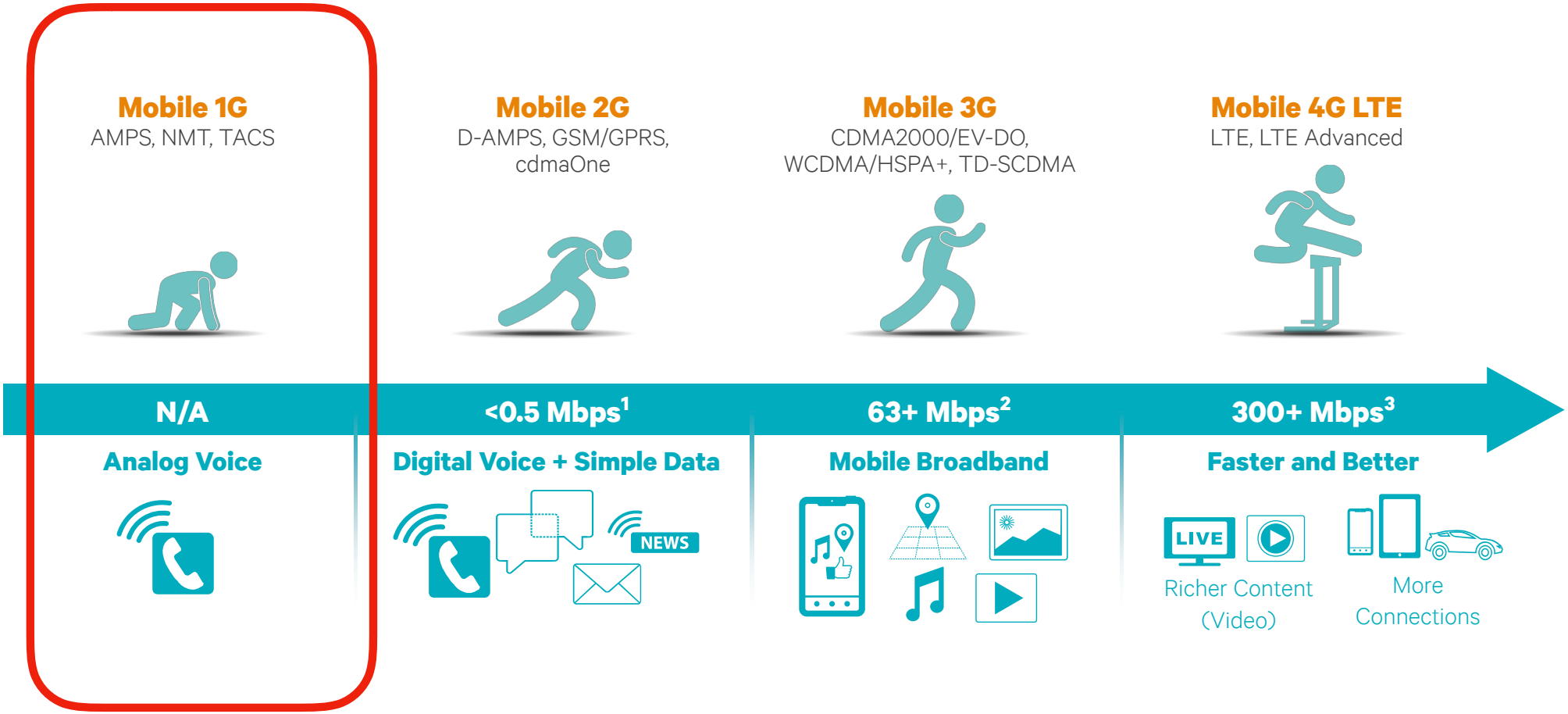
Cellular Network Security
Part 1

Lecture topics

- **Basic concepts** of mobile telephony
- **Evolution** from 1G to 5G
- **Security properties**
  - Authentication, confidentiality, location privacy…
- **Points of vulnerability**
  - Crypto, protocols, physical layer, network management…
- **Trade-offs**
  - Security and performance and cost

Evolution of Cellular Networks

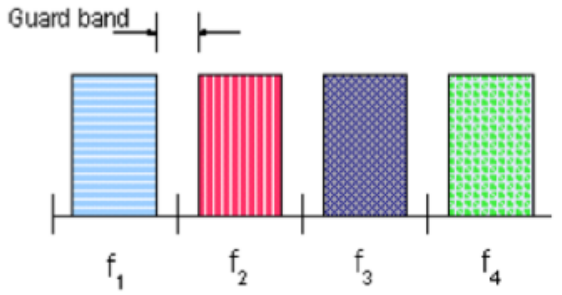


1G overview

- **Analog system**
  - Voice calls (to fixed telephone network)
  - Introduced in early 1980's

- Medium access
  - Available bandwidth split using **FDMA**
  - When call active, one frequency used both directions

- Regional standards
  - Advanced Mobile Phone Service (AMPS) in the US
  - NMT in Nordic countries
  - NTT in Japan
  - …



Main goal: connect mobile phone users to the fixed telephony network

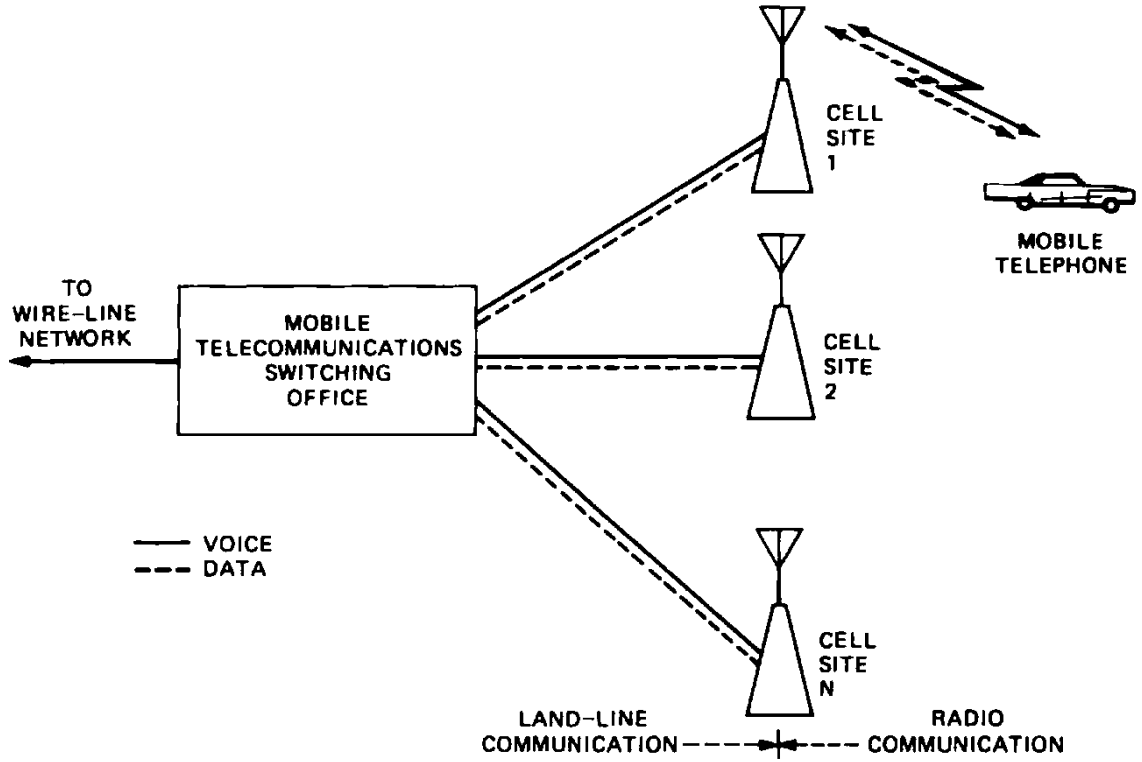


Fig. 3—AMPS system control elements.

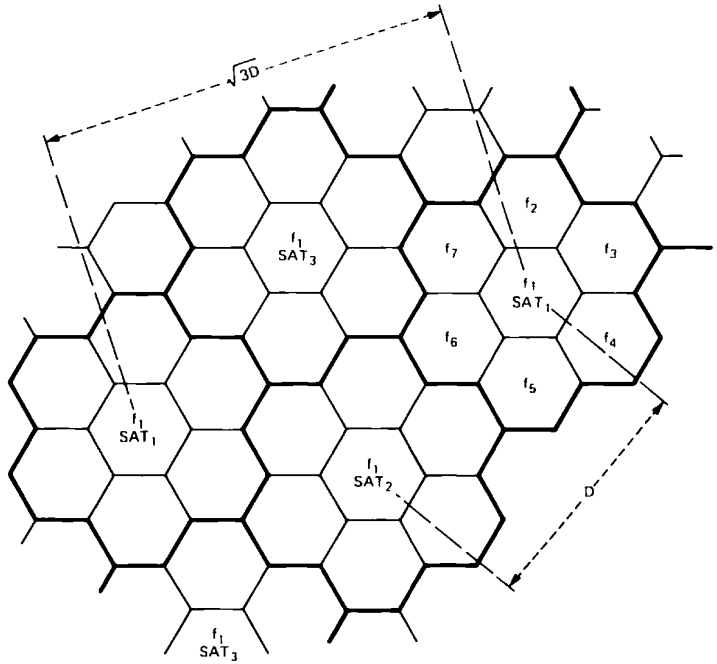
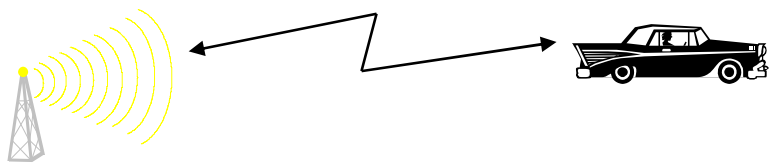


Fig. 5—SAT spatial allocation.

Functionality 1: Mobile Originated Call



Pass to PSTN ← Origination message (MIN, ESN, called party)

Control message → Tune to voice channel

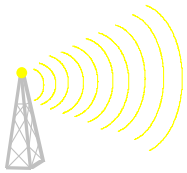
Send supervisory signal to confirm forward channel →

Answers and starts conversation ← Send supervisory signal to confirm reverse channel

MIN = Mobile Identification Number
ESN = Electronic Serial Number
PSTN = Public Switched Telephone Network

source: University of Pittsburg lecture 2720

Functionality 2: Mobile Terminated Call

Base station    **Mobile station**

Mobile ID from PSTN; page control message →

Receives page

← Page response message (MIN, ESN)

Control message; tune to voice channel →

Tune to voice channel

Send supervisory signal to confirm forward channel ↔

Send supervisory signal to confirm reverse channel

Functionality 3: Handover

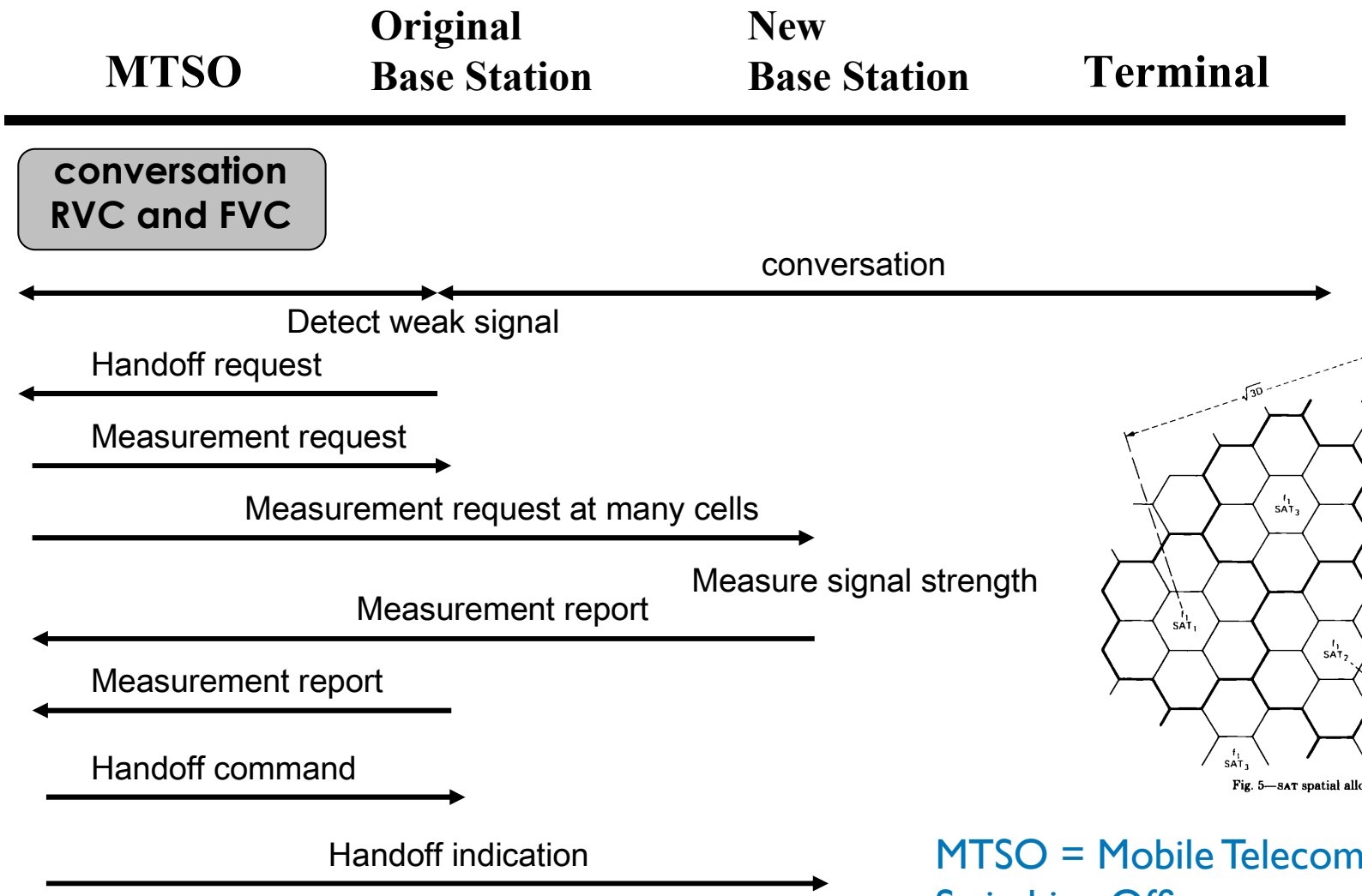


Fig. 5—SAT spatial allocation.

