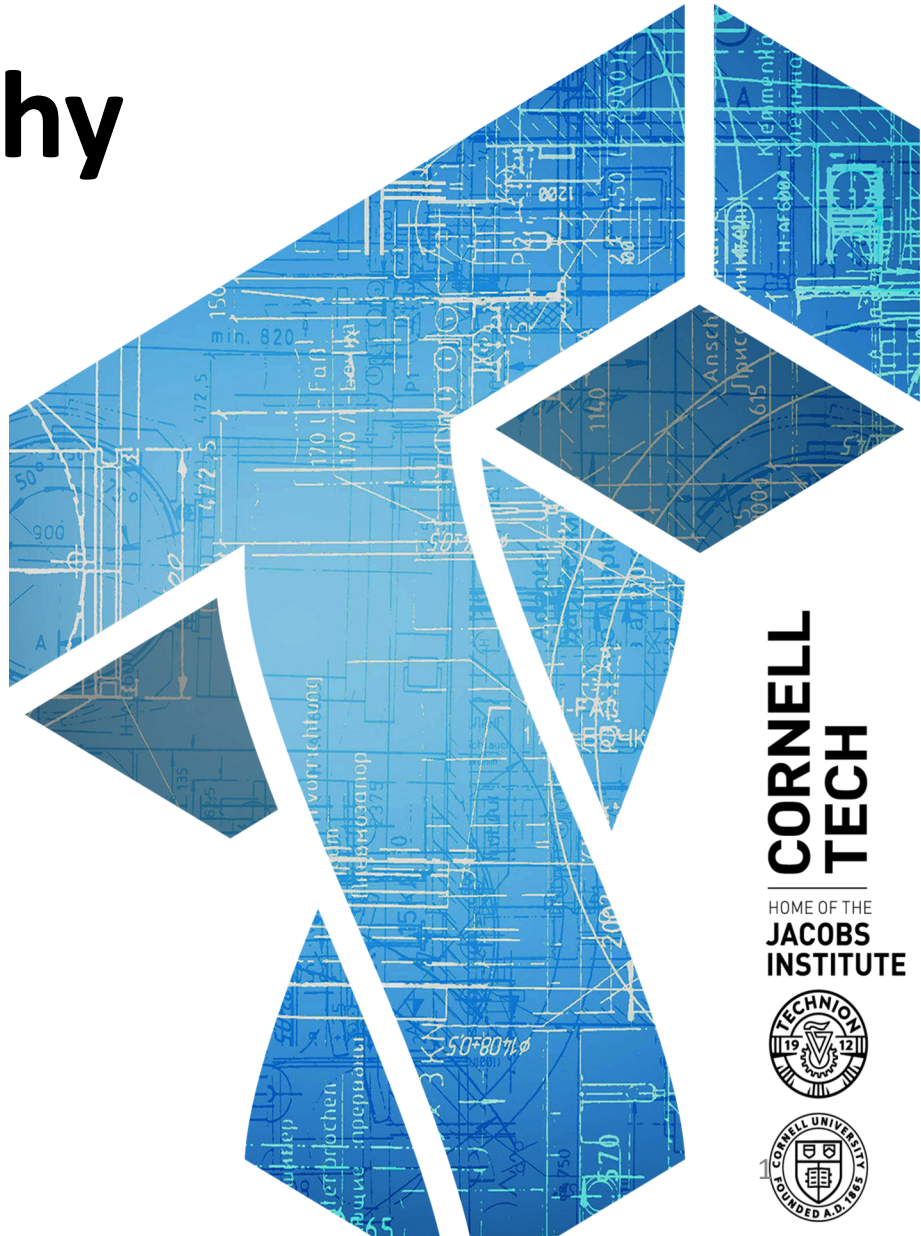
CS 6831
Designing Secure Cryptography

Tom Ristenpart

Cornell CIS
Computer Science



CORNELL TECH
HOME OF THE
JACOBS
INSTITUTE

Ciphers

$\Sigma = (E, D)$ is a pair of algs.

