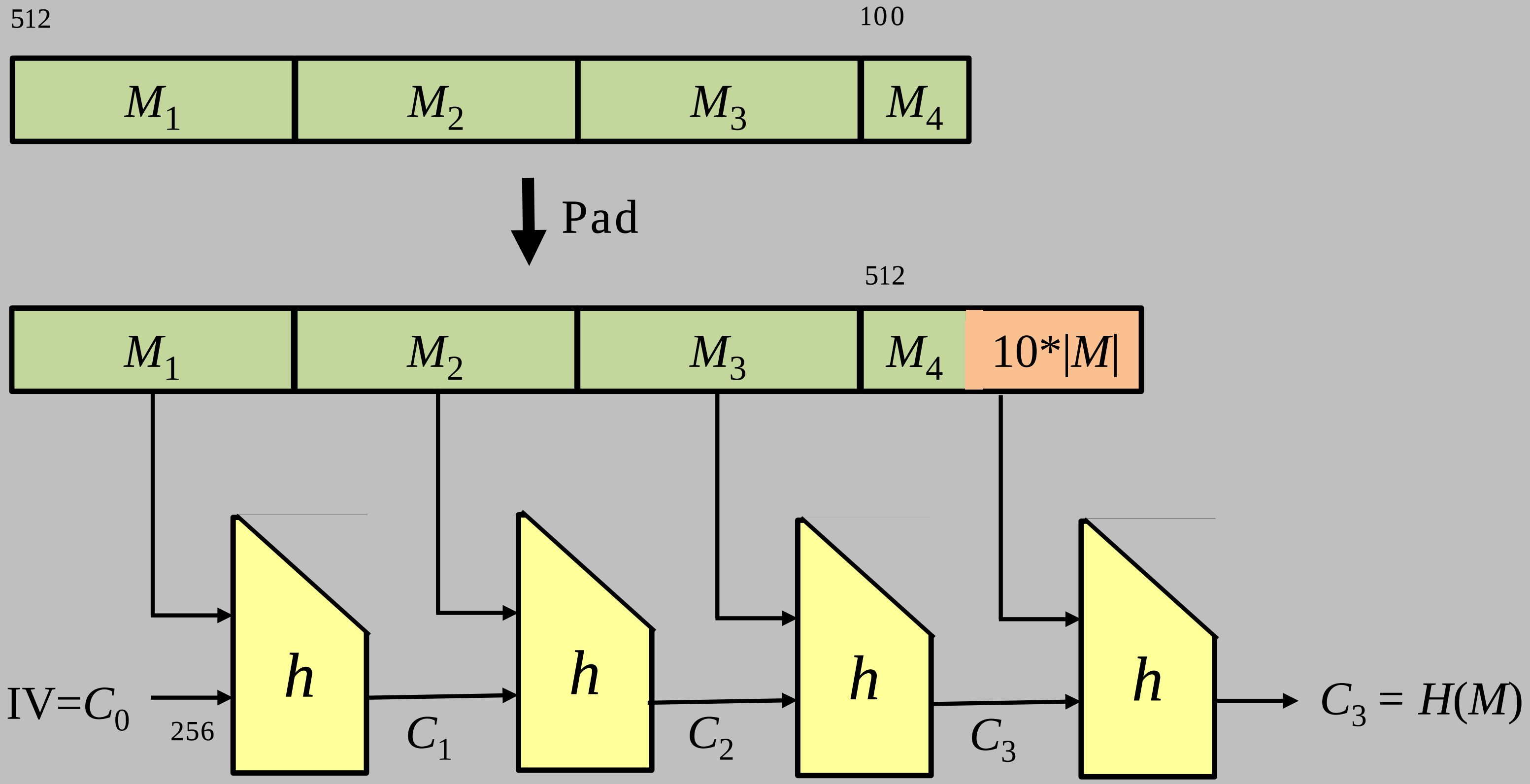
Merkle–Damgård Hash

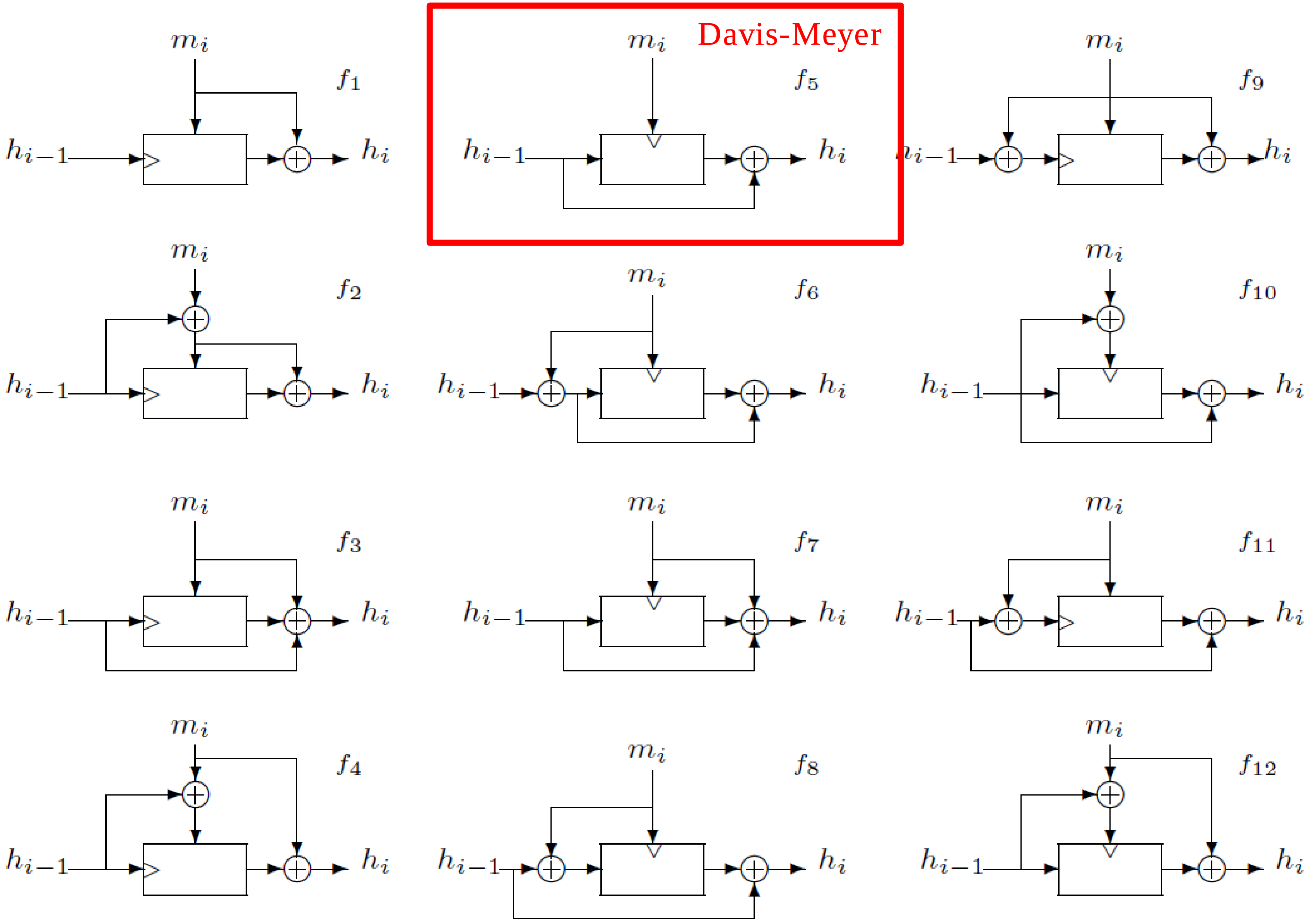
Pad(M) determines M

|Pad(M)| is a positive multiple of n

$|M|=|M'| \Rightarrow |\text{Pad}(M)|=|\text{Pad}(M')|$

$|M|\neq|M'| \Rightarrow \text{last}(\text{Pad}(M)) \neq \text{last}(\text{Pad}(M'))$