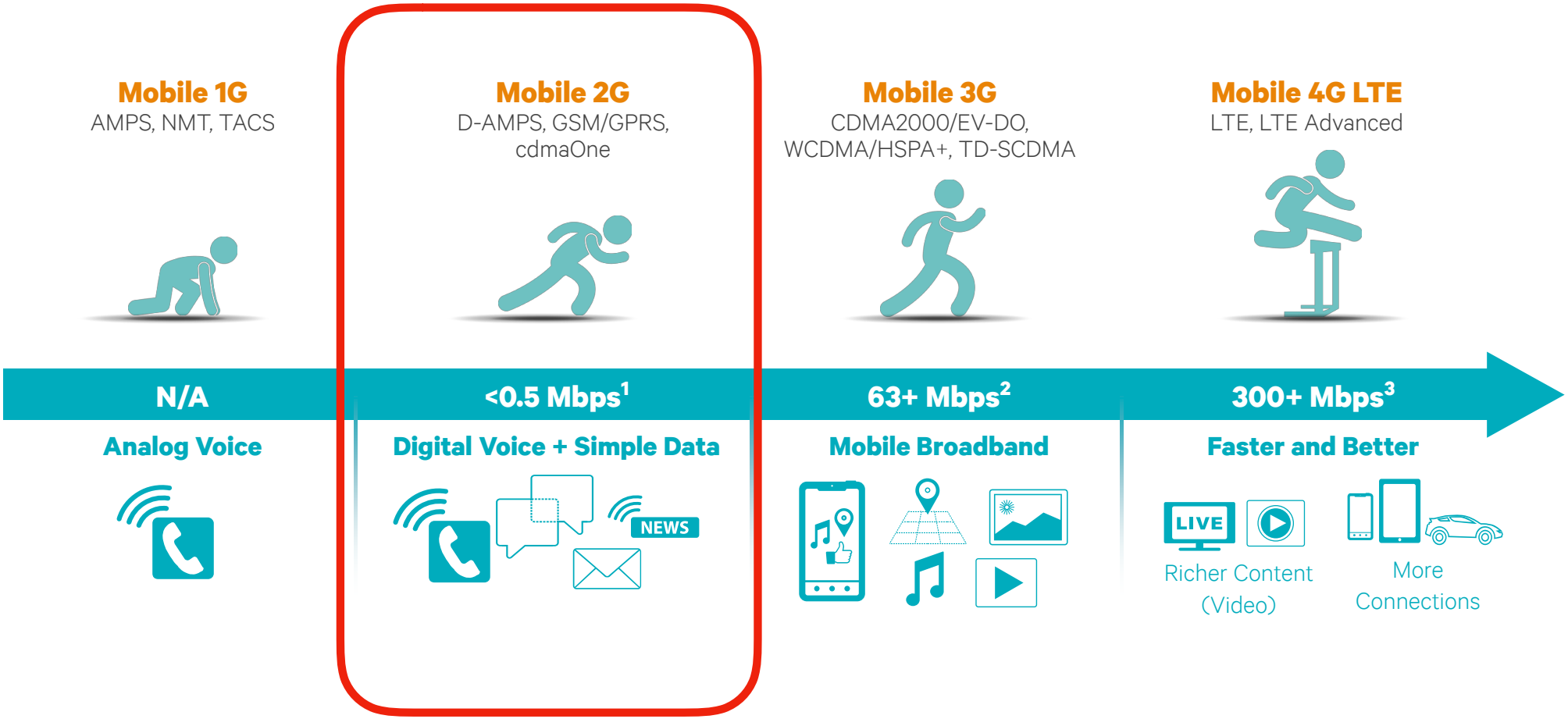
MTSO = Mobile Telecommunications Switching Office
RVC = Reverse Voice Channel
FVC = Forward Voice Channel

First generation security?

- **No security!**
  - Identification: Serial Number (ESN) and Telephone Number (MIN)
  - Control messages and voice: **analog tones**

- Obvious problems
  - Eavesdropping —> privacy problem
  - Mobile cloning —> **billing fraud**

Second generation



2G overview

- **Digital system**
  - Voice calls and text messages
  - Introduced in the early 1990's

- Medium access
  - Combination of FDMA and **TDMA**
  - Split carrier into t**ime slots** that are organized as **frames**
  - Each voice call is assigned a time slot

- **Digital voice transmission**
  - Compression, error correction, less power, more capacity
- **Digital control channels**
  - Services like text messages and security…

GSM standard

GSM (Global System for Mobile Communications)

- Popular in Europe and Asia
- Initially limited coverage and support in USA

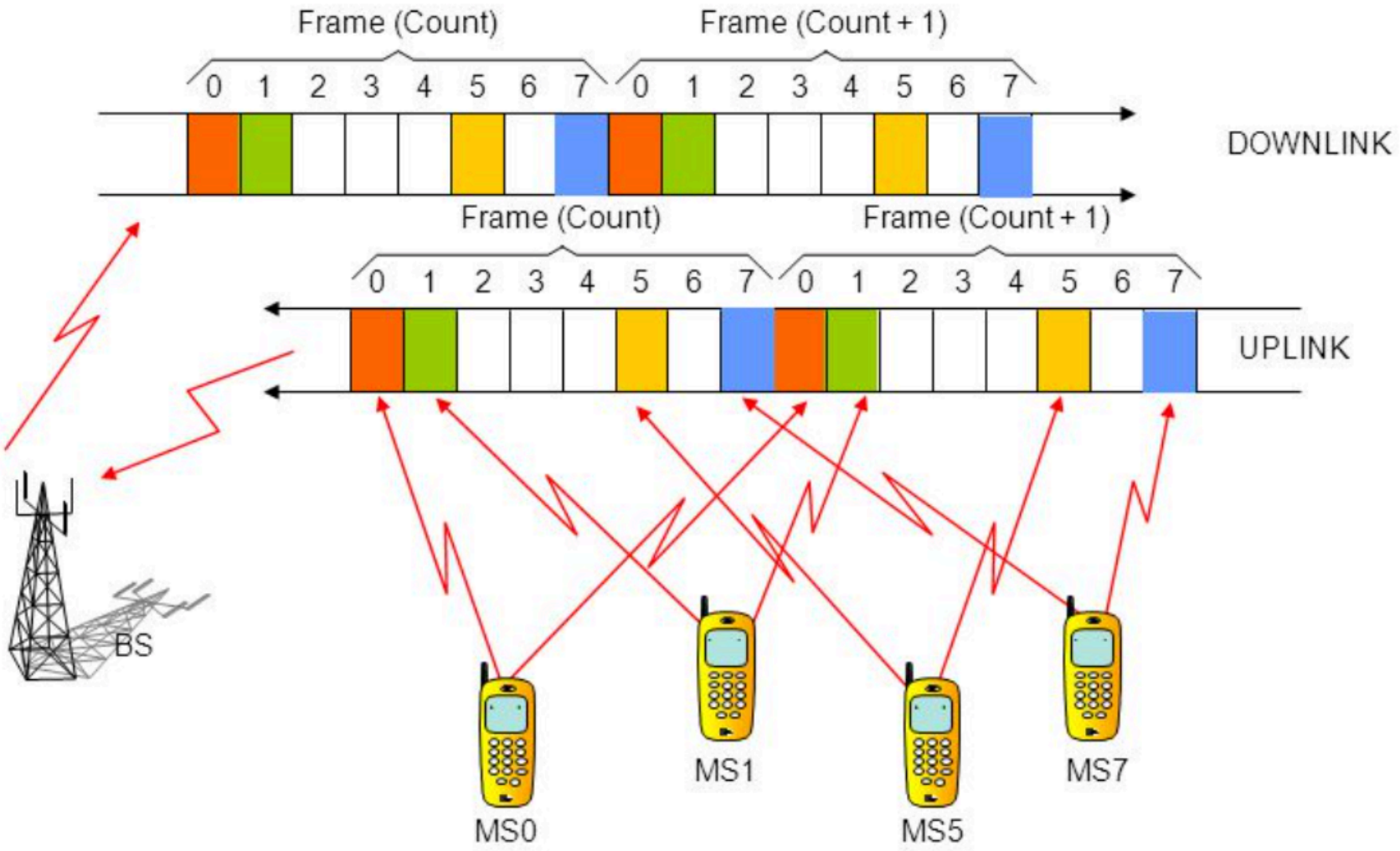
Radio link properties

- Uplink (890-915 MHz), downlink (935-960 MHz)
- 25 MHz subdivided into 124 carrier frequency channels
  - **TDMA**: 8 speech channels per radio frequency channel
- Channel data rate is 270.833 kbps
- Voice transmitted at 13 kbps

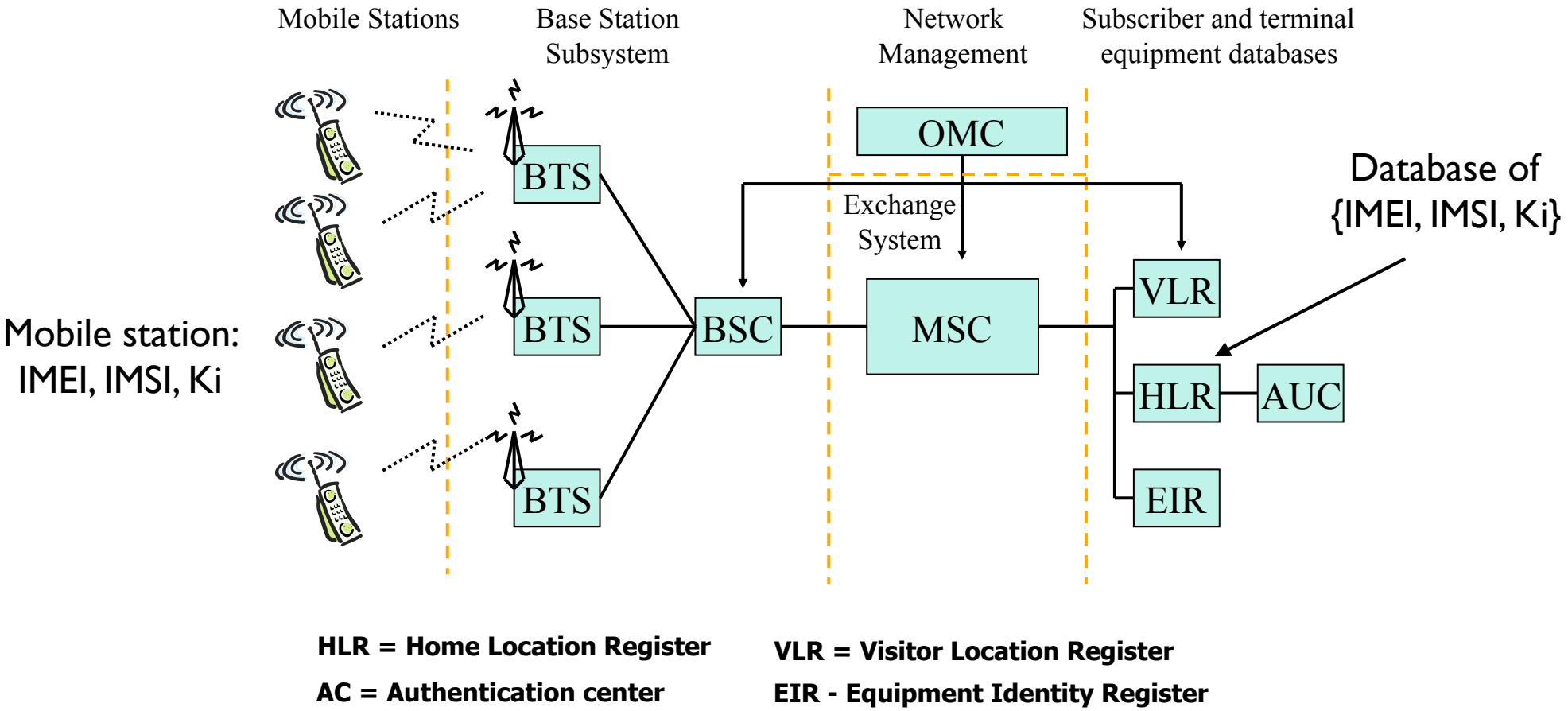
Handset power

- **Max 2 watts** in GSM900 and 1 watt in GSM1800
- Cell size up to **35 km**

GSM Medium Access



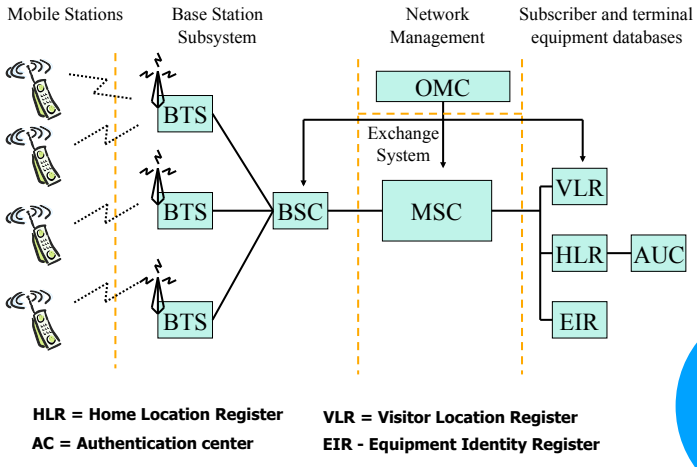
GSM Architecture



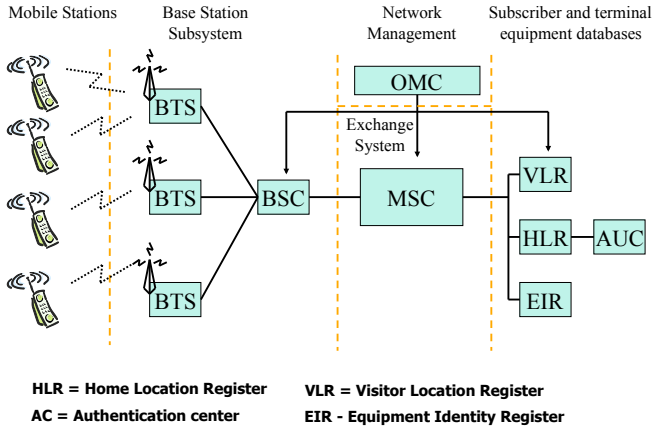
IMEI = International Mobile Equipment Identity
IMSI = International Mobile Subscriber Identity
Ki = shared symmetric key

