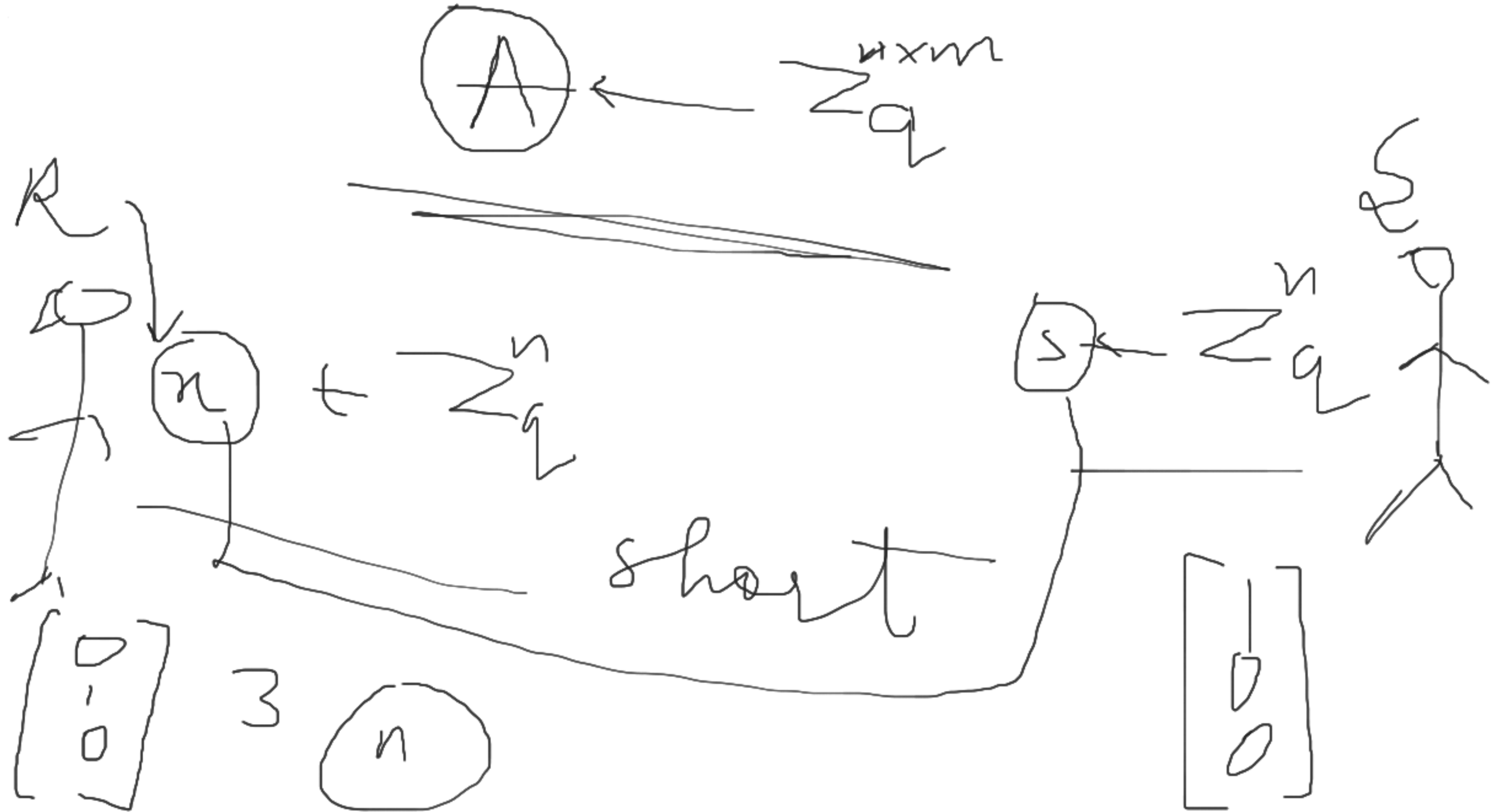


public key cryptosystem using LWE

4-7.



$R$  $A^{m \times n}$  $x$ 

$$\boxed{y} = Ax$$

$$y = Ax$$

$$(m > n \log \frac{1}{\epsilon})$$

 $y, x, S$  $S$  $S$

$$R \quad 0 / \square = \text{bit}$$

$$x \quad 6 \times 10^{-30}$$

$$b^t = s^t A y + e^t$$

$$u = A x$$

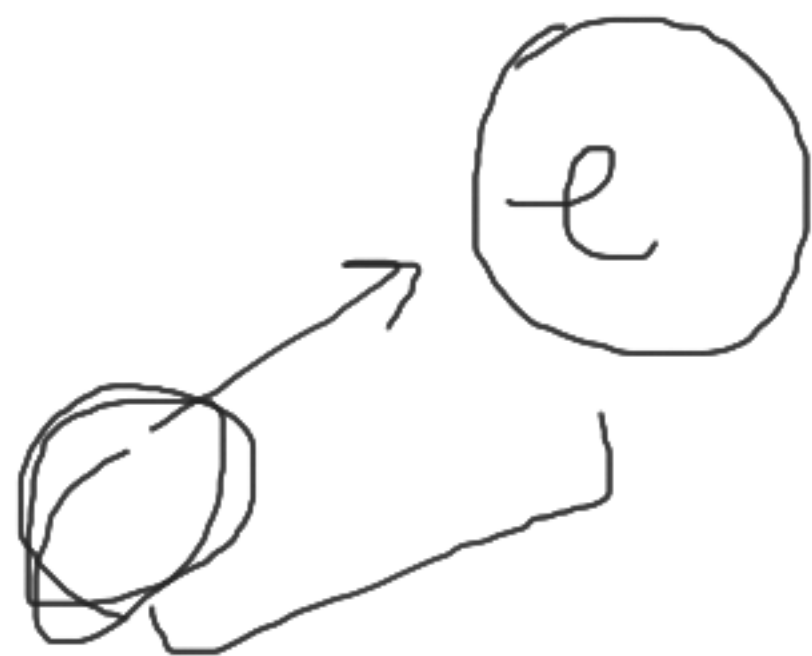
$$b' = s^t u + e'' + \frac{q}{2} \cdot \text{bit}$$

