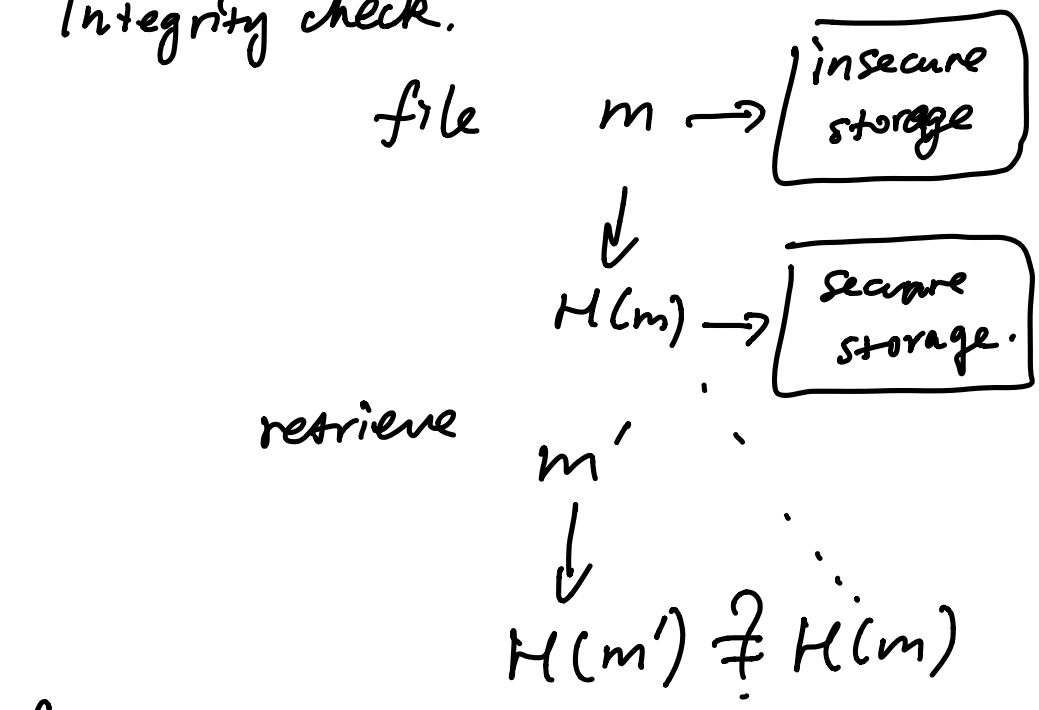
ECE 471/571 Hash functions

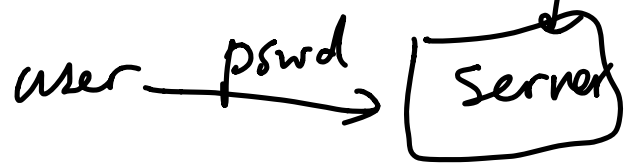
Applications:

Integrity check.



fingerpins.

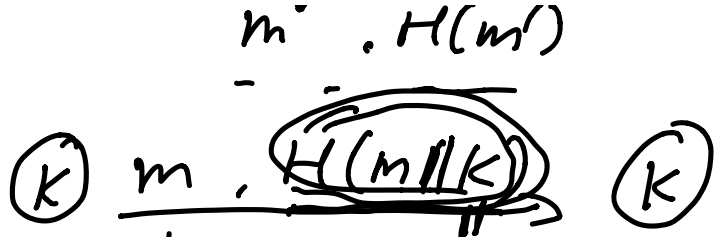
password hashing



- one-wayness of hash function

user authentication

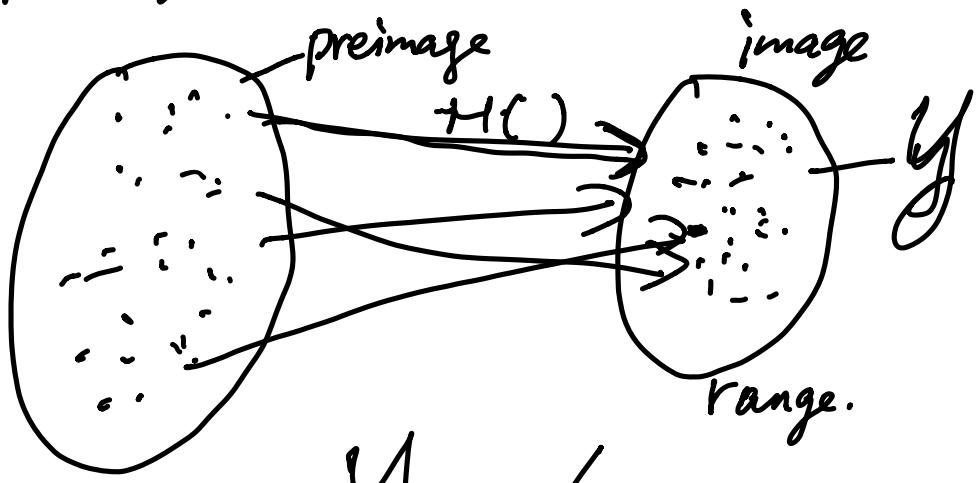
Data authentication



$H(m'||K) \neq H(m||K)$ hard. to satisfy.

