Keyed Hash Functions

Security Notion

Universal: $H: \mathcal{M} \xrightarrow{K} \mathcal{T}$ is called ϵ-universal if for all $m, m' (\neq m) \in \mathcal{M}$, $\Pr_{k \xleftarrow{R} K}\left[H_k(m) = H_k(m')\right] \leq \epsilon$.

Almost-Xor-Universal: $H: K \times \mathcal{M} \to \mathcal{T}$ is called ϵ-axu if for all $m, m' \in \mathcal{M}$, $\Delta \in \mathcal{T}$, $k \in K$, $\Pr_{k \xleftarrow{R} K}\left[H_k(m) \oplus H_k(m') = \Delta\right] \leq \epsilon$

Regular: $H: K \times \mathcal{M} \to \mathcal{T}$ ..... ϵ-regular

$\Pr\left[H_k(m) = \Delta\right] \leq \epsilon$.

Implication

1> H is $\in$-axu implies H is $\in$-universal.

2> Verify other implications, if any.

Keyed Hash Function

① Algebraic Hash (Poly Hash)

$GF(2^n)$

$K = \{0,1\}^n$

$|M_i| = n$

$$H(k, M) = k^{\ell} \odot M_1 \oplus k^{\ell-1} \odot M_2 \oplus \cdots \oplus k \odot (M_\ell \| 10^*)$$

$k^2 = k \odot k$

$k^3 = k^2 \odot k$

$\vdots$

ⓐ PolyHash is ϵ-universal, where $\epsilon = \frac{\ell}{2^n}$

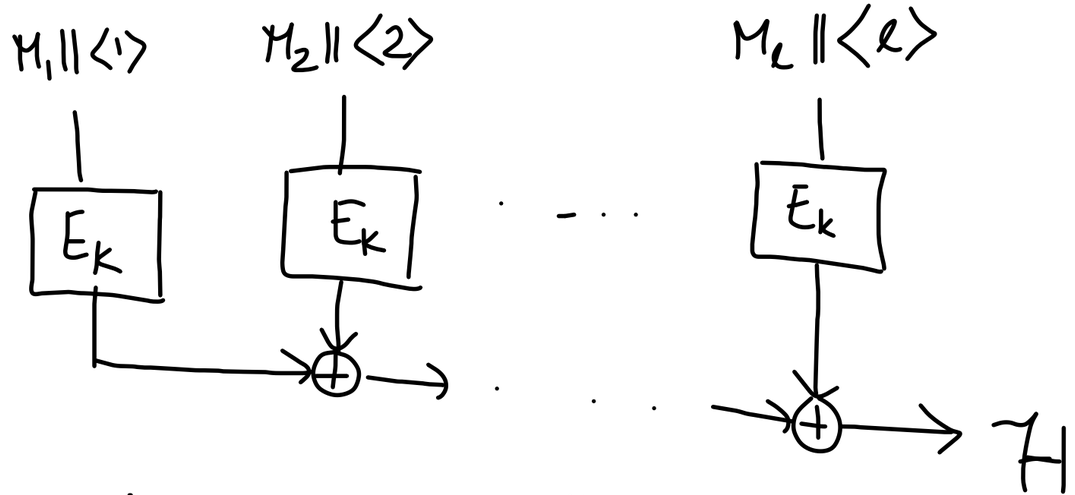
Assume $|M| = |M'| = \ell$

$$\Pr[H(k,M) = H(k,M')] = \Pr[k^{\ell} \odot (M_1 \oplus M_1') \oplus k^{\ell-1} \odot (M_2 \oplus M_2') \oplus \cdots \oplus k \odot (M_\ell \oplus M_\ell') = 0] \leq \frac{\ell}{2^n}$$

ⓑ PolyHash is δ-axu ⇒ Find δ

ⓒ PolyHash is γ-regular ⇒ Find γ

② Light-MAC Hash



Block-cipher Based Hash

M_1, M_2, M_3
M_1, M_2', M_3'

$$Pr\left[H_k(M) = H_k(M')\right]$$

$$= Pr\left[E_k(M_2\|\langle 2\rangle) \oplus E_k(M_2'\|\langle 2\rangle) \oplus E_k(M_3\|\langle 3\rangle) \oplus E_k(M_3'\|\langle 3\rangle) = 0\right]$$

$$\leq \frac{1}{2^n - 3} \leq \frac{2}{2^n}$$

AXU ⇒ ?

Regular ⇒ ?

