EXERCISES

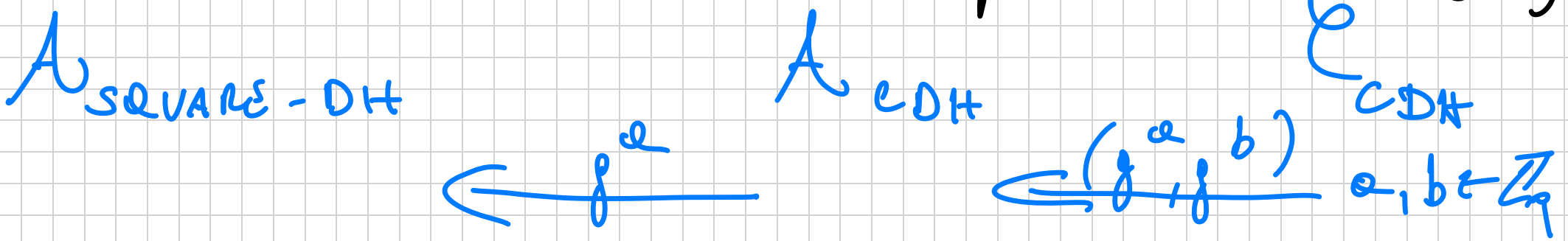
*) Consider the following assumption:

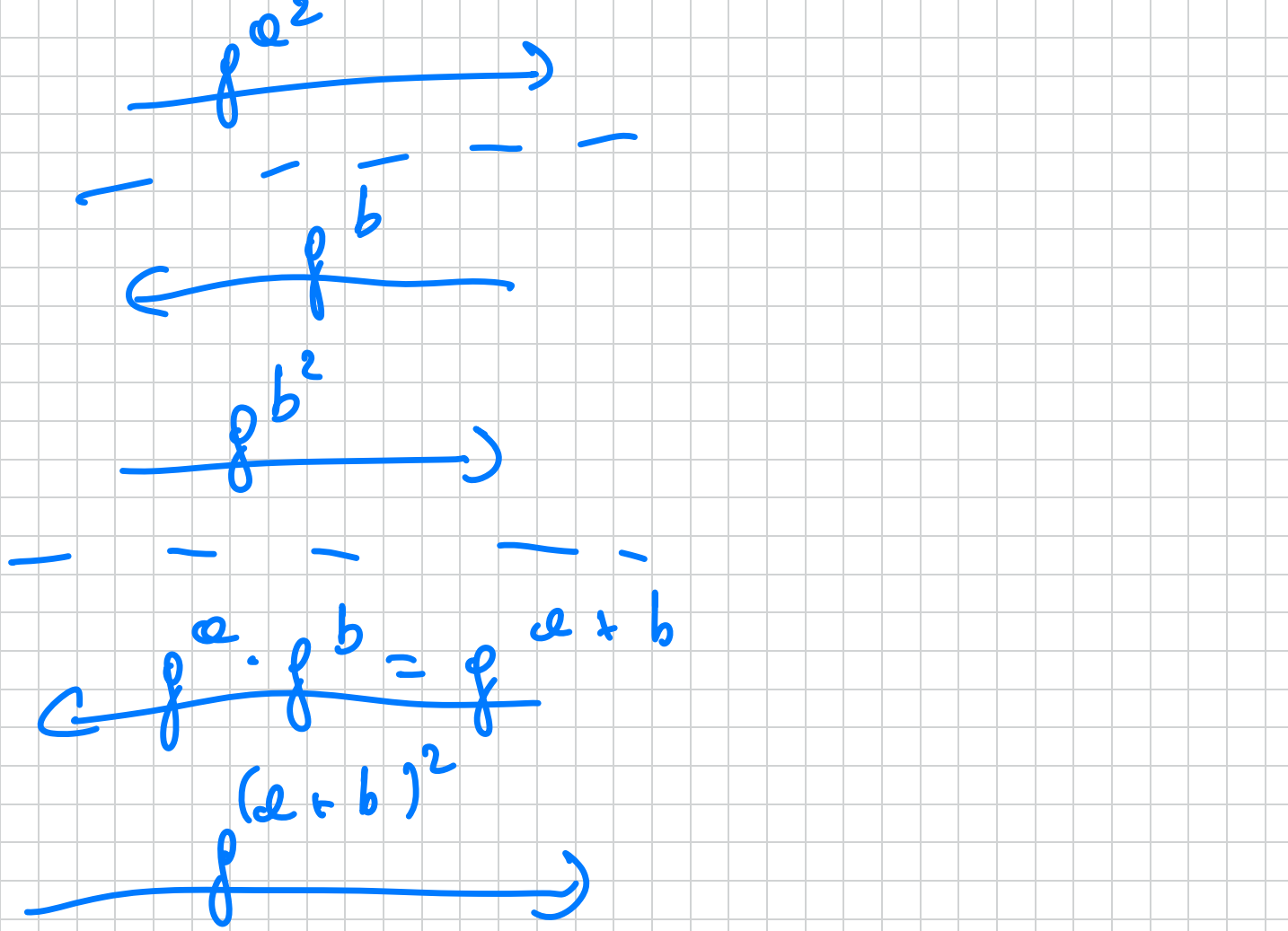
SQUARE-DH: given g^a, compute $g^{(a^2)}$, where $(\mathbb{G}, g, q) \leftarrow \text{GroupGen}(1^\lambda)$

