

组号

码字

缓冲区

 $\text{HASH}(D_1)$ D_l

[1]

 D_l h_1

...

HASH(

[j]

$$D_j$$
$$h_j$$

...

 D_l h_1

...

 D_{j-1}
$$h_{i-1}$$
 D_j

...