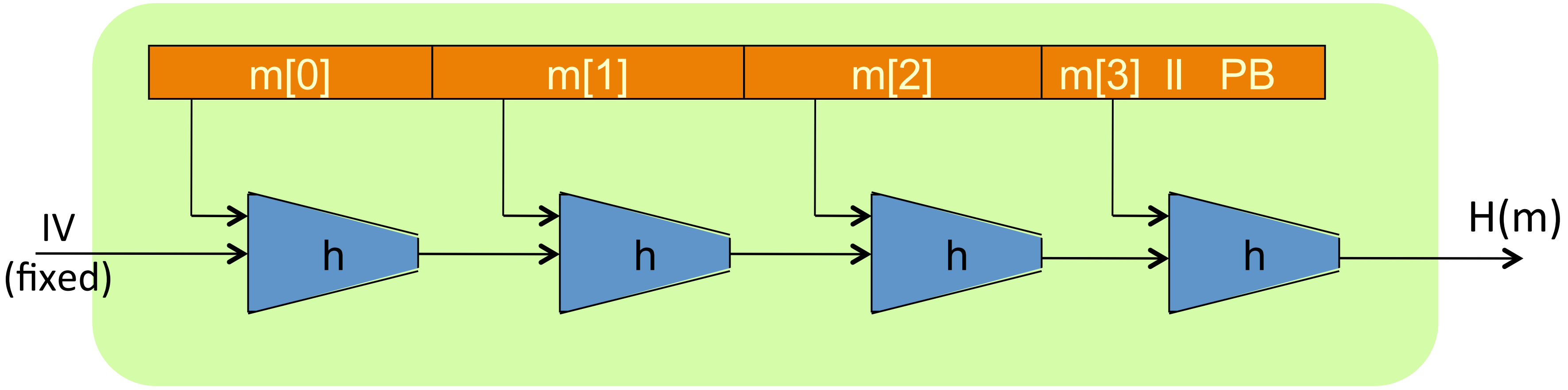
Collision resistance

Constructing Compression Functions

The Merkle-Damgard iterated construction



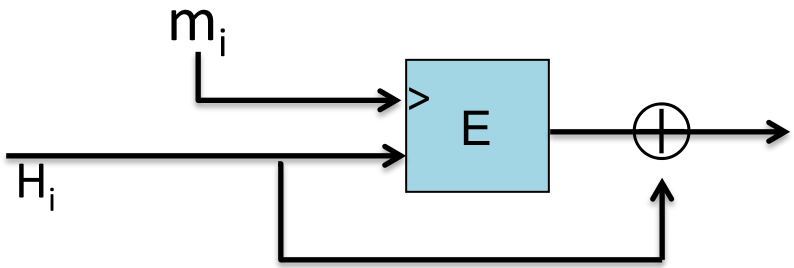
Thm: h collision resistant $\Rightarrow$ H collision resistant

Goal: construct compression function **h: T × X ⟶ T**

Compr. func. from a block cipher

E: K× {0,1}^{n} ⟶ {0,1}^{n} a block cipher.

The **Davies-Meyer** compression function: **$h(H, m) = E(m, H) \oplus H$**



<u>Thm</u>: Suppose E is an ideal cipher (collection of |K| random perms.).

Finding a collision **h(H,m)=h(H',m')** takes **$O(2^{n/2})$** evaluations of (E,D).

Best possible !!

Suppose we define **$h(H, m) = E(m, H)$**

Then the resulting h(.,.) is not collision resistant:

to build a collision (H,m) and (H',m')

choose random (H,m,m') and construct H' as follows:

- $H' = D(m', E(m,H))$ $\Longleftarrow$ $E(m', H') = E(m, H)$
- $H' = E(m', D(m,H))$
- $H' = E(m', E(m,H))$
- $H' = D(m', D(m,H))$

Other block cipher constructions

Let $\mathbf{E: \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n}$ for simplicity

Miyaguchi-Preneel: $\mathbf{h(H, m) = E(m, H) \oplus H \oplus m}$ **(Whirlpool)**

$\mathbf{h(H, m) = E(H \oplus m, m) \oplus m}$

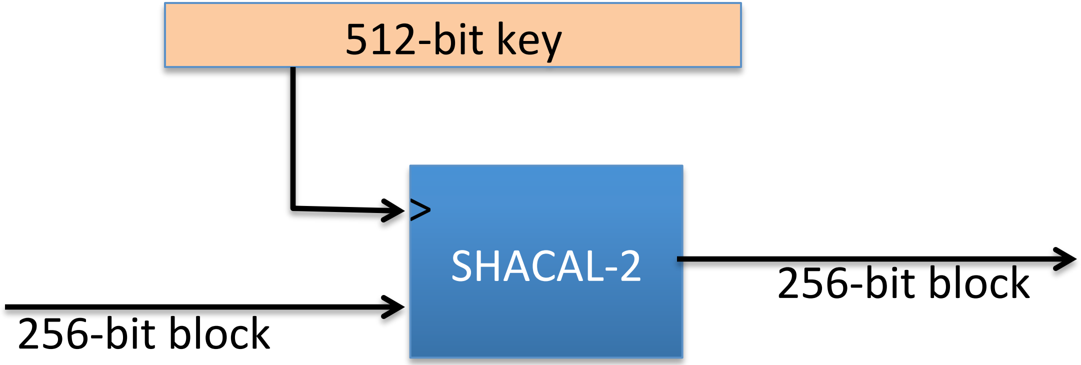
total of 12 variants like this

Other natural variants are insecure:

$h(H, m) = E(m, H) \oplus m$ (HW)

Case study: SHA-256

- Merkle-Damgard function
- Davies-Meyer compression function
- Block cipher: SHACAL-2



Provable compression functions

Choose a random 2000-bit prime p and random $1 \leq u, v \leq p$.

For $m,h \in \{0,\ldots,p\text{-}1\}$ define $\boxed{h(H,m) = u^H \cdot v^m \pmod{p}}$

<u>Fact:</u> finding collision for h(.,.) is as hard as
solving "discrete-log" modulo p.

Problem: slow.

End of Segment