NDSS Symposium 2024

AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials

Hexuan Yu*, Changlai Du*, Yang Xiao†, Angelos Keromytis‡, Chonggang Wang§, Robert Gazda§,
Y. Thomas Hou*, Wenjing Lou*

*Virginia Polytechnic Institute and State University
†University of Kentucky
‡Georgia Institute of Technology
§InterDigital Inc.

VICE

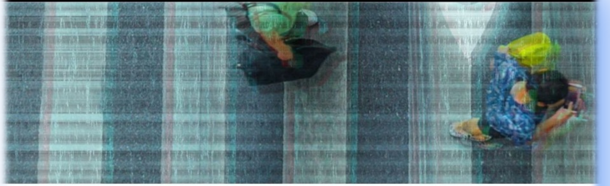


IMAGE: SHUTTERSTOCK. REMIX: JASON KOEBLER

MOTHERBOARD
TECH BY VICE

I Gave a Bounty Hunter $300. Then He Located Our Phone

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

By Joseph Cox

In 2020, FCC proposed over **$200M** fine against the four major carriers (*AT&T, Verizon, Sprint, and T-Mobile*) for **"apparently failing to protect customer location information."**

The New York Times

Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data

Mobile Users’ Location Data Faces Privacy Hazard!

Mobile Network Operators (MNOs) sold or disclosed users’ location information to 3rd parties **without users’ consent:**

- **Location Information Aggregators** (e.g., *LocationSmart, Zumigo*)
    - Then purchased by other **Location-based service (LBS) providers** or **Data Brokers**

- **Unauthorized Law Enforcement Agencies (LEA)** — **Illegal surveillance**
    - Obtain **Cell-site Location Information (CSLI)** *without* a valid warrant/court order

      CSLI: which cell tower a particular mobile device was communicating with

Mobile Tracking — A Growing Privacy Concern in the **5G and Beyond Era**

❑ **MNOs** are commercializing user location data …

❑ Profiling and tracking User Equipment(**UE**) is made easier due to

1. **Unprecedented cellular connectivity**

- smartphones, smartwatches, tablets, IoTs, etc

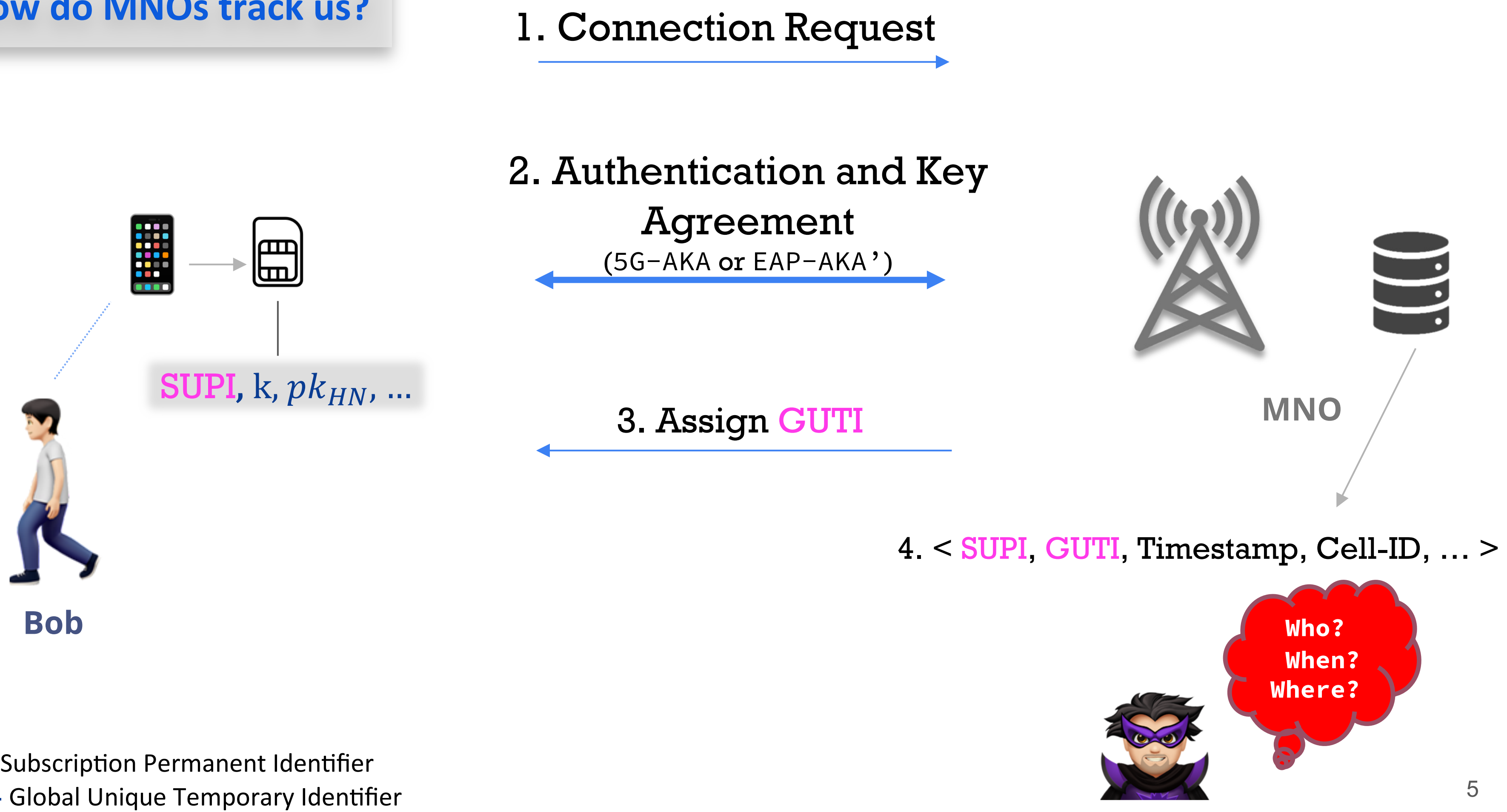
2. **Advancement in 5G localization and positioning technologies**

