GSM Security

Claude Castelluccia

INRIA

Technology behind GSM

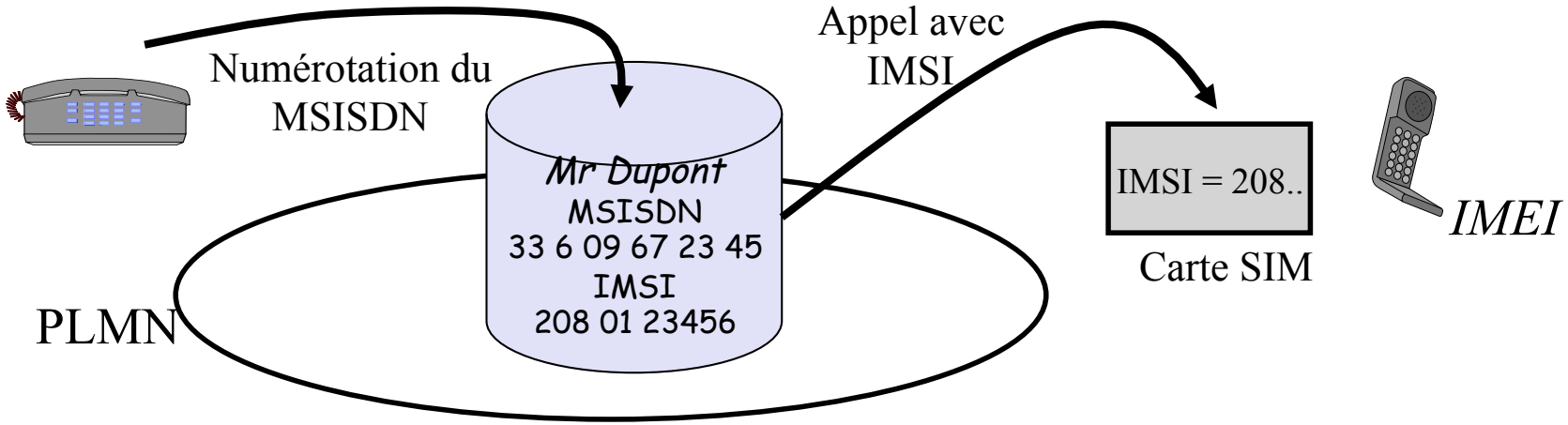
- 900 MHz (or 1800 MHz) band
- uplink frequency band 890-915 MHz
- downlink frequency band is 935-960 MHz
- 25 MHz subdivided into 124 carrier frequency channels, each 200 kHz apart
- Time division multiplexing (TDMA) allows 8 speech channels per radio frequency channel
- Channel data rate is 270.833 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 and terminal

- In GSM, the terminal and subscription is separated
- In older system, phone number was coded in the phone
  - Changing the terminal meant changing your phone number!
- With GSM, :
  - The terminal is dumb and does not contain any (or little configaration data)
  - The SIM(Subscriber Identity Module) card contains all the data…
- The SIM card:
  - Describes the subscription type…
  - And memorizes the environment of the user (password, list of numbers,..) and of the radio (number of the latest BS)
- GSM makes the difference between:
  - The subscriber number (IMSI) which identifies the subscriber
  - And the user current phone number (MSIDN)

GSM and Terminal (2)

- A database is used to link the IMSI and the MSISDN
- An operator can change the MSISDN of a subscriber without changing the SIM card…



- Each terminal is identified by an unique number, the IMEI (International Mobile Equipement Identity) which is used to invalided stolen devices.

GSM
Architecture

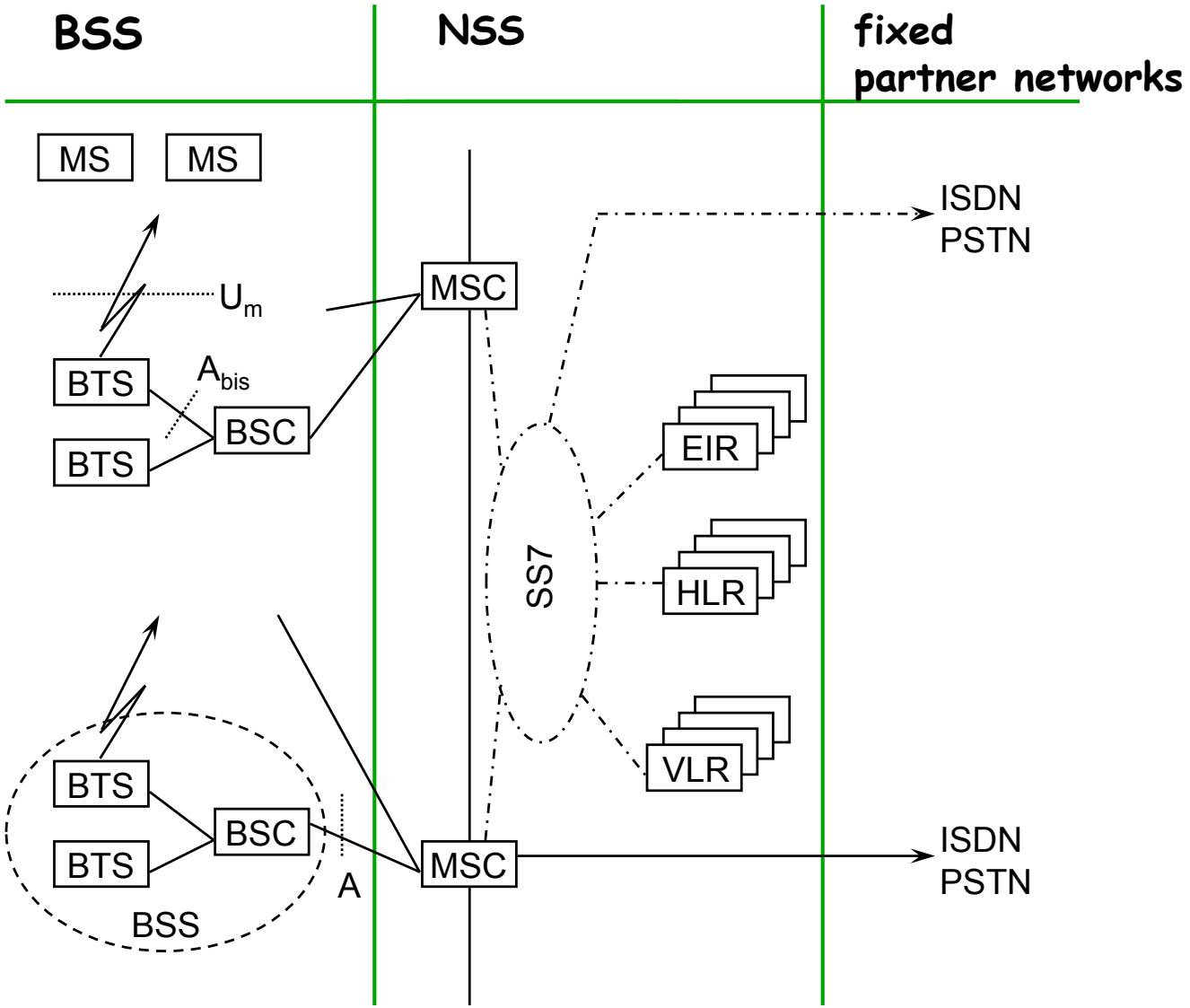
Architecture

- The GSM network's main goal is to establish a phone communication between:
  - A mobile subscriber
  - And another mobile subscriber or a terminal of the fixed network
- It is composed of switches
- And caracterized by a radio access network
- It is structured in PLMN (Public Land Mobile Network)
  - Network installed and managed by a single operator..
  - There are 3 PLMN is France: Orange, SFR, Bouygues.
  - A PLMN can be used by subscribers of another PLMN, if a roaming agreement exists…

Architecture (2)

- A GSM network is composed of 3 main components:
  - The BSS (Base Station Sub-system), or access network, which manages the radio transmissions…
  - The NSS (Network sub-system), or fixed network, which contains all the functions that are needed to establish call and to managed mobility…
  - The OSS (Operation Sub-system) which is used to manage the network (management network).

GSM: architecture

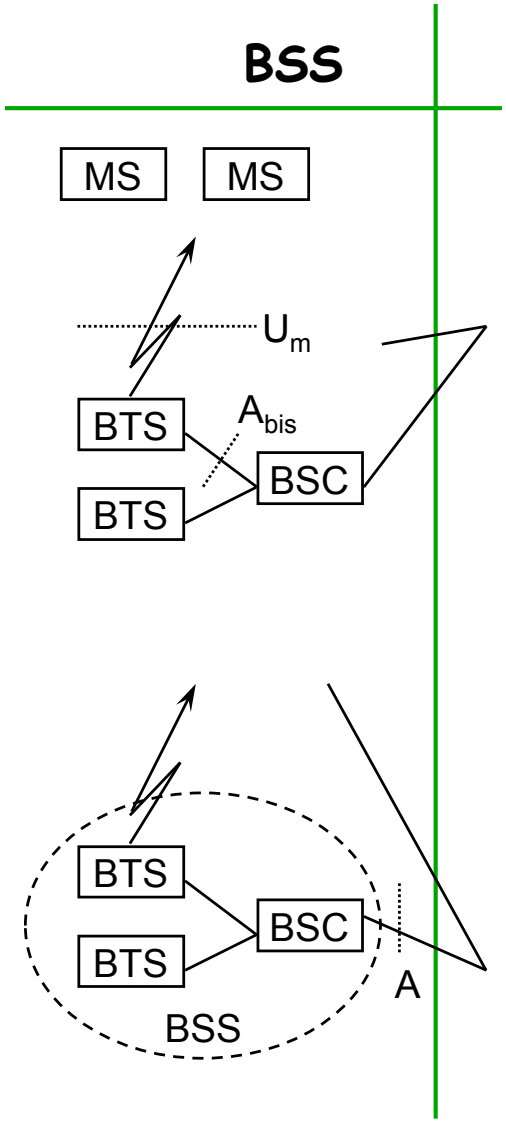


Nomadicity vs Mobility

- Nomadicity
  - Nomadicity is defined as the possibility to use a device anywhere..
  - The subscriber can then make a call and will be billed on its own account…he can also receive a phone call as if he were on his network…
  - The network then needs to locate the subscriber and forwards the communication calls to his current position…
  - However, it is impossible for the user to move and/or unplug his phone and plug it somewhere-else **while he is communicating**…
  - Nomadicity is managed by the NSS

- Mobility (Handover)
  - Allows a user to move (i.e. change access points) while communicating…this implies what is called handover…
  - Managed by the BSS and NSS…

Architecture of the BSS



The BSS is composed of:

- Several BTS (Base Transceiver Stations), which are "simple" radio transmitter-receivers…similar to hubs

- Several BSC (Base Station Controllers) which manage a set of BTS…

The BTS

- A BTS is a set of transmitter-receivers (TRX).
- It is in charged of:
  - The radio transmission, i.e. modulation, demodulation, equalization, error code correction…
  - Managing the physical layer
    - » TDMA multiplexing, frequency hopping, coding/ encrypting…
    - » Performing radio measurements that are used by the BSC to allocate channels…
  - The maximum capacity of a BTS is 16 carriers, i.e. it can support at most 112 (7*16) simultaneous communications.

