

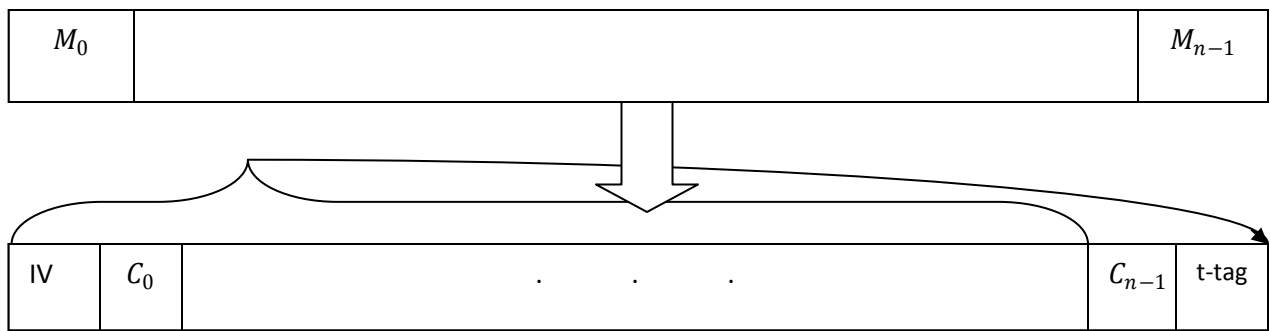
Chosen Ciphertext Secure Encryption

Suppose  $E'$  is a  $(t, q, \epsilon)$  – Real or Random secure encryption scheme, and  $M$  is a  $(t, q', q'', \epsilon')$  secure MAC.

Let:

$$E(k \parallel k', m) = c \parallel M(k', c), \text{ where } c = E'(k, m)$$

$$D(k \parallel k', c \parallel t) = \begin{cases} D'(k, c) & \text{if } t = M(k', c) \\ \perp (\text{error}) & \text{otherwise} \end{cases}$$

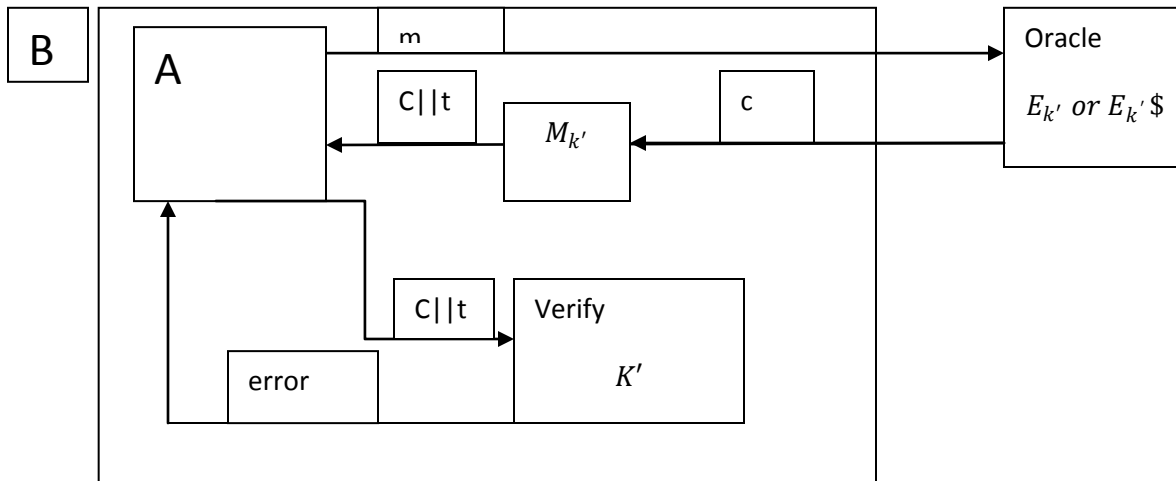


Then  $E$  is  $(t - O(q, q', q''), \min(q, q'), q'', \epsilon + \epsilon')$  IND-CCA2 secure

\*Definition: An encryption scheme is  $(t, q, q', \epsilon)$  IND-CCA secure if:

$\text{Adv. A} = |\text{Pr}[A^{E_k, D_k} = 1] - \text{Pr}[A^{E_{k'}, D_{k'}} = 1]| \leq \epsilon \forall A$  running in time  $\leq t$  and making at most  $q$   $E$  queries and  $q'$   $D$  queries and only makes valid queries.

Proof (by contrapositive) Suppose  $A$  breaks  $E$ .



Observation 1 If A ever makes a successful decryption query then A has forged a MAC. This happens with probability at most  $\epsilon'$ . Let's call this bad.

$$\begin{aligned}
 \text{Adv. A} &= (\text{Adv A} \mid \text{Bad}) \Pr[\text{Bad}] + (\text{Adv A} \mid \neg \text{Bad}) \Pr[\neg \text{Bad}] \\
 &\leq \Pr[\text{Bad}] + (\text{Adv A} \mid \neg \text{Bad}) * 1 \\
 &\leq \epsilon' + (\text{Adv A} \mid \neg \text{Bad}) \\
 &\leq \epsilon' + \text{Adv B} \\
 &\leq \epsilon' + \epsilon
 \end{aligned}$$

Encrypt then MAC == Good

MAC-then-Encrypt == Bad

Encrypt-and-Mac == Bad