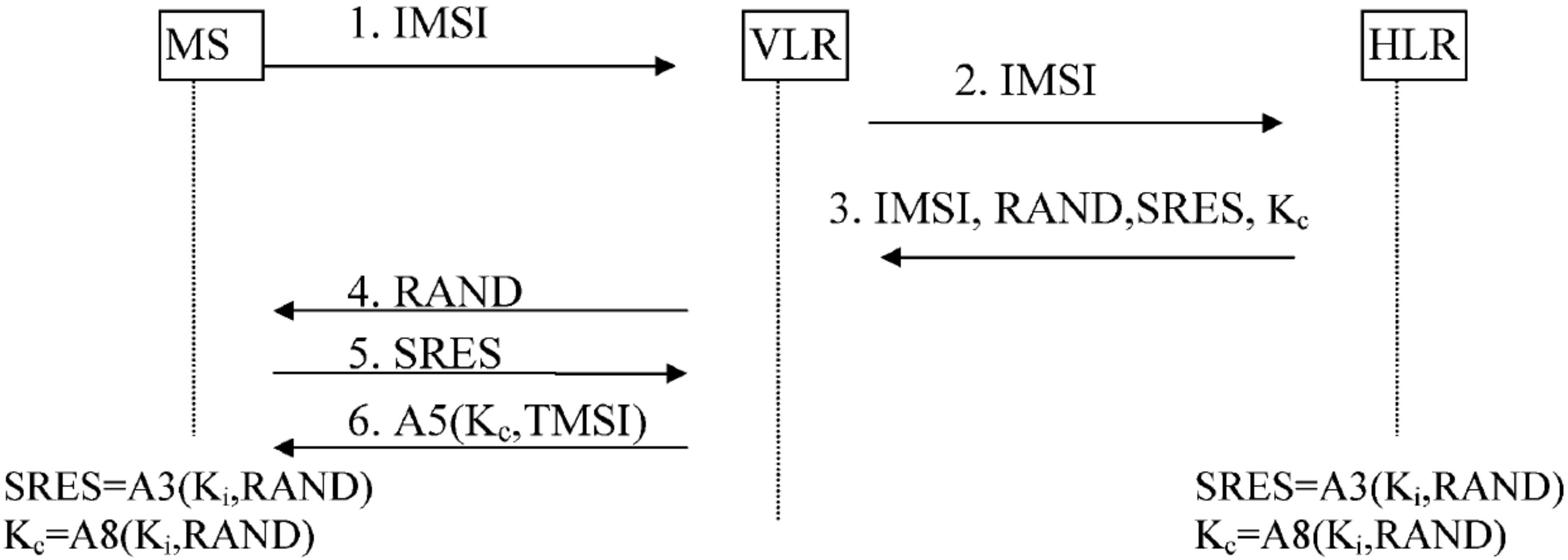
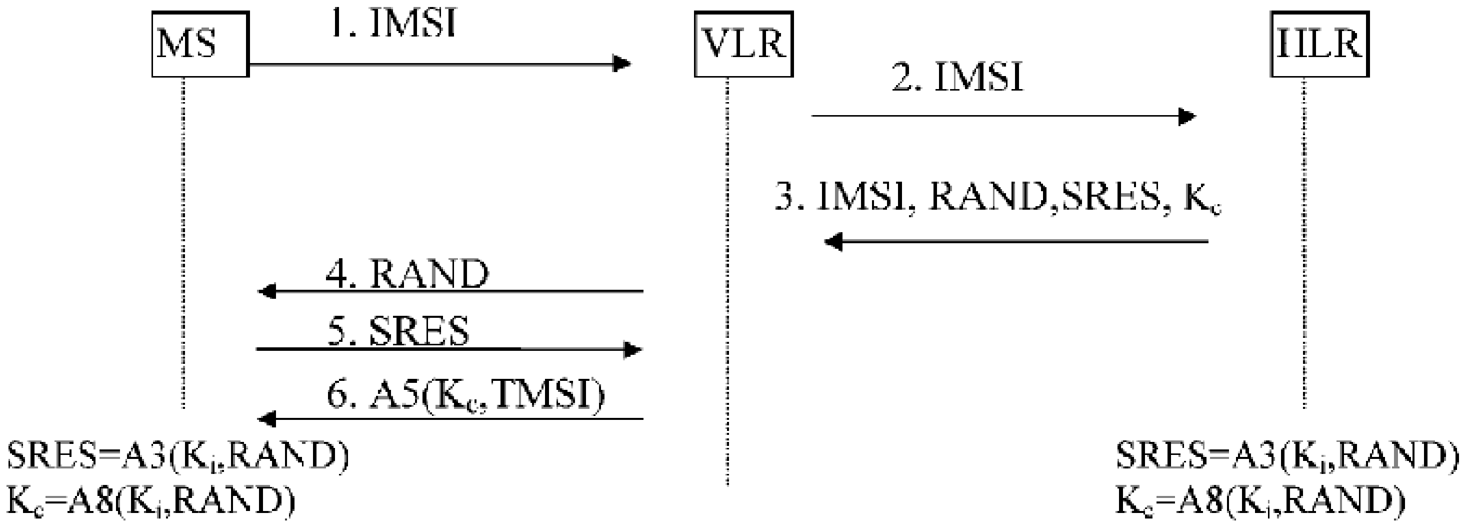
Tutorial 8

