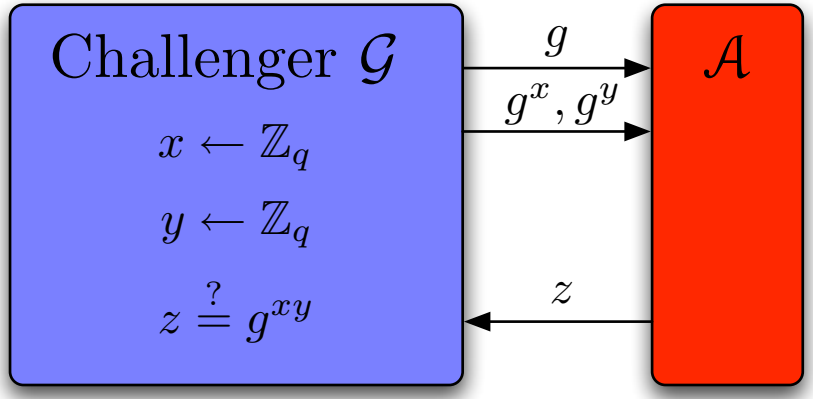

$\mathcal{G}^{\mathcal{A}}$

$$\left[\begin{array}{l} x \leftarrow \mathbb{Z}_q \\ y \leftarrow \mathbb{Z}_q \\ z \leftarrow \mathcal{A}(g, g^x, g^y) \\ \textbf{return } [g^{xy} \stackrel{?}{=} z] \end{array}\right.$$