$a \leftarrow \mathbb{Z}_q$

Prove CDH equivalent to SQUARE-DH.

CDH $\Rightarrow$ SQUARE-DH. (Assume we can compute square roots in $\mathbb{G}$.)





$$f^{a^2},\ f^{b^2},\ f^{(a+b)^2} \qquad f^{(a+b)^2} = f^{a^2+b^2+2ab}$$

$$\Rightarrow \quad f^{a^2+b^2+2ab} = f^{2ab}$$

$$f^{a^2} \cdot f^{b^2}$$

$\sqrt{g^{2ab}} = g^{ab}$

$$\Pr[A_{CDH} \text{ wins}] \geq \Pr[A_{SQ\text{-}DH} \text{ wins}]$$

$$\geq 1/\text{poly}(\lambda) .$$

SQ-DH $\Rightarrow$ CDH.

A_{CDH} $\leftarrow (g^a, g^a)$

$A_{SQ\text{-}DH}$ $\leftarrow g^a$ $\leftarrow \zeta_{SQ\text{-}DH}$

$a \leftarrow \mathbb{Z}_q$

$g^{a \cdot a} = g^{a^2}$ ⟶

This does not work as ACDH expects

To see a pair (g^a, g^b) s.t. a, b are UNIFORM. Sample $r \leftarrow \mathbb{Z}_q$

⟵ $(g^a, g^{a+r} = g^a \cdot g^r)$

$g^{a(a+r)} = g^{a^2 + ar}$ ⟶

$= g^{a^2} \cdot g^{ar}$

$= g^{a^2} (g^a)^r$

Divide $g^{a(e+r)} / (g^e)^r = g^{a^2}$ ✓

→

*) Prove that CPA PKE for $M = \{0,1\}$ implies CPA PKE for $M = \{0,1\}^n$ for any $n = n(\lambda) = \text{poly}(\lambda)$.

Let $\Pi = (\text{Kgen}, \text{Enc}, \text{Dec})$ be the given CPA scheme.

Вывод $\Pi' = (Kgen', Enc', Dec')$.