The BSC

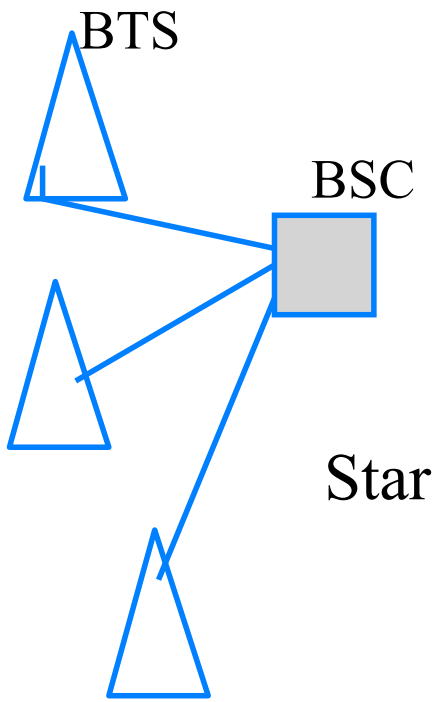
- The BSC is the "brain" of the BSS
- It manages the radio
  - Allocates channels
  - Uses the measures, performed by BTS, to control the transmission power of the mobile terminals and the BTS, decides/controls hadovers.
- It is also a switch to the MSCs
- A BSC is connected to a BTS and a MSC via one or several MIC links (64 bbps digital links).
- The BTS-BSC link is similar to an ISDN link and used the LAPD protocol
- The BSC-MSC link used the CCITT 7 protocol.

The BSC (2)

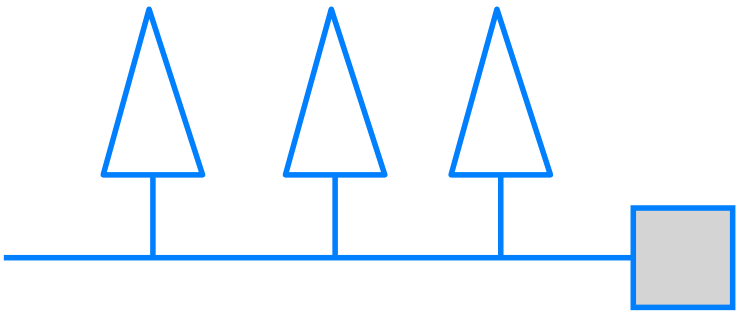
- Different types of BSC can be used:
  - BSC with "low" capacity
    - » cheaper
    - » Minimizes distance BTS-BSC
    - » Requires more BSC for a given area
    - » Well adapted to urban (dense) area
  - BSC with « high » capacity
    - » More expensive
    - » …but more adapted to rural areas
  - to optimize frequence utilization…

BTS-BSC Configurations

- There are different possible BTS-BSC configurations
- BTS are usually connected to a BSC according to a chain or star topology…

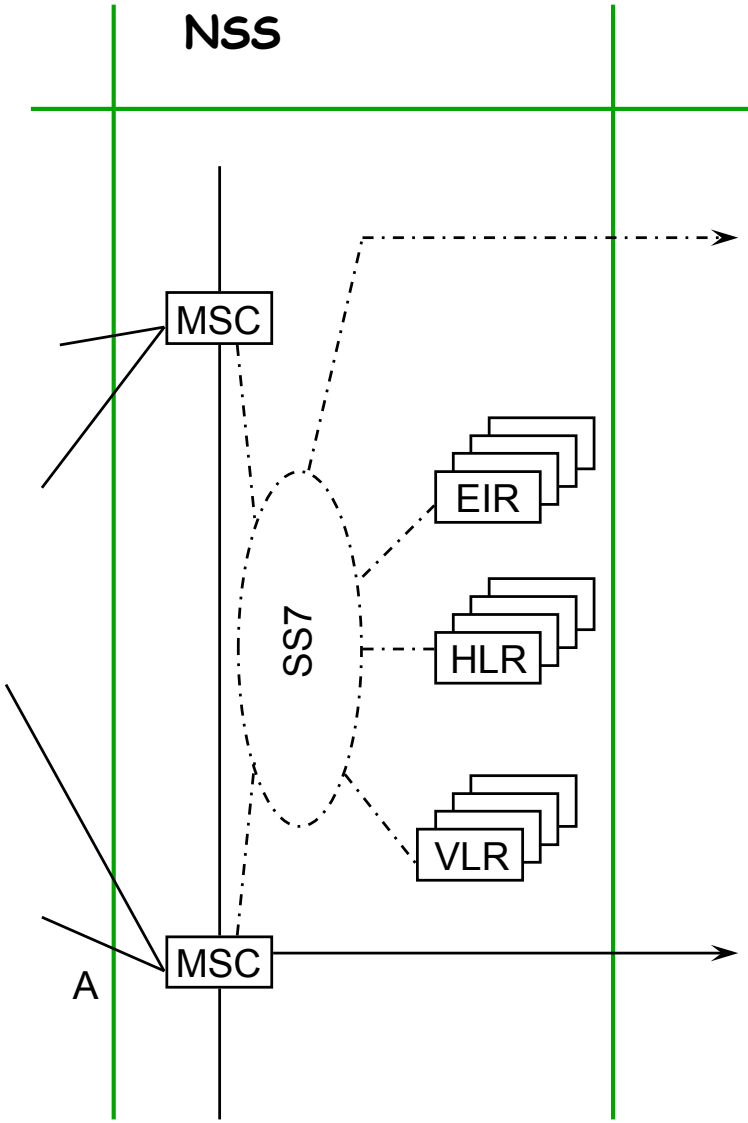


Star



Chain

NSS Architecture



The NSS is composed of databases and switches:

- the MSC (Mobile-services Switching Center) are switches which are associated to the VLR (Visitor Location Register),
- The HLR (Home Location Register) is a location database that contains the caracteristics of the subscribers…
- The EIR (Equipment Identity Register) is a database that contains the identities of the mobile terminals (IMEI).

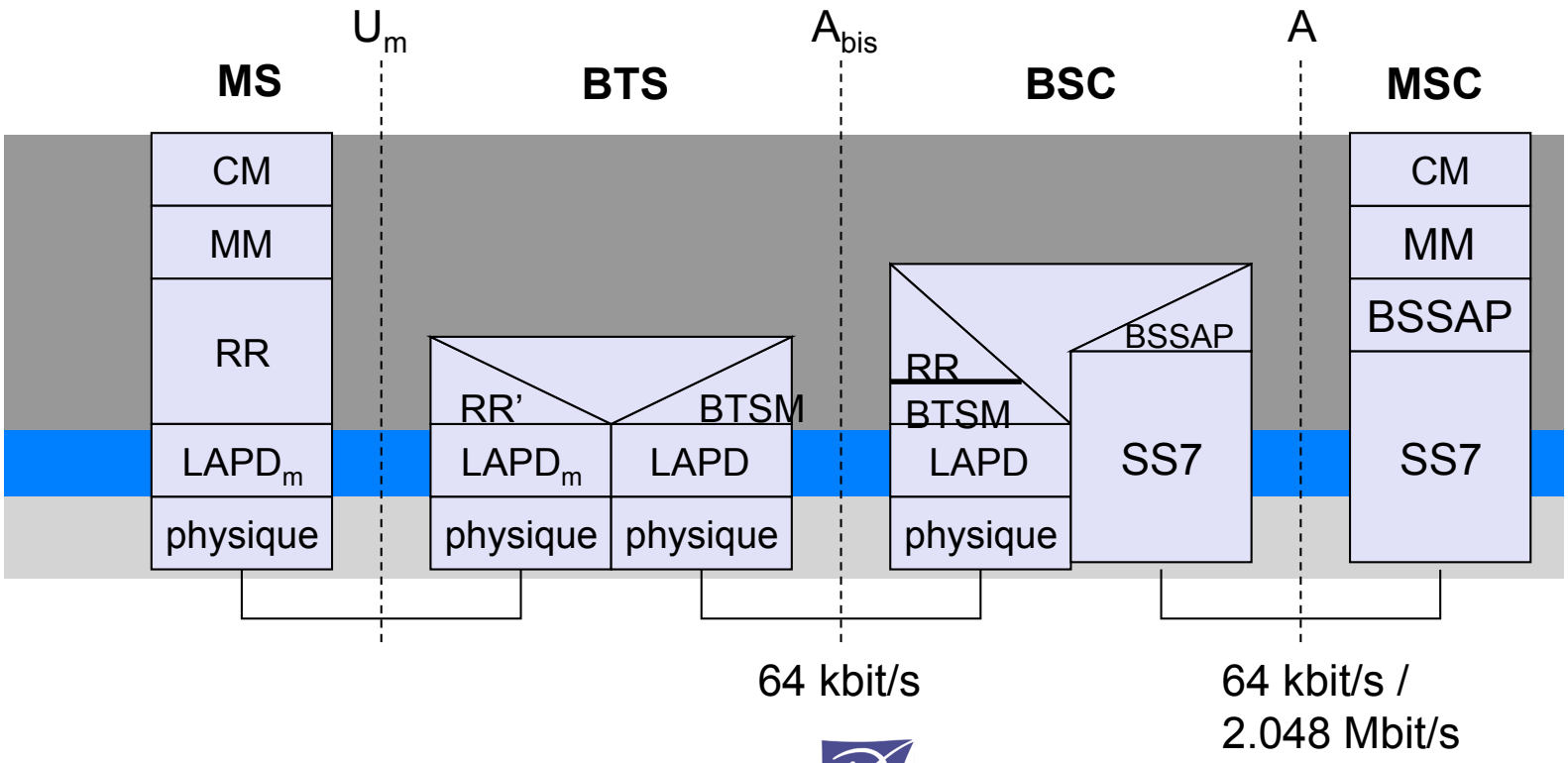
The HLR

- The HLR (Home Location Register) is a database that manages the subscribers of a PLMN
- It stores:
  - The data of each subscribers
    - » Its IMSI, its number (MSISDN), its profil (international calls, type of subscription).
    - » This data is entered by the operator using its administration system
  - The current VLR of each subscriber
    - » This information is updated by the mobile terminal
- The HLR can be:
  - Centralized: it's a specific machine…
  - Decentralized: it is integrated into the MSCs abd the data of a given subscriber are stored on the MSC that he uses the most frequently…
  - In all cases, each subscriber is associated to a unique HLR identifiable from its phone number (MSISDN).

The MSC and VLR

- The MSC (Mobile-service Switching Center):
  - Manages communication establishments between a mobile terminal and another MSC
  - Transmission of short messages
  - Manages handovers
  - Communicates with the VLR to manage user mobility: verification of visiting users that establish communications, transfer of localization information…
- The VLR (Visitor Location Register)
  - Database that stores the subscription data of users that are roaming in the area it is in charge of …
  - Its data are similar to the ones of the HLR but only concern users that are roaming in its area.
  - The VLR provide a more accurate localization of users
    - » HLR knows the current VLR
    - » The VLR knows the current BSC…

BSS layered Architecture



NSS Layered architecture

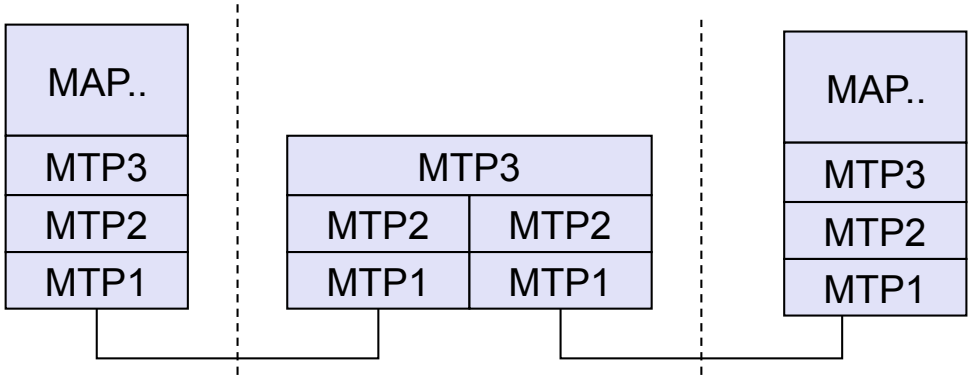
- Signalisation in the NSS is based on SS7
- SS7 (MTP) is implemented on the MSC, VLR and HLR.
- Another protocol, MAP, (Mobile Application Part) is added to the MSC, VLR et HLR to manage mobility.

