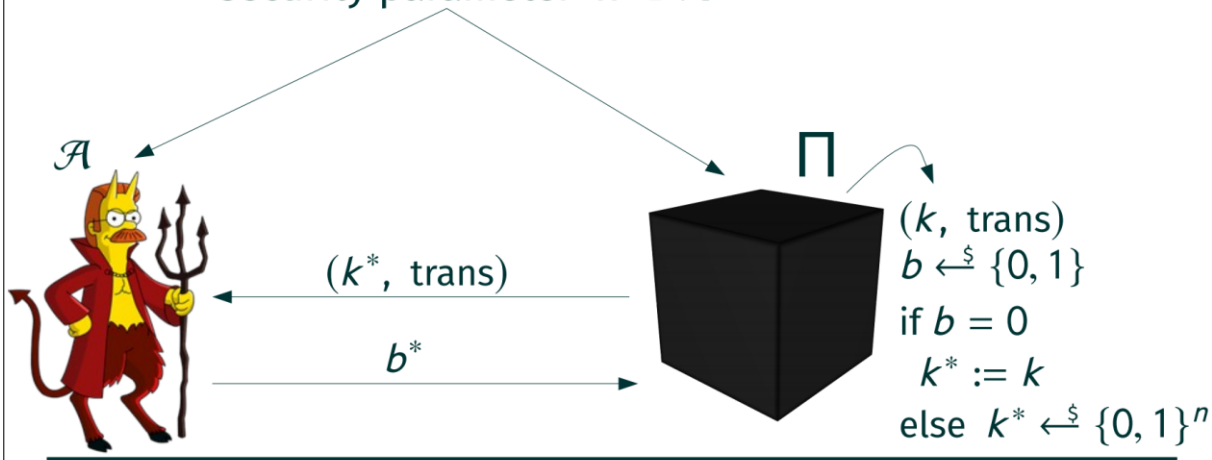
Key Exchange - Security Definition

$KE^{eav}_{\mathcal{A},\Pi}$ Security §10.3

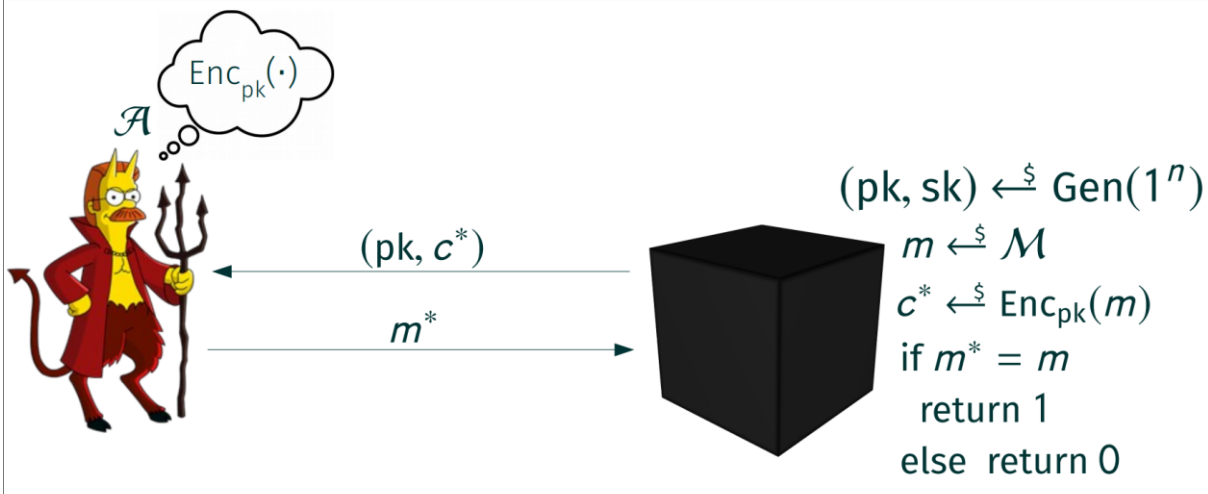
security parameter $n \in \mathbb{N}$



A key-exchange protocol Π is secure in the presence of an eavesdropper if for every PPT adversary **A**

$$\Pr[b = b^*] \leq \tfrac{1}{2} + \text{negl}(n)$$

OW-CPA Security

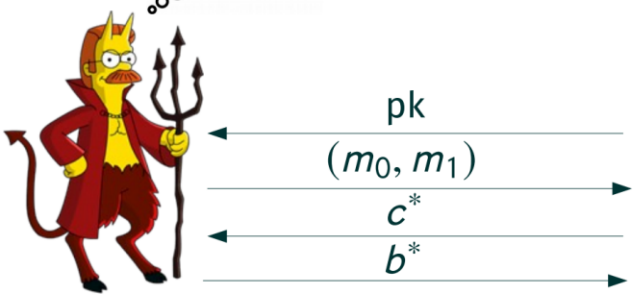


A public-key encryption scheme Π = (Gen, Enc, Dec) has one-way encryptions in the presence of an eavesdropper if for all PPT adversaries **A** there is a negligible function negl s.t.

