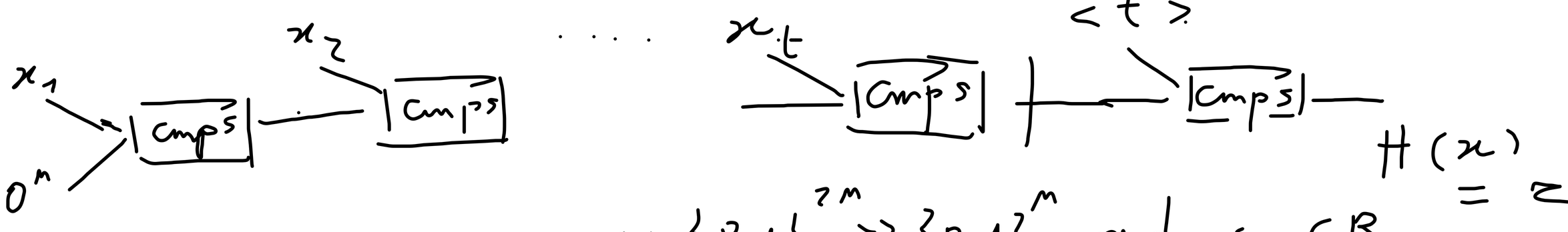
EXERCISES

*) Consider TAG $H(k \| m) = Tag(k, m)$

where H is a CRH using MERKLE–DAMGAARD.

Show that TAG NOT UF-CMA.



Here: $x = k \| m$.

cmps: $\{0,1\}^{2n} \to \{0,1\}^n$ and is CR.

A gets τ on msg $m \in \{0,1\}^*$

$m^* = m \| 1 \| <t> \| 1$ $\quad \tau^* = cmps(\tau \| <t+1>)$

$= \tau^*$

Alternatively, $m^* = m \| \langle t \rangle \| m' \quad m \in \{0,1\}^n$

$$\tau^* = cmps\left(\langle t+1 \rangle, cmps(\tau \| m')\right)$$

Fix: hash twice. HMAC STANDARD.

Observation: The above is SECURE in the ROM!

*) Let G be a group with generator g and order q.

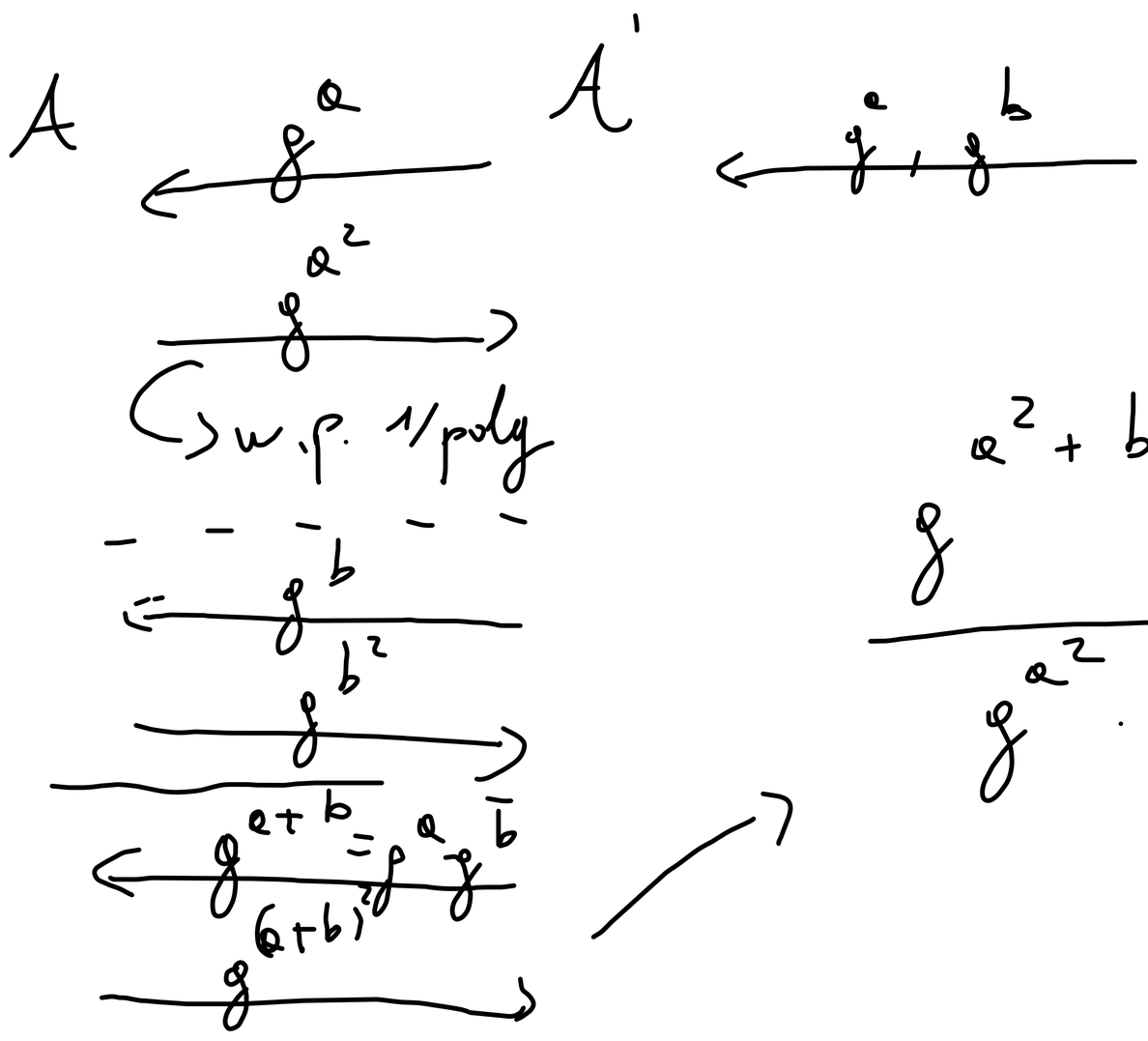
Prove CDH is equivalent to:

- SQUARE DH: Given (g, g^a, g^b) for $a \leftarrow \mathbb{Z}_q$

  Compute $g^{(a^2)}$. Assume square root efficiently computable in G.

CDH => SQUARE DH Assume PPT $\mathcal{A}$

solving SQUARE DH w.p. 1/poly. Build $\mathcal{A}'$

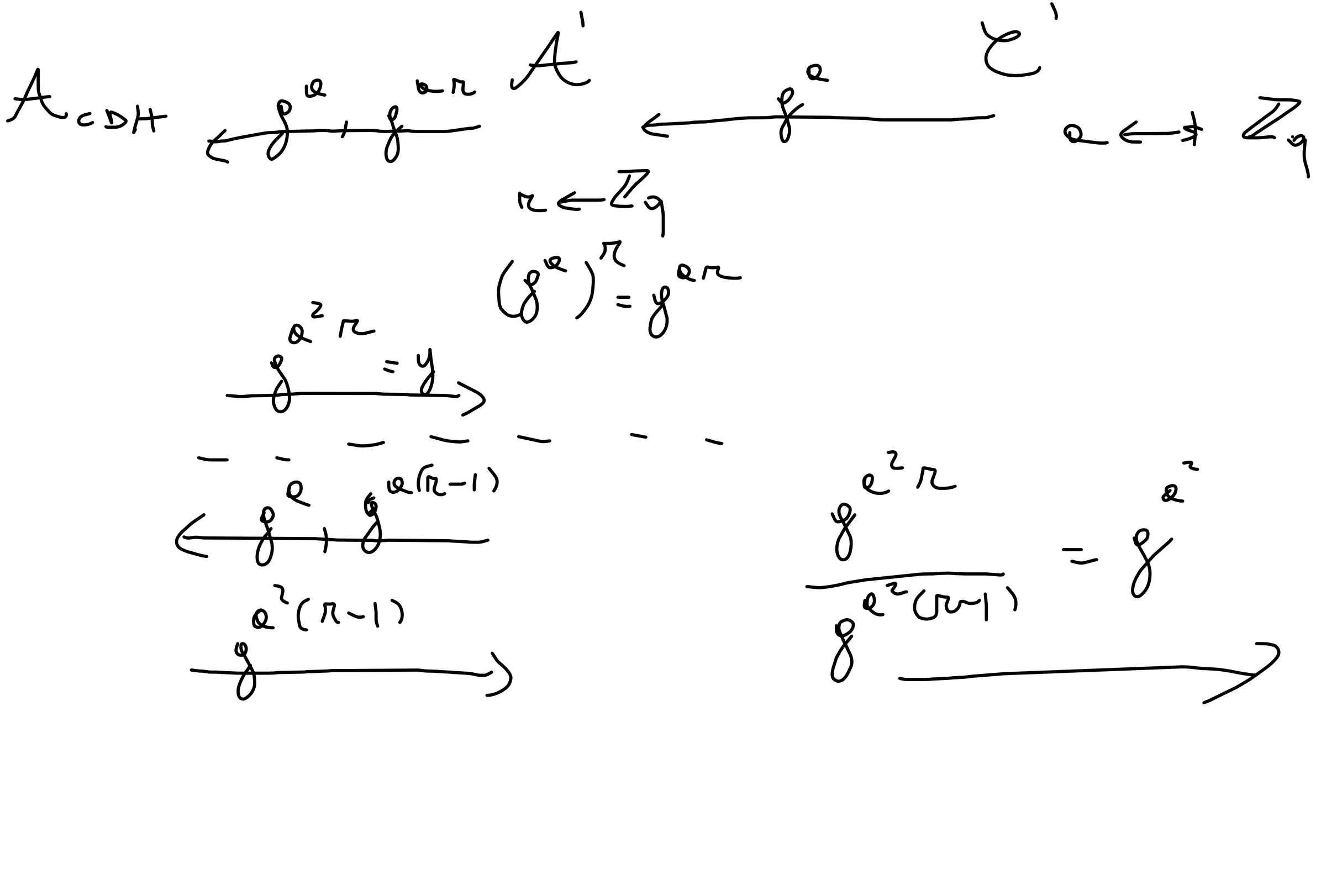


$$a^2 + b^2 + 2ab$$

