EECS 575: Advanced Cryptography
Fall 2022
Lecture 12

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

Announcements

- HW3 is out, due 10/21

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

Indistinguishability under chosen-plaintext attack

$SKE = (Gen, Enc, Dec)$

$\underline{IND\text{-}CPA\,O^{?}}$

$K \leftarrow Gen$

$b \leftarrow A^{Enc(k,\cdot),\, C_b(\cdot,\cdot)}$

$\underline{C_b(m_0, m_1):}$

$Ret\ Enc(k, m_b)$

$\underline{IND\text{-}CPA\,1^{\lambda}:}$

$K \leftarrow Gen$

$b \leftarrow A^{Enc(k,\cdot),\, C_1(\cdot,\cdot)}$

$\underline{C_1(m_0, m_1):}$

$Ret\ Enc(k, m_1)$

(IND-CPA vs SM1 vs. perfect secrecy?

SKE is IND-CPA if $\forall$ nupt A,

$$\left| Pr[IND\text{-}CPA O^{\lambda} = 1] - Pr[IND\text{-}CPA 1^{\lambda} = 1] \right| = negl(\lambda)$$

$\{Enc(k,\cdot)\ C_0(\cdot,\cdot)\} \approx_c \{Enc(k,\cdot),\ C_1(\cdot,\cdot)\}$

Indistinguishability under chosen-plaintext attack

	IND-CPA	SMI	Perfect Secrecy
(only) Computational	✓	✓	✗
adaptive	✓	✗	✗
use k many times	✓	✗	✗
$\lvert R\rvert < \lvert M\rvert$	✓	✓	✗
Dec oracle?	✗	✗	✗

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

An IND-CPA scheme

f_K is PRF family $\quad F_K : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

SKE[f_K]:

- Gen: outputs $K \leftarrow$ PRF.Gen
- Enc(K, m):
  $r \leftarrow \{0,1\}^n$
  Ret $(r, m \oplus F_K(r))$
- Dec(K, C=(r, c')):
  Ret $c' \oplus F_K(r)$

Exercise: extend Schemes proof to poly-n bit inputs

Counter mode! ∫GCM chacha20

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

Analyzing the scheme

Thm: $SKE[F_s]$ is IND-CPA secure

- Gen: outputs $k \leftarrow$ PRF.Gen
- Enc(k, m):
  $r \leftarrow \{0,1\}^n$
  Ret $(r, m \oplus F_k(r))$
- Dec(k, c = (r, c')):
  Ret $c' \oplus F_k(r)$

Sketch:

1. Exchange f_s with random f'n
   → $R \leftarrow U_{n,n}$ Enc(k, m):
   $r \leftarrow \{0,1\}^n$
   Ret $(r, R(r) \oplus m)$
2. Collisions in r break !
3. All oracles output random b.'s

Analyzing the scheme

H_0 : IND-CPA$^{\mathcal{A}}_{SKE[f_s]}$

H_1 : IND-CPA$^{\mathcal{A}}_{SKE[R]}$

H_2 : IND-CPA$^{\mathcal{A}}_{U(\cdot),\, U(\cdot,\cdot)}$

H_2 doesn't depend on $O/1$.

Can get to IND-CPA1

Analyzing the scheme

$H_{1,0}$

IND-CPA$\mathcal{O}^{\mathcal{A}}$:

$K \leftarrow$ PRF.Gen

$b \leftarrow \mathcal{A}^{Enc(\cdot), C_0(\cdot,\cdot)}$

Ret b

Enc(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 $(r, m_0 \oplus F_K(r))$

$H_{1,\mathcal{A}}$:

$T \leftarrow []$

$b \leftarrow \mathcal{A}^{Enc(\cdot), C_0(\cdot,\cdot)}$

Ret b

Enc(m):

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

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

$C_0(m_0, m_1)$:

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

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

R(x):

If $T[x] = \perp$
$T[x] \leftarrow \{0,1\}^n$

Ret $T[x]$

→ Lazy-sample random f'n

$H_0 \approx_c H_1$

Analyzing the scheme

Show $H_0 \approx_c H_1$ by simulator $\mathcal{A}$:

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

$b \leftarrow \mathcal{A}^{Enc, \overline{C_0}}$

$\overline{Enc}(m)$:

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

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

$\overline{C_0}(m_0, m_1)$:

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

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

If F is f_K, PRF

$\mathcal{A}$ in H_0

If F is rand. f'n,

$\mathcal{A}$ in H_1

By composition lemma,

$H_0 \approx_c H_1$

Agenda for this lecture

- Announcements
- Recap from last time
- An IND-CPA symmetric-key encryption scheme
- Analyzing the scheme
- Message authentication

Message authentication