CCITT no7 (SS7)

- The current digital phone networks contain 2 sub-networks (plans)
  - The sub-network that transports the phone communication. It is connection-oriented.
  - The signalisation sub-network that transports the signalisation. It is packet oriented (commutation).
  - …used by SMS…
- The signalisation sub-system is called CITT7 or SS7 (Signalling System 7)
  - It allows NSS components (i.e. switches and HLR/VLR) to communicate without establishing a communication.

CCITT no7 (SS7)

- When a user A wants to establish a communication with B
  - A request is sent to B using the signalisation-sub-network
  - If B is available, a connection is then established
  - If not….the transport sub-network is not solicitated
  - In analog systems, the connection was established switch-to-switch until destination
    - » If B was busy, the communication was then cancelled (waste of ressource!)
- SSS7 architecture

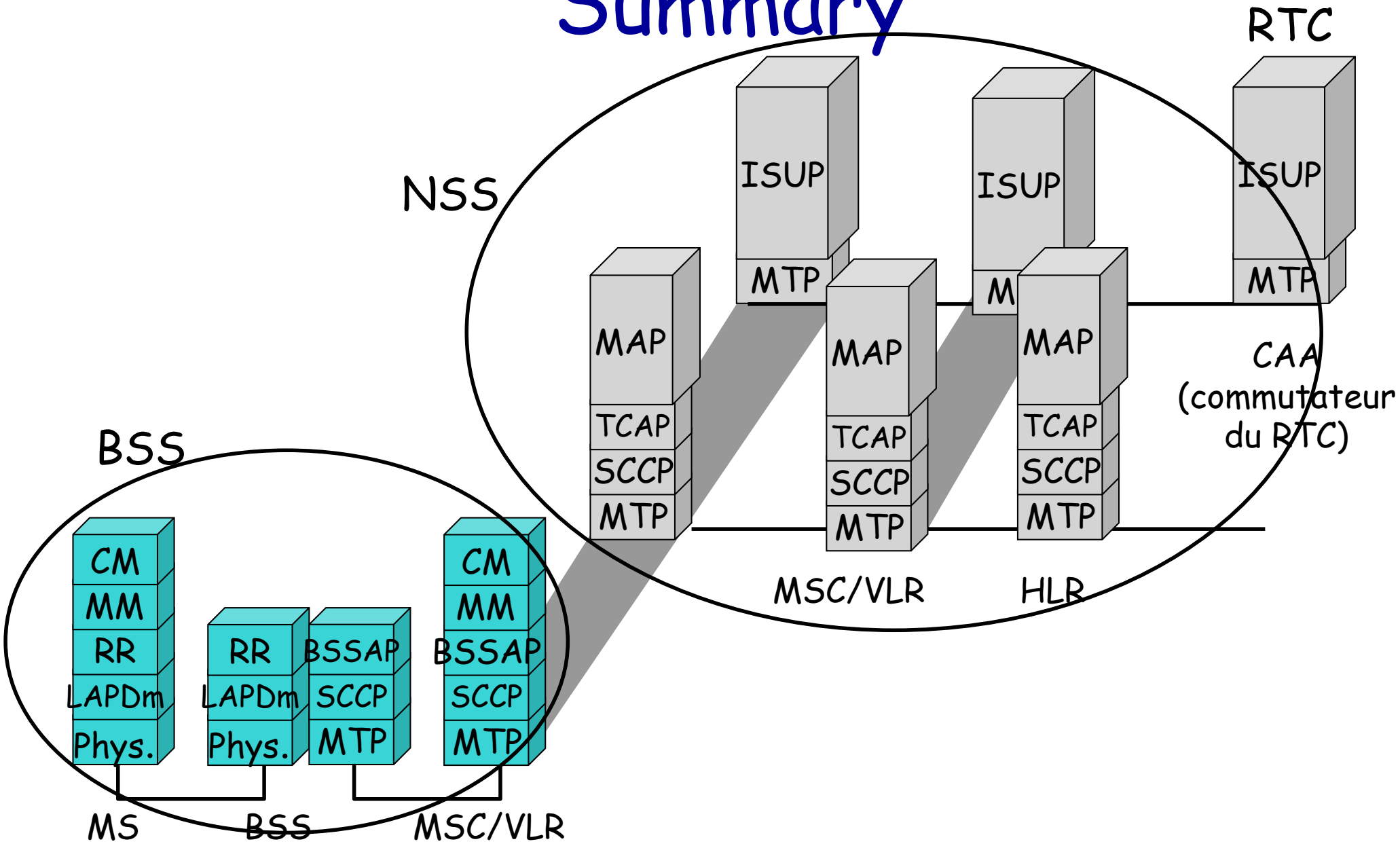


CCITT no7 (2)

- The MTP (Message Transport Part) is a reliable transport protocol (a bit like TCP)

- The MAP (Mobile Application Part) is the protocol that manages all the exchanges between the NSS equipments i.e. MSC, VLR, HLR et EIR:
  - Mobile registration
  - Localisation of a destination mobile
  - Handover of a mobile terminal between 2 MSCs
  - Transmission of short messages
  - Identification of a mobile terminal and allocation of a TMSI
  - IMEI verification

Summary

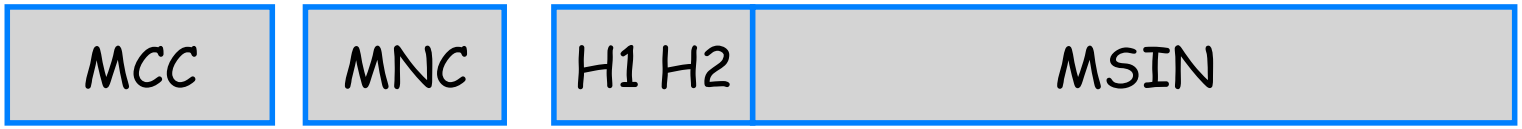

RTC
NSS
ISUP
ISUP
ISUP
MTP
M
MTP
MAP
MAP
MAP
TCAP
SCCP
MTP
TCAP
SCCP
MTP
TCAP
SCCP
MTP
CAA
(commutateur
du RTC)
BSS
MSC/VLR
HLR
CM
MM
RR
LAPDm
Phys.
RR
LAPDm
Phys.
BSSAP
SCCP
MTP
CM
MM
BSSAP
SCCP
MTP
MS
BSS
MSC/VLR

GSM
Addressing

GSM Addressing

GSM uses 4 addresse types:

- IMSI (International Mobile Subscriber Identity)
  - Is seldomly transmitted over the radio interface for security reasons .
  - It used by the network to locate/identify a user when the TMSI is not available



  - L'IMSI is composed of (at most) 60 bits and is composed of:
    - » Mobile Country Code (MCC): country area number: 208 for france
    - » Mobile Network Code (MNC): PLMN number (10 for SFR)
    - » Mobile Subscriber Identification Number (MSIN): subscriber id in its PLMN. (H1 H2) defines the user's HLR in its PLMN.

GSM Addressing (2)

- TMSI (Temporary Mobile Station identity)
  - Temporary identity (number) assigned to a mobile terminal that is visiting a VLR
  - It is local, i.e. only valid within the VLR area. It is only known by the local MS-MSC/VLR…the HLR does not know it!
  - A new TMSI is allocated, each time a terminal changes VLR…
  - The structure is free and can be defined by operator. It is 4 bytes long.

GSM Addressing (3)

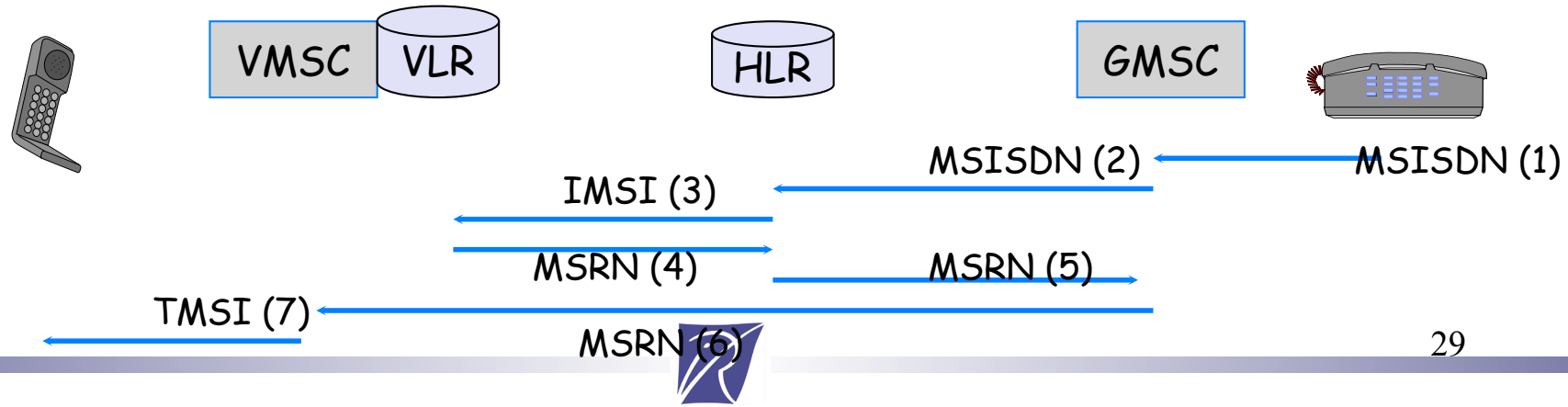
- MSISDN (Mobile Station ISDN Number)
  - Phone number of the user
  - Only the HLR knows the MSISDN-IMSI mapping.
  - It follows the internation addressing standard E.164, i.e. is composed of:
    - » Country Code (CC): indicatif du pays (33 pour la France).
    - » National Mobile Number: numéro national du mobile composé du National Destination Code (NDC) déterminant le PLMN et le Subscriber Number (SN) définissant l'abonné dans son PLMN. Les premiers chiffres du SN permet d'identifier le HLR de l'abonné.
  - In France, a MSISDN looks like 33 6 AB PR MCDU where:
    - » 6 indiques that this is a GSM phone number
    - » AB identifies the Mobile GSM operator (07, 08 and 04 for FT...)
    - » PR is the HLR logical number
    - » MCDU is the subscribed id in the HLR
    - » ex: 33 6 07 10 3445

GSM Addressing (4)

- MSRN (Mobile Station Roaming Number)
  - Is the address of the current MSC of the mobile terminal
  - It used to route incoming communications
  - Is allocated to the mobile terminal by the VLR when there is an incoming call…
  - Has the same structure of a MSISDN address (i.e. E.164)

GSM Addressing (5)

- Example: Incoming call…
  - (1) The MSISDN is dialed by the caller. The connection is routed by the fixed network to the closed MSC that acts as a GMSC (Gateway MSC).
  - (2) The GMSC queries the HLR to identify the MSC that must be used to route the connection.
  - (3) The HLR translates the MSISDN in IMSI and queries the mobile terminal's VLR using its IMSI.
  - (4) The VLR allocates a MSRN to the MT and transmits this number to the HLR.
  - (5) The HLR then transmits this MSRN to the the GMSC.
  - (6) The GMSC establishes a connection with the current MSC of the TS, as if the MSRN was the terminal's adress.
  - (7) The MSC then calls the MT by using its temporary IMSI…



GSM
Security

GSM Security Concerns

- 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

GSM Security Design Requirements

- The security mechanism
  - MUST NOT
    - » Add significant overhead on call set up
    - » Increase bandwidth of the channel
    - » Increase error rate
    - » Add expensive complexity to the system
  - MUST
    - » Cost effective scheme
  - Define security procedures
    - » Generation and distribution of keys
    - » Exchange information between operators
    - » Confidentiality of algorithms

