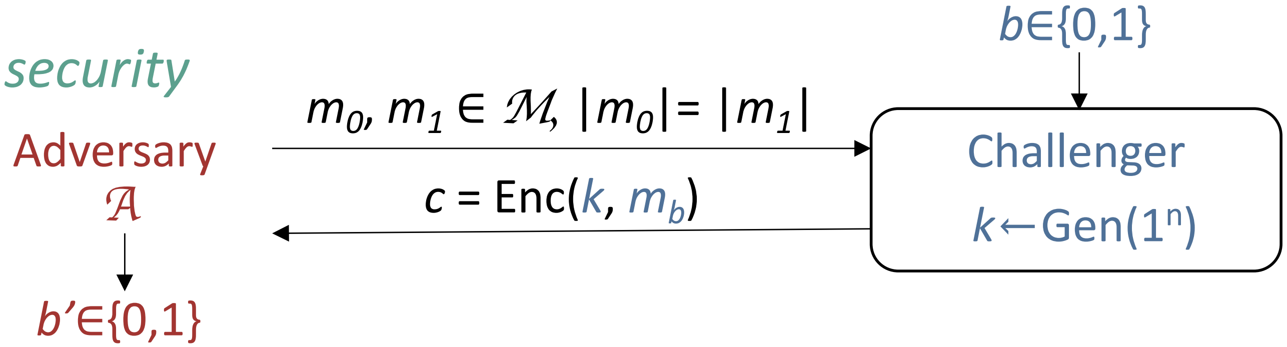
Security Notions (Encryption) -

Semantic security


$b \in \{0,1\}$
$m_0, m_1 \in \mathcal{M}, |m_0| = |m_1|$
Adversary
$\mathcal{A}$
$c = \mathrm{Enc}(k, m_b)$
Challenger
$k \leftarrow \mathrm{Gen}(1^n)$
$b' \in \{0,1\}$

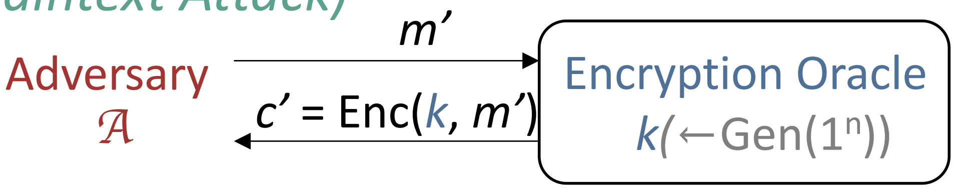
$\pi = (\mathrm{Enc}, \mathrm{Dec})$ is semantically secure if $\forall \mathcal{A}$ PPT, $\exists\, \varepsilon(n)$ negligible such that

$$\Pr[\mathrm{Priv}^{eav}_{\mathcal{A},\pi}(n)=1] \leq ½ + \varepsilon(n)$$

$\mathrm{Priv}^{eav}_{\mathcal{A},\pi}(n) = 1$ if b'=b and 0 otherwise

CPA-security (Chosen-Plaintext Attack)

Semantic security +



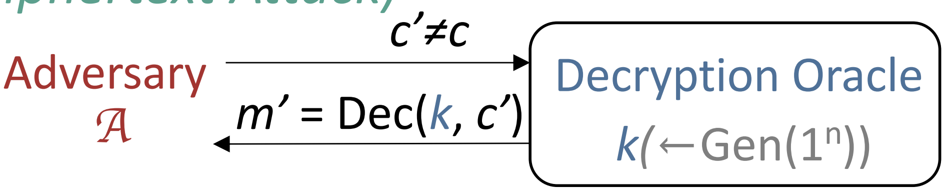
$\pi = (\mathrm{Enc}, \mathrm{Dec})$ is CPA-secure if $\forall \mathcal{A}$ PPT, $\exists\, \varepsilon(n)$ negligible such that

$$\Pr[\mathrm{Priv}^{cpa}_{\mathcal{A},\pi}(n)=1] \leq ½ + \varepsilon(n)$$

$\mathrm{Priv}^{cpa}_{\mathcal{A},\pi}(n) = 1$ if b'=b and 0 otherwise

CCA-security (Chosen-Ciphertext Attack)

CPA-security +



$\pi = (\mathrm{Enc}, \mathrm{Dec})$ is CCA-secure if $\forall \mathcal{A}$ PPT, $\exists\, \varepsilon(n)$ negligible such that

$$\Pr[\mathrm{Priv}^{cca}_{\mathcal{A},\pi}(n)=1] \leq ½ + \varepsilon(n)$$

$\mathrm{Priv}^{cca}_{\mathcal{A},\pi}(n) = 1$ if b'=b and 0 otherwise

Π semantic secure at multiple interceptions ➡ Π non-deterministic ; Π CCA-secure ➡ Π non-malleable

increased capabilities

Stronger security

+ multiple interceptions / integrations

+ adaptive adversary

www.ruxandraolimid.weebly.com/pagesonsecurity

Pages on SecuRity by Ruxandra F. Olimid