

Def:

An encryption scheme is (t, q, q', ϵ) **IND-CCA2 (INDistinguishability under adaptive Chosen Ciphertext Attack)** secure if for all adversaries A running in time $\leq t$ and making at most q encryption queries and q' decryption queries:

$$\text{Adv A} = | \Pr [A^{EK, DK} = 1] - \Pr [A^{EKoS, DK} = 1] | \leq \epsilon$$

An IND-CCA secure encryption scheme is also called Chosen Ciphertext Secure encryption scheme.

Building an IND-CCA2 Encryption Scheme using an IND-CPA Encryption Scheme and a MAC:

We can build an IND-CCA2 encryption scheme using E' , a (t, q, ϵ) Real-or-Random secure encryption scheme and M , a (t, q', q'', ϵ') secure MAC.

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

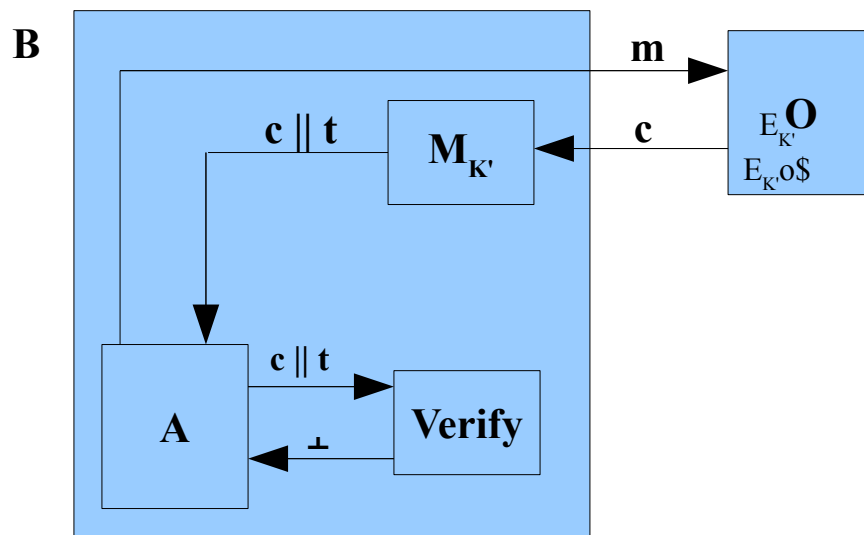
Let $E(K \parallel K', m) = c \parallel M(K', c)$ where $c = E'(K, m)$

$D(K \parallel K', c \parallel t) = \{ D'(K, c) \text{ if } t = M(K', c) \text{ or } \perp$

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

Proof: (By contra-positive)

Suppose A breaks E



Remarks:

- Verify should check the validity of the tag but our construction does not have a Decryption Oracle so it always returns \perp .
- The attacker cannot send for verification a $c \parallel t$ pair that she received from the Encryption Oracle.

Argument:

If A ever makes a successful encryption query then A has forged a MAC. This happens with probability ϵ' . Lets call this event BAD:

$$\text{Adv A} = (\text{Adv A} \mid \text{BAD}) \text{Pr}[\text{BAD}] + (\text{Adv A} \mid \neg\text{BAD}) \text{Pr}[\neg\text{BAD}]$$

If we consider the advantage of A to be 1 in case BAD does happen and consider the probability of $\neg\text{BAD}$ to be 1, neglecting ϵ' in comparison to $1-\epsilon'$:

$$\leq \epsilon' + (\text{Adv A} \mid \neg\text{BAD}) = \epsilon' + \text{Adv B} = \epsilon' + \epsilon$$

Time taken in breaking the encryption scheme is:

$$\begin{aligned} & \text{time taken in breaking E} - \text{time taken in running } q + q' + q'' \text{ queries} \\ & = t - O(q + q' + q'') \end{aligned}$$

The above result can be proved by contra-positive i.e. if new scheme can be broken in time less than $t - O(q + q' + q'')$, then E can be broken in time less than t.

The new encryption scheme can be broken by either breaking E or forging MAC. Hence total no of encryption queries required:

$$\min(q, q')$$

Summing everything up, new scheme is $(t - O(q + q' + q''), \min(q, q'), q'', \epsilon + \epsilon')$ IND-CCA2 secure.

Remarks:

- Encrypt then MAC is provably secure.
- MAC then encrypt [$E_K(m \parallel \text{MAC}_K(m))$] is insecure in certain cases.
- Encrypt and MAC [$E_K(m) \parallel \text{MAC}_K(m)$] is highly insecure because majority of MACs are deterministic and appending a deterministic value to the non-deterministic encryption, we are undoing the non-determinism.