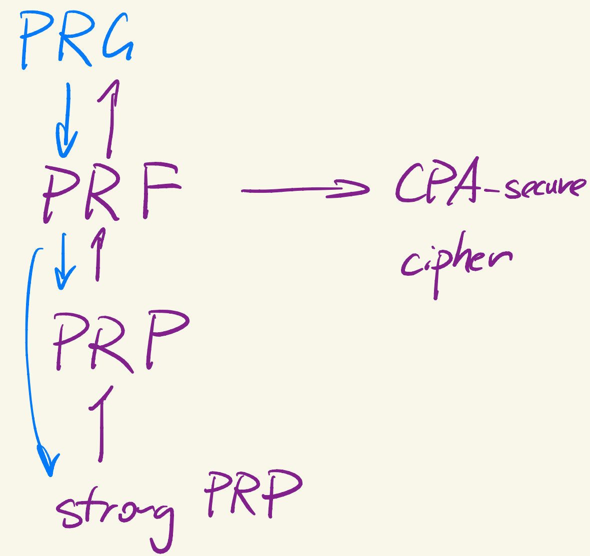
Chained CBC is not CPA-secure

4) Output Feedback (OFB)



5) Counter (CTR) mode





How to construct PRF from PRG

$f: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^\lambda$ $\qquad g: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$

