30TH USENIX SECURITY SYMPOSIUM

Privacy-Preserving and Standard-Compatible AKA Protocol for 5G

Yuchen Wang[†,*], Zhenfeng Zhang[†] and Yongquan Xie[§]

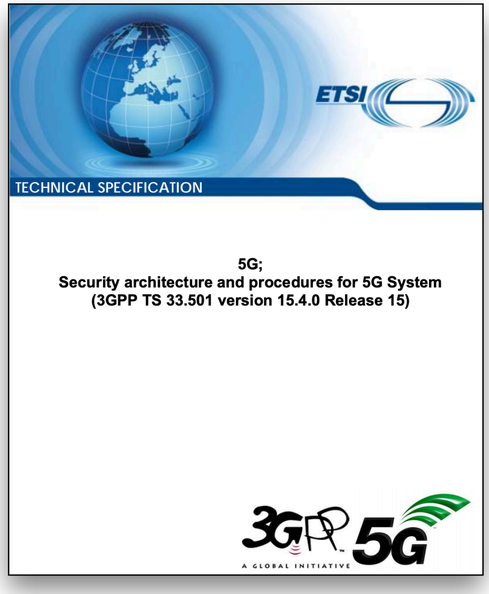
[†] Institute of Software, Chinese Academy of Sciences

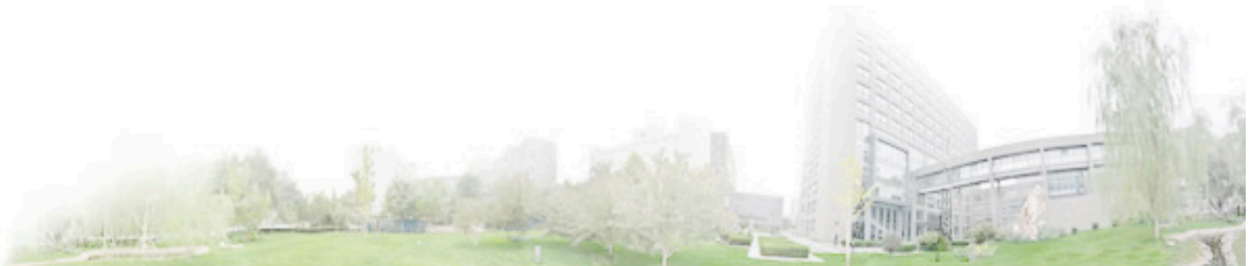
[*] Alibaba Group

[§] Commercial Cryptography Testing Center of State Cryptography Administration

The 5G standardization and 5G-AKA protocol

- 3GPP has started the standardization of 5G since 2015
- TS 33.501: the 5G Authentication and Key Agreement (5G-AKA) Protocol
  - Mutual Authentication and Key Agreement between User Equipment (UE) and Home Network (HN)
  - Inherit may design characteristics from 3G/4G-AKA
- 5G-AKA makes progress on protecting users' privacy
  - Disallowing the plaintext transmission of SUPI over the radio
  - SUPI is encrypted with ECIES and sent as SUCI
  - Avoids the SUPI-catching attack