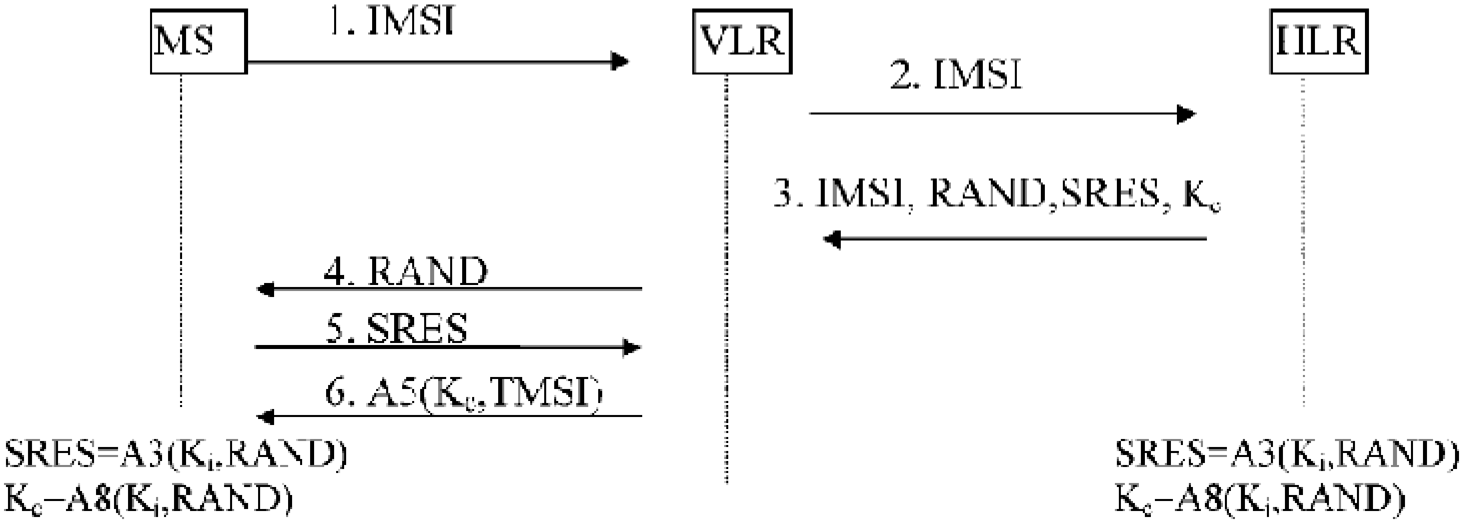
GSM AKA


MS
VLR
HLR
1. IMSI
2. IMSI
3. IMSI, RAND,SRES, K_c
4. RAND
5. SRES
6. A5(K_c,TMSI)
SRES=A3(K_i,RAND)
K_c=A8(K_i,RAND)
SRES=A3(K_i,RAND)
K_c=A8(K_i,RAND)



- Is a replay attack against the protocol possible?

- Is the 3GPP AKA protocol vulnerable to the replay attack?



- In order to enhance the anonymity of the mobile station, suppose the following modified protocol is used
  - The MS and the VLR perform a Diffie-Hellman key exchange on-the-fly
  - The MS uses the agreed Diffie-Hellman key to encrypt its identity (i.e., IMSI) and sends the encrypted identity to VLR
  - VLR decrypts the data to obtain IMSI and continues the rest of the protocol
- Does the above approach work?

