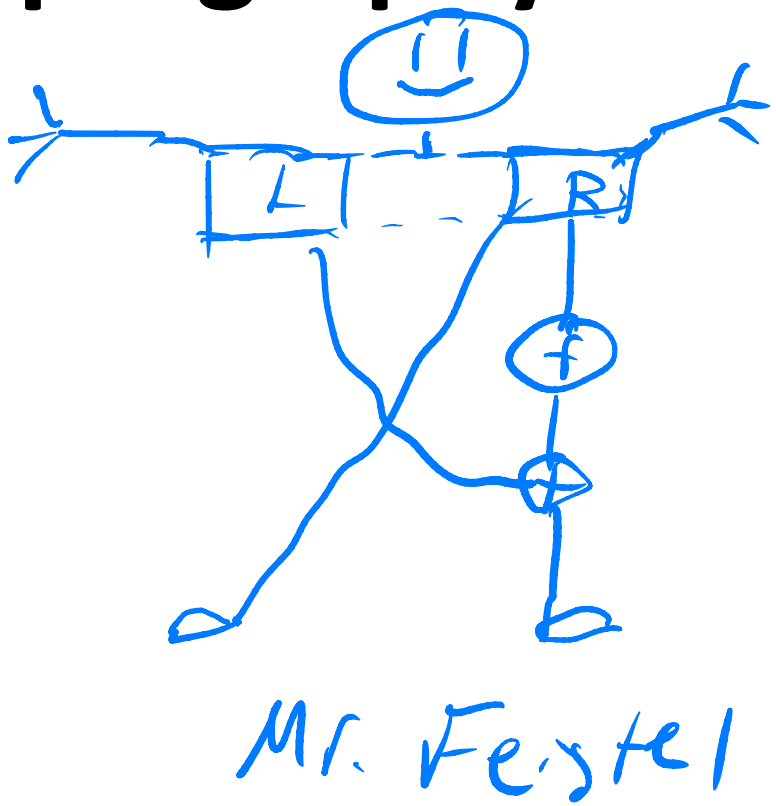
EECS 575: Advanced Cryptography
Fall 2021
Lecture 11



Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

Announcements

- Take-home exam 1 is due 10/11.
- Anthony will have office hours today at 2pm

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

Recap from last time

* Pseudorandom Permutation

  Family of permutations, indexed $s \in \{0,1\}^\lambda$

  * Efficient to evaluate

  * Pseudorandomness

    Hard for ppt distinguisher to differentiate

    F_s, F_s^{-1} or R, R^{-1}

    F_s, F_s^{-1}: Sample from family

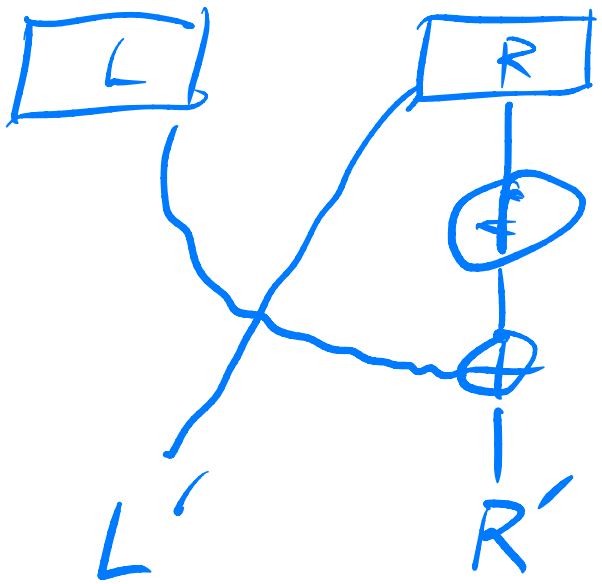
    * Choice from 2^λ possibilities

    R, R^{-1}: uniform random permutation on n bits

    * Choice from $2^n!$ possibilities

Recap from last time

* Feistel network



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

* Security of Feistel:

1 rd / 2 rds Not secure

Luby/Rackoff: 3 rds gives weak PRP → only secure if adversary can't call f_s^{-1}

4 rds gives strong PRP

Recap from last time

* Security for symmetric-key encryption
  - Single-message indist.
    $\forall m_0, m_1$

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

  - Compare to perfect-secrecy

* pseudorandomness: $\forall m$

$$\{k \leftarrow Gen : Enc_k(m)\} \approx_c \{U_{|C|}\}$$

(ciphertext space)

* pseudorandomness $\Rightarrow$ sml

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

Security for Symmetric-Key Encryption

Multi-message indist

* Symkey scheme: $Enc_K(m) = m \oplus G(K)$

"short" OTP. Not secure for multiple encryptions!

$Enc_K(m_0) \oplus Enc_K(m_1) = m_0 \oplus m_1$

English text: use "crib dragging"

* MMI: Enc. scheme is mmi if for $q = poly(\lambda)$,

$\forall (m_0, \ldots, m_q), (m_0', \ldots, m_q') \in \mathcal{M}^q$ ← "choose" non-adaptively

$\{Enc_K(m_0), \ldots, Enc_K(m_q)\} \approx_c \{Enc_K(m_0'), \ldots, Enc_K(m_q')\}$

- over $K \leftarrow Gen$ and randomness of Enc.

Security for Symmetric-Key Encryption

* Indist. Chosen plaintext attack (IND-CPA):

  Enc. scheme is IND-CPA secure if

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

On input m_0, m_1, Returns $Enc_K(m_0)$

input m_0, m_1, Returns $Enc_K(m_1)$

* Adaptive! Requires randomized encryption.

* Exercise: Show IND-CPA $\Rightarrow$ MM, but not the other way.