$\underline{Kgen'(1^\lambda)}$: $(pk, sk) \leftarrow Kgen(1^\lambda)$

$\underline{Enc'(pk, m \in \{0,1\}^n)}$: $m = (m_1, \dots, m_n)$
$m_i \in \{0,1\}$

Output: $c' = (c_1, \dots, c_n)$; $c_i \leftarrow Enc(pk, m_i)$

$\underline{Dec'(sk, c')}$: $c' = (c_1, \dots, c_n)$

Output: $(Dec(sk, c_1), \dots, Dec(sk, c_n))$

$\mathcal{A}'$ $\qquad \mathrm{GAME}^{cpa}_{\Pi', \mathcal{A}'}(\lambda, b)$ $\qquad \mathcal{C}'$

$(pk, sk) \leftarrow KGen'(\lambda')$

$\xleftarrow{\quad pk \quad}$

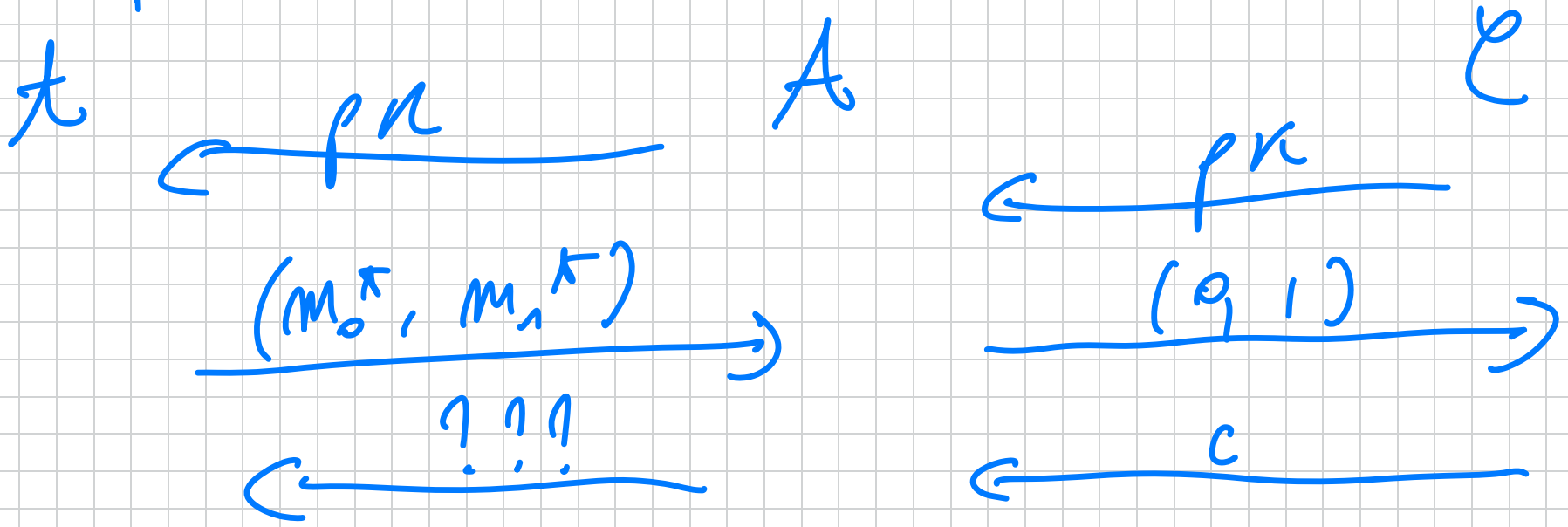
$\xrightarrow{\quad (m_0^*, m_1^*) \quad}$

$m_b^* = (m_b^*[1], \ldots, m_b^*[n])$

$\xleftarrow{\quad c^* \quad}$

$c^* = (c_1, \ldots, c_n)$

$\xrightarrow{\quad b' \quad}$



Hybrid argument !

