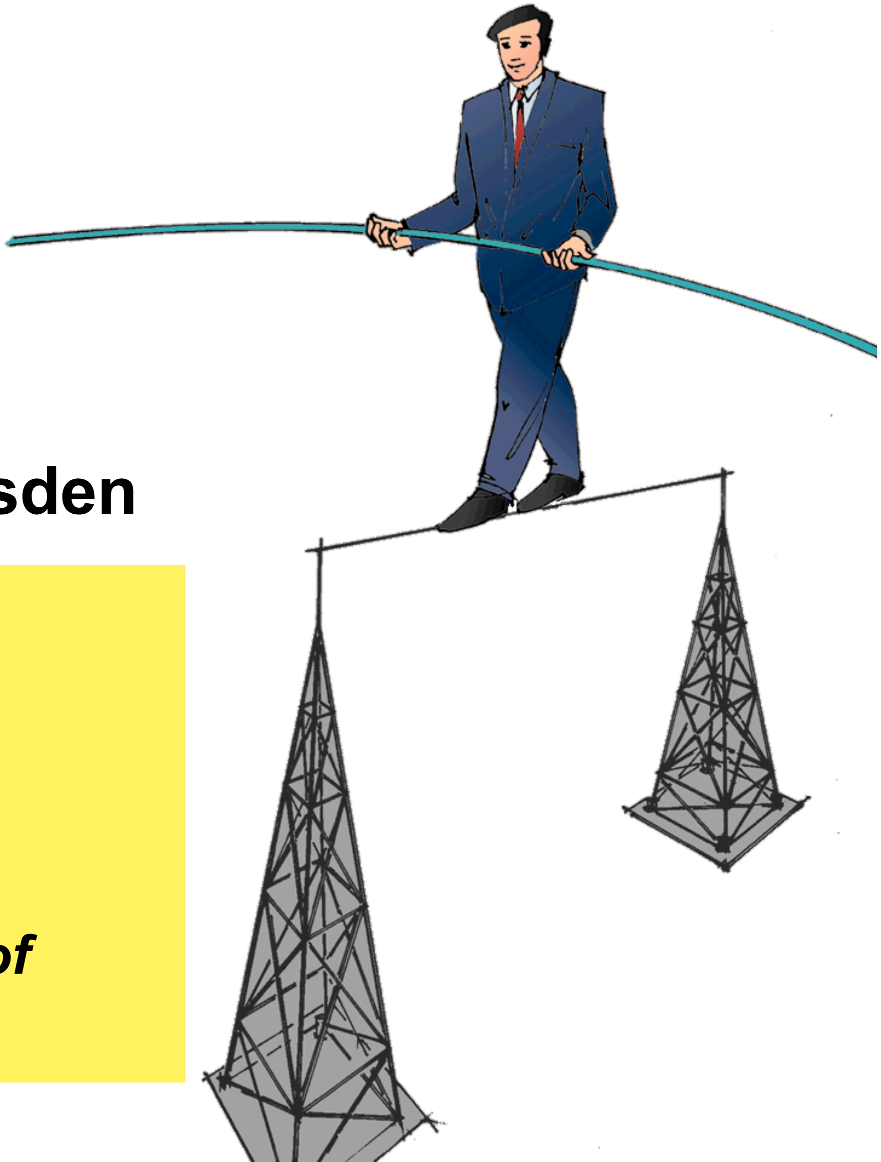
Security functions in mobile communication systems

Dr. Hannes Federrath

University of Technology Dresden



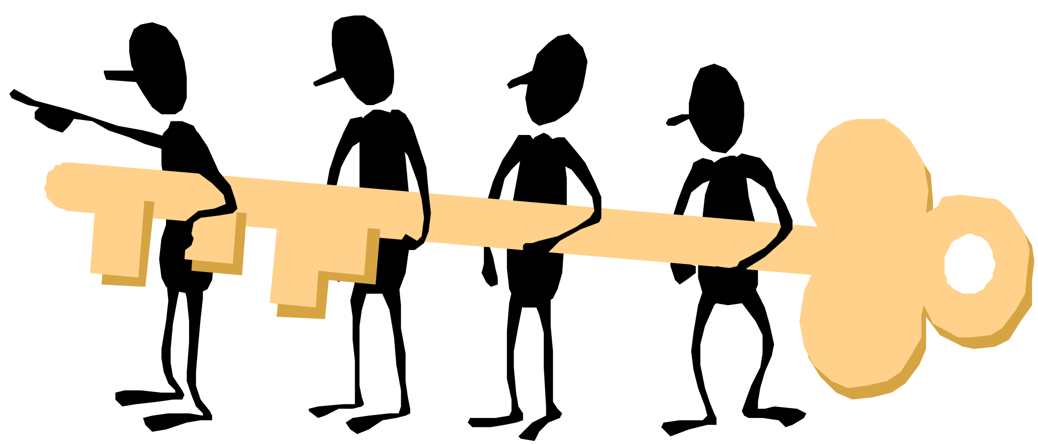
- *Security demands*
- *Security functions of GSM*
- *Known attacks on GSM*
- *Security functions of UMTS*
- *Concepts for hiding locations of mobile users*

Security deficits of existing mobile networks

- ***Example of security demands: Cooke, Brewster (1992)***
  - protection of user data
  - protection of signaling information, incl. location
  - user authentication, equipment verification
  - fraud prevention (correct billing)
- ***Security deficits of GSM (selection)***
  - Only symmetric cryptography (algorithms no officially published)
  - Weak protection of locations (against outsiders)
  - No protection against insider attacks (location, message content)
  - No end-to-end services (authentication, encryption)
- ***Summary***
  - GSM provides protection against <u>external attacks</u> only.
  - "…the designers of GSM did not aim at a level of security much higer than that of the fixed trunk network." Mouly, Pautet (1992)

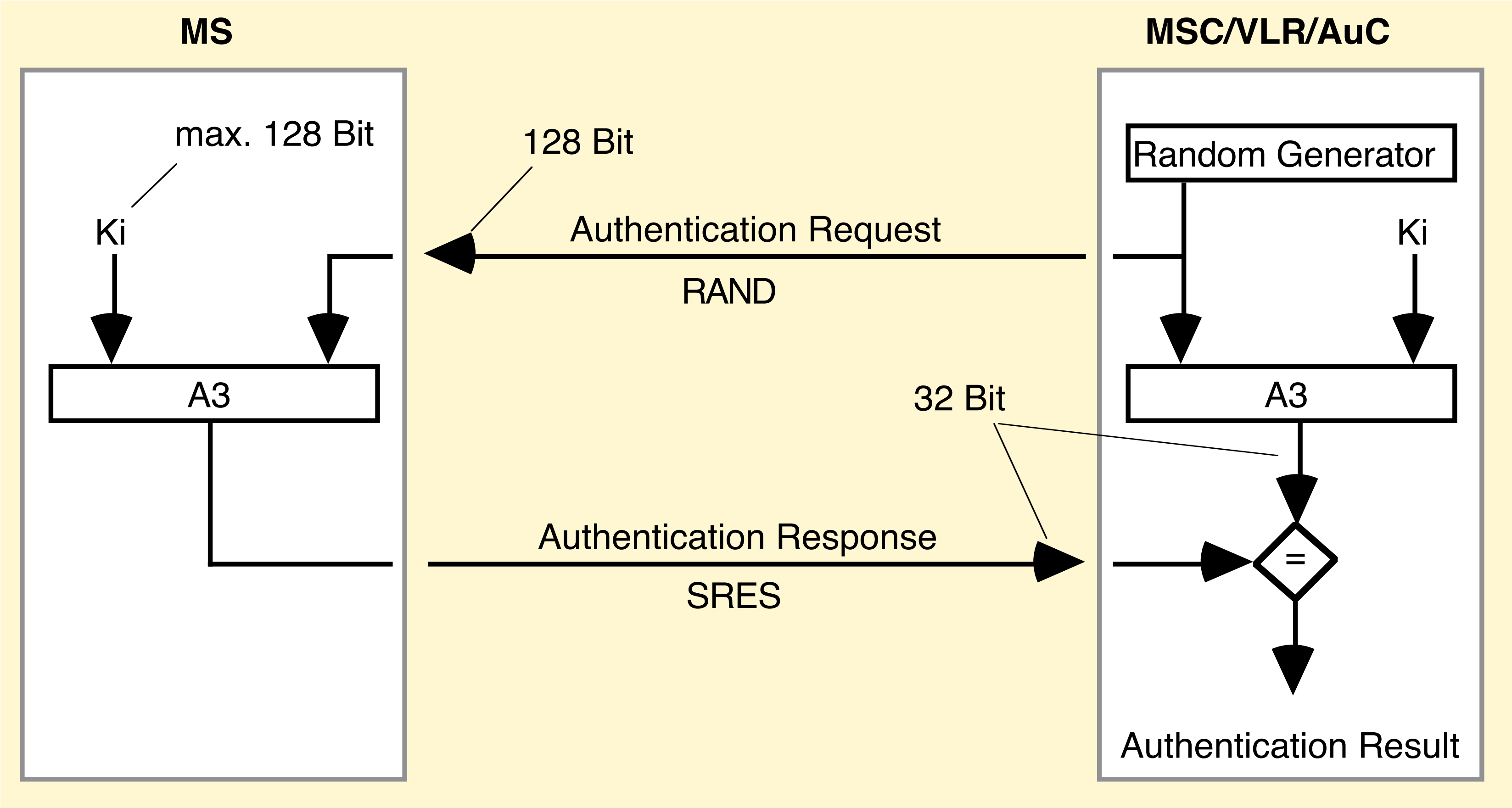
Security functions of GSM

- *Overview*
  - **Subscriber Identity Module** (SIM, smart card)
    - Admission control and crypto algorithms
  - **Authentication** (Mobile station network)
    - Challenge-Response-Authentication (A3)
  - **Pseudonymization of users** on the air interface
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Link encryption** on the air interface
    - Generation of session key: A8
    - Encryption: A5



Challenge-Response-Authentication

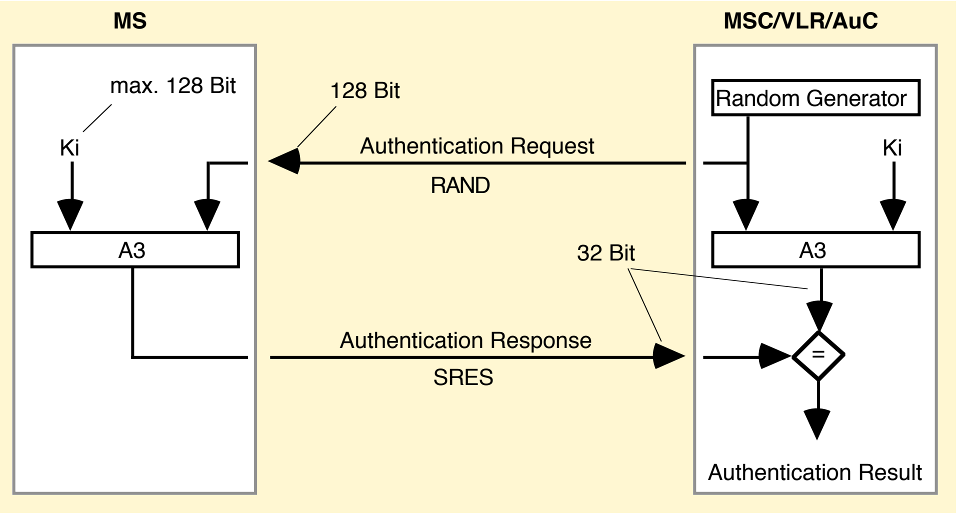
- ***When initialized by the mobile network?***
  - Location Registration
  - Location Update when changing the VLR
  - Call Setup (both directions)
  - Short Message Service
- ***Protocol***