$$256 \leftarrow n$$

$$512$$

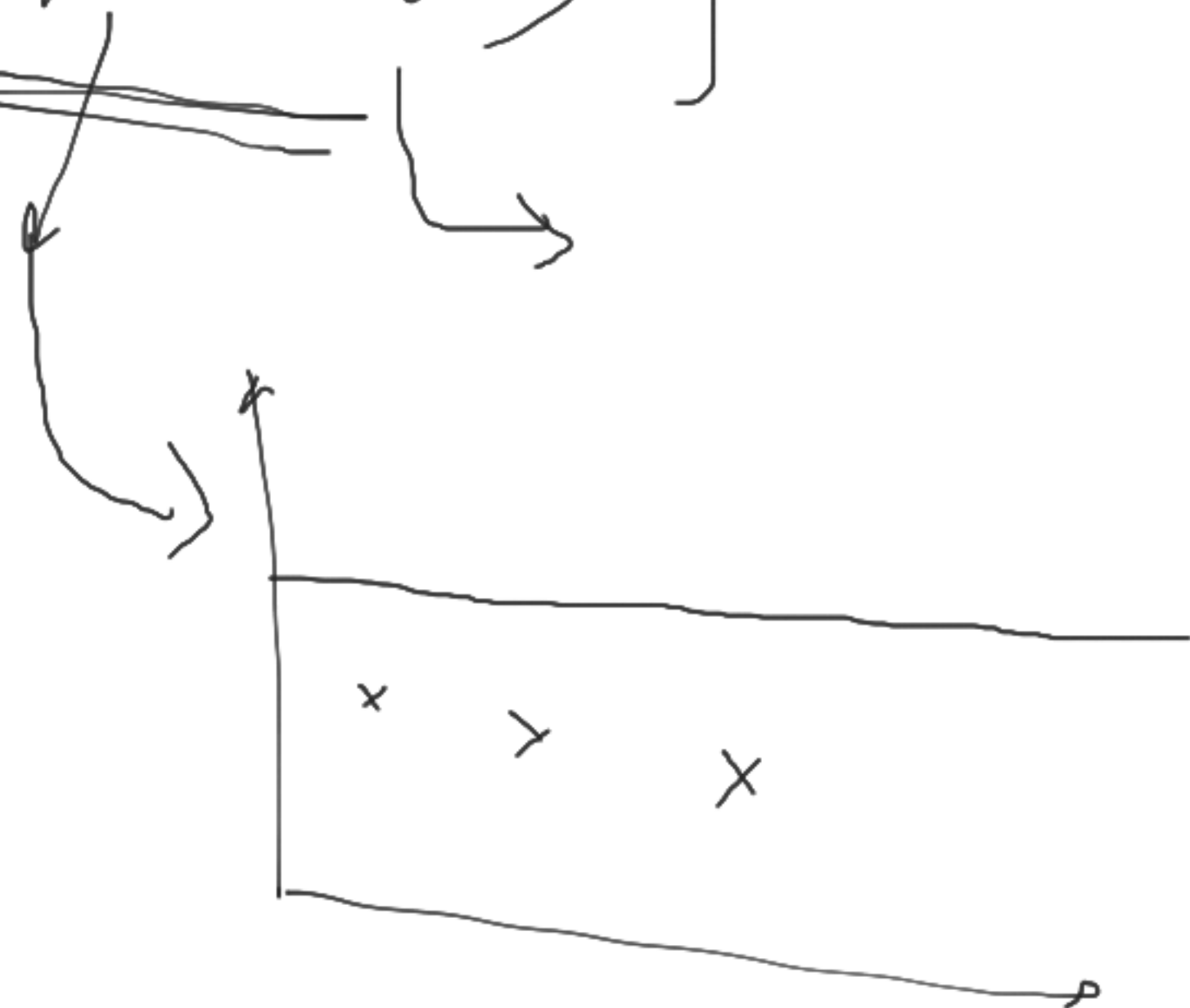
$$b' - b^t = s^t u - s^t u - \frac{e + e' + \frac{q}{2} \cdot \text{bit}}{\frac{q}{2}}$$

