$\boldsymbol{PMSI, P_{new}, \kappa}, \mathcal{K}, SQN$

$$\mathrm{S} = \left\{ s = \langle i, \mathcal{K}, SQN, \boldsymbol{\kappa, p, p', \underline{p'', f_{p'}}} \rangle | \forall i \in I \right\}$$

SIM

SN

HN

IMSI Inquiry

~~update $PMSI \leftarrow P_{new}$~~

update $q \leftarrow P_{new}$

it is allowed to update $q \leftarrow PMSI$

IMSI Inquiry Response (q)

AV Request (q)

$i, \mathcal{K}, SQN, \kappa, p, p', \underline{p'', f_{p'}} \leftarrow s \in S$ where $s_p = q \vee s_{p'} = q \vee \underline{s_{p''} = q}$

~~if $s_{p'} = PMSI$ then~~

~~update $s_p \leftarrow s_{p'}$~~

~~update $s_{p'} \leftarrow \{0,1\}^{34} \notin \{ s_p, s_{p'} | \forall s \in S \}$~~

$\underline{p\_in\_RAND = \mathbf{choosep}(q, s_i, s_p, s_{p'}, s_{p''}, f_p)}$

$RAND \leftarrow E_\kappa \left(u = (\underline{p\_in\_RAND}, SQN) \right)$

BOX A

authentication request $(RAND, AUTN)$

$RAND, AUTN, XRES, CK, IK$

BOX B

$\underline{p\_in\_RAND} \leftarrow E_\kappa^{-1}(RAND)$

verify $XSQN = \underline{p\_in\_RAND_{SQN}}$

~~update $P_{new} \leftarrow u_{p'}$~~

update $PMSI \leftarrow P_{new}$

update $P_{new} \leftarrow u_{p\_in\_RAND}$

authentication response $(SRES)$

verify $SRES = XRES$

encrypted with CK

authenticity protected with IK

location update (q)

$\underline{i, \mathcal{K}, SQN, \kappa, p, p', p'', f_{p'} \leftarrow s \in S \text{ where } s_p = q \vee s_{p'} = q \vee s_{p''} = q}$

$\underline{forget\_flag, toggle\_flag = \mathbf{locupdate}(q, s_i, s_p, s_{p'}, s_{p''}, f_{p'})}$

$\underline{\text{if } forget\_flag = true \text{ then}}$

$\underline{\mathbf{forgetp}(s_i, s_p, s_{p'}, s_{p''})}$

$\underline{\text{if } flag\_toggle = true \text{ then}}$

$\underline{\mathbf{togglefp}(s_i)}$