Exercises

*) Let f be a length-preserving one-way function, and h be HARD-CORE for f. Establish if the following is a secure PRG:

$$G(x) = f(x) \| h(x).$$

(Recall: We have proven that if G is a PRG if f is a OWP.

The proof : $f : \{0,1\}^n \to \{0,1\}^n$

$$G(U_n) \equiv f(U_n) \| h(U_n)$$

$$\approx_c f(U_n) \| U_1$$

$$\equiv U_n \| U_1 \equiv U_{n+1}$$ (QED)

It doesn't work. To disprove it we must give $f : \{0,1\}^n \to \{0,1\}^n$ s.t.

f is OWF but G not secure.

e.g. $f(x) = f(x_1, x_2) = g(x_1) \| 0^{n_2}$

where $f : \{0,1\}^{n_1} \to \{0,1\}^{n_1}$ is a OWF

$|x_1| = n_1$; $|x_2| = n_2$

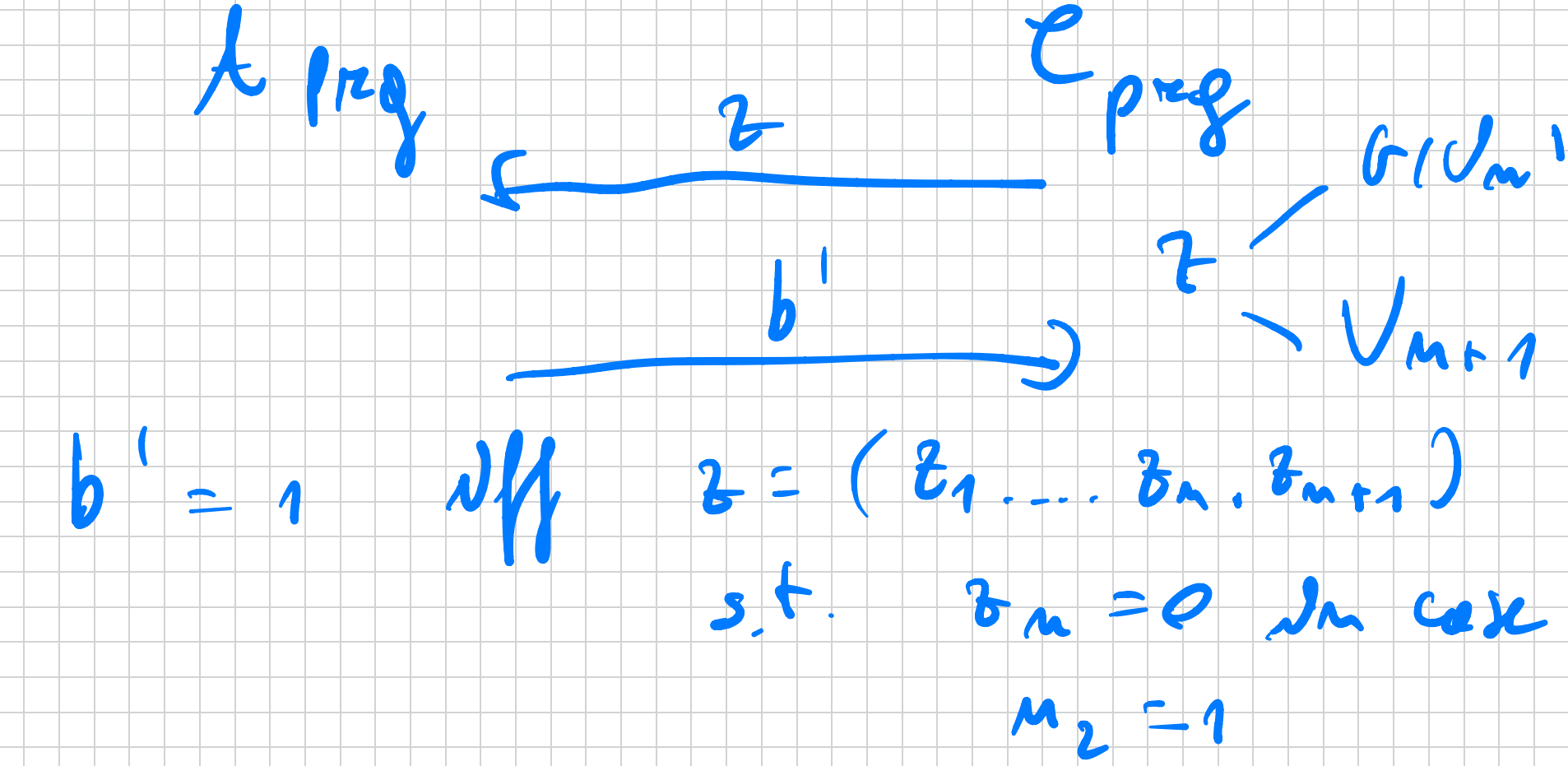
e.g. $n_1 = n - 1$; $n_2 = 1$. Now :