$H_0(\lambda) \equiv \text{GAME}(\lambda, 0)$

$H_1(\lambda)$

$c^* \leftarrow (Enc(pk, m_0^*[1]),$
$\vdots$
$Enc(pk, m_0^*[n]))$

$c^* \leftarrow (Enc(pk, m_1^*[1])$
$Enc(pk, m_0^*[2]),$
$\vdots$
$Enc(pk, m_0^*[n]))$

$H_m(\lambda)$

$c^* \leftarrow (\mathcal{E}nc(pk, m_1^*, r_1)$

$\vdots$

$c^* \leftarrow \mathcal{E}nc(pk, m_1^*, r_m))$

LEMMA $\forall \lambda : H_\lambda(\lambda) \approx_c H_{N_m}(\lambda)$

*) Is it CCA secure?

Warm-up: Is El Gamal CCA secure?

$h = pk$; g^x, $sk = x$; $c = (g^r, h^r \cdot m) =$

$r \leftarrow \mathbb{Z}_q \quad = (c_1, c_2)$

What if: $r' \in \mathbb{Z}_q$ and let

$$\tilde{c} = (\tilde{c}_1, \tilde{c}_2) = (g^r \cdot g^{r'}, h^r \cdot m \cdot h^{r'})$$

$$= (c_1 \cdot g^{r'}, c_2 \cdot h^{r'})$$

$$= (g^{r+r'}, h^{r+r'} \cdot m)$$

$\tilde{c} \neq c$

$$Dec(sk, (\tilde{c}_1, \tilde{c}_2)) = ? \quad \tilde{c}_2 / (\tilde{c}_1)^x$$

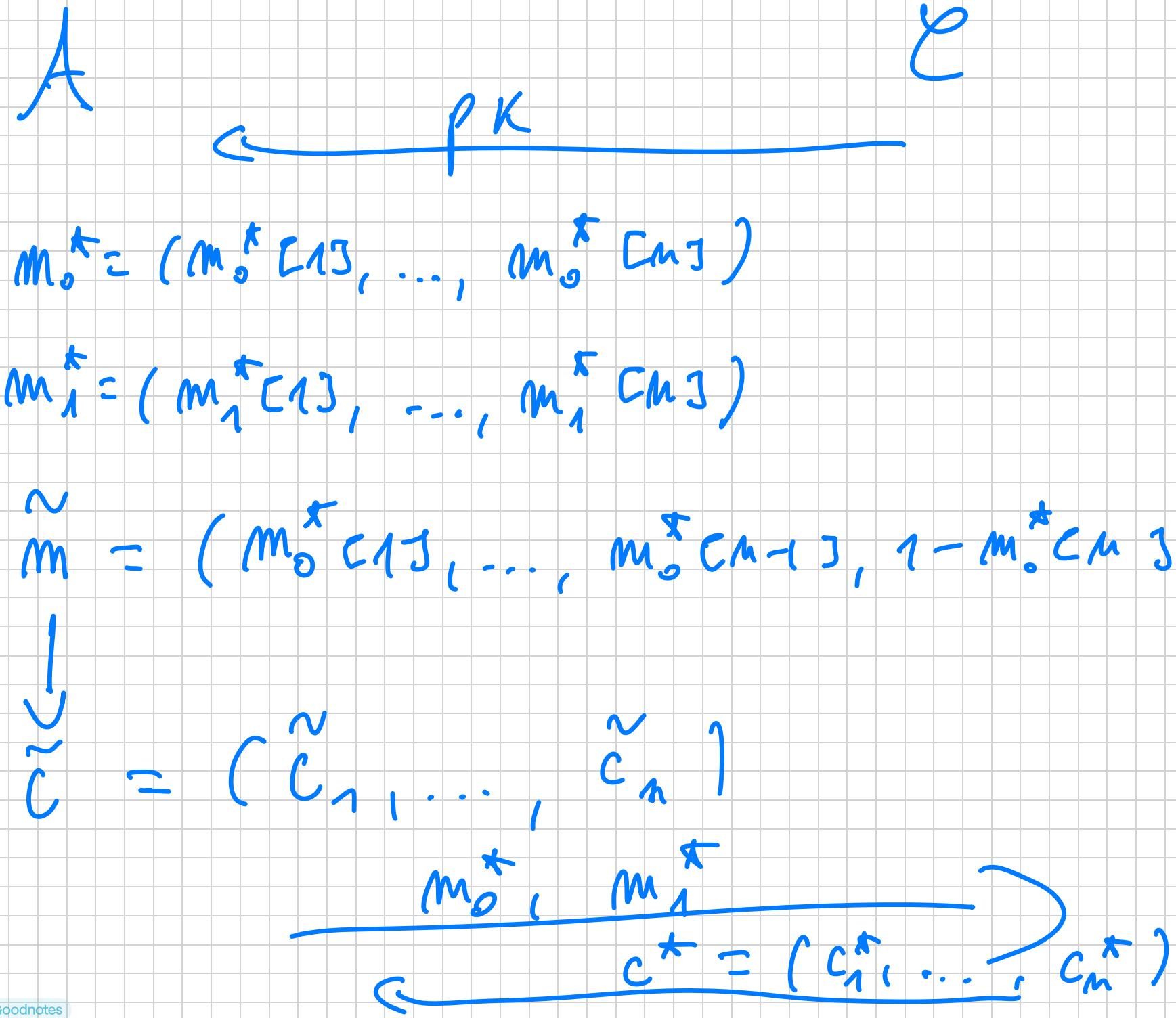
$$\frac{h^{r+r'} \cdot m}{(g^{r+r'})^x} = \frac{h^{r+r'} \cdot m}{(g^x)^{r+r'}} = m$$

