



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Security of Wireless Networks

Srdjan Čapkun

Department of Computer Science

ETH Zurich

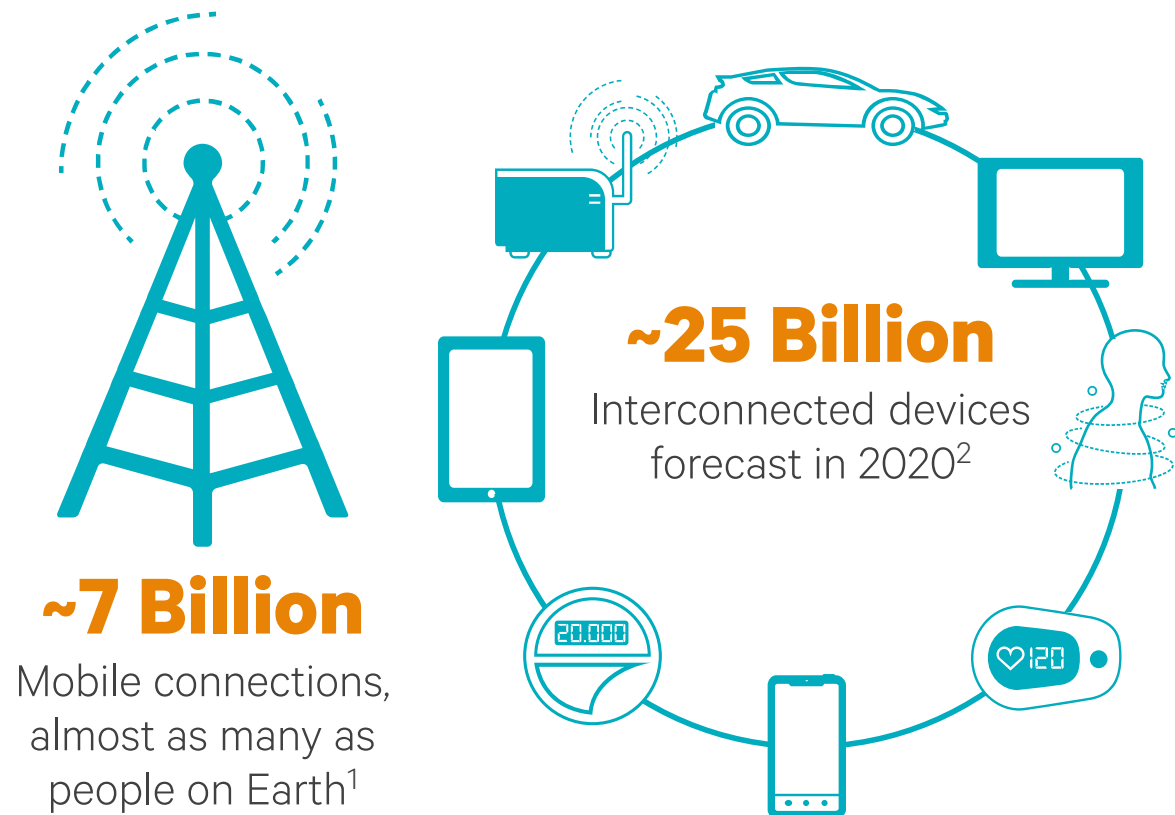
Recommended Readings

- **On Security Research towards Future Mobile Network Generations**, *David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Poepper*, <https://arxiv.org/pdf/1710.08932.pdf>
- **Security for Telecommunications Networks**. Springer, Series: **Advances in Information Security**, *P. Traynor, P. McDaniel and T. La Porta*, August, 2008. (available ETH online library)

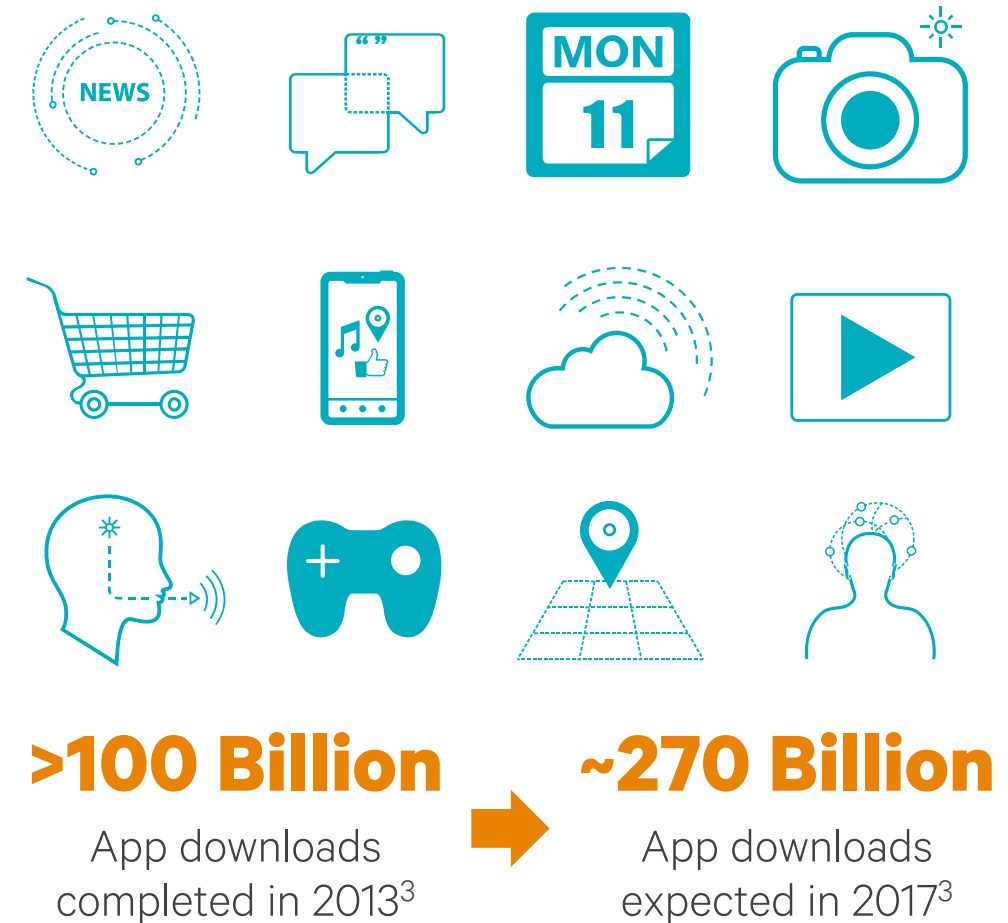
Cellular Networks - Security

The explosion of mobile phones...

Billions of Mobile Connections



Billions of Mobile Experiences



¹ Source: GSMA Intelligence, Apr. '14; ² Source: Machina Research, '13; ³ Source: Gartner, Sep. '13

Evolution of Cellular Networks

Mobile 1G
AMPS, NMT, TACS



Mobile 2G
D-AMPS, GSM/GPRS,
cdmaOne



Mobile 3G
CDMA2000/EV-DO,
WCDMA/HSPA+, TD-SCDMA



Mobile 4G LTE
LTE, LTE Advanced



N/A

Analog Voice



<0.5 Mbps¹

Digital Voice + Simple Data



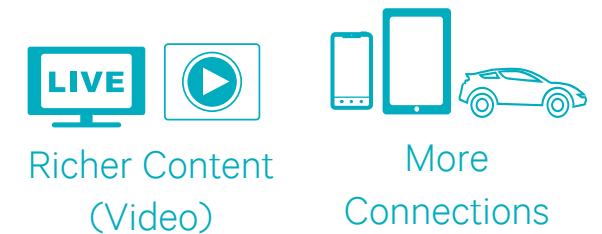
63+ Mbps²

Mobile Broadband



300+ Mbps³

Faster and Better



GSM

GSM (Global System for Mobile Communications) is still the most widely used cellular standard

- > 600 million users, mostly in Europe and Asia; limited coverage and support in USA
- Based on TDMA radio access and PCM trunking
- Use SS7 signalling with mobile-specific extensions
- Provides authentication and encryption capabilities
- Third generation (3G) and future (4G)

GSM

900 MHz (or 1800 MHz) band

- uplink frequency band 890-915 MHz
- downlink frequency band is 935-960 MHz
- 25 MHz subdivided into 124 carrier frequency channels, each 200 kHz apart

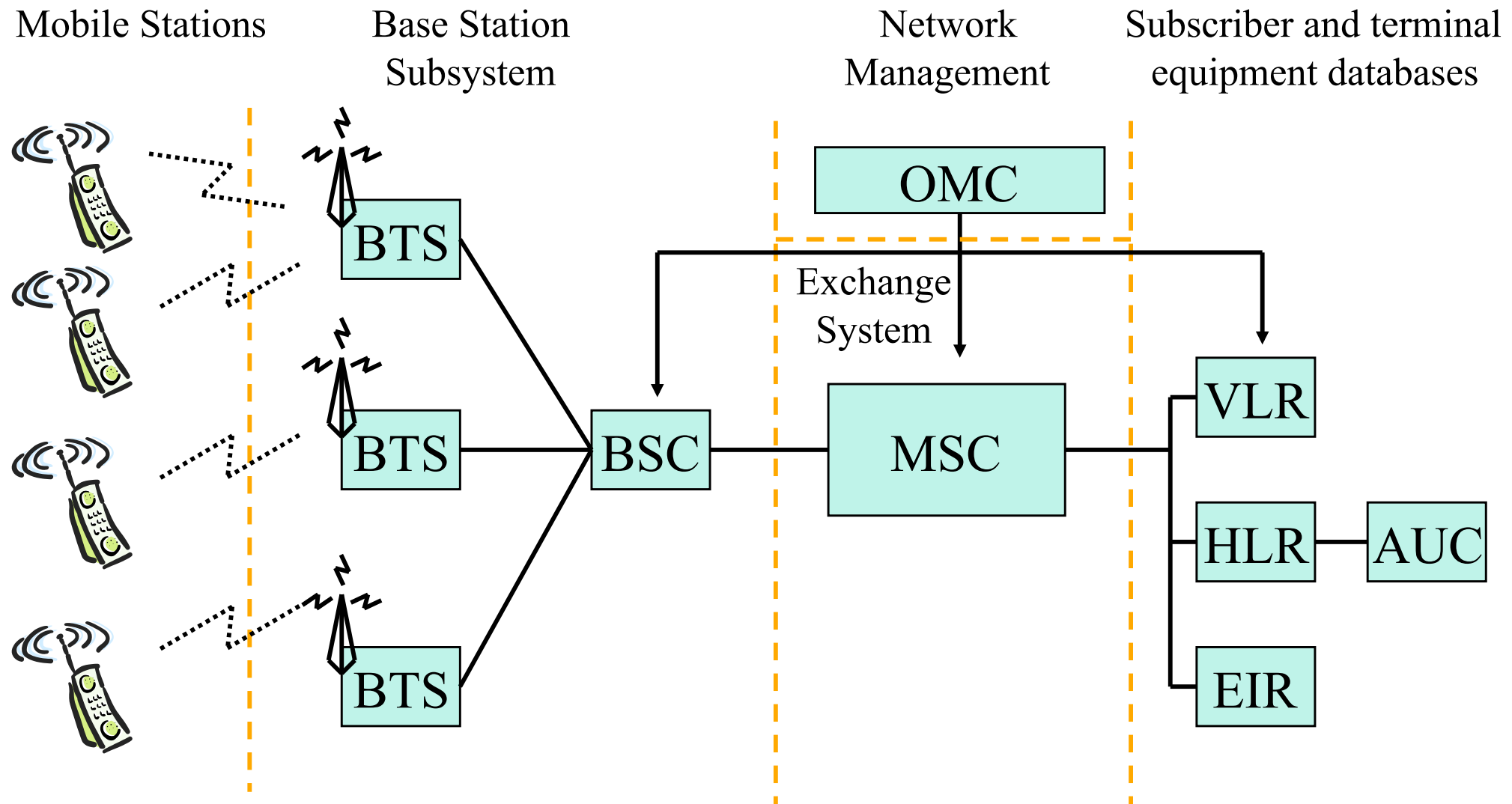
Time division multiplexing (TDMA)

- allows 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 GSM850/900 and 1 watt in GSM1800/1900

Cell size up to 35 km

GSM Architecture



HLR = Home Location Register
AC = Authentication center

VLR = Visitor Location Register
EIR - Equipment Identity Register

GSM Security Goals

Operators

- Bills right people
- Avoid fraud
- Protect Services

Customers

- Privacy
- Anonymity

Make a system at least secure as PSTN?

GSM Security Goals

Confidentiality and Anonymity on the radio path

Strong client *authentication* to protect the operator against the billing fraud

Prevention of operators from compromising of each others' security

- Inadvertently
- Competition pressure

my grandgrandma ...

Two issues:

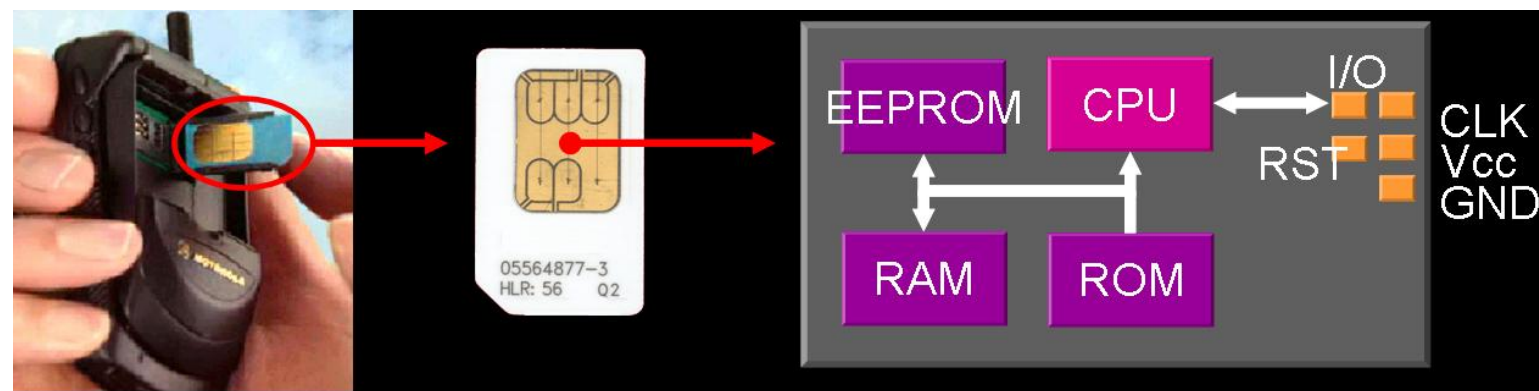
- Talking for free: How do you prove that you are the customer of a network?
- Talking on someone else's expense: How do you differ between two customers?