GSM Security Features

- ***Key management is independent of equipment***
  - Subscribers can change handsets without compromising security
- ***Subscriber identity protection***
  - not easy to identify the user of the system intercepting a user data
- ***Detection of compromised equipment***
  - Detection mechanism whether a mobile device was compromised or not
- ***Subscriber authentication***
  - The operator knows for billing purposes who is using the system
- ***Signaling and user data protection***
  - Signaling and data channels are protected over the radio path

IMSI protection: the TMSI

- The IMSI is seldomly sent over the radio interface…to prevent an user from being traced…
- Instead a TMSI is used instead the VLR…
- The VLR maintains The IMSI and TMSI mapping
- The IMSI is used when the MT is activated and changes VLR.
- A new TMSI is allocated at each VLR or more frequently is the MT wants it…
- The TMSI is encrypted when it is first sent to the MT …

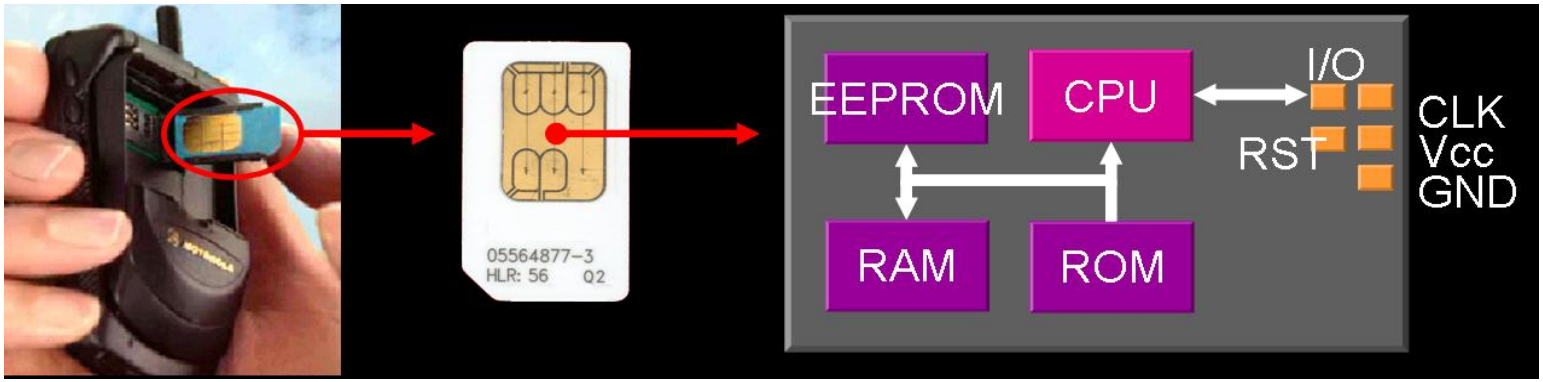
Authentication and Encryption: Basic blocks

- To achieve authentication and encryption, GSM uses:
  - Random numbers RAND
  - An authentication key Ki and an encryption key Kc
  - An algorithm A3 that generates a random SRES from RAND and Ki
  - An algorithm A8 to generate the key Kc from RAND and Ki
  - An algorithm A5 to encrypt and decrypt data with Kc

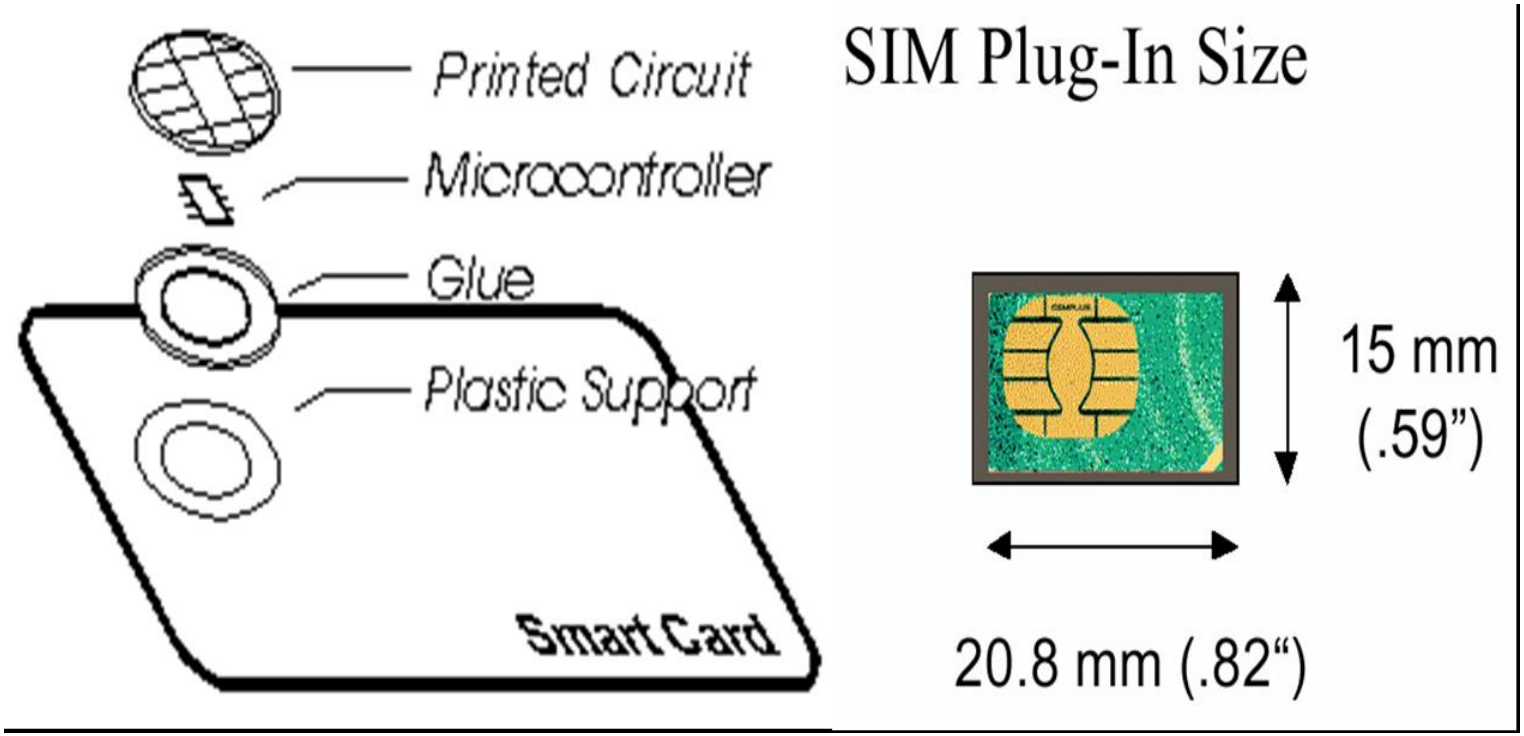
- The algorithms A3, A5 and A8 are the same for all the users of a network
  - But can be different from one network to another!
- The operator allocates to each user a key Ki (stored in SIM card)

A SIM card

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



Smart Card Anatomy



Microprocessor 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

The PIN and PUK…

- The SIM card is activated by the user with the PIN number
  - PIN (Personal Identity Number) is a 4-8 digit access code which can be used to secure your telephone from use.
- The PUK (Personal Unblocking Key) is used to unlock the PIN if your SIM card is blocked
  - Very useful for forensics analysis…

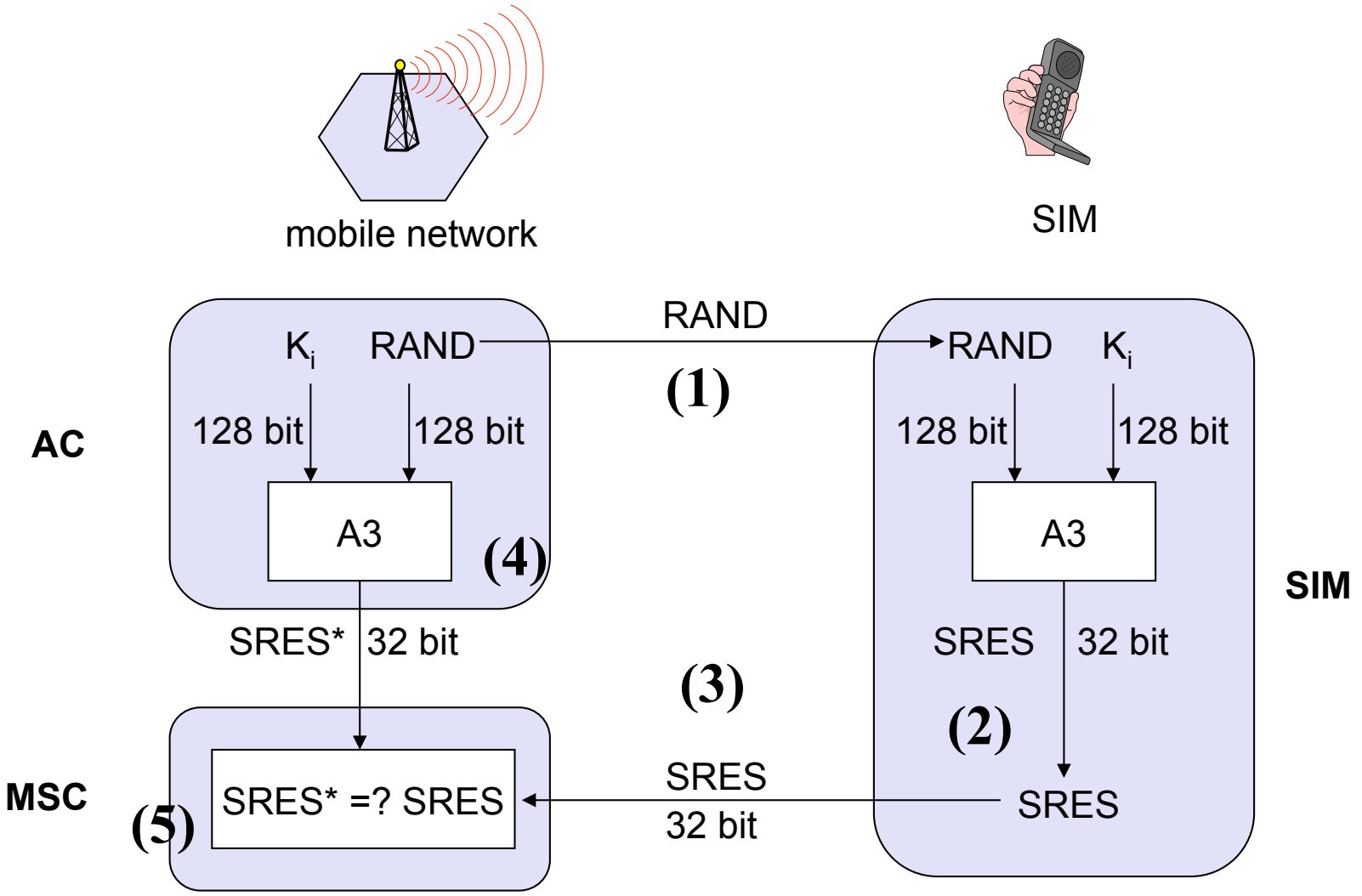
The Key is in the SIM card

- K_i – 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

User Authentication

- Authentication is used to verifier the identity of the user
  - Avoid impersonation
  - Control access to the network
- It can be performed by the network, each time the MT moves, establishes a communication or requests a service. If the authentication fails, the MT can't access the network.
- Steps:
  - The network sends a RAND
  - The SIM card computes the signature of RAND using A3 and Ki
    - » The result SRES is sent to the network
  - The networks compares it with the value it has computed…
- Note: The network is never authenticated by the mobile terminal…