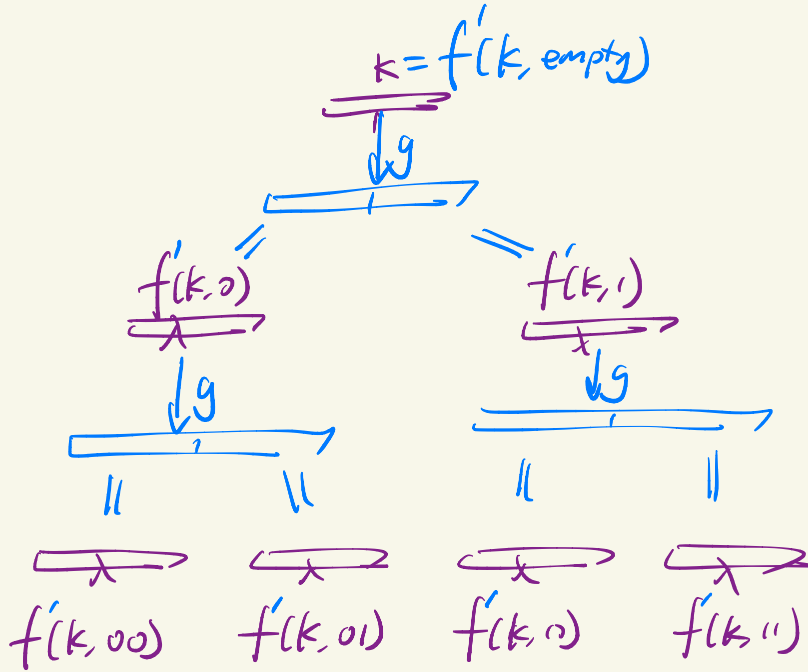
Define f and f' as

$$f': \{0,1\}^\lambda \times \{0,1\}^{\leq n} \to \{0,1\}^\lambda$$

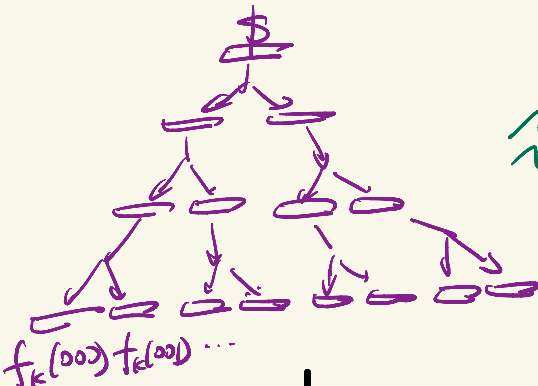
$$f'(k, \text{empty}) = k$$

$$f'(k, x0) \| f'(k, x1) = g(f'(k, x))$$

$$f(k, x) = f'(k, x)$$

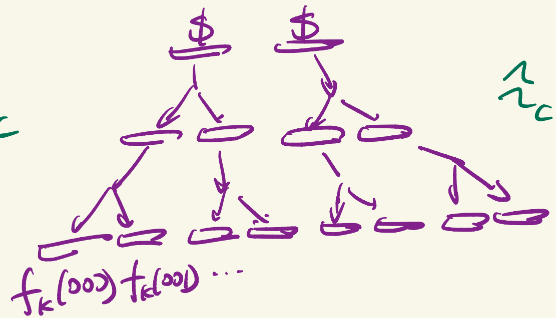


Proof f is a PRF, $f: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^\lambda$

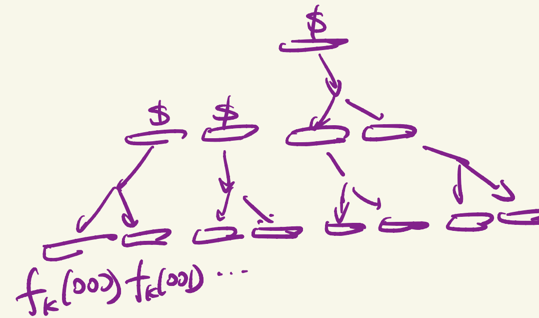


Real World

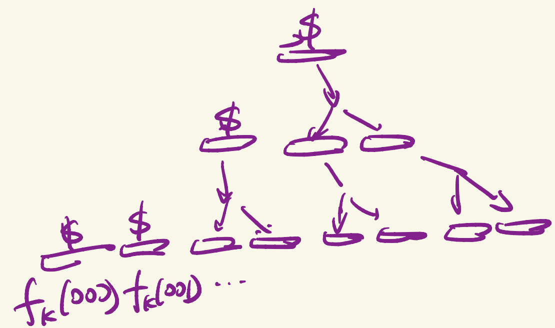
$\approx_c$



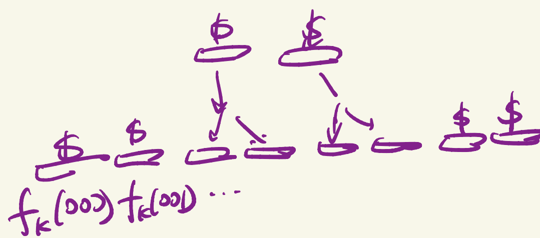
$\approx_c$



$\approx_c$



$\approx_c$



$f: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$ when $m \geq \lambda$

exists PRF $f': \{0,1\}^\lambda \times \{0,1\}^{n + \log \frac{m}{\lambda}} \to \{0,1\}^\lambda$

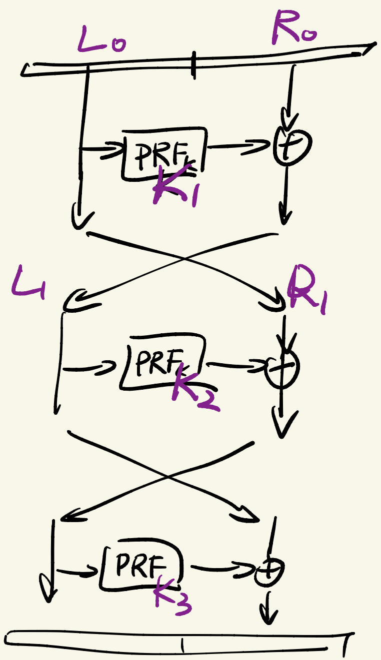
let $f_k(x) = \left(f'_k(x, 0), f'_k(x, 1) \ldots, f'_k\left(x, \frac{m}{\lambda} - 1\right)\right)$ is a PRF

