GSM Security

PPKE, ITK

Csapodi Márton

GSM Evolution

2G (1991-)

- GSM

2.5G (1999-)

- GPRS: MMS, WAP

3G

- EDGE (2003-)
- UMTS (WCDMA, HSDPA , HSUPA, HSPA+)

4G

- LTE

GSM Security Goals

- Operators
  - bills right people
  - avoid fraud
  - protect services
- Customers
  - privacy
  - anonymity
- Make a system at least as 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
- 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

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 Subscriber Integrated Services Digital Network Number (the telephone number)
      - PIN – Personal Identity Number protecting a SIM
      - LAI – location area identity

GSM Architecture

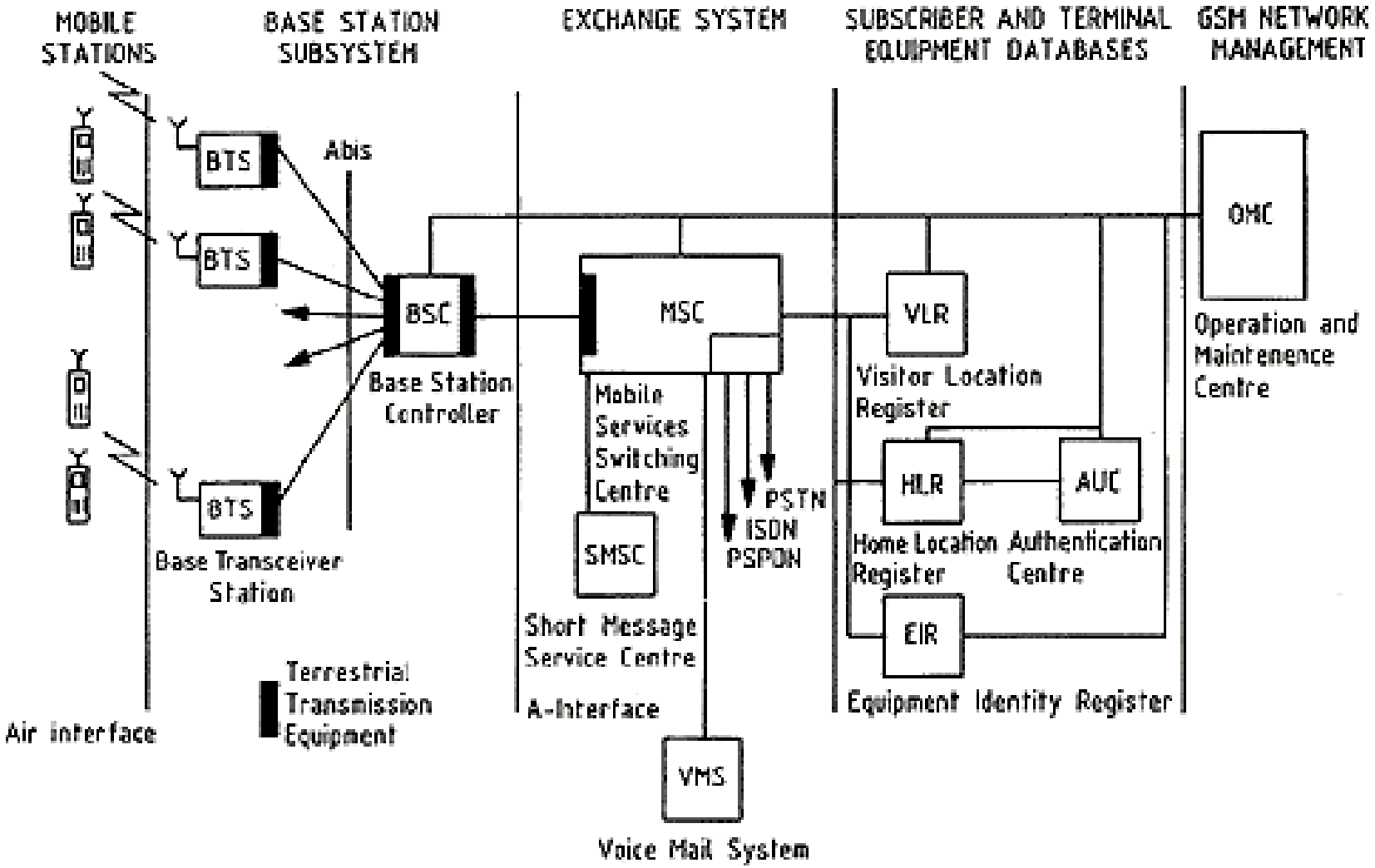


Fig. 1. GSM network architecture

Into the architecture

- Mobile phone is identified by SIM card.
- Key feature of the GSM
- Has the “secret” for authentication