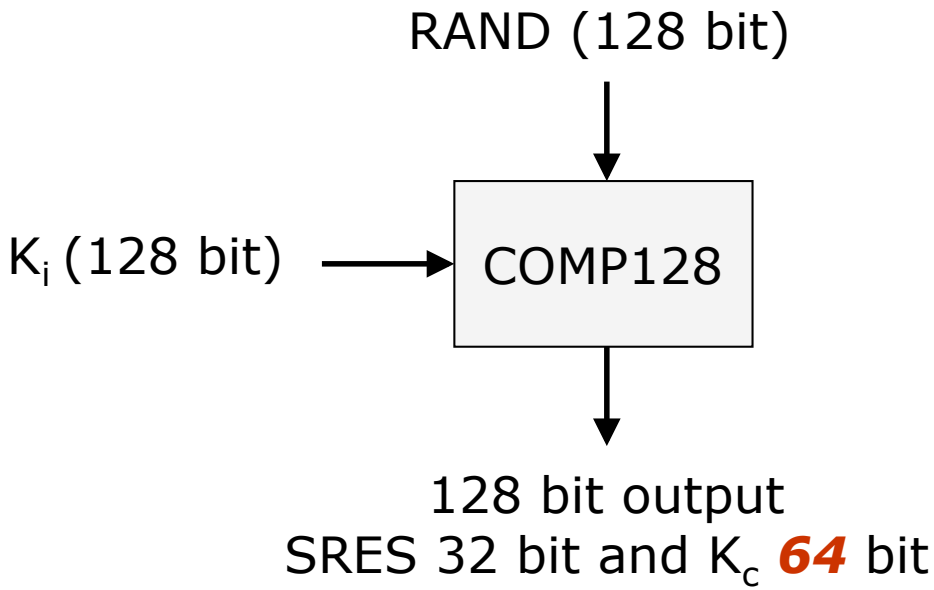
Authentication (2)



K_i: individual subscriber authentication key SRES: signed response

Implementation of A3 and A8

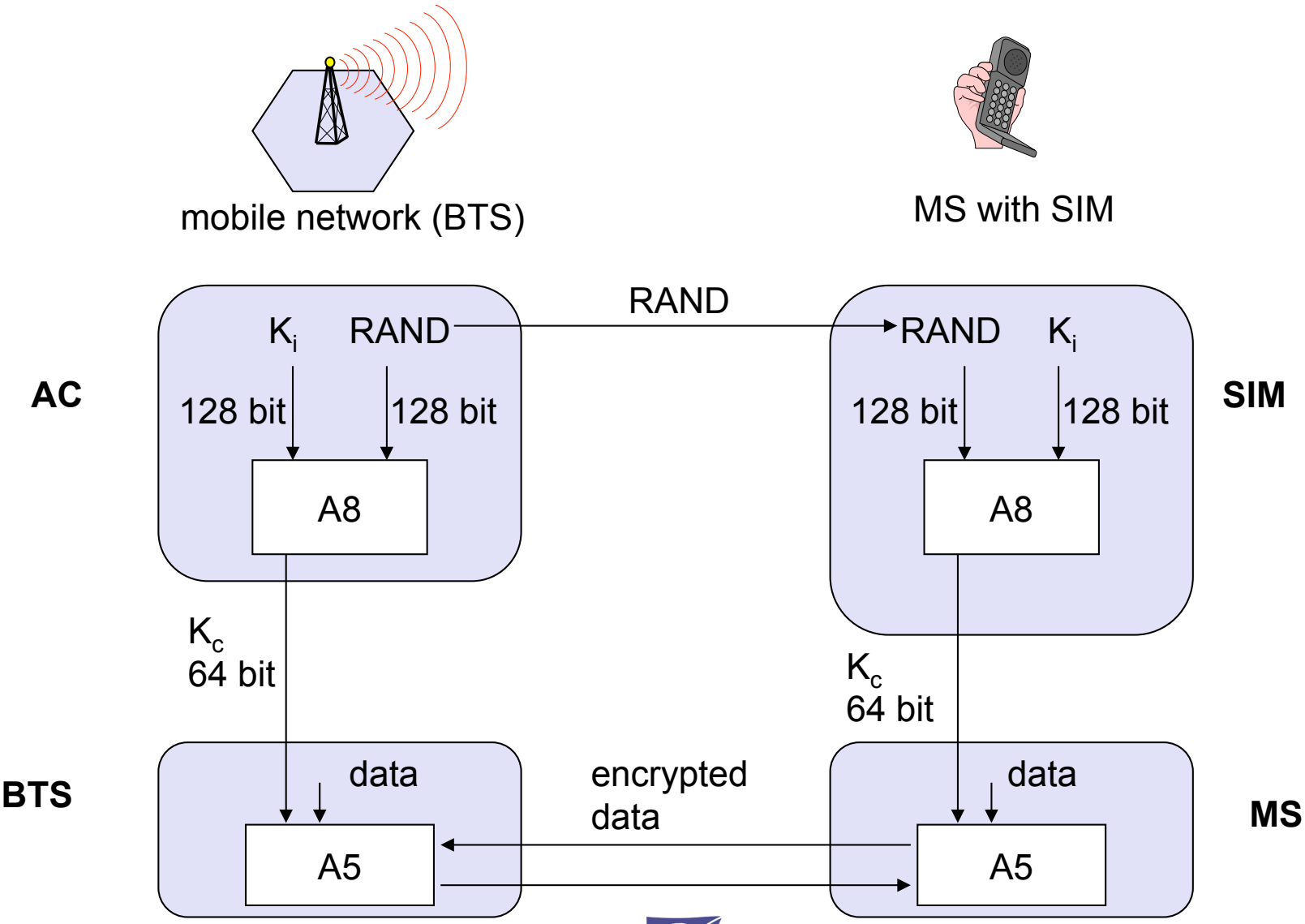
- COMP128 is used for both A3 and A8 in most GSM networks.
  - COMP128 is a keyed hash function



Confidentiality

- Encrypt to protect confidentiality of communications
- This is not an end-to-end service…only the MS-BTS part is encrypted.
- GSM uses an symmetric encryption algorithm A5
- Generation encryption key Kc:
  - Networks sends RAND to the MT
  - The MT and the network compute from A8, RAND and Ki, the secret key Kc
- Encryption
  - Encryption is performed by the MT and the BTS, using A5
  - Encryption can be activated once the MT has been authenticated and the key Kc generated…

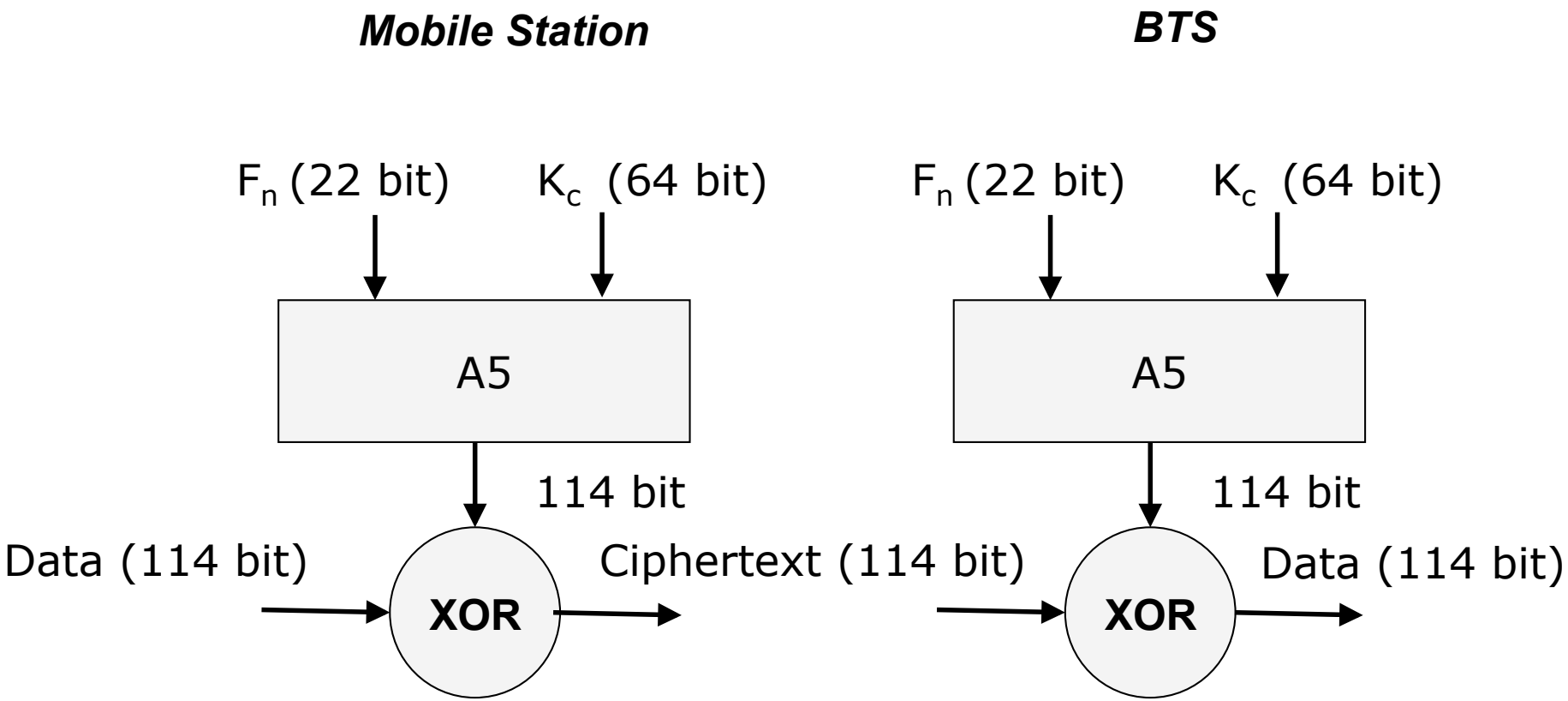
Encryption.


mobile network (BTS)
MS with SIM
AC
SIM
BTS
MS
K_i
RAND
RAND
K_i
128 bit
128 bit
128 bit
128 bit
A8
A8
K_c
64 bit
K_c
64 bit
data
data
encrypted
data
A5
A5

A5 – Encryption Algorithm

- 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

A5 Implementation

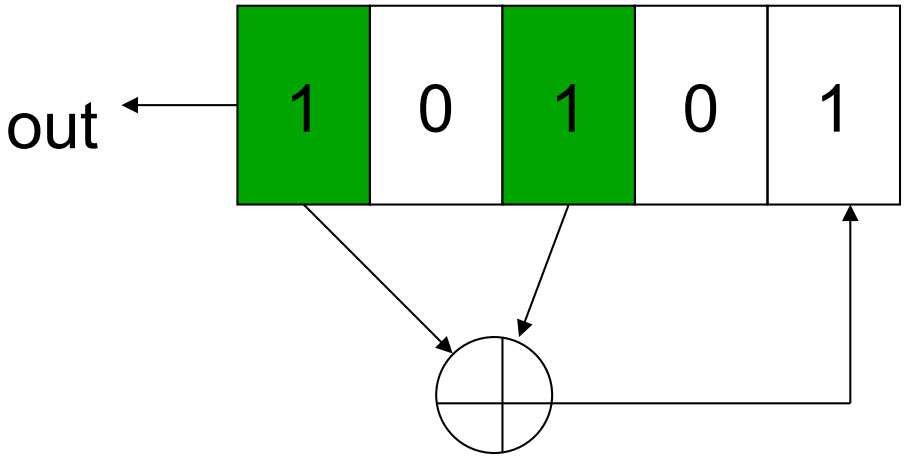


A5- Linear Feedback Shift Registers

- A5 uses Linear Feedback Shift Registers…
- Properties
  - LFSRs are well-suited to hardware implementation;
  - can produce sequences of large period
  - can produce sequences with good statistical properties
  - because of the structure, can be analyzed using algebra
- Definition
  - LFSR of length L consists of L stages numbered 0, 1, …, L– 1, each capable of storing one bit and having one input and one output, and clock which controls the movement of data
    - » content of stage 0 is output and forms part of the output sequence
    - » the content of stage i is moved to stage i – 1 for each i, $1 \leq i \leq L - 1$
    - » new content of stage L – 1 is feedback bit s_j calculated by adding together modulo 2 previous contents of fixed subset of stages

LFSR (cnt.)

