通 信 安 全

L11—第三代移动通信系统安全技术

- 教师：崔爱娇
- 编号：ELEC3019
- 学时：32学时

概 要

第三代移动通信系统安全技术

- 3G移动通信技术简介
- 3G的安全体系结构
- 存在的问题

概 要

第三代移动通信系统安全技术

3G移动通信技术简介

3G的安全体系结构

存在的问题

3G移动通信技术简介

- WCDMA和cdma2000是两种主流的第三代移动通信标准，其规范的制定分别由国际组织3GPP（第三代移动通信伙伴计划）和3GPP2（第三代移动通信伙伴计划2）负责。

◆WCDMA阵营：由GSM延伸得来，以UMTS(Universal Mobile Telecommunication System)命名。

◆CDMA2000阵营：由CDMA演变发展而来，包括CDMA 1X中的各个版本。

3G移动通信系统的安全原则

- 3G是从2G的基础上发展而来的。

- 保留2G系统中被认为是必须的以及应增强的安全特性。
- 改进2G系统存在和潜在的弱安全功能。
- 对提供的新业务提供安全保护。

安全原则

- 3G安全特性须综合考虑业务情况下的风险性。
- 非话音业务在3G中主要地位，对安全性要求更高；
- 存在多种预付费和后付费业务，3G系统应提供相应保护；
- 用户对服务范围的控制和终端的应用能力大大提高；
- 必须能够抵御用户的主动攻击；
- 终端能力进一步加强，同一终端可能使用多SIM卡，同时支持不同的应用环境，系统应保证多种平台和应用环境的安全性；
- 为了提高传属性，才能采用固定网络传输，故应考虑适应固定线路传输。

安全特性

3G移动通信系统的安全目标

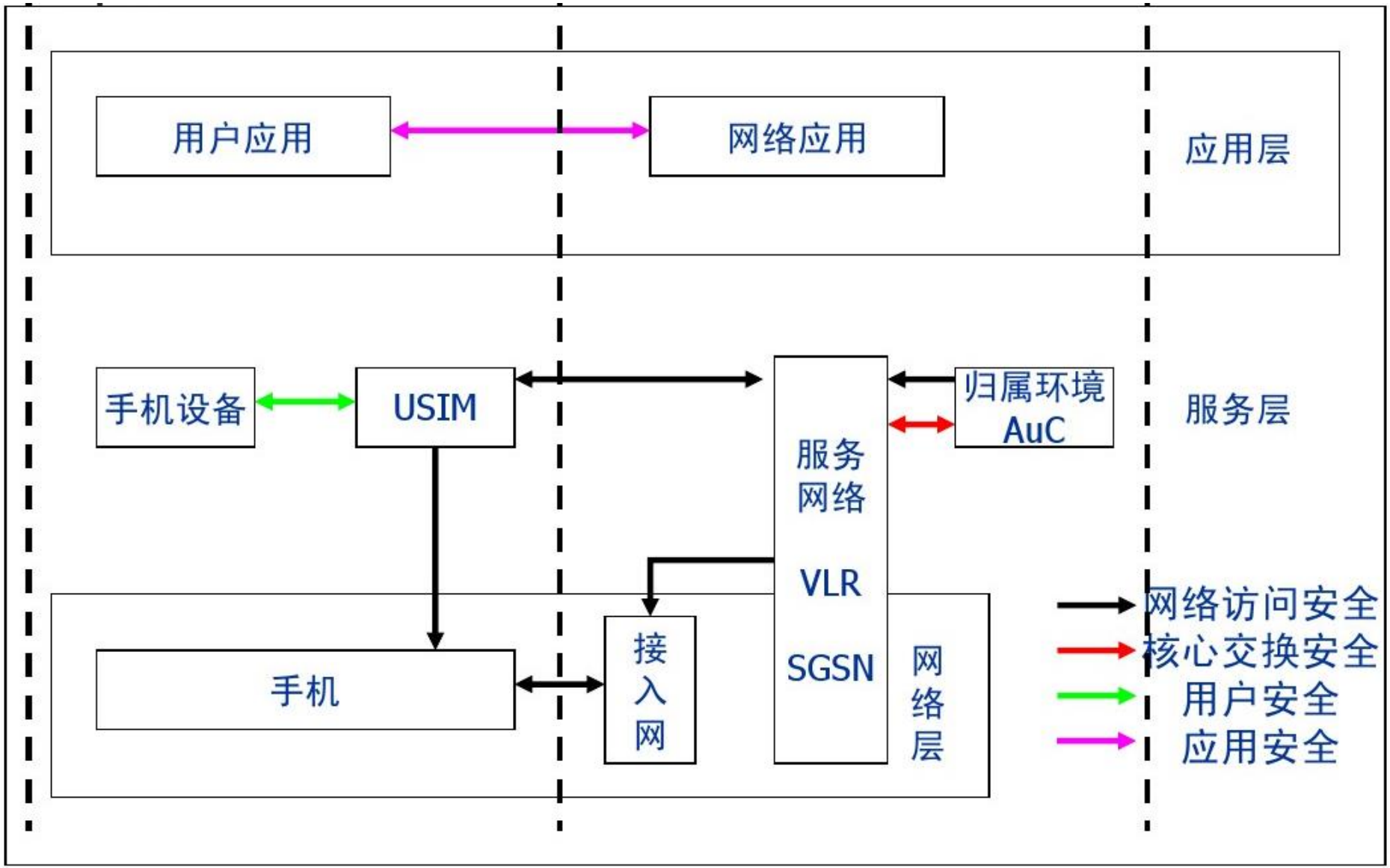
用户层面	• 保护用户产生相关信息，防止盗用
网络层面	• 保护归属和拜访网络提供的资源和服务，防止盗用
运营商层面	• 确保方案有世界范围内的通用性 • 确保方案标准化，从而保证不同服务网络间漫游
未来层面	• 确保3G安全特性和机制是可扩展和可增强的，可以根据新的威胁和服务不断改进提供。

