Message Integrity

CBC-MAC and NMAC

MACs and PRFs

Recall: secure PRF **F** ⇒ secure MAC, as long as |Y| is large

$S(k, m) = F(k, m)$

Our goal:

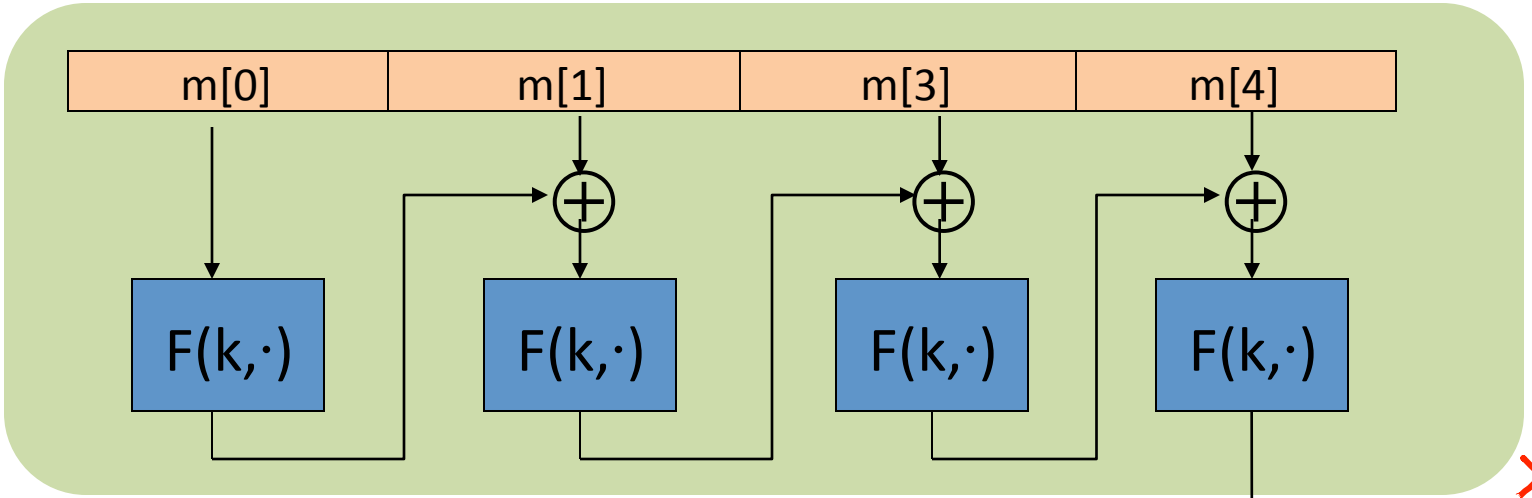
given a PRF for short messages (AES)

construct a PRF for long messages

From here on let $X = \{0,1\}^n$ (e.g. n=128)

