Advanced Network Security

Mobile telephony

Fabian van den Broek

Agenda

- Introduction
- 2G / 3G / 4G
  - Security
    - Authentication
    - Cryptography
- Eavesdropping
- Privacy
  - Tracking
  - A solution: PMSI

Telephony security

Source: https://nl.wikipedia.org/wiki/Almon_Strowger

Telephony security

Source: http://sites.psu.edu/thedeepweb/2015/09/17/captain-crunch-and-his-toy-whistle/

Introduction

- Standards by ETSI and 3GPP
- 2G: GSM (Global System for Mobile Communication)
- 2.5G: GPRS (General Packet Radio Service)
- 3G: UMTS (Universal Mobile Telecommunications System)
- 4G: LTE (Long Term Evolution)
- 5G
- About 8.5 billion connections and 5 billion subscribers

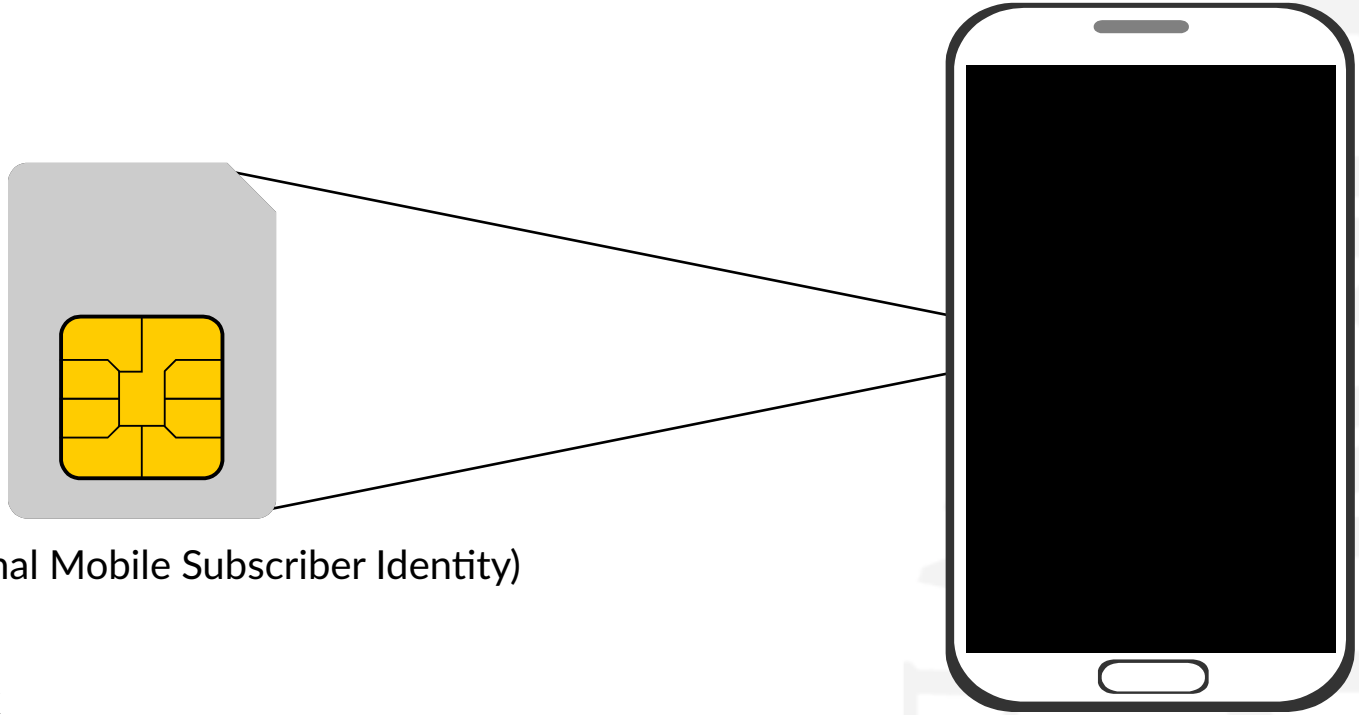
2G (GSM)

- 1G was analogue without any encryption in place
- 2G deployed in 1990s
- 2G is digital and provides authentication and encryption
- Still relevant for ICS/SCADA systems (e.g. ERTMS)

GSM-R

- Part of ERTMS (European Rail Traffic Management System)
- Used for communication between personnel as well as trains and track-side equipment
- Used, for example, to grant trains permission to drive on parts of the tracks and to provide speed limits

Identifiers

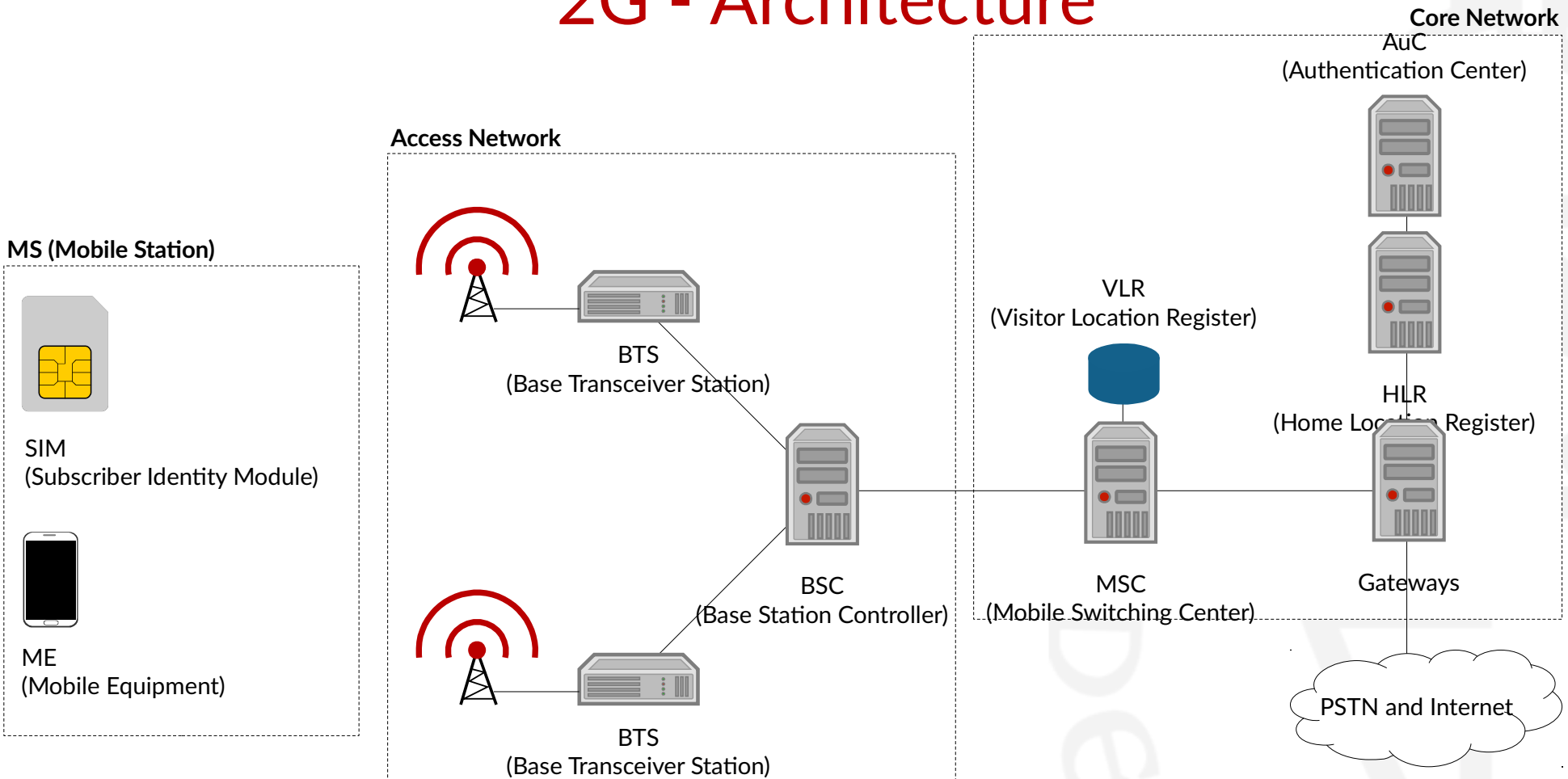


IMSI (International Mobile Subscriber Identity)