概 要

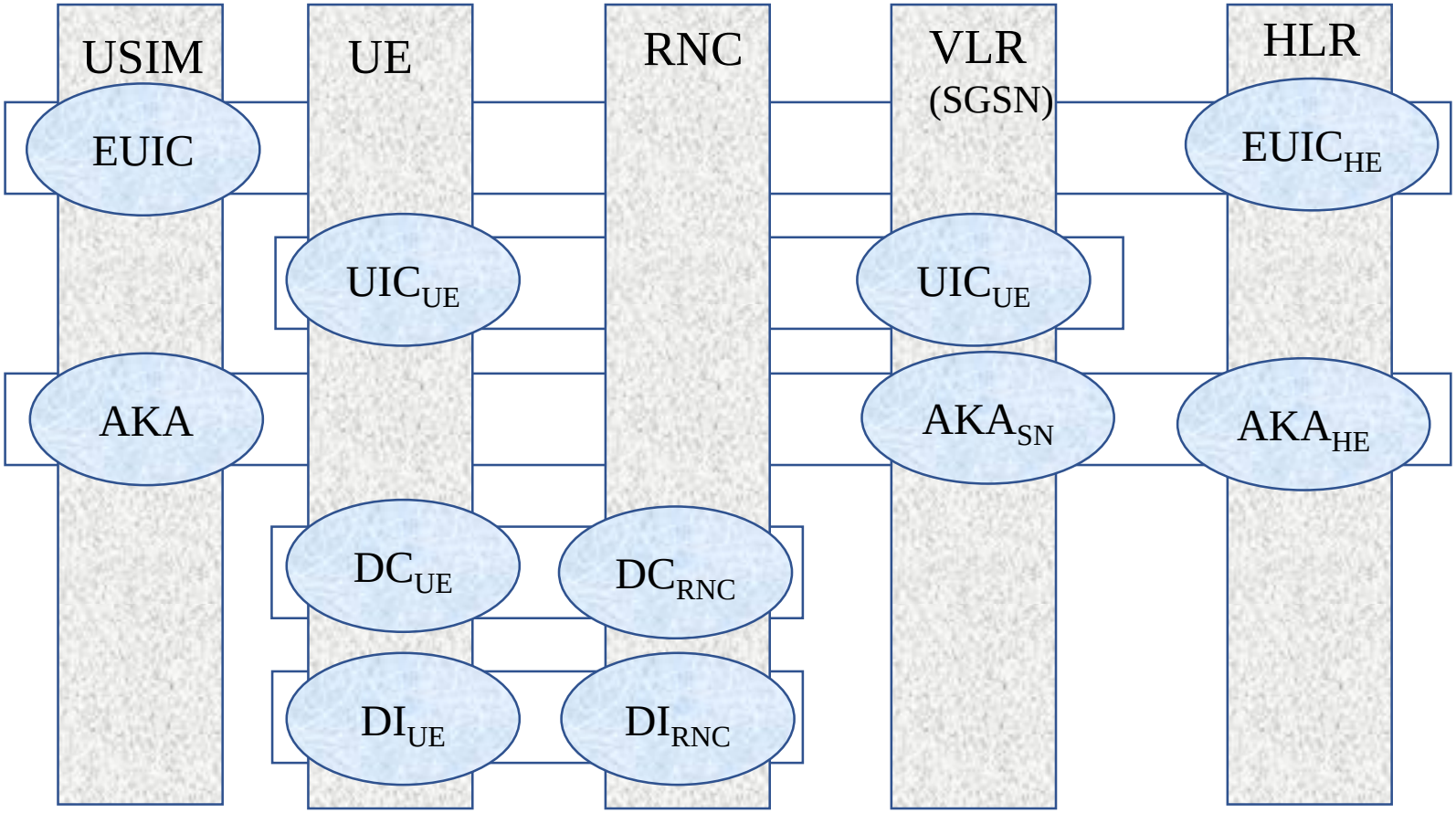
第三代移动通信系统安全技术

- 3G移动通信技术简介
- 3G的安全体系结构
- 存在的问题

3G系统的安全体系结构



3G安全功能结构



USIM:用户业务识别模块
EUIC:增强用户身份保密
AKA：认证与密钥分配
UE：用户终端
UIC:用户与服务身份认证

DI:数据完整性
DC:数据加密
RNC：无线网络控制器
VLR：访问位置寄存器
HE: 本地环境

SGSN:服务GPRS支持节点
SN:服务网络
HLR: 归属位置寄存器

3G的安全体系结构-5类安全措施

一、增强用户身份保密（ EUIC ）：通过HE/AuC（本地环境/认证中心）对USIM（用户业务识别模块）身份信息进行认证；

二、用户与服务网间身份认证（ UIC ）；

三、认证与密钥分配AKA：用于USIM、VLR/SGSN（访问位置寄存器/服务GPRS支持节点）、HLR（归属位置寄存器）间的双向认证及密钥分配；

四、数据加密DC：UE（用户终端）与RNC（无线网络控制器）间信息的加密；

五、数据完整性DI：用于对交互信息的完整性、时效性及源与目的地进行认证。

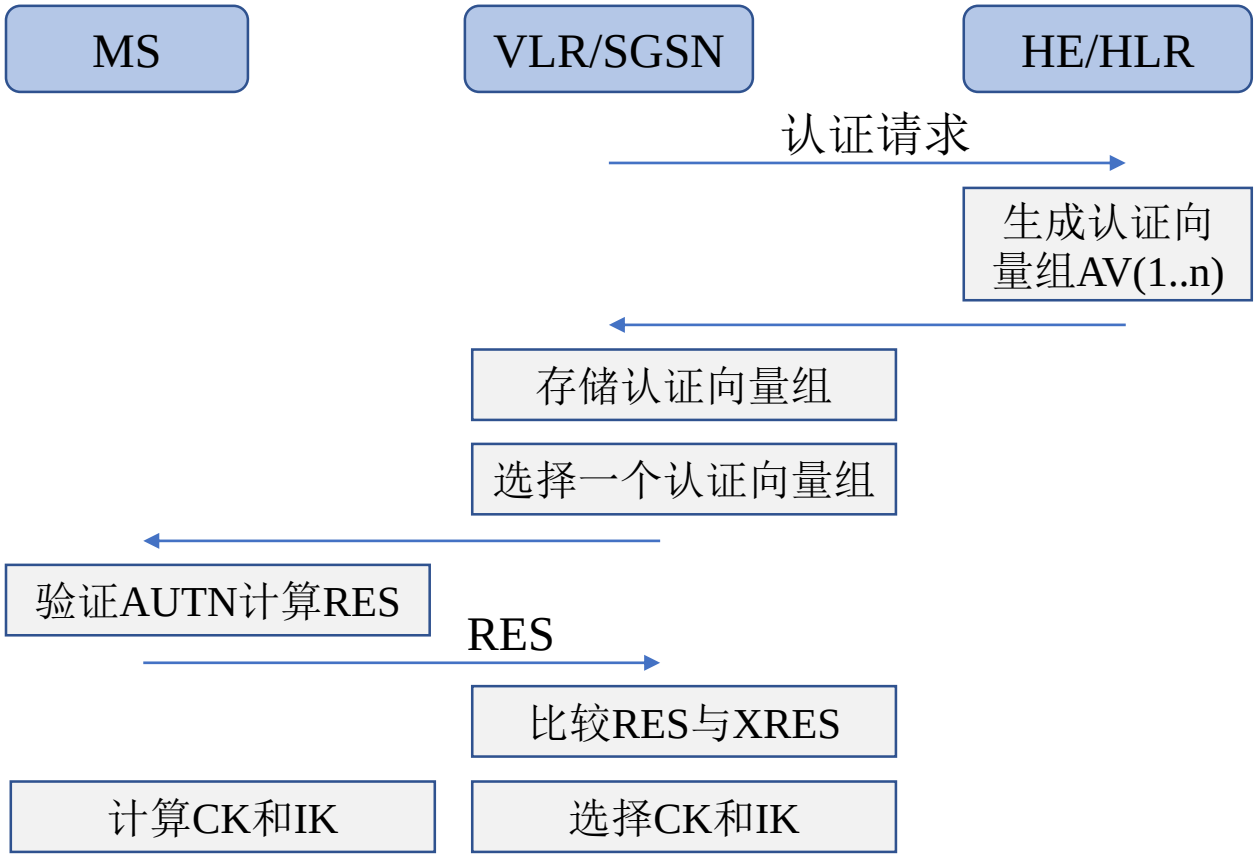
系统定义了11个安全算法：f0、f1*、f1~f9，以实现其安全功能。f8、f9实现DC和DI标准算法。f6、f7用于实现EUIC。AKA由f0 ~f5实现。

