Network Security: Cellular Security

Tuomas Aura

T-110.5241 Network security

Aalto University, Nov-Dec 2013

Outline

- Cellular networks
- GSM security architecture and protocols
- Counters
- UMTS AKA and session protocols

Cellular networks

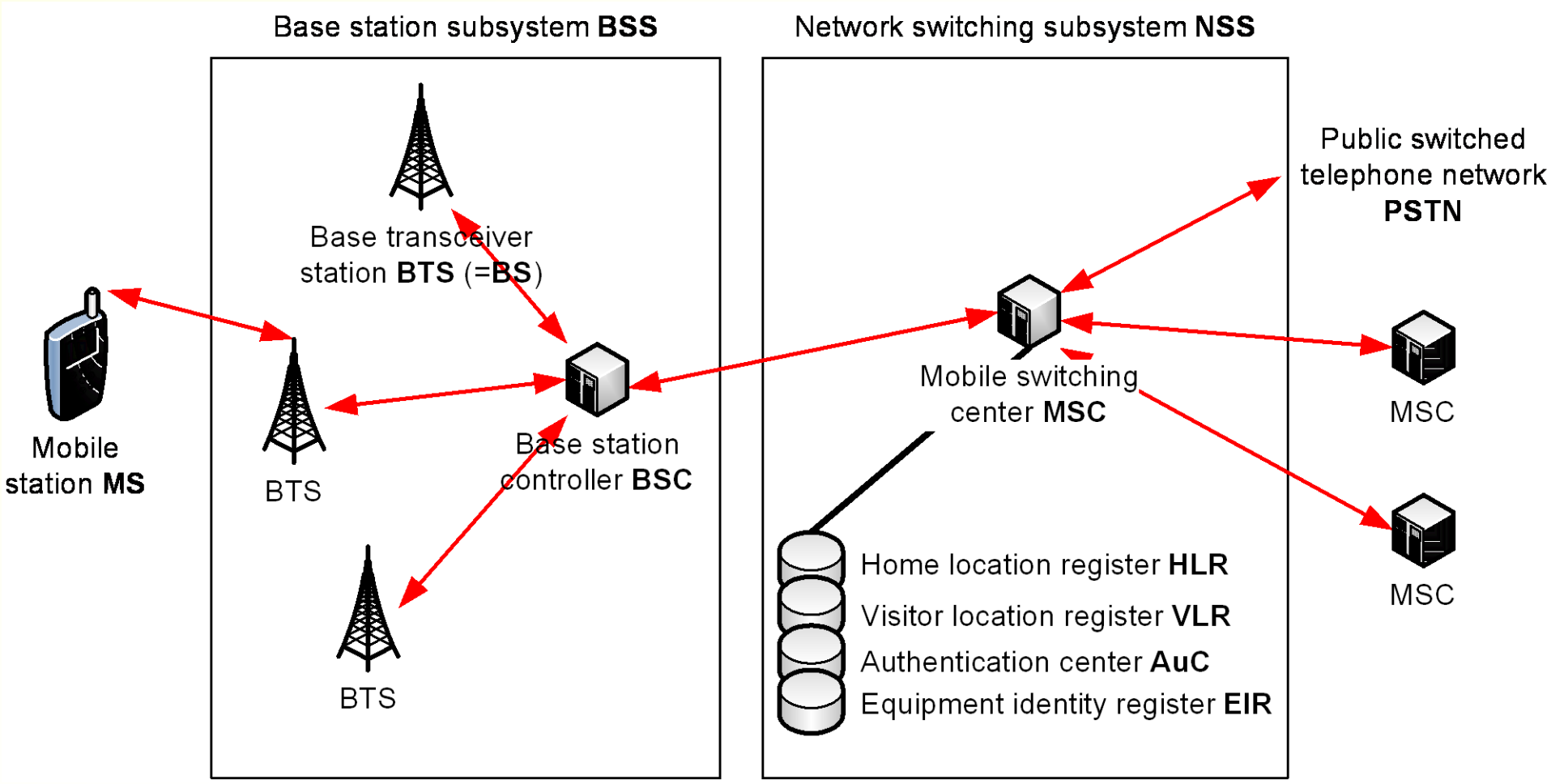
History

- GSM
  - Groupe Spéciale Mobile (GSM) founded in 1982
  - Standardized by European Telecommunication Standards Institute (ETSI)
  - Renamed Global System for Mobile Communications (GSM)
  - First Release in 1990, GPRS (2.5G) in 1997
- UMTS
  - Universal Mobile Telecommunications System (UMTS)
  - Standardized by the 3rd Generation Partnership Project (3GPP) formed by ETSI and Japanese, Korean and Chinese standards bodies
  - First Release 1999
  - High-Speed Downlink Packet Access (HSDPA) standardized in 2001; came into wide use in 2007-8
  - LTE (4G networks) standardized in 2009

GSM network

- Mobile station (MS) = mobile equipment (ME) + subscriber identity module (SIM)
- Base station subsystem (BSS) = base station controller (BSC) + base transceiver stations (BTS)
  - BTS = base station (BS)
- Network switching subsystem (NSS) = mobile switching centers (MSC) and their support functions
  - MSC is an advanced telephone exchange
  - MSC uses the SS7 signalling network (but moving to IP)
- Advanced functions (not covered in this lecture):
  - Text messages
  - GPRS, HSDPA
  - IP multimedia subsystem (IMS)

