

Chosen Cipher text Secure Encryption.

Suppose E' is a (t, q, ϵ) R-or-R secure encryption scheme and M is a (t, q', q'', ϵ') secure MAC.

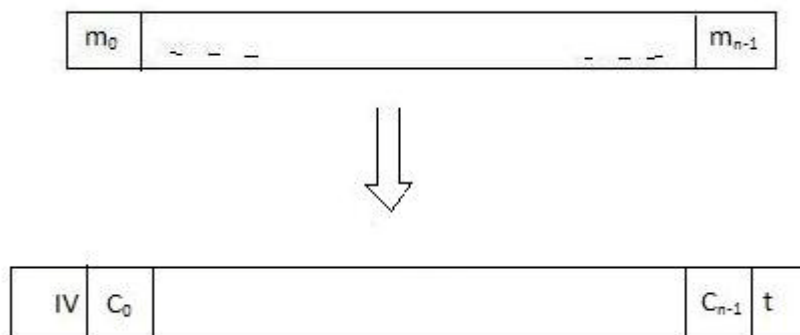
Let

$$E(K || K', m) = C || M(K', C) \text{ where } C = E'(K, m)$$

And $D(K || K', C || t) = D'(K, t)$ if $t = M(K', C)$

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

Example:



Definition:

An encryption scheme (t, q, q', ϵ) is IND-CCA secure if

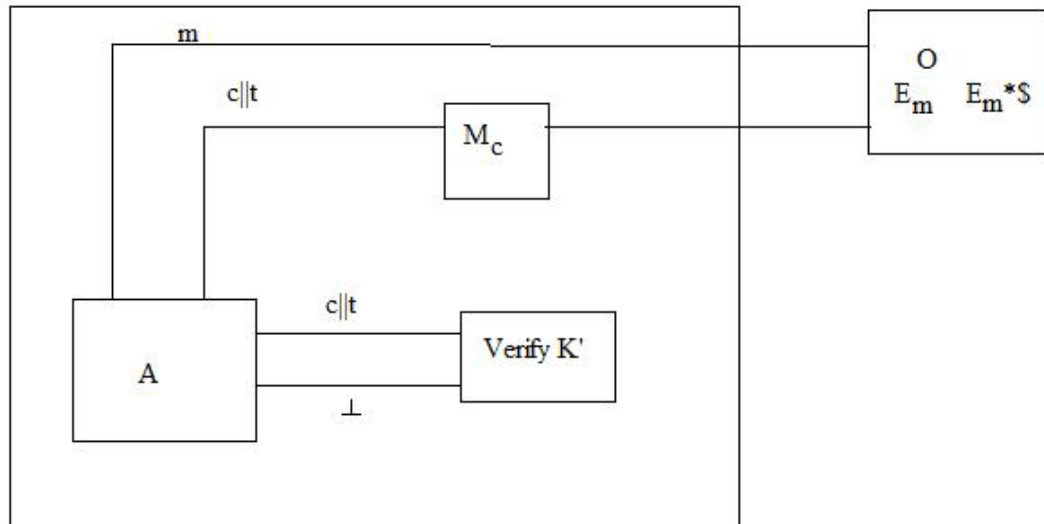
$$\text{Adv } A = |\Pr[A_k^E, D_k = 1] - \Pr[A_k^E, \hat{S}_k, D_k = 1]| \leq \epsilon$$

$\forall A$ running in time $\leq t$ at most q E queries and q' D queries.

PROOF: By contra positive.

Suppose A breaks

t



Observation 1:

If A ever makes successful decryption query then A has forged a MAC. This happens with Pr at most ϵ'

Let's Call this BAD

$$\text{Adv } A \leq (\text{Adv } A \mid B) \Pr[\text{BAD}] + (\text{Adv} \mid \Gamma \text{BAD}) \Pr[\Gamma \text{BAD}]$$

$$\leq \Pr[\text{BAD}] + (\text{Adv } A \mid \Gamma \text{BAD})$$

$$\leq \epsilon' + (\text{Adv } A \mid \Gamma \text{BAD})$$

$$\leq \epsilon' + (\text{Adv } B)$$

$$\leq \epsilon' + \epsilon$$

NOTE:

- Encrypt then MAC secure \rightarrow SECURE
- MAC-then – Encrypt $\rightarrow E_k(m \parallel \text{MAC}(k',m))$ X Not secure
- Encrypt and MAC $\rightarrow E_k(M) \parallel \text{MAC}_{k'}(M)$