E is enciphering $E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

D is deciphering $D: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

$\mathcal{K} = \{0,1\}^k$

$\mathcal{M} = \{0,1\}^n = \mathcal{C}$

block cipher

Associated to E:

$\mathcal{K}$ is key space

$\mathcal{M}$ is message space

$\mathcal{C}$ is ctxt space

Correctness $\forall m \in \mathcal{M}, \forall k \in \mathcal{K}$

$D(k, E(k, m)) = m$

$E_k(m) = E(k, m)$

$D_k(c) = D(k, c)$

Ciphers

Simple OTP cipher. $K = M = C = \{0,1\}^n$

$E(K, m) = m \oplus K$

$D(K, C) = C \oplus K$

(1) keys should remain secret

(2) Message confidentiality maintained

Ciphers: game plan

- Key recovery security notions
  - Relationships between security notions
  - Exhaustive key search attacks
- PRP and PRF security
  - PRP/PRF switching lemma
  - Identical-until-bad proofs
- Constructing PRFs from PRPs
  - Feistel construction & Luby-Rackoff

Target key recovery security

$\underline{\mathrm{TKR}^{\mathcal{A}}_{\mathcal{E}}}$

$K \leftarrow\!\!\$\ \mathcal{K}$

$K^* \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$

Ret $(K = K^*)$

$\underline{\mathrm{Fn}(M)}$

$C \leftarrow E_K(M)$

Ret C

$$\mathbf{Adv}^{\mathrm{tkr}}_{\mathcal{E}}(\mathcal{A}) = \Pr\left[\,\mathrm{TKR}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow \mathsf{true}\,\right]$$

Adversary chooses messages

Chosen-message attack

Target key recovery security

- TKR security does not provide message confidentiality
  - Trivial identity map cipher
- "Unfair" to adversary, since can be many keys that are ***consistent*** on query transcript

$E(K, m) = m$

$D(K, c) = c$

$K = \{0,1\}^k$

For any A, it holds:

$$Adv^{tkr}_{E}(A) \leq \frac{1}{2^k}$$

Key recovery security

$\underline{\mathrm{KR}_{\mathcal{E}}^{\mathcal{A}}}$

$K \xleftarrow{\$} \mathcal{K}$

$K^* \xleftarrow{\$} \mathcal{A}^{\mathrm{Fn}}$

win $\leftarrow$ true

For $M \in \mathcal{X}$:

  If $E_{K^*}(M) \neq E_K(M)$ then

    win $\leftarrow$ false

Ret win

$\underline{\mathrm{Fn}(M)}$

$\mathcal{X} \leftarrow \mathcal{X} \cup \{M\}$

$C \leftarrow E_K(M)$

Ret C

$$\mathbf{Adv}^{\mathrm{kr}}_{\mathcal{E}}(\mathcal{A}) = \Pr\left[\mathrm{KR}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow \mathsf{true}\right]$$

Vacuous definition

So restrict to adversaries that make $q > 0$ queries

$\mathcal{E}$ is "KR secure"

$\mathcal{E}(K, M) = \bar{\mathcal{E}}_K(M) \| M$

Comparing security definitions

We can formally compare security definitions

$$\text{DEF1} \not\Rightarrow \text{DEF2}$$

TKR $\not\Rightarrow$ KR

Example: identity map

$$\text{DEF1} \Rightarrow \text{DEF2}$$

KR $\stackrel{?}{\Rightarrow}$ TKR

We can show a ***counter-example***:

- Scheme such that show no (reasonable) DEF1-adversary gets good advantage
- We give DEF2-adversary that gets good DEF2 advantage

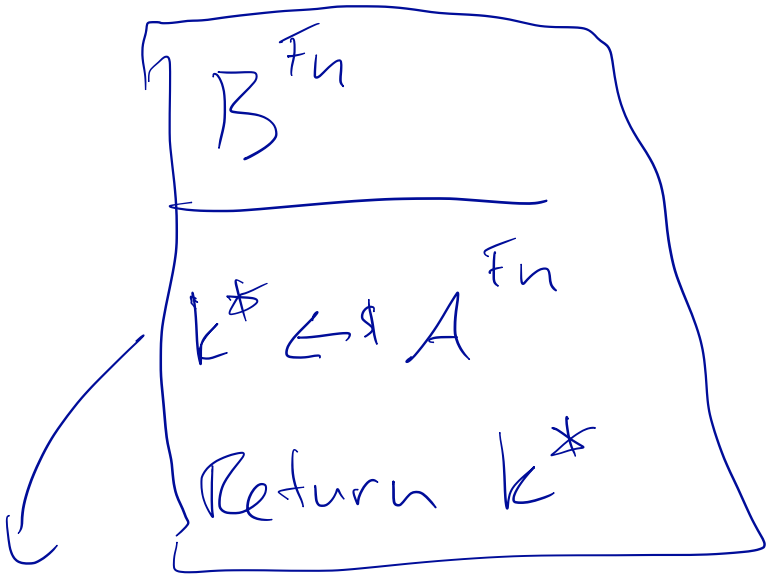
We can show a ***reduction***:

