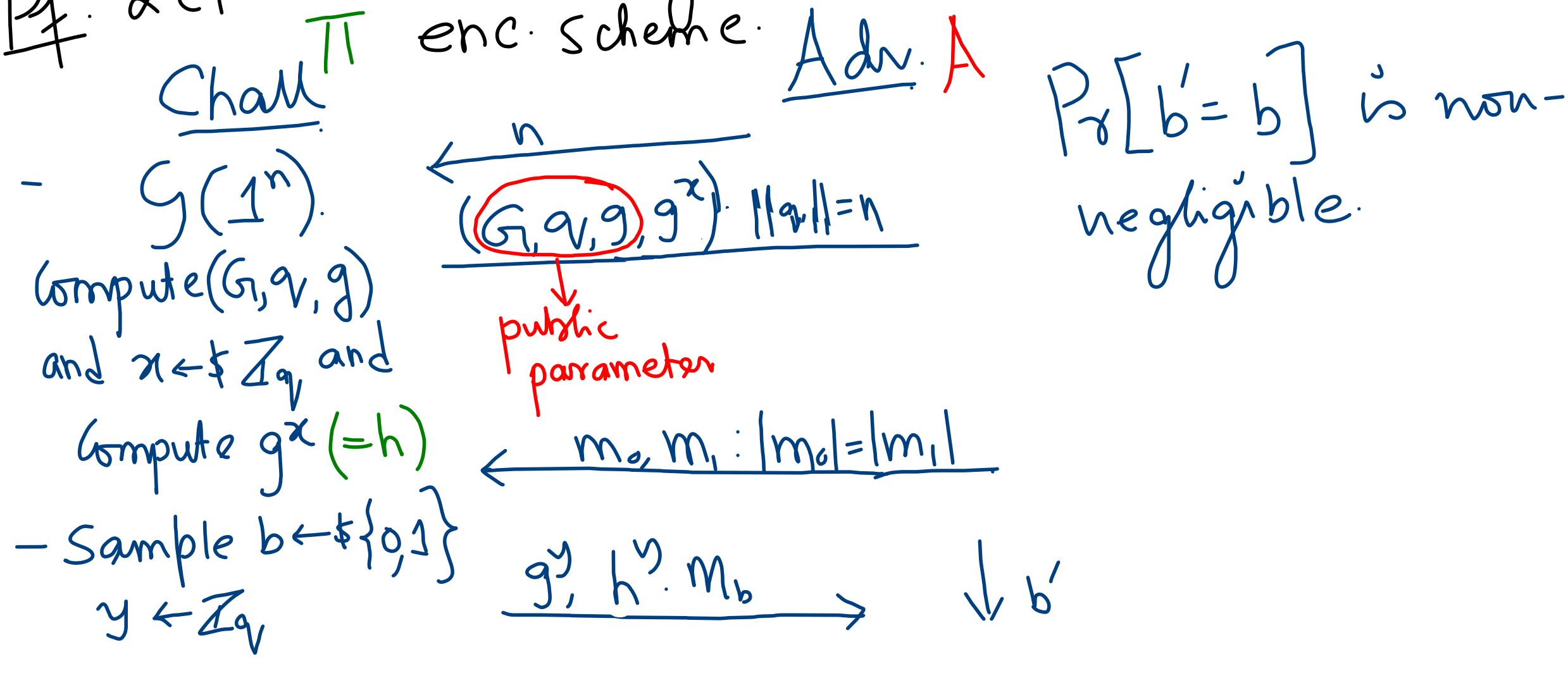
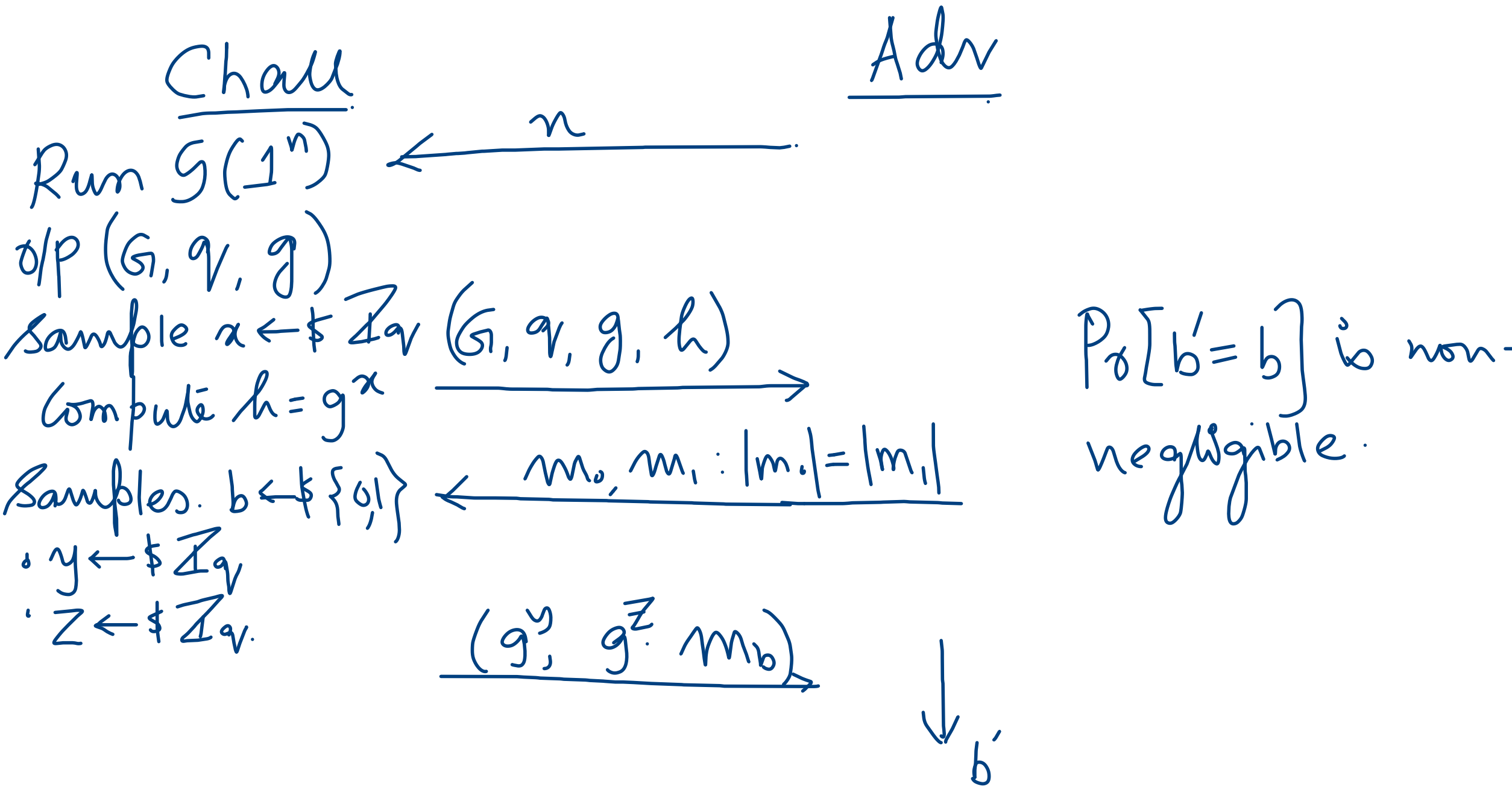
Thm: If DDH assumption is hard over a finite cyclic group, then El-gamal encryption scheme is CPA-secure