GSM和3G的安全比较

		GSM	3G
网络认证用户身份		有	有
用户认证网络身份		无	有
数据加密传输	算法	A5	f8
	密钥	Kc:64bit	CK:128bit
	算法灵活性	固定的加密算法	用户可与网络协商加密算法
数据完整性保护		无	有
用户身份识别（IMSI的传送）		IMSI以明文方式在无线链路上传送	增强的用户身份认证（EUIC）
安全服务对用户的可见性		无	增加安全操作对用户的可见性

3G和GSM系统安全性能比较

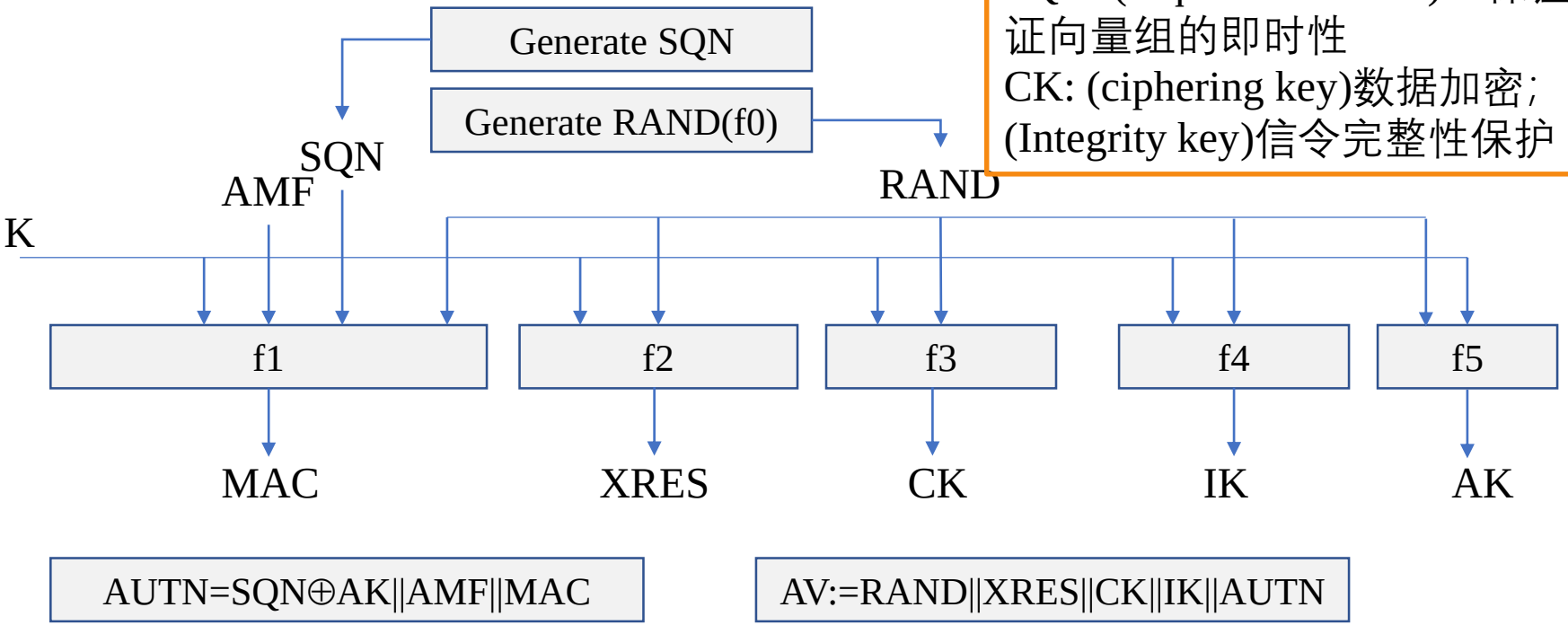
3G的安全体系结构-3G鉴权认证过程



认证鉴权过程详解

一、认证中心AuC为每个用户生成基于序列号的认证向量组（RAND,XRES,CK,IK,AUTN）,并且按照序列号排序。AuC产生认证向量组的流程如下图所示：

SQN: (sequence number)：保证认证向量组的即时性
CK: (ciphering key)数据加密；IK: (Integrity key)信令完整性保护