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

↪ Take $\sqrt{(\cdot)}$ in $\mathbb{G}$.

SQUARE-DH ⇒ CDH



*). Show how to get multi-bit CPA PKE from single-bit CPA PKE.

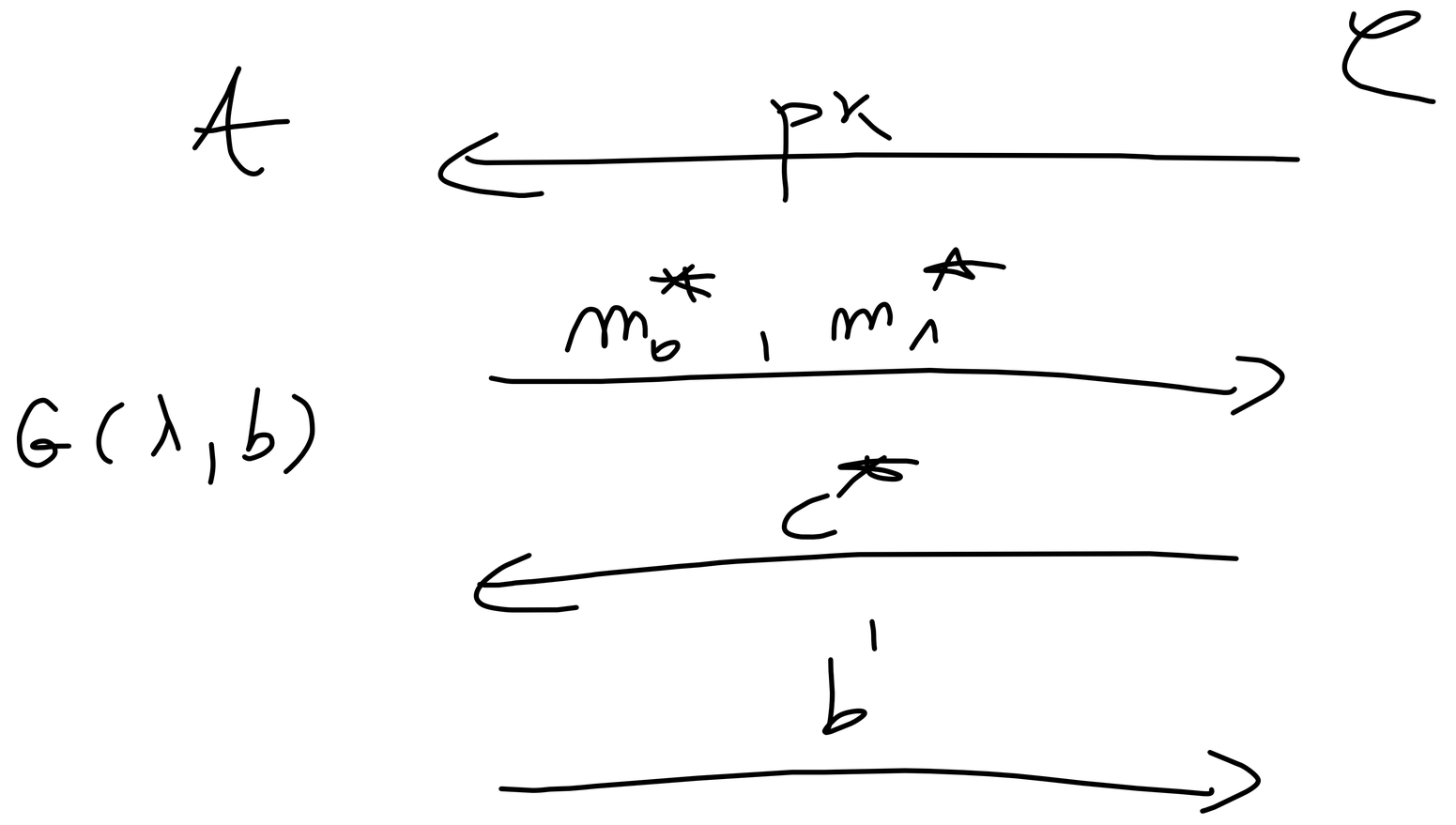
Let $\Pi = (Kgen, Enc, Dec)$ be for $\mathcal{M} = \{0,1\}$.

