

Challenger \mathcal{G}

$$x \leftarrow \mathbb{Z}_q$$

$$y \leftarrow \mathbb{Z}_q$$

$$z \stackrel{?}{=} g^{xy}$$

g

g^x, g^y

\mathcal{B}

g

g^x

\bar{x}

\mathcal{A}

$$z \leftarrow (g^y)^{\bar{x}}$$

z