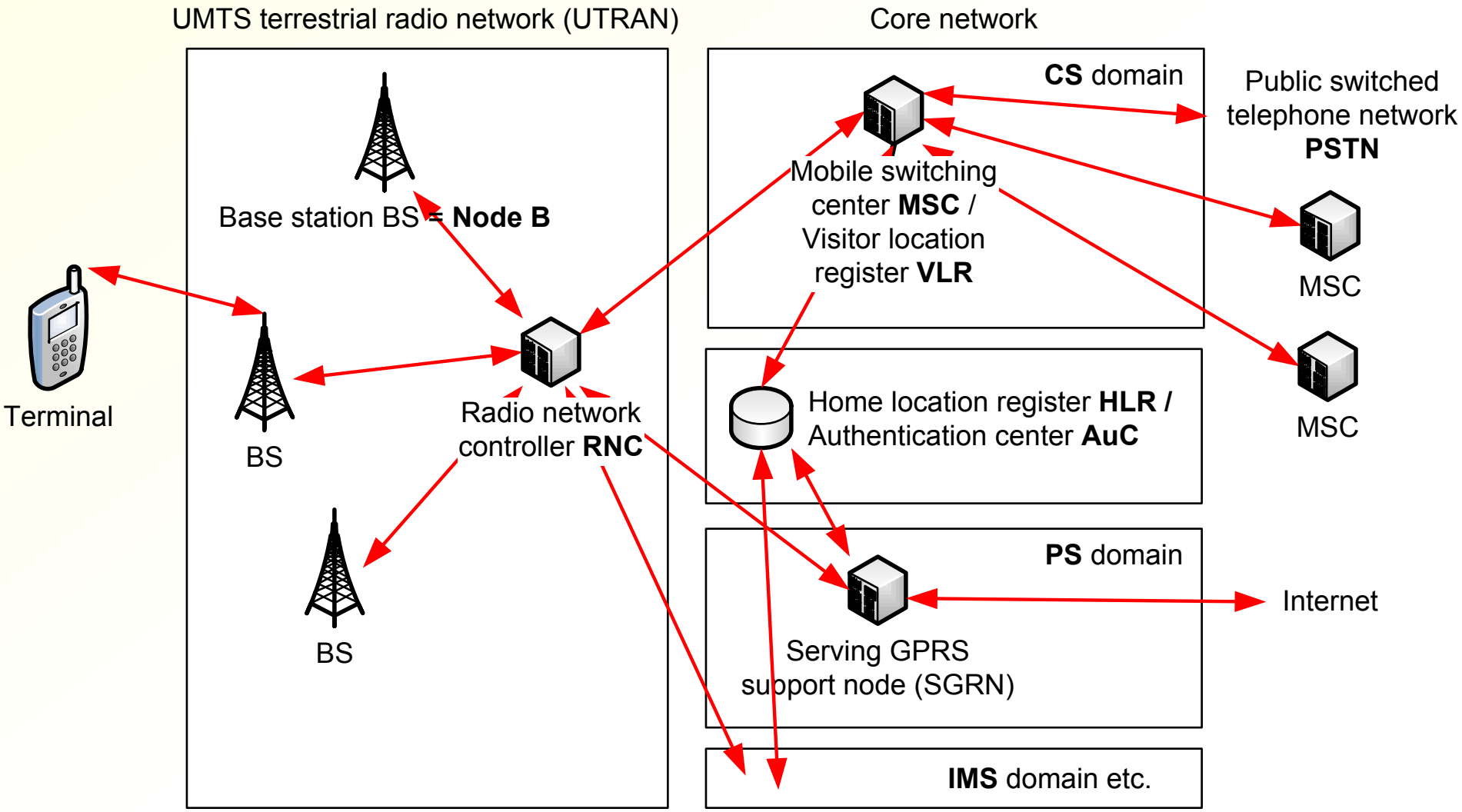
GSM network architecture



UMTS network

- Based on the GSM architecture
- User equipment (UE) i.e. terminal = mobile equipment (ME) + universal subscriber identity module (USIM)
- UMTS terrestrial radio access network (UTRAN) = radio network controller (RNC) + base stations (BS)
- Core network = different service domains + home location register
- 3GPP Release 8 specifies an all-IP network for signalling and data, but deployment will take time
- Circuit-switched (CS) domain for voice
- Packet-switched (PS) domain for IP data

UMTS architecture



Threats against cellular networks

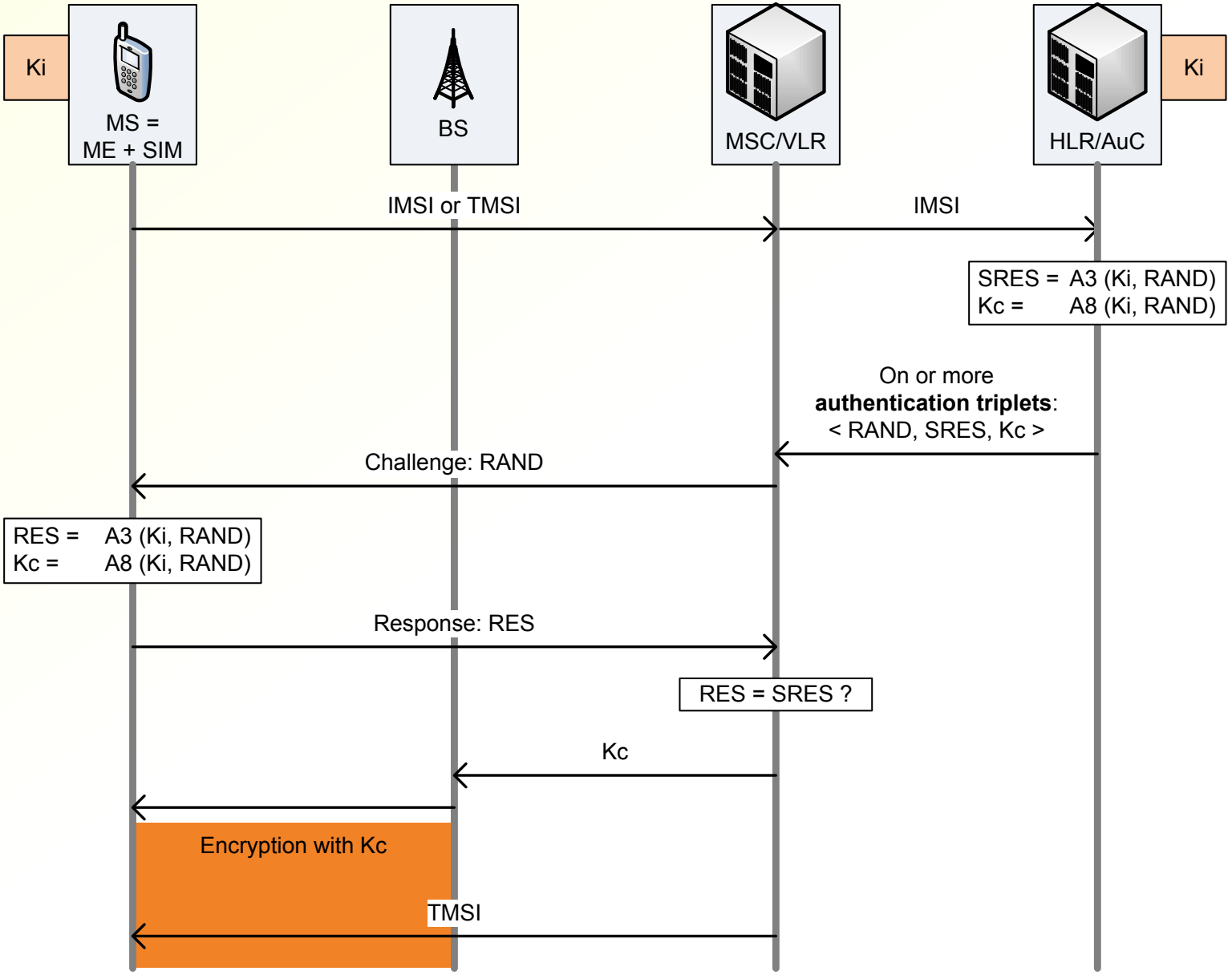
- Discussion: What the threats?
- Charging fraud, unauthorized use
- Charging disputes
- Handset cloning (impersonation attack)
  - → multiple handsets on one subscription
  - → let someone else pay for your calls
- Voice interception → casual eavesdropping and industrial espionage
- Location tracking
- Handset theft
- Handset unlocking (locked to a specific operator)
- Network service disruption (DoS)
- What about integrity?

