$PMSI, P_{new}, \kappa, \mathcal{K}, SQN$ $S = \{s = \langle i, \mathcal{K}, SQN, \kappa, p, p' \rangle | \forall i \in I\}$

SIM	SN	HN

SIM ← IMSI inquiry — SN

update $PMSI \leftarrow P_{new}$

SIM — IMSI Inquiry response ($PMSI$) → SN — AV Request ($PMSI$) → HN

$i, \mathcal{K}, SQN, \kappa, p, p' \leftarrow s \in S$ where $s_p = PMSI \lor s_{p'} = PMSI$
if $s_{p'} = PMSI$ then
         update $s_p \leftarrow s_{p'}$
         update $s_{p'} \leftarrow \{0,1\}^{34} \notin \{s_p, s_{p'} | \forall s \in S\}$
$RAND \leftarrow E_\kappa(u = (p', SQN))$

$MAC \leftarrow f_1(\mathcal{K}, SQN, AMF, RAND)$ BOX A
$XRES \leftarrow f_2(\mathcal{K}, RAND)$
$CK \leftarrow f_3(\mathcal{K}, RAND)$
$IK \leftarrow f_4(\mathcal{K}, RAND)$
$AK \leftarrow f_5(\mathcal{K}, RAND)$
$AUTN \leftarrow \langle SQN \oplus AK, AMF, MAC \rangle$
update $s_{SQN} \leftarrow SQN + 1$

SIM ← authentication request ($RAND, AUTN$) — SN ← $RAND, AUTN, XRES, CK, IK$ — HN

$AK \leftarrow f_5(\mathcal{K}, RAND)$ BOX B
$XSQN \leftarrow AK \oplus AUTN_{SQN \oplus AK}$
$XMAC \leftarrow f_1(\mathcal{K}, XSQN, AUTN_{AMF}, RAND)$
      verify $XMAC = AUTN_{MAC}$
      verify $SQN \leq XSQN \leq (SQN + range)$
update $SQN \leftarrow SQN + 1$
$SRES \leftarrow f_2(\mathcal{K}, RAND)$
$CK \leftarrow f_3(\mathcal{K}, RAND)$
$IK \leftarrow f_4(\mathcal{K}, RAND)$

$u \leftarrow E_\kappa^{-1}(RAND)$
    verify $XSQN = u_{SQN}$
update $P_{new} \leftarrow u_{p'}$

SIM — authentication response ($SRES$) → SN

verify $SRES = XRES$

SIM ←— encrypted with CK —→ SN
authenticity protected with IK