Construction 1: encrypted CBC-MAC

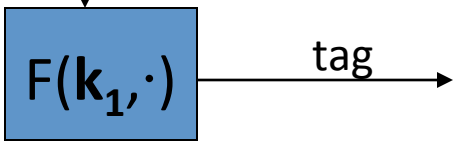
raw CBC



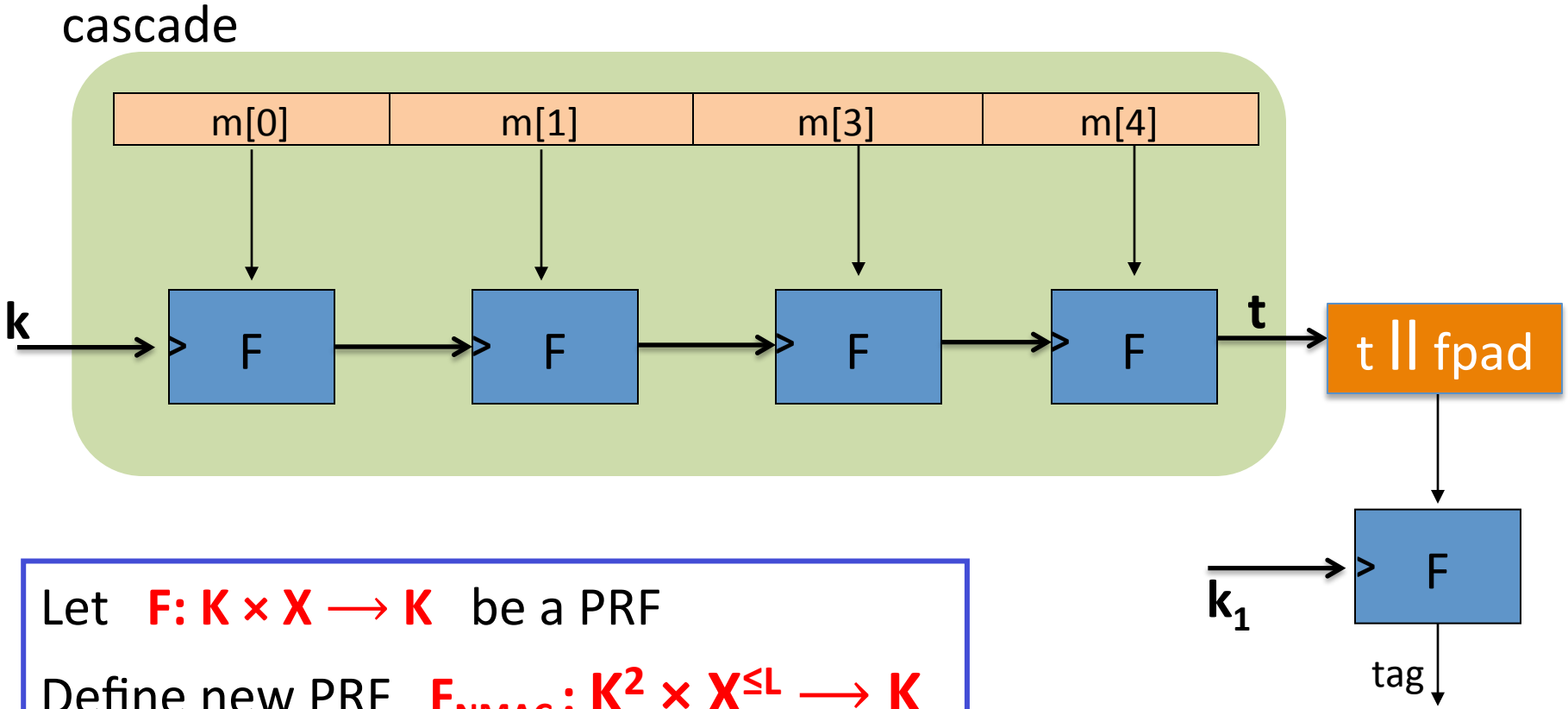
$X^{\leq L} = \bigcup_{i=1}^{L} X^i$

Let $F: K \times X \longrightarrow X$ be a PRP

Define new PRF $F_{ECBC} : K^2 \times X^{\leq L} \longrightarrow X$



Construction 2: NMAC (nested MAC)



Let $F: K \times X \longrightarrow K$ be a PRF

Define new PRF $F_{NMAC}: K^2 \times X^{\leq L} \longrightarrow K$

Why the last encryption step in ECBC-MAC and NMAC?

NMAC: suppose we define a MAC I = (S,V) where

S(k,m) = cascade(k, m)

- ○ This MAC is secure
- ○ This MAC can be forged without any chosen msg queries
- ○ This MAC can be forged with one chosen msg query
- ○ This MAC can be forged, but only with two msg queries

cascade(k,m) ⇒ cascade(k, m||w) for any w

Why the last encryption step in ECBC-MAC?

Suppose we define a MAC $I_{RAW} = (S,V)$ where

$$S(k,m) = \text{rawCBC}(k,m)$$

Then I_{RAW} is easily broken using a 1-chosen msg attack.

Adversary works as follows:

- Choose an arbitrary one-block message $m \in X$
- Request tag for m. Get $t = F(k,m)$
- Output t as MAC forgery for the 2-block message $(m, t \oplus m)$

Indeed: $\text{rawCBC}\big(k, (m, t\oplus m)\big) = F\big(k, F(k,m)\oplus(t\oplus m)\big) = F(k, t\oplus(t\oplus m)) = t$

ECBC-MAC and NMAC analysis

Theorem: For any L>0,

For every eff. q-query PRF adv. A attacking F_{ECBC} or F_{NMAC} there exists an eff. adversary B s.t.:

$$Adv_{PRF}[A, F_{ECBC}] \le Adv_{PRP}[B, F] + 2\, q^2 / |X|$$

$$Adv_{PRF}[A, F_{NMAC}] \le q \cdot L \cdot Adv_{PRF}[B, F] + q^2 / 2|K|$$

CBC-MAC is secure as long as $q << |X|^{1/2}$

NMAC is secure as long as $q << |K|^{1/2}$ (2^{64} for AES-128)

