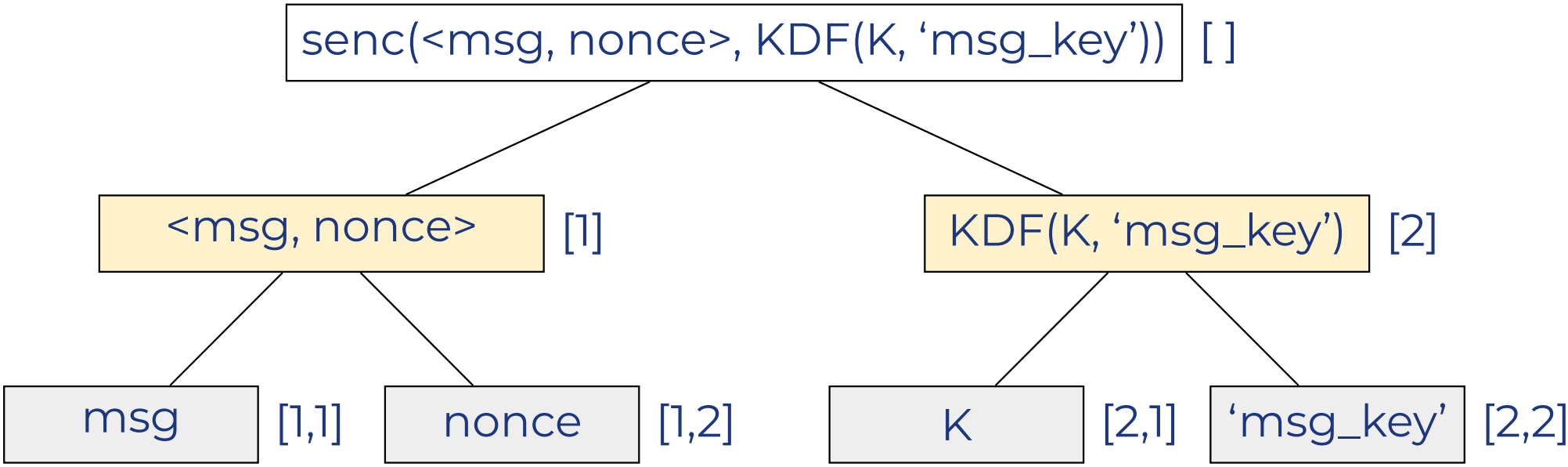
senc(<msg, nonce>, KDF(K, ‘msg_key’))
[ ]
<msg, nonce>
[1]
KDF(K, ‘msg_key’)
[2]
msg
[1,1]
nonce
[1,2]
K
[2,1]
‘msg_key’
[2,2]