- Convert DEF2-adversary A into DEF1-adversary B s.t. B's DEF1 advantage upper bounds A's DEF2 advantage

$\mathrm{KR} \Rightarrow \mathrm{TKR}$

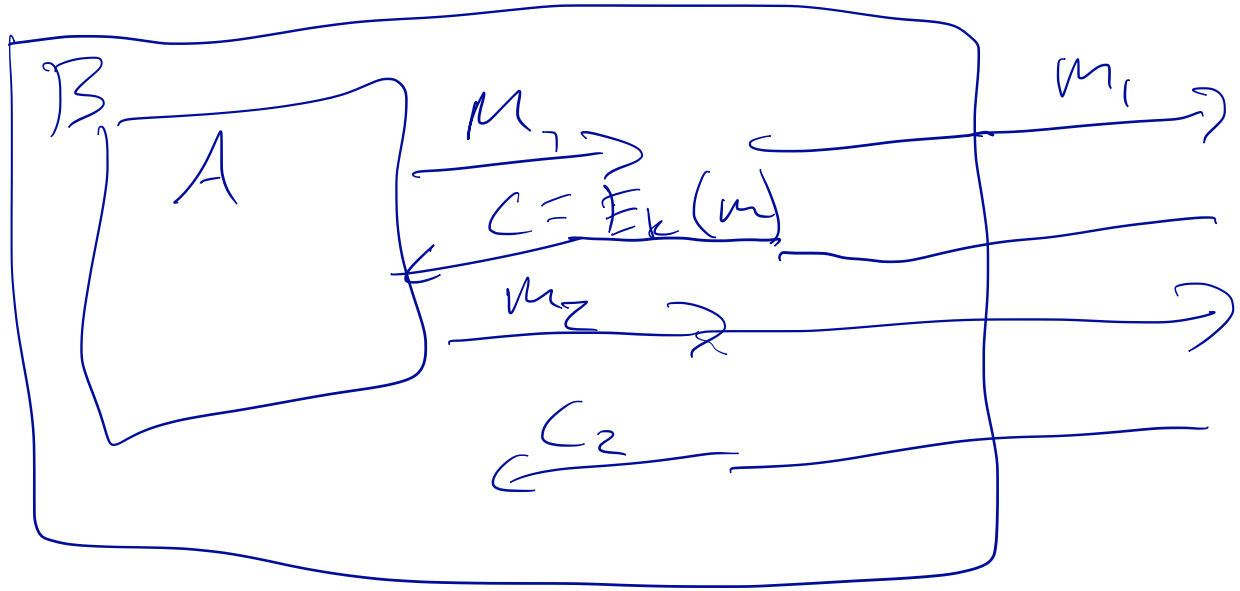
Theorem 1 *Let $\mathcal{E}$ be a cipher. For any $\mathrm{TKR}_{\mathcal{E}}$-adversary $\mathcal{A}$, we give a $\mathrm{KR}_{\mathcal{E}}$-adversary $\mathcal{B}$ such that* $\mathbf{Adv}^{\mathrm{tkr}}_{\mathcal{E}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kr}}_{\mathcal{E}}(\mathcal{B})$.

