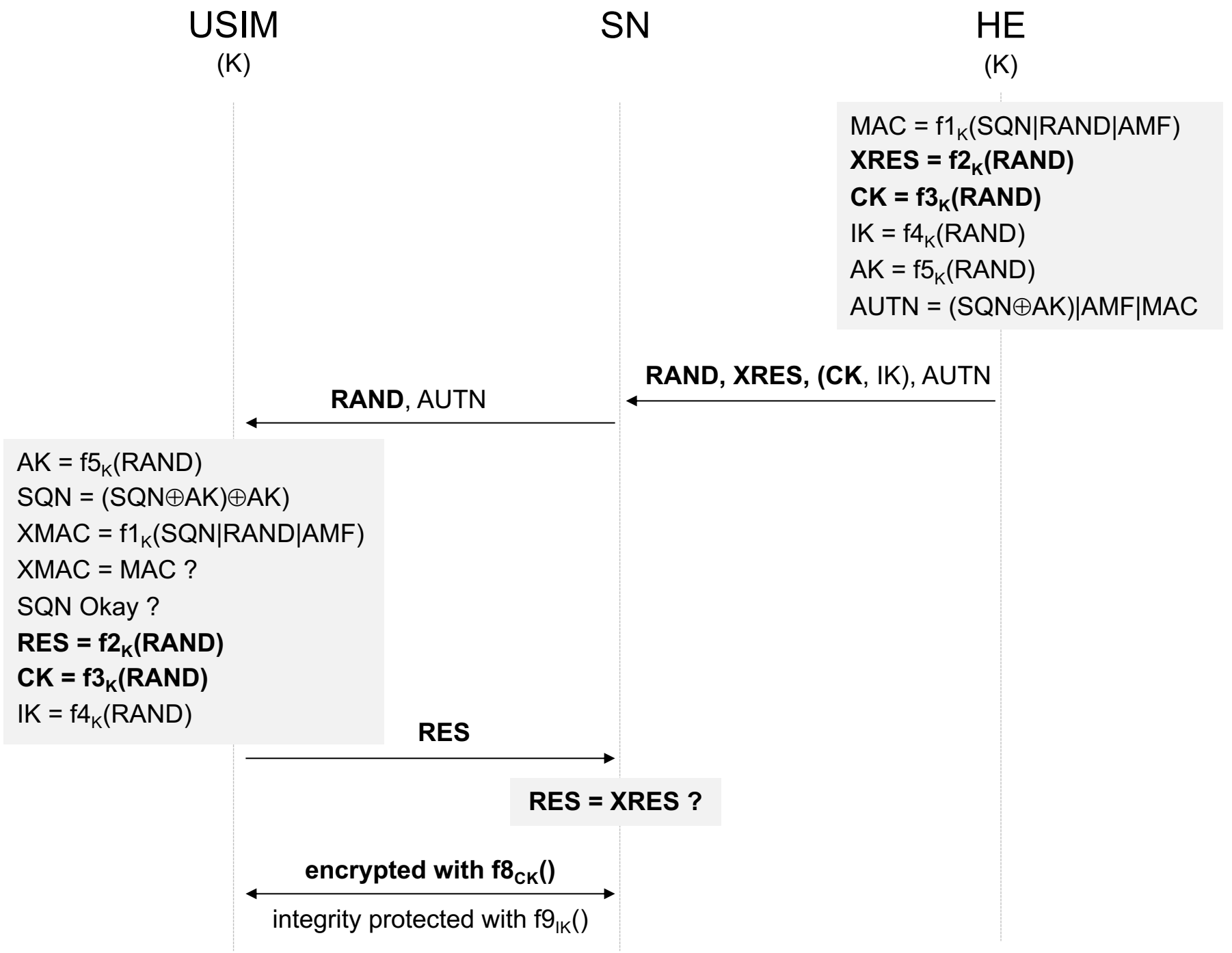
USIM
(K)
SN
HE
(K)
MAC = f1K(SQN|RAND|AMF)
XRES = f2K(RAND)
CK = f3K(RAND)
IK = f4K(RAND)
AK = f5K(RAND)
AUTN = (SQN⊕AK)|AMF|MAC
RAND, XRES, (CK, IK), AUTN
RAND, AUTN
AK = f5K(RAND)
SQN = (SQN⊕AK)⊕AK)
XMAC = f1K(SQN|RAND|AMF)
XMAC = MAC ?
SQN Okay ?
RES = f2K(RAND)
CK = f3K(RAND)
IK = f4K(RAND)
RES
RES = XRES ?
encrypted with f8CK()
integrity protected with f9IK()