安全协议设计与分析

第六讲：移动通信中的安全协议

李晖 网络空间安全学院

Previous lectures:

- **Goals for security protocol**
  - To know if a protocol is secure you must know what is aims to achieve.
  - Example: Diffie-Hellman & STS Protocol.
- **Attacks and Principles**
  - Common types of attacks on protocols.
  - Good design principles for protocol.
- **Basic security protocols**
  - Authentication protocols

This lecture

- 移动通信安全的发展过程
- 2G(GSM)中的接入认证与密钥协商协议
- 3G(WCDMA)中的接入认证与密钥协商协议
- 4G(LTE)中的接入认证与密钥协商协议
- 5G中的接入认证与密钥协商协议

移动安全的发展

移动通信网络的空口安全历史

- 安全从无到有
- 安全从弱到强
- 安全从简单到复杂

无任何安全机制

1G

1.单向认证
2.机密性保护
3.临时标识匿名

2G

1.双向认证
2.机密性保护
3.临时标识匿名
4.完整性保护

3G

1.双向认证
2.机密性保护
3.临时标识匿名
4.完整性保护
5.复杂密钥体系

4G

1.新的认证协议
2.机密性保护
3.完整性保护
4.引入安全锚功能
5.新增认证服务器
6.更为复杂的密钥体系
7.基于公钥的匿名

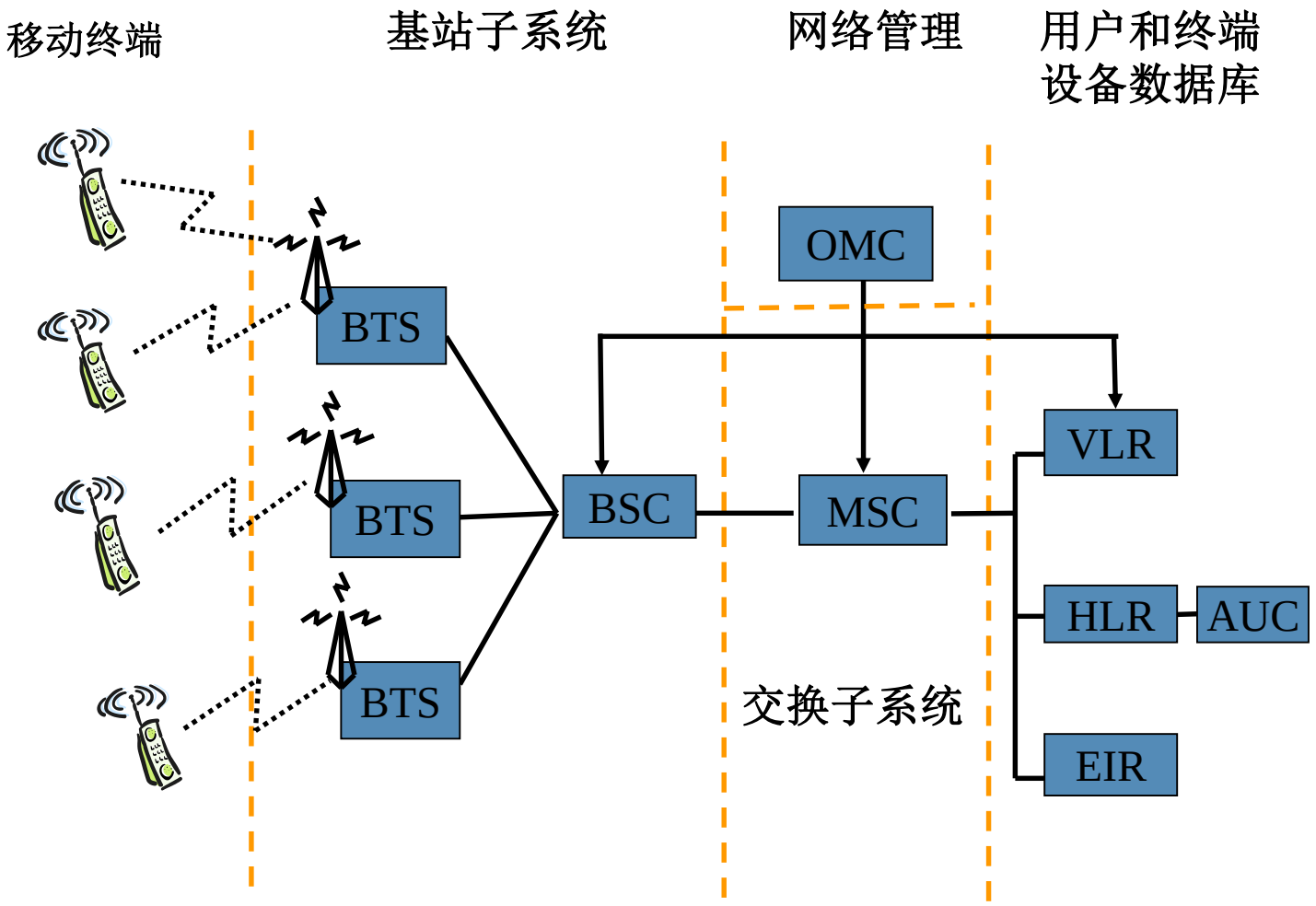
5G

种类繁多

This lecture

- 移动通信安全的发展过程
- 2G(GSM)中的认证与密钥协商协议
- 3G(WCDMA)中的认证与密钥协商协议
- 4G(LTE)中的认证与密钥协商协议
- 5G中的认证与密钥协商协议

2 GSM系统网络结构


移动终端
基站子系统
网络管理
用户和终端
设备数据库
BTS
BTS
BTS
BSC
OMC
MSC
VLR
HLR
AUC
EIR
交换子系统

GSM中的标识码

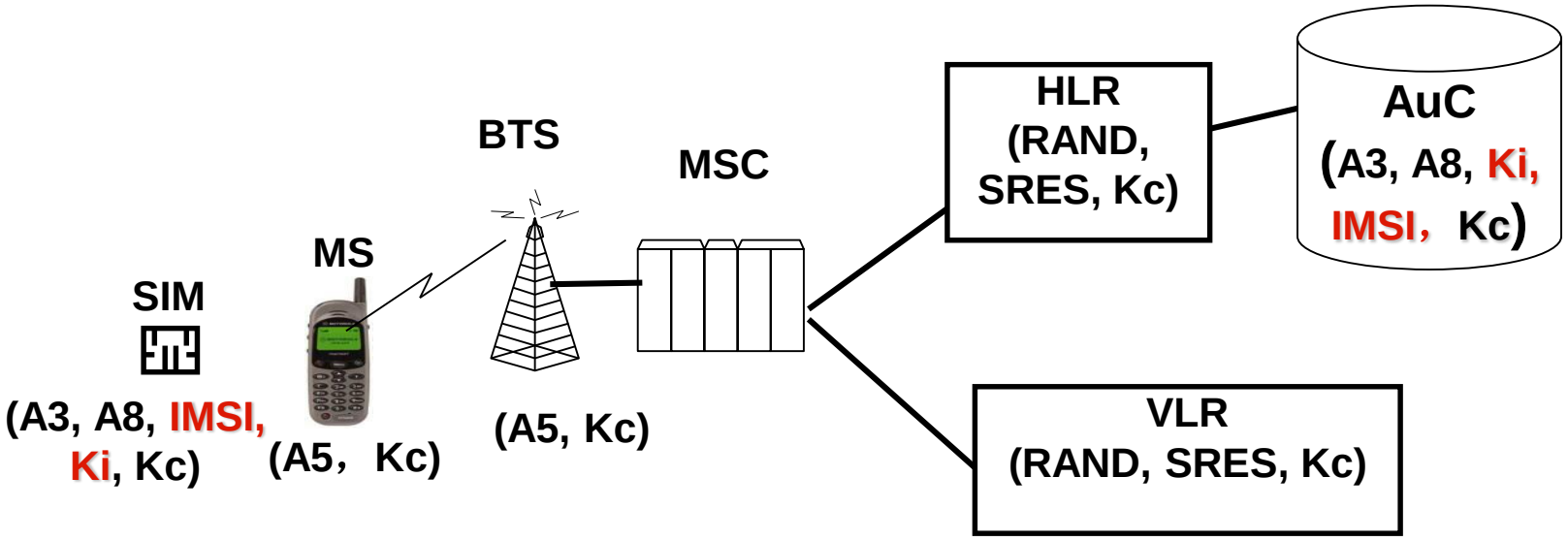
- IMEI：国际移动台设备识别码(6+2+6+1位数字)

- MSISDN：国际移动用户电话号码

- IMSI：国际移动用户标识（3+2+10位数字，64bits）

- TMSI: 临时移动用户标识（32bits）

GSM安全相关参数和算法分布



- 两种密钥K_i和K_c
- 三个算法**A3**、**A8**和**A5**

HLR: Home Location Register
MSC: Mobile Switch Center
AuC: Authentication Center
RAND: Random
SRES: Signed Response

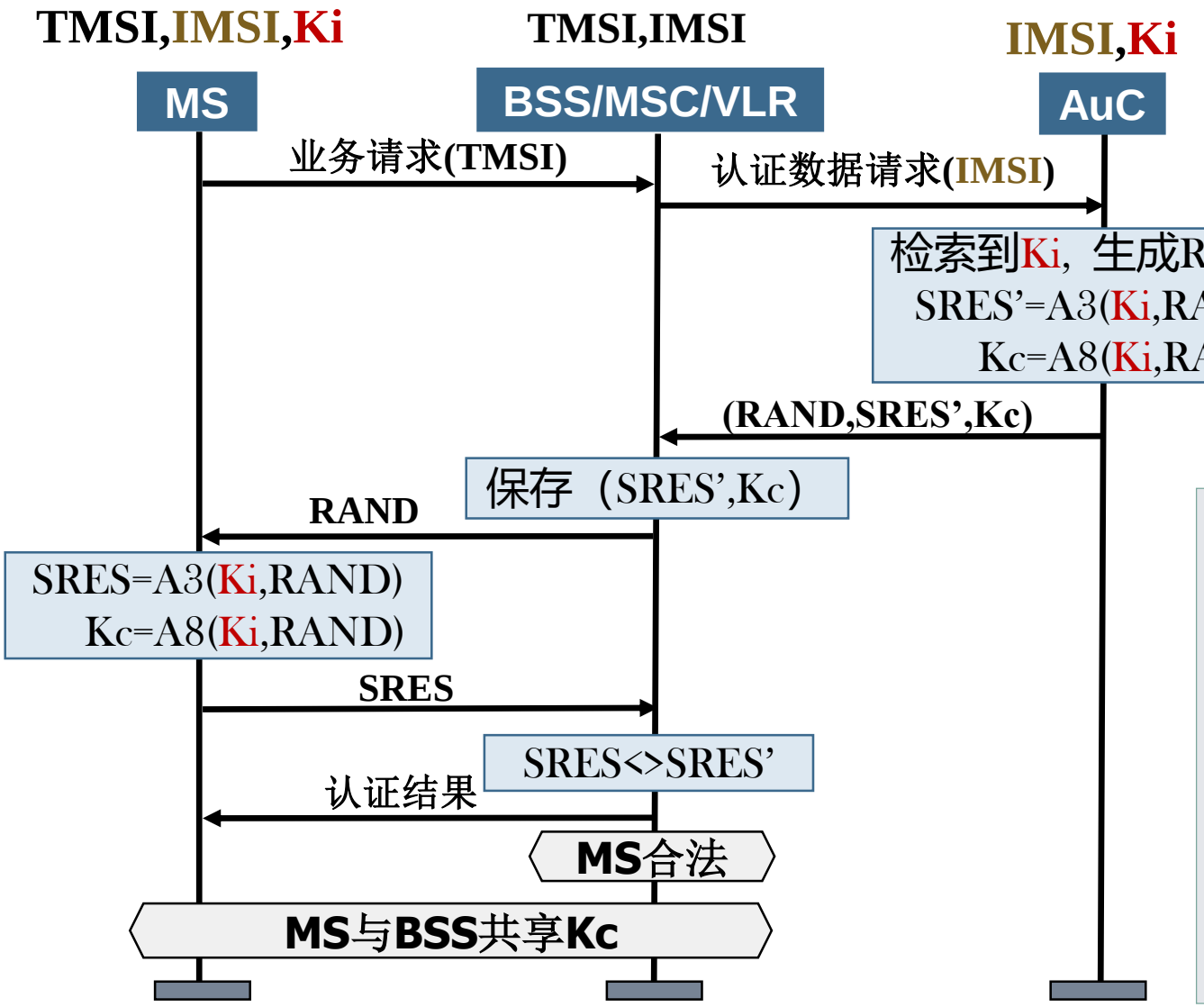
用户鉴权

- **鉴权的目的**
  - 鉴别SIM卡的合法性
  - 保护网络免受非授权使用
  - 建立会话密钥
- **鉴权方案**
  - 通过IMSI或TMSI标识用户
  - 通过挑战－应答方式由网络认证用户

