Location Privacy, 5G AKA, and Enhancements

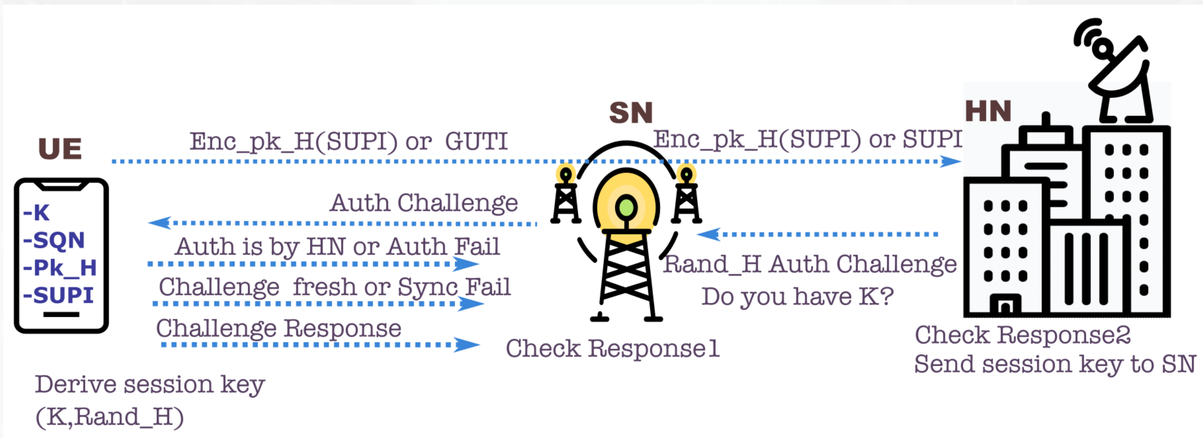
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Mohamed Taoufiq Damir, Valtteri Niemi
Tommi Meskanen, Sara Ramezanian

University of Helsinki
mohamed.damir@helsinki.fi, valtteri.niemi@helsinki.fi
, sara.ramezanian@helsinki.fi, tommi.meskanen@iki.fi

The 5G Authentication and Key Agreement (5G AKA)

Terminology: UE: user equipment, e.g., SIM and phone. SN: serving network. SUCI: encrypted permanent identifier. GUTI: temporary identifier. K: UE long term key. SQN: sequence number. pk_H: HN public key.

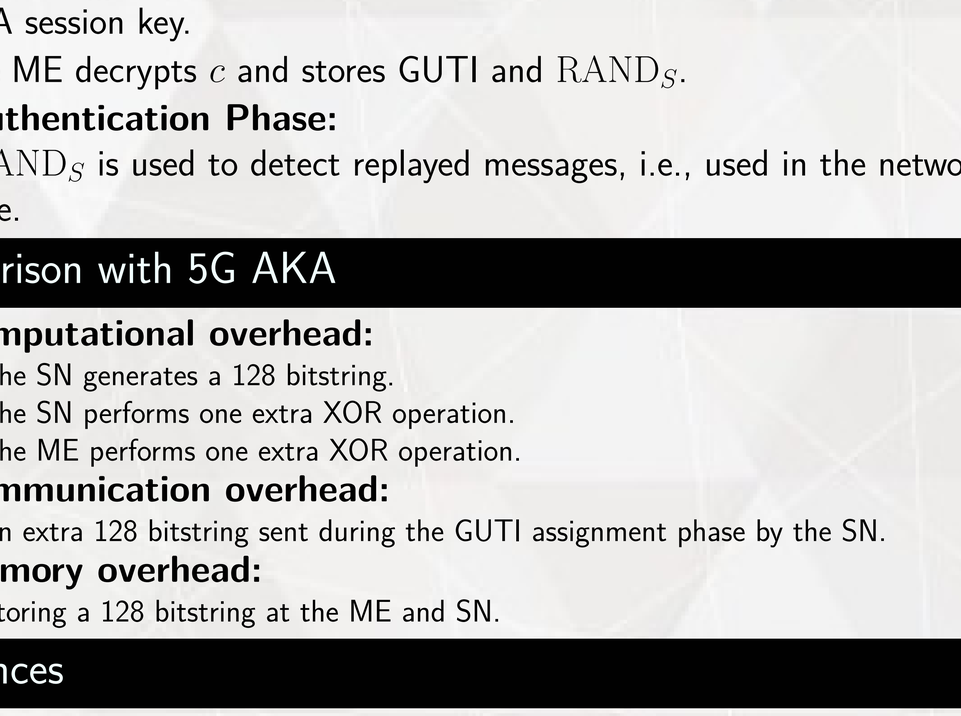


The Replay In GUTI (RIG) Attack [1]

The Discovery Phase:

1. The attacker sniffs the network traffic for a GUTI-based 5G AKA protocol run related to a target user U_t.
2. The attacker records the authentication vector sent by the SN to the UE consisting of the target's AUTN and RAND that we denote by $\mathrm{AV_t}$.

