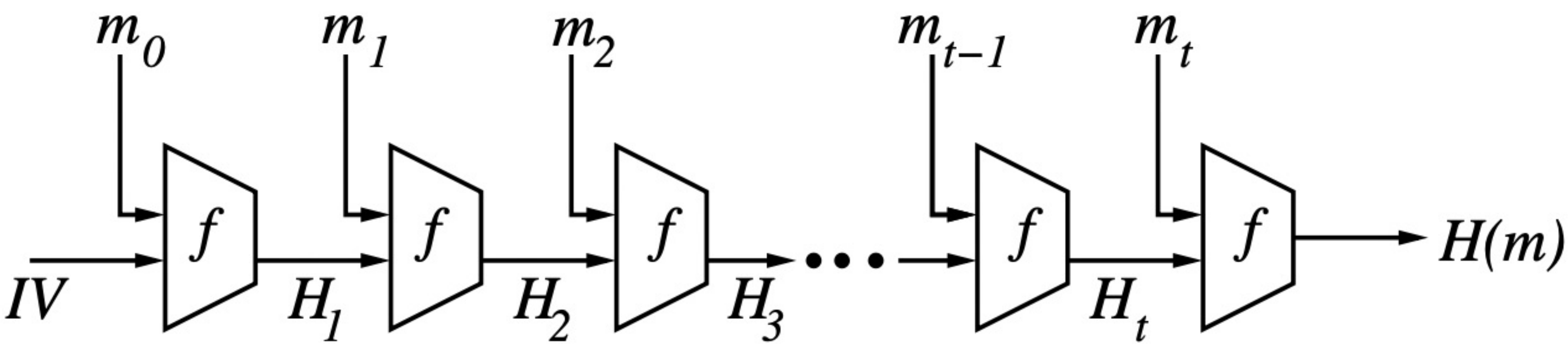
Collision resistance of Merkle Damgård

CO 487

Topic 2.1



$\boxed{\text{Theorem}}$

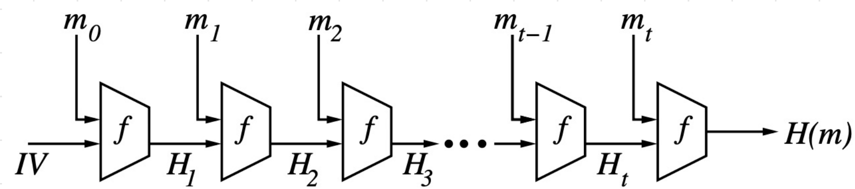
If the compression function f is collision-resistant, then the hash function H is also collision-resistant.

Proof (sketch)

Suppose $H(m) = H(m')$ but $m \neq m'$.
Suppose for simplicity $|m| = |m'|$.
Let the blocks of m and m' be

$$m = m_0 m_1 \dots m_t \qquad m' = m_0' m_1' \dots m_t'.$$

Since $m \neq m'$, there exists index $i \in \{0, \dots, t\}$ s.t. $m_i \neq m_i'$.



Since $H(m) = H(m')$, we have that

$$f(m_t, H_t) = f(m'_t, H'_t)$$

If $(m_t, H_t) \neq (m'_t, H'_t)$, then we found a collision in f $\Rightarrow$ done!

If $(m_t, H_t) = (m'_t, H'_t)$, then recurse on H_t, H'_t.

In particular, if $H_t = H'_t$, then we have that

$$f(m_{t-1}, H_{t-1}) = f(m'_{t-1}, H'_{t-1}).$$

If $(m_{t-1}, H_{t-1}) \neq (m'_{t-1}, H'_{t-1})$, then we found a collision in f

$\Rightarrow$ done!

Can construct an inductive argument that, if $H_j = H_j'$,

either $(m_{j-1}, H_{j-1}) \neq (m_{j-1}', H_{j-1}')$, which is a collision in f,

or $H_{j-1} = H_{j-1}'$.

By assumption, $\exists\, i$ s.t. $m_i \neq m_i'$.

Thus we will eventually find a collision. $\square$