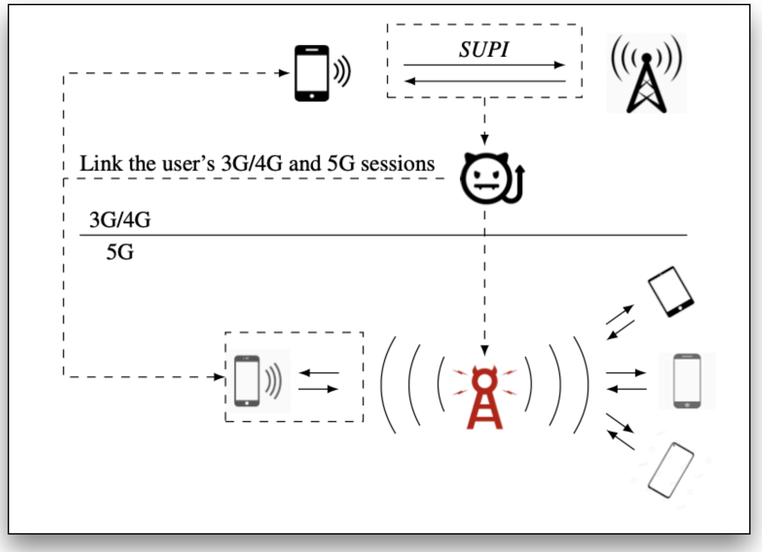


5G-AKA is still vulnerable to active attackers

- 5G-AKA cannot protect users' privacy against active attackers
  - Emit radio signal actively (comp. passive attacker only monitor the radio traffic)
  - Distinguish a target UE by replaying messages
  - Linkability attacks: Link the target UE with its previous session
  - Monitor the target UE/Infer the user's real-world identity
- Several kinds of linkability attacks have been discovered
  - The failure message linkability attack by Arapinis et al. [AMR+12] and Basin et al. [BDH+18]
  - The sequence number inference attack by Borgaonkar et al. [BHP+18]
  - The encrypted SUPI replay attack by Fouque et al. [FOR16] and Koutsos [Kou19]

The vulnerability may be exploited in a cross-protocol attack

- Linkability attacks may break 5G-AKA's protection for SUPI
  - Link a 5G target UE with its 3G/4G-AKA session
  - A 3G/4G-AKA session includes plaintext SUPI
- The possibility of a 3G/4G-5G cross-protocol attack
  - Many vendors support reusing 3G/4G SIM cards
  - Open-source 5G communication solutions
  - An attacker may perform linkability attacks with acceptable costs as in 3G/4G-era
- The improvement of 5G-AKA is necessary and urgent

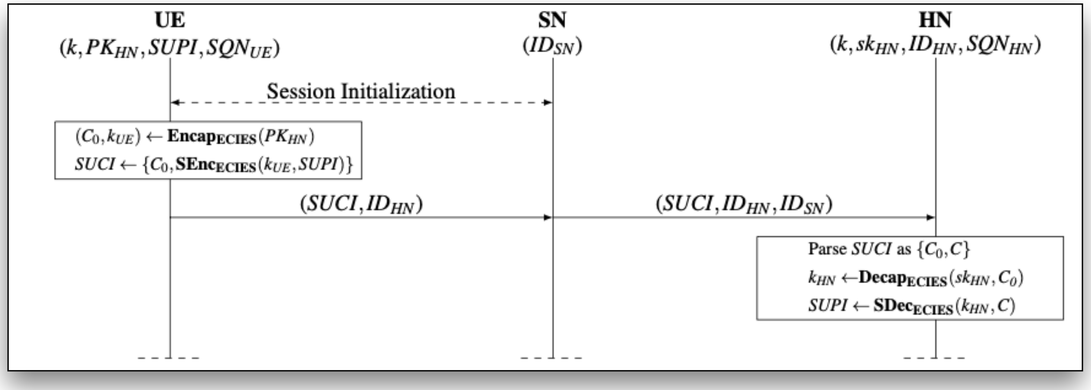


Fix 5G-AKA is not a trivial task

- Several linkability attacks must be fixed “in one shot”
- Compatibility with current 5G specifications
  - A non-compatible proposal is cumbersome to be deployed in practice
  - SIM card compatibility: Require the vendor to change SIM cards for all users
  - Serving Network (SN) compatibility: All SNs have to change their implementations accordingly
- Goal: Fix all linkability attacks while preserving SIM card and SN compatibilities
  - Can be deployed in a way of reusing SIM cards and SN implementations
  - Only both endpoints (i.e., UE and HN) need to be updated

