UNIVERSITY OF HELSINKI

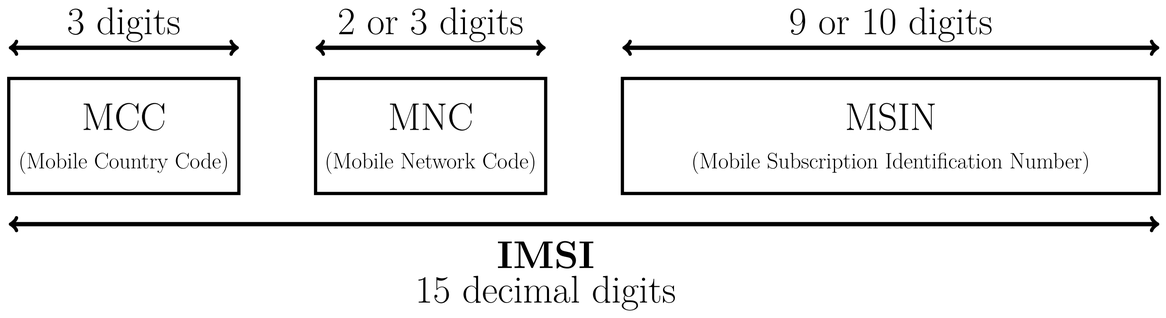
Department of Computer Science

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

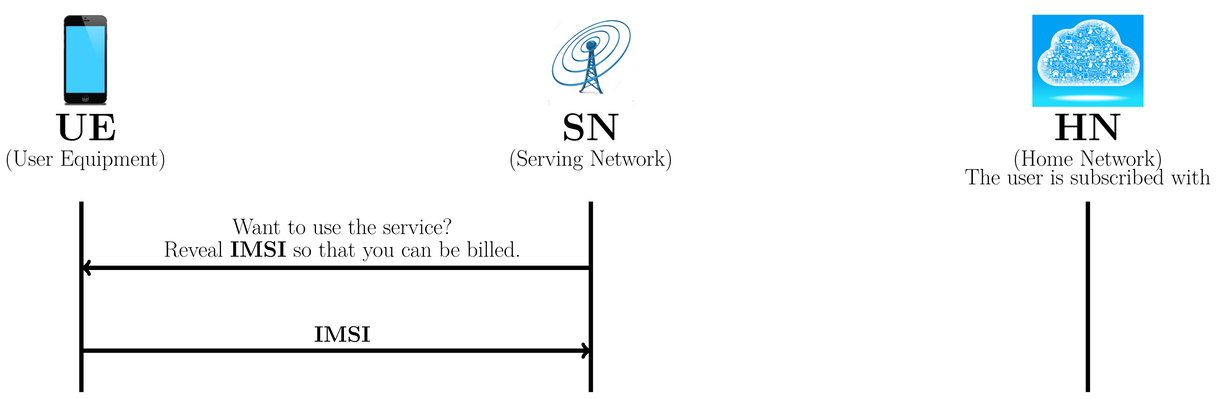
IMSI

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



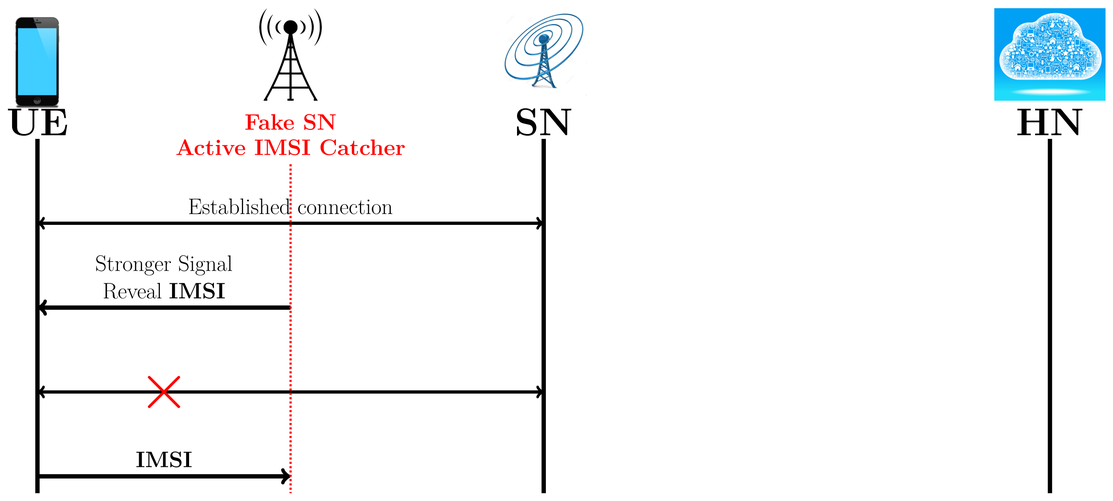
MOBILE NETWORK

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



