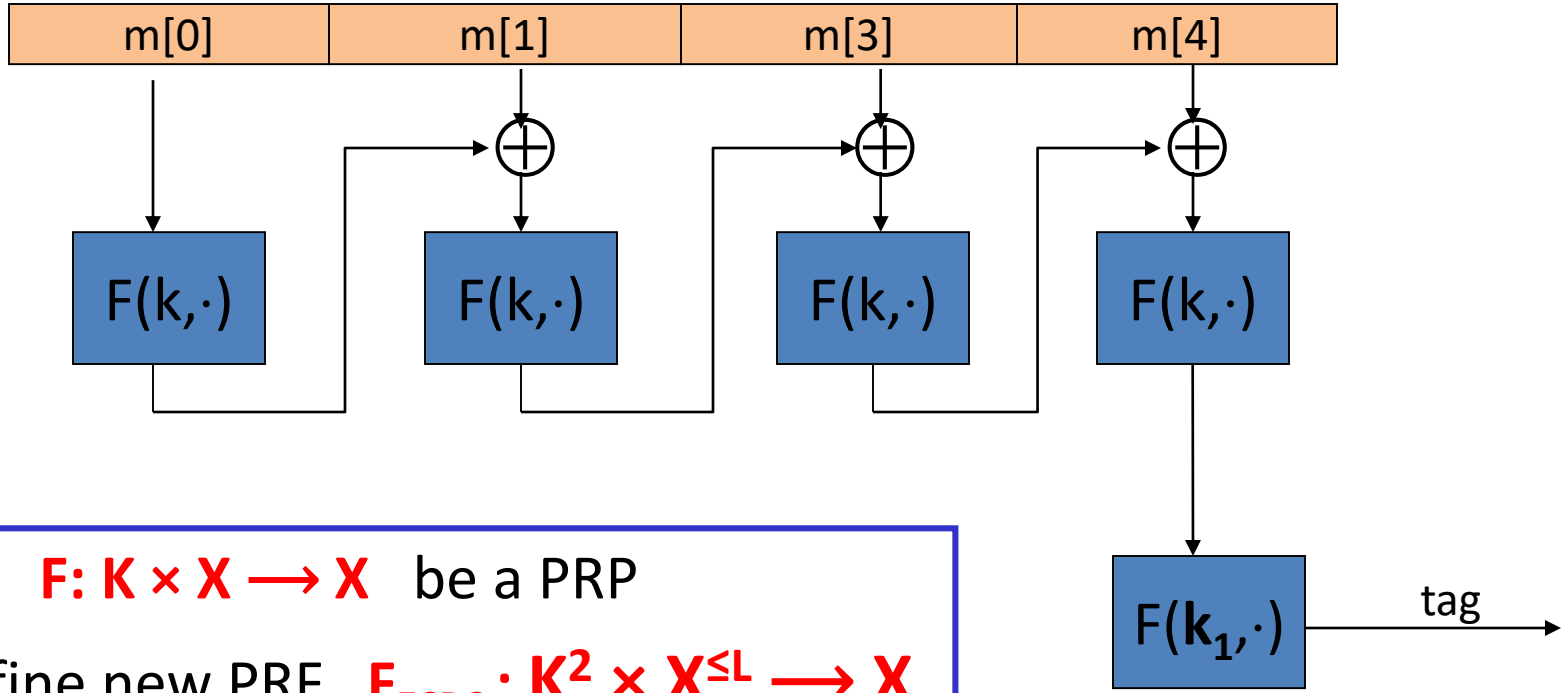
Message integrity

Message Integrity

MAC padding

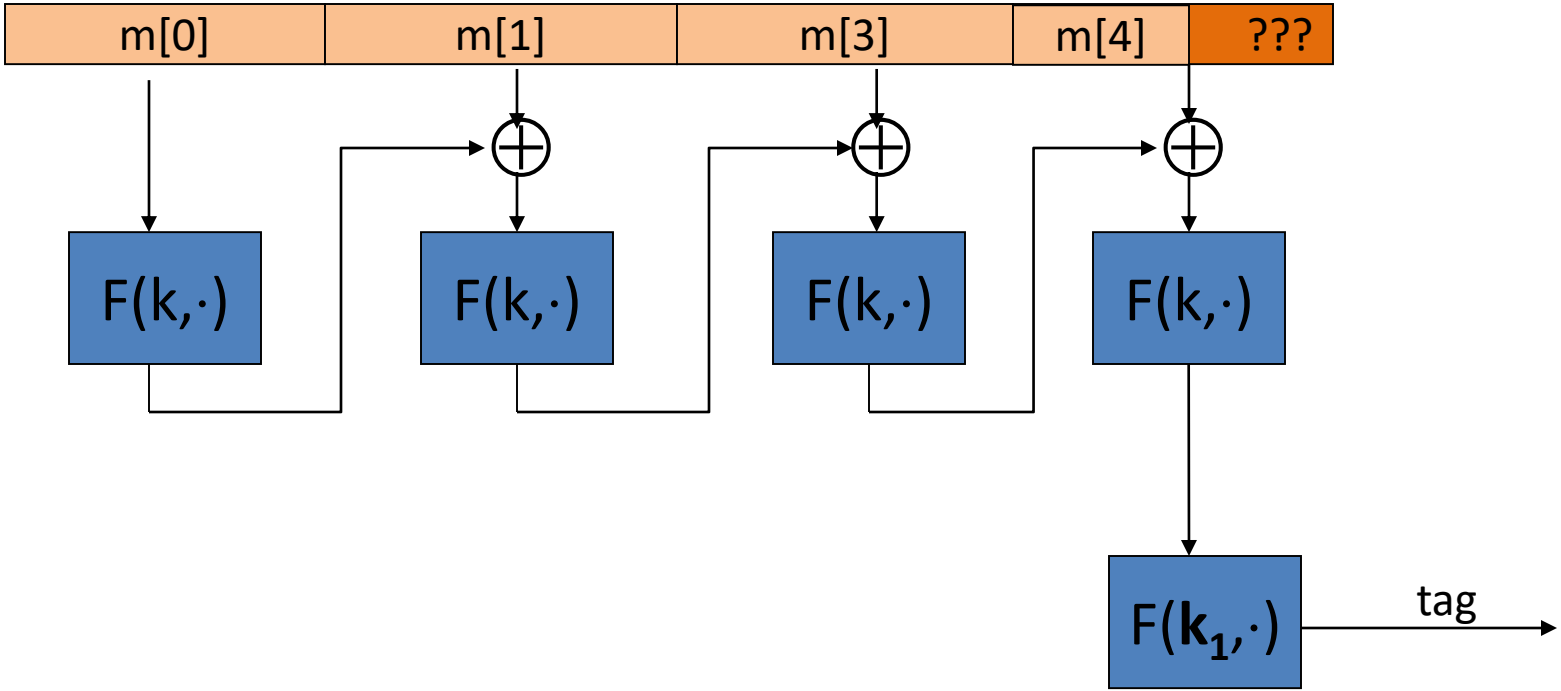
Recall: ECBC-MAC



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

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

What if msg. len. is not multiple of block-size?



CBC MAC padding

Bad idea: pad m with 0's

Is the resulting MAC secure?

