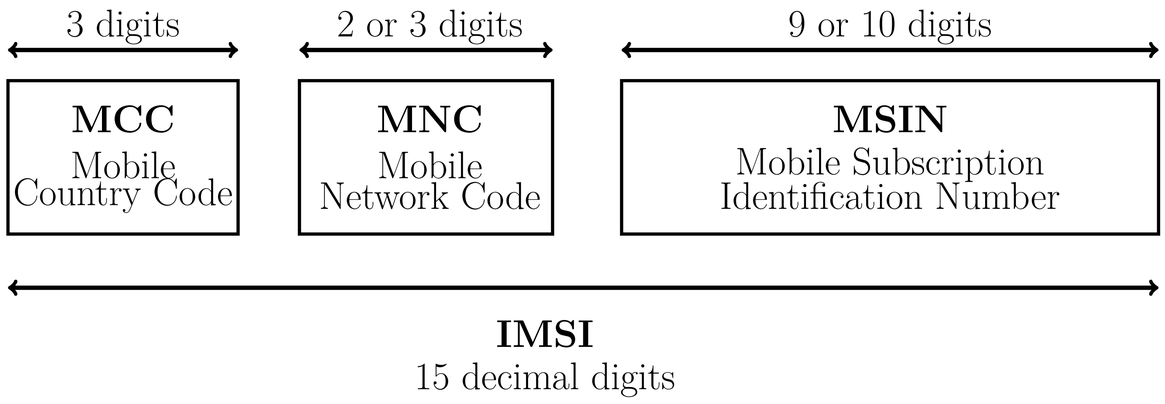
UNIVERSITY OF HELSINKI
Department of Computer Science

Mohsin Khan[1]
Philip Ginzboorg[2,3]
Valtteri Niemi[1]
[1]University of Helsinki
[2]Huawei Technologies, [3]Aalto University

IDENTITY PRIVACY IN 5G, DEFEATING DOWNGRADE ATTACK

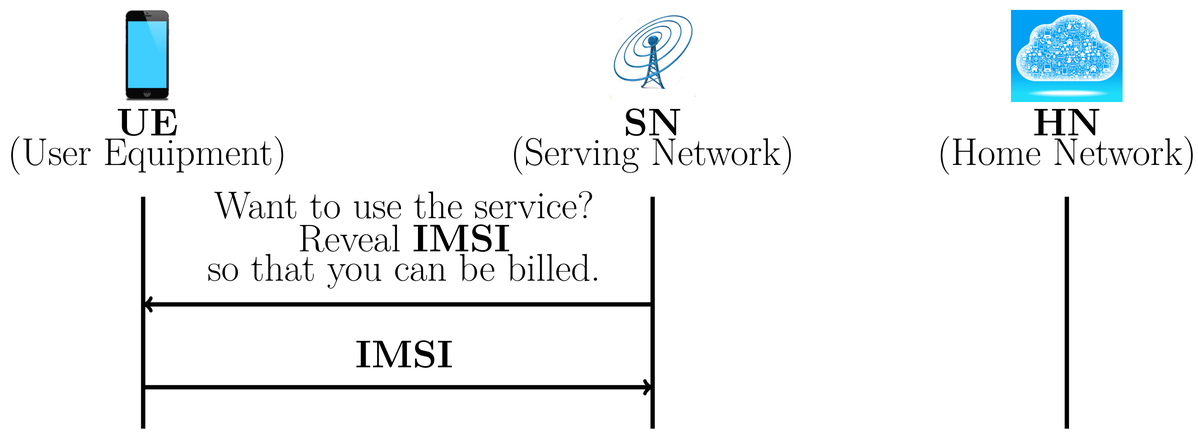
IMSI

- Stands for International Mobile Subscriber Identity. Also called SUPI in 5G
- Globally Unique



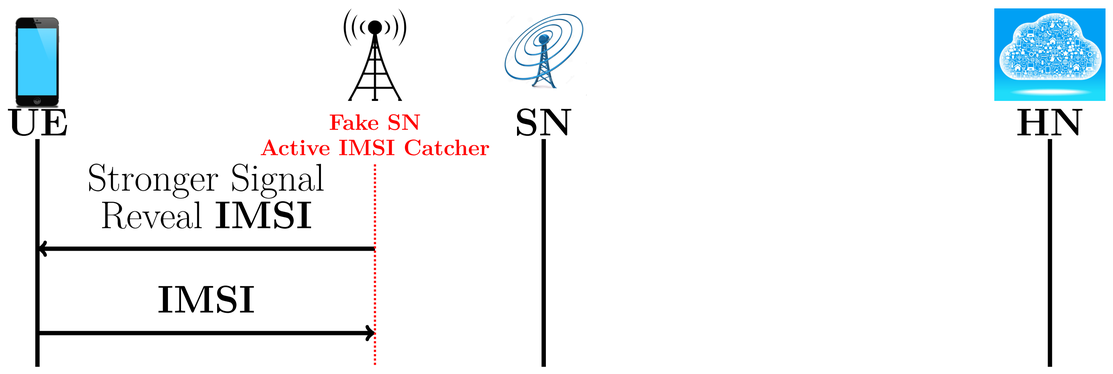
MOBILE NETWORK

The SN and the HN are in a roaming contract. In case the UE is not roaming, SN and HN are the same network.



