

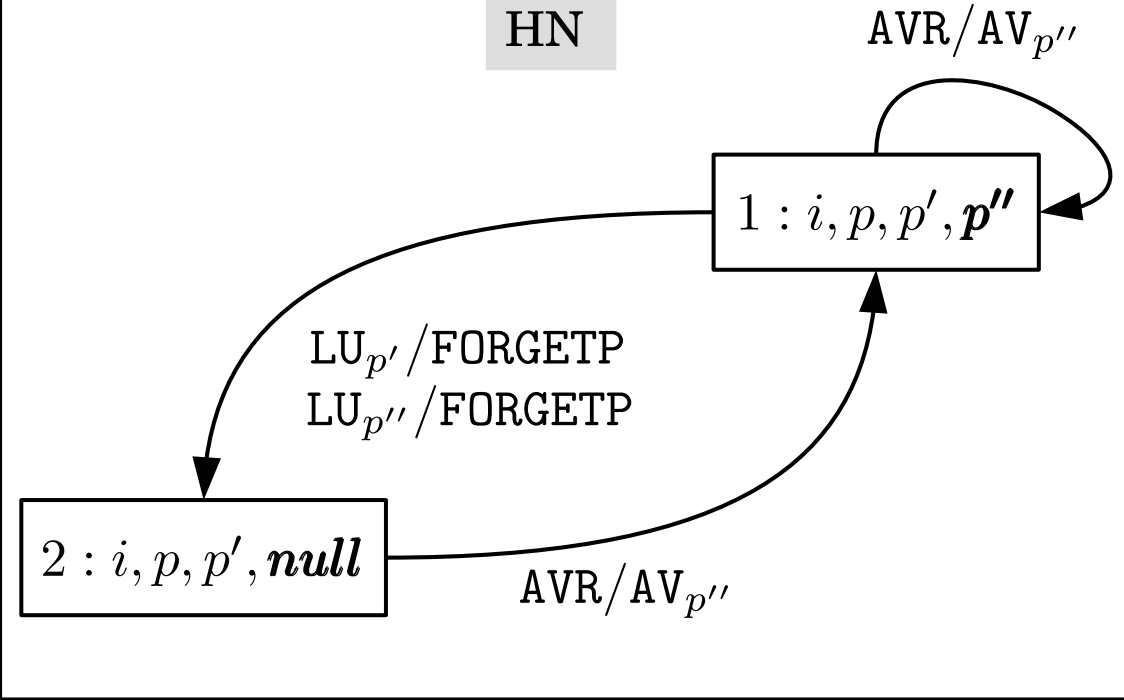
UE

$AKA(P_{new}, y) / \text{FORGETPMSI}$



Where $y \notin \{PMSI, P_{new}\}$

HN



$AVR = AV$ request has arrived using any of the identities i, p, p', p''

$AV_x = AV$ sent to SN with x in $RAND$

$LU_x =$ Location update for x has arrived

$AKA(x, y) =$ UE identified with x , the AKA is successful, y is the next pseudonym

$$\text{FORGETP} = \begin{cases} p \leftarrow p' \\ p' \leftarrow p'' \\ p'' \leftarrow null \end{cases}$$

$$\text{FORGETPMSI} = \begin{cases} PMSI \leftarrow P_{new} \\ P_{new} \leftarrow y \end{cases}$$