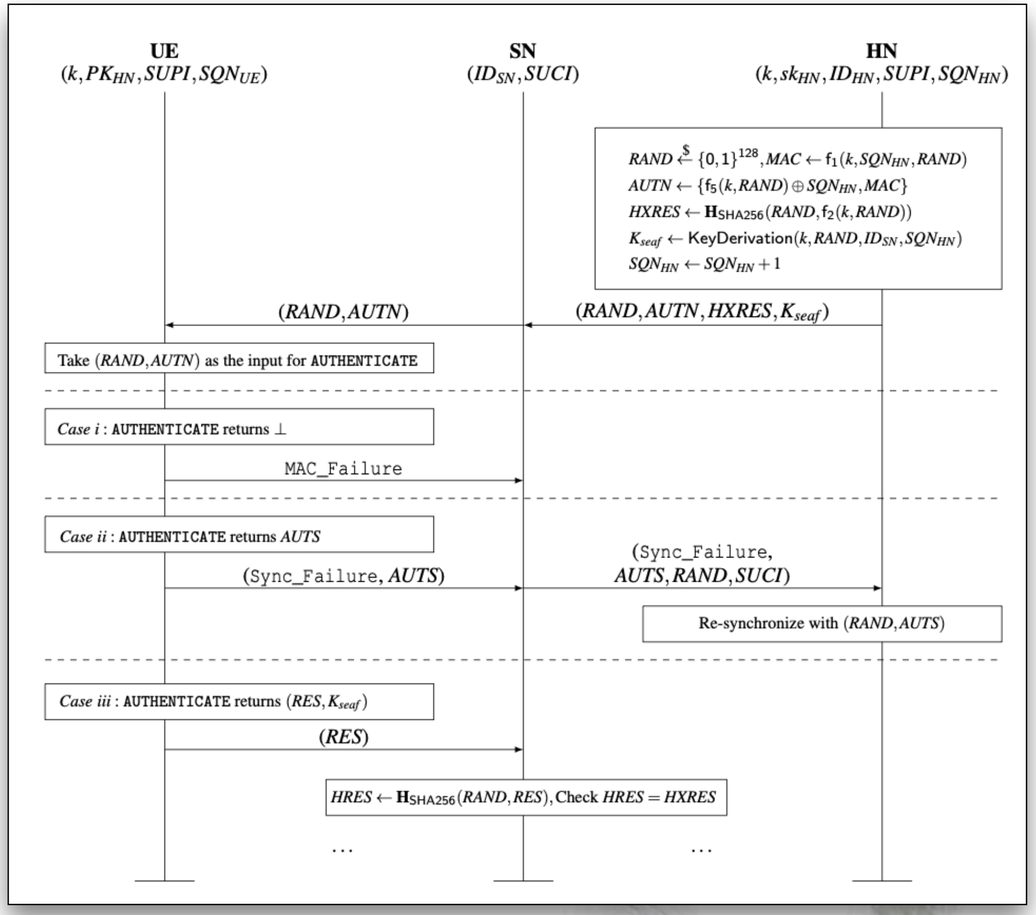
Background: 5G-AKA

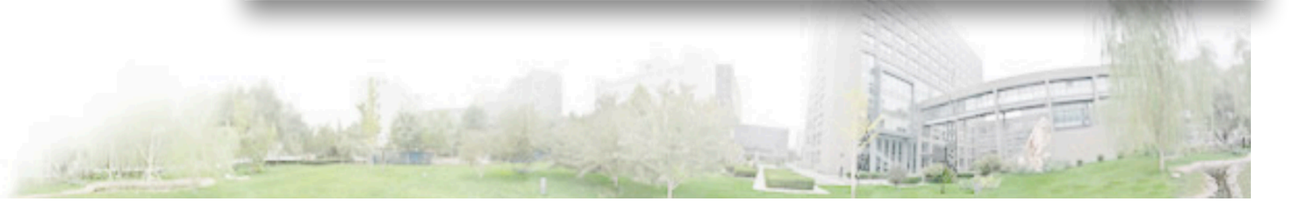
- The Initiation Phase
  - SUPI is encrypted with ECIES
- The Challenge-Response Phase



