Security of cellular networks

Srdjan Čapkun

Department of Computer Science
ETH Zurich

Some material from Hubaux, Stepanov

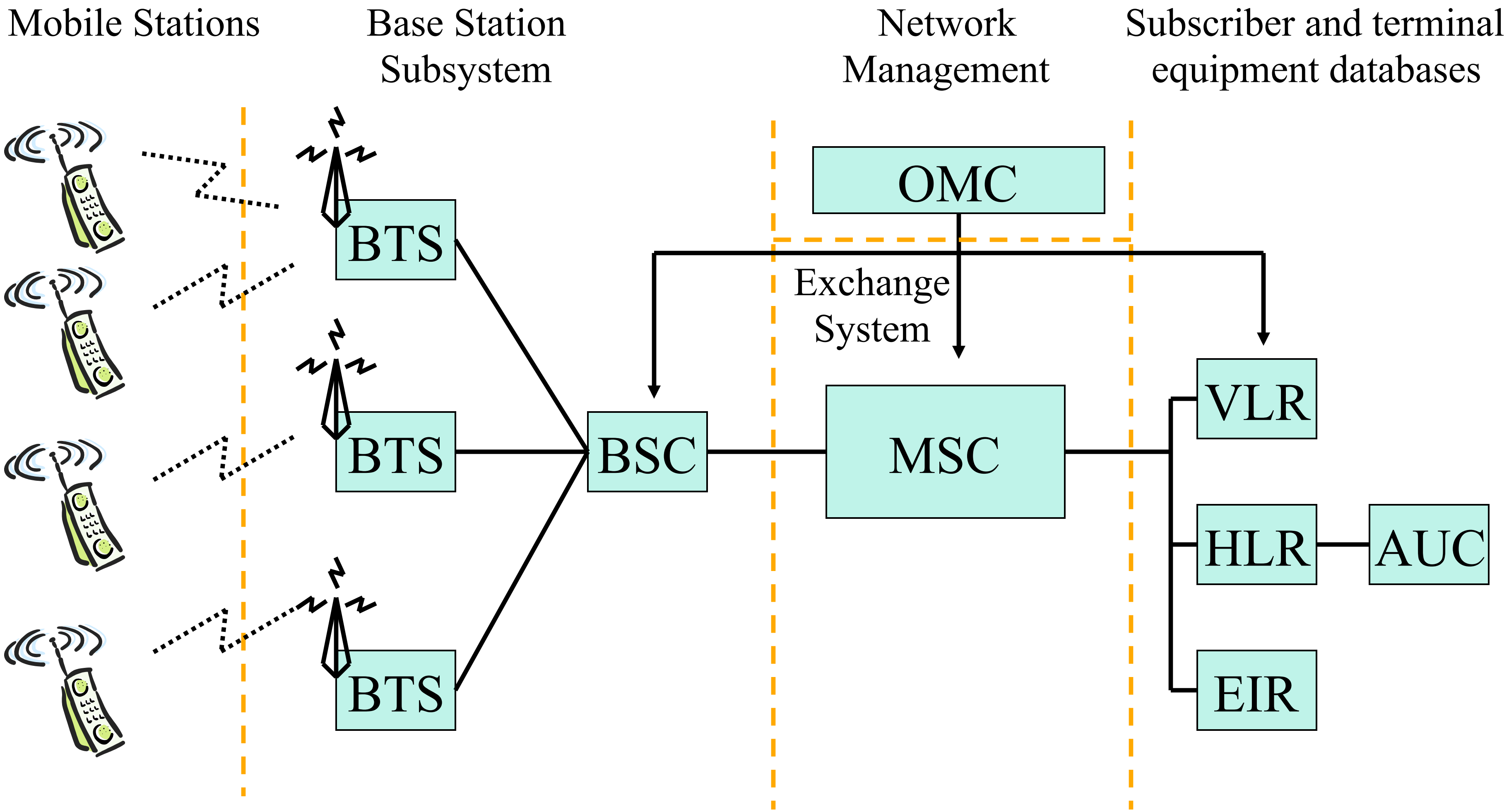
GSM: Introduction

- GSM is the most widely used cellular standard
- Over 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
- Today's networks are 2G evolving to 2.5G
- Third generation (3G) and future (4G)

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 Architecture



HLR = Home Location Register

AC = Authentication center

VLR = Visitor Location Register

EIR - Equipment Identity Register

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

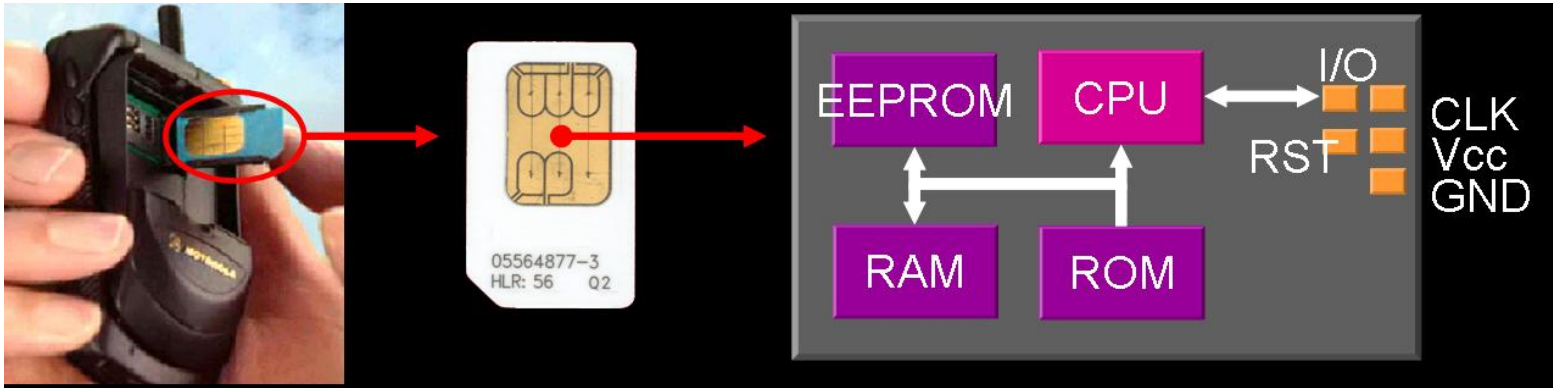
my grandgrandma ...

- Two issues:
- ***Talking for free:*** How do you prove that you are the costumer of a network?
- ***Talking on someone else’s expense:*** How do you differ between two costumers?

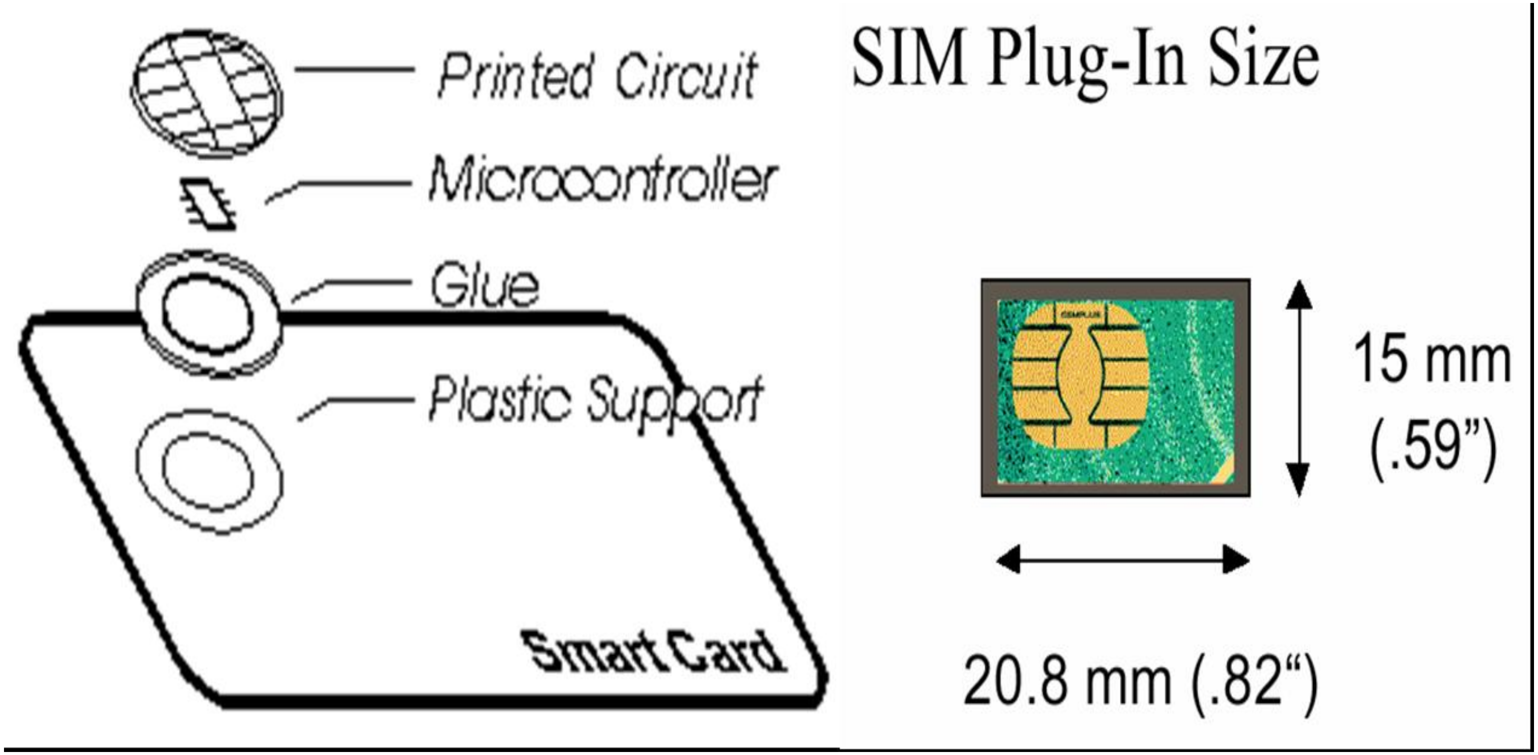
- => we need a way to distinguish between users **(authentication)**

