# EECS 575: Advanced Cryptography
# Fall 2022
# Lecture 10

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

# Announcements

- Exam 1 is online, due next Monday at 11pm EST
- VictorCrypto meeting tomorrow night!

victorcrypto.org

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

# Pseudorandom functions and GGM

$F_S(x_1 \cdots x_n) = G_{x_n}(\cdots G_{x_1}(S)\cdots)$

$G(S) : \{0,1\}^n \rightarrow \{0,1\}^{2n}$

$G_0(S) : G(S)_L$

$G_1(S) : G(S)_R$

# Pseudorandom functions and GGM

$G^c(A)$:

$(s_0^1, s_1^1), \ldots, (s_0^q, s_1^q) \leftarrow$

$b \leftarrow A^F$

Ret $b$

$F(x_1 \ldots x_n)$:

$j \leftarrow 1$; $T \leftarrow []$

$P \leftarrow x_1 \ldots x_i$

If $T[P] = \perp$

$T[P] \leftarrow (s_0^j, s_1^j)$

$j += 1$

$s_0^P, s_1^P \leftarrow T[P]$

Ret $G_{x_i}(\ldots G_{x_{i+1}}(s_{x_i}^P)\ldots)$

$H_i$: GGM, but $i$th level of tree is random strings

$H_{i+1}$: " but $i+1$ level is random

$H_0 \approx_c H_1$

Because $G$ is PRG, can build simulator & use composition Lemma

# Pseudorandom functions and GGM

Build simulator for $i$/$i+1$ hybrid

$\$_i^{\mathcal{A}}((s_0^1, s_1^1) \cdots (s_0^q, s_1^q))$:

$j = 1$
$T = []$
$b \leftarrow \mathcal{A}^{FSim}$ ← oracle: opaque black box implementing $f$
Ret $b$

$FSim(x_1 \cdots x_n)$:

If $T[x_1 \cdots x_i] = \perp$
  $T[x_1 \cdots x_i] \leftarrow (s_0^j, s_1^j)$
  $j = j + 1$
$p = x_1 \cdots x_i$
$(s_{0,p}, s_{1,p}) \leftarrow T[p]$
Ret $G_{x_n}(\cdots G_{x_{i+2}}(s^p_{x_{i+1}}) \cdots)$

Claim: If the $(s_0^i, s_1^i)$s are PRG outputs, $\$_i = H_i$.
If they're **fresh** strings $\$_i = H_{i+1}$

# Pseudorandom functions and GGM

$S_0^P \| S_1^P = G(t)\ ;\ t \leftarrow U_n$

$G_{x_n}(\cdots G_{x_{i+2}}(G_{x_{i+1}}(t)\cdots)$ ← $i+1^{th}$ level is PRG outputs — $H_i$

$G_{x_1}(\cdots G_{x_{i+2}}(S_{x_{i+1}})\cdots)$ ← $i+1^{th}$ level is random strings — $H_{i+1}$

$H_i \approx_c H_{i+1}$

Exercise (Hybrid): Need to show — If $G$ PRG $(G(s_1), \ldots G(s_q)) \approx (U_{2n}, \ldots, U_{2n}^q)$

# Pseudorandom functions and GGM

**Thm:** If $G$ PRG, then

$$\underbrace{(G(U_n)^1 \cdots G(U_n)^q}_{H_0} \approx_c (U_{2n}^1, \ldots, U_{2n}^q)$$

**Proof:** Hybrid lemma

$H_0$: $(G(U_n) \cdots G(U_n))$

$H_i$: $(\underbrace{U_{2n} \cdots U_{2n}}_{i}, G(U_n) \cdots G(U_n))$

$H_q$: $(U_{2n} \cdots U_{2n})$

$\$(G(U_n)) = H_{i-1}$

$\$(U_{2n}) = H_i$.

If $S_0 \| S_1 = G(U_n)$ $H_{i-1} \approx_c H_i$ by composition

$(\underbrace{U_{2n} \cdots}_{i-1} \underbrace{G(U_n) \cdots G(U_n)}_{q-i+1}$

$\$(S_0, S_1)$:

Ret $(\underbrace{U_{2n}^1, \ldots}_{i-1}, \underbrace{U_{2n}^i}_{i}, \underbrace{(S_0, S_1)}_{i}, \underbrace{G(U_n)^{i+1} \cdots G(U_n)^q}_{q-i})$

\underbrace{ }

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

# Analyzing GGM

See prev.

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

# Pseudorandom Permutations (PRP)

What is PRP? PRF that is permutation!