Background: 5G-AKA

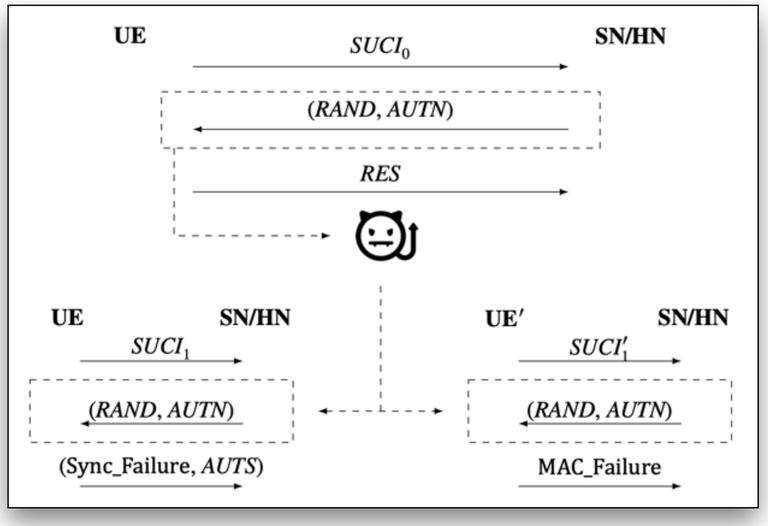
- The Initiation Phase
- The Challenge-Response Phase
  - $RAND$: A random challenge
  - $AUTN$: A MAC value of $RAND$ keyed with UE's long-term key, and a concealed sequence number
  - UE takes $(RAND, AUTN)$ as the input for SIM card command AUTHENTICATE (TS 31.102)
  - Output case (i): MAC failure
  - Output case (ii): Synchronization failure
  - Output case (iii): Response and session key

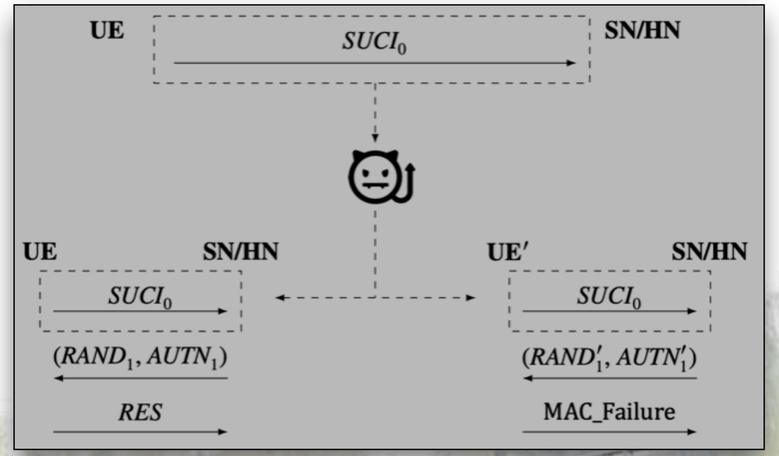




Background: Linkability attacks

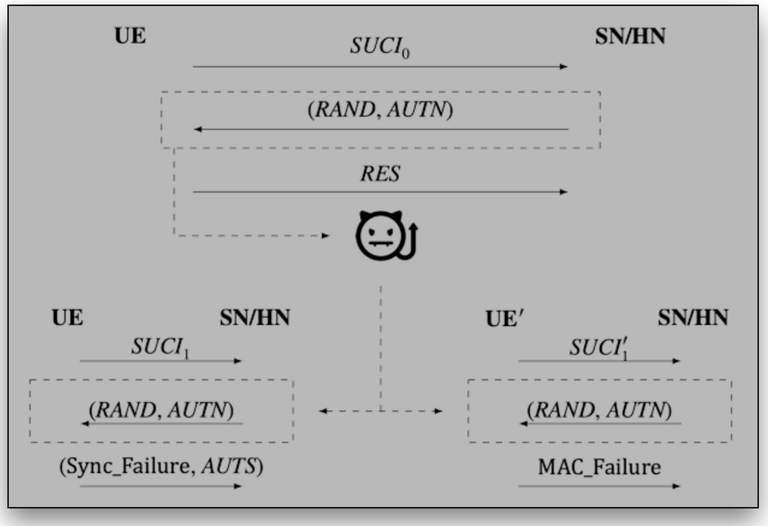
- The failure message linkability attack
  - Replay $(RAND, AUTN)$
  - Target UE replies with Sync_Failure
  - Non-target UE replies with MAC_Failure
- The sequence number inference attack
  - Variant of failure message linkability attack
  - Infer the target UE's sequence number increase pattern on the base of linkability
- The encrypted SUPI replay attack

