Symmetric Crypto Lec 3 (Apr 6, 2026)

Recap:

OWFs $\xrightarrow{\text{Lec1}}$ PRG_{+1} $\xrightarrow{\text{Lec2}}$ PRG_{poly} $\xrightarrow{\text{Lec2}}$ PRFs

↓ TODAY!

BC/PRPs

Outline:

- Block Ciphers
- Feistel Network
- PRP Construction
- Proof (High-Level)

Block Ciphers:-

A BC is a pair of deterministic, efficient algorithms

$(E : K \times X \to X \;,\; D : K \times X \to X)$

such that,

K: Key space

X: Input and Output space

(i) For any $k \in K$, $E(k, \cdot)$ is a permutation on X, and $D(k, \cdot)$ is its inverse.

(ii) E is a pseudo-random permutation

Defn. almost identical to PRF....

Def: A deterministic, efficient algorithm $E: K \times X \to X$ is a PRP if for all efficient adversaries A,

$$PRPAdv[A, E] \leq negl(\lambda)$$

defined via Exp0, Exp1 below:

Exp 0:

Chal.

$k \xleftarrow{R} K$

$f \leftarrow E(k, \cdot)$

A.

x_i →

← $f(x_i)$

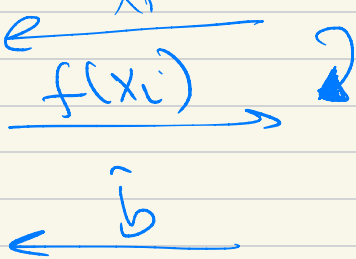
→ This arrow means that A can query evaluations of f many times, at any x_i.

Exp 1: set of all permutations on X

Chal

A:

$f \xleftarrow{\$} Perms[X]$



for $b \in \{0,1\}$, let W_b be the event that A outputs 1 in Exp b.

Def: $PRPAdv[A,E] = |P_A(W_0) - P_A(W_1)|$

Relation between PRPs and PRFs?

Q: Is a secure PRP a secure PRF? $(E: K \times X \to X)$

Ans: (i) If $|X|$ is small: NO!

Adv can distinguish E from a

random function as follows:

1. Query the challenger for f at all $x \in X$.

2. If for any $x \neq x' \in X$, $f(x) = f(x')$, output 1, else 0.
   ↳ 'collision'

✡ If f was a PRP i.e. Exp 0, (i.e. Chal sampled $k \xleftarrow{\$}$, $f = E(k, \cdot)$) then $f(x) = f(x')$ would never happen.

✡ But if f was a random function, (i.e. Exp 1, where Chal samples $f \xleftarrow{\$} \text{Func}[X,X]$) then, $f(x) = f(x')$ can happen for some x, x' with probability $1 - \frac{N!}{N^N}$ where $N = |X|$.

(ii) If $|X|$ is large: YES!

Switching Lemma!

Thm: Let $|X|$ be superpolynomial in λ (i.e. $\frac{1}{|X|}$ is $negl(\lambda)$).

A pair of algorithms (E, D) as defined in (i) and (ii) above is a block cipher if and only if E is a pseudo random function.

More formally, for any PPT adversary A that makes Q queries to its challenger,

$$|PRPAdv[A, E] - PRFAdv[A, E]| \leq \frac{Q^2}{2 \cdot |X|}$$

* Intuitively, if $|X|$ is large, Adv. cannot query at all $x \in |X|$.

With only just Q queries:

PRP: no collision

PRF: collision with

probability $\leq \left(\frac{Q^2}{|X|}\right)$

(think Birthday bound!)

$\Rightarrow$ negligible if $|X|$ large.

Thus, to show (E, D) is a Block cipher, it is enough to:

(i) show that D is the inverse of E.

(ii) show that E is a PRF.

HOW to build such a (E, D)?

Luby Rackoff: Block cipher from PRFs!

* But How do we even construct a permutation (and its inverse) from a function?