Construct Π' for $\mathcal{M} = \{0,1\}^l$ and $l = poly(\lambda)$.

Let $Kgen(1^\lambda) = (pk, sk)$

$$Enc'(pk, m = m_1, \cdots, m_l) = Enc(pk, m_1), \cdots, Enc(pk, m_l)$$

Prove: CPA secure. Hybrid argument.



$H(\lambda)$: $c^* = Enc(pk, b_1), \dots, Enc(pk, b_\ell)$

$b_1, \dots, b_\ell \leftarrow \{0,1\}$.

Need to prove: $G(\lambda, b) \approx_c H(\lambda) \quad \forall b \in \{0,1\}$.

Alternative: Directly define

$H_i(\lambda)$: $c^* = \Big(Enc(pk, m^*_{0,1}), \dots, Enc(pk, m^*_{0,i}),$

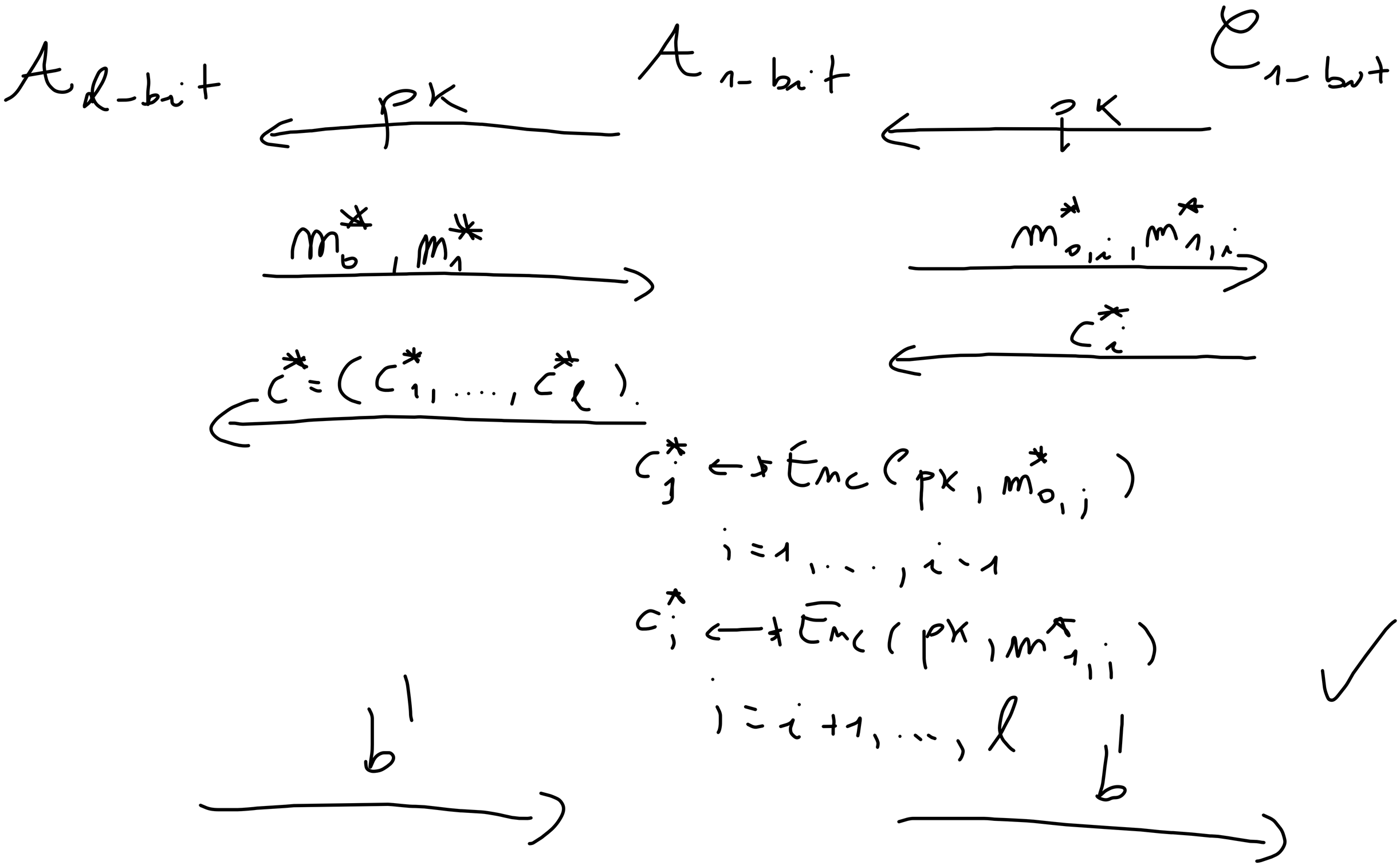
$Enc(pk, m^*_{1,i+1}, \dots, Enc(pk, m^*_{1,l}) \Big)$

