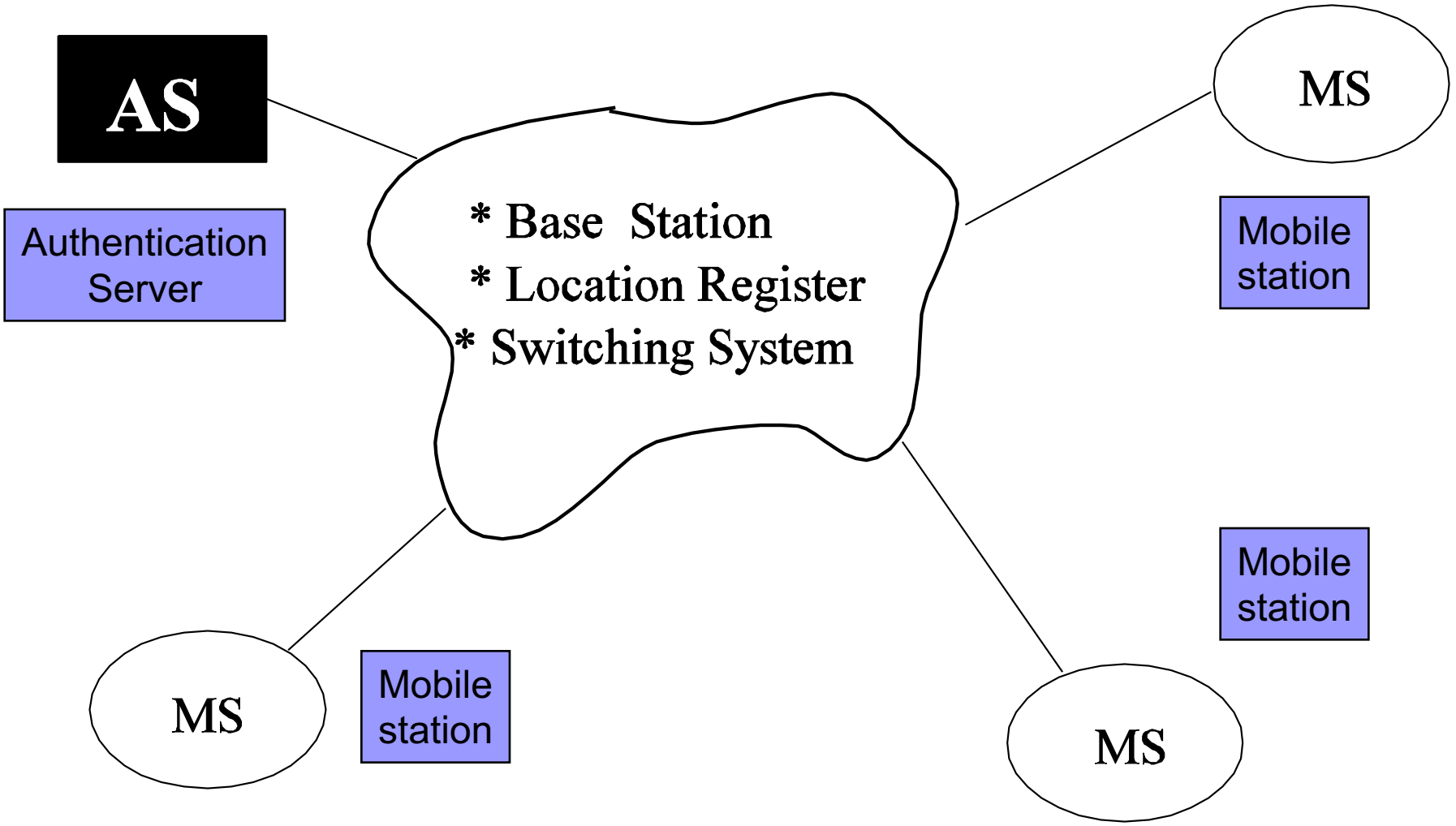
Mobile System Security

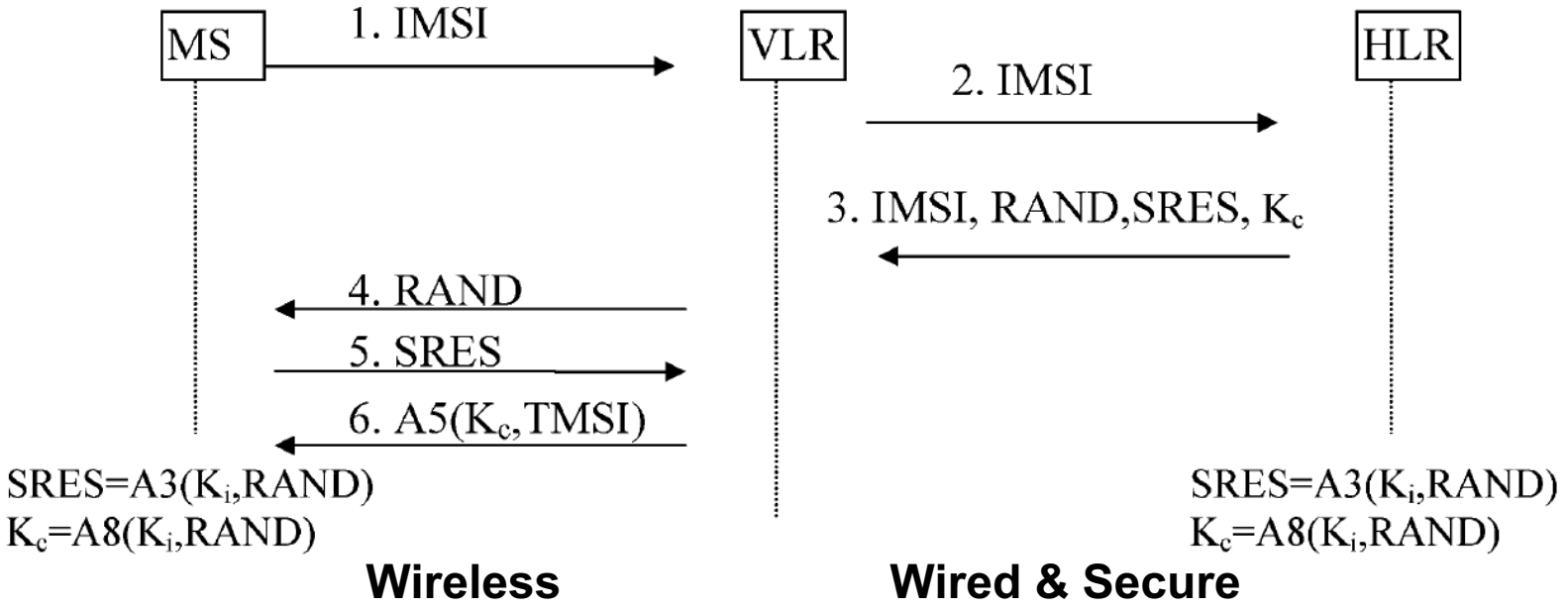
The mobile environment



Mobile System Security

- 2/…/5G telecommunication systems
- Security issues:
  - Authentication
  - Confidentiality
  - Integrity
  - ***Anonymity***

GSM Authentication and Key Agreement



IMSI: International mobile subscriber identity
TMSI: Temporary Mobile Subscriber Identity
Ki: the long-term symmetric-key shared between MS & HLR
RAND: a freshly generated random number
A3/5/8: cryptographic algorithms

VLR: visitor location register
HLR: Home location register

Step 0 - Setup

- MS subscribes to a mobile service provider
- A hardware token (e.g., a SIM card) is issued to the MS
  - An unique mobile ID (a.k.a. IMSI) and a secret key (i.e., Ki in the figure) are stored in the SIM card
  - The mobile ID and secret key are also stored in the database of the mobile service provider (i.e., HLR)

Step 1

- **MS → VLR: IMSI**

- When the MS is powered on, it sends its IMSI to the VLR
- The IMSI will allow VLR to identify the HLR of the MS

Step 2

- **VLR → HLR: IMSI**

- The VLR forwards the IMSI to HLR in order to obtain a set of authentication credentials

Step 3

- **HLR → VLR: IMSI, RAND, SRES, Kc**

- Upon receiving the request from VLR, HLR locates the secret key Ki for IMSI
- It generates a random number RAND, and computes SRES = A3(Ki, RAND), Kc = A8(Ki, RAND)
- HLR sends RAND, SRES and Kc to VLR

The communication between VLR and HLR is done through a secure channel

Step 4

- **VLR → MS: RAND**

- Upon receiving the authentication credentials (i.e., RAND, SRES, Kc) from VLR, it forwards RAND to MS as a challenge

