

Message Integrity



$$t = \text{MAC}(k, m)$$

if $\text{MAC}(k, m') = t'$

output m'

else

output \perp

t - tag

m - message

k - key

Mallory's Goals

- Modify m and t to match
- Compute tag for some message of her choosing
- Compute k
- Find tag collision
- X Recognize correct tags?
- X Denial of Service

Attacker's Resources

- Observe valid (m, t) pairs
- Query MAC oracle
- Query verification oracle

Def: A MAC scheme is (t, q, q', ϵ) secure if for all adversaries 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 .

Thm: If $F: \text{keys} \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ is a (t, q, ϵ) -PRF.

Then F is a $(t - O(q), q', q - q', \epsilon + (q - q')/(2^l))$ MAC

Proof By Contrapositive: Assume F is not a MAC. Let A break F as a MAC. If $O = R$, then $\Pr[A \text{ forges}] = (q - q')/(2^L)$, i.e. $\Pr[B^O = 1] = (q - q')/(2^L)$. If $O = F_k$, then $\Pr[A \text{ forges}] \geq \epsilon + (q - q')/(2^L)$, by assumption that A breaks F_k as a MAC, $\Pr[B^{F_k} = 1] \geq \epsilon + (q - q')/(2^L)$, therefore $|\Pr[B^R = 1] - \Pr[B^{F_k} = 1]| \geq \epsilon$

