



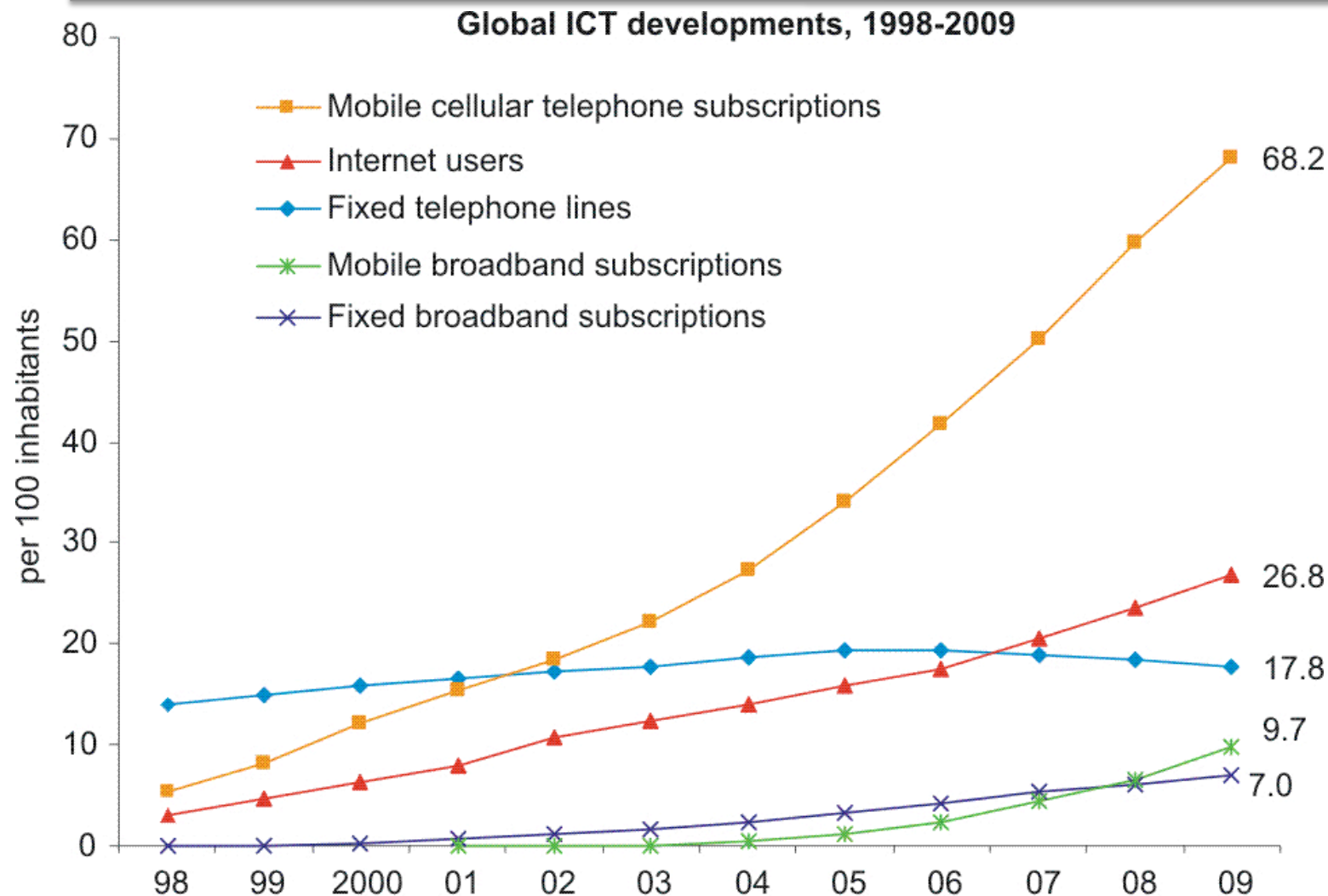
---

# Mobile and Sensor Systems

## Lecture 3: Telecommunication Systems

**Dr. Cecilia Mascolo**

# Mobile Phone Subscribers



Source: ITU World Telecommunication/ICT Indicators database.

# Telecomms Stats & GSM



- July 2010 (gsmworld.com): The GSMA announced that the number of global mobile connections has surpassed the 5 billion mark, according to new data from mobile industry analysis firm Wireless Intelligence. The achievement comes just 18 months after the 4 billion connection milestone was reached at the end of 2008, and Wireless Intelligence is predicting that the mobile industry will reach 6 billion global connections in the first half of 2012.
- GSM
  - formerly: Groupe Spéciale Mobile (founded 1982)
  - now: Global System for Mobile Communication
- Today many providers all over the world use GSM (219 countries in Asia, Africa, Europe, Australia, America)
  - more than 75% of all digital mobile phones use GSM

# How does it work?



- How can the system locate a user?
- Why don't all phones ring at the same time?
- What happens if two users talk simultaneously?
- Why don't I get the bill from my neighbor?
- Why can an Australian use her phone in Berlin?