"runnable" reductions



"elementary wrapper"

$$\Pr[\mathrm{TKR}^{A}_{\mathcal{E}} \Rightarrow \mathrm{true}] \leq \Pr[\mathrm{KR}^{B}_{\mathcal{E}} \Rightarrow \mathrm{true}]$$



$\underline{\mathrm{TKR}^{\mathcal{A}}_{\mathcal{E}}}$

$K \leftarrow\!\!\$\ \mathcal{K}$

$K^* \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$

Ret $(K = K^*)$

$\underline{\mathrm{Fn}(M)}$

$C \leftarrow E_K(M)$

Ret C

$\Pr[\mathrm{TKR}^{\mathcal{A}}] = \frac{1}{2^k}$

$\underline{\mathrm{KR}^{\mathcal{A}}_{\mathcal{E}}}$

$K \leftarrow\!\!\$\ \mathcal{K}$

$K^* \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$

win $\leftarrow$ true

For $M \in \mathcal{X}$:

  If $E_{K^*}(M) \neq E_K(M)$ then

    win $\leftarrow$ false

Ret win

$\underline{\mathrm{Fn}(M)}$

$\mathcal{X} \leftarrow \mathcal{X} \cup \{M\}$

$C \leftarrow E_K(M)$

Ret C

Exhaustive key search

- Can we lower-bound (T)KR security in general?
  - ***Generic*** attack: one that works against any cipher

$\underline{\mathcal{A}^{\mathrm{Fn}}_{\mathrm{eks}}}$
$C \leftarrow \mathrm{Fn}(M)$
For $K^* \in \mathcal{K}$ do:
    If $C = E(K^*, M)$ then
        Return K^*
Return $\perp$

Exhaustive key search

- Can we lower-bound (T)KR security in general?
  - ***Generic*** attack: one that works against any cipher

$\underline{\mathcal{A}^{\mathrm{Fn}}_{\mathrm{eks}}}$
$C \leftarrow \mathrm{Fn}(M)$
For $K^* \in \mathcal{K}$ do:
    If $C = E(K^*, M)$ then
        Return K^*
Return $\perp$

$$\mathbf{Adv}^{\mathrm{kr}}_{\mathcal{E}}(\mathcal{A}_{\mathrm{eks}}) = 1$$

$$\mathbf{Adv}^{\mathrm{tkr}}_{\mathcal{E}}(\mathcal{A}_{\mathrm{eks}}) = ?? \approx 1$$

for "real" blockciphers

Worst-case running time? $|\mathcal{K}|$

Expected running time? $\frac{|\mathcal{K}|}{2}$

Computational security

- Big paradigm shift: focus on computationally bound adversaries
- Which adversaries that we've seen so far are computationally efficient?
- How do we measure computational costs?
  - Simple solution: assume abstract unit costs of (most) operations
  - Course-grained but useful

Is KR a good notion?

- Identity cipher (example of why TKR bad) is insecure under KR

Is KR a good notion?

- Identity cipher (example of why TKR bad) is insecure under KR
- But KR doesn’t imply message confidentiality
  - It’s a necessary, but not sufficient goal

PRP and PRF security

- Standard goal for cipher security is security in the sense of pseudorandom permutations and/or pseudorandom functions

- For simplicity in following, focus on ***block ciphers***

$$E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \qquad \mathcal{K} = \{0,1\}^k \quad \mathcal{M} = \{0,1\}^n$$

- Let Perm(n,n) be set of all permutations on n bits

$|\{0,1\}^n| = 2^n$

$|\text{Perm}(n)| = 2^n!$

- Let Func(n,n) be set of all functions from $\{0,1\}^n$ -> $\{0,1\}^n$

$|\text{Func}(n,n)| = (2^n)^{2^n}$

PRF security games

Pseudorandom function: indistinguishability from a random function (RF)

$\underline{\mathrm{PRF1}^{\mathcal{A}}_{\mathcal{E}}}$
$K \leftarrow\!\!\$\ \mathcal{K}$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(M)}$
Return $E_K(M)$

$\underline{\mathrm{PRF0}^{\mathcal{A}}_{\mathcal{E}}}$
$\rho \leftarrow\!\!\$\ \mathrm{Func}(n, n)$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(M)}$
Return $\rho(M)$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{E}}(\mathcal{A}) = \left|\Pr\left[\,\mathrm{PRF1}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right] - \Pr\left[\,\mathrm{PRF0}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right]\right|$$

Generic block cipher PRF security attack

Can we give generic distinguishing attack for any cipher?

