



Message Integrity

MACs based on PRFs

Review: Secure MACs

MAC: signing alg. $S(k,m) \rightarrow t$ and verification alg. $V(k,m,t) \rightarrow 0,1$

Attacker's power: **chosen message attack**

- for m_1, m_2, \dots, m_q attacker is given $t_i \leftarrow S(k, m_i)$

Attacker's goal: **existential forgery**

- produce some new valid message/tag pair (m, t) .

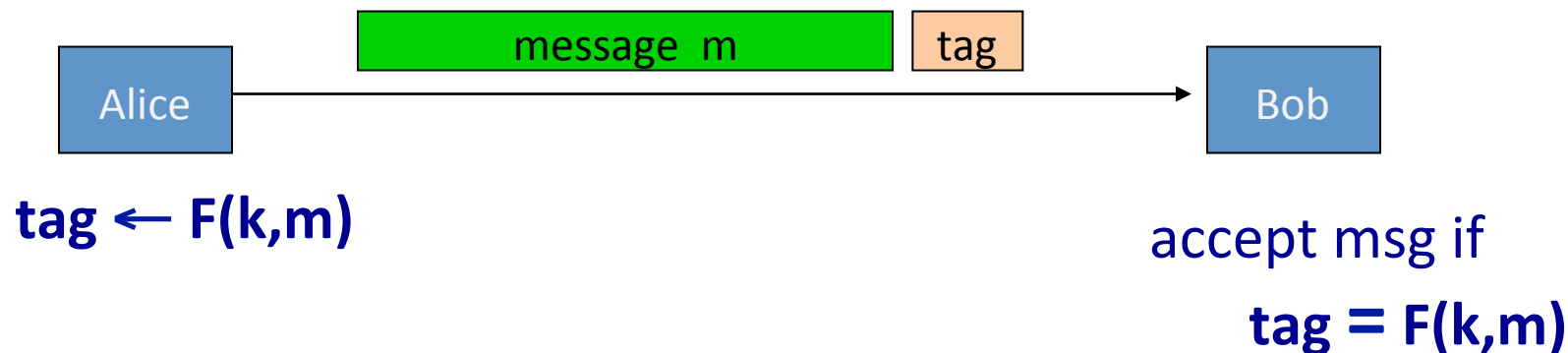
$$(m, t) \notin \{ (m_1, t_1), \dots, (m_q, t_q) \}$$

\Rightarrow attacker cannot produce a valid tag for a new message

Secure PRF \Rightarrow Secure MAC

For a PRF $F: K \times X \rightarrow Y$ define a MAC $I_F = (S, V)$ as:


- $S(k, m) := F(k, m)$
- $V(k, m, t)$: output 'yes' if $t = F(k, m)$ and 'no' otherwise.



A bad example

Suppose $F: K \times X \rightarrow Y$ is a secure PRF with $Y = \{0,1\}^{10}$

Is the derived MAC I_F a secure MAC system?

- ☐ Yes, the MAC is secure because the PRF is secure
-  ☒ No tags are too short: anyone can guess the tag for any msg
- ☐ It depends on the function F

$$Adv[A, I_F] = 1/1024$$

Security

Thm: If $F: K \times X \rightarrow Y$ is a secure PRF and $1/|Y|$ is negligible (i.e. $|Y|$ is large) then I_F is a secure MAC.

In particular, for every eff. MAC adversary A attacking I_F there exists an eff. PRF adversary B attacking F s.t.:

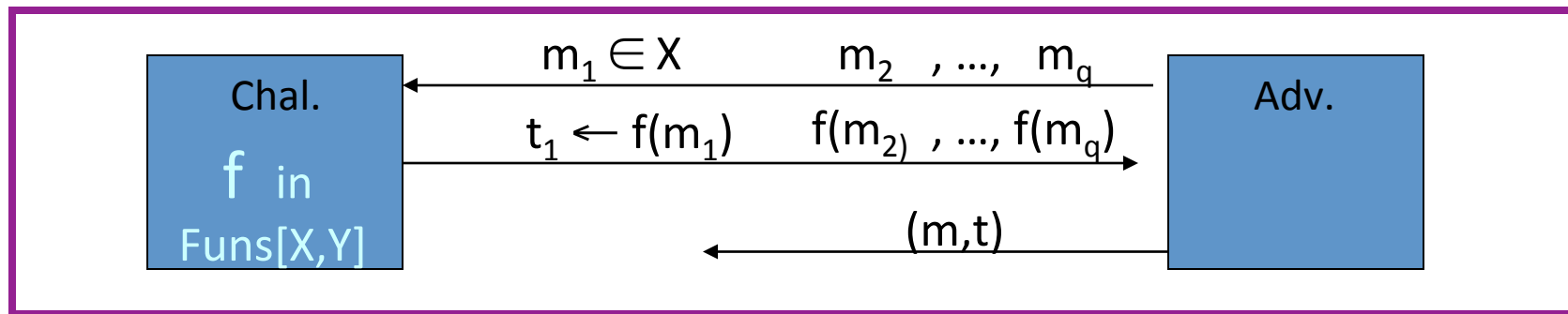
$$\text{Adv}_{\text{MAC}}[A, I_F] \leq \text{Adv}_{\text{PRF}}[B, F] + 1/|Y|$$

$\Rightarrow I_F$ is secure as long as $|Y|$ is large, say $|Y| = 2^{80}$.

Proof Sketch

Suppose $f: X \rightarrow Y$ is a truly random function

Then MAC adversary A must win the following game:



A wins if $t = f(m)$ and $m \notin \{m_1, \dots, m_q\}$

$\Rightarrow \Pr[A \text{ wins}] = 1/|Y|$ same must hold for $F(k,x)$

Examples

- AES: a MAC for 16-byte messages.
- Main question: how to convert Small-MAC into a Big-MAC ?
- Two main constructions used in practice:
 - **CBC-MAC** (banking – ANSI X9.9, X9.19, FIPS 186-3)
 - **HMAC** (Internet protocols: SSL, IPsec, SSH, ...)
- Both convert a small-PRF into a big-PRF.

Truncating MACs based on PRFs

Easy lemma: suppose $F: K \times X \rightarrow \{0,1\}^n$ is a secure PRF.

Then so is $F_t(k,m) = \underbrace{F(k,m)[1\dots t]}_{\text{first } t\text{-bit of output}}$ for all $1 \leq t \leq n$

\Rightarrow if (S,V) is a MAC is based on a secure PRF outputting n -bit tags
the truncated MAC outputting w bits is secure
... as long as $1/2^w$ is still negligible (say $w \geq 64$)

End of Segment