f OWF $\Rightarrow$ f OWF but

$$G(x) = f(x) \| h(x)$$

$$= f(x_1) \| 0^{n_2} \| h(x)$$

is not a PRG



$b' = 1$ iff $z = (z_1 \dots z_m, z_{m+1})$

s.t. $z_m = 0$ in case

$m_2 = 1$

*) Let G be a group of prime order q. Assume it's possible to compute $\sqrt{\cdot}$ over G if it exists.

Prove that CDH is equivalent to:

- SQUARE-DH: given (g, g^a) for $a \leftarrow \mathbb{Z}_q$ output g^{a^2}.

We must prove:

(1) CDH $\Rightarrow$ SQUARE-DH

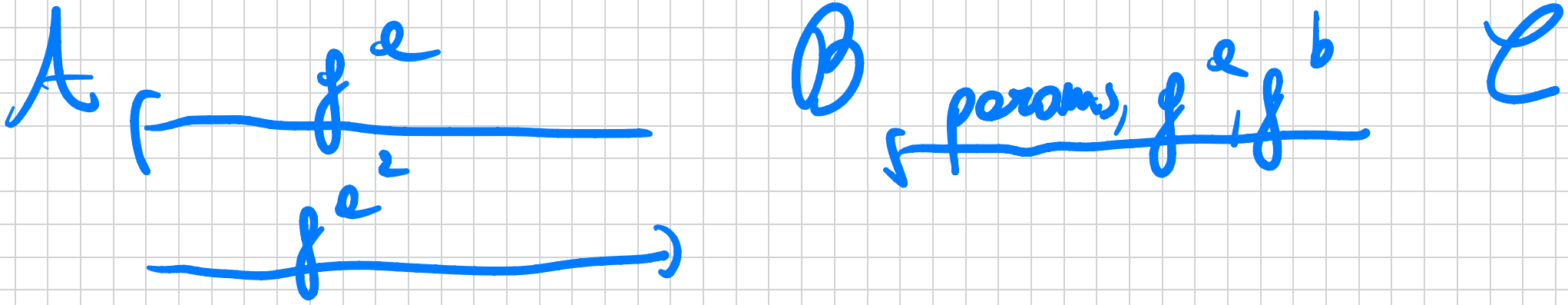
(Ne) SQUARE-DH $\Rightarrow$ CDH

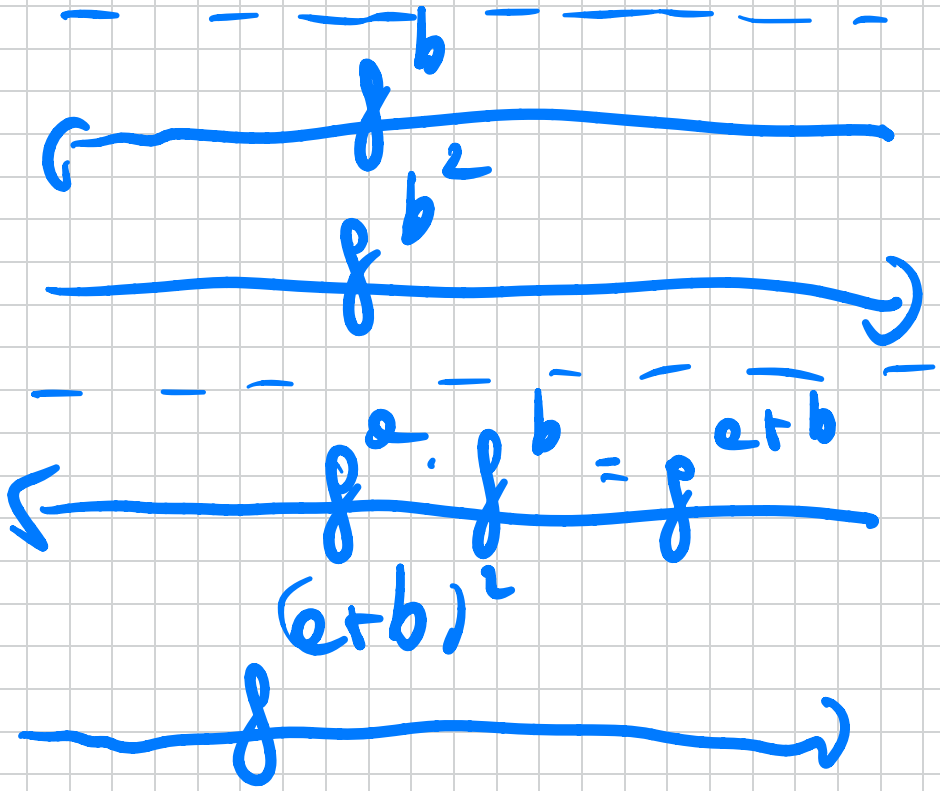
(N) fool: $\exists$ PPT A s.t.

$$\Pr[A(\text{params}, g^a) = g^{a^2}] \geq \frac{1}{\text{poly}}$$

$$\text{params} = (\mathbb{G}, g, q), \quad a \leftarrow \mathbb{Z}_q$$

Then build PPT $\mathcal{B}$ against CDH.





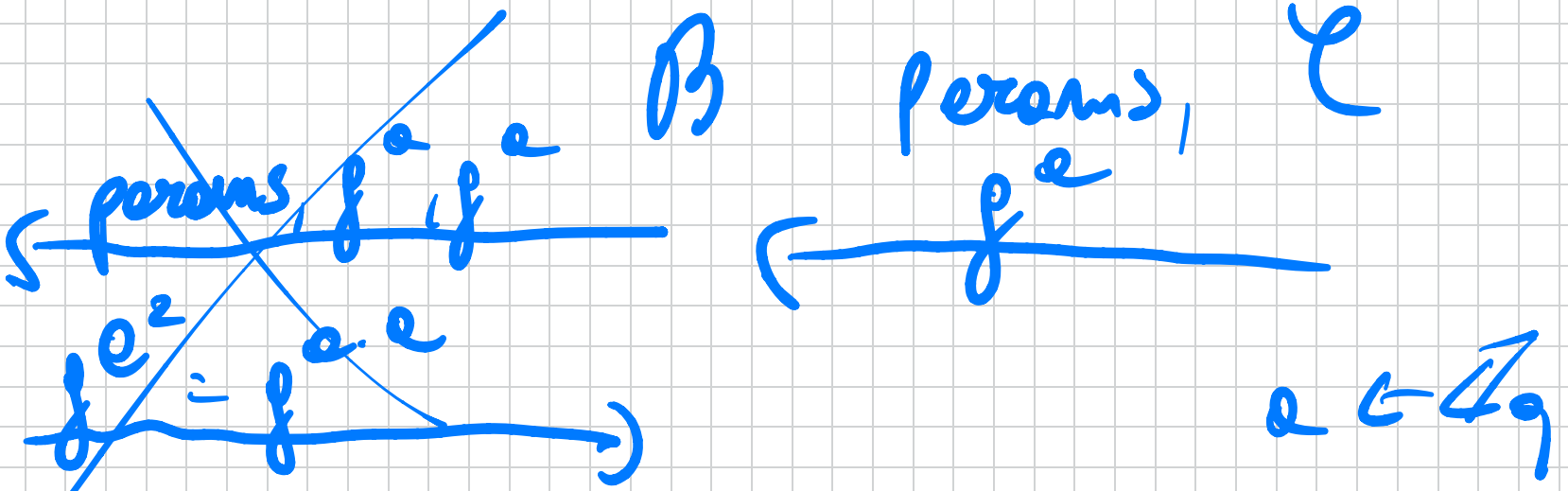
$\Rightarrow$ w.p. $\left(\frac{1}{poly(\lambda)}\right)^3 = \frac{1}{poly(\lambda)}$ we know

