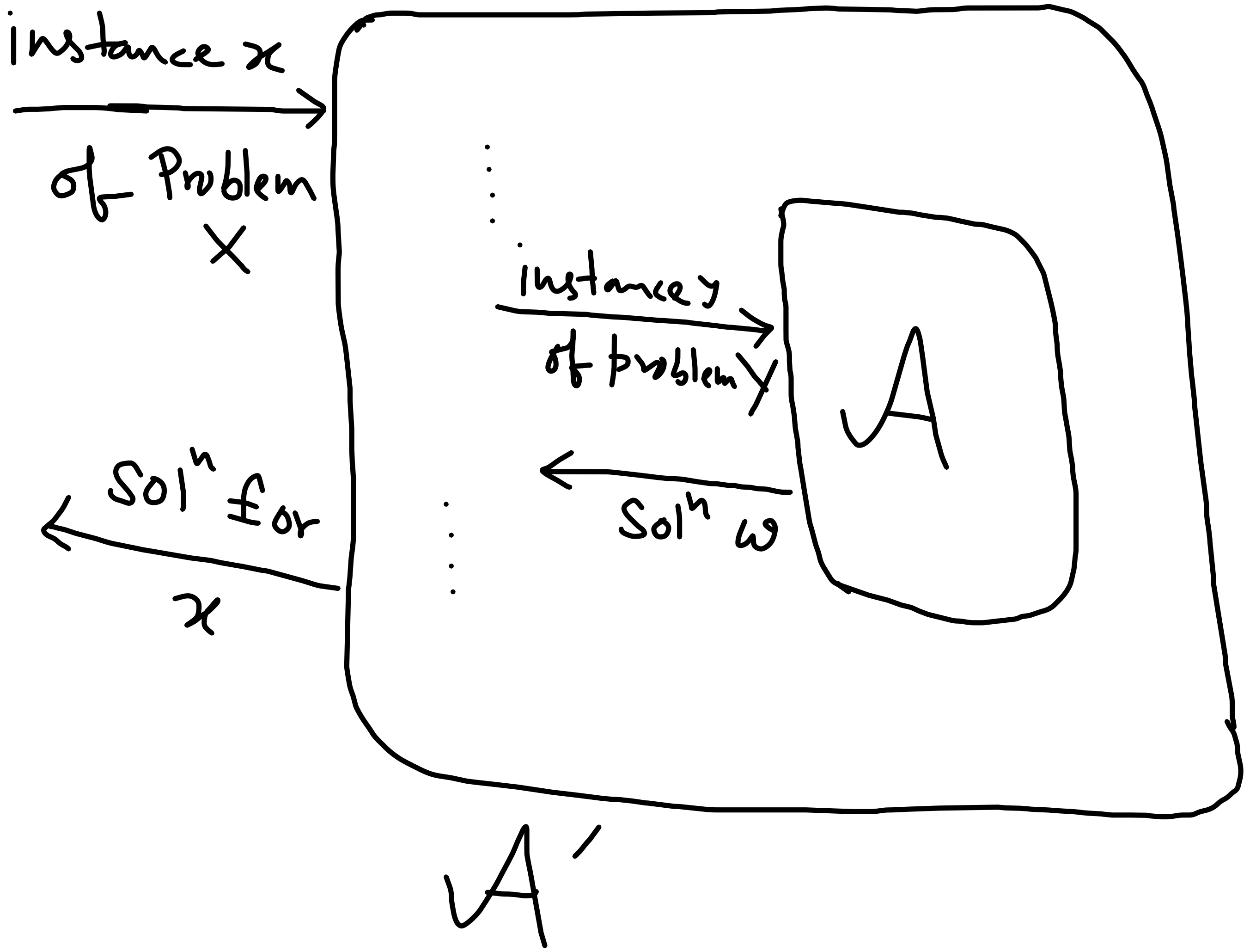
Proof by Reduction

Assumption: Solving Problem X is difficult

Proof by Reduction: Problem Y is difficult to solve (under the above assumption)



- Assume A solves problem Y efficiently.
- Our goal is to construct A′ that solves problem X.

