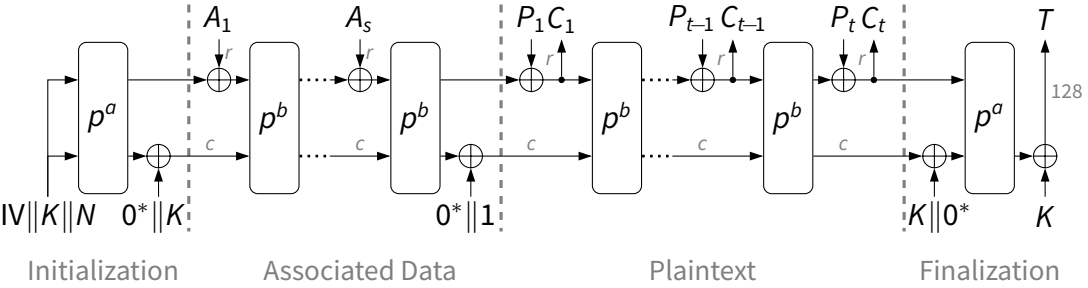
$A_1$
$A_s$
$P_1 C_1$
$P_{t-1} C_{t-1}$
$P_t C_t$
$T$
$p^a$
$p^b$
$r$
$c$
128
IV‖$K$‖$N$
$0^*$‖$K$
$0^*$‖1
$K$‖$0^*$
$K$
Initialization
Associated Data
Plaintext
Finalization