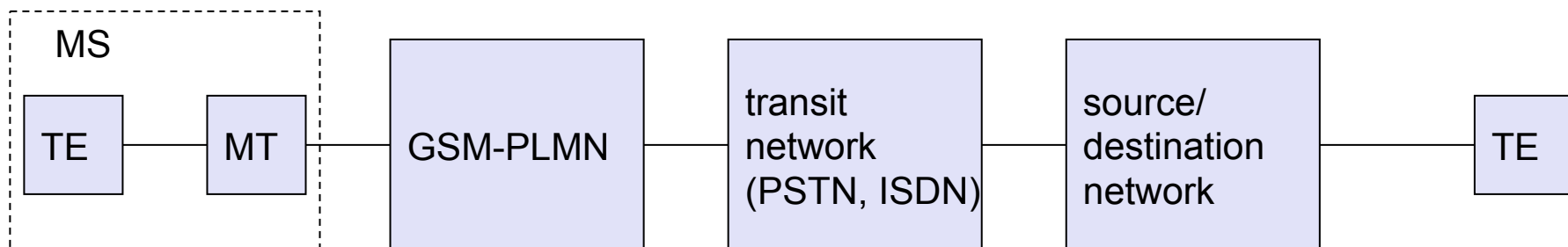


- Why can't I simply overhear the neighbor's communication?
- How secure is the mobile phone system?
- What are the key components of the mobile phone network?

# GSM: Mobile Services



- GSM offers
  - several types of connections
    - voice connections, data connections, short message service
    - multi-service options (combination of basic services)
- Three service domains
  - Bearer Services
  - Telematic Services
  - Supplementary Services (not discussed)



# Bearer Services



- Telecommunication services to transfer **data**
  - This service is the one which needed to change most given the importance that data transfer is acquiring
- Specification of services up to the terminal interface (OSI layers 1-3)
- Original standard:
  - data service (circuit switched or packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s
  - Low rates assuming data is a small proportion of the traffic!!
- Today: data rates of approx. 50 kbit/s possible, given the importance of data transmission

# Tele Services I



- Telecommunication services enable **voice** communication on mobile phones
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
  - mobile telephony  
primary goal of GSM was to enable mobile telephony offering the traditional analog bandwidth of 3.1 kHz
  - Emergency number  
common number throughout Europe; mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)

# Tele Services II



- Additional services
  - Non-Voice-Teleservices
    - group 3 fax
    - voice mailbox (implemented in the fixed network supporting the mobile terminals)
    - electronic mail (MHS, Message Handling System, implemented in the fixed network)
    - ...
    - **Short Message Service (SMS)**  
alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS  
**(almost ignored in the beginning now the most successful add-on!:** *note that it does not use the data service but the voice channels)*



# Ingredients 1: Mobile Phone

---



The visible but **smallest part** of the network!

# Ingredients 2: Antennas



Still visible – cause many discussions...

# Ingredients 3: Infrastructure 1



Base Stations



Microwave links

Cabling





# Ingredients 3: Infrastructure 2



Switching units



Management  
Data bases

Not „visible“, but comprise  
the **major part** of the network  
(also from an investment  
point of view...)