$H_0(\lambda) \equiv G(\lambda, 1)$; $H_l(\lambda) \equiv G(\lambda, 0)$

$\forall i$: $H_i(\lambda) \approx_c H_{i+1}(\lambda)$.

Let A l-bit be distinguisher from H_i and H_{i+1}.

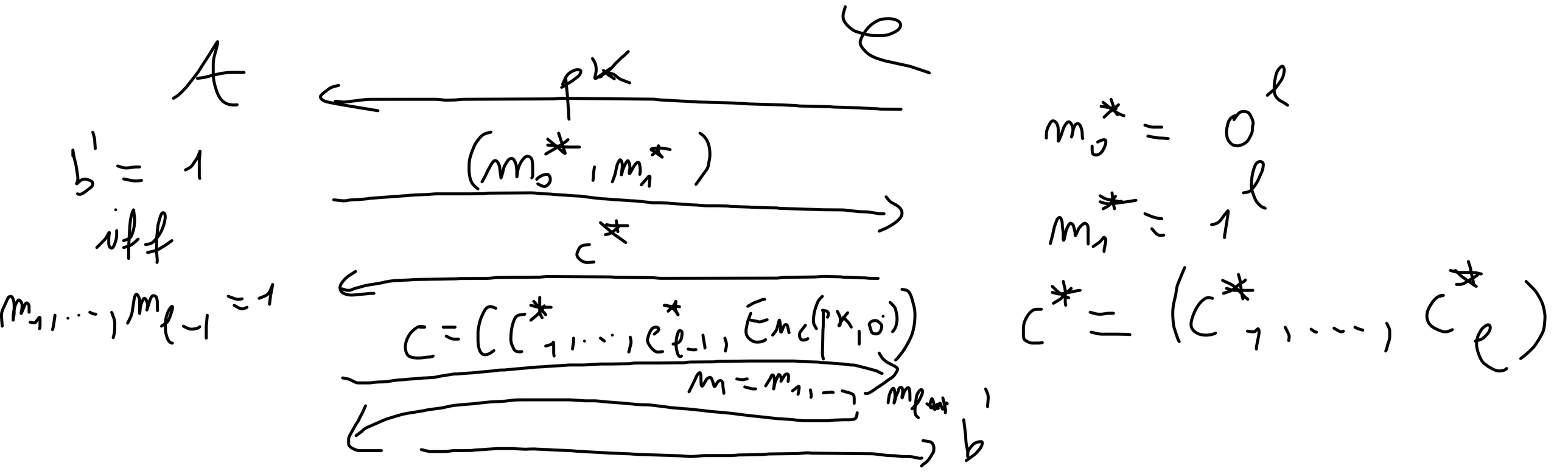
The reduction:



*) Show previous construction not CCA secure.

$$Enc'(pk, m) = \big(Enc(pk, m_1), \ldots, Enc(pk, m_\ell)\big)$$

$Enc \equiv$ single-bit CCA.



