

Challenger

Choose bad x

$y \leftarrow \mathbb{Z}_q$

g

g^{x+y}

x_*

\mathcal{A}