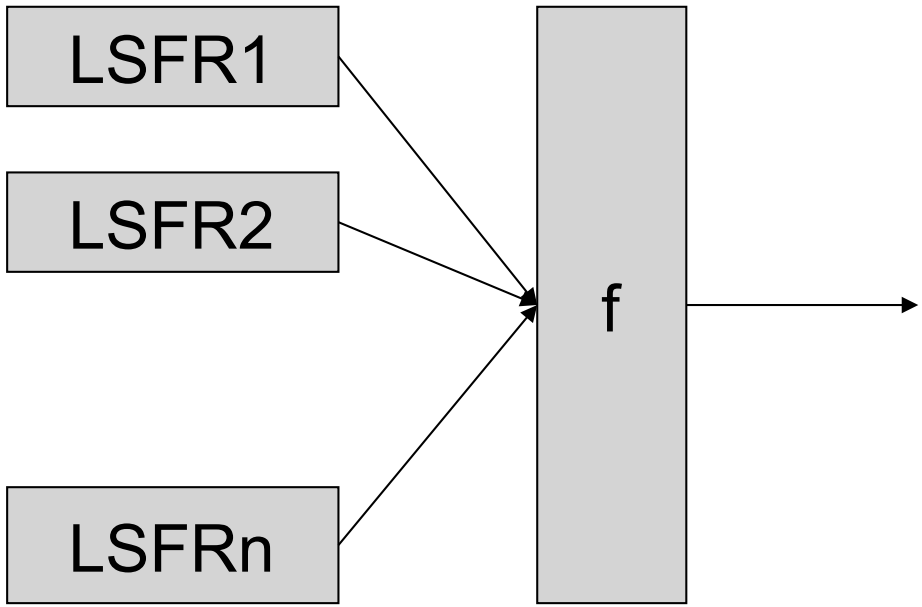
- Output sequence
  - $s_j = (c_1 s_{j-1} + c_2 s_{j-1} + \ldots + c_L s_{j-L}) \bmod 2$
- Example



output	1	0	1	0	1
1	0	1	0	1	0
0	1	0	1	0	0
1	0	1	0	0	0
0	1	0	0	0	0
1	0	0	0	0	1
0	0	0	0	1	0

Stream ciphers based on LFSR

- Why
  - To augment Linear Complexity, use non-linear combination of stream ciphers
- Example



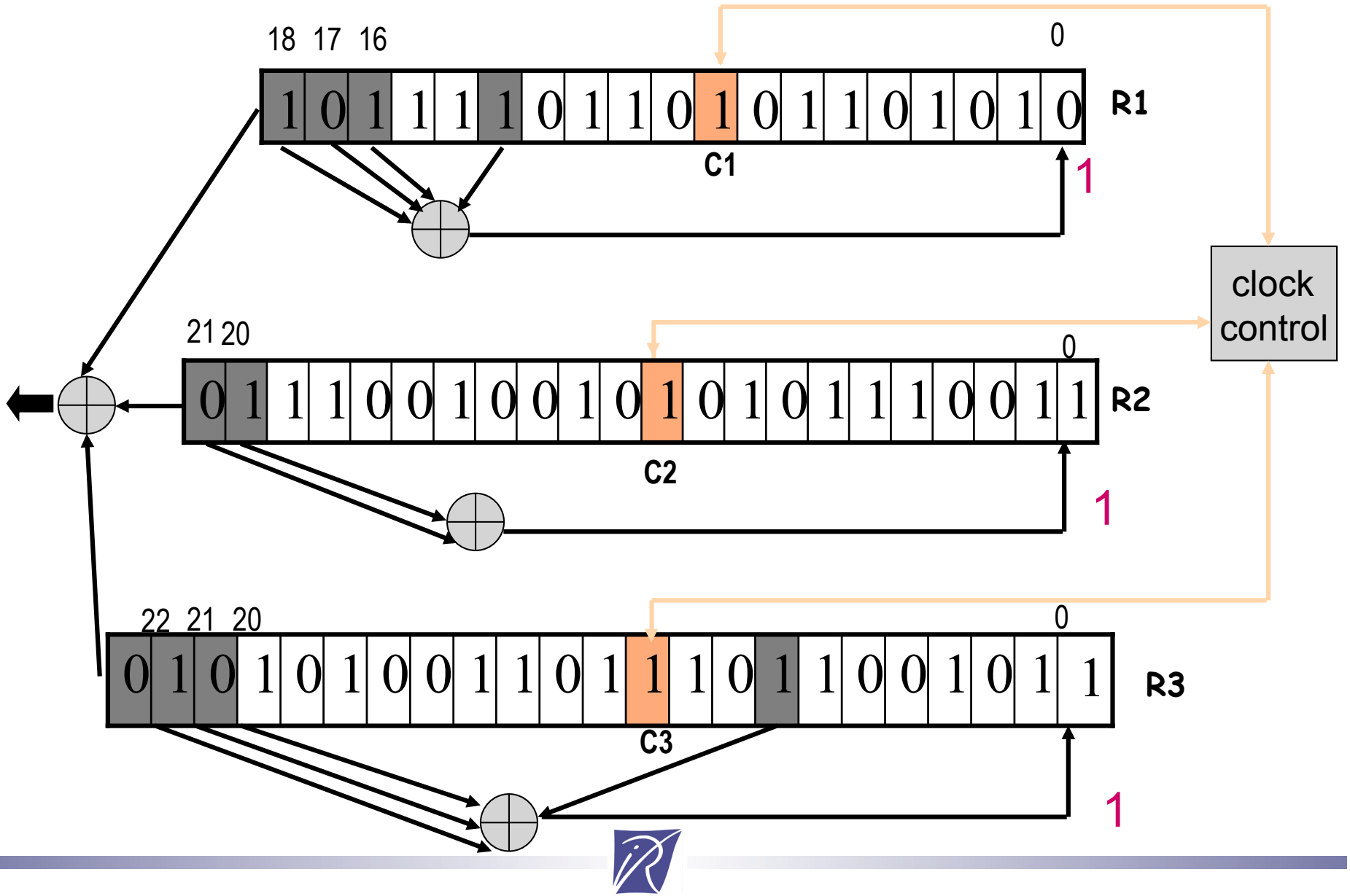
A5...

- A GSM conversation is sent as a sequence of frames
  - One (TDMA) frame is sent every 4.6 millisecond.
  - Each frames contains 228 bits
  - Each frame uses a new session key K
    - » This key is mixed up with a publicly known frame counter Fn (similar as IV) to initialize the state of the shift registers in A5/1.
  - It then produces a 228 bit keystream...
- A5/1 is a stream cipher
- Consists of 3 LFSRs of 19,22,23 bits length.
- The 3 registers are clocked in a stop/go fashion using the majority rule.
  - Clock-controlled generator is used to introduce nonlinearity into LFSR-based keystream...

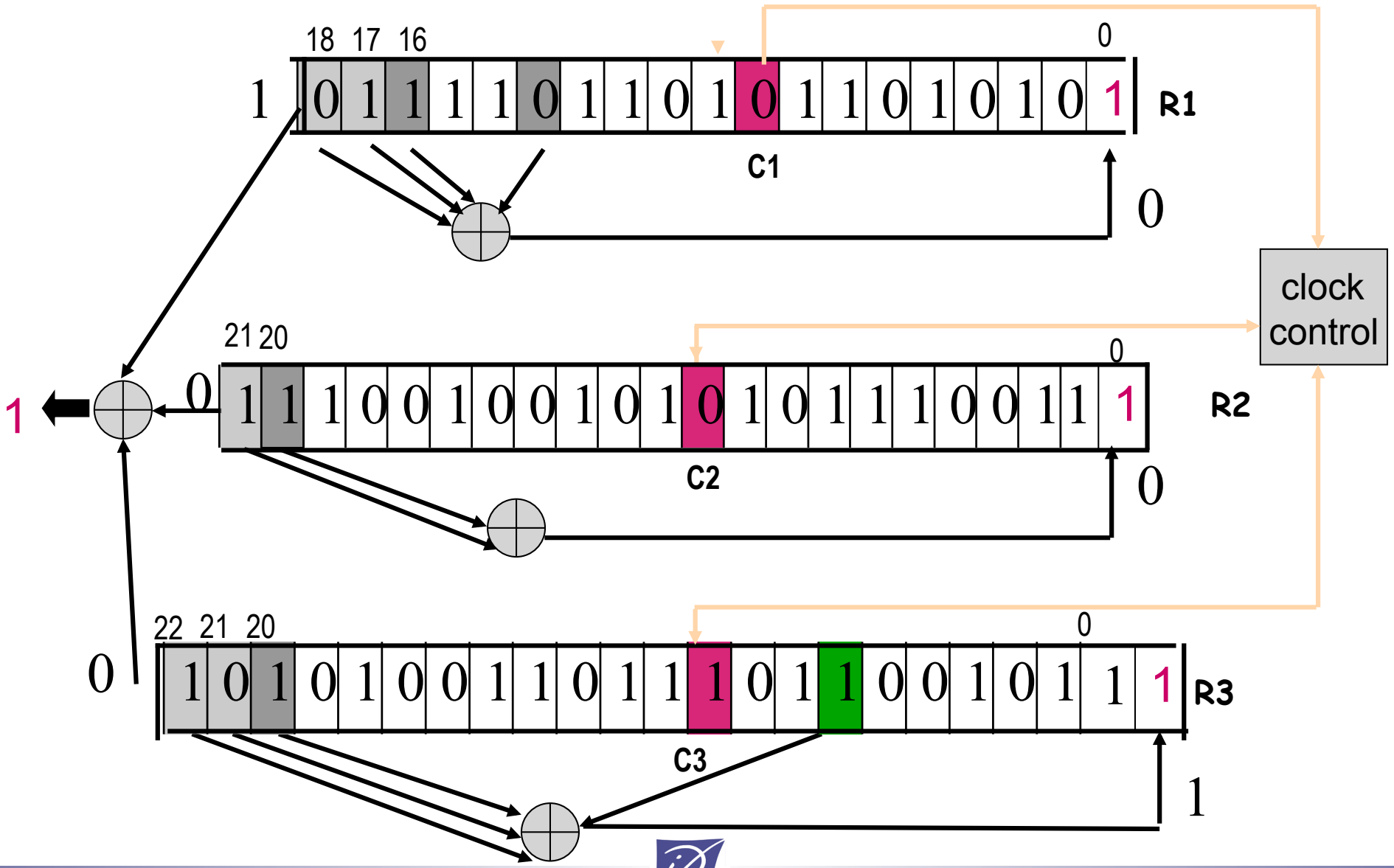
A5/1 : Operations

- All 3 registers are zeroed
- And then initialized with key Kc
  - 64 cycles (without the stop/go clock) :
    - » Each bit of K (lsb to msb) is XOR'ed in parallel into the lsb's of the registers
  - 22 cycles (without the stop/go clock) :
    - » Each bit of F_n (lsb to msb) is XOR'ed in parallel into the lsb's of the registers
- 100 cycles with the stop/go clock control, discarding the output
- 228 cycles with the stop/go clock control which produce the output bit sequence.
- Basic idea behind A5 are good
  - It passes all known statistical test
  - But its registers are too short!