=> we need a way to distinguish between users
(authentication)

SIM (Subscriber Identification Module)

Subscriber Identification Module (SIM)

- Smart Card – a single chip computer containing OS, File System, Applications
- Owned by operator (*i.e. trusted*)



SIM Cards

Typical specification

- 8 bit CPU
- 16 K ROM
- 256 bytes RAM
- 4K EEPROM
- Cost: \$5-50

Smart Card Technology

- Based on ISO 7816 defining
- Card size, contact layout, electrical characteristics
- I/O Protocols: byte/block based
- File Structure

GSM Mobile

Mobile Equipment (ME)

- Physical mobile device
- Identifiers
 - IMEI – International Mobile Equipment Identity

Subscriber Identity Module (SIM)

- Smart Card containing keys, identifiers and algorithms
- Identifiers
 - Ki – Subscriber Authentication Key
 - IMSI – International Mobile Subscriber Identity
 - TMSI – Temporary Mobile Subscriber Identity
 - MSISDN – Mobile Station International Service Digital Network
 - PIN – Personal Identity Number protecting a SIM
 - LAI – location area identity

The Key is in the Card

Ki – Subscriber Authentication Key

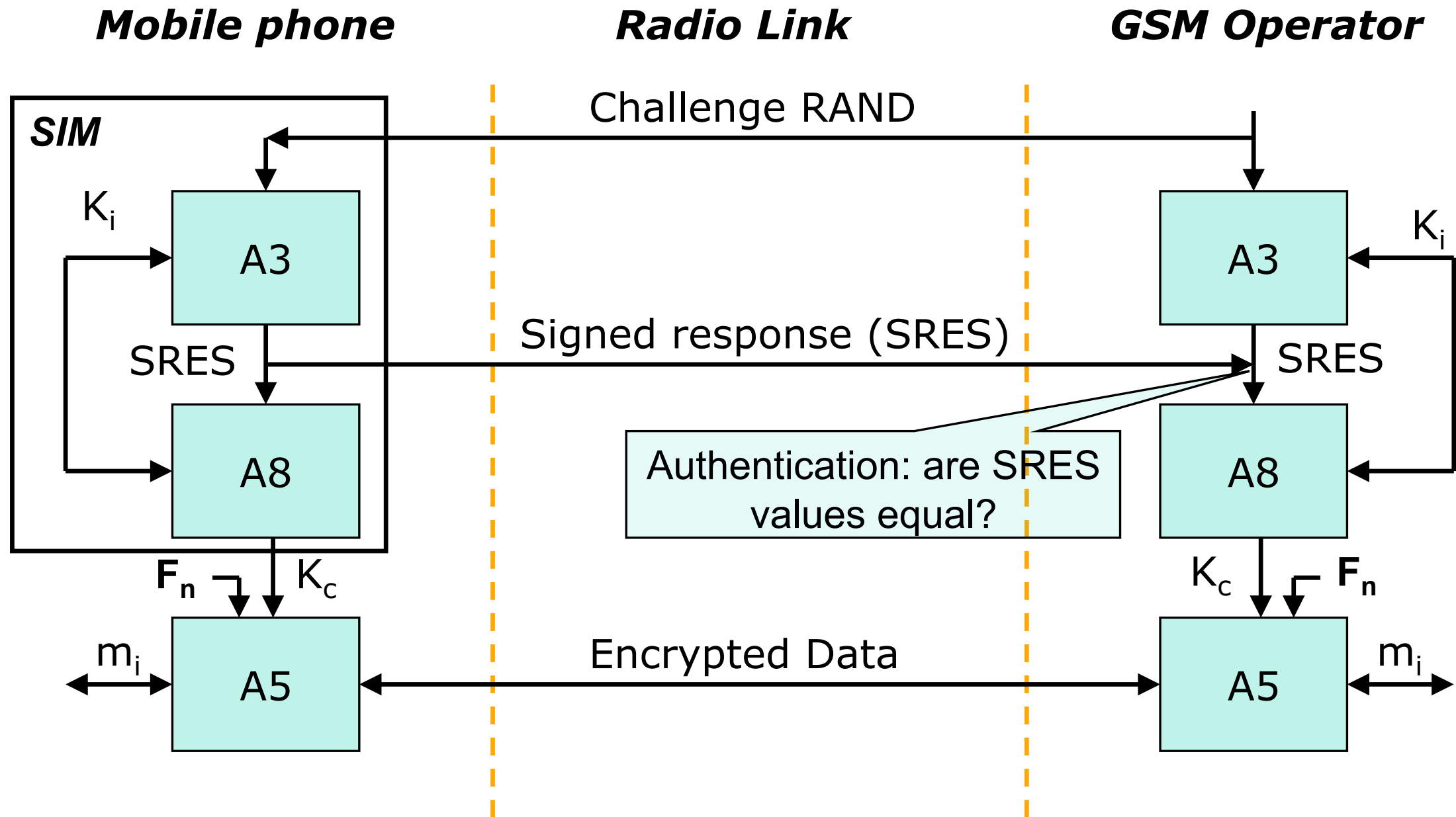
- Shared 128 bit key used for authentication of subscriber by the operator

Key Storage

- Subscriber's SIM (owned by operator, i.e. trusted)
- Operator's Home Locator Register (HLR) of the subscriber's home network



GSM User Authentication



GSM User Authentication

AuC – Authentication Center

- Provides parameters for authentication and encryption functions (RAND, SRES, Kc)

HLR – Home Location Register

- Provides MSC (Mobile Switching Center) with triples (RAND, SRES, Kc)
- Handles MS location

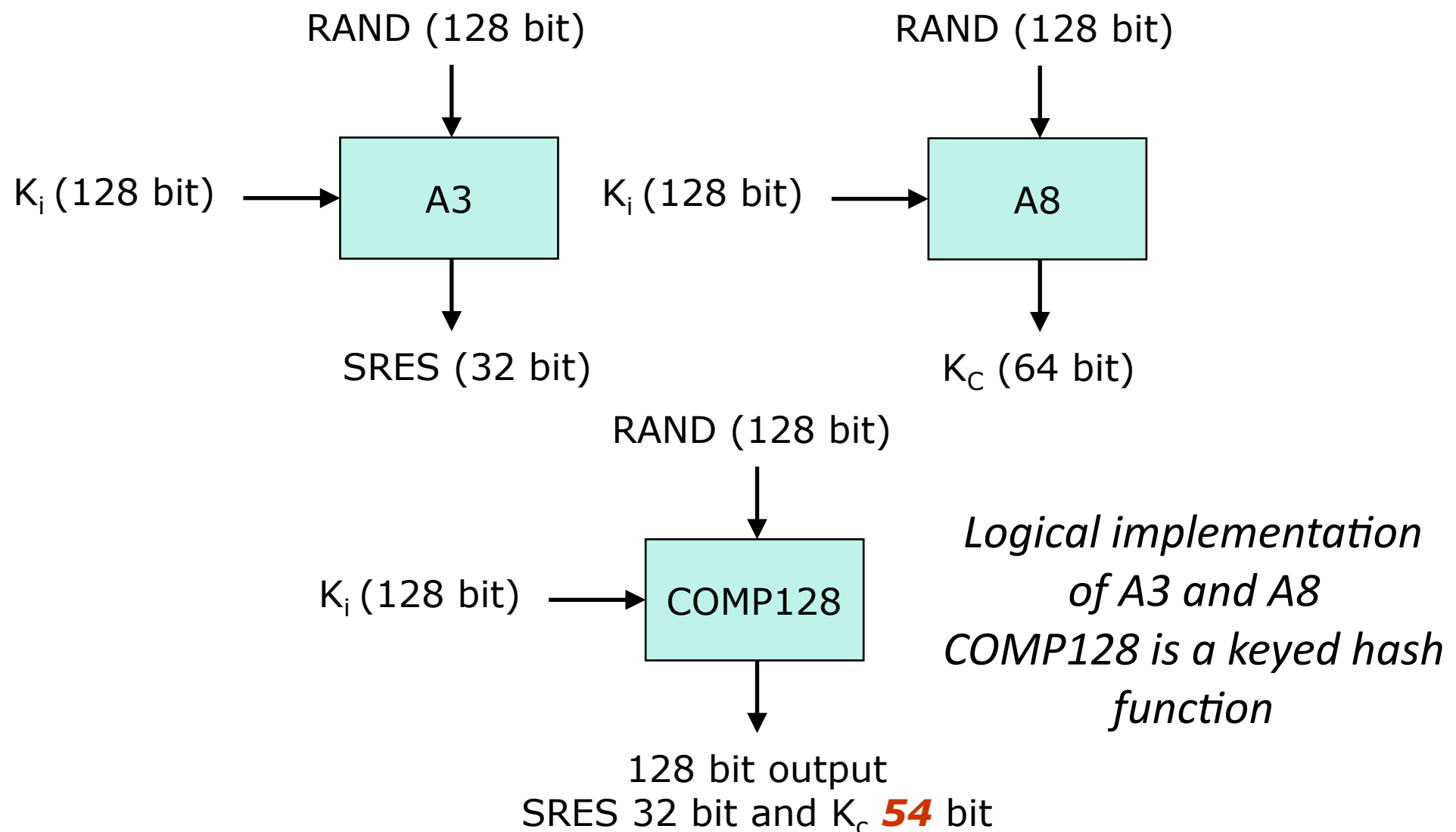
VLR – Visitor Location Register

- Stores generated triples by the HLR when a subscriber is not in his home network
- One operator doesn't have access to subscriber keys of the another operator.

A3 and A8 (Authentication and Session Key)

Both A3 and A8 algorithms are implemented on the SIM

- Operator can decide, which algorithms to use.
- Algorithm implementation is independent of HW and operators.
- A8 was never made public



A5 (Confidentiality)

A5 is a stream cipher

- Implemented very efficiently on hardware

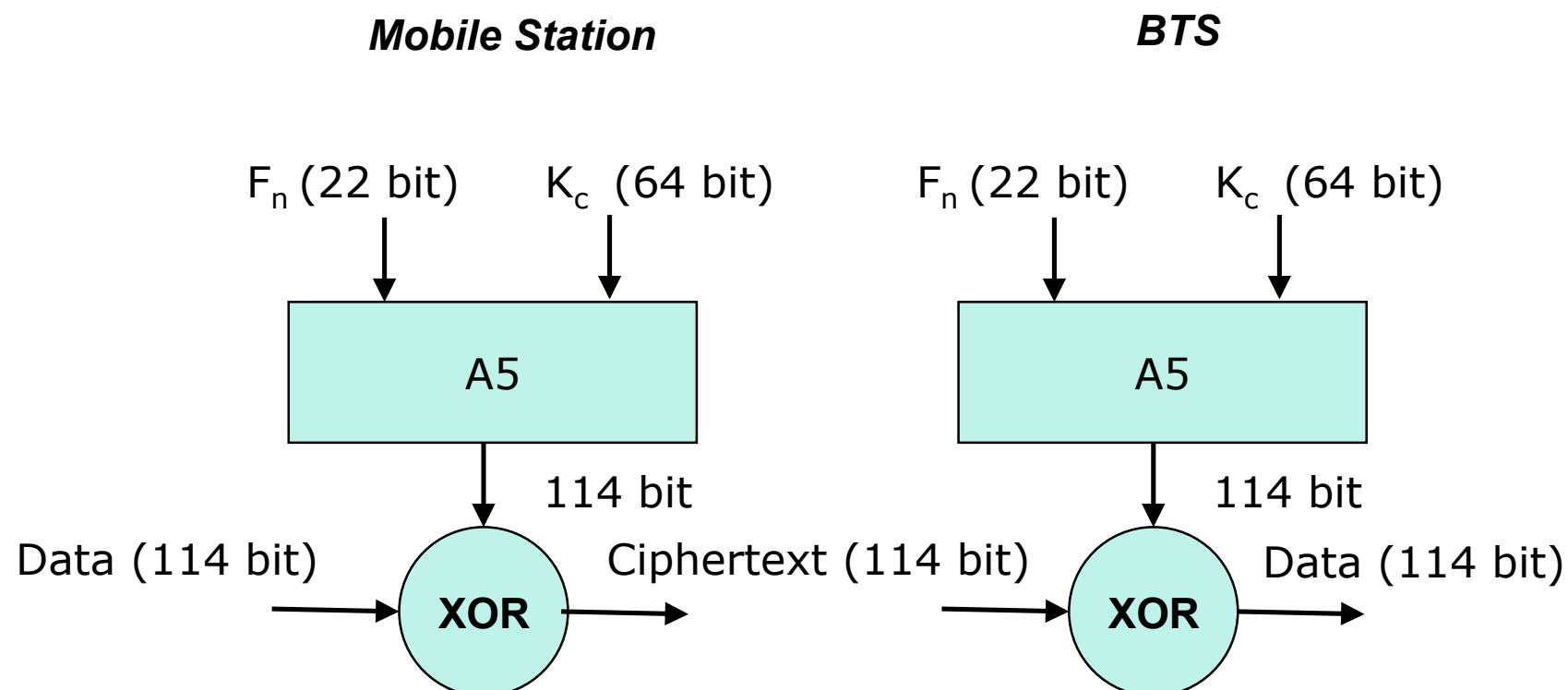
Design was never made public

- Leaked to Ross Anderson and Bruce Schneier

Variants: A5/1 – the strong version, A5/2 – the weak version, A5/3

GSM Association Security Group and 3GPP design

Based on Kasumi algorithm used in 3G mobile systems



Attack History (Authentication and Confidentiality)

1991: First GSM implementation.

April 1998

- The Smartcard Developer Association (SDA) together with U.C. Berkeley researchers cracked COMP128 algorithm stored in SIM and succeeded to get Ki within several hours. They discovered that Kc uses only 54 bits.

August 1999

- The weak A5/2 was cracked using a single PC within seconds.

December 1999

- Alex Biryukov, Adi Shamir and David Wagner have published the scheme breaking the strong A5/1 algorithm. Within two minutes of intercepted call the attack time was only 1 second.

