Constructing Block Ciphers!

Recap

Lec 1   Lec 2   Today!

$$\text{OWFs} \rightarrow \text{PRGs}_{+1} \rightarrow \text{PRG}_{+\text{poly}} \rightarrow \text{PRFs} \rightarrow \text{BC/PRPs}$$

Outline

- Review
- BCs
- Fiestel Networks
- Construction

Review!

Def: A deterministic, efficient algorithm $F: K \times \mathcal{X} \rightarrow \mathcal{Y}$ is a PRF if for all efficient adversaries A,

$$\text{PRFadv}[A, F] \leq \text{negl}(\lambda)$$

Exp $b \in \{0,1\}$:

Chal

- If $b=0$: $k \xleftarrow{r} K$, $f \leftarrow F(k, \cdot)$.
  o/w: $f \xleftarrow{r} \text{Funs}[\mathcal{X}, \mathcal{Y}]$.

$\xleftarrow{\;x_i\;}$ **A**

$\xrightarrow{\;f(x_i)\;}$

A outputs $\hat{b} \in \{0,1\}$

For $b \in \{0,1\}$, W_b is the event that A outputs 1 in Exp b.

$$\text{PRFadv}[A,F] := \left| \Pr[W_0] - \Pr[W_1] \right|$$

A is called <u>Q-query</u> if A issues at most Q queries.

Block Ciphers

① A Block Cipher is a pair of deterministic, eff algs $(E : K \times X \to X,\ D : K \times X \to X)$ such that

② · For any $k \in K$, $E(k, \cdot)$ is a permutation on X and $D(k, \cdot)$ is it's inverse.

· E is a pseudorandom permutation.

Def is almost identical to a pseudorandom function except now:

· $F : K \times X \to X$ is a permutation

· In Exp 1, $f \xleftarrow{r} \text{Perms}[X]$.

Theorem (PRF Switching Lemma):

Let $|X|$ be super polynomial in the security parameter (i.e. $\frac{1}{|X|}$ is $\text{negl}(\lambda)$). A pair of algorithms (E, D) as defined in ① with property ② is a block cipher if and only if E is a pseudorandom function.

$$\left| \text{PRPadv}[A,E] - \text{PRFadv}[A,E] \right| \leq \frac{Q^2}{2|X|}$$

Thus, to show (E, D) is a Block cipher, it suffices to show E is just a PRF rather than a PRP.

Intuitively, for large $\mathcal{X}$, it should be hard to distinguish a random Function from a random Permutation.

Feistel Network

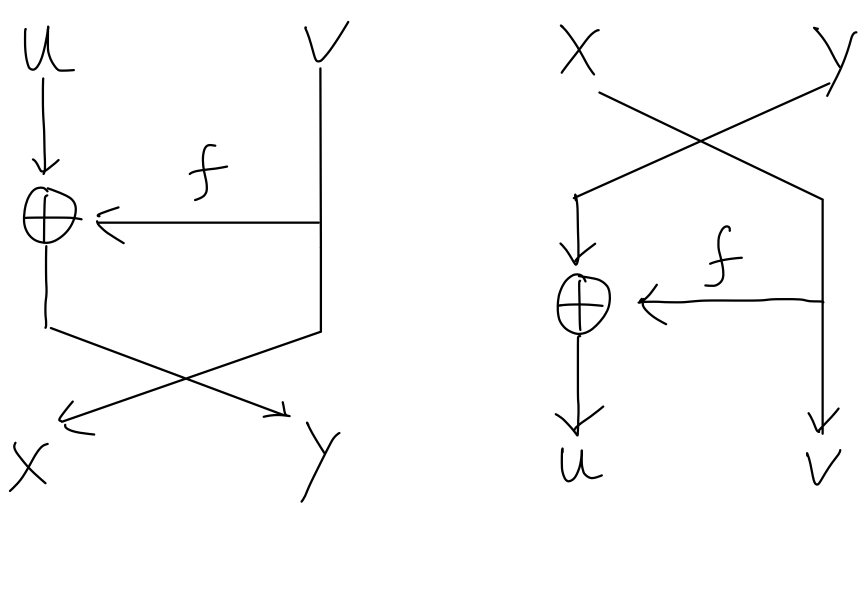
Ultimately, we want to construct a block cipher from a PRF. But, how would you even construct a permutation from a function?

"Feistal Permutation"

Let $f : \mathcal{X} \to \mathcal{X}$ be a function. Then,

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

are permutions on $\mathcal{X}^2$ and inverses.



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

Construction

Intuition: Replace the f in the fiestal permutation with $F(k,\cdot)$ where F is a PRF. Then, apply the fiestal permutation three times with distinct keys.

