- prime p, g primitive root of p : $\forall y : \exists x : g^x = y \bmod p$.
- DL : Given prime p, p.r of p g, and $1 \le y < p$, find x s.t $g^x = y \bmod p$.

DL assumptions = ↗ hard problem.

- DDH : Given prime p, p.r. of p g, $1 \le g^a, g^b, g^c < p$ decide $c = a \cdot b \bmod p-1$.

↓

assumption : hard.

$$\left| \Pr_{r \leftarrow g^a, g^b, g^{ab}}[A(r) = 1] - \Pr_{r \leftarrow g^a, g^b, g^c}[A(r) = 1] \right| \le \text{negl}. \quad \frac{1}{\text{poly}(c)}$$

Diffie-Hellman key Exchange

common secret K

$\mathbb{Z}_p^* = \{1, \dots, p-1\}$

K^{-1}

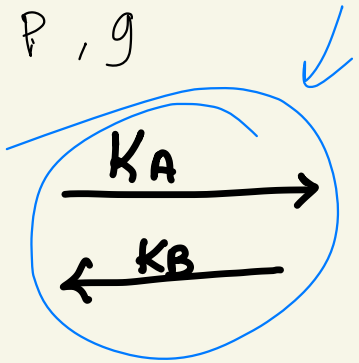
A

$a \xleftarrow{r} \mathbb{Z}_p^*$

$K_A = g^a \bmod p$

$K = (K_B)^a \bmod p$

p, g



B

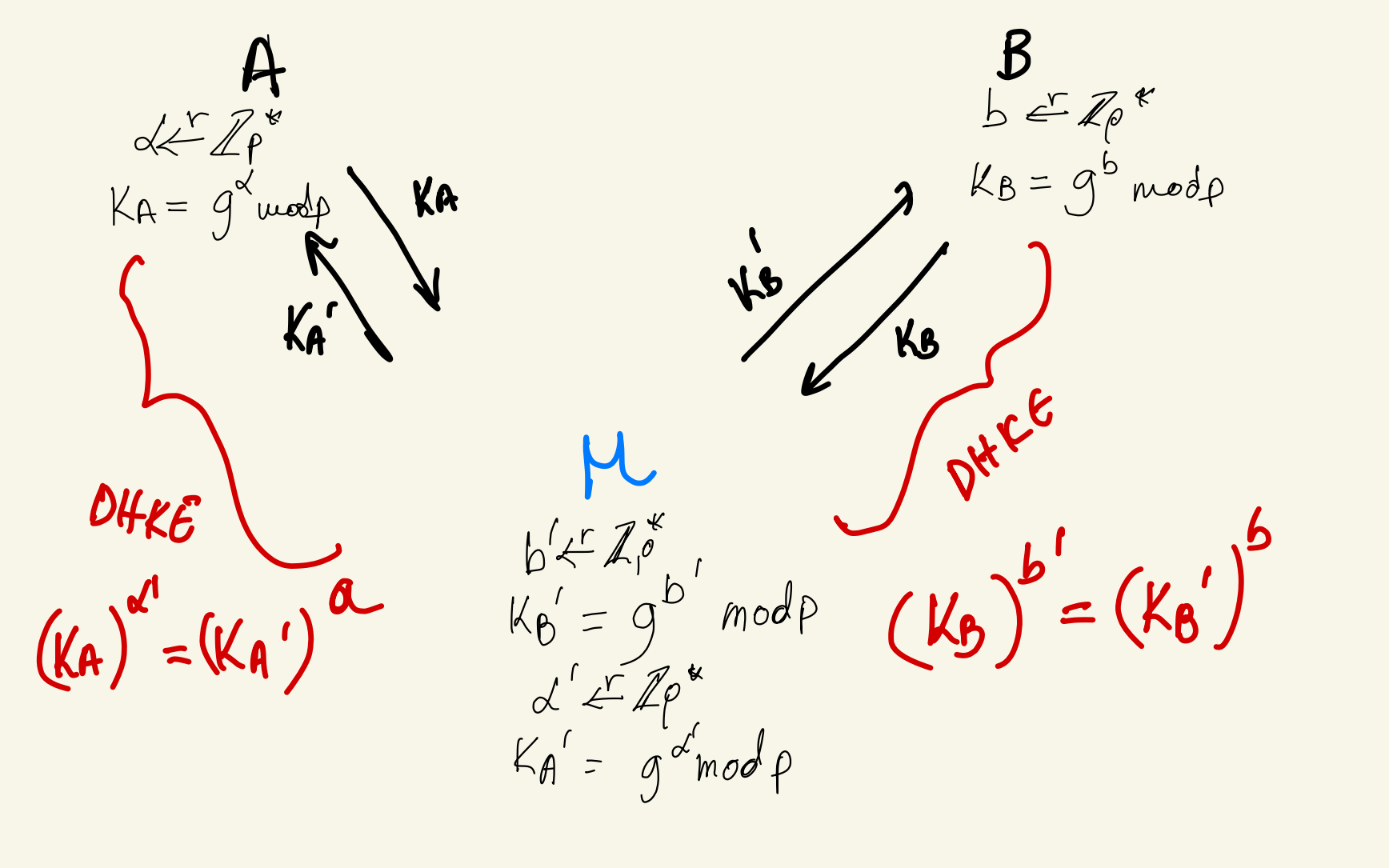
$b \xleftarrow{r} \mathbb{Z}_p^*$

$K_B = g^b \bmod p$

$K' = (K_A)^b \bmod p$

Correctness:

$$K' = (K_A)^b = (K^a)^b = K^{ab} = (K^b)^a = (K_B)^a = K \bmod p.$$


A
$\alpha \xleftarrow{r} \mathbb{Z}_p^*$
$K_A = g^{\alpha} \bmod p$
K_A
K_A'
DHKE
$(K_A)^{\alpha'} = (K_A')^{a}$
M
$b' \xleftarrow{r} \mathbb{Z}_p^*$
$K_B' = g^{b'} \bmod p$
$\alpha' \xleftarrow{r} \mathbb{Z}_p^*$
$K_A' = g^{\alpha'} \bmod p$
B
$b \xleftarrow{r} \mathbb{Z}_p^*$
$K_B = g^{b} \bmod p$
K_B'
K_B
DHKE
$(K_B)^{b'} = (K_B')^{b}$

Public-key Cryptosystems

secret key , public key

Digital Signatures

Encryption Schemes

Keychen: (DL) p, g

$x \xleftarrow{r} \mathbb{Z}_p^*$

