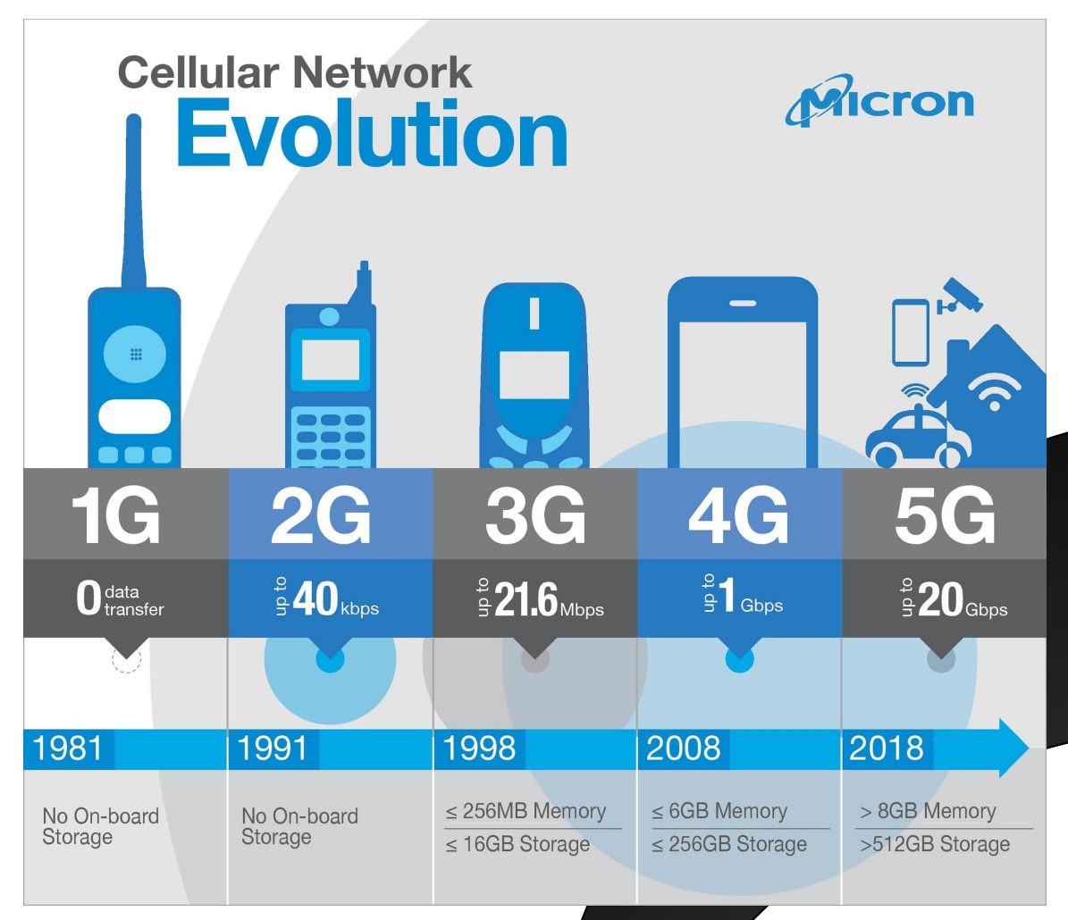
# Formal Methods Analysis of 5G-AKA Protocol with Comparison to 4G EPS-AKA Protocol

CSEE Department, University of Maryland, Baltimore County
Baltimore, MD 21250, USA

December 10,2020

Prajna Bhandary, Ryan Jahnige,
Jason Schneck

● -> sends message
● -> receives message
○ -> state message
● -> unrealized node
——— -> messages sent and received are the same
– – -> messages sent and received are not he same



Hilson, Gary. Cellular Network Evolution. EE times, accessed Dec. 10, 2020.https://www.eetimes.com/5g-needs-more-memory-to-compute/

## Introduction

- Added speed and volume expands the network in 5G.
- Security of the protocol still raises questions.
- IoT devices have the highest potential of using 5G AKA. .
- Cybersecurity concerns related 5G AKA protocol
- Specification of 5G AKA recently updated - never been analysed
- 4G EPS-AKA has many security concerns
- 5G AKA protocol claims to have solved all issues in 4G EPS AKA.