$\underline{\mathrm{PRF1}^{\mathcal{A}}_{\mathcal{E}}}$	$\underline{\mathrm{PRF0}^{\mathcal{A}}_{\mathcal{E}}}$
$K \leftarrow\$\ \mathcal{K}$	$\rho \leftarrow\$\ \mathrm{Func}(n,n)$
$b' \leftarrow\$\ \mathcal{A}^{\mathrm{Fn}}$	$b' \leftarrow\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'	Return b'
$\underline{\mathrm{Fn}(M)}$	$\underline{\mathrm{Fn}(M)}$
Return $E_K(M)$	Return $\rho(M)$

"Birthday" attack

Fn

A_{bday}

Let $M_1, \ldots, M_q \in \{0,1\}^n$ distinct

For $i = 1$ to q do $C_i \leftarrow \mathrm{Fn}(M_i)$

If $\exists i \neq j$. $C_i = C_j$ then Ret 0

Ret 1

$C_1, C_2, \ldots, C_q$ iid $\{0,1\}^n$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{E}}(\mathcal{A}) = \left|\Pr\left[\,\mathrm{PRF1}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right] - \Pr\left[\,\mathrm{PRF0}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right]\right|$$

1

$(1 - q^2/2^n)$

$q^2/2^n$

PRP security games

Pseudorandom permutation: indistinguishability from a random permutation (RP)

$\underline{\mathrm{PRP1}^{\mathcal{A}}_{\mathcal{E}}}$
$K \xleftarrow{\$} \mathcal{K}$
$b' \xleftarrow{\$} \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(M)}$
Return $E_K(M)$

$\underline{\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}}$
$\pi \xleftarrow{\$} \mathrm{Perm}(n)$
$b' \xleftarrow{\$} \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(M)}$
Return $\pi(M)$

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathcal{E}}(\mathcal{A}) = \left|\Pr\left[\,\mathrm{PRP1}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right] - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}} \Rightarrow 1\,\right]\right|$$

PRP/PRF switching lemma

- Can we relate the two security notions?
- Intuitively: no difference between RF and RP when observing only a few input-output pairs

PRP/PRF switching lemma

- Can we relate the two security notions?
- Intuitively: no difference between RF and RP when observing only a few input-output pairs

Lemma 1 *Let $\mathcal{E}$ be a cipher with ciphertext space $\{0,1\}^n$. Let $\mathcal{A}$ be an adversary making at most q queries. Then*

$$\left|\Pr\left[\,\mathrm{PRF0}_{\mathcal{E}}^{\mathcal{A}} \Rightarrow 1\,\right] - \Pr\left[\,\mathrm{PRP0}_{\mathcal{E}}^{\mathcal{A}} \Rightarrow 1\,\right]\right| \leq \frac{q^2}{2^n}\ .$$

Let Dist be event in $\mathrm{PRF0}_{\mathcal{E}}^{\mathcal{A}}$ game that all values returned from Fn are distinct.

$$\Pr\left[\mathrm{PRP0}_{\mathcal{E}}^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathrm{PRF0}_{\mathcal{E}}^{\mathcal{A}} \Rightarrow 1 \mid \mathrm{Dist}\right]$$

BR06 paper

$\Pr[G0 \Rightarrow 1] = \Pr[\mathrm{PRP}_E^A \Rightarrow 1]$

$\Pr[G1 \Rightarrow 1] = \Pr[G0 \Rightarrow 1]$

$\Pr[G2 \Rightarrow 1] = \Pr[\mathrm{PRF}_E^A \Rightarrow 1]$ lazy sampling

G1 & G2 identical-until-bad

Fundamental lemma of game playing

$\Pr[G1 \Rightarrow 1] \leq \Pr[G2 \Rightarrow 1] +$

$\Pr[\mathrm{bad}_2 \text{ set true}]$

$\leq q^2/2^n$

G0

$b' \leftarrow\$ \mathcal{A}^{\mathrm{Fn}}$

Return b'

$\underline{\mathrm{Fn}(M)}$

If $\mathtt{F}[M] = \perp$ then

  $\mathtt{F}[M] \leftarrow\$ \{0,1\}^n \setminus \mathtt{F}$

Return $\mathtt{F}[M]$

Chose from set of points not previously returned

G1 G2

$b' \leftarrow\$ \mathcal{A}^{\mathrm{Fn}}$

Return b'