GSM security

GSM security architecture

- Home location register (HLR) keeps track of the mobile's location
- Visitor location register (VLR) keeps track of roaming mobiles at each network
- Shared key Ki between SIM and authentication center (HRL/AuC) at the home network
- VLR of the visited network obtains authentication triplets from AuC of the mobile's home network and authenticates the mobile
- Encryption between mobile and the base station

GSM authentication



GSM authentication

- Alice-and-Bob notation:

  1. Network → MS: RAND
  2. MS → Network: A3 (Ki, RAND)

  Ki = shared master key

  Kc = A8 (Ki, RAND) = session key

- After authentication, BS asks mobile to turn on encryption. A5 cipher with the key Kc

GSM security

- Mobile authenticated → prevents charging fraud
- Encryption on the air interface
  - → No casual sniffing
  - → Encryption of signalling gives some integrity protection
- TMSI → not easy to track mobile with a passive radio
- Algorithms A3, A8 can be replaced by home operator
  - AuC and SIM must use the same algorithms
- Non-protocol features:
  - Subscriber identity module (SIM) is separate from the handset
    - → Flexibility
    - → Thiefs and phone unlockers don't even try to break the SIM
  - International mobile equipment identity (IMEI) to track stolen devices

GSM security weaknesses

- Only the mobile is authenticated, network not
- BS decides when to turn on encryption; mobiles have no indicator
  → Possible to set up a fake BS that uses no encryption
- Integrity protection depends on encryption but some networks do not use encryption
- Decryption at BS, but BS may be at a hard-to-monitor location and compromised
- Early encryption algorithms based on COMP128, which has been broken. A5 cannot be upgraded without replacing the handset
- Authentication triplets transferred over the SS7 signalling network, which can be accessed by thousands of operators
- No non-repudiation → no protection against false charges from dishonest operators
- IMSI sent when requested by BS → IMSI catchers to track mobiles
- IMEI not authenticated → can be changed to prevent the tracking of stolen mobiles

UMTS improvements over GSM

- RAN separate from CN
  - Roles of radio-network operator and service operator separated
- Encryption endpoint moved from BS to RNC
- Mutual authentication protocol AKA
- Support for multiple service domains
  - Circuit-switched, packet-switched, multimedia, WLAN
- Protection of core-network signalling
- Security indicator to user (e.g. encryption off)

Counters

Using counters for freshness

- Simple shared-key authentication with nonces:
  1. A → B: N_A
  2. B → A: N_B, $MAC_K(Tag2, A, B, N_A, N_B)$
  3. A → B: $MAC_K(Tag3, A, B, N_A, N_B)$

  K = master key shared between A and B

  SK = $h(K, N_A, N_B)$
- Using counters can save one message or roundtrip:
  1. ~~A → B:~~
  2. B → A: N_B, SQN, $MAC_K(Tag2, A, B, SQN, N_B)$
  3. A → B: $MAC_K(Tag3, A, B, SQN, N_B)$

  SK = $h(K, SQN, N_B)$
- Another benefit: B can pre-compute message 2
- A must check that the counter always increases

