Algorithm OMAC1(K, M)
$L \leftarrow E(K, 0^n)$
if $\mathtt{msb}(L) = 0$ **then** $L \cdot \mathtt{u} \leftarrow L \ll 1$
else $L \cdot \mathtt{u} \leftarrow (L \ll 1) \oplus \mathtt{Constant}$
if $\mathtt{msb}(L \cdot \mathtt{u}) = 0$ **then** $L \cdot \mathtt{u}^2 \leftarrow (L \cdot \mathtt{u}) \ll 1$
else $L \cdot \mathtt{u}^2 \leftarrow ((L \cdot \mathtt{u}) \ll 1) \oplus \mathtt{Constant}$
/* `Constant` is `0x0...087` (when $n = 128$),
and `0x0...01b` (when $n = 64$) */
$Y[0] \leftarrow 0^n$
Break M into blocks $M[1], M[2], \ldots, M[m]$
/* $|M[i]| = n$ for $i = 1, \ldots, m-1$, 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** $X[m] \leftarrow M[m] \oplus Y[m-1] \oplus L \cdot \mathtt{u}$
else $X[m] \leftarrow (M[m]10^{n-1-|M[m]|}) \oplus Y[m-1] \oplus L \cdot \mathtt{u}^2$
$T \leftarrow E(K, X[m])$
Tag $\leftarrow$ t-bit truncation of T
return Tag