CSE 575: Advanced Cryptography
Fall 2024
Lecture 10

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

Announcements

- HW2 online, due TODAY
- I have OH right after class

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

Continuing SKE analysis

$F_s : \{0,1\}^n \to \{0,1\}^n$

CTR[f]

- Gen: $k \leftarrow \{0,1\}^n$
- Enc(k, m):
  $r \leftarrow \{0,1\}^n$
  Ret $r, f_k(r) \oplus m$
- Dec(k, c):
  Parse c as r, c_0
  Ret $c_0 \oplus f_k(r)$

Thm: If f_k PRF, then CTR[f] IND-CPA

Proof:

H_0: IND-CPA$_{CTR[f]}$

H_1: Same except f is replaced RF

H_2: H_1 except □ replaced with unif. random bits

H_3: H_2 except oracle outputs random bits

Continuing SKE analysis

$\underline{IND\text{-}CPA^{\mathcal{A}}_{SKE}}$:

$K \leftarrow Gen$

$b \leftarrow \mathcal{A}^{\mathcal{E}_0(\cdot,\cdot)}$

Ret b

$\underline{\mathcal{E}_0(m_0, m_1)}$:

Ret $SKE.Enc(K, m_0)$

$\underline{IND\text{-}CPA1^{\mathcal{A}}_{SKE}}$:

$K \leftarrow Gen$

$b \leftarrow \mathcal{A}^{\mathcal{E}_1(\cdot,\cdot)}$

Ret b

$\underline{\mathcal{E}_1(m_0, m_1)}$:

Ret $SKE.Enc(K, m_1)$

SKE is IND-CPA if $\forall$ n-PPT $\mathcal{A}$,

$|Pr[IND\text{-}CPA^{\mathcal{A}}_{SKE} = 1] - Pr[IND\text{-}CPA1^{\mathcal{A}}_{SKE} = 1]| = negl(n)$

Continuing SKE analysis

$\underline{IND\text{-}CPA^{A}_{CTR[F]}}$:

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

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

Ret b

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

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

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

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

$T \leftarrow [\,]$

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

Ret b

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

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

If $T[r] = \perp$

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

Set $T[r] = p$

Ret $(r, m_0 \oplus T[r])$

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

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

Ret b

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

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

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

Ret $(r, p \oplus m_0)$

$\underline{H_3^{A}}$:

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

Ret b

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

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

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

Ret (r, p)

IND-CPA $\rightarrow H_1$:

negl by composition

$H_1 \rightarrow H_2$:

Let A be event that A outputs 1 in H_1

" B " A outputs 1 in H_2

F: event that $\exists i,j$ s.t. $r_i = r_j$

$|\Pr[H_1 = 1] - \Pr[H_2 = 1]| \leq \frac{q^2}{2^n}$ by union bound

$H_2 \rightarrow H_3$

by inspection

$\square$

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

Message authentication (MAC)

Enc(k, m):
r ← {0,1}^n
Ret (r, F_k(r) ⊕ m)

- Gen: k ← {0,1}^n
- Tag(k, m): output t ∈ {0,1}^n
- Ver(k, m, t): outputs 0/1

MAC is UF-CMA if ∀ nuPPT A,

$Pr[UF\text{-}CMA^{A}_{MAC} = 1] = negl(n)$

$SUF\text{-}CMA^{A}_{MAC}$:

k ← Gen
m', t' ← $A^{T(\cdot)}$
Ret Ver(k, m', t')
∧ m' ∉ Q (1)
∧ (m', t') ∉ Q (2)

T(m):
t ← Tag(k, m)
Add (m, t) to Q
Ret t

(SUF: replace (1) with (2))

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

PRFs are good MACs

MAC[f]

- Gen: $k \leftarrow \{0,1\}^n$
- Tag(k, m):
  Ret $f_k(m)$
- Ver(k, m, t)
  Ret $f_k(m) \stackrel{?}{=} t$

Thm: If f is PRF, MAC[f] is UF-CMA

Proof:

H_0 MAC[f]

$k \leftarrow Gen$
$m', t' \leftarrow A^{T(\cdot)}$
Ret $f_k(m') = t \wedge m' \notin Q$

T(m):
Add m to Q
Ret $f_k(m)$

H_1 MAC[f]

$R \leftarrow []$
$m', t' \leftarrow A^{T(\cdot)}$
If $R[m'] = \perp$
  $t \leftarrow \{0,1\}^n$
  $R[m'] = t$
Ret $R[m'] = t' \wedge m' \notin Q$

T(m):
Add m to Q
If $R[m] = \perp$
  $t \leftarrow \{0,1\}^n$
  $R[m] = t$
Ret $R[m]$

$H_0 \rightarrow H_1$
PRF security

$Pr[H_1 = 1] \leq \frac{1}{2^n}$

$\square$

Analyzing the scheme

MACs in practice

- PRFs [HMAC]
- Fast algebraic MACs
  Carter-Wegman '79
  GMAC, Poly1305
- CBC-MAC

Agenda for this lecture

- Announcements
- IND-CPA secure SKE from a PRF
- Message authentication
- MACs from PRFs
- Authenticated encryption

Authenticated Encryption