Hash Function

- Keyed Hash Function
- Un-keyed Hash Function
- Security Properties
  - Collision resistance
  - Pre-image resistance
  - 2nd Pre-image resistance
  - } Unkeyed
  - Universal
  - almost xor universal
  - regular
  - } Keyed
- Random oracle Model.
- Constructions
  - MD Hash
  - Sponge Hash
- Attacks (Collision)
  - Birthday Attack
  - Joux's Multicollision attack
- Applications
  - Real life Applications
  - Applications in designing MACs

(Unkeyed) Hash Function

$H: \mathcal{M} \to \mathcal{T}$

Typically, $\mathcal{T} = \{0,1\}^\ell$

$\mathcal{M}$ can be arbitrarily large

$|\mathcal{M}| = \{0,1\}^\ell \cup \cdots \cup \{0,1\}^{2^{512}}$

$\ell \to 256/512$

Security Properties

Collision Resistance

Find Collision

$(m, m') \leftarrow \mathcal{A}$ s.t.

$H(m) = H(m')$; $m \neq m'$

H is CR if $\forall \mathcal{A}$,

Find Collision is difficult

Pre-image Resistance

Find_PI(y)

$m \leftarrow \mathcal{A}$ s.t.

$H(m) = y$

H is PIR if $\forall \mathcal{A}$,

FindPI is difficult

2nd Pre-image Resistant

Find_2PI(m)

$m' \leftarrow \mathcal{A}$ s.t.

$H(m) = H(m')$

H is 2PIR if $\forall \mathcal{A}$,

Find-2PI is difficult.

Implications

If H is collision resist then H is 2nd Pre-image Resistant.

Proof.

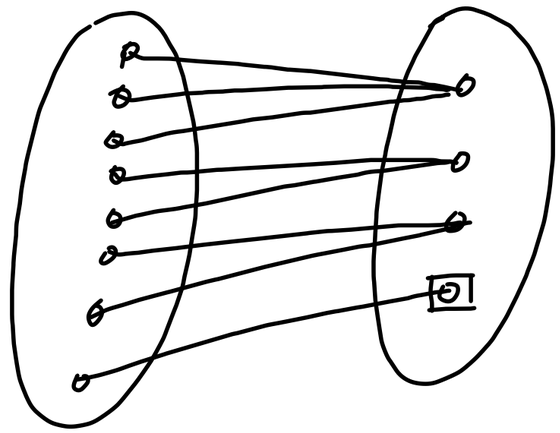
- $\mathcal{A}_{2PI}$ breaks 2nd Pre-image of H.
- $m \xleftarrow{\$} \mathcal{M}$. Send m to $\mathcal{A}_{2PI}$
- $\mathcal{A}_{2PI}$ returns m'.
- return (m, m')

Implications

If H is collision resist then H is Pre-image Resistant $\left(|M| \geq 2|T|\right)$

Proof.

- $\mathcal{A}_{2PI}$ breaks Pre-Image of H
- $y \xleftarrow{\$} T$. Ask $\mathcal{A}_{2PI}$ to find Pre-Image of H twice.
- Let the o/ps be m, m'
- Return (m, m')



$$\Pr[\text{Coll}] = \left(\frac{1}{4}\cdot 0 + \frac{1}{4}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{2}{3}\right) = \frac{1}{4} + \frac{1}{6} = \frac{5}{12}$$

$$\frac{|M|}{|T|} > 2 \qquad \frac{1}{2|T|}$$

$\sum x_i = |M|$

$$\left(\frac{x_1-1}{x_1} + \frac{x_2-1}{x_2} + \frac{x_3-1}{x_3} + \frac{x_4-1}{x_4}\right)$$

$$(1+1+1+1) - \left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4}\right)$$

$$4 - ($$

$[x] = \{x_1 : h(x_1) = h(x)\}$

$[x_1], [x_2], \ldots, [x_\tau]$

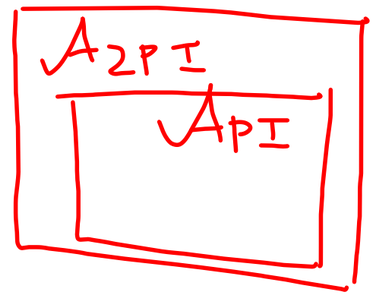
$\downarrow \qquad\qquad \downarrow$

$|[x_1]| \qquad\qquad |[x_\tau]|$

$$\Pr[\text{Coll}] = \frac{1}{|T|}\sum_{i=1}^{|T|}\frac{|[x_i]|-1}{|[x_i]|}$$

Implications

If H is 2PI-resistant then H is Pre-image Resistant $\left(|M| \geq 2|T|\right)$.