MSC = Mobile Switching Center
- connects wireless to core network
- gateway to PTSN
- assists in handoffs, billing…

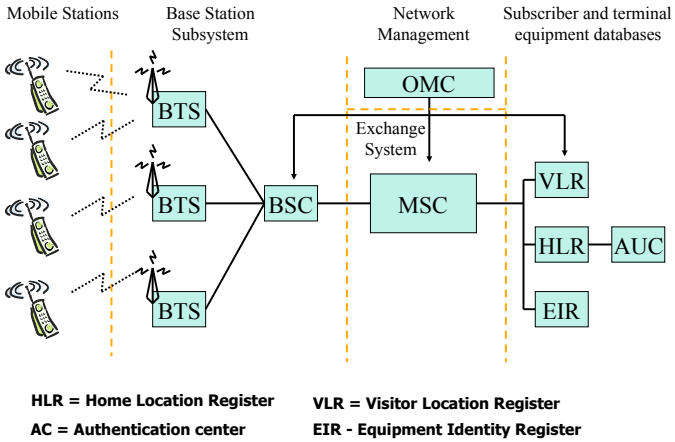
Bigger picture



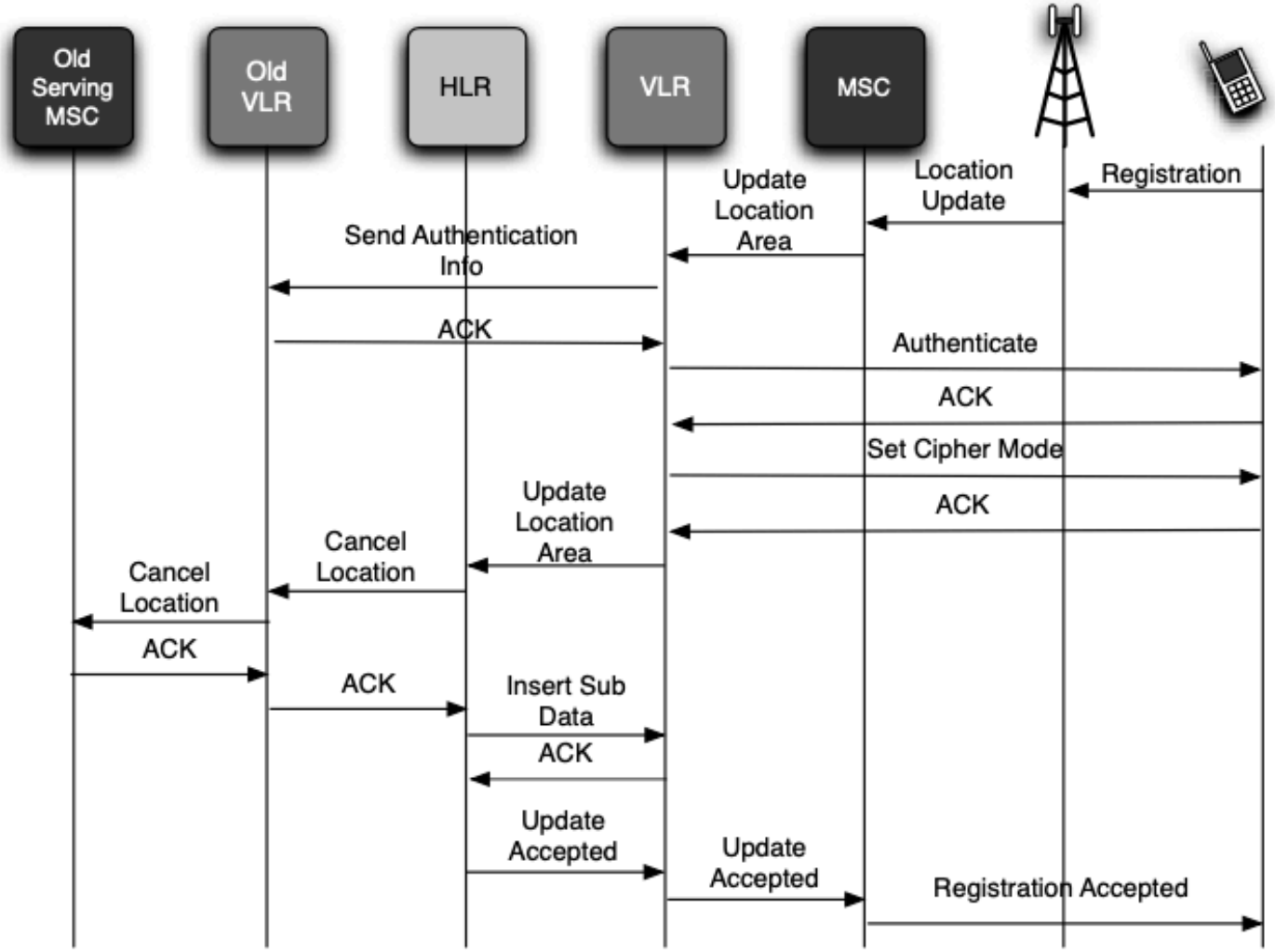
SS7



SS7 = Signaling System 7



Example: mobile device registration



Source: Traynor et al. Security for Telecommunications Networks. Springer 2008

GSM Security Goals and Mechanisms

Main security goals for **operators**

- Correct billing (to avoid fraud)
- Protect services

Main security goals for **customers**

- Privacy protection
- Correct billing

Main security mechanisms

1. User **authentication**
2. Communication **encryption**

GSM Security Mechanism

Both authentication and encryption based on **shared key**

Ki – Subscriber Authentication Key

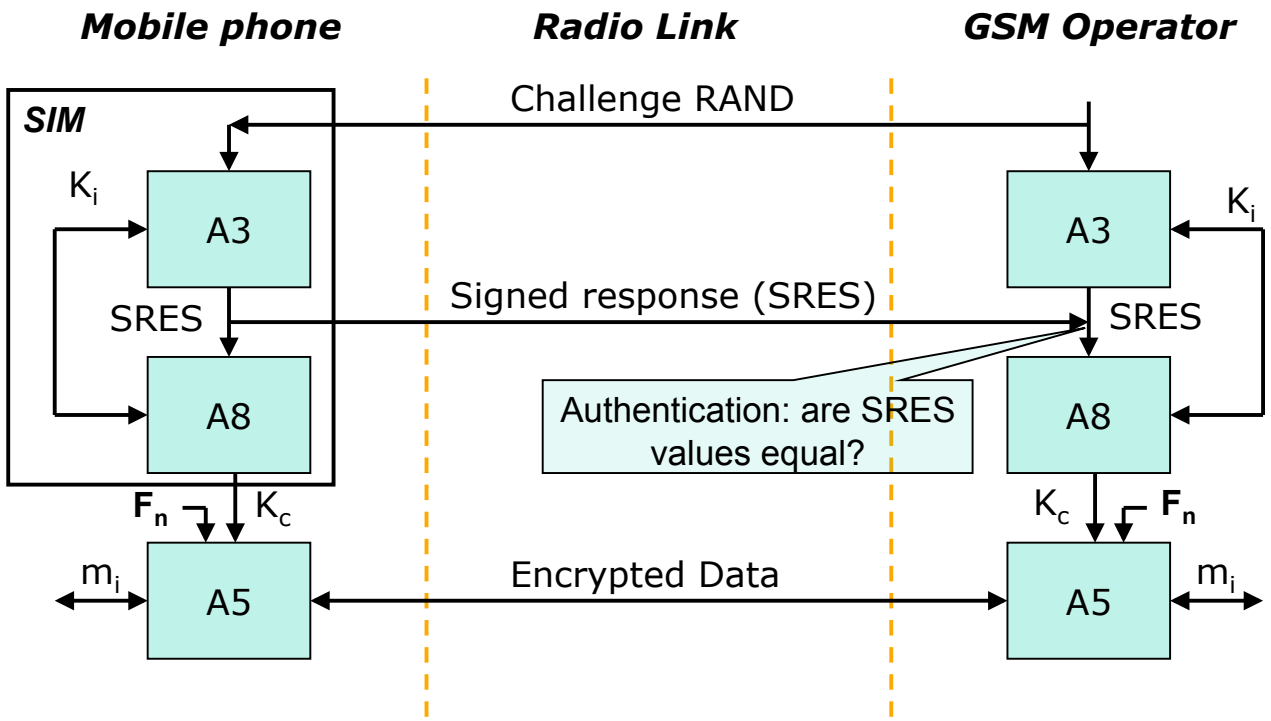
- Shared 128 bit key
- Resides in **subscriber SIM** (owned by operator, trusted)
- HLR of the subscriber's home network

GSM standard assumes 3 crypto algorithms

- A3 for authentication
- A8 for key derivation
- A5 for encryption

Algorithms initially supposed to be **secret**

GSM Authentication and Encryption overview



A3 and A8 on implemented SIM

- operator can choose!
- common choice: COMP128 keyed hash algorithm

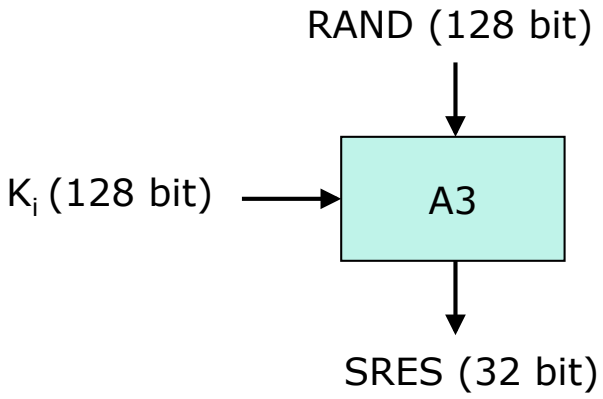
A5 is a stream cipher

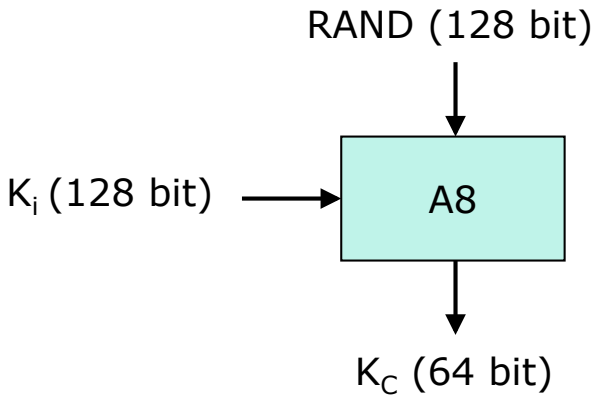
- designed for efficient hardware implementation
- variants: A5/1 “strong”, A5/2 intentionally weakened