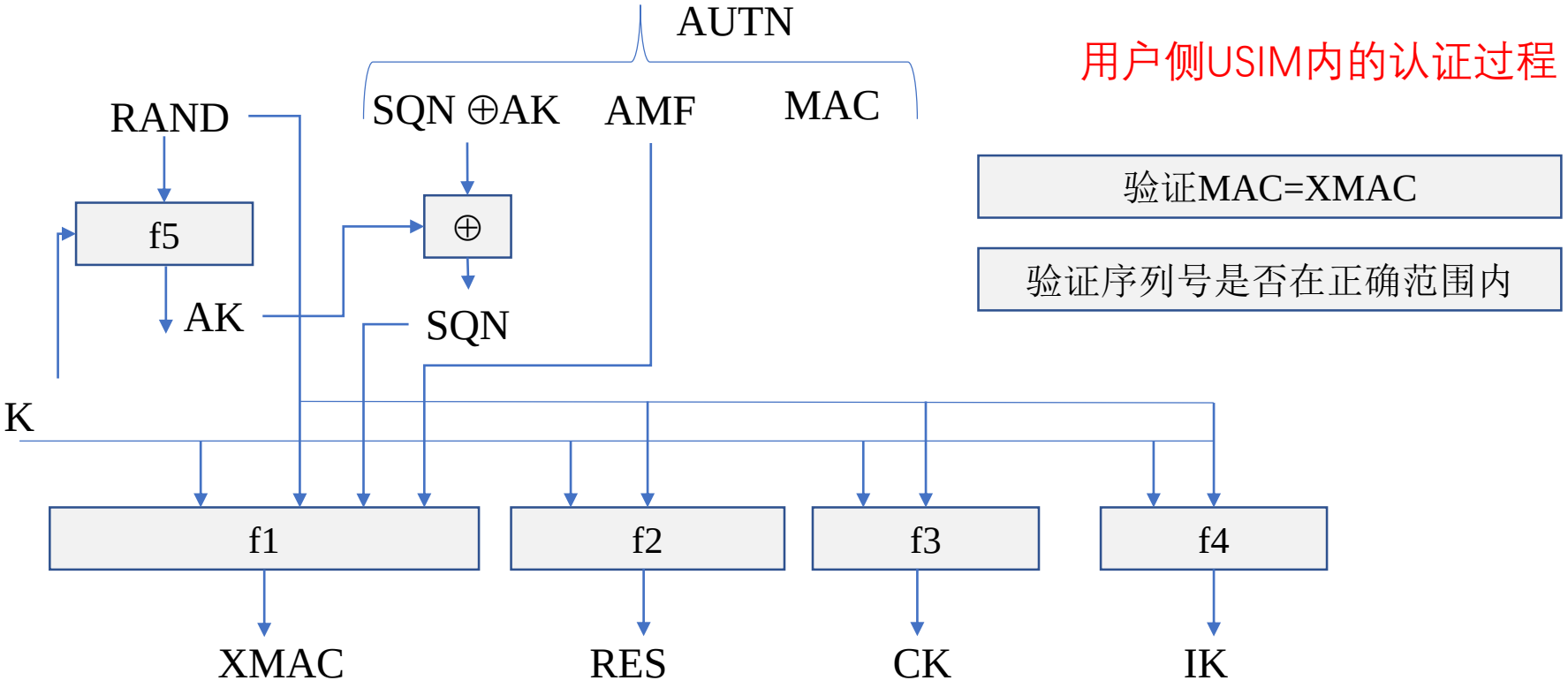


f0是一个伪随机数生成函数，只存放于AuC中，用于生成随机数RAND。3G认证中有一个“认证令牌”AUTN（authentication token），用户验证网络的合法性；包含了一个序列号，使得用户可以避免受到重传攻击。其中AK是用来在AUTN中隐藏序列号，因为序列号可能会暴露用户的身份和位置信息。

认证鉴权过程详解

二、当认证中心收到VLR/SGSN的认证请求，发送N个认证向量组给VLR/SGSN。在VLR/SGSN中，每个用户的N个认证向量组，按照先入先出（FIFO）的规则发送给移动台，用于鉴权认证。

三、VLR/SGSN初始化一个认证过程，选择一个认证向量组，发送其中的RAND和AUTN给用户。用户收到后RAND||AUTN后，在USIM卡中进行下列操作。



认证鉴权过程详解

◆ 首先计算AK并从AUTN中将序列号恢复出来SQN=(SQN⊕AK) ⊕AK ;

◆ USIM计算出XMAC，将它与AUTN中的MAC值进行比较。如果不同，用户发送一个“用户认证拒绝”信息给VLR/SGSN，放弃该认证过程。在这种情况下，VLR/SGSN向HLR发起一个“认证失败报告”过程，然后由VLR/SGSN决定是否重新向用户发起一个认证过程。

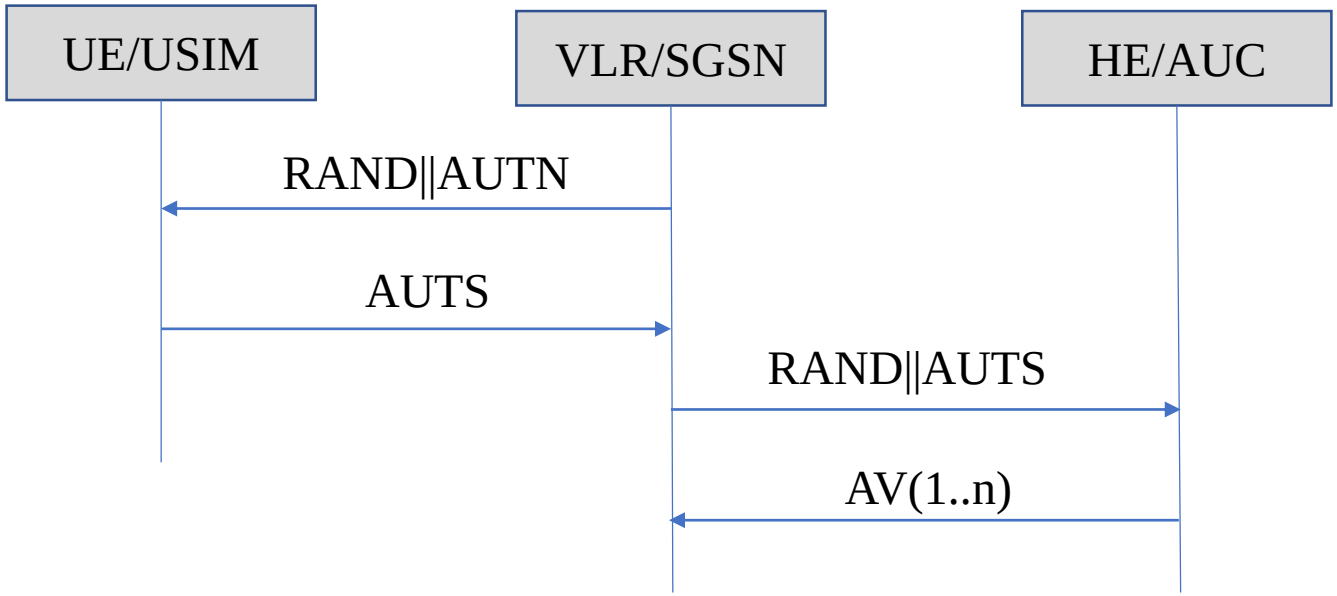
◆ 用户比较收到的SQN是否在正确范围内（为了保证通信的同步，同时防止重传攻击，SQN应该是目前使用的最大的一个序列号，由于可能发生延迟等情况 ，定义了一个较小的“窗口”，只要SQN收到的在该范围内，就认为是同步的。）