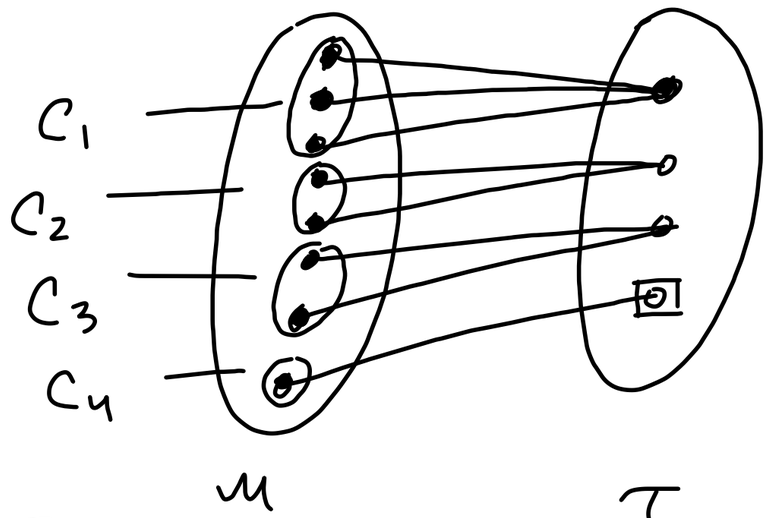


Proof.

- A_{PI} breaks Pre-Image of H
-
  - $x \xleftarrow{\$} M$. Ask A_{PI} to find Pre-Image of $H(x)$.
  - Suppose A_{PI} returns x'
  - Return x'

$\Rightarrow$ Successful if $x \neq x'$

Note: This implies if H is Collision resistant then it is PI resistant. (Assuming $|M| \geq 2|T|$)



$$\Pr[\text{Coll}] = \frac{1}{8}\cdot\frac{2}{3}\cdot 3 + \frac{1}{8}\cdot\frac{1}{2}\cdot 4 + \frac{1}{8}\cdot 0.1$$

$$= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

$\frac{|M|}{|\tau|} > 2$

$\frac{1}{2|\tau|}$

$\Pr[\text{Succ}]$

$$= \frac{1}{|M|}\sum_{i=1}^{|\tau|}\frac{c_i - 1}{c_i}\cdot c_i$$

$$= \frac{1}{|M|}\left(|M| - |\tau|\right)$$

$$\geq \frac{1}{2}$$

class $\to |\tau|$

$\to C_1, C_2, \ldots, C_{|\tau|}$

$|C_i| = c_i$

$\sum_{i=1}^{|\tau|} c_i = |M|$

Random Oracle Model

— Behaviour of an ideal hash function

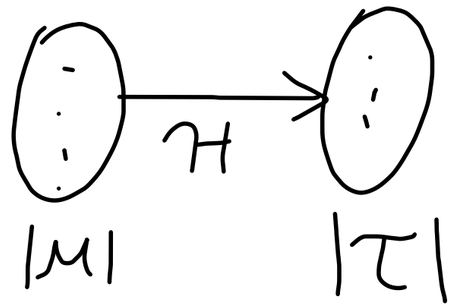
- $h(m_1), h(m_2), \ldots, h(m_q)$ — Known

  $h(m_{q+1}) \rightarrow$ you have to compute the hash value
  (you cannot obtain the value from previous queries)

$$\Pr[h(m_{q+1}) = t \mid \ldots] = \frac{1}{|\tau|}$$

Finding Collisions in Hash Function

(Birthday Paradox) → Among 23 people 2 should share their B'day



$H \rightarrow$ random oracle model

- Makes queries $m_1, \ldots, m_q$
- Check if $h(m_i) = h(m_j), \forall i \neq j$ (Coll$_{ij}$)
- If Coll$_{ij}$ return (m_i, m_j)

- Exhaustive
  - ↳ Makes $m_1, \ldots, m_{|T|+1}$ many queries
  - ↳ You will get a collision

$E_i \Rightarrow$ event that $H(m_i) \notin \{H(m_1), \ldots, H(m_{i-1})\}$

$$Pr[E_i \mid E_1 \wedge E_2 \wedge \ldots \wedge E_{i-1}] = 1 - \frac{(i-1)}{|T|}$$