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

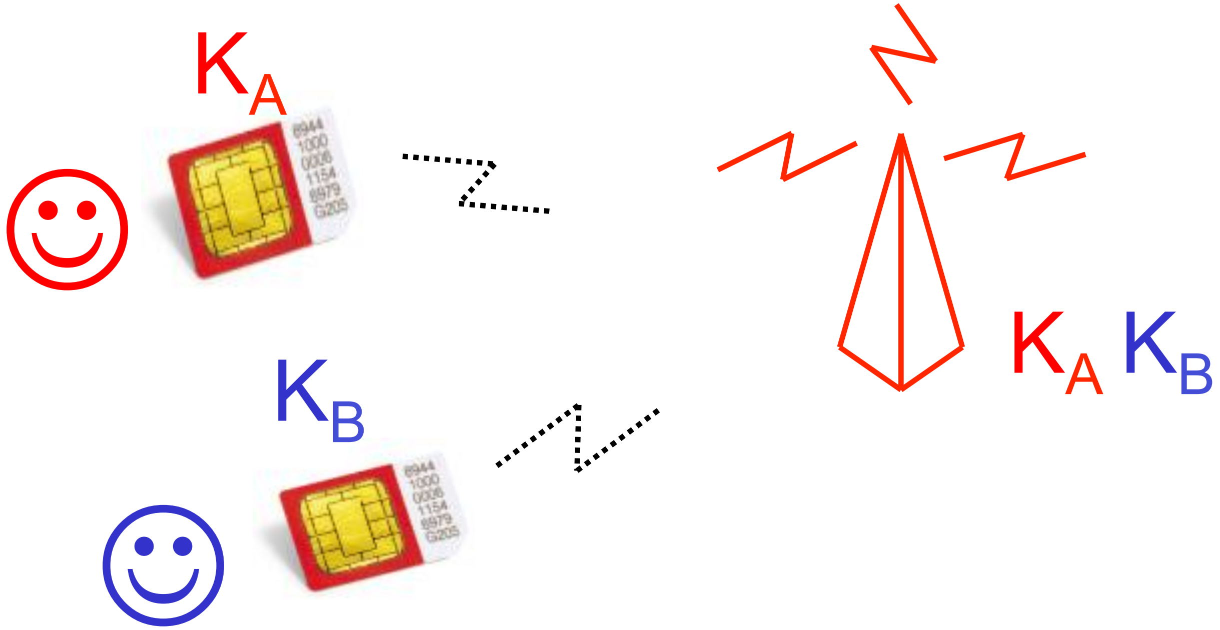
GSM Mobile Station

- Mobile Station
  - Mobile Equipment (ME)
    - Physical mobile device
    - Identifiers
      - IMEI – International Mobile Equipment Identity
  - Subscriber Identity Module (SIM)
    - Smart Card containing keys, identifiers and algorithms
    - Identifiers
      - **K_i** – 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 SIM card

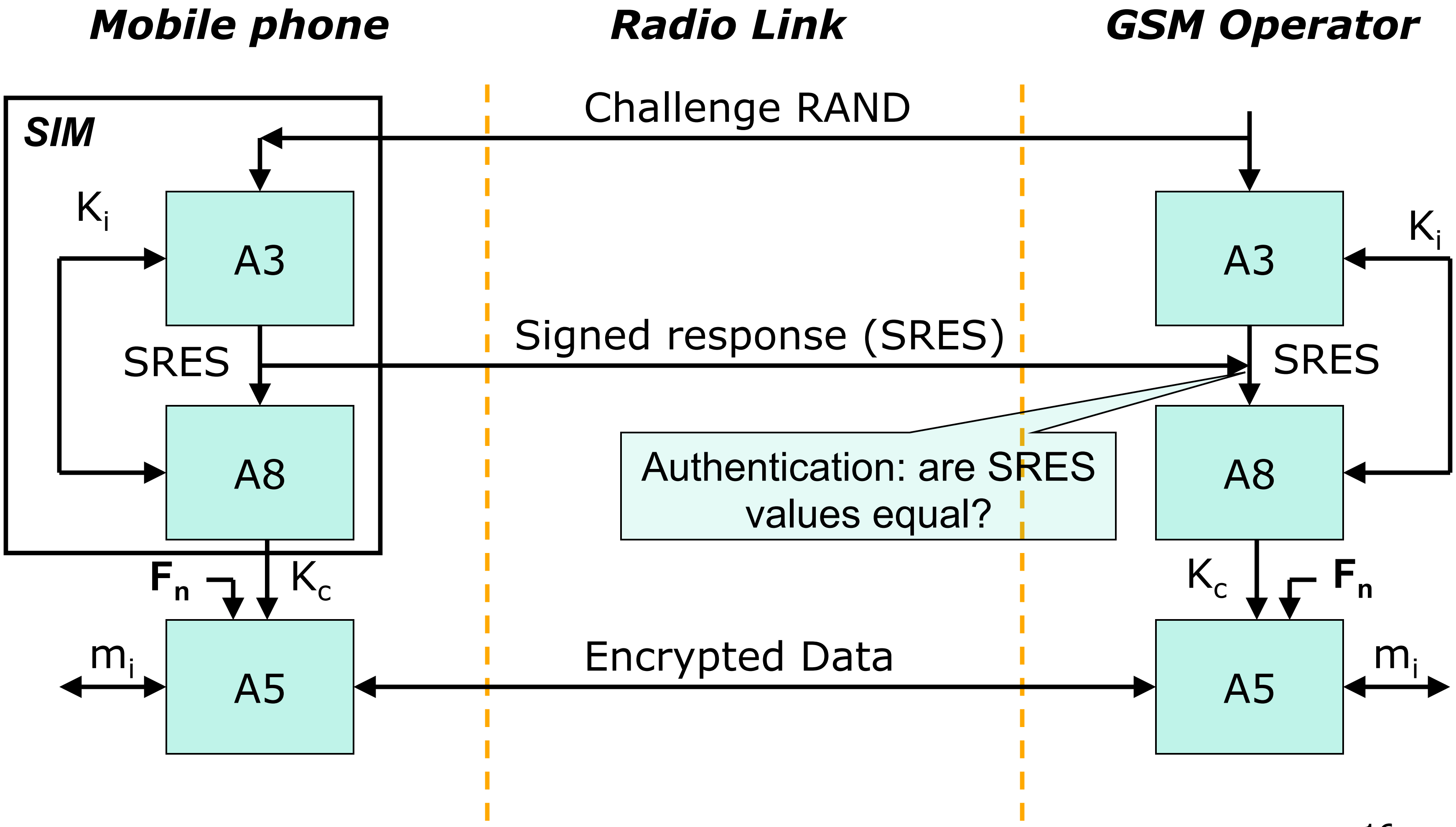
- **K_i** – Subscriber Authentication Key
  - Shared 128 bit key used for authentication of subscriber by the operator
  - Key Storage
    - **Subscriber' s SIM** (owned by operator, i.e. trusted)
    - **Operator' s Home Locator Register (HLR)** of the subscriber' s home network

Keys



We now have different key for each user, but how do we use them to Identify (authenticate) users?

User authentication in GSM



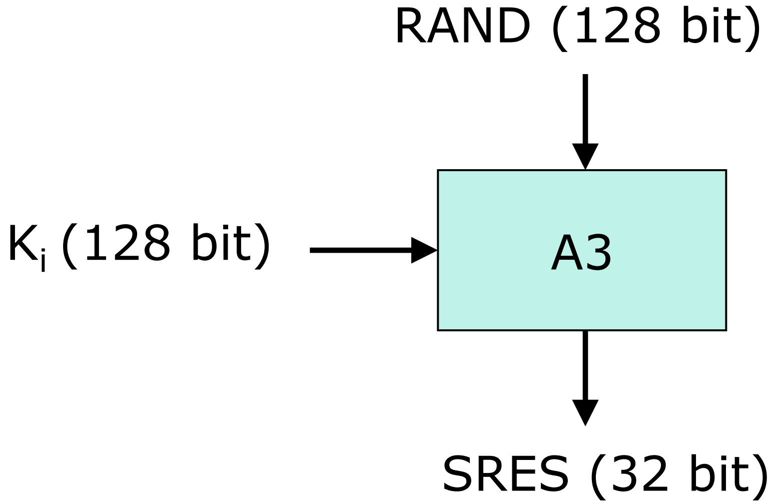
Authentication: are SRES values equal?

Authentication

- AuC – Authentication Center
  - Provides parameters for authentication and encryption functions (RAND, SRES, K_c)
- HLR – Home Location Register
  - Provides MSC (Mobile Switching Center) with triples (RAND, SRES, K_c)
  - 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.

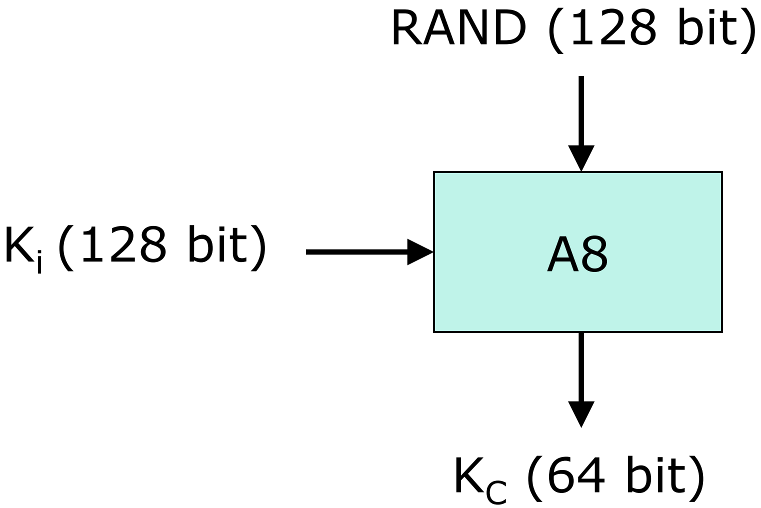
A3 – MS Authentication Algorithm

- Goal
  - Generation of SRES response to MSC’s random challenge RAND



A8 – Voice Privacy Key Generation Algorithm

- Goal
  - Generation of session key K_s
    - A8 specification was never made public

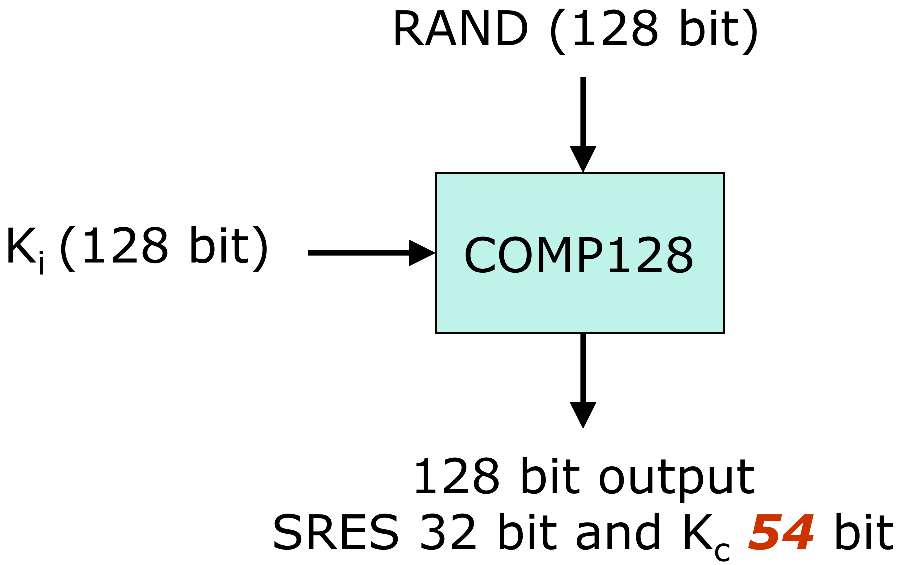


Logical Implementation of A3 and A8

- Both A3 and A8 algorithms are implemented on the SIM
  - Operator can decide, which algorithm to use.
  - Algorithms implementation is independent of hardware manufacturers and network operators.