$$\Pr[\text{PubK}^{\text{ow-cpa}}_{A,\Pi}(n)=1] \leq \text{negl}(n)\,.$$

IND-CPA Security

$\mathrm{PubK}^{eav}_{\mathcal{A},\Pi}$ Security §11.2.1



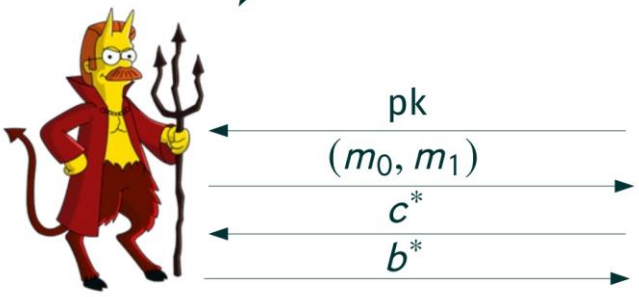
$(pk, sk) \xleftarrow{\$} \mathrm{Gen}(1^n)$
$b \xleftarrow{\$} \{0,1\}$
$c^* \xleftarrow{\$} \mathrm{Enc}_{pk}(m_b)$
if $b^* = b$
return 1
else return 0

A public-key encryption scheme Π = (Gen, Enc, Dec) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries **A** there is a negligible function negl s.t.

$$\Pr[\mathrm{PubK}^{eav}_{A,\Pi}(n)=1] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

IND-CCA Security

Oracle $\mathrm{Dec}'_{sk}(\cdot)$
if $c_i = c^*$
return $\perp$
else return $\mathrm{Dec}_{sk}(c_i)$

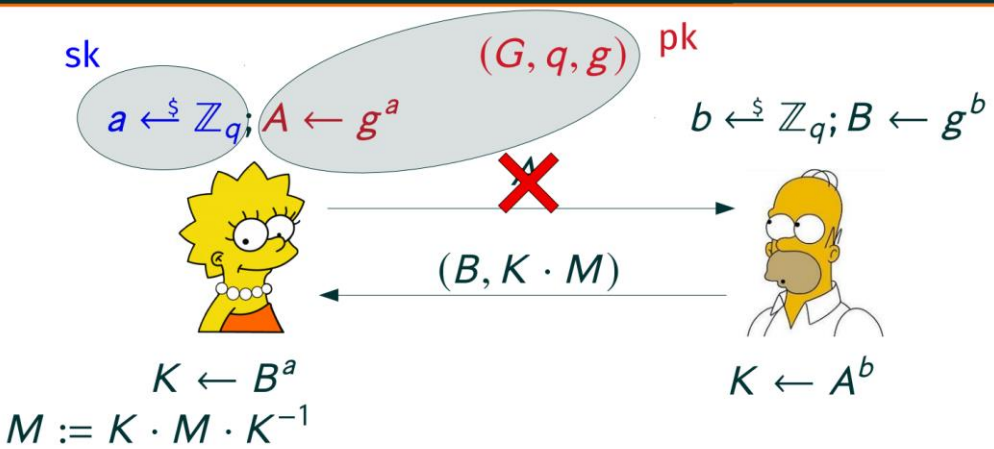


$(pk, sk) \xleftarrow{\$} \mathrm{Gen}(1^n)$
$b \xleftarrow{\$} \{0,1\}$
$c^* \xleftarrow{\$} \mathrm{Enc}_{pk}(m_b)$
if $b^* = b$
return 1
else return 0

A public-key encryption scheme Π = (Gen, Enc, Dec) has indistinguishable encryptions under chosen-ciphertext attacks if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function negl s.t.

$$\Pr[\mathrm{PubK}^{cca}_{\mathcal{A},\Pi}(n)=1] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

ElGamal Encryption - Intuition



- Take the DH KE protocol and fix "first message" A (together with group parameters) of Alice as her public key (secret a is her secret key)
- To encrypt to Alice, Bob chooses ephemeral key B, uses K as one-time pad to encrypt a message $M \in G$ and additionally sends B
- Any KE protocol that is secure in the presence of an eavesdropper (Def. 10.1) yields an IND-CPA secure PKE

ElGamal Encryption

- Gen(1^n): Run $(G, q, g) \leftarrow G(1^n)$, pick $x \leftarrow^{\$} Z_q$ compute $y := g^x$ and output $(sk, pk) := ((G, q, g, x), (G, q, g, y))$