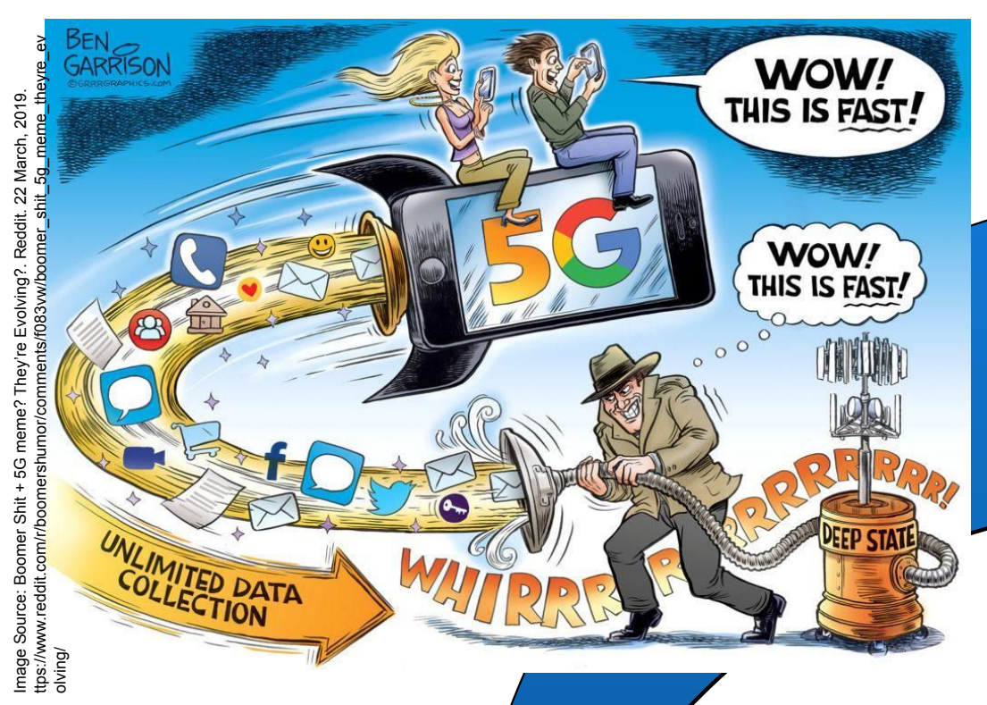
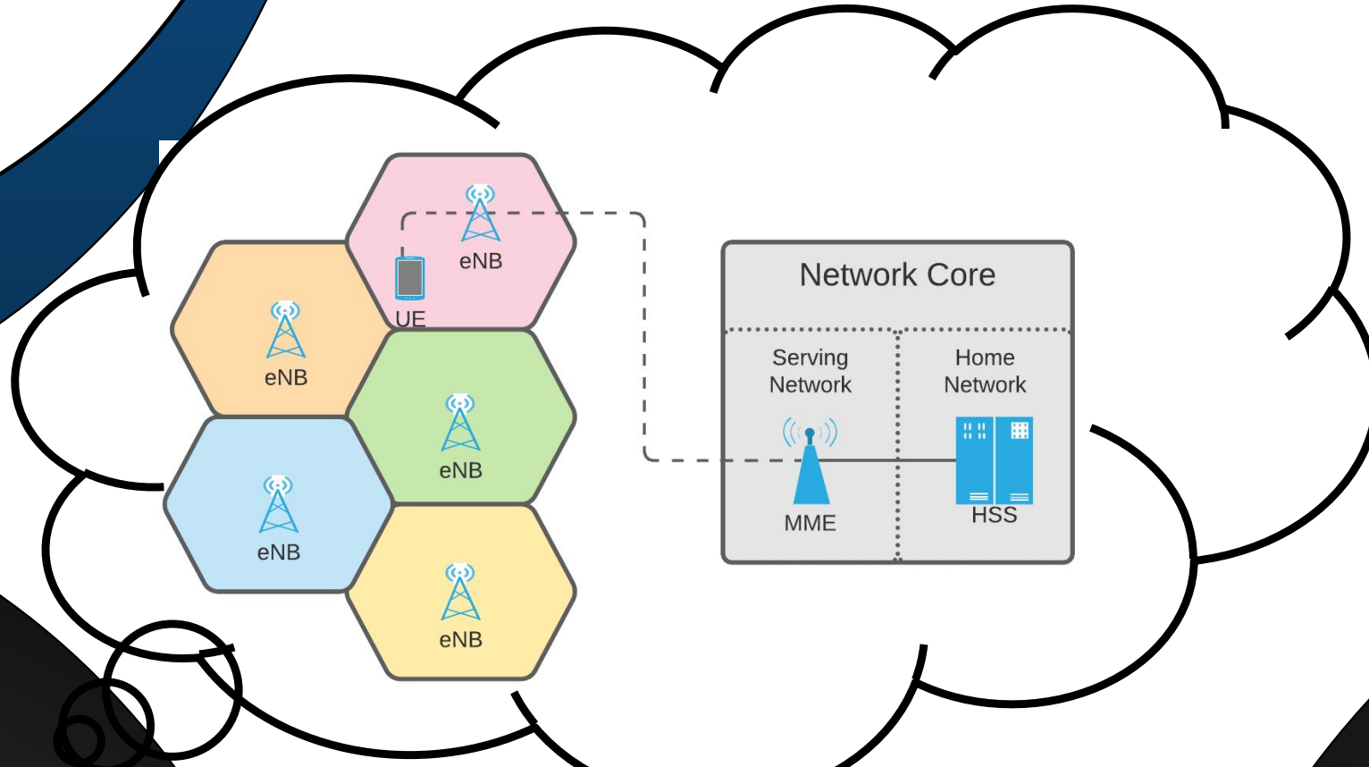
