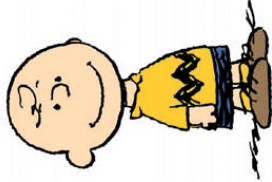
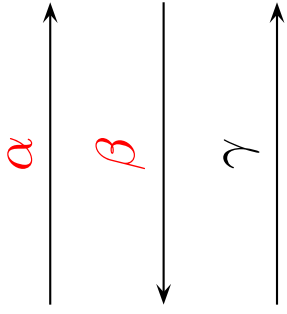


$$\alpha \leftarrow \mathcal{R} \qquad \beta \leftarrow \mathcal{B}$$



$$\mathcal{V}_{pk}(\alpha, \beta, \gamma)$$

Sigma protocols are

$\Rightarrow$  interactive

$\Rightarrow$  non-transferrable

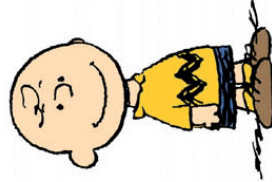
and cannot be linked to

$\Rightarrow$  particular messages

$$\alpha \leftarrow \mathcal{R}$$



$$\xrightarrow{m} s = (\alpha, \beta, \gamma)$$



$$\mathcal{V}_{pk}(\alpha, \beta, \gamma) \wedge h(m, \alpha) \stackrel{?}{=} \beta$$

If  $\beta \leftarrow h(m, \alpha)$  then

$\Rightarrow$  the signer cannot cheat

$\Rightarrow$  the protocol is non-interactive

$\Rightarrow$  the protocol is transferable