

```

Algorithm OMAC2( $K, M$ )
 $L \leftarrow E(K, 0^n)$ 
if  $\text{msb}(L) = 0$  then  $L \cdot u \leftarrow L \ll 1$ 
    else  $L \cdot u \leftarrow (L \ll 1) \oplus \text{Constant}$ 
        /* Constant is 0x0...087 (when  $n = 128$ ),
           and 0x0...01b (when  $n = 64$ ) */
if  $\text{lsb}(L) = 0$  then  $L \cdot u^{-1} \leftarrow L \gg 1$ 
    else  $L \cdot u^{-1} \leftarrow (L \gg 1) \oplus \text{Constant}'$ 
        /* Constant' is 0x80...043 (when  $n = 128$ ),
           and 0x80...0d (when  $n = 64$ ) */
 $Y[0] \leftarrow 0^n$ 
Break  $M$  into blocks  $M[1], M[2], \dots, M[m]$ 
    /*  $|M[i]| = n$  for  $i = 1, \dots, m - 1$ , and  $|M[m]| \leq n$  */
for  $i \leftarrow 1$  to  $m - 1$  do
     $Y[i] \leftarrow E(K, M[i] \oplus Y[i - 1])$ 
if  $|M[m]| = n$  then  $X[m] \leftarrow M[m] \oplus Y[m - 1] \oplus L \cdot u$ 
    else  $X[m] \leftarrow (M[m]10^{n-1-|M[m]|}) \oplus Y[m - 1] \oplus L \cdot u^{-1}$ 
 $T \leftarrow E(K, X[m])$ 
Tag  $\leftarrow t$ -bit truncation of  $T$ 
return Tag

```