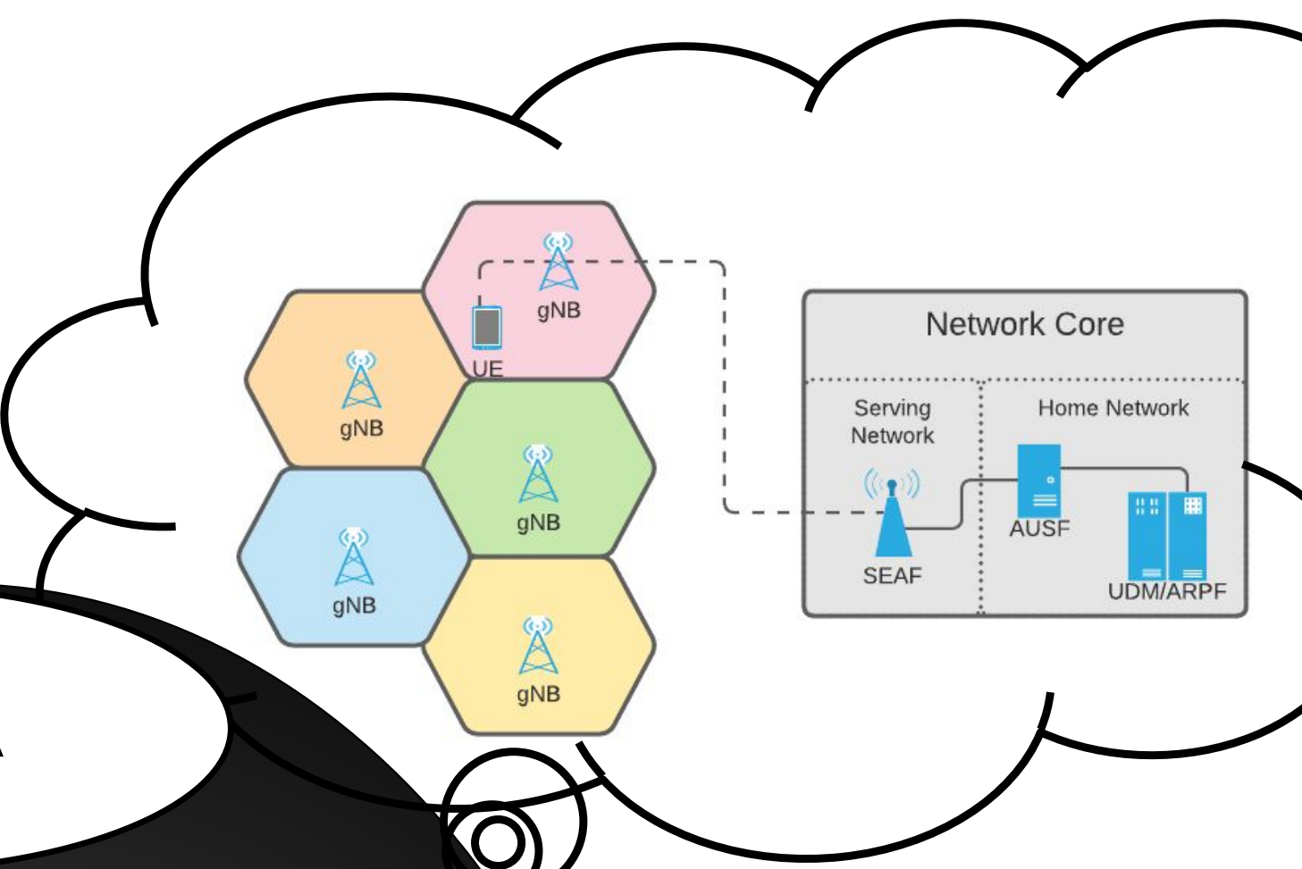