An example

$$Adv_{PRF}[A, F_{ECBC}] \le Adv_{PRP}[B, F] + \mathbf{2\, q^2 / |X|}$$

q = # messages MAC-ed with k

Suppose we want $Adv_{PRF}[A, F_{ECBC}] \le 1/2^{32}$ $\Leftarrow$ $q^2 / |X| < 1/ 2^{32}$

- AES: $|X| = 2^{128} \Rightarrow q < 2^{48}$

  So, after 2^{48} messages must, must change key

- 3DES: $|X| = 2^{64} \Rightarrow q < 2^{16}$

The security bounds are tight: an attack

After signing $|X|^{1/2}$ messages with ECBC-MAC or

$|K|^{1/2}$ messages with NMAC

the MACs become insecure

Suppose the underlying PRF F is a PRP (e.g. AES)

- Then both PRFs (ECBC and NMAC) have the following extension property:

$$\forall x,y,w: \quad F_{BIG}(k, x) = F_{BIG}(k, y) \quad \Rightarrow \quad F_{BIG}(k, \mathbf{x||w}) = F_{BIG}(k, \mathbf{y||w})$$

The security bounds are tight: an attack

Let $F_{BIG}: \mathbf{K \times X \longrightarrow Y}$ be a PRF that has the extension property

$$F_{BIG}(k, x) = F_{BIG}(k, y) \quad \Rightarrow \quad F_{BIG}(k, \mathbf{xllw}) = F_{BIG}(k, \mathbf{yllw})$$

Generic attack on the derived MAC:

step 1: issue $|Y|^{1/2}$ message queries for rand. messages in X.

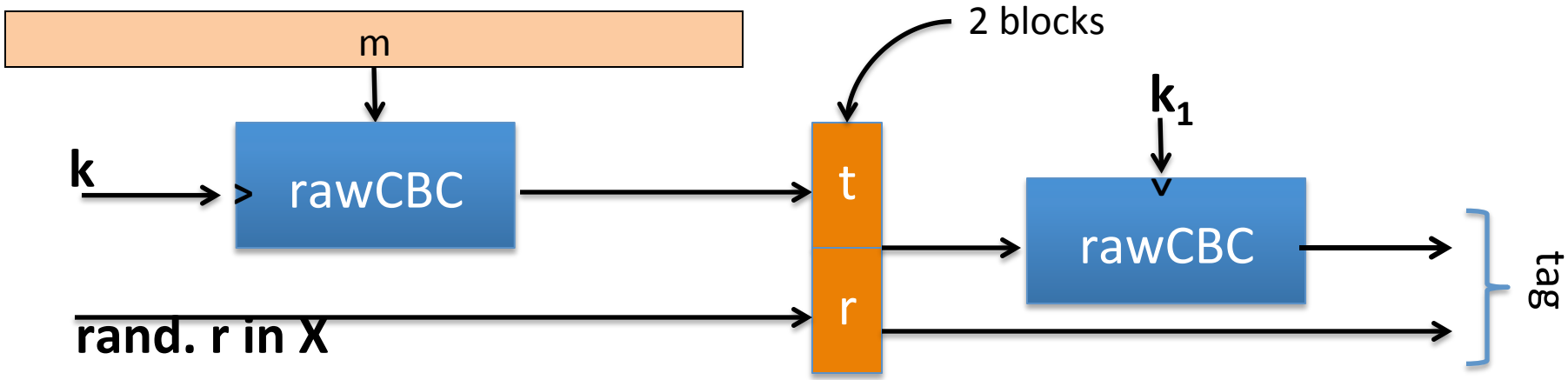
obtain (m_i, t_i) for $i = 1, \ldots, |Y|^{1/2}$

step 2: find a collision $t_u = t_v$ for $u \neq v$ (one exists w.h.p by b-day paradox)

step 3: choose some w and query for $t := F_{BIG}(k, \mathbf{m_u llw})$

step 4: output forgery $\mathbf{(m_v llw, t)}$. Indeed $t := F_{BIG}(k, \mathbf{m_v llw})$

Better security: a rand. construction



Let **F: K × X ⟶ X** be a PRF. Result: MAC with tags in X^2.

Security: $Adv_{MAC}[A, I_{RCBC}] \le Adv_{PRP}[B, F] \cdot (1 + 2\, q^2 / |X|)$

⇒ For 3DES: can sign **$q=2^{32}$** msgs with one key

Comparison

ECBC-MAC is commonly used as an AES-based MAC

- CCM encryption mode (used in 802.11i)
- NIST standard called CMAC

NMAC not usually used with AES or 3DES

- Main reason: need to change AES key on every block
  requires re-computing AES key expansion
- But NMAC is the basis for a popular MAC called HMAC (next)

End of Segment