INTRODUCTION TO WIRELESS AND MOBILE NETWORKS

CHAPTER 9: GSM Security

GSM Security Concerns

- Operators
  - Bills right people
  - Avoid fraud
  - Protect Services
- Customers
  - Anonymity and privacy, no profiles of the movements of the users
  - Confidentiality of communication (voice and data)
  - Correct billing
- 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

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
    - Be cost effective scheme
    - Define security procedures
      - Generation and distribution of keys
      - Exchange information between operators

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 by 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

Security in GSM

- 3 algorithms specified in GSM for security
  - A3 for authentication
  - A5 for encryption
  - A8 for key generation

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

Subscriber Identity Protection

- TMSI – Temporary Mobile Subscriber Identity
  - Goals
    - TMSI is used instead of IMSI as an a temporary subscriber identifier
    - TMSI prevents an eavesdropper from identifying of subscriber
  - Usage
    - TMSI is assigned when IMSI is transmitted to AuC on the first phone switch on
    - Every time a location update (new MSC) occur the network assigns a new TMSI
    - TMSI is used by the MS to report to the network or during a call initialization
    - Network uses TMSI to communicate with MS
    - On MS switch off TMSI is stored on SIM card to be reused next time
  - The Visitor Location Register (VLR) performs assignment, administration and update of the TMSI

Key Management Scheme

- **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
- SIM can be used with different equipment