Into the architecture(2)

- BTS – houses the radiotransceivers of the cell and handles the radio-link protocols with the mobile
- BSC – manages radio resources (channel setup, handover) for one or more BTSs

Into the architecture(3)

- MSC – Mobile Switching Center
- The central component of the network
- Like a telephony switch plus everything for a mobile subscriber: registration, authentication, handovers, call routing, connection to fixed networks.
- Each switch handles dozens of cells

Into the architecture(4)

- HLR – database of all users + current location. One per network
- VLR – database of users + roamers in some geographic area. Caches the HLR
- EIR – database of valid equipment
- AUC – Database of users' secret keys

Subscriber Identity Protection

- TMSI – Temporary Mobile Subscriber Identity
  - Goals
    - TMSI is used instead of IMSI as 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) occurs 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

- $\mathbf{K_i}$ – 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 Authentication Centre (AUC) of the subscriber's home network
- SIM can be used with different equipment

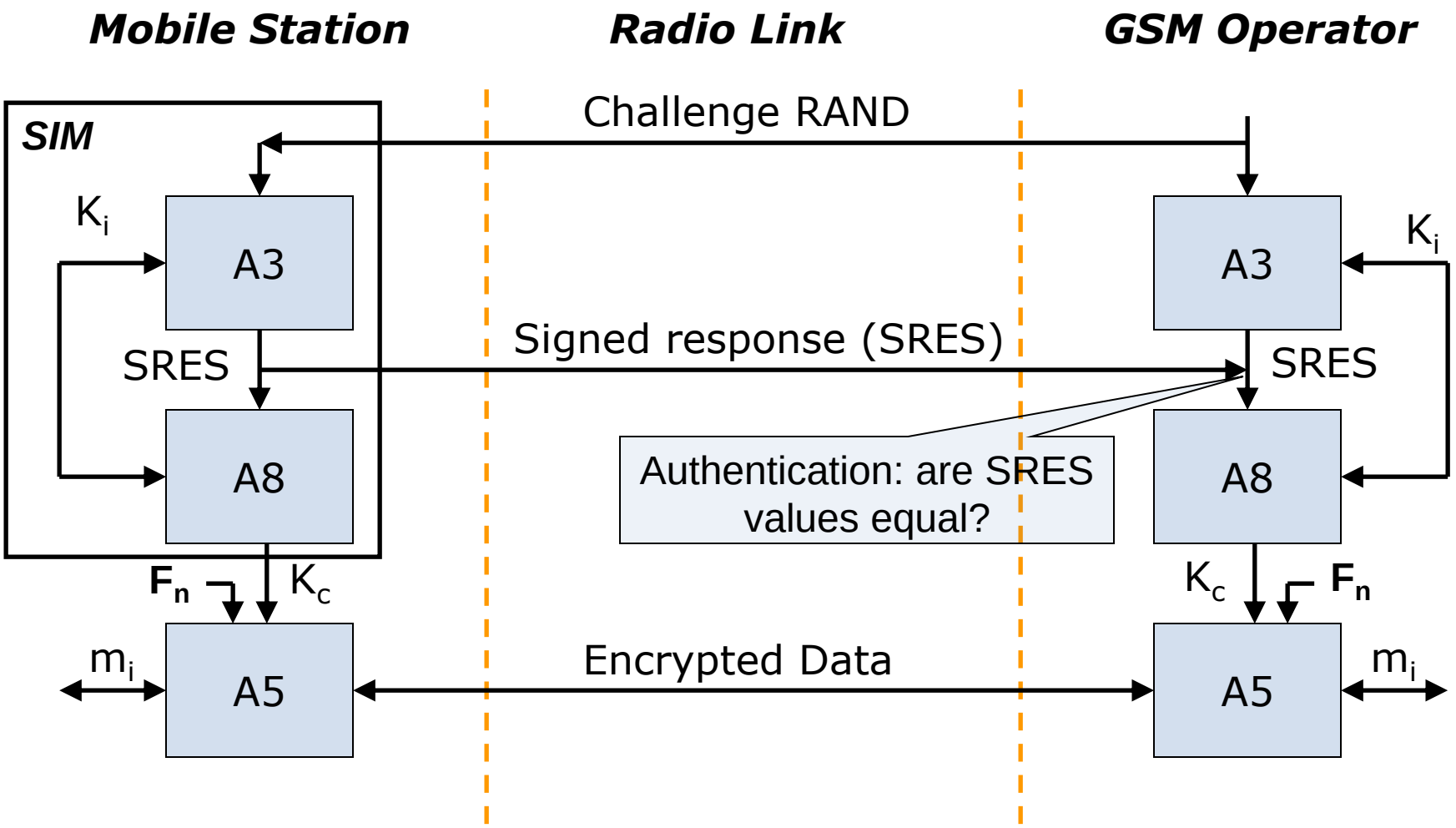
Detection of Compromised Equipment

- International Mobile Equipment Identifier (IMEI)
  - Identifier allowing to identify mobiles
  - IMEI is independent of SIM
  - Used to identify stolen or compromised equipment (*#06#)
- 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

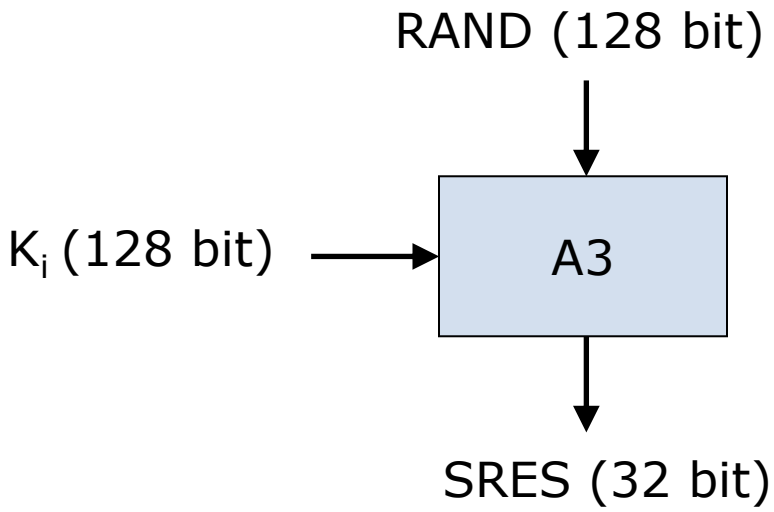
- Authentication Goals
  - Subscriber (SIM holder) authentication
  - Protection of the network against unauthorized use
  - Create a session key
- Authentication Scheme
  - Subscriber identification: IMSI or TMSI
  - Challenge-Response authentication of the subscriber by the operator