- Assume A wins with prob $\epsilon(n)$.
- If A provides correct result, then A′ wins with prob $\frac{1}{p(n)}$.
- A′ solves the prob with prob $\geq \frac{\epsilon(n)}{p(n)}$.

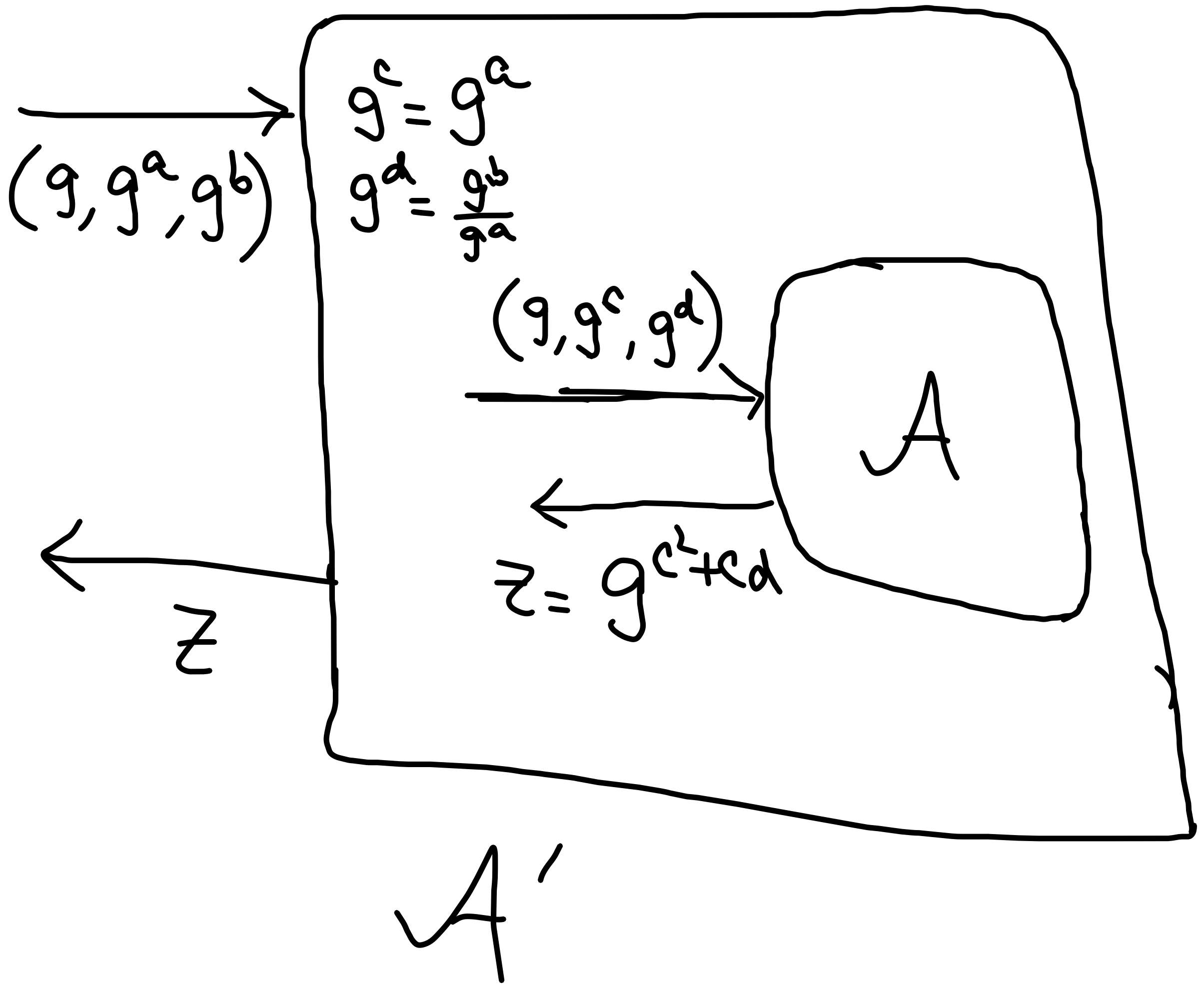
Problem X

CDH: cyclic group G. Choose $g \xleftarrow{\$} G$, $a, b \xleftarrow{\$} \mathbb{Z}$