Image Source: Boomer Shit + 5G meme? They're Evolving?. Reddit. 22 March, 2019. https://www.reddit.com/r/boomershumor/comments/f083vw/boomer_shit_5g_meme_theyre_evolving/

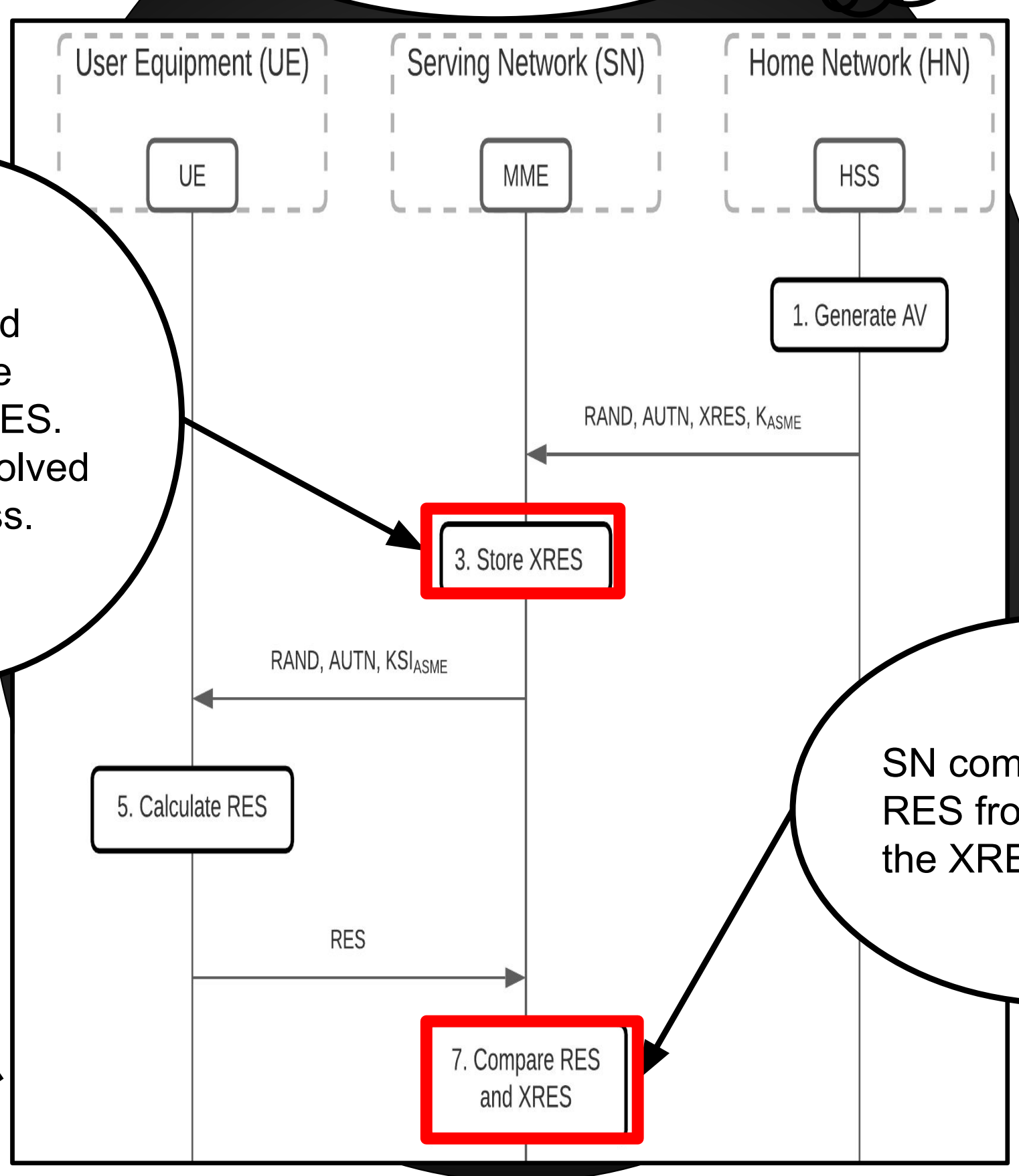
## Questions

- What visualizations are produced in modeling the 5G AKA protocol using CPSA?
- What is found from analyzing the visualizations produced by the tool?
- Are the security properties of 5G better than 4G?
- Do the changes made to 4G to solve the identified security flaw?
- Could the solutions be simplified?
- Did any additional problems arise when the solution was introduced for a security flaw of 4G?





