W3 6-3 The Merkle-Damgard Paradigm

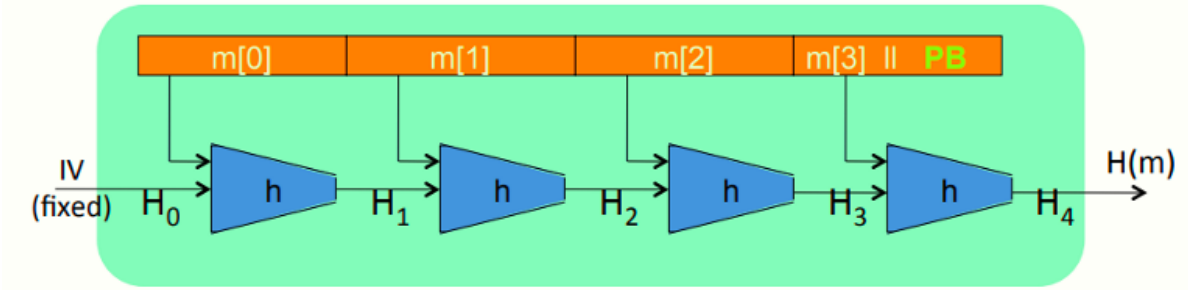
默尔克-达姆加德范式，常用于生成抗碰撞hash函数

1、Collision resistance: review

记H: M →T 为一hash函数（|M| >> |T|）

目标：C.R.（collision resistant）hash函数

2、The Merkle-Damgard iterated construction



如图所示，记h: T × X ⟶ T为一接收短消息为输入的C.R. hash函数（也叫压缩函数），初始向量IV为固定在代码或芯片中的值，消息作为输入并分块为m_0，m_1，.....

链式变量Hi：H: $X^{\leq L}$ ⟶ T，对于m_0而言，将m_0和IV作为h的输入，输出H_1，再与下一块消息m_1作为下一轮h的输入

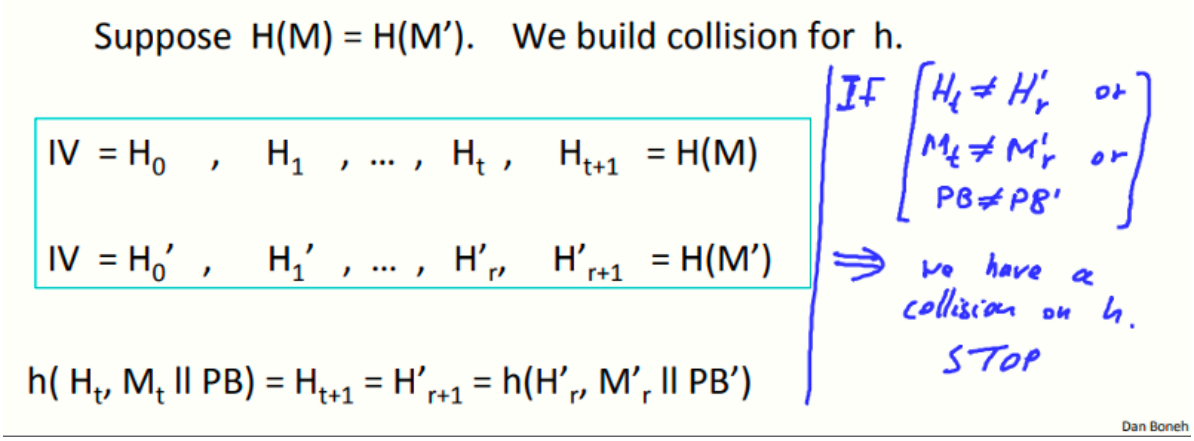
填充块PB：pandding block，包含1个1，若干个0和64 bits的消息长度，必须附加这个填充块，若消息尾部的长度不足以放下PB，则需要添加一个新的消息块

3、M-D collision resistance

定理：若h为一C.R. hash函数，则H也是

含义：若我们希望构造一个能接收长消息作为输入的C.R. hash函数，则我们只需要构造一个C.R.压缩函数即可

证明：反证法（collision on H ⇒ collision on h）



Otherwise,

Suppose $H_t = H'_r$ and $M_t = M'_r$ and PB = PB'

$\hookrightarrow t = r$

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

If $\begin{bmatrix} H_{t-1} \neq H'_{t-1} \\ \text{or} \\ M_{t-1} \neq M'_{t-1} \end{bmatrix}$ 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:

(1) find collision on h, or

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

Dan Boneh