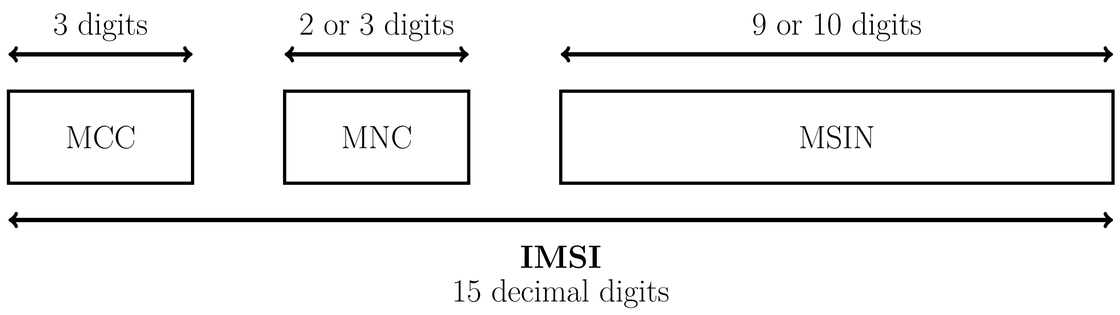
UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE
Department of Computer Science

Mohsin Khan
Valtteri Niemi

IDENTITY PRIVACY IN 5G, DEFEATING DOWNGRADE ATTACK

IMSI

- Identity of a mobile subscriber
- Globally Unique
- Also called SUPI in 5G



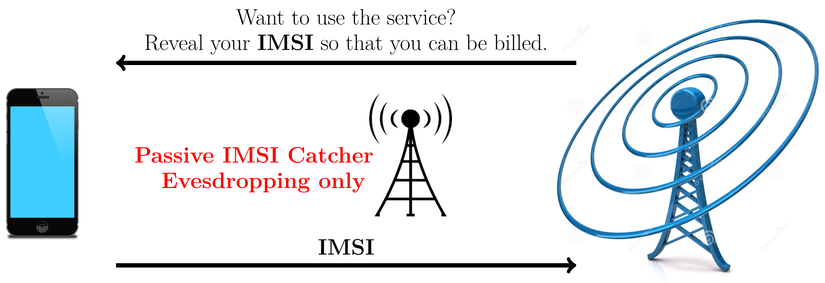
IMSI=International Mobile Subscriber Identity