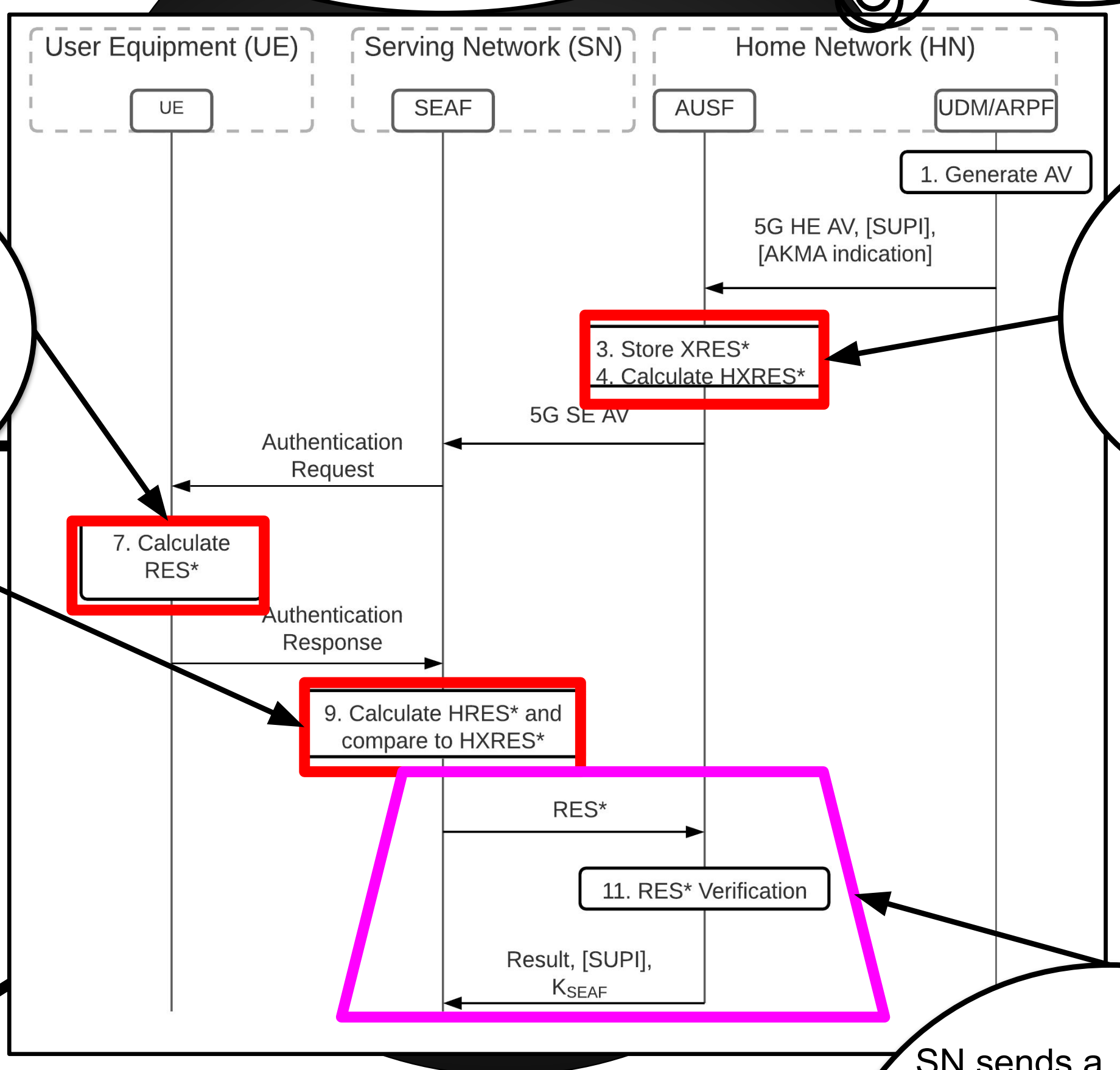
## 4G EPS-AKA



SN stores and calculates the response XRES. HN is not involved in this process.