*) Combiners for PKE:

$\Pi_1 = (KGen_1, Enc_1, Dec_1)$ — $\mathcal{M}$ = "$\mathcal{M}_1$" = $\mathcal{M}_1$, $\mathcal{C}_1$

$\Pi_2 = (KGen_2, Enc_2, Dec_2)$ — $\mathcal{M}_2, \mathcal{C}_2$

Either Π_1 or Π_2 is CPA, but don't know which.

Make CPA secure Π^* using Π_1, Π_2.

An idea that always works: 2-OUT-OF-2 SECRET SHARING

m

$m_1 = m \oplus r$ $\quad$ $r = m_2$ $\quad$ $r \leftarrow \mathcal{M}$.

$$p(X) = a_t X^t + a_{t-1} X^{t-1} + \cdots + a_1 X + a_0 \pmod p$$

$$a_0 = s = p(0)$$

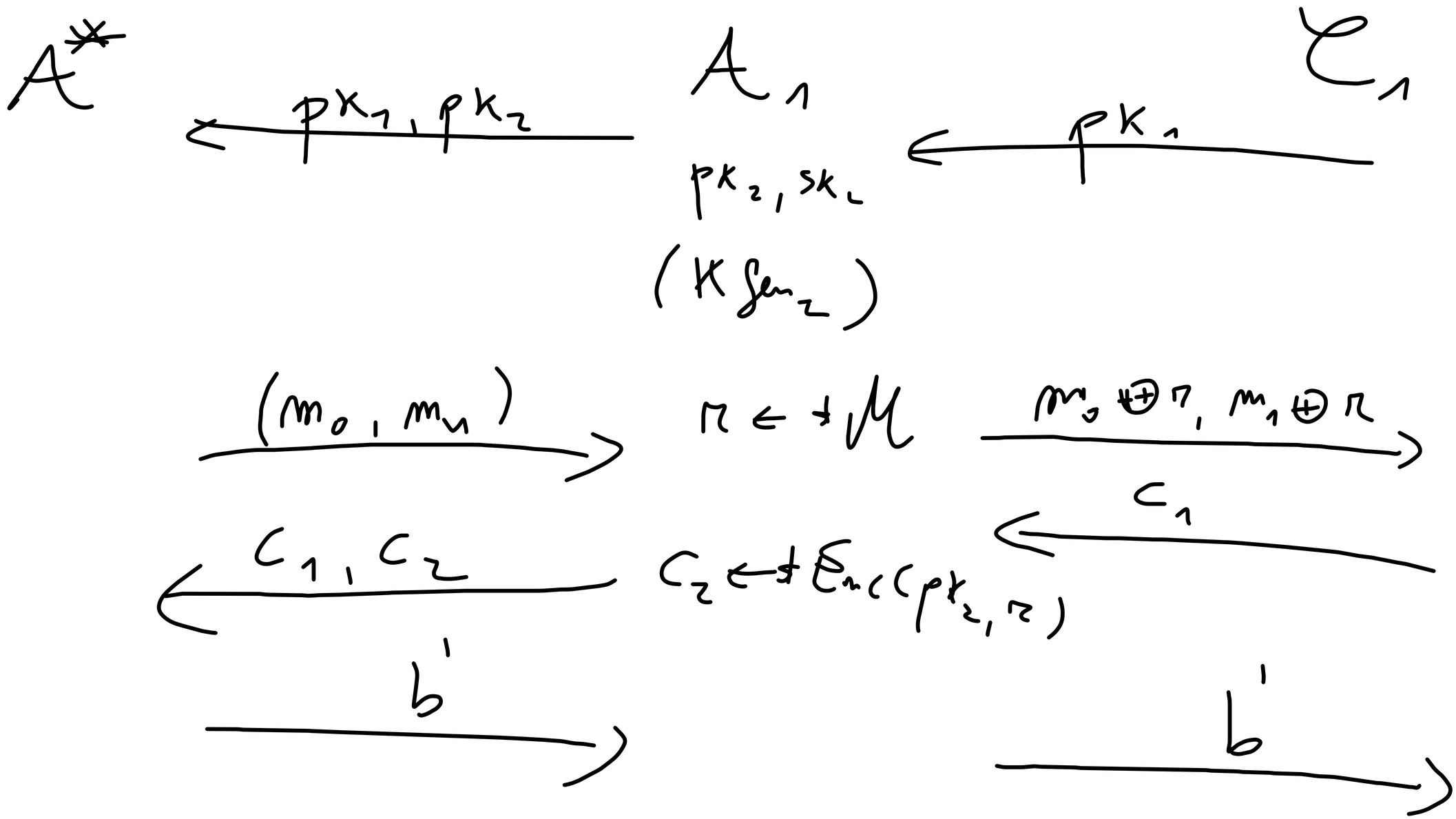
$$p(3) = a_3 3^t + a \cdots + a_0$$

p = 1-bit prime

$$pk^* = (pk_1, pk_2)$$

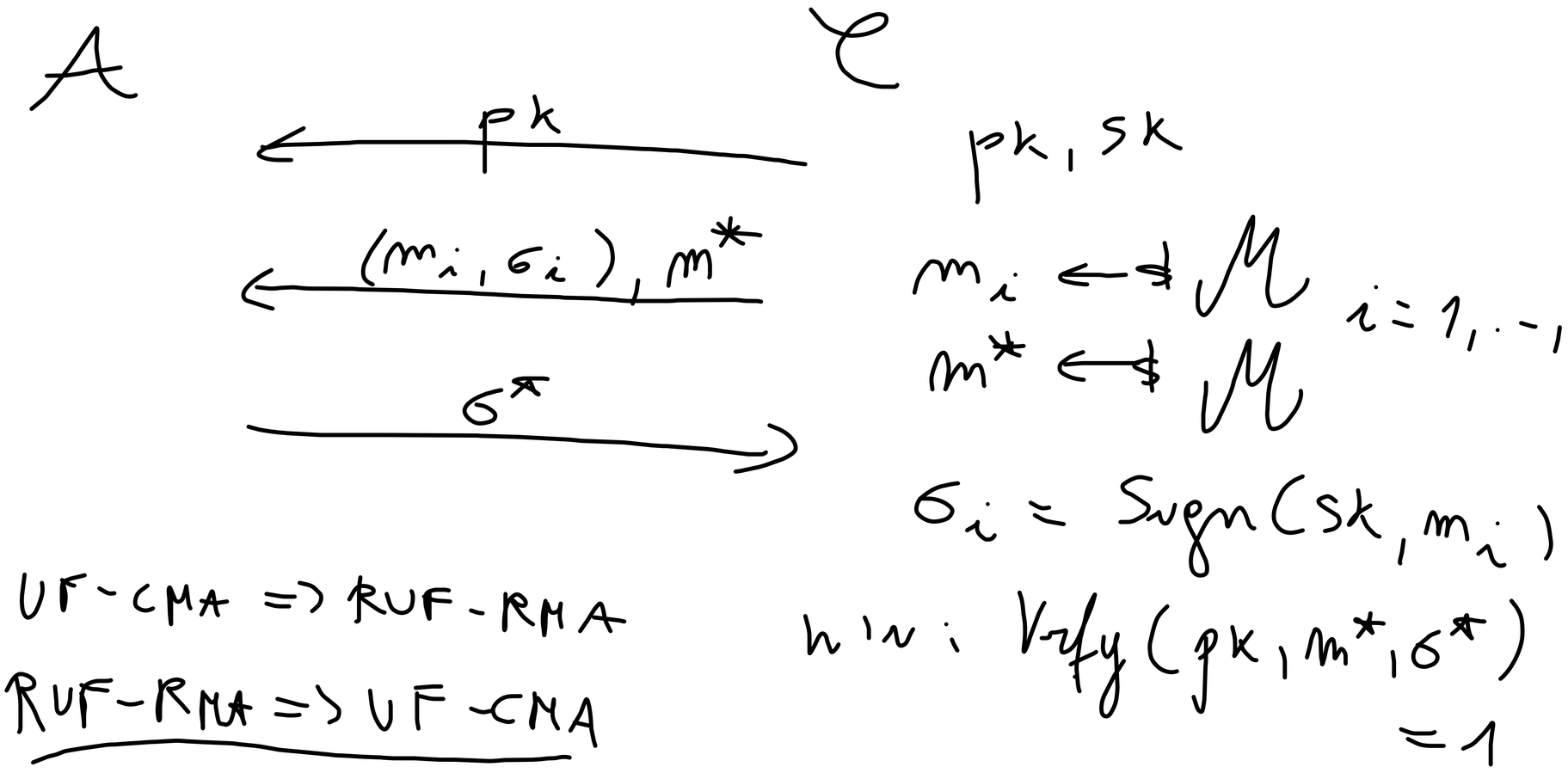
$$Enc^*(pk^*, m) = \left(Enc_1(pk_1, m \oplus r),\ ;\ r \leftarrow \mathcal{U}_{\mathbb{Z}} \right) \left(Enc_2(pk_2, r) \right) = (c_1, c_2)$$

Reduction. Assume Π_1 CPA secure.