(Luby – Rackoff) Let $F: K \times X \to X$ be a PRF such that $|\mathcal{X}| = \{0,1\}^\lambda$. We will construct (E, D) where $E: K^3 \times \mathcal{X}^2 \to \mathcal{X}^2$, $D: K^3 \times \mathcal{X}^2 \to \mathcal{X}^2$

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

- $w \leftarrow u \oplus F(k_1, v)$
- $x \leftarrow v \oplus F(k_2, w)$
- $y \leftarrow w \oplus F(k_3, x)$

Output (x, y)

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

- $w \leftarrow y \oplus F(k_3, x)$
- $v \leftarrow x \oplus F(k_2, w)$
- $u \leftarrow w \oplus F(k_1, v)$

Output (u, v)

What goes wrong with only applying the permutation one or two times instead?

Thm: If F is a PRF, then (E, D) is a Block Cipher.

Road Map

1) Prove E is a PRF. ← we'll do this.
2) By the PRF switching Lemma and 1), (E, D) is a block cipher.

Lemma: E is a PRF

Consider an efficient PRF adversary A that makes at most Q queries. We will show $\text{PRFadv}[A, E] \leq \text{negl}(\lambda)$.

$\boxed{\text{Step 1}}$: Simplifying the Adversary

Claim: We can construct an adversary A' s.t.

- $\text{PRFadv}[A, E] = \text{PRFadv}[A', E]$
- A' always makes exactly Q distinct queries.
- A' is efficient if A is efficient.

Sketch: A' is a trivial wrapper around A that

- Keeps a table of distinct queries from A and responses.
- A' forwards distinct queries to the challenger and simulates / forwards responses to A's queries.
- If A makes less than Q queries, A' will make extra distinct queries until Q is reached.

We will proceed WLOG that the prior conditions (*) apply to A, since the advantage of A' is identical.

$\boxed{\text{Step 2:}}$ Sequence of Hybrids

Intuition: We can replace the PRF evaluations $F(k_1,\cdot)$, $F(k_2,\cdot)$, $F(k_3,\cdot)$ with truly random functions f_1, f_2, f_3.

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

We can show with high probability that all the w_i's resulting from the queries are distinct. This will imply the x_i's are random and independent. As a result, we can similarly show they are distinct with high probability. This will allow us to conclude that the y_i's are similarly random and independent.

Proof: Overview

- Games 0, 1, 2, 3 are played between A and different challengers.
- Game 0 will correspond to Exp 0 and Game 3 will correspond to Exp 1 of the PRF game.
- Let W_j be the event that A outputs 1 in Game j. $p_j = Pr[W_j]$
- We will show for $j = 1, \ldots, 3$. $|Pr[W_j] - P[W_{j-1}]| \leq negl(\lambda)$.

· Thus, $\mathrm{PRFadv}[A, E] = |\Pr[W_3] - \Pr[W_0]|$

$$= |(P_3 - P_2) + (P_2 - P_1) + (P_1 - P_0)|$$

$$\leq |P_3 - P_2| + |P_2 - P_1| + |P_1 - P_0|$$

$$\leq \mathrm{negl}(\lambda)$$

<u>Game 0 Challenger</u>

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

Receive (u_i, v_i) (for $i = 1, \ldots, Q$)

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

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

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

Send (x_i, y_i) to A

<u>Game 1 Challenger</u>

$f_1, f_2, f_3 \xleftarrow{r} \mathrm{Funs}[\mathcal{X}, \mathcal{X}]$

Receive (u_i, v_i) (for $i = 1, \ldots, Q$)

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

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

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

Send (x_i, y_i) to A

<u>Theorem</u>: There exists an adversary B, just as efficient as A, such that

$$|\Pr[W_1] - \Pr[W_0]| = 3 \cdot \mathrm{PRFadv}[B, F]$$

<u>Exercise:</u> See if you can show this!

Hint: Construct a PRF adversary against the 3-PRF.

<u>Game 2</u>: In this game, we will replace the challenger with an identical challenger called a <u>faithful gnome</u> such that

- $\Pr[W_2] = \Pr[W_1]$ (i.e. the chal behaves identically)
- We can reason more explicitly about the randomness used.

$f_1 \xleftarrow{r} \mathrm{Funs}[\mathcal{X}, \mathcal{X}]$

$X_1, \ldots, X_Q \xleftarrow{r} \mathcal{X}$ "randomness for f_2, f_3 queries"

$Y_1, \ldots, Y_Q \xleftarrow{r} \mathcal{X}$

- Receive (u_i, v_i) (for $i = 1, \ldots, Q$)

  $w_i \leftarrow u_i \oplus f_1(v_1)$

  $x_i' \leftarrow X_i$

  ☆ If $w_i = w_j$ for some $j < i$: $x_i' \leftarrow x_j'$

  $x_i \leftarrow v_i \oplus x_i'$

  Makes sure we simulate f_2 as a random function

  $y_i' \leftarrow Y_i$

  ☆ If $x_i = x_j$ for some $j < i$: $y_i' \leftarrow y_j'$

  $y_i \leftarrow w_i \oplus y_i'$

  Simulate f_3

  Send (x_i, y_i) to A.

