Hash Function

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

(*)

Collision Resistant

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

$\mathcal{A}$

1. Find $m_0, m_1 \in \mathcal{M}$
2. $\mathcal{A}$ wins if $H(m_0) = H(m_1)$ ($\Leftrightarrow$ Event Coll)

$\in$

A hash function is collision resistant if $\forall$ PPT $\mathcal{A}$, $Pr[Coll] \leq \epsilon$

Pre-Image

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

$\mathcal{A}(y)$ $\quad y \xleftarrow{\$} \mathcal{T}$

1. Return m
2. $\mathcal{A}$ wins if $H(m) = y$ ($\Leftrightarrow$ PI)

A hash func is ϵ pre-image registant if

$\forall$ PPT $\mathcal{A}$, $Pr[PI] \leq \epsilon$

Second Pre-Image

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

$\mathcal{A}(m)$ $\quad m \xleftarrow{\$} \mathcal{M}$

1. Return m'
2. $\mathcal{A}$ wins if $H(m) = H(m')$ ($\Leftrightarrow$ 2PI)

A hash func is ϵ second pre-image registant if

$\forall$ PPT $\mathcal{A}$, $Pr[2PI] \leq \epsilon$.

① If H is ϵ-Collision Resistant then H is ϵ-Second Preimage Resistant.

A_{2PI} : Given x, find x' s.t. $H(x) = H(x')$

$\underline{A_{CR}}$

1. $x \xleftarrow{\$} M$
2. Give x as i/p to A_{2PI}
3. Obtains x' from A_{2PI}
4. Return (x, x') as collision pair

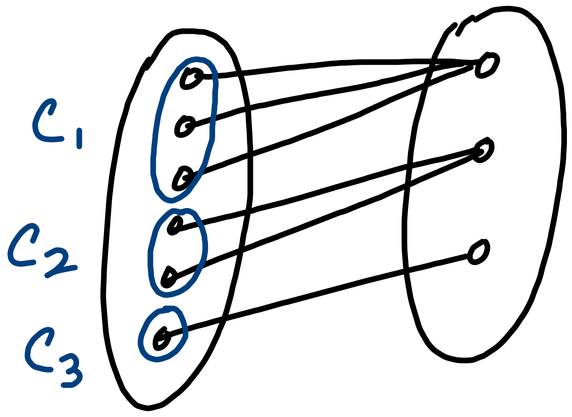
① If H is Collision Resistant (ϵ-) then H is $\left(1-\frac{|\tau|}{|\mathcal{M}|}\right)$ Preimage Resistant.

A_{PI} : Given y, finds $x \in \mathcal{M}$ s.t. $H(x) = y$

A_{CR}

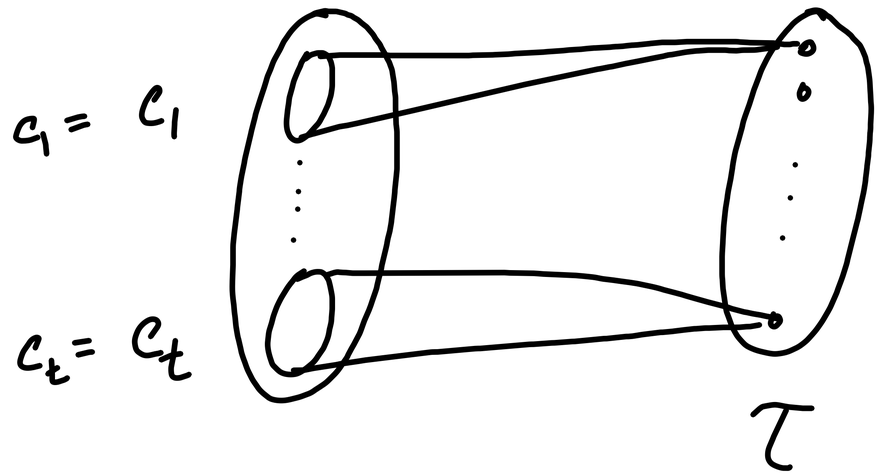
1. $x \xleftarrow{\$} \mathcal{M}$, $y = H(x)$
2. Give y as i/p to A_{PI}
3. Obtains x' from A_{PI}
4. If $x \neq x'$, return (x, x').

$$\begin{cases} H: \mathcal{M} \to \tau \\ |\mathcal{M}| \geq 2|\tau| \\ m \geq 2t \end{cases} \quad |\mathcal{M}| \gg |\tau|$$