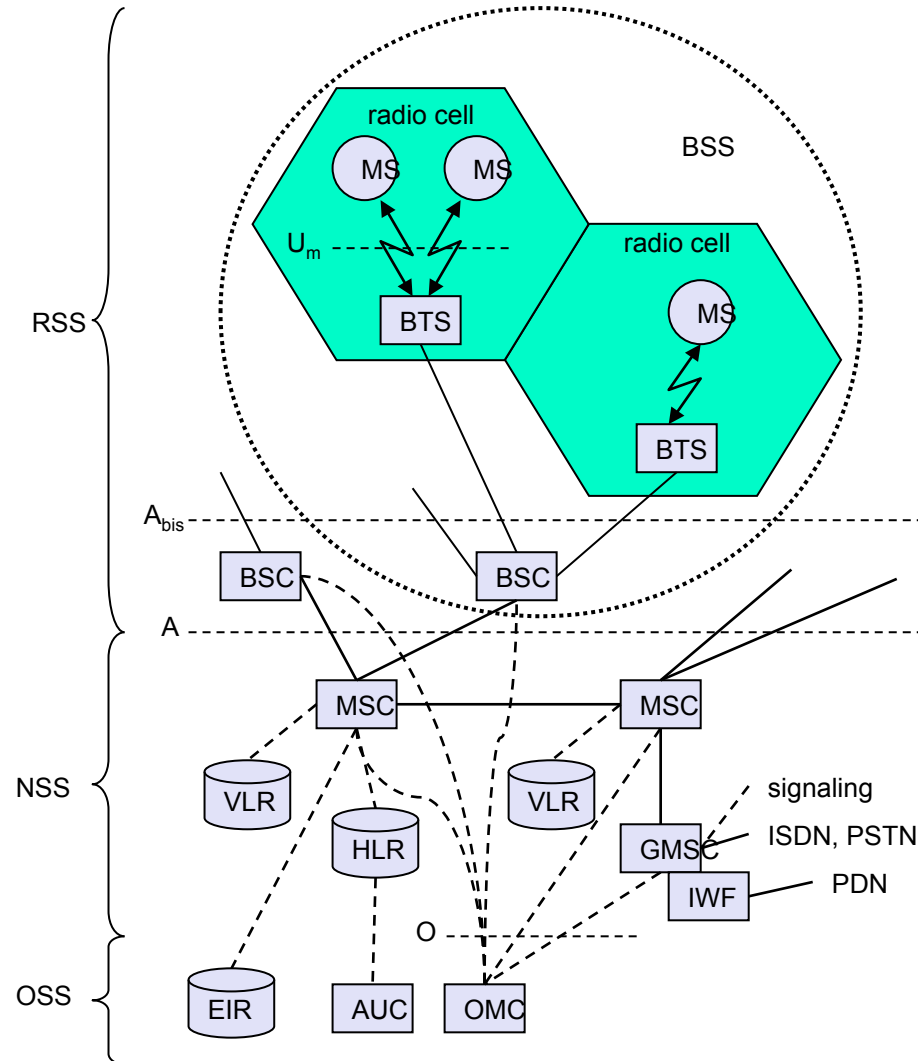
Monitoring

# Architecture of the GSM system

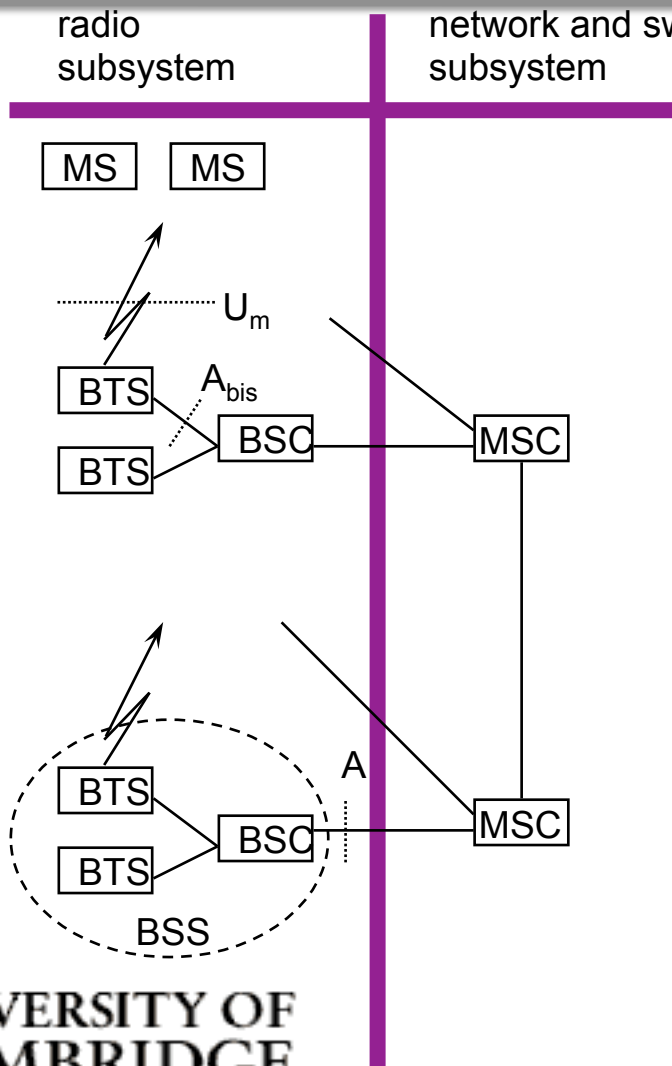


- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

# GSM: elements and interfaces



# System architecture: radio subsystem



- **Components**
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- **Interfaces**
  - $U_m$  : radio interface
  - $A_{bis}$  : standardized, open interface with 16-64 kbit/s user channels
  - $A$  : standardized, open interface with 64 kbit/s user channels