$$\frac{e^1 - e^t}{1} + \text{bit} \cdot \frac{1}{2}$$



$$\frac{1}{1} \cdot \frac{1}{2} \cdot 1.0005$$

~~$(A, u)$~~  } *variables*

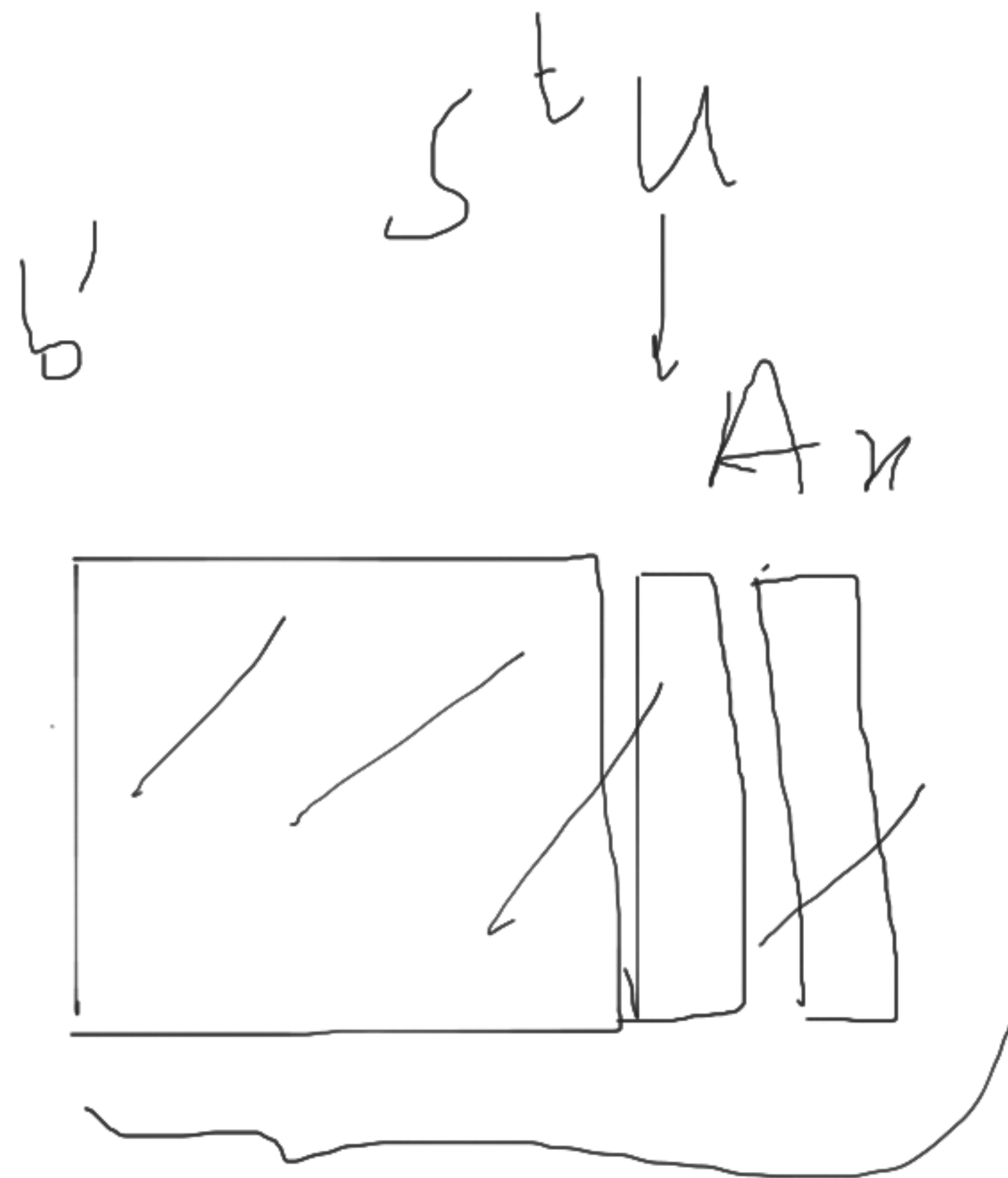
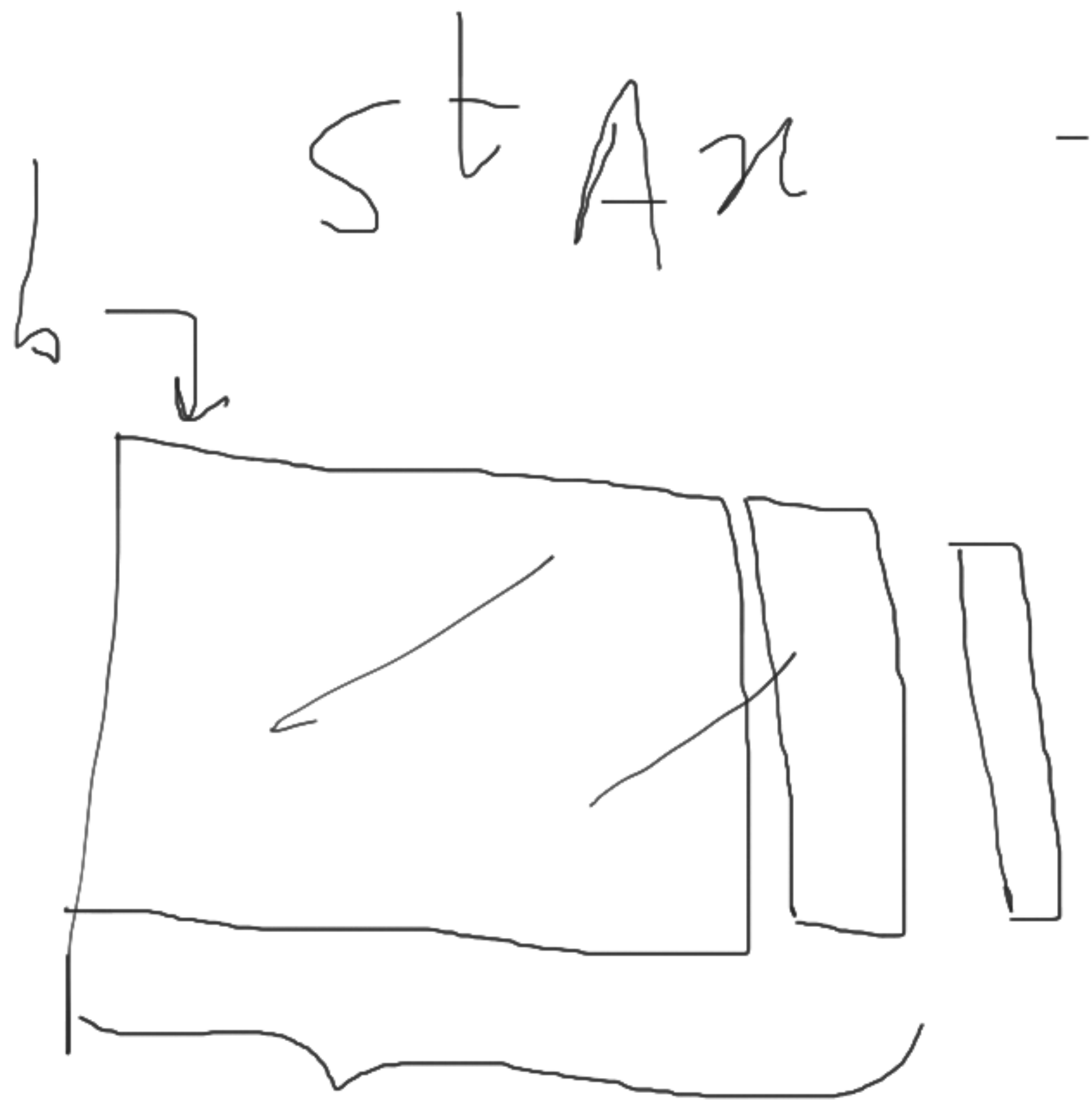