---

① preimage resistance



given $y \in Y$. $\not\Rightarrow$ x. s.t. $H(x) = y$.

one-wayness.

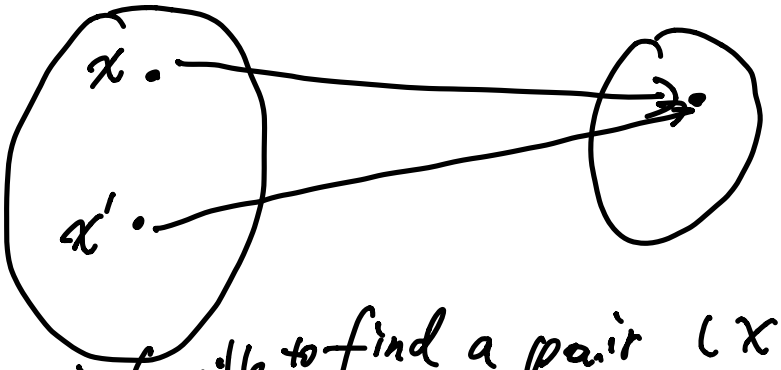
② second preimage resistance

given x, and $h(x)$.

Infeasible to compute $x' \neq x$

s.t $H(x) = H(x')$.

③ Collision-resistance



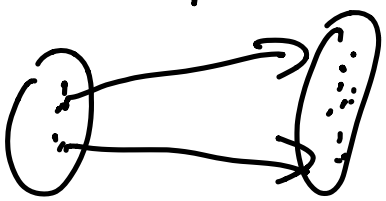
infeasible to find a pair (x, x')

$H(x) = H(x')$ $\quad x \neq x'$

④ randomness.

change in input ⟹ 50% to change output bits

two outputs are uncorrelate



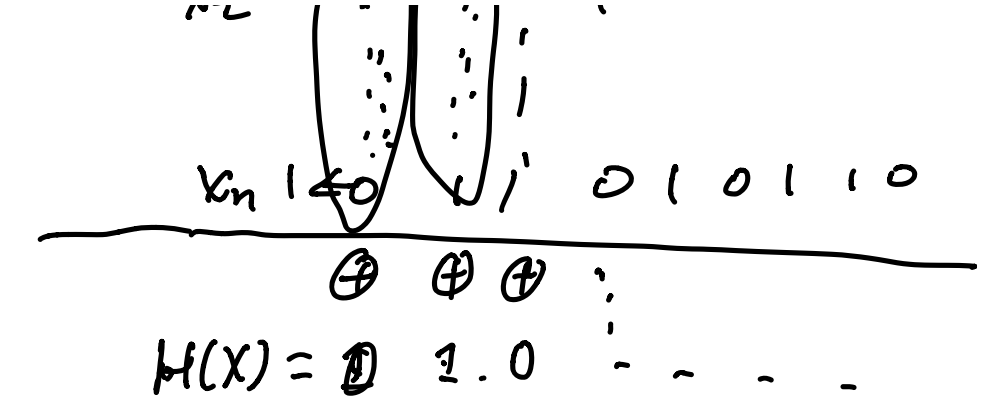
random oracle model.

x,	$H(x)$
⋮	

$x = x_1 \| x_2 \| x_3 \cdots \| x_n$

x_1 ← 0 1 0 1 0 0 0 1 0

x_2 ← 1 0 0 1 0 1 1 0 0



$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

NOT collision resistance

Ex. $H(x) = x^2 \bmod 2$.

if $x=5$. $H(5)=1$

$x=6$. $H(6)=0$

- pre-image: if $H(x)=1 \bmod 2$

  $x = 2k+1$. $k = \pm 1, \pm 2, \cdots \pm 3$.