May 2002

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

Attack: Extracting the Key from the SIM card

Attack Goal

- Ki stored on SIM card
- Knowing Ki it's possible to clone SIM

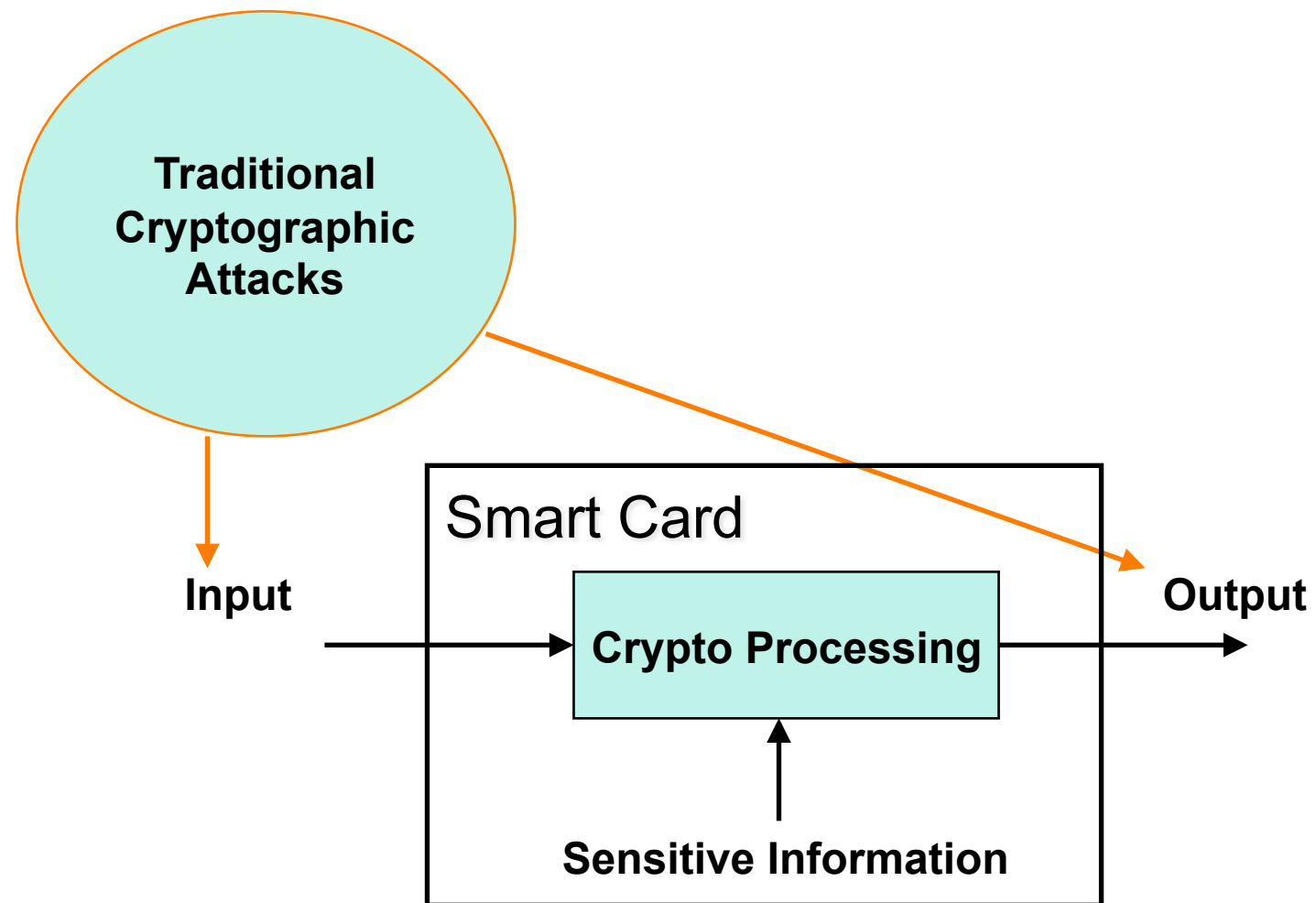
Cardinal Principle

- Relevant bits of all intermediate cycles and their values should be statistically independent of the inputs, outputs, and sensitive information.

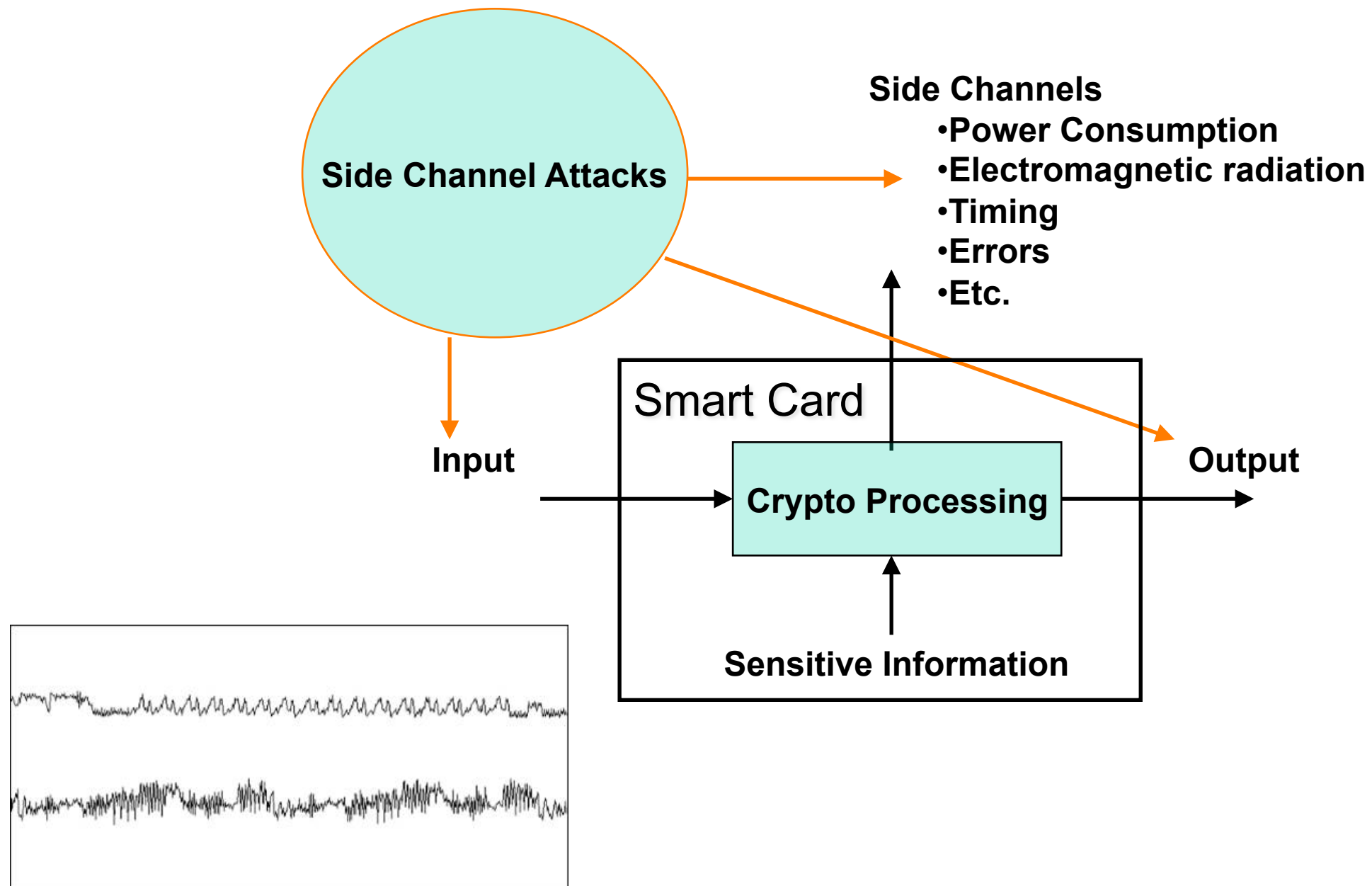
Attack Idea

- Find a violation of the Cardinal Principle, i.e. side channels with signals does depend on input, outputs and sensitive information
- Try to exploit the statistical dependency in signals to extract a sensitive information

Attack: Extracting the Key from the SIM card



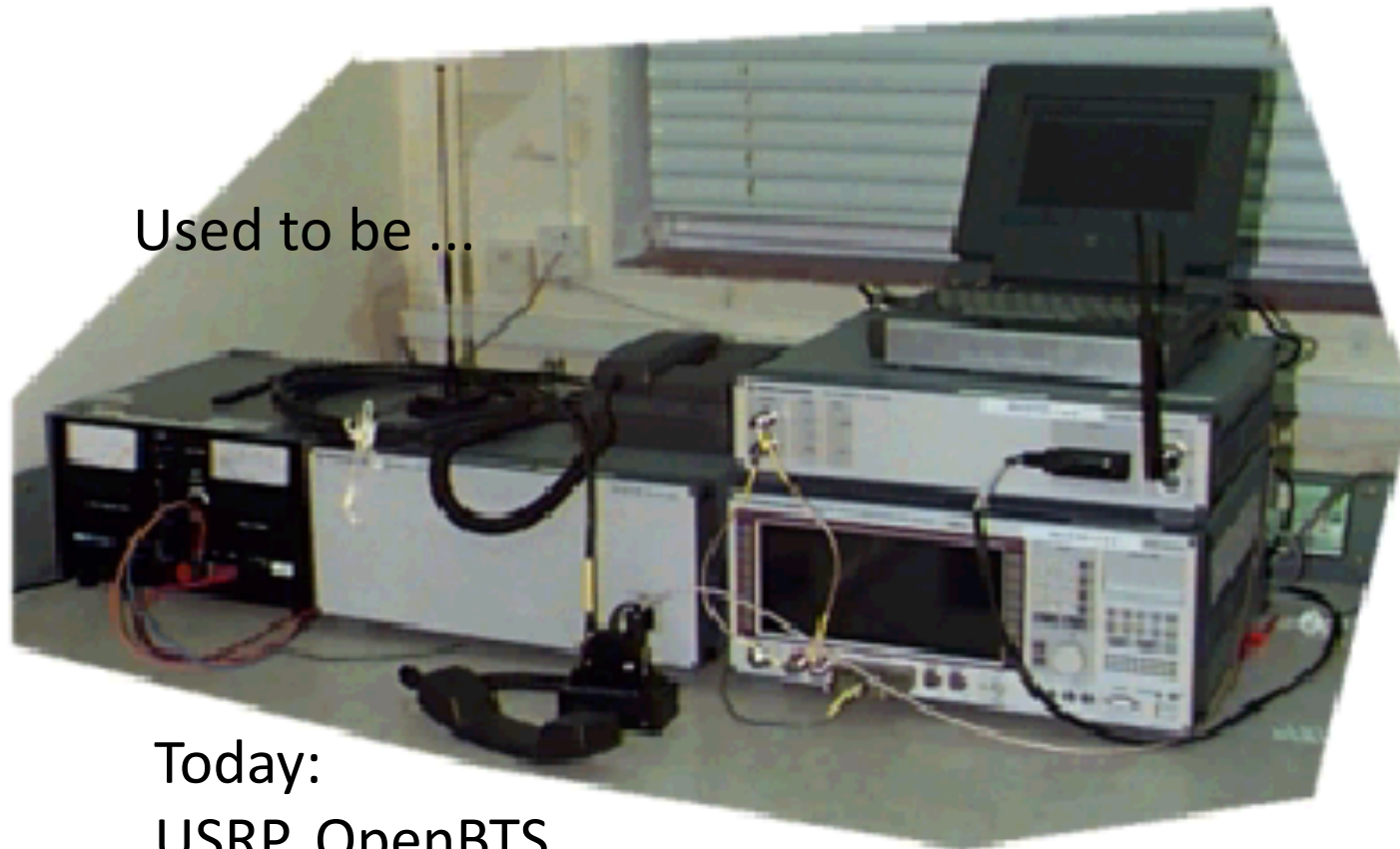
Attack: Extracting the Key from the SIM card



Attack: Fake BS

- IMSI catcher by Law Enforcement
- Intercept mobile originated calls
-

Used to be ...