Mobile Authentication Protocol based on PKC

- GSM and 3GPP are based on symmetric key cryptography
- Limitations:
  - Weak anonymity
  - No forward secrecy
- Protocols with stronger security can be obtained by using PKC
- Below is an example

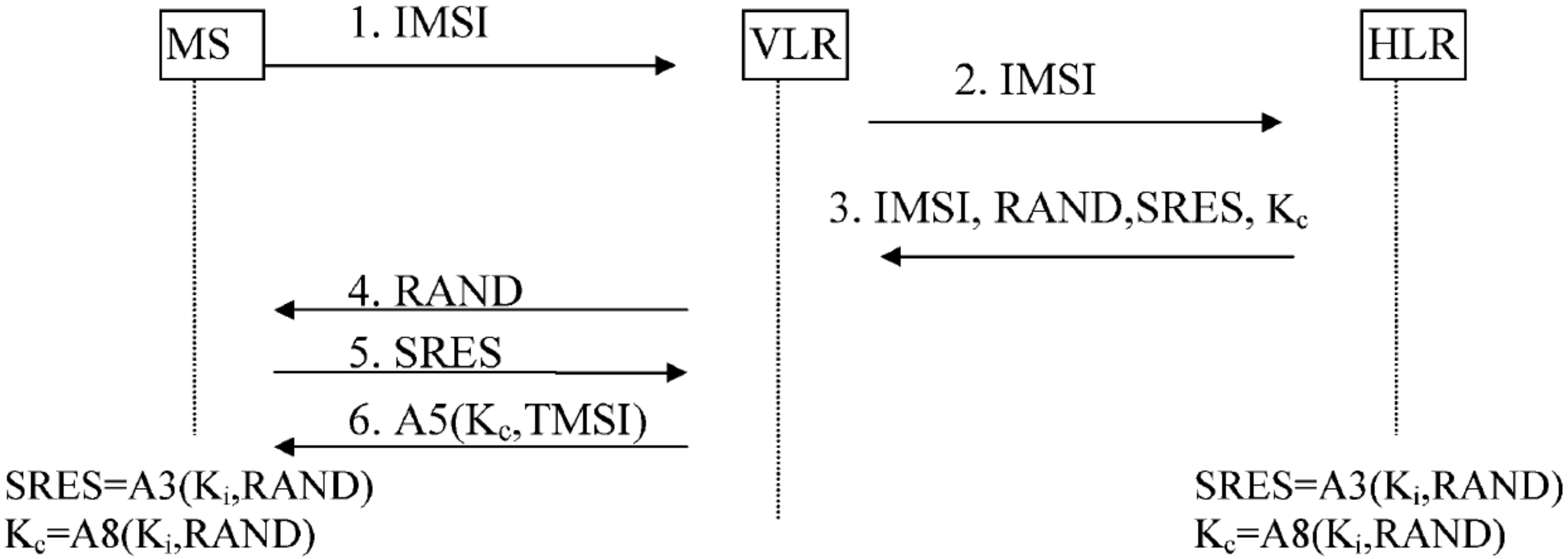
$$
\begin{array}{lll}
(1) & M \rightarrow V & g^{r_M}, TID_M, H \\
(2) & V \rightarrow H & g^{r_V}, g^{r_M}, TID_M, \\
 & & \{h(g^{r_V}, g^{r_M}, TID_M, V)\}_{SK_V}, T_V, cert_V \\
(3) & V \leftarrow H & g^{r_H}, [\{h(g^{r_H}, g^{r_V}, h(M) \oplus g^{r_M}, H)\}_{SK_H}, \\
 & & h(M) \oplus g^{r_M}]_{K_{VH}}, T_H, cert_H \\
(4) & M \leftarrow V & g^{r_V}, \{h(g^{r_V}, g^{r_M}, TID'_M, V), T_H\}_{K_{MV}}, \\
 & & T'_V, cert_V \\
(5) & M \rightarrow V & [\{h(g^{r_M}, g^{r_V}, T_H, V)\}_{SK_M}, T'_V, cert_M]_{K_{MV}}
\end{array}
$$

- $K_{MH} = g^{SK_H \cdot r_M}$, is used to encrypt the information about real identity of a user M and generate his initial temporary identity $TID_M = \{h(M) \oplus g^{r_M}\}_{K_{MH}}$. It can be computed with the random number selected by M and the public key of the home network H, $PK_H = g^{SK_H}$, already known to the user.
- $K_{VH} = h1(g^{r_V \cdot r_H}, g^{r_H \cdot SK_V})$, which is used for message encryption between V and H. It can be computed with the random numbers chosen by both parties and the public key of V.
- $K_{MV} = h1(g^{r_M \cdot r_V}, g^{SK_V \cdot r_M})$, is used for the message encryption and authentication between M and V. It can be computed with the random numbers chosen by both parties and the public key of V

$$TID_M = \{h(M) \oplus g^{r_M}\}_{K_{MH}}$$

$$TID'_M = h(g^{r_M \cdot r_V}, h(M))$$

GSM Authentication and Key Agreement



MS

VLR

HLR

1. IMSI

2. IMSI

3. IMSI, RAND,SRES, K_c

4. RAND

5. SRES

6. A5(K_c,TMSI)

SRES=A3(K_i,RAND)
K_c=A8(K_i,RAND)