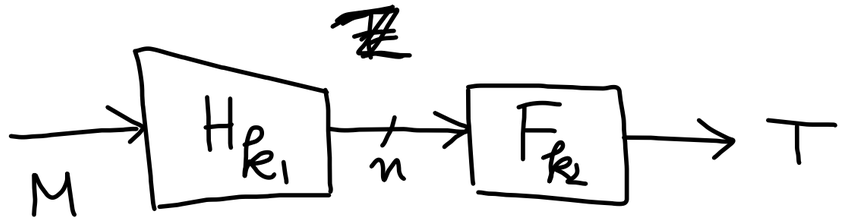
$$Pr\left[H_k(M) = H_k(M')\right] \quad (M \neq M',\ |M| = \ell,\ |M'| = \ell')$$

$$\leq \frac{1}{2^n - (\ell + \ell') + 1}$$

((Assuming $(\ell + \ell') < 2^{n-1}$

$$\leq \frac{1}{2^{n-1}}$$

MACs from Hash Function



UHF, then PRF

If H is ϵ_1-universal & F is ϵ_2-PRF then H∘F is Secure MAC.

$$Pr[\text{Forge}] \leq \binom{q}{2} \cdot \epsilon_1 + \epsilon_2$$

$M_1 \to z_1 \to T_1$
$\vdots$
$M_q \to z_q \to t_q$

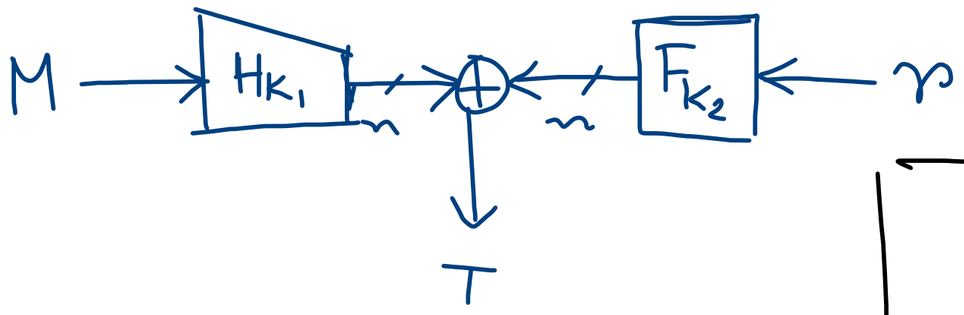
$$Pr[\exists z_i = z_j] \leq \binom{q}{2} \epsilon_1$$

PolyHash → $\frac{q^2 \ell}{2^n}$

$n = 128$, $\ell = 2^{32}$

then I get security upto $q = 2^{48}$.

Wegman-Carter Construction



$MAC(k, M) = (r, T)$

$H \rightarrow \epsilon_1$-axu & F is ϵ_2-PRF

$$Pr[Forge] \leq \epsilon_1 + \epsilon_2 + \frac{\binom{q}{2}}{2^n} + \frac{1}{2^h}$$

$Adv(EUF\text{-}CMA)$

$r \xleftarrow{\$} \{0,1\}^n$

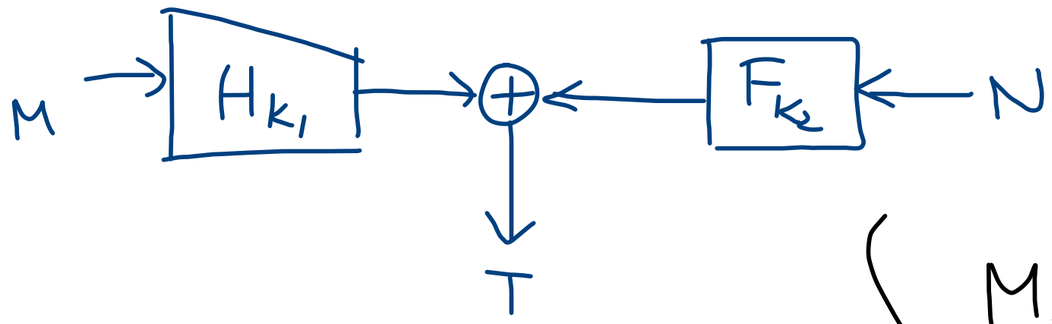
Say, $H_{k_1}(M_1) \oplus H_{k_2}(M_2) = \Delta$

$\Downarrow$

$M_1 \rightarrow (r_1, T_1)$

Forgery $\Rightarrow$ $(M_2, r_1, T_1 \oplus \Delta)$

Nonce-based Wegman Carter



- Katz - Lindell
- Boneh - Shoup (*)