- Home country
- Home network
- User

IMEI (International Mobile Equipment Identity)

2G - Architecture



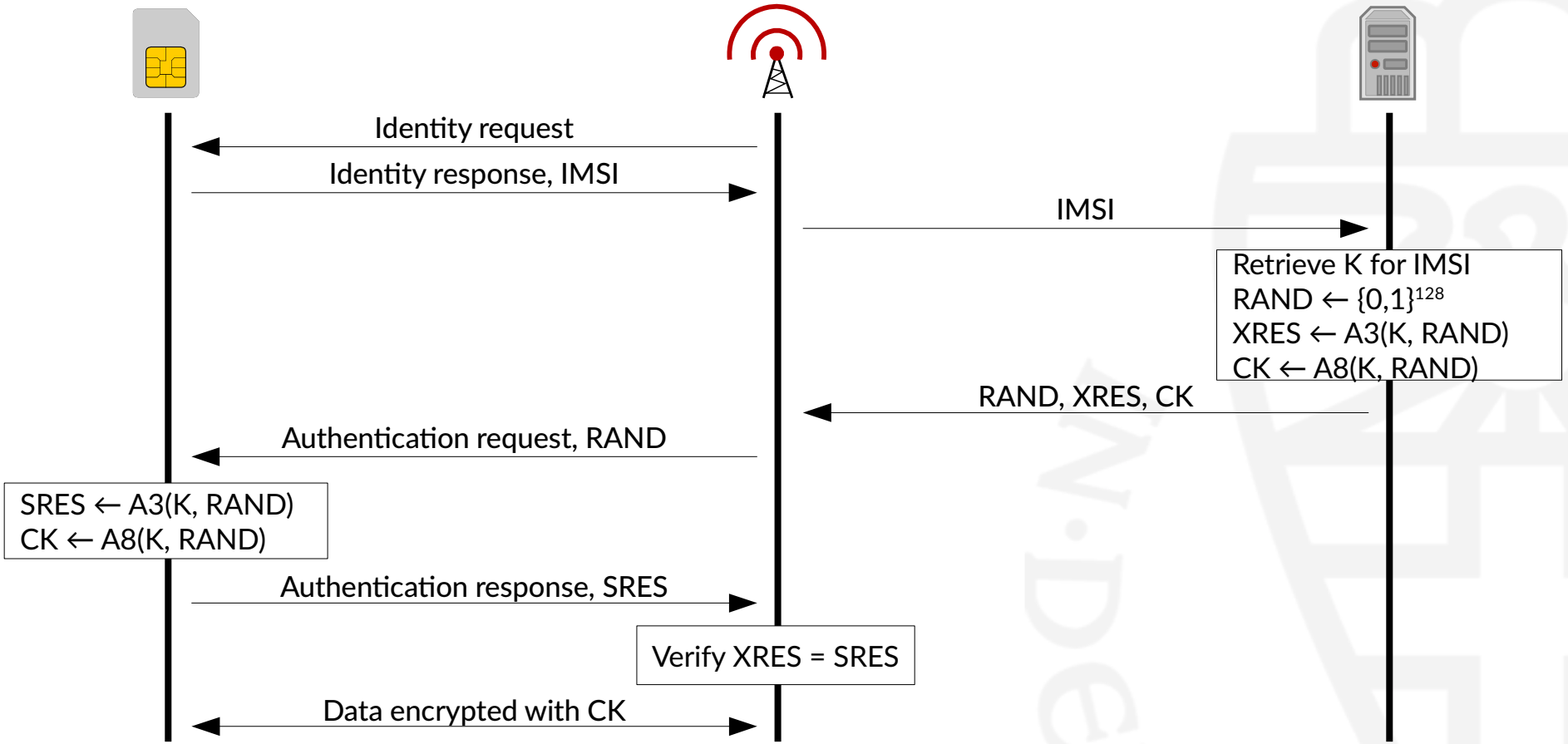
2G - Architecture

- Visitor Location Register (VLR) keeps track of phones present in its area
  - Mapping between IMSI and TMSI
- Home Location Register (HLR) stores permanent information about subscribers
  - Authentication Center (AuC) stores long-term shared secrets with SIMs

2G - Authentication

- Authentication and Key Agreement (AKA)
- Shared symmetric key K between SIM and home network
- Two algorithms, A3 and A8
  - Can be determined by the provider

2G - Authentication



Roaming

- Phone can use a network different than its providers network
  - Visited Network (VN) or Serving Network
  - Home Network (HN)
- Visiting Network requests authentication information from Home Network
- Authentication information provided by Home Network
- Visited Network performs authentication
- Visited Network reports presence of phone
  - Home Network informs previous network that phone left
- Home Network keeps track of the current location of its subscribers
  - Necessary for, e.g., incoming calls

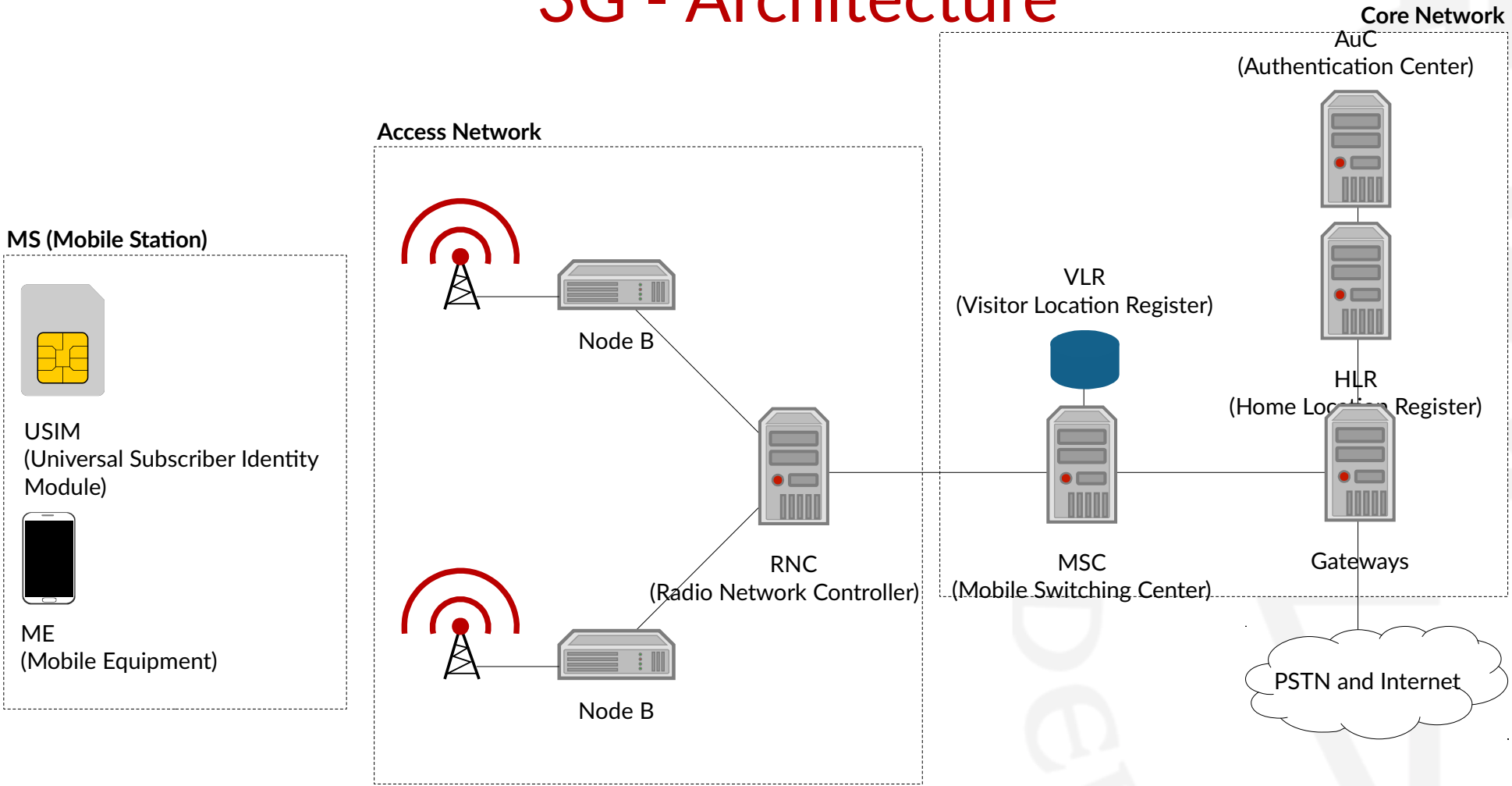
2G - Encryption algorithms

- A5/0
  - No encryption
- A5/1
  - Proprietary stream cipher
- A5/2
  - Weaker cipher for export
- A5/3
  - KASUMI, a block cipher based on MISTY
    - Used with 64 bit keys