Logical Implementation of A3 and A8

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



RAND (128 bit)

K_i (128 bit)

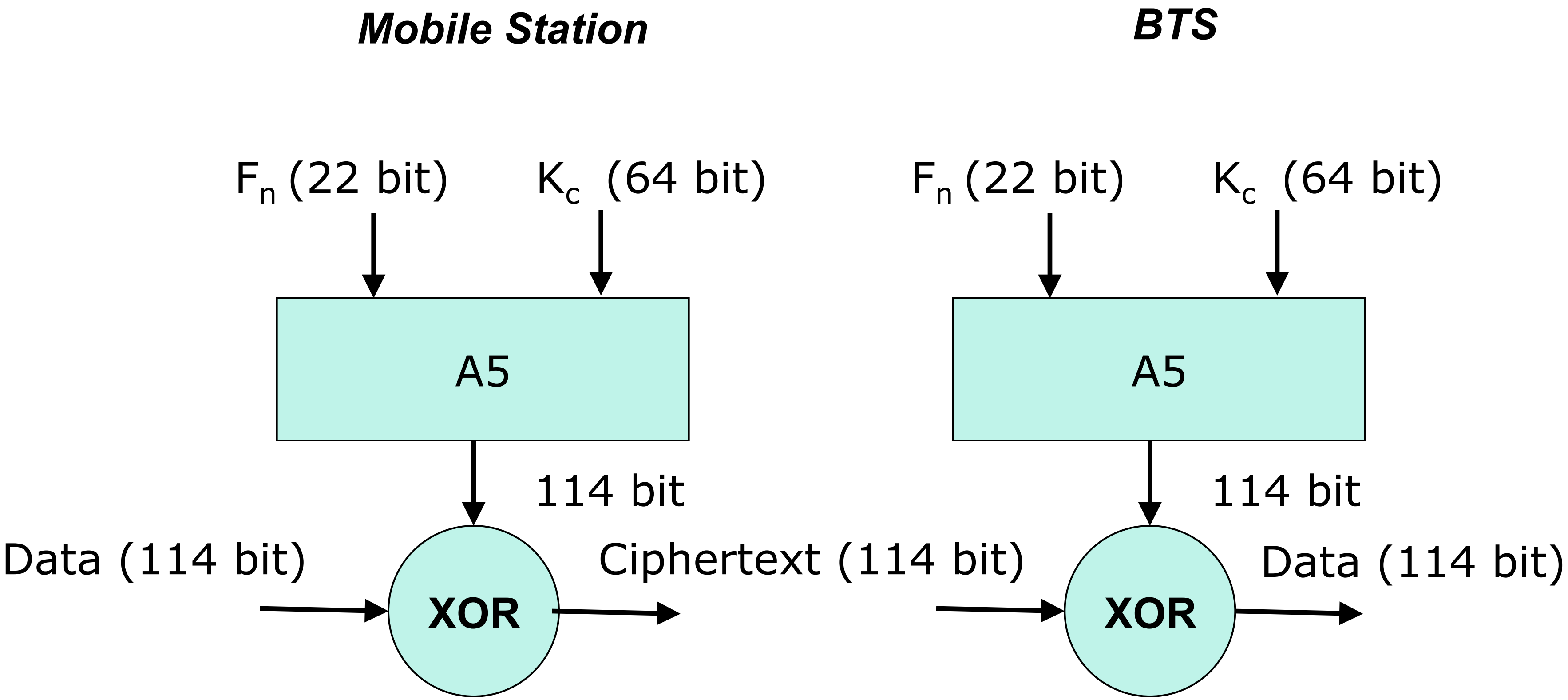
COMP128

128 bit output
SRES 32 bit and K_c ***54*** bit

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

Logical A5 Implementation



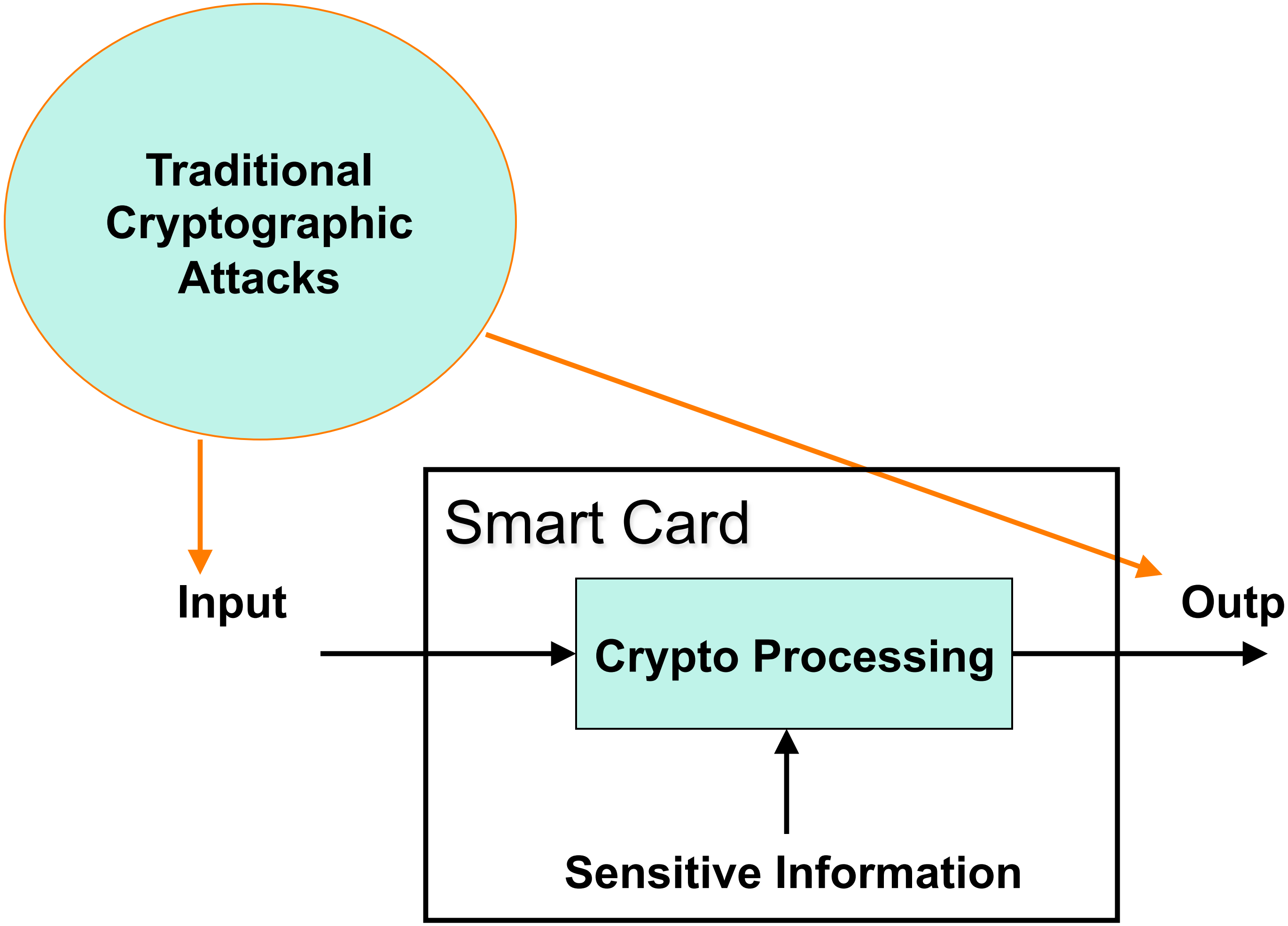
Attacks on GSM

- SIM Attacks
- Radio-link interception attacks
- Operator network attacks
  - GSM does not protect an operator’s network