用户鉴权（2）

- **鉴权场合**
  - 移动用户发起呼叫（不含紧急呼叫）
  - 移动用户接受呼叫
  - 移动台位置登记
  - 移动用户进行补充业务操作
  - 切换（包括同一MSC内从一个BS切换到另一个BS、在不同MSC之间切换）

用户鉴权（3）



✓ **认证成功:**

SIM卡和AuC共享密钥Ki及算法A3

✓ **Kc的一致性:**

认证成功及A8的一致性

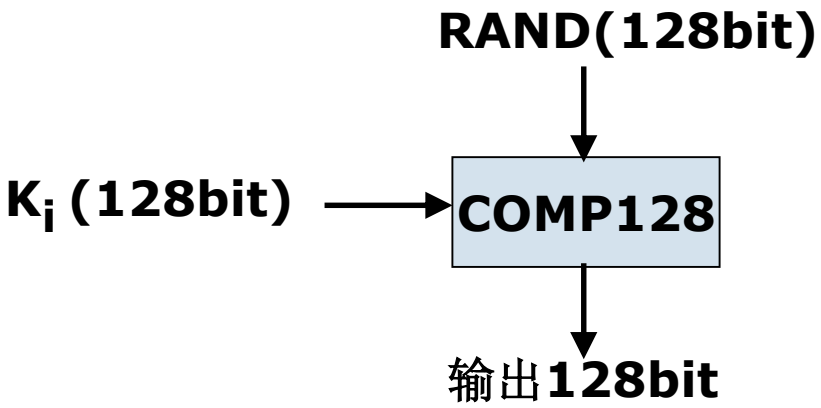
✓ **Kc的排它性**

Kc不会在空中传输

GSM用户鉴权协议

A3和A8算法的实现

- **A3和A8算法都在SIM卡和AuC中实现**
- **A3和A8算法在SIM卡中的运算时K_i不出卡**
- **算法的具体实现由运营商决定**
- **大部分的GSM网络运营商都选用COMP128作为A3和A8算法的实现**
- **COMP128是一个带密钥的散列函数。**



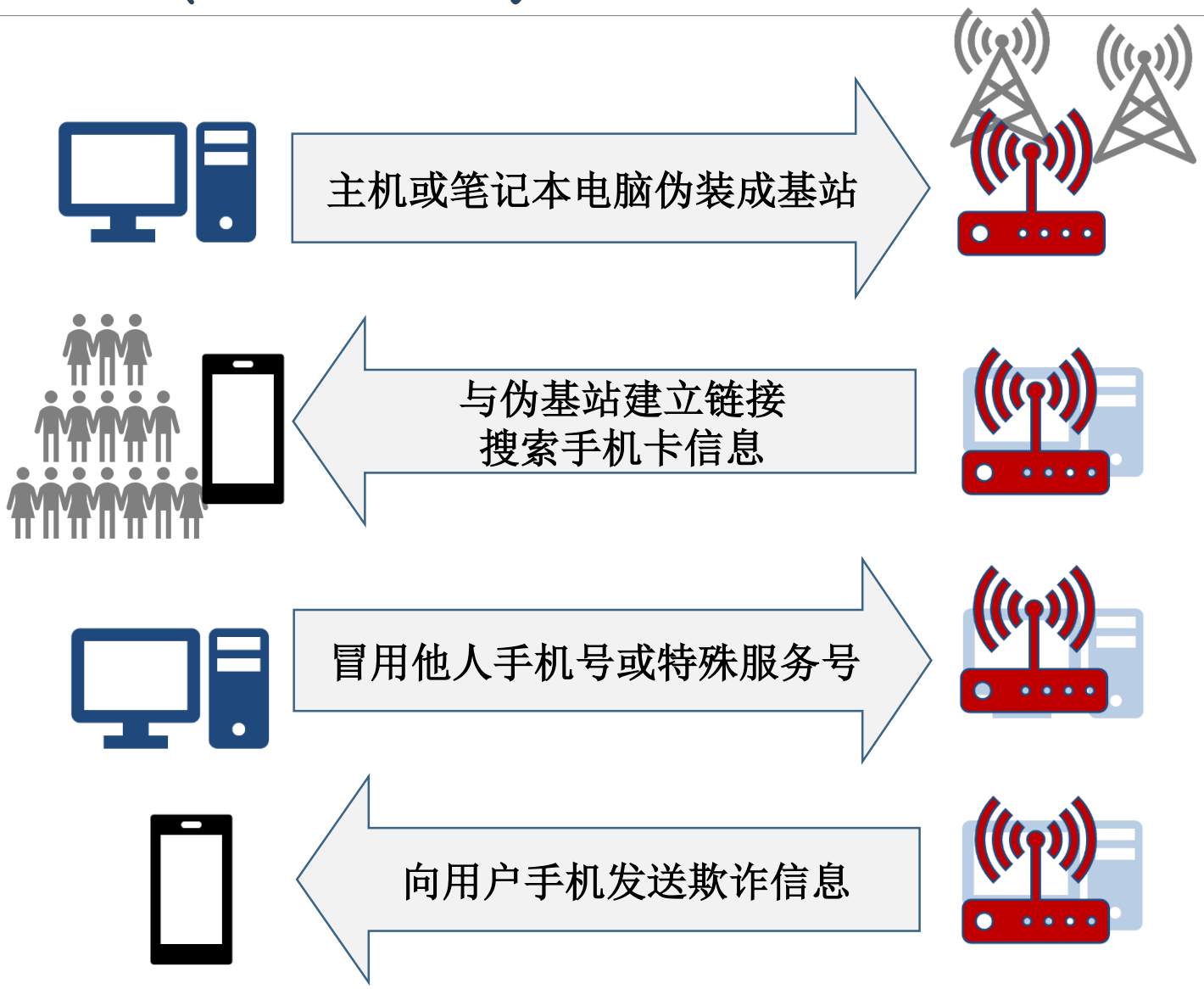
0-31bit作为SRES, 74-127（*54*） bit 作为Kc，后10位由0来补充

空中接口攻击(伪基站攻击)

- “伪基站”即假基站，设备一般由主机和笔记本电脑或手机组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息，利用2G移动通信的缺陷，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

空中接口攻击(伪基站攻击)

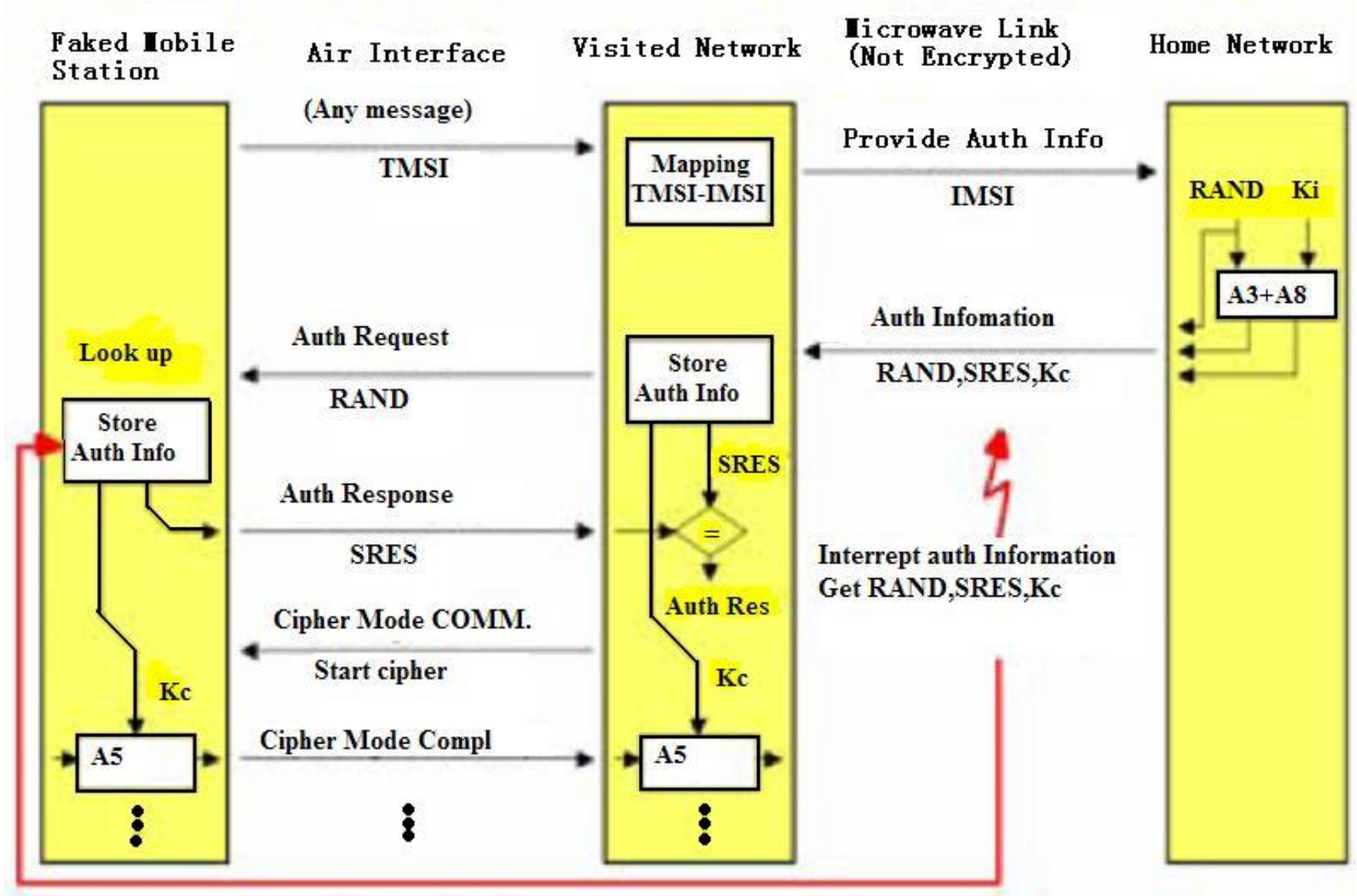
伪基站攻击



空中接口攻击(伪基站攻击)

- 伪基站攻击的原因
  - 无线接口是开放信道
  - GSM中的鉴权是单向的，缺乏MS对网络侧的认证
- 伪基站攻击的特点
  - 伪基站具有很强的流动性，很难检测
  - 伪基站设备主要由主机、笔记本电脑组成，犯罪成本低
  - 伪基站对用户及通信造成的损失难以估计、定罪周期长