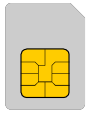
3G (UMTS)

- 3G (UMTS) introduced in 2001
- Algorithms used for encryption and MACs
  - KASUMI (128 bit key)
  - SNOW 3G, stream cipher by Lund University
- Mutual authentication

3G - Architecture



3G - Authentication



Identity request

Identity response, IMSI

IMSI

Retrieve K and SQN for IMSI
RAND ← $\{0,1\}^{128}$
MAC ← f1(K,SQN,AMF,RAND)
XRES ← f2(K,RAND)
CK ← f3(K,RAND)
IK ← f4(K,RAND)
AK ← f5(K,RAND)
AUTN ← (SQN XOR AK,AMF,MAC)
Update SQN ← SQN + 1

Authentication request, RAND, AUTN

RAND, AUTN, XRES, CK, IK

AK ← f5(K,RAND)
XSQN ← (SQN XOR AK) XOR AK
XMAC ← f1(K,XSQN,AMF,RAND)
Verify XMAC = MAC
Verify SQN <= XSQN <= SQN + range
Update SQN ← XSQN
SRES ← f2(K,RAND)
CK ← f3(K,RAND)
IK ← f4(K,RAND)

Authentication response, SRES

Verify XRES = SRES

Data encrypted with CK
and authenticated with IK

3G - Authentication

- Functions f1 to f5 not standardised
  - Only used by SIM card and provider's authentication server
- Recommendation for f1 to f5 is to use Rijndael

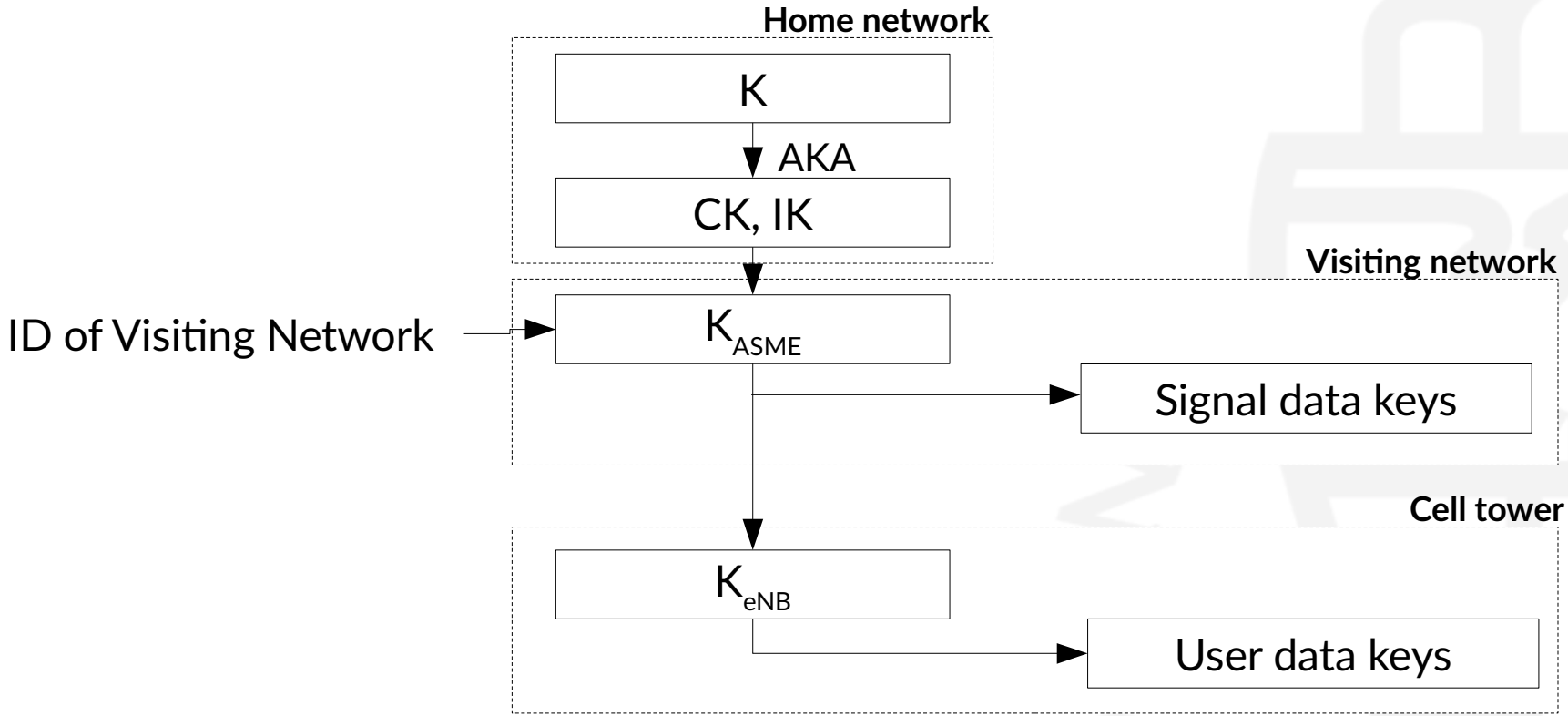
4G (LTE)

- 4G (LTE) introduced in 2010
  - Almost 90% coverage reported by Open Signal in February 2018
- Algorithms used for encryption and MACs
  - SNOW 3G
  - AES
- Cell towers are assumed to be smarter
- Separation between signal and data channel
  - Signal channel encrypted between phone and core network
  - Data channel encrypted between phone and cell tower
  - Possible to perform handover directly between cell towers

4G - Authentication

- Authentication protocol the same as 3G
- More elaborate key hierarchy
  - Reduce times necessary to execute (slow) AKA protocol
  - Cell towers get their own keys
  - Mechanisms to protect against compromise of cell towers