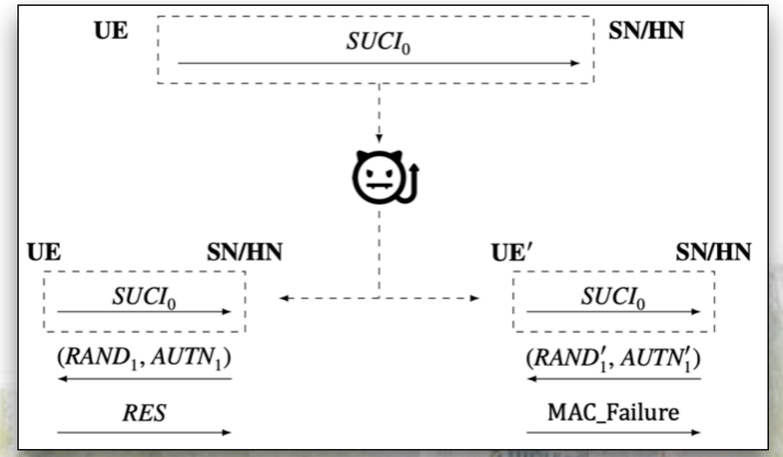




Background: Linkability attacks

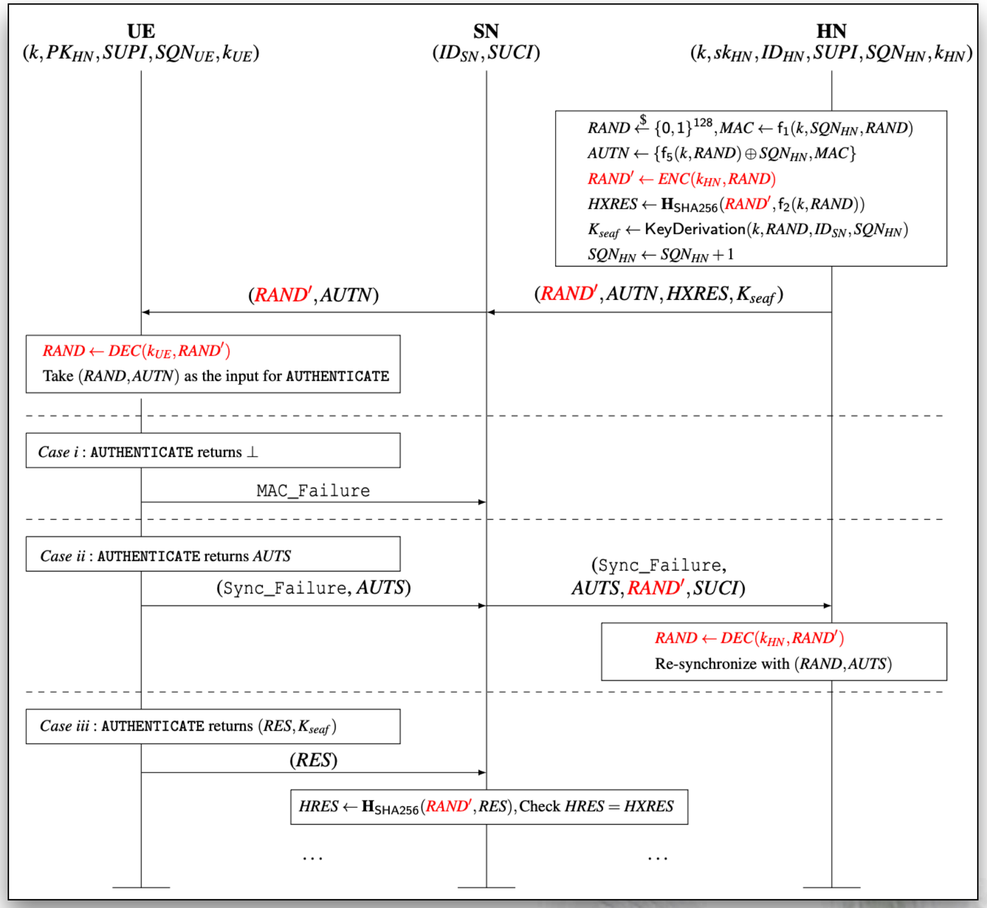
- The failure message linkability attack
- The sequence number inference attack
- The encrypted SUPI replay attack
  - Replay *SUCI* (encrypting target UE's *SUPI*) to the HN
  - HN takes all UEs as the target UE
  - Target UE replies with RES
  - Non-target UE replies with MAC_Failure