secret key K_S

$y = g^x \bmod p$

public key K_P

Digital Signatures

- Authentication : origin
- integrity : alter m
- non-repudiation : cannot deny signing m

---

1. KeyGen : (Kp, Ks)
2. Sign : $(K_s, m) \rightarrow \sigma$ signature on m
3. Verify : $(K_p, m, \sigma) \rightarrow$ valid or not $\{0, 1\}$.

Correctness : $\text{Verify}(K_p, m, \underset{\sigma}{\text{Sing}}(K_s, m)) = 1$

Unforgeability : $m - \sigma \rightarrow$ valid (K_s did not sign m)

ElGamal DS

A (m) k_s ← Key gen: $k_p = g^{k_s} \bmod p$ (schoolbook) → B

$h(m') = h(m)$

Sign:

$x \xleftarrow{r} \mathbb{Z}_p^*$, $\gcd(x, p-1) = 1$

$r = g^x \bmod p$

$s = (h(m) - k_s \cdot r) \cdot x^{-1} \bmod p-1$

s'

DL

$\sigma = (r, s)$, m →

Verify:

$h(m)$

$g^{h(m)} = k_p^r \cdot r^s \bmod p$

Correctness:

$k_p^r \cdot r^s = g^{k_s \cdot r} \cdot g^{x \cdot (m - k_s \cdot r) \cdot x^{-1}} =$

$g^{k_s \cdot r - k_s \cdot r + m} = g^m \pmod p$

Existential Forgery Attack

M Kp B

$v \xleftarrow{r} \mathbb{Z}_p^*$

$r = g^v \cdot K_p \mod p$

$S = -r \mod p$

$m = v \cdot S$

σ

$(s, r), m \longrightarrow$

$g^m = K_p^r \cdot r^s \mod p$

Verify: $K_p^r \cdot r^s = K_p^{-s} \cdot (g^v \cdot K_p)^s = K_p^{-s+s} \cdot g^{v \cdot s} = g^m \mod p$

valid

Cryptographic Hash Functions

- Hash function:
- Easy compute
- One-Way: difficult to invert (OWF)
  $h(x)$
- Collision Resistance

