Keyed Hash Function:

$F : K \times D \to R$

for every $k \in K$

$F_k : D \to R$

$$\Pr_{k \leftarrow \$ K}\left[A^{F_k()} = 1\right] - \Pr_{RF \leftarrow Func(D,R)}\left[A^{RF()} = 1\right]$$

$H : K \times M \to R$

H is the collection of

$\{H_k : M \to R\}_{k \in K}$

Properties of Keyed Hash.

(a) Universal Advantage

A family of keyed hash fn: $H : K \times X \to Y$ is called ϵ-universal if for every $x \neq x' \in X$

$$\Pr_{k \leftarrow_{\$} K}\left[H_k(x) = H_k(x') \right] \leq \epsilon$$

(b) Almost-xor-universal advantage:

A family of keyed hash fns $H: K \times X \to Y$ is ϵ-AXU if for every $x \neq x' \in X$ and for every $\Delta \in Y$

$$\Pr\left[H_K(x) \oplus H_K(x') = \Delta\right] \leq \epsilon$$

(c) Regular Advantage

A family of keyed hash fns $H: K \times X \to Y$ is ϵ-regular if for every $x \in X$ and for every $\Delta \in Y$, $\Pr[H_K(x) = \Delta] \leq \epsilon$

Polynomial Hash fn.

Conditional padding

$$GF(2^n) \equiv (\{0,1\}^n, \oplus, \cdot)$$

$$Poly : \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$$

Suppose $M \in \{0,1\}^* = \bigcup_{i \geq 0} \{0,1\}^i$

$|M|$, $\boxed{\ell = \frac{|M|}{n}}$

Suppose $|M|$ is a multiple of n.

$M = M_1 \| M_2 \| \cdots \| M_\ell$, where $M_i \in \{0,1\}^n$

When $|M| \equiv 0 \mod n$

$$Poly_{K_h}(M) = (M_1 K_h^{\ell} \oplus M_2 K_h^{\ell-1} \oplus \cdots \oplus M_\ell K_h)$$

When $|M| \not\equiv 0 \mod n$

$$M^* \leftarrow M \| \underbrace{1 0^{(n - |M| \bmod n - 1)}}_{\text{min. no. of } 0}$$

Conditional padding does not make the polyhash fn. a secure keyed hash fn.

Can you find out a pair of msg M, M' such that

$$\Pr\left[\mathrm{Poly}_{K_h}(M) = \mathrm{poly}_{K_h}(M')\right] = 1$$

Provided you have the conditional padding.

Conditional padding does not make the polyhash fn a secure keyed hash fn

Can you find out a pair of msg M, M' such that

$$\Pr\left[Poly_{K_h}(M) = poly_{K_h}(M')\right] = 1$$

Provided you have the conditional padding.

Example: $M = m_1 \| \underbrace{1\,1\,0^{n-2}}_{m_2}$ $\quad M' = m_1 \| 1$

Conditional padding does not work!

Remedy: Always Pad!

With the defn. of always padding, we can show that polyhash fn. is $\ell/2^n$-universal, $\ell/2^n$-AXU and $\ell/2^n$-regular; where ℓ is the max. no. of msg. blocks.

Proof idea:

Let $M \neq M'$

$$\Pr[\mathrm{Poly}_{K_h}(M) = \mathrm{Poly}_{K_h}(M')] = \Pr\left[\left(K_h^{\ell} \cdot C_1 \oplus K_h^{\ell-1} \cdot C_2 \oplus \cdots \oplus K_h \cdot C_\ell\right) = 0\right] \leq \frac{\ell}{2^n}$$