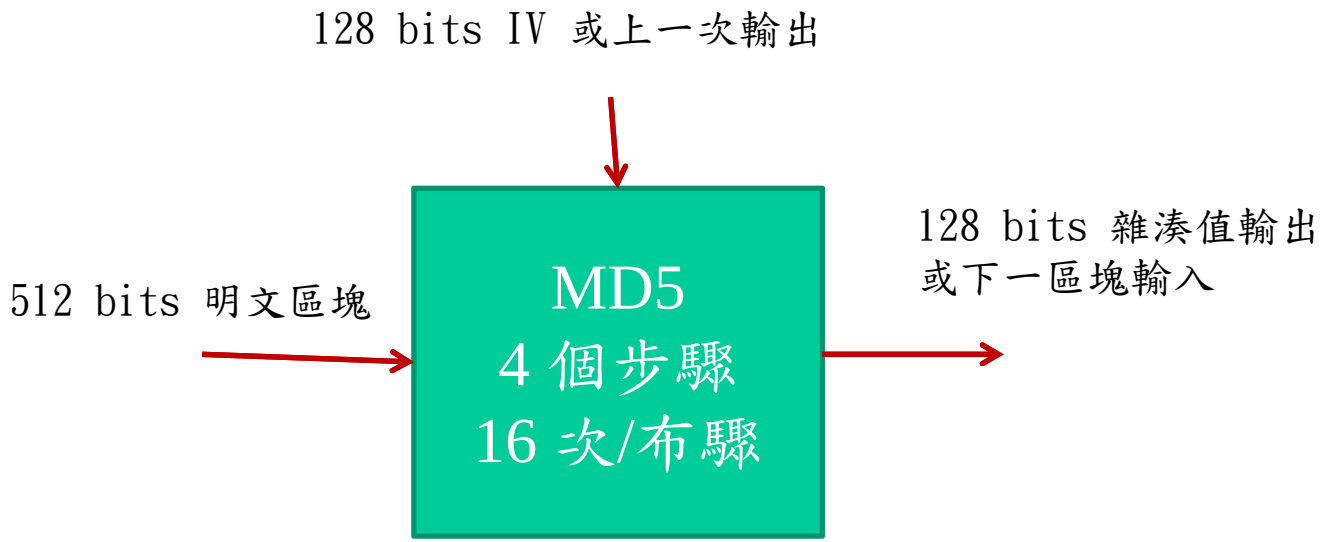
MD5 演算法

MD5 演算法

- 兩組輸入：512 bits 明文區塊與 128 bits 上一區塊的輸出(或 IV)。
- 輸入資料區分為四個暫存器：A, B, C, D。
- 區分為四個步驟，每步驟計算 16 次，合計 64 次。
- 加入 sin(x) 非線性函數參數值。



MD5 演算法

- 處理步驟：
  - 步驟 1：將輸入明文（512 bits）以每 32 bits 為單位，分別存入X[k]中，其中 k =0, 1, 2, .., 15。
  - 步驟 2：初始化 A、B、C 與 D 暫存器，如下：