Using counters

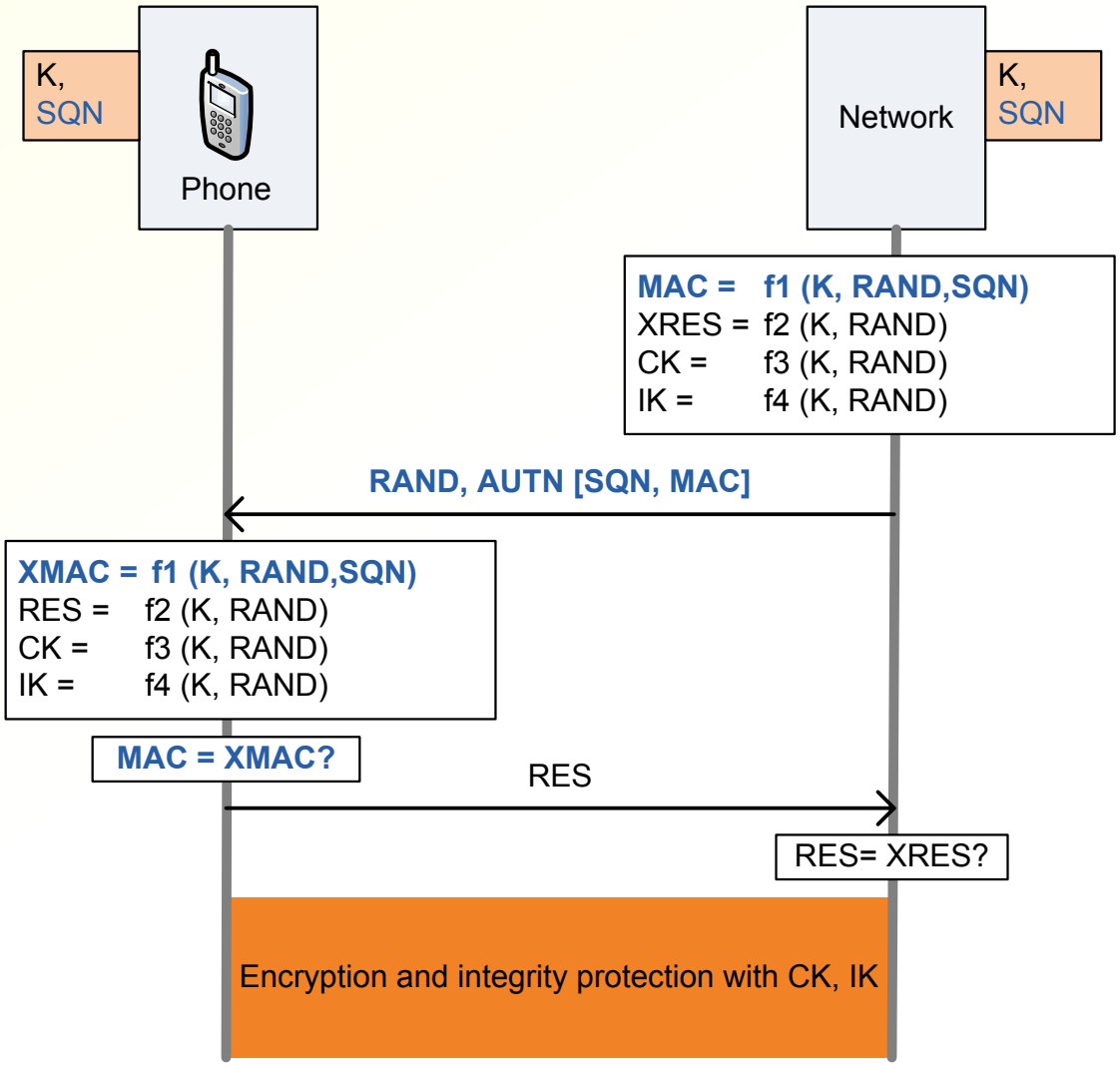
- Counters must be monotonically increasing
  - Never accept previously used values
  - Persistent state storage needed
- Recovering from lost synchronization:
  - Verifier can maintain a window of acceptable values to recover from message loss or reordering
  - Protocol for resynchronization if badly off
- Values must not be exhausted
  - Limit the rate at which values can be consumed
  - But support bursts of activity
  - Long enough counter to last equipment or key lifetime

UMTS authentication and key agreement (AKA)

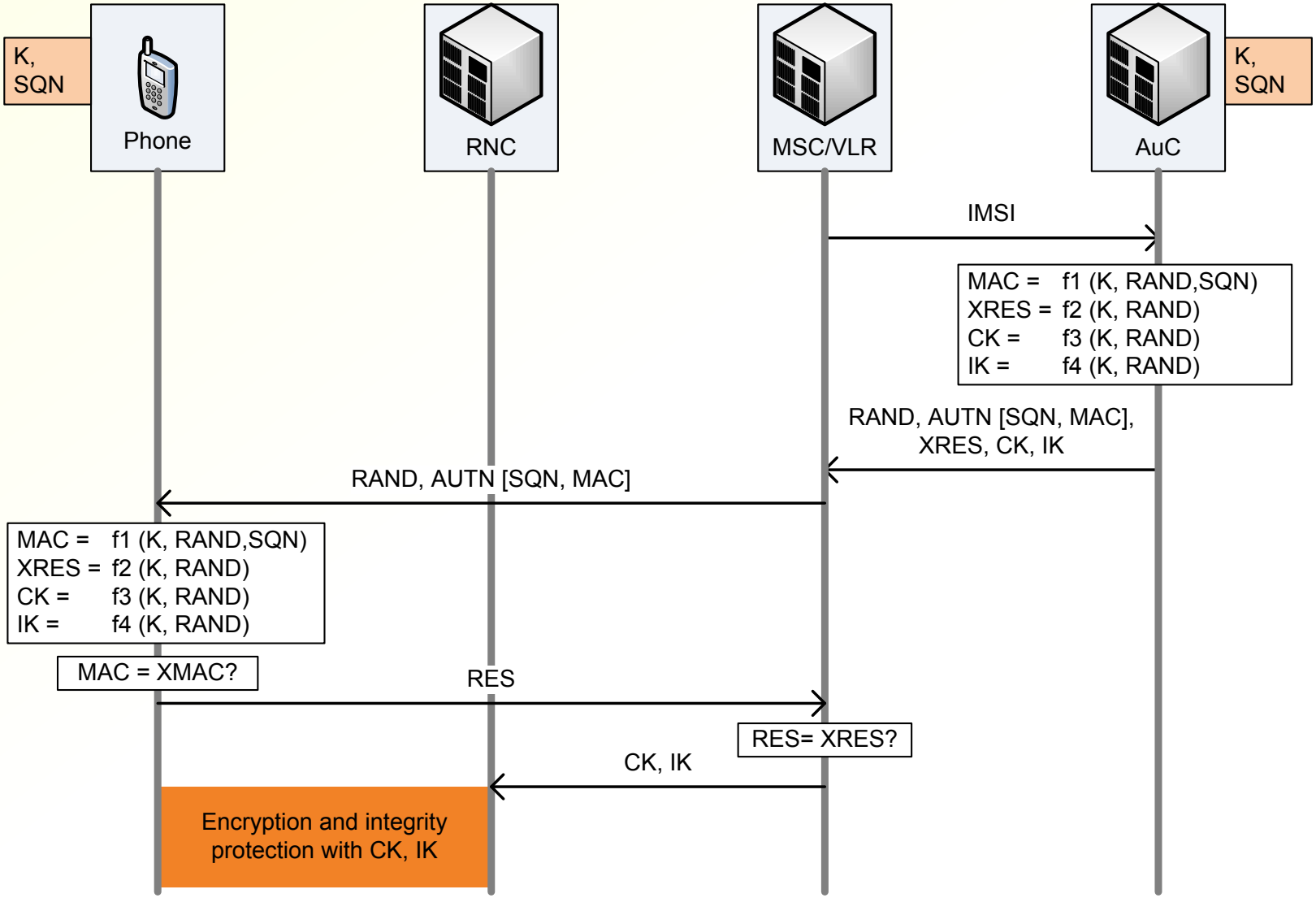
UMTS AKA

- AKA = authentication and key agreement
- Based on GSM authentication
- Mutual authentication
- Sequence number for freshness to mobile
  → saves one roundtrip to AuC
  → authentication vectors can be retrieved early, several at a time
  - Why is this so important? Why not just use a client nonce?