*) Define notions of UF-CMA.

- RUF-RMA



Prove/disprove: UF-CMA ⇒ RUF-RMA

RUF-RMA ⇒ UF-CMA

UF-CMA $\Rightarrow$ RUF-RMA. TRIVIAL. By reduction.

RUF-RMA $\not\Rightarrow$ UF-CMA.

Start with $\Pi = (Kgen, Sign, Vrfy)$

UF-CMA. Make $\overline{\Pi}$

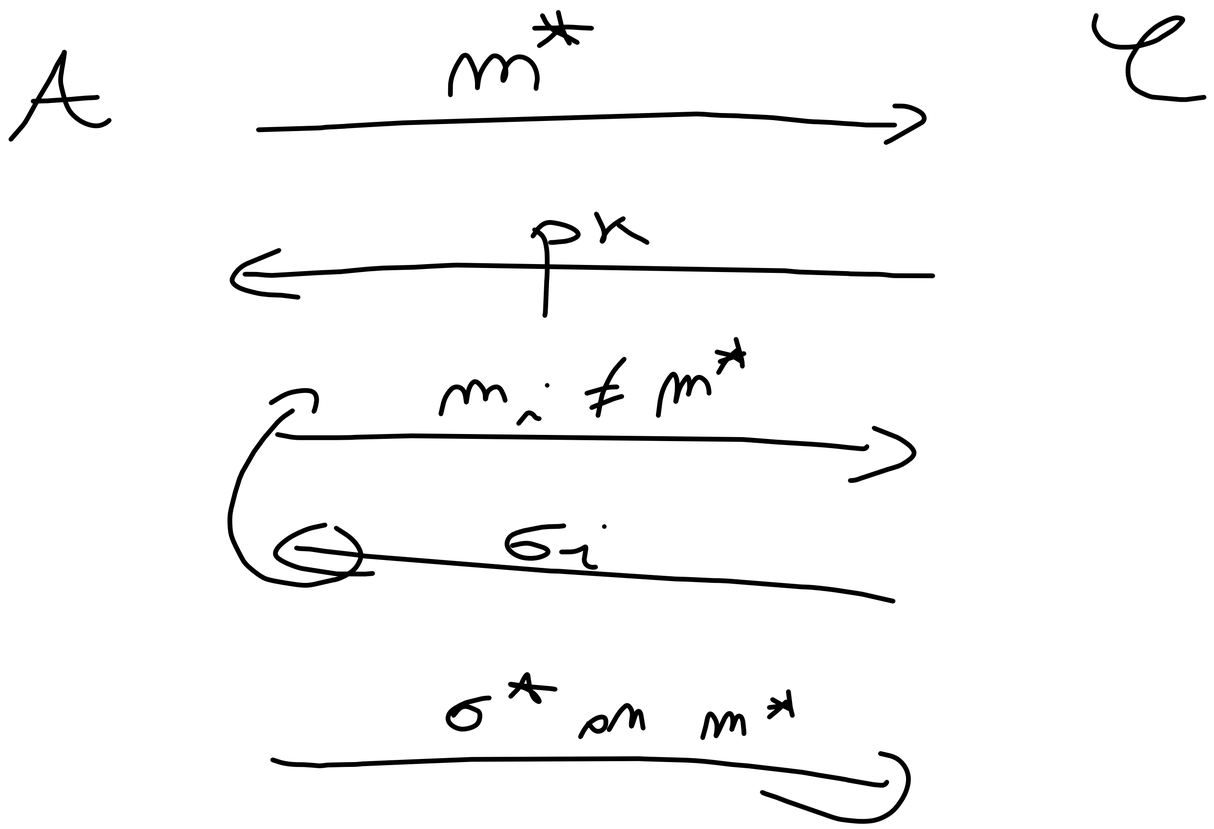
$$\overline{pk} = (pk, \bar{\sigma}) \; ; \; \bar{\sigma} = Sign(sk, 0^m)$$

$$\overline{sk} = sk$$

Prove: $\overline{\Pi}$ not UF-CMA

$\overline{\Pi}$ vs RUF-RMA.

*) Selective UF-CMA:



Prove/disprove: UF-CMA $\Leftrightarrow$ selective UF-CMA.

Try to prove: ~~UF~~ selective UF-CMA $\Rightarrow$ UFCMA if $|m| = O(\log \lambda)$.