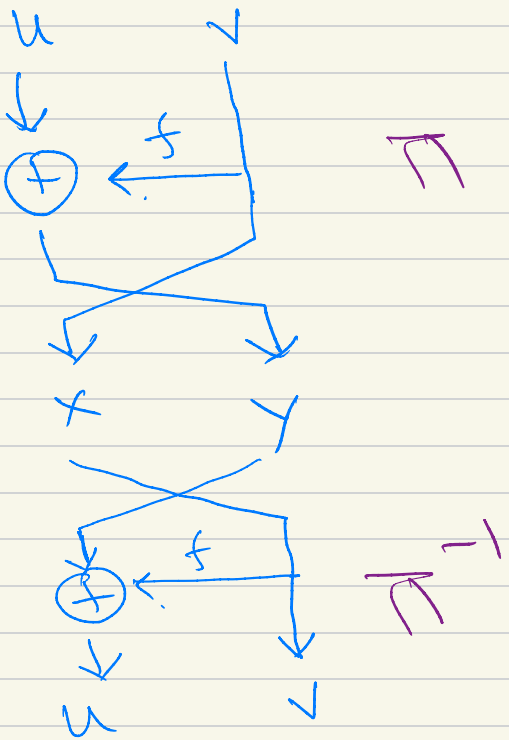
Key Technique: Feistel Permutation:

Let $f: X \to X$ be a function.

Then, a Feistel Permutation is defined as $\Pi: X \times X \to X \times X$:

$$\pi(u,v) = (v, u \oplus f(v))$$

$$\pi^{-1}(x,y) = (y \oplus f(x), x)$$



* Easy to see that π^{-1} is indeed inverse of π:

$$\pi^{-1}(\pi(u,v)) = \pi^{-1}(v, u \oplus f(v))$$

$$= ((u \oplus f(v)) \oplus f(v), v)$$

$$= (u, v).$$

n - round

Feistel Network : Apply Feistel permutation n times.

* DES is based on Feistel Networks!

Luby Rackoff Construction :

(secure Block Cipher from PRFs)

Idea : Replace f with a PRF $F(k, \cdot)$, Apply feistel permutation 3 times with distinct keys.

Formally :

Let $F : K \times X \to X$ be a PRF such that $|X|$ is superpoly(λ). We will construct (E, D) s.t:

$E : K^3 \times X^2 \to X^2$, $D : K^3 \times X^2 \to X^2$

$E((k_1, k_2, k_3), (u, v))$:

$w \leftarrow u \oplus F(k_1, v)$ ~ Feistel - I permutation:

$(u,v) \to (v,w)$

$x \leftarrow v \oplus F(k_2, w)$: Feistel - II $(v,w) \to (w,x)$

$y \leftarrow w \oplus F(k_3, x)$: Feistel - III $(w,x) \to (x,y)$

Output (x,y)

$D((k_1,k_2,k_3),(x,y))$:

$w \leftarrow y \oplus F(k_3, x)$: Invert III

$v \leftarrow x \oplus F(k_2, w)$: Invert II

$u \leftarrow w \oplus F(k_1, v)$: Invert I

Output (u,v)

Q: What goes wrong if we only applied Feistel just once?

A: If just one round:

$(u,v) \to (v, u \oplus F(k_1, v))$:

Adv can easily distinguish this output from a random function !!

1st Half of output is NOT Random, its just copied from the input !

Adv can make ONE query to Oval, for some (u,v), say Oval returns (x,y):

- If $x = v$, output 0 else 1

Happens for feistel design w.p. 1

Happens for a Random func. with negligible probability!

Q: What about 2 rounds? Exercise.

Thm: If f is a secure PRF, then (E,D) is a secure Block cipher.

Roadmap:

1.) Prove D is inverse of E (straightforward!)

2.) Prove E is a PRF. ← we'll do this.

3.) By Switching Lemma and 1), 2), (E,D) is a Block cipher.

Lemma. E is a secure PRF. Consider a PPT adversary A that makes at most Q queries.

Step 1: Without loss of generality, we can assume that A makes exactly Q queries, all of which are distinct.