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

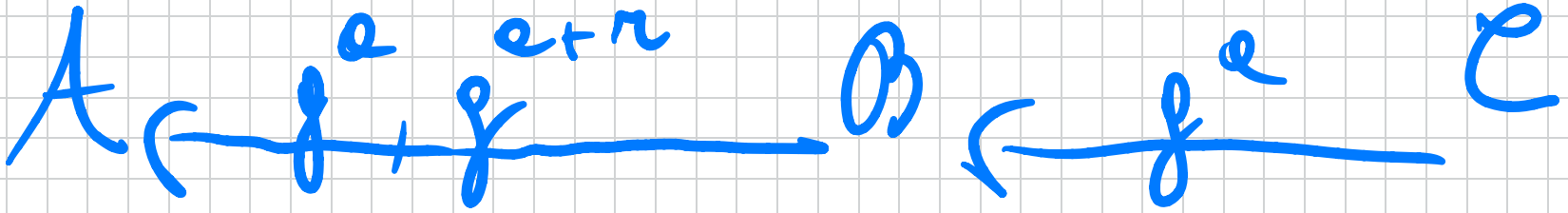
$$\frac{g^{(a+b)^2}}{g^{a^2} \cdot g^{b^2}} = g^{2ab} = \left(g^{ab}\right)^2$$

Then, take $\sqrt{\cdot}$ over G.

(NN) A B performs, C



$a \leftarrow \mathbb{Z}_q$



$r \leftarrow \mathbb{Z}_q$

$$g^{ab} = g^{a(a+n)}$$

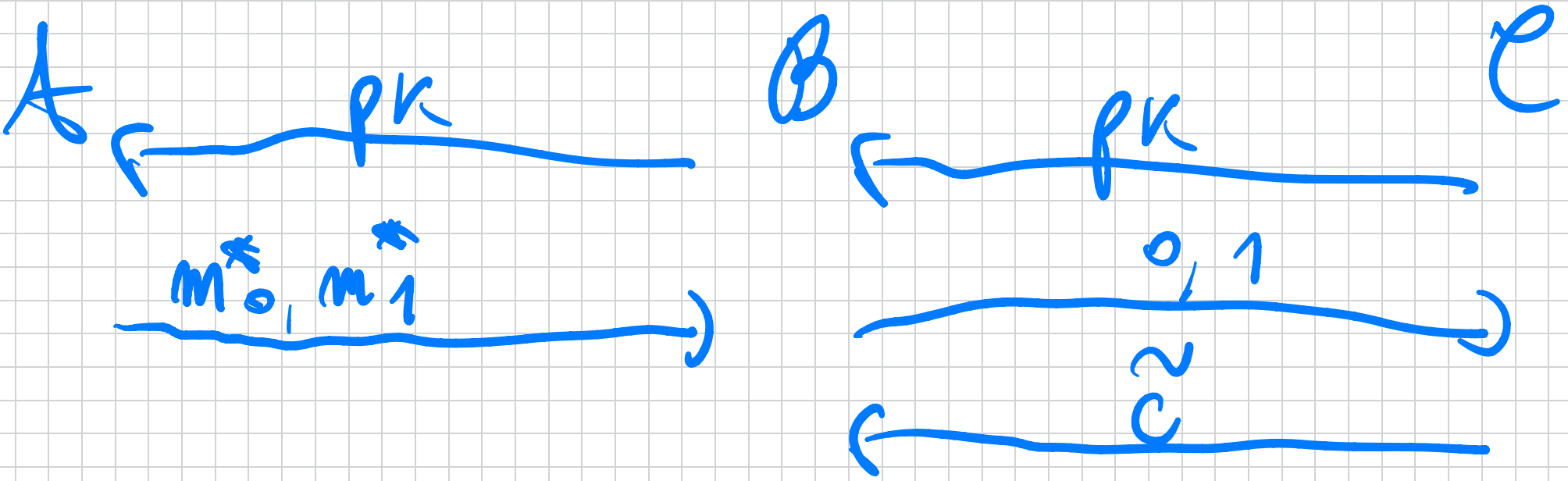
$$g^{a(a+n)} = g^{a^2+an} = g^{a^2} \cdot g^{an}$$

$\Rightarrow$ Comparo $(g^a)^n = g^{an}$ ed è dimostrata.

