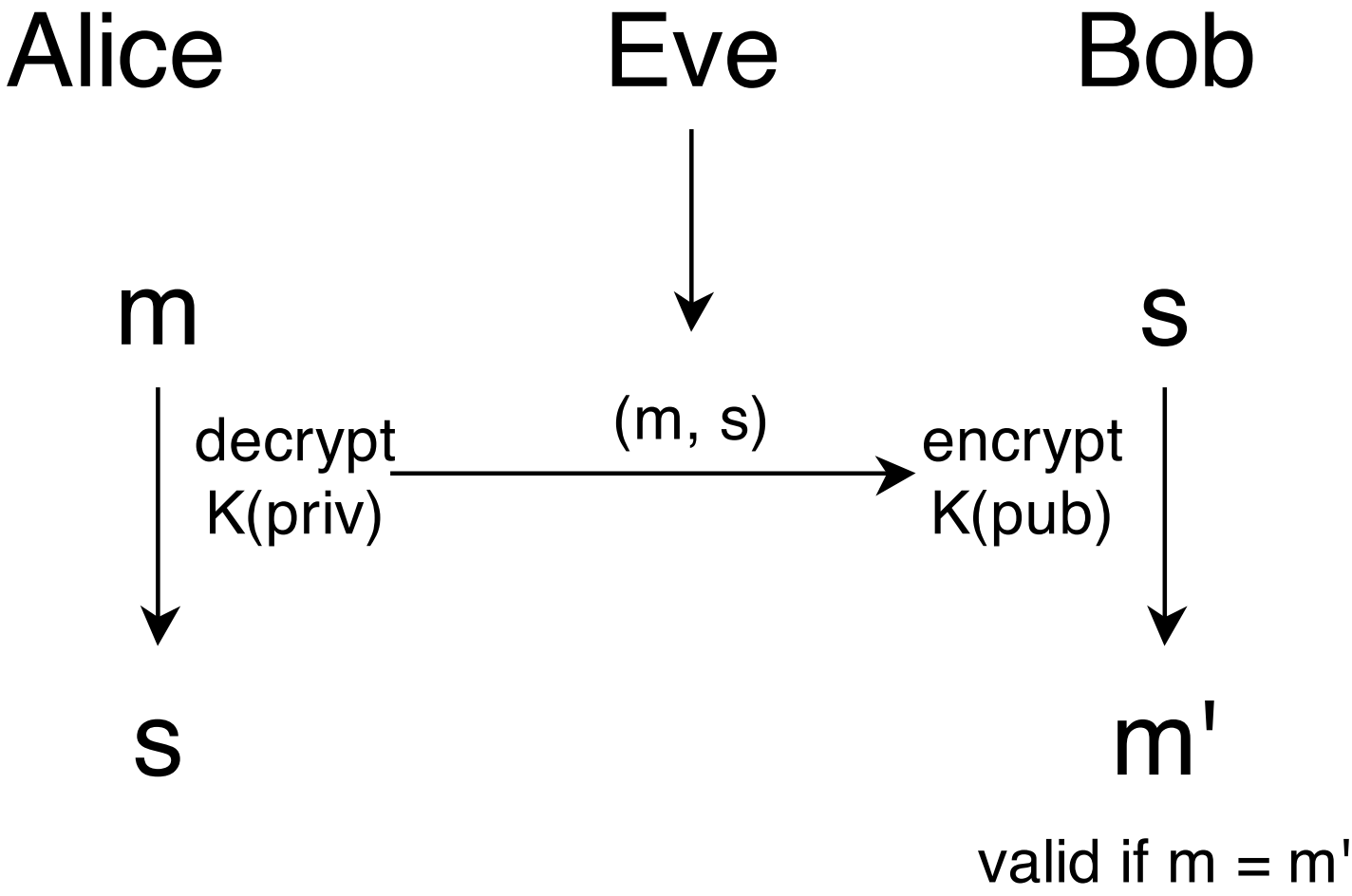
Alice
Eve
Bob
m
s
decrypt
K(priv)
(m, s)
encrypt
K(pub)
s
m'
valid if m = m'