Challenge-Response-Authentication

- *Algorithm A3*
  - Implemented on SIM card and in Authentication Center (AuC)
  - Cryptographic one way function A3:

    SRES’ = A3(Ki, RAND)   (Ki: individual user key)
  - Interfaces are standardized, cryptographic algorithm not standardized
- *Specific algorithm can be selected by the network operator*
  - Authentication data (RAND, SRES) are requested from AuC by the visited MSC
  - visited MSC: only compares SRES == SRES’
  - visited MSC has to trust home network operator



Attacks – Telephone at the expense of others

- ***SIM cloning***
  - –Weakness of authentication algorithm
- ***Interception of authentication data***
  - –Eavesdropping of internal communication links
- ***IMSI catcher***
  - –Man-in-the-middle attack on the air interface

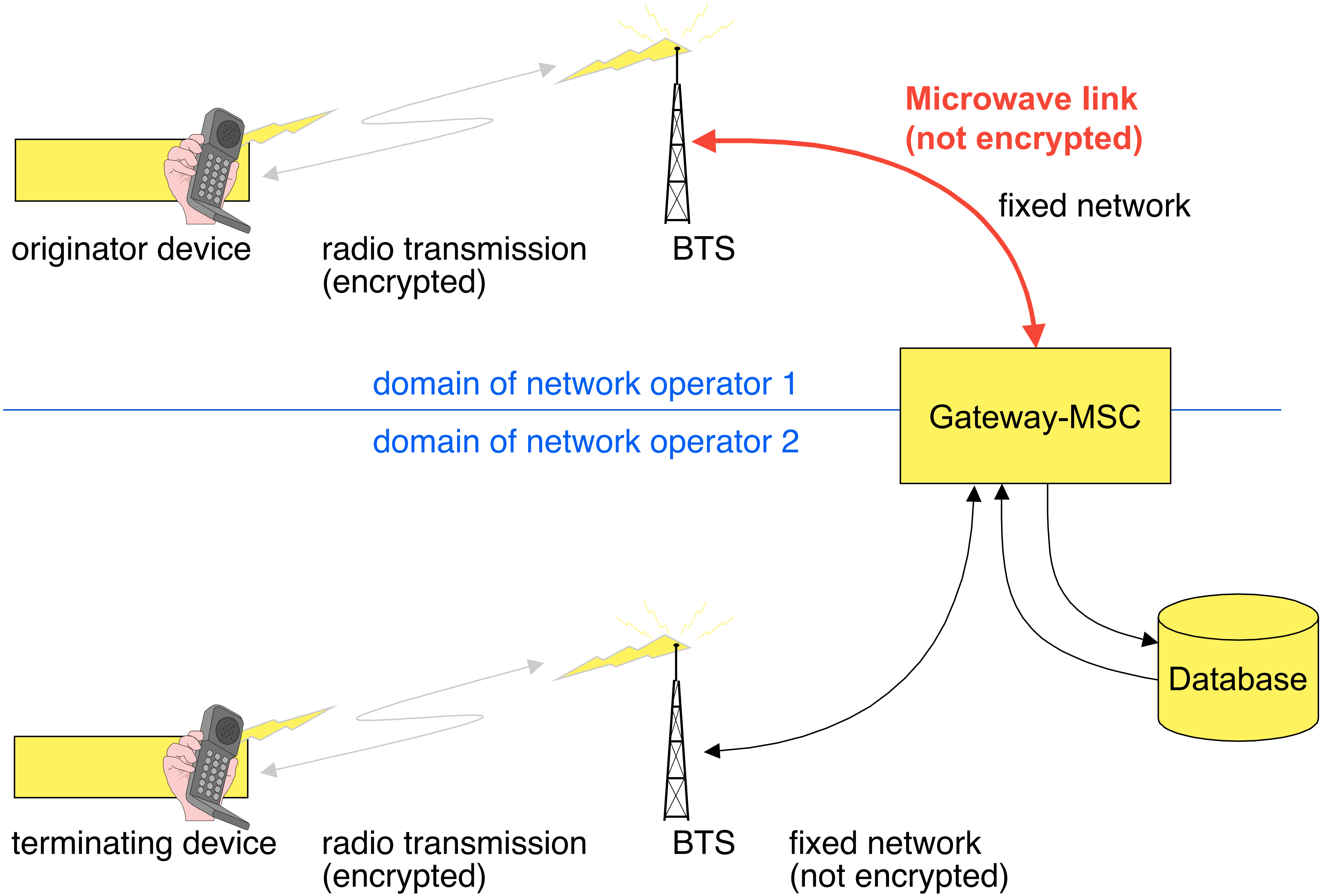
SIM cloning

- ***Scope***
  - Telephone at the expense of others
  - Described by Marc Briceno (Smart Card Developers Association), Ian Goldberg and Dave Wagner (both University of California in Berkeley)
  - http://www.isaac.cs.berkeley.edu/isaac/gsm.html
  - Attack uses a weakness of algorithm COMP128, which implements A3/A8
  - SIM card (incl. PIN) must be under control of the attacker for at least 8-12 hours
- ***Effort***
  - Approx. 150.000 calculations to determine Ki (max. 128 bit)
  - 6,25 calculations per second only, due to slow serial interface of SIM card

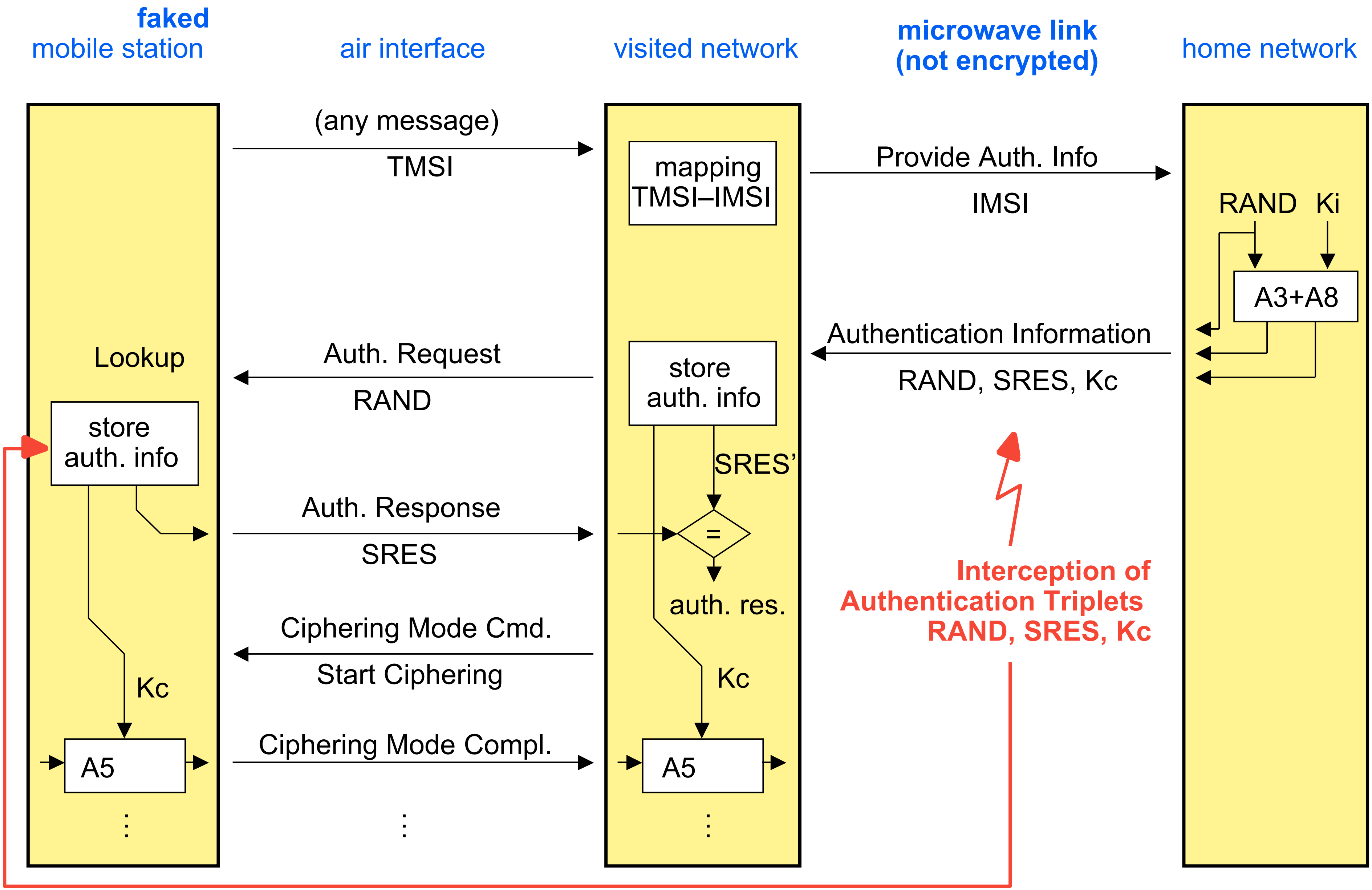
Interception of authentication data

- ***Scope***
  - Telephone at the expense of others
  - Described by Ross Anderson (University of Cambridge)
  - Eavesdropping of unencrypted internal transmission of authentication data (RAND, SRES) from AuC to visited MSC
- ***Weakness***
  - GSM standard only describes interfaces between network components.
  - They forgot the demand for internal encryption.
  - Microwave links are widely used for internal linkage of network components.