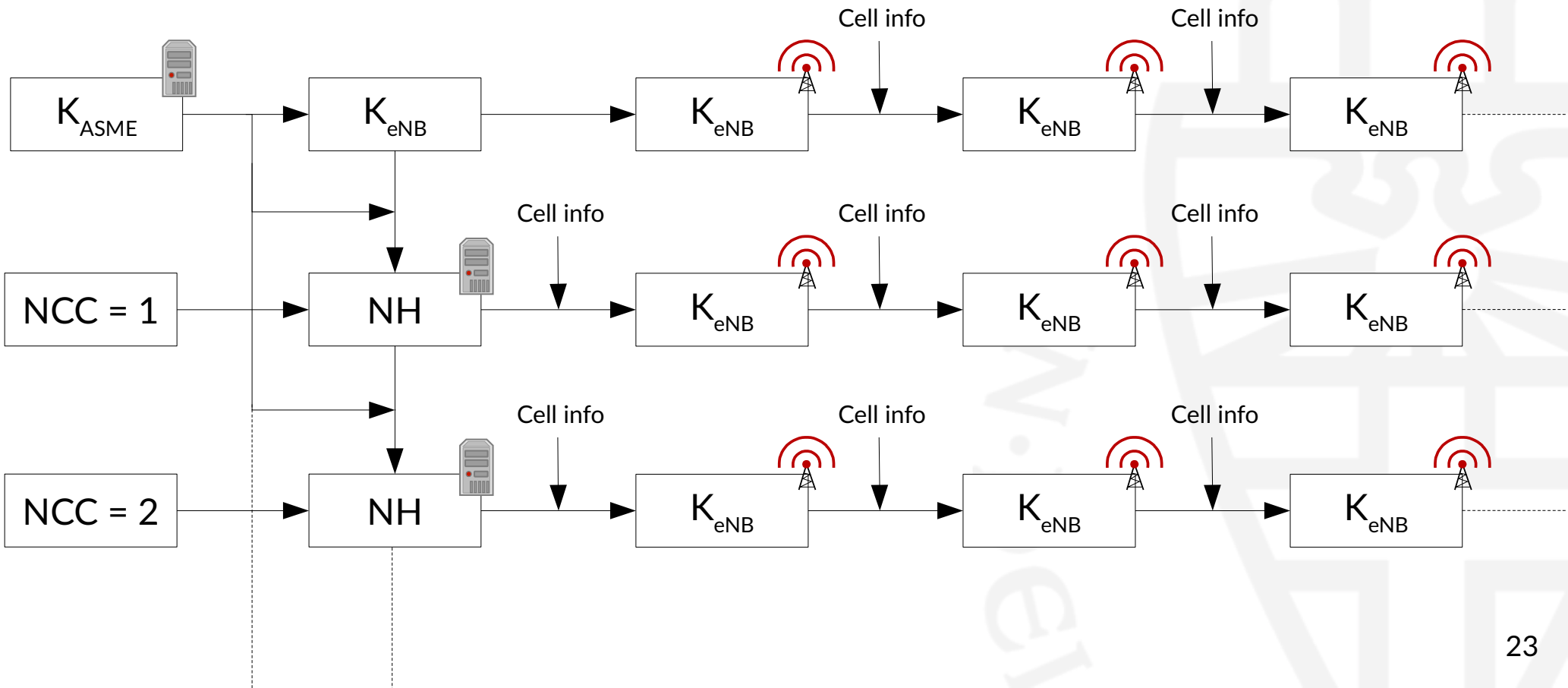
4G – Key hierarchy



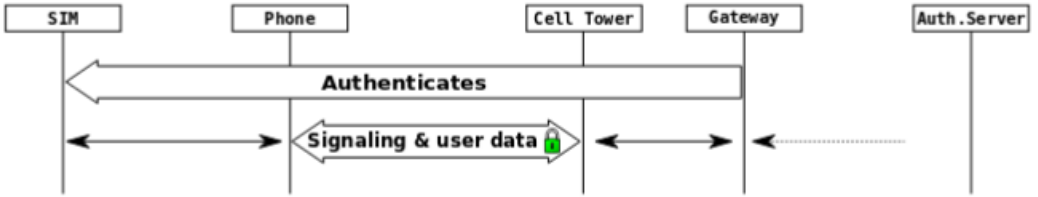
4G - Handover

- Handover between cell towers can be done without interference of backend
- Key update mechanisms to provide forward and backward security
  - Only involving cell towers provides backward security
  - Involving backend also provides forward security
- SIM and backend generate the Next-hop parameter (NH)
  - Based on a shared secret and counter

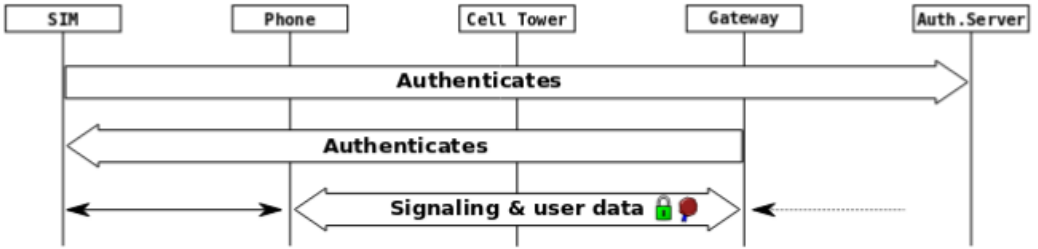
4G – Key derivation



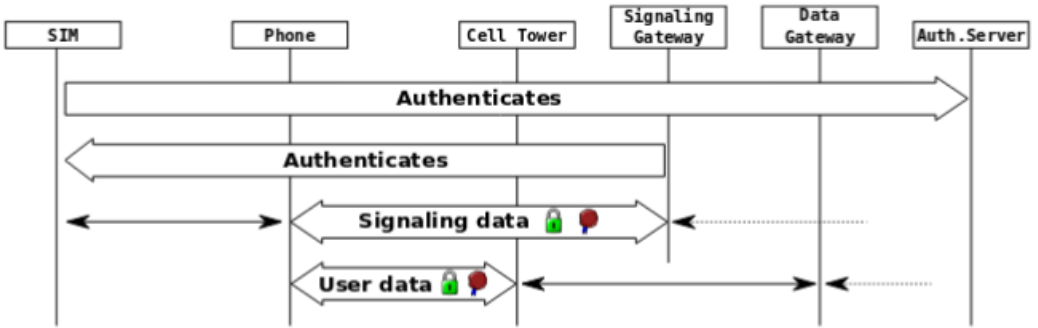
Authentication comparison



(a) GSM



(b) UMTS



(c) LTE

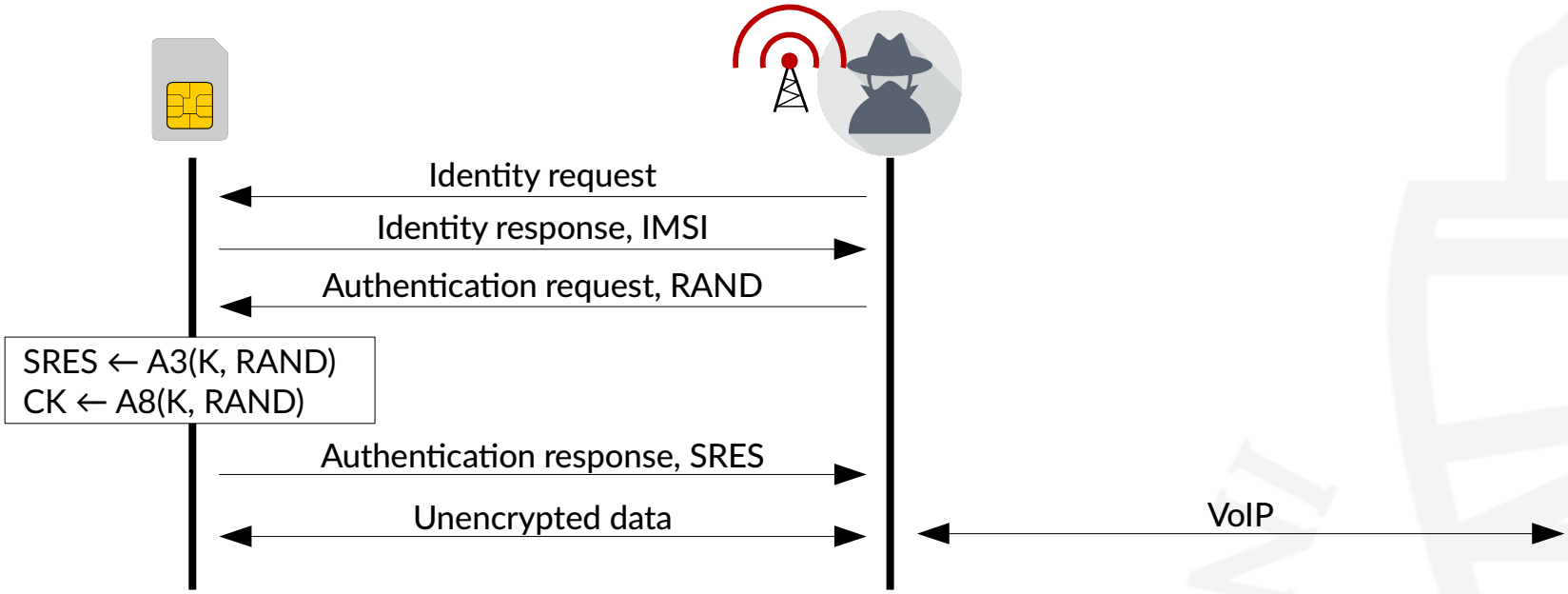
Eavesdropping

- Different approaches
  - Passive
  - Active (i.e. with a man-in-the-middle)
- Works mainly well with 2G
  - Only authentication of the phone
  - Weak or no encryption supported
- Often fallback to 2G is possible