Authentication and Encryption Scheme



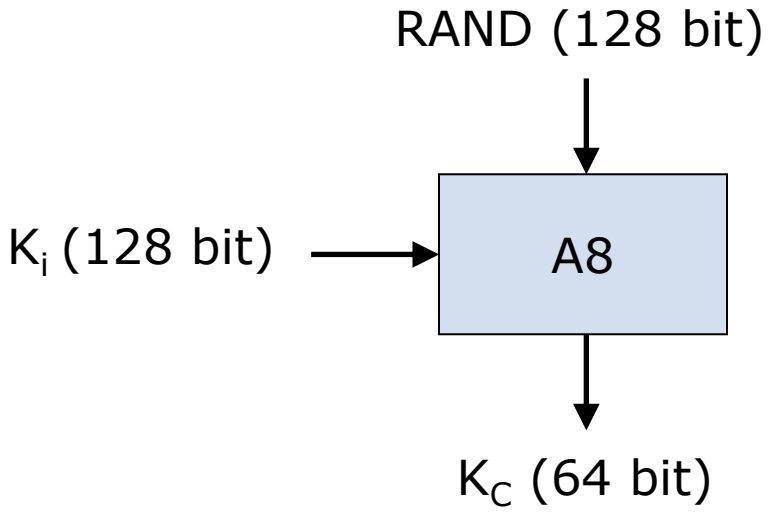
A3 – MS Authentication Algorithm

- 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

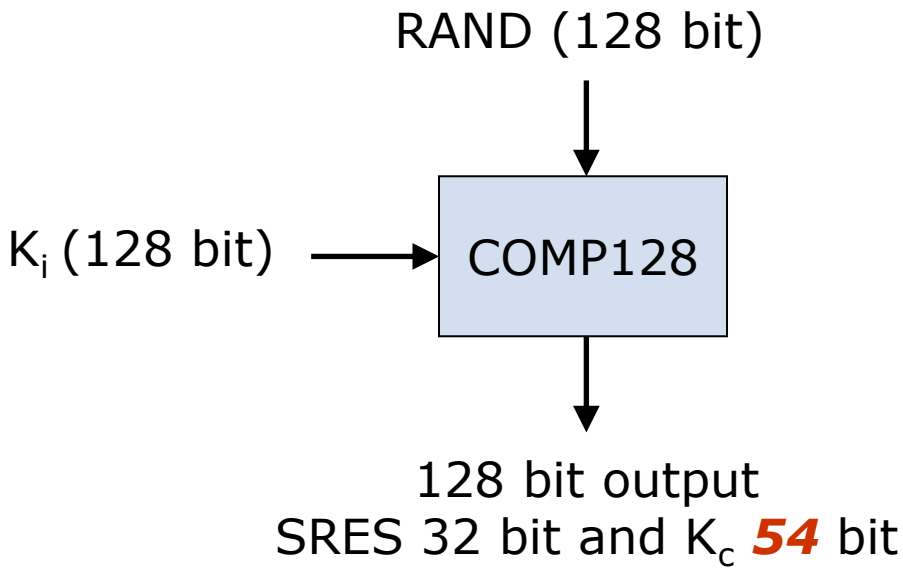


Logical Implementation of A3 and A8

- Both A3 and A8 algorithms are implemented on the SIM