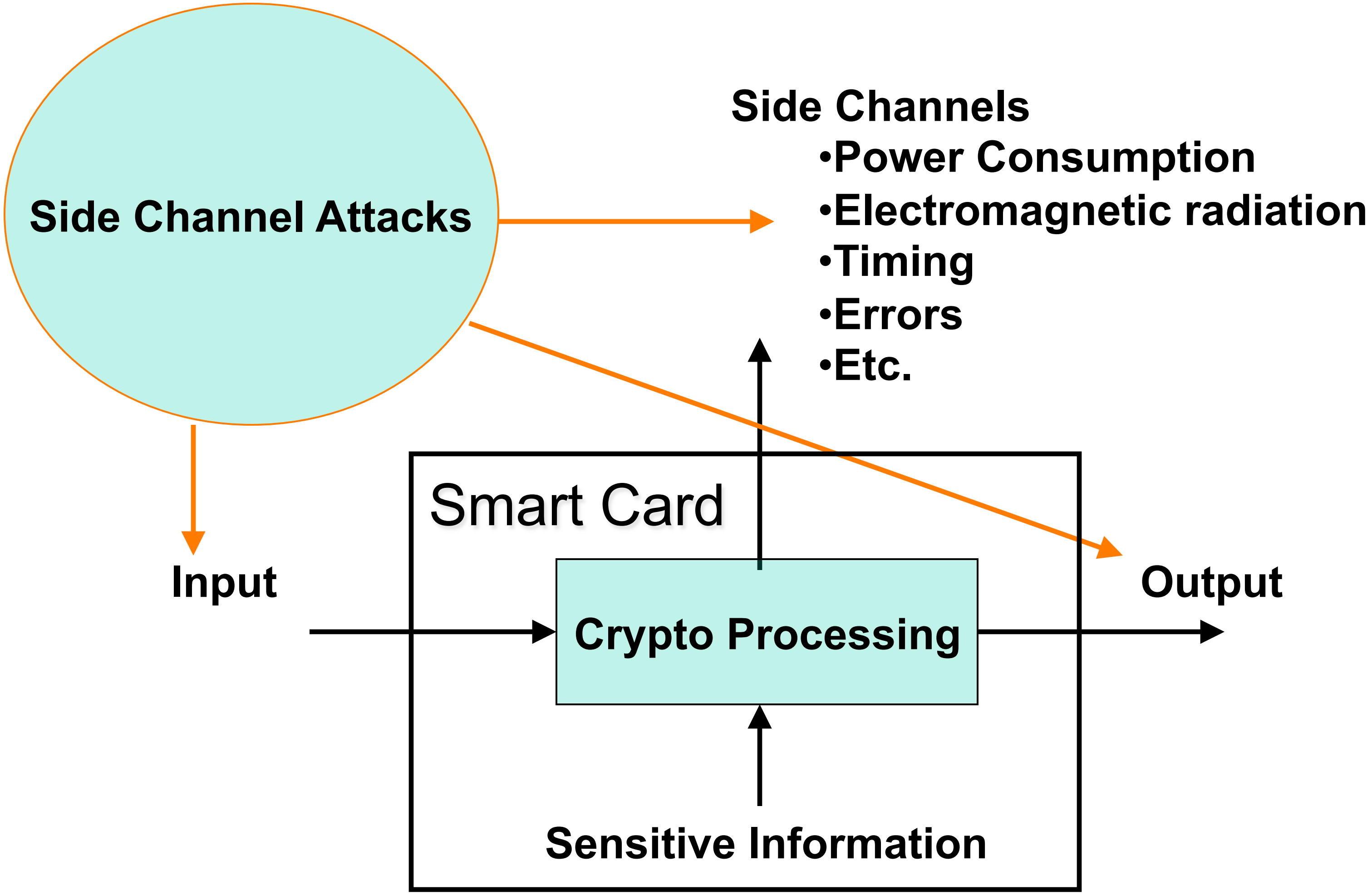
Attack History

- 1991
  - First GSM implementation.
- 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 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.

Traditional Cryptographic Assumptions



Actual Information Available

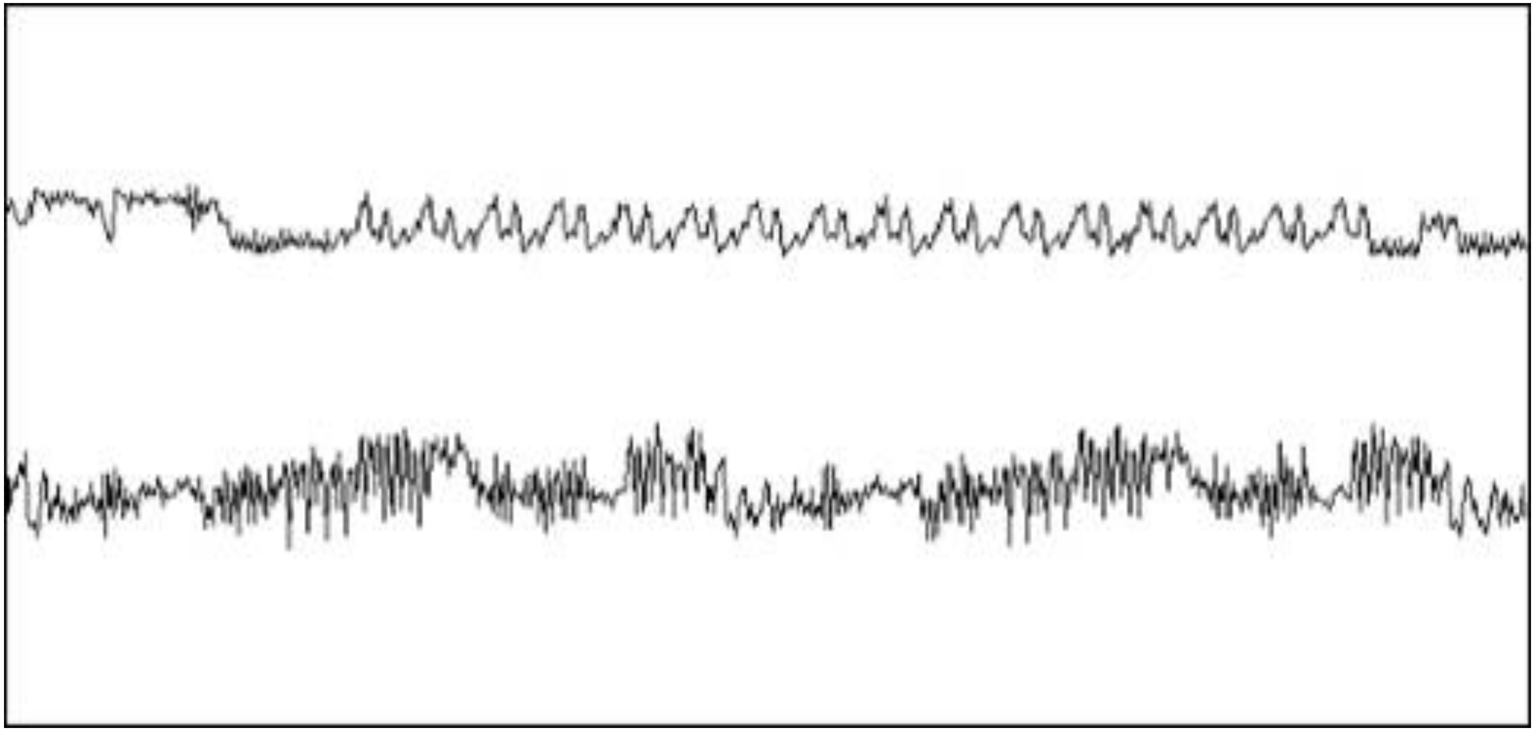


Side Channel Attacks

Side Channels

- Power Consumption
- Electromagnetic radiation
- Timing
- Errors
- Etc.

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

Partitioning Attack on COMP128

- 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

Another attack: fake BTS

- IMSI catcher by Law Enforcement
- Intercept mobile originated calls
- Can be used for over-the-air cloning

Signalling Security

- Mobile networks primarily use Signaling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control. The messages unique to mobile communications are MAP messages.
- The security of the global SS7 network as a transport system for signaling messages e.g. authentication and supplementary services such as call forwarding is open to major compromise.
- The problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner

Low-tech Fraud

- Call forwarding to premium rate numbers
- Bogus registration details
- Roaming fraud
- Terminal theft
- Multiple forwarding, conference calls

Countermeasures for low-tech fraud

Fraud Management systems look for:

- Multiple calls at the same time,
- Large variations in revenue being paid to other parties,
- Large variations in the duration of calls, such as very short or long calls,
- Changes in customer usage, perhaps indicating that a mobile has been stolen or is being abused,
- Monitor the usage of a customer closely during a 'probationary period'

Problems with GSM security

- Only provides *access security* – communications and signalling traffic in the fixed network are not protected.
- Does not address *active attacks*, whereby some network elements (e.g. BTS: Base Station)
- Only as secure as the fixed networks to which they connect
- Lawful interception only considered as an after-thought
- Terminal identity cannot be trusted
- Difficult to upgrade the cryptographic mechanisms
- Lack of user visibility (e.g. doesn’t know if encrypted or not)

Attacks on GSM networks

- **Eavesdropping**. This is the capability that the intruder eavesdrops signalling and data connections associated with other users**. The required equipment is a modified MS.**

- **Impersonation of a user**. This is the capability whereby the intruder sends signalling and/or user data to the network, in an attempt to make the network believe they originate from the target user**. The required equipment is again a modified MS.**

- **Impersonation of the network**. This is the capability whereby the intruder sends signalling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network**. The required equipment is modified BTS.**

Attacks on GSM networks

- **Man-in-the-middle**. This is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signalling and user data messages exchanged between the two parties. **The required equipment is modified BTS in conjunction with a modified MS.**

- **Compromising authentication vectors in the network**. The intruder possesses a compromised authentication vector, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signalling messages on network links.

De-registration spoofing

- An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface.
- The intruder spoofs a de-registration request (IMSI detach) to the network.
- The network de-registers the user from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for mobile terminated services.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the de-registration request allows the serving network to verify that the de-registration request is legitimate.

Location update spoofing

- An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface.
- The user spoofs a location update request in a different location area from the one in which the user is roaming.
- The network registers in the new location area and the target user will be paged in that new area.
- The user is subsequently unreachable for mobile terminated services.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the location update request allows the serving network to verify that the location update request is legitimate.

Camping on a false BTS

- An attack that requires a modified BTS and exploits the weakness that a user can be enticed to camp on a false base station.
- Once the target user camps on the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered.

- **3G**: **The security architecture does not counteract this attack.** However, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

Camping on false BTS/MS

- An attack that requires a modified BTS/MS and exploits the weakness that a user can be enticed to camp on a false base station.
- A false BTS/MS can act as a repeater for some time and can relay some requests in between the network and the target user, but subsequently modify or ignore certain service requests and/or paging messages related to the target user.

- **3G**: The security architecture does not prevent a false BTS/MS relaying messages between the network and the target user, neither does it prevent the false BTS/MS ignoring certain service requests and/or paging requests.
- Integrity protection of critical message may however help to prevent some denial of service attacks, which are induced by modifying certain messages.

Passive Identity Caching

- A passive attack that requires a modified MS and exploits the weakness that the network may sometimes request the user to send its identity in cleartext.

- **3G**: The identity confidentiality mechanism counteracts this attack. The use of temporary identities allocated by the serving network makes passive eavesdropping inefficient since the user must wait for a new registration or a mismatch in the serving network database before he can capture the user’s permanent identity in plaintext.
- The inefficiency of this attack given the likely rewards to the attacker would make this scenario unlikely.