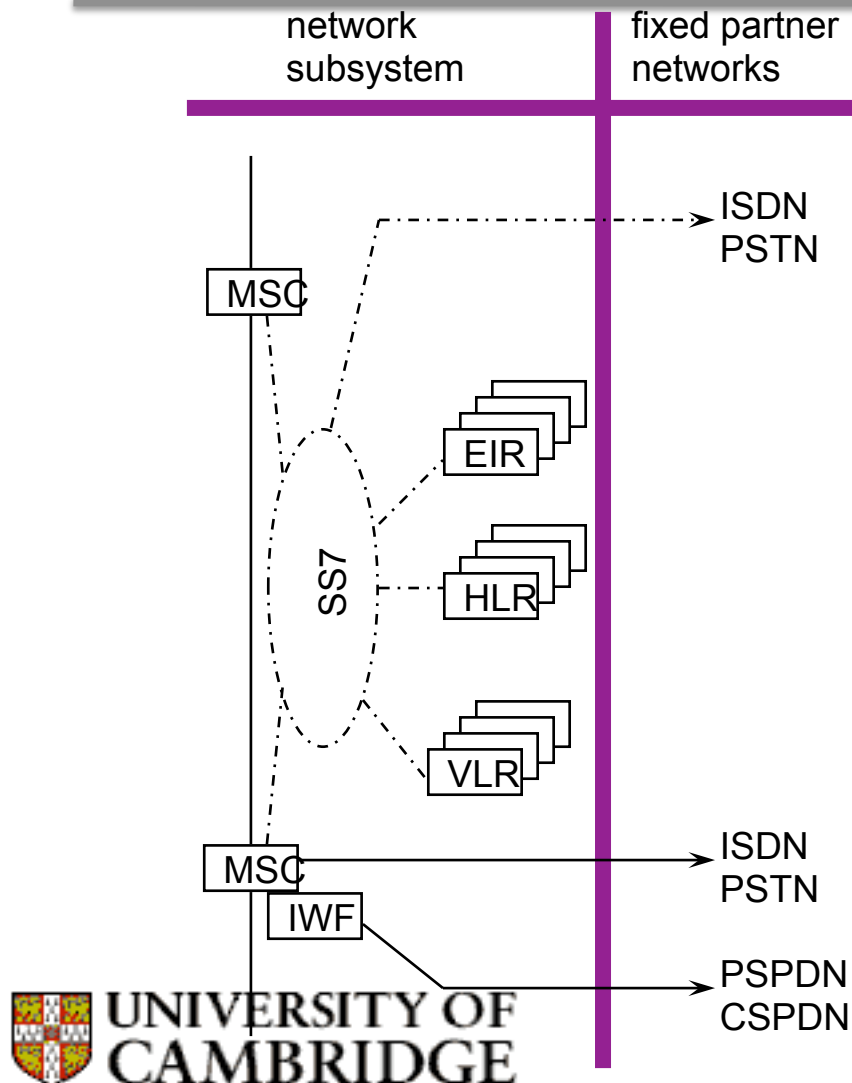
# Radio subsystem



- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels ( $U_m$ ) onto terrestrial channels (A interface)
  - Mobile Stations (MS)



# System architecture: network and switching subsystem



## • Components

- MSC (Mobile Services Switching Center):
- IWF (Interworking Functions)
- ISDN (Integrated Services Digital Network)
- PSTN (Public Switched Telephone Network)
- PSPDN (Packet Switched Public Data Net.)
- CSPDN (Circuit Switched Public Data Net.)

## • Databases

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- EIR (Equipment Identity Register)
- SS7: covers routing within the network and connectivity

# Network and switching subsystem

---



- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - Mobile Services Switching Center (MSC)  
controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)  
central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)  
dynamic and local database for a subset of user data, including data about all user currently in the domain of the VLR. VLRs avoid continuous access to HLR

# Operation subsystem

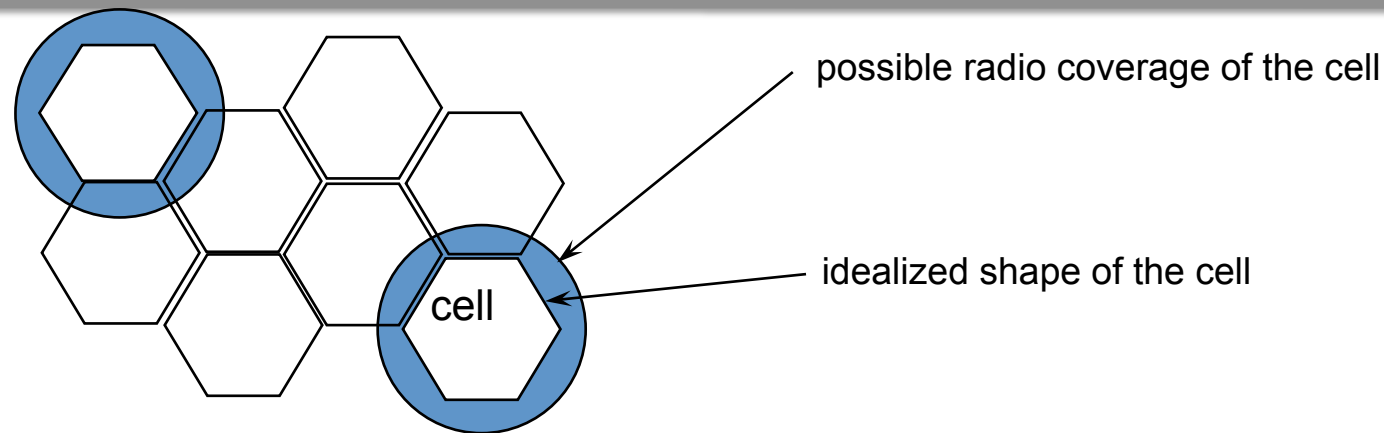


- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

# GSM: cellular network



segmentation of the area into cells



- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells handover of the connection to the neighbor cell

# Base Transceiver Station and Base Station Controller



- Tasks of a BSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

| Functions                                  | BTS | BSC |
|--|-----|-----|
| Management of radio channels               |     | X   |
| Frequency hopping (FH)                     | X   | X   |
| Management of terrestrial channels         |     | X   |
| Mapping of terrestrial onto radio channels |     | X   |
| Channel coding and decoding                | X   |     |
| Rate adaptation                            | X   |     |
| Encryption and decryption                  | X   | X   |
| Paging                                     | X   | X   |
| Uplink signal measurements                 | X   |     |
| Traffic measurement                        |     | X   |
| Authentication                             |     | X   |
| Location registry, location update         |     | X   |
| Handover management                        |     | X   |