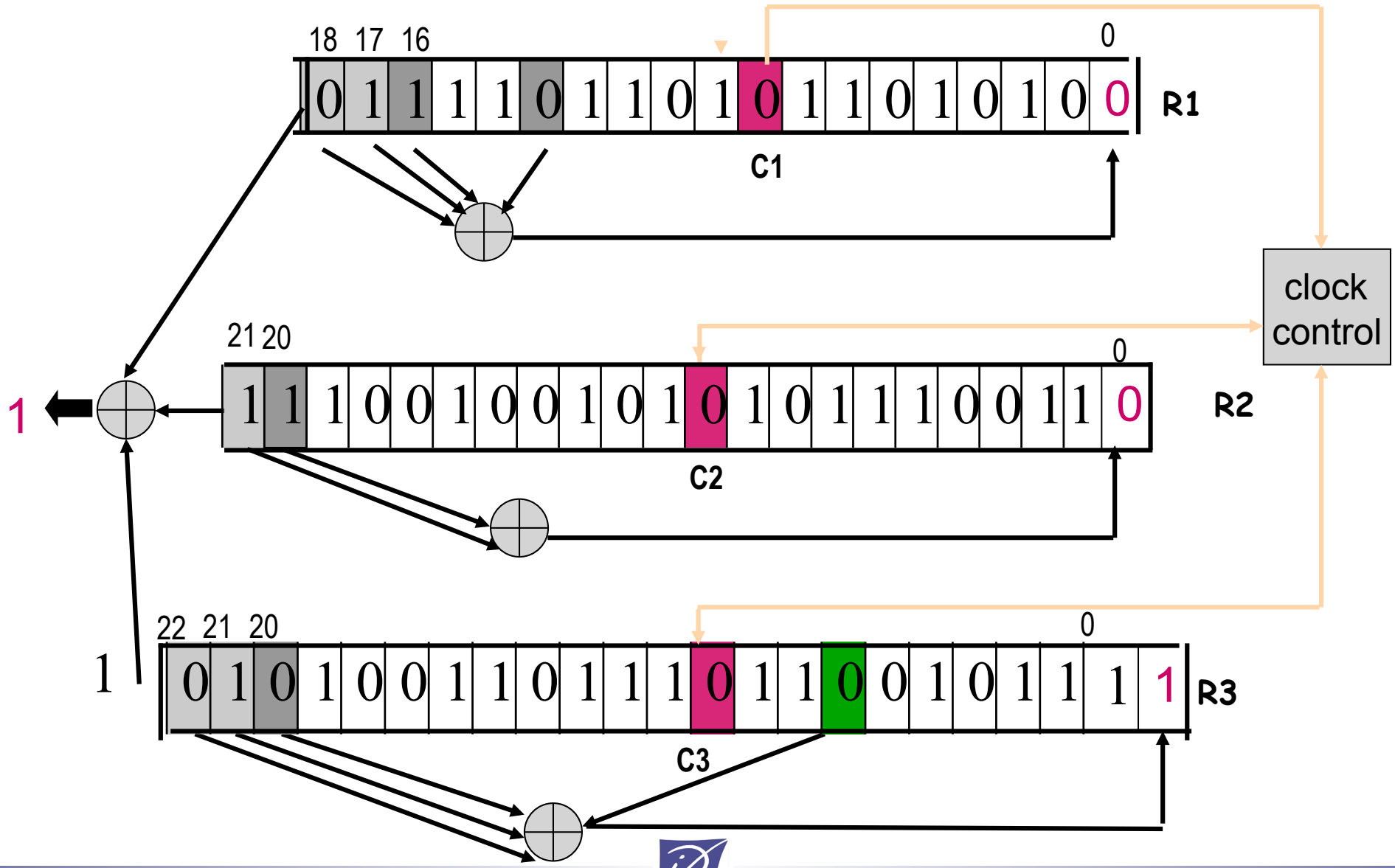
A5/1


18 17 16
0
1 0 1 1 1 1 0 1 1 0 1 0 1 1 0 1 0 1 0
R1
C1
1
clock control
21 20
0
0 1 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1
R2
C2
1
22 21 20
0
0 1 0 1 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 1 0 1 1
R3
C3
1

A5/1 (2)


18 17 16
0
1 0 1 1 1 1 0 1 1 0 1 0 1 1 0 1 0 1 0 1
R1
C1
0
clock control
21 20
0
1 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 1
R2
C2
0
1
0
22 21 20
0
1 0 1 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 1 0 1 1 1
R3
C3
1
0

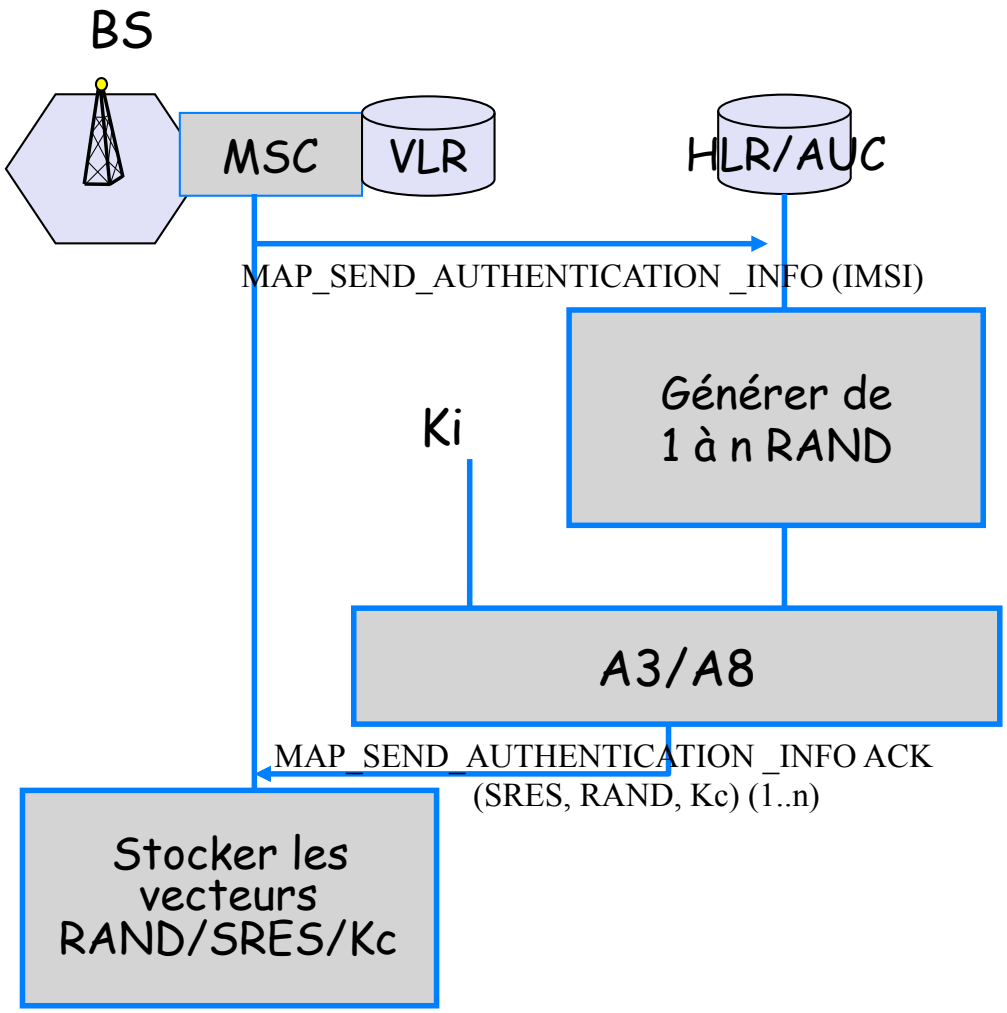
A5/1 (3)


18 17 16
0
0 1 1 1 1 0 1 1 0 1 0 1 1 0 1 0 1 0 0
R1
C1
clock control
21 20
0
1 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 0
R2
C2
1
1
22 21 20
0
0 1 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 1 0 1 1 1 1
R3
C3

Key Management in GSM

- The key Ki is stored in the user's SIM card and the AUC (authentication Center)
  - Database usually co-located with the HLR
- The key Ki is never transmitted on the network!
- How???
  - AUC computes triplets (RAND,SREC,Kc) and sends them to the HLR that stores them
  - When a MSC/VLR needs to authenticate a MT, it asks its HLR for some triplets…
  - Note1: the visited network (MSC/VLR) does not need to know the A3 and A5 algorithms!!
  - Each operator can design and deploy its own A3 and A8 algorithms..
    - » Not true for the encryption algorithm (A5) that also needs to be known by the BTS!!
  - Note2: No confidential info. (Ki, Kc, algo.) is sent over the wireless access network!!

Transmission of Security Information between HLR and VLR



Attack History

- 1991
  - First GSM implementation.
- 1994
  - A sketch of the A5/1 algo. Was leaked and was fully reverse engineered in 1999. Few attacks then followed…
- April 1998
  - The Smartcard Developer Association (SDA) together with U.C. Berkeley researches cracked the COMP128 algorithm stored in SIM and succeeded to get K_i within several hours. They discovered that Kc uses only 64 bits.
- August 1999
  - The *weak* A5/2 was cracked using a single PC within seconds.

Attack History (2)

- December 1999
  - Alex Biryukov, Adi Shamir and David Wagner have published the scheme breaking the *strong* A5/1 algorithm. With 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.
- 2003
  - Barkan, Biham and Keller, proposed the strongest known to date A5/2 attacks
    - » Requires only few milliseconds of encrypted voice (4 frames) to recover the encryption key Kc in less than 1 second.

Attack History (3)

- December 2009
  - Karsten Nohl ammounced that he had cracked the A5/1 cipher. He developped a number of rainbow tables and found new sources for known plaintext attacks.
  - In 2010, treathpost.com reported that a group of cryptographer has broken Kasumi (name for the A5/3 algorithm used to secure most 3G traffic)

Consequence

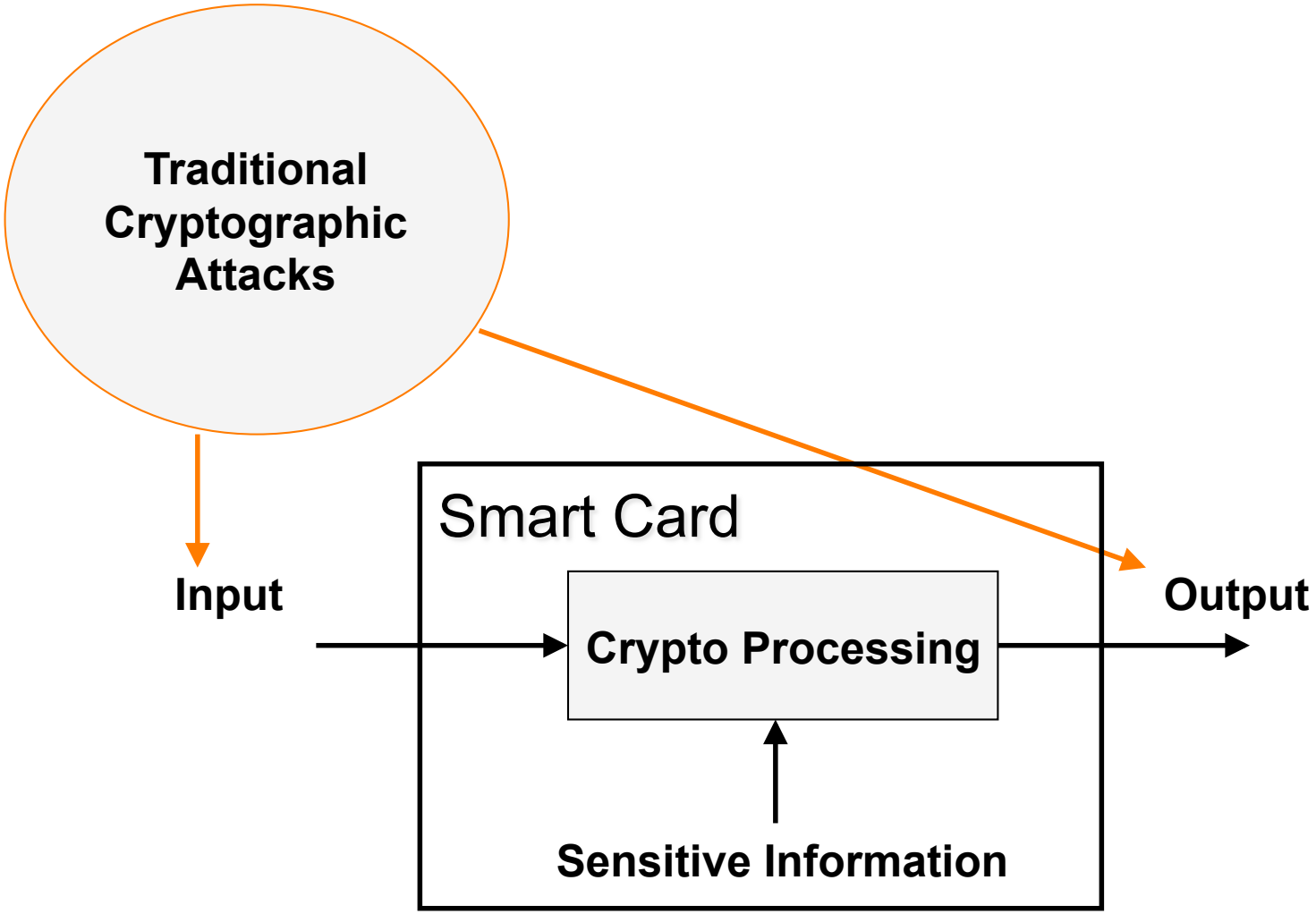
	Confidentiality	Authentication	Keying
US Analog	None	None	None
US Digital	XOR mask & CMEA (ORYX)	CAVE	CAVE
GSM	A5/0, A5/2, or A5/1 (soon: A5/3)	COMP128 (COMP128-2, 3DES-CBC-MAC)	COMP128 (same)