Given $y = h(x)$ can't find x' — Weak

$\leq$

$\exists x, x' : h(x) = h(x')$ — Strong

$h(x') = h(x)$

- Strong Collision Resistance $\geq$ OWF

h easy to invert, $h(x) \xrightarrow{\text{invert}} x' \neq x$

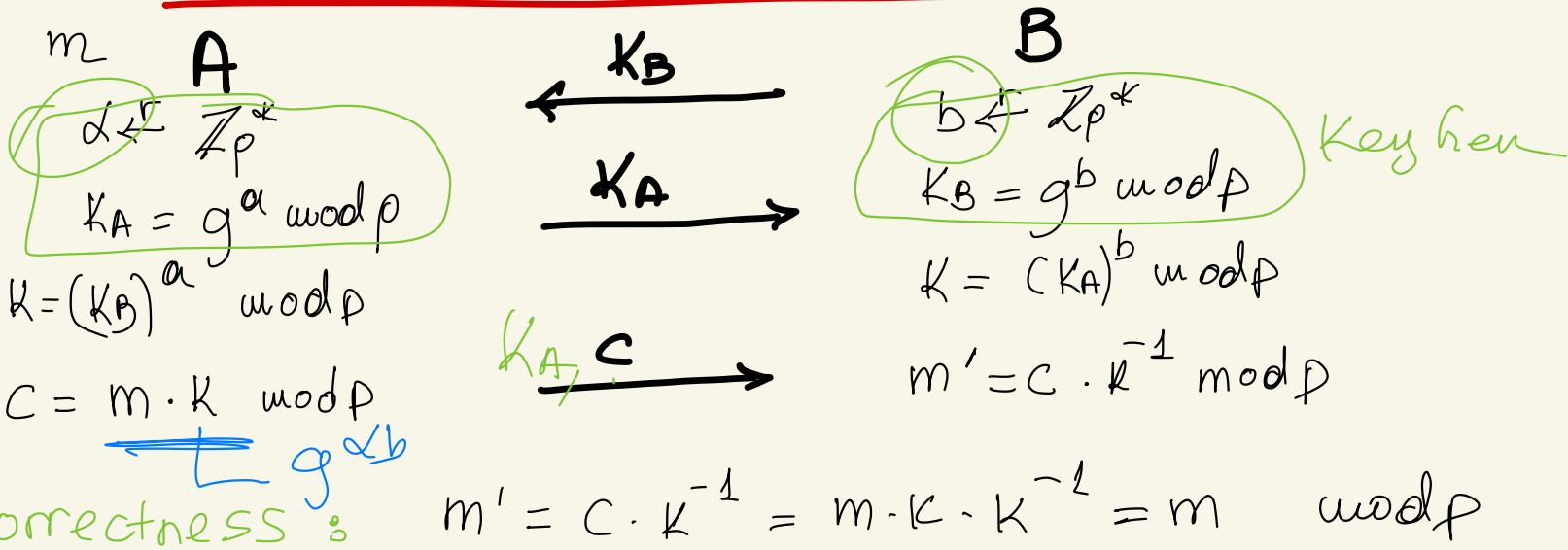
- **One Way Functions $\Rightarrow$ $P \neq NP$**

- f one-way
- Build P_1 : Given (x', y) $\exists x$ s.t. $x' < x$ $f(x) = y$

↓ $P_1 \notin P$ $x : f(x) = y$

$(X, y) \longrightarrow f(x) = y$ $P_1 \in NP$

DH KE & encryption



correctness:

$$m' = c \cdot K^{-1} = m \cdot K \cdot K^{-1} = m \bmod p$$

ElGamal Enc Scheme

A (m) — B

$K_D = K_B$ ←

KeyGen: $K_S \xleftarrow{r} \mathbb{Z}_p^*$

$K_P = g^{K_S} \bmod p$

Enc (m, K_P):

$x \xleftarrow{r} \mathbb{Z}_p^*$ — K_A ephemeral key

$C_1 = g^x \bmod p$

$C_2 = m \cdot K_P^x \bmod p$

(C_1, C_2) →

$(K_B)^x = K$

Dec (C, K_S):