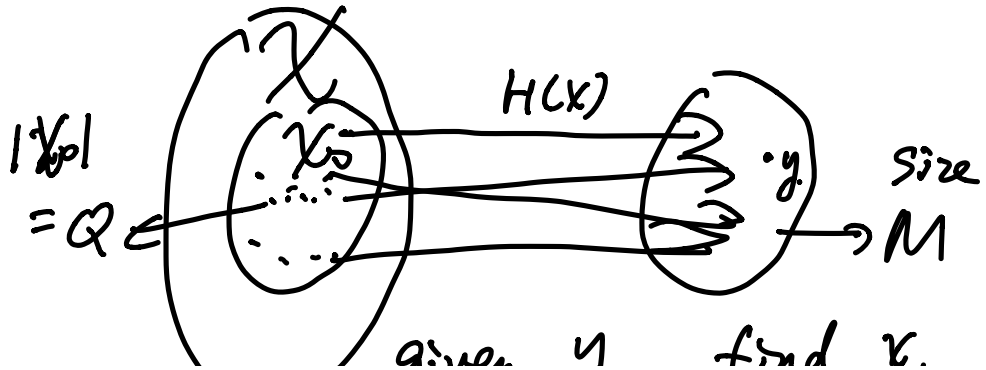
- 2nd pre-image: $x=5$. $H(x)=1$

  ? x' $H(x')=1$. $x'=3$.

- collision. (x, x'). $H(x)=H(x')$

odd # $\Rightarrow$ 1.

even $\Rightarrow$ 0.



given y find x. s.t. $H(x)=y$

given $x_i \in X_0$ $\Pr[H(x_i) = y] = \frac{1}{M}$

$\Pr[$None of $x_i \in X_0$ hash to $y]$

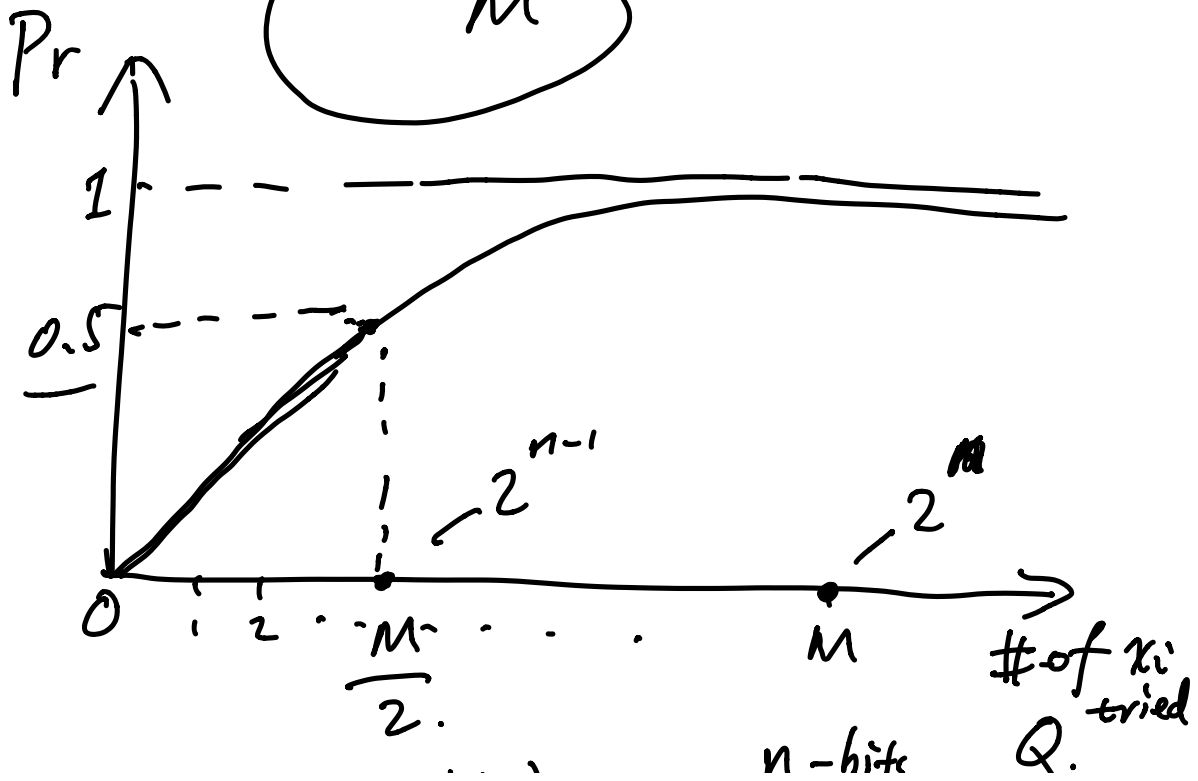
$$= \left(1 - \frac{1}{M}\right)^Q$$

$\Pr[$At least one x_i hash to $y]$

$$= 1 - \left(1 - \frac{1}{M}\right)^Q$$

$$\simeq 1 - \left(1 - \frac{Q}{M}\right).$$

$$= \frac{Q}{M}$$



(n-1 bits).