Given (g, g^a, g^b), it is difficult to find g^{ab}. $\Rightarrow \Pr[A' \text{ wins}] = \text{negl}(n)$

Problem Y: cyclic group G. Choose $g \xleftarrow{\$} G$, $c, d \xleftarrow{\$} \mathbb{Z}$

Given (g, g^c, g^d), it is difficult to find g^{c^2+cd}



- Assume $\mathcal{A}$ solves Y.
- Now we have to construct $\mathcal{A}'$.
- $\Pr[\mathcal{A}' \text{ wins}] \geq \Pr[\mathcal{A} \text{ wins}]$
- $\Pr[\mathcal{A} \text{ wins}] \leq \text{negl}(n)$

Problem X

CDH: cyclic group G. Choose $g \xleftarrow{\$} G$, $a, b \xleftarrow{\$} \mathbb{Z}$ $\Rightarrow$ negl(n)

Given (g, g^a, g^b), it is difficult to find g^{ab}.

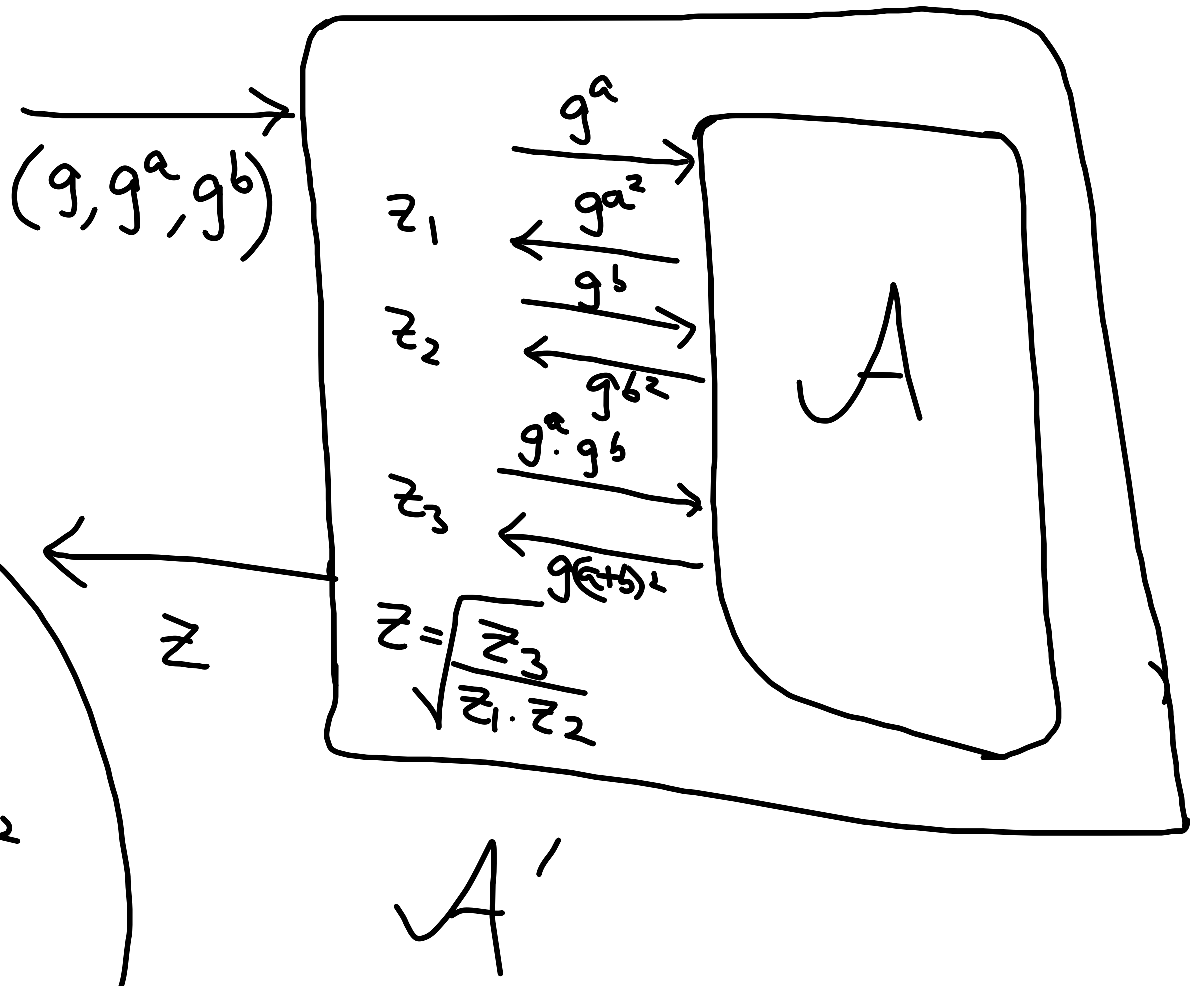
SDH: cyclic group G. Choose $g \xleftarrow{\$} G$, $c \xleftarrow{\$} \mathbb{Z}$

