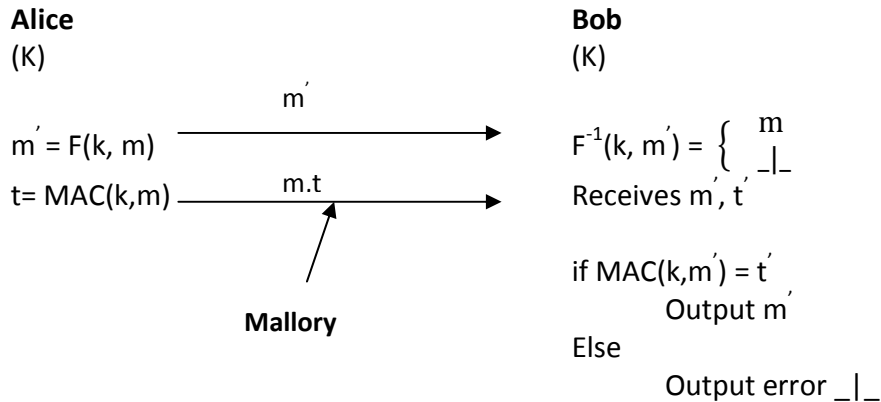


## Network Security Notes (October 2 2009)

By Supreet Padhi

### Message Integrity



Here tag  $t$  is computed as a deterministic and stateless function of  $m, k$ . This scheme is called Message Authentication Code (MAC).

### Mallory Goals

- Modify  $m$  and modify  $t$  to  $m', t'$
- Compute tag for some message
- Find tag collision

### Attacker's Resources

- Observe valid  $m, t$  pairs
- Query MAC oracle
- Query verification oracle

### Message Integrity

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

$$P_r [ A^{\text{MAC}_k, \text{Verf}_k} \text{ forges} ] \leq \epsilon$$

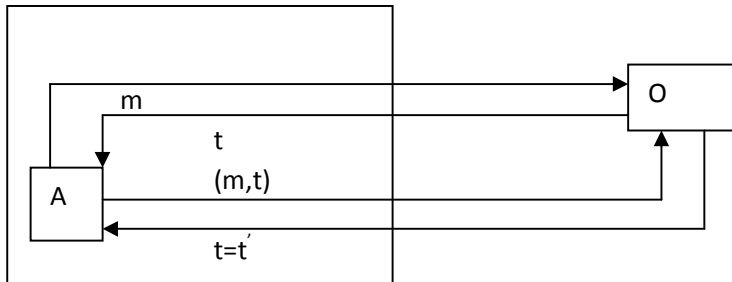
Where  $A$  forges if  $A$  queries  $\text{Verf}_k$  on  $(m, t)$  and  $\text{Verf}_k(m, t) = 1$

and  $A$  hasn't previously queried  $\text{MAC}_k$  on  $M$ .

If  $F_k: \text{Keys} \times \{0, 1\}^* \longrightarrow \{0, 1\}^K$  is  $(q, t, q', \epsilon)$ -PRF. Then  $F$  is a  $(t-O(q), q', q-q', \epsilon + \frac{(q-q')}{2^1})$  MAC

**Proof by contrapositive**

B



In the above diagram

- A queries MAC oracle to get tag  $t' = \text{MAC}(k,m)$
- A queries verification oracle  $\text{Ver}_k(m,t)$

By assumption  $t=t'$  and  $\text{Ver}_k(m,t)=1$

Assume F is not a MAC, Let A breaks F as a MAC

If  $O=R$  then

$$P_r [ A \text{ forges } ] = 2^{-l}$$

$$\text{i.e. } P_r [ B^R = 1 ] = 2^{-l} \text{-----1}$$

if  $O=F_k$  then

$$P_r[A \text{ forges}] \geq \epsilon + \frac{q-q'}{2^l} \text{ by assumption that A breaks } F_k \text{ as a MAC.}$$

$$\text{i.e. } P_r [ B^{F_k} = 1 ] \geq \epsilon + \frac{q-q'}{2^l} \text{-----2}$$

From 1 and 2

$$| P_r [ B^R = 1 ] - P_r [ B^{F_k} = 1 ] | \geq \epsilon \text{ which is false for PRF and hence proved.}$$