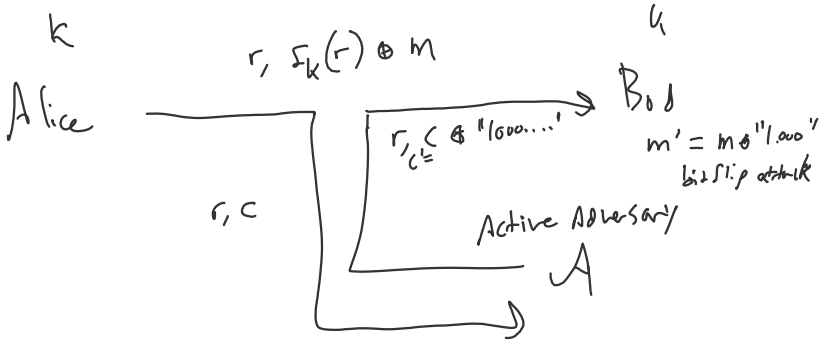
Authentication

Tuesday, October 8, 2019 11:18 AM



Message Auth. Code

Syntax: $k \leftarrow Gen(1^n)$

$tag \leftarrow MAC(k, m)$

$\{0,1\} \leftarrow Verify(k, m, tag)$

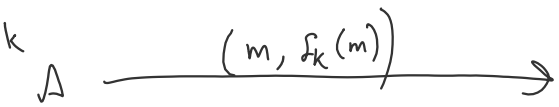
Properties:

- Correctness
- Unforgeability:

$$\forall A,\ Pr\left[k \leftarrow Gen(1^n),\ m', tag' \leftarrow A^{MAC(k,\cdot)} : \begin{array}{l} m' \text{ is not one of the oracle queries,} \\ \text{and } Verify(k, m', tag') = 1 \end{array}\right] \in negl$$

$tag \leftarrow MAC(k, m) = F_k(m)$

PRF



Authentication + encryption

F, g prfs

- encrypt then mac

(check then decrypt) $\underbrace{(r, F_k(r) \oplus m)}_{\text{encryption}}, \underbrace{g_k((r, F_k(r) \oplus m))}_{\text{mac}}$

- mac and encrypt

$(r, f_k(r) \oplus m),\ g_k(m)$

– mac then encrypt

(decrypt then check) $\left(r, \left(m, g_k(m)\right) \oplus f_k(r)\right)$