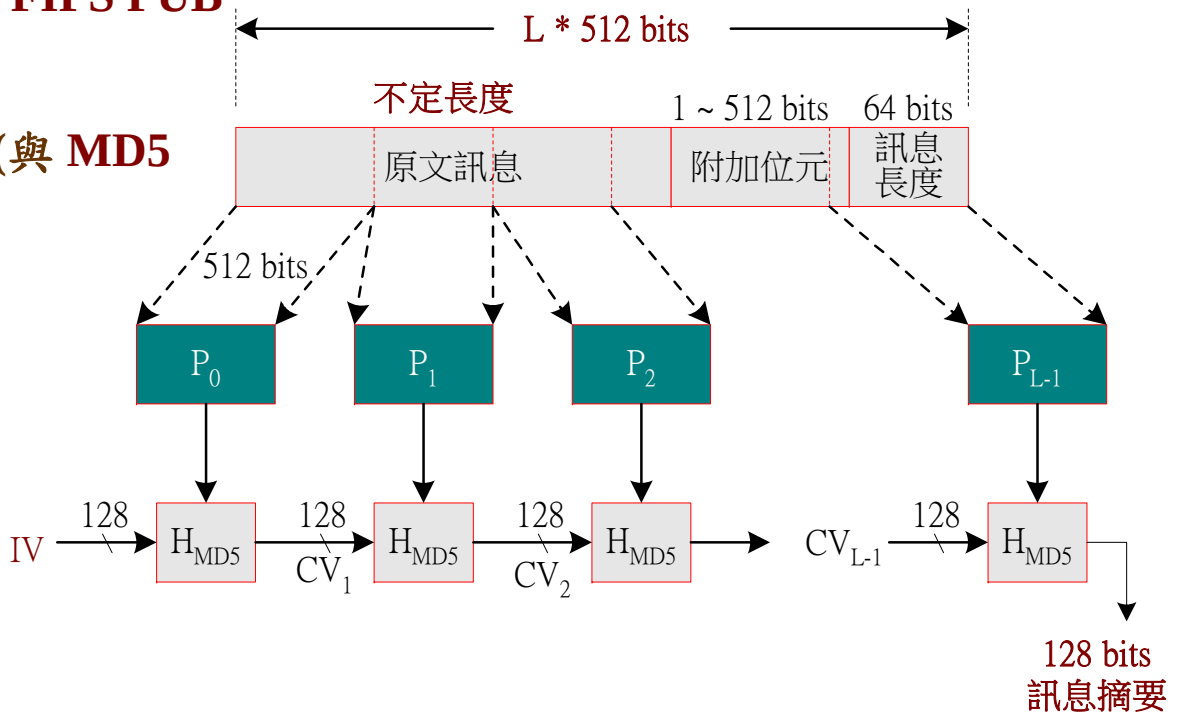