  - Algorithm implementation is independent of hardware manufacturers and network operators.

Logical Implementation of A3 and A8

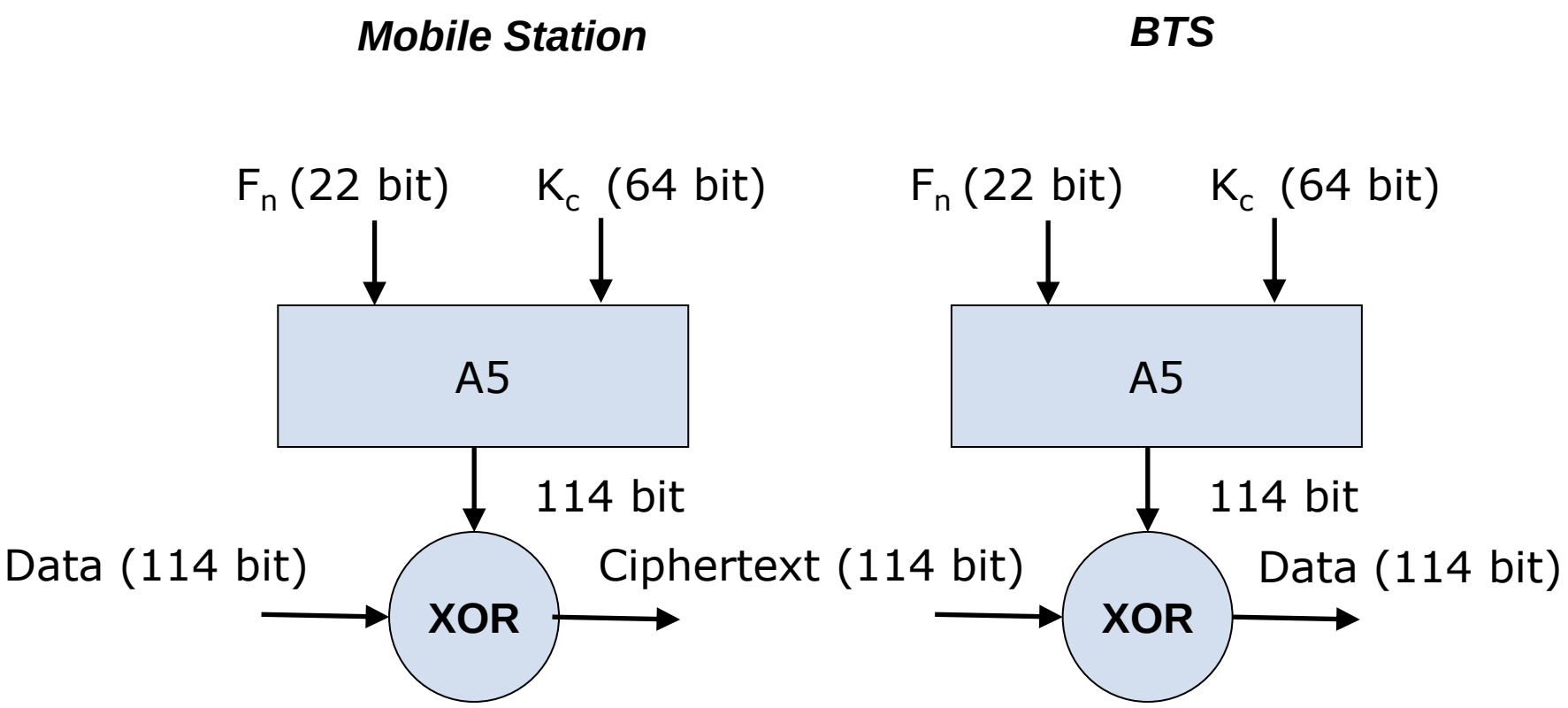
- COMP128 is used for both A3 and A8 in most GSM networks.
  - COMP128 is a keyed hash function