Active Identity Caching

- An active attack that requires a modified BTS and exploits the weakness that the network may request the MS to send its permanent user identity in cleartext.
- An intruder entices the target user to camp on its false BTS and subsequently requests the target user to send its permanent user identity in cleartext perhaps by forcing a new registration or by claiming a temporary identity mismatch due to database failure.

- **3G**: The identity confidentiality mechanism counteracts this attack by using an encryption key shared by a group of users to protect the user identity in the event of new registrations or temporary identity database failure in the serving network.

Hijacking outgoing calls in networks with encryption disabled

- This attack requires a modified BTS/MS. While the target user camps on the false base station, the intruder pages the target user for an incoming call.
- The user then initiates the call set-up procedure, which the intruder allows to occur between the serving network and the target user, modifying the signalling elements such that for the serving network it appears as if the target user wants to set-up a mobile originated call.
- The network does not enable encryption. After authentication the intruder cuts the connection with the target user, and subsequently uses the connection with the network to make fraudulent calls on the target user's subscription.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the connection set-up request allows the serving network to verify that the request is legitimate.
- In addition, periodic integrity protected messages during a connection helps protect against hijacking of un-enciphered connections after the initial connection establishment.

Hijacking outgoing calls in networks with encryption enabled

- This attack requires a modified BTS/MS. In addition to the previous attack this time the intruder has to attempt to suppress encryption by modification of the message in which the MS informs the network of its ciphering capabilities.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the MS station classmark and the connection set-up request helps prevent suppression of encryption and allows the serving network to verify that the request is legitimate.

Hijacking incoming calls in networks with encryption disabled

- This attack requires a modified BTS/MS. While the target user camps on the false base station, an associate of the intruder makes a call to the target user's number.
- The intruder acts as a relay between the network and the target user until authentication and call set-up has been performed between target user and serving network. The network does not enable encryption.
- After authentication and call set-up the intruder releases the target user, and subsequently uses the connection to answer the call made by his associate. The target user will have to pay for the roaming leg.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the connection accept message allows the serving network to verify that the request is legitimate.
- In addition, periodic integrity protected messages during a connection helps protect against hijacking of un-enciphered connections after the initial connection establishment.

Hijacking incoming calls in networks with encryption enabled

- This attack requires a modified BTS/MS. In addition to the previous attack this time the intruder has to suppress encryption.

- **3G**: Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the MS station classmark and the connection accept message helps prevent suppression of encryption and allows the serving network to verify that the connection accept is legitimate.

Security of 3G networks

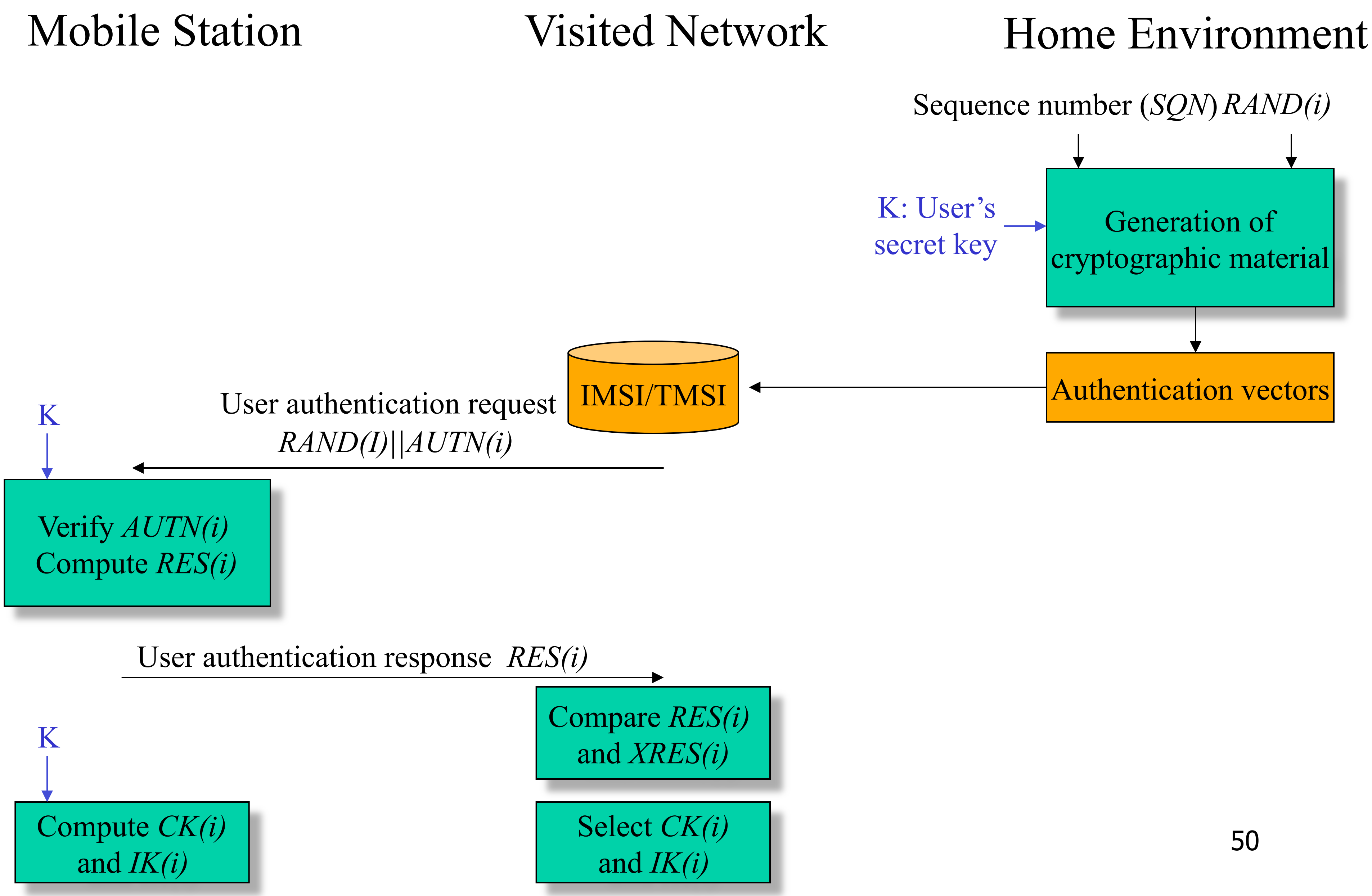
3GPP Security Principles (1/2)

- 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 (especially on the radio interface)
- Correction of the following weaknesses of the previous generation:
  - Possible attacks from a faked base station
  - Cipher keys and authentication data transmitted in clear between and within networks
  - Encryption not used in some networks ➔ open to fraud
  - Data integrity not provided
  - …

3GPP Security Principles (2/2)

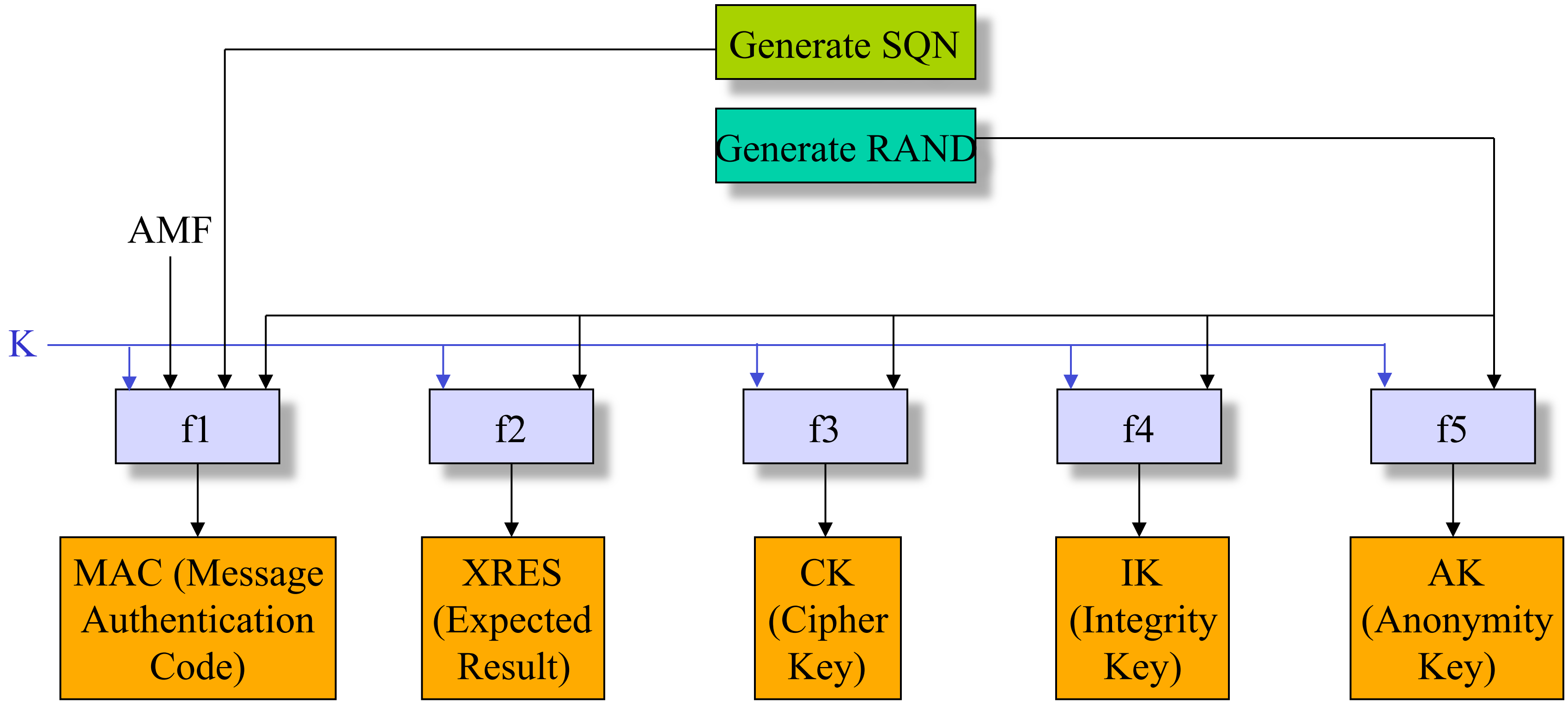
- New security features
  - New kind of service providers (content providers, HLR only service providers,…)
  - Increased control for the user over their service profile
  - Enhanced resistance to active attacks
  - Increased importance of non-voice services
  - …

Authentication in 3GPP (with a visited network)



