$IMSI, \mathcal{K}, SQN$ $S = \{s = \langle i, \mathcal{K}, SQN \rangle | \forall i \in I\}$

SIM   **SN**   **HN**

SIM ← IMSI inquiry ← SN

SIM → IMSI inquiry Response ($PMSI$) → SN

SN → AV request ($IMSI$) → HN

$i, \mathcal{K}, SQN, \kappa, p, p' \leftarrow s \in S$ where $s_i = IMSI$

$RAND \leftarrow \{0,1\}^{128}$

$MAC \leftarrow f_1(\mathcal{K}, SQN, AMF, RAND)$

$XRES \leftarrow f_2(\mathcal{K}, RAND)$

$CK \leftarrow f_3(\mathcal{K}, RAND) \quad IK \leftarrow f_4(\mathcal{K}, RAND) \quad AK \leftarrow f_5(\mathcal{K}, RAND)$

$K_{ASME} \leftarrow KDF(CK, IK, SQN \oplus AK, SNID)$ (LTE only)

$AUTN \leftarrow \langle SQN \oplus AK, AMF, MAC \rangle$

update $s_{SQN} \leftarrow SQN + 1$

BOX A

$RAND, AUTN, XRES, CK, IK$ (UMTS)

$RAND, AUTN, XRES, K_{ASME}$ (LTE)

SIM ← authentication request ($RAND, AUTN$) ← SN

$AK \leftarrow f_5(\mathcal{K}, RAND)$

$XSQN \leftarrow AK \oplus AUTN_{SQN \oplus AK}$

$XMAC \leftarrow f_1(\mathcal{K}, XSQN, AUTN_{AMF}, RAND)$

verify $XMAC = AUTN_{MAC}$

verify $SQN \leq XSQN \leq (SQN + range)$

update $SQN \leftarrow SQN + 1$

$SRES \leftarrow f_2(\mathcal{K}, RAND) \qquad CK \leftarrow f_3(\mathcal{K}, RAND)$

$IK \leftarrow f_4(\mathcal{K}, RAND) \qquad AK \leftarrow f_5(\mathcal{K}, RAND)$

$K_{ASME} \leftarrow KDF(CK, IK, SQN \oplus AK, SNID)$ (LTE only)

BOX B

SIM → authentication response ($SRES$) → SN

verify $SRES = XRES$