

Challenger  $\mathcal{G}$

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

$$x \stackrel{?}{=} \bar{x}$$

$g$

$g^x$

$\bar{x}$

$\mathcal{A}$