Mobile Station
Visited Network
Home Environment
Sequence number (*SQN*) *RAND(i)*
K: User's secret key
Generation of cryptographic material
Authentication vectors
IMSI/TMSI
User authentication request *RAND(I)||AUTN(i)*
K
Verify *AUTN(i)* Compute *RES(i)*
User authentication response *RES(i)*
Compare *RES(i)* and *XRES(i)*
K
Compute *CK(i)* and *IK(i)*
Select *CK(i)* and *IK(i)*

Generation of the authentication vectors (by the Home Environment)

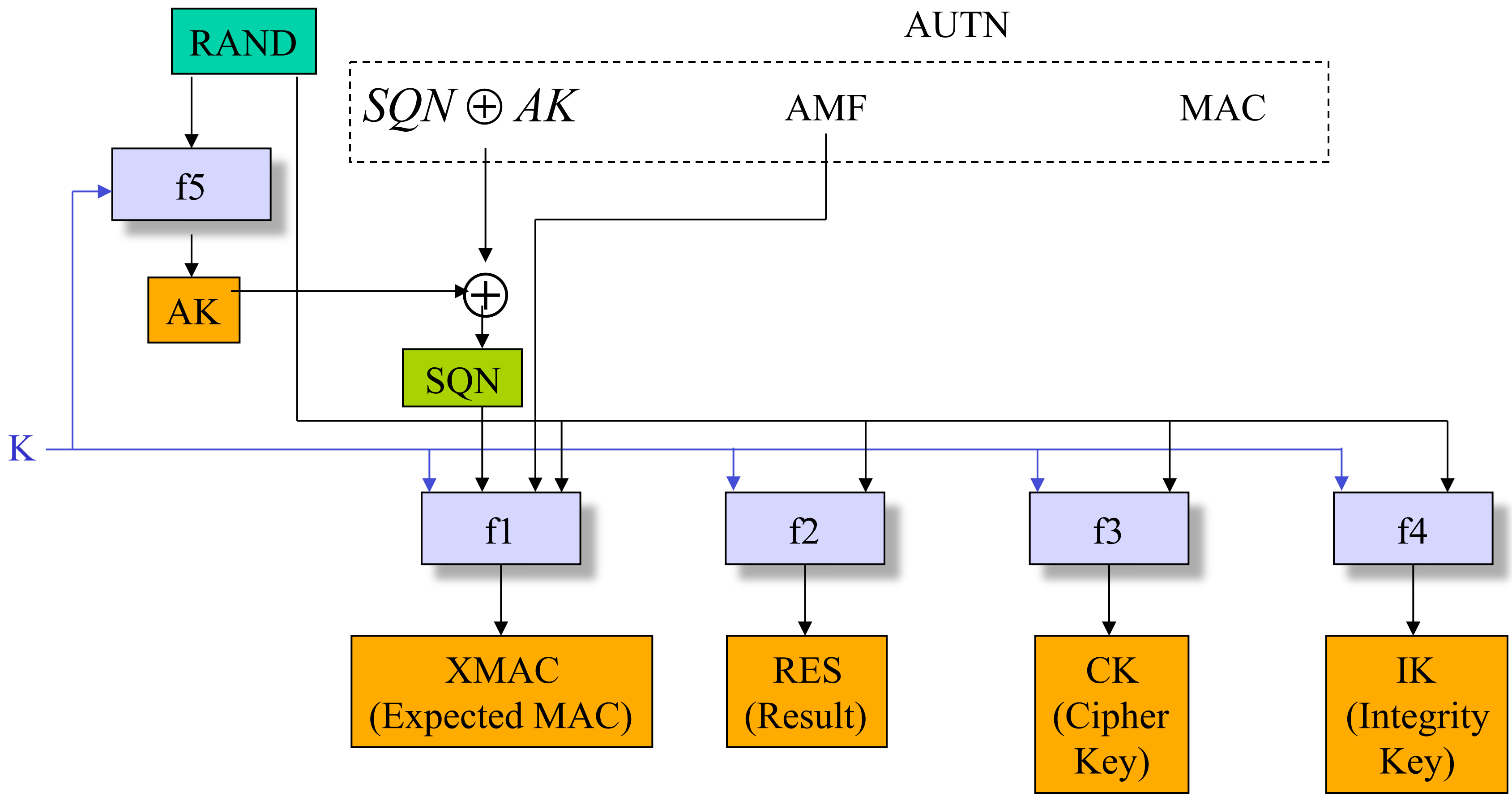


Authentication token: AUTN = (SQN⊕AK)|| AMF|| MAC

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

AMF: Authentication and Key Management Field

User Authentication Function in the USIM



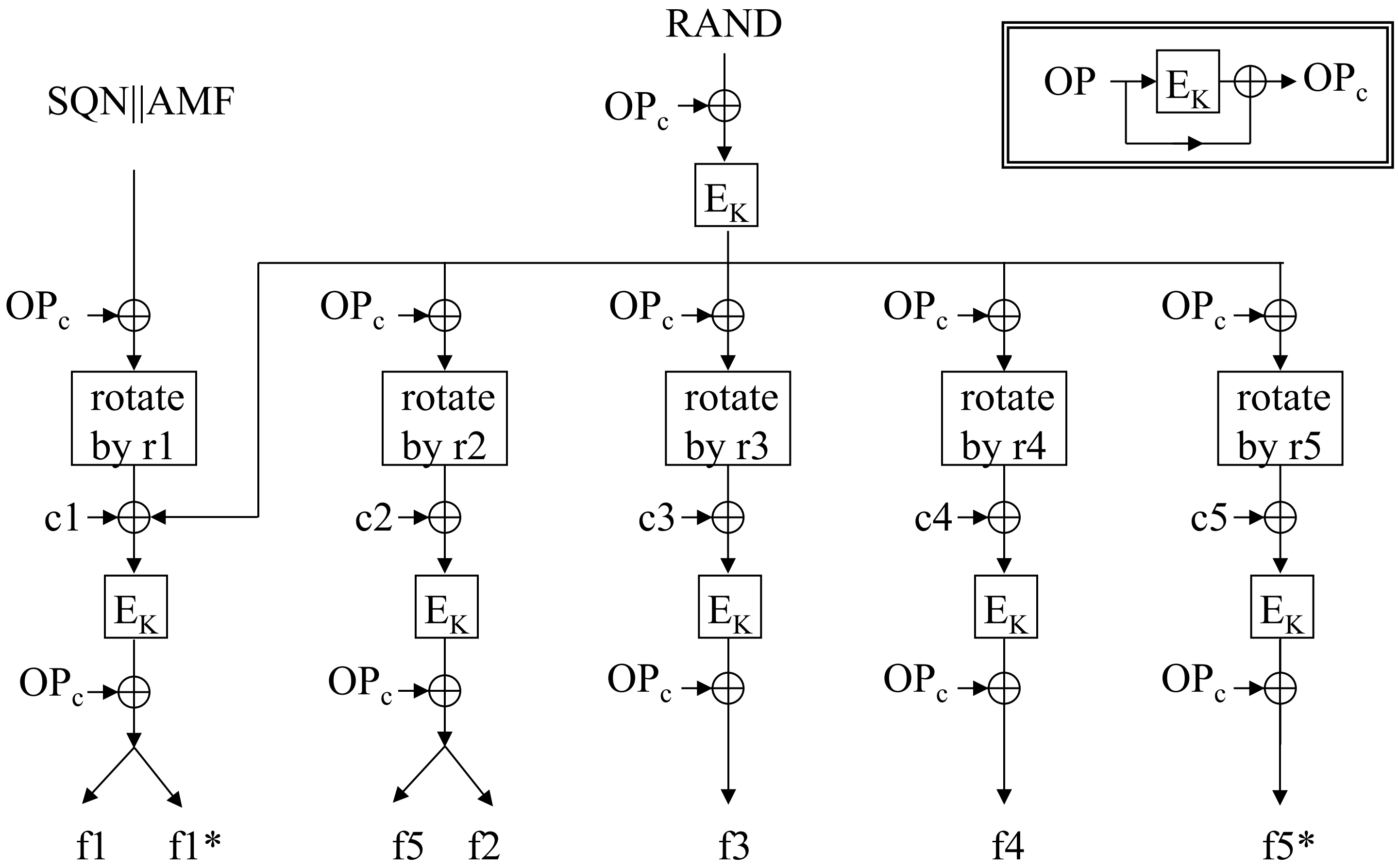
- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module

More about the authentication and key generation function

- In addition to f1, f2, f3, f4 and f5, two more functions are defined: f1* and f5*, used in case the authentication procedure gets desynchronized (detected by the range of SQN).
- f1, f1*, f2, f3, f4, f5 and f5* 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 f1…f5* is based on the Rijndael algorithm

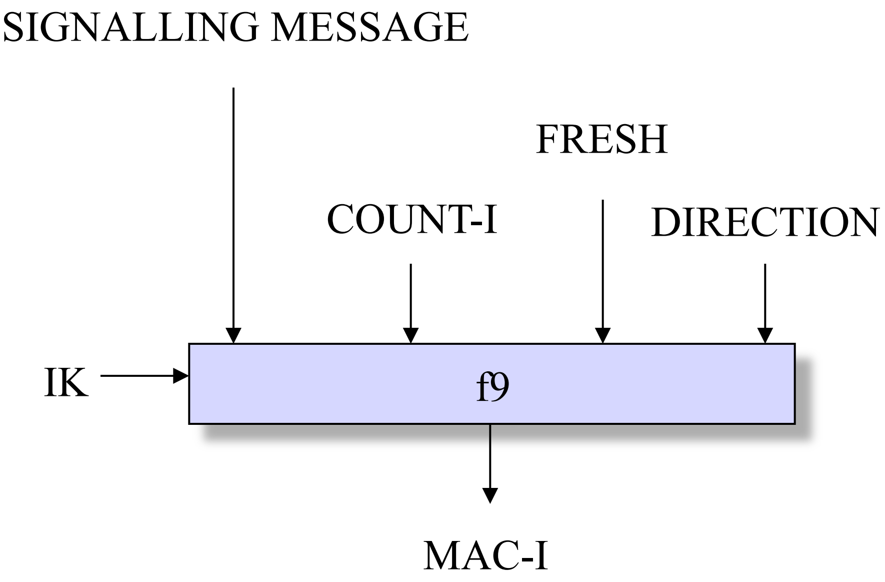
Authentication and key generation functions f1… f5*