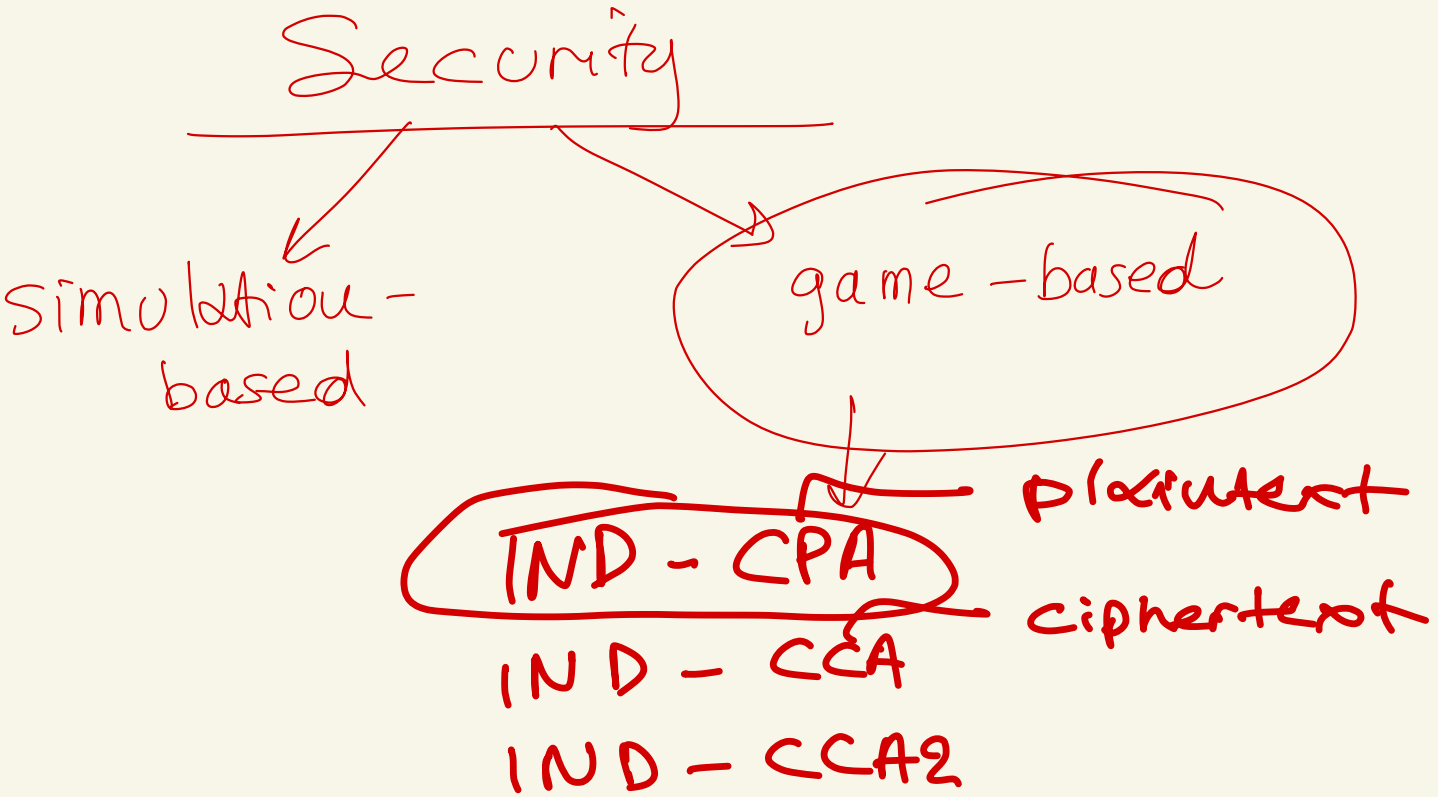
$m' = C_2 \cdot C_1^{-K_S} \bmod p$

Correctness:

$\text{Dec}(K_S, \text{Enc}(m, K_P)) = m$

$m' = C_2 \cdot C_1^{-K_S} = m \cdot K_P^x \cdot g^{-xK_S} =$

$= m \cdot g^{K_S \cdot x} \cdot g^{-xK_S} = m \quad (\bmod p)$


Security
simulation-based
game-based
IND-CPA
IND-CCA
IND-CCA2
plaintext
ciphertext