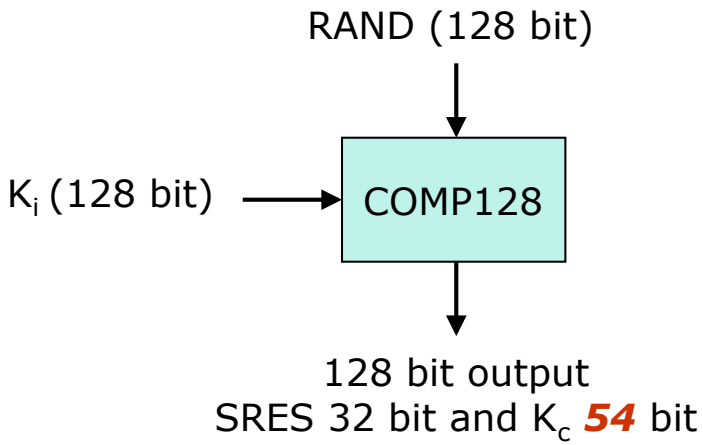
Some A3 and A8 details

Recall: A3 = authentication, A8 = key derivation

Implementation chosen by operators







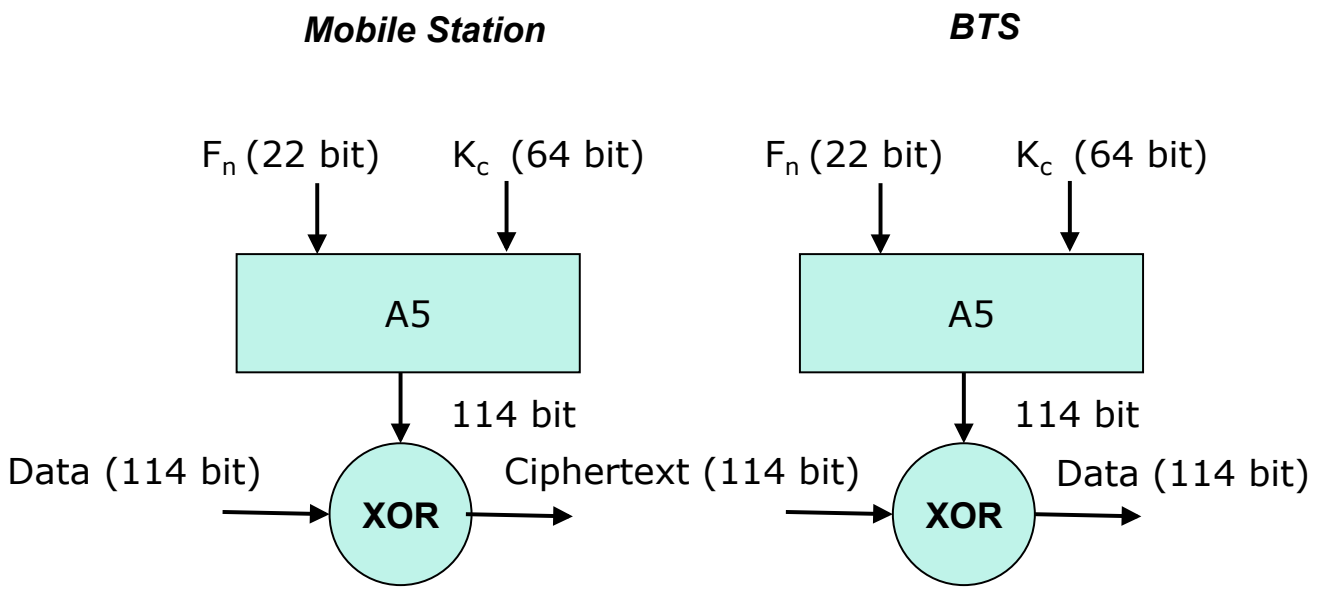
Logical implementation of A3 and A8
COMP128 is a keyed hash function

Some A5 details

A5 = stream cipher (that can be implemented easily and efficiently on simple hardware)

Design originally confidential, but later leaked

Variants: A5/1 – the strong version, A5/2 – the weak version



GSM Key Management

AuC – Authentication Center

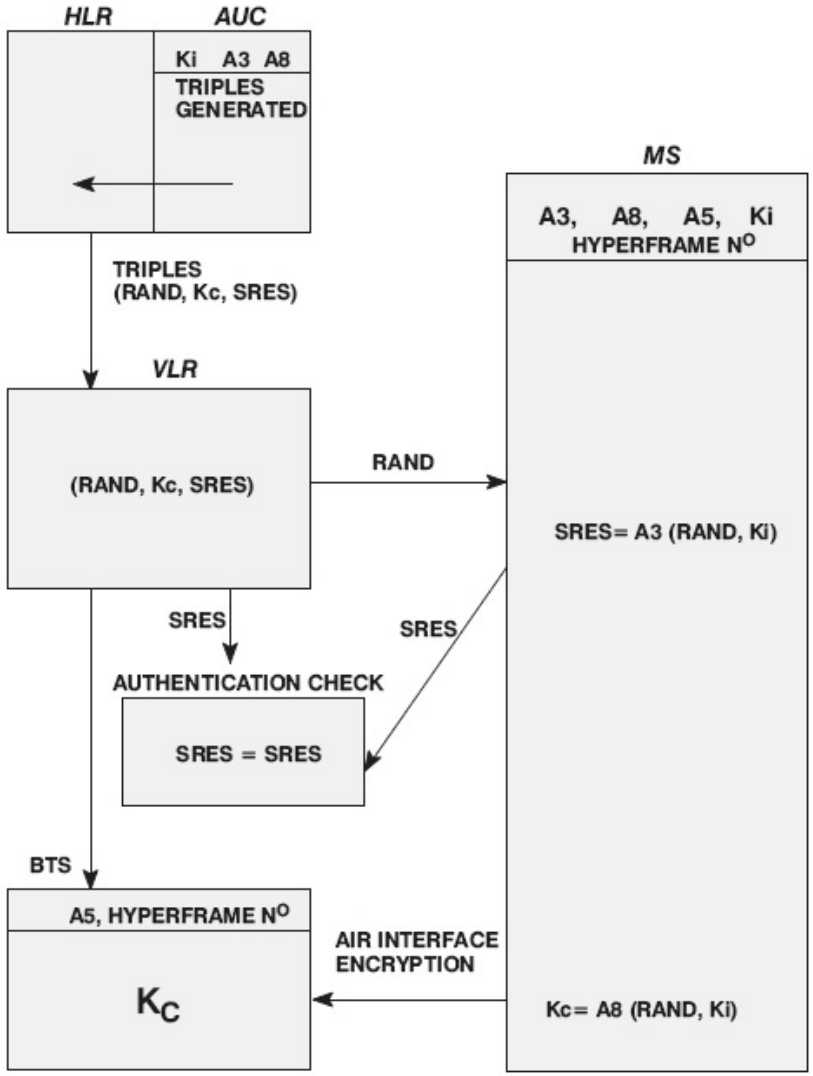
- Sends (RAND, SRES, Kc) to HLR

HLR – Home Location Register

- Sends (RAND, SRES, Kc) to VLR

VLR – Visitor Location Register

- Stores (RAND, SRES, Kc)
- Sends RAND to MS
- Authentication using SRES
- Encryption/decryption using Kc



GSM Crypto Attack History

1991: First GSM implementation.

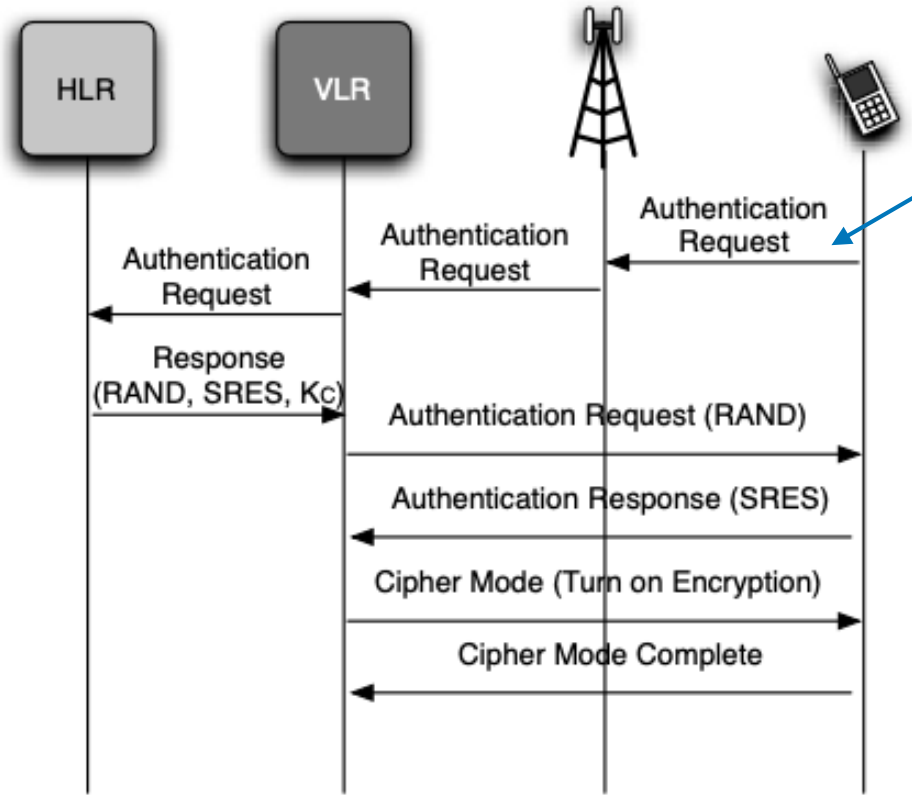
April 1998: Smartcard Developer Association (SDA) and U.C. Berkeley cracked COMP128 and extracted Ki from SIM within hours. Found that Kc uses only 54 bits.

August 1999: The weak A5/2 variant was cracked using a single PC within seconds.

December 1999: Biryukov et al. break the strong A5/1 variant with two minutes of intercepted call in 1 second.

May 2002: The IBM Research group discovered a new way to quickly extract the COMP128 keys using side channels.

Authentication process observations



Request contains IMSI (or TMSI)

Two observations:

1. Communication before authentication
2. No network authentication

Source: Traynor et al. Security for Telecommunications Networks. Springer 2008

Attack: Fake base station (BS)

IMSI catcher

- Determine user identity
- Track user
- Learn his location

Intercept mobile calls

- Record calls
- Break confidentiality

Over-the-air cloning

- Derive authentication key

Used to be ...

Today:
USRP, OpenBTS

GSM security summary

One of the main problems: **weak crypto algorithms**

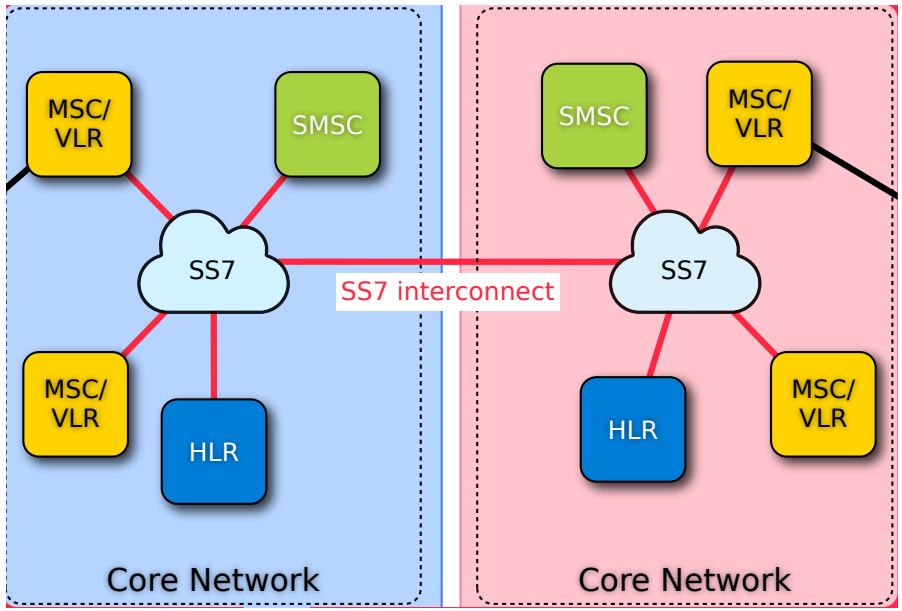
- Initially secret algorithms
- Eventually leaked or reverse-engineered and broken
- No strong user authentication or call confidentiality

Also several other issues

- No network authentication —> fake BS
- IMSI shared in plaintext —> user tracking
- Encryption is optional and limited to radio link…
- No integrity protection…

DISCUSS: Weak crypto due to bad design or very difficult task?

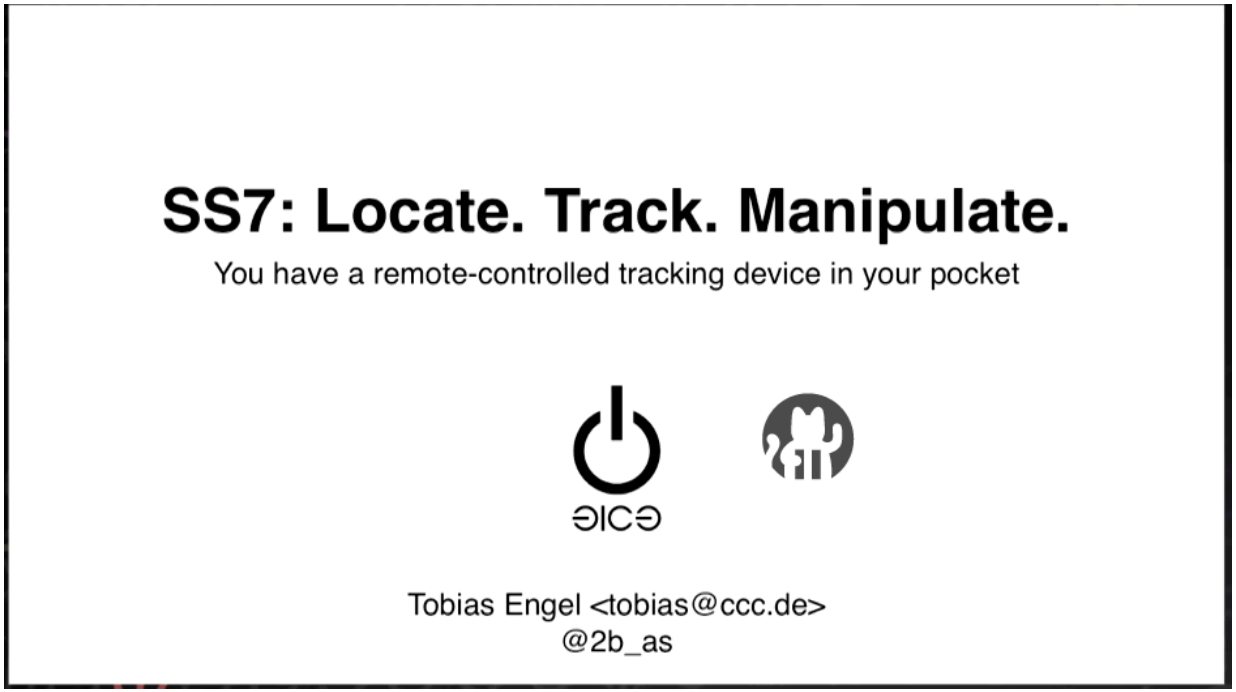
GSM core network (SS7)



- Signalling System #7 (SS7) is a protocol suite used by most telecommunication service providers to talk to each other
- Standardized in 1980's. **Trust model:** Service providers trust each other. **No authentication built in.**
- SS7 access can be bought from telecom providers for a few hundred dollars a month. Also, many unsecured SS7 hubs present on the web.

