Tikz Test

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

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

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

$s := [rx + k \mod q] \xrightarrow{\quad s \quad}$

$g^s \cdot y^{-r} \stackrel{?}{=} I$