Given (g, g^c), it is difficult to find g^{c^2}

$\boxed{\Pr[\mathcal{A} \text{ wins}] = \epsilon}$

$$\frac{g^{(a+b)^2}}{g^{(a-b)^2}}$$

$$\frac{g^{(a+b)^2}}{g^{a^2} \cdot g^{b^2}} = g^{2ab}$$



- Assume $\mathcal{A}$ solves Y.
- Now we have to construct $\mathcal{A}'$.
- $\Pr[\mathcal{A}' \text{ wins}] \geq \epsilon^3$

① Let (Gen, Enc, Dec) → fixed length preserving $\xrightarrow{} (\ell)$ encryption. in presence of an eavesdropper.

If Π is secure under EAV-indistinguishability then for any i, for PPT Adversary $\mathcal{A}'$,

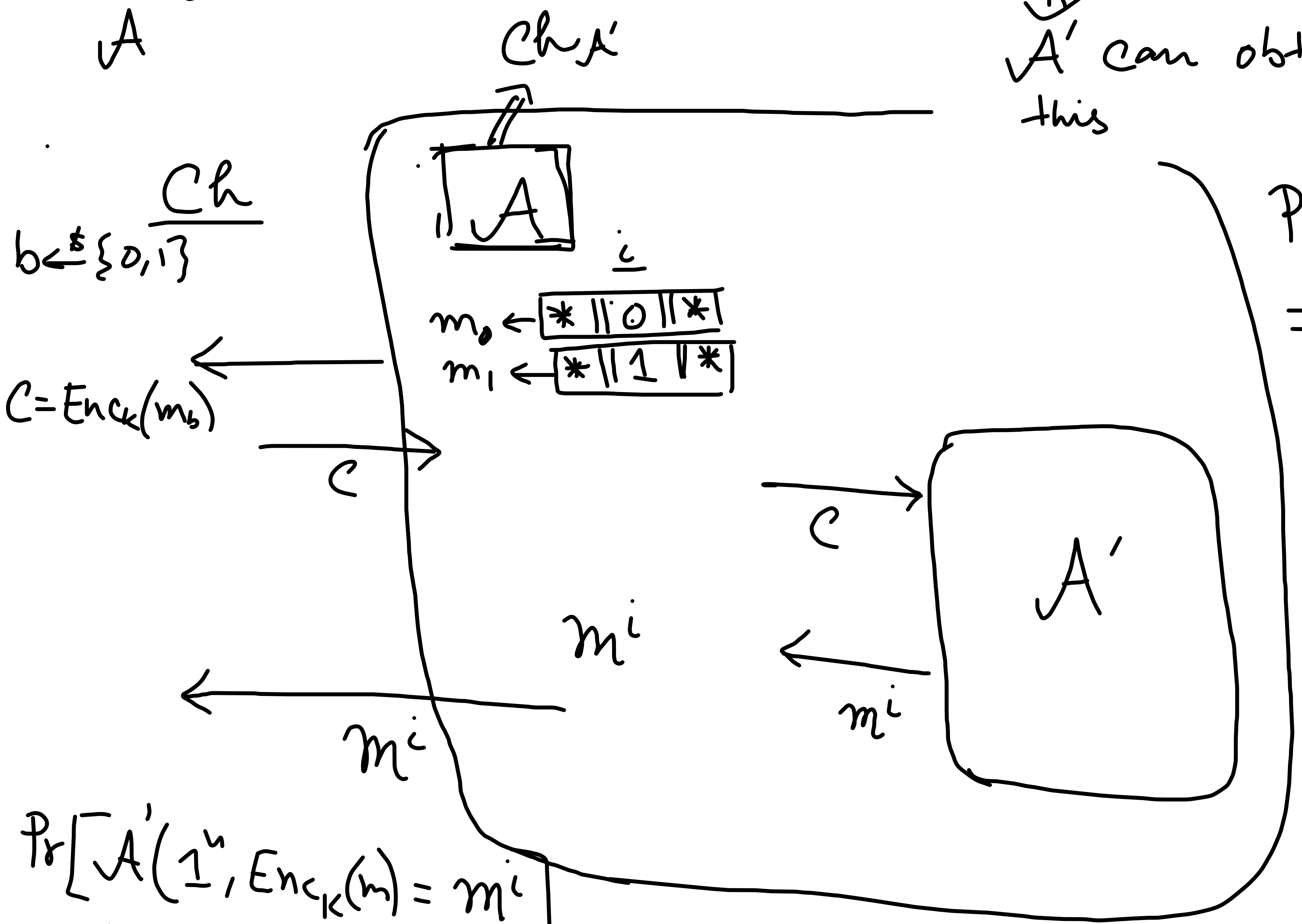
$$\Rightarrow \quad \Pr\left[\mathcal{A}'(1^n, Enc(m)) = m^i\right] \leq \frac{1}{2} + negl(n)$$

EAV-Indist

Ch		A
$k \leftarrow Gen(1^n)$		
$b \xleftarrow{\$} \{0,1\}$		
$c \leftarrow Enc_k(m_b)$	$\xleftarrow{m_0, m_1}$	
	$\xrightarrow{c}$	
	$\xleftarrow{\hat{b}}$	

$$\Pr\left[PrivK^{EAV}_{\Pi,\mathcal{A}}(n) = 1\right] = \Pr\left[\hat{b} = b\right] \leq \frac{1}{2} + negl(n)$$

Π is EAV-Indist $\Rightarrow$ given i, $\Pr\left[\mathcal{A}'(1^n, Enc_k(m)) = m^i\right] \leq \frac{1}{2} + negl(n)$



$\mathcal{A}'$ can obtain this

$$\Pr[\mathcal{A} \text{ wins}] = \Pr\left[\mathcal{A}'(1^n, Enc_k(m_b)) = b\right]$$

$$\Pr\left[\mathcal{A}'(1^n, Enc_k(m)) = m^i\right] = \frac{1}{2}\Pr\left[\mathcal{A}'(1^n, Enc_k(m_0)) = 0\right] + \frac{1}{2}\Pr\left[\mathcal{A}'(1^n, Enc(m_1)) = 1\right]$$