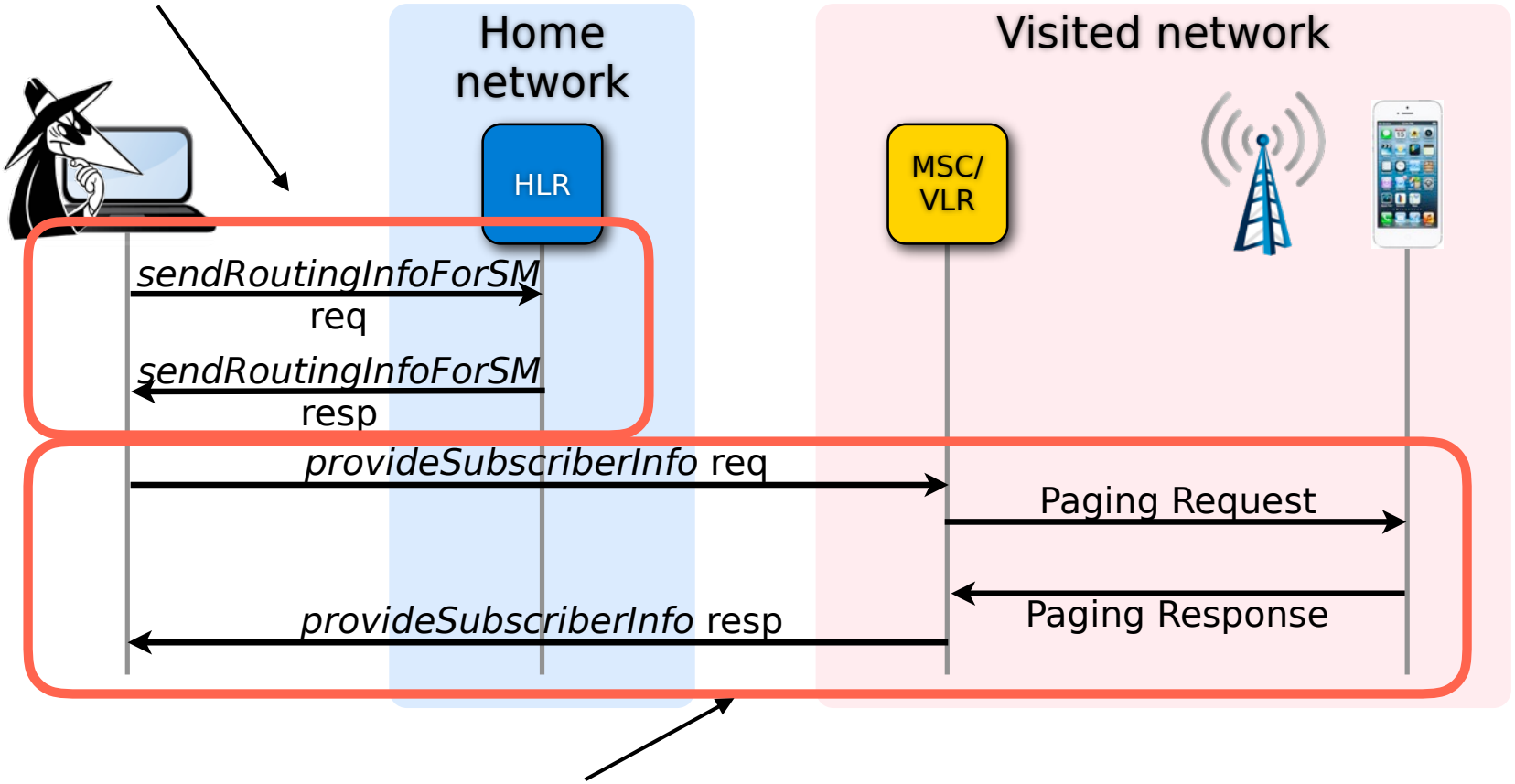
Entertaining video

Tobias Engel @ CCC congress 2014



Attack: Location Tracking using SS7

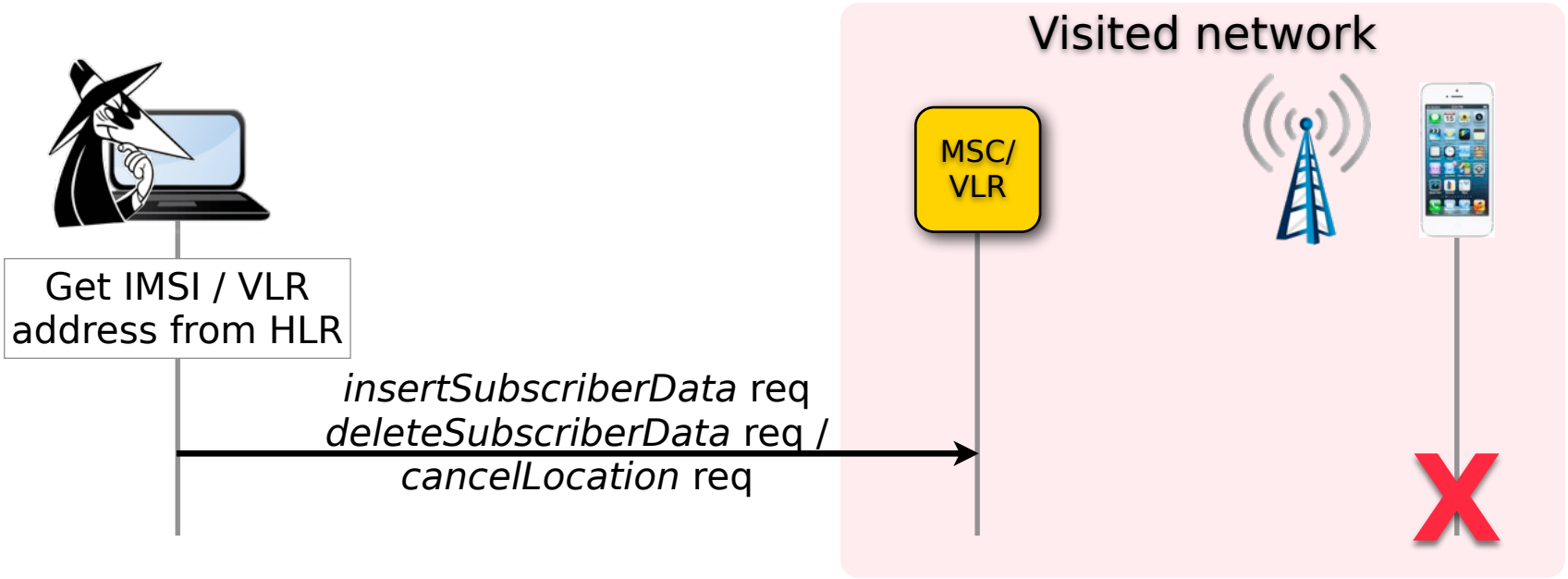
Step 1: Get IMSI and address of current MSC



Step 2: Request the cell id of the subscriber to the current MSC

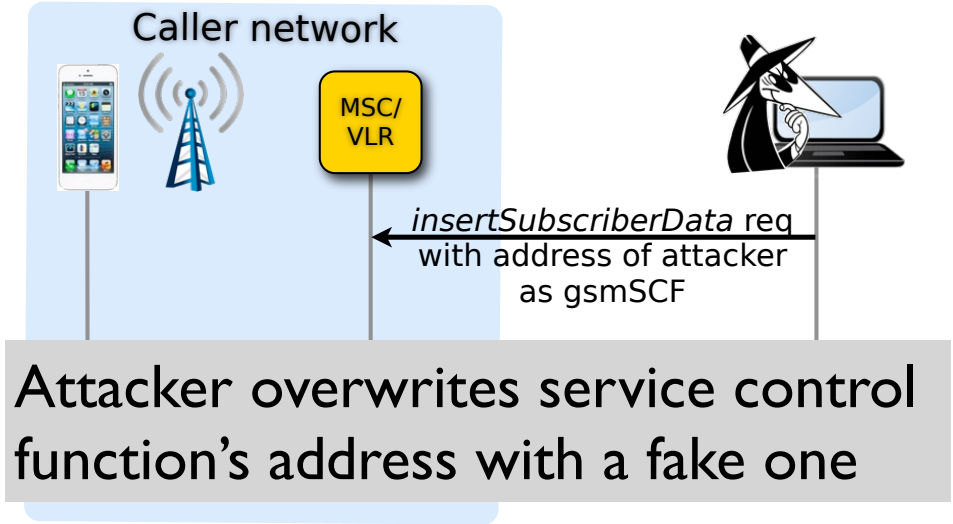
Several online services allow locating the subscriber using the paging response.

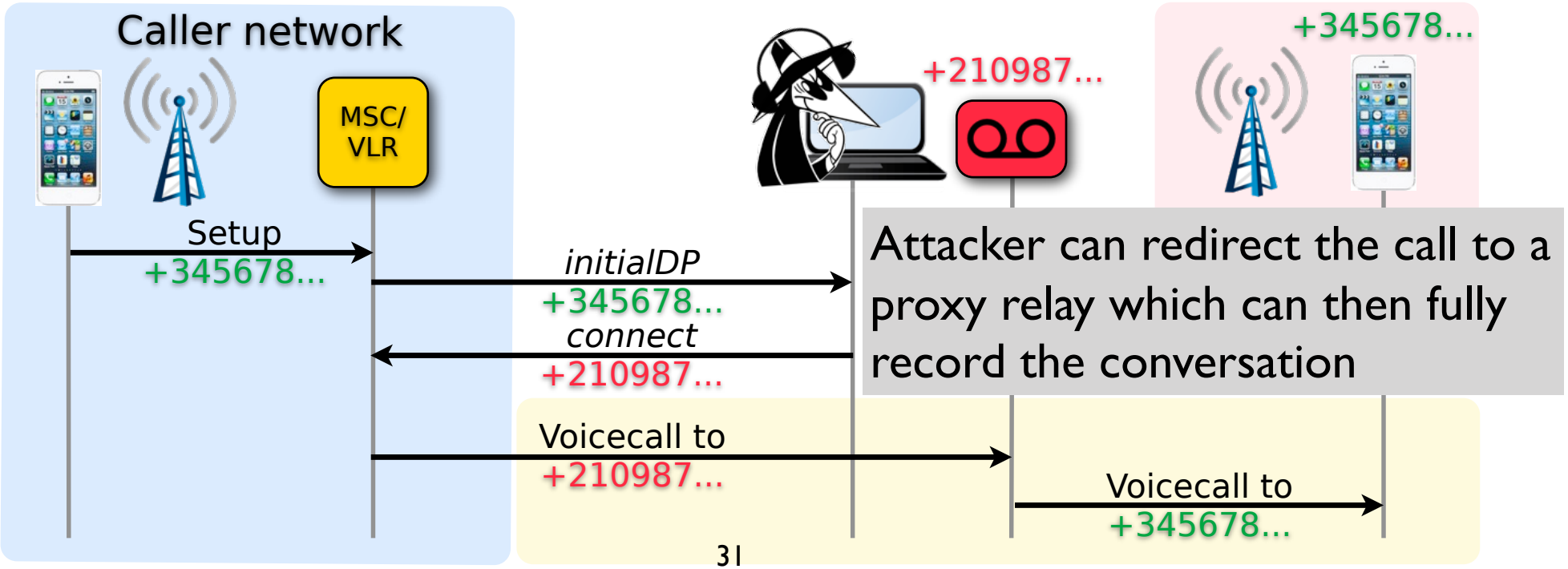
Attack: Denial of Service using SS7



- Attacker can modify subscriber data as well. No checks implemented by most telecom providers.
- Once IMSI and VLR addresses are available to the attacker, he can control all kinds of service availability to the subscriber e.g., disabling outgoing calls etc.