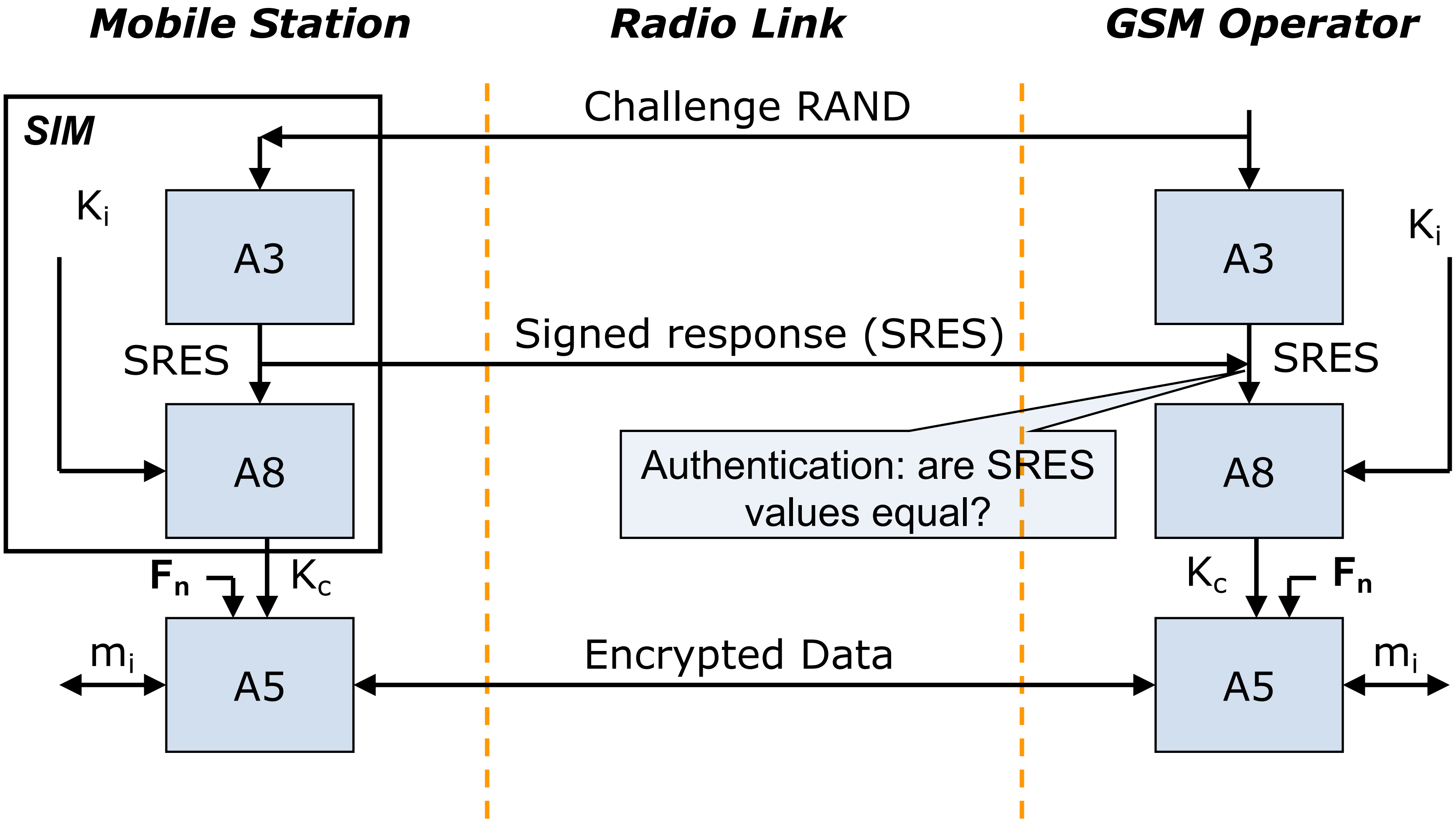
Detection of Compromised Equipment

- International Mobile Equipment Identifier (IMEI)
  - Identifier allowing to identify mobiles
  - IMEI is independent of SIM
  - Used to identify stolen or compromised equipment
- Equipment Identity Register (EIR)
  - Black list – stolen or non-type mobiles
  - White list - valid mobiles
  - Gray list – local tracking mobiles
- Central Equipment Identity Register (CEIR)
  - Approved mobile type (type approval authorities)
  - Consolidated black list (posted by operators)

Authentication

- Authentication Goals
  - Subscriber (SIM holder) authentication
  - Protection of the network against unauthorized use
  - Create a session key
- Authentication Scheme
  - Subscriber identification: IMSI or TMSI
  - Challenge-Response authentication of the subscriber by the operator