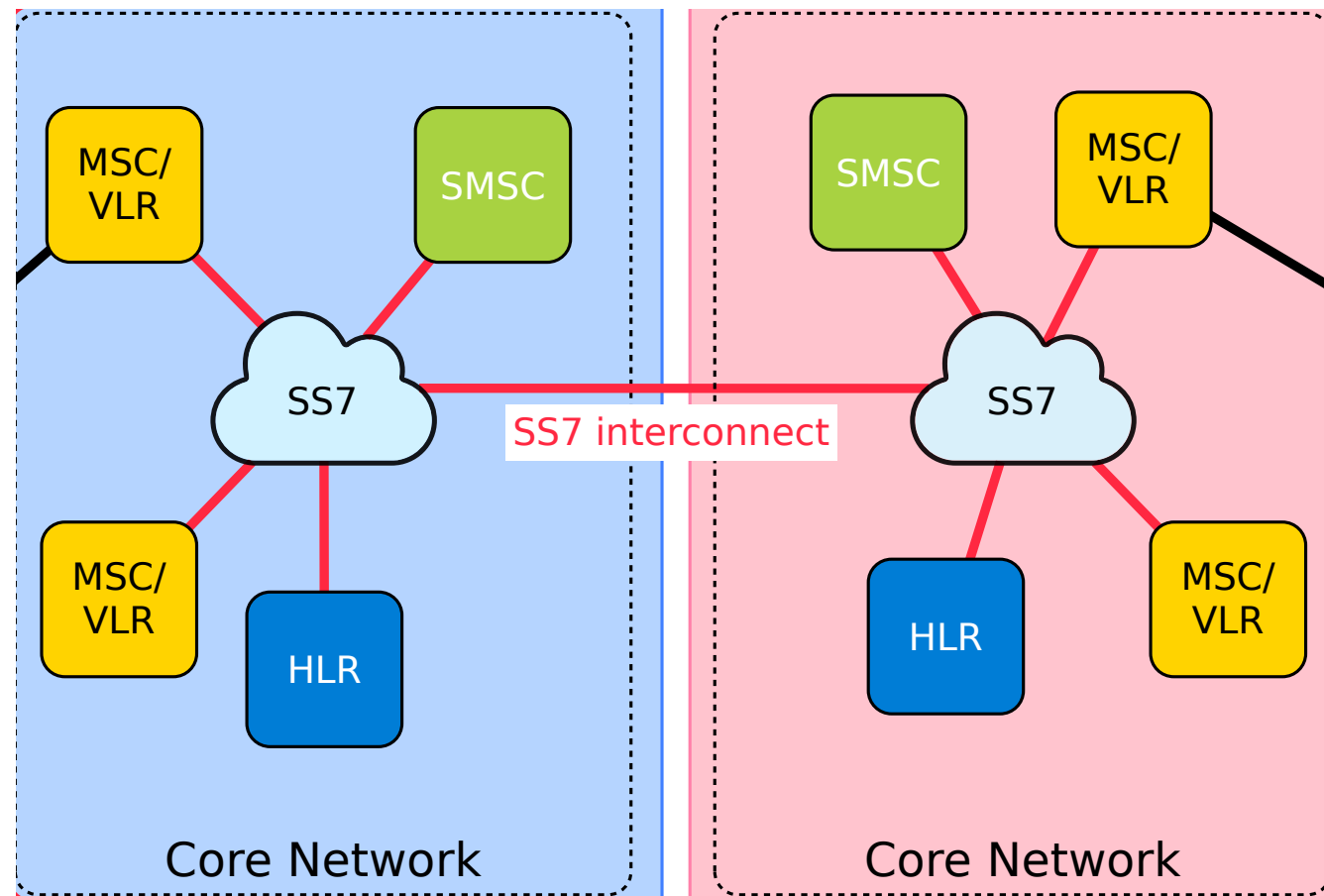


Today:
USRP, OpenBTS



Signalling System #7

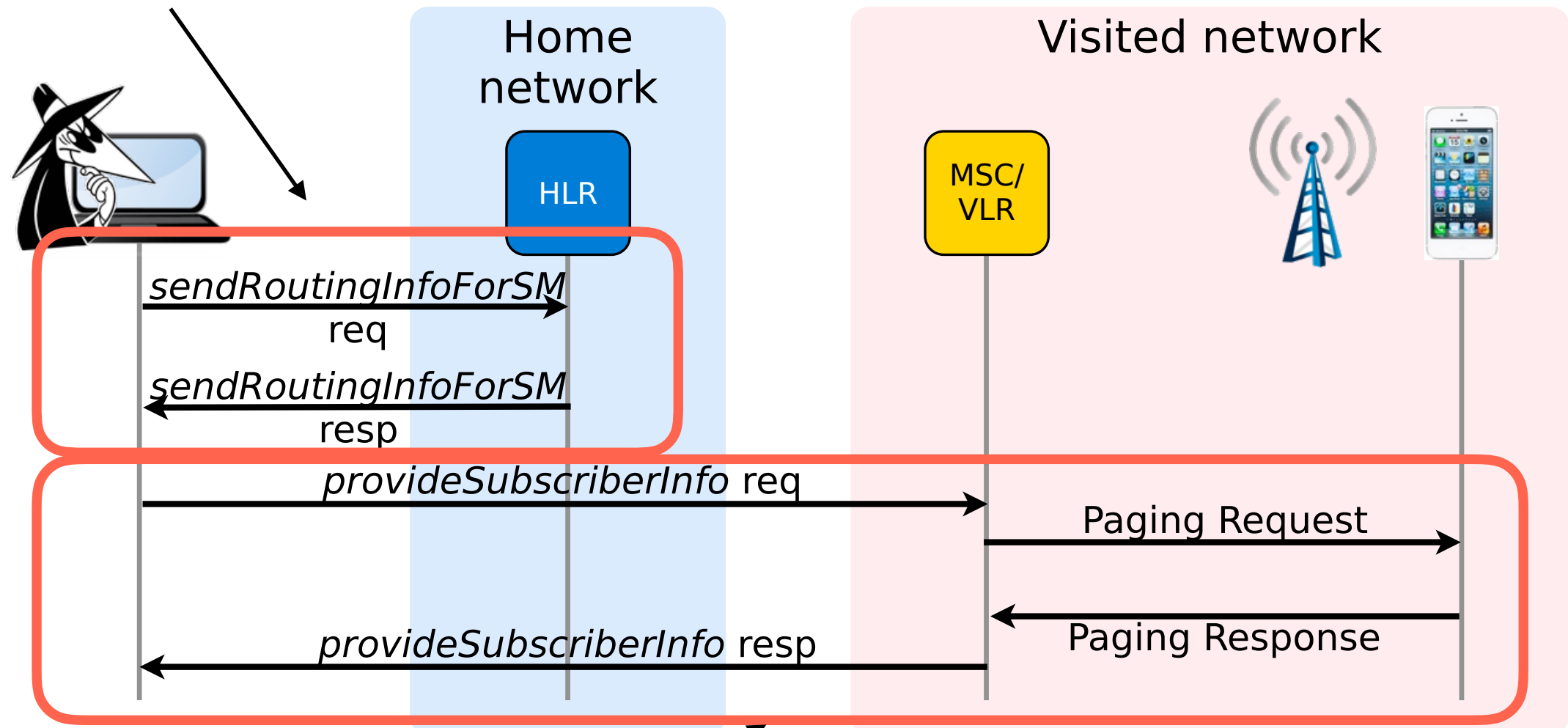
Attack: Location Tracking using SS7



- 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.

Attack: Location Tracking using SS7

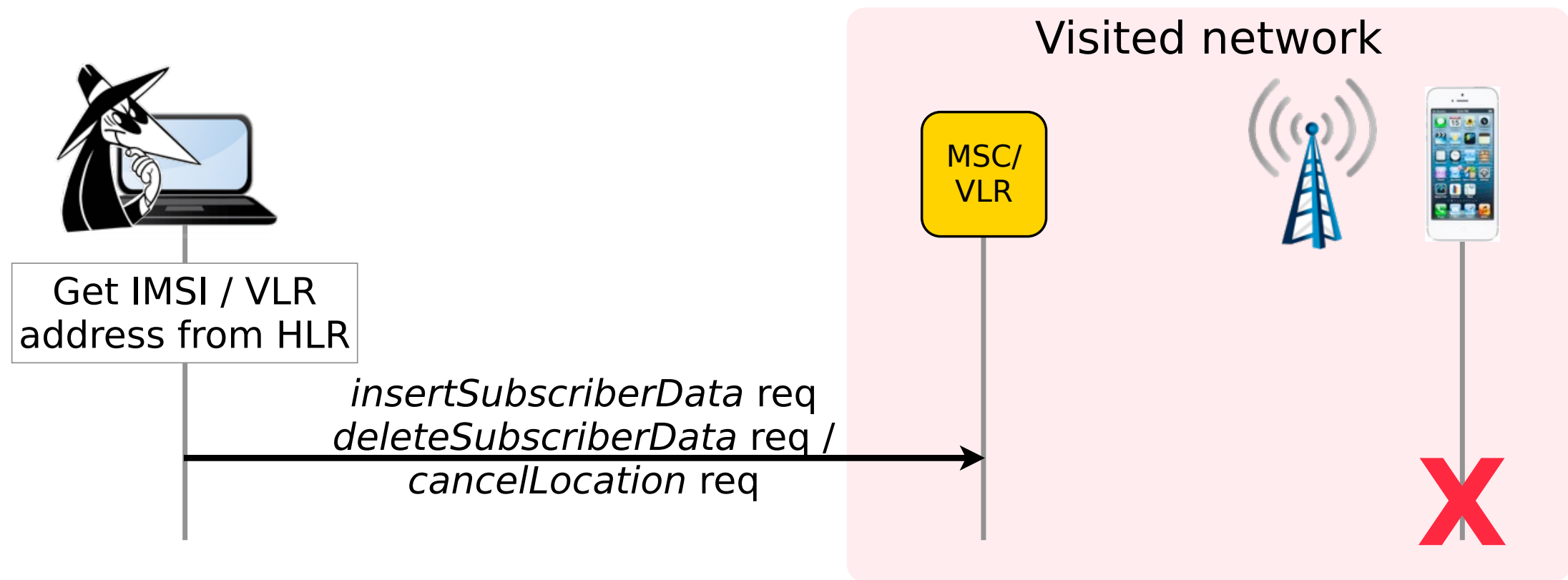
Step 1: Get IMSI and address of current MSC



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

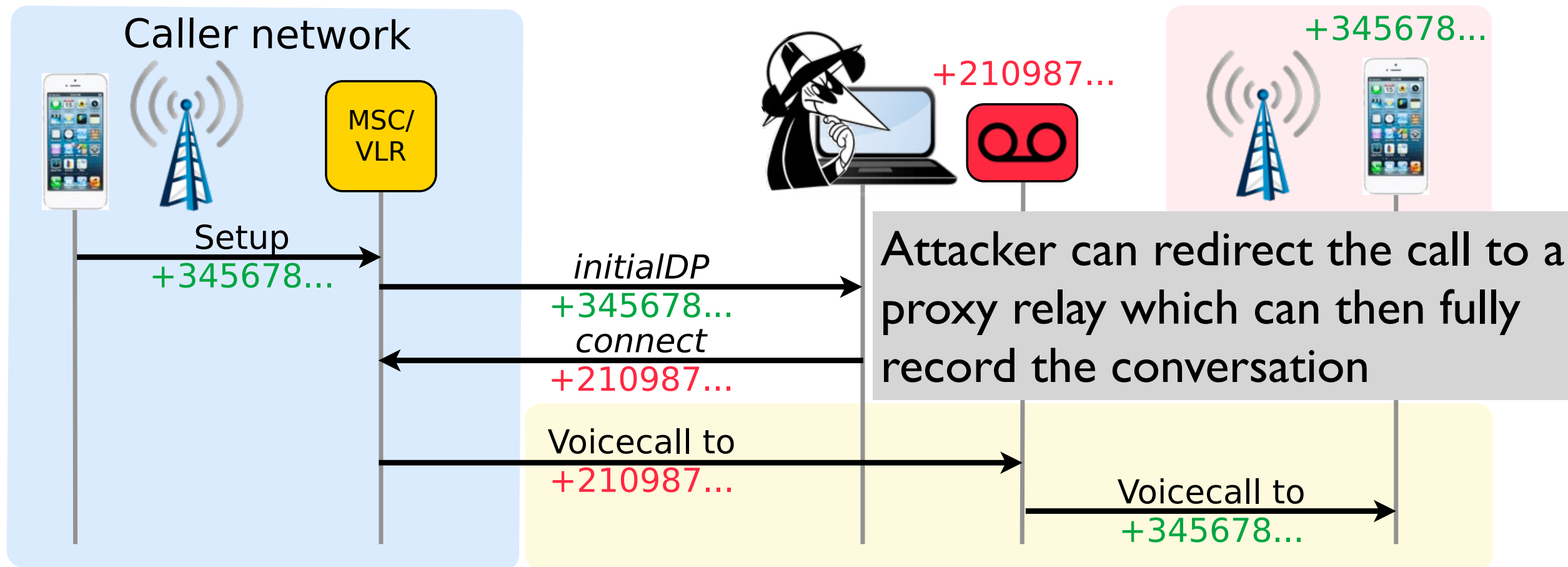
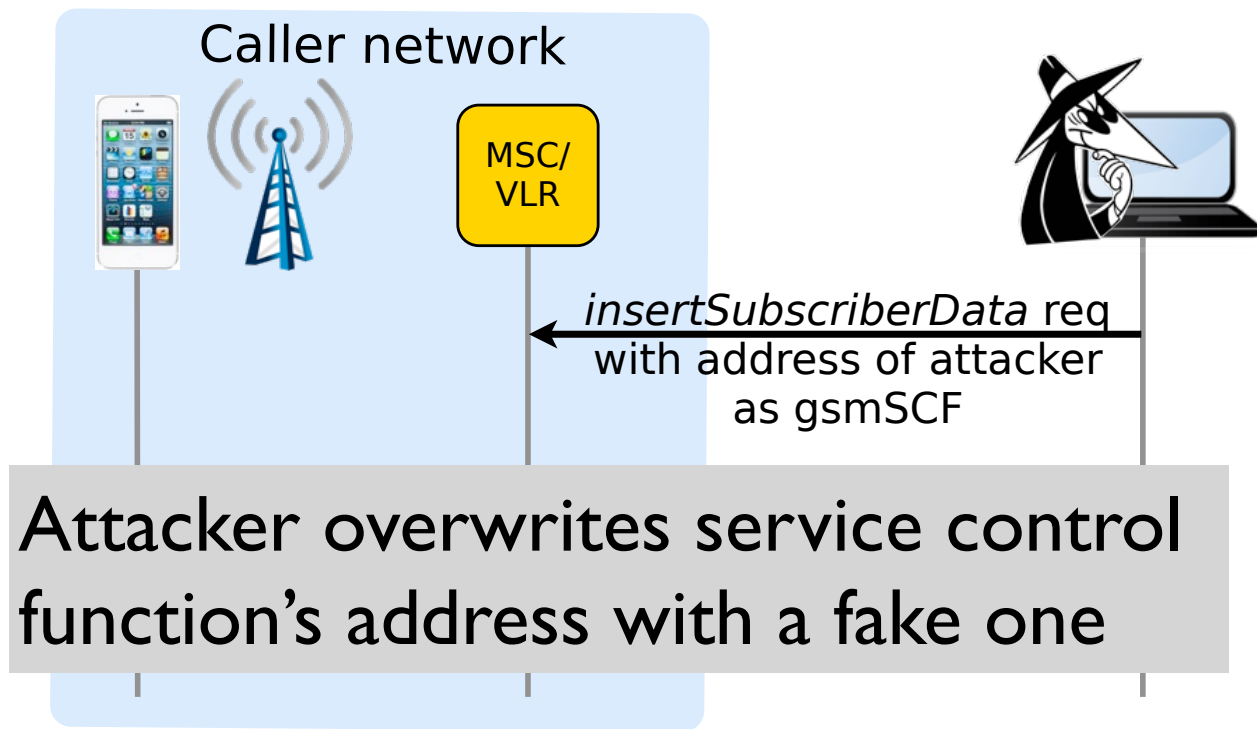
Several online services allow locating the subscriber using the paging response.

SS7: Denial of Service



- 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.

