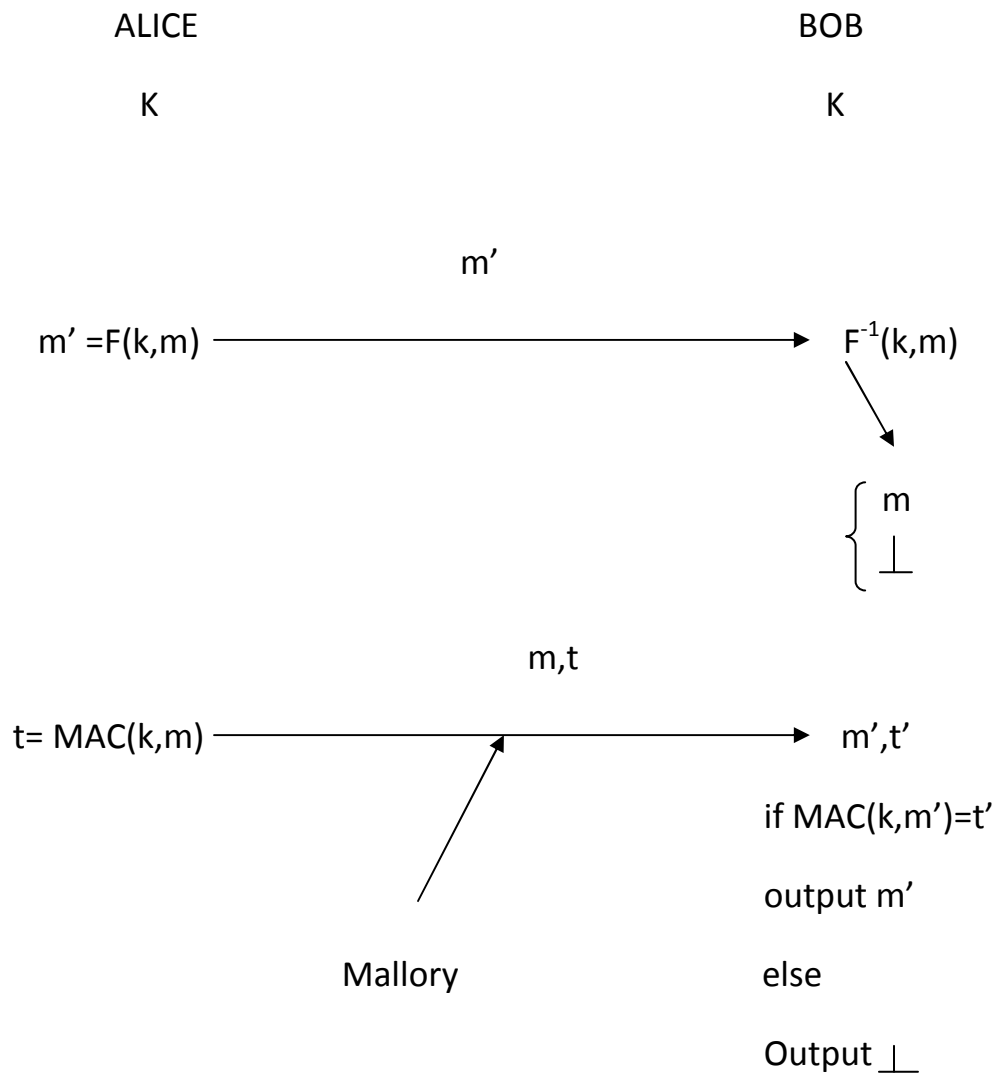


NETWORK SECURITY (2nd OCT)

Submitted by Sruthi Thummala

MESSAGE INTEGRITY

Alice sends Bob a message. Bob has to check the validity, ensure the that he received the original message.



Mallory's Goals

- Modify m and modify t "to match"
 - Compute tag for some message of her choosing.
 - Compute k
 - Find tag collision \rightarrow two messages with same tag.
 - Recognize correct tags
 - Denial of service
- } not considered
as goals here.

Attacker's Resources:

- Listen /observe valid m, t pairs.
- Query MAC oracle
- Query verification oracle

Def:

A MAC scheme is (t, q, q', ξ) secure if $\forall A$ running in time $\leq t$ and making at most q of MAC oracle queries and at most q' of verification oracle queries.

$$\Pr [A^{\text{mack,verfk}} \text{ forges}] \leq \xi$$

Where A forges if A queries $\text{verfk}(m, t) = \text{OK}$ and A did not query MAC_k previously on m .

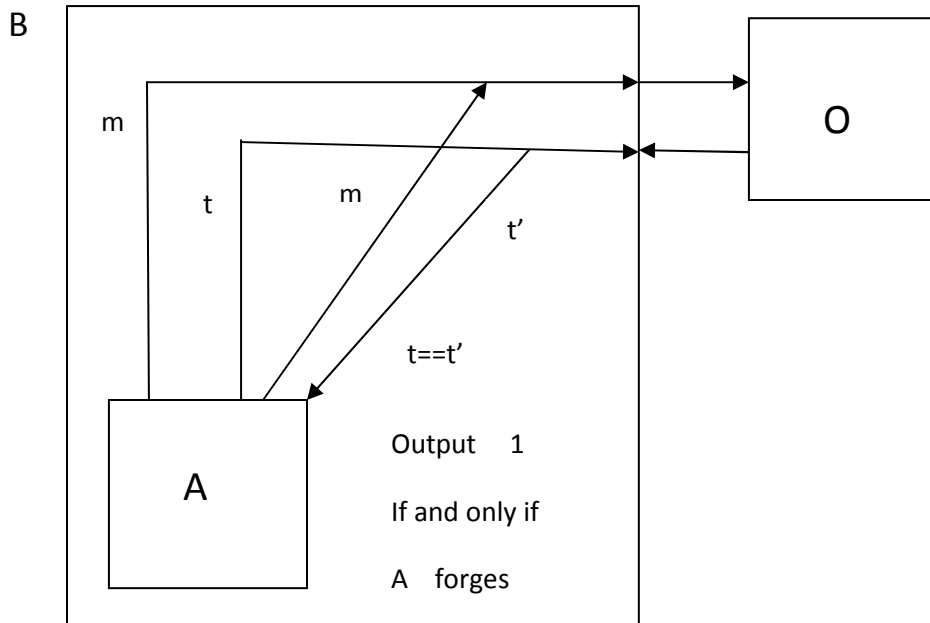
THEOREM:

IF F_i Keys $X \{0,1\}^* \rightarrow \{0,1\}^l$ is a (t, q, ξ) - PRF. The F is a $(t - o(q), q', q - q', \xi + (q - q')/2^l)$ MAC

Proof by contrapositive:

Assume F is not a MAC

Let A break F as a MAC



If $O=R$, then $\Pr [A \text{ forges}] = (q-q')/2^l$

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

If $O=F_k$, then $\Pr [A \text{ forges}] \geq \xi + (q-q')/2^l$

By assumption A breaks F_k as a MAC

ie. $\Pr [B^{F_k} = 1] \geq \xi + (q-q')/2^l$

Therefore,

$$|\Pr [B^R = 1] - \Pr [B^{F_k} = 1]| \geq \xi$$

PRF is a MAC.