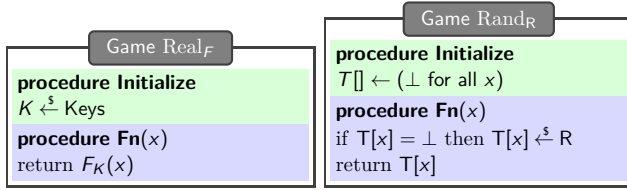


Games defining prf advantage of an adversary against F

Let $F: \text{Keys} \times D \rightarrow R$ be a family of functions.



Definition of $\text{Adv}_F^{\text{prf}}$

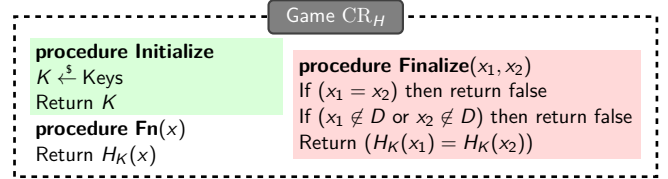
The (prf) **advantage** of A is

$$\text{Adv}_F^{\text{prf}}(A) = \Pr[\text{Real}_F^A \Rightarrow 1] - \Pr[\text{Rand}_R^A \Rightarrow 1]$$

Security: F is a (secure) PRF if $\text{Adv}_F^{\text{prf}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

Collision-resistance of a function family

The formalism considers a family $H: \text{Keys} \times D \rightarrow R$ of functions, meaning for each $K \in \text{Keys}$ we have a function $H_K: D \rightarrow R$ defined by $H_K(x) = H(K, x)$.

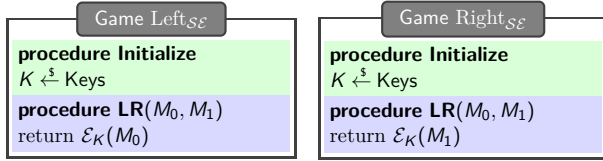


Let

$$\text{Adv}_H^{\text{cr}}(A) = \Pr[\text{CR}_H^A \Rightarrow \text{true}].$$

Games for ind-cpa-advantage of an adversary A

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme



Definition of $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}$

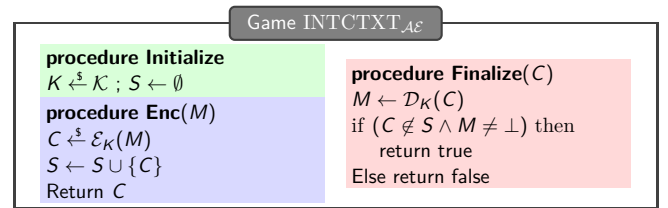
The (ind-cpa) **advantage** of A is

$$\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) = \Pr[\text{Right}_{\mathcal{SE}}^A \Rightarrow 1] - \Pr[\text{Left}_{\mathcal{SE}}^A \Rightarrow 1]$$

Security: \mathcal{SE} is IND-CPA-secure if $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

Ciphertext integrity

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme.



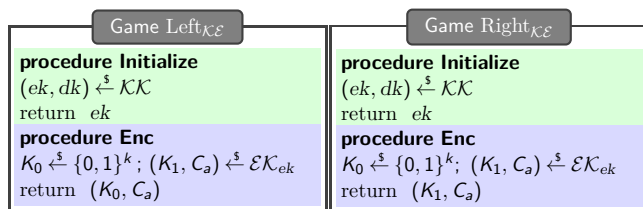
Definition: int-ctxt advantage

The int-ctxt advantage of an adversary A is

$$\text{Adv}_{\mathcal{AE}}^{\text{int-ctxt}}(A) = \Pr[\text{INTCTXT}_{\mathcal{AE}}^A \Rightarrow \text{true}]$$

KEM IND-CPA security games

Let $\mathcal{KE} = (\mathcal{KK}, \mathcal{EK}, \mathcal{DK})$ be a KEM with key length k .



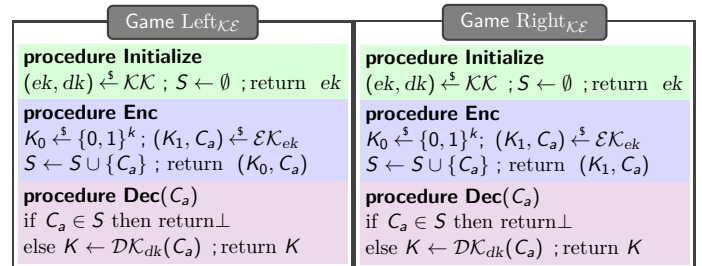
Definition (ind-cpa advantage $\text{Adv}_{\mathcal{KE}}^{\text{ind-cpa}}$ for KEMs)

The (ind-cpa) **advantage** of an adversary A is

$$\text{Adv}_{\mathcal{KE}}^{\text{ind-cpa}}(A) = \Pr[\text{Right}_{\mathcal{KE}}^A \Rightarrow 1] - \Pr[\text{Left}_{\mathcal{KE}}^A \Rightarrow 1]$$

KEM IND-CCA security games

Let $\mathcal{KE} = (\mathcal{KK}, \mathcal{EK}, \mathcal{DK})$ be a KEM with key length k .