ACTIVE IMSI CATCHERS

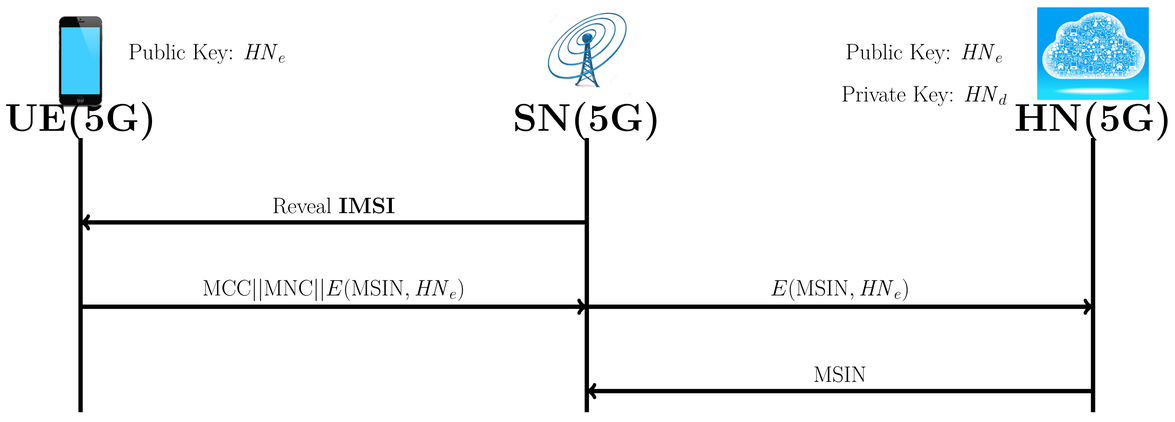
An active IMSI catcher impersonates a legitimate SN.



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

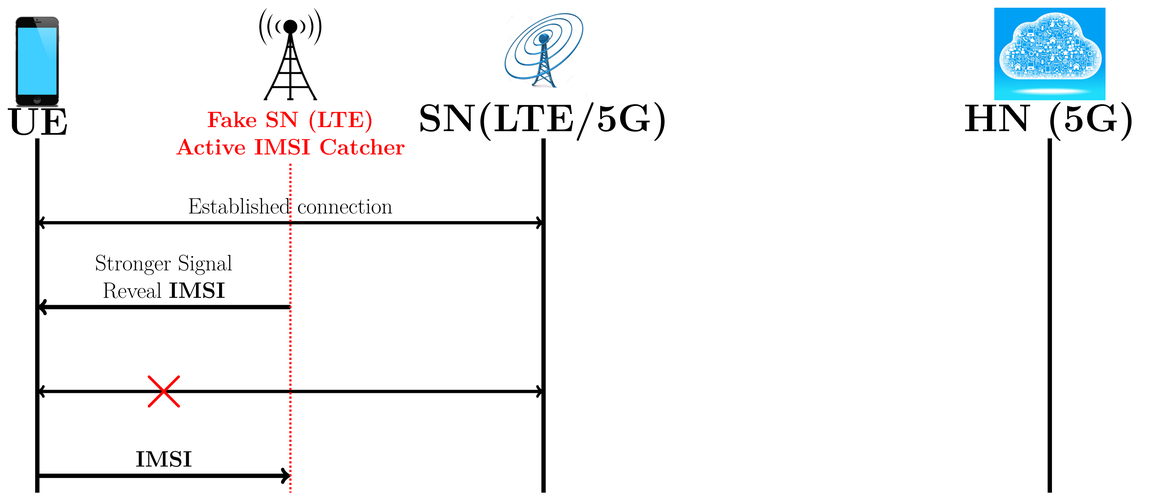
DEFEATING IMSI CATCHERS IN 5G (STANDARDIZED)

3GPP has decided to solve the problem using public-key encryption as follows.



