Lecture 3 Notes

Hash Function

\( h: \{0,1\}^* \rightarrow \{0,1\}^n \approx \text{"random" (recall random oracle)} \)

\( h(x) = y \)

\( h(x') = y \)

“collision”: \( h(x) = h(x') \)

Computational Difficulty

Asymptotic complexity (“rates of growth of difficulty”, \( \Theta(2^n) \))

Concrete complexity (constants matter)

Properties

   - 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 \( h(x_1) = y \)
   - \( \text{Prob}(x_1: h(x_1) = y) = 1/2^n \) (avg)

   Back of Envelope Calculation:
   - \( 2^{30} \) chips
   - \( 2^{34} \) trials/sec
   - \( \pi \times 10^7 \) sec/yr = \( 2^{25} \) sec/yr
   - \( 2^{64} \) trials/sec
   - \( 2^{80} \) trials half day
   - \( 2^{89} \) trials/yr

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

   - Infeasible of finding two distinct values \( x, x' \) s.t. \( h(x) = h(x') \)

   Difficulty = \( 2^{2n} \)

   Birthday Problem:
   - \( t \) values \( x_1, x_2, \ldots, x_t \) people
   - \( y_1, y_2, \ldots, y_t \) b-days

   \( \text{Prob}(y_1 = y_2) = 1/2^n \)

   \( \text{# pairs} = \binom{t}{2} = \frac{t(t-1)}{2} = \Theta(t^2) \)

   \( \text{E}[\text{# pairs w/ same b-day}] = \frac{1}{2} \cdot 2^n \)

   \( \approx 2^n \) \( \rightarrow t \approx 2^n \)

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 \( \Rightarrow \) CR

Proof: Want \( h \) that is OW but not CR

Let \( g \) be OW

\( y = h(x) = g(x) = g \) applied to all of \( x \) except for last bit

\( x = zb \)

\( h(0) = h(1) \rightarrow \text{collision!} \)

Inverting \( h \Rightarrow \) inverting \( g \)

Thm: CR \( \Rightarrow \) OW

Proof: Want \( h \) that is CR but not OW

Let \( g \) be CR

Let \( h(x) = \begin{cases} \text{if } |x| = n & \text{no collisions} \\ g(x) & \text{else} \end{cases} \)

\( g(x) \) is CR

h is CR

Thm: WCR \( \Rightarrow \) CR

Proof: Want \( h \) that is WCR but not CR

Let \( g^i(x) \) mean \( g(g(\cdots g(x))) \) – \( g \) is iteratively applied \( i \) times, \( g \) is OW and CR

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

\( h(x, x') \rightarrow \begin{cases} x = x_0 \quad \cdots \quad x_i \quad \text{least: ends in 4 zeros or until we take 100 steps (i=100)} \\ x = x_0 \quad \cdots \quad x_j \quad \text{ends in 4 zeros or j=100} \end{cases} \)

Output: \( (g^i(x), g^i(x), i+j) \)

\( h(x, g(x')) = h(g(x), x') \)

As bit string

Often
APPLICATIONS

① Password storage: store h(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: <a href = “http://...” sha1="AC47…09”> – 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