pk

$\beta \leftarrow_u \mathcal{B}$

Halt if $\beta_1 + \beta_2 \neq \beta$

Halt if $\mathcal{V}_1(\mathsf{pk}, \alpha_1, \beta_1, \gamma_1) = 0$

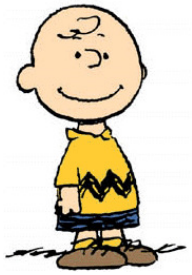
Halt if $\mathcal{V}_2(\mathsf{pk}, \alpha_2, \beta_2, \gamma_2) = 0$

α_1, α_2

β

$\beta_1, \beta_2, \gamma_1, \gamma_2$

$\mathsf{sk}_1 \vee \mathsf{sk}_2$



$\alpha_i \leftarrow \mathcal{P}_i(\mathsf{sk}_i)$

$(\alpha_j, \beta_j, \gamma_j) \leftarrow \mathcal{S}_j(\mathsf{pk})$

$\beta_i \leftarrow \beta - \beta_j$

$\gamma_i \leftarrow \mathcal{P}_i(\mathsf{sk}_i, \beta_i)$