No encryption of internal links

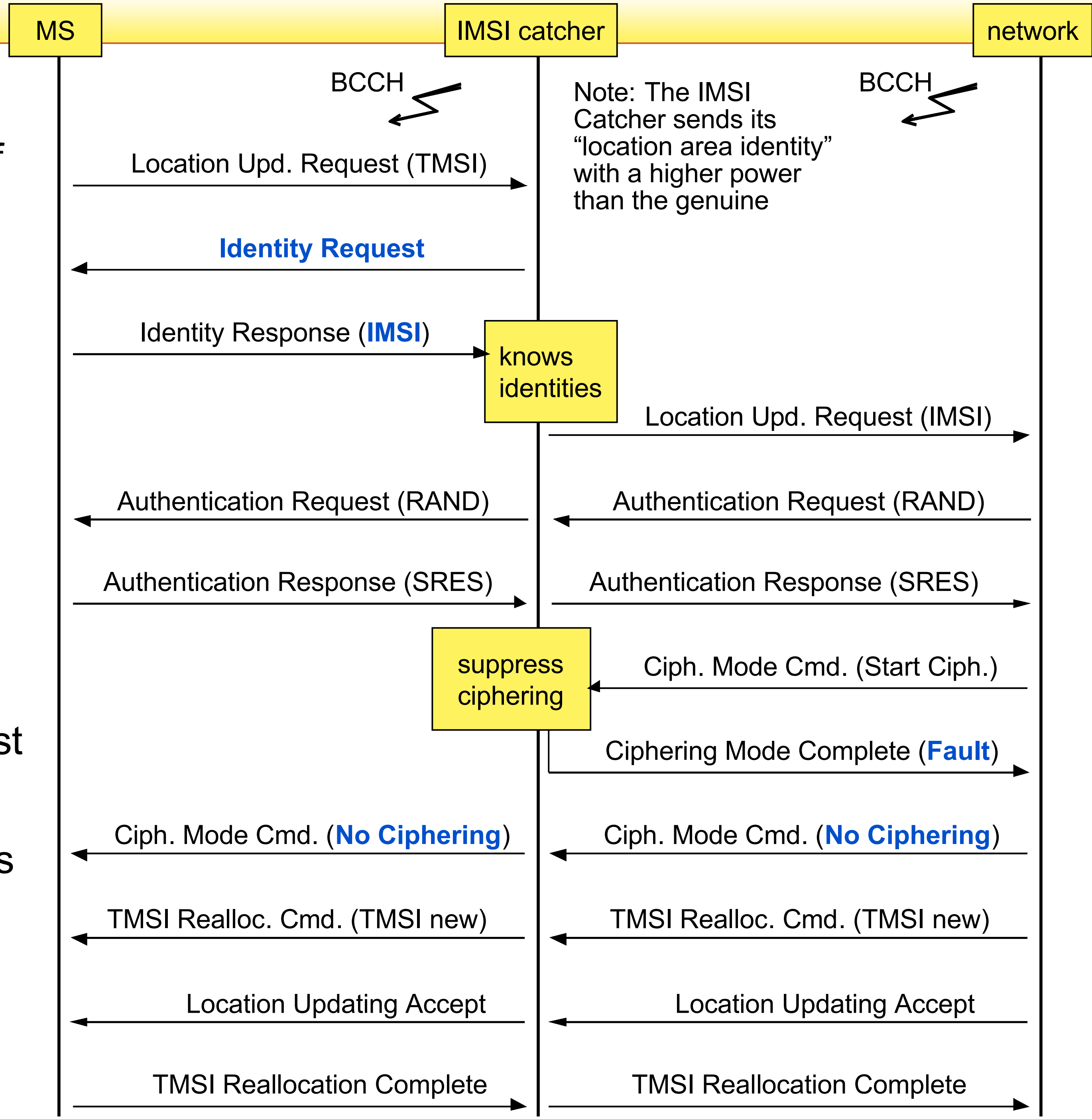


Interception of authentication data



IMSI-Catcher

- ***Scope***
  - Identities of users of a certain radio cell
  - Eavesdropping of communications
  - (Telephone at the expense of others)
- ***Man-in-the-middle attack (Masquerade)***
- ***Weakness***
  - No protection against malicious or faked network components



Universal mobile telecommunication system (UMTS)

- ***Security functions of UMTS …***

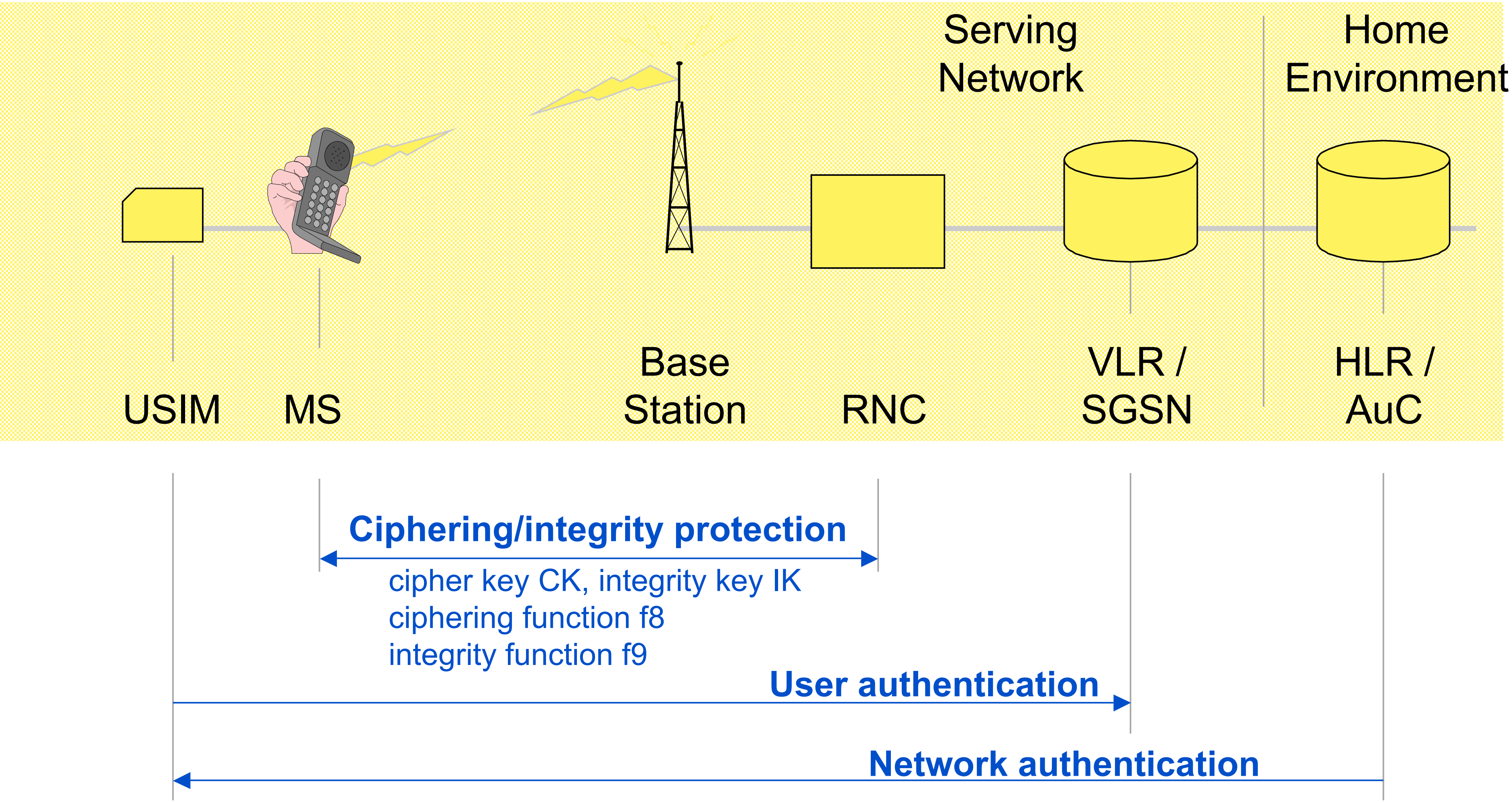
  … have been »inspired« by GSM security functions

- ***From GSM***
  - Subscriber identity confidentiality (TMSI)
  - Subscriber authentication
  - Radio interface encryption
  - SIM card (now called USIM)
  - Authentication of subscriber towards SIM by means of a PIN
  - Delegation of authentication to visited network
  - No need to adopt standardized authentication algorithms

- ***Additional UMTS security features***
  - Enhanced UMTS authentication and key agreement mechanism
  - Integrity protection of signaling information (prevents false-base-station attacks)
  - New ciphering / key agreement / integrity protection algorithms

  … and a few minor features

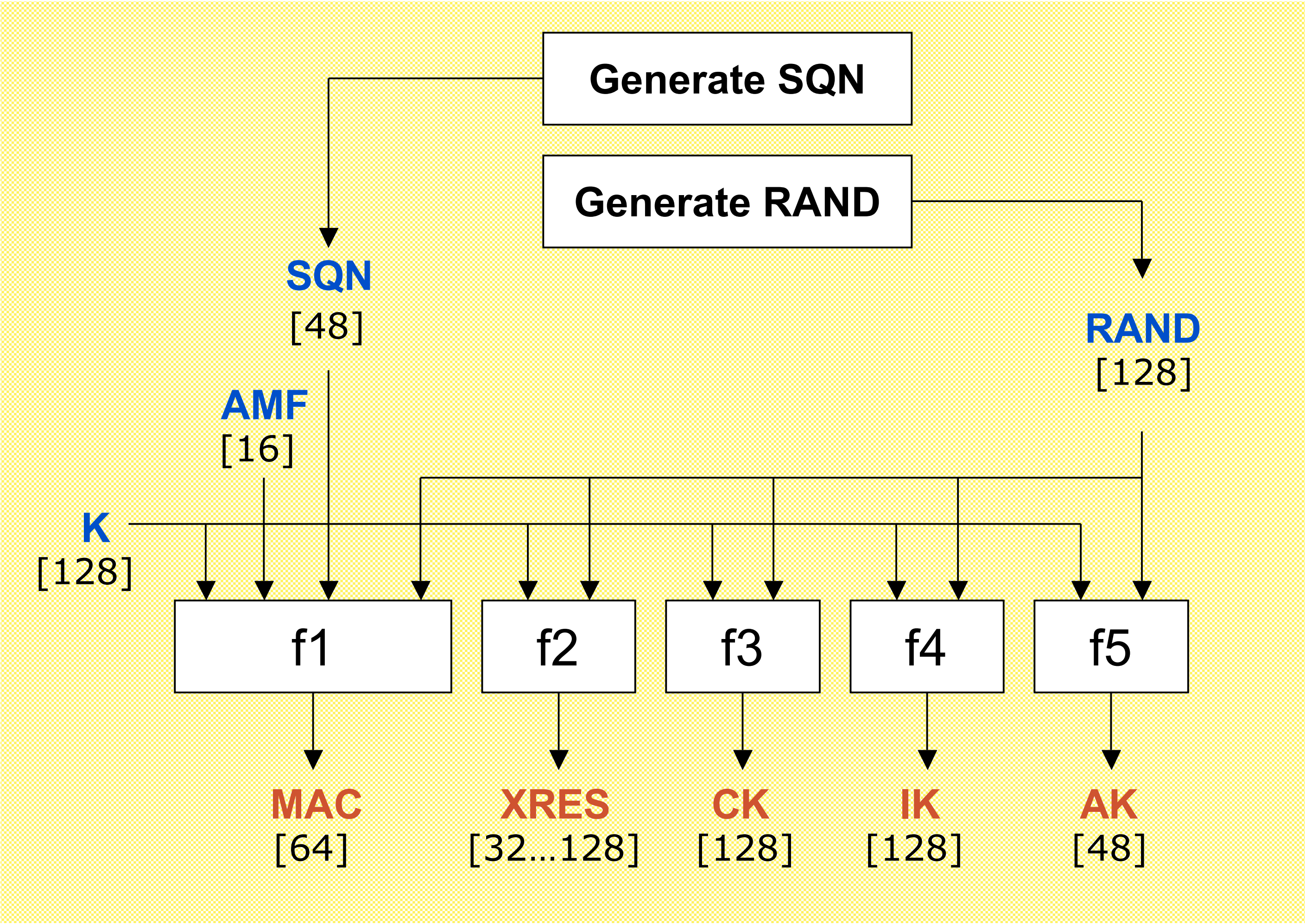
UMTS Security Architecture



authentication key K,
authentication function f1, f2
key generation function f3, f4, f5
sequence number management SQN