$$\frac{1}{2}\cdot\frac{2}{3}+\frac{1}{3}\cdot\frac{1}{2}+0$$

$$=\frac{1}{3}+\frac{1}{6}=\frac{1}{2}$$



$t=|\tau|$

$c_1+\cdots+c_t = |\mu| = m$

$$\frac{c_1}{m}\cdot\frac{(c_1-1)}{c_1}+\cdots+\frac{c_t(c_t-1)}{m\cdot c_t}$$

$$=\frac{(c_1+\cdots+c_t)-t}{m}=\frac{m-t}{m}\geq\frac{1}{2}$$

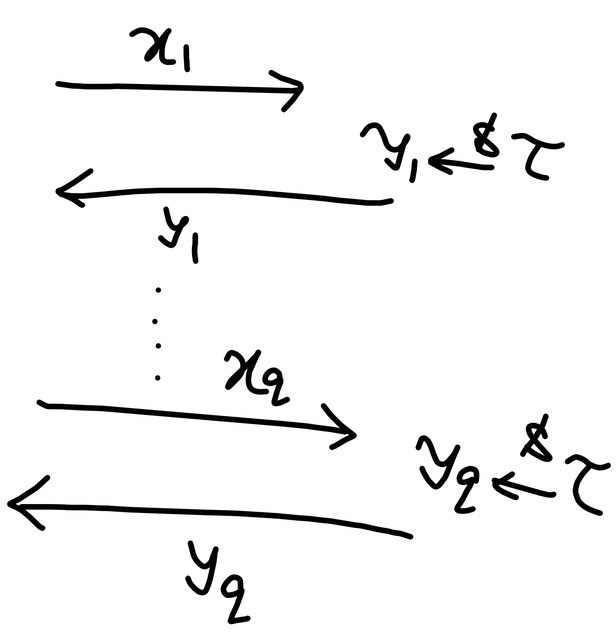
$H \rightarrow$ modeled as Random Oracle

(Stronger assumption)

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

$\forall q$

$$\begin{cases} Pr\left[H(x_q) = y_q \;\middle|\; H(x_1) = y_1, \ldots, H(x_{q-1}) = y_{q-1} \right] \\ = \dfrac{1}{|\mathcal{T}|} \end{cases}$$



$\mathcal{H}$ → Random Oracle

↳ Collision resistant
↳ PI
↳ 2PI

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

A → makes q - many queries

$$y_1, \ldots, y_q \xleftarrow{\$} \mathcal{T}$$

$$\text{Coll} : \exists\, i, j : y_i = y_j \qquad \| \qquad \text{Coll}_{i,j} : y_i = y_j$$

$$\Pr[\text{Coll}_{i,j}] = \frac{1}{|\mathcal{T}|}$$

$$\Pr[\text{Coll}] = \bigcup_{i,j} \Pr[\text{Coll}_{i,j}]$$

$$\leq \sum_{i,j} \Pr[\text{Coll}_{i,j}]$$

$$\leq \binom{q}{2} \cdot \frac{1}{|\mathcal{T}|}$$

$y_1, \ldots, y_q \xleftarrow{\$} \tau$

$\text{Coll}: \exists i, j: y_i = y_j \quad \| \quad \text{NoColl}_i: \nexists a, b \le i \text{ s.t. } y_a = y_b$

$$\Pr[\text{NoColl}] = \prod_{i=2}^{q} \frac{|\tau| - i + 1}{|\tau|}$$

$$\Pr[\text{Coll}] = 1 - \prod_{i=2}^{q} \left(1 - \frac{(i-1)}{|\tau|}\right)$$

$\vdots$

$\geq$

$$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = \frac{|\tau| - i + 1}{|\tau|}$$

$\Pr[\text{NoColl}_2] = \frac{|\tau|-1}{|\tau|}$

$\Pr[\text{NoColl}_3] = \Pr[\text{NoColl}_3 \mid \text{NoColl}_2] \cdot \Pr[\text{NoColl}_2]$

$= \frac{|\tau|-2}{|\tau|} \cdot \frac{|\tau|-1}{|\tau|} = \left(1 - \frac{2}{|\tau|}\right)\left(1 - \frac{1}{|\tau|}\right)$

$\Pr[A]$

$= \Pr[A \mid B] \cdot \Pr[B]$

$+ \Pr[A \mid \bar{B}] \cdot \Pr[\bar{B}]$

B'day Paradox

$y_1, \ldots, y_q \xleftarrow{\$} \tau$

$q \simeq \sqrt{\tau}$

$\text{Coll}: \exists i, j: y_i = y_j \quad \| \quad \text{NoColl}_i: \nexists a, b \le i \text{ s.t. } y_a = y_b$

$$\Pr[\text{NoColl}] = \prod_{i=2}^{q} \frac{|\tau| - i + 1}{|\tau|}$$

$$\Pr[\text{Coll}] = 1 - \prod_{i=2}^{q} \left(1 - \frac{(i-1)}{|\tau|}\right)$$

$$\vdots$$

$$\geq \frac{q^2}{|\tau|}$$

$$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = \frac{|\tau| - i + 1}{|\tau|}$$

$\Pr[\text{NoColl}_2] = \frac{|\tau|-1}{|\tau|}$

$\Pr[\text{NoColl}_3] = \Pr[\text{NoColl}_3 \mid \text{NoColl}_2] \cdot \Pr[\text{NoColl}_2]$

$= \frac{|\tau|-2}{|\tau|} \cdot \frac{|\tau|-1}{|\tau|} = \left(1 - \frac{2}{|\tau|}\right)\left(1 - \frac{1}{|\tau|}\right) \geq \left(1 - \frac{2}{|\tau|}\right)^2$

$\Pr[A] = \Pr[A \mid B] \cdot \Pr[B] + \Pr[A \mid \bar{B}] \cdot \Pr[\bar{B}]$