Authentication and Encryption Scheme

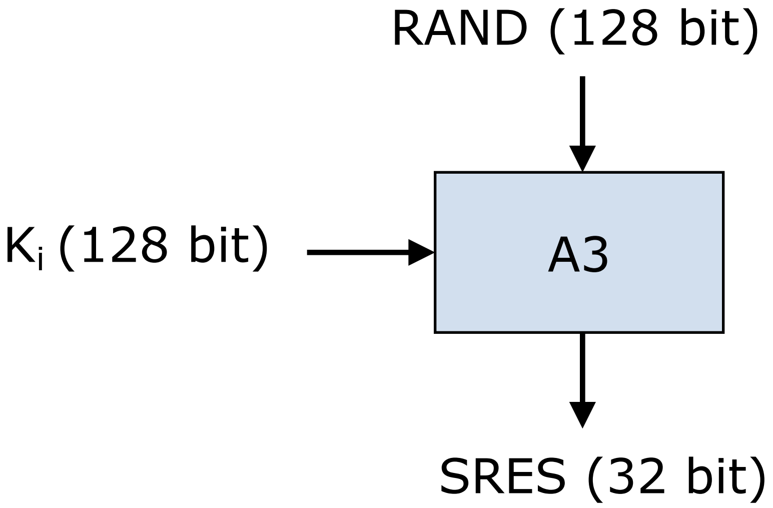


Authentication

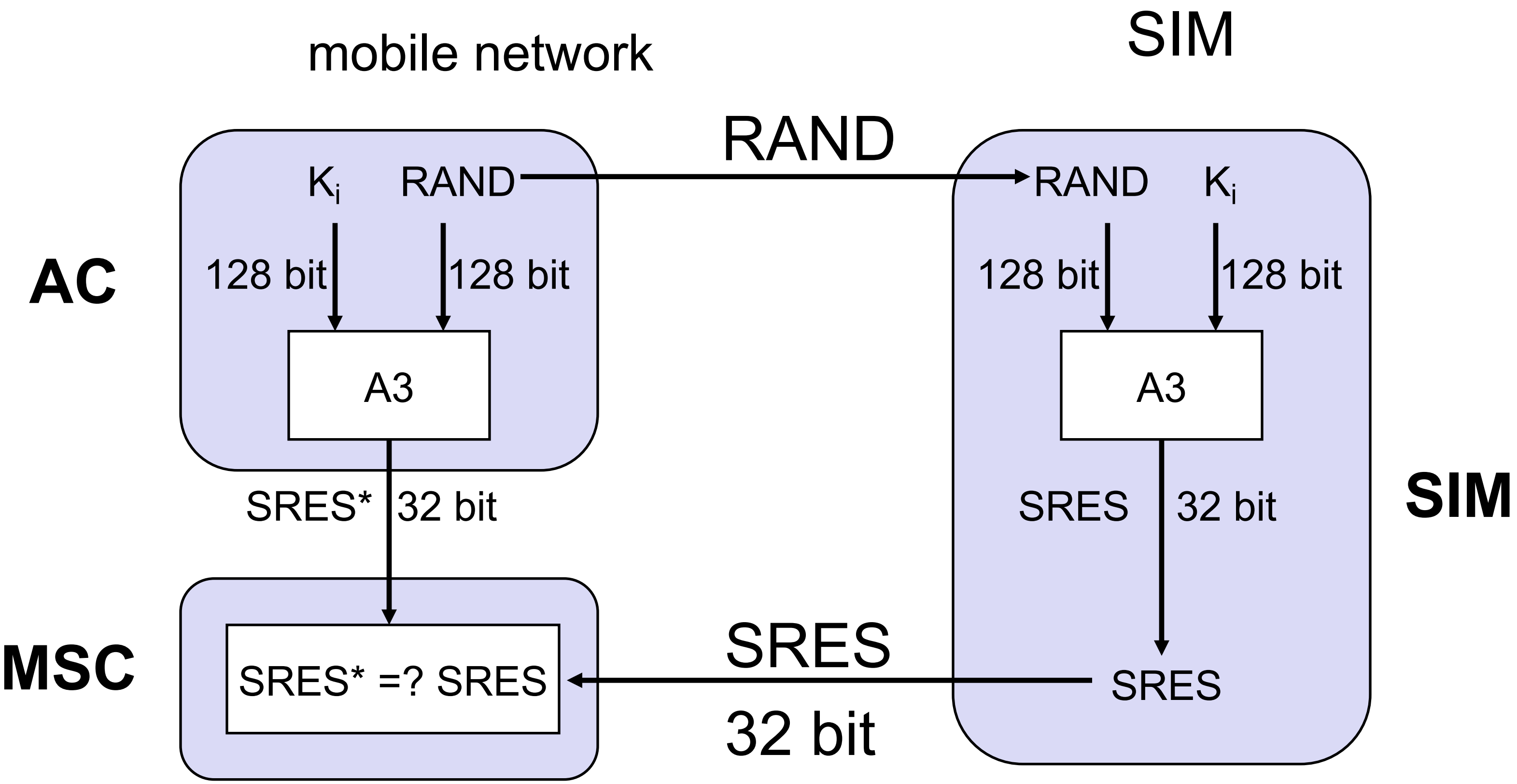
- AuC – Authentication Center
  - Provides parameters for authentication and encryption functions (RAND, SRES, K_c)
- HLR – Home Location Register
  - Provides MSC (Mobile Switching Center) with triples (RAND, SRES, K_c)
  - Handles MS location
- VLR – Visitor Location Register
  - Stores generated triples 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