- Yes, the MAC is secure
- It depends on the underlying MAC
- No, given tag on msg **m** attacker obtains tag on **m||0**
-

Problem: pad(m) = pad(m||0)

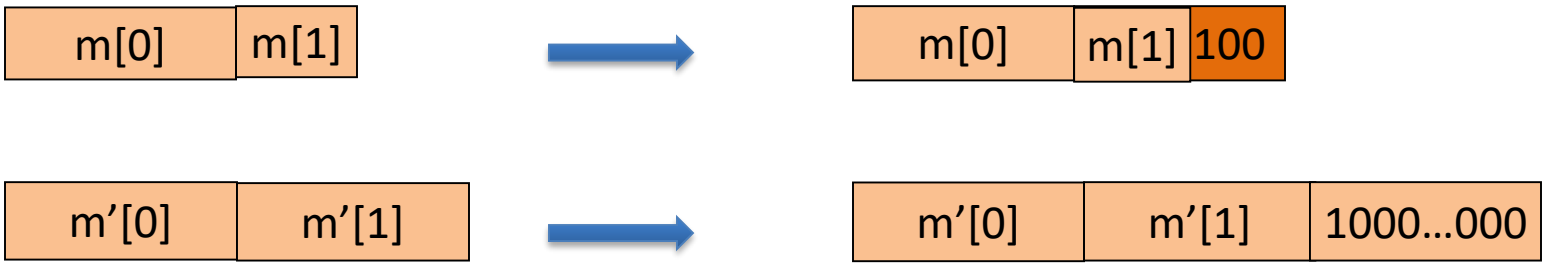
CBC MAC padding

For security, padding must be invertible !

$$m_0 \neq m_1 \quad \Rightarrow \quad pad(m_0) \neq pad(m_1)$$

ISO: pad with "1000…00". Add new dummy block if needed.