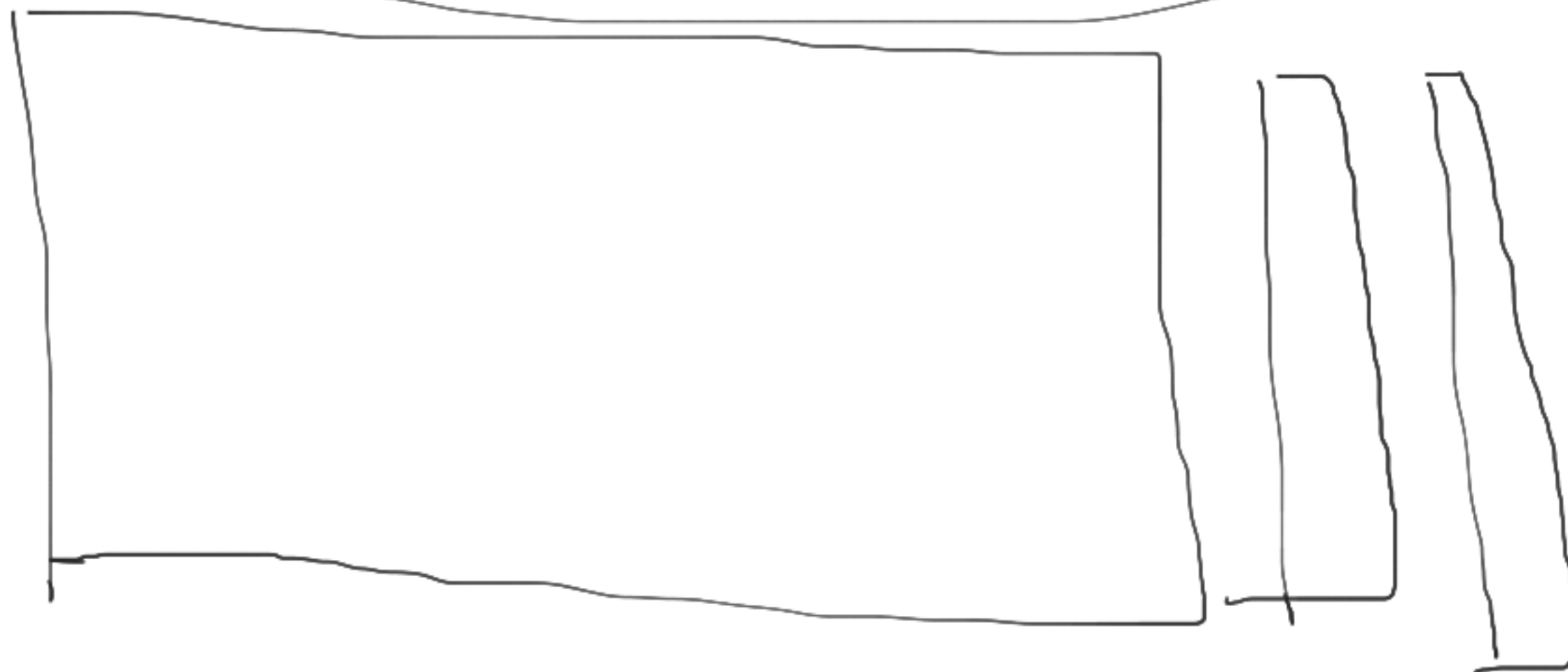
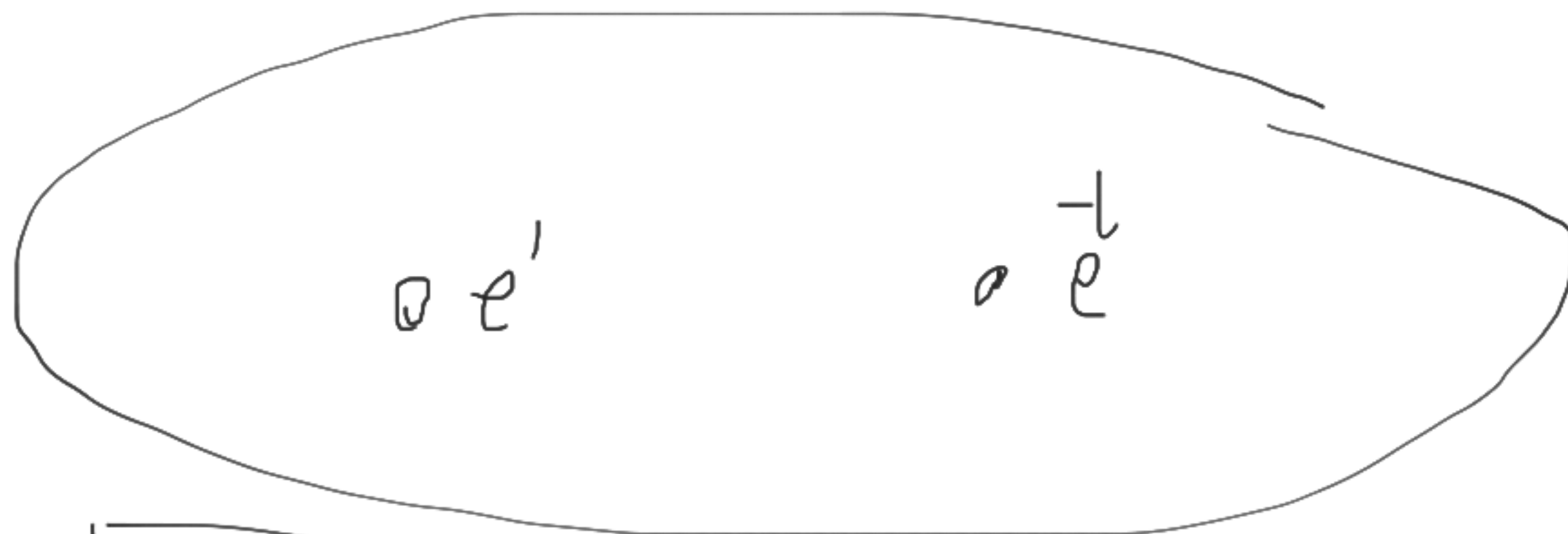
~~$(b - b')$~~

*wonder*

$s^+ A =$

$s^+ u$





Digital Sig

S | S

$u \geq A_n$

$\overline{u} \geq A_n + \ell$



$$vk = A$$

$$s \in \mathbb{Z}_q^n$$

$$\underline{Ax = 0}$$

$$\begin{array}{c} \swarrow \quad \searrow \\ sk = T \\ \downarrow \\ \underline{\text{Trapdoor}} \end{array}$$

①

$$vk = A \rightarrow \text{public}$$

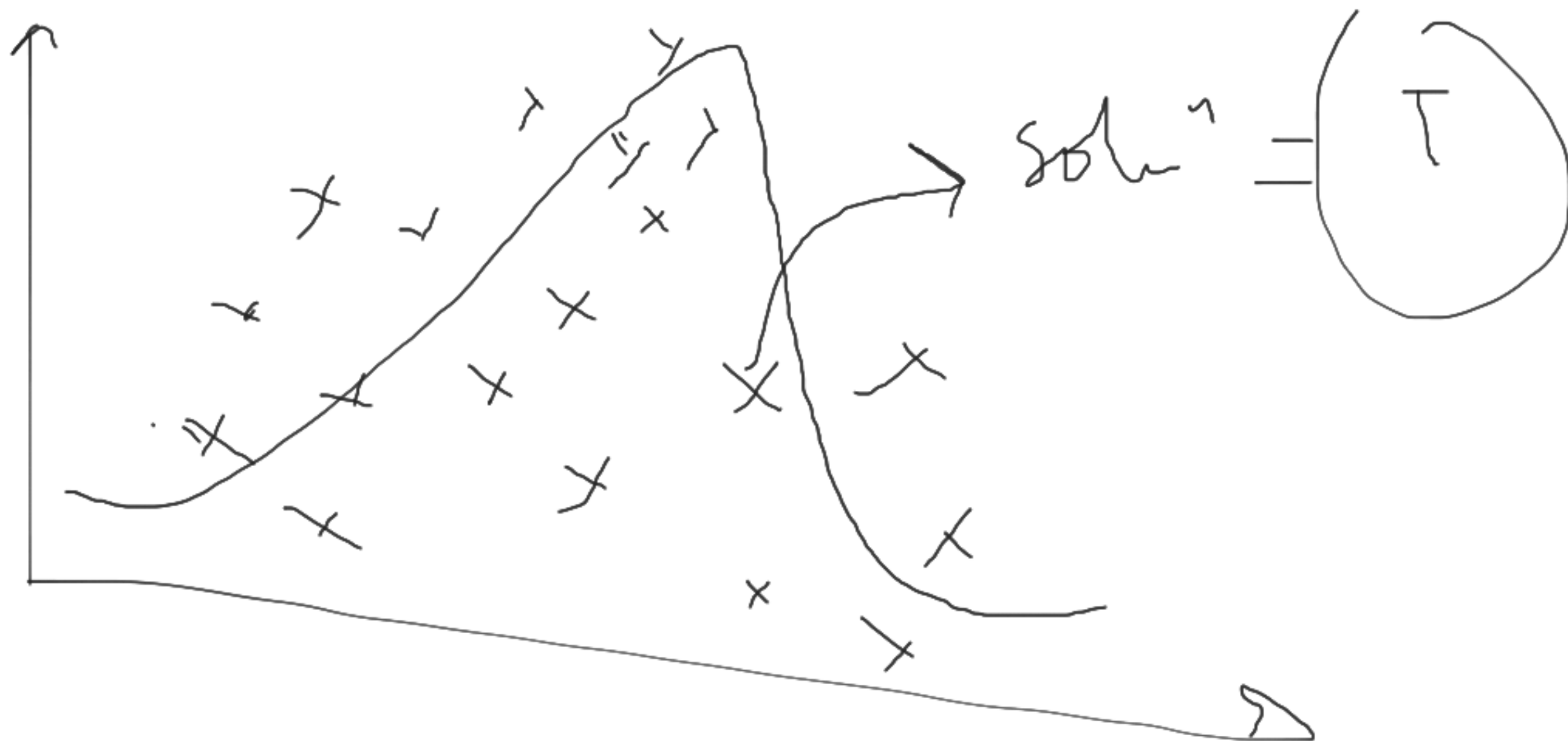
$$sk = T \rightarrow \begin{matrix} T \\ \downarrow \end{matrix}$$