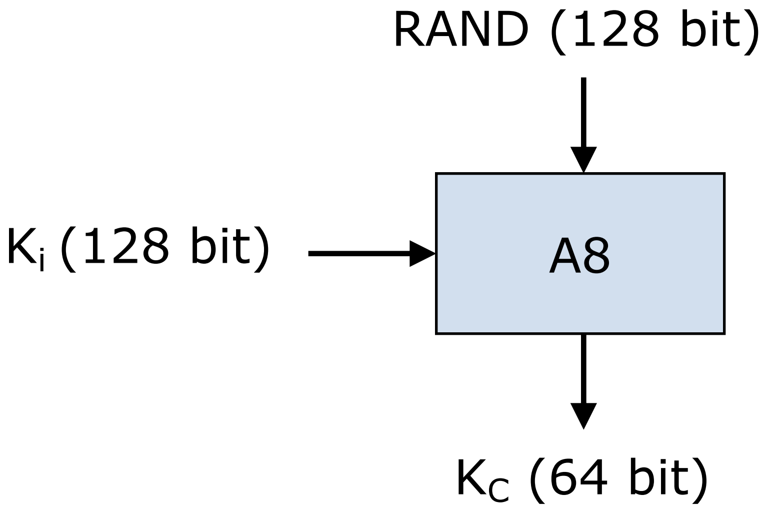
GSM - authentication



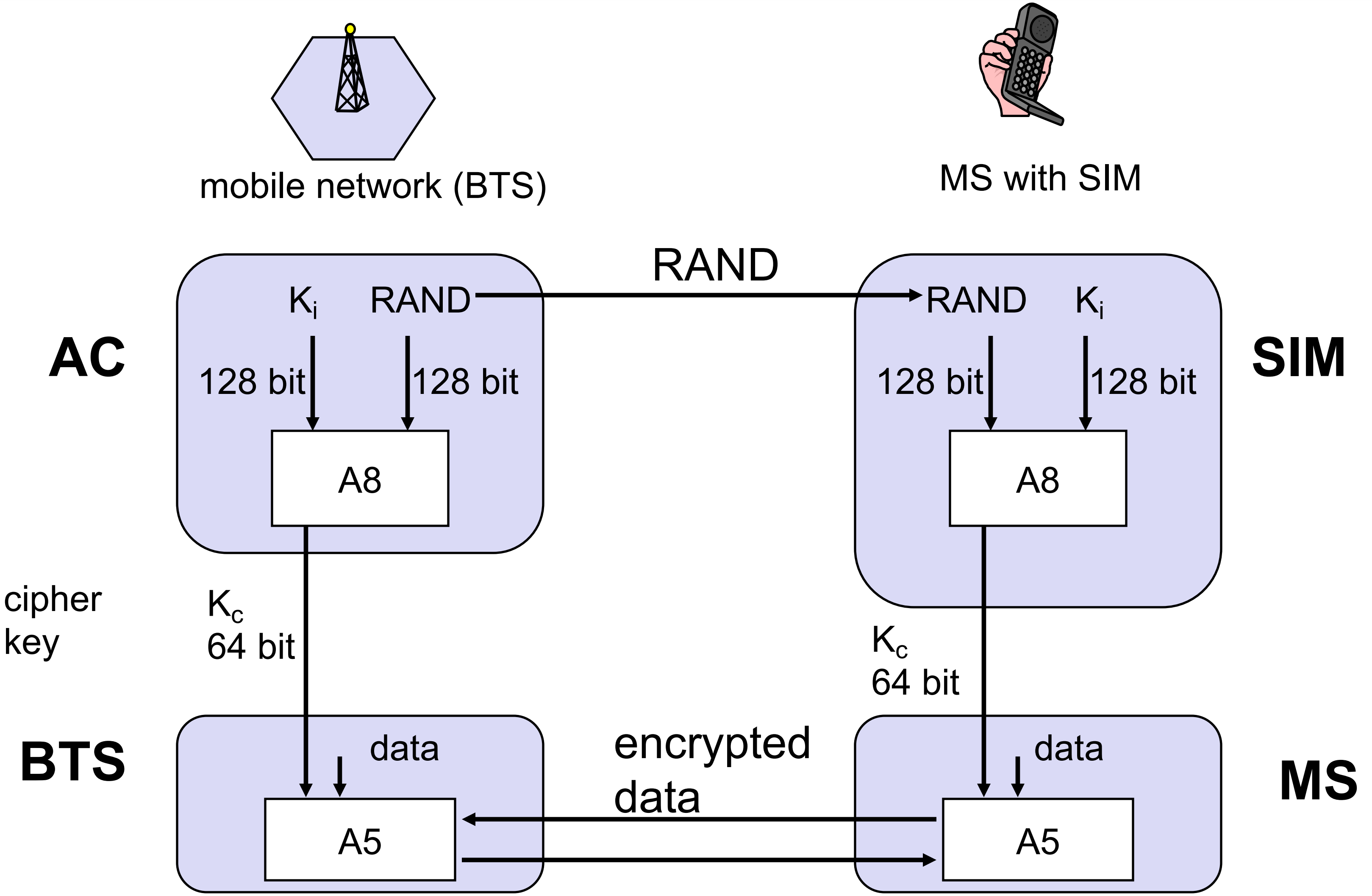
K_i: individual subscriber authentication key
SRES: signed response