*) Let $\Pi = (Kgen, Enc, Dec)$ be a PKE scheme for $M = \{0,1\}$.
Build Π' a PKE scheme for $M = \{0,1\}^\ell$ for $\ell(\lambda) = poly(\lambda)$.
Assume Π is CPA-secure. Π' also should be CPA-secure.
Suggestion: $(pk, sk) \leftarrow Kgen(1^\lambda)$ and given $m = (m[1], m[2], \ldots, m[\ell])$ output $c = (c_1, c_2, \ldots, c_\ell)$

$$c[j] \leftarrow Enc(pk, m[j]).$$

Proof of CPA-security: Assume not, a PPT A that breaks CPA security.



$$m_0^* = (m_0^*[1], \ldots, m_0^*[\ell])$$

$$m_1^* = (m_1^*[1], \ldots, m_1^*[\ell])$$

Let $\boxed{\cdot} \equiv Enc(pk, \cdot)$

CHALLENGE:

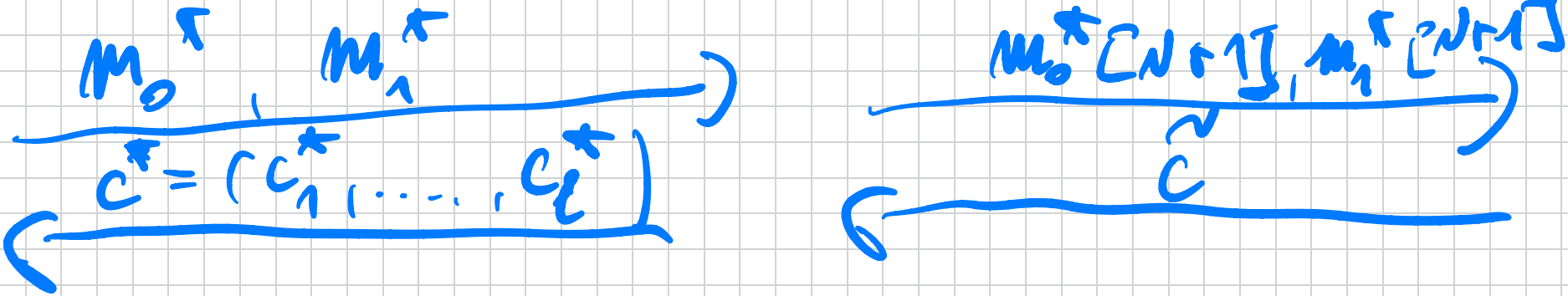
$H_0 \equiv \boxed{m_1^*[1]}, \ldots, \boxed{m_1^*[\ell]}$

$$H_w \equiv (\overline{m_0^*[1]}, \ldots, \overline{m_0^*[i]}, \overline{m_1^*[w-1]}, \ldots, \overline{m_1^*[l]})$$

