Ex. (Σ-protocol for Pedersen Commitment).

Prover and Verifier knows g, h and $y = g^x h^r$ ($= Com(x)$).

However, only Prover knows x and r.

i) [announcement]

- choose $s_1, s_2 \xleftarrow{\$} \mathbb{Z}_q^*$.
- compute $a = g^{s_1} h^{s_2}$ and sends a to Verifier.

ii) [challenge]

- choose $c \xleftarrow{\$} \mathbb{Z}_q^*$ and send c to Prover.

iii) [response]

- compute $r_1 = xc + s_1$ and $r_2 = rc + s_2$.
- send r_1 and r_2 to Verifier

iv) [verification]

- if $y^c a = g^{r_1} h^{r_2}$, then Verifier accepts.
  otherwise, Verifier rejects.

$$y^c a = (g^x h^r)^c \cdot g^{s_1} h^{s_2} = g^{xc+s_1} \cdot h^{rc+s_2} = g^{r_1} \cdot h^{r_2}$$

Ex. Prover and Verifier knows g, h, $y_1 = g^x h^{r_1}$ ($\to Com(x)$) and $y_2 = g^y h^{r_2}$ ($\to Com(y)$), $\alpha, \beta \in \mathbb{Z}_q$.

Prover proves the knowledge of x and y s.t. $y = \alpha x + \beta$

$\rightsquigarrow$ This is equivalent to proving knowledge of x s.t. $y_1 = Com(x) \wedge y_2 = y_1^{\alpha} \cdot g^{\beta}$.

use the above example.

i) [announcement]

- choose $s_1, s_2 \xleftarrow{\$} \mathbb{Z}_q^*$.
- compute $a = g^{s_1} h^{s_2}$ and sends a to verifier.

ii) [challenge]

iii) [response]

- compute $R_1 = cy + s_1$ and $R_2 = c\alpha r_1 + s_2$.

iv) [verification]

- if $y_1^{c\alpha} \cdot a \cdot g^{\beta c} = g^{R_1} h^{R_2}$, then Verifier accepts.
  otherwise, Verifier rejects.

$$g^{R_1} h^{R_2} = g^{cy+s_1} \cdot h^{c\alpha r_1 + s_2} = g^{s_1} \cdot h^{s_2} \cdot g^{c(\alpha x + \beta)} \cdot h^{c\alpha r_1} = a \cdot g^{c\alpha x} \cdot g^{c\beta} \cdot h^{c\alpha r_1}$$

$$= a \cdot (g^x \cdot h^{r_1})^{c\alpha} \cdot g^{c\beta} = a \cdot y_1^{c\alpha} \cdot g^{c\beta}$$