A8 – Voice Privacy Key Generation Algorithm

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



GSM - key generation and encryption



mobile network (BTS)

MS with SIM

AC

K_i RAND

128 bit 128 bit

A8

RAND

RAND K_i

128 bit 128 bit

A8

SIM

cipher key

K_c 64 bit

K_c 64 bit

BTS

data

A5

encrypted data

data

A5

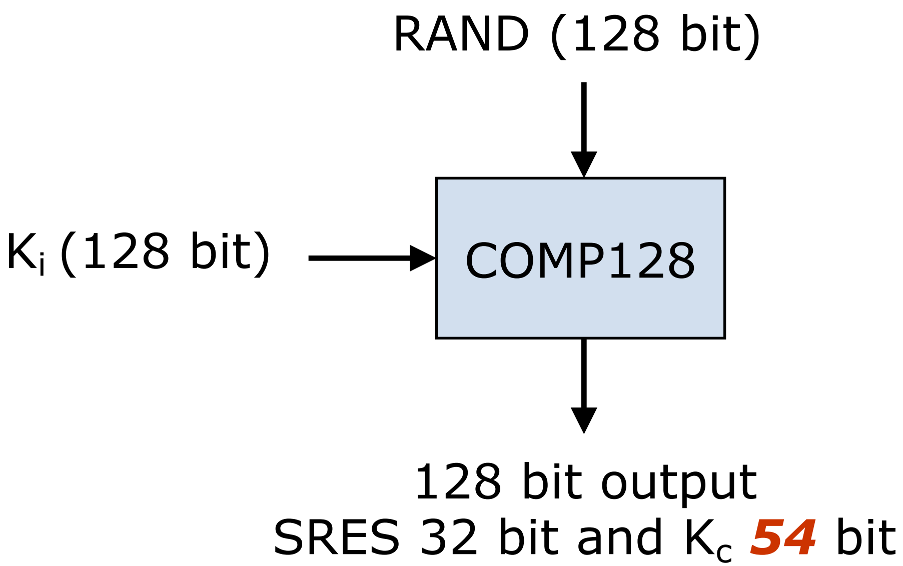
MS

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



A5 – Encryption Algorithm

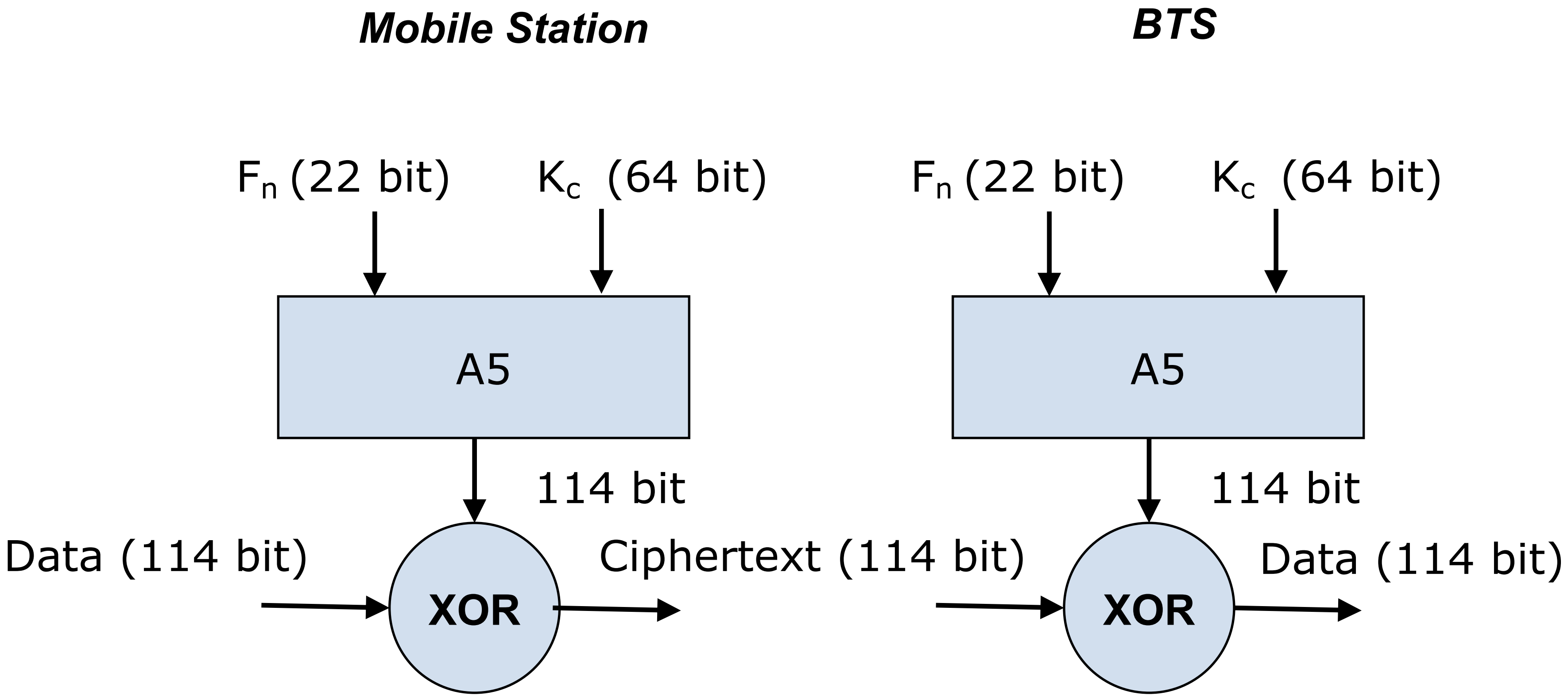
– A5 is a stream cipher

- Implemented very efficiently on hardware
- Design was never made public
- Leaked to Ross Anderson and Bruce Schneier

