



Prover (x)



Verifier (\mathbb{G}, q, g, y)

$$k \leftarrow \mathbb{Z}_q; I := g^k \xrightarrow{I}$$

$$\xleftarrow{r} r \leftarrow \mathbb{Z}_q$$

$$s := [rx + k \bmod q] \xrightarrow{s} g^s \cdot y^{-r} \stackrel{?}{=} I$$