- Finer-grained accuracy: from *sub-meter* to *sub-centimeter* level

3. **Highly softwarization and virtualization**

- Enlarged attack surface

How do MNOs track us?



SUPI - Subscription Permanent Identifier
GUTI - Global Unique Temporary Identifier

Related Works of Preserving **UE Privacy**

Most existing works are against outsiders, e.g.,

1) Enhance the present **5G-AKA protocol** and resist *linkability* attacks

   e.g., linkage brought by the stateful SQN synchronization.

   5G AKA+ (EuroS&P' 19) , AKA' (Usenix Security' 21) ...

2) Provide unpredictable GUTI Reallocation Mechanism (NDSS' 18)

   Infrequent refreshing renders 5G-GUTI a quasi-permanent identifier (*linkability*)

Existing works that against insiders (i.e., MNO):

1) ZipPhone (WiSec' 20)

   Model and quantify the location predictability and trajectory attacks

   Assume subscribers have the capability to update their permanent ID — *unpractical*

2) PGPP (Usenix Security' 21)

   Nullify **SUPI** — replaced by a token

   Rely on third-party components for authentication

Our Contributions (1/2) — Enhanced **UE Privacy** & Practicality

AAKA: Anonymous Authentication and Key Agreement

An Anti-Tracking Cellular Authentication Scheme utilizing *Anonymous credentials (AC)*

- Against **untrusted MNOs** (i.e., **insider**)
  - **Anonymity**
    - Allow subscribers to access the network **anonymously** without revealing permanent IDs (**`SUPI`**)
  - **Unlinkability**
    - Different sessions for a single UE are **indistinguishable**, thus making a UE *untraceable*
- Against **outsider**
  - Eavesdropping, impersonation, replay protection, etc
    - e.g., IMSI-Catching

Our Contributions (2/2) — Enhanced UE Privacy & **Practicality**

❑ **Accountability** — legal requirement, e.g., 3GPP Lawful Interception (LI)

Cryptographic Guarantee ✓

- Allow **lawful de-anonymization** under certain conditions
  - e.g., Geofence Search Warrant
- Prevent **massive surveillance**
  - De-anonymizing a target UE requires the collaboration of **MNO** and **authorized LEA** — a single party cannot abuse user data

❑ **Compatibility and Efficiency**

- Do not rely on **TTP**
- Do not introduce extra components to the existing 5G cellular architecture
- Minimal computation overhead on standard SIMs + constrained host devices

AAKA — Threat Model

Semi-Honest — MNOs — Home Network(**HN**) and Serving Network(**SN**)

- Want to learn user's location information
- Would follow the prescribed protocols correctly

Root of Trust — SIM

- All the confidential materials (e.g., keys) are provisioned into the SIM
- **Tamper-resistant** — cannot be modified without MNO's admin keys

Semi-Honest — ME (Mobile Equipment, e.g., phone)

