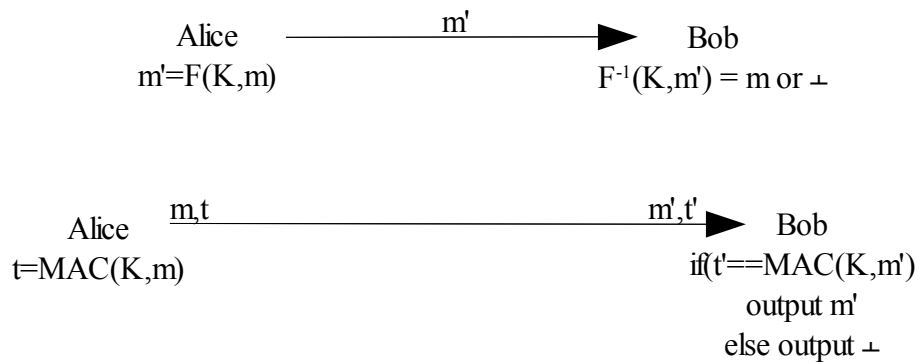


Message Integrity:



m , m' and t , t' may be the same or different. Here the MAC depends on both the key (K) and the message (m) and is in a way authenticates the sender also because only sender can have the key (K).

Goals of Mallory:

- Modify m and modify t to match to the modified m .
- Compute tag for a message of her choice
- Find tag collision
- Recover key K

Attacker Resources:

- Observe valid message, tag pairs
- Query MAC Oracle i.e. send the Oracle the messages and receive MACs on them
- Query Verification Oracle i.e. guess the MAC for a message and receive a verification for the guess.

Def:

A MAC scheme is (t, q, q', ϵ) secure if for all adversaries A running in time $\leq t$, and making at most q MAC Oracle queries and at most q' Verification Oracle queries,

$$\Pr [A^{\text{MAC}_K, \text{Verf}_K} \text{ forges}] \leq \epsilon$$

Where A forges if A queries Verf_K on (m, t) and $\text{Verf}_K(m, t) = \text{OK}$ and A has not previously queried MAC_K on m .

Theorem:

If $F: \text{keys} \times \{0,1\}^* \rightarrow \{0,1\}^l$ is a (t, q, ϵ) PRF then F is a $(t - O(q), q', q - q', \epsilon + (q - q')/2^l)$ MAC.

Proof: By contra-positive:

Suppose F is not a MAC with the given security parameters, then A (in the figure below) breaks F as a MAC with probability $> \epsilon + (q - q')/2^l$

$$\text{i.e. if } O = F^K \text{ then } \Pr[A \text{ Forges}] > \epsilon + (q - q')/2^l$$

If A forges then B can distinguish the PRF from a random function. Hence

$$\Pr [B^{F^K} = 1] > \epsilon + (q - q')/2^l$$

Now if $O = R$, then for $q - q'$ attempts

$$\Pr[\text{A Forges}] = (q - q')/2^l$$

$$\Pr[B^R = 1] = (q - q')/2^l$$

The advantage of B is:

$$|\Pr[B^{FK} = 1] - \Pr[B^R = 1]| > \epsilon$$

**Which is contrary to the definition of F as a PRF. Hence our assumption is incorrect.
Hence Proved.**