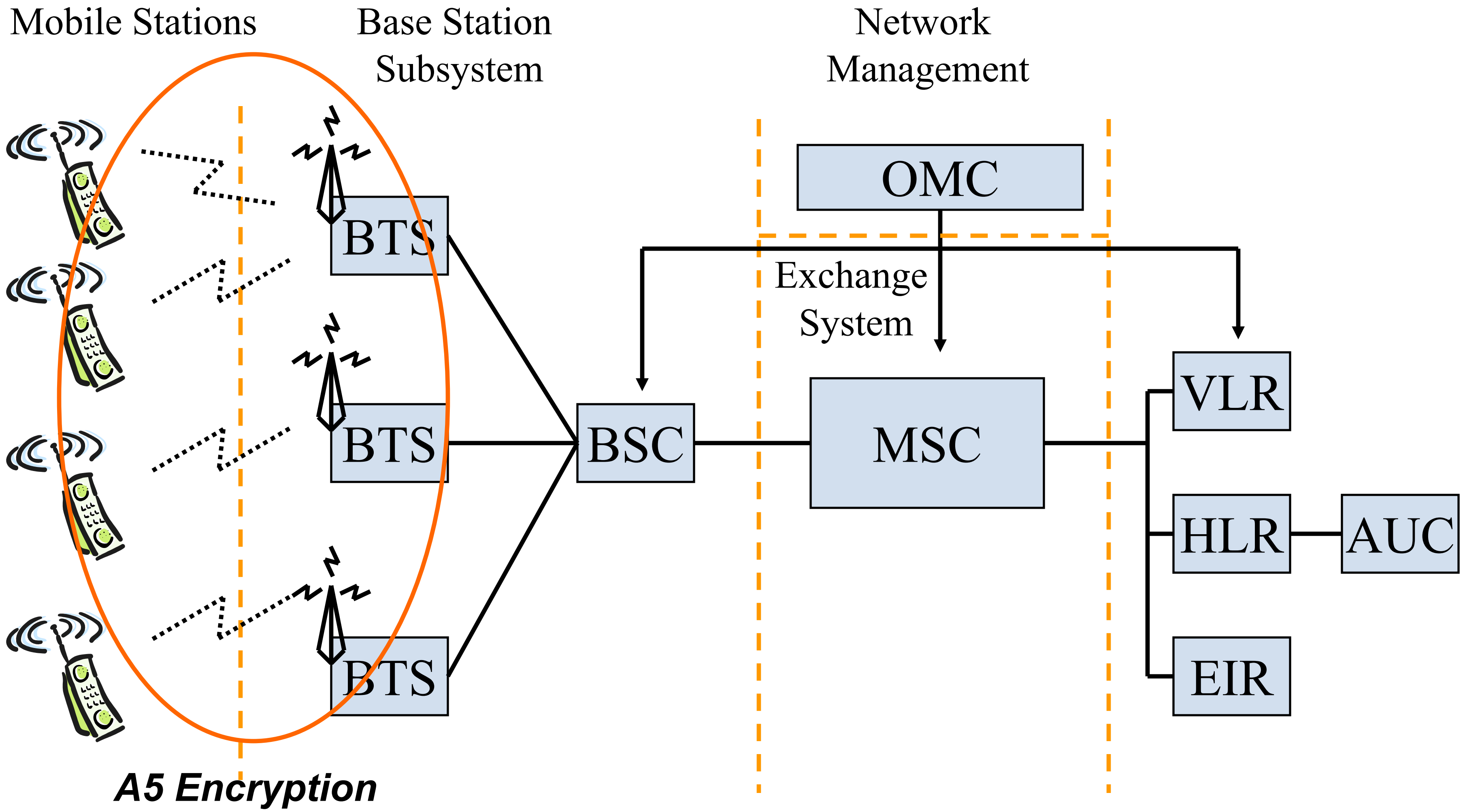
– Variants

- A5/1 – the strong version
- A5/2 – the weak version
- A5/3
  - GSM Association Security Group and 3GPP (***3**rd **G**eneration **P**artnership **P**roject*) design
  - Based on Kasumi algorithm used in 3G mobile systems

Logical A5 Implementation



A5 Encryption



Attacks on GSM

- 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
  - 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.