- Announcements
- IND-CPA
- Message Authentication
- Unforgeability
- Info-theoretic
- MACs from PRF

Announcements

- End at 10am
- My OH cancelled
- 1:30pm

IND-CPA

- Encryptions of any pair of msgs comp Ind.

- $Enc(k, m)$:
  $r \leftarrow \{0,1\}^n$
  Ret $(r, f_k(r) \oplus m)$

Problem?
Can be modified!

Capture
(r, c)
Send $(r, c \oplus 1)$
Decrypts to $m \oplus$ (Boy or Girl)

Goal: authenticate sender,
ensure msg not modified

Message Authentication code (MAC)

IND-CPA + 

→ Authenticated Encryption

MAC Syntax

- Gen: output $k \in \mathcal{K} (= \{0,1\}^n)$
- $Tag(k, m)$: outputs $t \in \{0,1\}^n$
  ($m \in \{0,1\}^*$)
- $Vrfy(k, m, t)$: outputs 0/1

Gen generates key
Tag tags msg, ensures auth/integrity
Vrfy checks tag: 1: good, 0: bad

Completeness:

$\forall k, m$

$Vrfy(k, m, Tag(k,m)) = 1$

w.p. 1

Info-theoretic MACs

- Knowing msg but <u>not</u> key, generate verifying tag w. negl. prob.

Perfect Unforgeability: MAC is ↓ if $\forall F, \forall m$:

$\Pr[PUF_{MAC}^{F} = 1] \leq \frac{1}{2^n}$

- Success(m, t, m', t', k):
  Ret $m \neq m' \wedge$ Ver$(k, m', t') = 1$

$PUF_{MAC}^{F,m}$:

$k \leftarrow$ Gen
$t \leftarrow$ Tag(k, m)
$(m', t') \leftarrow F(m, t)$
Ret Success(m, t, m', t', k)

$PSUF_{MAC}^{F,n}$:

$k \leftarrow Gen$

$t \leftarrow Tag(k, m)$

$(m', t') \leftarrow F(m, t)$

Ret $Success(m, t, m', t', k)$

$Success(m, t, m', t', k)$

$\rightarrow$

$Success(m, t, m', t', k)$:

Ret $m \neq m' \wedge$

$Ver(k, m', t') = 1$

$Success(m, t, m', t', k)$:

Ret $(m, t) \neq (m', t') \wedge$

$Ver(k, m', t') = 1$

If $Success(\cdots) = 1$ then $Success(\cdots) = 1$

MAC is PSUF if ! Not the reverse!

$\forall n, \forall F$

$Pr[PSUF_{MAC}^{F,n}] \leq \frac{1}{2^n}$

$= 0$

No! Can always guess

- Deterministic
- If tags unique, strong $\Leftrightarrow$ weak

Info-theoretic MACs

Yes!

Exercise!

Pairwise-independent hash

$\Rightarrow$ I-T MACs

Carter-Wegman '79

Computational MAC

MAC is Strongly unforgeable under chosen-message attack

If $\forall$ nuPPT $\mathcal{F}$, $Pr[SUF^{\mathcal{F}}_{MAC} = 1] = negl(\lambda)$

$SUF^{\mathcal{F}}_{MAC}$:

$k \leftarrow Gen$; $Q \leftarrow []$

$(m', t') \leftarrow \mathcal{F}^{Tag(\cdot)}(1^\lambda)$

Ret $SSuccess(Q, m', t', k)$

$Tag(m)$:

$t \leftarrow Tag(k, m)$

$Q[m] \leftarrow t$

Ret t

$SSuccess(Q, m', t', k)$:

Ret $m' \notin Q \wedge Ver(k, m', t') = 1$

$(m', t') \notin Q \wedge Ver(k, m', t') = 1$

Only one chance to succeed

Can enhance $\mathcal{SCH}$ to give VCR oracle

Is equivalent to SUF-CMA?

PRFs are MACs

Thm: If $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ is a PRF family, then MAC[F] is SUF-CMA.

MAC[F]:

- Gen: Ret PRF.Gen
- Tag(K, m): Ret $f_K(m)$
- Vrf(K, m, t):
  Ret $F_K(m) \stackrel{?}{=} t$

Proof Sketch:

Thm: If $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a PRF family, then MAC[F] is SUF-CMA.

IF MAC[F] not SUF-CMA, then F not PRF family

Assume $\exists$ $\mathcal{A}$ s.t.

$$Pr[\text{UF-CMA}^{\mathcal{A}}_{MAC[F]} = 1] > 1/p(n)$$

Build reduction $\mathcal{B}^{\mathcal{A}}$

$B^{F, F(\cdot)}$:

$Q \leftarrow [\,]$

$(m', t') \leftarrow F^{\widetilde{Tag}(\cdot)}$

Ret $\widetilde{Success}(Q, m', t')$

$\widetilde{Tag}(m)$:

$t \leftarrow f(m)$

$Q[m] \leftarrow t$

Ret t

$\widetilde{Success}(Q, m', t')$:

$t \leftarrow f(m')$

Ret $m' \notin Q \wedge t = t'$

Exercise ←

Claim: B^F's advantage $\geq Pr[F\ wins] - \frac{1}{2^n}$ = non-negl