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

IND-CPA-secure encryption from a PRF

Scheme PRFEnc: Let $\{F_K\}$ be a func. family from $\{0,1\}^n \to \{0,1\}^n$

$\mathcal{M} = \{0,1\}^n$, $\mathcal{C} = \{0,1\}^{2n}$

* Gen: $K \leftarrow Gen$, $k \in \{0,1\}^n$
* $Enc(K, m)$:
  - $r \leftarrow \{0,1\}^n$
  - Returns $(r, m \oplus f_K(r))$

* $Dec(K, (r, c))$: Return $c \oplus f_K(r)$

IND-CPA-secure encryption from a PRF

Theorem: If F_s is PRF fam. w., PRFEnc is IND-CPA.

PRFEnc

- $\mathcal{M} = \{0,1\}^n$, $\mathcal{C} = \{0,1\}^{2n}$
- * Gen: $K \leftarrow Gen$, $k \in \{0,1\}^n$
- * $Enc(K, m)$:
  - $r \leftarrow \{0,1\}^n$
  - Returns $(r, m \oplus f_K(r))$
- * $Dec(K, (r, c))$: Return $c \oplus f_K(r)$

Proof Idea: Two hybrid dists.

One reduces to PRF,

Second replaces $Enc(\cdot)/\mathcal{E}(\cdot,\cdot)$ with random strings

Will show $CPA_0 \approx_c U(\cdot), U(\cdot,\cdot)$

$CPA_0/CPA_1 \approx_c U(\cdot), U(\cdot,\cdot)$

$CPA_0 \approx_c U(\cdot), U(\cdot,\cdot) \approx_c CPA_1$

By hybrid lemma, $CPA_0 \approx_c CPA_1$

$Enc_K(\cdot), \mathcal{E}_0(\cdot,\cdot)$ $\quad$ $Enc_K(\cdot), \mathcal{E}_1(\cdot,\cdot)$

IND-CPA-secure encryption from a PRF

PRFEn

$\mathcal{M} = \{0,1\}^n$, $\mathcal{C} = \{0,1\}^{2n}$

* Gen: $K \leftarrow Gen$, $k \in \{0,1\}^n$
* Enc(K, m):
  - $r \leftarrow \{0,1\}^n$
  - Returns $(r, m \oplus f_K(r))$
* Dec(K, (r, c)): Return $c \oplus f_K$

Lemma: $CPA_0 \approx_c U(\cdot), U(\cdot,\cdot)$

Proof: Three hybrids:

* H_0: Same as CPA_0
* H_1: CPA_0 except using random function
* H_2: Enc(c) output random in $\{0,1\}^{2n}$

$H_0^{\mathcal{A}}$:

$K \leftarrow Gen$

Return $\mathcal{A}^{Enc_K(\cdot),\, C_0(\cdot,\cdot)}(1^n)$

$Enc_K(m)$:

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

Ret $(r, m \oplus f_K(r))$

$C_0(m_0, m_1)$:

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

Ret $(r, m_0 \oplus f_K(r))$

$H_1^{\mathcal{A}}$:

$F \leftarrow Func(n)$

Return $\mathcal{A}^{Enc_F(\cdot),\, C_0(\cdot,\cdot)}(1^n)$

$Enc_F(m)$:

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

Ret $(r, m \oplus F(r))$

$C_0(m_0, m_1)$:

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

Ret $(r, m_0 \oplus F(r))$

$H_2^{\mathcal{A}}$:

Return $\mathcal{A}^{Enc(\cdot),\, C_0(\cdot,\cdot)}(1^n)$

$Enc(m)$:

$c \leftarrow U_{2n}$

Ret c

$C_0(m_0, m_1)$:

$c \leftarrow U_{2n}$

Ret c

IND-CPA-secure encryption from a PRF

* Show $H_0 \approx_c H_1$. use simulator. (Exercise)
* Show $H_1 \approx_c H_2$. Need Difference lemma:

Let A, B, F be events in prob. space; $Pr[A \wedge \neg F] = Pr[B \wedge \neg F]$,

then $|Pr[A] - Pr[B]| \leq Pr[F]$. (Exercise)

→ upper-bound

$$|Pr[H_1^A \Rightarrow 1] - Pr[H_2^A \Rightarrow 1]| \leq Pr[\text{collision in } r \leftarrow \{0,1\}^n] \leq \frac{q^2}{2^n}$$ by union bound.

H_0^A:

$K \leftarrow Gen$

Return $A^{Enc_K(\cdot),\, Gc(\cdot,\cdot)}(1^n)$

$Enc_K(m)$:

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

Ret $(r, m \oplus f_K(r))$

$Gc(m_0, m_1)$:

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

Ret $(r, m_0 \oplus f_K(r))$

H_1^A:

$F \leftarrow Funcs(n)$

Return $A^{Enc_F(\cdot),\, Gc(\cdot,\cdot)}(1^n)$

$Enc_F(m)$:

what if this repeats?

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

Ret $(r, m \oplus F(r))$

$Gc(m_0, m_1)$:

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

Ret $(r, m_0 \oplus F(r))$

H_2^A:

Return $A^{Enc(\cdot),\, Gc(\cdot,\cdot)}(1^n)$

$Enc(m)$:

$c \leftarrow U_{2n}$

Ret c

$Gc(m_0, m_1)$:

$c \leftarrow U_{2n}$

Ret c

Agenda for this lecture

- Announcements
- Recap from last time
- Security for symmetric-key encryption
  - Multiple-message indistinguishability
  - indistinguishability under chosen-plaintext attack (IND-CPA)
- IND-CPA-secure encryption from a PRF
- Other “modes of operation” for PRFs and PRPs

Modes of operation for PRFs and PRPs