- Enc (m, pk): On input $m \in G$ and $pk = (G, q, g, y)$, pick $r \leftarrow^{\$} Z_q$, compute and output

$$C := (g^r, m \cdot y^r)$$

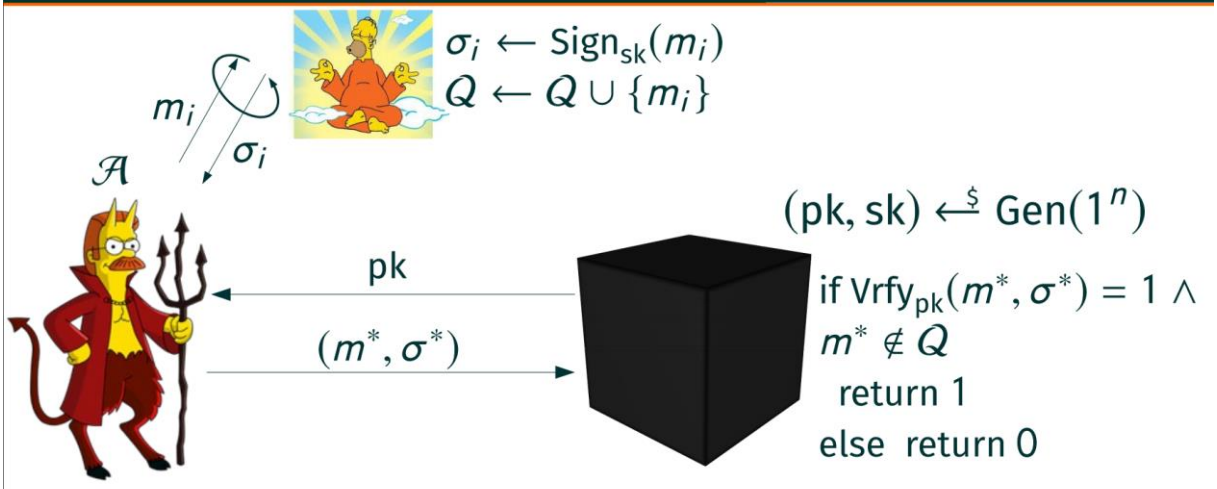
- Dec (C, sk): On input $C = (C_1, C_2)$ and $sk = (G, q, g, x)$, compute and output

$$m := C_2 \cdot (C_1^x)^{-1}$$

Correctness: $C_2 \cdot (C_1^x)^{-1} = m \cdot y^r \cdot ((g^r)^x)^{-1} = m \cdot y^r \cdot (y^r)^{-1} = m \cdot 1 = m$

We can also consider (G,q,g) as system parameters pp which are input to Gen and remove them from the keys. All algorithms then implicit have access to pp. So, many users can generate keys with respect to the same parameters (as typically the case with elliptic curve cryptography).

EUF-CMA Security



A signature scheme scheme Σ = (Gen, Sig, Vrfy) is existentially unforgeably under chosen message attacks (EUF-CMA) secure, if for all PPT adversaries $\mathcal{A}$ there is a negligible function negl s.t.

$$\Pr[\text{Sig-forge}^{\text{euf-cma}}_{\mathcal{A},\Sigma}(n)=1] \leq \text{negl}(n) .$$

Schnorr Signatures

- KeyGen: run $\mathcal{G}(1^n)$ to obtain (G, q, g). Choose $x \leftarrow^{\$} \mathbb{Z}_q$ and set $y := g^x$. The private key is x and the public key is (G, q, g, y). As part of key generation, a function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ is specified.
- Sign: on input a private key x and a message $m \in \{0, 1\}^*$, choose $k \leftarrow^{\$} \mathbb{Z}_q$ and set $I := g^k$. Then compute $r := H(I, m)$ and $s := rx + k \bmod q$. Output the signature $\sigma := (r, s)$.
- Vrfy: on input a public key (G, q, g, y), a message $m \in \{0, 1\}^*$, and a signature $\sigma = (r, s)$, compute $I := g^s \cdot y^{-r}$ and output 1 if $H(I, m) = r$.

Correctness: $g^s \cdot y^{-r} = g^{rx + k} \cdot g^{-xr} = g^k = I$

THEOREM: If the discrete-logarithm problem is hard relative to $\mathcal{G}$ and H is a random oracle, then the Schnorr signature scheme is EUF-CMA secure.

Formal Security Notions for Digital Signatures

- Attack model (increasing strength)
  - No-message attack (NMA): Adversary only sees public key
  - Random message attack (RMA): Adversary can obtain signatures for random messages (not in the control of the adversary)
  - Non-adaptive chosen message attack (naCMA): Adversary defines a list of messages for which it wants to obtain signatures (before it sees the public key)
  - Chosen message attack (CMA): Adversary can adaptively ask for signatures on messages of its choice

Formal Security Notions for Digital Signatures

- Goal of an adversary (decreasing hardness)
  - Universal forgery (UF): Adversary is given a target message for which it needs to output a valid signature
  - Existential forgery (EF): Adversary outputs a signature for a message of the adversary's choice

- **Security notion:** attack model + goal of the adversary

- For schemes used in practice: Adversary can not even achieve the weakest goal in the strongest attack model
  - **EUF-CMA**: existential unforgeability under chosen message attacks