SS7: Intercepting Calls



Network Access

GSM/UMTS

UMTS

UMTS (Universal Mobile Telecommunications System)

Uses W-CDMA,

- 1885-2025 MHz for the mobile-to-base (uplink) and 2110-2200 MHz for the base-to-mobile (downlink)
- supports up to 14 Mbps (in theory) (with HSDPA),
- users in deployed networks can expect up to 384 kbit/s for R99 handsets, and 3.6 Mbit/s for High-Speed Downlink Packet Access (HSDPA) handsets

UMTS Security

Reuse of 2nd generation security principles (GSM):

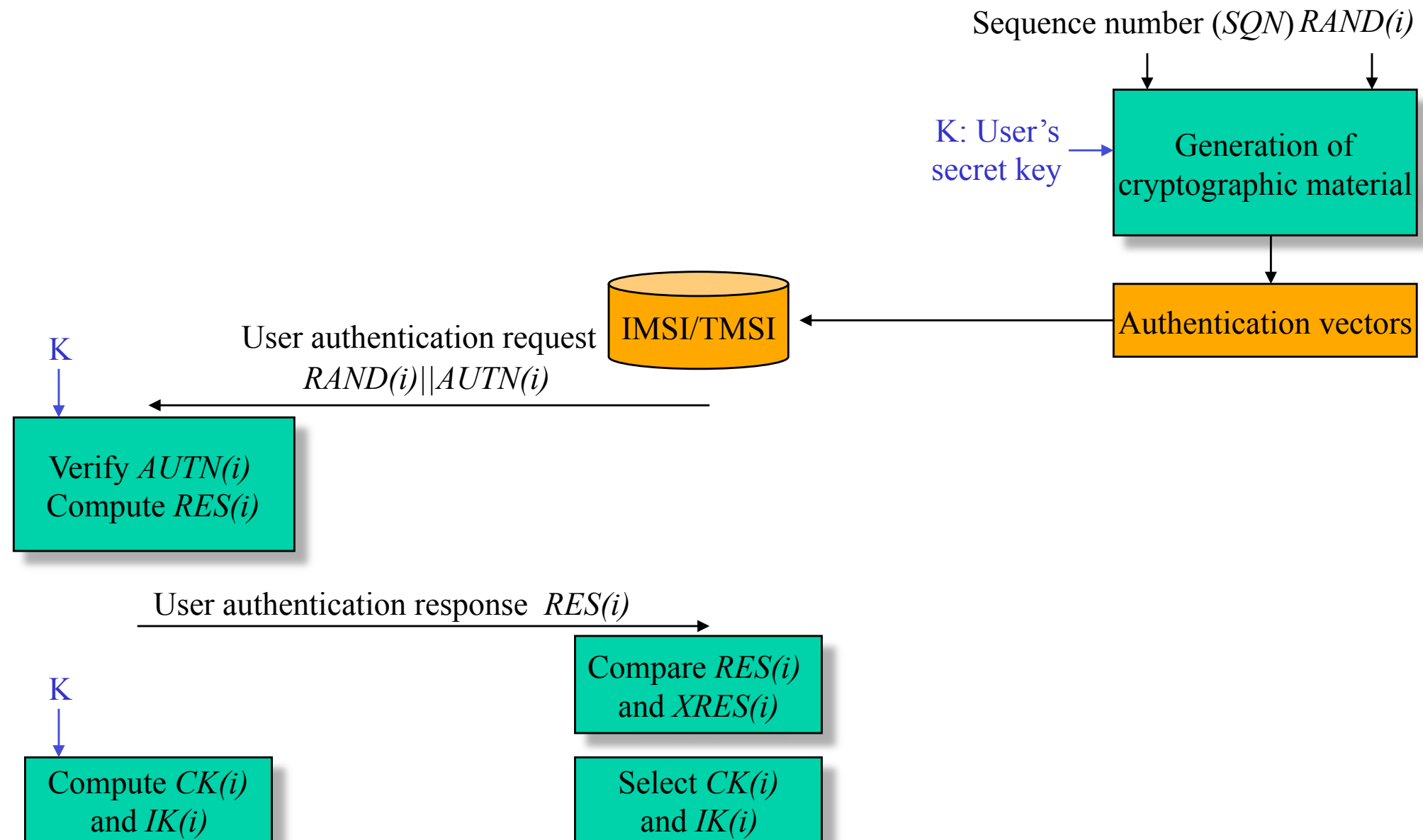
- Removable hardware security module
 - In GSM: SIM card
 - In 3GPP: USIM (User Services Identity Module)
- Radio interface encryption
- Limited trust in the Visited Network
- Protection of the identity of the end user
- Correction of the following weaknesses of the previous generation:
 - *Attacks from a faked base station*
 - *Cipher keys and authentication data transmitted in clear between and within networks*
 - *Encryption not used in some networks*
 - *Data integrity not provided*

UMTS Authentication (with a Visited Network)

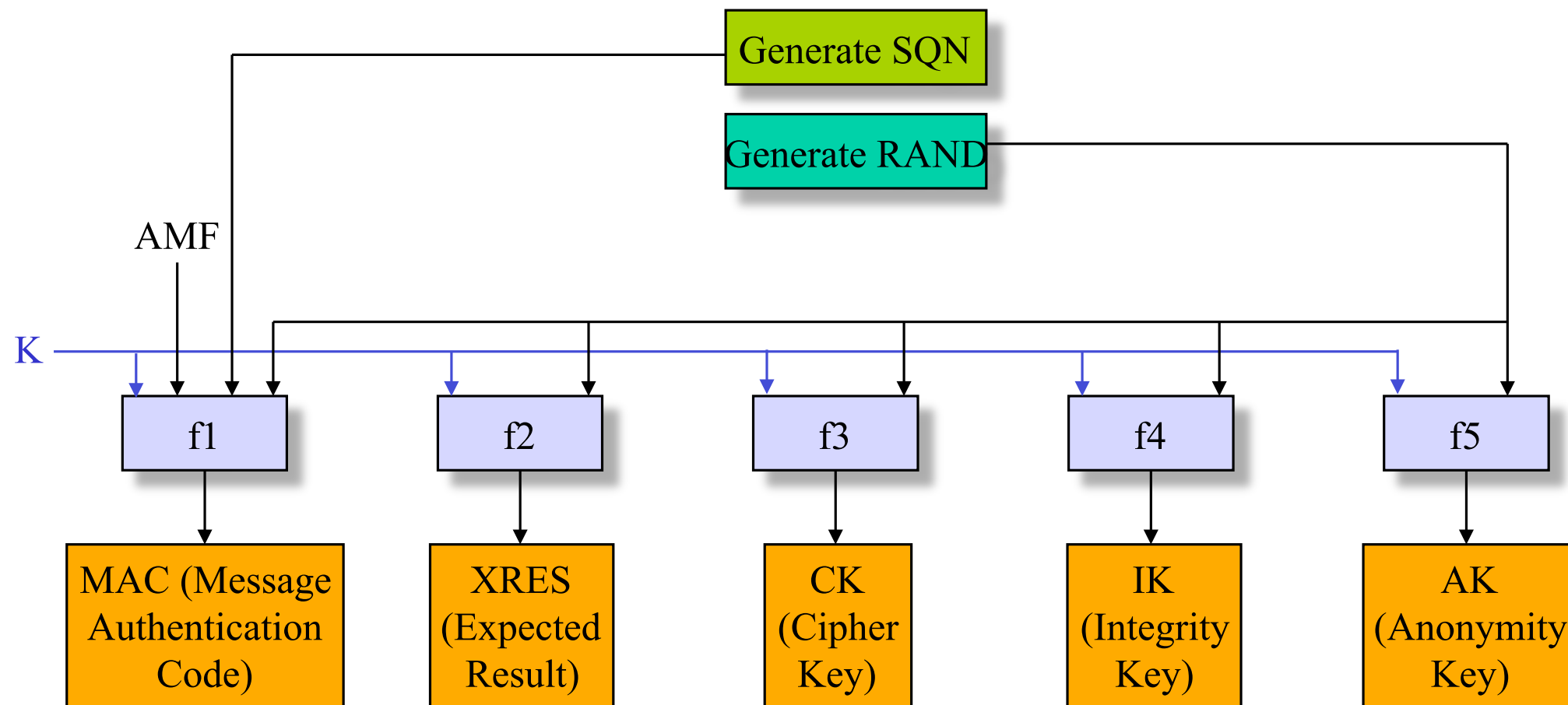
Mobile Station

Visited Network

Home Environment



Generation of Authentication Vectors (by the Home Environment)

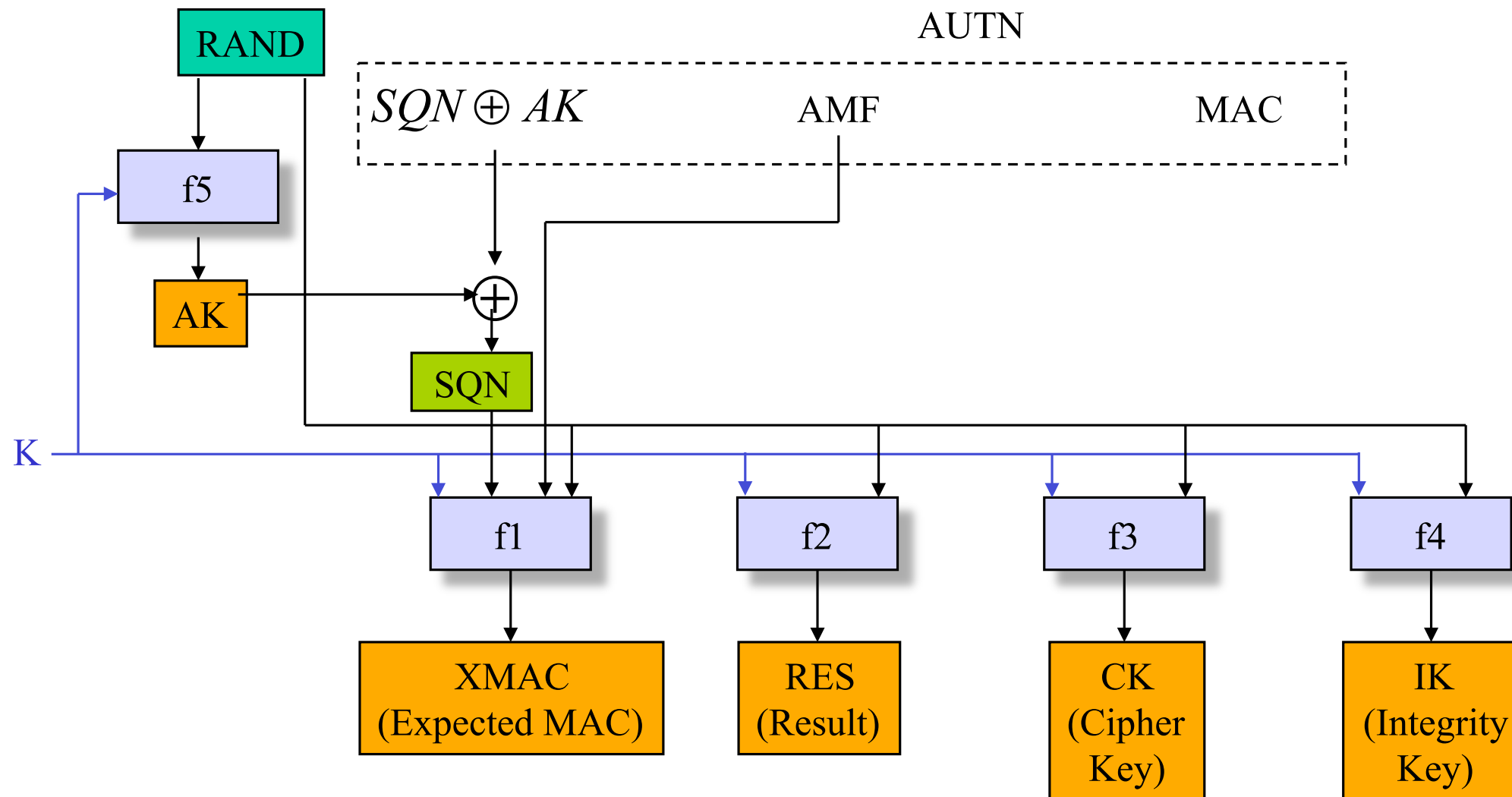


Authentication token: $AUTN = (SQN \oplus AK) || AMF || MAC$

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

AMF: Authentication and Key Management Field

User Authentication Functions in USIM



- Verify $MAC = XMAC$
- Verify that **SQLN** is in the correct range

USIM: User Services Identity Module

More About Authentication and Key Generation

In addition to f_1 , f_2 , f_3 , f_4 and f_5 , two more functions are defined: f_1^* and f_5^* , used in case the authentication procedure gets desynchronized (detected by the range of SQN).