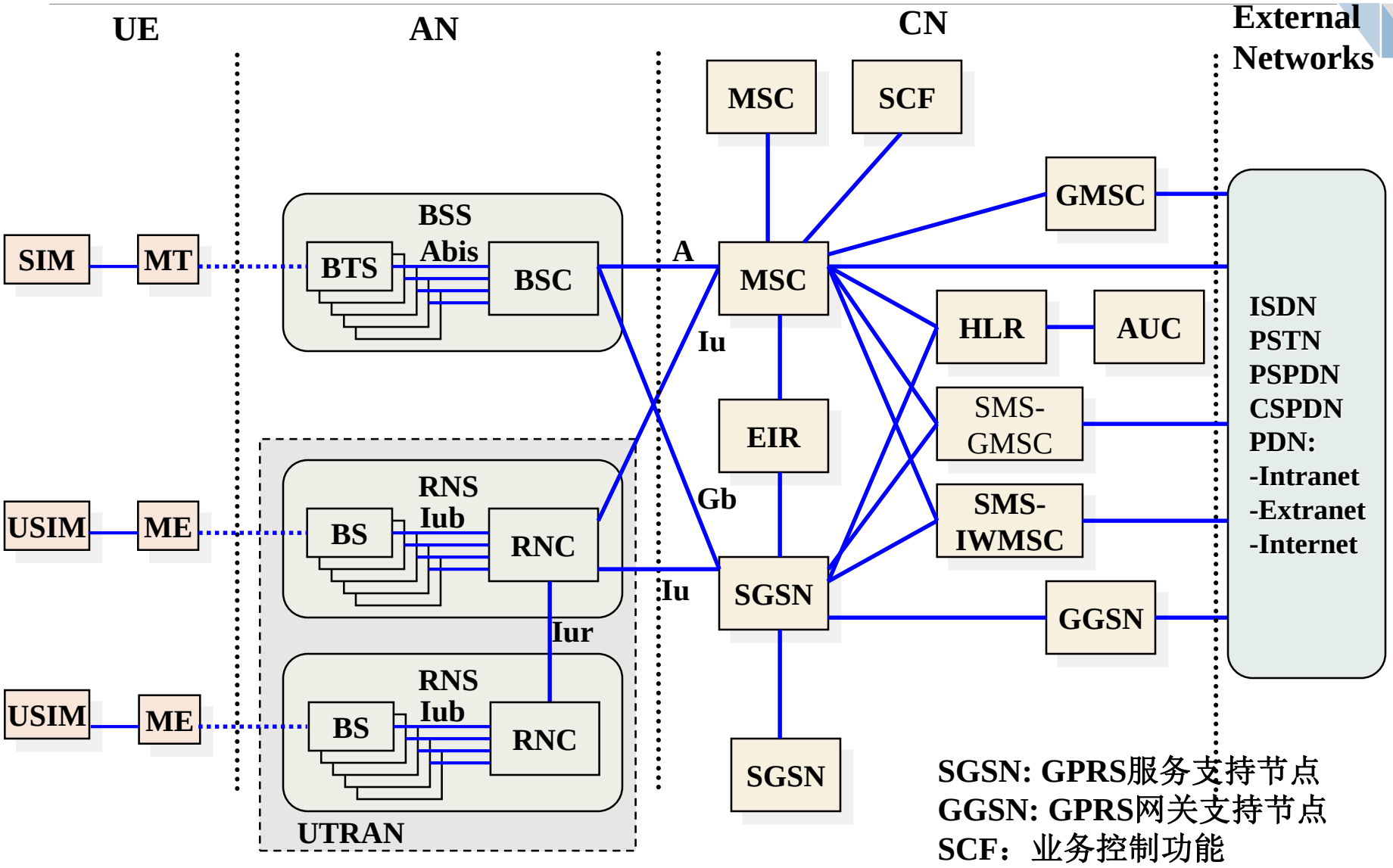
核心网络攻击


Faked Mobile Station
Air Interface
Visited Network
Microwave Link (Not Encrypted)
Home Network
(Any message)
TMSI
Mapping TMSI-IMSI
Provide Auth Info
IMSI
RAND
Ki
A3+A8
Look up
Auth Request
RAND
Store Auth Info
Auth Infomation
RAND,SRES,Kc
Store Auth Info
SRES
Auth Response
SRES
=
Interrept auth Information
Get RAND,SRES,Kc
Auth Res
Cipher Mode COMM.
Start cipher
Kc
Kc
A5
Cipher Mode Compl
A5

This lecture

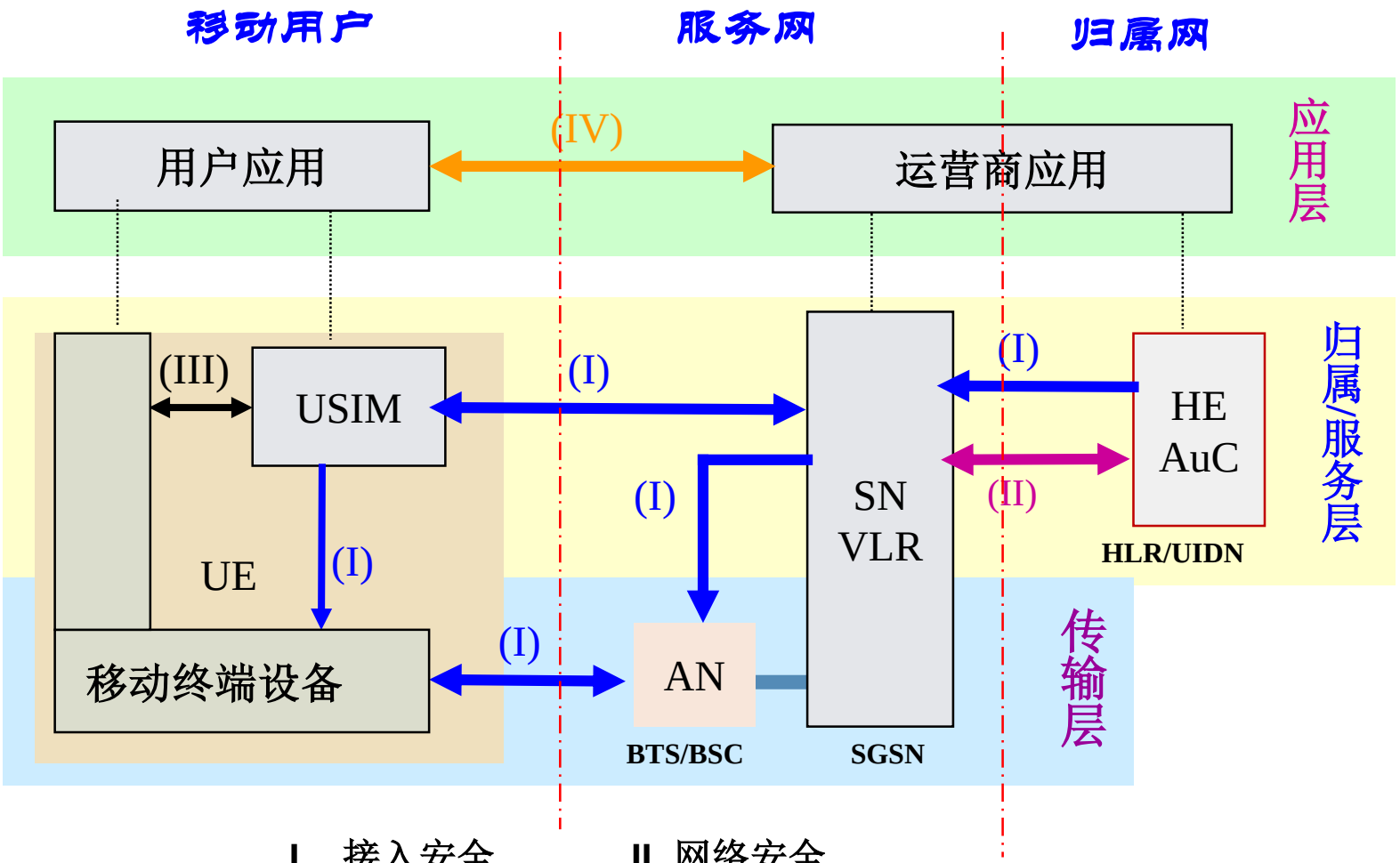
- 移动通信安全的发展过程
- 2G(GSM)中的认证与密钥协商协议
- 3G(WCDMA)中的认证与密钥协商协议
- 4G(LTE)中的认证与密钥协商协议
- 5G中的认证与密钥协商协议

3G系统网络结构



SGSN: GPRS服务支持节点
GGSN: GPRS网关支持节点
SCF：业务控制功能

3G安全体系结构



I. 接入安全　　II. 网络安全
III. 用户安全　　IV. 应用安全
V. 安全可见性与可配置性

认证与密钥协商(AKA)

- **AKA的目的**:
  - 完成网络与用户的双向认证
  - 生成加密密钥(CK) 和完整性密钥(IK)
  - 确保CK/IK 的新鲜性，即以前没有使用过
- **AKA的前提条件**:
  - 认证中心（AuC) 和USIM 卡共享：
    - ✓ 用户唯一的秘密认证密钥K
    - ✓ 消息认证函数f1,f1*,f2
    - ✓ 密钥产生函数f3,f4,f5,f5*
  - AuC 有随机数产生函数
  - AuC 能够产生新的序列号
  - USIM 能够验证收到的序列号的新鲜性

AKA中用到的变量和函数

K = 由USIM和AuC共享的主密钥

RAND = f0，由AuC产生的随机数，认证时的挑战（Challenge）

XRES = $f2_K$ (RAND)，由AuC计算的期望响应

RES = $f2_K$ (RAND)，由USIM计算出的响应

CK = $f3_K$ (RAND)，空中接口加密密钥

IK = $f4_K$ (RAND)，空中接口完整性保护密钥

AK = $f5_K$ (RAND)，匿名密钥（Anonymity Key）

SQN = 序列号

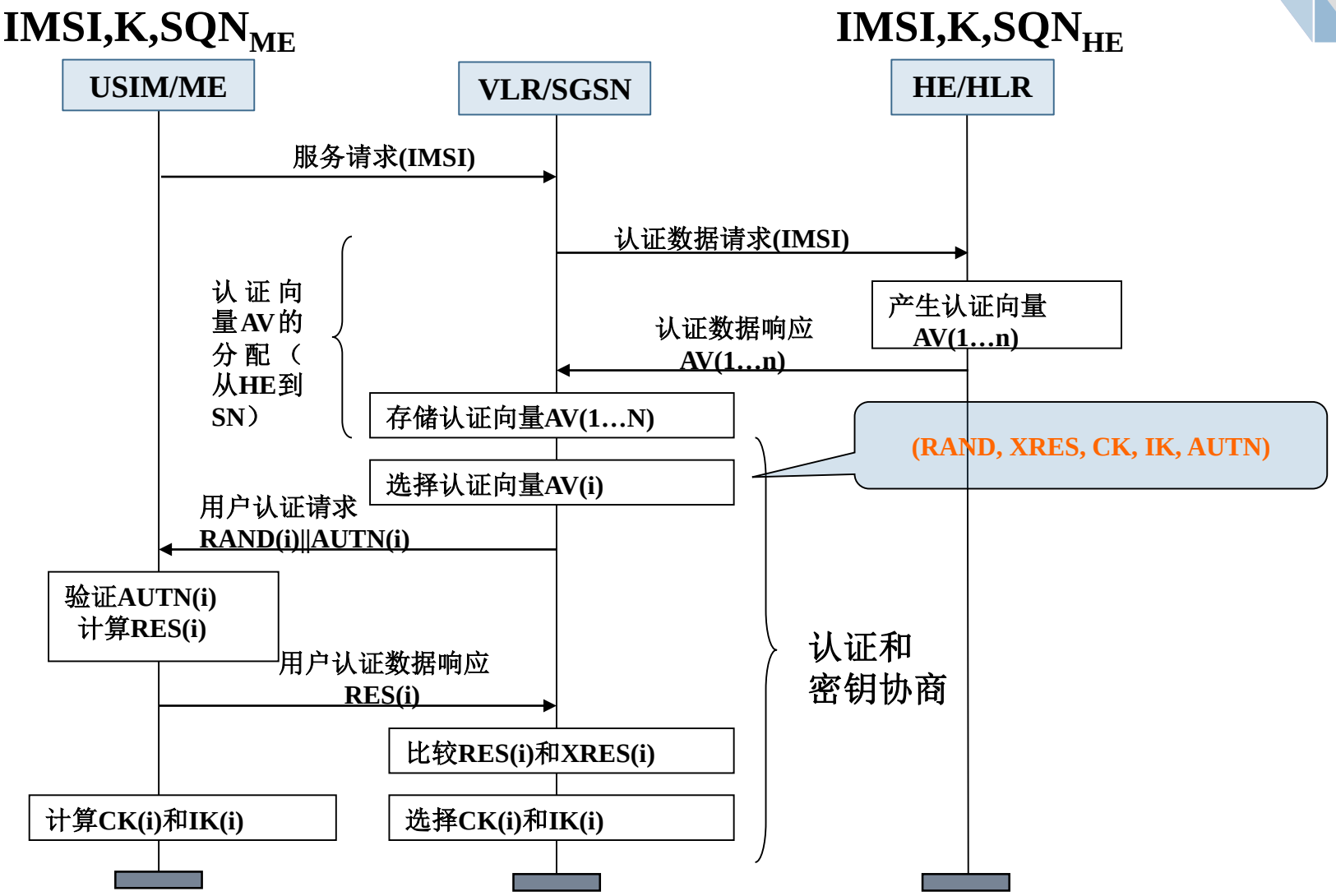
AMF = 认证管理域（Authentication Management Field）