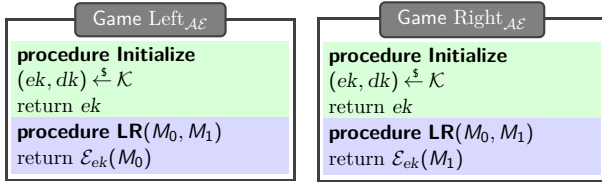
Definition (ind-cca advantage $\text{Adv}_{\mathcal{KE}}^{\text{ind-cca}}$ for KEMs)

The (ind-cca) **advantage** of an adversary A is

$$\text{Adv}_{\mathcal{KE}}^{\text{ind-cca}}(A) = \Pr[\text{Right}_{\mathcal{KE}}^A \Rightarrow 1] - \Pr[\text{Left}_{\mathcal{KE}}^A \Rightarrow 1]$$

PKE IND-CPA security games

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme.



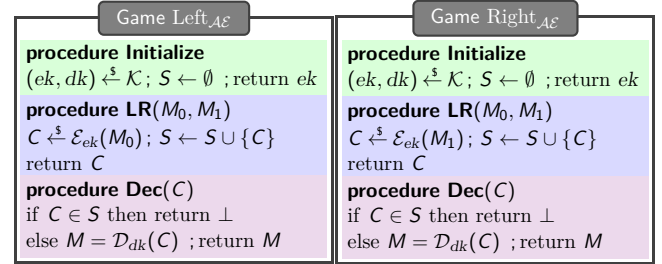
Definition (ind-cpa advantage $\text{Adv}^{\text{ind-cpa}}$, public-key version)

The (ind-cpa) **advantage** of an adversary A is

$$\text{Adv}_{\mathcal{AE}}^{\text{ind-cpa}}(A) = \Pr[\text{Right}_{\mathcal{AE}}^A \Rightarrow 1] - \Pr[\text{Left}_{\mathcal{AE}}^A \Rightarrow 1]$$

PKE IND-CCA security games

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme.



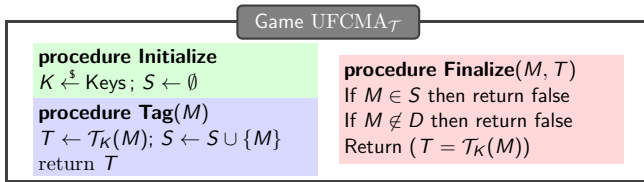
Definition (ind-cca advantage $\text{Adv}^{\text{ind-cca}}$)

The **ind-cca advantage** of an adversary A is

$$\text{Adv}_{\mathcal{AE}}^{\text{ind-cca}}(A) = \Pr[\text{Right}_{\mathcal{AE}}^A \Rightarrow 1] - \Pr[\text{Left}_{\mathcal{AE}}^A \Rightarrow 1]$$

UF-CMA (MACs)

Let $\mathcal{T}: \text{Keys} \times \mathcal{D} \rightarrow \mathcal{R}$ be a message authentication code.



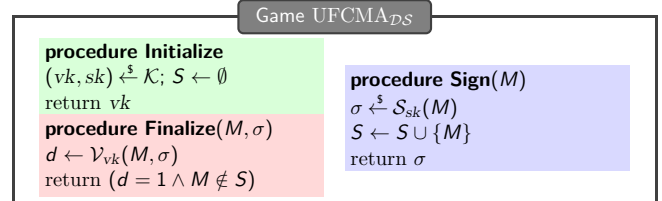
Definition: uf-cma advantage

The uf-cma advantage of an adversary A is

$$\text{Adv}_{\mathcal{T}}^{\text{uf-cma}}(A) = \Pr[\text{UFCMA}_{\mathcal{T}}^A \Rightarrow \text{true}]$$

UF-CMA (digital signatures)

Let $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ be a signature scheme.



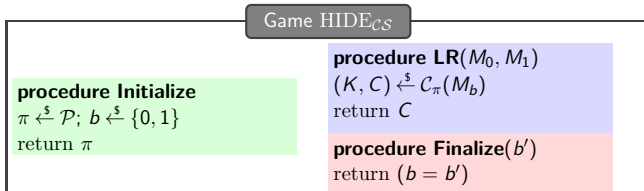
Definition: uf-cma advantage (digital signature version)

The uf-cma advantage of an adversary A is

$$\text{Adv}_{\mathcal{DS}}^{\text{uf-cma}}(A) = \Pr[\text{UFCMA}_{\mathcal{DS}}^A \Rightarrow \text{true}]$$

Hiding security

Let $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ be a commitment scheme.



Definition (hiding-advantage)

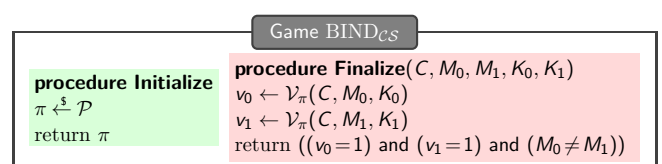
The hiding-advantage of an adversary A is

$$\text{Adv}_{\mathcal{CS}}^{\text{HIDE}}(A) = 2 \cdot \Pr[\text{HIDE}_{\mathcal{CS}}^A \Rightarrow \text{true}] - 1.$$

Hiding security asks that an adversary having C but not K should not learn even partial information about the message M .

Binding security

Let $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ be a commitment scheme.



Definition (binding-advantage)

The binding-advantage of an adversary A is

$$\text{Adv}_{\mathcal{CS}}^{\text{BIND}}(A) = \Pr[\text{BIND}_{\mathcal{CS}}^A \Rightarrow \text{true}].$$

Binding security asks that an adversary be unable to create a commitment C that it can open to two different messages.