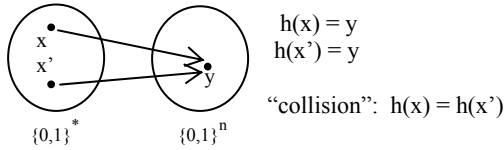


LECTURE 3 NOTES

HASH FUNCTION $h: \{0,1\}^* \rightarrow \{0,1\}^n \approx$ “random” (recall random oracle)



COMPUTATIONAL DIFFICULTY

asymptotic complexity (“rates of growth of difficulty”, $\Theta(2^n)$)
 concrete complexity (constants matter)

PROPERTIES

① “One-Way” – OW, “preimage resistance”
 Infeasible, given randomly chosen $y \in \{0,1\}^n$, to find any x s.t. $h(x) = y$

Given y :

Pick x_1 , check if $h(x_1) = y$
 \vdots
 $\text{Prob}(x_i : h(x_i) = y) = 1/2^n$ } time (# trials) is 2^n (avg)

Back of Envelope Calculation:

2^{30} chips
 $\frac{2^{34} \text{ trials/sec}}{2^{64} \text{ trials/sec}} = \frac{1}{2^{30}}$
 2^{89} trials/yr
 $\pi \times 10^7 \text{ sec/yr} = 2^{25} \text{ sec/yr}$
 2^{80} trials/ half day

SHA-1 has 160-bit output $\rightarrow 2^{71}$ yrs to break OW of SHA-1

② “Collision Resistance” – CR, “strong collision resistance”
 Infeasible of finding two distinct values x, x' s.t. $h(x) = h(x')$ difficulty = $2^{n/2}$

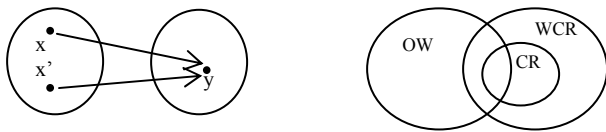
Birthday Problem:

t values x_1, x_2, \dots, x_t people
 $\downarrow h \downarrow h \downarrow h$
 y_1, y_2, \dots, y_t b-days } random function
 $\text{Prob}(y_i = y_j) = 1/2^n$

pairs = $\binom{t}{2} = \frac{t(t-1)}{2} = \Theta(t^2)$ $E[\# \text{ pairs w/ same b-day}] = \binom{t}{2} \cdot 2^{-n}$
 when $\binom{t}{2} \cdot 2^{-n} \approx 1$, expect collision $\rightarrow t \approx 2^{n/2} \rightarrow t \approx 2^{80}$

③ “Weak Collision Resistance” – WCR
 Infeasible, given randomly chosen x , to come up with x' s.t. $h(x') = h(x)$
 2^n time to break “random” hash function

“Thm”: CR \Rightarrow WCR contrapositive: \neg WCR \Rightarrow \neg CR



Thm: OW $\not\Rightarrow$ CR

Proof: Want h that is OW but not CR

Let g be OW
 $y = h(x) = g(z) = g$ applied to all of x except for last bit
 $x = zb$
 $h(0) = h(z1) \rightarrow$ collision! inverting $h \Rightarrow$ inverting g

Thm: CR $\not\Rightarrow$ OW

Proof: Want h that is CR but not OW

Let g be CR
 Let $h(x) = \begin{cases} 0x & \text{if } |x| = n \\ 1g(x) & \text{else} \end{cases} \leftarrow \begin{matrix} \text{no collisions} \\ g(x) \text{ is CR} \end{matrix} \right. h \text{ is CR}$

Thm: WCR $\not\Rightarrow$ CR

Proof: Want h that is WCR but not CR

Let $g^{(i)}(x)$ mean $g(g(g \dots g(x)))$ – g is iteratively applied i times, g is OW and CR

Inputs: (x, x') – pairs of strings w/ arbitrary length

$h(x, x')$ $x = x_0 \xrightarrow{g} x_1 \xrightarrow{g} \dots x_i$ least: ends in 4 zeros or until we take 100 steps ($i=100$)
 \downarrow $x = x_0' \xrightarrow{g} x_1' \xrightarrow{g} \dots x_j$ ends in 4 zeros or $j=100$

Output: $(g^{(i)}(x), g^{(j)}(x'), i+j)$ $h(x, g(x')) = h(g(x), x')$
 as bit string often

APPLICATIONS

- ① Password storage: store $h(\text{pw})$ on disk – Need OW
- ② Detecting file modification: store $h(F)$ for each file in system offline on secure CD – Need WCR
- ③ Secure URL: `` – Need WCR

④ Commitments:

- Alice has some bid x
- Alice can compute $C(x)$
- Alice submits $C(x)$ as her “sealed bid”
- Later on, she can “open” $C(x)$ to reveal x in only one way (binding)

Properties:

- Secrecy - Anyone who uses $C(x)$ should learn nothing about x
- “Non-malleable” – Not possible to come up with commitment to a related value x' (e.g. $x' = x + 1$)

Need OW, CR