

????????????????????????????????
 ?????????

The diagram illustrates the iterative process of a Merkle-Damgård hash function. A long message (represented by a row of 128 small squares) is divided into blocks of 512 bits (represented by groups of 16 small squares). Each block is processed by a compression function (represented by a box labeled 'C') to produce a 128-bit digest (represented by a row of 4 small squares). The digests are then concatenated to form the final 128-bit message digest (represented by a row of 4 small squares).

[illegible]

WI-AC-004 [Barcode]

image.png