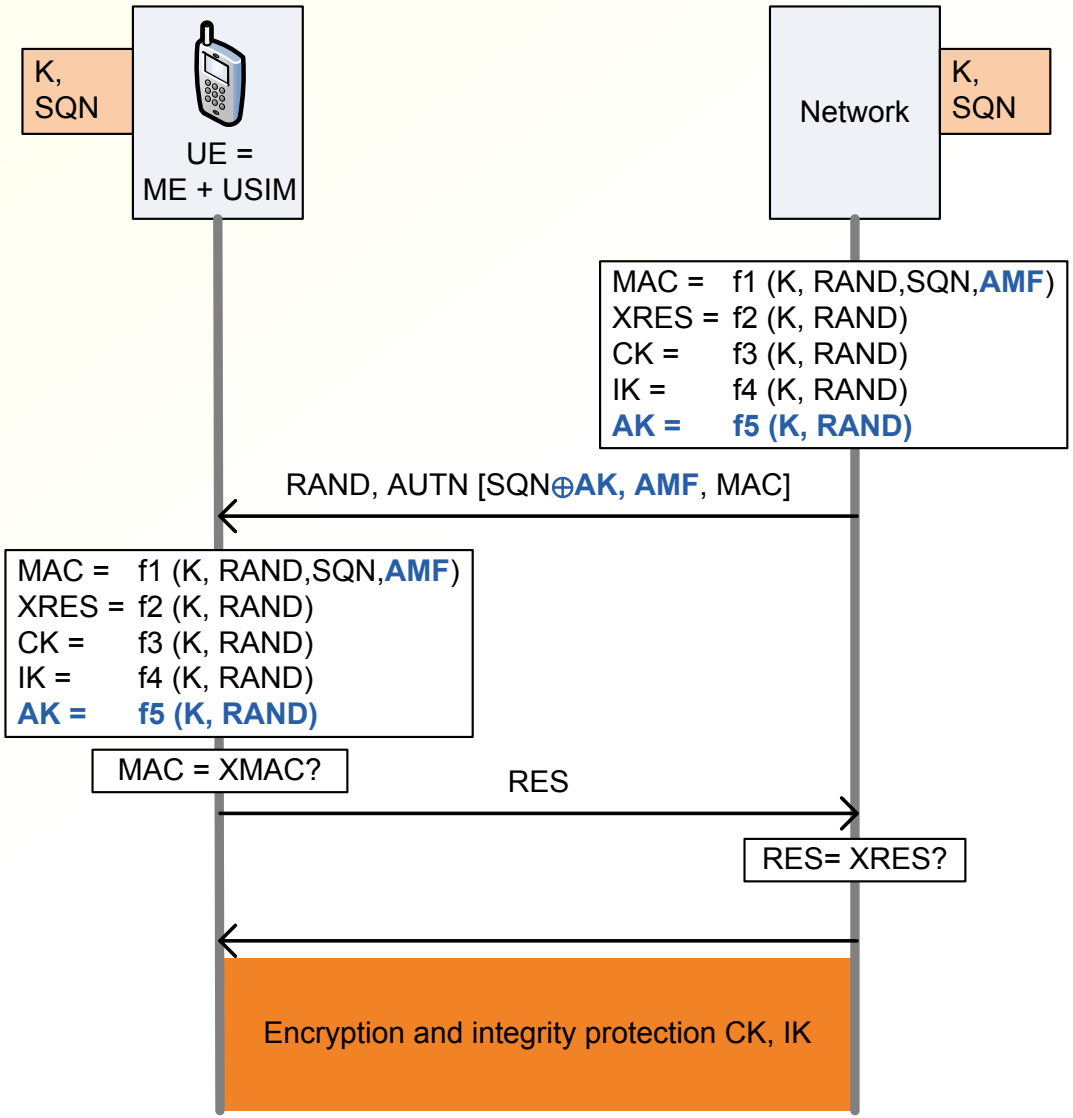
UMTS AKA (simplified)