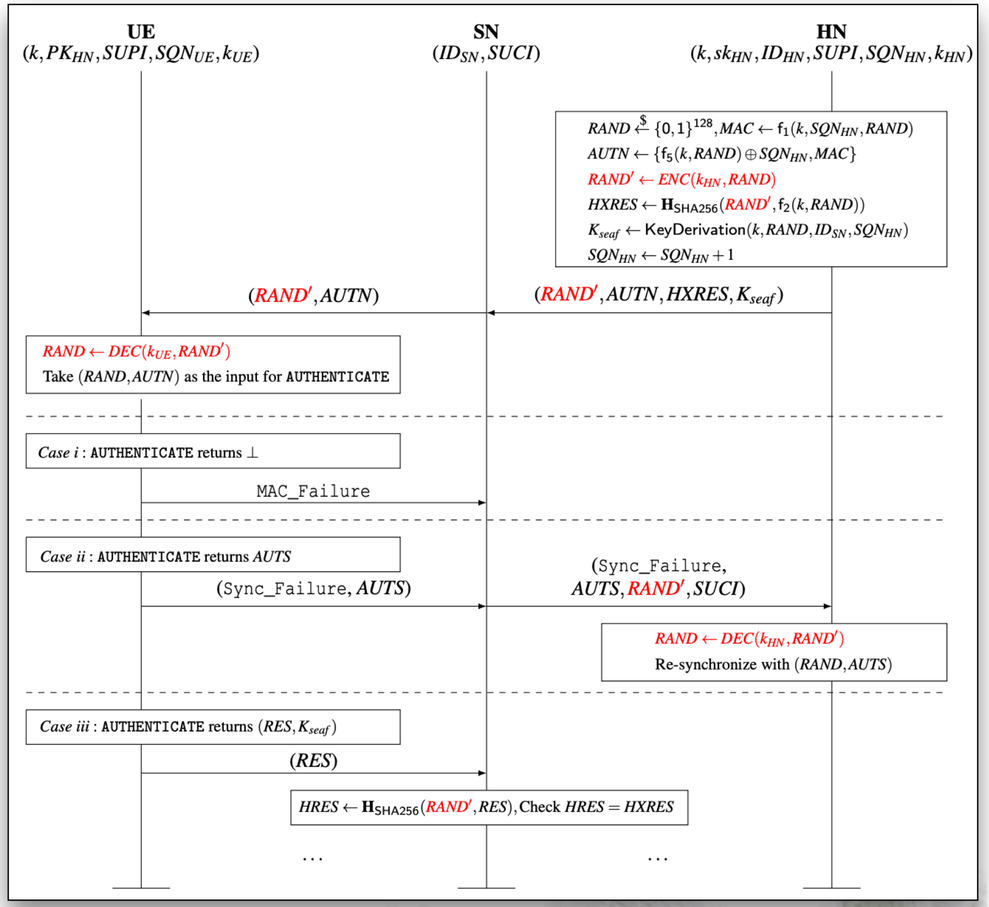
Our solution: 5G-AKA′

- Encrypt *RAND* with the key established by ECIES in the initiation phase
  - ECISE-KEM: establish temporary keys between UE and HN for each session (i.e., k_{UE} and k_{HN}).
  - ECIES-DEM: encrypt the actual payload.
  - HN encrypt, UE decrypt, only $RAND'$ is transmitted
  - The decrypted *RAND* is taken as input for SIM card
  - SIM-card compatibility
- SN only obtains encrypted *RAND*



Our solution: 5G-AKA′

- Encrypt *RAND* with the key established by ECIES-KEM
- SN only obtains encrypted *RAND*
  - *HXRES* is calculated with *RAND′* for comparison
  - HN needs to decrypt *RAND′* for re-synchronization
  - Presverve message syntax (TS 24.008)
    - Encryption without ciphertext expansion
    - Block size of 128 bit (i.e., AES-128-ECB)
  - SN-implementation compatibility



