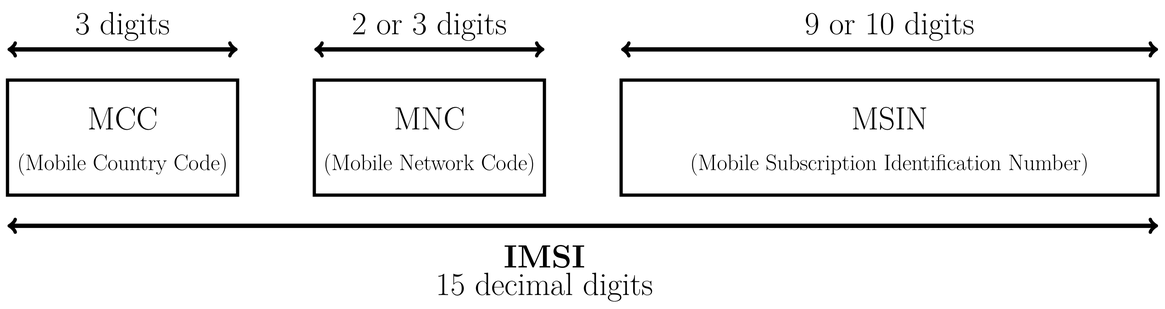
UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE
Department of Computer Science