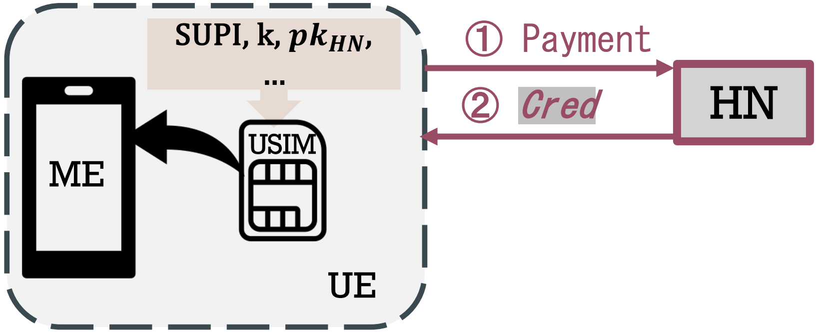
- Non-critical computations can be *optionally* offloaded from SIM to ME
- Computation is carefully splitted to make sure that the subscription credentials are *non-transferable*

AAKA Overview — High-level Workflow

AAKA consists of two sub-protocols:

(1) a subscription credential issuance protocol

HN issues **UE** a verifiable credential ② ***Cred*** based on its subscription status (e.g., right after receiving the ① Payment)



AAKA Overview — High-level Workflow

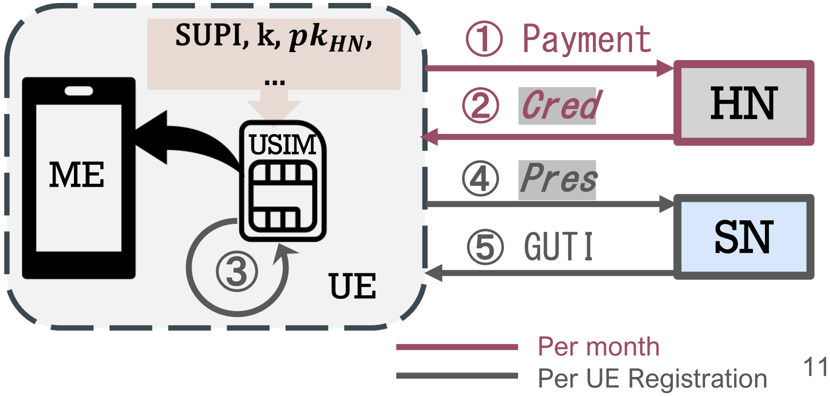
AAKA consists of two sub-protocols:

(1) a subscription credential issuance protocol

HN issues **UE** a verifiable credential ② ***Cred*** based on its subscription status (e.g., right after receiving the ① Payment)

(2) a presentation and verification protocol

③ **UE** derives and presents a one-time verifiable credential ④ ***Pres*** to **SN** and fulfills ⑤ *authentication and key agreement* anonymously (i.e., UE Registration)



Keyed-Verification **Anonymous Credentials** (KVAC)

AAKA leverages KVAC — one type of **Anonymous Credential (AC)**

- Allows users to prove that they satisfy certain properties **without disclosing unnecessary information**
- Constructed using **Algebraic Message Authentication Code**

Integration with other Cryptographic Primitives:

- ❑ **Zero-Knowledge Proof** (ZKP)
- ❑ **BBS signature** scheme (ZKP-friendly)
- ❑ **Commitment** scheme (e.g., Pedersen)

Sub-protocol I — Subscription Credential Issuance

Cred — a Verifiable Subscription Credential

- m_1 – ***Subscription activity status*** (0 or 1)
- m_2 – ***Time of Expiration*** (e.g., 01012024)
- m_3 – ***Home Network ID***, *i.e., MCC* (3-digit, e.g., 999) + *MNC* (2-digit, e.g., 70)
- m_4 – ***MSIN*** (The only unique field in **`SUPI`**, e.g., 000058610)

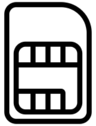
Cred – $(\vec{m}, \sigma, \{\sigma_i\}_{i=0}^{4})$

1) 4 attributes $\vec{m} = (m_1, m_2, m_3, m_4)$;
2) Digital signature (`BBS signature`) from Home Network :

$$\sigma = g_1^{\frac{1}{x_0 + \sum_{i=1}^{4} m_i x_i}} \qquad \sigma_i = \sigma^{x_i} \ for \ \ i = (0, \dots, 4)$$

Securely provisioned into **SIM** by Home Network through `Over-the-Air(OTA)provisioning` process