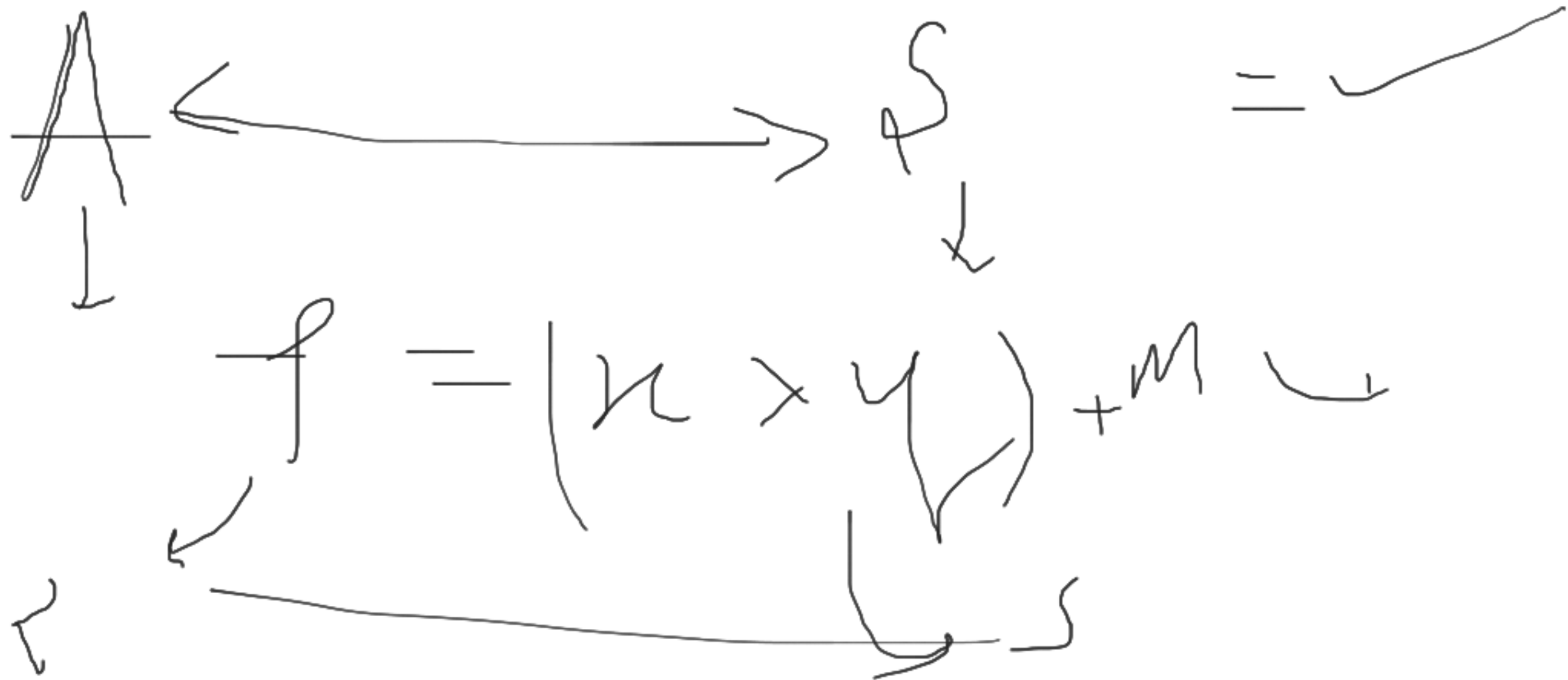
②



$$\text{Sign}(T, \mu) \quad Ax = H(\mu)$$

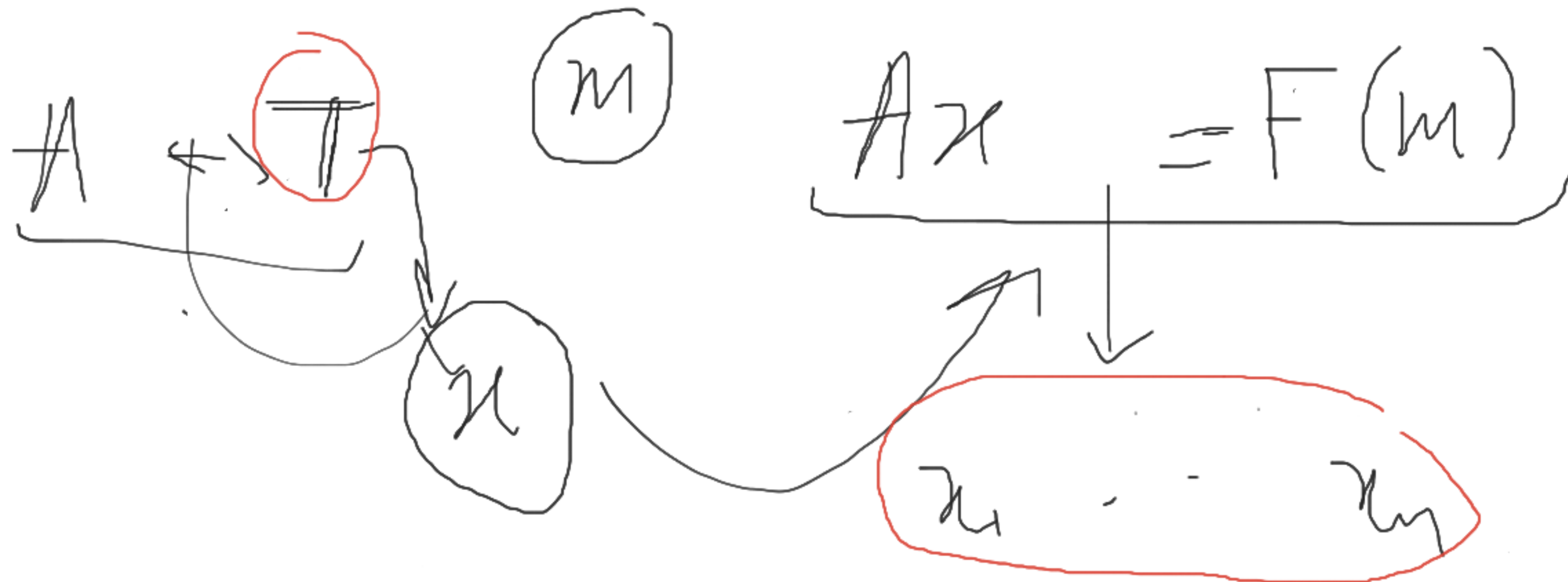