Elgamal is homomorphic:

given $c_1 = (g^{r_1}, h^{r_1} \cdot m_1) = (c_{1,1}, c_{1,2})$

$c_2 = (g^{r_2}, h^{r_2} \cdot m_2) = (c_{2,1}, c_{2,2})$

$(c_{1,1} \cdot c_{2,1}, c_{1,2} \cdot c_{2,2})$ is enc of $m_1 \cdot m_2$



Assume: $m_0^*[1] \neq m_1^*[1]$

$\tilde{c} = (c_1^*, Enc(pk, 0), \ldots, Enc(pk, 0))$

$\tilde{c}$ →

$\tilde{m} = (m_b^*[1], *, \ldots, *)$ ←

$b' = b$ →

*) Let $f : \{0,1\}^n \to \{0,1\}^n$ be a OWF.
Consider the following signature scheme for
$M = \{0,1\}^n$ for fixed $n \in \mathbb{N}$.

Key Gen (1^λ): $pk = ((y_{0,1}, y_{1,1}), \ldots (y_{0,n}, y_{1,n}))$

$sk = ((x_{0,1}, x_{1,1}), \ldots, (x_{0,n}, x_{1,n}))$

s.t. $y_{b,i} = f(x_{b,i})$

$\forall\ b = 0,1$

$i = 1, \ldots, n$

$Sign(SK, m = (m_1, \ldots, m_n)) = \sigma =$

$= (x_{m_1,1}, \ldots, x_{m_n,n})$

1 2 3

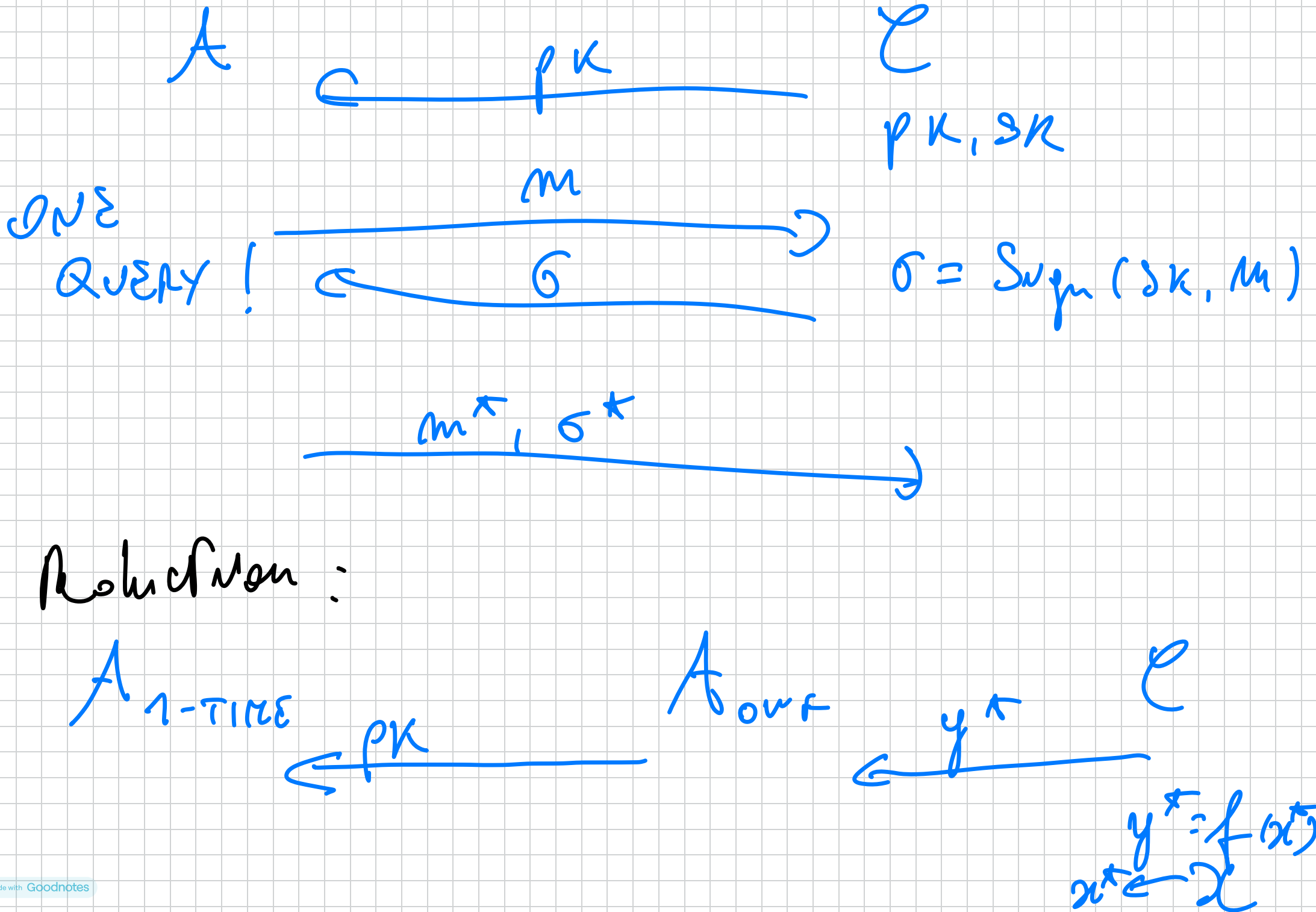
$m = 010$

$x_{0,1}$ $x_{0,2}$ $x_{0,3}$

$x_{1,1}$ $x_{1,2}$ $x_{1,3}$

$Vrfy(pk, m, \sigma)$: Just check the pre-images are correct w.r.t pk.

Prove UF $\Rightarrow$ ONE-TIME "UF-CMA".


A
pk
C
pk, sk
ONE QUERY !
m
σ
σ = Sign(sk, m)
m*, σ*
Reduction :
A 1-time
pk
A out
y*
C
y* = f(x*)
x*
x

Pick $b \in \{0,1\}$

$i \in [n]$

The reduction hopes that:

(i) $m^*[i] \neq m[i]$ w.p. $1/n$

(ii) $m^*[i] = b$ w.p. $1/2$

pk s.t. $y_{b,i} = y^*$

all the other y's are honestly computed.