Attack: Intercepting Calls using SS7





SS7 network security

Legacy system with no security protections

- Turned out to be major vulnerability

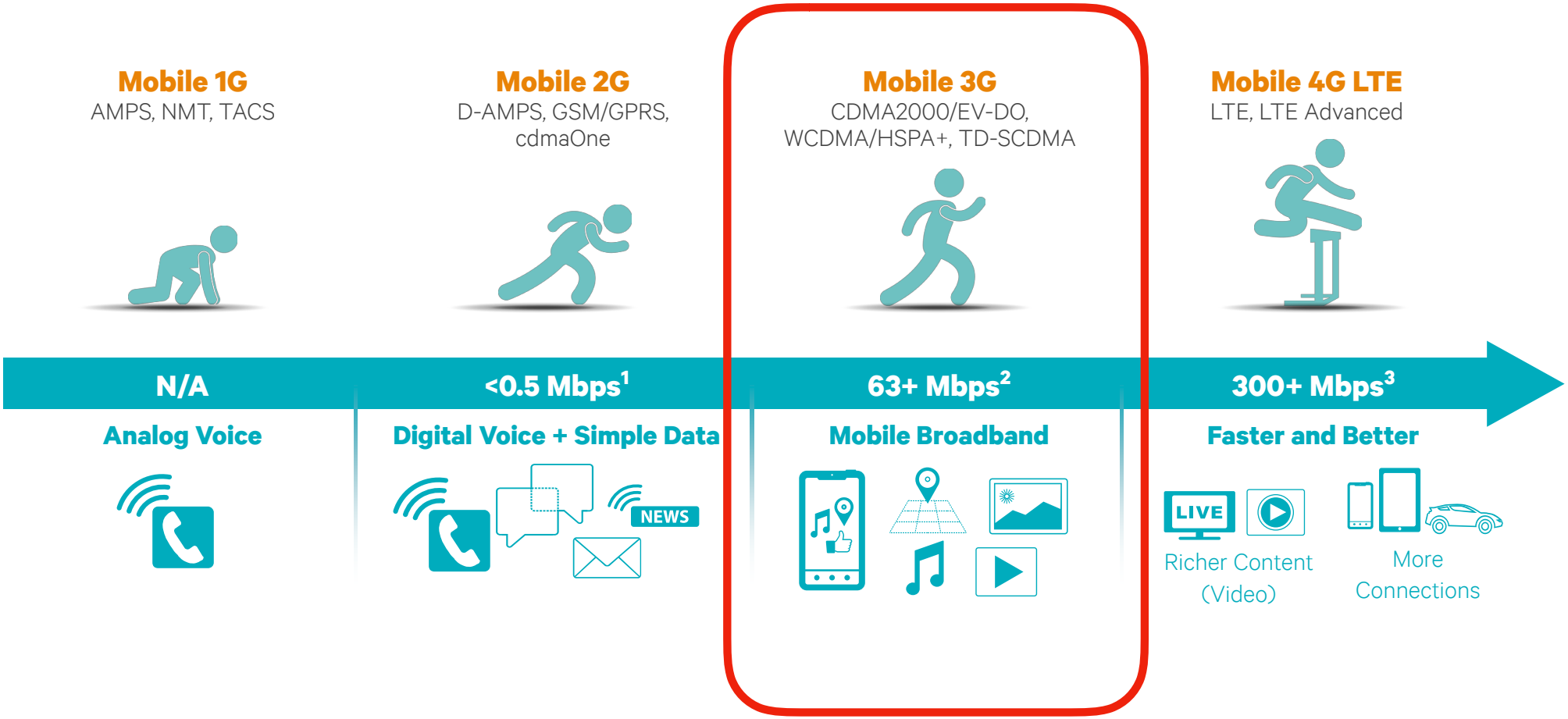
Root causes

- Designed for an outdated threat model
- Bad network management

Many of these issued have been fixed (since 2014)

DISCUSS: Operator negligence or actually challenging problem?

Third generation



3G overview

Introduced early 2000's

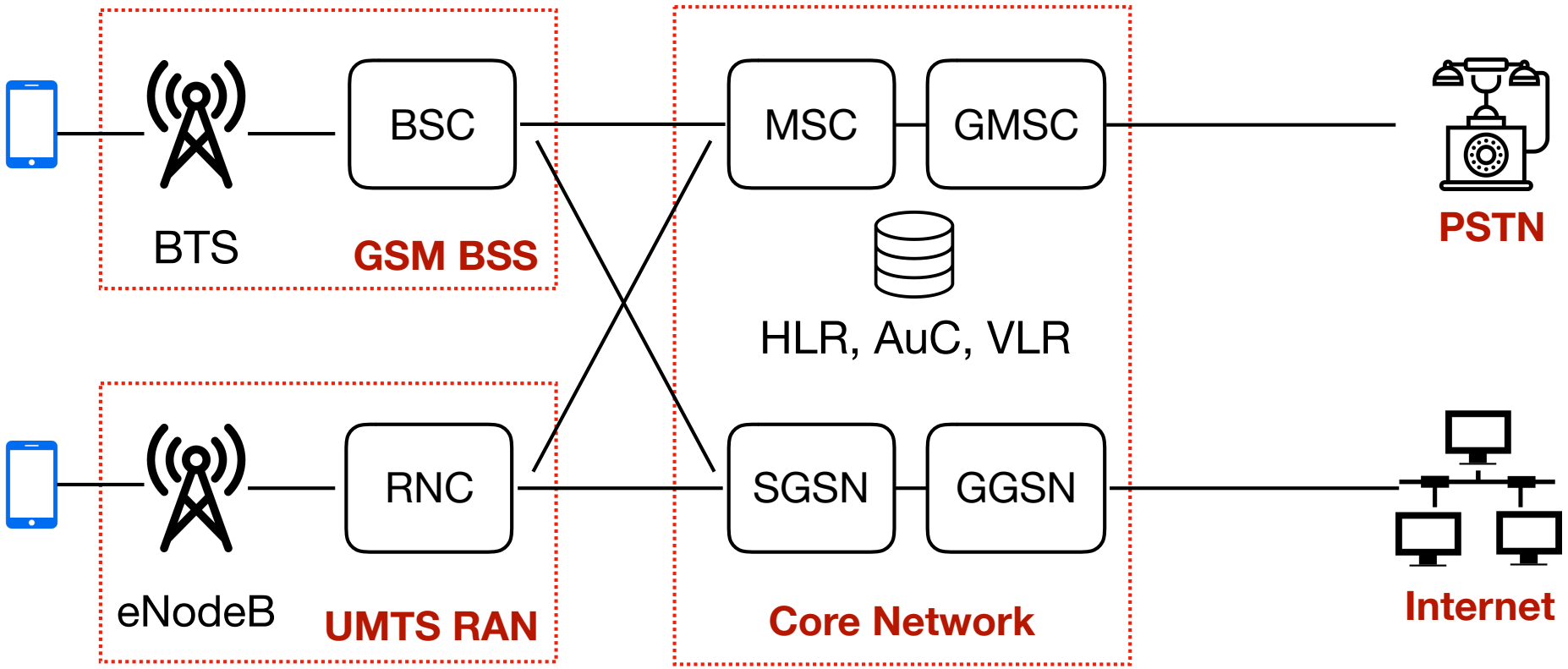
- Common 3G standard:
  - **UMTS** (Universal Mobile Telecommunications System)

Medium access:

- **W-CDMA:** wideband **code-division** multiple access
  - Several transmitters over single communication channel
  - Each user's data signal is spread across the spectrum using a separate spreading
  - 1885-2025 MHz uplink and 2110-2200 MHz downlink
- Supports up to 14 Mbps (in theory)

Updated terminology (GSM to UMTS)

- SIM —> USIM
- BTS —> eNodeB
- BSC —> RNC (Radio Network Controller)



3G main security updates

Main goal: fix the main problems of 2G (GSM) security

Specific measures:

1. Use **stronger crypto** algorithms
2. Protect user identities against fake base stations
3. Less trust in visited network in general
4. Mandate encryption
5. Extend encryption to core network
6. Provide integrity protection

Authentication and Key Agreement

New protocol

- roughly same design used in 4G and 5G

Assumes five functions f1, f2, f3, f4, f5

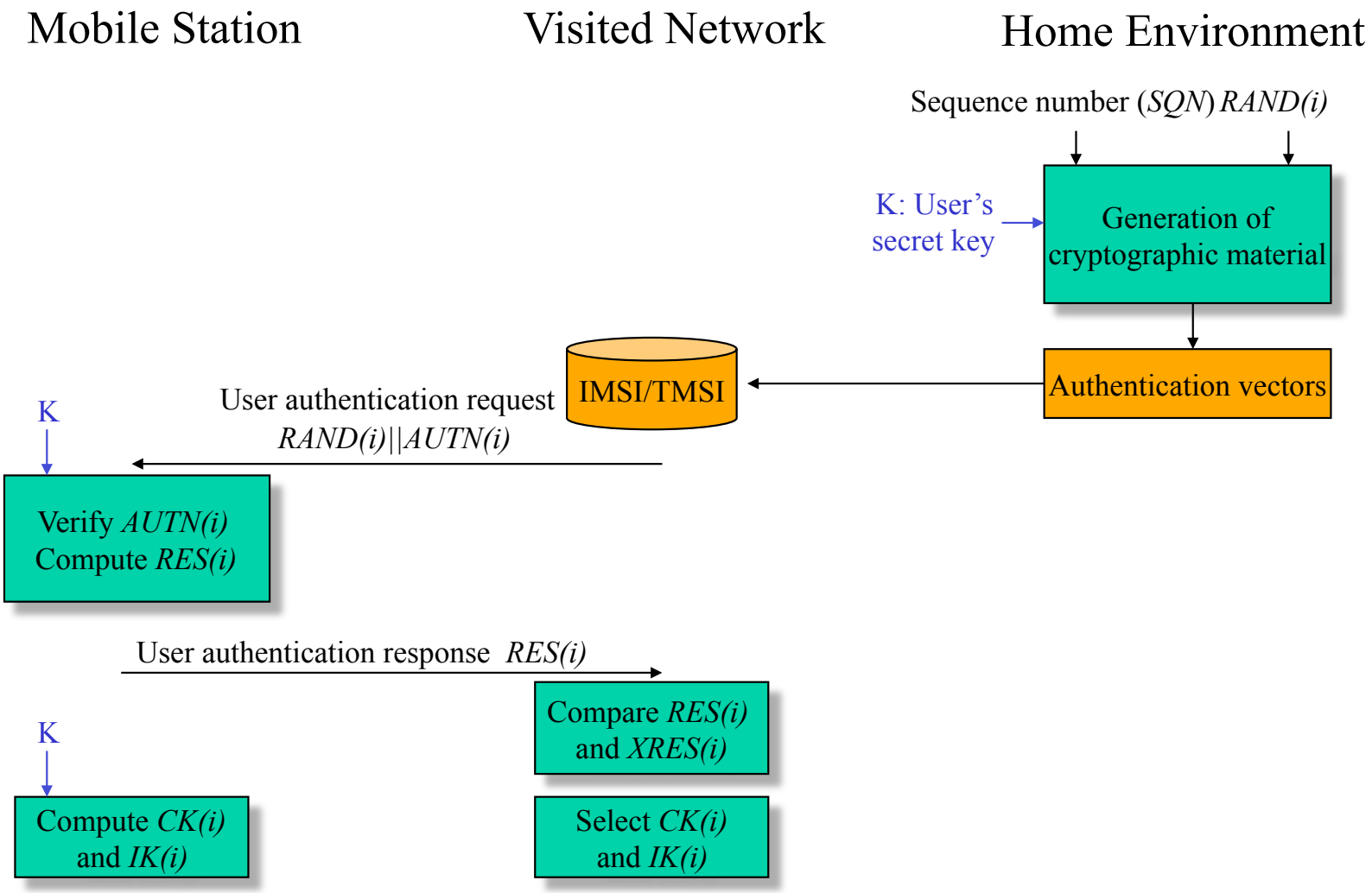
- these functions can be operator-specific

Adds nonce management for better replay protection

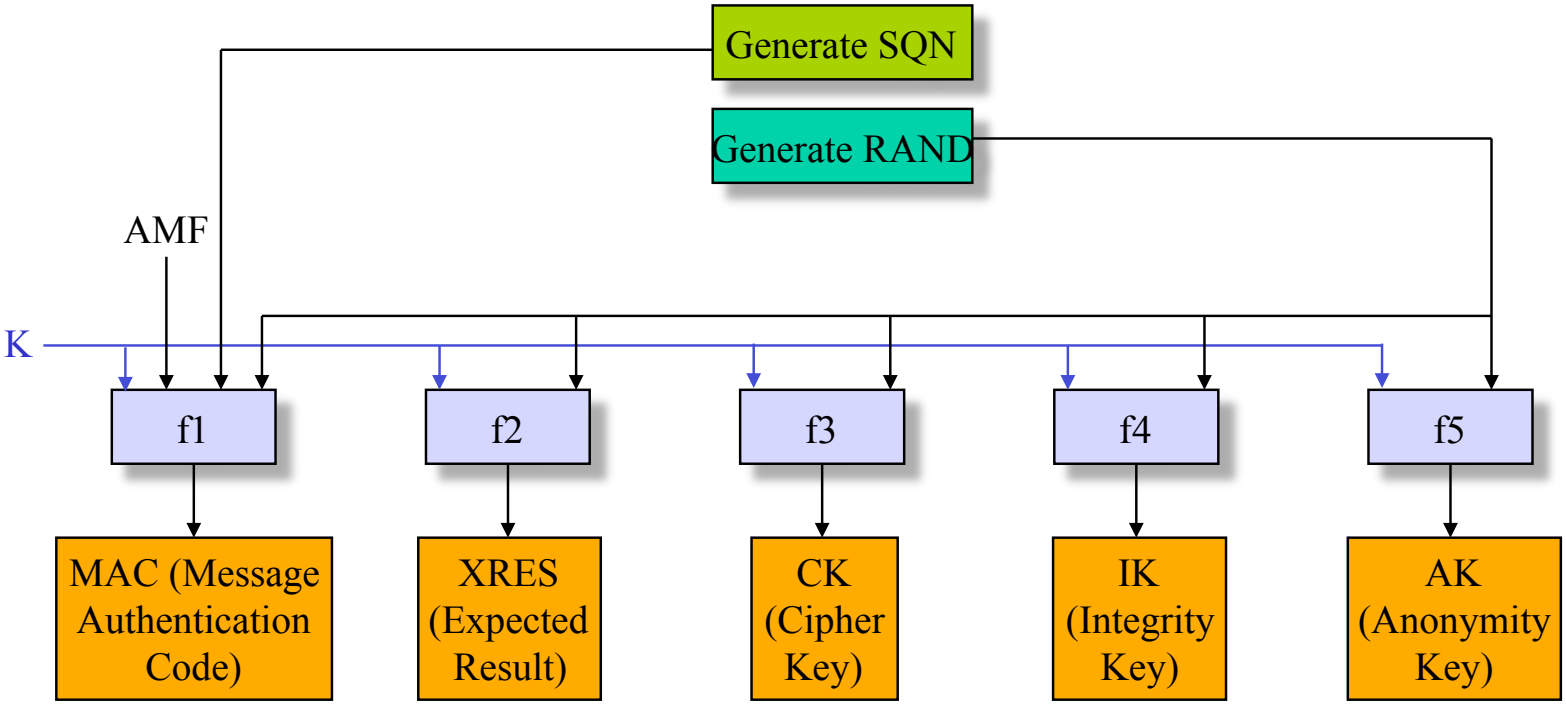
- two more functions f1* and f5*
- used for re-synchronization if operator and SIM get out of synch (not discussed in this lecture)