MAC = $f1_K$(SQN || RAND || AMF)，网络侧消息认证码

AUTN = SQN⊕AK || AMF || MAC，网络认证令牌

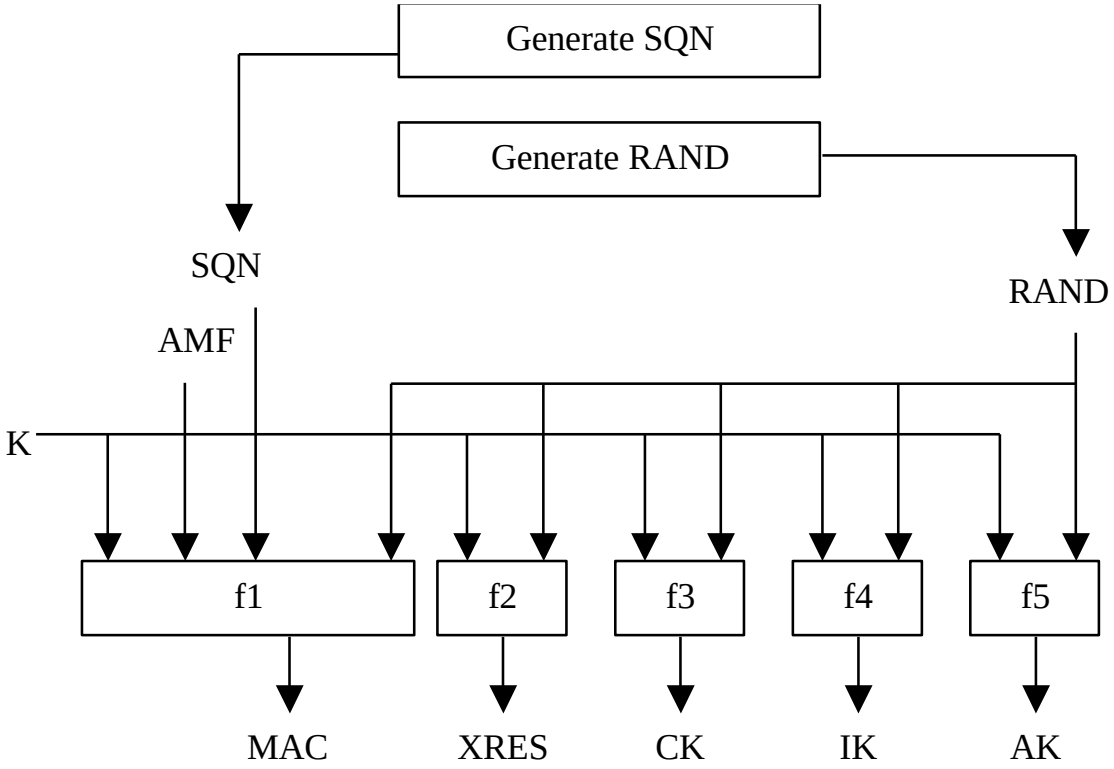
AV = (RAND, XRES, CK, IK, AUTN)，认证五元组或认证向量

认证和密钥协商过程



AUTN = SQN⊕AK || AMF || MAC; AV = (RAND, XRES, CK, IK, AUTN)

AuC中认证向量的产生



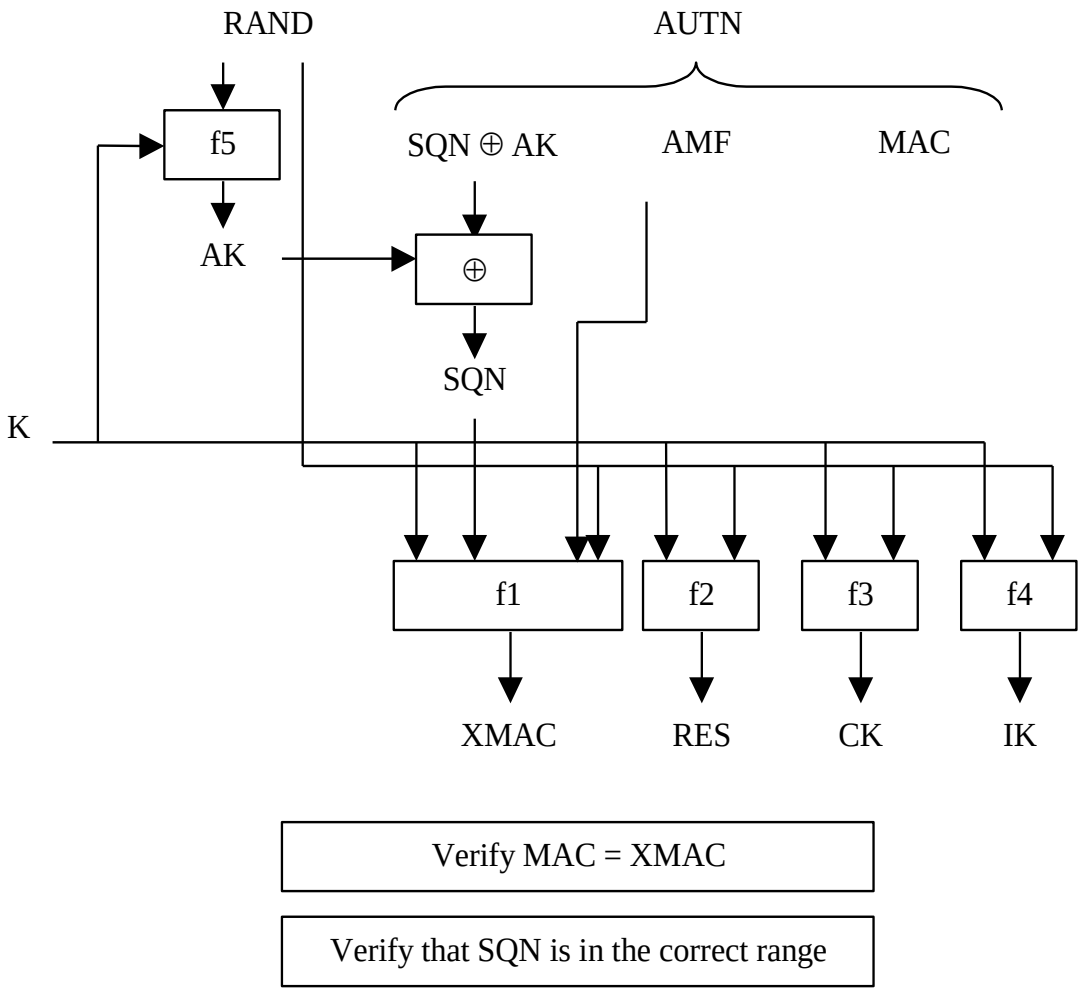
AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

各变量和参数的长度:

K	**128比特**
RAND	**128比特**
SQN	**48比特**
AMF	**16比特**
MAC	**64比特**
XRES	**32比特**
CK	**128比特**
IK	**128比特**
AK	**48比特**
AUTN	**128比特**

USIM卡中的认证功能



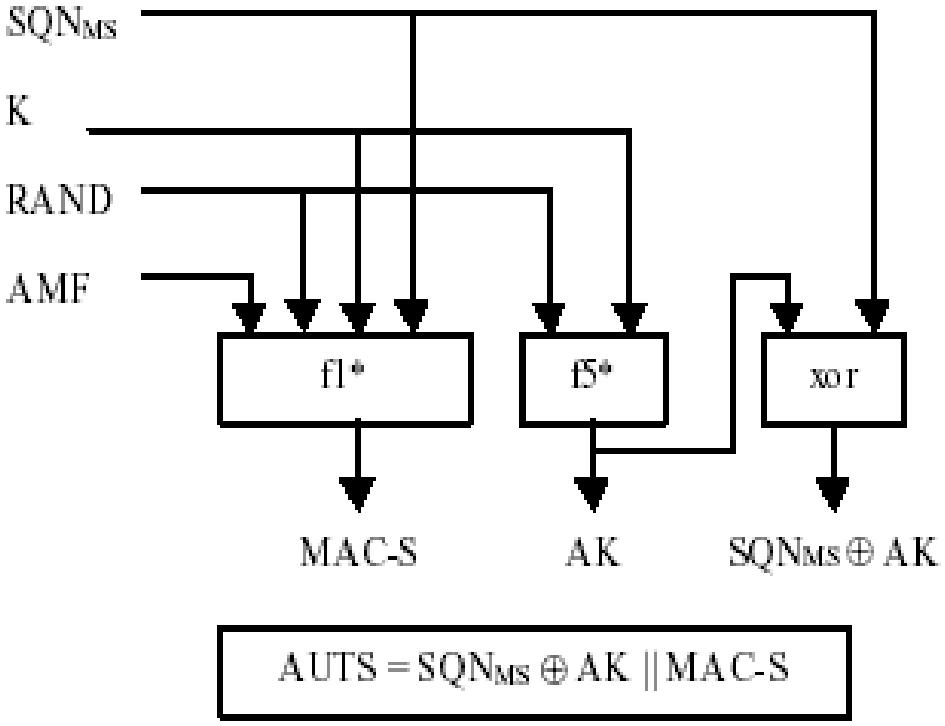
1.USIM卡接收到用户认证请求数据RAND||AUTN.

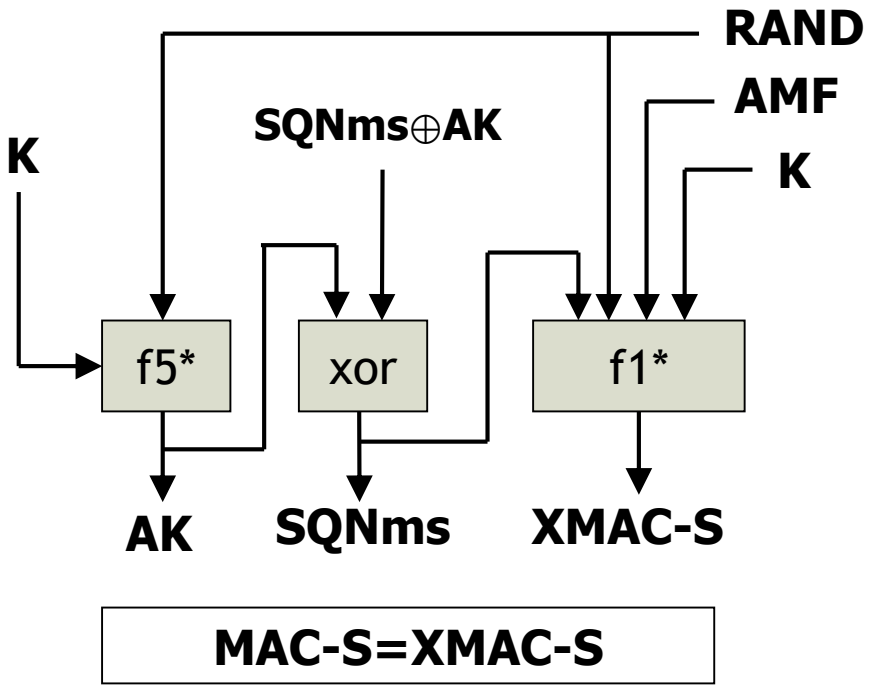
2.把RAND和K输入f5,产生匿名密钥,然后得到SQN.

3.计算XMAC,并与MAC比较是否相等,若不相等,发送用户认证拒绝消息给VLR/SGSN,并放弃该过程.

4.检查SQN是否在正确的范围内,若不在,发送同步失败消息给VLR/SGSN,并放弃该过程.

USIM和HLR/AuC的再同步





MS→HLR/AuC: 同步失败指示和一个（AUTS，RAND）对

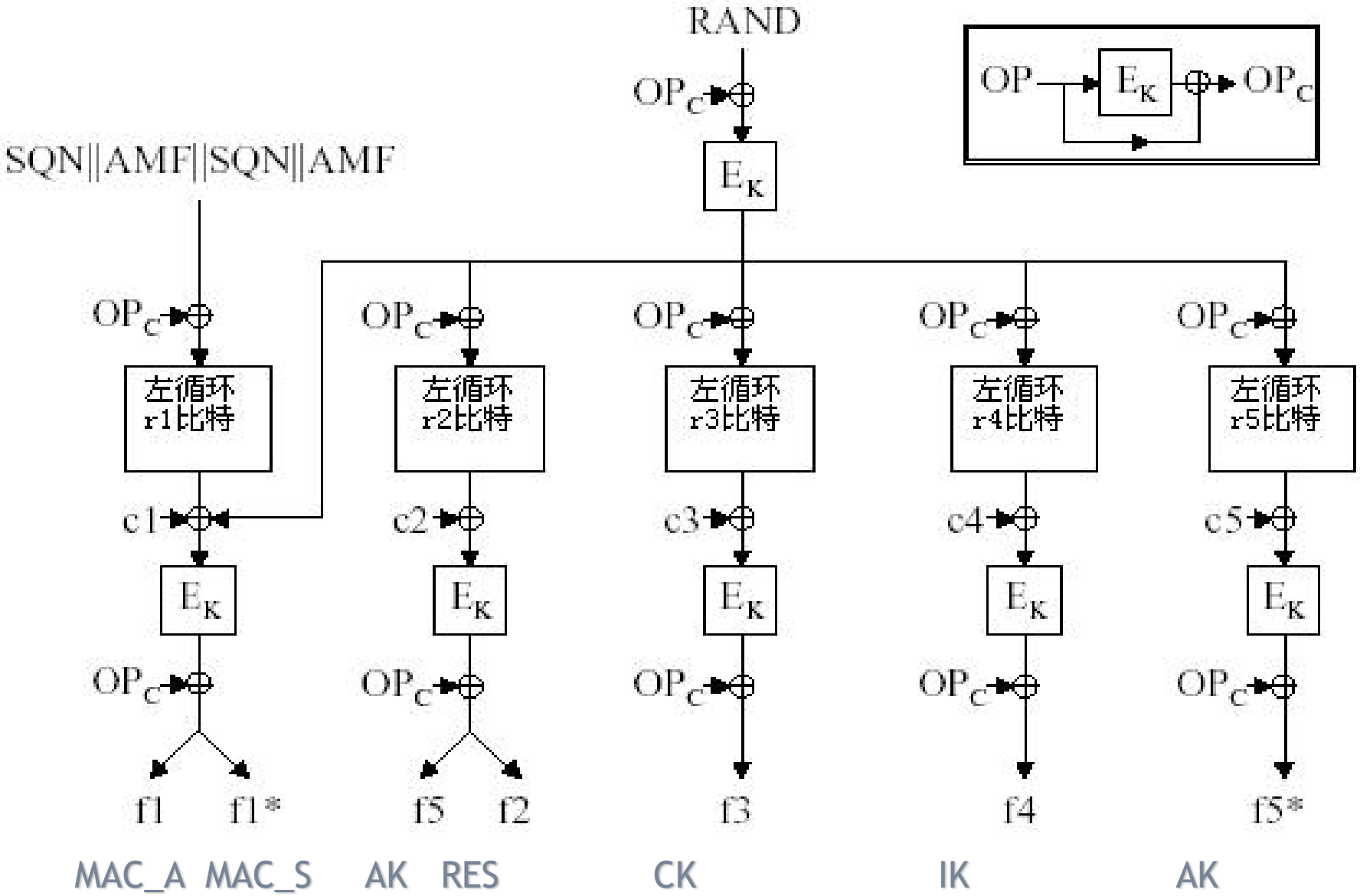
AKA算法要求

- 算法**功能要求**（f0~f5, f_1^*,f_5^* ）
- 算法的**接口要求**
- **通用要求**
  - 健壮性（使用期限20年）
  - 全球范围的可用性和使用情况
- 由SA3提出的**附加要求**
  - 算法需要在128位的算符变量配置下实现可控算法的私有化
  - 算法应围绕一个可替代的内核函数进行设计
  - 希望有公开/标准的可行算法来实现内核函数
  - 算法在USIM上实现时必须能够抵御简单功率分析(SPA)，微分功率分析（DPA）和其他相邻信道（side channel）攻击