Run your own network

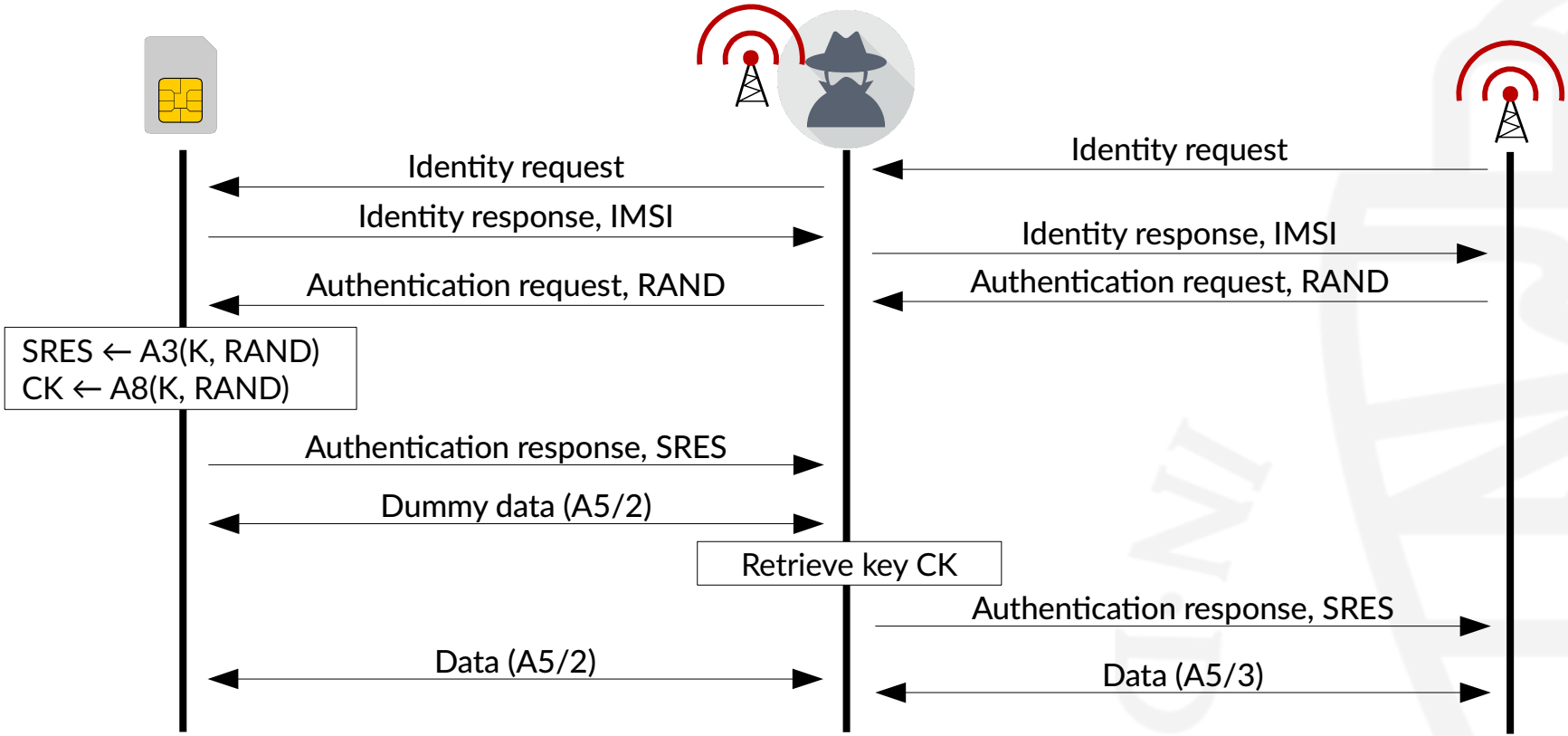
- Possible using a Software Defined Radio (SDR) and open source software (e.g. OpenBTS)
- Pretend to be your victims network and get them to connect to you
  - E.g. by jamming or providing a stronger signal

Man-in-the-middle (2G)



- Use A5/0 (no encryption)
- Forward calls via VoIP
  - No incoming calls

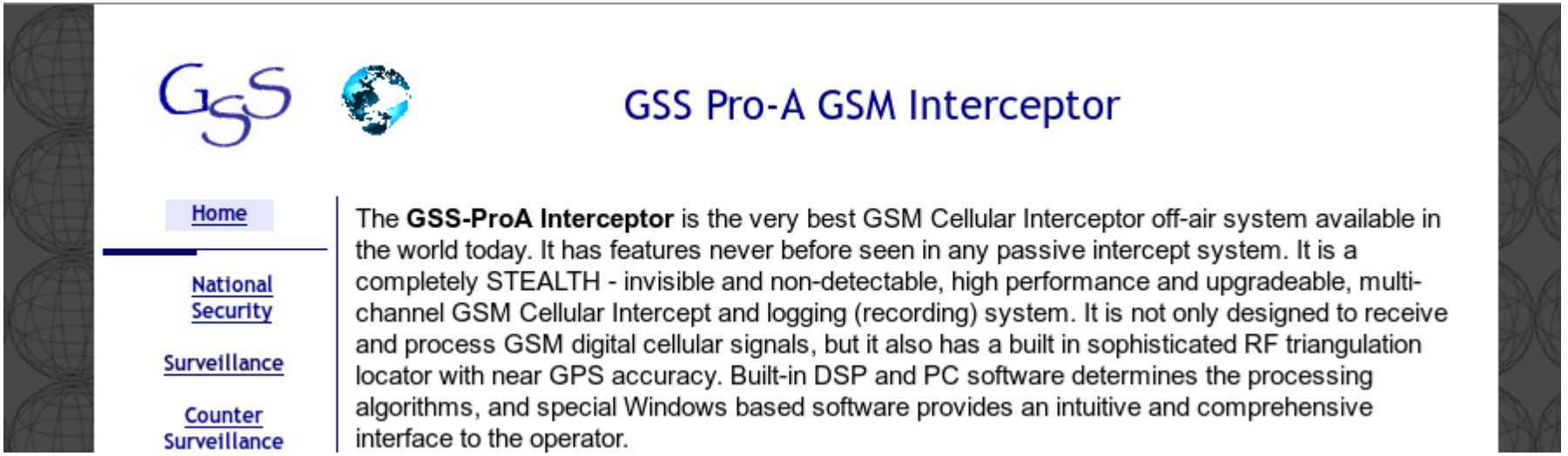
Man-in-the-middle (2G)



Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Barkan et al., 2010

Eavesdropping

- Complete solutions available for governmental organisations

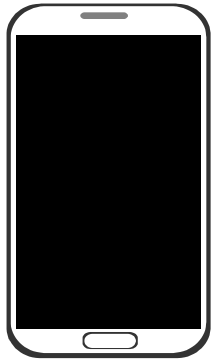


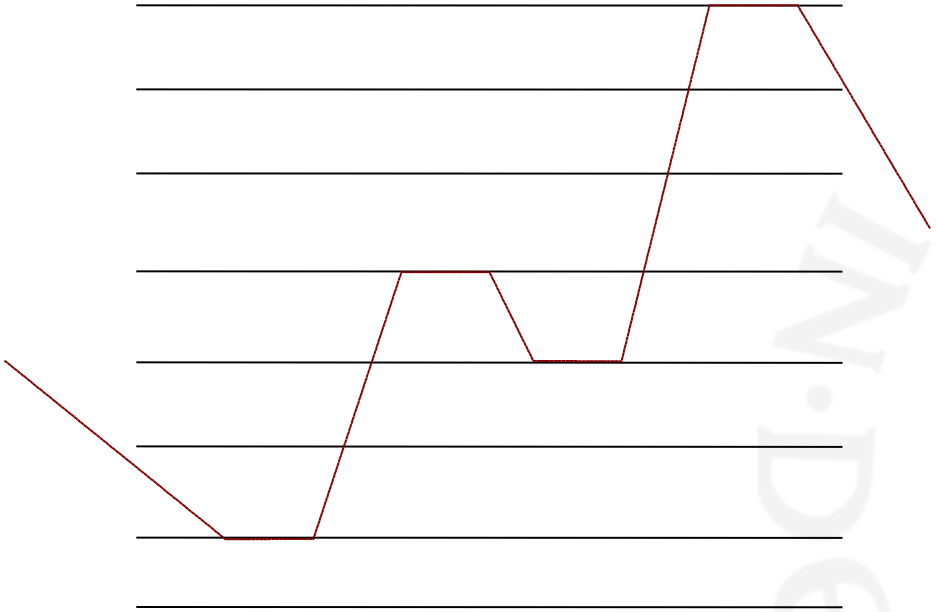
Intercepting signals

- Again using Software Defined Radios (SDR) and open source software (e.g. AirProbe)

Intercepting signals

- Problem: channel hopping
- Solution: multiple or more powerful radios





Cracking A5/1

- Weak algorithm
  - First attack publicly described by Anderson in 1994
  - Many more research since then
- A5/1 is a stream cipher, so if you have known plaintext you have part of the keystream