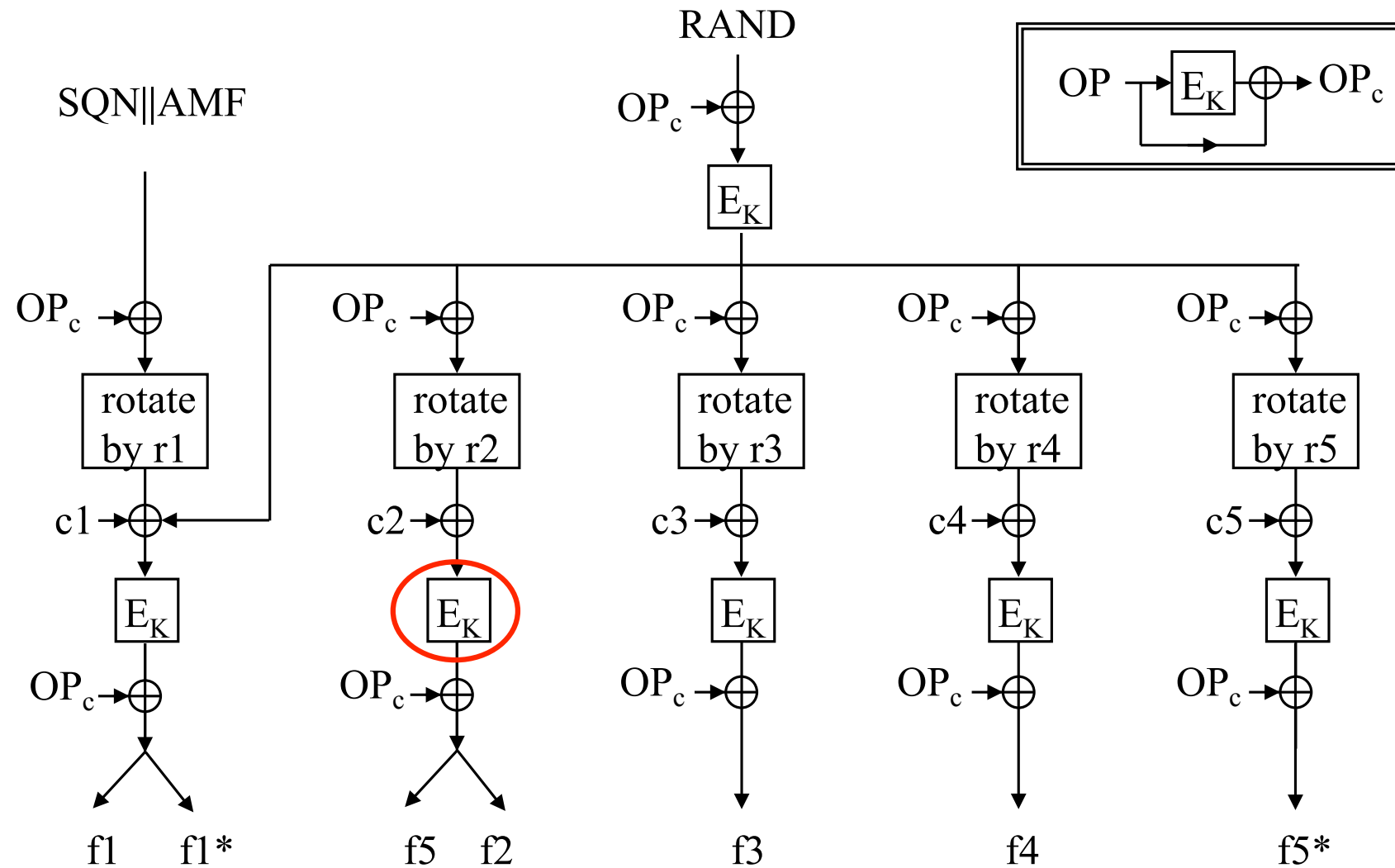
f_1 , f_1^* , f_2 , f_3 , f_4 , f_5 and f_5^* are operator-specific

However, 3GPP provides a detailed example of algorithm set, called MILENAGE

MILENAGE is based on the Rijndael block cipher

In MILENAGE, the generation of all seven functions $f_1 \dots f_5^*$ is based on the Rijndael algorithm

Authentication and Key Generation Functions (f1...f5*)

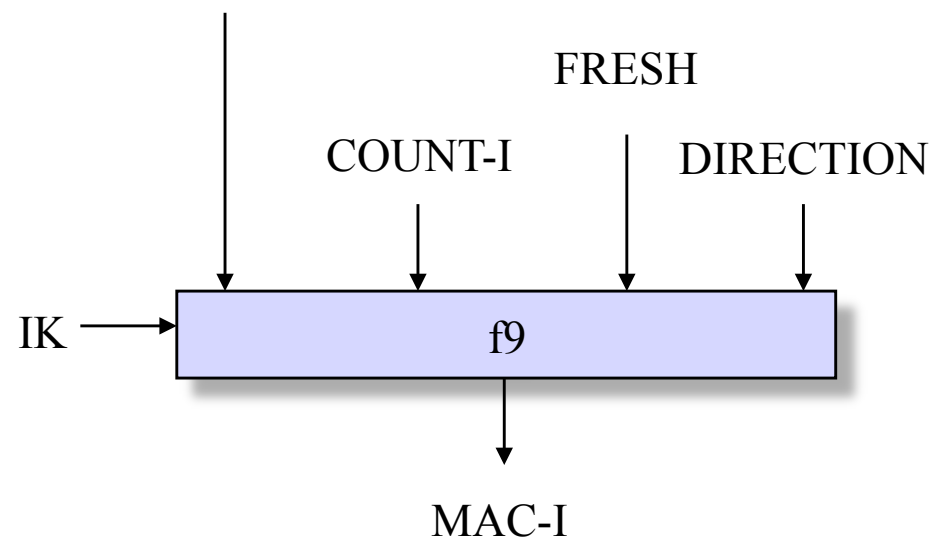


OP: operator-specific parameter
 r1,..., r5: fixed rotation constants
 c1,..., c5: fixed addition constants

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

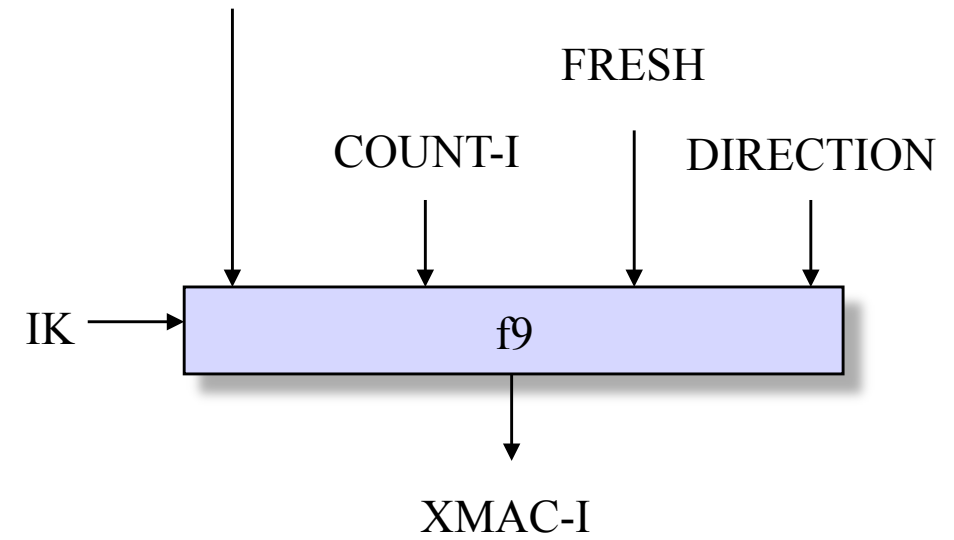
Signaling Integrity Protection

SIGNALLING MESSAGE



Sender
(Mobile Station or
Radio Network Controller)

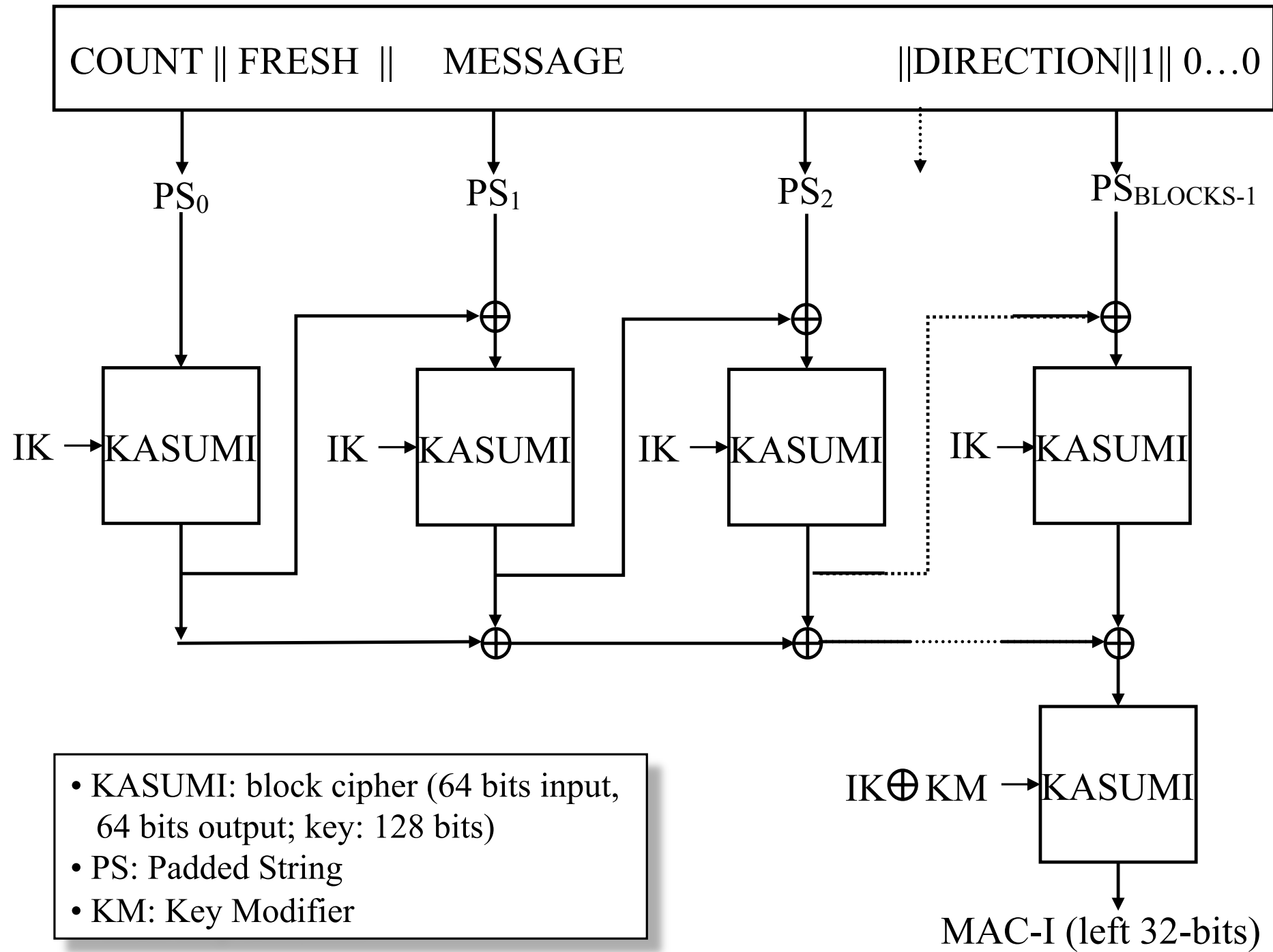
SIGNALLING MESSAGE



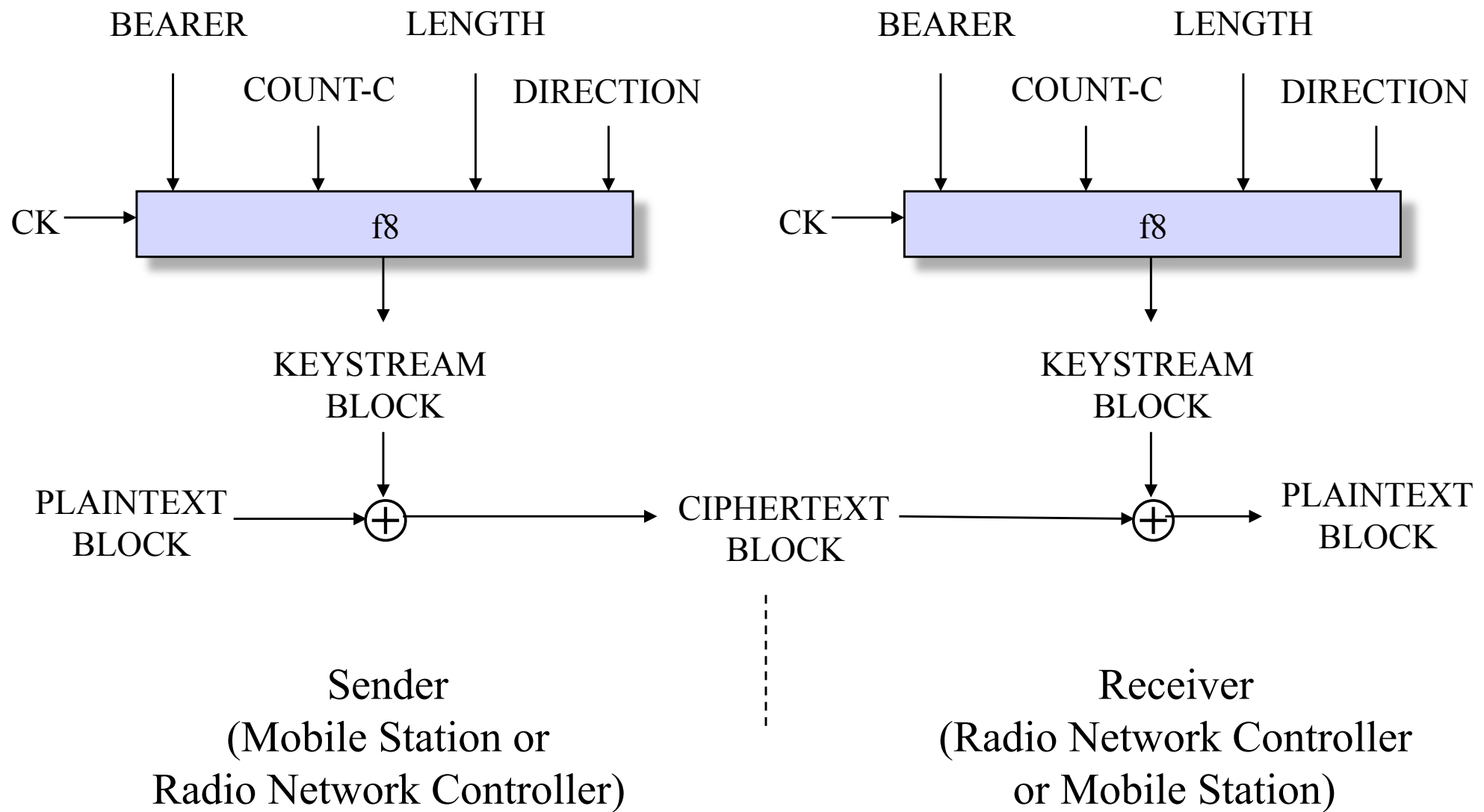
Receiver
(Radio Network Controller
or Mobile Station)

