EECS 575: Advanced Cryptography
Fall 2022
Lecture 11

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

Announcements

- Exam 1 is due tonight at 11pm

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

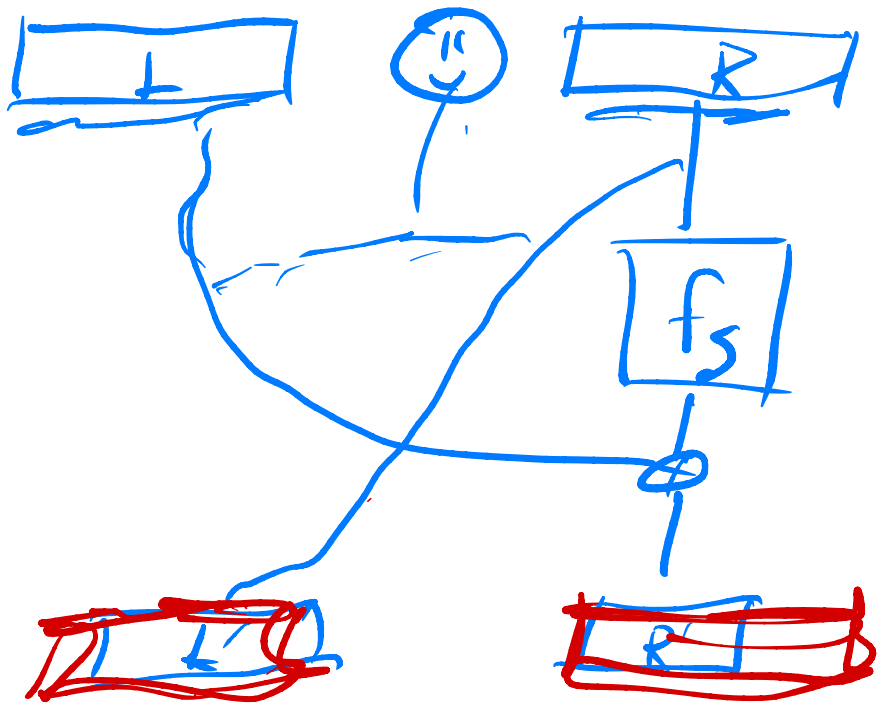
Pseudorandom permutations

↳ PRF that's a permutation

F is PRP family if

- PRF family
- $(F_S, F_S^{-1}) \approx_c (U_{Perm(n,n)}, U_{Perm(n,n)}^{-1})$

Pseudorandom permutations



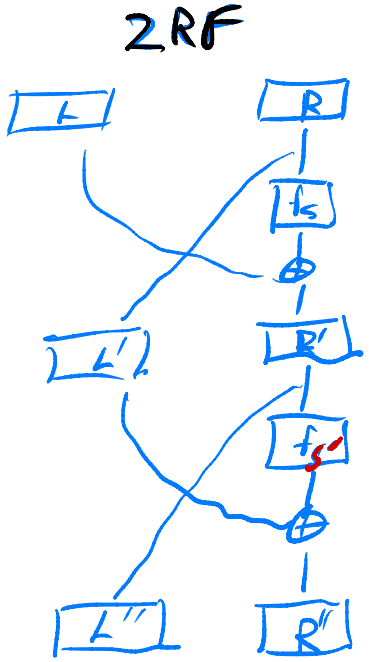
Mr. Feistel

"Round"

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

Feistel networks



Break this

Build distinguisher between 2RF and random permutation

$F_s(L, R) = (L \oplus f_s(R),$
$L' \oplus (f_{s'}(R'))$
$R \oplus (f_{s'}(R'))$

xor left halves, get $L \oplus L'$.

w.h.p., distinguish.