AKA算法实现

- **SAGE**接受了设计AKA相关算法的任务，并在2000年12月完成了AKA模板函数的设计；
- 整套算法称为“**MILENAGE**”算法；
- MILENAGE只是一个算法的框架，SAGE建议使用的**AES算法**只是适合这个框架的算法之一。

MILENAGE算法


RAND
OP
E_K
OP_C
SQN||AMF||SQN||AMF
左循环 r1比特
左循环 r2比特
左循环 r3比特
左循环 r4比特
左循环 r5比特
c1
c2
c3
c4
c5
f1
f1*
f5
f2
f3
f4
f5*
MAC_A
MAC_S
AK
RES
CK
IK
AK

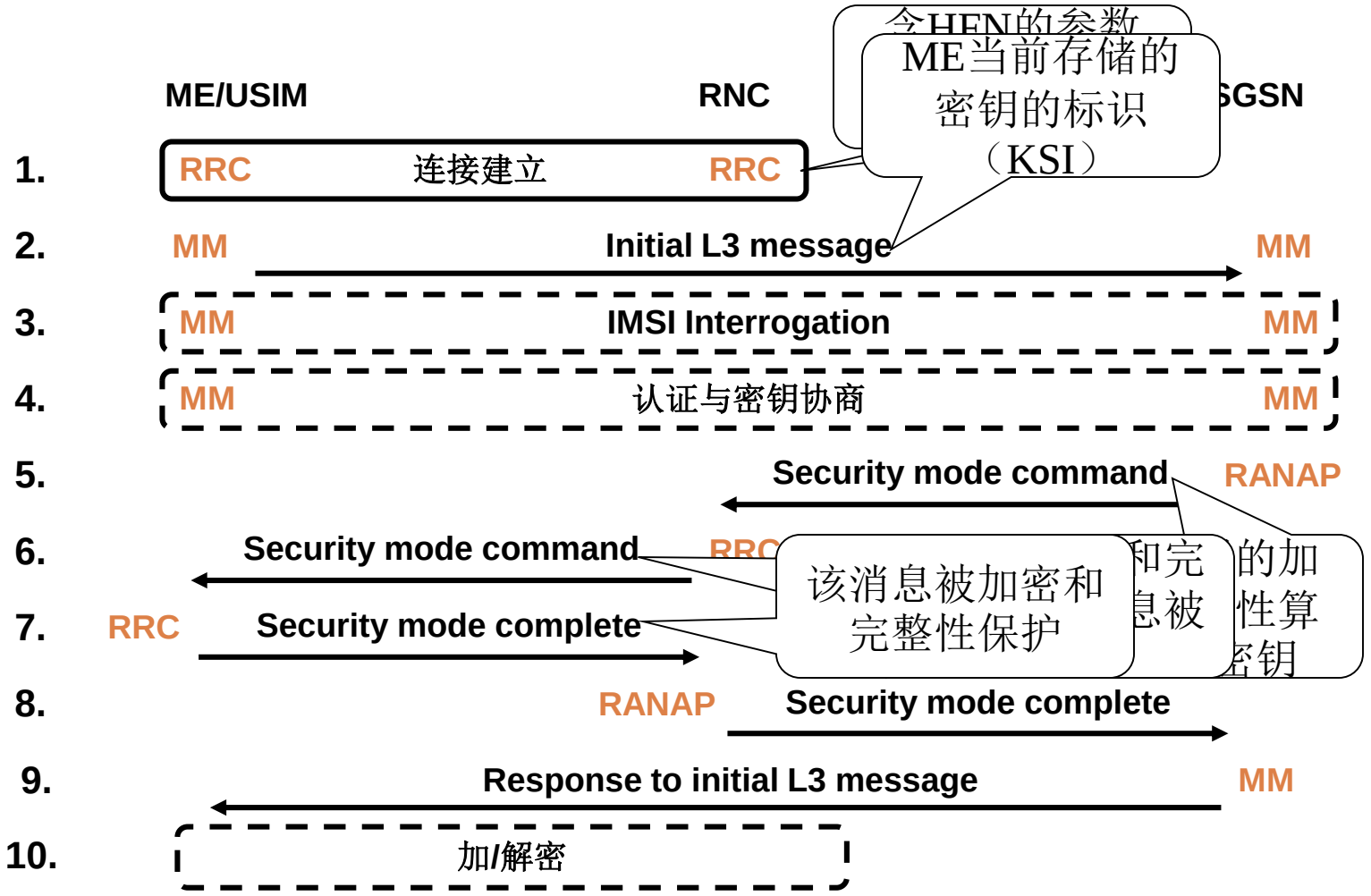
MILENAGE算法中变量的含义

- **Rot(x,r):**表示把x左循环r比特
- **OP:**是由运营商选择的一个128比特的值
- **常数c1,c2,c3,c4,c5的值分别为:**0,1,2,4,8
- **常数r1,r2,r3,r4,r5的值分别为:**64,0,32,64,96
- **IN1**:=SQN||AMF||SQN||AMF　　128比特
- **OUT1,OUT2,OUT3,OUT4,OUT5**是计算出来的128比特值，从中可以确定AKA过程中各种函数值.

AKA的安全性分析

- **双向认证**，认证完成后提供加密密钥和完整性密钥，防止假基站攻击
- **密钥的分发**没有在无线信道上传输，AV在固定网内的传输也由网络域安全提供保障
- **密钥的新鲜性**，由新的随机数提供，防止重放攻击
- 对有可能暴露用户位置信息和身份信息的SQN用AK异或，达到**隐藏SQN**的目的
- **MAC的新鲜性**，(SQN和RAND变化，防止重放攻击)

安全连接建立过程


ME/USIM
RNC
SGSN
含HFN的参数
ME当前存储的密钥的标识（KSI）
1.
RRC
连接建立
RRC
2.
MM
Initial L3 message
MM
3.
MM
IMSI Interrogation
MM
4.
MM
认证与密钥协商
MM
5.
Security mode command
RANAP
6.
Security mode command
RRC
7.
RRC
Security mode complete
该消息被加密和完整性保护
8.
RANAP
Security mode complete
9.
Response to initial L3 message
MM
10.
加/解密

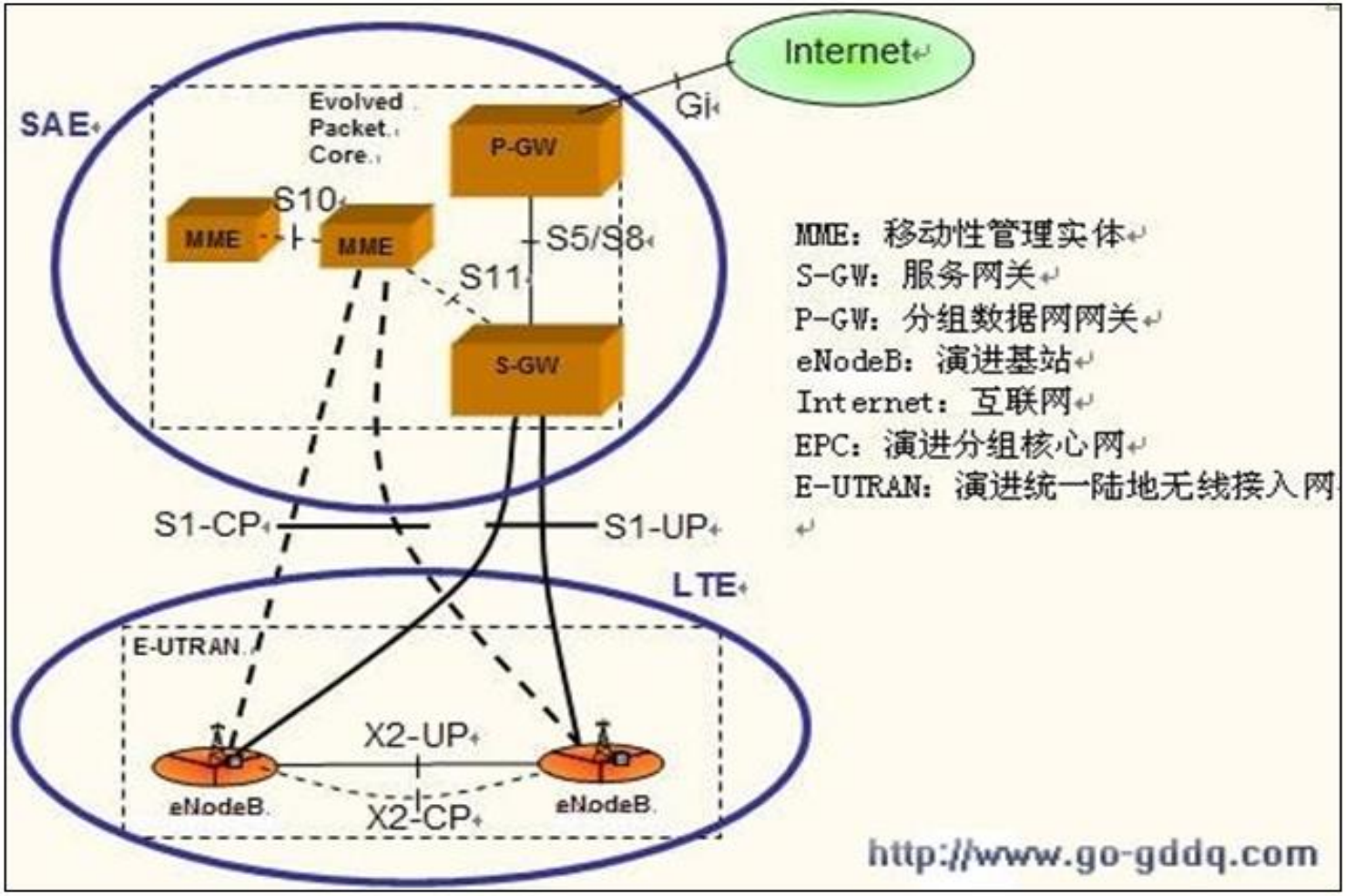
This lecture

- 移动通信安全的发展过程
- 2G(GSM)中的认证与密钥协商协议
- 3G(WCDMA)中的认证与密钥协商协议
- 4G(LTE)中的认证与密钥协商协议
- 5G中的认证与密钥协商协议