$$\mu \leftarrow \sum_{q=1}^n$$

$$Ax = v$$



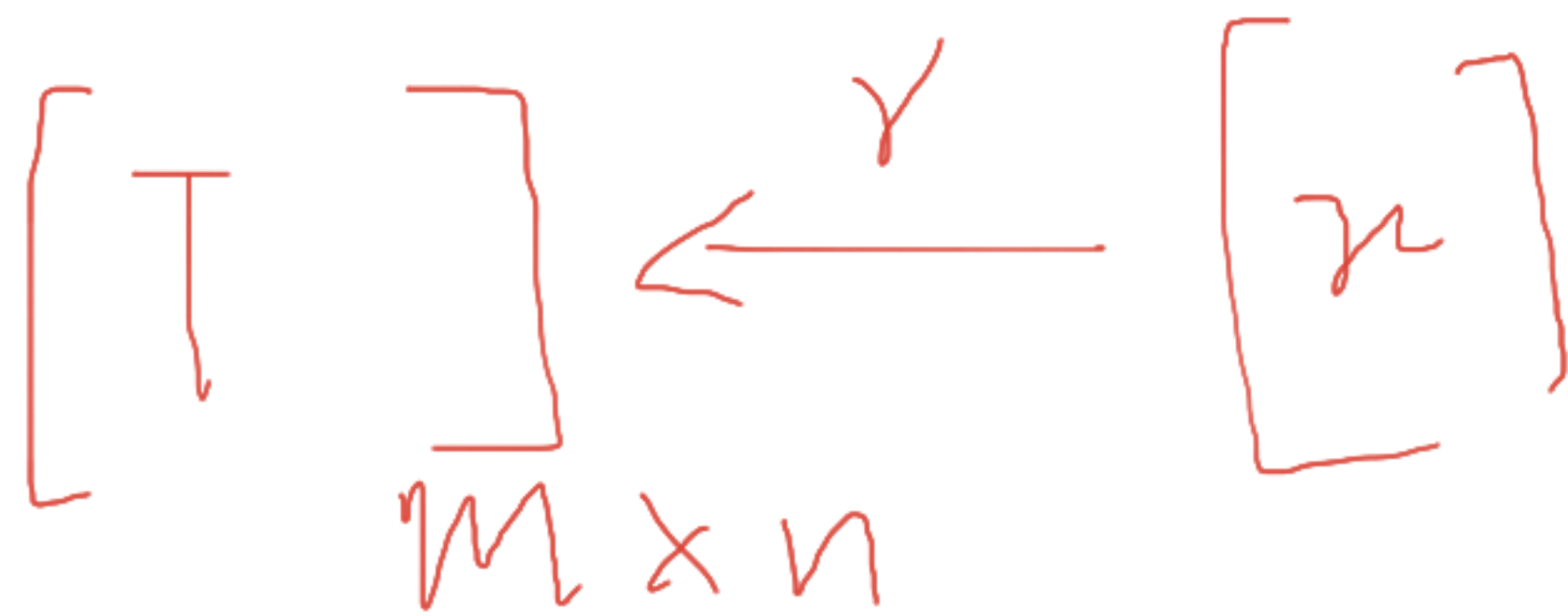
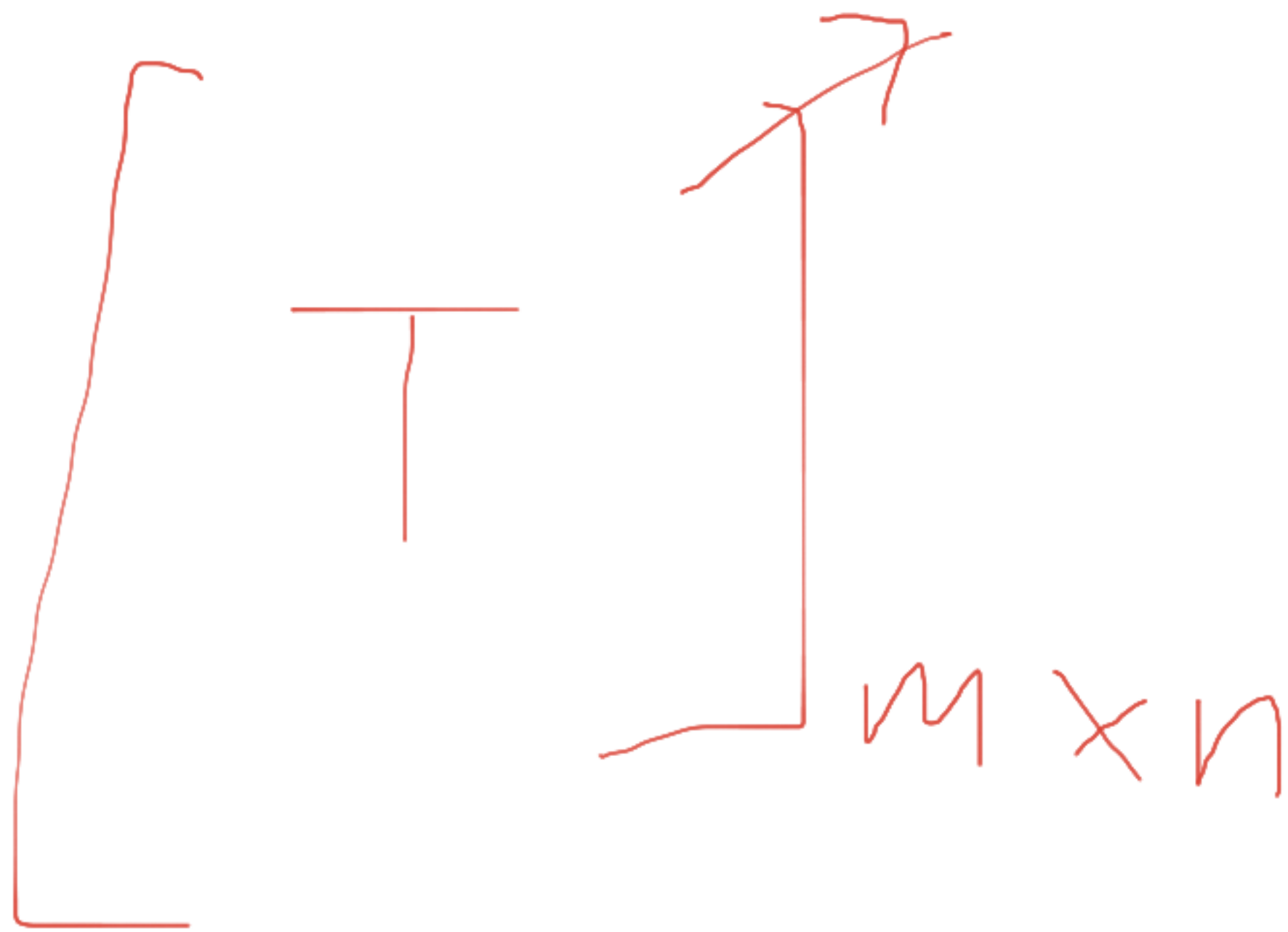