IND-CPA Game

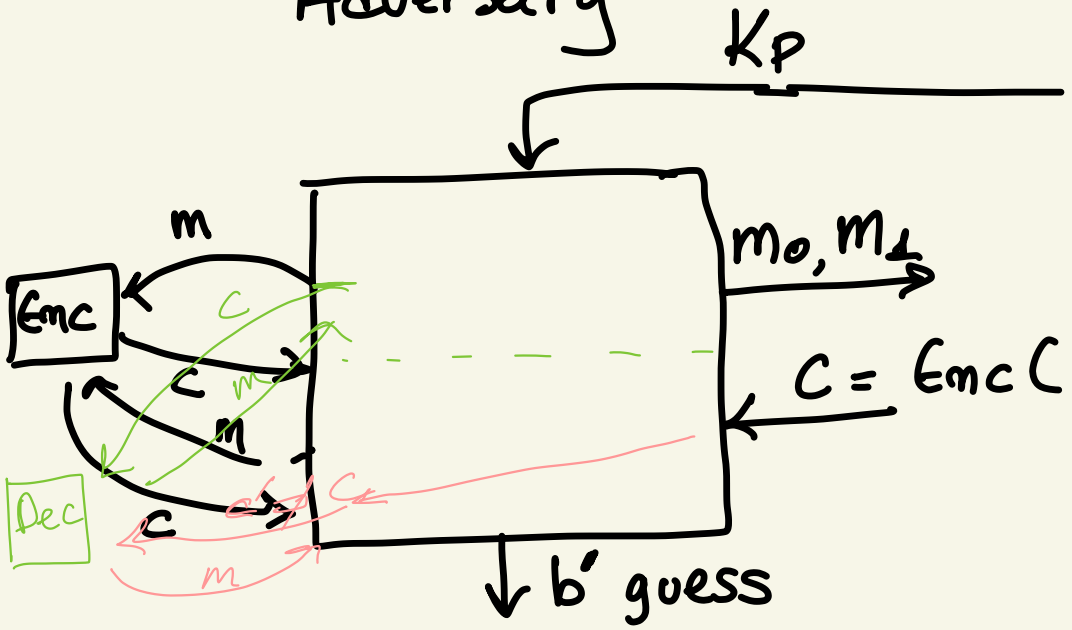
(PPT)

Adversary

CCA ciphertext

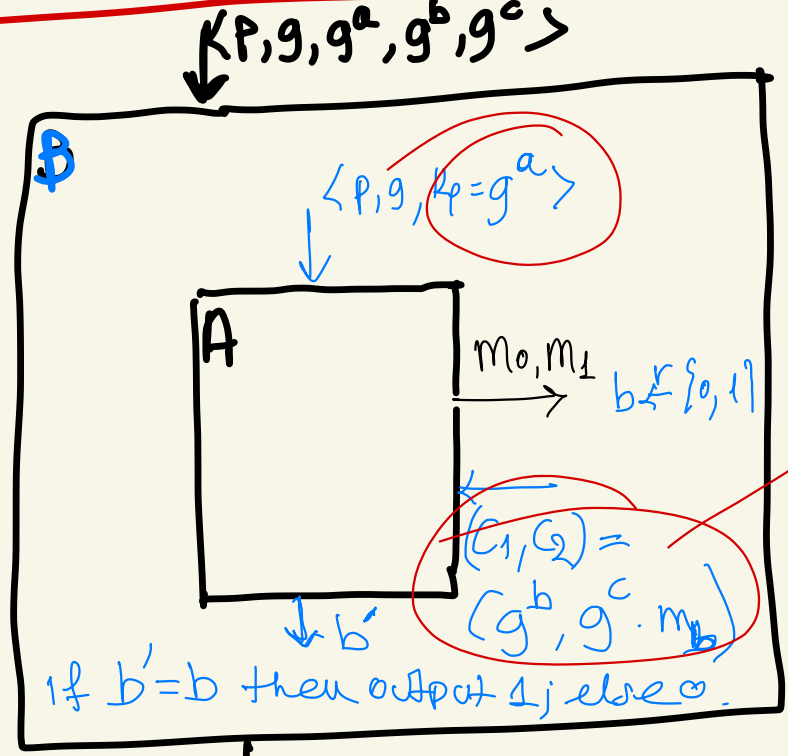
IND-CCA 2

Challenger



Wins IND-CPA: probability adversary wins $(b' = b)$ is $1/2 + \varepsilon(n)$ non-negligible

El Gamal Enc. Scheme is IND-CPA Secure under DDH.



$b' \in \{0,1\}$

$c \neq ab$ ↩ $c = ab$

If $c = ab$

$c_1 = g^b$

$c_2 = kp^b = (g^a)^b = g^{ab} = g^c \bmod p$

$b' = b$ $\quad 1/2 + \varepsilon(n)$ non-negl.