Mohsin Khan
Valtteri Niemi

# IDENTITY PRIVACY IN 5G, DEFEATING DOWNGRADE ATTACK

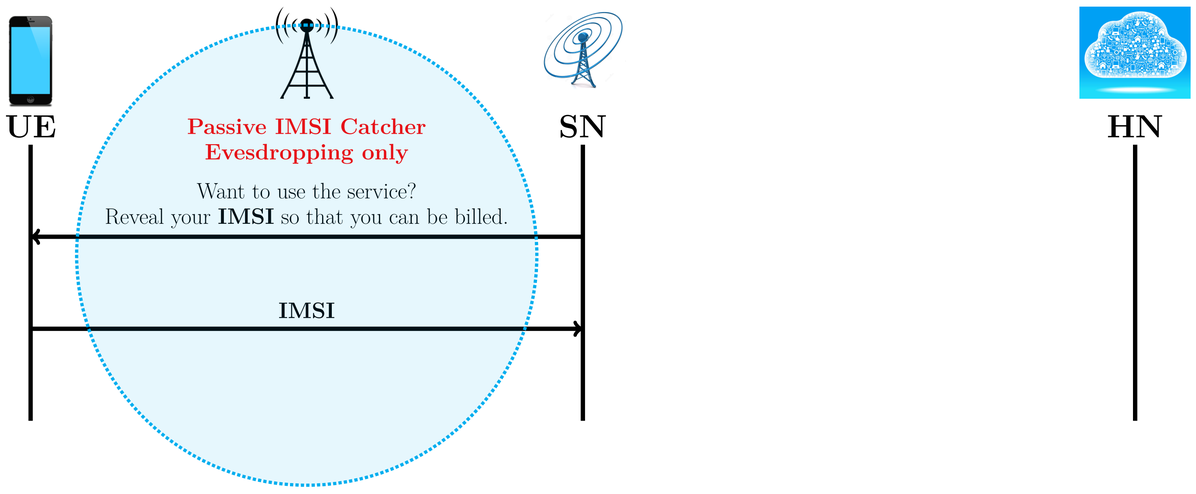
## IMSI

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




## PASSIVE IMSI CATCHERS

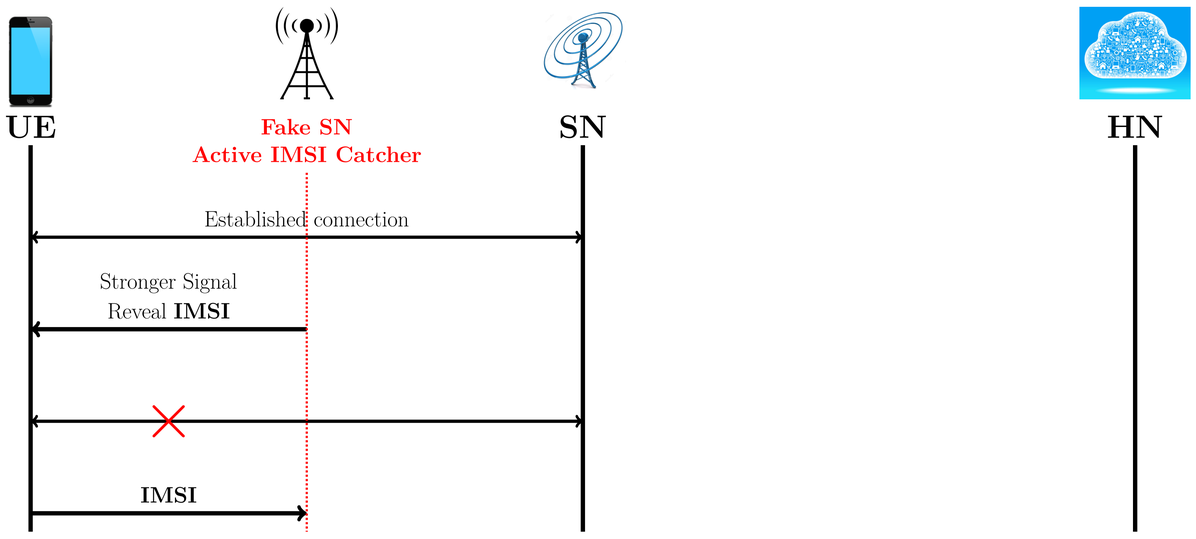
A passive IMSI catcher is always listening and waiting for an IMSI to be sent in plaintext.




Protected in GSM, 3G and LTE. It will be protected in 5G too.

## ACTIVE IMSI CATCHERS

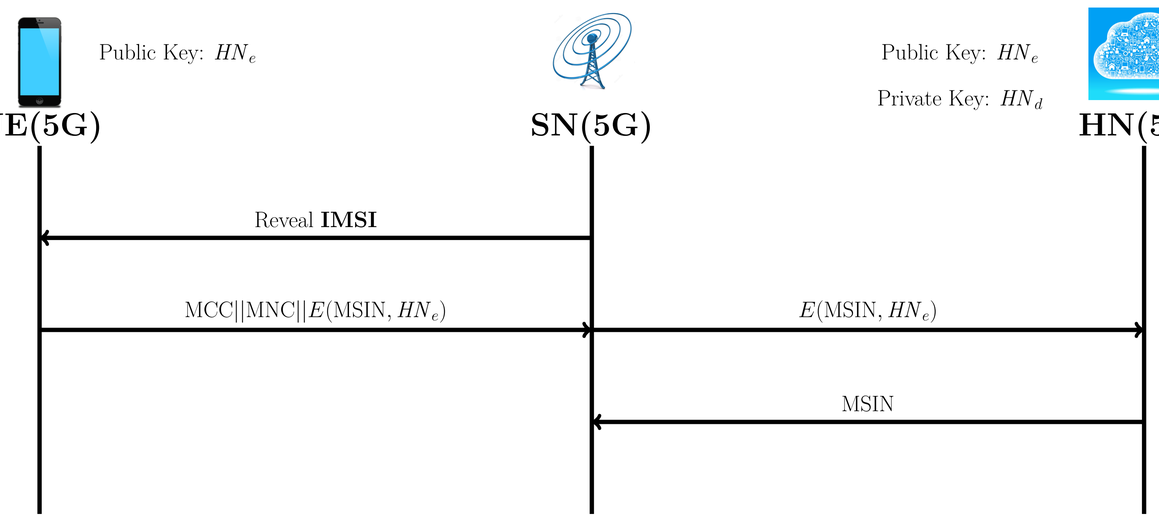
An active IMSI catcher impersonates a legitimate SN.




