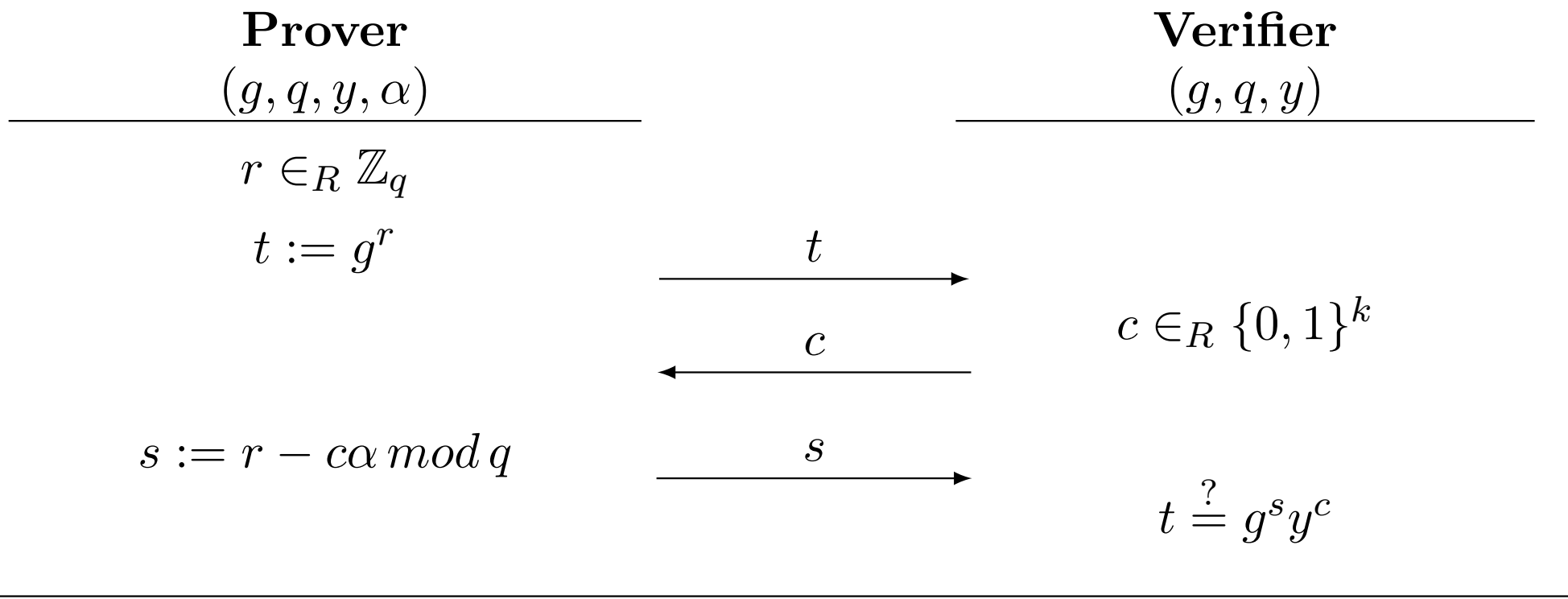
Prover
(g, q, y, α)
Verifier
(g, q, y)
$r \in_R \mathbb{Z}_q$
$t := g^r$
t
c
$c \in_R \{0,1\}^k$
$s := r - c\alpha \, mod \, q$
s
$t \stackrel{?}{=} g^s y^c$