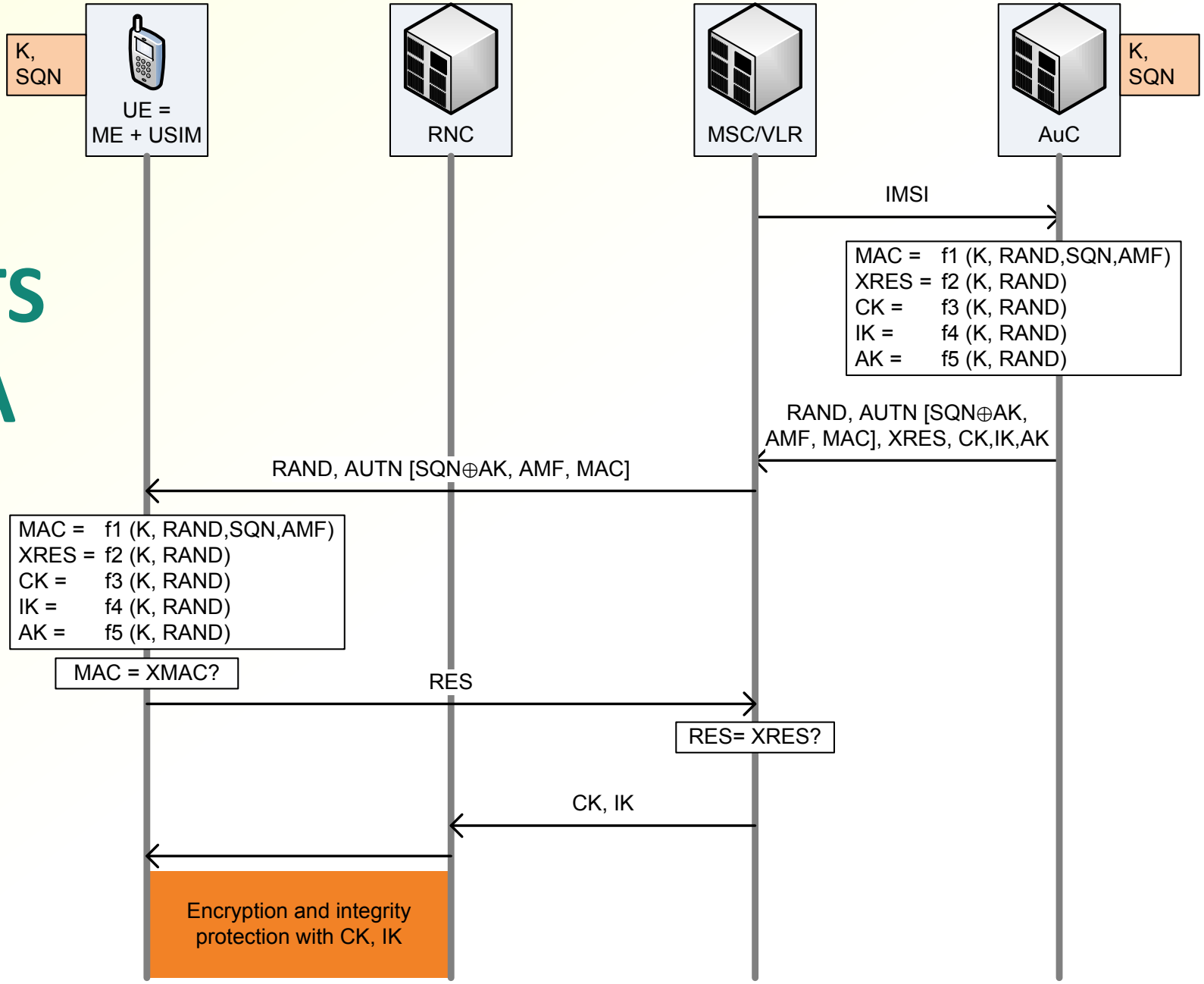
UMTS AKA (simplified)



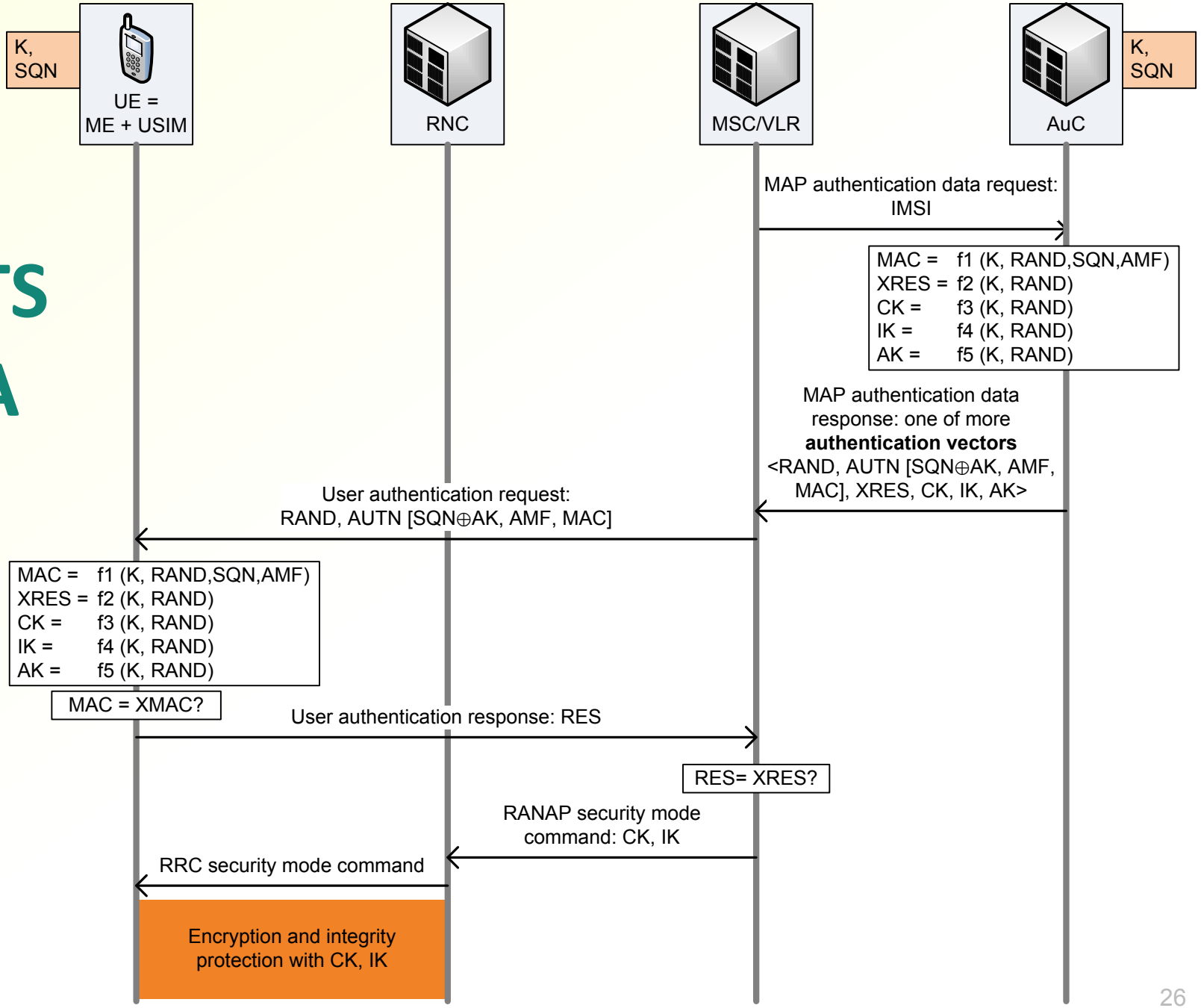
UMTS AKA


K,
SQN
UE =
ME + USIM
Network
K,
SQN
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
RAND, AUTN [SQN⊕AK, AMF, MAC]
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
MAC = XMAC?
RES
RES= XRES?
Encryption and integrity protection CK, IK