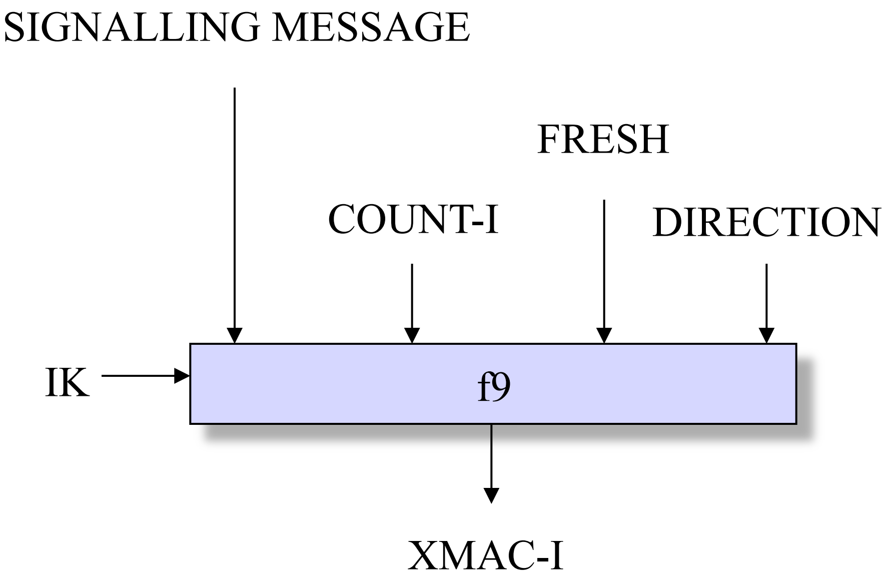
OP: operator-specific parameter
r1,…, r5: fixed rotation constants
c1,…, c5: fixed addition constants

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

Signalling integrity protection method



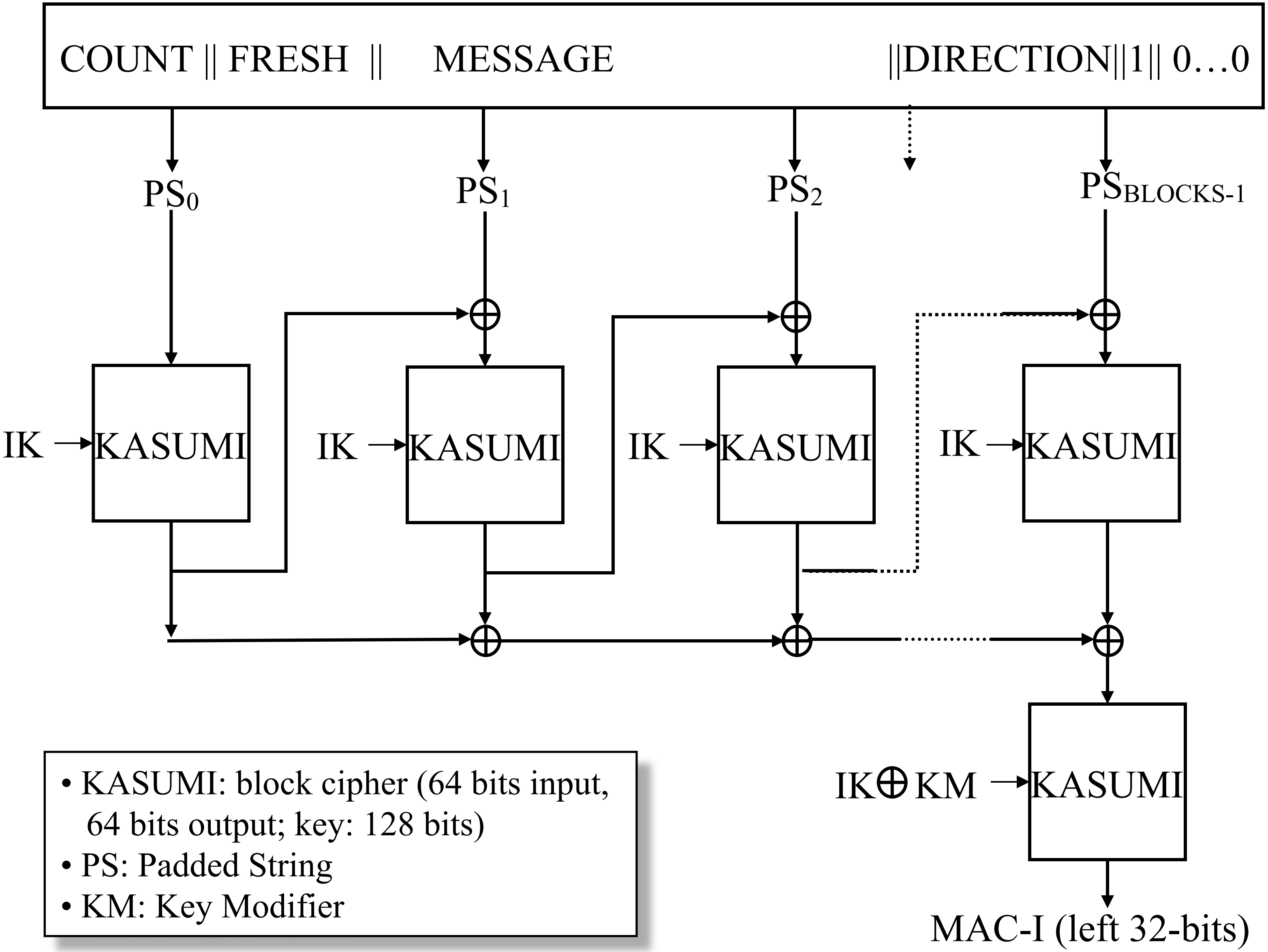
Sender
(Mobile Station or
Radio Network Controller)



Receiver
(Radio Network Controller
or Mobile Station)

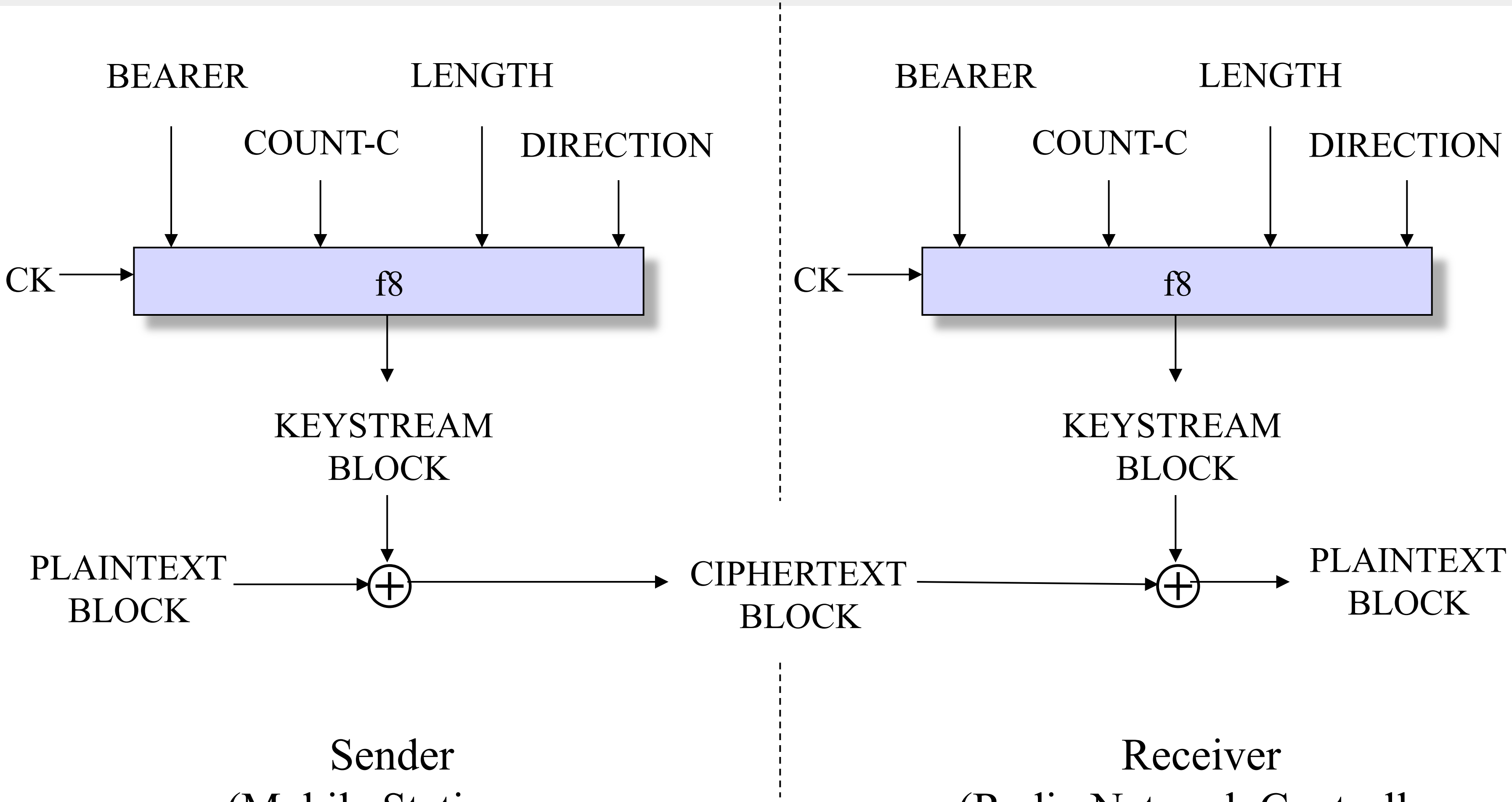
FRESH: random input

f9 integrity function



- KASUMI: block cipher (64 bits input, 64 bits output; key: 128 bits)
- PS: Padded String
- KM: Key Modifier