◆ 如果SQN在正确范围内，USIM计算出RES，发送给VLR/SGSN，比较RES是否等于XRES。如果相等，网络就认证了用户的身份。

◆ 最后，用户计算出加密密钥CK=f3(RAND，K)，完整性密钥IK=f4(RAND，K)。

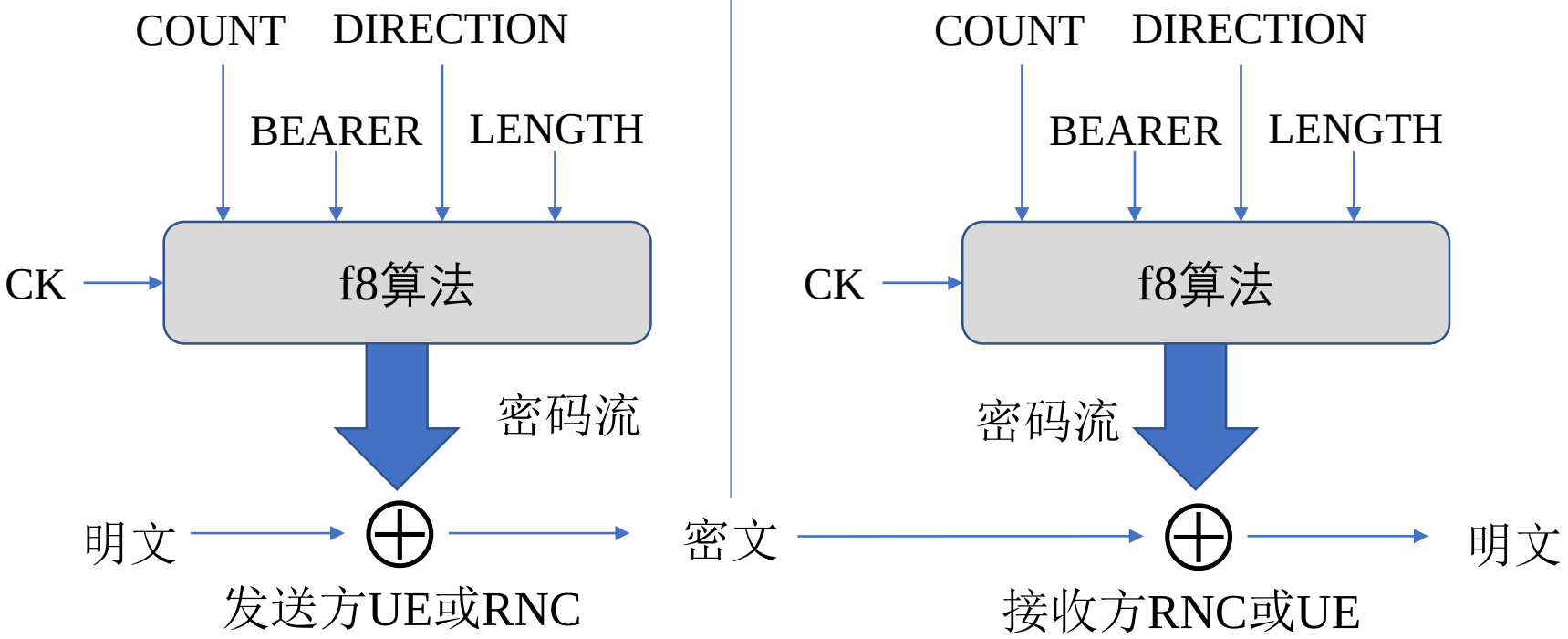
认证鉴权过程详解

四、如果用户计算出SQN(序列号)不在USIM认为正确的范围内，将发起一次“重新认证”



用户信息加密

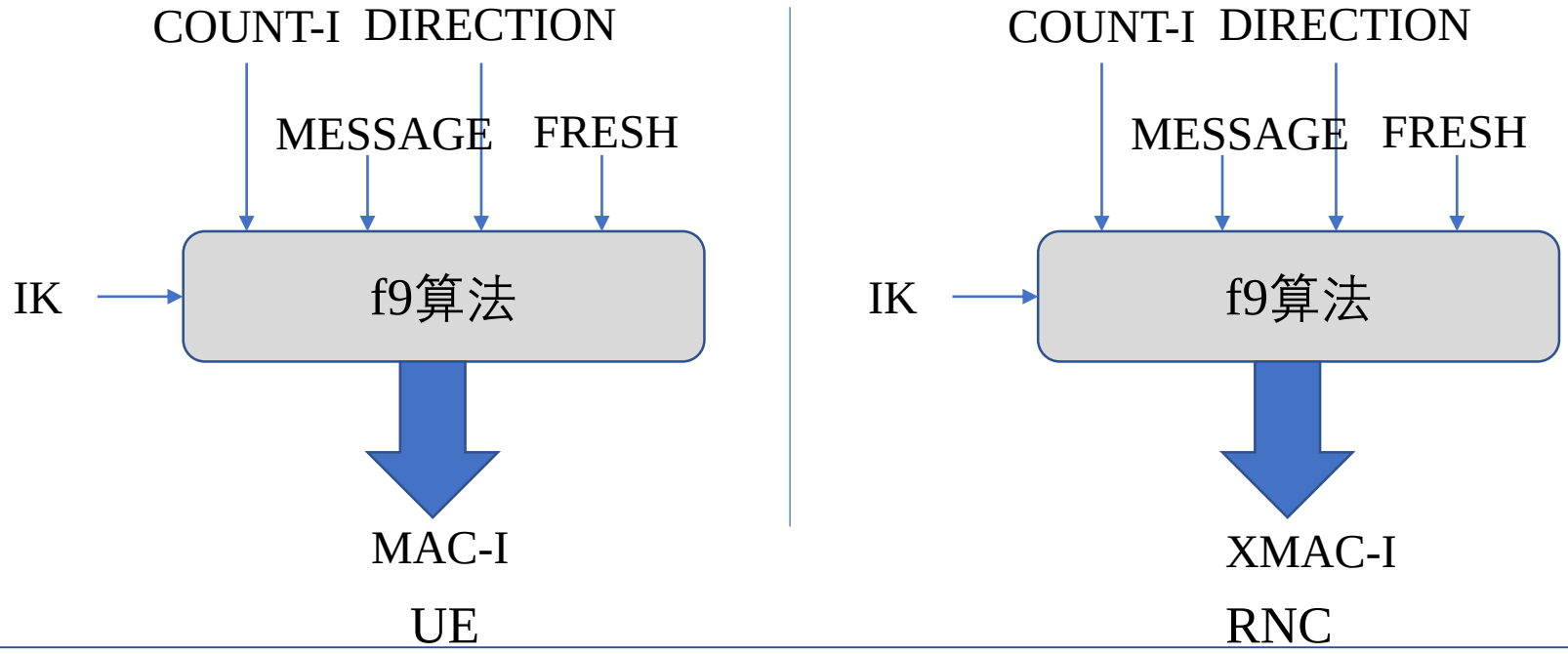
在完成了用户鉴权认证以后，在移动台生成了加密密钥CK。这样用户就可以以密文的方式在无线链路上传输用户信息和信令信息。发送方采用分组密码对原始数据加密，采用了f8算法。接收方接收到密文，经过相同过程，恢复出明文。



COUNT：密钥序列号，32bit；BEARER：链路身份指示，5bit；DIRECTION:上下行链路指示,1bit，消息从移动台到RNC，取值为0，反之为1；LENGTH:密码流长度指示，16bit;CK：加密密钥,128bit;