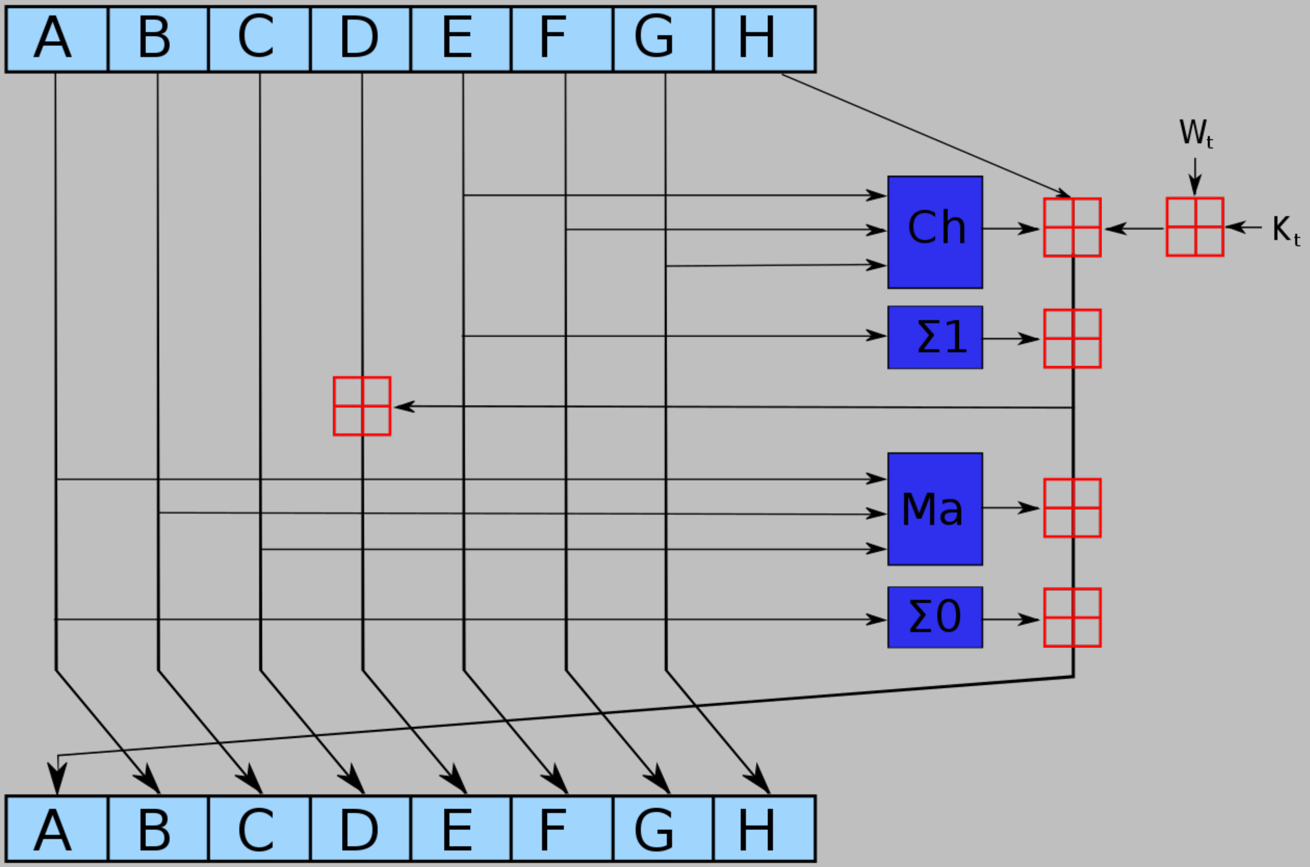




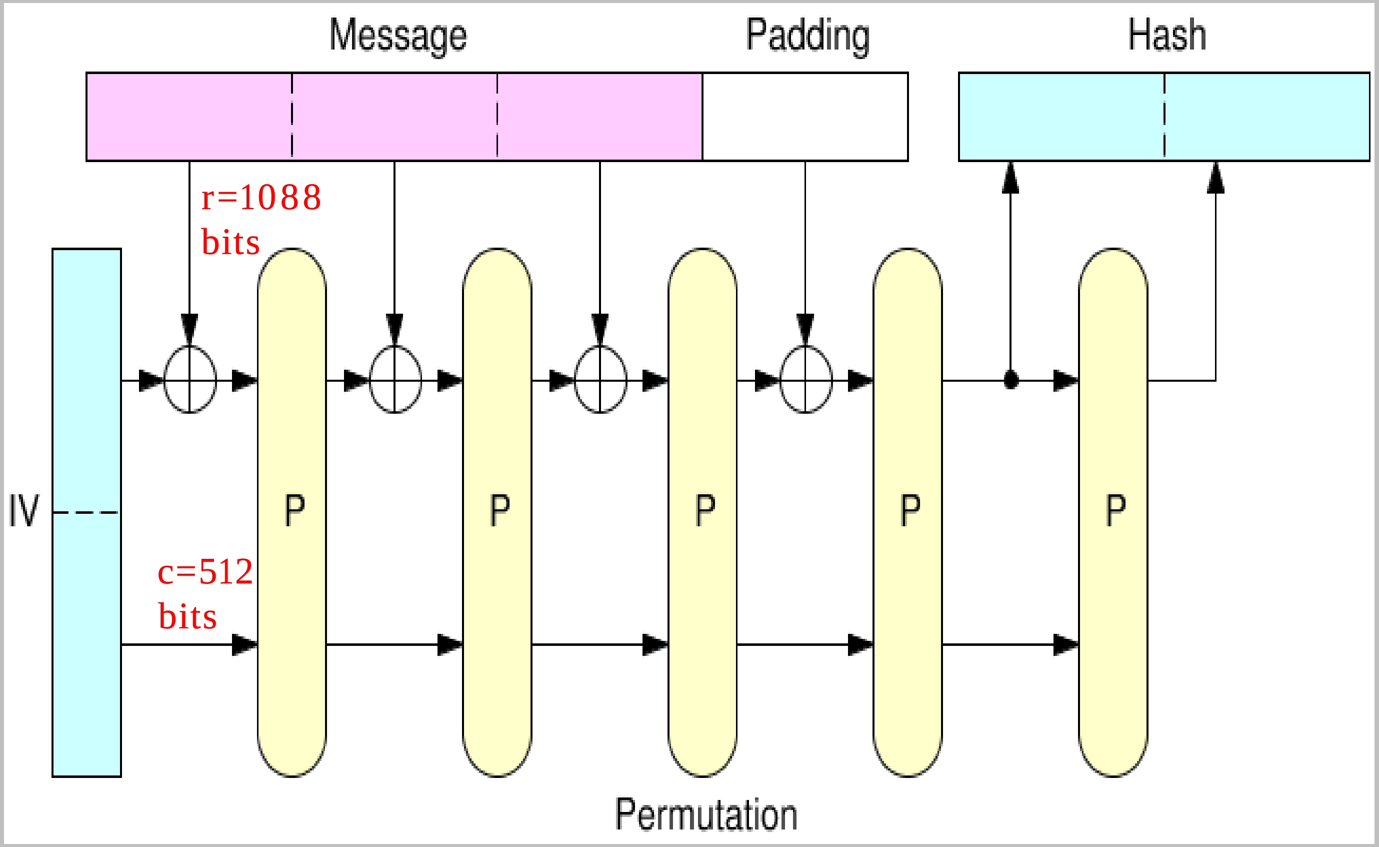
Davis-Meyer

```
algorithm SHA256BC (w, a b c d e f g h)  // blockcipherunderlying SHA-256
(k[0],…, k[63]) ← constants
Regard w as words w[0]...w[15]

for i ← 16 to 63
  s0 ← (w[i-15] >>> 7) ⊕ (w[i-15] >>> 18) ⊕ (w[i-15] >>> 3)
  s1 ← (w[i-2] >>> 17) ⊕ (w[i-2] >>> 19) ⊕ (w[i-2] >>> 10)
  w[i] ← w[i-16] + s0 + w[i-7] + s1

  for i ← 0 to 63
    S1 ← (e >>> 6) ⊕ (e >>> 11) ⊕ (e >>> 25)
    ch ← (e ∧ f) ⊕ (~e ∧ g)
    temp1 ← h + S1 + ch + k[i] + w[i]
    S0 ← (a >>> 2) ⊕ (a >>> 13) ⊕ (a >>> 22)
    maj ← (a ∧ b) ⊕ (a ∧ c) ⊕ (b ∧ c)
    temp2 ← S0 + maj
   (a,b,c,d,e,f,g,h) ← (temp1+temp2,a,b,c,d+temp1,e,f,g)

return a || b || c || d || e || f || g || h
```

One round (of 64) of the blockcipher sha256 underlying SHA256



SHA-3 – Keccak [Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche]


Message
Padding
Hash
r=1088 bits
c=512 bits
IV
P
P
P
P
P
Permutation