SRES=A3(K_i,RAND)
K_c=A8(K_i,RAND)

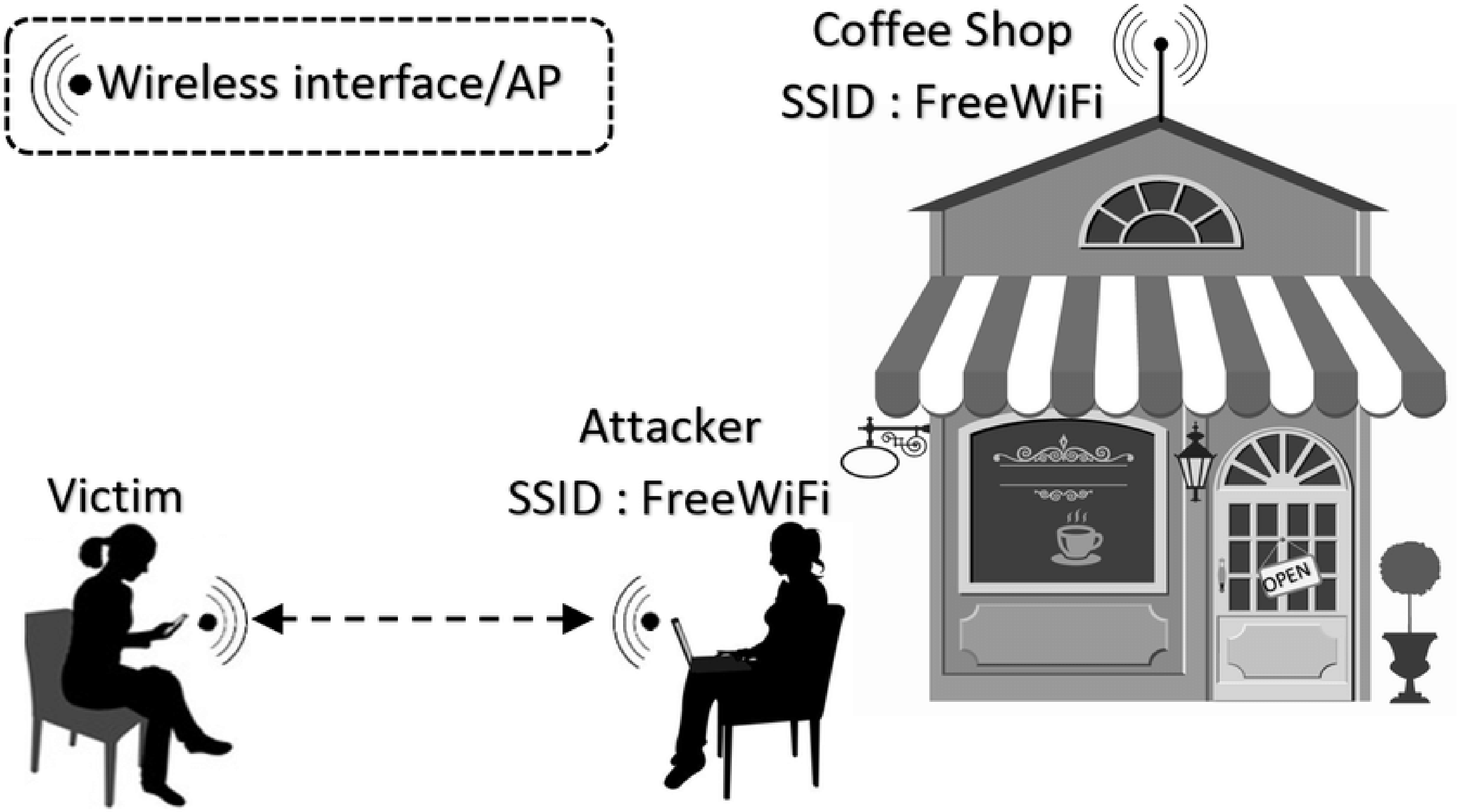
Wireless **Wired & Secure**

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

How to provide anonymity such that IMSI is unknown to VLR?

Discussions(Different Cases, Different Answers)



A coffee shop provides free wifi but an attacker is trying to cheat as the hotspot. When the victim is connecting to this hotspot, what could happen?