CSE 575: Advanced Cryptography
Fall 2024
Lecture 8

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

Announcements

- HW2 online, due 9/26

Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

Analyzing GGM

$G : \{0,1\}^n \to \{0,1\}^{2n}$

$G(s) = G_0(s) \| G_1(s)$

$f_s(x_1 \cdots x_n)$:

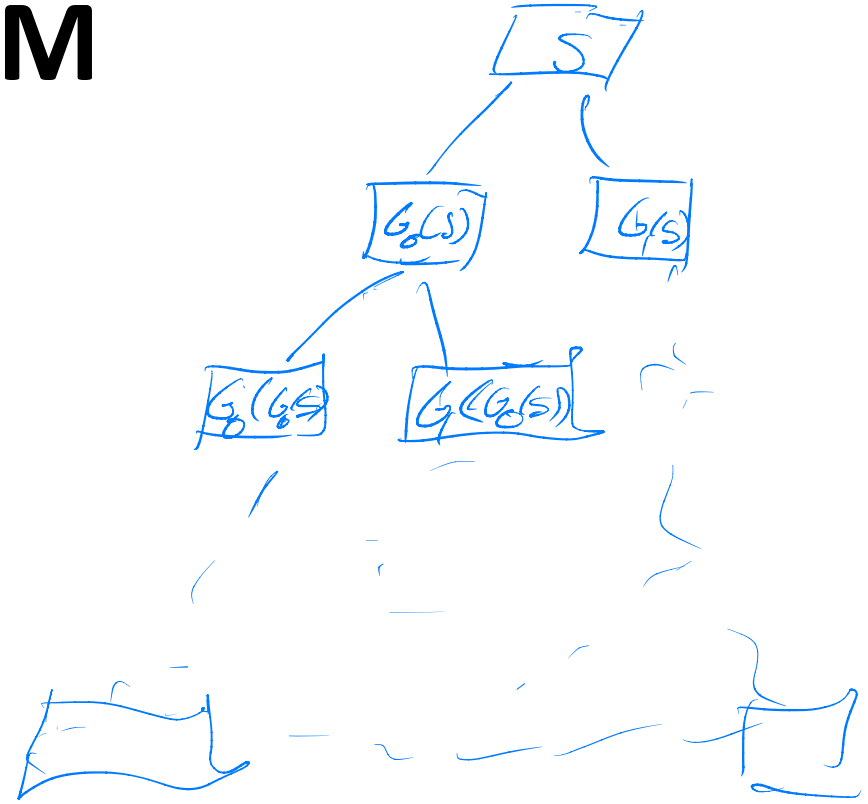
Ret $G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(s)\cdots))$

$H_0 := f_s$

$H_1 := G_{x_n}(\cdots G_{x_2}(s_{x_1})\cdots)$

$H_i := G_{x_n}(\cdots G_{x_{i+1}}(s_{x_1 \cdots x_i})\cdots)$

$H_n := U_{n \to n}$



Analyzing GGM

Analyzing GGM

$G : \{0,1\}^n \to \{0,1\}^{2n}$

$G(s) = G_0(s) \| G_1(s)$

$f_s(x_1 \cdots x_n)$:

Ret $G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(s)\cdots))$

$H_0 := f_s$

$H_1 := G_{x_n}(\cdots G_{x_2}(s_{x_1})\cdots)$

$H_i := G_{x_n}(\cdots G_{x_{i+1}}(s_{x_1 \cdots x_i})\cdots)$

$H_n := U_{n\to n}$

$S^{\mathcal{A}}(s_0^0, s_1^0), (s_0^1, s_1^1))$:

$T \leftarrow []$; $j := 0$

$b \leftarrow \mathcal{A}^{f_{s:m}}$

Ret b

$f^{i}_{s:m}(x_1 \cdots x_n)$:

If $T[x_1 \cdots x_i] = \perp$

$T[x_1 \cdots x_i] = (s_0^j, s_1^j)$

$j += 1$

$s_0, s_1 = T[x_1 \cdots x_i]$

Ret $G_{x_{i+1}} \cdots G_{x_{i+2}}(s_{x_{i+1}})\cdots)$

Exercise: S's input dists are $\approx_c$ ☒

Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

Pseudorandom permutations (PRP)

Family $F_S : \{0,1\}^n \to \{0,1\}^n$ is PRP if

- Easy to compute/sample
- permutation $\forall S$
- pseudorandom

$$\left| \Pr_{S \leftarrow \{0,1\}^s}[A^{F,F^{-1}} = 1] - \Pr_{F \leftarrow \text{Perms}(n)}[A^{f,f^{-1}} = 1] \right| = \text{negl}(n)$$

