Chap4 移动通信网络安全

- 4.1 移动通信网络概述
- 4.2 GSM安全
- 4.3 3G安全
- 4.4 4G安全
- 4.5 5G安全

4.1 1G\2G\2.5G\3G\4G\5G

1G、2G、3G、4G、5G是指第X代蜂窝移动通信系统（X表示1，2，3，4，5…），这种系统可以在非相邻的小区内使用相同的无线资源，即频率复用。每一代通讯标准都是建立在一种或多种技术突破的基础上实现数据速率的飞跃。


飞一般的感觉！5G网速比4G快100倍_电脑百事网
pc841.com | 594 × 232 jpeg | 图像可能受版权保护。
YOU ON 2G
YOU ON 3G
YOU ON 4G
YOU ON 5G

- **第一代：1G**
- 模拟语音时代，出现在1980年，属于语音时代。大哥大横空出世，没有移动、联通、电信。摩托罗拉、爱立信主宰天下。

- **第二代：2G**
- 2G时代是“文本时代”，这个时代我们的通信，不仅可以打电话还可以发短信。出现在1990年。诺基亚就是优秀代表，手机可以开始上网，但是只能看文字信息。下载速度也只有20K/s左右。

- **第三代：3G**
- 3G时代又被称为“图片时代”，实现了无线通信与互联网等多媒体通信手段的结合，能够传输数据信息。出现在2000年之后，流畅图文，语音，下载速度500K/s左右。
- 3G也成就了一个时代，那就是移动互联网。

- **第四代：4G**
- 被称为“视频时代”，能够传输高质量视频、图像且图像传输质量与清晰度可以与电视不相上下的技术产品。4G成就了很多视频公司，盘活了直播行业。

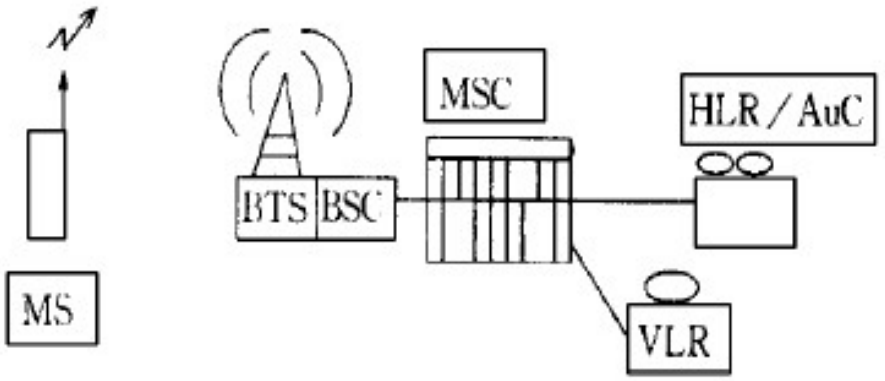
- **第五代：5G**
- 万物互联时代，是真正意义上的通信技术与互联网的融合。