Ciphering method

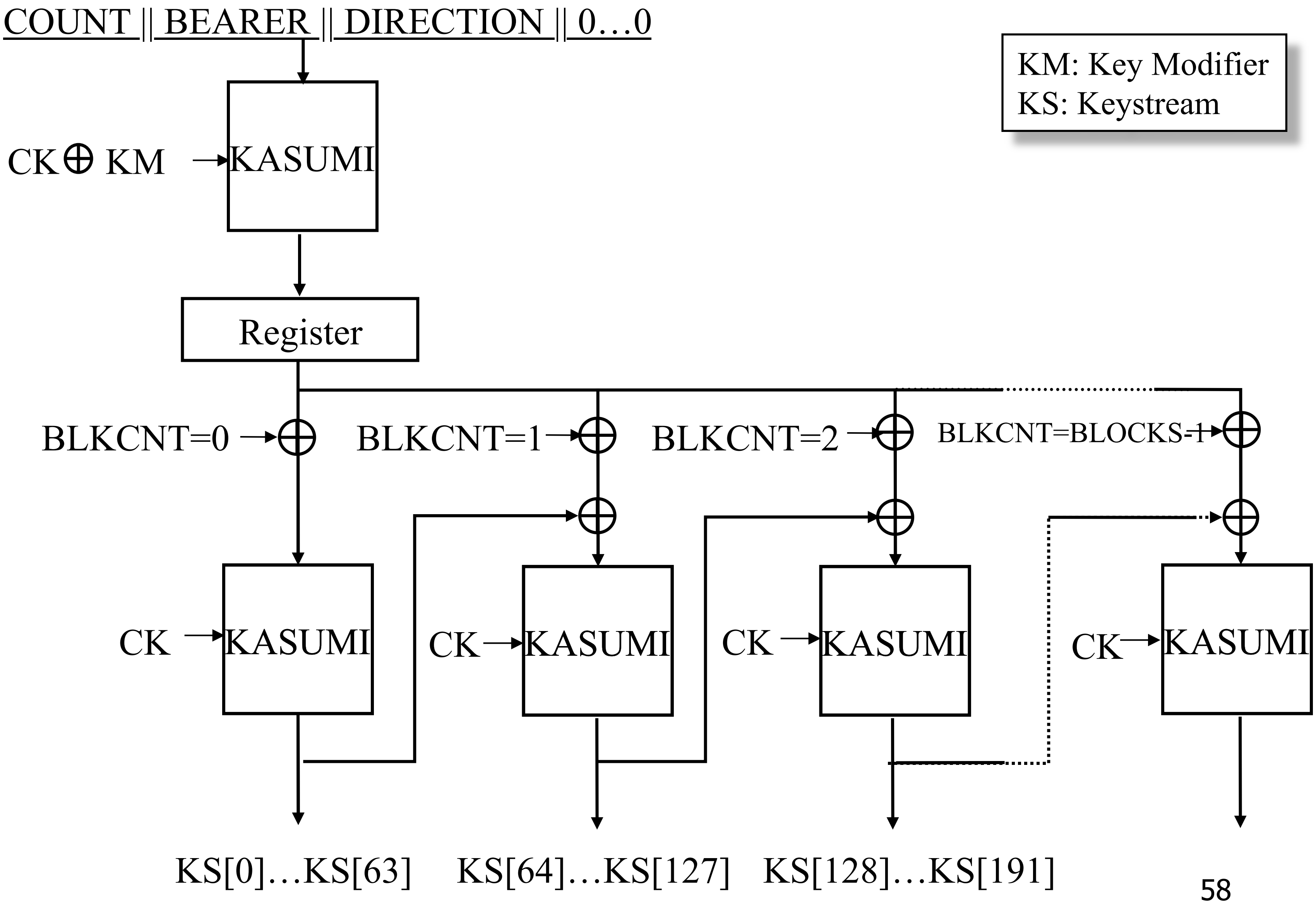


Sender
(Mobile Station or
Radio Network Controller)

Receiver
(Radio Network Controller
or Mobile Station)

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

f8 keystream generator



KM: Key Modifier
KS: Keystream

Detail of Kasumi

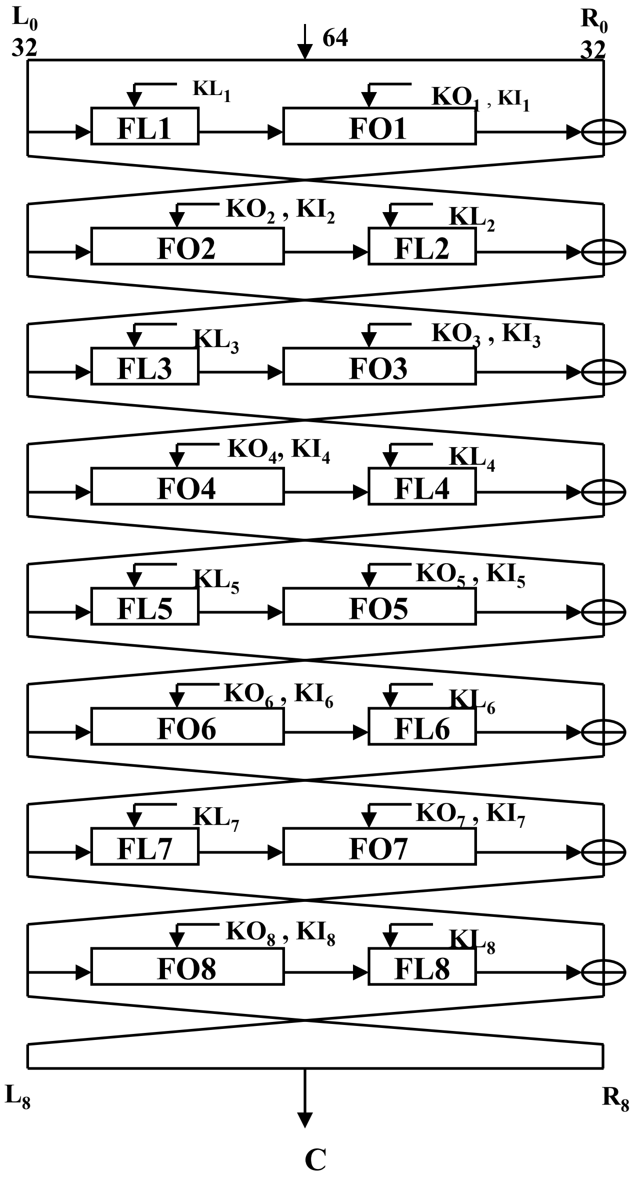


Fig. 1 **: KASUMI**

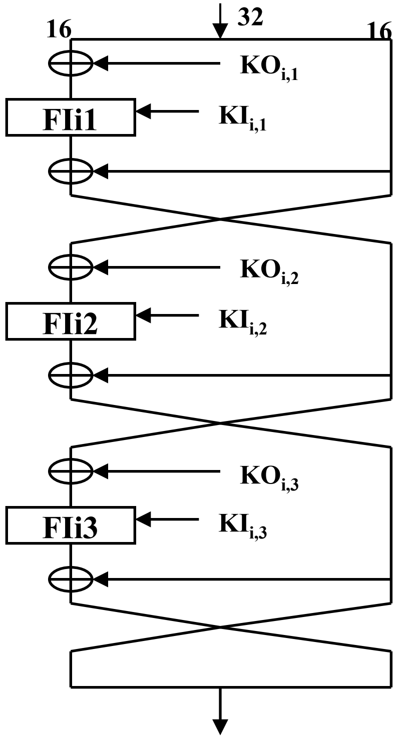


Fig. 2 **: FO Function**

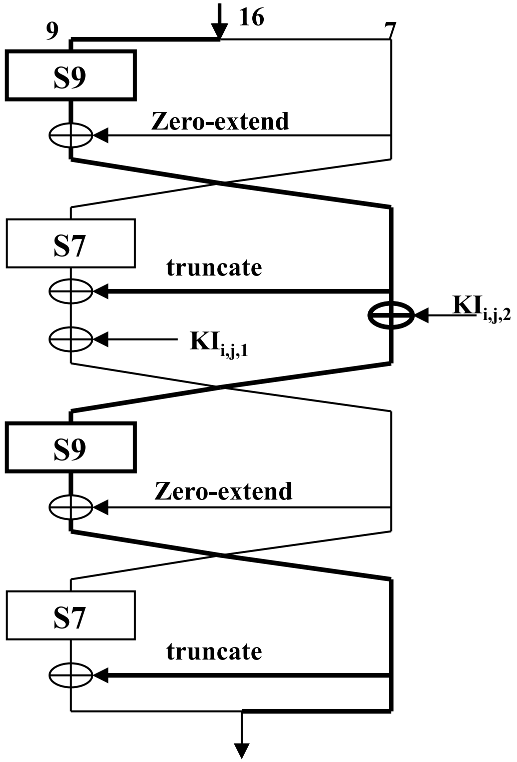


Fig. 3 **: FI Function**

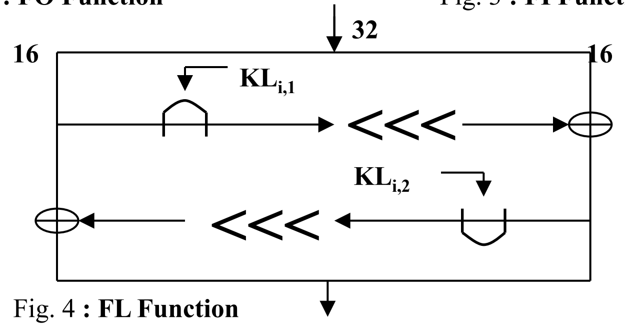


Fig. 4 **: FL Function**

KL_i, KO_i , KI_i : subkeys used at ith round
S7, S9: S-boxes

∩ Bitwise AND operation

∪ Bitwise OR operation

<<< One bit left rotation

Conclusion on 3GPP security

- Some improvement with respect to 2nd generation
  - Cryptographic algorithms are published
  - Integrity of the signalling messages is protected
- Quite conservative solution
- No real size experience so far
- Privacy/anonymity of the user not completely protected
- 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
- 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

References

On Signalling System 7

- Travis Russel, *Signaling System #7*, Second Edition, McGraw-Hill Telecommunications, 1998.
- Uyless Black, *ISDN and SS7,* Prentice Hall, 1997
- Abdi Modaressi and Ronald A. Skoog, *Signaling System N°7: A tutorial,* IEEE Communications Magazine, July 1990, pp 19-35.

- On GSM
  - D. Goodman: *Wireless Personal Communications Systems* Addison-Wesley, 1997
  - S. Redl et al.: *GSM and Personal Communication Handbook* Artech House Publ, 1998
  - A. Mehrotra: *GSM System Engineering* Artech House Publ, 1997
- On GPRS
  - R. Kalden et al.: *Wireless Interned Access Based on GPRS* IEEE Personal Communication Magazine, April 2000
- On 3GPP
  - 3rd Generation Partnership Project: http://www.3gpp.org