EECS 575: Advanced Cryptography
Fall 2021
Lecture 10

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Announcements

- Homework 3 is due tonight
- Take-home exam 1 will be released today, due 10/11. Good luck!

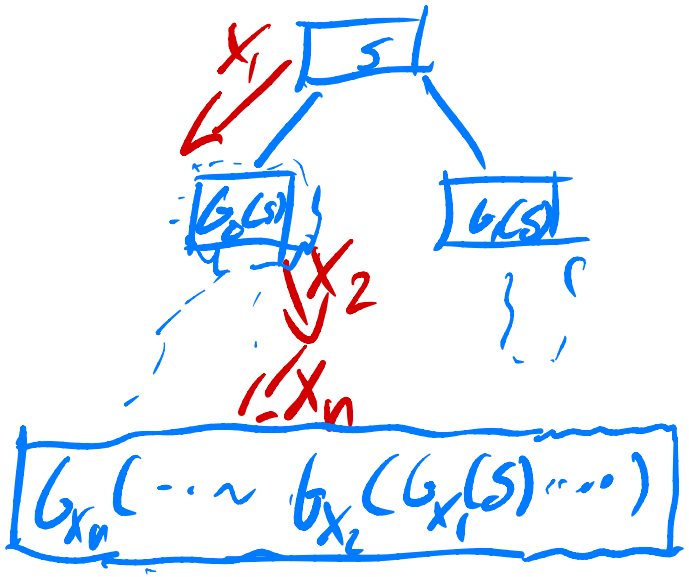
Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Recap from last time

Pseudorandom functions

* GGM construction



$F_s(x_1 \cdots x_n)$

* puncturable PRF -> "split" the key, delegate comp. PRF to different parties

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Pseudorandom Permutations

PRF with injectivity + surjectivity

A func. family $\{F_s : \{0,1\}^n \to \{0,1\}^n\}$ is a PRP family if:

* Efficient to compute ∃ det. ppt F s.t. $F(s,x) = f_s(x)$ $\forall s, x$

(strong / weak)

$|F_s| \simeq 2^n$

* Pseudorandomness

$|\mathrm{Perm}(\{0,1\}^n)| = 2^n!$

$$\left| \Pr_{f \leftarrow \{f_s\}}\left[A^{F, F^{-1}}(1^n) = 1\right] - \Pr_{F \leftarrow \mathrm{Perm}(\{0,1\}^n)}\left[A^{F, F^{-1}}(1^n) = 1\right] \right| = \mathrm{negl}(n)$$

All perms on n bits.

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Feistel Networks

Theorem: If PRFs exist, then PRPs exist

(Luby-Rackoff)

Idea: Feistel network transforms PRF into PRP

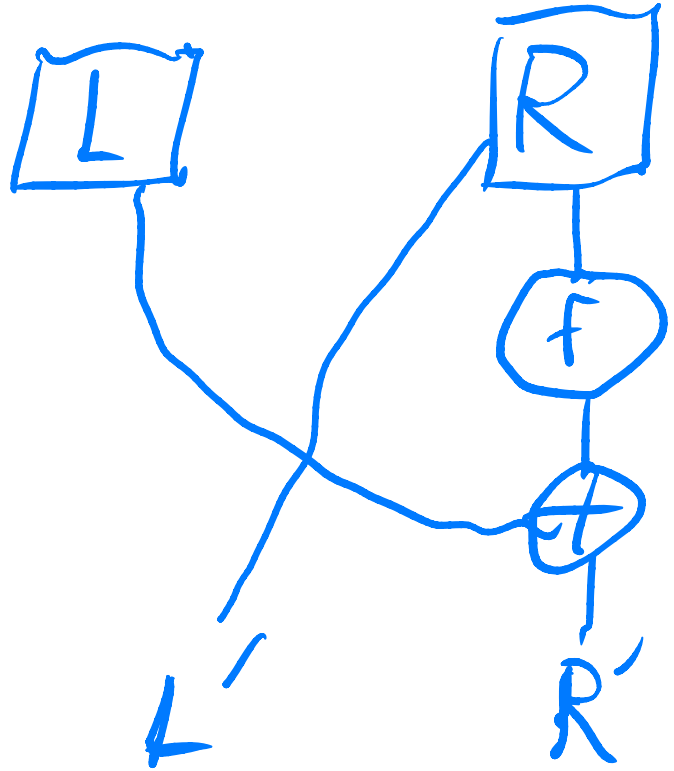
* Feistel networks predate Luby-Rackoff by ≈20 years!

