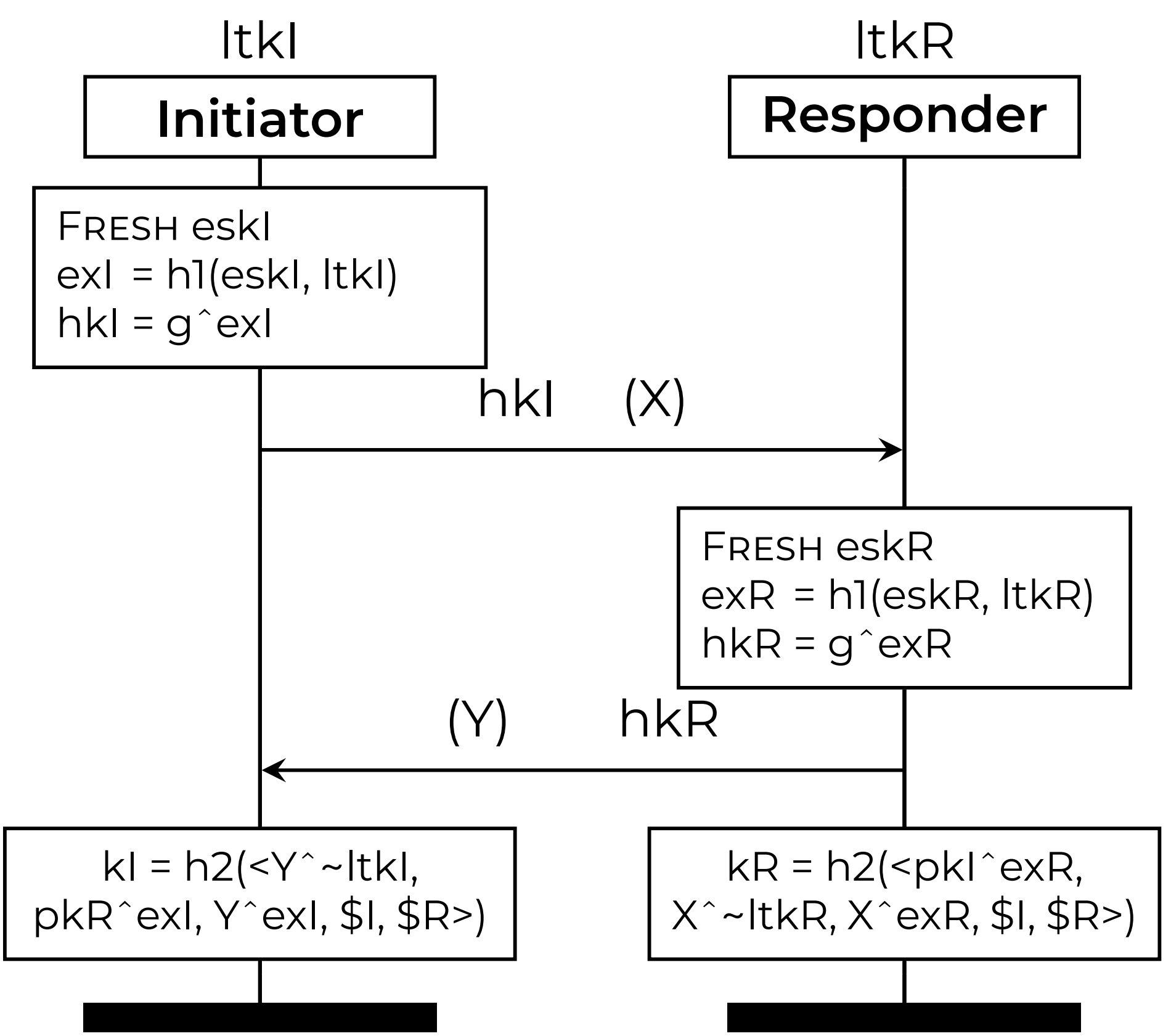
ltkI
ltkR
Initiator
Responder
Fresh eskI
exI = h1(eskI, ltkI)
hkI = g^exI
hkI (X)
Fresh eskR
exR = h1(eskR, ltkR)
hkR = g^exR
(Y) hkR
kI = h2(<Y^~ltkI,
pkR^exI, Y^exI, $I, $R>)
kR = h2(<pkI^exR,
X^~ltkR, X^exR, $I, $R>)