

Challenger  $\mathcal{G}$

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

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

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

$g$

$g^x, g^y$

$\mathcal{A}$

$z$

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

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

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

$$z \leftarrow \mathcal{A}(g, g^x, g^y)$$

$$\mathbf{return} [g^{xy} \stackrel{?}{=} z]$$