Pf: Let Π be the El-gamal enc. scheme.



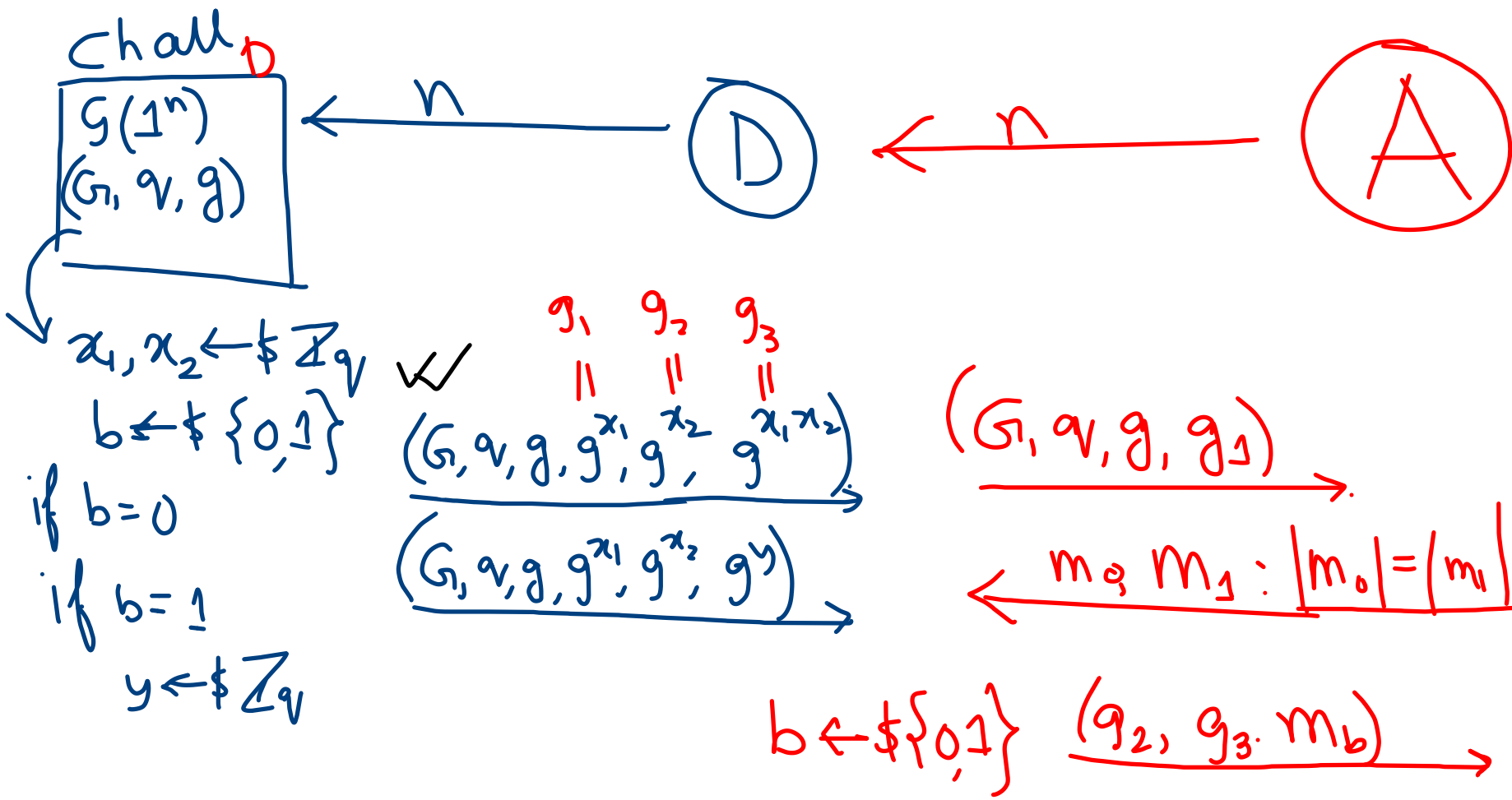
$Pr[b'=b]$ is non-negligible.

Let $\tilde{\Pi}$ be a slight variant of Π, defined as follows:



Distinguisher D for breaking DDH assumption.

D will be given (G, q, g, g_1, g_2, g_3), when D pings it's own challenger with i/p n.



- D will run A with $pk = (G, q, g, g_1)$.
- A will submit two msg. $m_0, m_1 : |m_0| = |m_1|$
- D will sample a bit $b \leftarrow \$ \{0, 1\}$.

  it sends $(c_1 = g_2, c_2 = g_3 \cdot m_b)$ as a ciphertext to A
- A will output b'
- D will output 1 if $b = b'$

Observation: D has received the tuple $\tau = (G, q, g, g_1, g_2, g_3)$

- $g_1 = g^{x_1}$, $g_2 = g^{x_2}$ $g_3 = g^{x_1 x_2} / g^y$

Case 1:

If $\mathcal{D}$ receives the tuple $x = (G, q, g, g_1, g_2, g_3)$.
where $g_1 = g^{x_1}$, $g_2 = g^{x_2}$, $g_3 = g^{x_1 x_2}$ for $x_1, x_2 \leftarrow\$ \mathbb{Z}_q$.

