Cryptography
CS 555

Topic 10: Constructing Message Authentication Codes

Reminder: Homework 1

- Due on **Friday (next class)** at the **beginning** of class

- Please typeset your solutions

Recap

- Data Integrity
- Message Authentication Codes
- Side-Channel Attacks
- ~~Build Secure MACs~~

Today's Goals:

- Build a Secure MAC
  - Key tool in Construction of CCA-Secure Encryption Schemes
- ~~Construct CCA-Secure Encryption Scheme~~

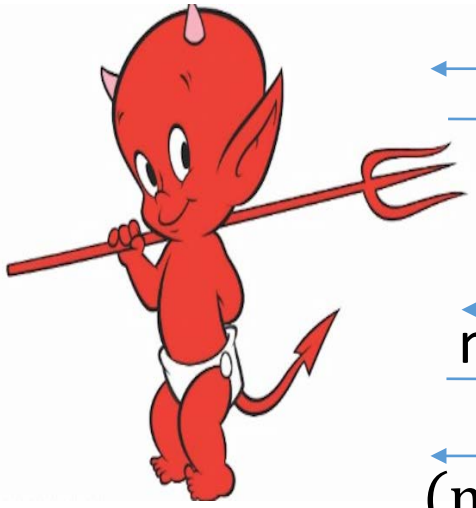
Message Authentication Code Syntax

Definition 4.1: A message authentication code (MAC) consists of three algorithms $\Pi = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$

- $\mathrm{Gen}(1^n; R)$ (Key-generation algorithm)
  - Input: security parameter 1^n (unary) and random bits R
  - Output: Secret key $\mathrm{k} \in \mathcal{K}$
- $\mathrm{Mac}_{\mathrm{k}}(m; R)$ (Tag Generation algorithm)
  - Input: Secret key $\mathrm{k} \in \mathcal{K}$ and message $\mathrm{m} \in \mathcal{M}$ and random bits R
  - Output: a tag t
- $\mathrm{Vrfy}_{\mathrm{k}}(m, t)$ (Verification algorithm)
  - Input: Secret key $\mathrm{k} \in \mathcal{K}$, a message m and a tag t
  - Output: a bit b (b=1 means “valid” and b=0 means “invalid”)

$$\mathrm{Vrfy}_{\mathrm{k}}(m, \mathrm{Mac}_{\mathrm{k}}(m; R)) = 1$$

Strong MAC Authentication ($\mathrm{Macsforge}_{A,\Pi}(n)$)



m_1

$t_1 = \mathrm{Mac}_K(m_1)$

m_2

$t_2 = \mathrm{Mac}_K(m_2)$

$\vdots$

m_q

$t_q = \mathrm{Mac}_K(m_q)$

(m, t) s.t $(m, t) \notin \{(m_1, t_1), \ldots, (m_q, t_q)\}$

$\mathrm{Macsforge}_{A,\Pi}(n) = \mathrm{Vrfy}_k(m, t)$

K = Gen(.)

$\forall PPT\ A\ \exists \mu$ (negligible) s. t

$\Pr[\mathrm{Macsforge}_{A,\Pi}(n) = 1] \leq \mu(n)$

Strong MAC Construction (Fixed Length)

Simply uses a secure PRF F

$$\mathrm{Mac}_k(m) = \mathrm{F}_K(m)$$

Canonical Verification Algorithm…

$$\mathrm{Vrfy}_k(m, t) = \begin{cases} 1 & \text{if } t = \mathrm{F}_K(m) \\ 0 & \text{otherwise} \end{cases}$$

Strong MAC Construction (Fixed Length)

$$\mathrm{Mac}_k(m) = \mathrm{F}_K(m)$$

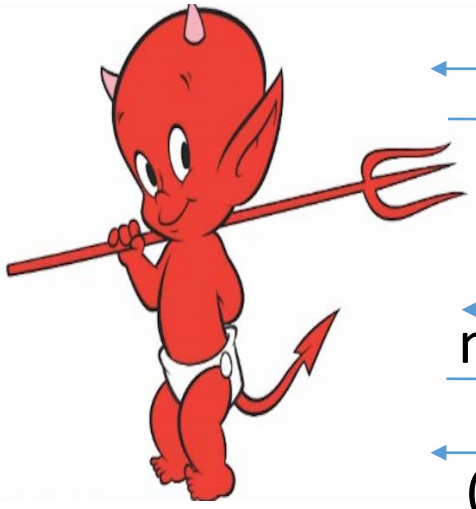
$$\mathrm{Vrfy}_k(m, t) = \begin{cases} 1 & \text{if } t = \mathrm{F}_K(m) \\ 0 & \text{otherwise} \end{cases}$$

Theorem 4.6: If F is a PRF then this is a secure (fixed-length) MAC for messages of length n.

