Message Integrity

A Parallel MAC

- ECBC and NMAC are sequential.

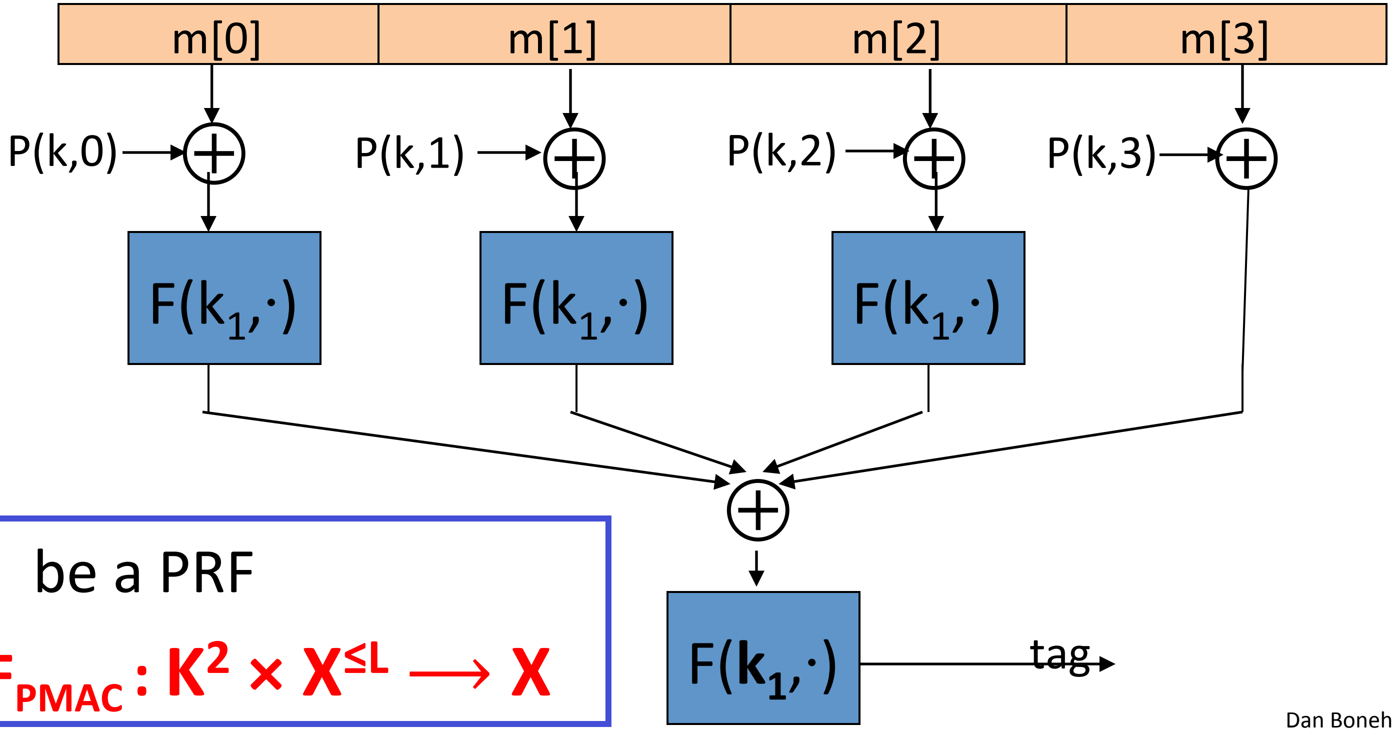
- Can we build a parallel MAC from a small PRF ??

Construction 3: PMAC – parallel MAC

P(k, i): an easy to compute function

key = (k, k_1)

Padding similar to CMAC



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

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

PMAC: Analysis

<u>PMAC Theorem</u>: For any $L>0$,

If F is a secure PRF over (K,X,X) then

F_{PMAC} is a secure PRF over $(K, X^{\leq L}, X)$.

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

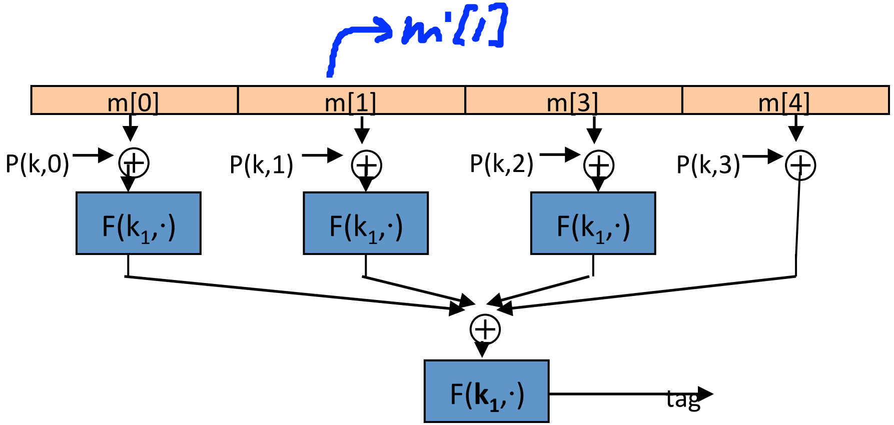
$$\mathrm{Adv}_{PRF}[A, F_{PMAC}] \leq \mathrm{Adv}_{PRF}[B, F] + \mathbf{2\, q^2\, L^2 / |X|}$$

PMAC is secure as long as $qL \ll |X|^{1/2}$

PMAC is incremental

Suppose F is a PRP.

When $m[1] \longrightarrow m'[1]$
can we quickly update tag?