Family $F = \{ f_s : \{0,1\}^n \to \{0,1\}^n \}_{s \in \{0,1\}^n}$

Strong

is a PRP family if

- Efficiency (incl inverses)
- permutivity

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

If $\forall$ nuppt $A$, is negl, $F$ is Strong PRP family

# Agenda for this lecture

- Announcements
- Recap from last time
- Finishing up GGM analysis
- Pseudorandom permutations
- Feistel networks, Luby-Rackoff

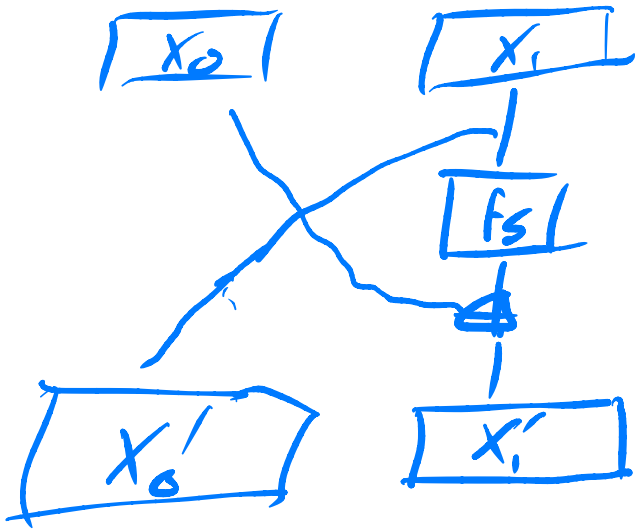
# Feistel Networks

Use PRFs!

Feistel round $F_s : \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}$

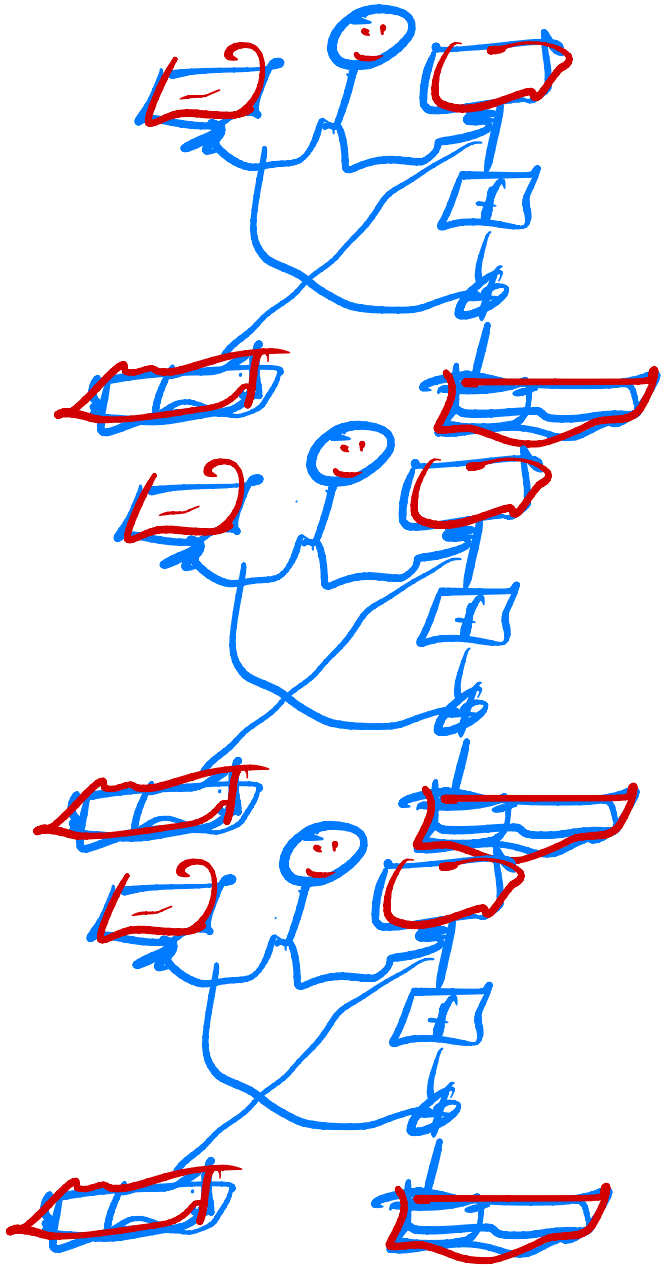
$FR[f_s](x_0, x_1)$: $(x_1, x_0 \oplus f_s(x_1))$

$FR^{-1}[f_s](x_0, x_1)$: $(x_1 \oplus f_s(x_0), x_0)$




Exercise: One round is not PRP
Two round is not PRP

# Feistel Networks



Mr. Feistel and his two friends!

With that friend, strong!