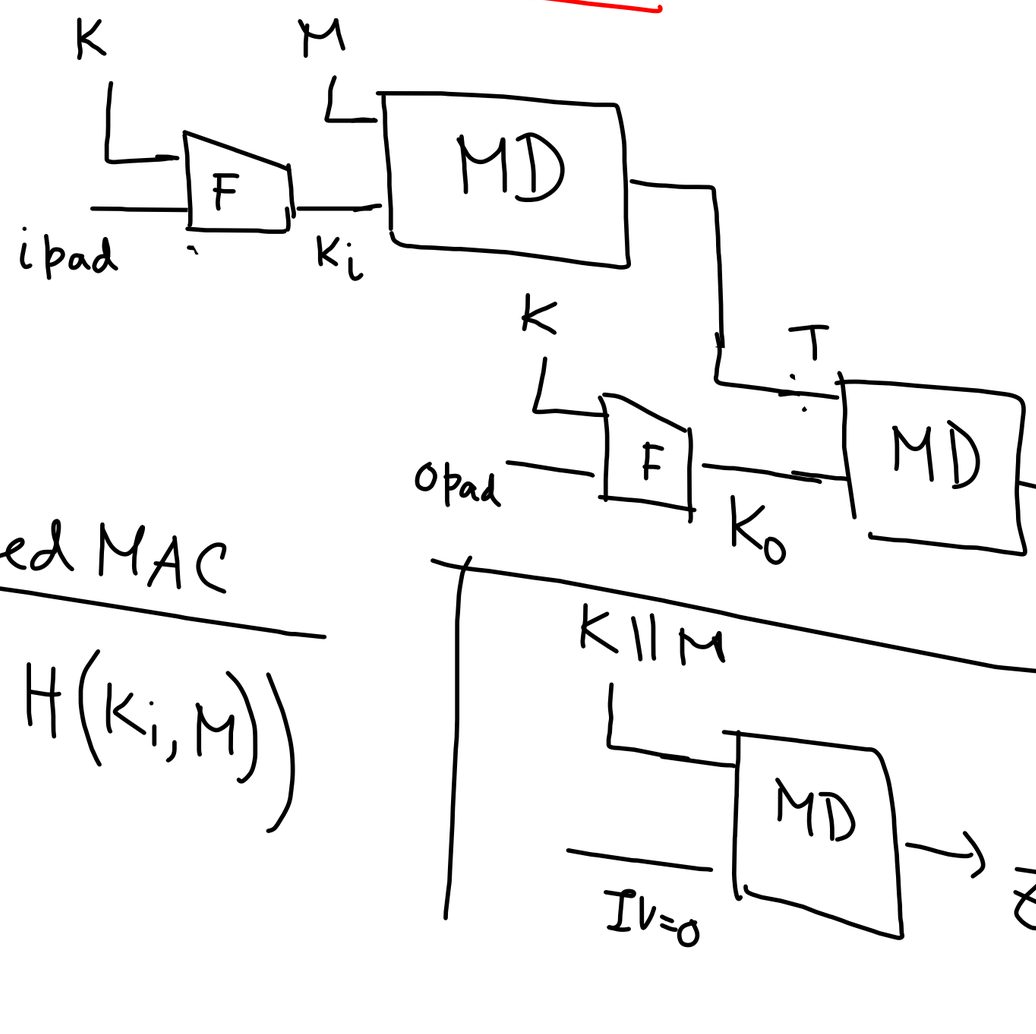
- N → distinct (but no randomness)

$$MAC\left(\underset{(k_1,k_2)}{k}, M, N\right) = H_{k_1}(M) \oplus F_{k_2}(N)$$

H → ϵ_1 - axu , F → ϵ_2 - PRF

NWC $\Rightarrow \left(\epsilon_1 + \epsilon_2 + \frac{1}{2^n}\right)$ - EUF - CMA

HMAC



MD → Merkle Damgard Hash

Nested MAC

$$H(K_o, H(K_i, M))$$

⇒ length-extension attack

Commitment Scheme

Online Auction

Hiding

$z = Com(m, s) \rightarrow$ should not reveal m.

Commit { (m, s) $\xrightarrow{com(m,s)}$

$Com(m, s) = Com(m', s') = z$ ||

Reveal { $(m, s, com(m,s))$

$r \xleftarrow{\$} \{0,1\}^n$

$H(m \| r)$

Binding