MCC=Mobile Country Code

MCC=Mobile Network Code

MSIN=Mobile Subscription Identification Number

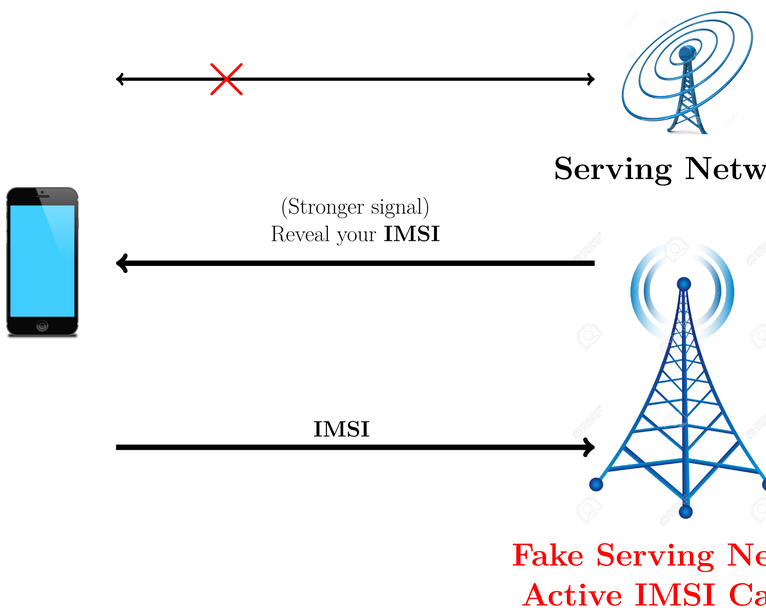
PASSIVE IMSI CATCHERS



Serving Network

Home Network

ACTIVE IMSI CATCHERS

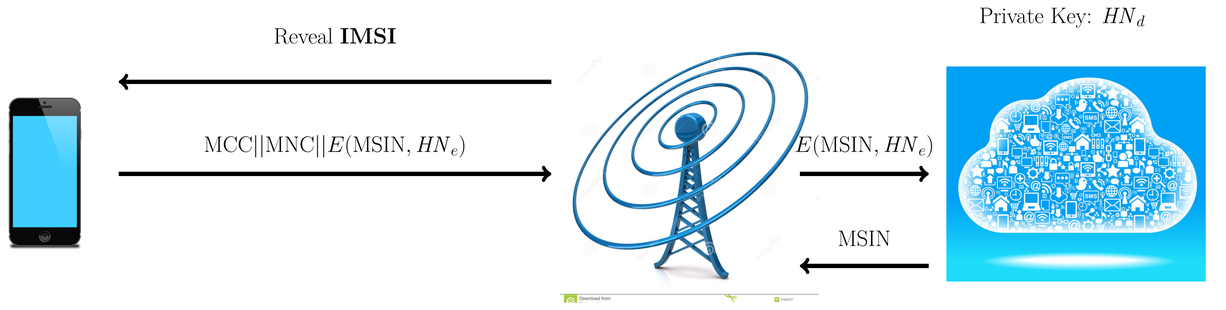


Fake Serving Network
Active IMSI Catcher

Home Network

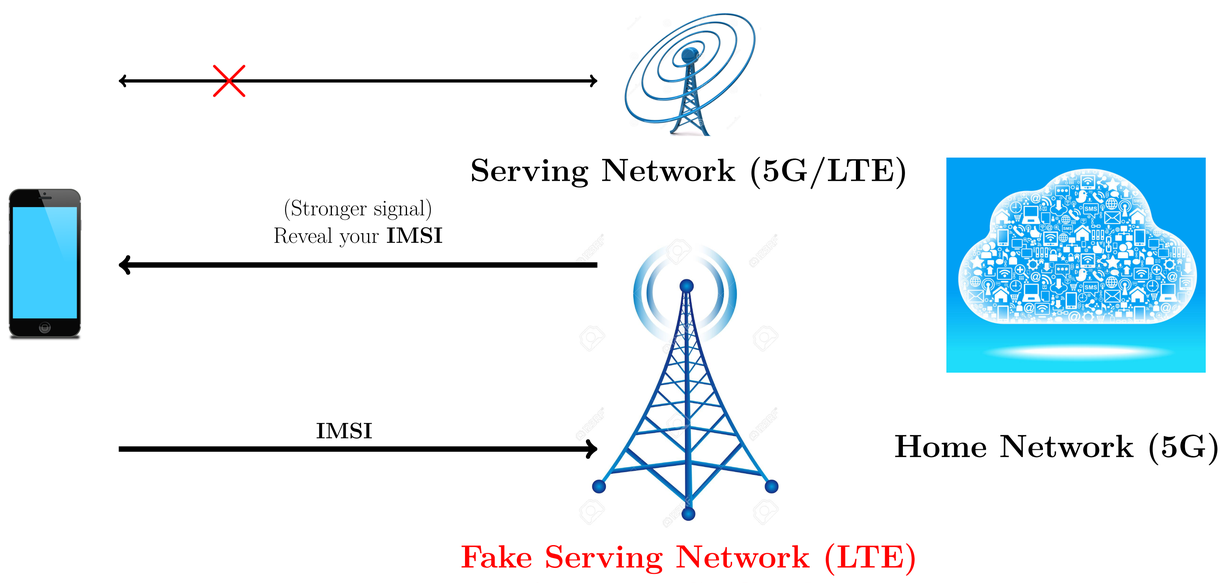
There is no protection against against active IMSI catchers in GSM, 3G and LTE. There will be protection in 5G.

DEFEATING IMSI CATCHERS IN 5G (STANDARDIZED)



Serving Network (5G) **Home Network (5G)**

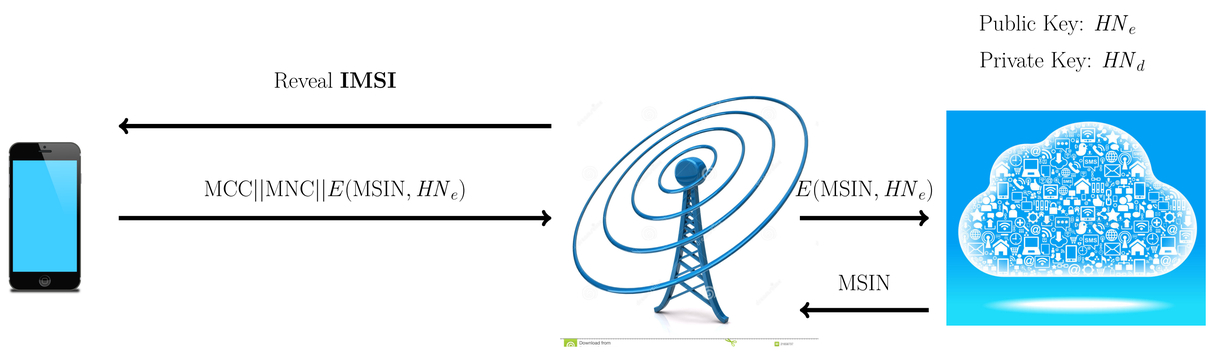
DOWNGRADE ATTACK



Fake Serving Network (LTE)
Active IMSI Catcher

DEFEATING DOWNGRADE ATTACK

A hybrid solution using public-key encryption and pseudonyms. Significant amount of study have been performed on pseudonym based solutions to defeat IMSI catchers [3, 1, 4, 2]. We propose a mixing of pseudonym and public-key encryption to defeat the downgrade attack.



Serving Network (5G) **Home Network (5G)**

REFERENCES

[1] Philip Ginzboorg and Valtteri Niemi. Privacy of the long-term identities in cellular networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia '16. ICST, 2016.

[2] Mohammed Shafiul Alam Khan and Chris J. Mitchell. Improving Air Interface User Privacy in Mobile Telephony. In *Second International Conference, SSR 2015, Proceedings*. Springer International Publishing, 2015.

[3] Karl Norrman, Mats Näslund, and Elena Dubrova. Protecting IMSI and User Privacy in 5G Networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia'16. ICST, 2016.

[4] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. Defeating IMSI Catchers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15. ACM, 2015.