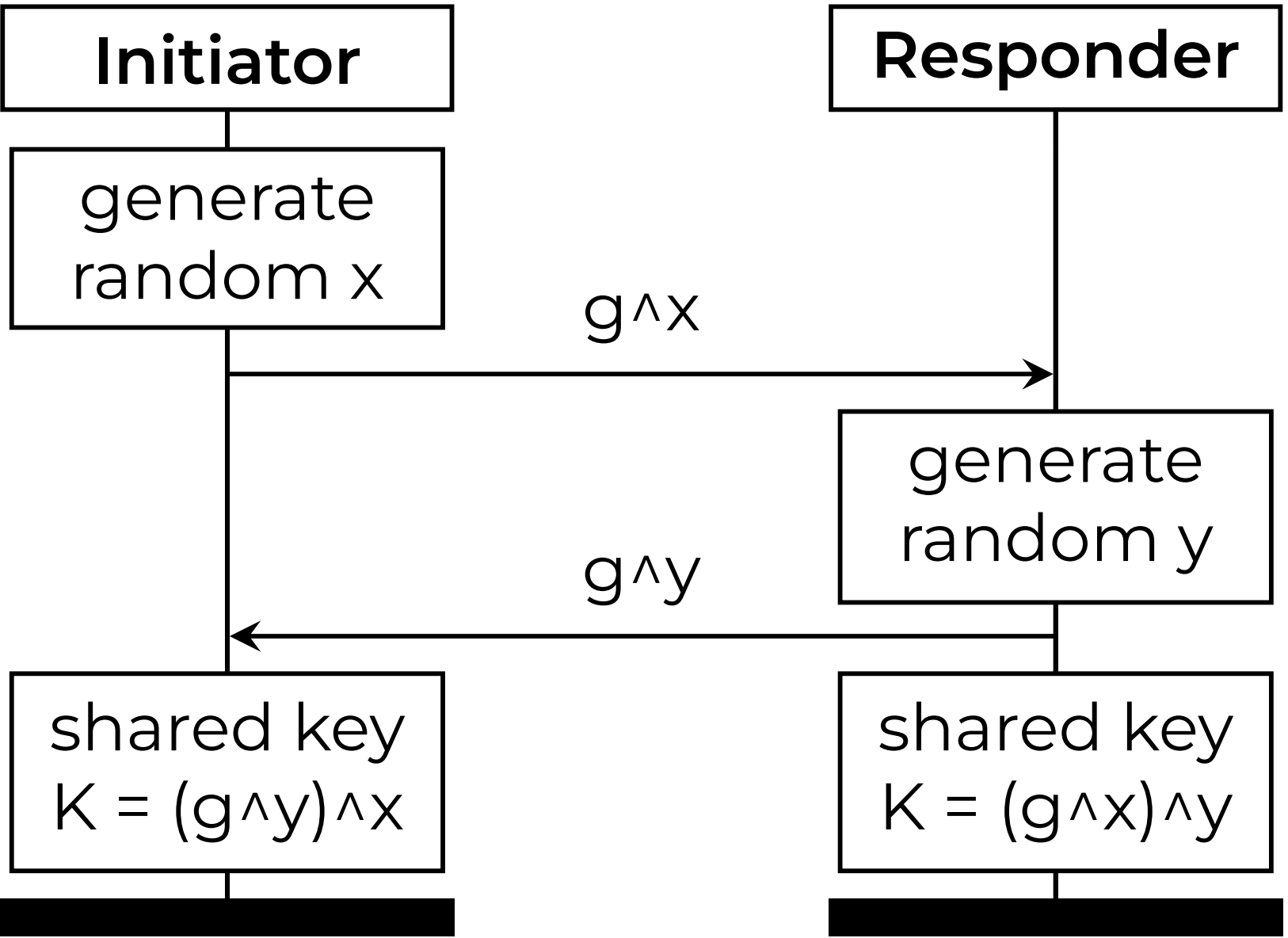
Initiator
Responder
generate
random x
g^x
generate
random y
g^y
shared key
K = (g^y)^x
shared key
K = (g^x)^y