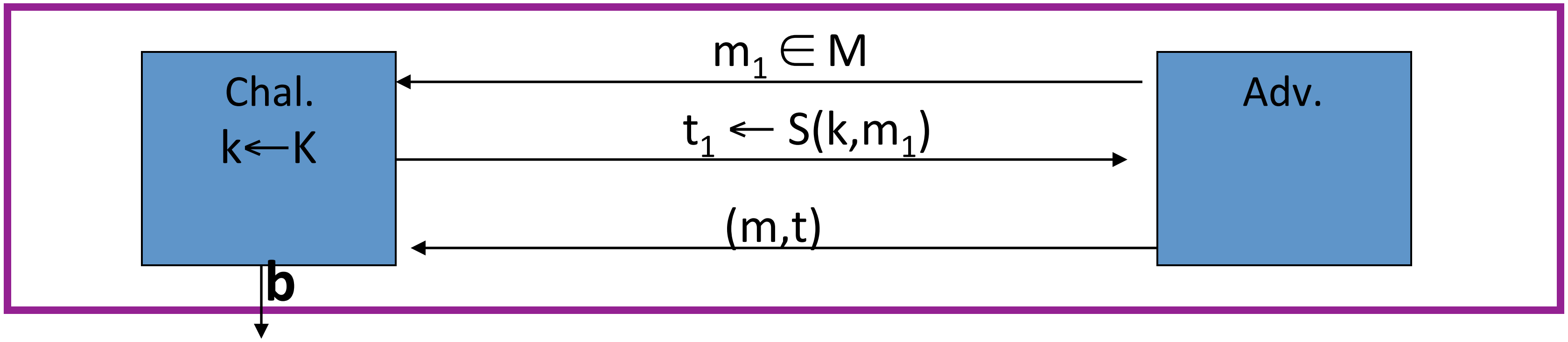


- no, it can't be done
- do $F^{-1}(k_1,tag) \oplus F\big(k_1, m'[1] \oplus P(k,1)\big)$
- do $F^{-1}(k_1,tag) \oplus F\big(k_1, m[1] \oplus P(k,1)\big) \oplus F\big(k_1, m'[1] \oplus P(k,1)\big)$
- do $tag \oplus F\big(k_1, m[1] \oplus P(k,1)\big) \oplus F\big(k_1, m'[1] \oplus P(k,1)\big)$

Then apply $F(k_1, \cdot)$

One time MAC (analog of one time pad)

- For a MAC I=(S,V) and adv. A define a MAC game as:



$$\begin{cases} \mathbf{b}=1 & \text{if } V(k,m,t) = \text{`yes'} \text{ and } (m,t) \neq (m_1,t_1) \\ \mathbf{b}=0 & \text{otherwise} \end{cases}$$

Def: I=(S,V) is a **secure MAC** if for all "efficient" A:

$\mathrm{Adv}_{\mathrm{MAC}}[A,I]$ = Pr[Chal. outputs 1] is "negligible."

Dan Boneh

One-time MAC: an example

Can be secure against **all** adversaries and faster than PRF-based MACs

Let q be a large prime (e.g. $\mathbf{q = 2^{128}+51}$)

key = (k, a) $\in \{1,\ldots,q\}^2$ (two random ints. in [1,q])

msg = (m[1], …, m[L]) where each block is 128 bit int.

$$\mathbf{S(\text{ key, msg }) = P_{msg}(k) + a \quad (\text{mod } q)}$$

where $P_{msg}(x) = m[L]\cdot x^L + \ldots + m[1]\cdot x$ is a poly. of deg L.

Fact: given **S(key, $\mathbf{msg_1}$)** adv. has no info about **S(key, $\mathbf{msg_2}$)**

Dan Boneh

One-time MAC ⇒ Many-time MAC

Let (S,V) be a secure one-time MAC over $(K_I, M, \{0,1\}^n)$.

Let $F: K_F \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

Carter-Wegman MAC: $\quad CW\big((k_1,k_2), m \big) = \big(r, \ \overbrace{F(k_1,r)}^{\text{slow but short inp}} \oplus \overbrace{S(k_2,m)}^{\text{fast long inp}} \big)$

for random $r \longleftarrow \{0,1\}^n$.

<u>**Thm**</u>: If (S,V) is a secure **one-time** MAC and F a secure PRF then CW is a secure MAC outputting tags in $\{0,1\}^{2n}$.

$$CW(\ (k_1,k_2),\ m) = \ (r,\ F(k_1,r) \oplus S(k_2,m)\ )$$

How would you verify a CW tag **(r, t)** on message **m** ?

Recall that $V(k_2,m,.)$ is the verification alg. for the one time MAC.

- Run $V(\ k_2,\ m,\ F(k_1, t) \oplus r)\ )$
- Run $V(\ k_2,\ m, r\ )$
- Run $V(\ k_2,\ m, t\ )$
- Run $V(\ k_2,\ m,\ F(k_1, r) \oplus t)\ )$

Construction 4: HMAC (Hash-MAC)

Most widely used MAC on the Internet.

… but, we first we need to discuss hash function.

Further reading

- J. Black, P. Rogaway: CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. J. Cryptology 18(2): 111-131 (2005)
- K. Pietrzak: A Tight Bound for EMAC. ICALP (2) 2006: 168-179
- J. Black, P. Rogaway: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. EUROCRYPT 2002: 384-397
- M. Bellare: New Proofs for NMAC and HMAC: Security Without Collision-Resistance. CRYPTO 2006: 602-619
- Y. Dodis, K. Pietrzak, P. Puniya: A New Mode of Operation for Block Ciphers and Length-Preserving MACs. EUROCRYPT 2008: 198-219

End of Segment