IMSI CATCHERS

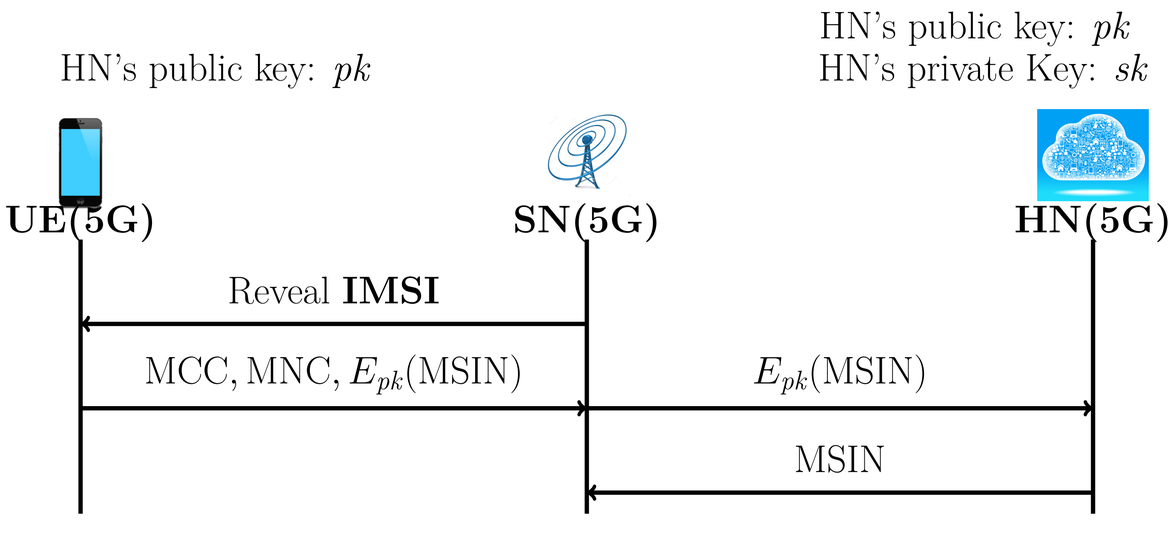
An IMSI catcher impersonates a legitimate SN.



No protection against IMSI catchers in GSM, 3G and LTE. There will be a protection in 5G.

DEFEATING IMSI CATCHERS IN 5G (STANDARDIZED)

3GPP solves the problem by encrypting the MSIN using the public key of the HN.