<u>Game 3</u>: In this game, the challenger will be identical to the Game 2 chal, except we remove the consistency checks ☆. This is referred to as the "forgetful gnome."

$f_1 \xleftarrow{r} \mathrm{Funs}[\mathcal{X}, \mathcal{X}]$

$X_1, \ldots, X_Q \xleftarrow{r} \mathcal{X}$

$Y_1, \ldots, Y_Q \xleftarrow{r} \mathcal{X}$

- Receive (u_i, v_i) (for $i = 1, \ldots, Q$)

  $w_i \leftarrow u_i \oplus f_1(v_1)$

  $x_i' \leftarrow X_i$

  $x_i \leftarrow v_i \oplus x_i'$

  no consistency checks

  $y_i' \leftarrow Y_i$

  $y_i \leftarrow w_i \oplus y_i'$

  Send (x_i, y_i) to A.

Intuition: If no collisions occur, then these challengers will behave identically; hence, an adversary would behave the same. We will show collisions rarely occur.

Probability: When comparing $\Pr[W_3]$ and $\Pr[W_2]$, we must be careful to ensure they are over the same probability space.

The following random variables determine the probability space

- Coins: randomness of the adversary
- f_1, $X_1, \ldots, X_Q$, $Y_1, \ldots, Y_Q$: randomness of the challenger

Claim 1: In game 3, Coins, f_1, $X_1, Y_1, \ldots, X_Q, Y_Q$ are mutually independent.

Proof Sketch: Observe, by construction, that the random variables Coins, f_1, $X_1, Y_1, \ldots, X_Q, Y_Q$ are mutually independent.

- Condition on fixed values for (Coins, f_1), the first query (u_1, v_1) and w_1 are fixed. However, (X_1, Y_1) are uniform and ind in the conditioned space. Hence, (x_1, y_1) are also.
- Then, conditioned on (Coins, f_1, x_1, y_1), (u_2, v_2, w_2) are fixed, but (X_2, Y_2) are uniform and independently distributed.
- Claim follows by induction.

Collision Events:

- Z_1: event where $w_i = w_j$ for some $i \neq j$
- Z_2: event where $x_i = x_j$ for some $i \neq j$
- $Z := Z_1 \vee Z_2$

Claim 2: $W_2 \wedge \bar{Z}$ occurs if and only if $W_3 \wedge \bar{Z}$

Proof Sketch: For fixed values of Coins, f_1, $X_1, \dots, X_Q$, $Y_1, \dots, Y_Q$ such that Z does not occur, we can show the sequence of queries (u_i, v_i) and responses (x_i, y_i) are identical by induction. In particular, the consistency checks are never triggered.

We will now show $|Pr[W_3] - Pr[W_2]| \leq negl(\lambda)$.

Proof:

$$\begin{aligned}
|Pr[W_3] - Pr[W_2]| &= \left| \begin{aligned} &Pr[W_3 \wedge Z] + Pr[W_3 \wedge \bar{Z}] \\ &- Pr[W_2 \wedge \bar{Z}] - Pr[W_2 \wedge Z] \end{aligned} \right| \\
&= |Pr[W_3 \wedge Z] - Pr[W_2 \wedge Z]| \\
&\leq Pr[Z] \leq Pr[Z_1] + Pr[Z_2]
\end{aligned}$$

By claim 1) and union bound, $Pr[Z_2] \leq \frac{Q^2}{2} \cdot \frac{1}{|\mathcal{X}|}$.

Next, we will show $Pr[Z_1] \leq \frac{Q^2}{2} \cdot \frac{1}{|\mathcal{X}|}$.

Consider any fixed pair of indices $i \neq j$.

Suppose $v_i = v_j$: Since A only makes distinct queries, we must have $u_i \neq u_j$; Thus, $w_i \neq w_j$.

Suppose $v_i \neq v_j$: By claim 1, $f_1(v_i)$ and $f_1(v_j)$ are uniformly and independently distributed ☆ in a conditioned probability space over fixed values

$$\Pr[u_i \oplus f_1(v_i) = u_j \oplus f_1(v_j)]$$
$$= \Pr[u_i \oplus u_j = f_1(v_i) \oplus f_1(v_j)]$$
$$= \frac{1}{|\mathcal{X}|}$$

Thus, $\Pr[w_i = w_j] \leq \frac{1}{N}$ and $\Pr[Z_1] \leq \frac{Q^2}{2} \cdot \frac{1}{|\mathcal{X}|}$ by union bound.
Therefore, $|\Pr[W_3] - \Pr[W_2]| \leq \frac{Q^2}{|\mathcal{X}|}$.

Finally, in summary,

$$\text{PRFadv}[A, E] \leq 3 \cdot \underbrace{\text{PRFadv}[B, F]}_{\text{negl}(\lambda)} + \underbrace{\frac{Q^2}{|\mathcal{X}|}}_{\text{negl}(\lambda)} \leq \text{negl}(\lambda)$$

By the PRF switching Lemma, (E, D) is a block cipher. □