(intuitively, A won't learn anything by making the same query twice)

Step 2: A sequence of HYBRIDS!

High-level idea:

(i) we can replace the PRF evaluation with truly random functions, by relying on PRF security:

Query at (u_i, v_i):

$$\left\{\begin{array}{l} w_i \leftarrow u_i \oplus F(k_1, v_i) \\ x_i \leftarrow v_i \oplus F(k_2, w_i) \\ y_i \leftarrow w_i \oplus F(k_3, x_i) \end{array}\right\} \approx \left\{\begin{array}{l} w_i \leftarrow u_i \oplus f_1(v_i) \\ x_i \leftarrow v_i \oplus f_2(w_i) \\ y_i \leftarrow w_i \oplus f_3(x_i) \end{array}\right\}$$

where f_1, f_2, f_3 are randomly sampled from $Funcs[X, X]$.

(ii) Now, if we could prove that all the x_i & y_i values are distributed uniformly at random (and independent) we'd be done.

(because then, responses to all of Adv's queries would look indistinguishable from a random function $f \leftarrow\!\$ Funcs(X \times X, X \times X]$)

To do so, (we will rely on f_1 being a random function)

* we will show with high probability, all the w_i values are distinct.
* Since $x_i = v_i \oplus f_2(w_i)$ where f_2 is a random function, this will imply the x_i values are all uniform random and independent. Hence, the x_i's

are also distinct w.h.p.

* Since $y_i = w_i \oplus f_3(x_i)$, this will imply that y_i's are also uniform random and independent!

Proof:

We will define 4 hybrids:

H0, H1, H2, H3. → real samples $\xleftarrow{\$}$ $k_1, k_2, k_3 \ldots$

H0 will just be Exp0 of PRF game

H3 " " " Exp1 " " "

↳ real samples

$f \xleftarrow{\$} Funcs[X \times X, X \times X]$

Let W_j be the event that A outputs 1 in H_j. Let $p_j = Pr[W_j]$.

We will show for $j = 1, 2, 3$,

$$|p_j - p_{j-1}| \leq negl(\lambda)$$

Then,

$$PRFADV[A, E] = |P_4[W_3] - P_4[W_0]|$$

$$= |p_3 - p_0| = |(p_3 - p_2) + (p_2 - p_1) + (p_1 - p_0)|$$

$$\leq |p_3 - p_2| + |p_2 - p_1| + |p_1 - p_0|$$

$$\leq negl(\lambda).$$

The hybrids :-

H_0 = Exp0

Challenger: Adv.

$k_1, k_2, k_3 \xleftarrow{\$} K$

(ith query for $i \in 1, \ldots, q_y$) $\xleftarrow{(u_i, v_i)}$

$w_i \leftarrow u_i \oplus F(k_1, v_i)$

$x_i \leftarrow v_i \oplus F(k_2, w_i)$

$y_i \leftarrow w_i \oplus F(k_3, x_i)$

$\xrightarrow{(x_i, y_i)}$

H1 : (Replacing PRFs with random func.)

Real.

A

$f_1, f_2, f_3 \leftarrow\$ \text{Funcs}[X, X]$

$\leftarrow (u_i, v_i)$

$w_i \leftarrow u_i \oplus f_1(v_i)$

$x_i \leftarrow v_i \oplus f_2(w_i)$

$y_i \leftarrow w_i \oplus f_3(x_i)$

$(x_i, y_i) \rightarrow$

Theorem: For any PPT A, we can construct a PPT adv. B s.t.

$$|P_{H1}[W_1] - P_{H1}[W_0]| = 3 \cdot \text{PRFAdv}[B, F]$$

Exercise: Prove this using Hybrids...

Hybrid H2:

Challenger is technically the SAME as Hybrid H_1, but we will write it in a different way...