– The "1" indicates beginning of pad.

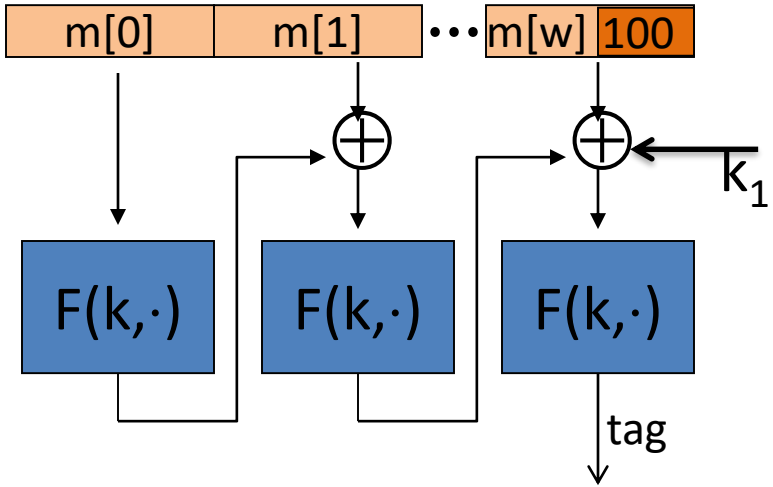


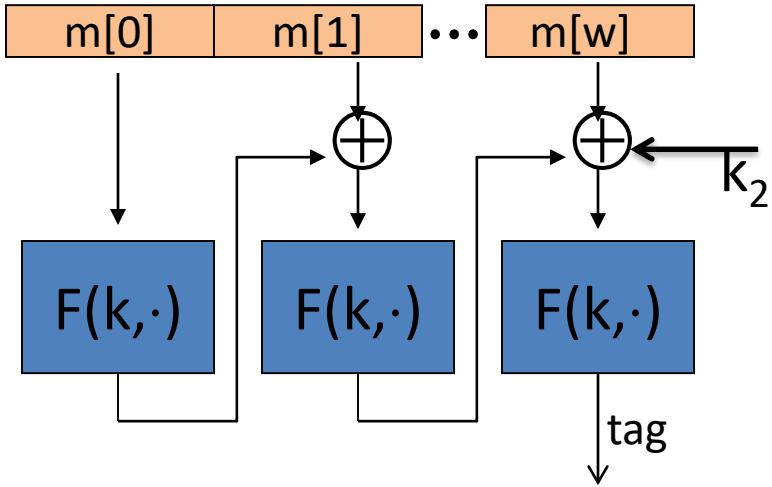
CMAC (NIST standard)

(k_1, k_2) derived from k

Variant of CBC-MAC where key = (k, k_1, k_2)

- No final encryption step (extension attack thwarted by last keyed xor)
- No dummy block (ambiguity resolved by use of k_1 or k_2)





End of Segment

Message Integrity

PMAC

- ECBC and NMAC are sequential.

