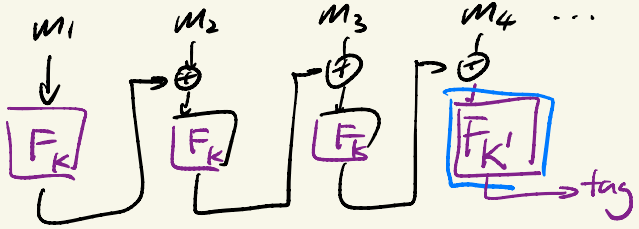
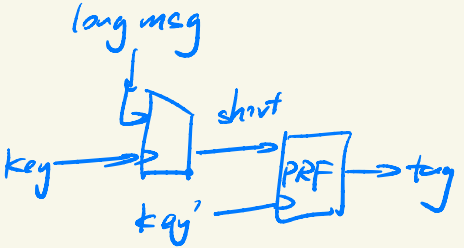
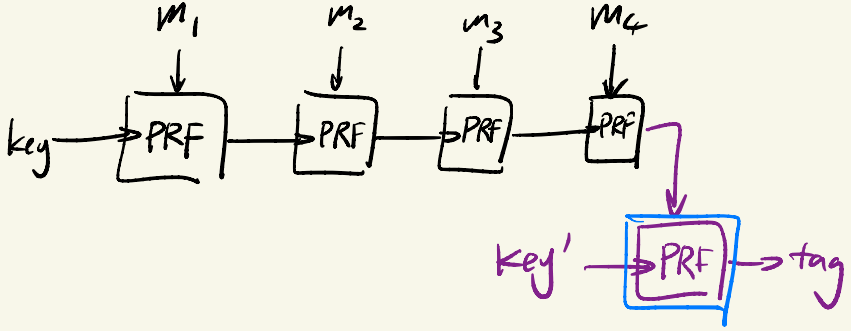
Recap. MAC construction.

CBC-mode

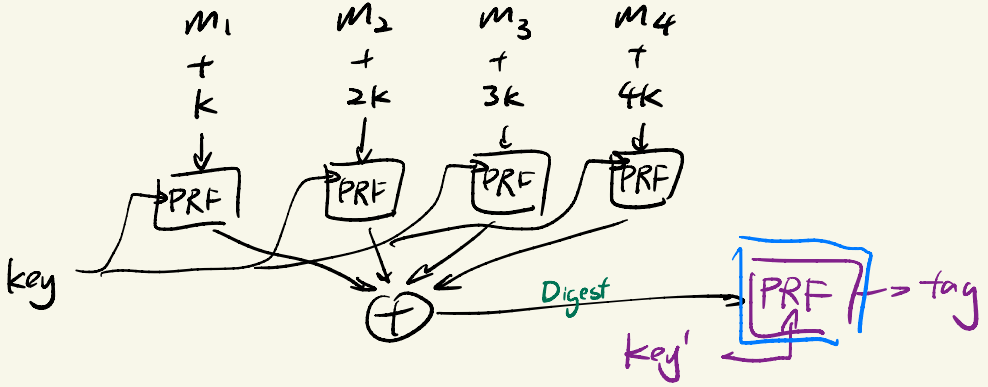


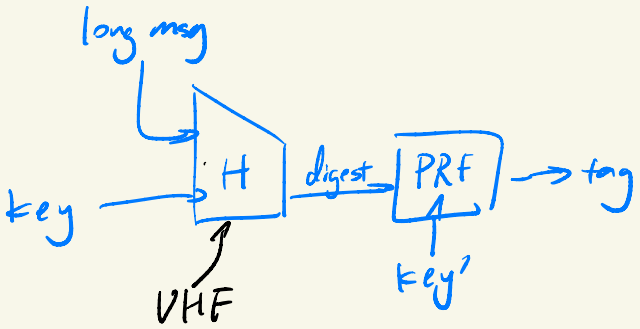


NMAC (cascade)



PMAC





VHF + PRF for fixed-length
⇒ MAC for arbitrary-length

Def. keyed hash function

$Gen(1^\lambda) \to key$

$H(key, m) \to d \in T_\lambda$ (e.g. $T_\lambda = \{0,1\}^\lambda$)

Def. Universal hash function (UHF)

$\forall$ adversary A ← p.p.t or poly

$A(1^\lambda) \to (m_0, m_1)$ s.t. $m_0 \neq m_1$

$Gen(1^\lambda) \to key$

A wins iff $H(key, m_0) = H(key, m_1)$

- H is a statistical universal hash function if $\forall$ adversary A, $Pr[A \text{ wins}] \leq negl(\lambda)$
- H is computational universal hash function if $\forall$ p.p.t. A, $Pr[A \text{ wins}] \leq negl(\lambda)$