Proof: Start with attacker who breaks MAC security and build an attacker who breaks PRF security (contradiction!)

Sufficient to start with attacker who breaks regular MAC security (why?)

Breaking MAC Security $(\text{Macforge}_{A,\Pi}(n))$



m_1

$t_1 = F_K(m_1)$

m_2

$t_2 = F_K(m_2)$

$\vdots$

m_q

$t_q = F_K(m_q)$

(m, t) s.t $m \notin \{m_1, \ldots, m_q\}$

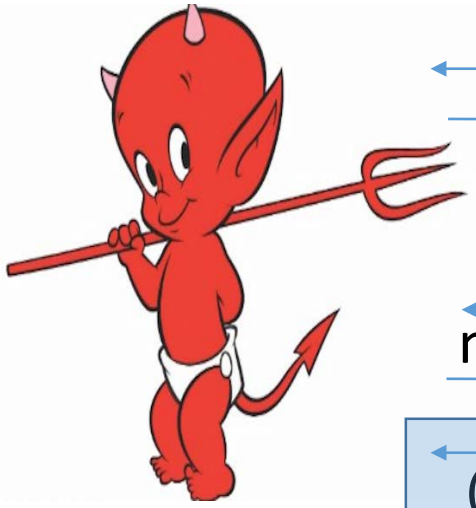
$\text{Macforge}_{A,\Pi}(n) = \text{Vrfy}_k(m, t)$

K = Gen(.)

$\exists PPT\ A\ and\ \mu$ (positive/non negligible) s. t

$$\Pr\left[\text{Macforge}_{A,\Pi}(n) = 1\right] > \mu(n)$$

A Similar Game $(\text{Macforge}_{A,\tilde{\Pi}}$



m_1

$t_1 = f(m_1)$

m_2

$t_2 = f(m_2)$

$\vdots$

m_q

$t_q = f(m_q)$

(m, t) s.t $m \notin \{m_1, \ldots, m_q\}$

$\text{Macforge}_{A,\tilde{\Pi}}(n) = \text{Vrfy}_k(m, t)$

Why? Because f(m) is distributed uniformly in $\{0,1\}^n$ so $\Pr[f(m)=t]=2^{-n}$

Truly Random Function
f $\in$ Func$_n$

Claim: $\forall A\ (not\ just\ PPT)$

$$\Pr\left[\text{Macforge}_{A,\tilde{\Pi}}(n) = 1\right] \leq 2^{-n}$$

PRF Distinguisher D

- Given oracle O (either F_K or truly random f)
- Run PPT Macforge adversary A
- When adversary queries with message m, respond with O(m)

- If O = f then

$$\Pr[D^{O}(1^n) = 1] = \Pr\left[\text{Macforge}_{A,\tilde{\Pi}}(n) = 1\right] \leq 2^{-n}$$

- If O=f then

$$\Pr[D^{O}(1^n) = 1] = \Pr\left[\text{Macforge}_{A,\Pi}(n) = 1\right] > \mu(n)$$

PRF Distinguisher D

- If O = f then

$$\Pr[D^{O}(1^n) = 1] = \Pr\left[\text{Macforge}_{A,\tilde{\Pi}}(n) = 1\right] \leq 2^{-n}$$

- If O=F_K then

$$\Pr[D^{O}(1^n) = 1] = \Pr\left[\text{Macforge}_{A,\Pi}(n) = 1\right] > \mu(n)$$

Advantage:

$$|\Pr[D^{F_K}(1^n) = 1] - \Pr[D^{f}(1^n) = 1]| > \mu(n) - 2^{-n}$$

Note that $\mu(n) - 2^{-n}$ is non-negligible and D runs in PPT if A does.