4.3 2G:GSM安全实现

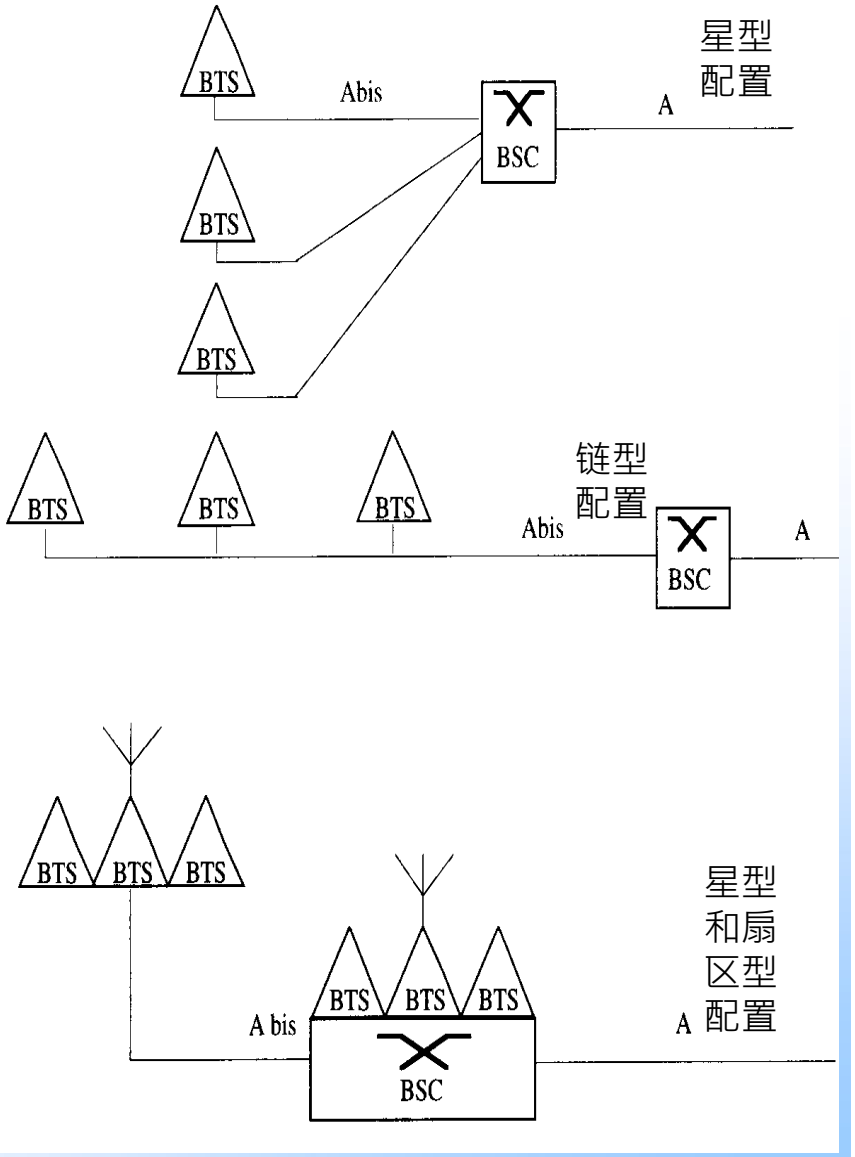
GSM特点

- “Global System for Mobile Communication”，即“全球移动通信系统”。它是第二代蜂窝系统的标准，是世界上第一个对数字调制、网络层结构和业务作了规定的蜂窝系统

GSM系统结构



MS:移动台　　BTS：收发信基站　BSC：基站控制器
MSC：移动业务交换中心　　HLR：归属位置寄存器
AUC：用户鉴权中心　　VLR：访问位置寄存器



基站控制器(BSC)：管理无线资源、信道的分配、根据BTS的测量结果来控制移动台或BTS的发射功率、决定是否执行切换（handover)。

移动业务交换中心(MSC)：对于位于它管辖区域中的移动台进行控制、交换的功能实体。

鉴权中心(AUC)：为认证移动用户的身份和产生相应鉴权参数(随机数RAND，符号响应SRES，密钥Kc)的功能实体。

- 归属位置寄存器(HLR)：管理部门用于移动用户管理的静态数据库。每个移动用户都应在其归属位置寄存器注册登记

—国际移动用户识别码IMSI（*International Mobile Subscriber Identity*），网络通过这个号码和用户联系，该号码是不对外的。

—用户使用的MSISDN（*Mobile Station ISDN Number*)号码，该号码是对外的。

① 目前，我国使用的手机号码为11位，其中各段有不同的编码方向：前3位———网络识别号； 第4-7位———地区编码；第8-11位———用户号码。它是唯一的识别移动电话的签约号码，每次签约都接至一个HLR