USIM	UMTS Subscriber Identity Module
MS	Mobile Station
RNC	Radio Network Controller
VLR	Visitor Location Reg.
SGSN	SG Serving Network
HLR	Home Location Register
AuC	Authentication Centre

Generation of authentication vectors

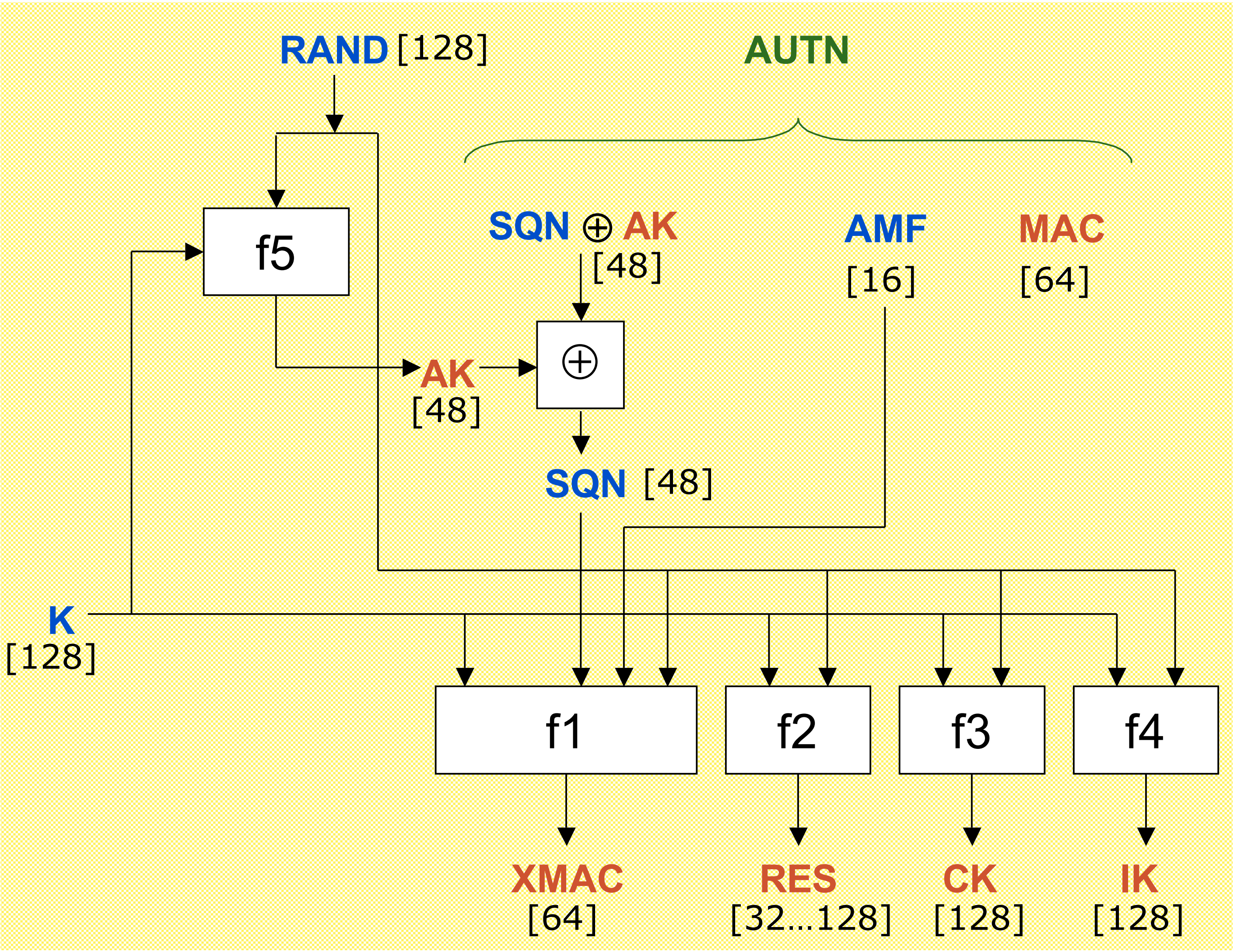


SQN	Sequence number
RAND	Random number
AMF	Authenticated Management Field
K	Secret Key
MAC	Message authen-tication code
XRES	Expected response
CK	Cipher key
IK	Integrity key
AK	Anonymity key
AUTN	Authentication token
AV	Authentication vector
[...]	# of bits

AUTN := SQN ⊕ AK || AMF || MAC

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

Authentication function in the USIM

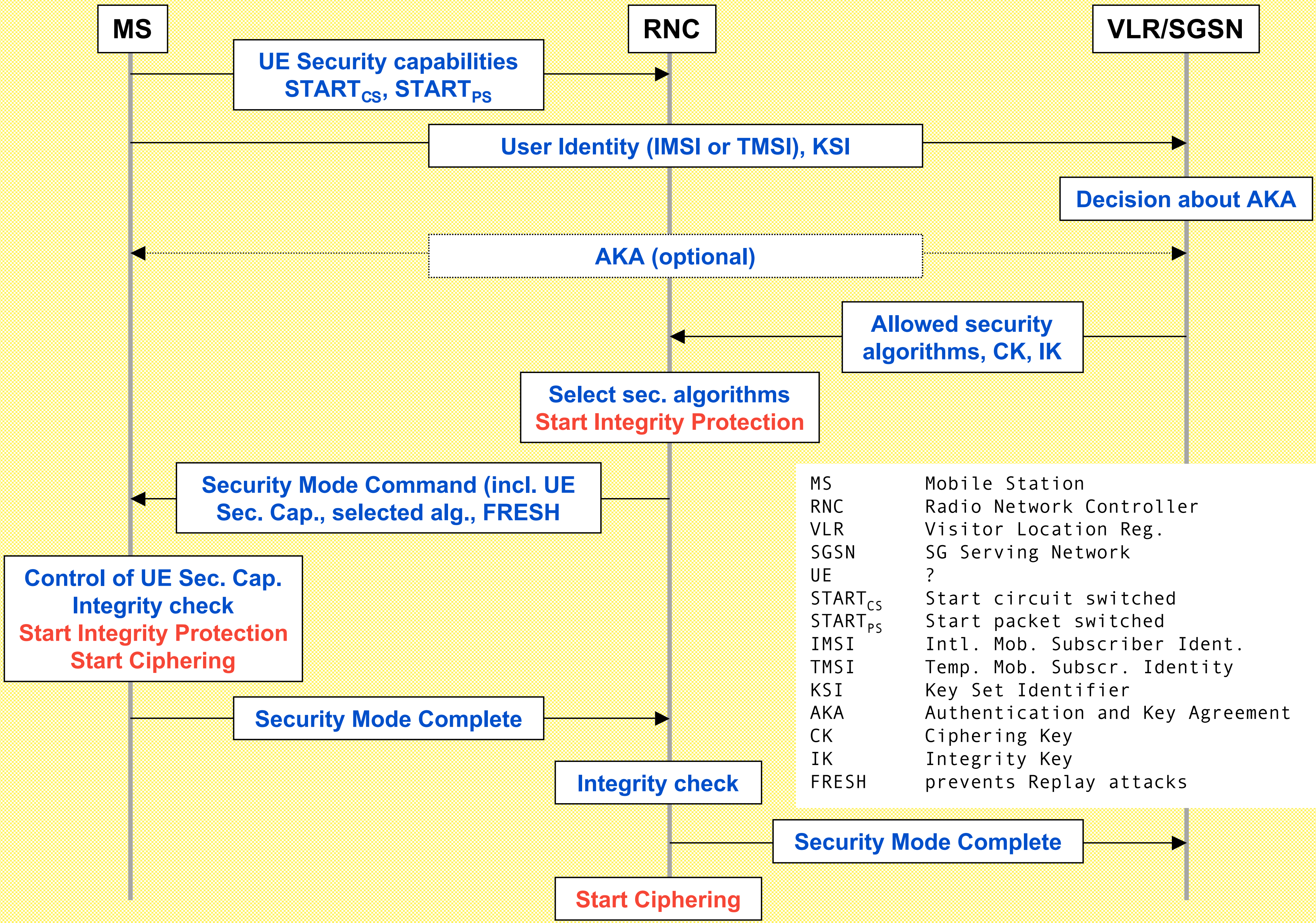


SQN	Sequence number
RAND	Random number
AMF	Authenticated Management Field
K	Secret Key
MAC	Message authen-tication code
XMAC	*Expected MAC*
RES	*Response*
CK	Cipher key
IK	Integrity key
AK	Anonymity key
AUTN	Authentication token
[…]	# of bits