Two additional functions for encryption (f8) and integrity (f9)

3G AKA protocol overview



Authentication Vector generation (operator side)

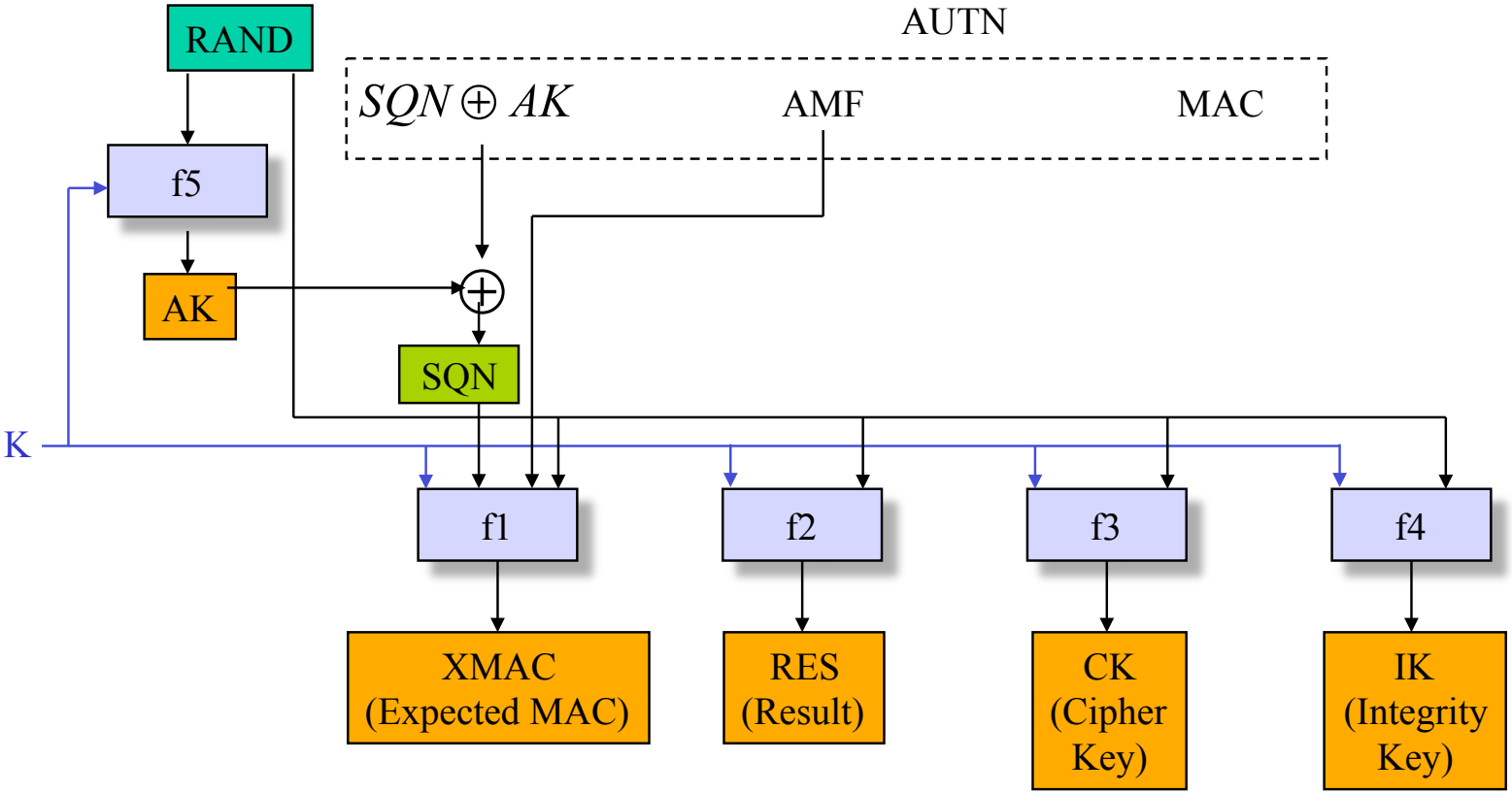


Authentication token: AUTN = (SQN⊕AK)|| AMF|| MAC

Authentication vector: AV = RAND|| XRES ||CK || IK || AUTN

AMF: Authentication and Key Management Field

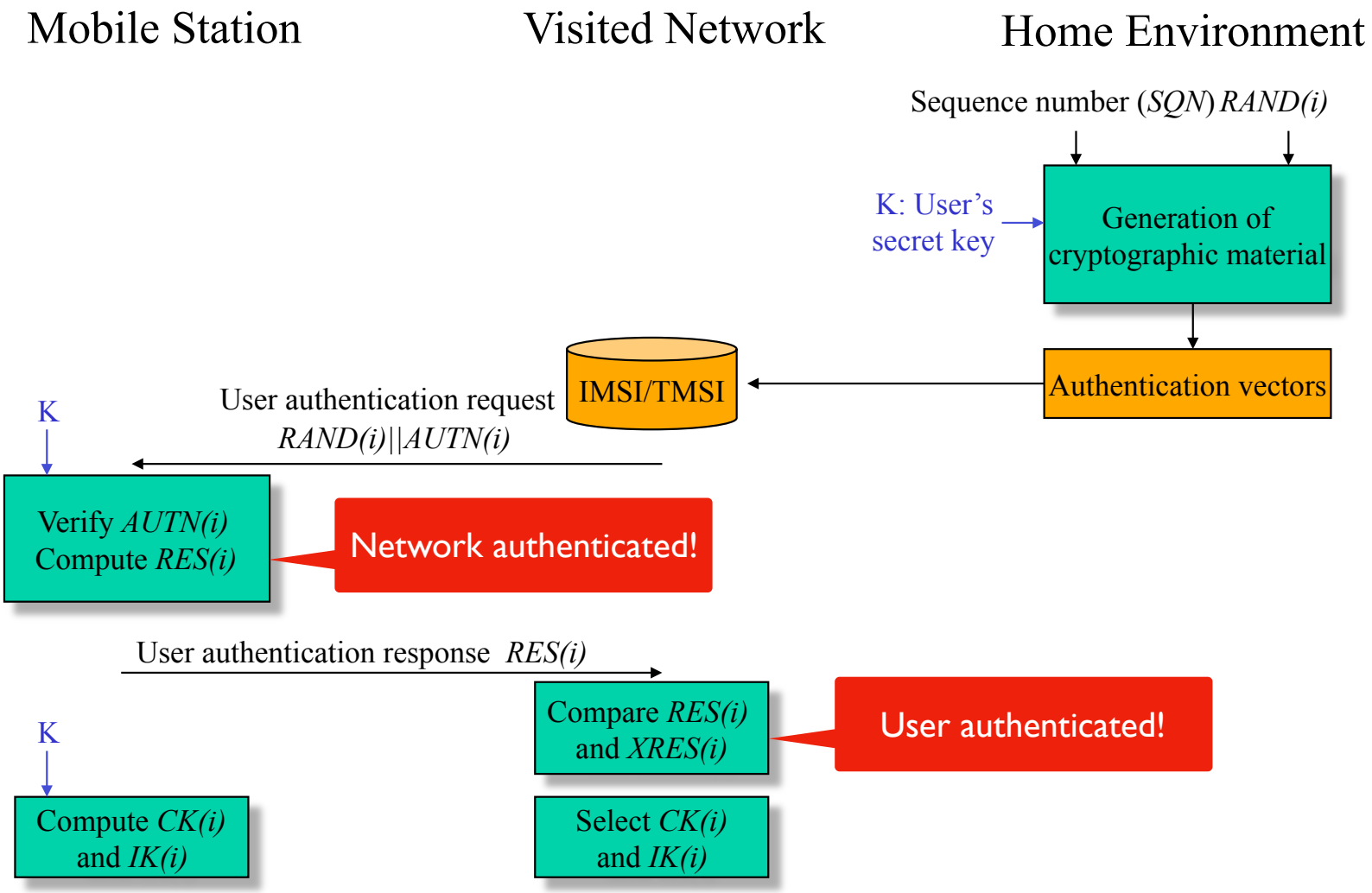
User Authentication (on USIM)



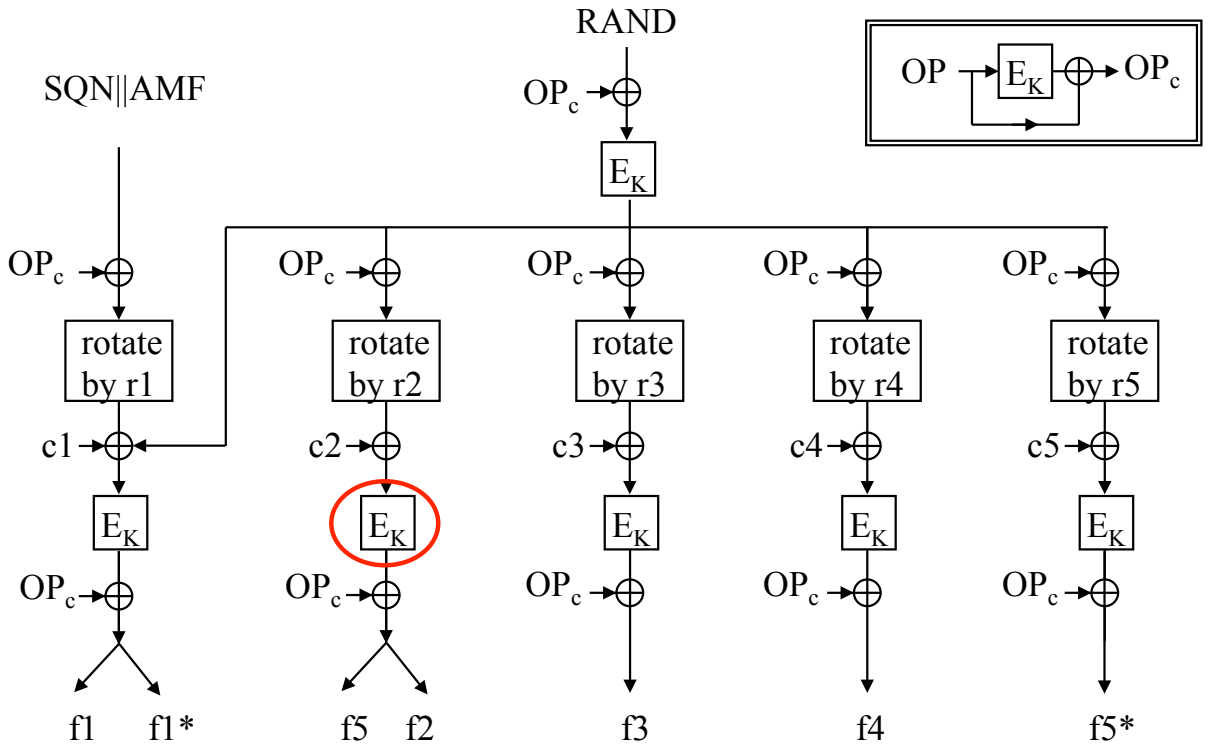
- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module

UMTS Authentication (in Visited Network)



Authentication and Key Generation (f1…f5*)



OP: operator-specific parameter
r1,…, r5: fixed rotation constants
c1,…, c5: fixed addition constants

E_K : Rijndael block cipher with 128 bits text input and 128 bits key

DISCUSS: Why such design?

