

IV

$c[0]$

$c[1]$

$c[2]$

$c[3]$

$D(k, \cdot)$

$D(k, \cdot)$

$D(k, \cdot)$

$D(k, \cdot)$

\oplus

\oplus

\oplus

\oplus

$m[0]$

$m[1]$

$m[2]$

$m[3]$