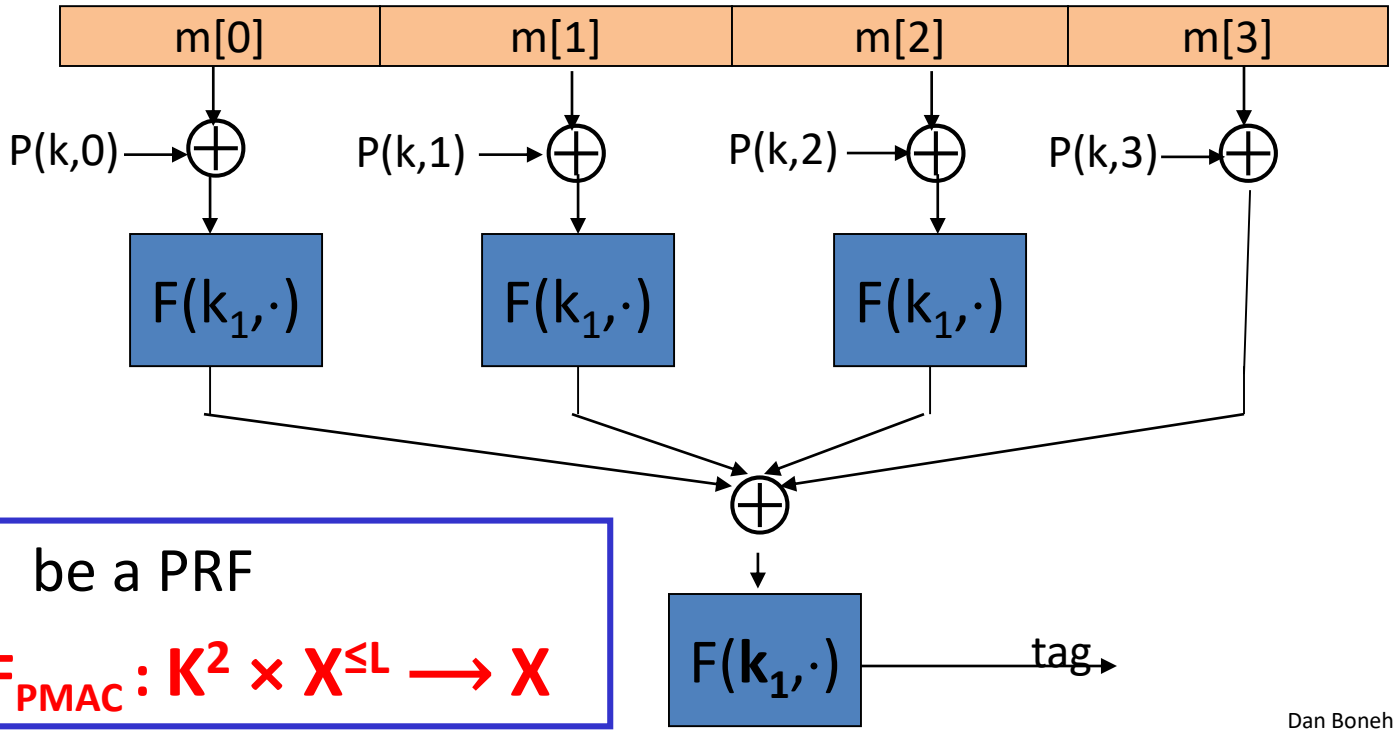
- Can we build a parallel MAC from a small PRF ??

Construction 3: PMAC – parallel MAC

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

key = (k, k_1)

Padding similar to CMAC



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

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

PMAC: Analysis

PMAC Theorem: 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.:

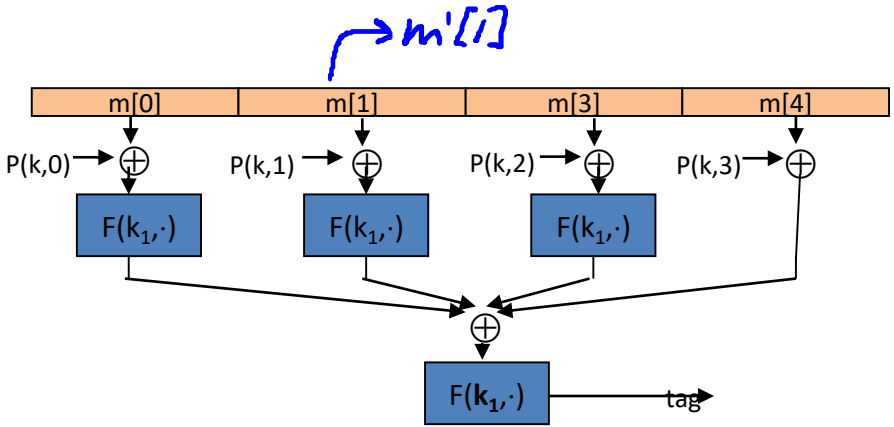
$$Adv_{PRF}[A, F_{PMAC}] \leq Adv_{PRF}[B, F] + \mathbf{2\, q^2\, L^2 / |X|}$$

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

PMAC is incremental

Suppose F is a PRP.

When m[1] ⟶ m’[1]
can we quickly update tag?



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

Then apply $F(k_1, \cdot)$

Construction 3: 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