Cred →



Sub-protocol II — Presentation and Verification

Pres —
a <u>one-time</u> Verifiable Subscription Credential

$\boldsymbol{m_1}$ – ***Subscription activity status***
$\boldsymbol{m_2}$ – ***Time of Expiration***
$\boldsymbol{m_3}$ – ***Home Network ID***
$\boldsymbol{m_4}$ – ***The Hidden Attribute*** *that conceals subscriber's ID*

1. Credential ***Cred*** Blinding

a) Only disclose $\boldsymbol{m_1}, \boldsymbol{m_2}, \boldsymbol{m_3}$, and hide $\boldsymbol{m_4}$

b) Randomize the original signatures $\sigma, \{\sigma_i\}_{i=0}^{4} \longrightarrow \sigma', \{\hat{\sigma}_i\}_{i=0}^{4}$

2. Identity Escrow Function Generation

a) Escrow (encrypt) $\boldsymbol{m_4}$ under LEA's $pk(\boldsymbol{h})$: $(c_1, c_2) = (g_1^r, \boldsymbol{m_4}\boldsymbol{h}^r)$

for target de-anonymization under legal circumstance

a) Commit that the escrowed tuple is genuine

Sub-protocol II — Presentation and Verification (cont'd)

The <u>One-time</u> Verifiable Subscription Credential

- m_1 – *Subscription activity status*
- m_2 – *Time of Expiration*
- m_3 – *Home Network ID*
- m_4 – ***The Hidden Attribute** that conceals subscriber's ID*

Escrowed Identity

$$(c_1, c_2) = (g_1^r, m_4 h^r)$$

Task A: Demonstrate the **authenticity of the randomized signature** given both **revealed** and **hidden** attributes

Task B: They are the same value.

Zero-knowledge Proof

$$\pi \in ZKP\{(m_4, r) : A = g_1^r \hat{\sigma}_4^{-m_4} \wedge A = g_1^r \hat{\sigma}_4^B \wedge -B^{-1} c_2 = h^r \wedge c_1 = g_1^r\}$$

$$e(\bar{\sigma}, g_2) \stackrel{?}{=} e(\sigma', X_0)$$

*Non-interactive zero-knowledge protocol (**NIZK**) via Fiat-Shamir heuristic*

AAKA – The Key Properties

The ZKP π allows **UE** to prove:

i. ***validity* of Cred without revealing**

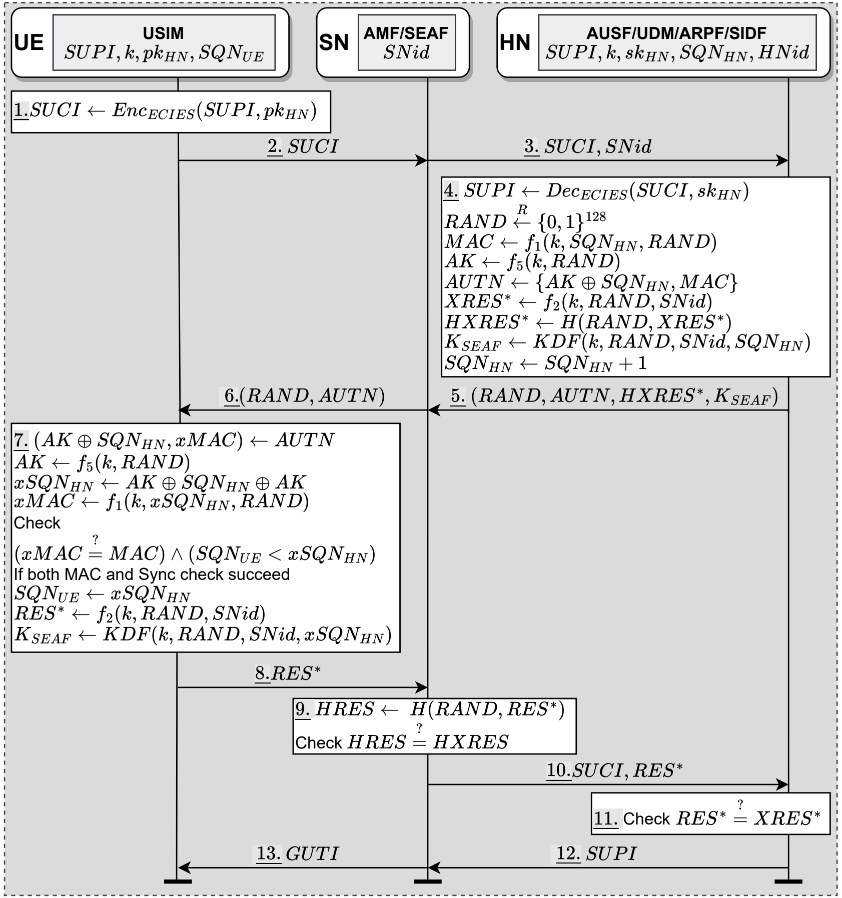
- Identity $\boldsymbol{m_4}$ — Anonymity
- Original signatures $\sigma, \{\sigma_i\}_{i=0}^{4}$ — Unlinkability