Key: = insecure

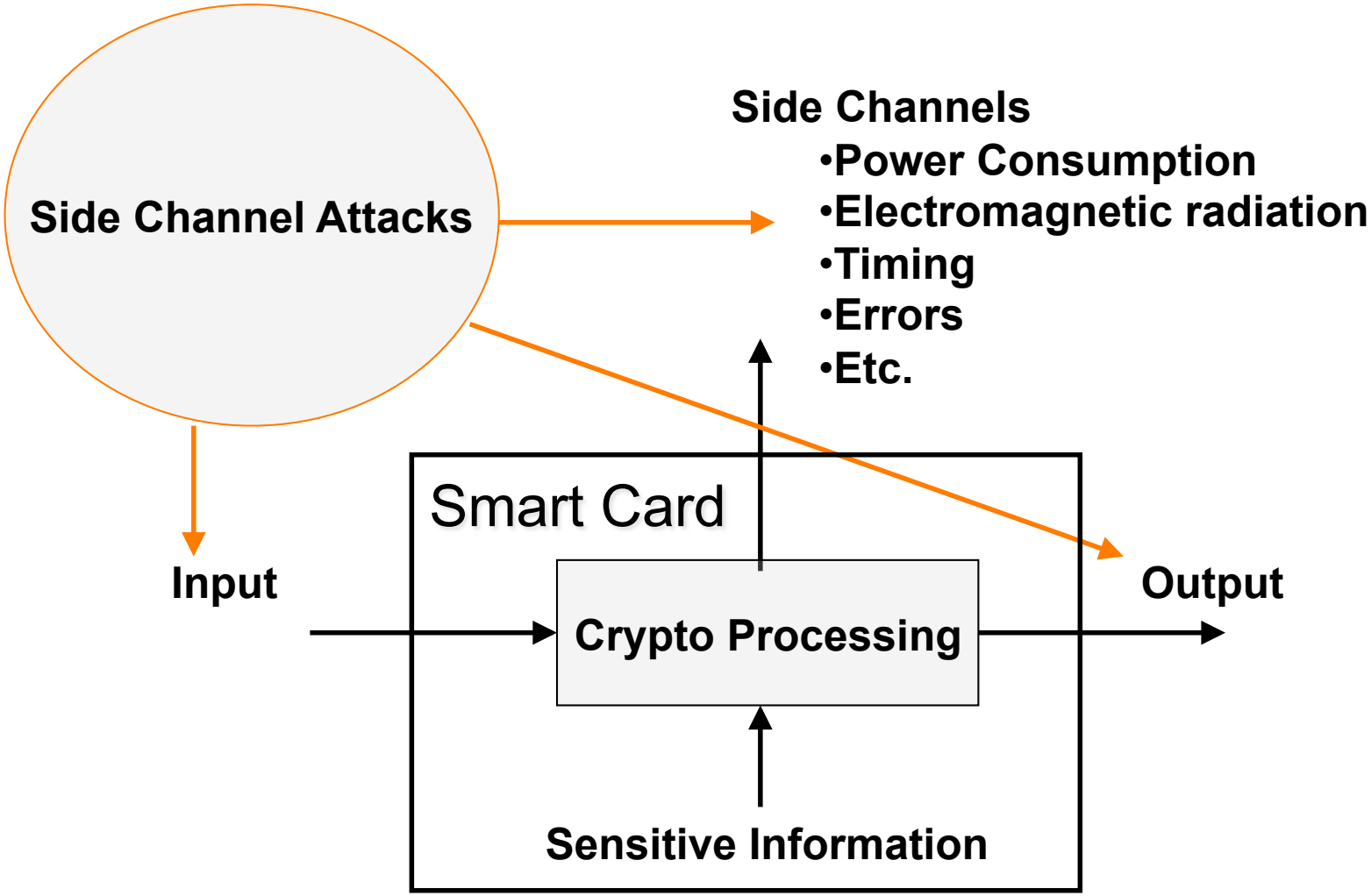
Extracting Ki from the SIM card

- Attack Goal
  - K_i stored on SIM card
  - Knowing K_i 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

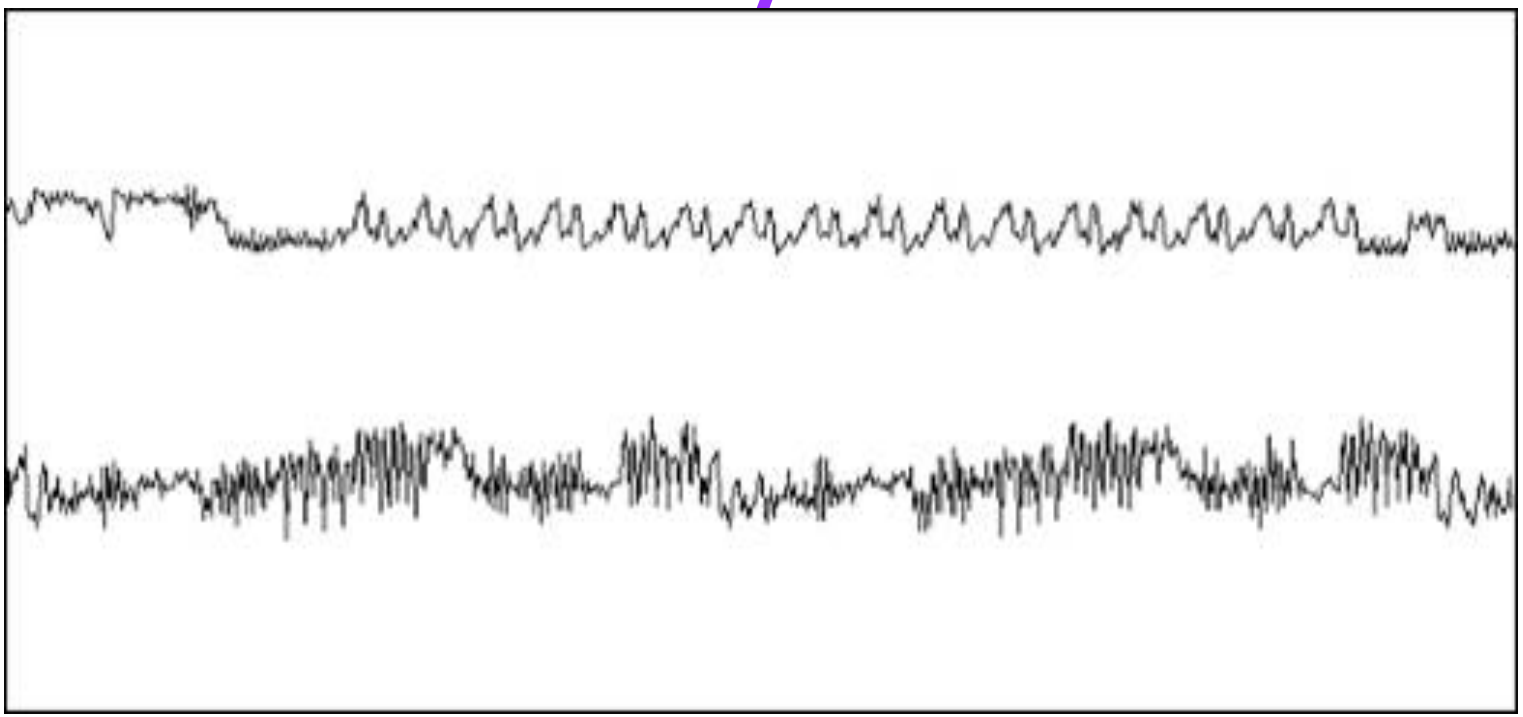
Attacks on SIM cards



Actual Information Available



Example: Simple Power DES Analysis



- SPA of DES operation performed by a typical Smart Card
  - Above: initial permutation, 16 DES rounds, final permutation
  - Below: detailed view of the second and third rounds

Attacks on Signaling Network

- The transmissions are encrypted only between MS and BTS. After the BTS, the protocols between MSC and BSC (BSSAP) and inside the operator's network (MAP) are unencrypted, allowing anyone who has access to the signaling system to read or modify the data on the fly !
- So, the SS7 signaling network is completely insecure. The attacker can gain the actual phone call, RAND & SRES…

Attacks on Signaling Network

- If the attacker can access the HLR, s/he will be able to retrieve the K_i for all subscribers of that particular network.
- If he gets access to a MSC, it can register, de-register, listen the communication,…i.e. it has full power…

Retrieving K_i over Air

- The K_i key can be retrieved from SIM over the air :
  - MS is required to respond to every challenge made by GSM network (there is no authentication of BTS).
  - Attack based on differential cryptanalysis could take 8-15 hours and require that the signal from the legitimate BTS be disabled for that time, but it's still real …
- The same attack could be applied to AuC
  - It also has to answer the requests made by the GSM network
  - It's much faster than SIM

Man-in-the-Middle Attack

- GSM is vulnerable to a MiTM attack
- The attacker impersonate a false base station
- The attacker forces the mobile station to connect to the fake BS
  - Most mobile station connects to the base station it receives the best.
- The fake BS can then impersonate the MS by resending the identity information it received from the mobile station.

Man-in-the-Middle Attack (2)

- By sending false information about its encryption capabilities to the network, the attacker can disable the encryption between himself and the network.
- It can also request to network to turn off the encryption between the mobile station and the fake base station.
- The attacker can then eavesdrop on the communication between the mobile station and the network …and insert/modify traffic.

Conclusions

- Security by Obscurity
- Only access security – doesn't provide end-to-end security
- GSM Security is broken at many levels, vulnerable to numerous attacks
- Even if security algorithms are not broken, the GSM architecture will still be vulnerable to attacks from inside or attacks targeting the operator's backbone
- No mutual authentication
- Confidential information requires additional encryption over GSM
- The future - 3GPP :
  - the design is public
  - mutual authentication (EAP-SIM Authentication), key-length increased, security within and between networks, etc.

Thank You !