Case 2:

If $\mathcal{D}$ receives the tuple $x = (G, q, g, g_1, g_2, g_3)$
where $g_1 = g^{x_1}$, $g_2 = g^{x_2}$, $g_3 = g^{y}$ for some $y \leftarrow\$ \mathbb{Z}_q$.

For case 1: A interacts with Chall_Π

For case 2: A interacts with $\text{Chall}_{\tilde{\Pi}}$.

Note that, the winning prob. of adv. A. when interacting with the challenger of $\tilde{\pi}$ is exactly $1/2$.

$$Pr\left[PubK^{eav}_{\tilde{\pi}}(A) = 1\right] = \frac{1}{2}.$$

$$Adv^{ind}_{DDH}(D) = \left| Pr\left[D(G, q, g, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1\right] - Pr\left[D(G, q, g, g^{x_1}, g^{x_2}, g^{y}) = 1\right] \right| \quad \text{— (1)}$$

$$Pr\left[D(G, q, g, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1\right] = Pr\left[PubK^{eav}_{\pi}(A) = 1\right] \quad \text{— (2)}$$

$$Pr\left[D(G, q, g, g^{x_1}, g^{x_2}, g^{y}) = 1\right] = Pr\left[PubK^{eav}_{\tilde{\pi}}(A) = 1\right] = \frac{1}{2} \quad \text{— (3)}$$

We have assumed that A breaks the CPA security of El-Gamal encryption scheme.

$$P\left[Pubk^{eav}_{\Pi}(A) = 1\right] > \frac{1}{2} + \varepsilon(n)$$, where $\varepsilon(n)$ is a non-negligible fn — (4)

From (1), (2), (3), (4)

$$Adv^{ind}_{DDH}(D) > \varepsilon(n)$$., which is non-negligible fn

Chosen Ciphertext Security:

- Adversary pings the oracle with a natural number n
- On i/p 1^n, $KGEN(1^n)$ will yield a (pk, sk) pair.
- Reveal the pk to the adversary A.
- A is also given the access to the decryption oracle $Dec_{SK}(\cdot)$.
- A will submit two messages m_0, m_1 and will be given $Enc_{pk}(m_b)$ for $b \in \{0,1\}$, denoted as $c^* = Enc_{pk}(m_b)$.
- A can also query to the decryption oracle, but cannot

query with c^*

- A will output b'

Adversary A wins the IND-CCA game if $b = b'$

Advantage of winning the IND-CCA game for a PKE scheme Π with respect to some PPT adversary A is

$$Adv_{\Pi}^{ind\text{-}cca}(A) = P[b' = b]$$

- **Textbook RSA is not CCA-secure:**

Suppose you receive $c = m^e \bmod n$.

Convert c to c' by $c' = 2^e c \bmod n$

$= 2^e \cdot m^e \bmod n$

$= (2m)^e \bmod n$

- **El-Gamal is not CCA secure.**

c_1 c_2

Suppose you receive a message $c = (g^y, h^y \cdot m)$

$c_2' = c_2 \cdot \hat{m}$ → upon decryption receiver will get $m \cdot \hat{m}$.

$\hat{c} = (c_1, c_2')$

Adversary does the following.

$c = (c_1, c_2)$, $c_1 = g^y$, $c_2 = h^y \cdot m$

- A will sample $y' \leftarrow \$ \mathbb{Z}_q$

$c_1' = (c_1)^{y'} = g^{y \cdot y'} \rightarrow g^{xy \cdot y'}$

$c_2' = (c_2)^{y'} = (h^y \cdot m)^{y'} = h^{y \cdot y'} \cdot m^{y'}$

A will send $c' = (c_1', c_2')$

A will receiver $m^{y'}$

A can recover m. by computing $(m^{y'})^{(y')^{-1}}$

$f \cdot m$

$c_1' = g^{y'} \cdot c_1 = g^{y'+y}$

$c_2' = c_2 \cdot h^{y'} \cdot \alpha$

$= h^{y+y'} \cdot m\alpha$

$c' = (c_1', c_2')$.

$c_2' ((c_1')^x)^{-1}$

$= m\alpha$.