Verify MAC == XMAC

Verify that SQN is in the correct range

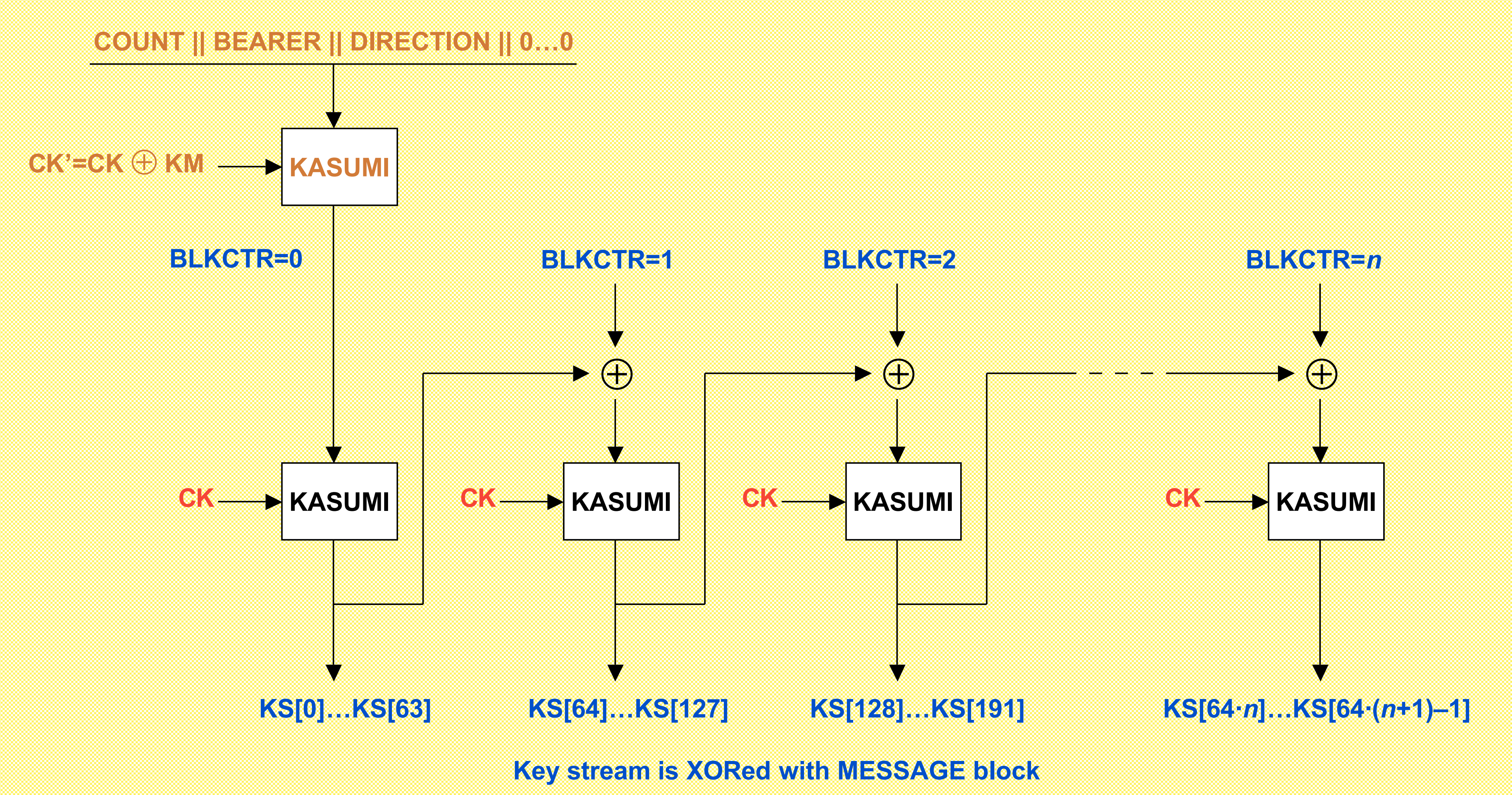
Security mode setup procedure



MS	Mobile Station
RNC	Radio Network Controller
VLR	Visitor Location Reg.
SGSN	SG Serving Network
UE	?
$START_{CS}$	Start circuit switched
$START_{PS}$	Start packet switched
IMSI	Intl. Mob. Subscriber Ident.
TMSI	Temp. Mob. Subscr. Identity
KSI	Key Set Identifier
AKA	Authentication and Key Agreement
CK	Ciphering Key
IK	Integrity Key
FRESH	prevents Replay attacks

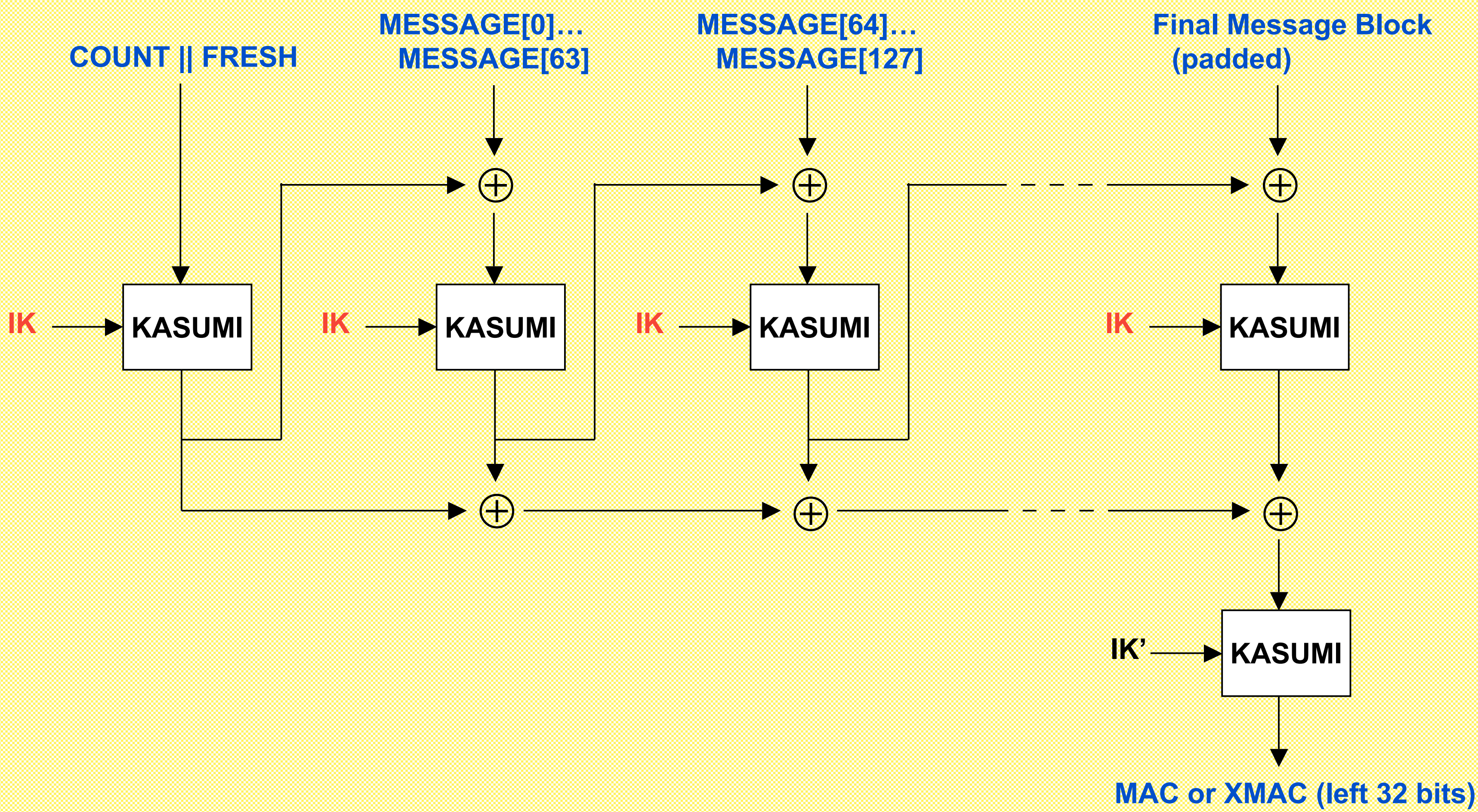
Cipher algorithm f8

- Combination of Output Feedback mode (OFB) and counter mode
- First encryption under CK’ prevents chosen plaintext attacks (initialization vector is encrypted, KM: key modifier)



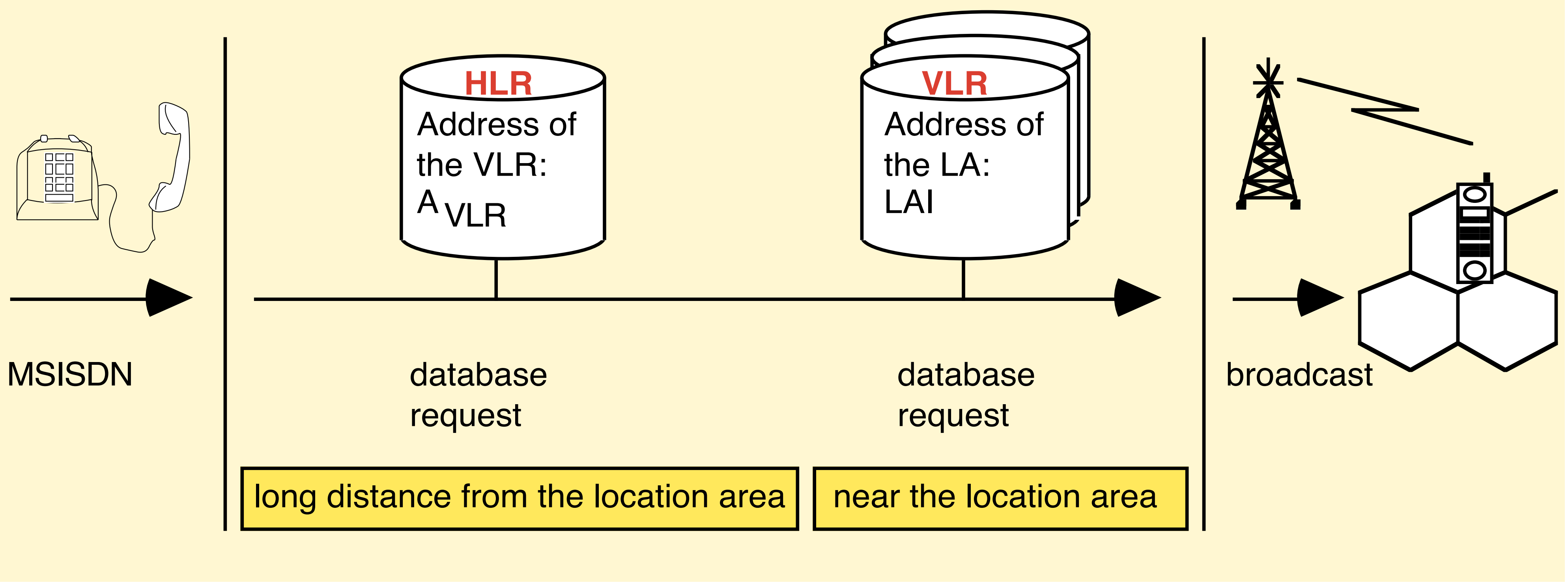
Integrity algorithm f9

- ISO/IEC 9797-1 (MAC algorithm 2)
- Sender and receiver use f9
- Receiver verifies MAC == XMAC