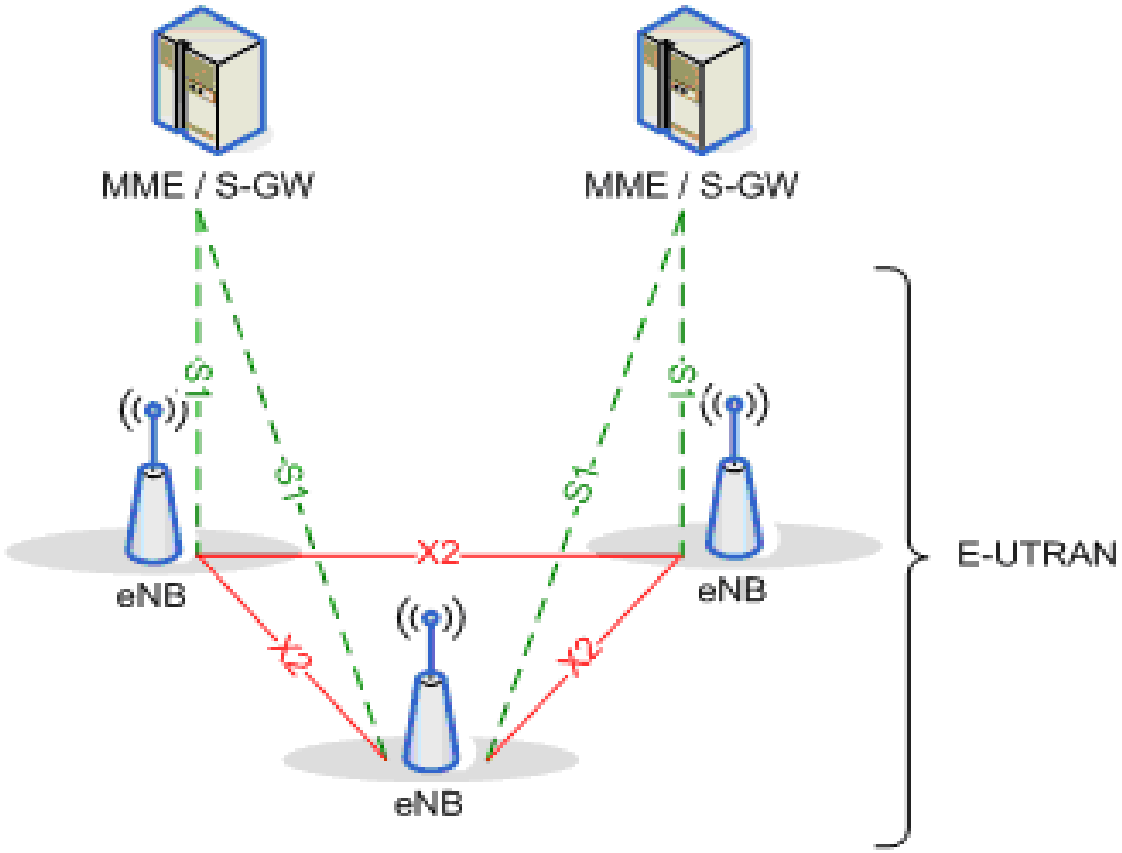
LTE简介

- LTE(Long Term Evolution)长期演进项目
- 2005年开始由3GPP组织制定
- 主要特点
  - 支持1.25MHz～20MHz带宽
  - 峰值数据率：上行50Mb/s，下行100Mb/s
  - 支持增强的IMS（IP多媒体子系统）和核心网
  - 取消电路交换（CS）域，CS域业务在包交换（PS）域实现，如采用VoIP

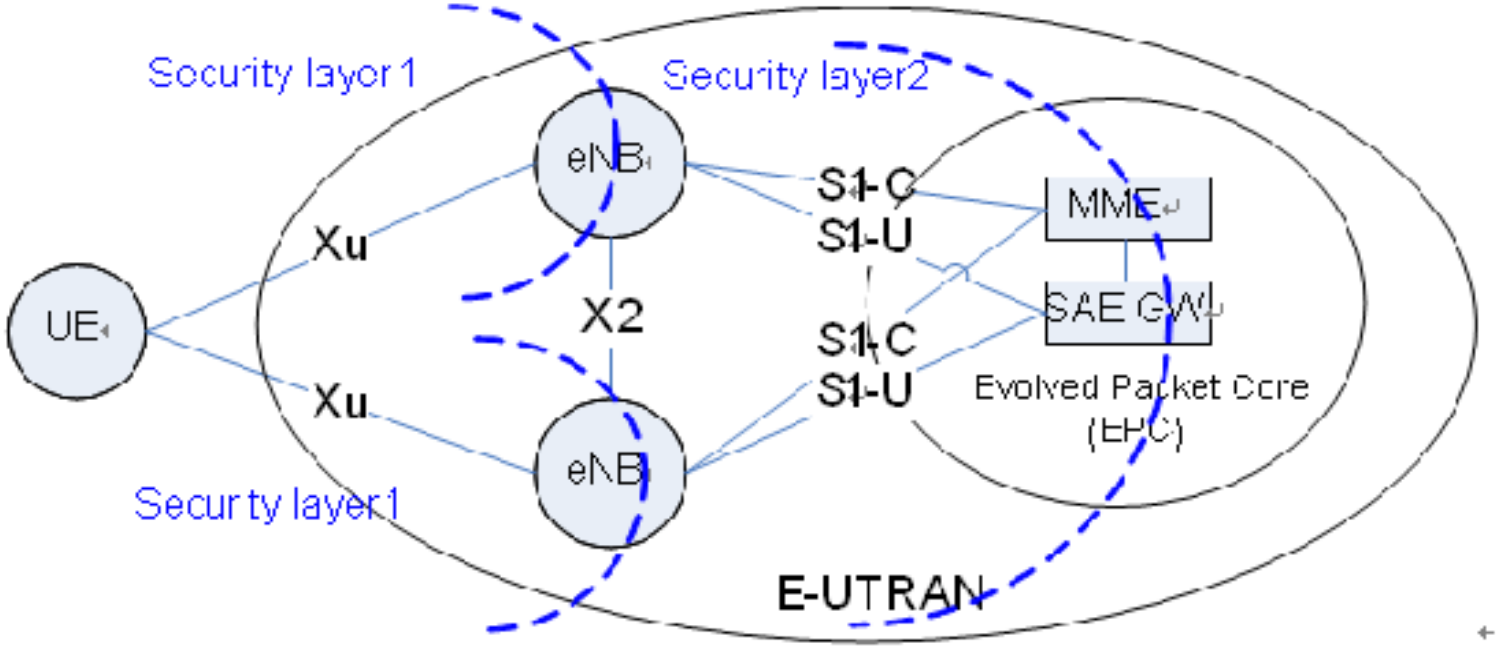
LTE简介


Internet
Gi
SAE
Evolved
Packet
Core
P-GW
S10
MME
MME
S5/S8
S11
S-GW
S1-CP
S1-UP
LTE
E-UTRAN
X2-UP
eNodeB
eNodeB
X2-CP
MME：移动性管理实体
S-GW：服务网关
P-GW：分组数据网网关
eNodeB：演进基站
Internet：互联网
EPC：演进分组核心网
E-UTRAN：演进统一陆地无线接入网
http://www.go-gddq.com

LTE/SAE的接入网络结构

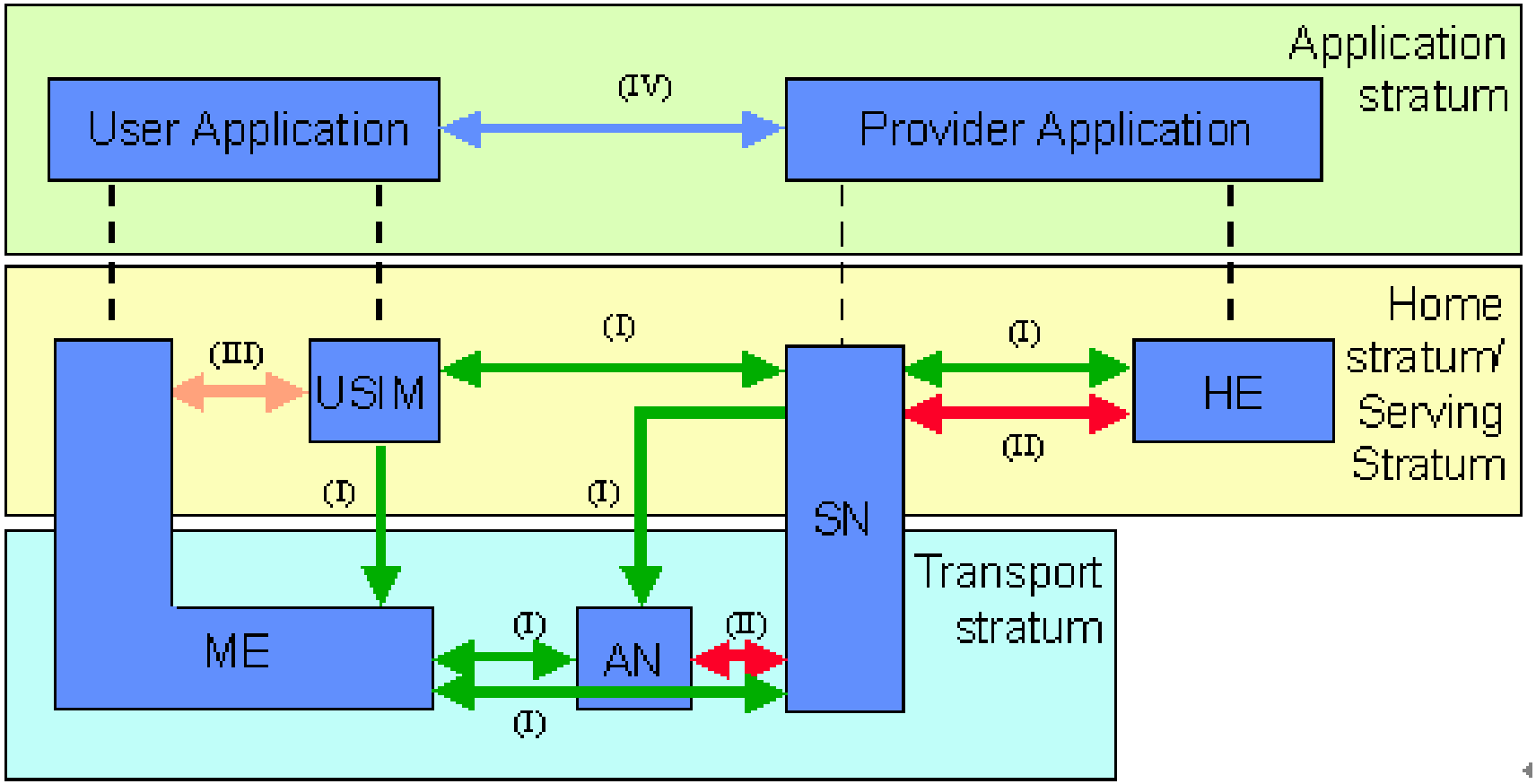


安全层次



- 由于eNB处于一个不完全信任区域，因此LTE/SAE的安全包括两个层次：
  - 接入层（AS）安全：UE与eNB之间的安全，主要执行AS信令的加密和完整性保护，用户面UP的加密性保护。
  - 非接入层（NAS）安全：UE与MME之间的安全，主要执行NAS信令的加密和完整性保护。

LTE安全架构


Application stratum
User Application
(IV)
Provider Application
Home stratum/ Serving Stratum
(III)
USIM
(I)
(I)
HE
(II)
(I)
(I)
SN
Transport stratum
ME
(I)
AN
(II)
(I)

匿名与认证

- **匿名**
  - 定义了一个UE临时标识GUTI，以隐藏UE或用户永久身份。
  - GUTI的完整格式为<GUTI> = <MCC><MNC><MMEGI><MMEC><M-TMSI>
  - S-TMSI是GUTI的缩简形式，以达到更高效的无线信令交互，如用在寻呼和服务请求中来识别移动终端。
  - <S-TMSI> = <MMEC><M-TMSI>
- **认证**
  - LTE/SAE的AKA过程继承了UTMS的AKA过程，认证过程和认证向量产生方法等基本一样，只是认证向量中CK，IK变为Kasme。

