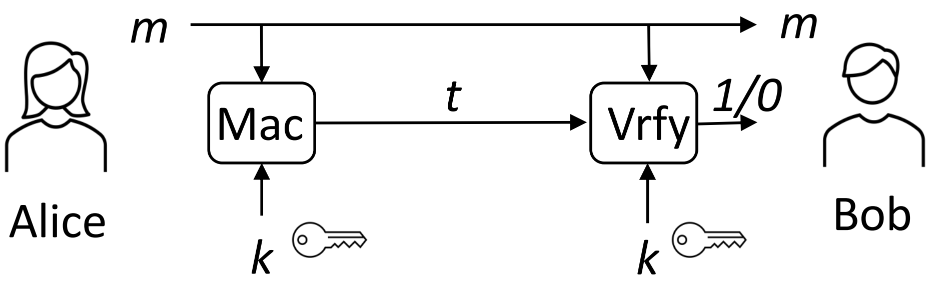
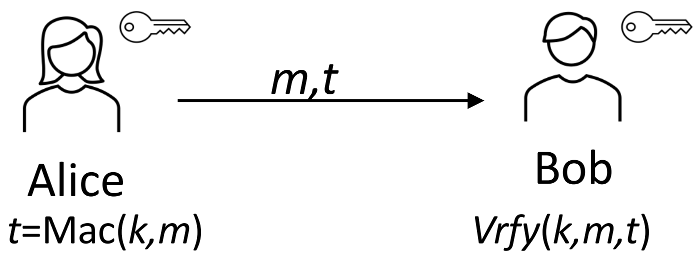
Message Authentication Code (MAC)-

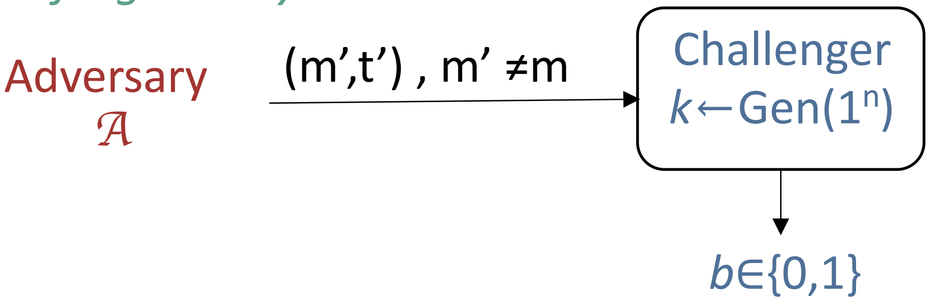


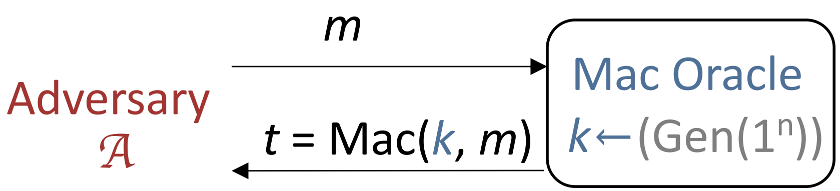
Tag generation: t = Mac(k,m)
Tag verification: *Vrfy*(k,m,t) = 1 for a valid tag, 0 otherwise
Correctness: $\forall m \in \mathcal{M}$, $k \in \mathcal{K}$ Vrfy(k,m,Mac(k,m)) = 1



No. of keys	
for N bi-directional communicating parties	
Each: N-1 [k]	*Total: N(N-1)/2 [k]*

Unforgeability





*poly no. of queries

$\text{Mac}^{\text{forge}}_{\mathcal{A},\pi}(n)$ = 1 if Vrfy(k,m,t)=1 and 0 otherwise

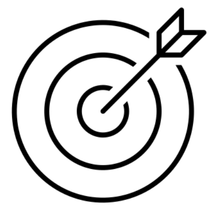
$\pi = (\text{Mac}, \text{Vrfy})$ is existentially unforgeable under an adaptive chosen message attack if $\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible such that

$$\Pr[\text{Mac}^{\text{forge}}_{\mathcal{A},\pi}(n)=1] \leq \varepsilon(n)$$

** Message Integrity Codes (MIC)*

Terminology

k: symmetric key *m*: plaintext	*t*: tag	Mac: tag generation algorithm Vrfy: tag verification algorithm



Integrity

www.ruxandraolimid.weebly.com/pagesonsecurity

Pages on SecuRity by Ruxandra F. Olimid