—用户的某些特征（允许使用的补充业务、允许打国际长途与否等)。

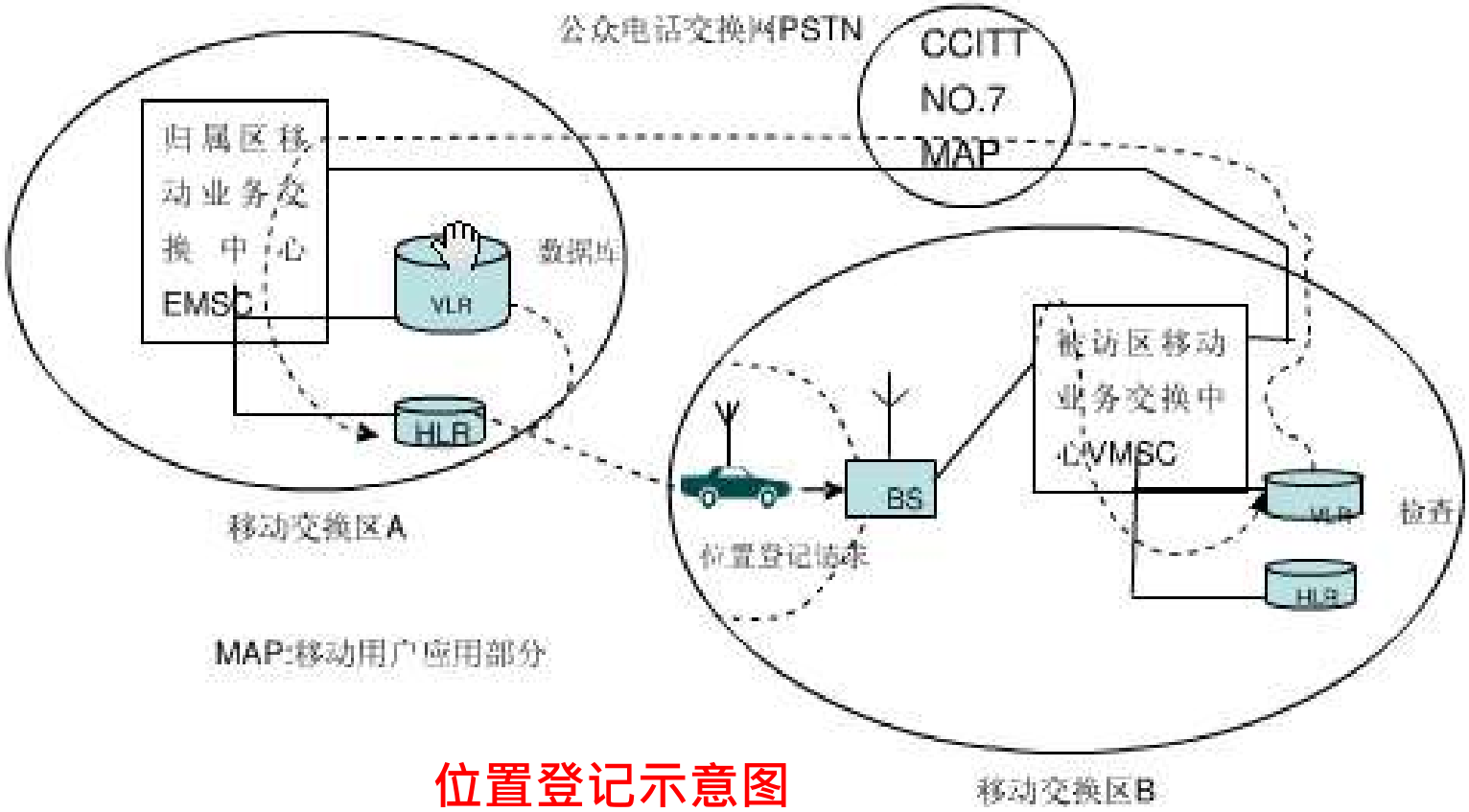
—为每个用户记录了访问过的访问用户位置寄存器VLR (Visitor Location Register)号码。

- 拜访位置寄存器(VLR)：是一个动态数据库，记录某个地区中出现的用户资料。这些资料是从该移动用户的归属位置寄存器HLR获取并暂时保存，一旦移动用户离开该VLR的控制区域，则该用户的数据就会被删除。

1. 当移动用户漫游到新的MSC控制区时，它必须向该地区的VLR申请登记。

2. VLR要从该用户的HLR查询有关的参数，要给该用户分配一个新的漫游号码（MSRN），并通知其HLR修改该用户的位置信息，准备为其它用户呼叫此移动用户时提供路由信息。

3. 如果移动用户由一个VLR服务区移动到另一个VLR服务区时，HLR在修改该用户的位置信息后，还要通知原来的VLR，删除此移动用户的位置信息。



位置登记示意图

移动设备：SIM卡

- 用户身份模块（Subscriber Identity Module，SIM ），通常称为“SIM卡”，是保存移动电话服务的用户身份识别数据的智能卡。SIM还能够存储短信数据和电话号码。
- SIM由CPU、ROM、RAM、EEPROM和I/O电路组成。
- SIM卡可供GSM网络对客户身份进行鉴别，并对客户通话时的语音信息进行加密。