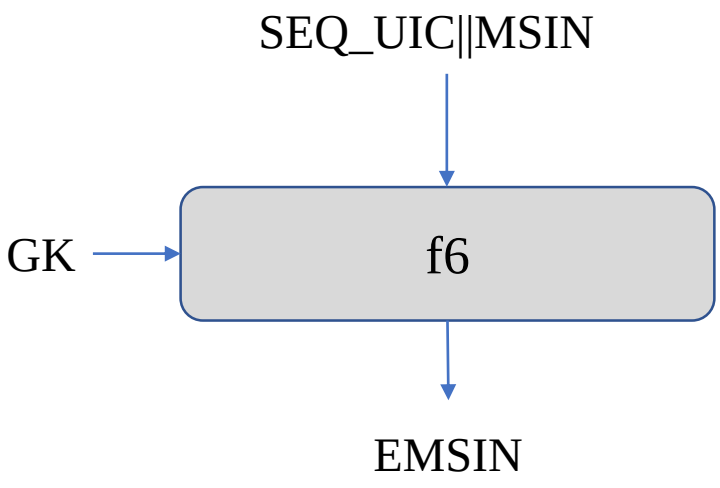
用户信息完整性保护

在3G中，采用了消息认证来保护用户和网络间的信令消息没有被篡改。发送方将要传送的数据用完整性密钥IK经过f9算法产生的消息认证码MAC，附加在发出的消息后面。接收方接收到的消息，用同样的方法计算得到XMAC。接收方把收到的MAC和XMAC相比较，如果两者相等，就说明收到的消息是完整的，在传输过程中没有被修改。

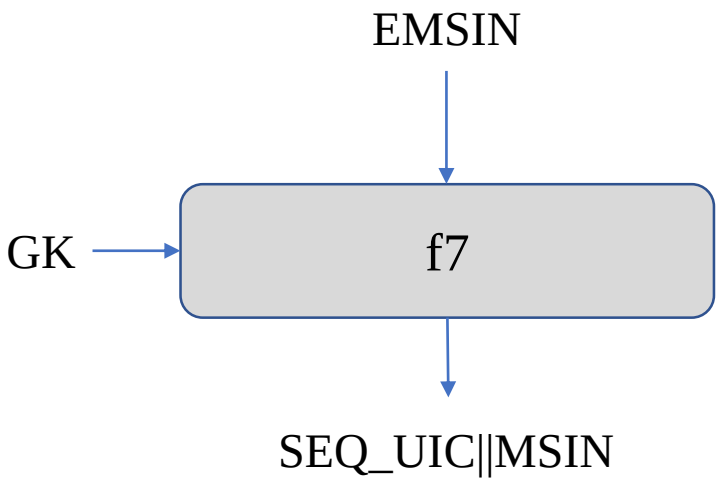


COUNT-I：密钥序列号，32bit；MESSAGE：消息，5bit；DIRECTION:上下行链路指示,1bit，消息从移动台到RNC，取值为0，反之为1；FRESH:网络生成的一个随机数，32bit; IK：完整性密钥,128bit；MAC-I:消息认证码。

增强的用户身份认证（EUIC）



USIM

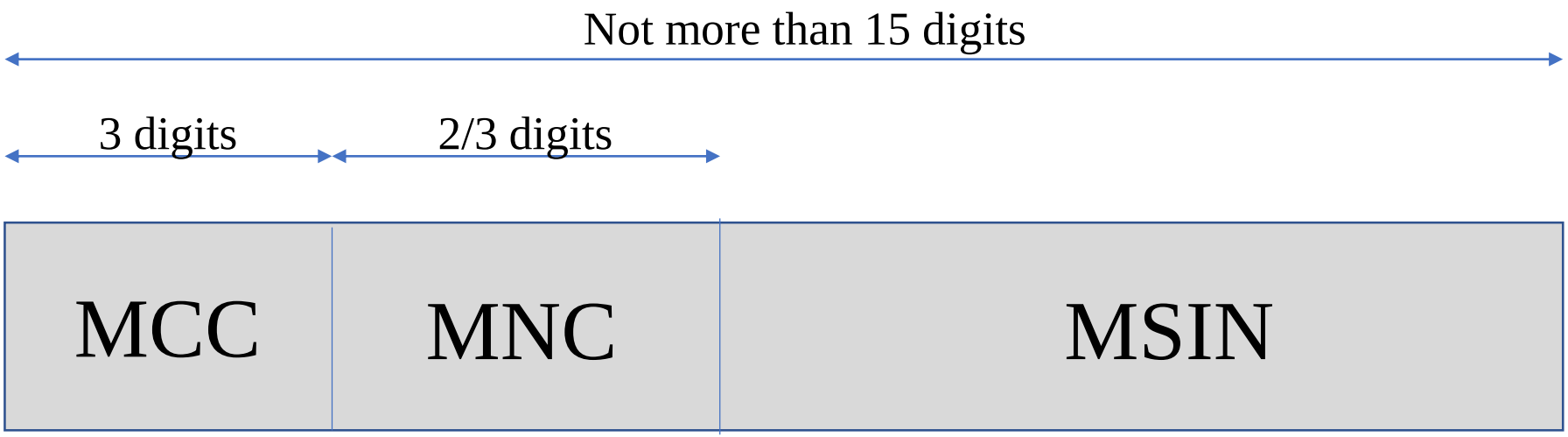


UIDN: user identity decryption node

EUIC的实现过程（对IMSI的加密解密算法）

GK：用户入网时，与HE/AuC及群中的其他用户共享的群密钥。SQN_UIC:USIM产生的序列号，每次均不同。

IMSI的组成



- MSIN(Mobile Station Identity Number)：移动用户鉴权码，是IMSI组成部分之一
- MCC：移动通信国家码
- MNC：移动网络码

3G中的密钥协商机制

3G系统中，增加了密钥协商机制，在认证和密钥协商机制的执行过程中实现。加密算法协商和完整性算法协商都是通过用户和网络之间的安全协商机制实现的。

◆ 当移动台需要与服务网络之间以加密方式通信时，以下列规则做出判断：

1. 如果移动台和服务网络没有相同版本的UEA（加密算法），但是网络规定要加密连接，则拒绝连接。
2. 如果移动台和服务网络没有相同版本的UEA(加密算法)，但是网络允许使用不加密的连接，则建立无加密的连接。
3. 如果移动台和服务网络有相同版本的UEA，由服务网络选择其中一个可接受的算法版本，建立加密连接。

