Chap 11 補充

Table 11.2 The MD4 family of hash functions

Algorithm		Output [bit]	Input [bit]	No. of rounds	Collisions found
MD5		128	512	64	yes
SHA-1		160	512	80	not yet
SHA-2	**SHA-224**	224	512	64	no
	SHA-256	256	512	64	no
	SHA-384	384	1024	80	no
	SHA-512	512	1024	80	no

11.3.2 Hash Functions from Block Ciphers

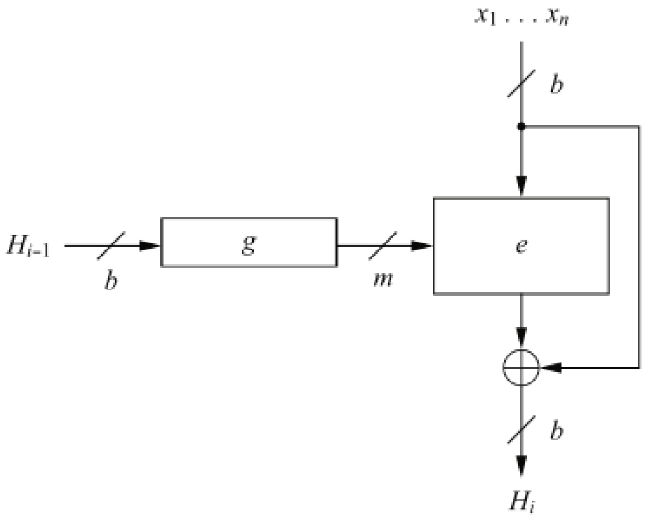

Fig. 11.6 The Matyas–Meyer–Oseas hash function construction from block ciphers

The function can be expressed as:

$$H_i = e_{g(H_{i-1})}(x_i) \oplus x_i$$

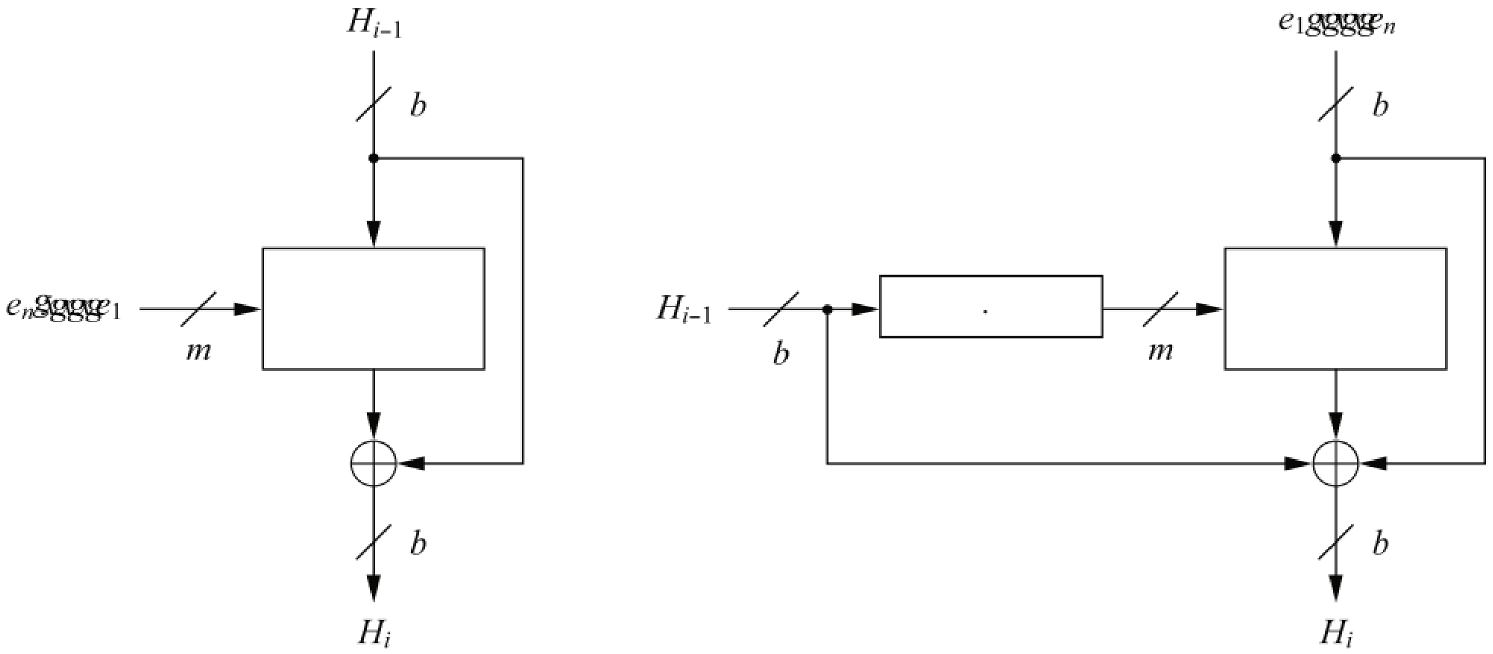

Fig. 11.7 Davies–Meyer (left) and Miyaguchi–Preneel hash function constructions from block ciphers

The expressions for the two hash functions are:

$$H_i = H_{i-1} \oplus e_{x_i}(H_{i-1}) \qquad \text{(Davies–Meyer)}$$

$$H_i = H_{i-1} \oplus x_i \oplus e_{g(H_{i-1})}(x_i) \qquad \text{(Miyaguchi–Preneel)}$$

All three hash functions need to have initial values assigned to H_0.

11.4.2 Hash Computation

Each message block x_i is processed in four stages with 20 rounds each as shown in Figure 11.11. The algorithm uses

- a message schedule which computes a 32-bit word $W_0, W_1, \ldots, W_{79}$ for each of the 80 rounds. The words W_j are derived from the 512-bit message block as follows:

$$W_j = \begin{cases} x_i^{(j)} & 0 \leq j \leq 15 \\ (W_{j-16} \oplus W_{j-14} \oplus W_{j-8} \oplus W_{j-3})_{\lll 1} & 16 \leq j \leq 79, \end{cases}$$

  where $X_{\lll n}$ indicates a circular left shift of the word X by n bit positions.