$Pr[E_1] = 1$

$Pr[E_2] = 1 - \frac{1}{|T|}$

$$Pr[\text{No Coll}] = Pr[E_1 \wedge E_2 \wedge E_3 \cdots \wedge E_q] = \prod_{i=1}^{q} \left(1 - \frac{(i-1)}{|T|}\right)$$

$$\approx e^{-\sum_{i=0}^{q-1} \frac{i}{|T|}}$$

$$\approx e^{-\frac{q(q-1)}{2|T|}}$$

$(1-x) \approx e^{-x}$ for very small x

$$Pr[\text{No Coll}] \leq \frac{1}{2}$$

$$e^{-\frac{q(q-1)}{2|T|}} \leq \frac{1}{2}$$

$$q \geq 1.17\sqrt{T}$$

(*)

Finding Pre-image or 2nd-Pre-image of A Hash

Given y, find $h^{-1}(y)$

- For $i = 1(1)\ q$
- guess m_i
- If $h(m_i) = y$
- return m_i

$E_i :=$ i^{th} step success and no success before.

$$Pr[E_i] = \frac{1}{|T|}$$

$$Pr[\text{Succ}] = Pr[E_1 \vee E_2 \cdots \vee E_q] = \frac{q}{|T|}$$

$$\frac{q}{|T|} \geq \frac{1}{2} \quad q \geq \frac{|T|}{2} \Rightarrow \#\text{queries} = O(|T|).$$

Hash Construction

Compression function

↳ $f: \{0,1\}^r \times \{0,1\}^c \to \{0,1\}^c$

(fixed length hash function from (r+c) bit to c bit)

Fix r & c

↙

(say r=64, c=128)

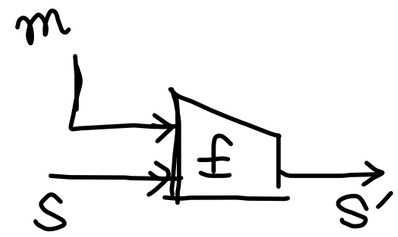
Suppose, you are given a collision resistant f. Can you compute a hash function from any domain? (Domain Extension).

Given $f: \{0,1\}^{r+c} \to \{0,1\}^c$, Can you construct $H: \{0,1\}^* \to \{0,1\}^c$

↓ (secure)

↓ (secure)