C. (U) PROCESSING				
C1. (S//SI) The fact that NSA can process **unencrypted** GSM.	SECRET//COMINT REL AUS/CAN/GBR/NZL/USA	1.4 (c)	20291123	
C2. (S//SI) The fact that NSA can process **encrypted** GSM when the cryptovariable is **known.**	SECRET//COMINT REL AUS/CAN/GBR/NZL/USA At a mimimum	1.4 (c)	20291123	
C3. (TS//SI) The fact that NSA can process **encrypted A5/1** GSM when the cryptovariable is **unknown.**	TOP SECRET// COMINT REL	1.4 (c)	20291123	(U) Details may require protection via a special access

Cracking A5/1

- Rainbow tables available to quickly retrieve used key
  - Known as Berlin tables
  - Released in 2010
  - Around 2TB
  - Probabilistic
  - Limited amount of known plaintext necessary
- Shortly afterwards the tool Kraken was released that could use these tables to crack GSM traffic

Cracking A5/2

- A5/2 was purposefully weak for export
- Can be cracked in seconds
  - Barkan et al., 2010
- No longer allowed in new phones since 2007

Cracking A5/3

- Attack published Dunkelman et al. in 2010
- Theoretical attack that might not be practical
- KASUMI weaker than MISTY on which it is based

SS7

- Signaling System 7
- Used in the core network and to communicate between providers
  - For example, used to exchange authentication requests, send location updates and deliver SMS messages
  - From an era where providers trusted each other...
- Originally when sending an SMS
  - Ask Home Network current network of phone (i.e. country and provider)
  - Send SMS directly to the phone's current network
- Fixed when using Home Routing
  - Home Network delivers the SMS
- Might enable intercepting for 3G

POLITICS APRIL 18, 2018 / 1:08 PM / 19 DAYS AGO

Four U.S. senators seek details on unusual cellular surveillance in D.C. area

David Shepardson

3 MIN READ

WASHINGTON (Reuters) - Four U.S. senators on Wednesday urged the U.S. Homeland Security Department (DHS) to disclose additional information about unusual cellular surveillance activity that has been detected around the nation's capital.

Privacy

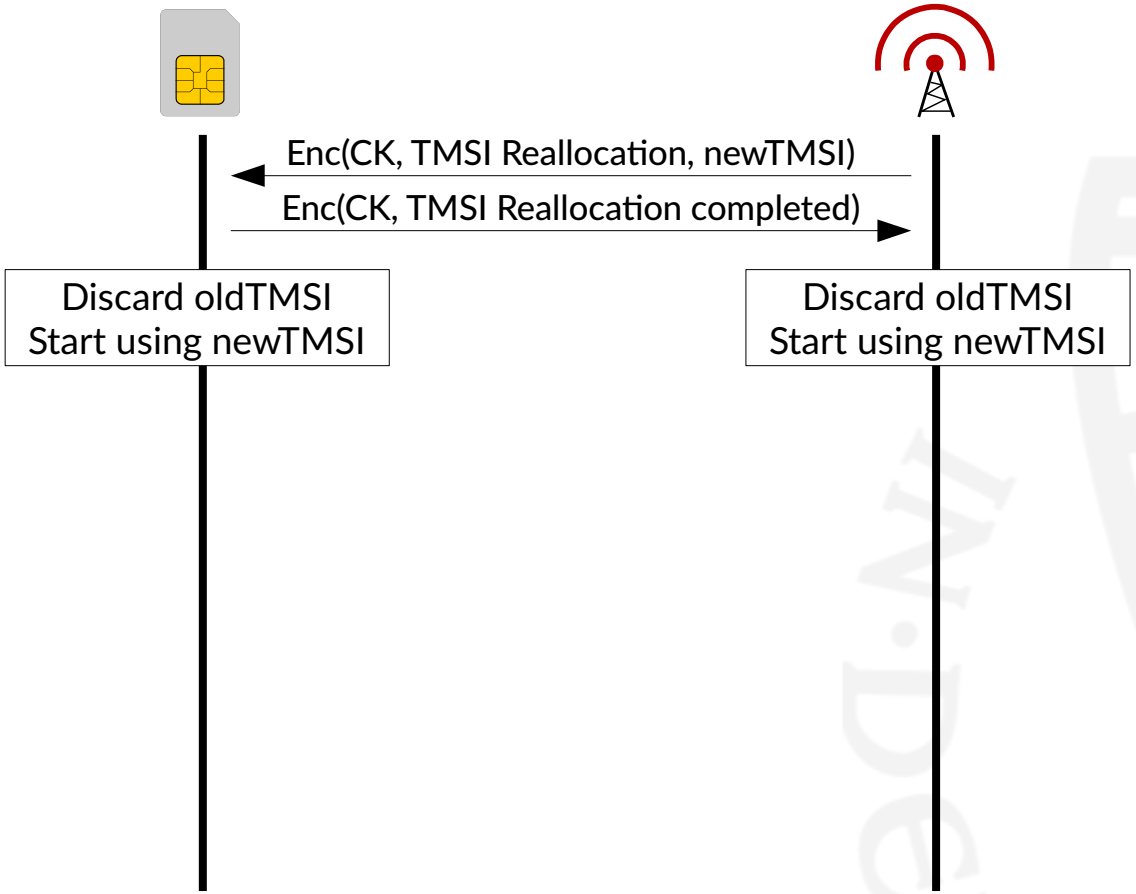
- IMSI catchers (a.k.a. StingRay) can be used to
  - Track users
  - Monitor locations
  - Link identities to devices
- Can pretend to be a base station to get to phones to connect and learn the IMSI