$\begin{cases} F_s(L, R) = (L \oplus f_s(R), R \oplus f_s(L \oplus f_s(R)) \; F_{s'}(L \oplus f_s(R)) \\ f_s(L', R) = L' \oplus f_s(R), \; \cdots \cdots \end{cases}$

Feistel networks

Thm: 3 rounds of Feistel $\Rightarrow$ weak PRP

4 rounds of " $\Rightarrow$ strong PRP

Luby-Rackoff

Feistel '71

DES is Feistel network '74

Differential cryptanalysis → DES

DeepCrack – key recovery

3DES – $f_{s'}(f_{s''}^{-1}(f_{s'}(m)))$

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

Symmetric-Key Encryption

- proving implications

OWF $\Rightarrow$ PRG $\Rightarrow$ PRF $\Rightarrow$ PRP

SKE

SKE

- Gen: outputs $k \in \{0,1\}^n$
- $Enc(k, m)$: outputs $c \in \{0,1\}^{\ell(n)}$
- $Dec(k, c)$: outputs $m \in \{0,1\}^n$

Perfect Secrecy: SKE is P.S. if $\forall m_0, m_1$, $\forall c$,

$$Pr[Enc(k, m_0) = c] = Pr[Enc(k, m_1) = c]$$

Symmetric-Key Encryption

Single-message indist. $\forall m_0, m_1$

$$\{K \leftarrow Gen : Enc(k, m_0)\} \approx_c \{k \leftarrow Gen : Enc(k, m_1)\}$$

Sanity check: P.S. $\Rightarrow$ SM1 ?

SKE is pseudorandom if $\forall m$,

$$\{k \leftarrow Gen : Enc(k, m)\} \approx_c \{U_{|c|}\}$$

Thm: If SKE pseudorandom, then SM1. $\forall m_0, m_1$

$$\{Enc(k, m_0)\} \approx_c \{U_{|c|}\} \approx_c \{Enc(k, m_1)\}$$

$$\{Enc(k, m_0)\} \approx_c \{Enc(k, m_0)\}$$

Symmetric-Key Encryption

SKE from a PRG G $\ell(n)$

- Gen: $k \leftarrow \{0,1\}^n$
- $Enc(k, m)$: $m \oplus G(k)$
- $Dec(k, c)$: $c \oplus G(k)$

$H_0 \approx_c H_1 \approx_s H_2$

PRG security — probability

- correctness
- Thm: SKE is pseudo random

IF G PRG, then SKE pseudo random

$\{Enc(k, m)\} = \{k \leftarrow \{0,1\}^n, m \oplus G(k)\} = H_0$

$H_1 = \{r \leftarrow \{0,1\}^{\ell(n)} : m \oplus r\}$

$H_2 = \{U_{\ell(n)}\}$

Symmetric-Key Encryption

Thm: ∃ SKE that aren't pseudorandom

Exercise!

Can we encrypt twice? No!

"pseudo" OTP

Single-message indistinguishability

Agenda for this lecture

- Announcements
- Recap from last time
- Feistel networks, Luby-Rackoff
- Symmetric encryption
- Indistinguishability under chosen-plaintext attack (IND-CPA)

IND-CPA

SKE IND-CPA if

$\{K \leftarrow Gen : C_0(\cdot,\cdot)\} \approx_c \{K \leftarrow Gen : C_1(\cdot,\cdot)\}$

$C_b(m_0, m_1)$: return $Ref\ Enc(k, m_b)$

- $q = poly(\lambda)$ oracle queries
- Encrypt any message of its choosing
- multiple msgs
- Adaptive!

IND-CPA

$\text{IND-CPA}^{\text{SKE}}_0(A)$:

$K \leftarrow \text{SKE.Gen}$

$b \leftarrow A^{\mathcal{O}_0(\cdot,\cdot)}(1^\lambda)$

Ret b

$\mathcal{O}_0(m_0, m_1)$:

Ret $\text{Enc}(K, m_0)$

$\text{IND-CPA}^{\text{SKE}}_1(A)$:

$K \leftarrow \text{SKE.Gen}$

$b \leftarrow A^{\mathcal{O}_1(\cdot,\cdot)}(1^\lambda)$

Ret b

$\mathcal{O}_1(m_0, m_1)$:

Ret $\text{Enc}(K, m_1)$

$$\left| \Pr[\text{INDCPA}^1_{\text{SKE}}(A) = 1] - \Pr[\text{INDCPA}^0_{\text{SKE}}(A) = 1] \right| = \text{negl}(n)$$

SKE Deterministic?

No! Must be randomized

An IND-CPA-secure scheme