Step 5

- **MS → VLR: SRES**

- Upon receiving RAND from the VLR, MS computes SRES = A3(Ki, RAND), Kc = A8(Ki, RAND) using the secret key Ki stored in the SIM card
- MS sends SRES as the response to VLR's challenge
- VLR verifies the SRES by comparing it with the SRES from HLR
- If the SRES from MS is correct, MS is authenticated

Step 6

- **VLR → MS: A5(Kc, TMSI)**

- VLR picks a temporary mobile ID (a.k.a. TMSI) for MS and sends it to MS in encrypted form
- MS derives Kc based on RAND and Ki, decrypts TMSI and uses it as its temporary ID
- TMSI is used as the identity of MS in the subsequent communications

Questions

- Is there any attack against this protocol?
- How does TMSI provide anonymity protection?

3GPP AKE

- VLR Authentication is included
- An SQN-based authentication mechanism is employed
  - Advantage: authentication can be done in one pass
  - Disadvantage: counters may become de-synchronized, and hence a re-synchronization mechanism is required

SQN-based authentication (from A to B)

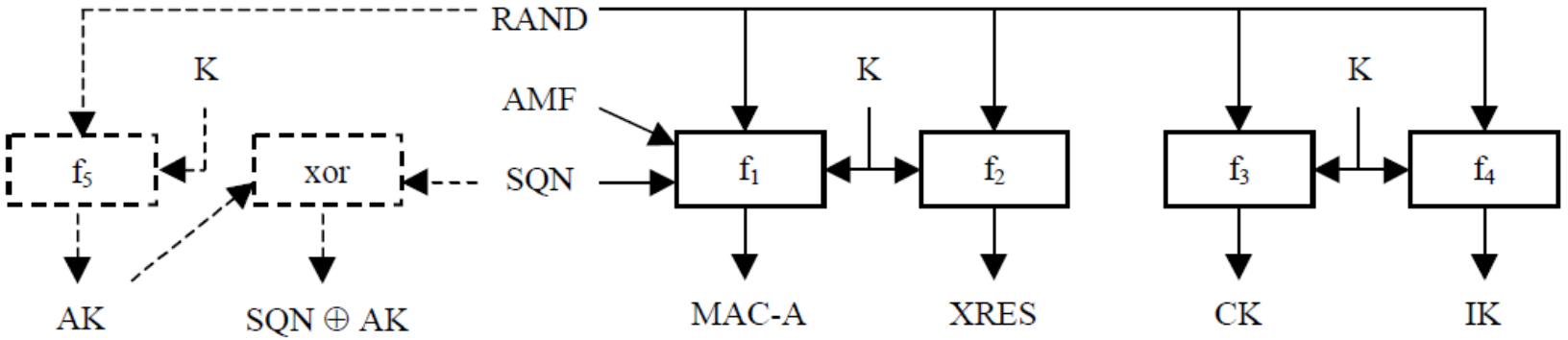
A (K, SQNa) B (K, SQNb)

- Setup:
  - A and B share a secret key K
  - A and B each maintains a sequence-number (or counter)
  - Initially, SQNa = SQNb
  - A and B share a Message Authentication Code function F

SQN-based authentication (from A to B)

- Authentication:
  - A updates its counter SQNa = SQNa + 1
  - A sends to B

    SQNa, M, MAC-A = F(K, SQNa, M)
  - B verifies that
    - SQNa > SQNb
    - MAC-A == F(K, M, SQNa)
    - If both verifications succeed, accept M and update SQNb = SQNa



AUTN = SQN [⊕ AK] || AMF || MAC-A
Q = (RAND, XRES, CK, IK, AUTN)

- **SQN-based VLR authentication in 3GPP**
- Setup: HLR (K, SQN) MS(K,SQN)

- Authentication protocol:
- Steps 1 & 2 remain the same as in GSM
- **Step 3:**
  - **Upon receiving the IMSI from VLR, HLR updates its counter to SQN = SQN + 1**
  - **HLR computes the authentication credential Q = (RAND, XRES, CK, IK, AUTN) and sends it to VLR**
- **Step 4:**
  - **VLR sends (RAND, AUTN) to the MS**
  - **MS verifies AUTN according to the SQN-based authentication**
- Finish the rest of the authentication protocol