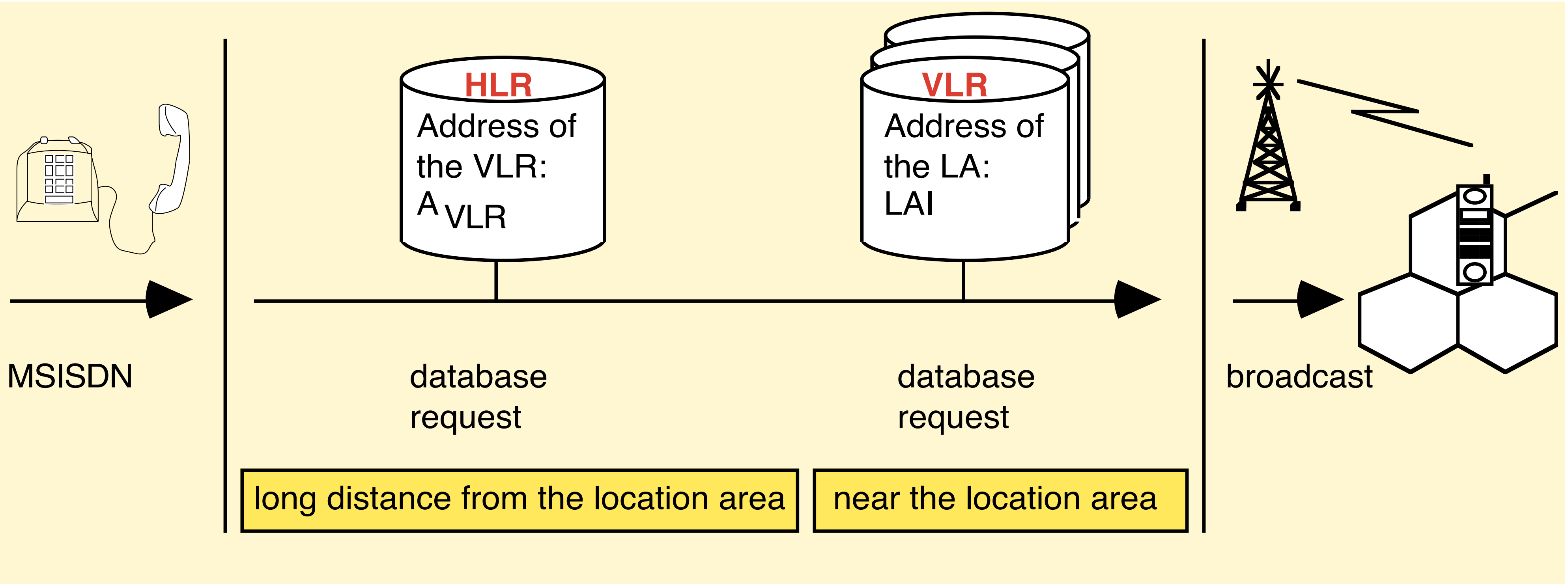
Protection of locations

- ***Mobile user***
  - whishes to be reachable at his current location.
  - He won't be localizable by outsiders and the network operator unless the explicitly gives his permission
- ***There is no mobile network that fulfills this demand.***



Protection of locations

- ***GSM (Global System for Mobile Communication)***
  - Distributed storage at location registers
    - Home Location Register (HLR)
    - Visitor Location Register (VLR)
  - Network operator has global view on location information
- ***Tracking of mobile users is possible***



Systematic: Protection of locations

A. Trust into the mobile station only

A.1 Broadcast method

A.2 Group pseudonyms

B. Additional trust into a private fixed station

B.1 Trusted address translation and broadcast

B.2 Reduction of broadcast areas

B.3 Explicit trustworthy storage of locations

B.4 Temporary pseudonyms (TP method)