UMTS AKA


K,
SQN
UE =
ME + USIM
RNC
MSC/VLR
AuC
K,
SQN
IMSI
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
RAND, AUTN [SQN⊕AK,
AMF, MAC], XRES, CK,IK,AK
RAND, AUTN [SQN⊕AK, AMF, MAC]
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
MAC = XMAC?
RES
RES= XRES?
CK, IK
Encryption and integrity
protection with CK, IK

UMTS AKA


K, SQN
UE = ME + USIM
RNC
MSC/VLR
AuC
K, SQN
MAP authentication data request: IMSI
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
MAP authentication data response: one of more authentication vectors <RAND, AUTN [SQN⊕AK, AMF, MAC], XRES, CK, IK, AK>
User authentication request: RAND, AUTN [SQN⊕AK, AMF, MAC]
MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)
MAC = XMAC?
User authentication response: RES
RES= XRES?
RANAP security mode command: CK, IK
RRC security mode command
Encryption and integrity protection with CK, IK

UMTS authentication

- Alice-and-Bob notation:
  1. Network → terminal: RAND, SQN⊕AK, f1 (K, RAND, SQN)
  2. Terminal → Network: f2 (K, RAND)

  CK = f3 (K, RAND)

  IK = f4 (K, RAND)

  AK = f5 (K, RAND)
- USIM must store the highest received SQN value
- AuC must also store SQN and increment it for each authentication
- TMSI used in 3G just like in GSM
  - Masking SQN with AK prevents the use of SQN to identify the mobile

Sequence number SQN

- Implementation can be changed in USIM and AuC
  - Length is fixed to 48 bits
- One suggested implementation:

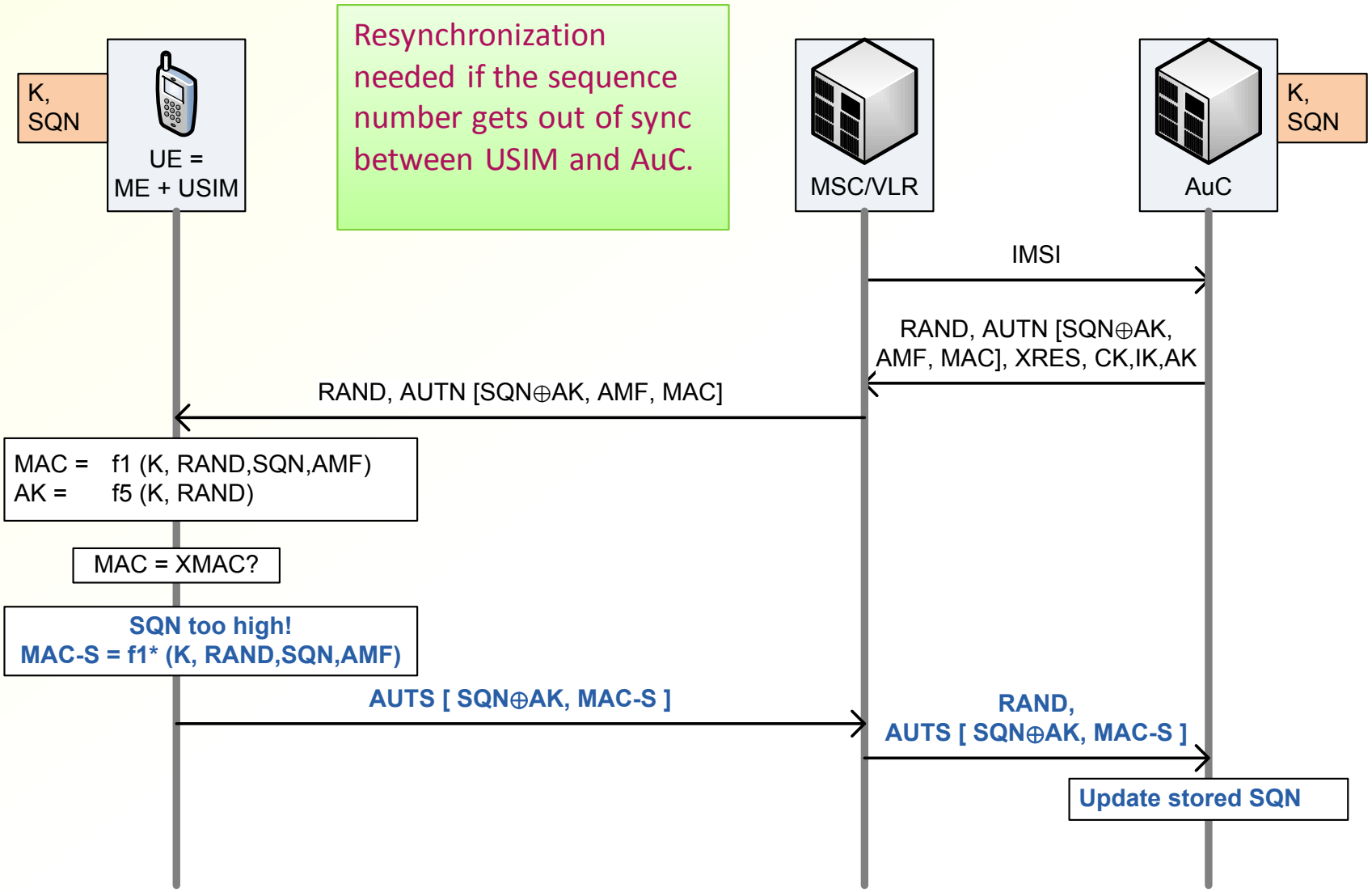
  - SEQ2 — time counter, 2^{24} seconds = 194 days, individual mobile may run ahead of the global time but can never be left behind
    (Note: the clock is local to AuC; mobile has no secure clock!)
  - SEQ1 — per-mobile epoch counter, incremented when SEQ2 wraps, or appears to wrap
  - IND — partitions the SQN space to independent sequences; highest used SEQ1|SEQ2 stored independently for each IND value 0..31
- IND enables creation of multiple simultaneously valid authentication vectors
  - Enables buffering of unused authentication vectors in VLR
  - Enables parallel authentication in CS, PS, IMS and WLAN domains