Real:

$f_1 \leftarrow\$ \text{Func}[X, X]$

for f_2, f_3, we will explicitly sample randomness :-

$A_1, \ldots, A_Q \leftarrow\$ X$; will be used for f_2

$B_1, \ldots, B_Q \leftarrow\$ X$; " for f_3

(ith query from Adv) $\leftarrow (u_i, v_i)$

$w_i \leftarrow u_i \oplus f_1(v_i)$

If for some $j < i$, $w_j = w_i$,

then $x_i \leftarrow v_i \oplus A_j$; if w_i is unique, A_i acts as $f_2(w_i)$

otherwise $x_i \leftarrow v_i \oplus A_i$

If for some $j<i$, $x_j = x_i$,
then $y_i \leftarrow w_i \oplus B_j$
Otherwise $y_i \leftarrow w_i \oplus B_i$; if x_i is unique, B_i acts as $f_3(x_i)$

$\xrightarrow{\quad (x_i, y_i) \quad}$

* Easy to see that $p_1 = p_2$.

Hybrid H3:

Challenger identical to H_2, except, we remove consistency checks

Oral:

$f_1 \leftarrow\$ \text{Funcs}[X, X]$

$A_1 \ldots A_Q \leftarrow\$ X$

$B_1 \ldots B_Q \leftarrow\$ X$

$\xleftarrow{(u_i, v_i)}$

$w_i \leftarrow u_i \oplus f_1(v_i)$

A

$x_i \leftarrow v_i \oplus A_i$

$y_i \leftarrow w_i \oplus B_i$

} no consistency checks!

(x_i, y_i) →

Intuition:

If no 'collisions' occur in H_3 i.e. $w_j \neq w_i \ \forall j<i$ and $x_j \neq x_i \ \forall j<i$, then, Chal behaves identically in H_2 and H_3! Hence, Adv. can't distinguish the two.

We will now prove that collisions rarely occur.

* Let us analyse events W_2, W_3 over the probability space of:
  - Coins: Randomness used by Adv.
  - Randomness of Challenger: $f_1, A_1 \cdots A_Q, B_1 \cdots B_Q$.

Claim 1: In H_3, the random variables coins, $f_1, x_1, y_1, \ldots, x_Q, y_Q$ are mutually independent.

Pf: By construction, coins, $f_1, A_1 \ldots A_Q, B_1 \ldots B_Q$ are mutually independent.

- Then, conditioned on fixed values of coins, f_1, the first query (u_1, v_1) is fixed, and so, w_1 is fixed.
- But, A_1, B_1 are uniform random even conditioned on coins, f_1.

Since $x_1 = v_1 \oplus \underbrace{A_1}_{\text{u.r.}}$, $y_1 = w_1 \oplus \underbrace{B_1}_{\text{u.r.}}$,

x_1, y_1 are also uniform random in this space.

- Now, lets condition on (coins, f_1, x_1, y_1), (u_2, v_2) and w_2 are fixed.

But, A_2, B_2 are u.r. even in this conditioned space. $\Rightarrow x_2, y_2$ are u.r.

... claim follows by induction!

Let us now define collision events:-

Z_1 : $w_i = w_j$ for some $j < i$

Z_2 : $x_i = x_j$ for some $j < i$

$Z = Z_1 \vee Z_2$, event $\bar{Z}$: NO collisions.

Claim 2: $\Pr[w_2 \wedge \bar{Z}] = \Pr[w_3 \wedge \bar{Z}]$

Proof:

Informally, If Z does not occur, Challenger identical in H2, H3...

Formally, consider any fixed values of the variables (coins, $f_1, A_1 \ldots A_{\alpha}, B_1 \ldots B_{\alpha}$) for which Z does not occur.

* (u_1, v_1) depends only on coins.

then, $w_1 = u_1 \oplus f_1(v_1)$ same in both games. Then x_1, y_1 also are equal in both games.

* Next, (u_2, v_2) only depends on (coins, x_1, y_1), it is also equal in both games. Then, since Z does not occur, $w_2 \neq w_1$, hence, x_2 will be $v_2 \oplus A_2$ in both games.