SN compares the RES from UE and the XRES from HN

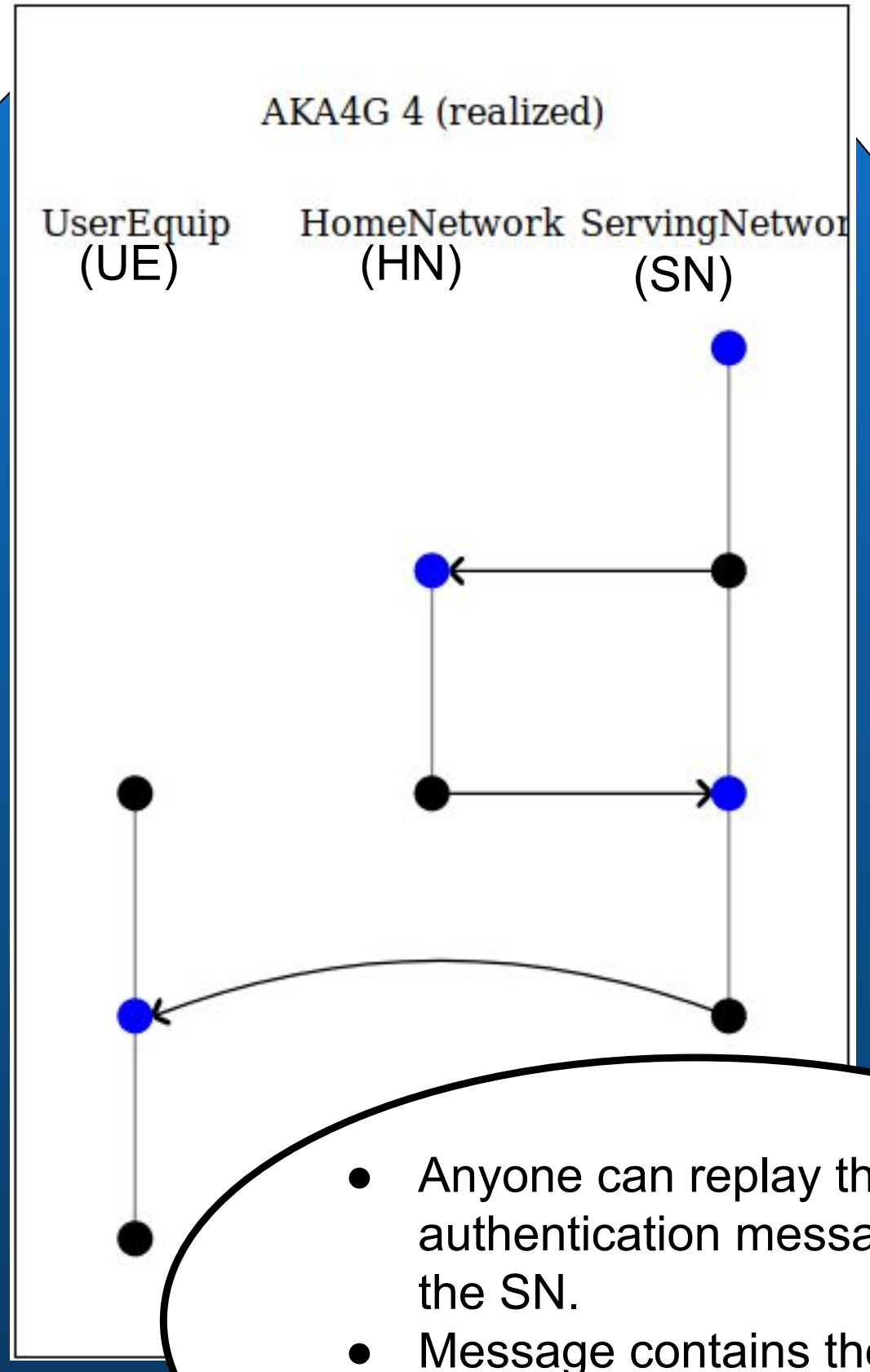
## 5G AKA



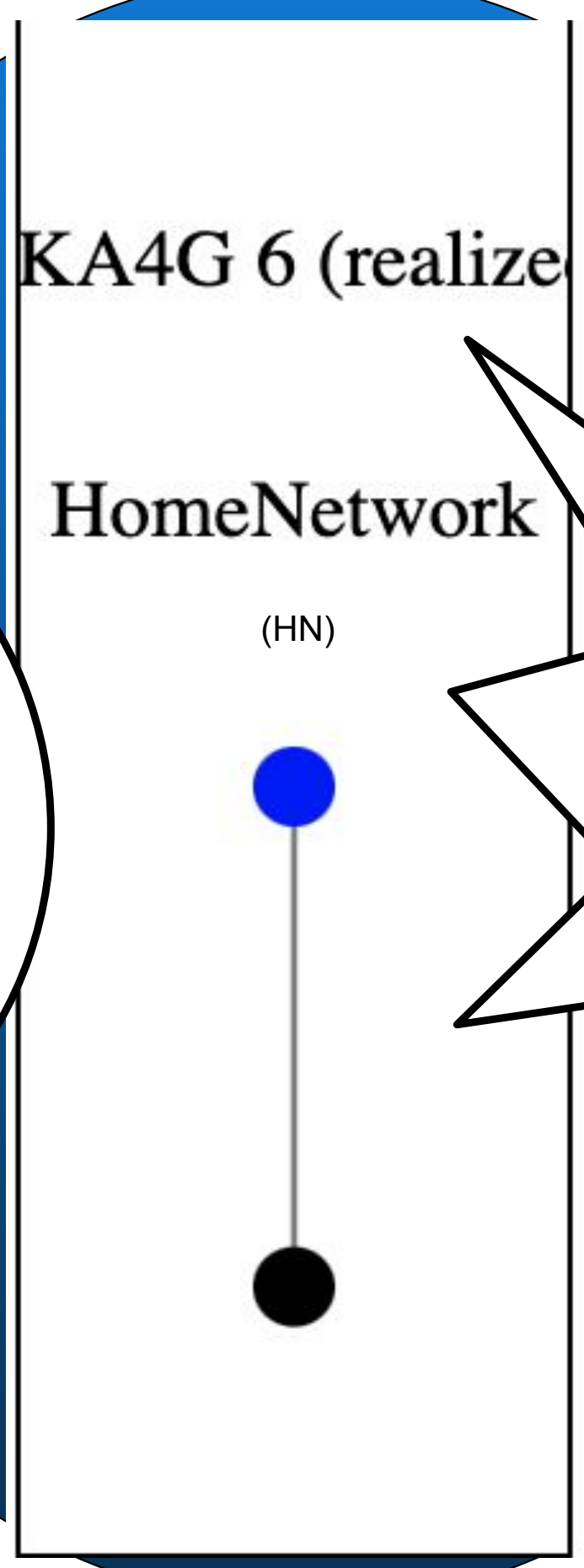
Response messages calculated are different from the 4G EPS AKA procedure.

