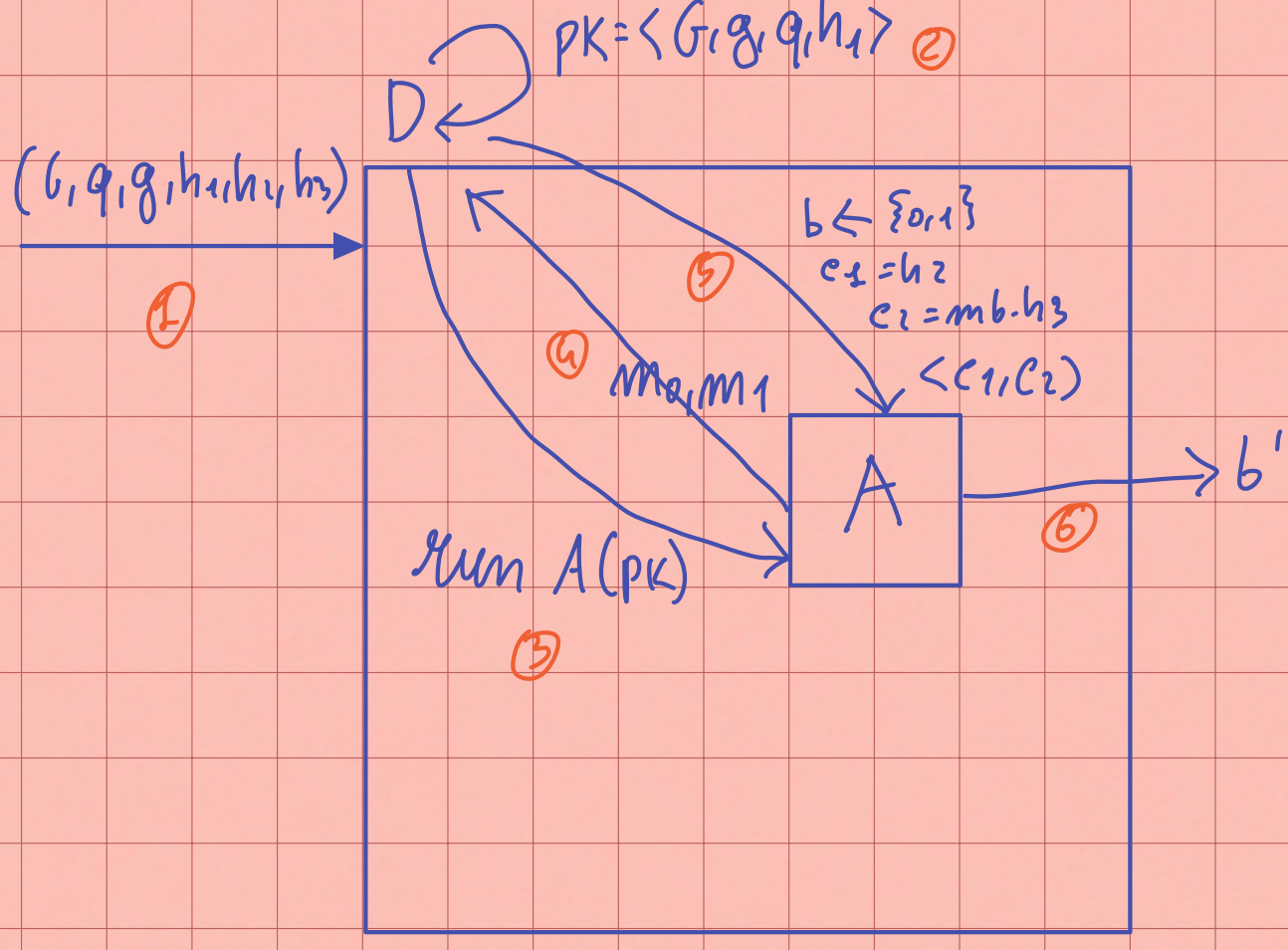
Teorema: Se DDH è difficile allora lo schema di cifratura a chiave pubblica basato su El Gamal è CPA sicuro

Esibisco una riduzione:
- D è un distinguisher che vuole risolvere il problema DDH
- A vuole rompere Π El Gamal.

Per dimostrare che Π è sicuro devo dimostrare che

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



- $\langle c_1, c_2 \rangle$ è come se fossero pk, c dell'esperimento $PubK^{eav}_{A,\Pi}(n)$, quindi A pensa di giocare in questo esperimento.
- Adesso si possono verificare due casi perché il challenger nel problema DDH poteva calcolare h_3 in due modi possibili, in base all'esito del lancio di una moneta.

Sia $\tilde{\Pi}$ tale che:

$c = \langle g^y, g^z \cdot m \rangle$

$pk = (G, g, q, h)$ e

$P_r[PubK^{eav}_{A,\tilde{\Pi}}(n) = 1] = \frac{1}{2}$

CASO 1:

$h_1 = g^x \quad h_2 = g^y \quad h_3 = g^z$

A riceve $\langle c_1, c_2 \rangle$ dove $c_1 = h_2$ e $c_2 = h_2 \cdot m$
quindi $\langle g^y, g^z \cdot m \rangle$ questa però è proprio la forma del cifrato in $\tilde{\Pi}$ quindi:

$$Pr[D(G, g, q, h_1, h_2, h_3) = 1] = Pr[D(G, g, q, g^x, g^y, g^z) = 1]$$

$$Pr[PubK^{eav}_{A,\tilde{\Pi}}(n) = 1] \leq \frac{1}{2}$$

CASO 2:

$h_1 = g^x \quad h_2 = g^y \quad h_3 = g^{xy}$

A riceve $\langle c_1, c_2 \rangle = \langle h_2, h_3 \cdot m \rangle = \langle g^y, g^{xy} \cdot m \rangle$
da cui
$Pr[D(G, g, q, h_1, h_2, h_3) = 1] = Pr[D(G, g, q, g^x, g^y, g^{xy}) = 1] =$

$$Pr[PubK^{eav}_{A,\Pi}(n) = 1]$$

Se DDH difficile sappiamo che:

$$|Pr[D(G,g,q,g^x,g^y,g^z)=1] - Pr[D(G,g,q,g^x,g^y,g^{xy}]| \leq negl(n)$$

per le uguaglianze

$$|Pr[PubK^{eav}_{A,\tilde{\Pi}}(n)=1] - Pr[PubK^{eav}_{A,\Pi}(n)=1]| \leq negl(n)$$

$\downarrow$

$\frac{1}{2}$

quindi:

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