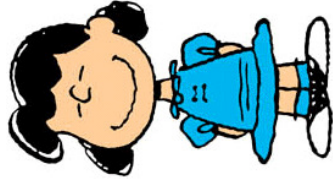


pk



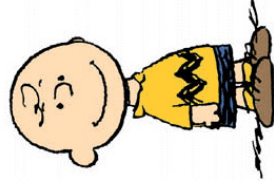
$$\beta \xleftarrow{u} \mathcal{B}$$

$$\begin{array}{c} \xrightarrow{\alpha_1, \alpha_2} \\ \xrightarrow{\beta} \\ \xrightarrow{\gamma_1, \gamma_2} \end{array}$$

Halt if $\mathcal{V}_1(\text{pk}, \alpha_1, \beta, \gamma_1) = 0$

Halt if $\mathcal{V}_2(\text{pk}, \alpha_2, \beta, \gamma_2) = 0$

sk₁, sk₂



$$\alpha_1 \leftarrow \mathcal{P}_1(\text{sk}_1)$$

$$\alpha_2 \leftarrow \mathcal{P}_2(\text{sk}_2)$$

$$\gamma_1 \leftarrow \mathcal{P}_1(\text{sk}_1, \beta)$$

$$\gamma_2 \leftarrow \mathcal{P}_2(\text{sk}_2, \beta)$$