

Network Security

Lecture Notes, October 9th 2009

Chosen Ciphertext Secure Encryption:

Suppose E' is a (t, q, \mathcal{E}) R-or-R secure encryption scheme and M is a $(t, q', q\mathcal{E}')$ secure MAC.

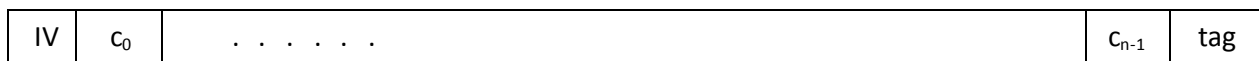
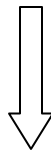
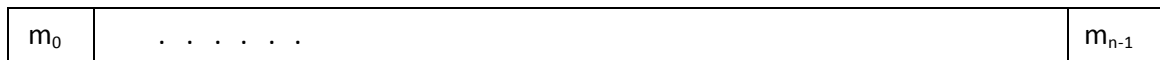
Let $E(k \parallel k', m) = E'(k, m) \parallel M(k', C)$

$$= C \parallel M(k', C)$$

Where $C = E'(k, m)$

$D(k \parallel k', c \parallel \text{tag}) = D'(k, C)$ if $t' = M(k', C)$

$D(k \parallel k', c \parallel \text{tag}) = \text{error}$, otherwise.

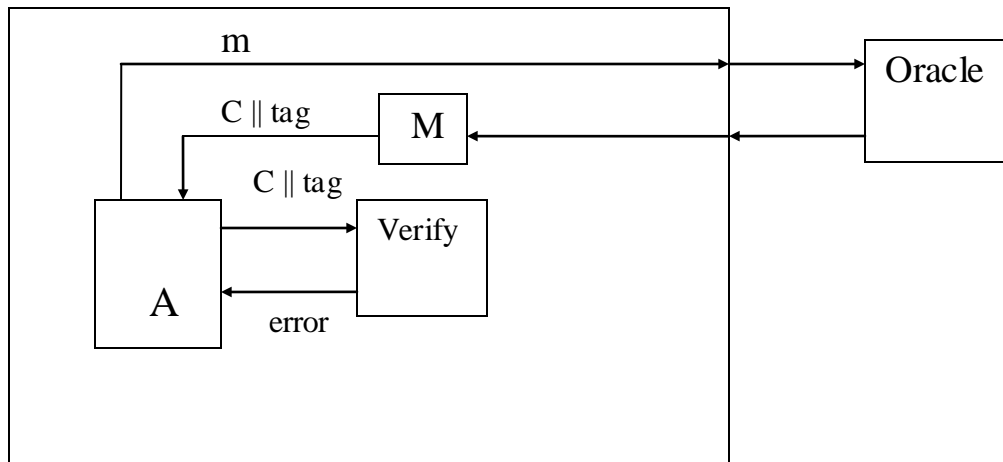


Definition:

An Encryption scheme is $(t, q, q \mathcal{E})$ IND -CCA secure if:

$\text{Adv } A = |\Pr[A_k^E, D_k = 1] - \Pr[A_k^{E \circ \mathcal{E}, D_k} = 1]| \leq \epsilon$, for all A running in time t and making at most q E queries and q' D queries and making only valid queries.

Proof: Suppose A breaks E .



Observation 1:

If **A** ever makes successful decryption query, then **A** has forged a Mac. This happens with probability ϵ' . Let us call this **Bad**.

Notation: $\sim\text{Bad}$: Not **Bad**.

$$\text{Adv } A = \Pr[\text{Adv } A / \text{Bad}] * \Pr[\text{Bad}] + \Pr[\text{Adv } A / \sim\text{Bad}] * \Pr[\sim\text{Bad}]$$

$$\leq 1 * \Pr[\text{Bad}] + \Pr[\text{Adv } A / \sim\text{Bad}] * \Pr[\sim\text{Bad}]$$

$$\leq \epsilon' + \Pr[\text{Adv } A / \sim\text{Bad}]$$

$$\leq \epsilon' + \text{Adv } B.$$

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