A5 – Encryption Algorithm

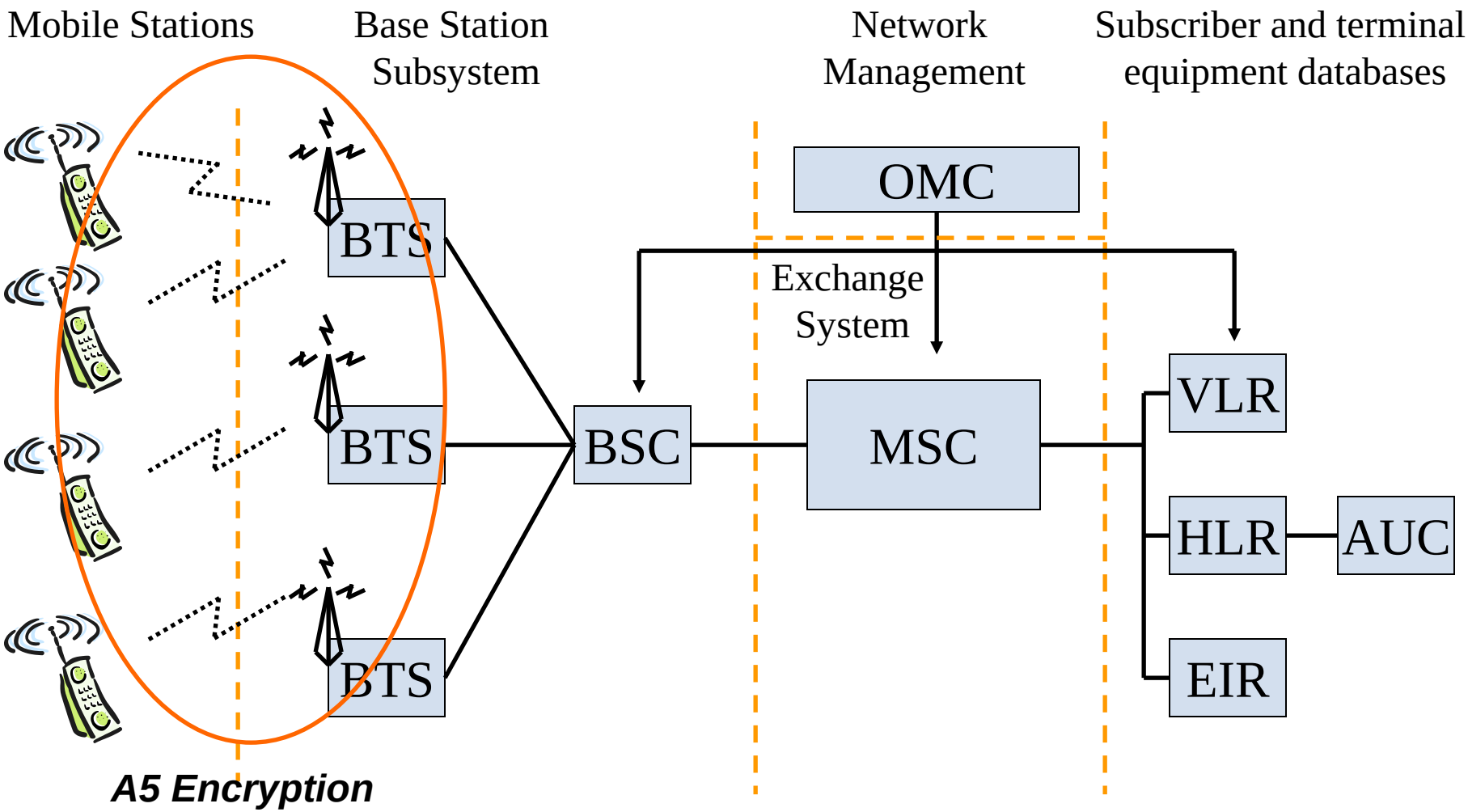
- A5 is a stream cipher
  - Implemented very efficiently on hardware
  - Design was never made public
  - Leaked to Ross Anderson and Bruce Schneier
- Variants
  - A5/1 – the strong version
  - A5/2 – the weak version
  - A5/3
    - GSM Association Security Group and 3GPP design
    - Based on Kasumi algorithm used in 3G mobile systems