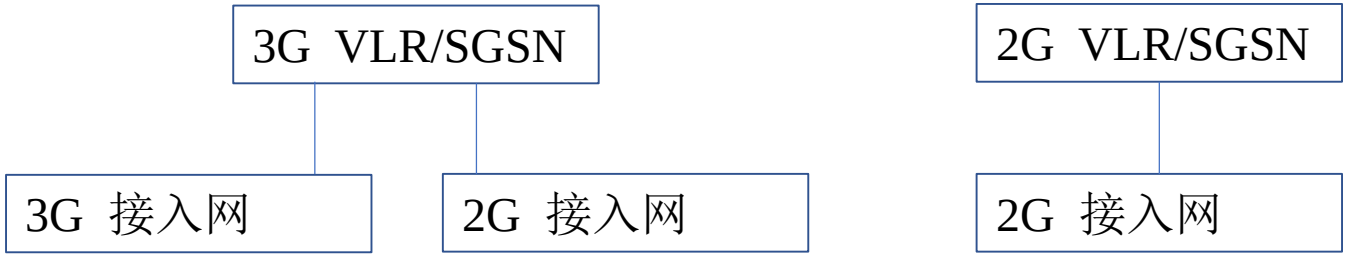
   3G系统中预留了15种UEA的可选范围。

为了实现用户信息和信令信息的完整性保护，服务网络与移动台之间以下列规则进行算法协商：

1. 如果移动台和服务网络没有相同版本的UIA（完整性算法），则拒绝连接。
2. 如果移动他和服务网络有相同版本的UIA，由服务网络选择一种可接收的算法版本，建立连接。3G系统中预留了16种UIA的可选范围。

通过实现算法协商，增加了3G系统的灵活性，使不同的运营商之间只要支持一种相同的UEA/UIA，就可以跨网通信。

2G和3G共存网络的安全性准则



2G和3G共存网络的接入环境

	USIM用户	SIM用户
3G VLR	3G 安全上下文	2G 安全上下文
2G VLR	2G 安全上下文	2G 安全上下文

通过实现算法协商，增加了3G系统的灵活性，使不同的运营商之间只要支持一种相同的UEA/UIA，就可以跨网通信。

2G和3G网络共存时的用户鉴权

用户使用USIM卡接入到2G和3G共存的网络中：

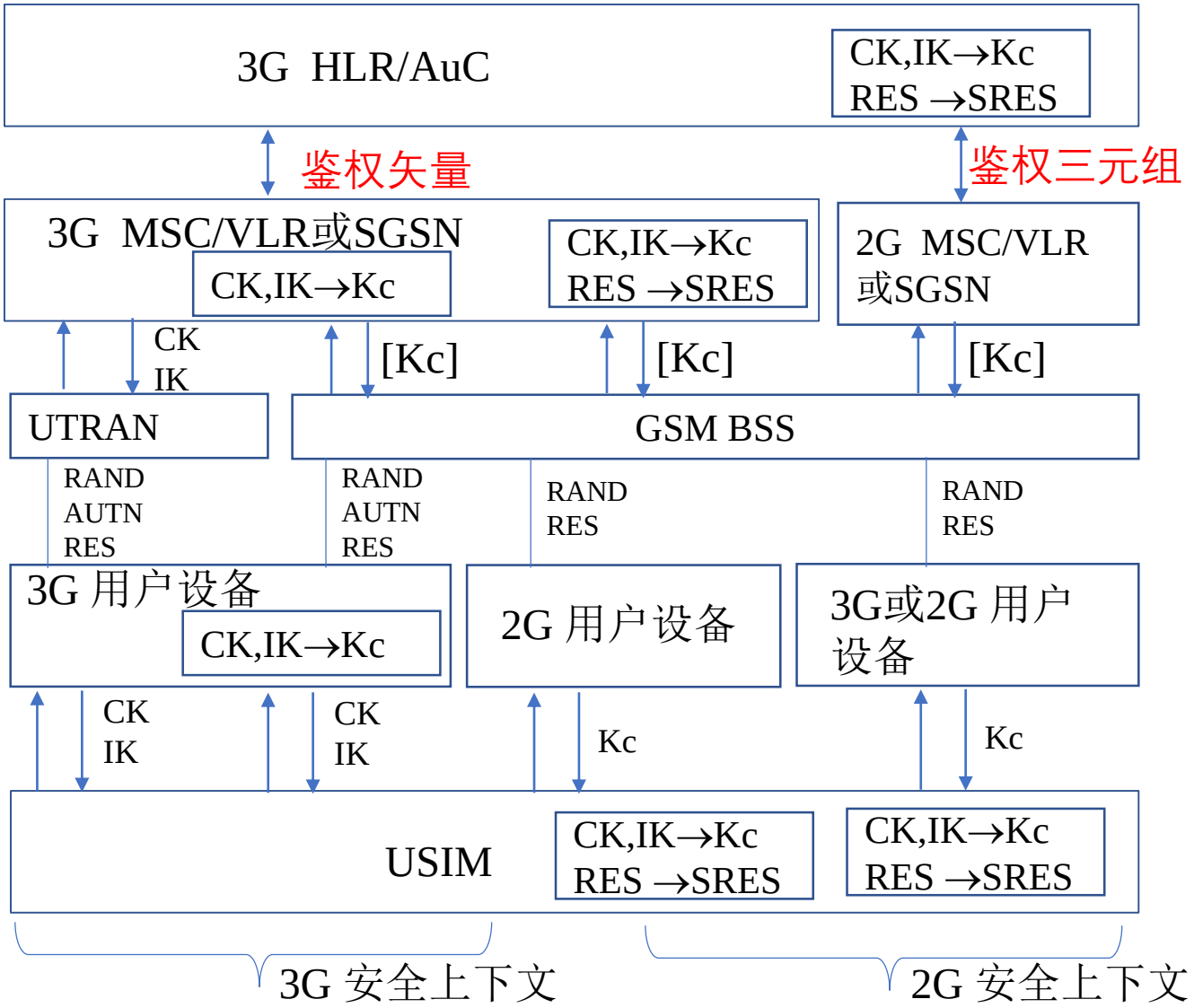
（1）通过UTRAN(WCAMA系统时IMT-2000家族的一员，它由CN(核心网)、UTRAN（UMTS陆地无线接入网）和UE(用户装置)组成。UTRAN和UE采用WCDMA无线接入技术。)接入时，使用UMTS（Universal Mobile Telecommunication System的缩写，中文译为通用移动电信系统）鉴权。

（2）当使用3G移动台和3G MSC/VLR或SGSN通过GSM BSS接入时使用UMTS鉴权机制。其中GSM密钥从UMTS CK和IK计算获得。

（3）如果使用2G移动台或2G MSC/VLR或SGSN通过GSM BSS接入，使用GSM鉴权机制。其中用户响应SRES和GSM密钥从UMTS SRES、CK和IK得到。