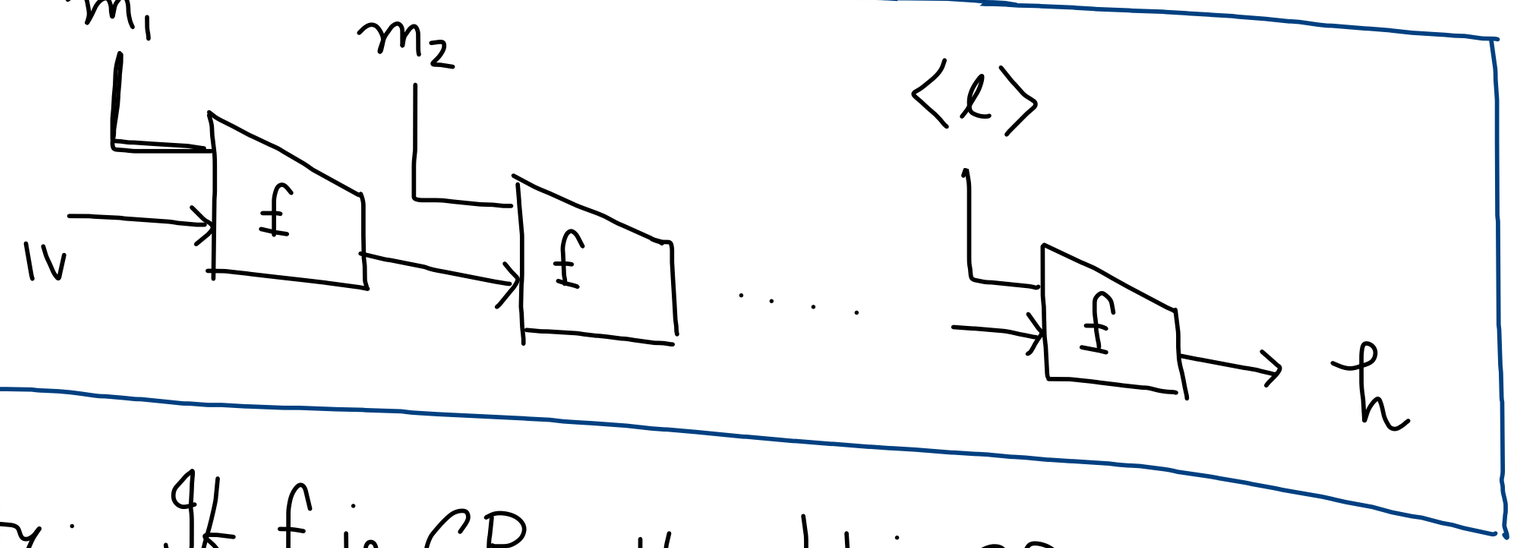
Merkle-Damgård Construction



$\underline{H(M)}$

$M \rightarrow Pad(M) = \underbrace{M \| 10^* \| \langle \ell \rangle}_{c \cdot r \text{ bits}} \rightarrow \left\lceil \frac{|M|}{r} \right\rceil$

$Pad(M) = m_1 \| m_2 \| \cdots \| m_{c-1} \| \langle \ell \rangle$

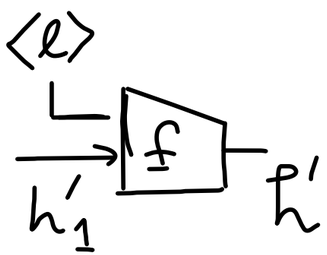


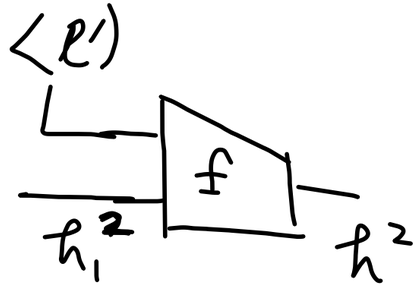
Security: If f is CR, then H is CR.

Suppose $\mathcal{H}$ is CR. We find M^1, M^2 s.t. $H(M^1) = H(M^2)$.

$h^1 = h^2$

Case 1. $\ell \neq \ell'$

$M^1 \Rightarrow$ 

$M^2 \Rightarrow$ 

Is appending ⟨ℓ⟩ redundant?

Collision in f

$m_1 \; m_2 \; m_3 \; m_4$

$m_1 \; m_2' \; m_3 \; m_4$

Case 2. $\ell = \ell'$

$h_1' \overset{?}{=} h_1^2$

- no → f collision in ℓ^{th} block
- yes → check f coll in $(\ell-1)^{th}$ block
  - no → f coll
  - yes → $m_{\ell-1} = m_{\ell-1}'$

Joux's Multicollision Attack

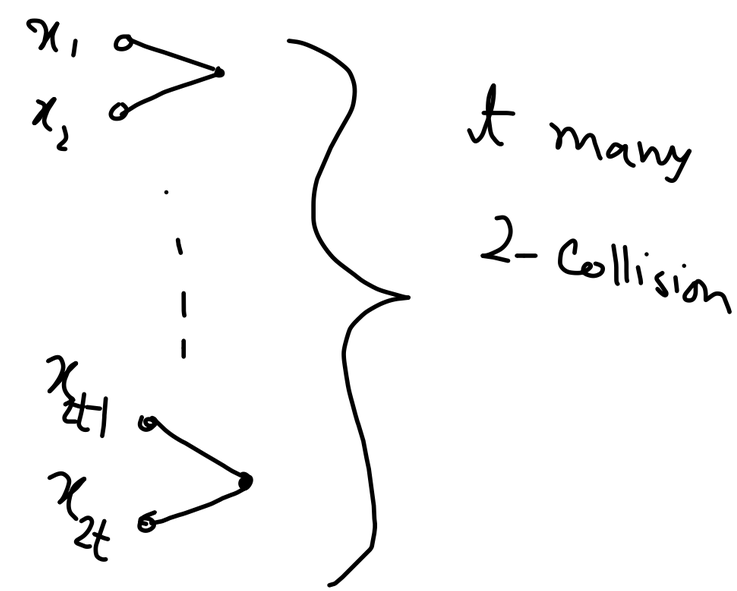
$H: \{0,1\}^* \to \{0,1\}^n$

(Iterated hash functions)

2 collision $\to \sqrt{n}$ queries

t-many 2-collision $\to$ $t\sqrt{n}$ queries

2^t - many 2-collision $\to$ $2^t \cdot \sqrt{n}$ queries



$\Downarrow$ Joux

2^t - many 2-Collision $\Rightarrow$ $t \cdot \sqrt{n}$ queries