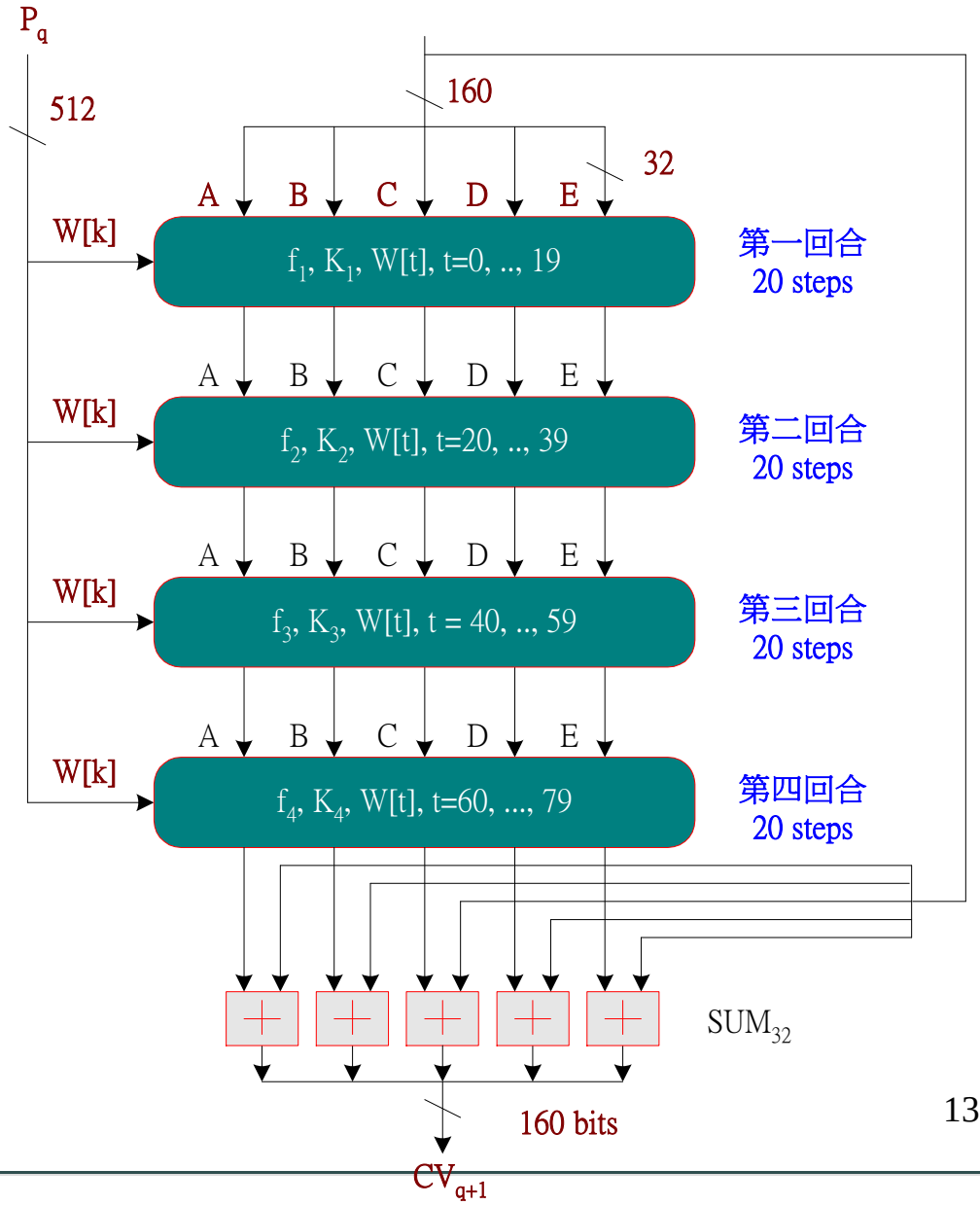
SHA-1 雜湊系統

