# Secure Hash Algorithm

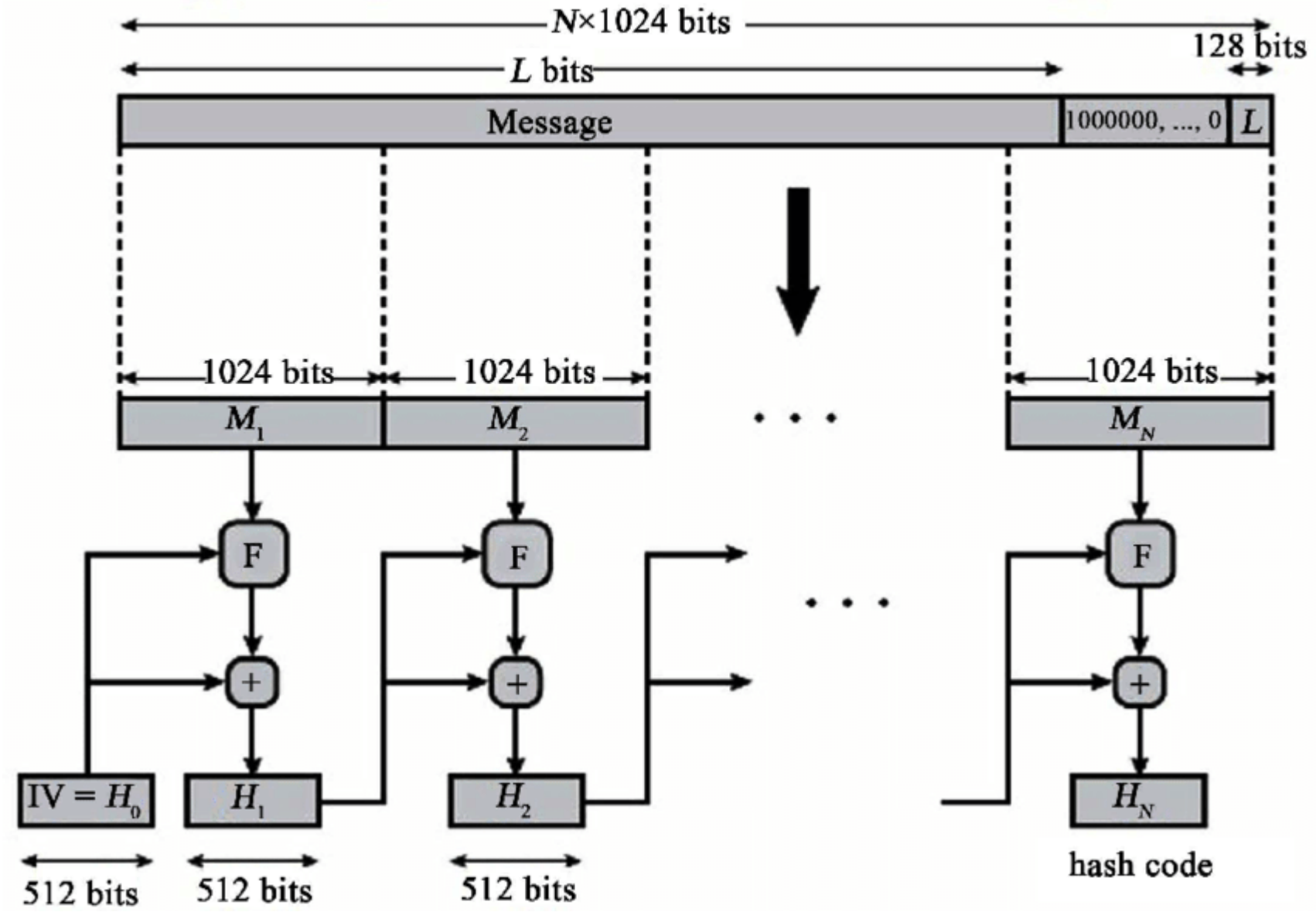
- Secure Hash Algorithm was developed by NIST in 1993
- Generally SHA referred as SHA-1
- SHA design is based on hash function MD4
- Different version of SHAs are SHA-1, SHA-256, SHA-384, SHA-512

Table 11.3 Comparison of SHA Parameters

| | SHA-1 | SHA-224 | SHA-256 | SHA-384 | SHA-512 |
|---|---|---|---|---|---|
| **Message Digest Size** | 160 | 224 | 256 | 384 | 512 |
| **Message Size** | $< 2^{64}$ | $< 2^{64}$ | $< 2^{64}$ | $< 2^{128}$ | $< 2^{128}$ |
| **Block Size** | 512 | 512 | 512 | 1024 | 1024 |
| **Word Size** | 32 | 32 | 32 | 64 | 64 |
| **Number of Steps** | 80 | 64 | 64 | 80 | 80 |

*Note:* All sizes are measured in bits.

