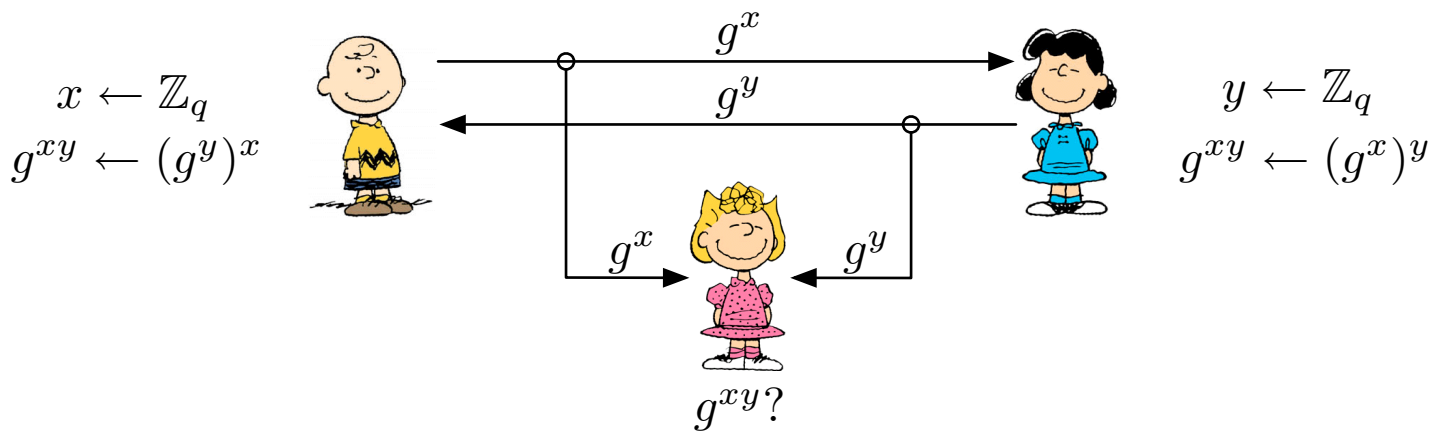
$x \leftarrow \mathbb{Z}_q$
$g^{xy} \leftarrow (g^y)^x$
g^x
g^y
$y \leftarrow \mathbb{Z}_q$
$g^{xy} \leftarrow (g^x)^y$
g^x
g^y
g^{xy}?