Logical A5 Implementation



Real A5 output is 228 bit for both directions

A5 Encryption



A5/1: Operation

- A5/1 is a stream cipher, which is initialized all over again for every frame sent.
- Consists of 3 LFSRs of 19,22,23 bits length.
- The 3 registers are clocked in a stop/go fashion using the majority rule.

A5/1: Operation

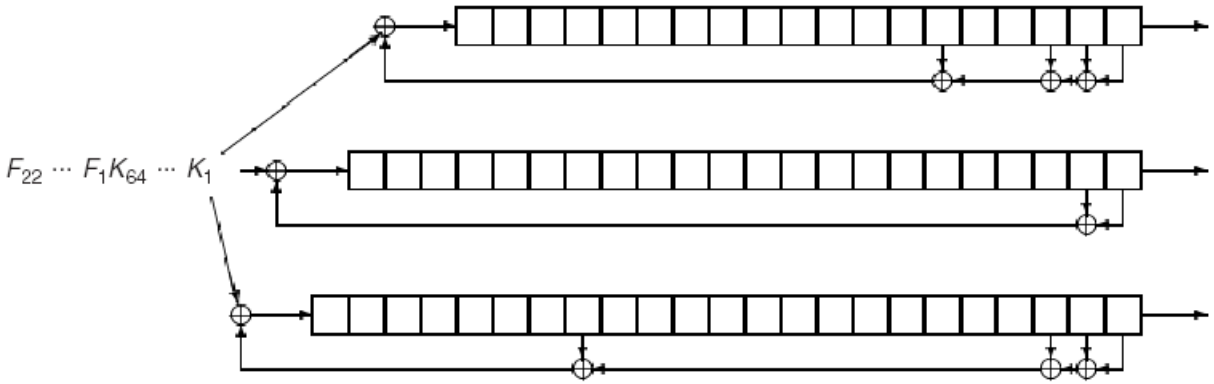


Fig. 1. Initialization of the A5/1 running-key generator

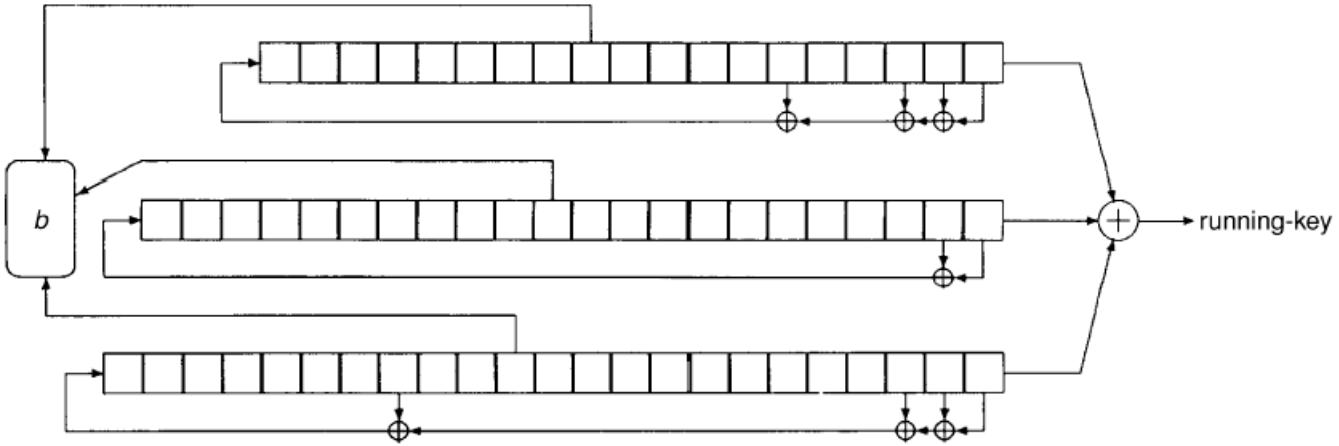
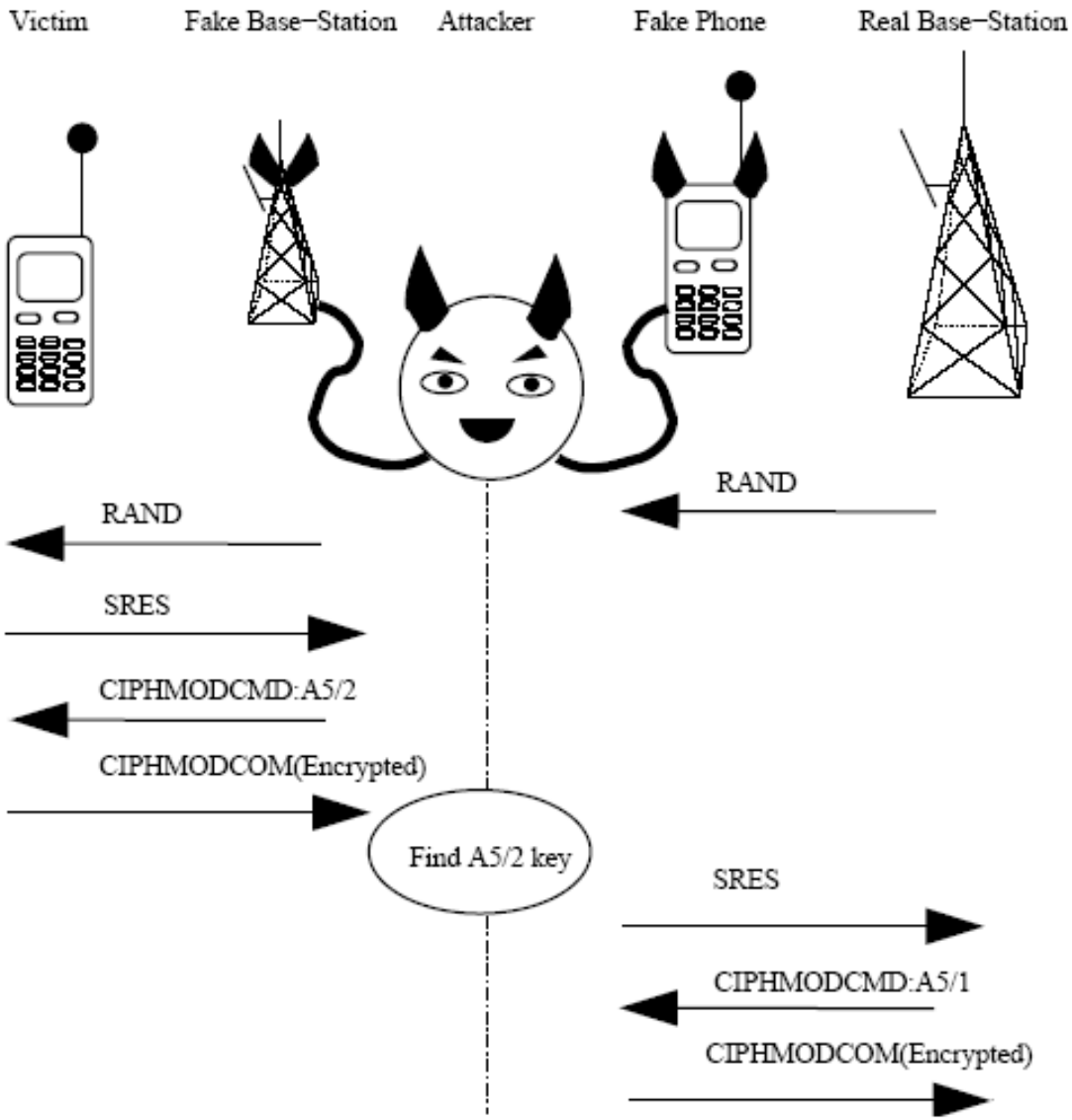


Fig. 2. A5/1 running-key generator

A5/1: Operation

- All 3 registers are zeroed
- 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.