Feistel Networks

Feistel rounds: given $F: \{0,1\}^n \to \{0,1\}^n$, build $D_f: \{0,1\}^{2n} \to \{0,1\}^{2n}$ as

$$D_f(L,R) = (R, L \oplus F(R))$$

in picture:

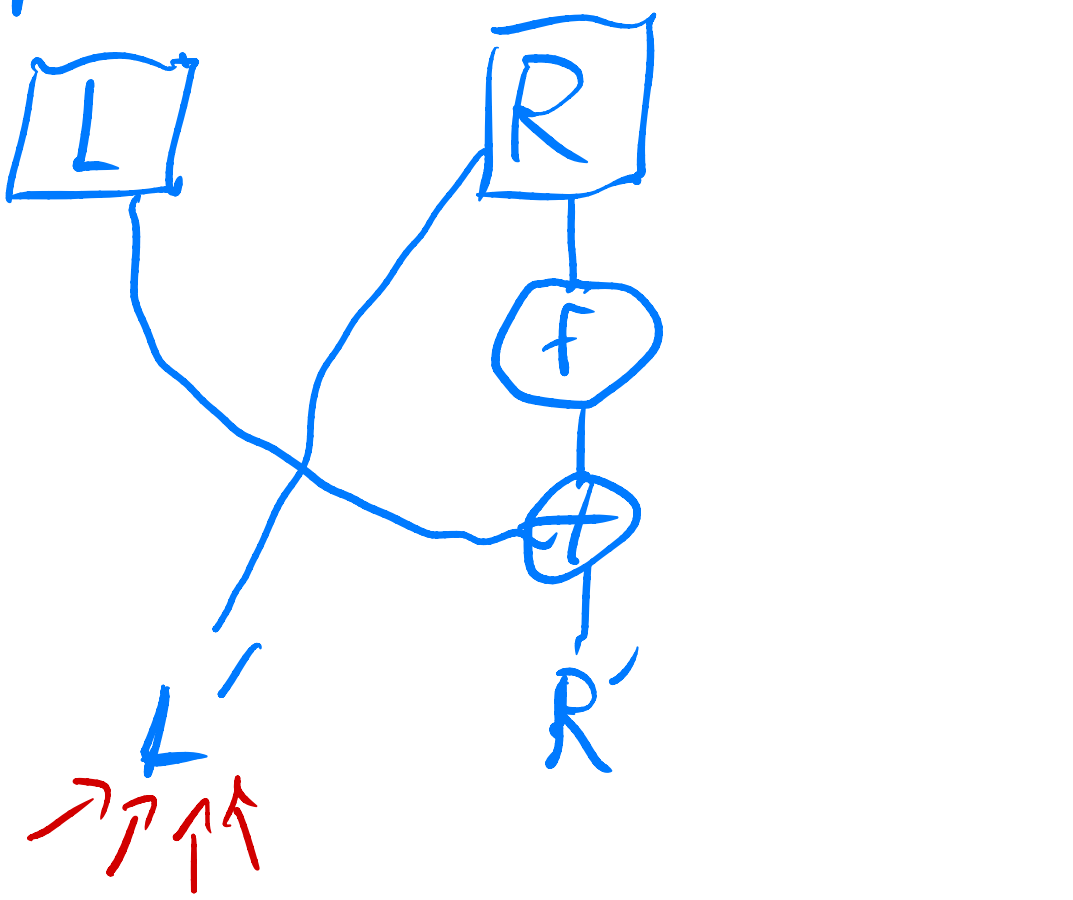


Question: What is D_f^{-1}?

$$D_f^{-1}(L',R') = (F(L') \oplus R', L')$$

Feistel Networks

$D_f(L, R) = (R, L \oplus F(R))$



Question:

Is D_f a PRP if f is a PRF?

