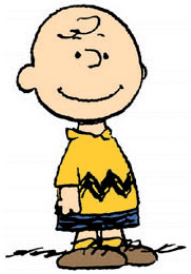
$$\boxed{\mathrm{ZK}_x[(x, w) \in R]}$$



x

x, w

$\beta \leftarrow_u \mathcal{B}$

$(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\beta)$

pk

c

α

d

γ

$\mathsf{pk} \leftarrow \mathsf{Gen}$

$\alpha \leftarrow \mathcal{P}_w$

$\beta \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d)$

$\gamma \leftarrow \mathcal{P}_w(\alpha, \beta)$

$\mathsf{Ver}_x(\alpha, \beta, \gamma)$