$\underline{\mathrm{Fn}(M)}$

$C \leftarrow\$ \{0,1\}^n$

If $C \in \mathtt{F}$ then

  bad $\leftarrow$ true

  $C \leftarrow\$ \{0,1\}^n \setminus \mathtt{F}$

$\mathtt{F}[M] \leftarrow C$

Return $\mathtt{F}[M]$

PRP/PRF switching lemma

- As long as $q << 2^n$, can move between considering RP or RF. Proving PRF and PRP (roughly) equivalent

- Proof shows ***game-hopping technique***
  - Conservative transitions (that do not change distrubution)
  - Identical-until bad transition

- We can show that PRF/PRP security implies KR security
  - Converse is not true

Summary so far

TKR KR PRP PRF

$$E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

- Computational security for ciphers. Requires sufficient
  - key length (exhaustive key search)
  - block size (when one needs a PRF)

PRPs from PRFs

- How does one securely build a PRP from a PRF?
- Feistel construction

Theorem 1 *Let $\mathcal{E}$ be the 3-round Feistel cipher using round function $F\colon \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^n$. For any $\mathrm{PRP}_{\mathcal{E}}$-adversary $\mathcal{A}$ making at most q queries we give an PRF_F-adversary $\mathcal{B}$ making at most $3q$ queries such that*

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathcal{E}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{2q^2}{2^n} + \frac{q^2}{2^{2n}} \ .$$

G0

$K \leftarrow\!\!\$\ \{0,1\}^k$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(LR)}$
$L_1 \leftarrow R$
$R_1 \leftarrow L \oplus F_K(\langle 1\rangle \,\|\, R)$
$L_2 \leftarrow R_1$
$R_2 \leftarrow L_1 \oplus F_K(\langle 2\rangle \,\|\, R_1)$
$L_3 \leftarrow R_2$
$R_3 \leftarrow L_2 \oplus F_K(\langle 3\rangle \,\|\, R_2)$
Return $L_3 \,\|\, R_3$

G1

$\rho \leftarrow\!\!\$\ \mathrm{Func}(2n, n)$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(LR)}$
$L_1 \leftarrow R$
$R_1 \leftarrow L \oplus \rho(\langle 1\rangle \,\|\, R)$
$L_2 \leftarrow R_1$
$R_2 \leftarrow L_1 \oplus \rho(\langle 2\rangle \,\|\, R_1)$
$L_3 \leftarrow R_2$
$R_3 \leftarrow L_2 \oplus \rho(\langle 3\rangle \,\|\, R_2)$
Return $L_3 \,\|\, R_3$

G2 G3

$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(LR)}$
$L_1 \leftarrow R$
If $\mathtt{F}[1, R] = \perp$ then
  $\mathtt{F}[1, R] \leftarrow\!\!\$\ \{0,1\}^n$
$R_1 \leftarrow L \oplus \mathtt{F}[1, R]$
$L_2 \leftarrow R_1$
$X_2 \leftarrow\!\!\$\ \{0,1\}^n$
If $\mathtt{F}[2, R_1] \neq \perp$ then
  bad $\leftarrow$ true
  $\boxed{X_2 \leftarrow \mathtt{F}[2, R_1]}$
$\mathtt{F}[2, R_1] \leftarrow X_2$
$R_2 \leftarrow L_1 \oplus X_2$
$L_3 \leftarrow R_2$
$X_3 \leftarrow\!\!\$\ \{0,1\}^n$
If $\mathtt{F}[3, R_2] \neq \perp$ then
  bad $\leftarrow$ true
  $\boxed{X_3 \leftarrow \mathtt{F}[2, R_2]}$
$\mathtt{F}[3, R_2] \leftarrow X_3$
$R_3 \leftarrow L_2 \oplus X_3$
Return $L_3 \,\|\, R_3$

G4

$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$
Return b'