Strong PRP

PRPs = block ciphers (e.g. AES)

Feistel networks

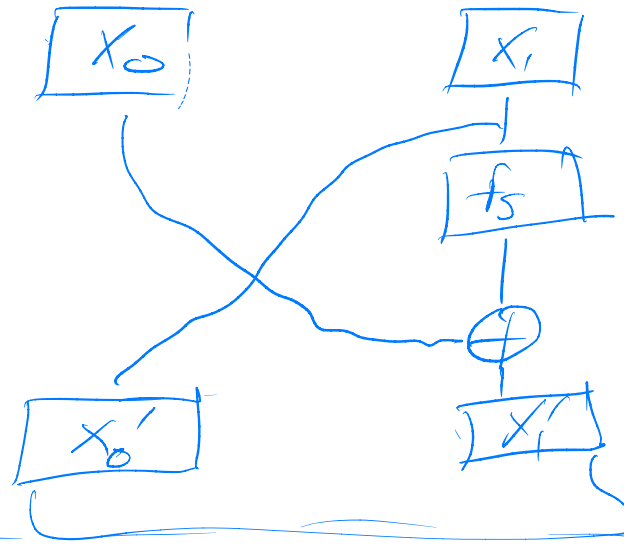
$f_s : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

$FR[f_s](X_0, X_1)$:

$(X_1, X_0 \oplus f_s(X_1))$

$FR^{-1}[f_s](X_0, X_1)$:

$(X_1 \oplus f_s(X_0), X_0)$



- Luby-Rackoff

(4) 3-round Feistel is strong PRP

Exercises:

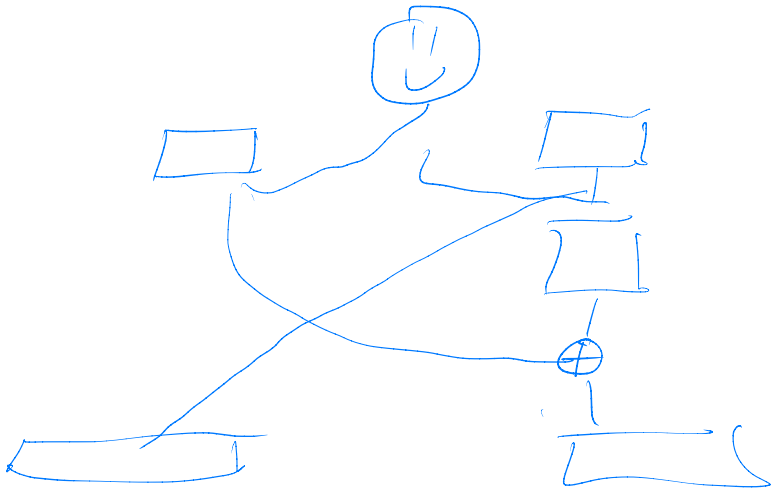
- 1 round Feistel not PRP
- 2 round not PRP

Horst Feistel: IBM cryptographer [Lucifer/DES]

DeepCrack '97

DES key recovery quickly!

Mr. Feistel



Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

Symmetric Encryption (SKE)

- OWF $\xrightarrow[\text{HILL}]{\text{GL}}$ PRG $\xrightarrow[\text{GGM}]{}$ PRF $\xrightarrow[\text{Rackoff}]{\text{Luby}}$ PRP
- Now, build SKE 🙂🙂!
- SKE
  - Gen: output $\{0,1\}^n$
  - Enc(K, m): output $c \in \{0,1\}^{\ell(n)}$
  - Dec(K, c): output $m \in \{0,1\}^n$

Correctness:
$\forall K, m$,
$\text{Dec}(k, E_K(K, m)) = m$

Security for SKE

Perfect secrecy: $\forall m_0, m_1, c$,

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

Single-message indist.

$\forall m_0, m_1$,

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

Alternative def'n: pseudorandomness

$\forall m$,

$$\{Enc(K, m)\}_{K \leftarrow Gen} \approx_c \{U_{\ell(n)}\}$$

Security for SKE

Thm: If SKE pseudorandom, SKE is SMI.

Proof: $\forall m_0, m_1,$

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

Exercise: show reverse is not true.

Security for SKE

Let $G: \{0,1\}^{n/2} \to \{0,1\}^n$

- Gen: output $k \leftarrow \{0,1\}^{n/2}$
- Enc(k, m): Ret $m \oplus G(k)$
- Dec(k, c): Ret $c \oplus G(k)$

Thm: IF G PRG, SKE pseudorandom

Proof: on wednesday

Agenda for this lecture

- Announcements
- Analyzing GGM
- Pseudorandom permutations
- Symmetric encryption
- IND-CPA security

IND-CPA security for SKE