移动设备：SIM卡中存储的相关标识

（1）国际移动用户识别码（IMSI）

international mobile subscriber identity

是用于区分蜂窝网络中不同用户的、在所有蜂窝网络中不重复的识别码。手机将IMSI存储于一个64比特的字段发送给网络。IMSI可以用来在归属位置寄存器（HLR，Home Location Register）或拜访位置寄存器（VLR，Visitor Location Register）中查询用户的信息。为了避免被监听者识别并追踪特定的用户，大部分情形下手机和网络之间的通信会使用随机产生的临时移动用户识别码（TMSI，Temporary Mobile Subscriber Identity）代替IMSI。

- 共15位，MCC+MNC+MIN

MCC：Mobile Country Code，移动国家码，中国为460;

MNC: Mobile Network Code，移动网络码，共2位，中国移动TD系统使用00，中国联通GSM系统使用01，中国移动GSM系统使用02，中国电信CDMA系统使用03

MIN：共有10位，移动用户识别号,运营商自信分配

IMSI 结构的范例

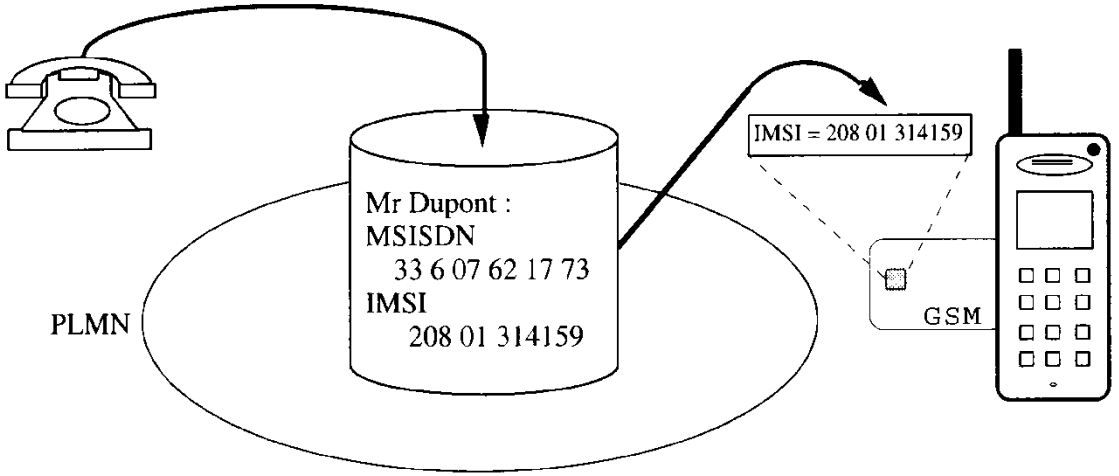
IMSI:310150123456789

MCC	310	美国
MNC	150	美国电话电报公司（AT&T Mobility）
MSIN	123456789	

IMSI:460001357924680

MCC	460	中华人民共和国
MNC	00	中国移动
MSIN	1357924680	

- IMSI，这个是用来唯一标识你 SIM 卡的，IMSI 和手机号对应（如果你手机卡丢了去补，新补来的卡 IMSI 和原有的不同，旧的卡就再也不能用了）。



（2）临时识别码(TMSI:Temporary Mobile Subscriber Identity)