$\underline{\mathrm{Fn}(LR)}$
$L_1 \leftarrow R$
If $\mathtt{F}[1, R] = \perp$ then
  $\mathtt{F}[1, R] \leftarrow\!\!\$\ \{0,1\}^n$
$R_1 \leftarrow L \oplus \mathtt{F}[1, R]$
$L_2 \leftarrow R_1$
If $\mathtt{F}[2, R_1] \neq \perp$ then
  bad $\leftarrow$ true
$\mathtt{F}[2, R_1] \leftarrow 1$
$R_2 \leftarrow\!\!\$\ \{0,1\}^n$
$L_3 \leftarrow R_2$
$X_3 \leftarrow\!\!\$\ \{0,1\}^n$
If $\mathtt{F}[3, R_2] \neq \perp$ then
  bad $\leftarrow$ true
$\mathtt{F}[3, R_2] \leftarrow 1$
$R_3 \leftarrow\!\!\$\ \{0,1\}^n$
Return $L_3 \,\|\, R_3$

$$
\begin{aligned}
\mathbf{Adv}^{\mathrm{prp}}_{\mathcal{E}}(\mathcal{A}) &= \left|\Pr\left[\,\mathrm{PRP1}^{\mathcal{A}}_{\mathcal{E}}\,\right] - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&= \left|\Pr\left[\,\mathrm{G0}\,\right] - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&\leq \left|\Pr\left[\,\mathrm{G1}\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&\leq \left|\Pr\left[\,\mathrm{G2}\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&\leq \left|\Pr\left[\,\mathrm{G3}\,\right] + \Pr\left[\,\mathsf{bad}_3\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&\leq \left|\Pr\left[\,\mathrm{G4}\,\right] + \Pr\left[\,\mathsf{bad}_4\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&\leq \left|\Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right] + \frac{q^2}{2^{2n}} + \Pr\left[\,\mathsf{bad}_4\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) - \Pr\left[\,\mathrm{PRP0}^{\mathcal{A}}_{\mathcal{E}}\,\right]\right| \\
&= \frac{q^2}{2^{2n}} + \Pr\left[\,\mathsf{bad}_4\,\right] + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) \\
&\leq \frac{q^2}{2^{2n}} + \frac{2q^2}{2^{n}} + \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{B})
\end{aligned}
$$

Summary

- KR security necessary, not sufficient
- PRF / PRP security a primary target for block cipher security
  - Indistinguishable from random functions (resp. random permutations)
- Game-playing arguments:
  - Small transitions to probability space, described in code to aid precision
- Feistel networks allow building PRPs from PRFs

Towards message privacy definitions

$\underline{\mathrm{otIND}^{\mathcal{A}}_{\mathcal{E}}}$

$K \leftarrow\!\!\$\ \mathcal{K}$

$b \leftarrow\!\!\$\ \{0,1\}$

$b' \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Fn}}$

$\mathrm{Ret}\ (b = b')$

$\underline{\mathrm{Fn}(M_0, M_1)}$

$C \leftarrow E_K(M_b)$

$\mathrm{Ret}\ C$

$$\mathbf{Adv}^{\text{ot-ind}}_{\mathcal{E}}(\mathcal{A}) = 2 \cdot \Pr\left[\,\mathrm{otIND}^{\mathcal{A}}_{E} \Rightarrow \mathsf{true}\,\right] - 1$$

OTP otIND security

Theorem 1 *Let $\mathcal{E}$ be the OTP cipher. Then for any single-query* $\mathrm{otIND}_{\mathcal{E}}$*-adversary $\mathcal{A}$ it holds that* $\mathbf{Adv}_{E}^{\mathrm{ot\text{-}ind}}(\mathcal{A}) = 0$.

Theorem 1 *Let $\mathcal{E}$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ such that for any* otIND_{E}*-adversary $\mathcal{A}$ it holds that* $\mathbf{Adv}_{E}^{\mathrm{ot\text{-}ind}}(\mathcal{A}) = 0$. *Then $|\mathcal{K}| \geq |\mathcal{M}|$.*

Shannon's theorem

Theorem 1 *Let $\mathcal{E}$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ such that for any otIND_E-adversary $\mathcal{A}$ it holds that $\mathbf{Adv}_E^{\mathrm{ot\text{-}ind}}(\mathcal{A}) = 0$. Then $|\mathcal{K}| \geq |\mathcal{M}|$.*