$$H_e \equiv (\overline{m_0^*[1]}, \ldots, \overline{m_0^*[l]})$$

$$\forall\, w : H_i \approx_c H_{w-1}$$

$$A \xleftarrow{\rho^K} B \xleftarrow{\rho^K} C$$

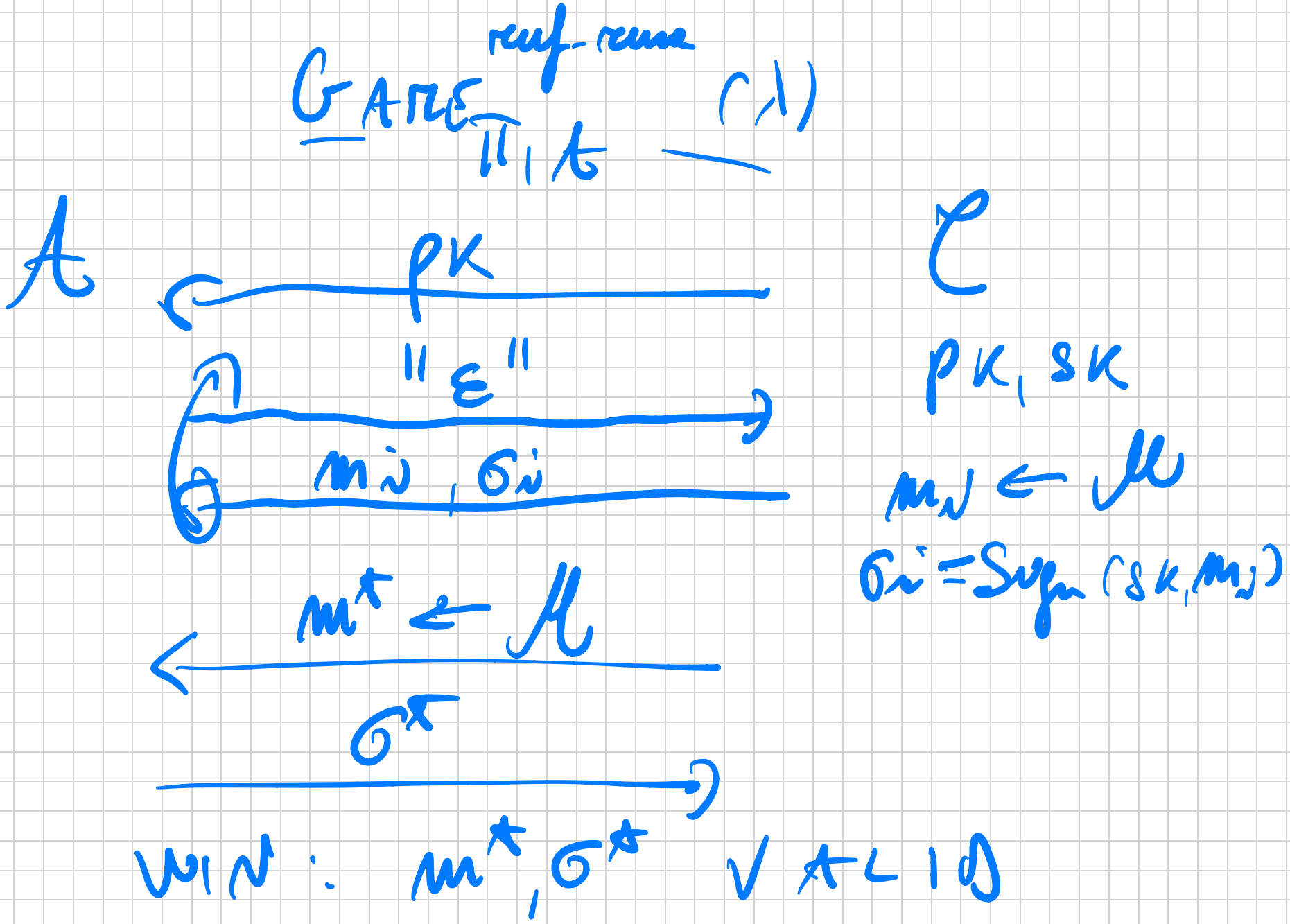


$c_1^*, \ldots, c_N^*$ ale $Enc(pk, m_0^*[i])$

$c_{N+1}^* = c$

$c_{N+2}^*, \ldots, c_\ell^*$ ale $Enc(pk, m_1^*[i])$

*) Consider EUF-CMA:



$|M| = \omega(\log \lambda)$.

Question: (i) UF-CMA $\Rightarrow$ RUF-RMA ?

(ii) RUF-RMA $\Rightarrow$ UF-CMA ?

(i) Trivial. (Work out the reduction.)

(ii) False. Take any UF-CMA Π and consider Π' with $|M'| = 2|M|$

$\sigma' = \text{Sign}(sk, m')$

Say $m' = m_1 \| m_2$ with $|m_1| = |m_2| = n$

Check: If $m_1 = 0^n$

$\sigma' = m_2$

Else $\sigma' = Sign(sk, m_2)$

Alternative: let $pk' = (pk, \bar{m}, \bar{\sigma})$

$\bar{m} \in M$, $\bar{\sigma} = Sign(sk, \bar{m})$

*) Let $f : \{0,1\}^n \to \{0,1\}^m$ be a OWF.