VHF Construction:

$\boxed{\mathbb{F} = \mathbb{Z}_p \text{ or } \mathbb{F}_{2^\lambda}}$

$m = (m_0\ m_1\ \cdots\ m_t) \in \mathbb{F}^{t}$

$$H(k, m) = \sum_i m_i k^i + k^{t+1}$$

$$= m_0 + m_1 k + m_2 k^2 + \cdots + m_t k^t + k^{t+1}$$

Keyless hash function

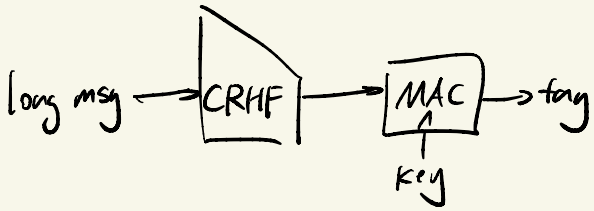
- $H(1^\lambda, msg) \to digest$

Def Collision-Resistence Hash Function (CRHF)

Game
- $A(1^\lambda) \to m_0, m_1$
- A wins iff $H(1^\lambda, m_0) = H(1^\lambda, m_1)$

H is a CRHF iff $\forall$ p.p.t. A, $Pr[A \text{ wins}] \in negl(\lambda)$

CRHF + MAC for fix-length $\Rightarrow$ MAC for arbitrary length



Keyless hash function

public parameter

- $PPGen(1^\lambda) \to PP$
- $H(pp, msg) \to digest$

Game
- $PPGen(1^\lambda) \to PP$
- $A(1^\lambda, PP) \to m_0, m_1$ s.t. $m_0 \neq m_1$
- A wins iff $H(pp, m_0) = H(pp, m_1)$

How to construct hash functions (CRHFs)

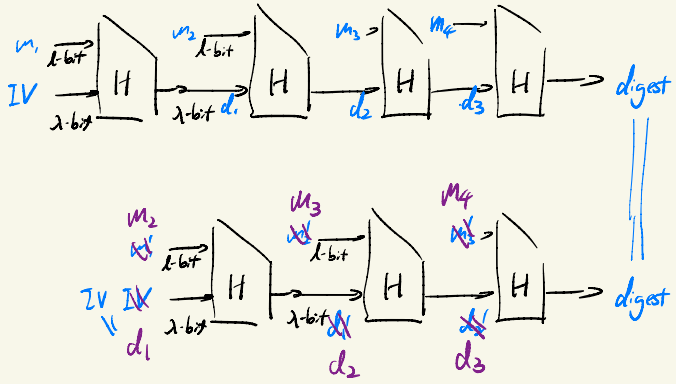
given CRHF: $H: \{0,1\}^{n(\lambda)} \to \{0,1\}^{\lambda}$ $\quad n(\lambda) = \lambda + l$

want CRHF $H': \{0,1\}^{*} \to \{0,1\}^{\lambda}$

sample $x \in \{0,1\}^{n(\lambda)}$

$y = H(x)$

Claim hard to invert y to find x' s.t. $H(x') = y$



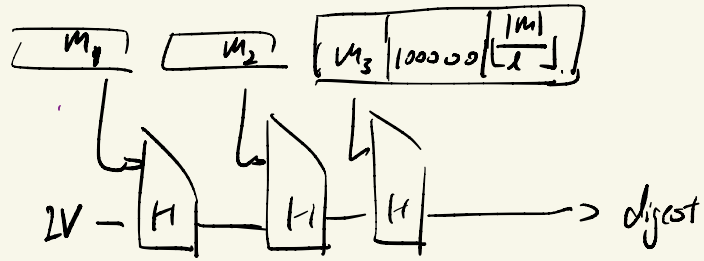
① Solution 1:

Additionally assume hardness of inverting $H'(IV)$

② Solution 2:

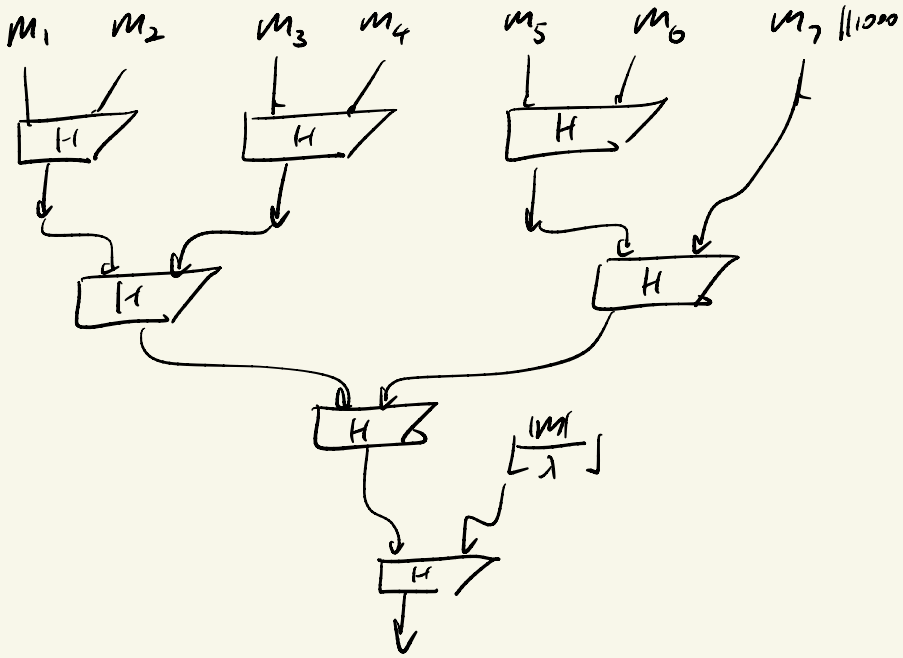
Padding

$m = m_1 \| m_2 \| m_3$



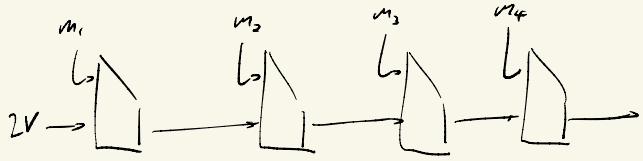
Merkle-Tree

'CRHF $H: \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$

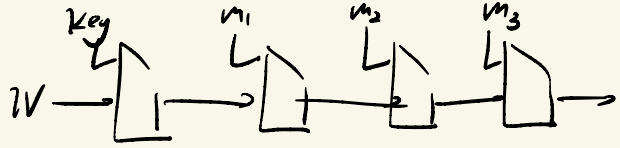


Merkle-Damgård

CRHF construction

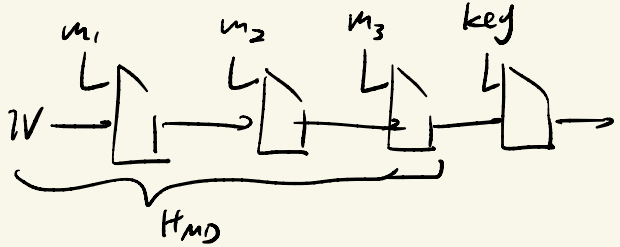


in ROM



"prefix-free PRF"

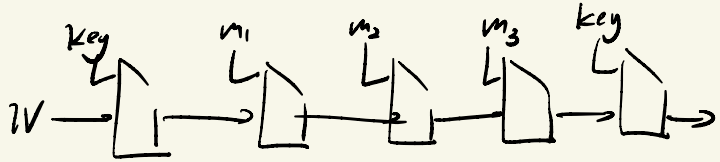
Prepend key $(k, m) \to H(k \| m)$



"PRF"

Append key $(k, m) \to H(m \| k)$

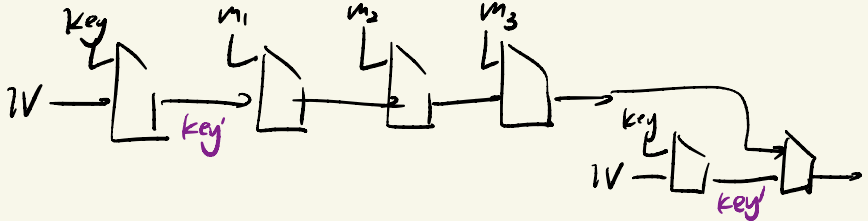
Envelop $(k, m) \to H(k \| m \| k)$



"PRF"

2-nest (HMAC)

$(k, m) \to H(k \| H(k \| m))$



"PRF"

keyless hash H

Preimage Attack given y — find x s.t. $H(x) = y$

2nd-Preimage Attack given x — find $x' \neq x$ s.t. $H(x) = H(x')$

given Δ — find x, x' s.t. $H(x) - H(x') = \Delta$

Collision Attack — find $x \neq x'$ s.t. $H(x) = H(x')$

t-way Collision Attack — find distinct $x_1 \cdots x_t$ s.t. $H(x_1) = \cdots = H(x_t)$

