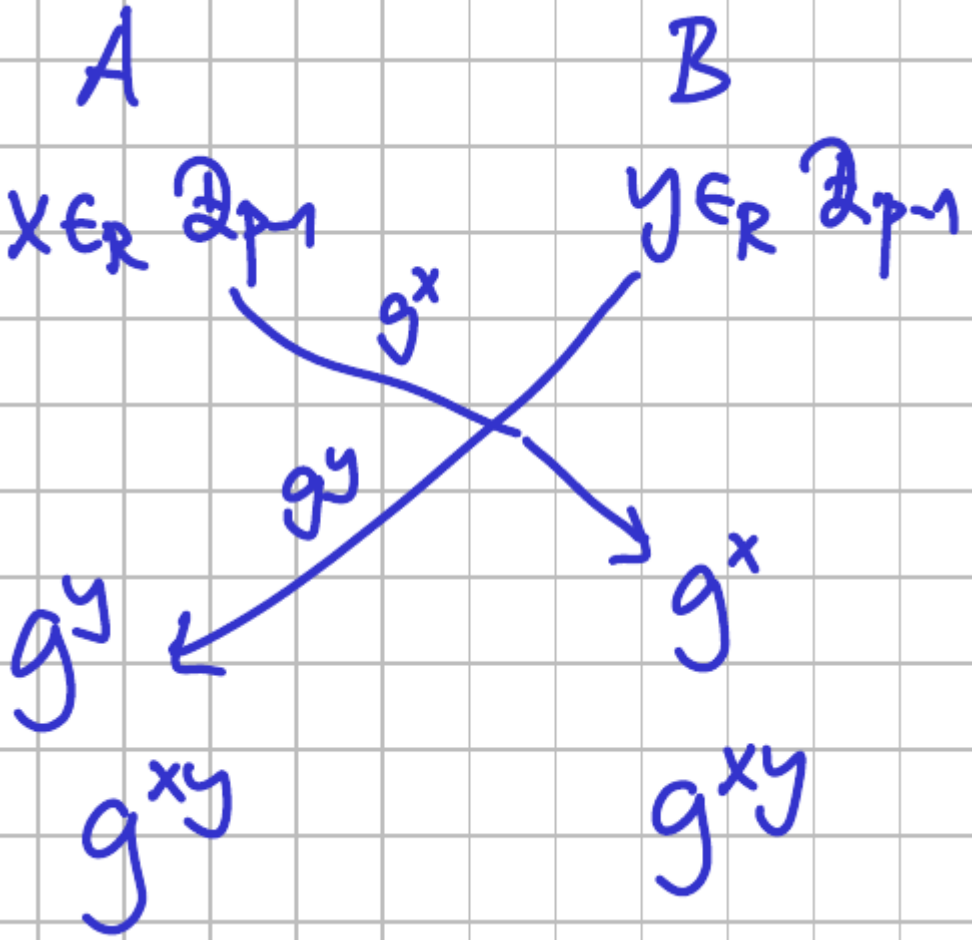
A
B
$x \in_R \mathbb{Z}_{p-1}$
$y \in_R \mathbb{Z}_{p-1}$
g^x
g^y
g^y
g^x
g^{xy}
g^{xy}