FRESH: random input

f9 integrity function

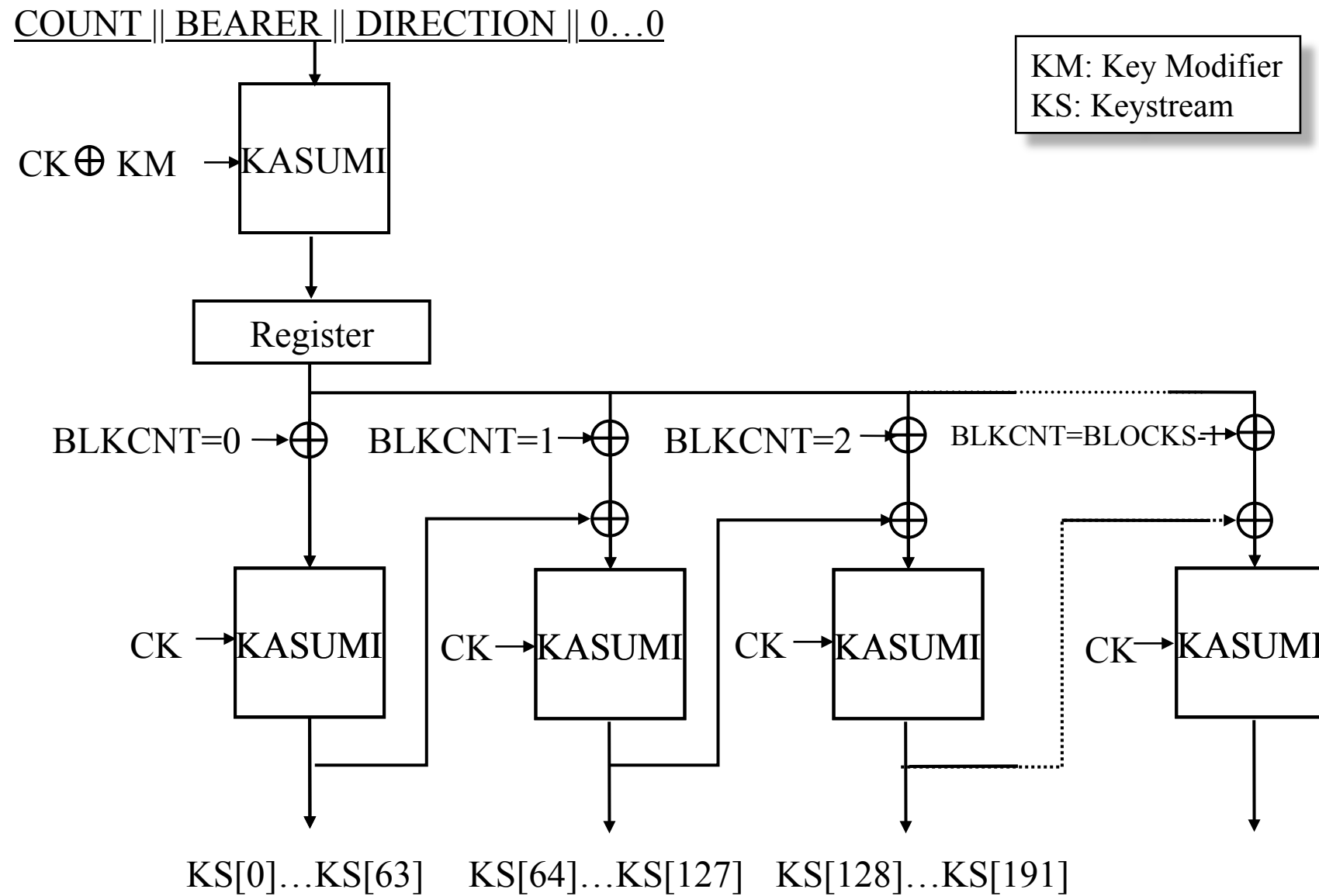


Encryption



BEARER: radio bearer identifier
COUNT-C: ciphering sequence counter

f8 keystream generator



Conclusion on UMTS Security

Some improvement with respect to 2nd generation

Cryptographic algorithms are published

Integrity of the signaling messages is protected

Quite conservative solution

2nd/3rd generation interoperation will be complicated and might open security breaches

All that can happen to a fixed host attached to the Internet could happen to a 3G terminal

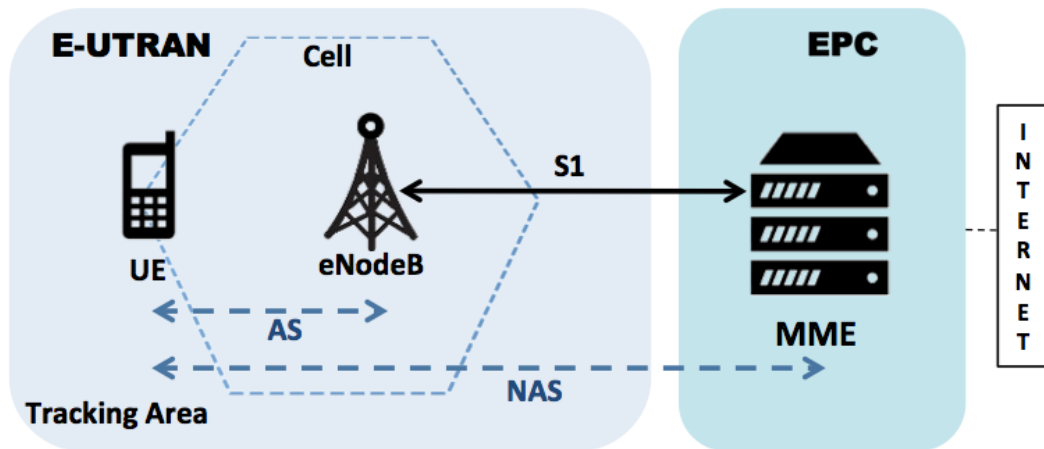
Privacy/anonymity of the user not completely protected: IMSI is sent in cleartext when the user is registering for the first time in the serving network (trusted third party can be a solution)

A user can be enticed to camp on a false BS. Once the user camps on the radio channels of a false BS, the user is out of reach of the paging signals of SN

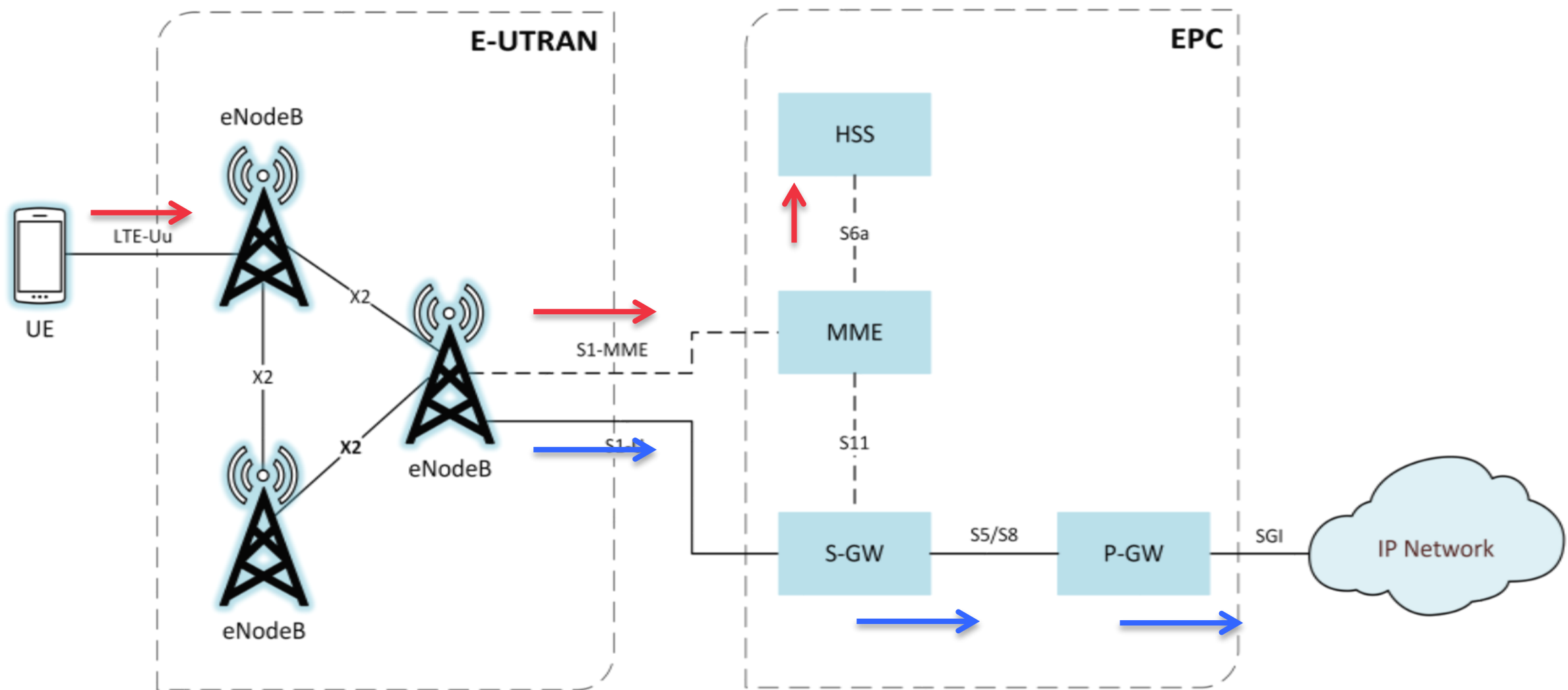
Hijacking outgoing/incoming calls in networks with disabled encryption is possible. The intruder poses as a man-in-the-middle and drops the user once the call is set-up

LTE

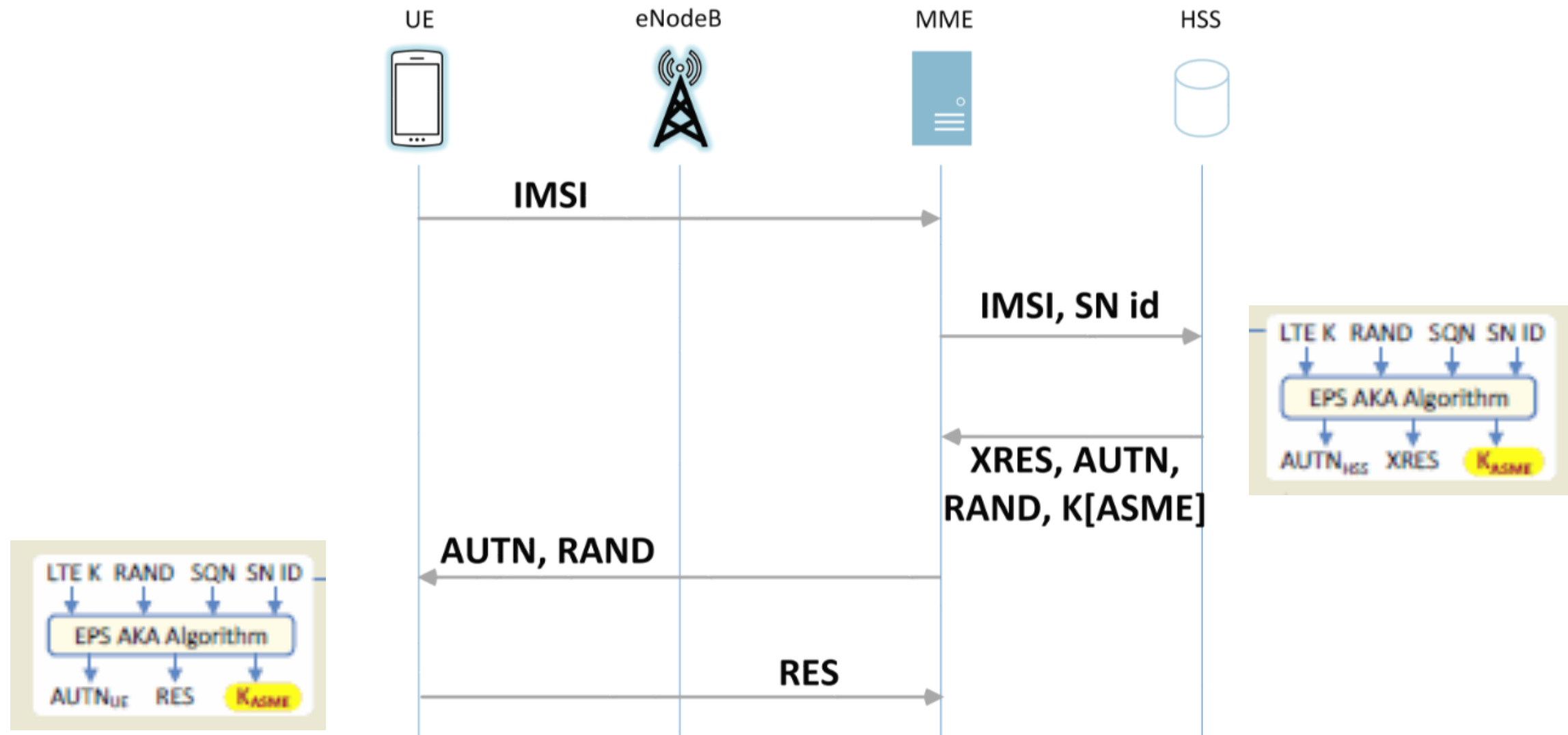
LTE System Architecture



- eNodeB: RF component of LTE
- MME: Mobility Management Entity (Primary Signalling Node)
- HSS: Home subscriber service. Similar to HLR in 2G



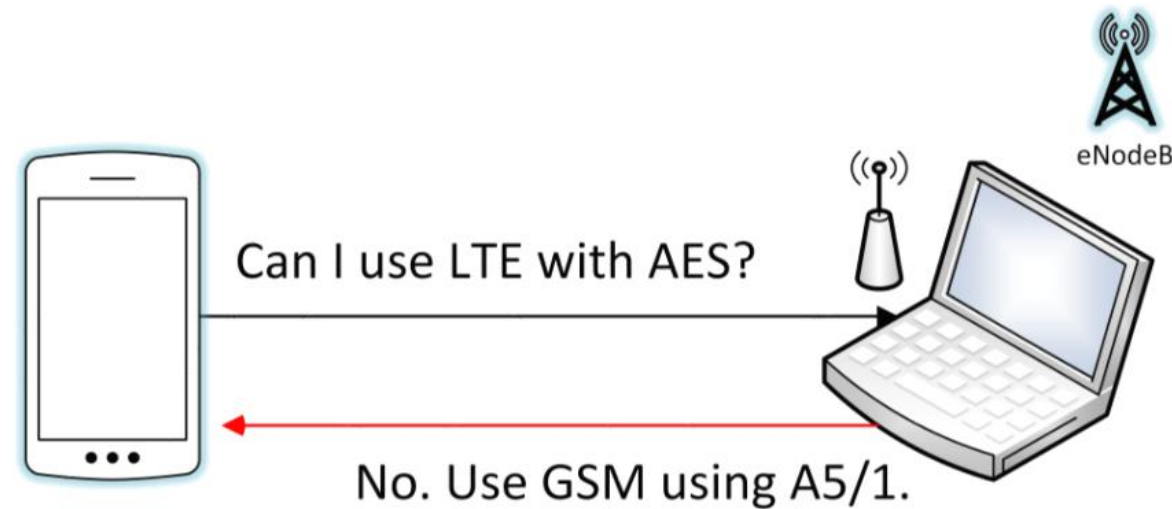
LTE Security Architecture (Authentication)



