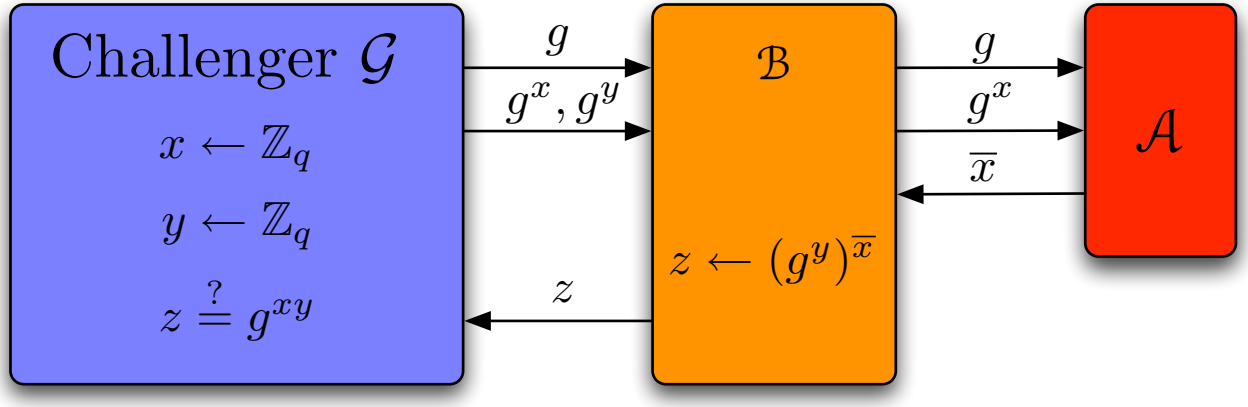
Challenger $\mathcal{G}$
$x \leftarrow \mathbb{Z}_q$
$y \leftarrow \mathbb{Z}_q$
$z \stackrel{?}{=} g^{xy}$
g
g^x, g^y
z
$\mathcal{B}$
$z \leftarrow (g^y)^{\overline{x}}$
g
g^x
$\overline{x}$
$\mathcal{A}$