LTE认证过程

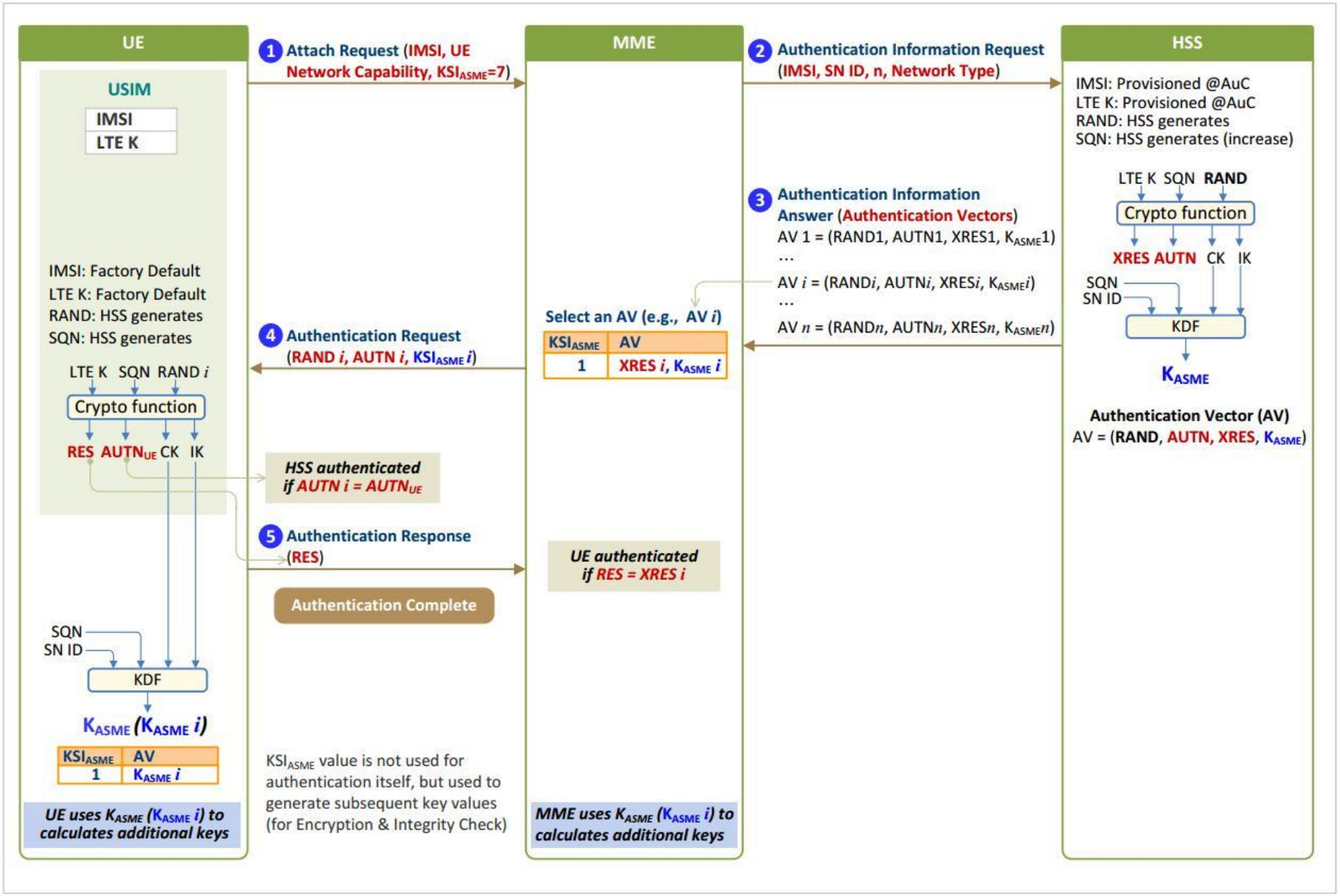
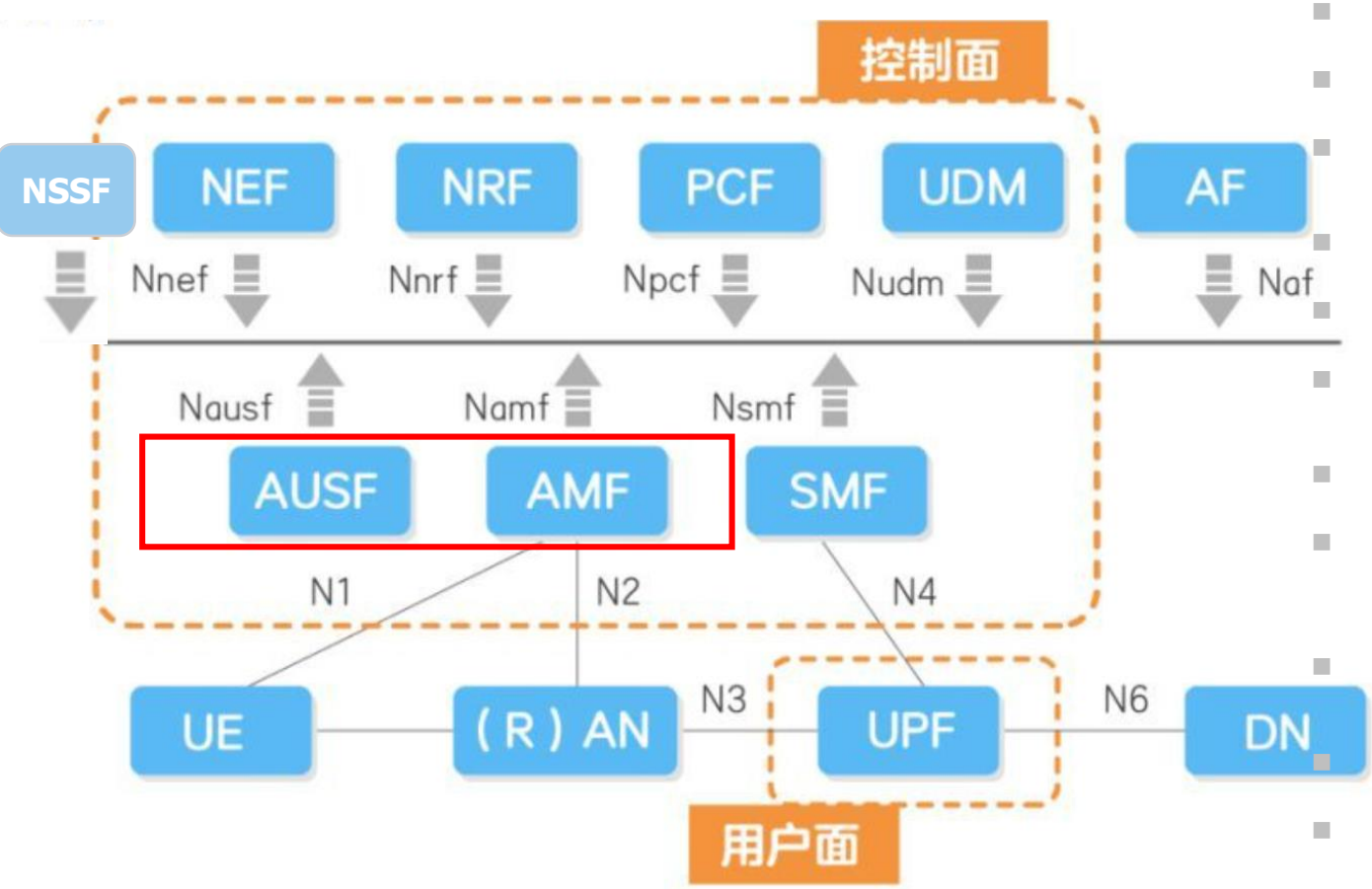


Figure 3. LTE authentication procedure

This lecture

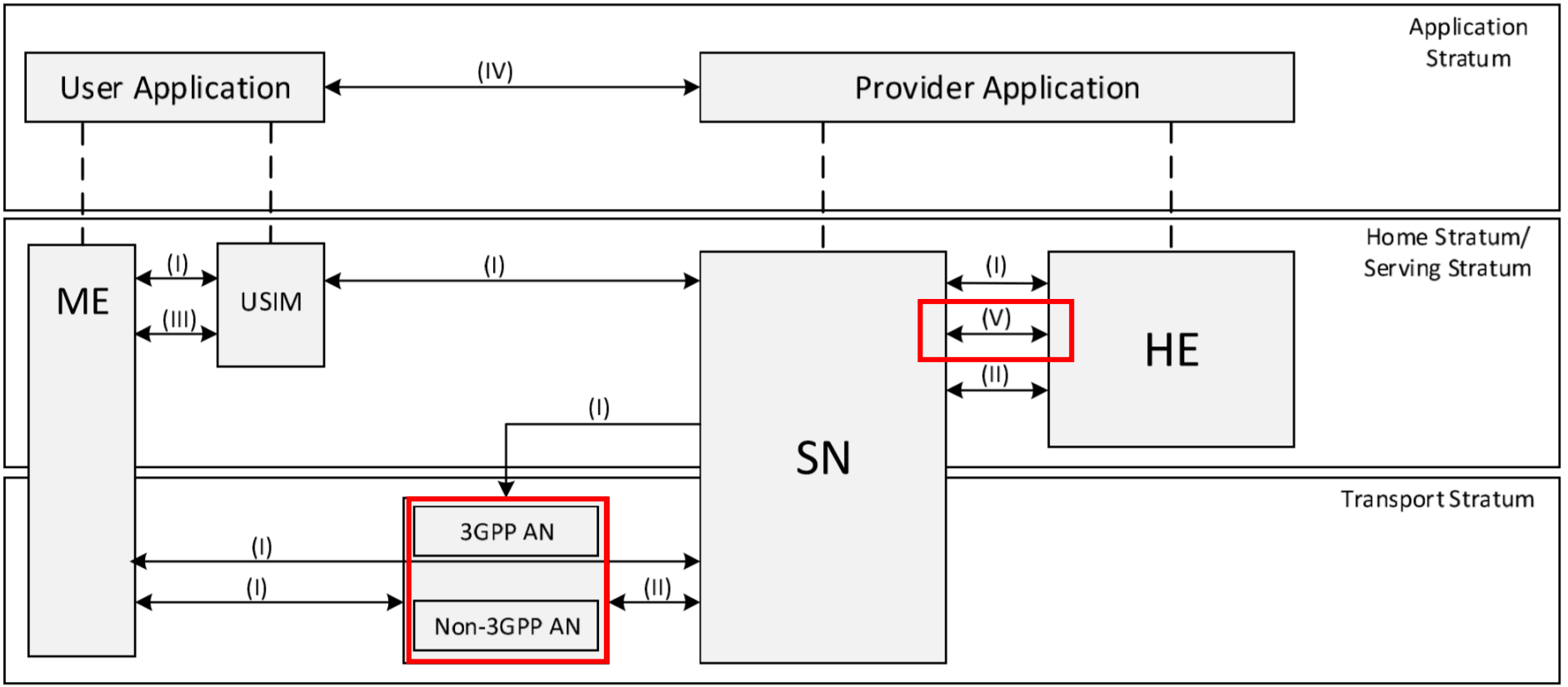
- 移动通信安全的发展过程
- 2G(GSM)中的认证与密钥协商协议
- 3G(WCDMA)中的认证与密钥协商协议
- 4G(LTE)中的认证与密钥协商协议
- 5G中的认证与密钥协商协议

5G网络架构



- **NSSF**网络切片选择功能
- **NEF**网络业务呈现功能
- **NRF**网络储存功能
- **PCF**策略控制功能
- **UDM**统一数据管理
- **AF** 应用功能
- **AUSF**认证服务器功能
- **AMF**接入与移动管理功能
- **SMF**会话管理功能
- **UE**用户设备
- **RAN**无线接入网络
- **UPF**用户面功能
- **DN**数据网络

5G安全架构


Application Stratum
User Application
(IV)
Provider Application
Home Stratum/ Serving Stratum
ME
(I)
(III)
USIM
(I)
(I)
(V)
(II)
HE
SN
(I)
Transport Stratum
3GPP AN
(I)
(I)
Non-3GPP AN
(II)

用户标识

- **SUPI**(SUbscriber Permanent Identifier)
  - 用户永久标识符
  - 是5G用户的永久身份，相当于IMSI。
- **SUCI**(SUbscription Concealed Identifier)
  - 用户隐藏标识符
  - 计算：使用归属网络的公钥对SUPI进行加密。
- **GUTI**(Globally Unique Temporary Identity)
  - 全球唯一临时标识
  - 在激活NAS安全功能后，由网络发到UE上的临时用户标识

解决方案

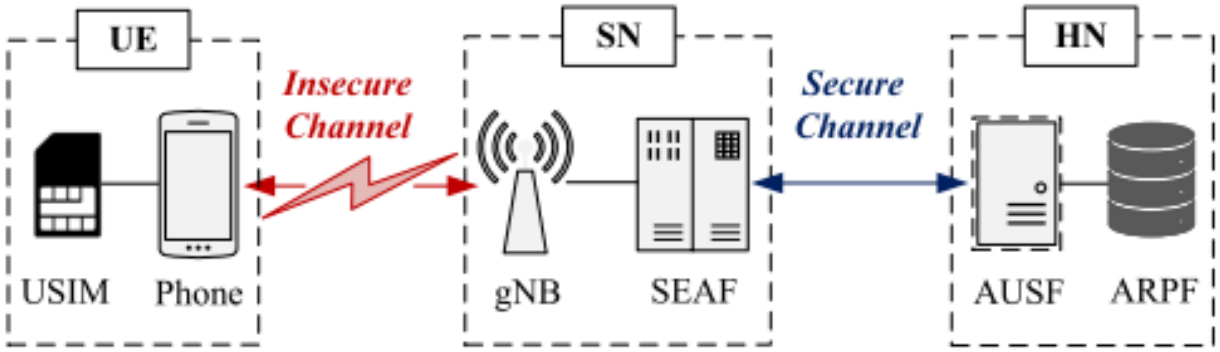
- **认证框架**
  - 以细粒度的方式满足不同的认证要求
- **认证技术**
  - **网络与业务的统一认证技术**：运营商统一进行网络和业务认证以达到进行一次网络认证便可直接访问和使用多种业务。
  - **业务认证用户，运营商信任垂直行业认证**：对某些垂直行业，运营商可以信任业务对用户的认证结果，为用 户提供网络服务。
  - **运营商和业务分别认证**：运营商负责设备的入网认证和管理，垂直行业对用户做业务认证。

