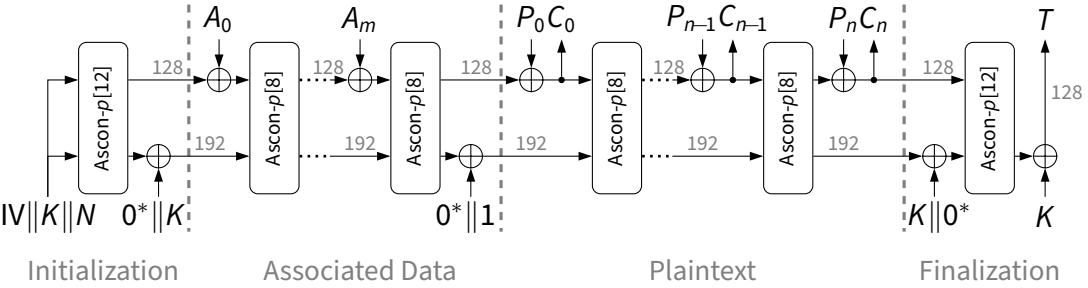
A_0
A_m
$P_0 C_0$
$P_{n-1} C_{n-1}$
$P_n C_n$
T
Ascon-p[12]
Ascon-p[8]
128
192
$\mathrm{IV} \| K \| N$
$0^* \| K$
$0^* \| 1$
$K \| 0^*$
K
Initialization
Associated Data
Plaintext
Finalization