C. Additional trust into a trusted third party

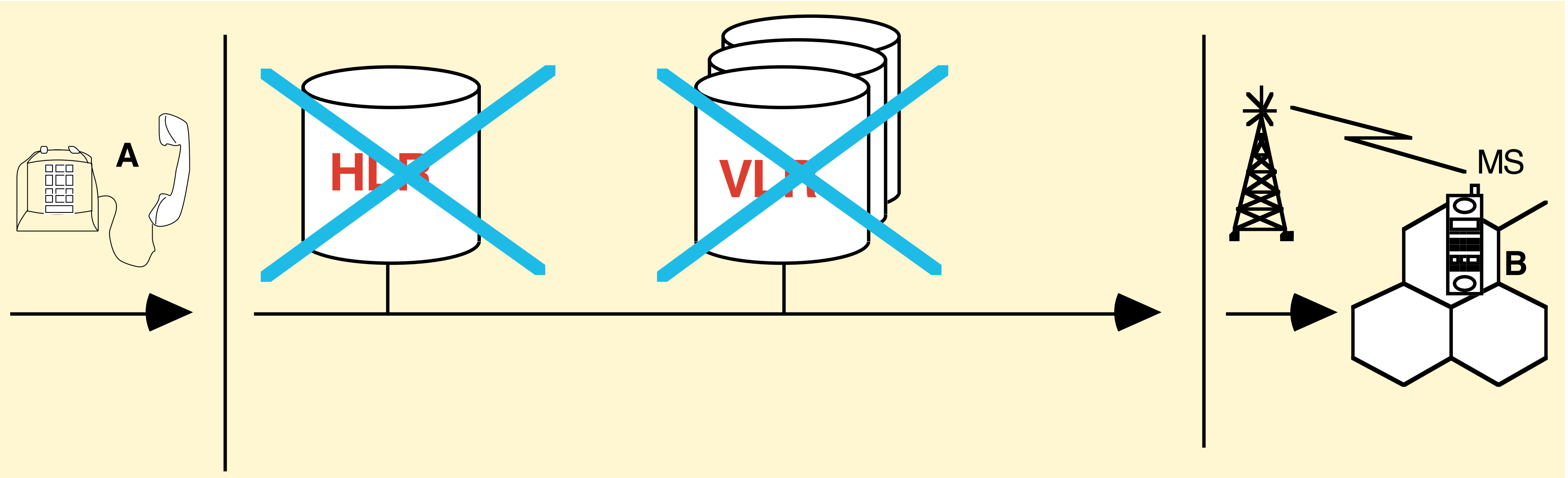
C.1 Trust Center

C.2 Co-operating chips

C.3 Mobile Communication-MIXing

Overview: Broadcast

- *No storage of locations and global paging of mobile users*

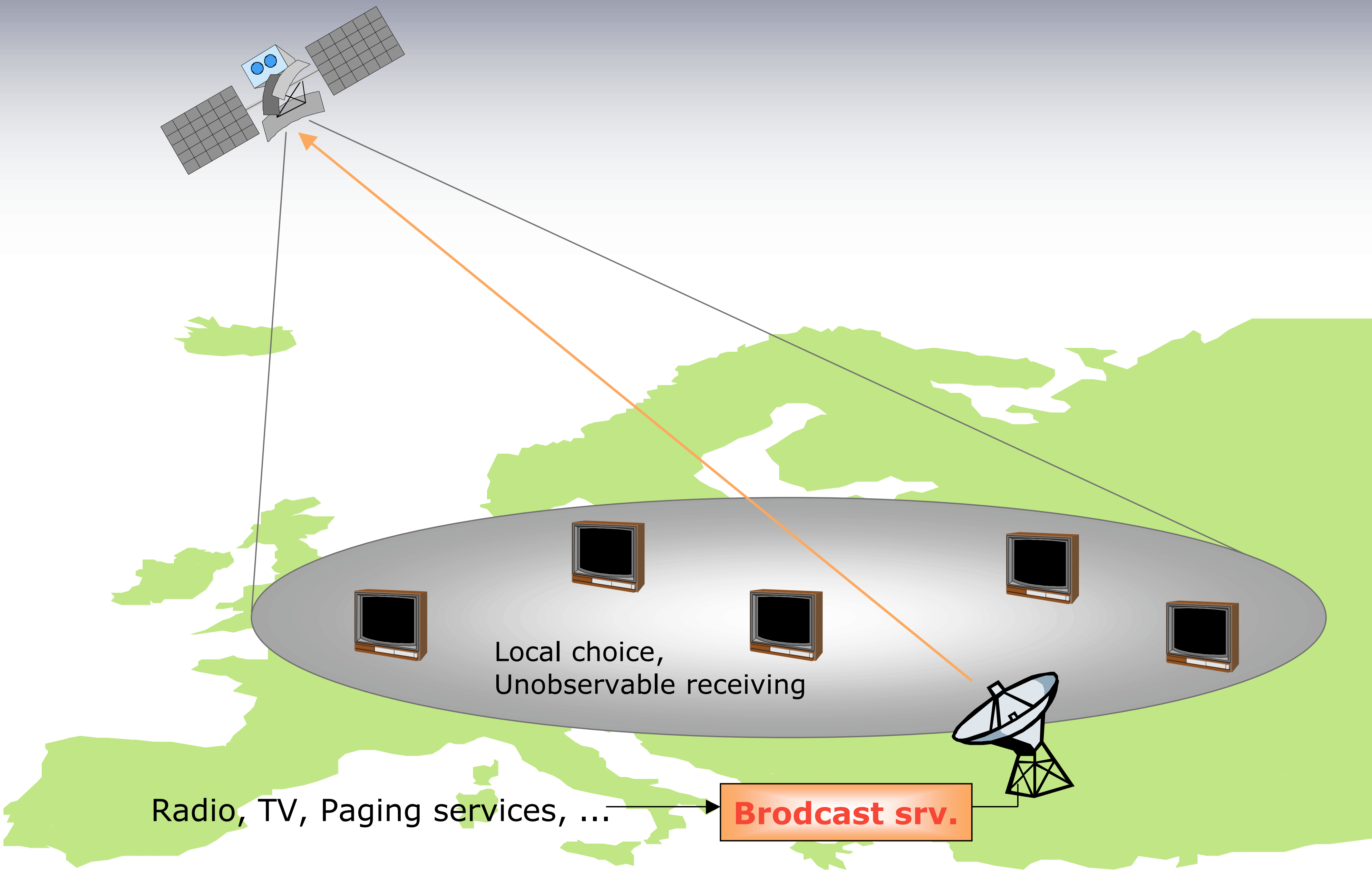


Overview: Broadcast

- *No storage of locations and global paging of mobile users*

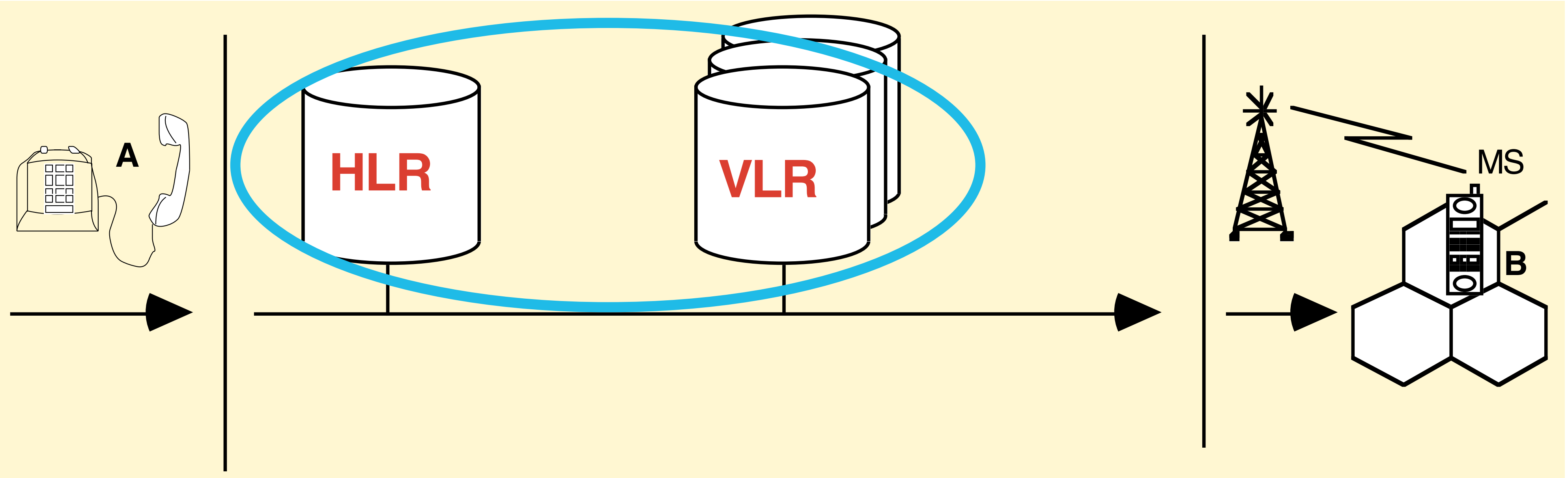
- *Immense costs for bandwith …*

Broadcast in general



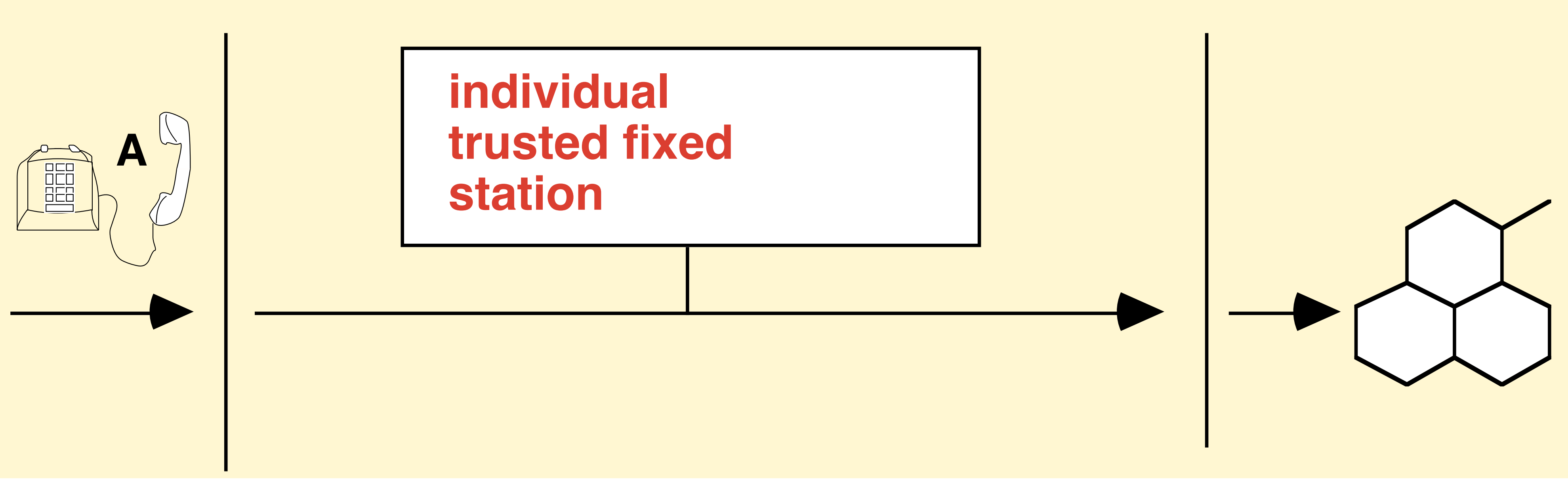
Overview : Trustworthy storage

- *Replace databases by trusted devices in the fixed network*



Overview : Trustworthy storage

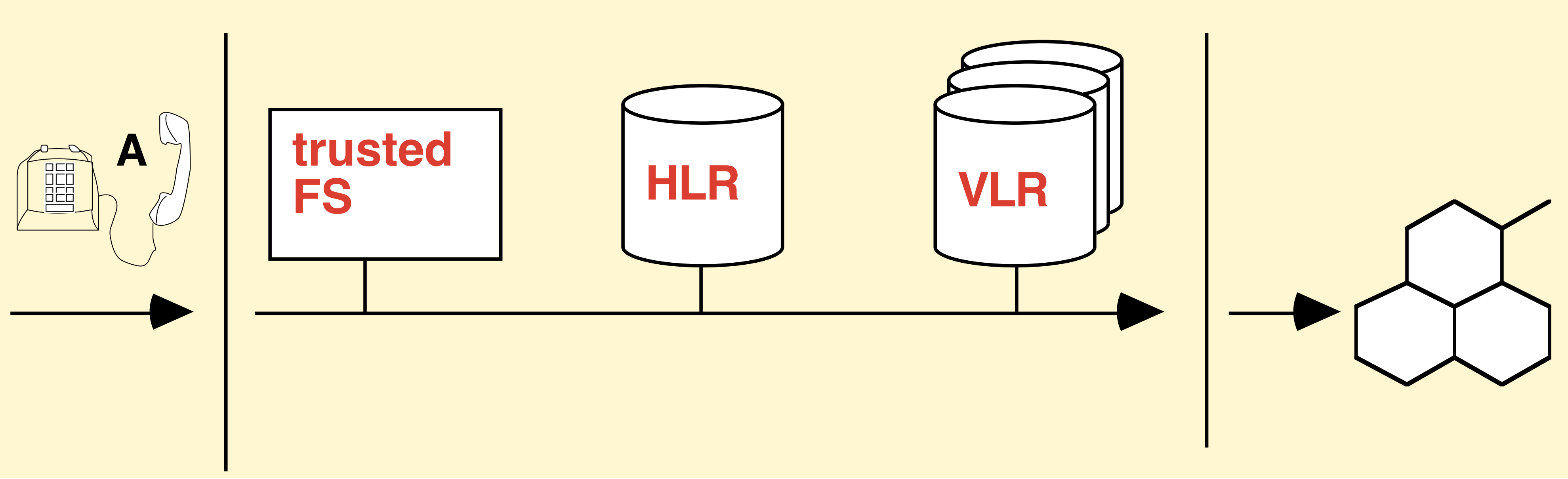
- *Replace databases by trusted devices in the fixed network*



- *Every location updating needs communication with trusted station.*
- *Question: How can we reduce cost of location updating?*

Overview : Trustworthy storage

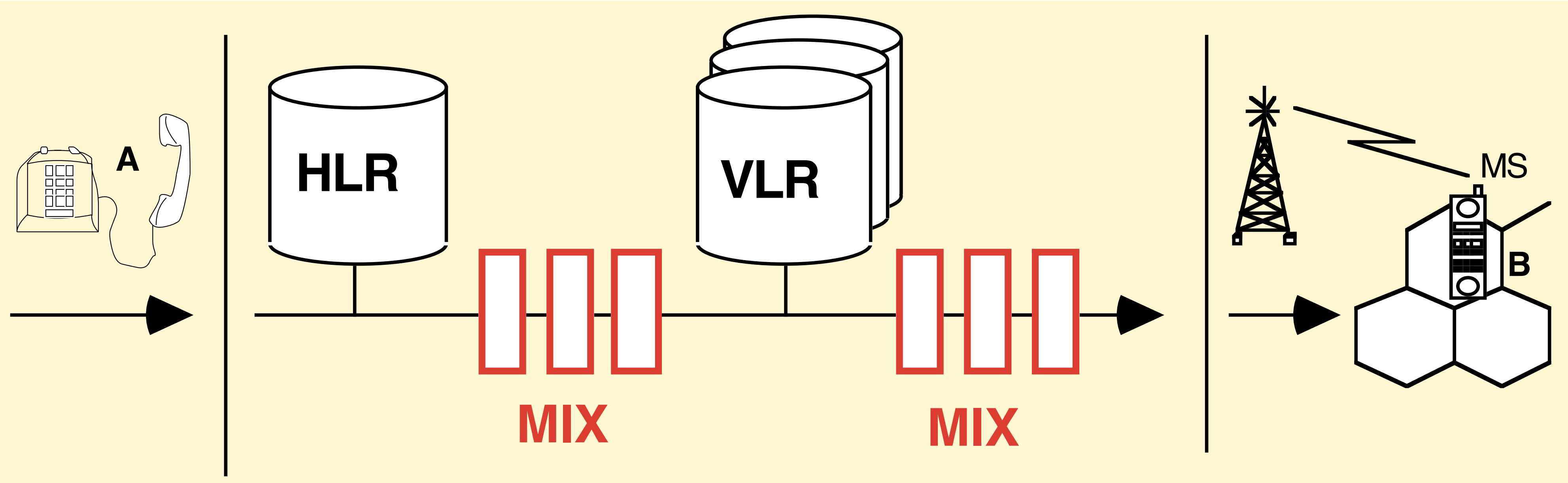
- *Tempory Pseudonyms (TP method)*



- *Can we do this without a trusted fixed station?*

Overview : Mobile Communication-MIXing

- *Covered storage of location information*



- *A MIX hides the communication relation between*
  - HLR and VLR
  - VLR and location area

