$sk = x$, $pk = g, g^x$

$Enc(pk, 0)$: $y \leftarrow \mathbb{Z}_p$ $\quad c = (g^y, g^{xy})$

$Enc(pk, 1)$: $y \leftarrow \mathbb{Z}_p, z \leftarrow \mathbb{Z}_p$ $\quad c = (g^y, g^z)$

$Dec(sk, c = (c_1, c_2))$ if $c_1^x = c_2$ output 0

otherwise output 1

$\mathcal{C}_{DDH}$ $\qquad \mathcal{R}$ $\qquad \mathcal{A}_{IND\text{-}CPA}$

$\xrightarrow{(g, g^x, g^y, Z)}$

$\xrightarrow{(g, g^x)}$

$\xleftarrow{0, 1}$

$\xrightarrow{(g^y, Z)}$

$\xleftarrow{b}$

if $b=0$ output "real"
else output "random"

$\longleftarrow$

Disadvantages: - large ciphertexts (can only encrypt one bit at a time)

- not perfectly correct
may choose $z = xy$ w/ prob $\frac{1}{p}$

Σ_1: Keygen: sample $x \leftarrow \mathbb{Z}_p$, $sk = x$

$pk = (g, g^x)$

Sign(sk, m): $\sigma = x + m$

Verify(pk, m, σ): check $g^m \cdot pk = g^\sigma$

$C_{DLog} \xrightarrow{(g, g^x)} R \xrightarrow{(g, g^x)} A_{EUF\text{-}NMA}$

$g^m \cdot g^x = g^{m+x}$

$R \xleftarrow{m, \sigma} A$

$x' = \sigma - m$

$C \xleftarrow{x'} R$

EUF-CMA A:

request σ on random $m \in \mathbb{Z}_p$

compute $sk = \sigma - m$

choose $m' \neq m \in \mathbb{Z}_p$

Sign$(sk, m') = \sigma'$

output (m', σ')

KeyGen$_2$: $sk = x \in \mathbb{Z}_p$ $pk = (g, g^x)$

Sign$(sk, m = (m_1, m_2) \in G \times G)$:

$$\sigma = m_1^{-x} \cdot m_2 = \text{ElGamal.Dec}(sk, m)$$

Verify $\text{EG.Enc}(pk, \sigma) = m$

$\Leftrightarrow$ choose $r \leftarrow \mathbb{Z}_p$

outputs $g^r, (g^x)^r \cdot \sigma$

w/ prob $1 - \frac{1}{p}$ $g^r \neq m_1$

$KeyGen_1 = KeyGen_0$

$Enc_1(pk, m) = Enc_0(pk, m \| 1)$

$Dec_1(sk, c) := m \| b = Dec_0(sk, c)$

if $b = 1$ output m

otherwise output sk

IND-CPA:

$\mathcal{E}_{IND\text{-}CCA_0}$ $\quad$ R $\quad$ A_1 INDCPA

$\mathcal{E} \xrightarrow{pk} R \xrightarrow{pk} A_1$

$\mathcal{E} \xleftarrow{m_0 \| 1,\ m_1 \| 1} R \xleftarrow{m_0, m_1} A_1$

$\mathcal{E} \xrightarrow{c} R \xrightarrow{c} A_1$

$\mathcal{E} \xleftarrow{b} R \xleftarrow{b} A_1$

IND-CCA1 adversary:

$Enc(pk, m \| 0) \to c$

query $Dec(sk, c)$

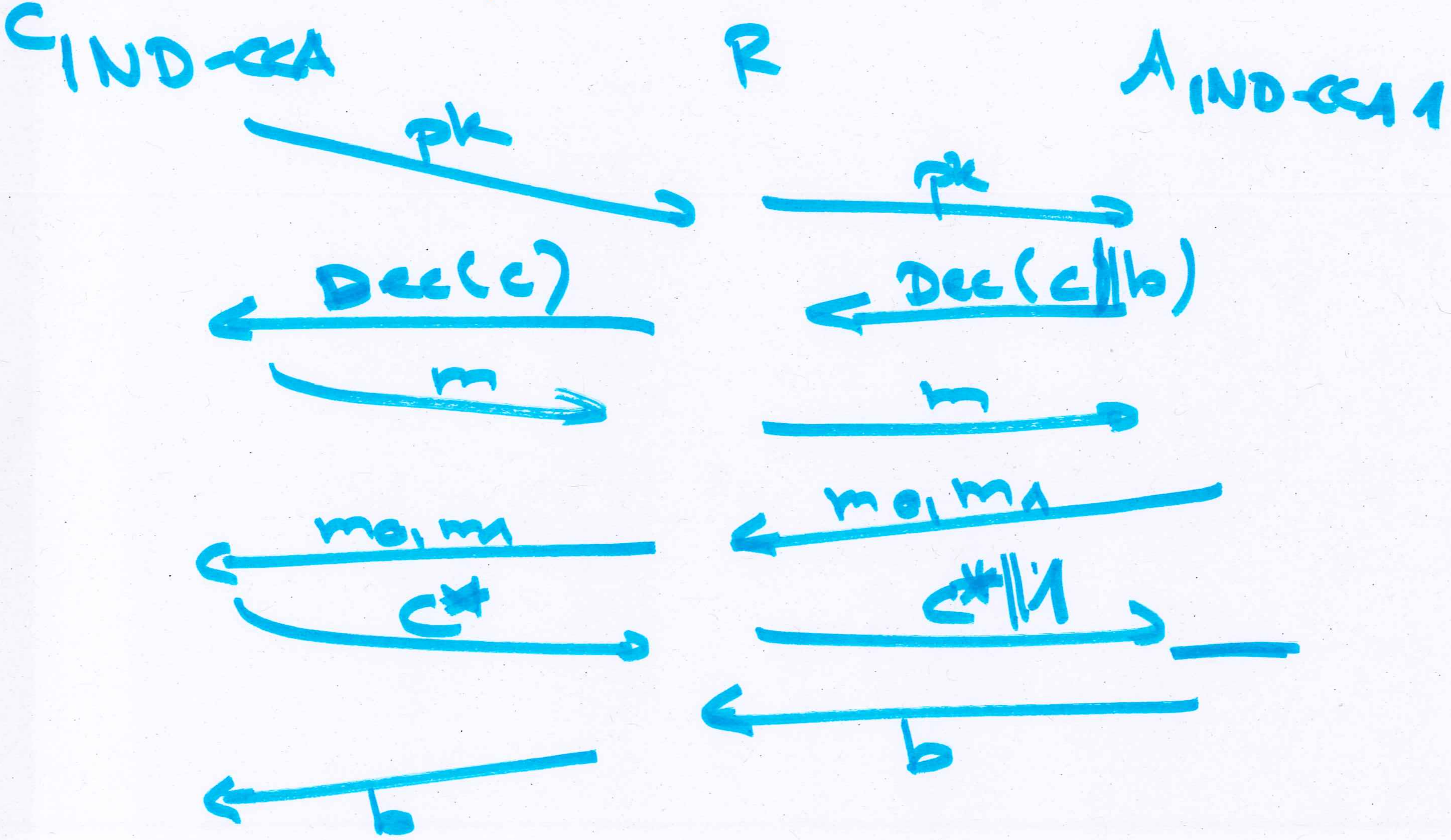
gets sk

use sk to break IND-CCA1

$KeyGen_2 = KeyGen_0$

$Enc_2(pk,m) = Enc_0(pk,m) \| 1$

$Dec_2(sk, c\|b) = Dec_0(sk, c)$



IND-CCA Adversary (pk)

choose m_0, m_1

get $c^* = c' \| 1$

query $c' \| 0$ to Dec oracle

$\neq c^*$

get m_b

output b