Our solution: 5G-AKA′

- Resistance against failure message linkability attack and sequence number inference attack
  - Attacker replays $(RAND', AUTN)$ or $(RAND, AUTN)$
  - $RAND'$ is encrypted with k_{HN} used in previous session
  - UE decrypts $RAND'$ or $RAND$ with k_{UE} in current session
  - Target UE: decrypt a wrong $RAND$ which cannot pass the check on MAC
  - Non-target UE: also fail the check on MAC
- Resistance against encrypted SUPI replay attack

Our solution: 5G-AKA′

- Resistance against failure message linkability attack and sequence number inference attack
- Resistance against encrypted SUPI replay attack
  - Attacker replays $SUCI$
  - $SUCI$ is encrypted with the k_{UE} used in previous session
  - HN also uses the old k_{HN} to encrypt $RAND$
  - All UEs decrypt $RAND'$ with k_{UE} for current session, and reply with MAC_Failure

Our solution: 5G-AKA′

- Performance of 5G-AKA′
  - Does not raise additional bandwidth cost
  - Only introduces limited additional time cost from 0.02%~0.03%
- The migration from 5G-AKA to 5G-AKA′ may only involve the modification of about 20 Line-of-Code (LoC) for endpoints (i.e., UE and HN)

	UE^1	HN^1	UE^2	HN^2	UE^3	HN^3
5G-AKA	13124.73	835.10	13158.29	853.44	13132.40	847.46
5G-AKA′	13128.65	835.27	13162.44	853.71	13136.25	847.64
time$^+$	3.92 (0.03%)	0.17 (0.02%)	4.15 (0.03%)	0.27 (0.03%)	3.85 (0.03%)	0.18 (0.02%)

Our solution: 5G-AKA′

- Formal Analysis with Tamarin Prover
  - Authentication and Secrecy Goals
    - Follow the lemmas and models established by Basin et al. [BDH+18] for 5G-AKA
    - 5G-AKA′ satisfies the goals for authentication and secrecy as 5G-AKA
  - Privacy Goals
    - Model the case of a target UE and a non-target UE w.r.t., an old session by the target UE
    - 5G-AKA′ is resistant to all known linkability attacks

Point of View	UE		SN		HN	
Partner	SN	HN	UE	HN	UE	SN
Weak agreement	✓	✓	✓	✓	✓	✓
Agreement on K_{seaf}	**I**	**I**	**I**	**I**	**I**	**I**
Agreement on ID_{SN}	wa	**NI**	wa	wa	**NI**	wa
Agreement on $SUPI$	wa	wa	wa	**NI**	wa	-
Secrecy on K_{seaf}		✓		✓		✓

Left Hand System (LHS)	Right Hand System (RHS)
$UE_1'^{\dagger}$	$UE_1'^{\dagger}$
$(k_1, SUPI_1, SQN_{UE_1})$	$(k_1, SUPI_1, SQN_{UE_1})$
⇣	⇣
UE_1	UE_2
$(k_1, SUPI_1, SQN_{UE_1}+1)$	$(k_2, SUPI_2, SQN_{UE_2})$

Conclusions and Takeaways

- 5G-AKA′: A privacy-preserving and standard-compatible AKA protocol for 5G
  - Resistant to all known linkability attacks
  - Compatible with SIM cards and SN implementations
  - May be deployed with only software modifications for both endpoints (i.e., UE and SN)
  - Zero additional bandwidth cost, 0.02%~0.03% additional time cost
- We hope 5G-AKA′ can contribute to the next-phase of 3GPP's 5G standardization process

Thanks for the attention !

Privacy-Preserving and Standard-Compatible AKA Protocol for 5G

Yuchen Wang[†,*], Zhenfeng Zhang[†] and Yongquan Xie[§]

[†] Institute of Software, Chinese Academy of Sciences

* Alibaba Group

[§] Commercial Cryptography Testing Center of State Cryptography Administration

Contact: zhenfeng@iscas.ac.cn, yqxie_occsa@163.com