# Storing Information of Users

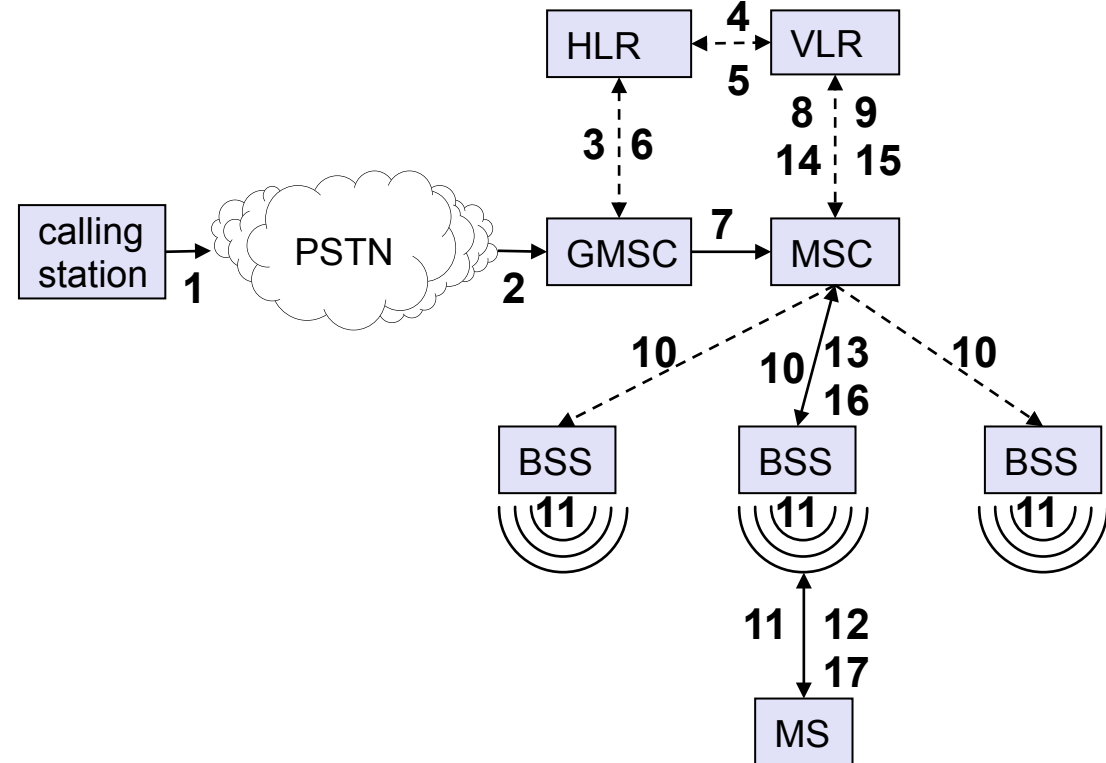


- The Home location register (HLR) stores the mobile ISDN number, international subscriber identity but also location area (LA) and the mobile subscriber roaming number (MSRN), the current VLR and MSC.
- Information is updated when user leaves the LA
- The Visitor location register (VLR) is associated to each MSC and is dynamic: stores same info as HLR copying it from HLR as soon as a users comes into the LA. It avoids frequent access to HLR.

# Mobile Terminated Call



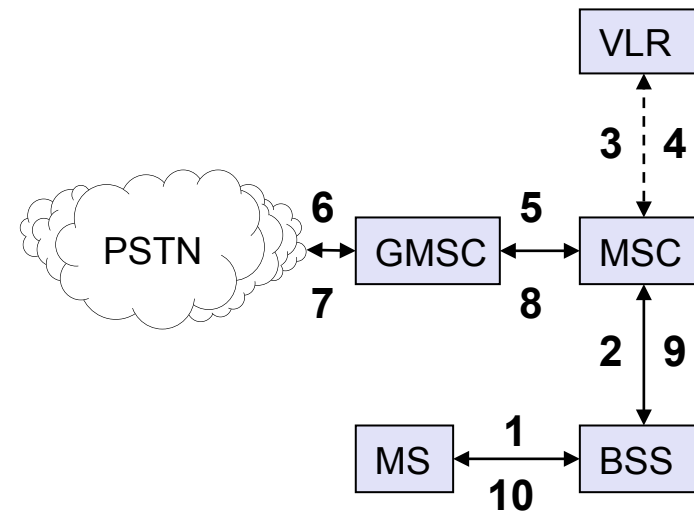
- 1: calling a GSM subscriber
- 2: forwarding call to Gateway MSC
- 3: signal call setup to HLR
- 4, 5: request MSRN (mobile station roaming number) from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection



# Mobile Originated Call



- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



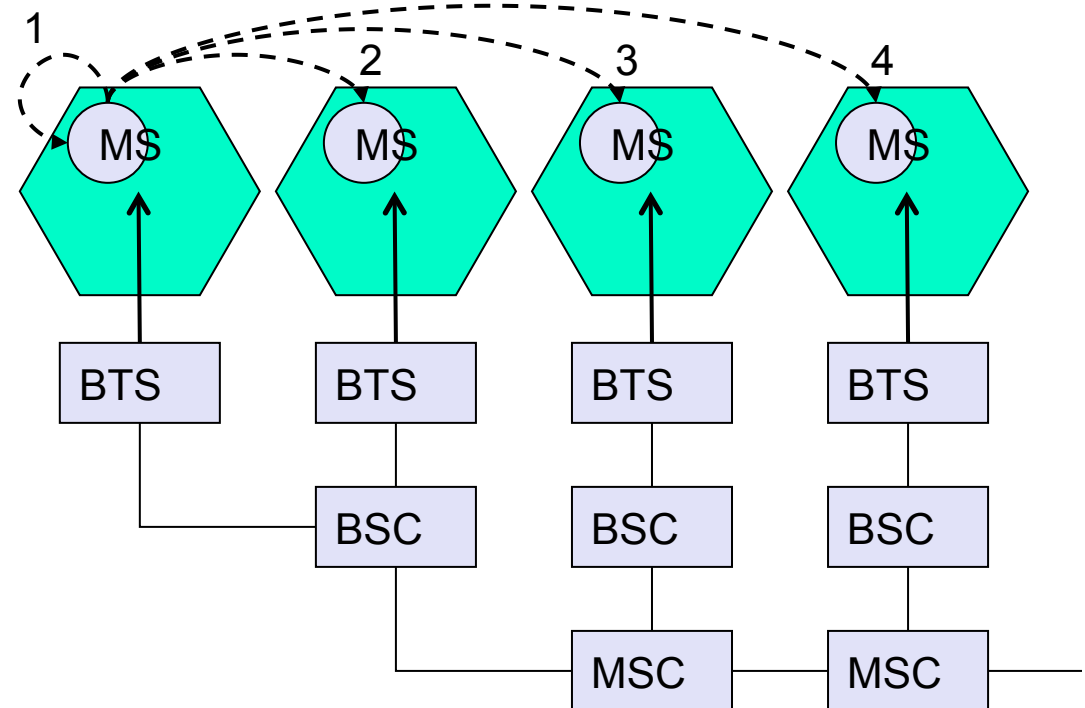


# 4 types of handover

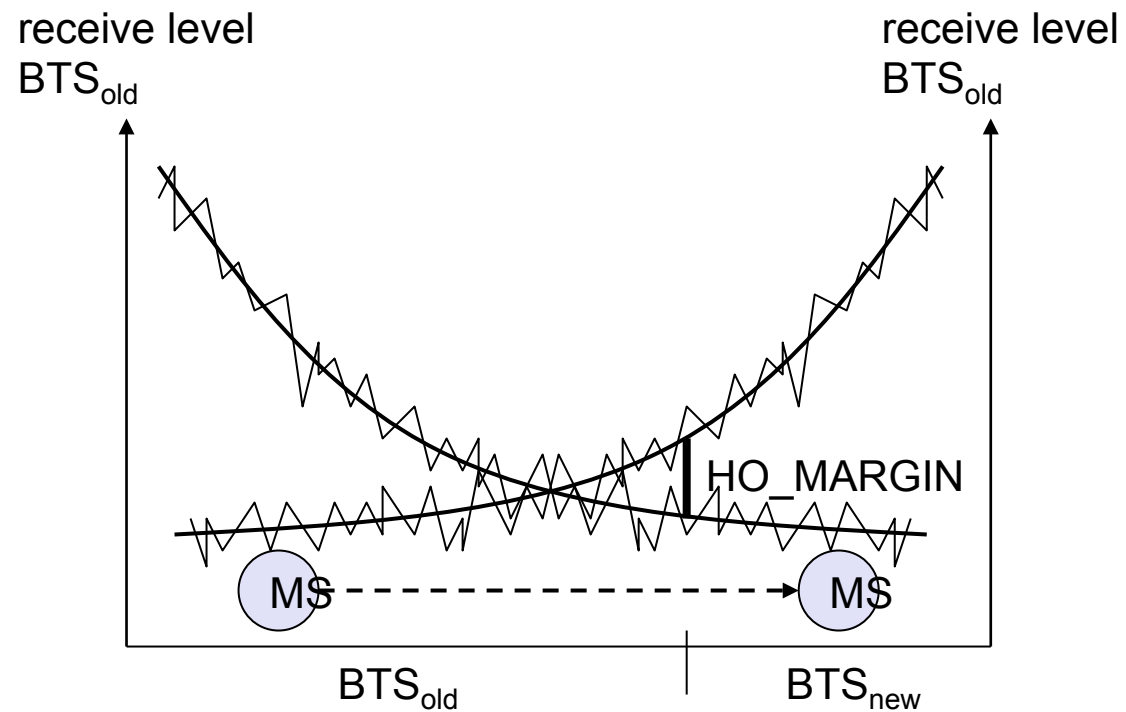


There are 4 types of handover:

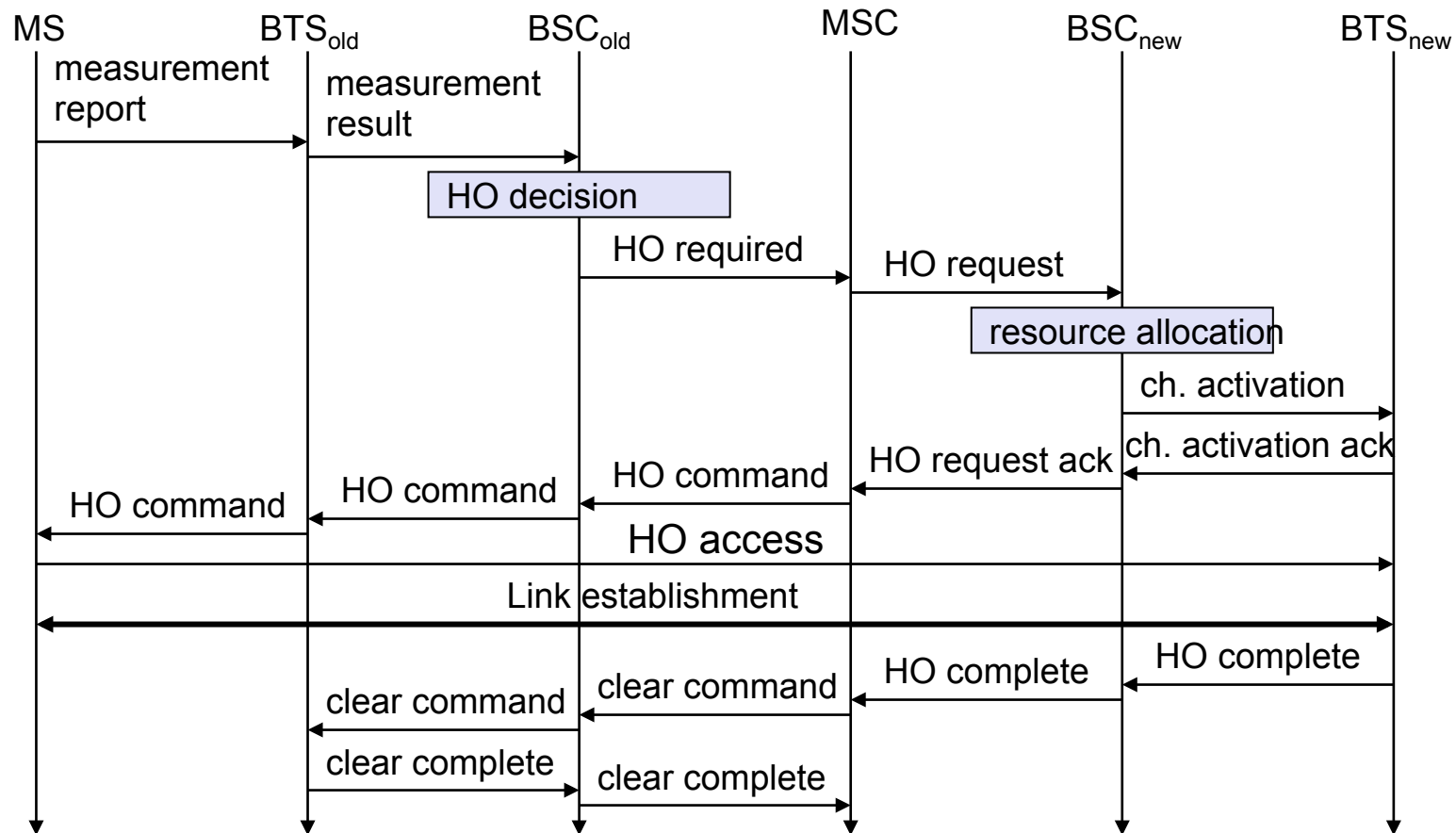
- Change of frequency due to interference inside a cell
- Handover between BTSs
- Handover between BSCs (described later)
- Handover between MSCs