- **SHA-1 (Secure Hash Algorithm) 演算法**
  - **FIPS PUB 180 與 FIPS PUB 180-1**
  - **區段雜湊演算法 (與 MD5 相同)**



SHA-1 演算法

- SHA-1 演算法
  - 雜湊值：160 bits
  - 5 個 32 bits 暫存器。
  - 攪拌 4 回合，20 次/回合
    合計 80 回合。



SHA-1 演算法

- 暫存器初始值
  - A：67 45 23 01
  - B：EF CD AB 89
  - C：98 BA DC FE
  - D：10 32 54 76
  - E ：C3 D2 E1 F0
- 輸入常數
  - 『鹽』的功能
- 訊息擴充
  - W[K], k=0, 1, ..., 79，32 bits 區段
  - 訊息 512 bits 分成 W[0] ~ W[15]
  - W[16] 以後的填入方式：

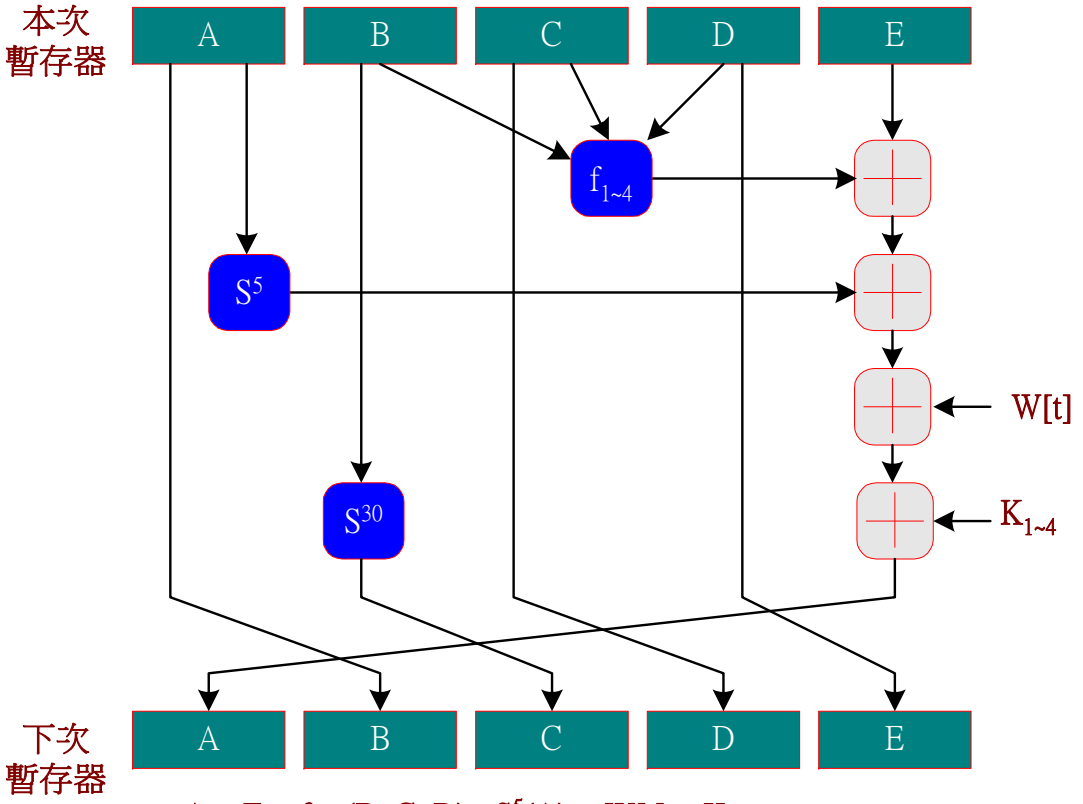
    $W[t] = S^1(W[t-16] \oplus W[t-14] \oplus W[t-8] \oplus W[t-3])$,

    $t = 16, 17, \ldots, 79$
  - 譬如：
    - $W[16] = S^1(W[0] \oplus W[2] \oplus W[8] \oplus W[13])$
    - $W[17] = S^1(W[1] \oplus W[3] \oplus W[9] \oplus W[14])$
    - $W[79] = S^1(W[63] \oplus W[65] \oplus W[71] \oplus W[76])$
    - 其中：S^1 表示向左迴旋一個位元。

回合	步驟編號	輸入常數	取值方式 (整數)
第一回合	$0 \leqq t \leqq 19$	K_1 = 5A82799	$[2^{30} \times 2]$
第二回合	$20 \leqq t \leqq 39$	K_2 = 6ED9EBA1	$[2^{30} \times 3]$
第三回合	$40 \leqq t \leqq 59$	K_3 = 8F1BBCDC	$[2^{30} \times 5]$
第四回合	$60 \leqq t \leqq 79$	K_4 = CA62C1D6	$[2^{30} \times 10]$

SHA-1 壓縮函數

- 處理程序：4 回合，共計 80 次；5 個暫存器
  - $A = E + f_{1\text{-}4}(B, C, D) + S^5(A) + W[t] + K_{1\text{-}4}$
  - $B = A$
  - $C = S^{30}(B)$
  - $D = C$
  - $E = D$



$A = E + f_{1\sim4}(B, C, D) + S^5(A) + W[t] + K_{1\sim4}$;

$B = A$; $C = S^{30}(B)$; $D = C$; $E = D$