Source: U.S. Patent and Trademark Office / AP Photo

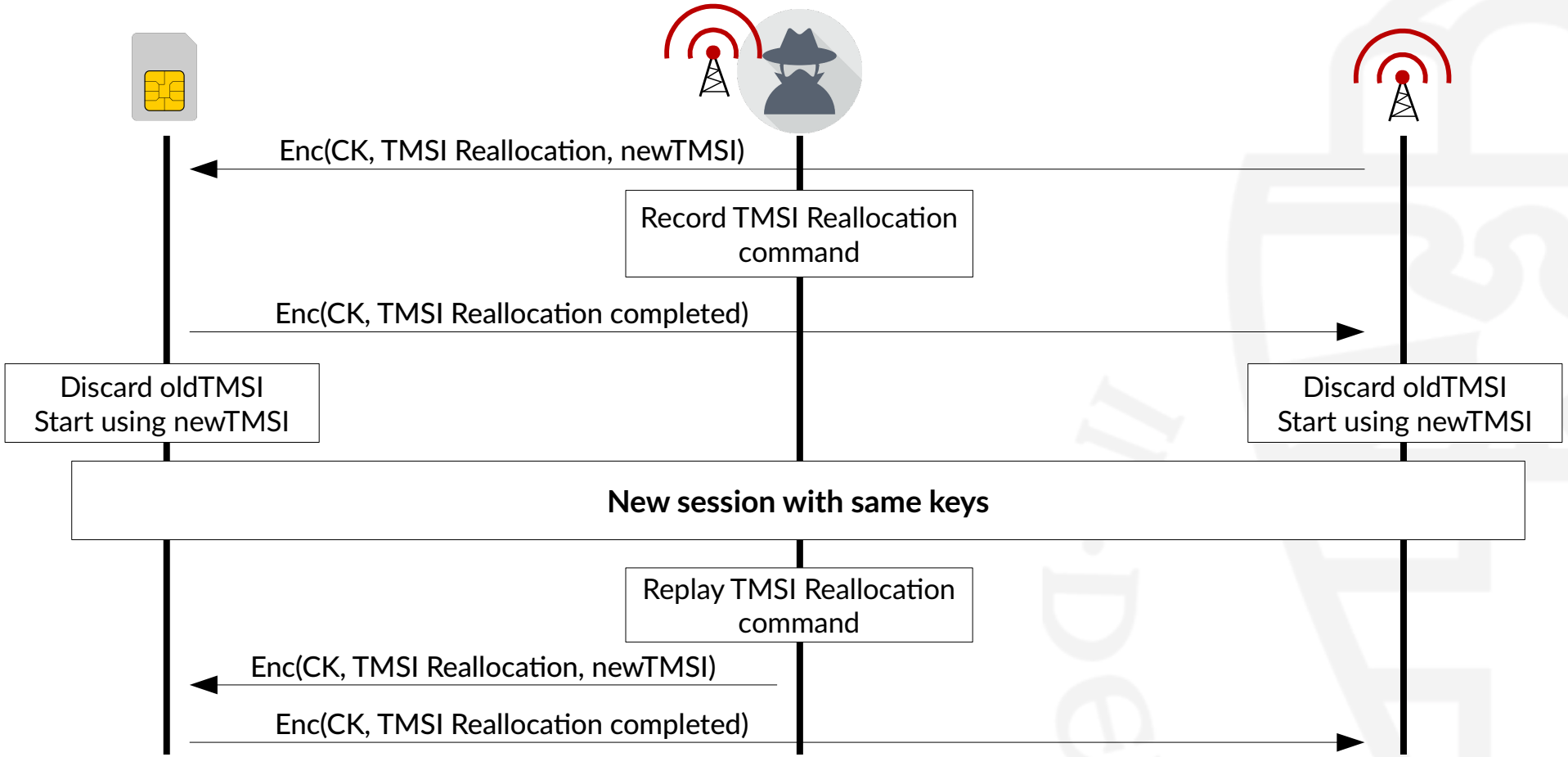
Privacy

- IMSI is always provided upon request
  - No protection provided by mutual authentication
- TMSI introduced to provide some anonymity
  - Temporary Mobile Subscriber Identity
  - Can be used instead of IMSI
  - Provided by the visited network to the phone under encryption
  - Should only be used for one location
- Can we still trace users?

Allocation of TMSI



TMSI reallocation attack



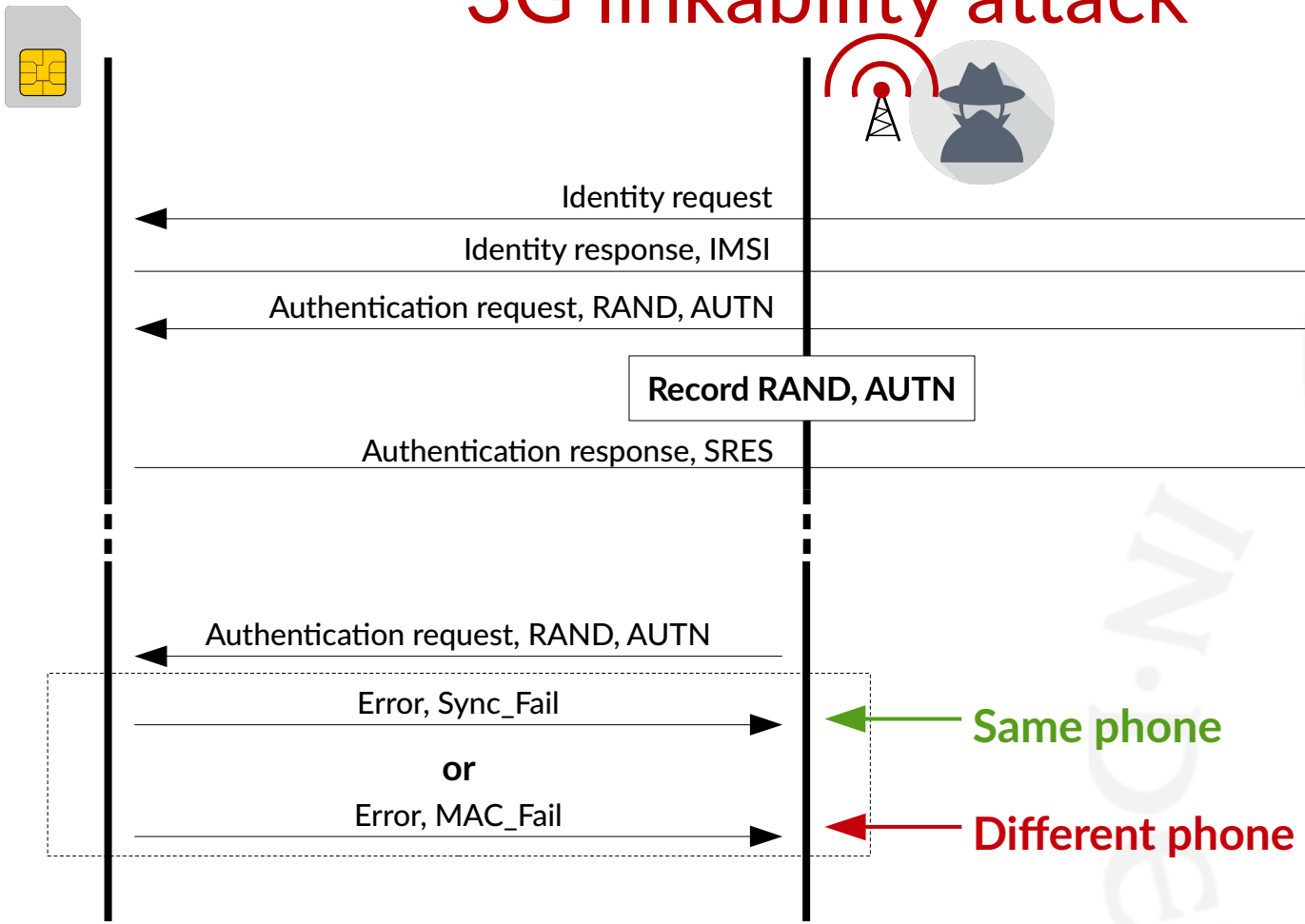
TMSI reallocation attack

- Attack presented by Arapinis et al.
- Attacker records an encrypted TMSI allocation command
- Replay the recorded command later to distinguish victim's phone from others
  - As long as the same keys (CK and, optionally, IK) are used
- Only victim's phone will respond to the encrypted command
  - Other phones will ignore it as decryption fails
- Mainly a theoretical attack

3G linkability attack

- Attack presented by Arapinis et al.
- Attack on 3G's AKA protocol
- Uses the fact that different error messages are used for
  - MAC failure
  - Invalid sequence number

3G linkability attack



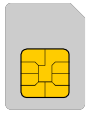
Defeating IMSI catchers

- TMSI does not provide enough protection
  - IMSI can be requested without authentication or encryption
  - Visited network always learns the IMSI
  - IMSI is needed to determine the provider and retrieve the shared key
- How can we protect against the interception of IMSIs?
  - Introduce a new identifier: a temporary pseudonym PMSI
    - Provided by the home network
  - Works with minimal modification to the current standards
    - IMSI catching still possible, but less interesting
  - Additional benefit: mutual authentication for 2G
  - Considered for inclusion in one of the 5G proposals

Defeating IMSI catchers

- PMSI is shared between the SIM and provider
- Same structure as IMSI
  - First part identifies the country and provider
  - Last part identifies the user
- PMSI is used instead of IMSI and is regularly updated
- How do we get the PMSI to the SIM?
  - Hijack the RAND variable

3G / 4G - Authentication



Identity request

Identity response, IMSI

IMSI

Retrieve K and SQN for IMSI
RAND ← {0,1}^{128}
MAC ← f1(K,SQN,AMF,RAND)
XRES ← f2(K,RAND)
CK ← f3(K,RAND)
IK ← f4(K,RAND)
AK ← f5(K,RAND)
AUTN ← (SQN XOR AK,AMF,MAC)
Update SQN ← SQN + 1

RAND, AUTN, XRES, CK, IK

Authentication request, RAND, AUTN

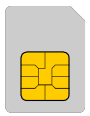
AK ← f5(K,RAND)
XSQN ← (SQN XOR AK) XOR AK
XMAC ← f1(K,XSQN,AMF,RAND)
Verify XMAC = MAC
Verify SQN <= XSQN <= SQN + range
Update SQN ← XSQN
SRES ← f2(K,RAND)
CK ← f3(K,RAND)
IK ← f4(K,RAND)

Authentication response, SRES

Verify XRES = SRES

Data encrypted with CK
And authenticated with IK

3G / 4G - PMSI (simplified)



Identity request

Identity response, **PMSI**

PMSI

Retrieve K, KP and SQN for PMSI
PMSI' ← {0,9}^{10}
RAND ← F(KP,PMSI',SQN)
...