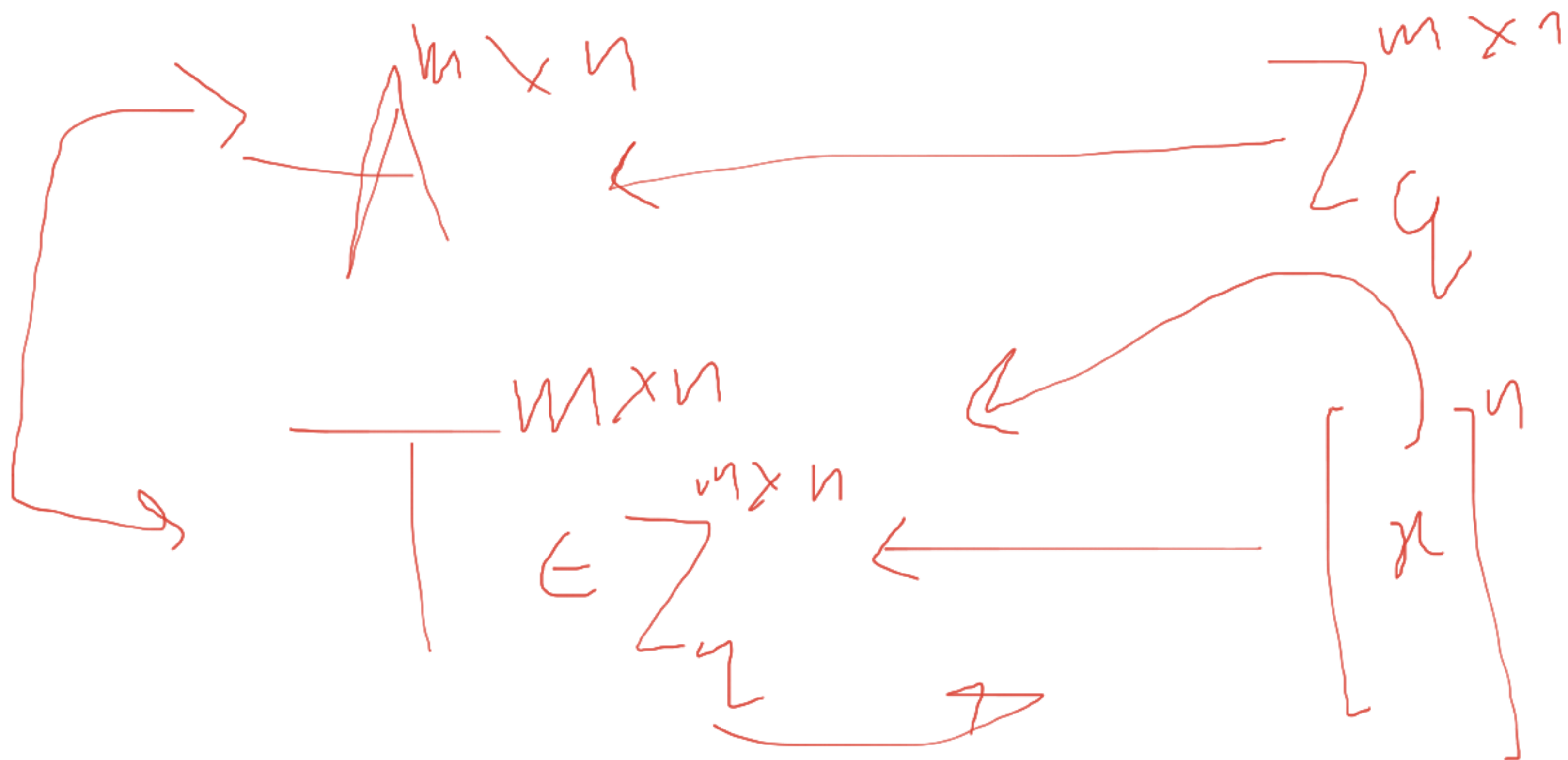
$vk =$    $\rightarrow$  pub  
 $sk =$    $\rightarrow$  secret  $\begin{bmatrix} A \\ T \end{bmatrix}$





