

From the Hash function shown in figure 1, the size of input is 1 block (9 bits in length). The input (1 block) will be separated into 3 words which have 3 bits per 1 word. Assume that the rule of word expansion is that

$$\text{The 4}^{\text{th}} \text{ word will be } W_3 = (W_0 \text{ ex-or RotShift}_{2-2}(W_1) \text{ ex-or } W_2)$$

where

$\text{RotShift}_{x-y}(W_i)$  is the x-bit Right Rotation of  $W_i$  and then follow by Ex-or with the y-bit Left Shift of  $W_i$

Find the output (Message Digest) of the Hash function when the input is “001 111 101”

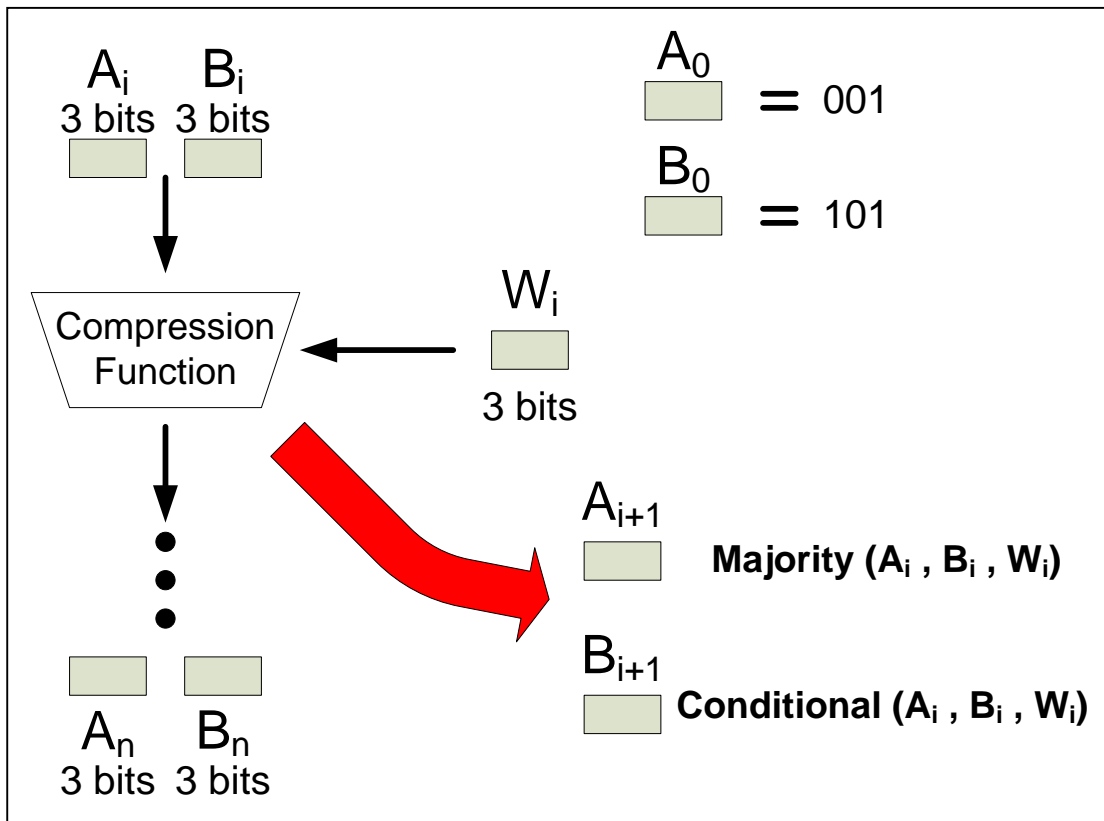


Figure 1 Hash Function