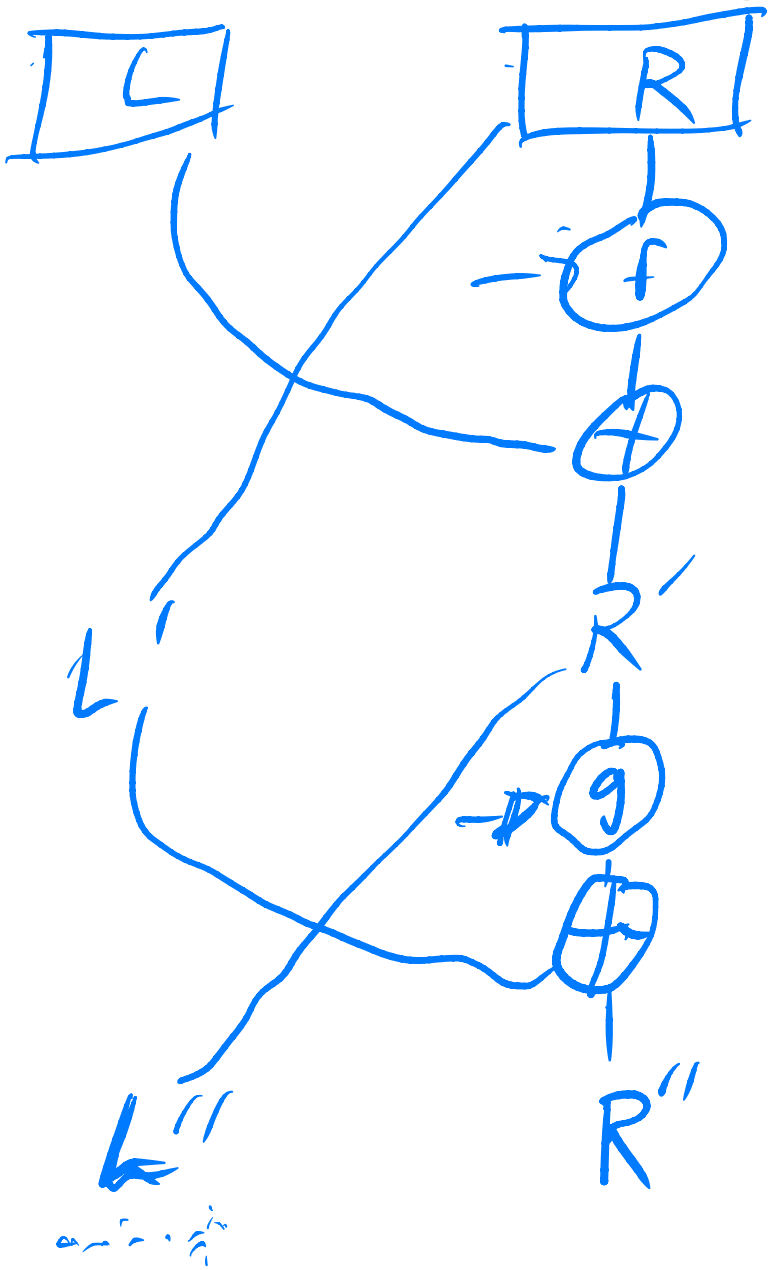
\# Efficient to compute ✓

\# Pseudorandomness? X

No! Left half of $D_f(L, R) = R$.

Only happens for negl. small fraction of all perms!

Feistel Networks



$D_f'(L,R)$

Question:

Is D_f' a PRP iff f is a PRF?

* Efficient ✓
* pseudorandom ✗

Still no!

Evaluate D_f' at two points where $L_1 \neq L_2$ but $R_1 = R_2$

$\text{Left}(D_f'(L_1,R)) \oplus \text{Left}(D_f'(L_2,R))$

$= L_1 \oplus f(R) \oplus L_2 \oplus f(R)$

$= L_1 \oplus L_2$

Happens w/ random perm only w/ negl prob.

Luby-Rackoff

Theorem: 3 rounds of Feistel is weak PRP,
4 rounds " " strong PRP.
needs 3 (resp.) independent PRFs as round funcs

Proof:

Somewhat complicated.

Cryptographers don't agree about correctness of Luby-Rackoff!

(Result is true)

History ("*Horst*-ory"!!) of Feistel Networks

Inventor of Feistel Networks was Horst Feistel

* IBM cryptographer. started w/ block ciphers in early 70s
  In '72/'73, published "Lucifer" at IBM
* Solicited proposals for Block Cipher designs
  IBM submits Lucifer, NSA likes it.
  NSA + IBM work together to standardize;
  eventually become DES (1977)
* NSA requested 2 changes:
  (1) change to round funcs ← why?? 1990/91 Biham/Shamir Differential crypt.
  (2) reducing key size to 56-bit key

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom permutations
- Feistel networks, the Luby-Rackoff result
- Security for symmetric-key encryption

Symmetric-Key Encryption

Sym-key enc is three algos:

* Gen : randomized, outputs key
* $Enc(K, X)$: randomized, encrypts X with K
* $Dec(K, C)$: deterministic, decrypts C

Perfect secrecy: If $m_0, m_1, \bar{c}$

$$\Pr_{K \leftarrow Gen}[Enc_K(m_0) = \bar{c}] = \Pr_{K}[Enc_K(m_1) = \bar{c}]$$

Symmetric-Key Encryption

Computational analog to Info-theoretic security notion

Single-message indistinguishability $\forall m_0, m_1$,

$$\{k \leftarrow Gen : Enc_k(m_0)\} \approx_c \{k \leftarrow Gen : Enc_k(m_1)\}$$

Lemma: Let (Gen, Enc, Dec) be a sym. enc. scheme.
If $\{k \leftarrow Gen : Enc_k(m)\}$ is pseudo random
$(\forall m)$ over ct. space, then scheme is SM1.

Proof:

$$\{Enc_k(m_0)\} \approx_c \{U(l)\} \approx_c \{Enc_k(m_1)\}$$

↑ ↑

Symmetric-Key Encryption

Describe a sym-key enc scheme. Let G is a PRG. output space $\ell(n)$

* $Gen: k \leftarrow \{0,1\}^n$
* $Enc_k(x): x \oplus G(k)$
* $Dec_k(c): c \oplus G(k)$

This has pseudorandom ciphertexts $\Rightarrow$ SUI.