$f(\cdots)$ is low-degree polynomial — find x_1, x_2 s.t. $f(x_1, x_2, H(x_1), H(x_2)) = 0$

$f(x, y) = a_1 x_1 + a_2 x_2 - y$ — find x s.t. $f(x, H(x)) = 0$

$a_1 x_1 + a_2 x_2 = H(x)$

Random Oracle Model (ROM)

model H is a random function

$$H: \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$$
$$H: \{0,1\}^{*} \to \{0,1\}^{\lambda}$$

① Randomly sampled H

② Everyone can access an oracle that computes H

equivalently

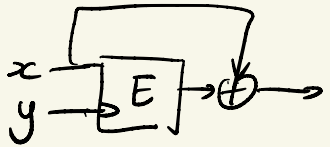
① Everyone can access an oracle that computes H

② $H(x)$ is sampled when x is queried for the first time

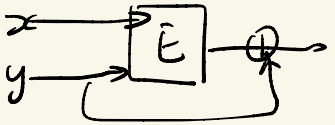
Given a Block cipher (PRP) $E: \{0,1\}^{\lambda} \times \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$

Construct Hash Function (Candidates)

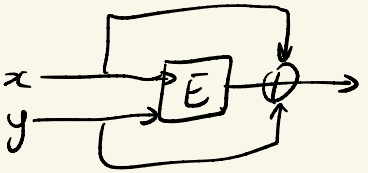
Davies-Meyer $(x, y) \longmapsto E(y, x) \oplus x$



Mortgas-Meyer-Oseas $(x, y) \longmapsto E(x, y) \oplus y$



Miyaguchi-Preneel $(x, y) \longmapsto E(x, y) \oplus y \oplus x$



Ideal Cipher Model

- for each k, sample $E(k, \cdot)$ as a random permutation
- Oracle compute E for everyone

One-time MAC

Game

Adversary $A(1^\lambda) \to m, st$

Challenger $Gen(1^\lambda) \to key$

$MAC(key, m) \to t$

Adversary $A(1^\lambda, t, st) \to m', t'$

A wins if and only if $m' \neq m$ and

$Verify(key, m', c') \to acc$

Q: How to construct $(Gen, MAC, Verify)$

s.t. any computationally unbounded adversary wins a small probability

---

UHF $H(k, m) = m_0 + m_1 k + m_2 k^2 + \cdots + m_\ell k^\ell + k^{\ell+1}$

is not a one-time MAC

$H'(k, m) = k - H(k, m)$

$= m_0 k + m_1 k^2 + \cdots + m_\ell k^{\ell+1} + k^{\ell+2}$

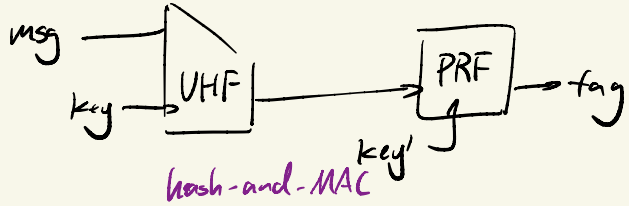
DVHF

(difference unpredictable hash function)

$MAC((k_1, k_2), m)$

$= H'(k_1, m) + k_2$

UHF + PRF ⇒ MAC for arbitrary length



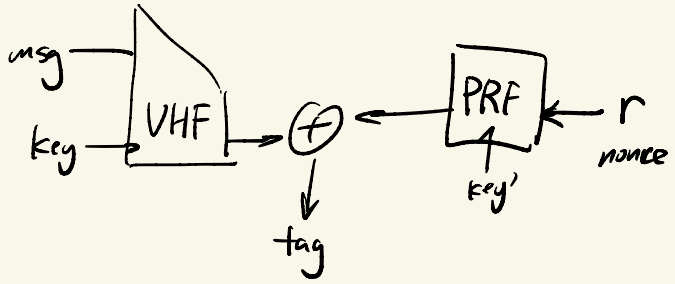
Hash-and-MAC

Adversary makes $q(\lambda)$ queries

the total advantage of A =

$$(q(\lambda))^2 \cdot UHFadv(\lambda) + PRFadv(\lambda)$$

Carter-Wegman MAC



$$PRFadv(\lambda) + Pr[\text{nonce collision}] + q(\lambda) \cdot UHFadv(\lambda)$$

$$\leq \frac{q^2(\lambda)}{2^\lambda}$$

if nonce is a counter security improves