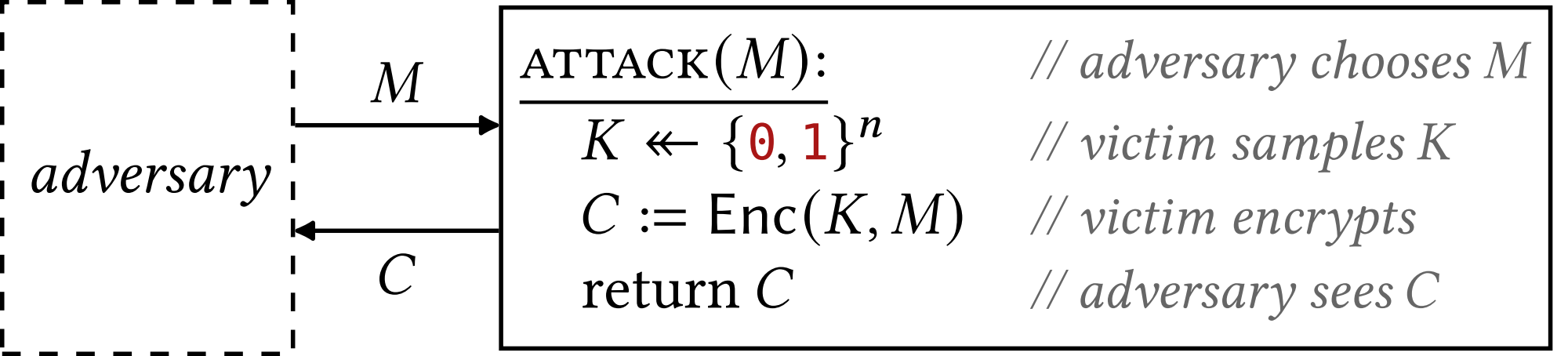
adversary
M
C
ATTACK(M):
// adversary chooses M
K ← {0,1}^n
// victim samples K
C := Enc(K, M)
// victim encrypts
return C
// adversary sees C