$\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$

adversary A

challenger

pk

$m_0, m_1 \leftarrow A^{\mathrm{Enc}_{pk}(\cdot),\mathrm{Dec}_{sk}(\cdot)}(pk)$

$|m_0|=|m_1|$

m_0, m_1

$(pk,sk) \leftarrow \mathrm{Gen}(1^n)$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathrm{Enc}_{pk}(m_b)$

c

$b' \leftarrow A^{\mathrm{Enc}_{pk}(\cdot),\mathrm{Dec}_{sk}(\cdot)}(c)$

b'

adv A cannot ask to decrypt c !

b=b'

b≠b'

1

0