# Message Digest Generation Using SHA-512

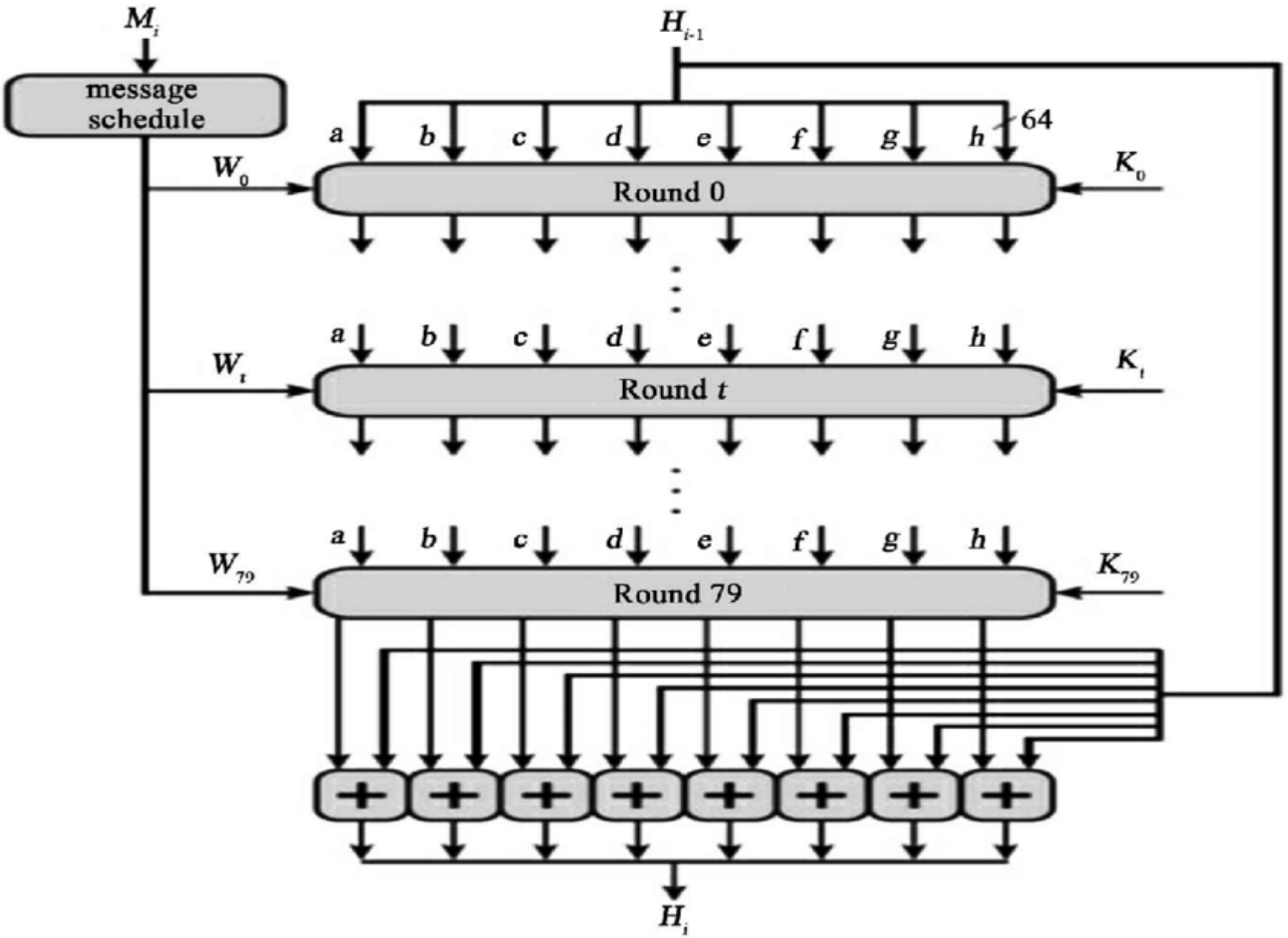


# Steps for SHA-512 logic

1. Append padding bits
2. Append length
3. Initialize hash buffer
4. Process message in 1024 bit(128 word)blocks
5. Output

1. Append padding bits
   - Number of padding bits is in the range of 1 to 1024
   - Padding consists of a single-1 bit followed by the necessary number of 0-bits
2. Append length
   - A block of 128 bits is appended to the message
   - Sequence of 1024-bit blocks $M_1, M_2, \ldots M_n$
3. Initialize hash buffer
   - A 512 bit buffer is used to hold intermediate and final results of the hash function
   - The buffer can be represented as eight 64-bit registers (a,b,c,d,e,f,g,h)
   - These registers are initialized as hexadecimal values

# 4. Process message in 1024 bit blocks



5. Output
   - After all N 1024-bit blocks have been processed, the output from the Nth stage is the 512-bit message digest
   - We can summerize the behavior of SHA-512 as follows:
     - $H_0 = IV$
     - $H_i = SUM64(H_{i-1}, abcdefgh_{i)}$
     - $MD = H_N$

   where,
   - IV : Initial value of the abcdefgh buffer
   - $abcdefgh_i$ : output of the last round of processing of the *i*th message block
   - N : number of blocks in the message
   - $SUM_{64}$ : Addition modulo $2_{64}$ performed separately on each word of the pair of inputs
   - MD : final message digest value