Keyed Hash Functions

— Universal

— Almost XOR Universal (AXU)

— Regular

PolyHash$_K(M)$

$M \leftarrow M_1 \| M_2 \| \cdots \| M_\ell$

return $\left(K^{\ell+1} \oplus M_1 \odot K^\ell \oplus M_2 \odot K^{\ell-1} \oplus \cdots \oplus M_\ell \odot K\right)$

$$\begin{cases} K^2 = K \odot K \\ K^3 = K \odot K \odot K \\ \vdots \end{cases}$$

$\mathcal{H}$ is ϵ-univ if

$$\Pr_K\left[H_K(M_1) = H_K(M_2)\right] \leq \epsilon$$

$\mathcal{H}$ is ϵ-axu if $\forall \delta$,

$$\Pr_K\left[H_K(M_1) \oplus H_K(M_2) = \delta\right] \leq \epsilon.$$

$\mathcal{H}$ is ϵ-reg if $\forall \delta$,

$$\Pr_K\left[H_K(M_1) = \delta\right] \leq \epsilon.$$

PolyHash$_K(M_1 \| M_2 \| \cdots \| M_\ell)$

return $\underline{K^{\ell+1} \oplus K^{\ell} \circ M_1 \oplus K^{\ell-1} \circ M_2 \oplus \cdots \cdots \oplus K \circ M_\ell}$

$M = M_1 M_2 \cdots M_\ell$

$M' = M_1' M_2' \cdots M_{\ell'}'$

$\Pr[H_K(M) = H_K(M')]$

$$\boxed{\frac{\ell+1}{2^n} - \text{AXU}}$$

$\Pr[K^{\ell+1} \oplus K^{\ell} \circ M_1 \oplus \cdots \oplus K \circ M_\ell$
$= K^{\ell'+1} \oplus K^{\ell'} \circ M_1' \oplus \cdots \oplus K' \circ M_{\ell}']$

<u>Case 1</u> $\ell > \ell'$ (w.l.o.g)

$\Pr[K^{\ell+1} \oplus \cdots \cdots \oplus \cdots = 0] \le \dfrac{\ell+1}{2^n}$

<u>Case 2</u>
$\ell = \ell'$

$\Pr[K^{i} \oplus \cdots = 0] \le \dfrac{\ell}{2^n}$

$i \le \ell$

Q Is $\text{PolyHash}'_K(M_1 \| \cdots \| M_\ell)$

$= K^\ell \odot M_1 \oplus K^{\ell-1} \odot M_2 \oplus \cdots \oplus K \odot M_\ell$ an AXU? ①

$= K^{\ell-1} \odot M_1 \oplus K^{\ell-2} \odot M_2 \oplus \cdots \oplus K \odot M_{\ell-1} \oplus M_\ell$ an AXU? ②

② $\Rightarrow$

$\text{PolyHash}'_K(M_1 \| M_2) = K \odot M_1 \oplus M_2$

$\text{PolyHash}'_K(M_1 \| 0) = K \odot M_1 \oplus 0$

$PH'_K(M_1 \| M_2) \oplus PH'_K(M_1 \| 0) = M_2$

Not AXU

① $\Rightarrow$

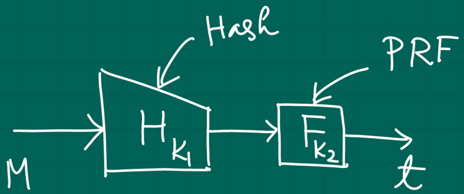
$\text{PolyHash}'_K(0 \| 0) = 0$

$\text{PolyHash}'_K(0 \| 0 \| 0) = 0$

Not AXU

Designing MACs

① Universal Hash Function, PRF Composition

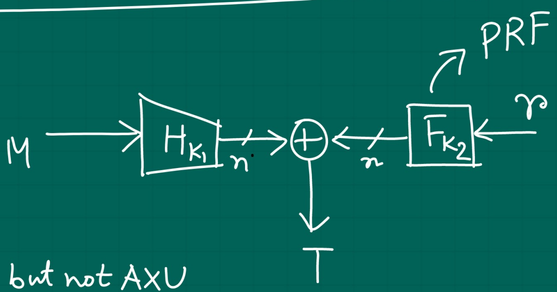


H is ϵ-AXU

$$\binom{q}{2} \cdot \epsilon + \epsilon'_{PRF}$$

② Wegman-Carter MAC

$M \in \{0,1\}^*$



$r \xleftarrow{\$} R$

return (r, t)

$\mathcal{H}$ is Universal but not AXU

$\Downarrow$

$$H_K(M_1) \oplus H_K(M_2) = \delta$$

ϵ_1- $\quad \epsilon_2$-

$M_1 \Rightarrow (r, T) \qquad T = F_K(r) \oplus H_K(M_1)$

Forge $\left(M_2, (r, T \oplus \delta) \right) \qquad T \oplus \delta = F_K(r) \oplus H_K(M_2)$

$\mathcal{H}$ is AXU, $F \to$ PRF

$$Adv^{MAC}_{WC}(\mathcal{A}) \leq \epsilon_1 + \epsilon_2 + \frac{\binom{q}{2}}{R} + \frac{1}{2^n}$$

$$M_1 \rightarrow (r, T_1)$$
$$M_2 \rightarrow (r, T_2)$$

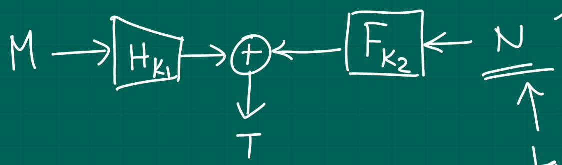
$$T_1 = \cancel{F_{K_2}(r)} \oplus H_{K_1}(M_1)$$
$$T_2 = \cancel{F_{K_2}(r)} \oplus H_{K_1}(M_2)$$

$$\underbrace{T_1 \oplus T_2}_{\delta} = H_{K_1}(M_1) \oplus H_{K_1}(M_2)$$

$$M_1 \rightarrow (r', T_1')$$

$$\text{Forge}\left(M_2, (r', T_1' \oplus \delta) \right)$$

③ Nonce-based WC



$\Rightarrow$ Domain $\rightarrow$ n-bit $\{0,1\}^n$

takes different value at each Query

ϵ_1-AXU, ϵ_2-PRF

$$\text{MAC Advantage} \leq \left(\epsilon_1 + \epsilon_2 + \frac{1}{2^n}\right)$$