DOWNGRADE ATTACK

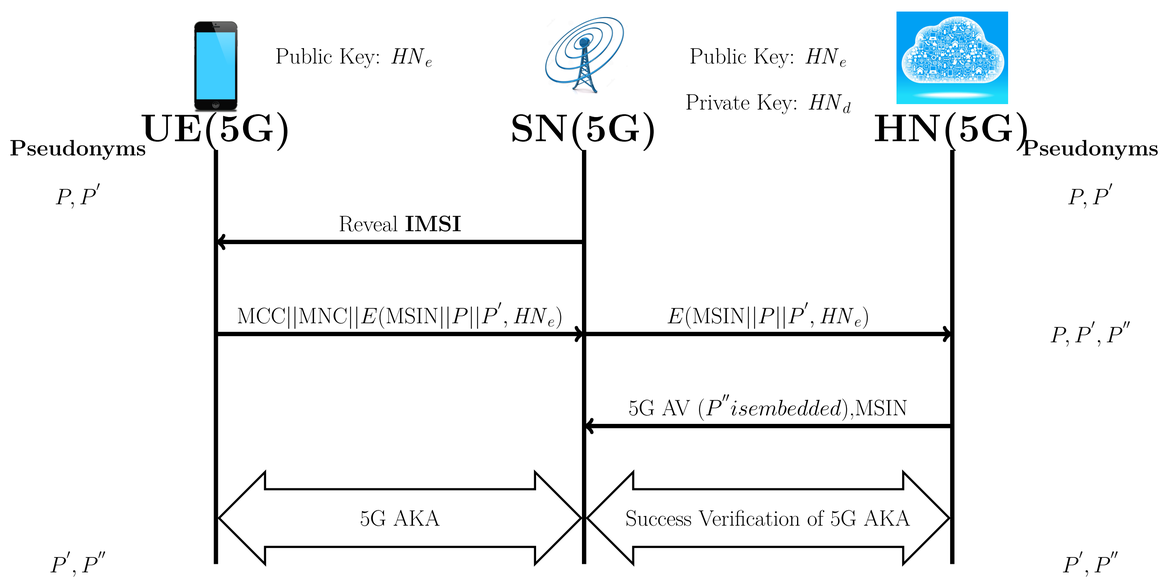
5G and LTE interworks ⇒ An LTE based active IMSI catcher can mount an attack.



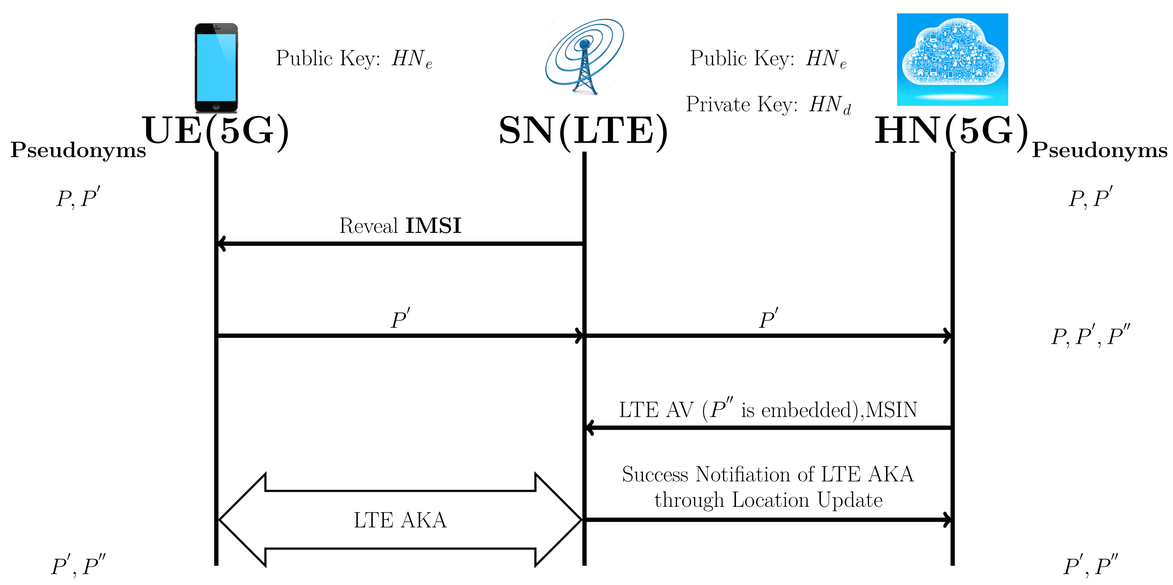
DEFEATING DOWNGRADE ATTACK

Hybrid solution using public-key encryption and pseudonyms.

5G SN:



LTE SN:



Advantages

- No standardization. Works even when EAP-AKA′ is used.
- Major Disadvantages of pseudonym based solution disappears
  - In case of de-synchronization of pseudonyms, resynchronization can be done just by connecting through a 5G SN.
  - A malicious SN can not mount an attack to de-synchronize pseudonyms, because the HN verifies the success of a 5G AKA and EAP-AKA′.
  - Hence, the management of pseudonyms in the subscriber database becomes less vulnerable to unwanted modification.

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).