How to construct PRP from PRF

$$f : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$$

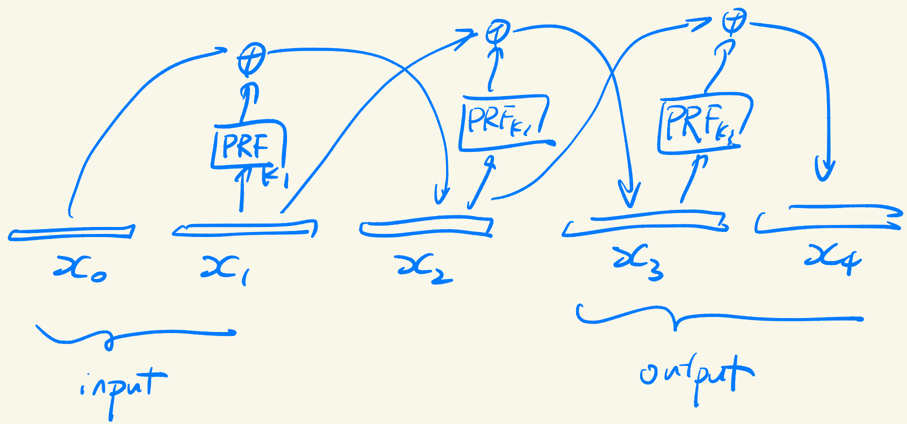
Feistel Network $P : \{0,1\}^? \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

$x \in \{0,1\}^{2n}$



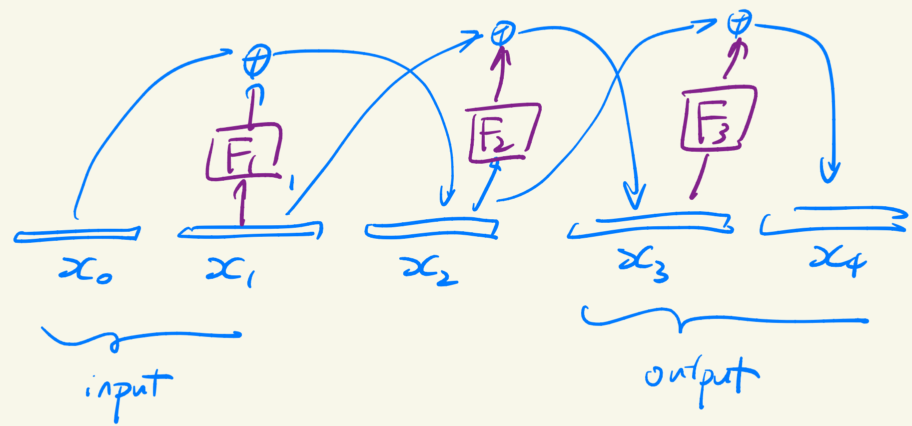
- 3-round Feistel is a PRP
- 4-round Feistel is a strong PRP

$$x_{i-1} \oplus x_{i+1} = f_{k_i}(x_i)$$



Proof 3-round Feistel is PRP

- Replace f_{k_1} f_{k_2} f_{k_3} with random F_1 F_2 F_3



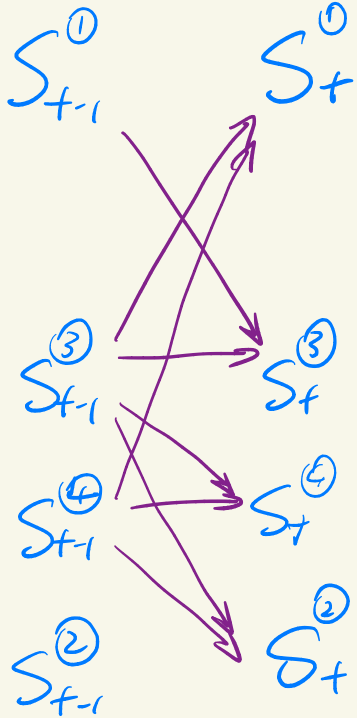
- let i-th query (x_0^i, x_1^i)

  W.l.o.g. $(x_0^i, x_1^i) \neq (x_0^j, x_1^j)$ for all $i \neq j$.