Network Authentication:
 $AUTN_{ue} = AUTN_{hss}$

User Authentication:
 $RES = XRES$

LTE Attacks: Renegotiation Attacks



- The UE to eNodeB interface can be protected using either of the three algorithm
 - SNOW 3G, ZUC and AES
- Rogue base station can force a UE to downgrade to 2G where significant weaknesses exists

LTE Attacks: Location & Identity Leaks

- **Paging** refers to the process used when MME needs to locate a UE in a particular area and deliver a network service, such as incoming calls.
- MME sends a broadcast signal with the corresponding IMSI/T-IMSI to all eNodeBs in a specific tracking area
- UE decodes the paging message and if its IMSI is present, generates a “random access procedure”.
- A passive attacker can collect set of IMSIs in the area by simply sniffing over the LTE air interface (coarse grained location tracking).
- Once coarse grained location is available, the attacker can force the UE to attach to a rogue eNodeB and estimate its fine grained location estimate through unauthenticated reconfiguration requests

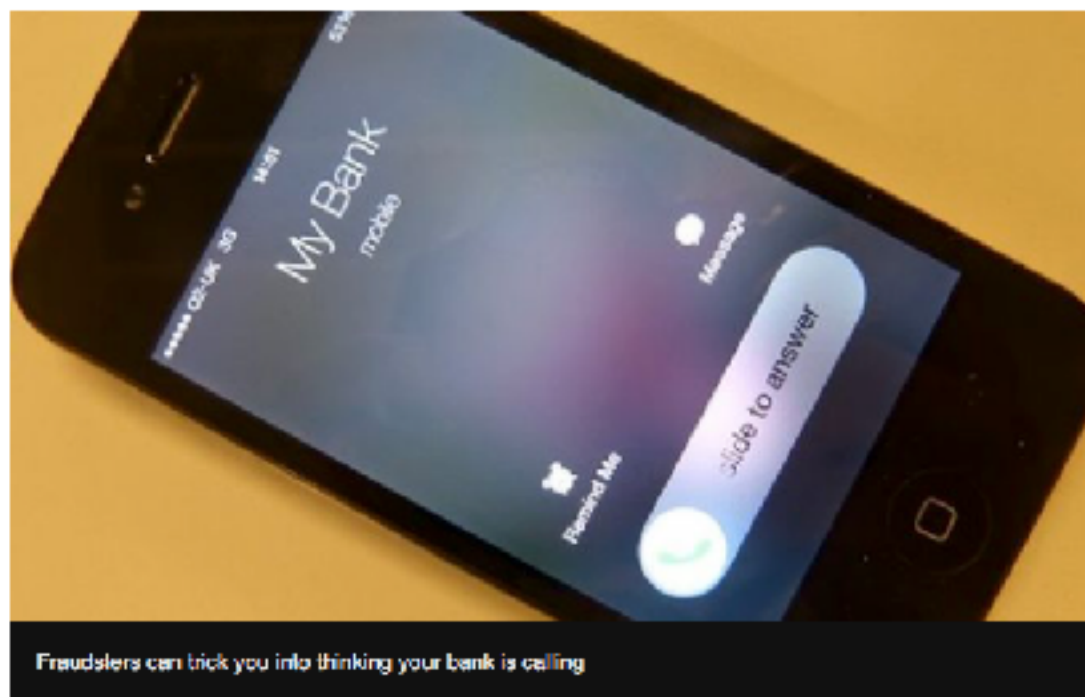
Security Issues of Modern Telephony Systems

Caller ID spoofing

New 'number spoofing' scam nets millions for fraudsters

29 October 2014 Business

f t b e Share



OCT 6, 2016 @ 09:30 AM 92,738 VIEWS

Dozens Arrested In IRS Phone Scam Call Center Raids



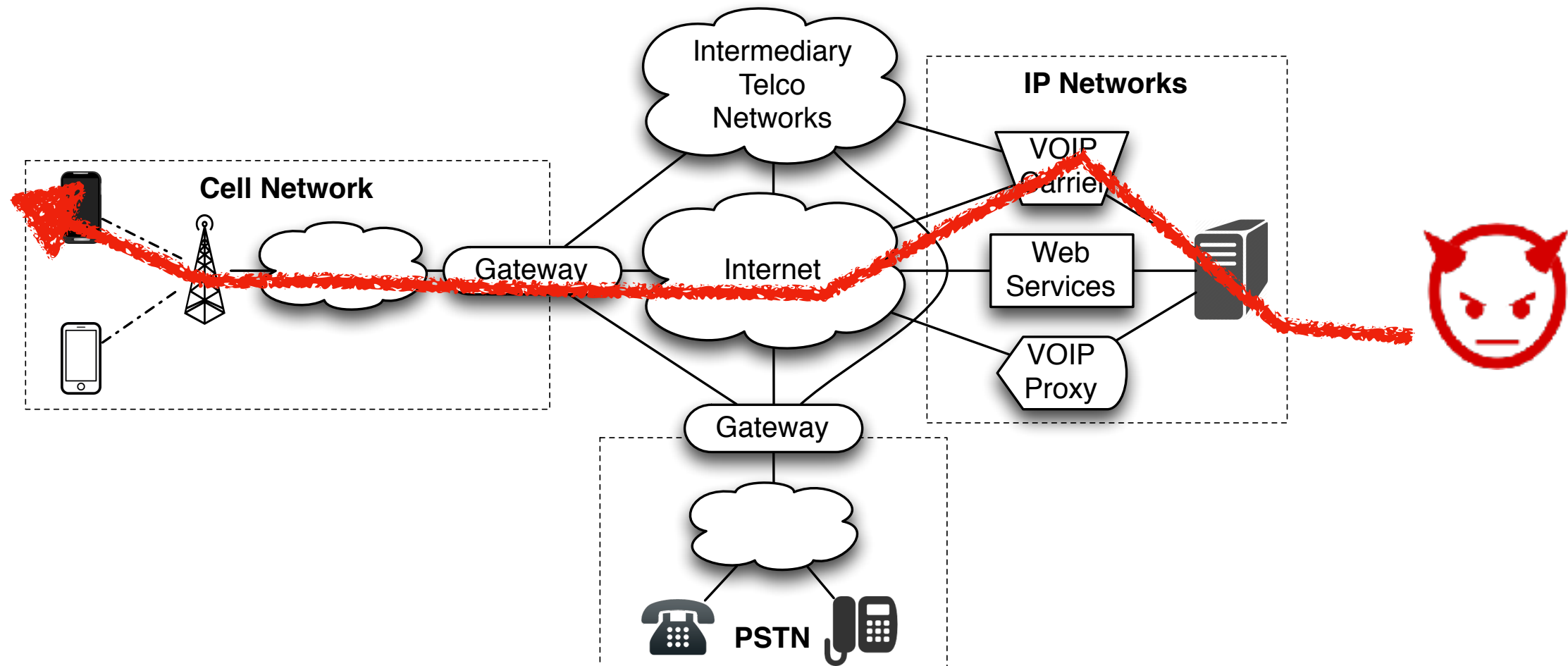
Kelly Phillips Erb, FORBES STAFF

I cover tax: paying tax is painful but reading about it shouldn't be. FULL BIO

theguardian

The terror of swatting: how the law is tracking down high-tech prank callers

Spoofing caller id is easy...



- Majority of scammers use VOIP to spoof the caller id
- Many apps available today



Authentication in Telephony Networks

- No authentication of ID
- Challenging to implement as protocols change as the call is established and placed over the telephony network.
- Data is modified as it flows through the network (e.g., different codecs)
- No common channel for transmitting data across networks

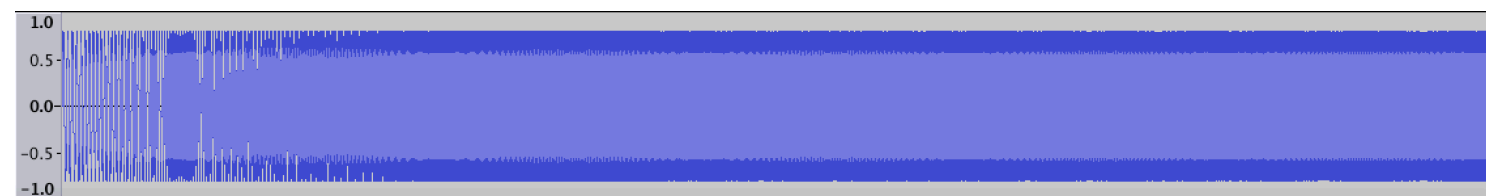
How to guarantee that real UBS / Credit Suisse is calling?

AuthLoop: Cryptographic Authentication over Voice Channel

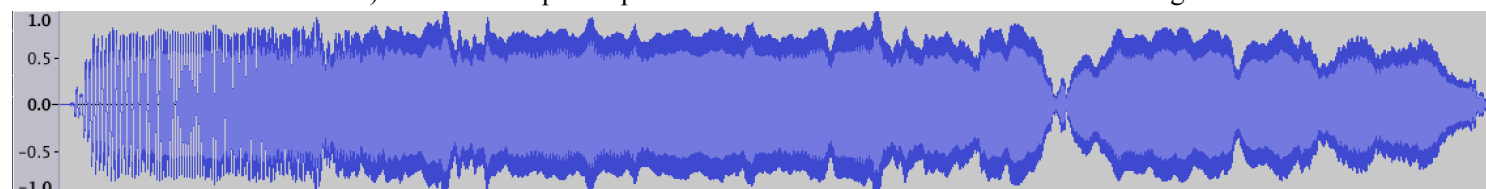
- Why not standard TLS handshake?

Site Name	Total Bits	Transmission Time at 500 bps
Facebook	41,544	83.088 s
Google	42,856	85.712 s
Bank of America	53,144	106.288 s
Yahoo	57,920	115.840 s
Average	48,688	97.232 s

- Solution: Stripped down TLS (no long HMACs, cipher agreement)
- The data exchange has to be implemented as **FSK** (other modulation schemes unreliable due to changes in codecs as the signal traverses the network)



a) 1-second chirp sweep from 300 - 3300 Hz before AMR-NB encoding



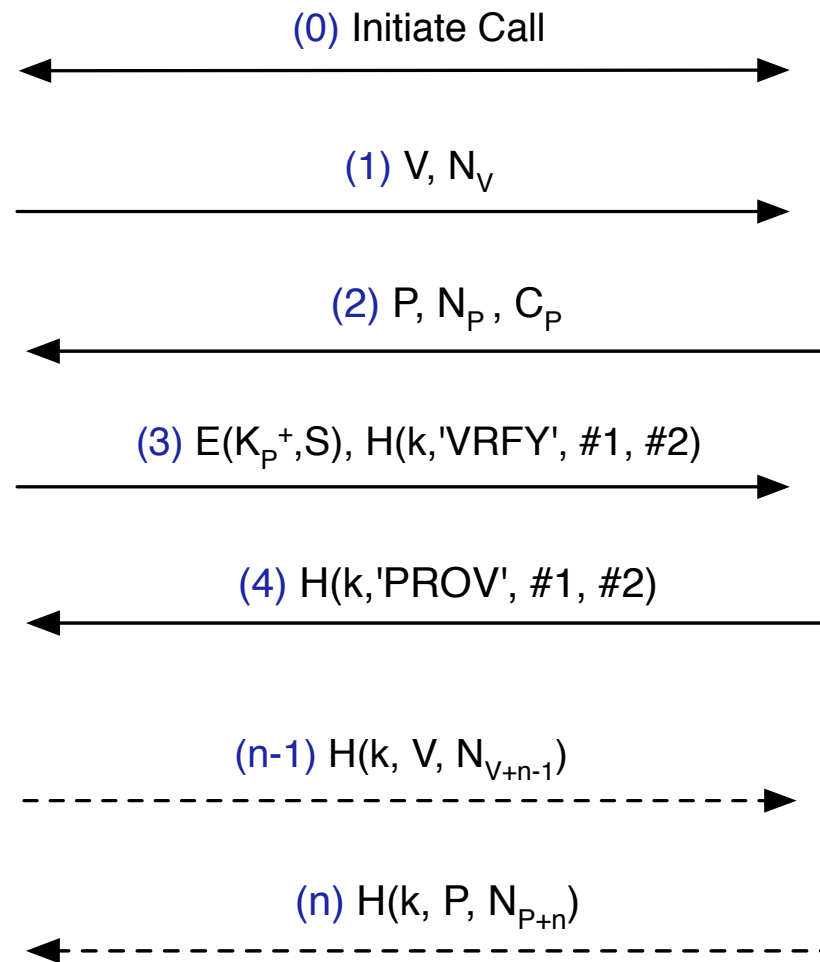
b) 1-second chirp sweep from 300 - 3300 Hz after AMR-NB encoding

AuthLoop Protocol

Mobile
(Verifier)



Call Center
(Prover)



Handshake complete
Prover is authenticated
Secret key is established

Send periodic
keepalive messages
to prove liveness

C: Certificate
E: Encryption
H: HMAC
D: Digital Signature
K^{+, -}: Public/Private Key
k: Symmetric Key
N: Nonce
P: Prover
S: Pre-Master Secret
V: Verifier

Codec	Cached Certificate	Certificate Exchanged
G.711	4.463 s	8.279 s
AMR-NB	5.608 s	10.374 s
Speex	4.427 s	8.279 s
Average	4.844 s	8.977 s

References

- **AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels**, *B. Reaves, L. Blue and P. Traynor*, In Proceedings of the USENIX Security Symposium (SECURITY), 2016.
- **SS7: Locate. track. manipulate.** Engel, Tobias, 31st Chaos Computer Congress.