Man-in-the-Middle Attack



Kapcsolódó termékek

http://www.toplinkpac.com/ibis.html

http://www.toplinkpac.com/gtres.html

http://www.toplinkpac.com/3g-cat.html

https://phantom-technologies.com/cpi1890-gsm-interception-system/

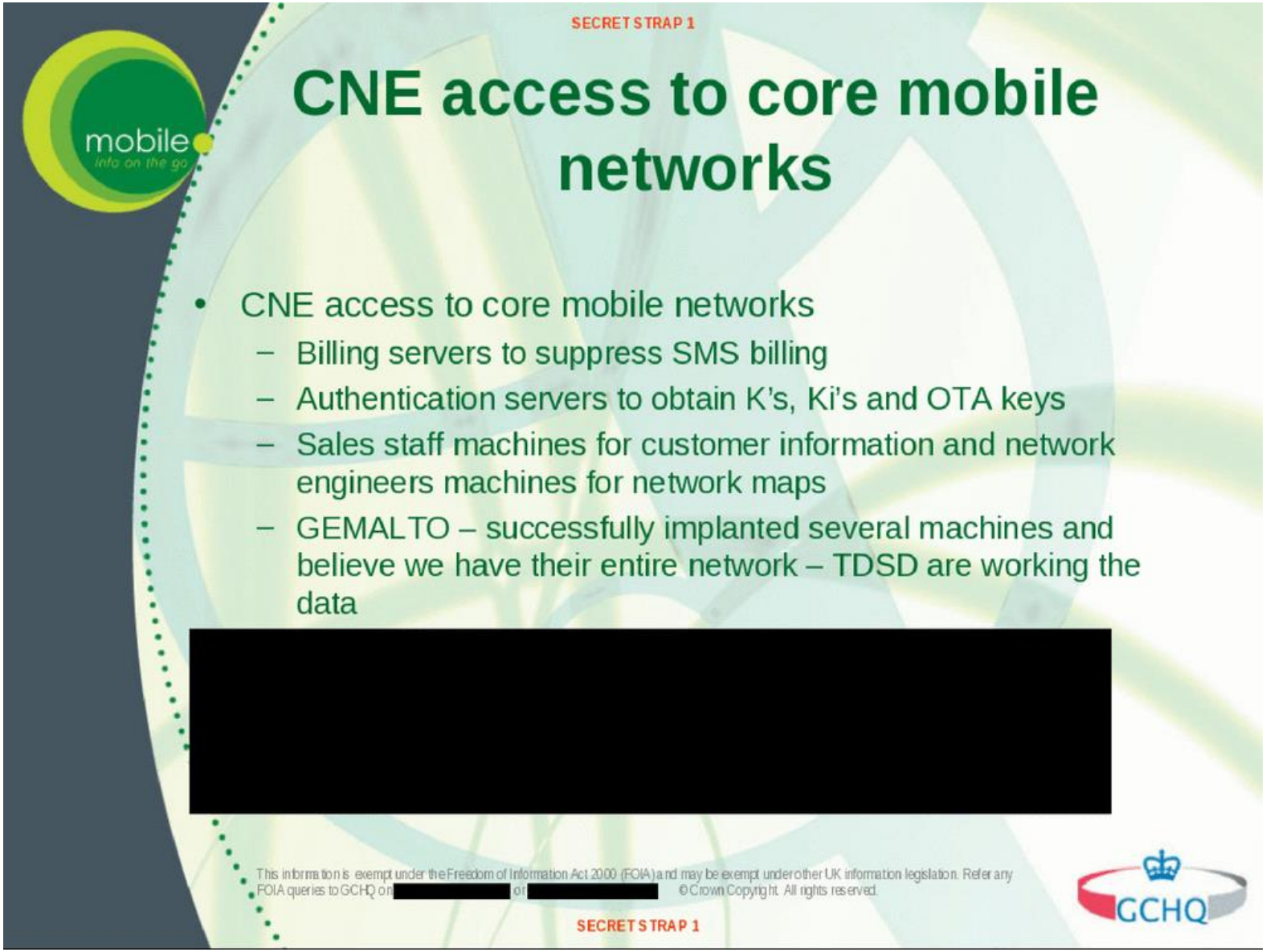
https://phantom-technologies.com/imsi400-imsi-catcher/

SIM klónozás

https://www.mobiledit.com/sim-cloning

http://www.tech2hack.com/how-to-clone-sim-card-easily/

Snowden


SECRET STRAP 1
mobile
info on the go
CNE access to core mobile networks
• CNE access to core mobile networks
– Billing servers to suppress SMS billing
– Authentication servers to obtain K's, Ki's and OTA keys
– Sales staff machines for customer information and network engineers machines for network maps
– GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data
[redacted]
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]
© Crown Copyright. All rights reserved.
GCHQ
SECRET STRAP 1