ii. ***consistency* of the <u>escrowed identity</u>** — Accountability

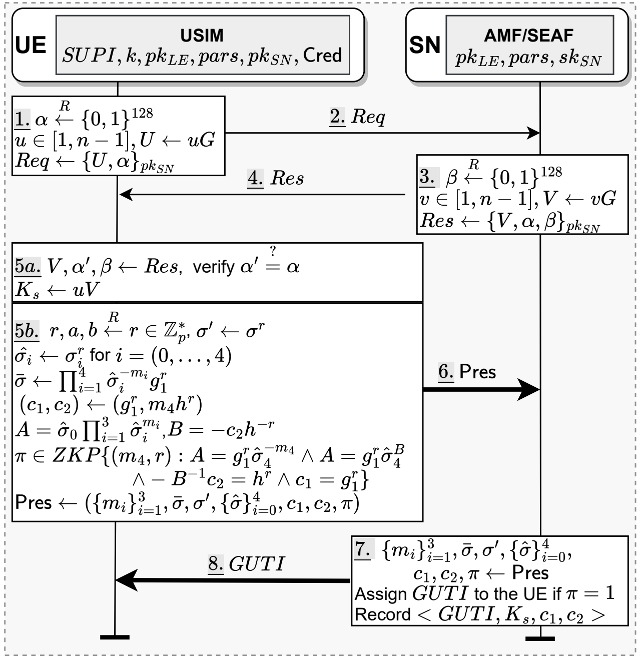
- If *Lawful De-anonymization* is needed —

  only authorized LEA can decrypt the **Escrowed Identity** tuple

5G-AKA



AAKA

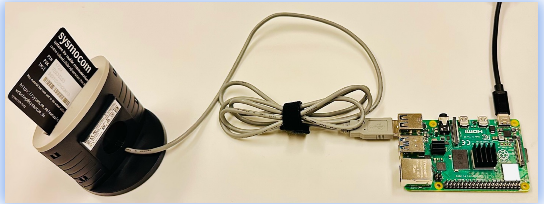


It accomplishes:

- <u>Mutual AKA</u> between **MNO** and **UE**
- Generation of the <u>shared session key</u> K_s
- Assignment of the <u>temporary ID</u> (**GUTI**)

Experimental Environment

MNOs : a standard PC (Intel Core i7-11700k, 3.6GHZ, 8-core, 64-bit CPU with a Linux OS)



UE:

Two standard programmable **SIMs**:

- ❑ Card **A** (standard cellular SIM), *sysmoISIM-SJA2*, 64KB EEPROM.
    - Contains standard **5G EF file** structure (e.g., **SUPI**, k)
    - Only supports Java Card SDK 2.2.1
- ❑ Card **B** (a general-purpose Java Card), *NXP JCOP J3R110*, 110KB EEPROM.
    - Supports Java Card SDK 3.0.5 (allows EC point scalar, SHA-256, etc)

ME : Raspberry Pi 4 (1.5GHz 64bit quad-core Cortex A72 ARM v8, 4GB RAM and 64GB SD card**)**

Performance Results

TABLE III: **Time Consumption** (in milliseconds) of different stages in AAKA Protocol

HN		UE			SN	
Issue	Verify	Obtain	Req + SNAuth	PresGen	Res	Verify
1.87	1.09	38.66	131.30	51.72	0.078	4.51

5G-AKA as the **benchmark**

- Standard cryptographic parameters and libraries
  - ANSI-X9.63 KDF, Curve 25519 in Montgomery form, BN-254, pySim, GlobalPlatform Pro. etc.

A **credential presentation generation** takes ~52 ms on **UE**

A **credential verification** takes ~4.6 ms on **SN**

Comparison to 5G-AKA

- In **non-roaming** case: **AAKA** introduces approx. 50% (~60 ms) of computation overhead
- In **roaming** case: even less overhead, as communications between **SN** and **HN** are eliminated (non-interactive roaming support)

Thank you for your attention!

Q&A