If $c \neq ab$: $1/2$

DDH: P, g, g^a, g^b, g^c, decide $c = ab$.

$$\left| \text{Prob}_{\tau \leftarrow g, P, g^a, g^b, g^{ab}}[A(\tau) = 1] - \text{Prob}_{\tau \leftarrow g, P, g^a, g^b, g^c}[A(\tau) = 1] \right| \leq \text{negl}$$

$1/2 + \varepsilon$ — PPT — $1/2$ $\geq$ non-negl

Reduction: A wins IND-CPA game with prob $1/2 + \varepsilon \geq$ non-negl.

$\Downarrow$

PPT B that violates

Homomorphic : $Enc(m) * Enc(m') = Enc(m * m')$

El Gamal is Homomorphic :

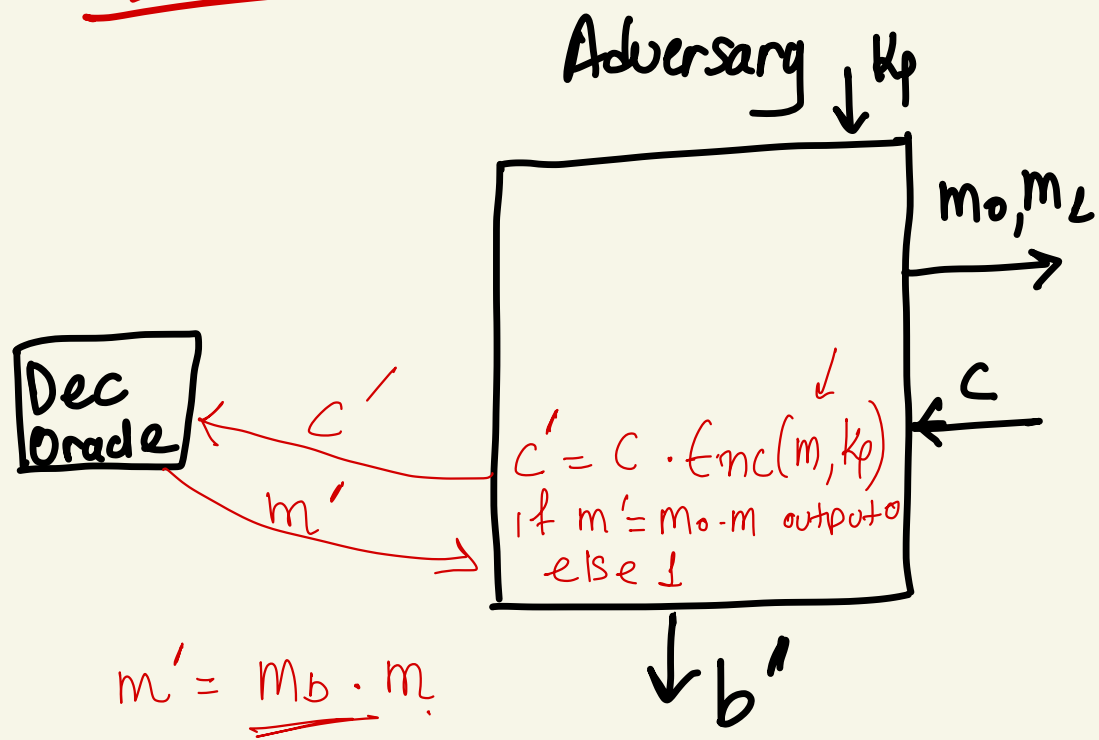
$$Enc(k_p, m) = (c_1, c_2) = (g^x, k_p^x \cdot m)$$

$$Enc(k_p, m') = (c_1', c_2') = (g^{x'}, k_p^{x'} \cdot m')$$

$$Enc(k_p, m) \cdot Enc(k_p, m') = (c_1 \cdot c_1', c_2 \cdot c_2') =$$

$$= (g^{\underbrace{x+x'}_{y}}, k_p^{\underbrace{x+x'}_{y}} \cdot m \cdot m') = Enc(m \cdot m', k_p)$$

Any homorphic Enc. Scheme is NOT IND-CCA2 secure



malleability: $c = Enc(m, k_p)$ ↝ f known

$c' \rightarrow m' = f(m)$