RAND, AUTN, XRES, CK, IK

Authentication request, RAND, AUTN

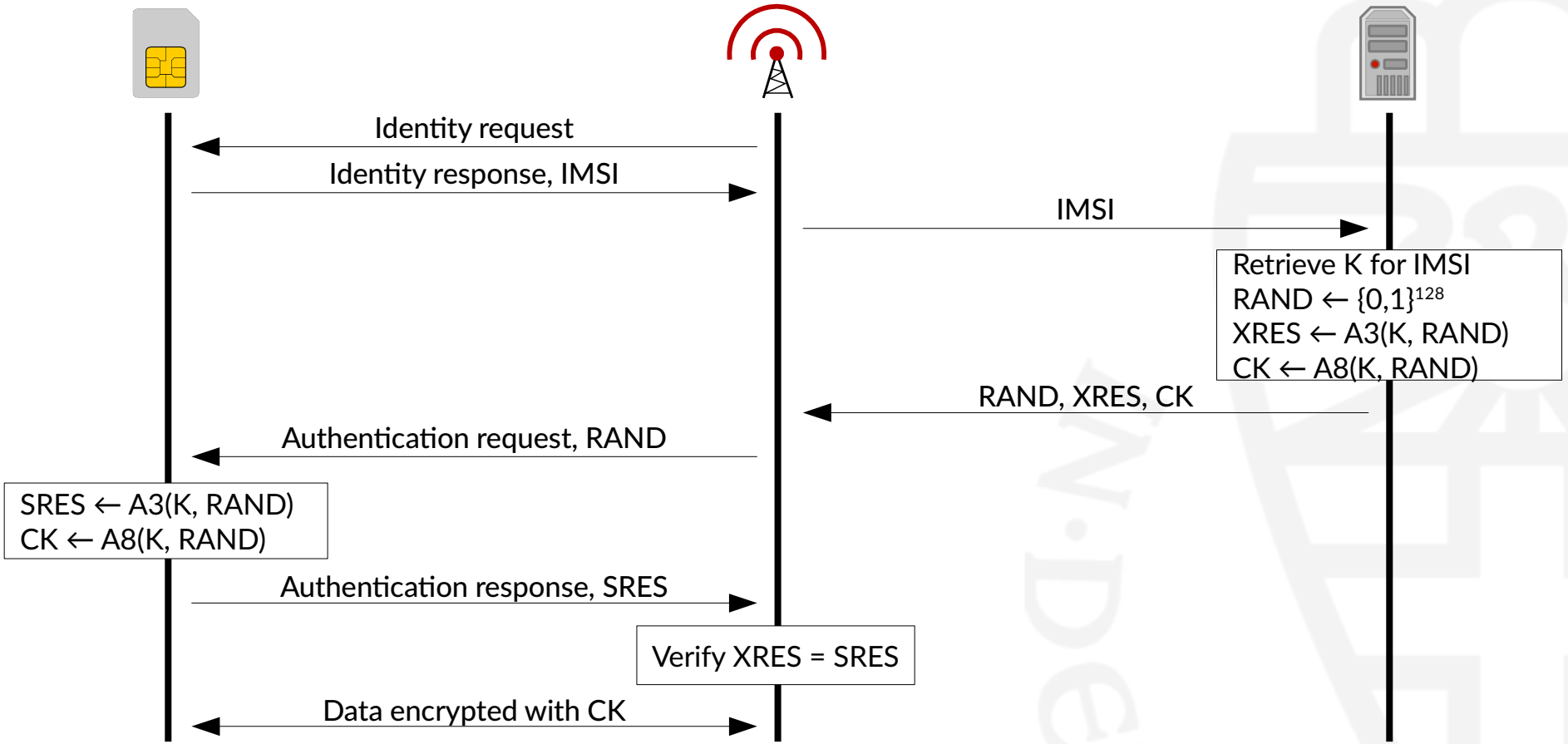
...
PMSI', SQN' ← F^{-1}(KP,RAND)
Verify SQN' = XSQN
Update PMSI ← PMSI'

Authentication response, SRES

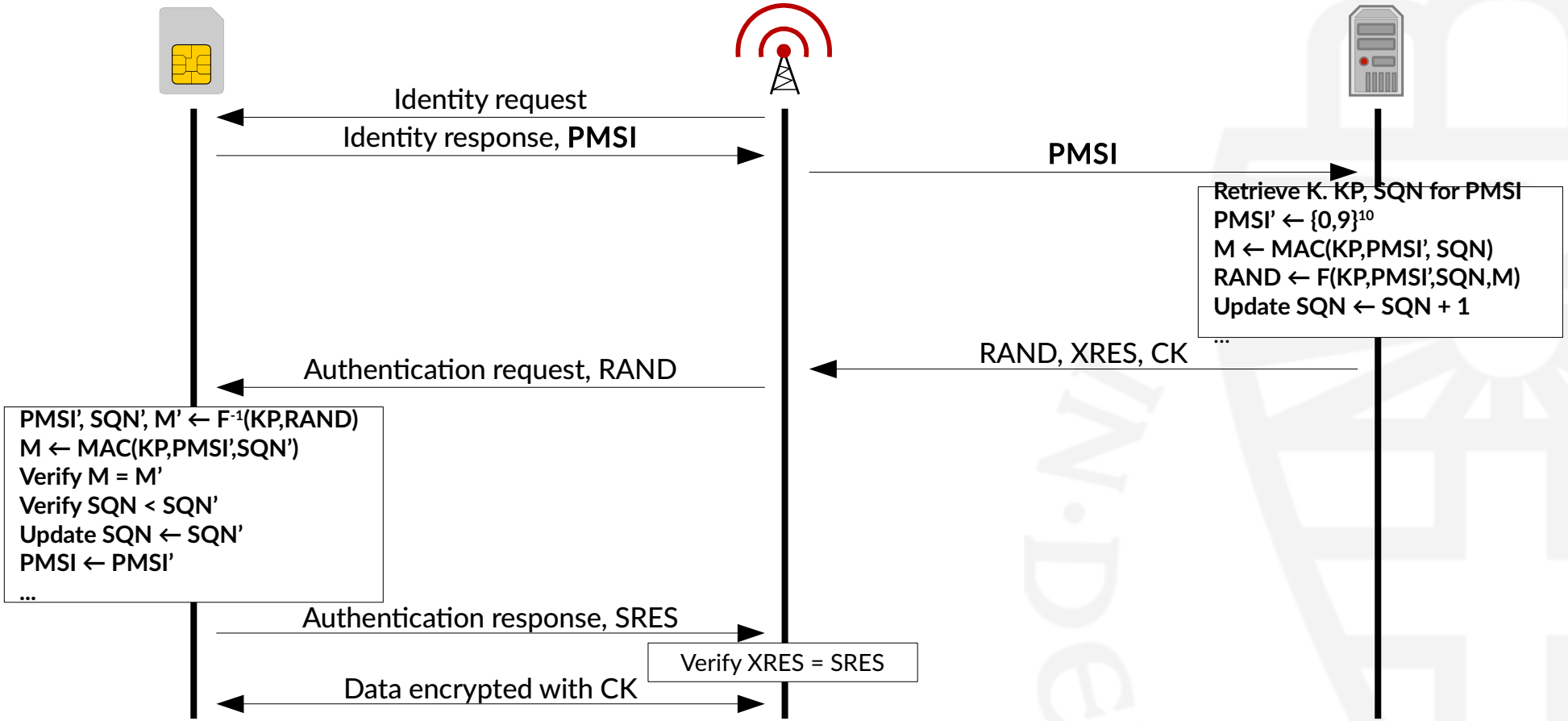
Verify XRES = SRES

Data encrypted with CK
And authenticated with IK

2G - Authentication



2G – PMSI (simplified)



Defeating IMSI catchers

- All values fit within current lengths of used variables
  - No modification of messages needed
- Can be implemented by a single provider
  - Only changes needed in SIM and authentication server
- Actually two PMSIs stored in SIM and at provider
  - Current PMSI
  - Next PMSI
    - Once used promoted to current PMSI and fresh next PMSI generated
- MAC prevents desynchronisation attacks in 2G solution

Further activities

- Read chapters 2 and 3 of:

  Mobile communication security
  Fabian van den Broek
  PhD thesis, 2016

- Optional reading:

  Defeating IMSI Catchers
  Fabian van den Broek, Roel Verdult and Joeri de Ruiter
  22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15), ACM, 2015

  Analysis of privacy in mobile telephony systems
  Myrto Arapinis, Loretta Ilaria Mancini, Eike RitterMark D. Ryan
  International Journal of Information Security, October 2017