# Handover decision



# Handover procedure



# Security in GSM

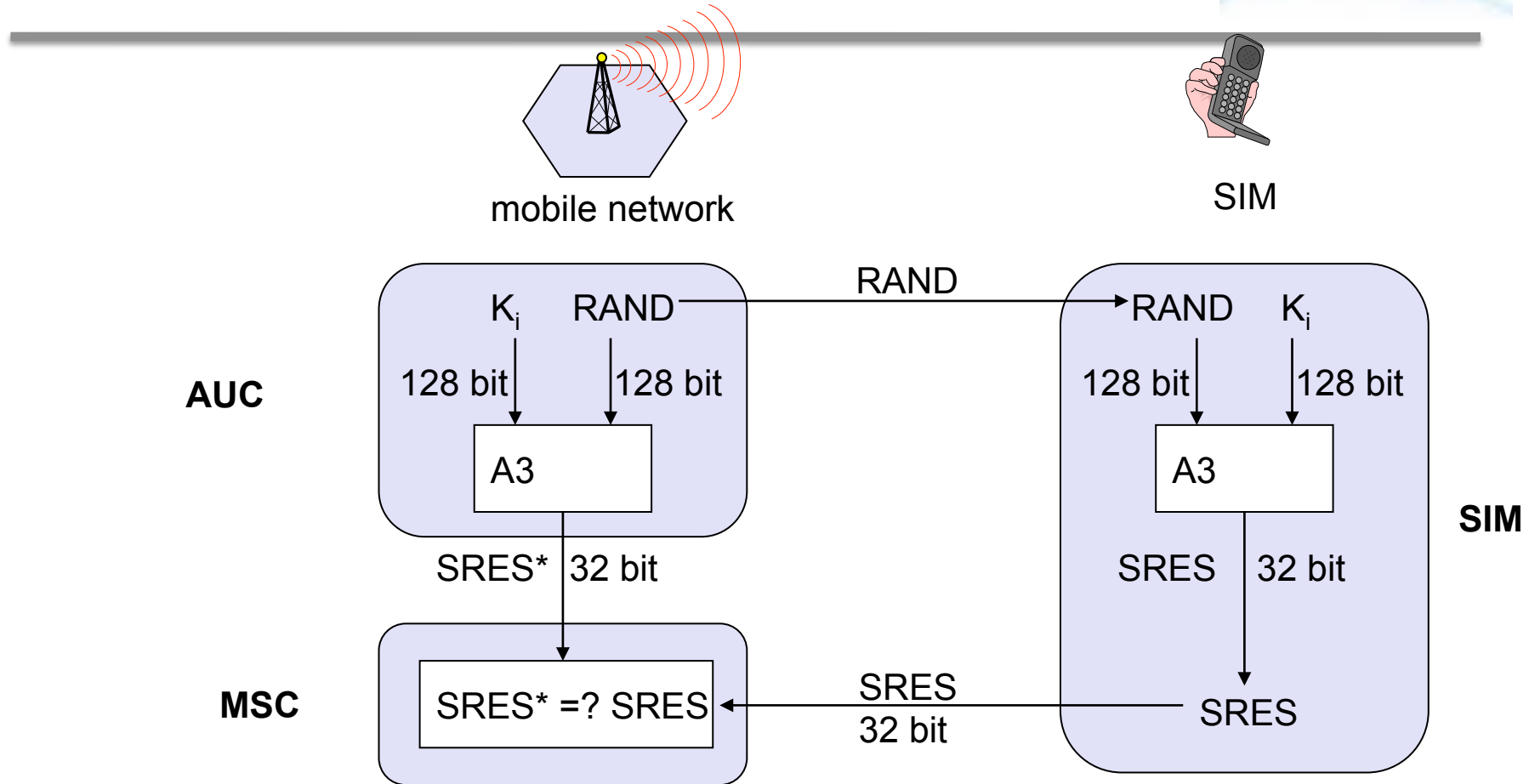


- Security services
  - access control/authentication
    - user  $\rightsquigarrow$  SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM  $\rightsquigarrow$  network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - Only VLR assigned user temporary identifiers TMSI (Temporary Mobile Subscriber Identity) are used
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication (“secret”, open interface)
  - A5 for encryption (standardized)
  - A8 for key generation (“secret”, open interface)

“secret”:

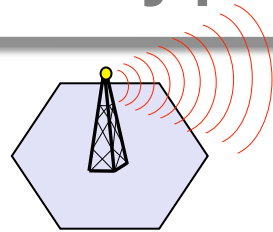
- A3 and A8 available via the Internet
- network providers can use stronger mechanisms

# GSM - authentication



$K_i$ : individual subscriber authentication key      SRES: signed response

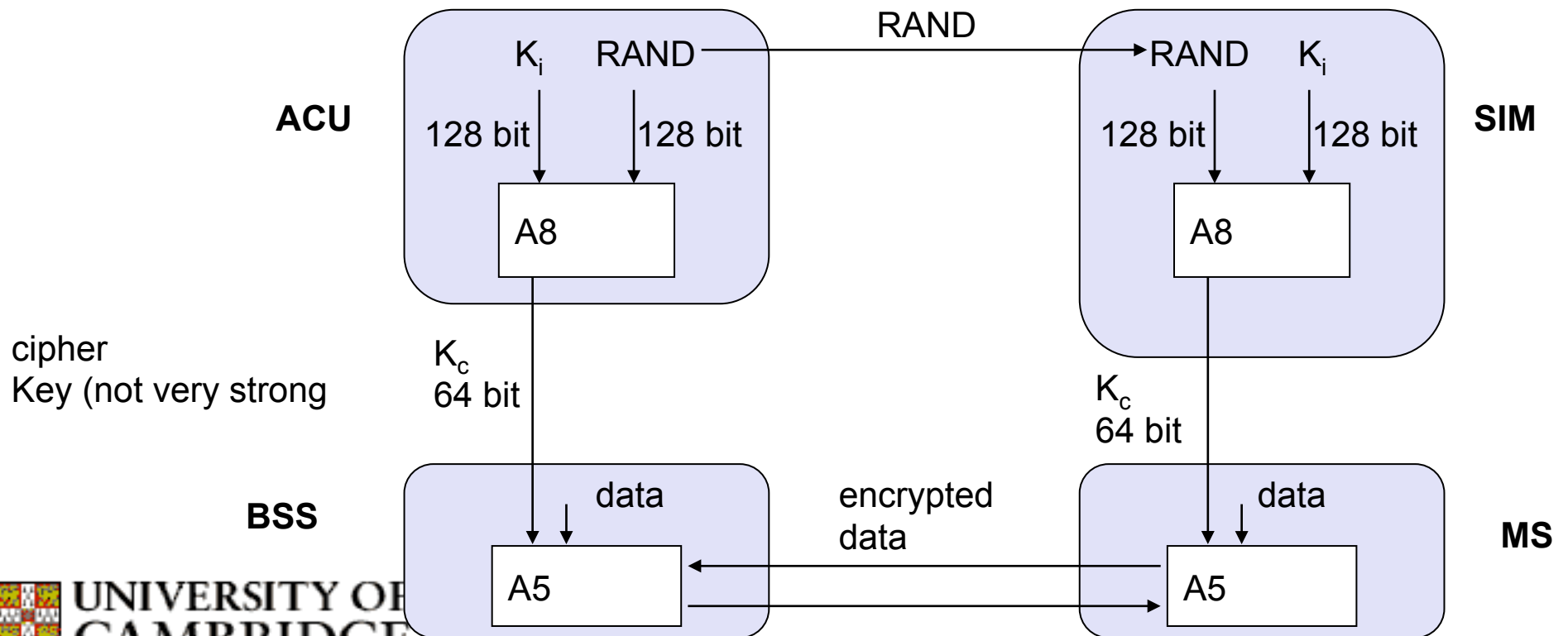
# GSM - key generation and encryption



mobile network (BTS)



MS with SIM



# Summary

---



- We have described the basic principles and architecture of a telecommunication system and given the concrete example of GSM