Ek = “kernel function” = Rijndael = AES

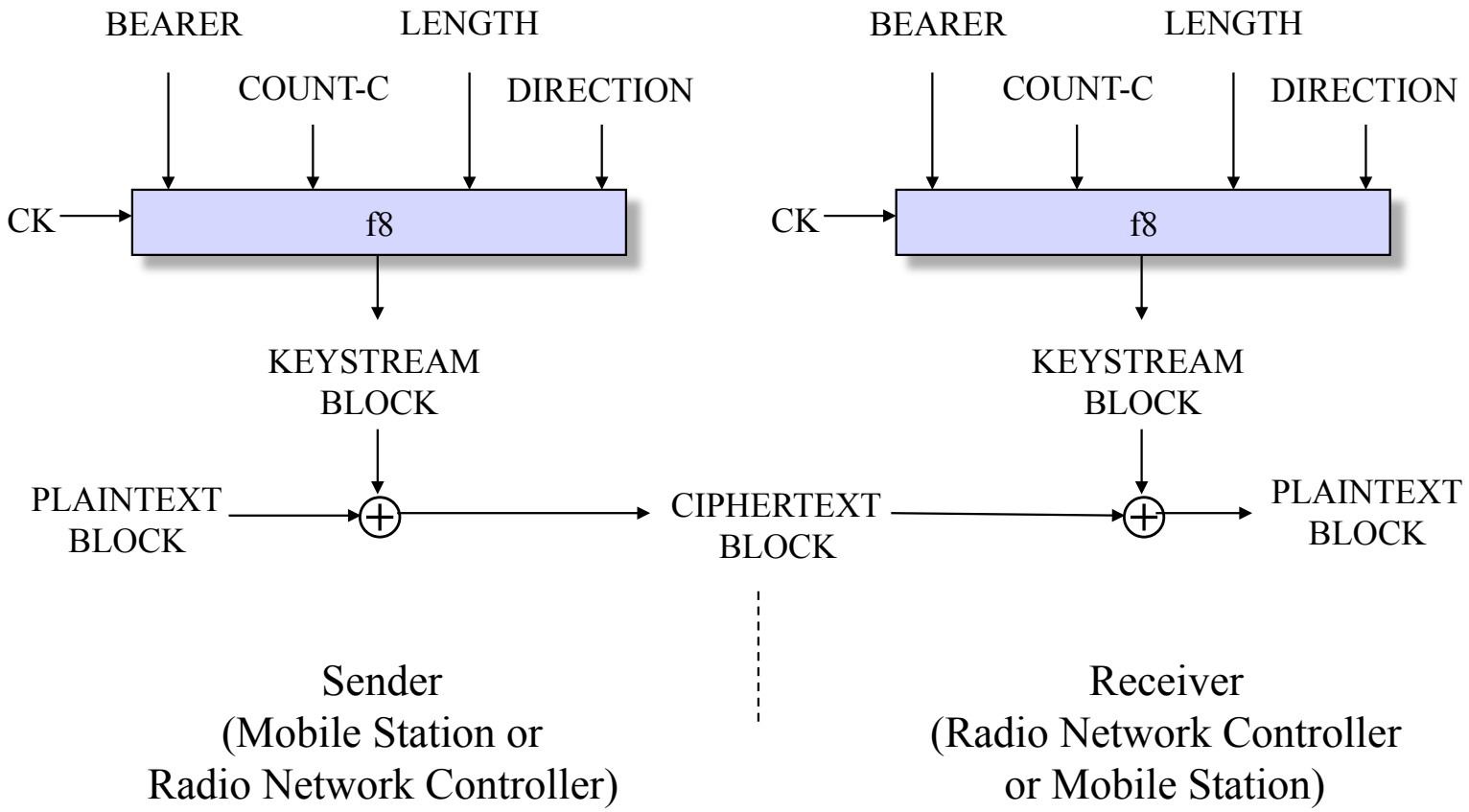
OPc = “operator constant”

Side note on the operator constant

From UMTS Specification:

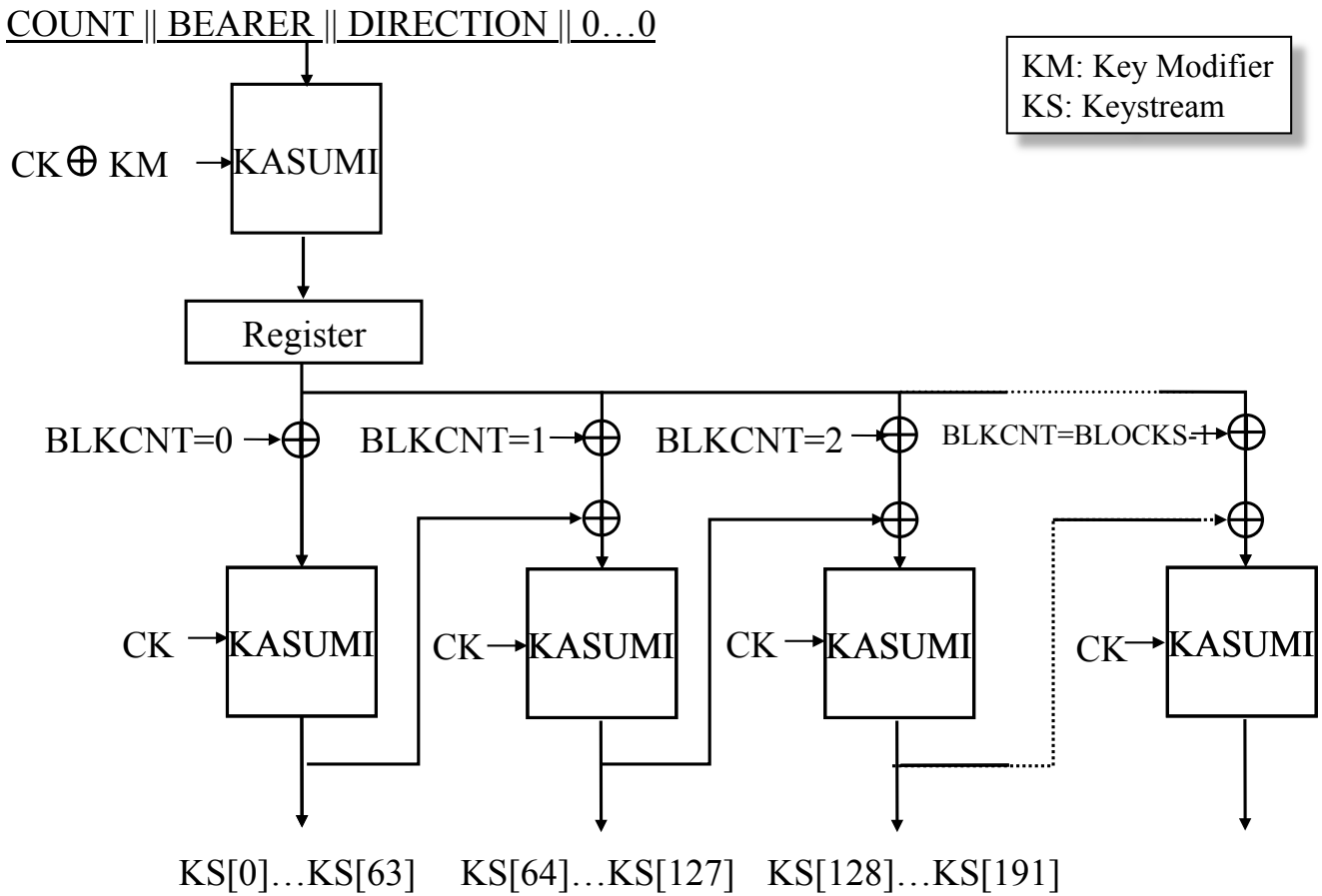
> The algorithm set is designed to be secure whether or not OP is publicly known; however, operators may see some advantage in keeping their value of OP secret as a secret OP is one more hurdle in the attacker's path.
>
> It should be difficult for someone who has discovered even a large number of (OPc, K) pairs to deduce OP. That means that the OPc associated with any other value of K will be unknown, which may make it (slightly) harder to mount some kinds of cryptanalytic and forgery attacks.

Encryption using f8 function (data and signaling)

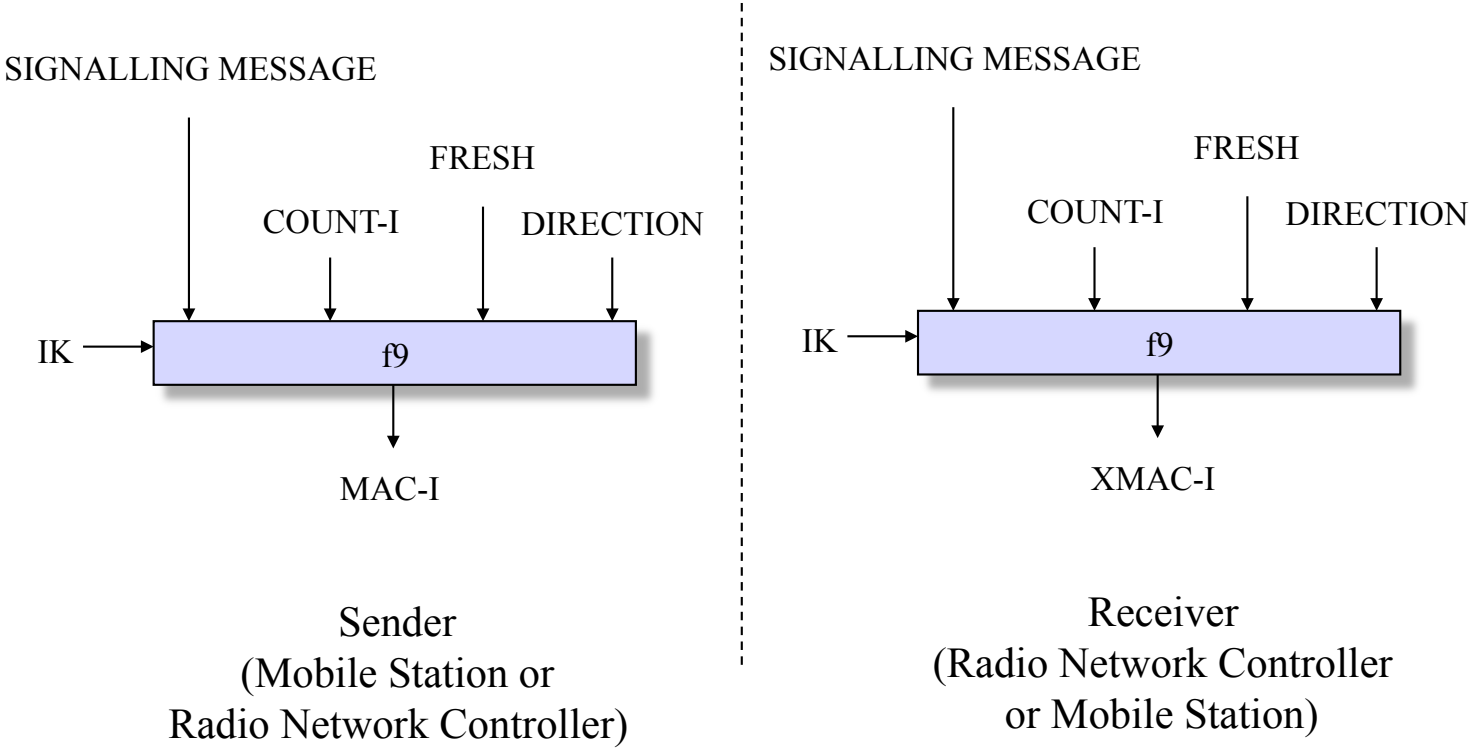


f8 = KASUMI block cipher

Some f8 details
(use block cipher to generate a key stream)



Integrity Protection using f9
(mandatory for signaling, optional for voice and data)



f9 = KASUMI

FRESH: random input

DISCUSS: Why define integrity as optional?

Why optional integrity protection?

Two types of traffic: voice and data

Voice considerations

- Typical voice packet is 40 bytes, MAC is 8 bytes
  - 20% overhead
- Single bit error would cause packet to be dropped
  - Unacceptable real-time voice quality
- Voice data is encrypted
  - Few bit flips probably acceptable for voice

Data considerations

- Security-critical applications should use TLS anyway…

3G confidentiality

Confidentiality based on **KASUMI** block cipher

- 8-round Feistel Network
- Means “mist” in Japanese :)

Good design process: public review

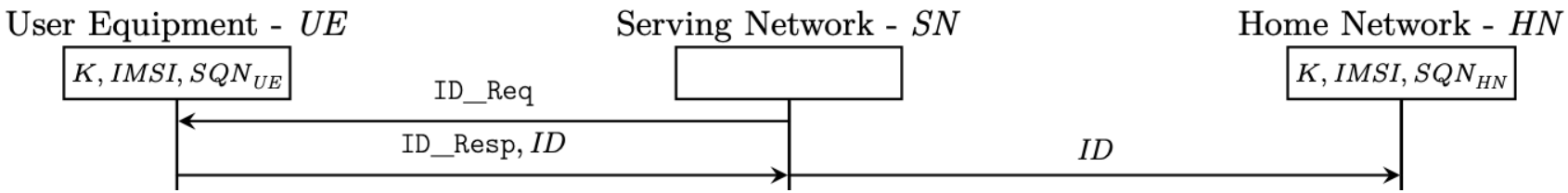
- Has proven to be secure design

Example cryptanalysis / partial attacks:

- Attacks that break subset of rounds in feasible time
- Attacks that assume strange models (“related key attack”)

DISCUSS: Why not just use AES?

Registration and paging



Source: Borgaonkar et al. New Privacy Threats on 3G, 4G and Upcoming 5G AKA protocols. PETS'19.

Registration

- User identity (**IMSI**) sent in plaintext before authentication
- After registration, serving network assigns UE a random and temporary identifier called **TMSI**

- Paging
  - After period of inactivity, UE switches to idle mode
  - Serving network sends **paging messages** using TMSI for incoming calls and messages

User tracking

Assume an adversary that is able to eavesdrop traffic

Possible sources of user identity and location leakage

- New registration —> leaks permanent IMSI
- Paging messages —> leaks temporary TMSI

Refresh rate of TMSI is operator-specific setting…

DISCUSS: Why not encrypt IMSI and TMSI?

Downgrade attack

3G (UMTS) introduced to co-exist with 2G (GSM)

Simple downgrade attack:

- Phone: I want to register to network
- Fake BS: I only support GSM…

3G summary

Better crypto algorithms

- Authentication based on AES
- Confidentiality and integrity based KASUMI

Improved authentication protocol (AKA)

- Mutual authentication
- Better replay protection with sequence numbers

Remaining issues

- Optional integrity protection…
- User (IMSI / TMSI) tracking…
- Downgrade attack…

Lecture end

Next week

- 4G and 5G security + discussion

Reading material

- Rupprecht et al. “On Security Research Towards Future Mobile Network Generations”, 2018.

Watching material

- Engel. SS7: Locate. Track. Manipulate. 2014.