Again, since Z does not occur, $x_2 \neq x_1$, hence, $y_2 = w_2 \oplus B_2$ in both.

:

continuing, $\forall i \in \{1, \ldots, Q^2\}$, $\{u_i, v_i, w_i, x_i, y_i\}$ equal in both.

since adv only sees these variables, its output must be the same in both!

$\Rightarrow$ $W_2 \wedge \bar{Z}$ happens iff $W_3 \wedge \bar{Z}$

$\Rightarrow$ QED.

We will now show $|p_2 - p_3| \leq \text{negl}(\lambda)$.

Proof:

$$|p_2 - p_3| = |\Pr[W_3] - \Pr[W_2]|$$ Total Probability

$$= \left| \begin{array}{l} \Pr[W_3 \wedge Z] + \Pr[W_3 \wedge \bar{Z}] \\ -\Pr[W_2 \wedge Z] - \Pr[W_2 \wedge \bar{Z}] \end{array} \right|$$

$$= |\underbrace{\Pr[W_3 \wedge Z]}_{\leq \Pr[Z]} - \underbrace{\Pr[W_2 \wedge Z]}_{\leq \Pr[Z]}|$$

Hence, union bound

$$|p_2 - p_3| \leq \Pr[Z] \leq \Pr[Z_1] + \Pr[Z_2]$$

Z_2: $x_i = x_j$ for some $j < i$

But recall, by Claim 1,

all x_i values are u.r. and independent

Hence

$$\Pr[Z_2] \leq {}^{\theta}C_2 \cdot \frac{1}{|X|} \leq \frac{\theta^2}{2|X|}$$

union bound over $\Pr[x_i = x_j]$ across all $j < i$.

Let us now analyse event Z_1:

Z_1 : $w_i = w_j$ for some $j < i$

Consider any fixed $j < i$:

Suppose $v_i = v_j$: Since Adv makes only distinct queries, $u_i \neq u_j$

Hence, $w_i \neq w_j$

$u_i \oplus f_1(v_i)$ $\hookrightarrow$ $u_j \oplus f_1(v_j)$

Suppose $v_i \neq v_j$: By Claim 1,

f_1 is uniformly distributed over $\text{Funcs}[X, X]$

$\Rightarrow$ $f_1(v_i)$ and $f_1(v_j)$ are u.r. over X.

$$\Rightarrow \Pr[u_i \oplus f_1(v_i) = u_j \oplus f_1(v_j)]$$

$$= \Pr[f_1(v_j) = u_i \oplus u_j \oplus f_1(v_i)]$$

$$= \frac{1}{|X|}$$

Thus, for a fixed i, j,

$$\Pr[w_i = w_j] \leq \frac{1}{|X|}$$

$$\Rightarrow \Pr[Z_1] \leq {}^{q}C_2 \cdot \frac{1}{|X|} \leq \frac{q^2}{2|X|}.$$

(By union Bound)

Hence,

$$|p_2 - p_3| \leq Pr[Z_1] + Pr[Z_2]$$

$$\leq \frac{Q^2}{|X|}.$$

To complete the proof,

Recall, we said H_3 will be equivalent to Exp1 of PRF game where Chal just samples a random function $f \leftarrow\!\$ \text{Funcs}[X \times X, X \times X]$.

WHY?

By Claim 1: $x_1, y_1, \ldots x_Q, y_Q$ are u.r. and independent

↓

This is EXACTLY the distribution of $f_1(u_i, v_i)$ for Q distinct (u_i, v_i) queries !!!

Combining everything,

$$\mathrm{PRFAdv}[A, E]$$

$$\leq |p_1 - p_0| + |p_2 - p_1| + |p_3 - p_2|$$

$$\leq 3 \cdot \mathrm{PRFAdv}[B, F] + 0 + \frac{Q^2}{|X|}$$

↑ negl if F is secure

↑ negl if $Q = \mathrm{poly}(\lambda)$ and $\frac{1}{X} = \mathrm{negl}(\lambda)$

By switching lemma, (E, D) is a Block Cipher!