

Collision Resistance

Let $H: M \rightarrow T$ be a hash function

$$(|T| \ll |M|)$$

A collision for H is a pair $m_0, m_1 \in M$

$$\text{s.t. } m_0 \neq m_1 \text{ and } H(m_0) = H(m_1)$$

$$|T| < |M| \Rightarrow \text{collisions must exist?}$$

Def. A function $H: M \rightarrow T$ is collision resistant (CRH) if for all explicit eff. algo A :

$$\text{Pr}[A \text{ outputs collision for } H]$$

is negligible

\Rightarrow hard to find an explicit collision

Std. examples

2001: SHA256, SHA384, SHA512 \leftarrow most widely used, Intel HWT instructions
(since 2019, ARM since 2017)
2014: SHA3-256, SHA3-384, SHA3-512

Immediate approach

small MAC \Rightarrow big MAC

$\rightarrow (s, v)$ secure MAC over (K, M, T) for short msgs.

$\rightarrow H: M^{\text{big}} \rightarrow T$ a CRH

\rightarrow Def (s, v) a MAC over (K, M^{big}, T)

$$\text{where } \begin{cases} S'(k, m) := S(k, H(m)) \\ V'(k, m, t) := V(k, H(m), t) \end{cases}$$

Then: (s, v) a secure MAC, H a CRH

Then (s', v') is a secure MAC

Why CRH needed?

Suppose adv has $m_0 \neq m_1 \in M^{\text{big}}$ s.t. $H(m_0) = H(m_1)$

attack on (s', v') :

\rightarrow req tag on m_0 , get t

\rightarrow output forgery (m_1, t)

\Rightarrow valid forgery b/c $V(k, H(m_1), t)$ succeeds

CAH generic attacks

General attack: "birthday attack"

Bday parolox:

Let $r_0 \dots r_n \xleftarrow{R} \{1, B\}$ be ind. uniform RVs

Then: When $n \geq 1.2\sqrt{B}$ then $\Pr[\exists i \neq j: r_i = r_j] \geq \frac{1}{2}$

Proof:

$$\begin{aligned}\Pr[\exists i \neq j: r_i = r_j] &= 1 - \Pr[\forall i \neq j: r_i \neq r_j] \\&= 1 - \left(1 - \frac{1}{B}\right)\left(1 - \frac{2}{B}\right)\left(1 - \frac{3}{B}\right) \dots \left(1 - \frac{n}{B}\right) \\&= 1 - \prod_{i=1}^n \left(1 - \frac{i}{B}\right) \geq 1 - \prod_{i=1}^n e^{-i/B} \\&\geq 1 - e^{-n^2/2B} \geq 1 - e^{-1/2 \cdot 1.2^2} \approx 0.53\end{aligned}$$

Bday attack:

1. Choose random $m_0 \dots m_{2^{1/2}} \in M$
2. Compute $H(m_0) \dots H(m_{2^{1/2}})$
3. Look for collision
4. If no collision, goto 1.

after exp. 2 iters, will find collision

$$\text{time} = O(\sqrt{|M|})$$

So: 128-bit hash: collision time 2^{64} (bad)
256-bit hash 2^{128} ✓

Generic attack on SHA256 takes ~ same time
as on AES128

Naively: memory $O(2^{42})$

Puzzle: can find collision in time $O(2^{41/2})$
using $O(1)$ space

Quantum

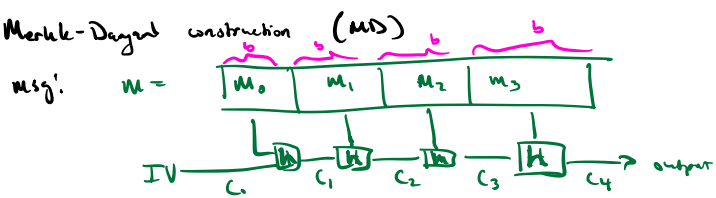
Some evidence that collisions can be found in

time $O(2^{41/3})$, but still open

(lots of space too)

Constructing a CRH

1. Merkle-Damgård construction (MDS)



Terminology: ① $h: \{0, 1\}^b \times T \rightarrow T$ compression func

② $c_0 \dots c_n$ chaining vars

③ IV: fixed initial value

SHA256: input size 512 bits (32 bytes)

pad: ensures msg-len is a multiple of b

$$\text{pad} = [100 \dots 0 \text{msg-len}]$$

$\underbrace{\hspace{1cm}}_{\text{size } b}$

if no space for pad - dummy block.

Thm. h is CRH $\rightarrow H_{\text{MDS}}$ is CRH.