认证

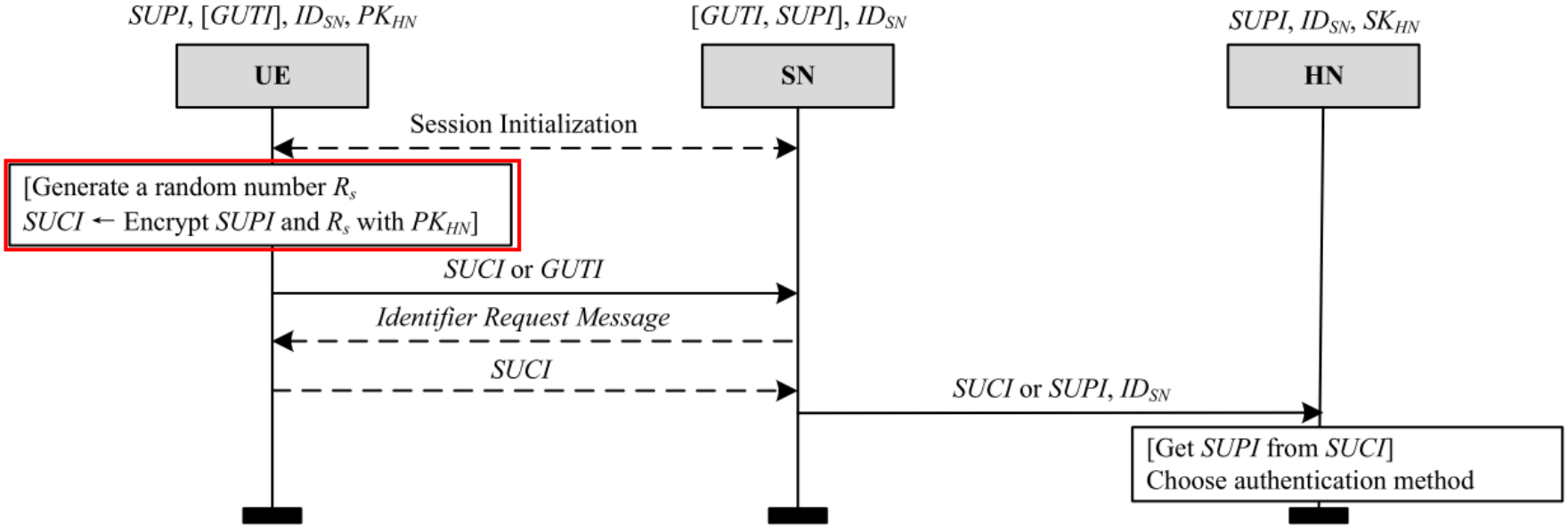
- **目的**：
  - 实现UE与网络之间的双向认证
  - UE和服务网络之间进行密钥协商
  - 基于K_{SEAF}进行密钥派生，避免走完整认证流程
- **不同场景下有不同认证协议**
  - **5G-AKA**
    - 每次认证请求发送一个安全向量AV
  - **EAP-AKA'**
    - 以实现统一框架下的双向认证，可支持非3GPP的接入

5G-AKA

Architecture

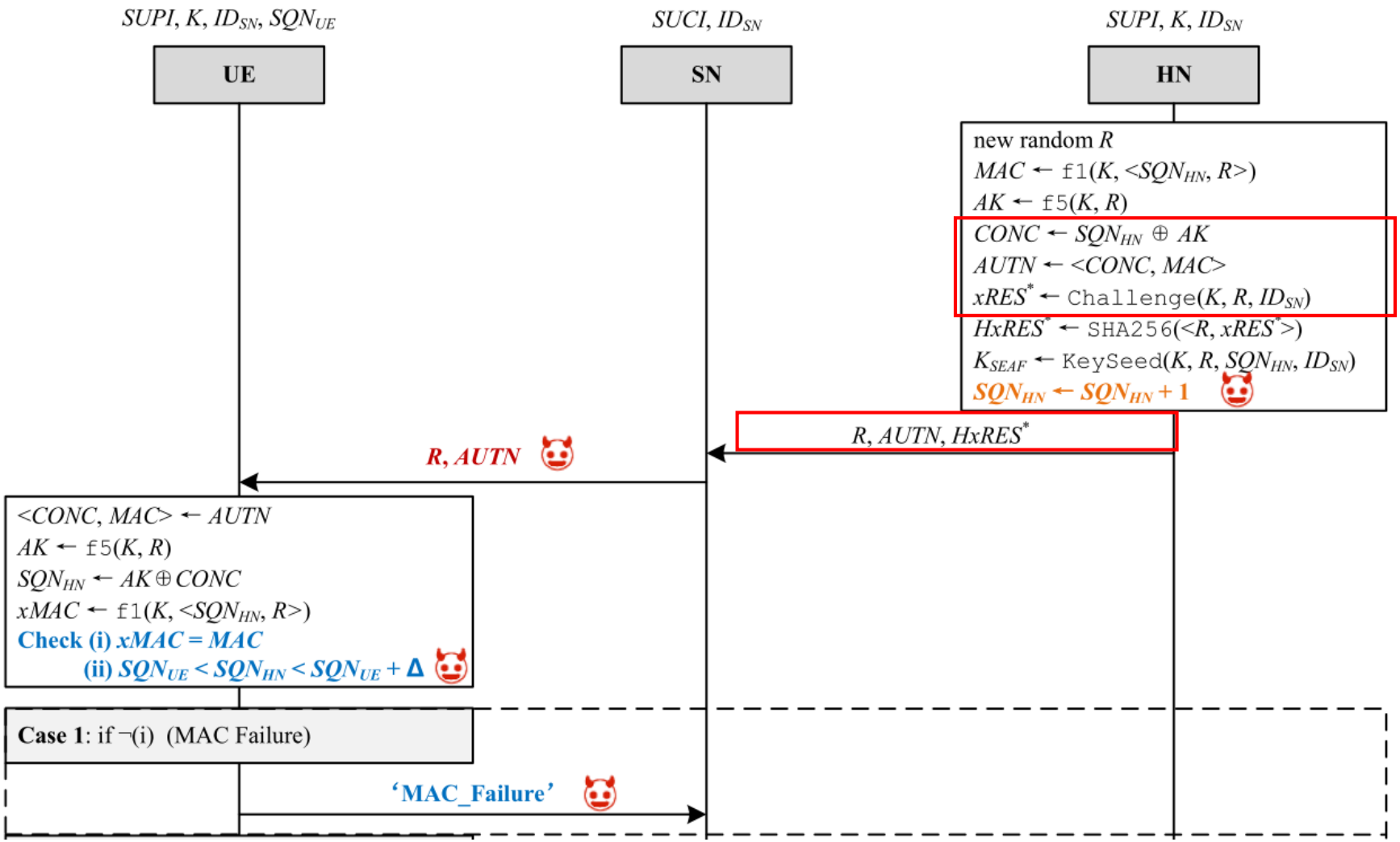


Initiation

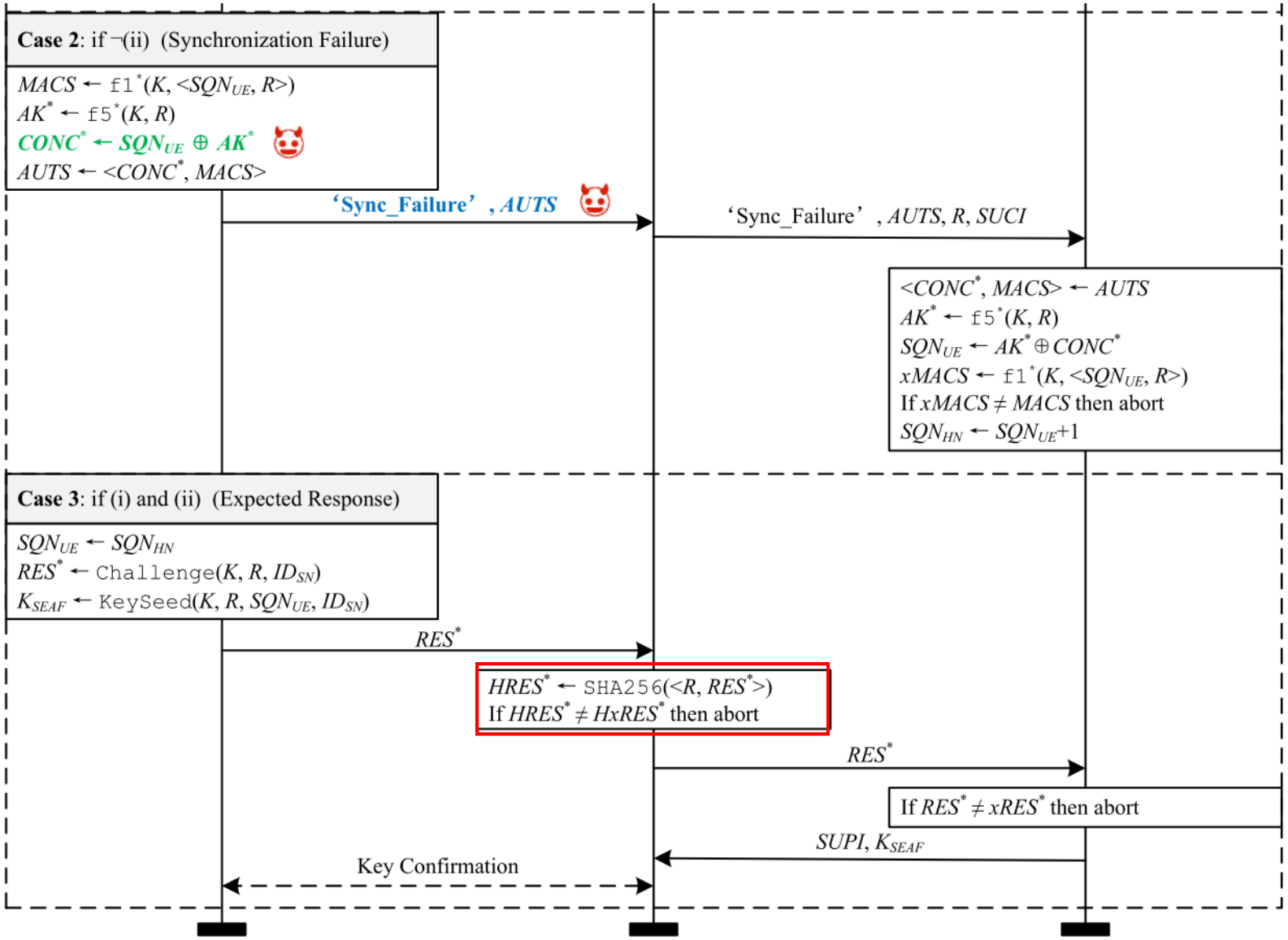


5G-AKA

Challenge-Response



5G-AKA ➢Challenge-Response(contiuned)



AKA协议的缺陷

- **AKA可链接性攻击**（2012）
  - 目标UE和其他UE将对重放的认证请求或安全模式命令消息做出不同的响应。因此，攻击者通过监听不同的UE对同一个认证请求消息的反馈，判断出哪个是目标UE，从而对目标UE进行追踪
- **同步失败攻击**（2018）
  - 针对LTE，该攻击导致UE无法验证网络侧的SQN。尽管核心网络可以重新同步其序列号，但对手可以继续重复攻击，以阻止UE向EPC注册，并最终导致受害UE遭受服务中断。
- **SQN暴露攻击**（2019）
  - Borgaonkar等人揭示了AKA协议中的一个新的**逻辑漏洞**，该**漏洞能够暴露SQN**，攻击者可以利用该漏洞进行位置攻击或对用户进行长期远程监控

This lecture

- 移动通信安全的发展过程
- 2G(GSM)中的认证与密钥协商协议
- 3G(WCDMA)中的认证与密钥协商协议
- 4G(LTE)中的认证与密钥协商协议
- 5G中的认证与密钥协商协议

References

- 3GPP, "Security architecture and procedures for 5G System," 3rd Generation Partnership Project (3GPP), Technical Specifi cation (TS) 33.501, 06 2022, version 17.6.0
- D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," in Proceedings of the 2018 CCS
- R. Borgaonkar, L. Hirschi, S. Park, A. Shaik, New privacy threat on 3g, 4g, and upcoming 5G AKA protocols, Proc. Priv. Enhancing Technol. 2019
- Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In NDSS Symposium 2018.

Next Time

- 课程项目中期检查

谢谢大家！欢迎提问！