Staying in sync

SEQ1 (19 bits)	SEQ2 (24 bits)	IND (5 bits)

- Mobile may run ahead of the global time counter SEQ2 if it needs a burst of values; long-term authentication rate capped at 1/s
- Incrementing SEQ at AuC:
  - if SEQ2 is less than the global time counter, set equal
  - if equal or slightly (at most 2^{16}) higher than global time, increment by 1
  - otherwise, SEQ2 has wrapped → set SEQ2 equal to global time and increment SEQ1
- USIM stores the largest received value of SEQ1|SEQ2 for each IND value 0..31
  - If mobile receives a lower or equal value, authentication fails
  - If mobile receives a slightly higher value (SEQ1|SEQ2 increased by at most 2^{28} = 8.5 years), USIM updates the stored value
  - If the increment is larger than 2^{28}, USIM initiates a resynchronization procedure

RSQ Resynchronization



SQN resynchronization

- If USIM receives an SEQ1|SEQ2 value that is too much higher than the previous stored value, it sends AUTS to the AuC:

  AUTS = SQN⊕AK, MAC-S

  MAC-S = f1*(K, SQN, RAND, AMF)

  SQN = USIM's stored sequence number

- One extra roundtrip to AuC
  - May cause a noticeable delay, similar to when switching on a phone in a new country for the first time
  - The delay only takes place in exceptional situations → example of an optimistic protocol

Session protocol: encryption

- Encryption of MAC SDUs and RLC PDUs between terminal and RNC with the 128-bit session key CK
  - BS does not have the key → can use untrusted BS hardware
- Ciphertext =
  PDU ⊕ f8(CK, COUNT-C, bearer, direction, length)
  - f8 — based on block cipher KASUMI
  - CK = f3(K, RAND)
  - bearer – radio bearer identity, to enable simultaneous connection to multiple bearers, e.g. 3G and WLAN
  - direction — one bit, uplink or downlink
  - length — PDU length
  - COUNT-C = HFN|CFN
    CFN — RLC frame number
    HFN — hyper frame number, incremented when CFN wraps
    HFN is set to zero when rekeying with AKA

Session protocol: signalling integrity

- Authentication for RRC messages between terminal and RNC — signalling only!
- Message authentication code = f9(IK, message, direction, COUNT-I, FRESH)
  - f9 — based on block cipher KASUMI
  - IK = f4(K, RAND)
  - direction — one bit, uplink or downlink
  - COUNT-I = HFN|RRC sequence number
    HFN — incremented if the RRC sequence number wraps
    HFN is set to zero when rekeying with AKA
  - FRESH — random nonce chosen by RNC
- Monotonously increasing counter COUNT-I protects against replays during one session
- USIM stores highest COUNT-I, but RNC might not remember it. FRESH prevents the replay of old signalling messages if the RNC reuses old authentication tuples and, thus, old session keys

Session protocol: data integrity

- Integrity of voice data is not protected
  - Bit errors on the radio link are common
  - Voice encodings cope well with bit errors
  - Resending corrupt data would lead to lower voice quality
- Periodic local authentication: counter check
  - Terminal and RNC periodically compare the high-order bits of COUNT-C
  - Integrity of the counter check is protected by the MAC on RRC signalling
  - Release connection if large differences in couters
  - Makes it more difficult to spoof significant amounts of data

UMTS security weaknesses

- IMSI may still be sent in clear
- IMEI still not authenticated
- Non-repudiation for roaming charges is still based on server logs. No public-key signatures
- Still no end-to-end security
  - Thousands of legitimate radio network operators
    → Any government or big business gain control of one and intercept calls at RNC

Backward compatibility

- 3G users may roam in GSM networks:
  - Challenge RAND = c1(RAND)
  - Response SRES = c2(RES)
  - Encryption key Kc = c3 (CK, IK)
- Possible because the keys and algorithms are shared between SIM and AuC only, not by the mobile equipment or radio network

User authentication with mobile phone

User authentication with mobile phone

- Generic bootstrapping architecture (GBA):
  - The mobile operator provides an authentication service for the mobile subscriber to third parties e.g. to web-based services
  - Authentication is based on AKA and the secret key K in the USIM
  - 3GPP standard, but not widely used
- Mobile signature service (ETSI MSS) = mobile certificate
  - SIM card contains a public key pair and certificate, which is used to authenticate to third parties
  - Home operator needed every time to send an authentication request to the SIM (needed for charging, not for security)
  - E.g. see http://password.aalto.fi/
  - Detailed information: http://www.mobiilivarmenne.fi/en/, http://www.mobiilivarmenne.fi/documents/MSS_FiCom_Implementation_guideline_2.1.pdf
- Text messages as a second authentication method
  - Assumes that text messages cannot be intercepted
  - Google, Microsoft etc. send a secret code to the user's mobile phone for a second method of authentication (used in addition to a password)
  - Banks send transaction details and a secret code to the phone (used in addition to the password and one-time passcode)

Exercises

- Who could create false location traces in the GSM HLR and how? Is this possible in UMTS?
- Consider replacing the counter with a client nonce in AKA. What would be lost?
- Try to design a protocol where the IMSI is never sent over the air interface, i.e. the subscriber identity is never sent in clear. Remember that the terminal may have just landed from an intercontinental flight, and the terminal does not know whether it has or not
- Find the current cost of an IMSI catcher and fake GSM/3G base station for intercepting calls
- Learn about GBA and MSS. How is the operator involved in the protocols, and is it necessary?
- In GBA and MSS, there is a concept called *four-corner model*. What does it mean? Can you find a link between roaming and the four-corner model.

Related reading

- Gollmann, Computer security, 3rd ed. chaptes 19.2–19.3