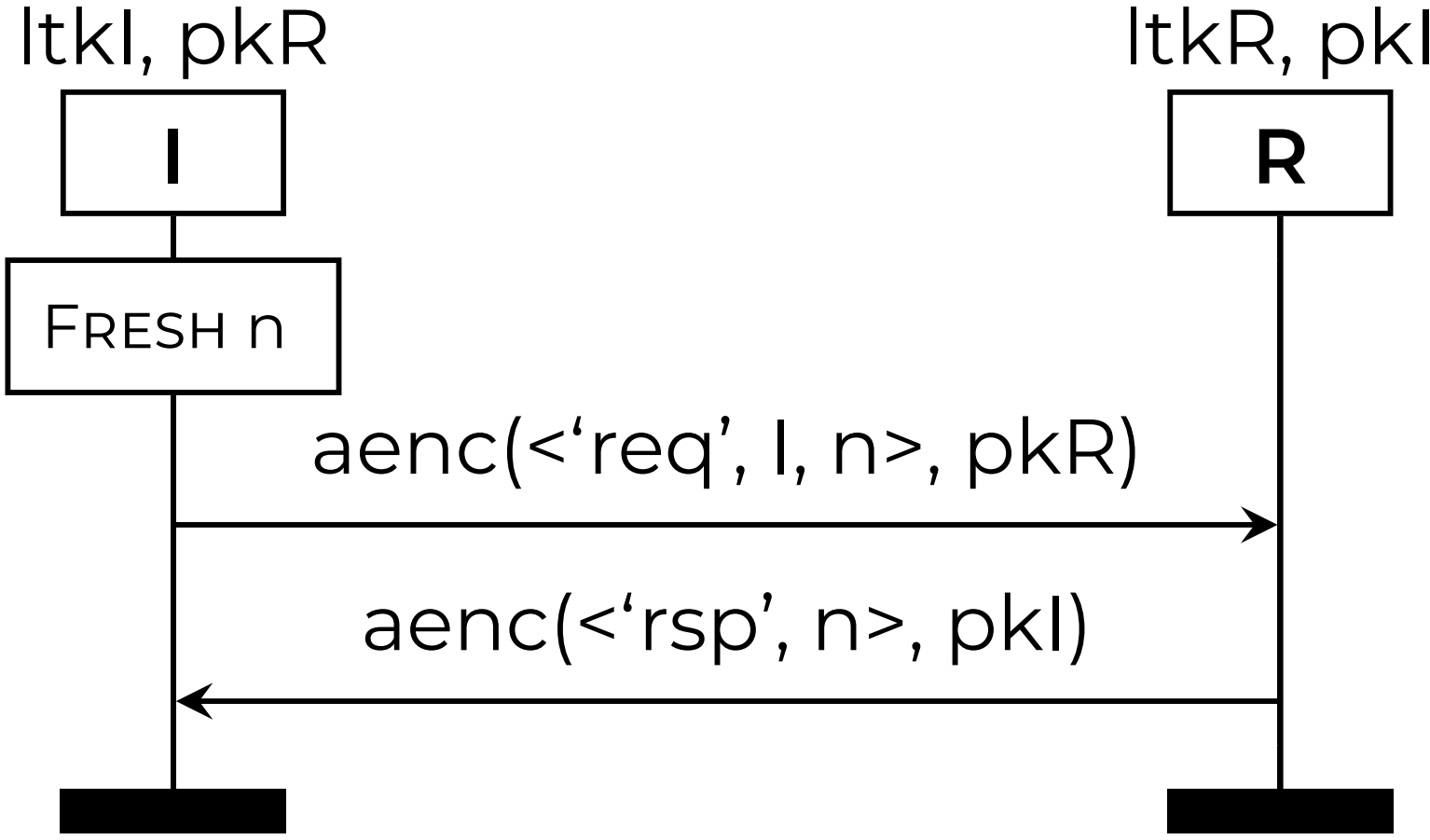
ltkI, pkR
ltkR, pkI
I
R
Fresh n
aenc(<‘req’, I, n>, pkR)
aenc(<‘rsp’, n>, pkI)