- In ideal world

  every time the adversary queries it receives a i.i.d. random string

- In Real world



1) before D makes the t-th query

$F_1(x)$ for $x \in \{x_1^1 \cdots x_1^{t-1}\}$ is close uniform

conditioning on A's knowledge

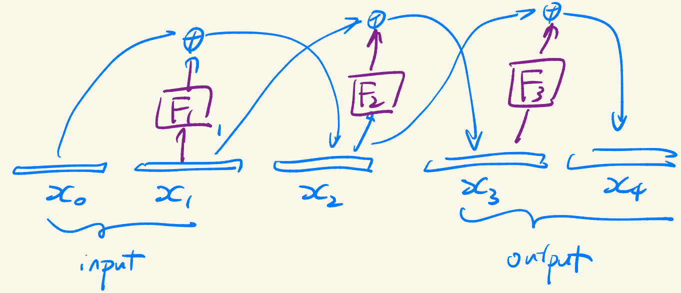
for $i<j<t$ $\quad x_2^i \neq x_2^j$

for $i<j<t$ $\quad x_3^i \neq x_3^j$

(x_3^t, x_4^t) is close to uniform

conditioning on A's knowledge before t-th query

3-round Feistel is not a strong PRP



arbitrarily choose x_0 x_1 Δ

query (x_0, x_1) get x_3 x_4, say x_2 is the hidden value

query $(x_0 + \Delta, x_1)$ get x_3' x_4'

query $(x_3, x_4 + \Delta)$ get x_0' x_1'

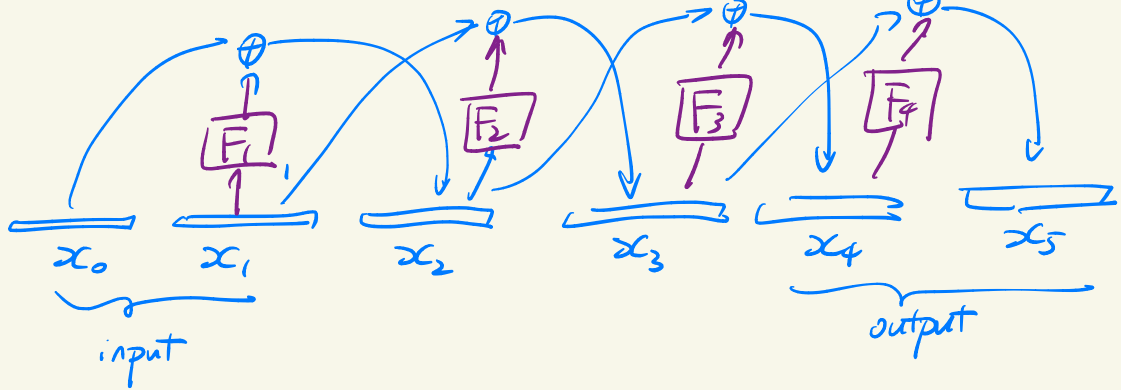
if the oracle is a 3-round Feistel

$$x_1 \oplus x_3' = x_2 \oplus \Delta = x_1' \oplus x_3$$

if the oracle is a random permutation

$$x_1 \oplus x_3' \neq x_1' \oplus x_3 \quad \text{with high probability}$$

4-round Feistel is a strong PRP



S_t: $\quad F_1(x)$ for $x \in \{x_1^1 \cdots x_1^t\}$
$\quad\quad F_4(x)$ for $x \in \{x_4^1 \cdots x_4^t\}$ is close to uniform conditioning on A's knowledge before the t-th query

$\forall i, j < t \quad x_2^i \neq x_2^j \quad x_3^i \neq x_3^j$

$(x_4^t \; x_5^t)$ is close to uniform conditioning on A's knowledge before the t-th query

otherwise $(x_0^t \; x_1^t)$