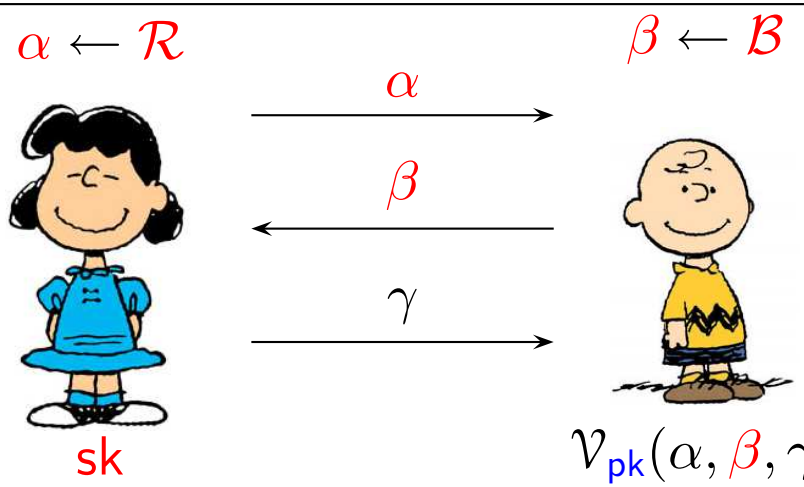


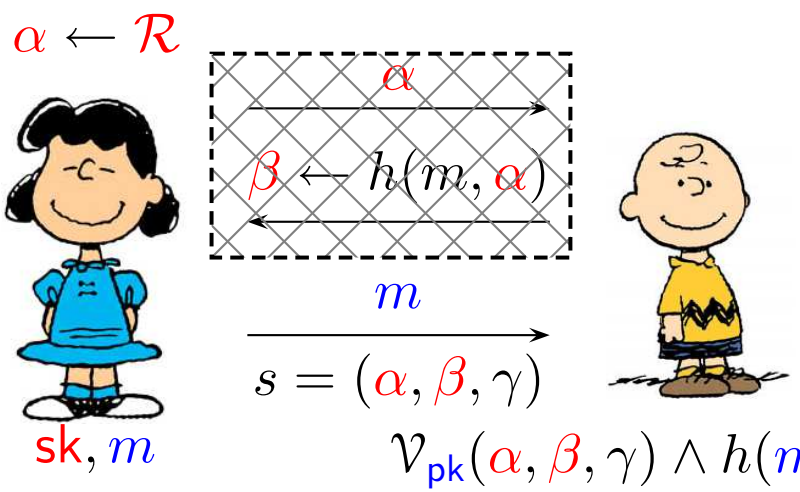
Sigma protocols are

$\Rightarrow$ interactive

$\Rightarrow$ non-transferrable

and cannot be linked to

$\Rightarrow$ particular messages



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

$\Rightarrow$ the signer cannot cheat

$\Rightarrow$ the protocol is non-interactive

$\Rightarrow$ the protocol is transferable