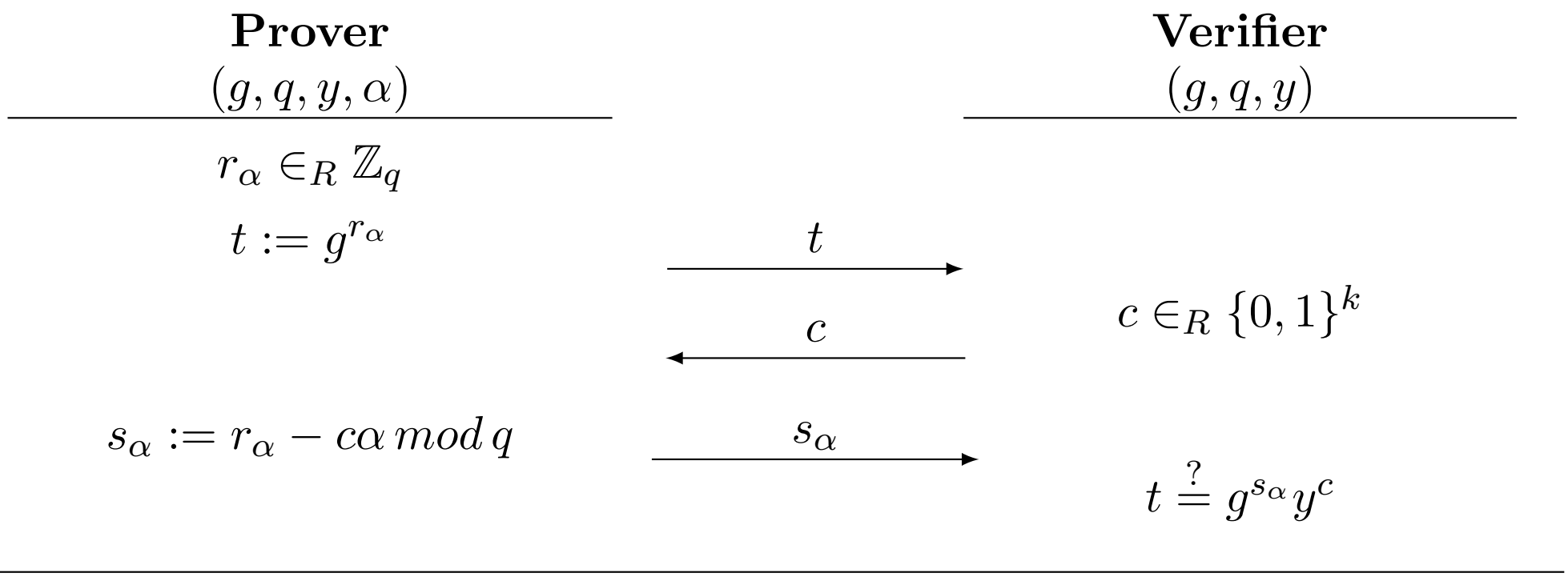
Prover
Verifier
(g, q, y, α)
(g, q, y)
$r_\alpha \in_R \mathbb{Z}_q$
$t := g^{r_\alpha}$
t
c
$c \in_R \{0,1\}^k$
$s_\alpha := r_\alpha - c\alpha \, mod \, q$
s_α
$t \stackrel{?}{=} g^{s_\alpha} y^c$