HN stores XRES* and calculates the response HXRES* for verification later.

SN sends a confirmation message when the authentication is successful to the HN. HN verifies the response. These steps are not included in the 4G-AKA authentication procedure.



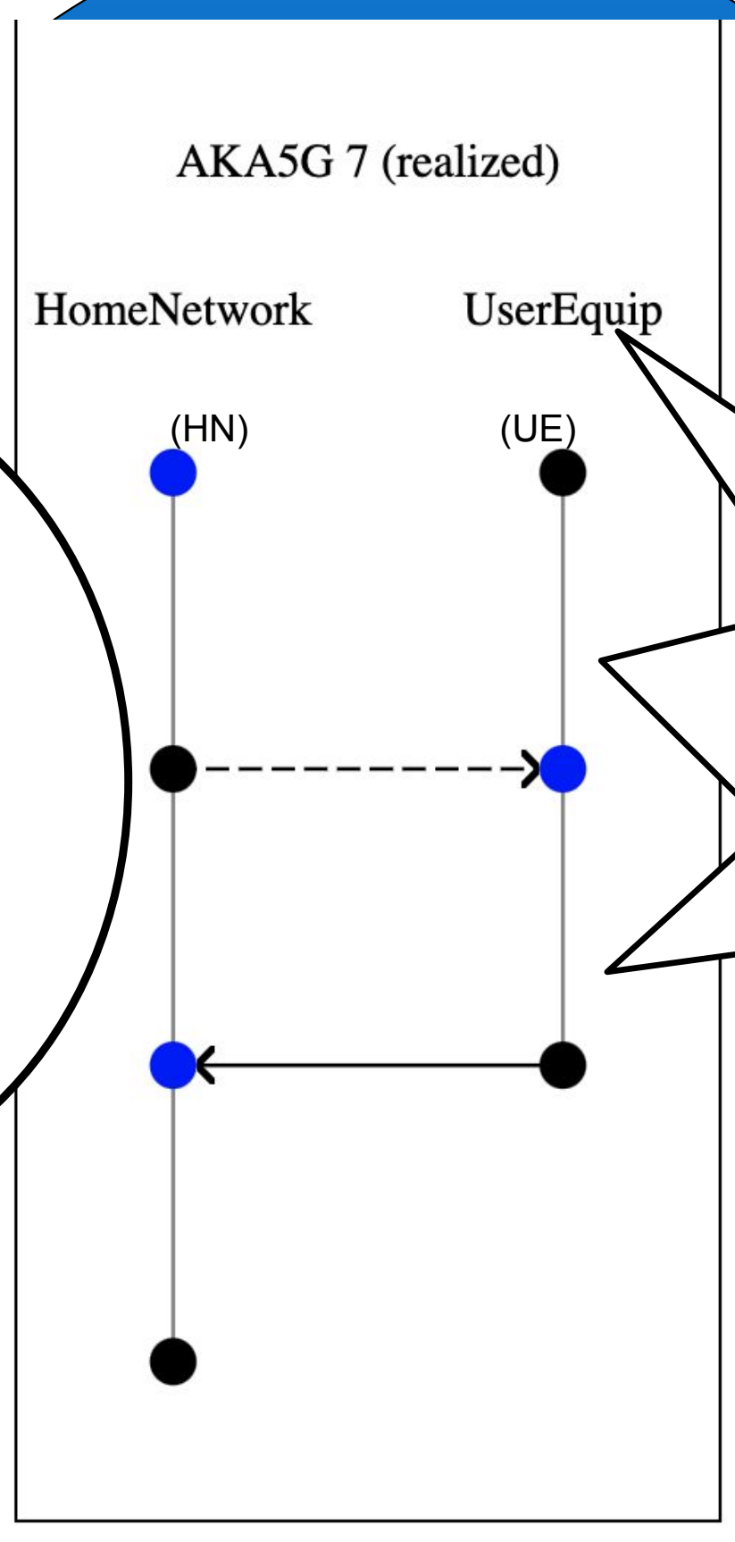
- Anyone can replay the initial authentication message to the SN.
- Message contains the UE's identity, so an adversary can track users.



