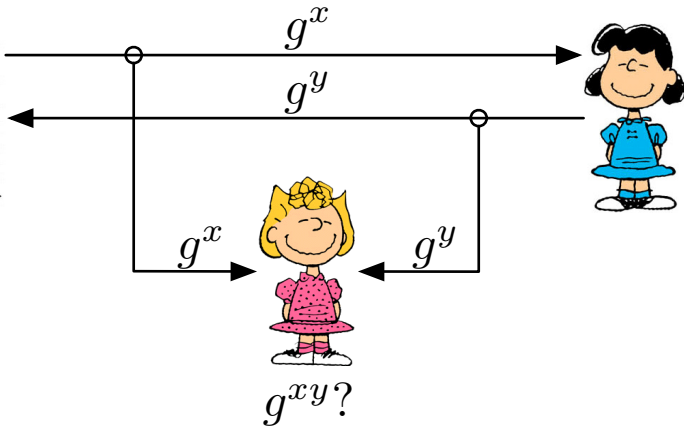


$$x \leftarrow \mathbb{Z}_q$$

$$g^{xy} \leftarrow (g^y)^x$$



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

$$g^{xy} \leftarrow (g^x)^y$$