Consider the following $\Pi = (Kgen, Sign, Vrfy)$.

$\underline{Kgen}(1^n)$: $SK = (x_i^0, x_i^1)_{i \in [l]}$

$x_i^0, x_i^1 \leftarrow \{0,1\}^n$

$PK = (y_i^0, y_i^1)_{i \in [l]}$

$\forall\, b \in \{0,1\}$, $y_i^b = f(x_i^b)$

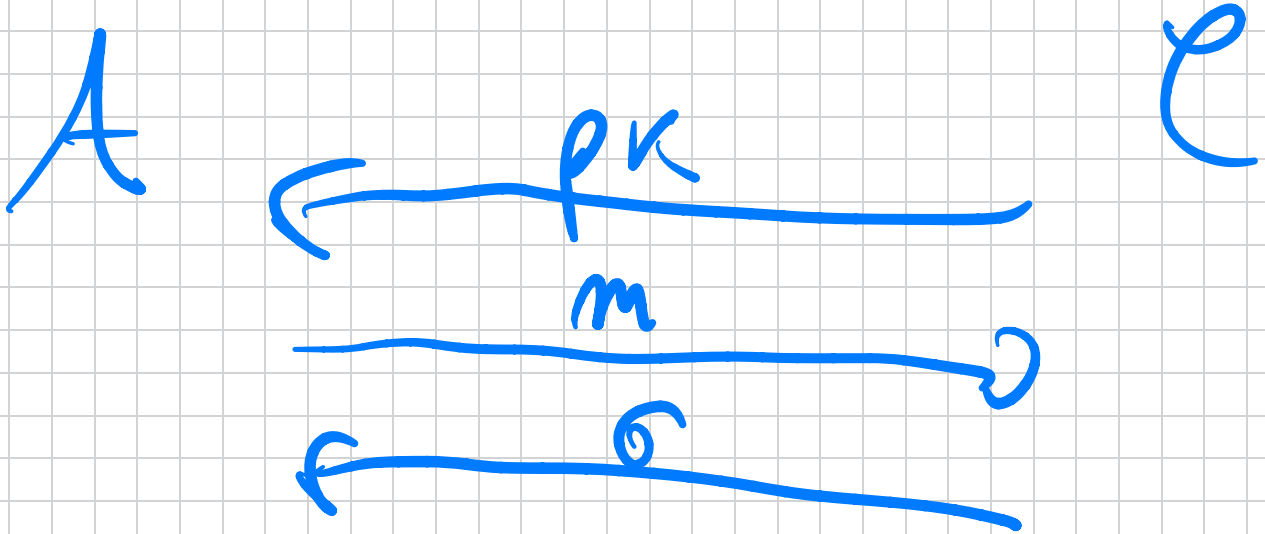
$Sign(SK, m = m[1], \ldots, m[l])$

Output $\sigma = \left(x_i^{m[i]}\right)_{i \in [\ell]}$

Verify: Just check that

$$f\left(x_j^{m[n]}\right) = y_j^{m[n]} \quad \forall n.$$

Prove: Π is one-time secure assuming f is OWF.



$m^* \neq m$, σ^* → 1 vs 0

Observation: $\exists\, j$ s.t. $m^*[j] \neq m[j]$.

For this position j, σ contains x_j^0 a pre-image of y_j^0 but σ^* contains x_j^1 a pre-image of y_j^1. This suggests the following reduction:

$A \hookrightarrow \{0,1\}^k$ — B — $y^* = f(x^*)$ — $\mathcal{C}$

$j \in [\ell]$, $b \in \{0,1\}$

$x^* \in \{0,1\}^n$

$pk = (y_i^0, y_i^1)$ like in the signature scheme, but $pk[j] = (y_j^0, y_j^1)$

s.t. $y_j^b = y^*$

The reduction knows all other pre-images x_j^0, x_j^1

$m = (m[1], \ldots, m[l])$

m^*, σ^*

Hope: $m[j] \neq b$ and $m[j] \neq m^*[j]$