$$\mu + \eta = 0$$







A  $x = f(m)$

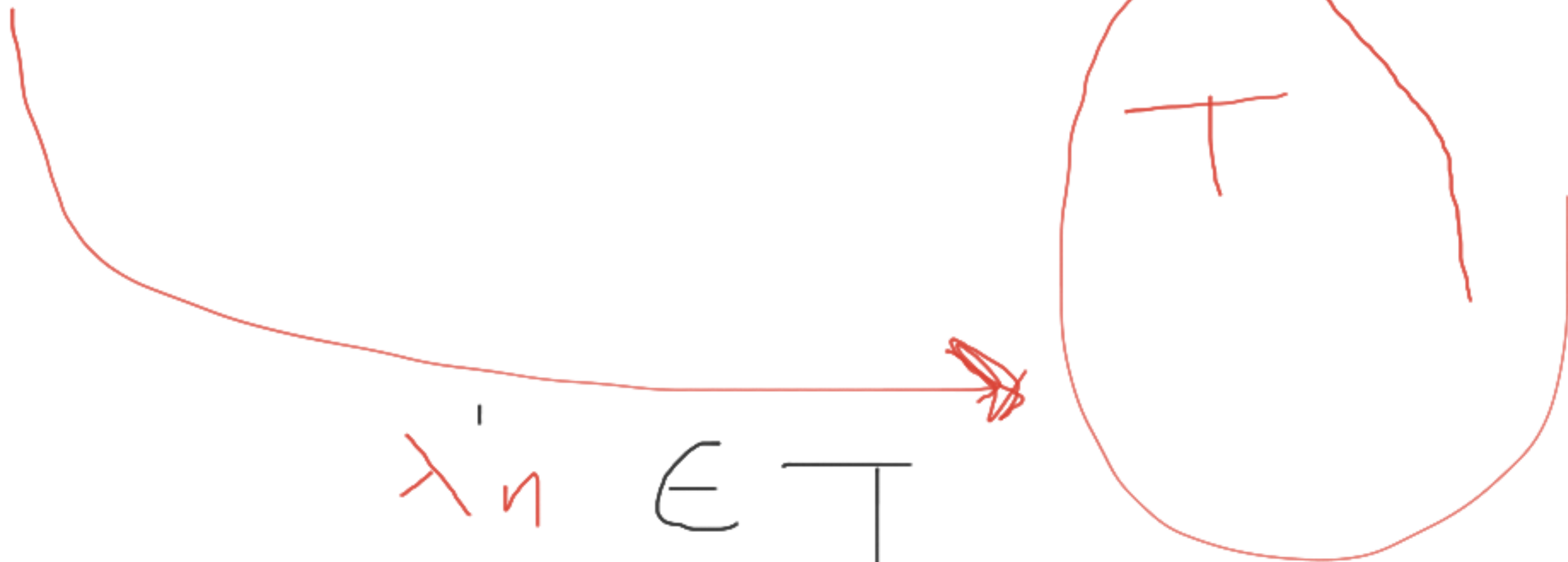
↓

So  $h$

A  $\circ x?$

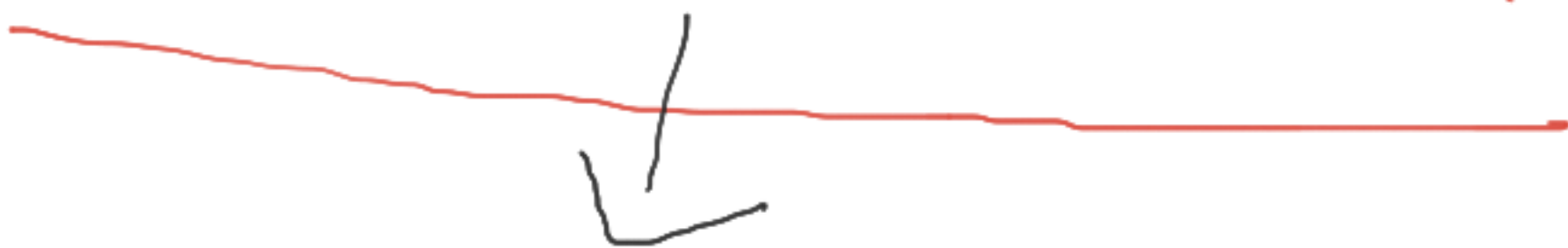
$= f'(m)$

~~A~~ =  $F(m)$



~~$x_{1,1}$~~

$x_{11} \in T$



$x_{1,1}$

$x_{11-r} \xrightarrow{10} \delta_1 \leftarrow 20$

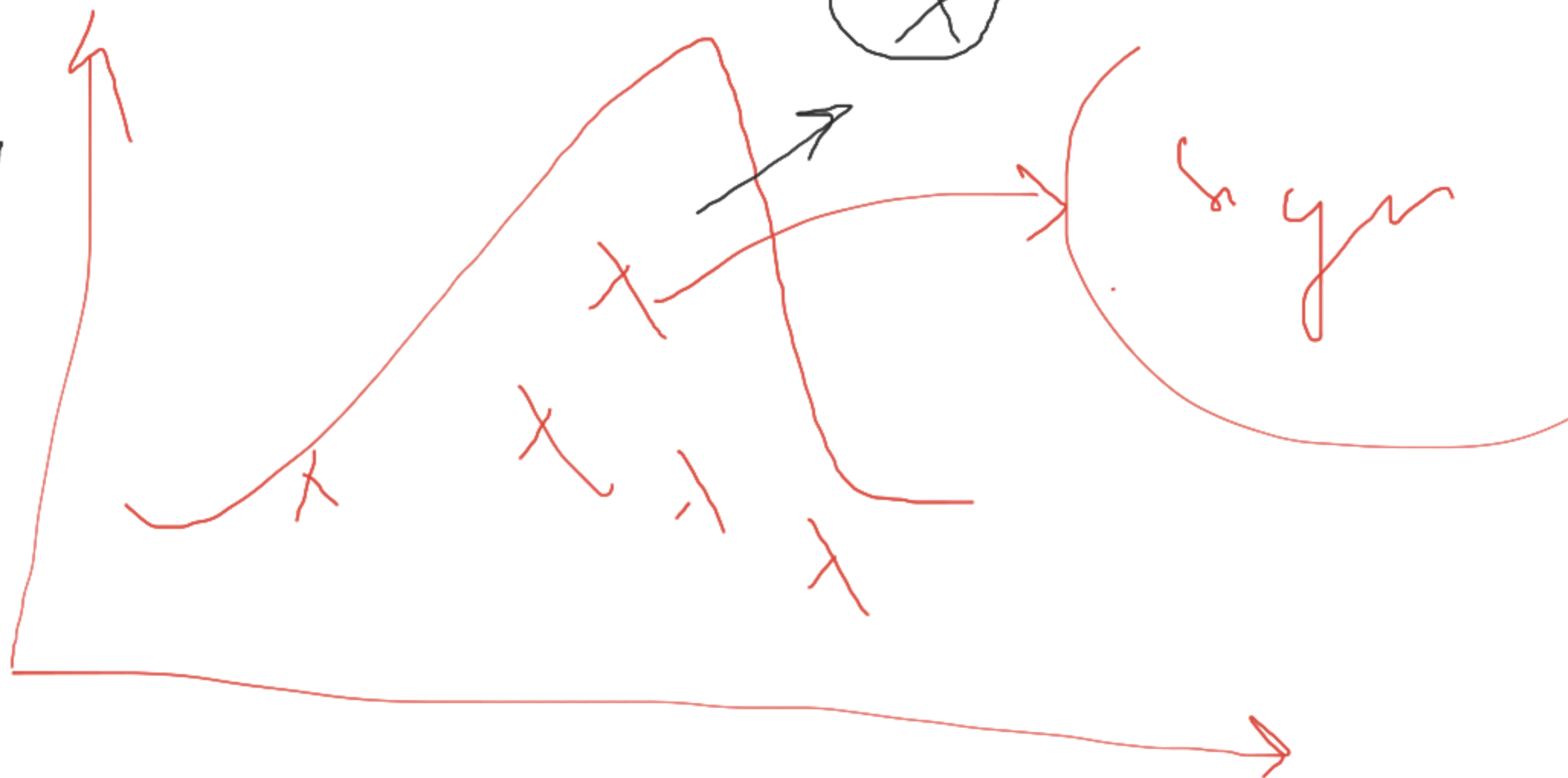
$\delta$

$t=1 \rightarrow \mu_1$

$t=2 \rightarrow \mu_2$

$S$   
 $\mu_2$   
 $\downarrow$

$\sigma_s$

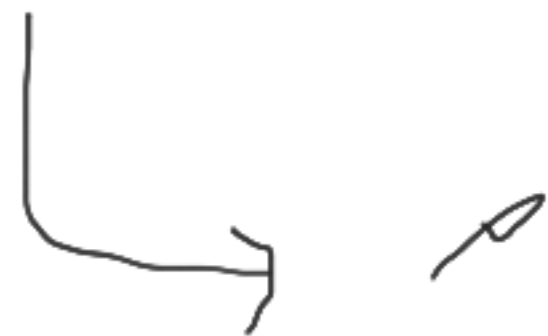


Verify  $(A, m, \lambda)$

$$\underline{A\lambda} = f(m)$$



$$A \underline{\lambda} = f(m)$$



1-✓

0-x