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

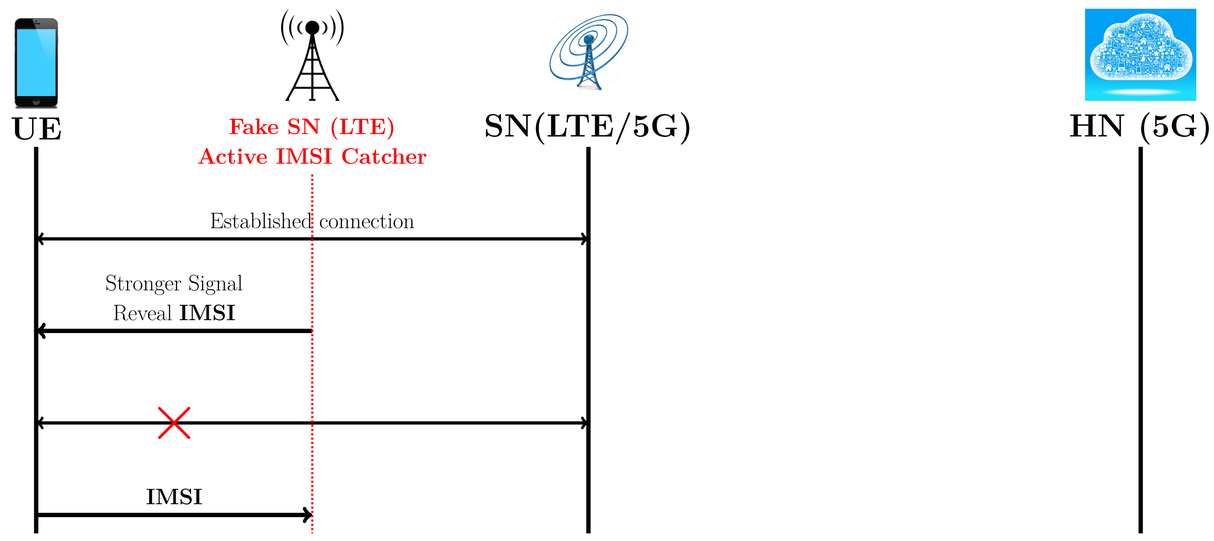
## DEFEATING IMSI CATCHERS IN 5G (STANDARDIZED)

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



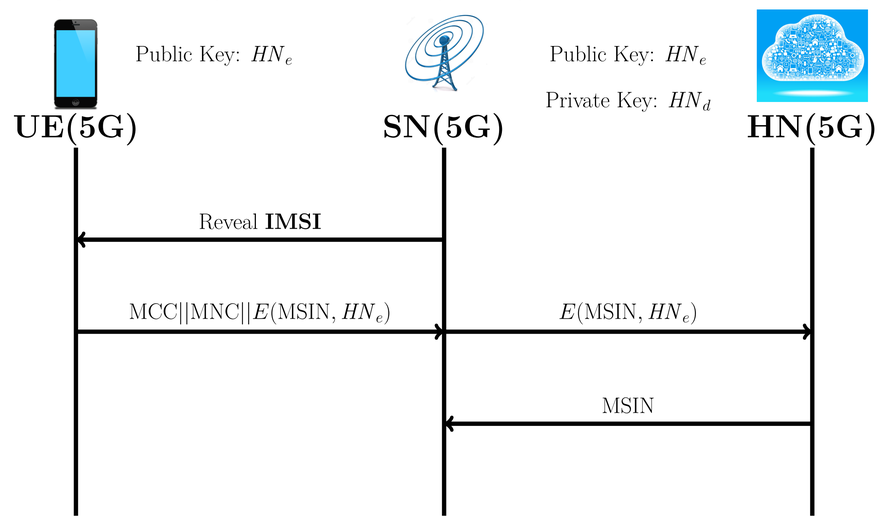

## DOWNGRADE ATTACK

5G phones will be interworking with LTE networks. So, an LTE based active IMSI catcher can still mount an attack.




## 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.




## 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.