
# Collision resistance

## The Merkle-Damgard Paradigm

# Collision resistance: review

Let $H: M \to T$ be a hash function ( $|M| >> |T|$ )

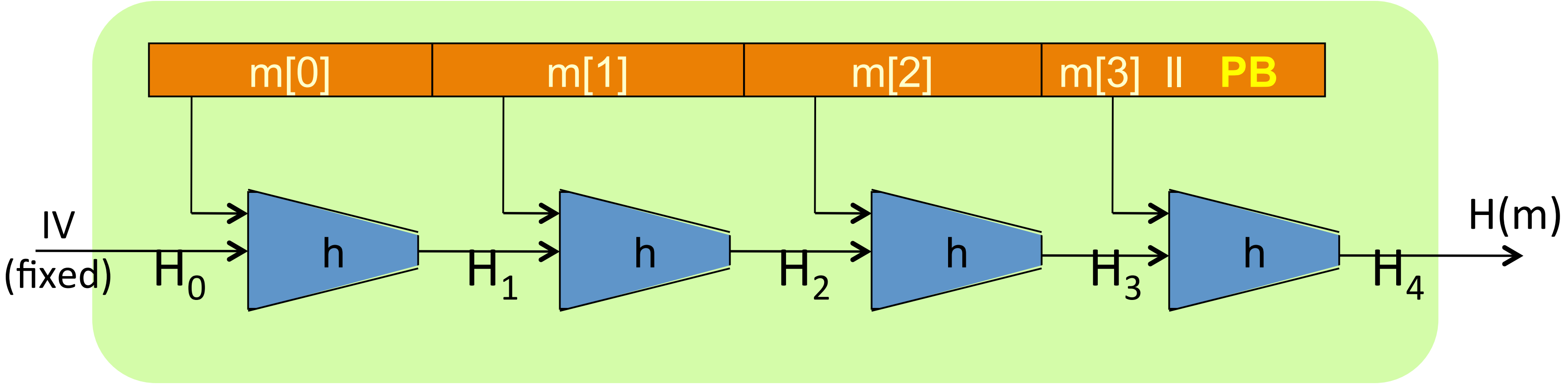
A **collision** for H is a pair $m_0, m_1 \in M$ such that:

$$H(m_0) = H(m_1) \quad \text{and} \quad m_0 \neq m_1$$

Goal: collision resistant (C.R.) hash functions

Step 1: given C.R. function for **short** messages,
construct C.R. function for **long** messages

# The Merkle-Damgard iterated construction




Given $h: T \times X \longrightarrow T$ (compression function)

we obtain $H: X^{\leq L} \longrightarrow T$ . $H_i$ - chaining variables

PB: padding block


If no space for PB add another block

# MD collision resistance

**Thm**: if h is collision resistant then so is H.

**Proof**: collision on H $\Rightarrow$ collision on h

Suppose $H(M) = H(M')$. We build collision for h.

$$IV = H_0 \quad , \quad H_1 \quad , \ \dots \ , \quad H_t \ , \quad H_{t+1} = H(M)$$

$$IV = H_0' \quad , \quad H_1' \quad , \ \dots \ , \quad H'_r, \quad H'_{r+1} = H(M')$$

$$h(H_t, M_t \parallel PB) = H_{t+1} = H'_{r+1} = h(H'_r, M'_r \parallel PB')$$

If $\left[ \begin{array}{l} H_t \neq H'_r \text{ or} \\ M_t \neq M'_r \text{ or} \\ PB \neq PB' \end{array} \right]$

$\Rightarrow$ we have a collision on h.

STOP

Otherwise,

Suppose $\underline{H_t = H'_r}$ and $\underline{M_t = M'_r}$ and $PB = PB'$ $\Rightarrow t = r$

Then: $\boxed{h(H_{t-1}, M_{t-1})} = H_t = H'_t = \boxed{h(H'_{t-1}, M'_{t-1})}$

If $\left[\begin{array}{c} H_{t-1} \neq H'_{t-1} \\ \text{or} \\ M_{t-1} \neq M'_{t-1} \end{array}\right]$ then we have a collision on h. STOP.

otherwise, $H_{t-1} = H'_{t-1}$ and $M_t = M'_t$ and $M_{t-1} = M'_{t-1}$.

Iterate all the way to beginning and either:

$\boxed{\text{(1) find collision on } h \text{ or}}$

(2) $\forall i: M_i = M'_i \Rightarrow M = M'$ ⟸ cannot happen because $M, M'$ are collision on $H$.

$\Rightarrow$ To construct C.R. function,

suffices to construct compression function

# End of Segment