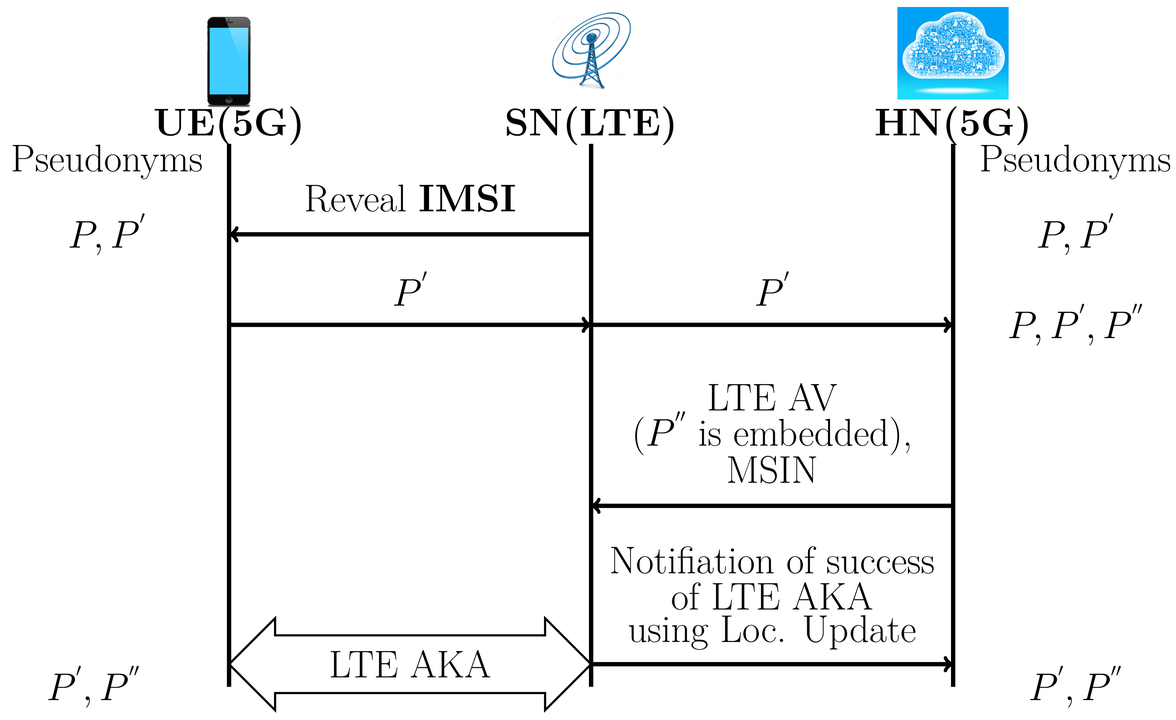
DOWNGRADE ATTACK

5G and LTE interwork – a 5G phone can connect to an LTE SN. So, even though 5G has a protection against IMSI catchers, LTE based IMSI catcher can mount a downgrade attack.

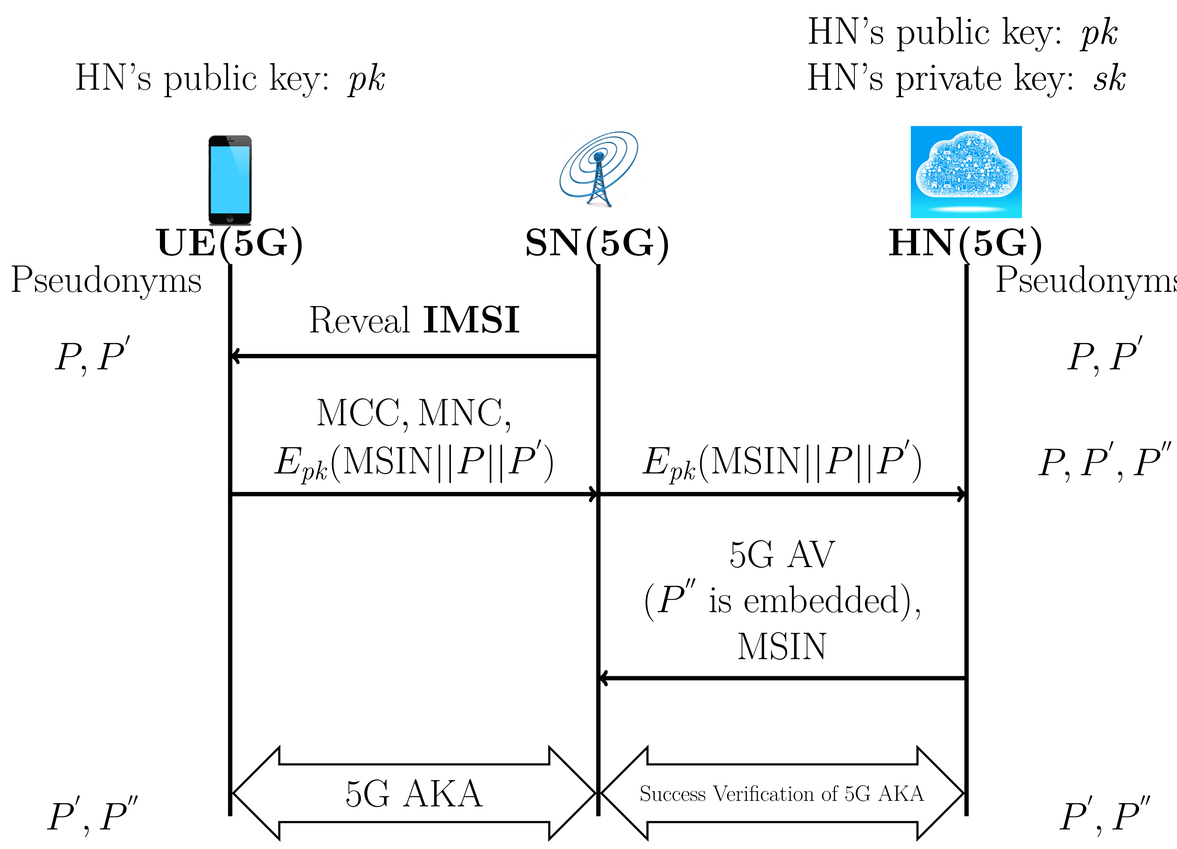
DEFEATING DOWNGRADE ATTACK

Hybrid solution using public-key encryption and pseudonyms.

When the SN is from an LTE Network:



When the SN is from a 5G Network:



Other Advantages:

Apart from defeating the downgrade attack there are other advantages of using the hybrid solution

- If synchronization of pseudonyms is lost, resynchronization can be done just by connecting through a 5G SN.
- Works for both 5G AKA and EAP-AKA$'$.

Challenges:

- A 5G UE may connect with multiple SNs. Thus the UE will have multiple active connection using different pseudonyms simultaneously. These may create complications – when a UE or the HN may forget an old pseudonym?
- SN has to rely on the HN for lawful interception – identifying a user using SUPI (IMSI).