2G和3G网络共存时的用户鉴权

用户使用USIM卡接入到2G和3G共存的网络中：

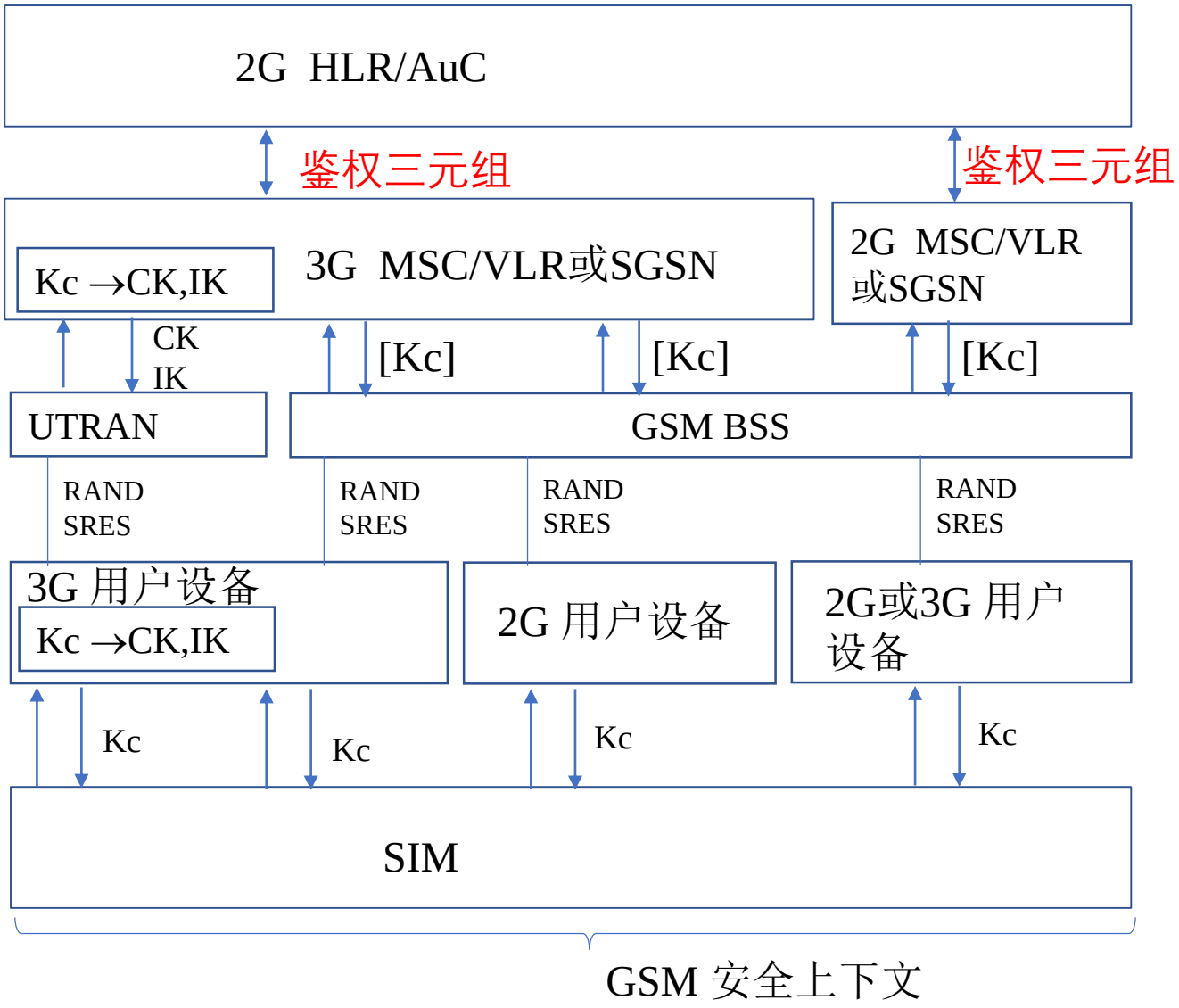


2G和3G网络共存时的用户鉴权

在2G和3G共存网络中，用户也可以使用SIM卡接入到网络中。由于GSM SIM用户只支持GSM系统安全特性，所以鉴权过程必然是GSM系统的。

注意：在SIM卡用户接入到UTRAN，与VLR/SGSN进行鉴权认证的过程以后，3G VLR/SGSN将利用CK和IK为用户提供安全保护，但由于此时用户安全特性的核心仍是GSM密钥Kc,所以用户并不具备3G的安全特性。

2G和3G网络共存时的用户鉴权



2G和3G网络共存时的用户鉴权

2G和3G安全上下文之间转换运算的算法

c1: RAND[GSM]=RAND

c2: SRES[GSM]=XRES*1 xor XRES*2 xor XRES*3 xor XRES*4

GSM中RES是32bit，所以将3G中的XRES分成每段为32bit的四部分。

XRES*=XRES*1 || XRES*2 || XRES*3 || XRES*4

如果XRES为128bit，XRES=XRES*
如果XRES不足128bit，就用0补足，即XRES*=XRES||0..0。

c3: Kc [GSM]=CK1 xor CK2 xor IK1 xor IK2

Kc是64bit，CK和 IK 是128bit，所以将CK、IK分为两半：CK=CK1||CK2，IK=IK1||IK2

c4: CK [USIM]=0..0||Kc，即Kc占据CK的低64bit，高64bit为0。

c5: IK [USIM]=Kc||Kc

概 要

第三代移动通信系统安全技术

3G移动通信技术简介

3G的安全体系结构

存在的问题

3G认证鉴权中可能存在的问题

A.3G认证方案实现了VLR对MS以及MS对HLR的认证，但不要求MS对VLR进行认证。因此攻击者X可以利用截获的合法IMSI进行如下的攻击：

① MS→X:IMSI;
② X →VLR:IMSI;
③ VLR →HLR: IMSI;
④ HLR →VLR: AV=RAND || XRES || CK || IK || AUTN;
⑤ VLR →X:RAND || AUTN;
⑥ X →MS: RAND || AUTN;
⑦ MS →X: RES;
⑧ X →VLR: RES.

这样，X就可以假冒该MS入网。但由于CK与IK未在无线接口中传输，攻击者无法获得这些密钥而进行正常的通信。但是3G认证方案没有考虑到网络端的认证与保密通信。若攻击者X对VLR和HLR之间的信息进行窃听，就可能获得HLR传给VLR的认证向量AV从而获得CK与IK。此后攻击者X在假冒该MS入网，即可实现正常的保密通信，而合法用户传送的信息也就失去了保密性。

3G认证鉴权中可能存在的问题

B.由于用户在不同的PLMN(Public Land Mobile Network)之间漫游，这些不同PLMN甚至可以是在不同的国家，为了对用户进行鉴权认证，本地网络（HE/HLR）会把用户的鉴权五元组发送到漫游的网络的VLR/SGSN，在这个过程中，用户鉴权向量组，穿过不同的网络，很容易受到攻击。

C. 在用户开机注册到网络的时候，或者网络无法从TMSI恢复出IMSI的时候（比如VLR/SGSN的数据库错误），用户将向网络以明文形式发送IMSI，这是非常不安全的做法，很容易遭到中间人攻击的。

D. 加密密钥和加密算法在3G中，不再是固定的（比如GSM中的A5加密算法是固定的）。但是必须要由一种安全的方法让用户和网络之间对加密密钥和加密算法进行协商。

作业

简述GSM与3G鉴权认证过程的不同。