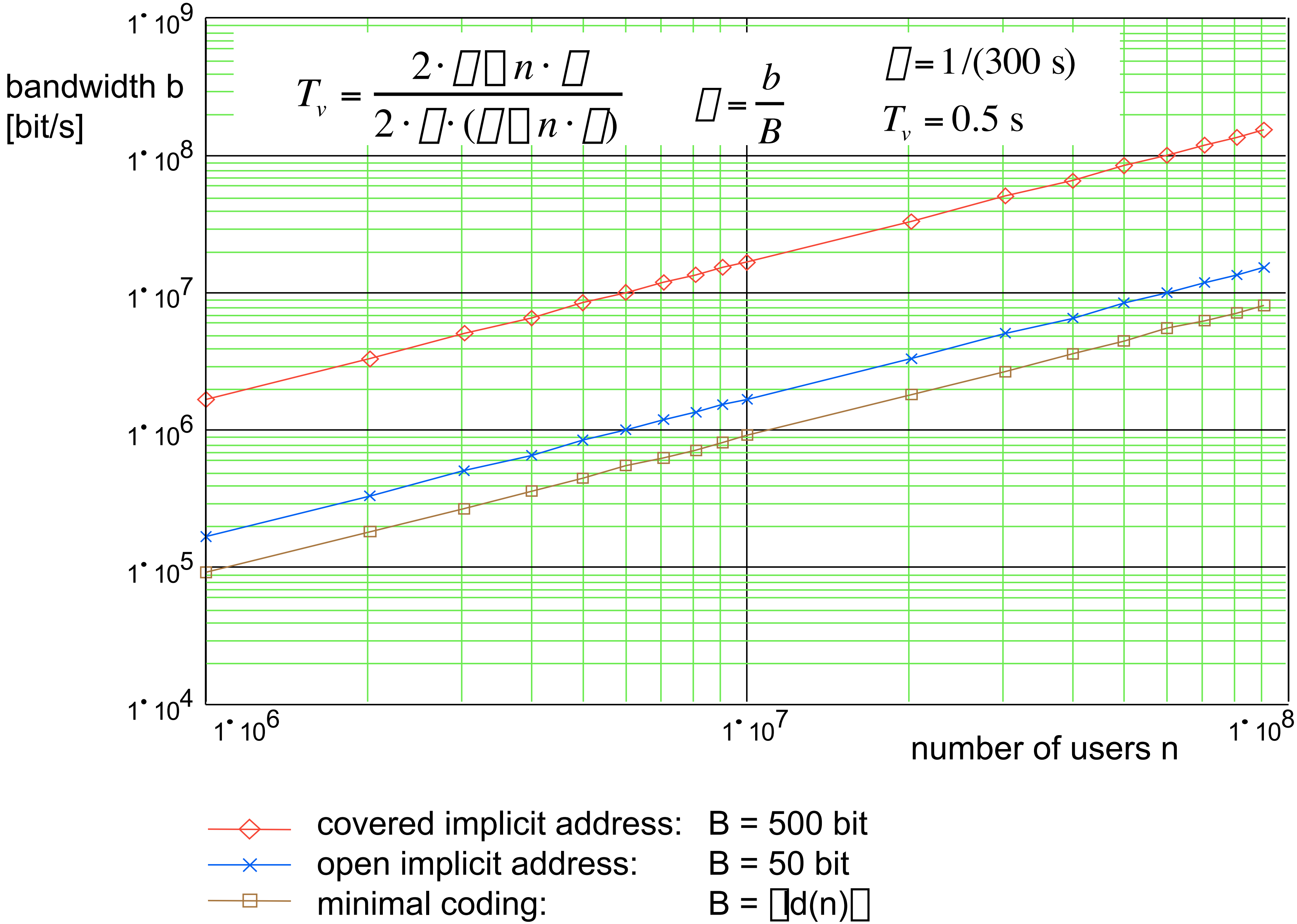
Implicit Addresses

- ***First contact:*** ***Covered Implicit Address CIA***
  - Recipient publishes public encryption key **c**
  - Sender creates **CIA := c(R,S,M)**
    - Redundancy **R**
    - Seed **S** of a pseudo-random generator **PRG**
    - Message **M** (optional, may contain symmetric key **k**)
  - Recipient decrypts *all* received messages with private key **d**
    - Finds correct **R** for own messages only

- ***Following addressing:*** ***Open Implicit Address OIA***
  - **OIA_{i+1} := PRG(i,seed)** (i = 0,1,2,…)
  - Sender :
    - calculates next **OIA**
    - encrypts message (optional) **M** under k
    - Sends **OIA, M**
  - Receiver: Associative memory of all valid **OIA**s to recognize own messages

Broadcast method

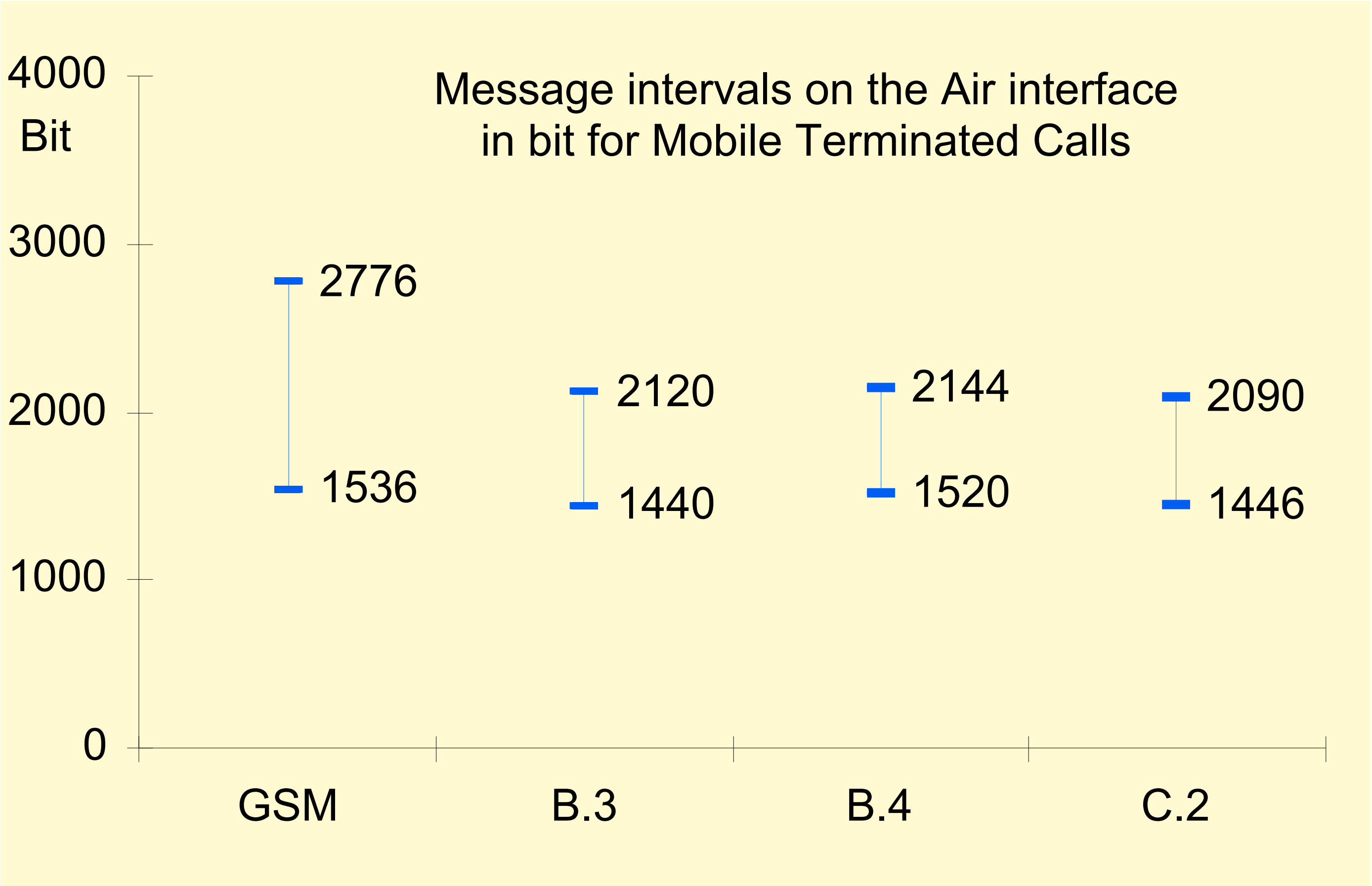
- *Performance*



Performance: Message lengths on the air interface

- ***Mobile Terminated Calls***

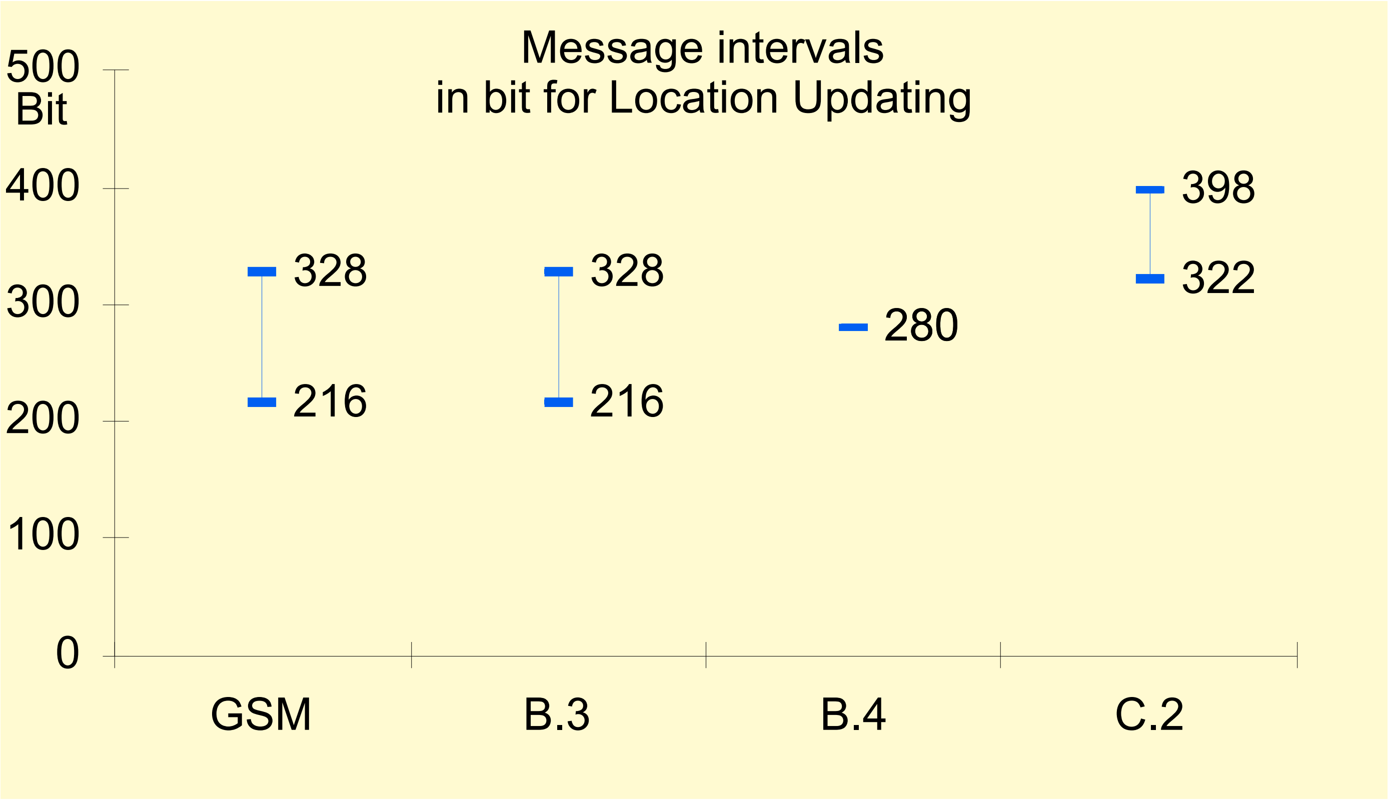
GSM	reference
B.3	explicit trustworthy storage
B.4	TP method
C.2	cooperating chips



Performance: Message lengths on the air interface

- ***Location Update***

GSM reference
B.3 explicit trustworthy storage
B.4 TP method
C.2 cooperating chips



Security of mobile communication

- *Conclusion*
  - Protection of locations can be technically realized
  - However, there is a demand for legal enforcement
- *More information*
  - http://www.inf.tu-dresden.de/~hf2/mobil/