    A：01 23 45 67

    B：89 ab cd ef

    C：fe dc ba 98

    D：76 54 32 10
  - 步驟 3：進入第一回合運算，執行 16 次：

    a = b+((a+F(b, c, d)+X[k]+T[i]) <<<s)
  - 步驟 4：進入第二回合運算，執行 16 次：

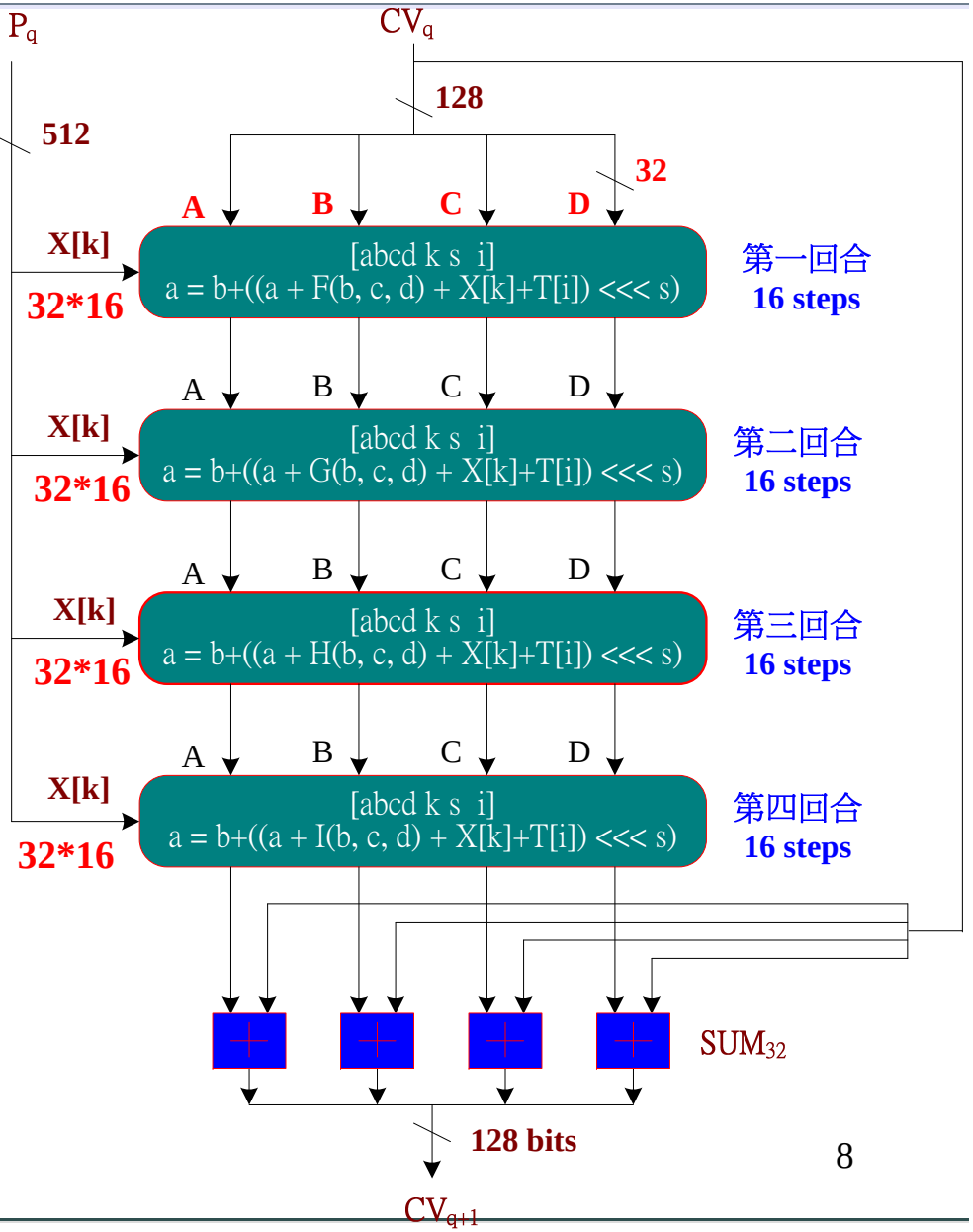
    a = b+((a+G(b, c, d)+X[k]+T[i]) <<<s)
  - 步驟 5：進入第三回合運算，同樣執行 16 次：

    a = b+ ((a+ H(b, c, d)+ X[k]+T[i]) <<<s)
  - 步驟 6：進入第四回合運算，同樣執行 16 次：

    a = b+ ((a+ H(b, c, d)+ X[k]+T[i]) <<<s)
  - 步驟 7：輸出訊息摘要，執行 SUM_{32} 計算。

MD5 演算法

- 非線性函數：sun(x) 的『鹽』
  - T[i] = $2^{32} \times$ (abs(sin(i))，i 為弧度。
  - i = 1, 2, 3, …, 64 (查表)
- 初始值：（16 進位表示）
  - A：01 23 45 67
  - B：89 ab cd ef
  - C：fe dc ba 98
  - D：76 54 32 10



MD5 壓縮函數

- **MD5 運算處理**
  - a = b + ((a + g(b, c, d) + X[k] + T[i]) <<< s)
  - b = b
  - c = c
  - d = d
- **G(b, c, d)**
  - 第一回合：F(b, c, d) = = bc + d
  - 第二回合：G(b, c, d) = = db +
  - 第三回合：H(b, c, d) = b⊕c⊕d
  - 第四回合：I(b, c, d) = c⊕ = c⊕ =