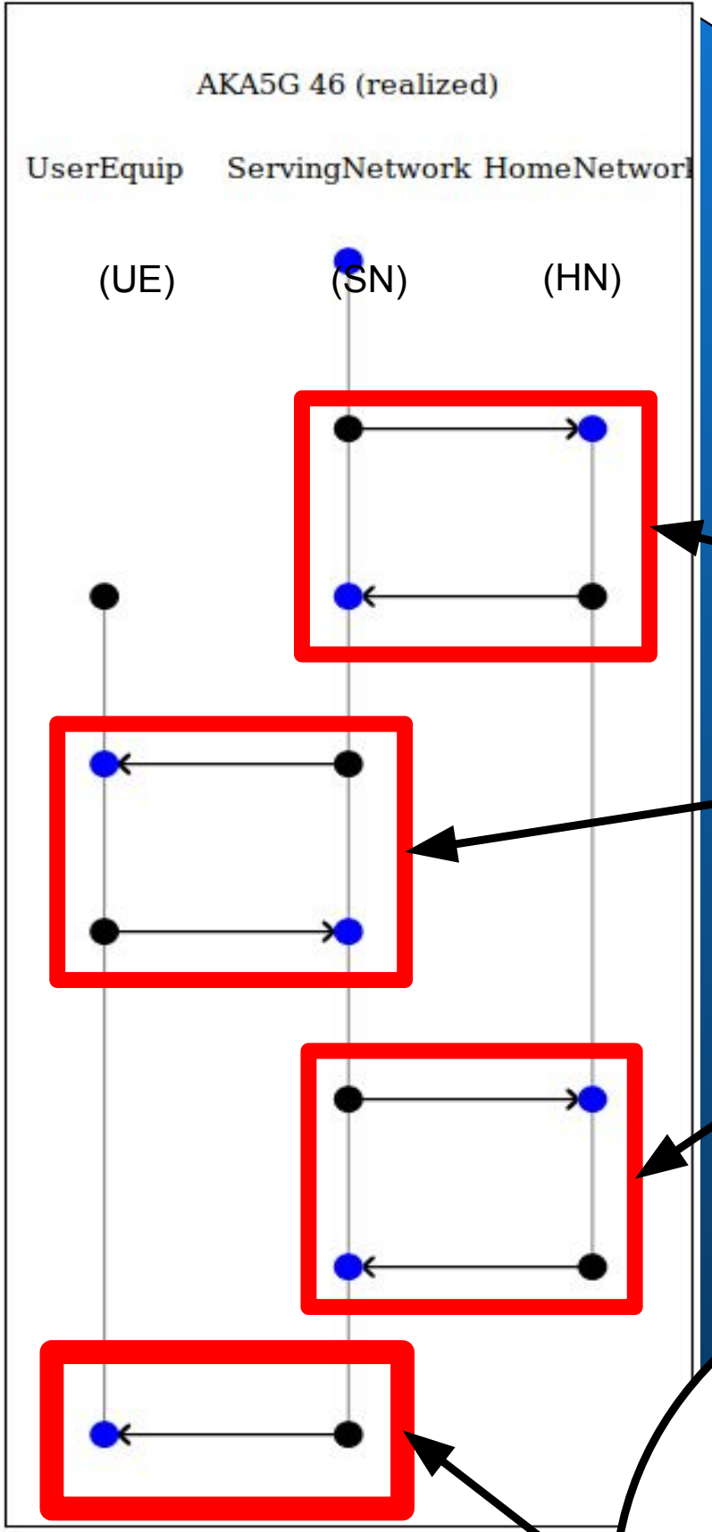
HN does not know with which SN or UE it is communicating with. Once it receives the SUPI it simply generates the AV and passes it along the network.

Model when the channel between the HN and SN is not secure, the HN has no way of authenticating participants.

In 5G, an adversary is still able to replay the initial authentication message (i.e., SUCI).
Adversary has no information about the identity of the UE.



Model when the channel between the HN and SN is not secure, the SN is not needed for authentication.



Increased HN control allows the HN to verify that the authentication was successful.

Additional key confirmation round verifies whether the implicit agreement on $K_{SEAF}$ is sufficient to establish agreement on the SN.

Guest. Acknowledgement vs. Acknowledgment. Grammarly Blog. accessed Dec. 10, 2020. https://www.grammarly.com/blog/what-is-the-difference-between-acknowledgement-and-acknowledgment/

## Thank you

- Edward Ziegler- Technical Director
- Alan Sherman- Faculty Advisor

## 4G EPS-AKA Analysis

- HN cannot authenticate the UE.
- Channel between the SN and HN is supposed to be confidential because it is a wired connection. If we remove that assumption then the HN cannot verify the SN or UE.
- User sends its Identity (IMSI) in plaintext over the network. Adversary can track IMSI by identifying eNodeB its connected to.
- Insecure IMSI could lead to a MITM attack among others.
- Adversary can impersonate an eNodeB and replay messages.

Deborah Gabriel. Qualitative data analysis. Blog. accessed Dec. 10, 2020. https://deborahgabriel.com/2013/04/25/qualitative-data-analysis/

## 5G AKA Analysis

- Initialization message can still be replayed.
- Underspecified channel between HN and SN. Adding a long-term shared key between HN and SN will provide confidentiality.
- Removing confidentiality assumption could lead to a possible replay attack by a malicious server.

## Results

- Different entities have different security properties.
- Lack of explanation in the documentation about confidentiality and authenticity between SH and HN.
- Solution: Introduce long-term key between SN and HN.
- SUPI seems secure in 5G.
- Additional verification of the response by SN improves authentication of HN.
- Key hierarchy plays a major role in the authentication procedure.