The Attack Phase:



A USIM compatible Fix

The GUTI Assignment Phase:

- The SN generates a GUTI and RAND_S then sends $c = \mathrm{Enc}_{K_{ses}}(\mathrm{GUTI}, \mathrm{RAND}_S)$, where K_{ses} is the previously established 5G AKA session key.
- The ME decrypts c and stores GUTI and RAND_S.

The Authentication Phase:

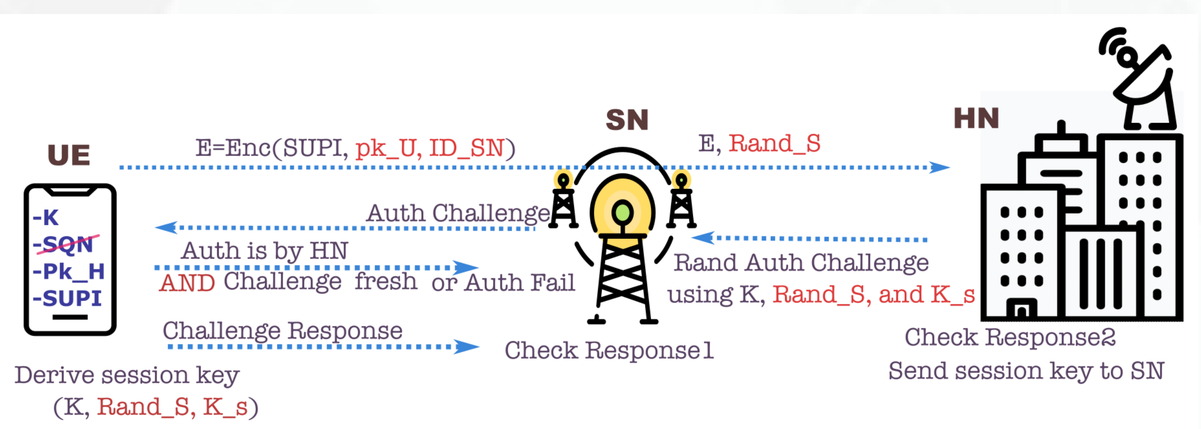
Idea: RAND_S is used to detect replayed messages, i.e., used in the network's challenge.

Comparison with 5G AKA

1. **Computational overhead:**
   - The SN generates a 128 bitstring.
   - The SN performs one extra XOR operation.
   - The ME performs one extra XOR operation.
2. **Communication overhead:**
   - An extra 128 bitstring sent during the GUTI assignment phase by the SN.
3. **Memory overhead:**
   - Storing a 128 bitstring at the ME and SN.

A Novel Beyond-5G AKA [2]

A high level description of our protocol:



1. ID_{SN}: the identity of the SN.
2. pk_U: a freshly generated *key encapsulation mechanism* (KEM) public-key by the UE.
3. $Rand_S$: a random bitstring generated by the SN.
4. K_s: a KEM key encapsulated key by the HN using pk_U.

The GUTI Case

1. After each successful SUPI-based protocol run, both the UE and the HN store a hash value
$$K_S = h(K_s, R_{SN}).$$
2. With every GUTI assignment, the SN generates and sends, in addition to the GUTI, a random bitstring R'_{SN} to the UE over the established secure channel.

The idea behind our solution for the GUTI case is to replace K_s with
$$K'_S = K_S \oplus R'_{SN}.$$
in our SUPI-based protocol.

Advantages of our Protocol

1. User's privacy, i.e., identity, and session key confidentiality;
2. Mutual authentication between UE and SN via the HN;
3. Perfect forward and backward secrecy;
4. Compatibility with the KEM paradigm, esp. with standardized PQ KEMs;
5. Resistance to known linkability attacks.
6. Resistance to our RIG attack.
7. Protection against some compromised/impersonated SNs attacks.

Remark: our proposal improves privacy and security (properties in blue) compared to the current 5G AKA and six recently proposed AKA for mobile networks.

Tools and Evaluation

- We proved that our protocol satisfies the desired security properties using ProVerif.
- Evaluated the communication and computational costs of our protocol using post-quantum KEMs from the NIST standardization process.

References

[1] Damir, M.T., Niemi, V. Location Privacy, 5G AKA, and Enhancements. (NordSec 2022).

[2] Damir, M.T., Meskanen, T., Ramezanian, S., Niemi, V. A Beyond-5G Authentication and Key Agreement Protocol. (NSS 2022).