Strong MAC Construction (Fixed Length)

$$\mathrm{Mac}_k(m) = \mathrm{F}_K(m)$$

$$\mathrm{Vrfy}_k(m, t) = \begin{cases} 1 & \text{if } t = \mathrm{F}_K(m) \\ 0 & \text{otherwise} \end{cases}$$

Theorem 4.6: If F is a PRF then this is a secure (fixed-length) MAC for messages of length n.

Limitation: What if we want to authenticate a longer message?

MACs for Arbitrary Length Messages

- Building Block Π'=(Mac',Vrfy'), a secure MAC for length n messages

First: A few failed attempts

Let m = m_1,…,m_d where each m_i is n bits and let $t_i = \mathrm{Mac}'_K(m_i)$

$$\mathrm{Mac}_K(m) = \langle t_1, \ldots, t_d \rangle$$

What is wrong?

Block-reordering attack

$$\mathrm{Mac}_K(m_d,\ldots,m_1) = \langle t_d, \ldots, t_1 \rangle$$

MACs for Arbitrary Length Messages

- Building Block Π'=(Mac',Vrfy'), a secure MAC for length n messages

Attempt 2

Let m = m_1,…,m_d where each m_i is n bits and let $t_i = \mathrm{Mac}'_K(i \parallel m_i)$

$$\mathrm{Mac}_K(m) = \langle t_1, \ldots, t_d \rangle$$

Addresses block-reordering attack.

Any other concerns?

Truncation attack!

$$\mathrm{Mac}_K(m_1,\ldots,m_{d-1}) = \langle t_1, \ldots, t_{d-1} \rangle$$

MACs for Arbitrary Length Messages

- Building Block Π'=(Mac',Vrfy'), a secure MAC for length n messages

Attempt 3

Let m = $m_1,\ldots,m_d$ where each m_i is n bits and m has length $\ell = nd$

Let $t_i = \mathrm{Mac}'_K(i \parallel \ell \parallel m_i)$

$$\mathrm{Mac}_K(m) = \langle t_1, \ldots, t_d \rangle$$

Addresses truncation.

Any other concerns?

Mix and Match Attack!

MACs for Arbitrary Length Messages

Let m = m_1,…,m_d where each m_i is n bits and m has length $\ell = nd$

Let m' = m'_1,…,m'_d where each m'_i is n bits and m has length $\ell = nd$

Let $t_i = \mathrm{Mac}'_K(i \parallel \ell \parallel m_i)$ and $t'_i = \mathrm{Mac}'_K(i \parallel \ell \parallel m_i\ ')$

$$\mathrm{Mac}_K(m) = \langle t_1, \ldots, t_d \rangle$$

$$\mathrm{Mac}_K(m') = \langle t'_1, \ldots, t'_d \rangle$$

Mix and Match Attack!

$$\mathrm{Mac}_K(m_1, m'_2, m_3, \ldots) = \langle t_1, t'_2, t_3, \ldots \rangle$$

MACs for Arbitrary Length Messages

- A non-failed approach ☺
- Building Block Π'=(Mac',Vrfy'), a secure MAC for length n messages
- Let m = m_1,…,m_d where each m_i is n/4 bits and m has length $\ell < 2^{n/4}$

Mac_K(m)=

- Select random n/4 bit string r
- Let $t_i = Mac'_K(r \parallel \ell \parallel i \parallel m_i)$ for i=1,…,d
  - (Note: encode i and ℓ as n/4 bit strings)
- **Output** $\langle r, t_1, \ldots, t_d \rangle$

MACs for Arbitrary Length Messages

$Mac_K(m)$=

- Select random n/4 bit string r
- Let $t_i = Mac'_K(r \parallel \ell \parallel i \parallel m_i)$ for i=1,…,d
  - (Note: encode i and ℓ as n/4 bit strings)
- **Output** $\langle r, t_1, \ldots, t_d \rangle$

Theorem 4.8: If Π' is a secure MAC for messages of fixed length n, above construction $\Pi = (\mathrm{Mac}, \mathrm{Vrfy})$ is secure MAC for arbitrary length messages.

Next Class

- Read Katz and Lindell 4.4-4.5
- CBC-MAC and Authenticated Encryption