



Initialization

Associated Data

Ciphertext

Finalization

T

128

K

$K \parallel 0^*$

$P_n C_n$

$P_{n-1} C_{n-1}$

$P_0 C_0$

A_m

A_0

128

128

128

128

128

128

192

192

192

192

192

192

$\text{Ascon-}p[12]$

$\text{Ascon-}p[8]$

$\text{Ascon-}p[8]$

$\text{Ascon-}p[8]$

$\text{Ascon-}p[8]$

$\text{Ascon-}p[12]$

$\text{IV} \parallel K \parallel N$

$0^* \parallel K$

$0^* \parallel 1$

$K \parallel 0^*$

K