- 临时识别码的设置是为了防止非法个人或团体通过监听无线路径上的信令交换而窃得移动客户真实的客户识别码(IMSI)或跟踪移动客户的位置。

（3）国际移动设备识别码（IMEI：International Mobile Equipment Identification Number）

- 是区别移动设备的标志，储存在移动设备中，可用于监控被窃或无效的移动设备。
- 防止盗用或使用非法设备入网

（4）基站识别码（BSIC）

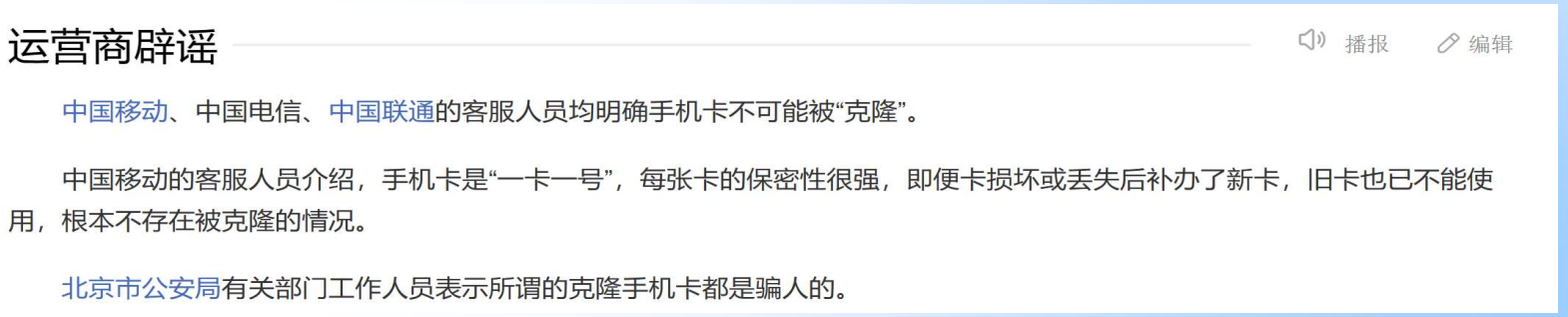
- BSIC用于移动台识别不同的相邻基站，BSIC采用6比特编码。

（5）区域识别码LAI

用于移动用户的位置更新。 LAI=MCC+MNC+LAC 。MCC=移动国家码，识别国家。MNC=移动网号。LAC=位置区号码，识别一个GSM网中的位置区。

SIM卡存储的数据可分为四类：

- 第一类是固定存放的数据。这类数据在ME（Mobile Equipment）被出售之前由SIM卡中心写入，包括国际移动用户识别号（IMSI）、鉴权密钥（KI）等；
- 第二类是暂时存放的有关网络的数据。如位置区域识别码（LAI）、移动用户暂时识别码（TMSI）、禁止接入的公共电话网代码等；
- 第三类是相关的业务代码，如个人识别码（PIN）、解锁码（PUK）、计费费率等；
- 第四类是电话号码簿，是手机用户随时输入的电话号码。



SIM卡的保密算法和密钥

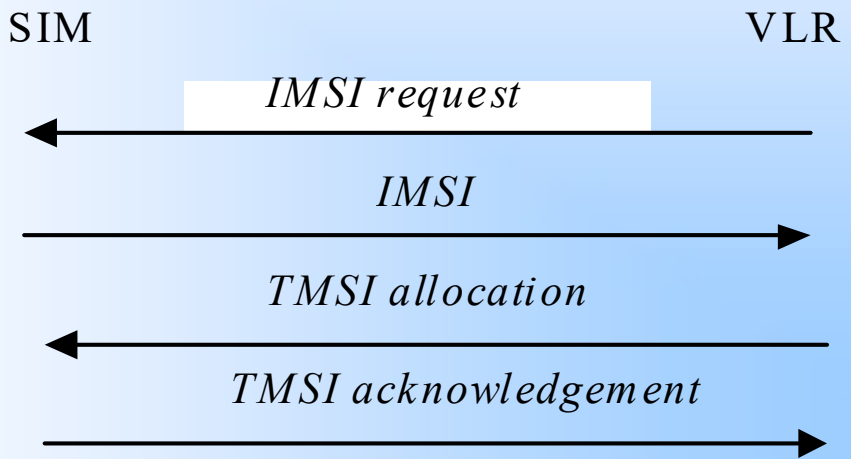
- SIM卡中最敏感的数据是保密算法A3、A5、A8算法、密钥Ki、和Kc。
- A3、 A5、 A8算法是在生产SIM卡的同时写入的，一般人都无法读；
- Kc是在加密过程中由Ki （16 个字节的密钥数据）导出；
- IMSI、Ki同时保存在SIM卡中、AUC鉴权中心。

eSIM卡

- eSIM就是电子化的SIM卡，是一个数据文件，可通过网络下载到移动终端。功能上和普通SIM卡无异，有了它，各种电子产品就能连接上网、接播电话、发短信等。

GSM用户身份保密

- IMSI相当于用户在GSM网络里的身份证，可以用它来处理用户身份识别、统计通信费用等网络内部需求。
- 为了实现保密，用TMSI（Temporary Mobile Subscriber Identity）代替IMSI,存储在GSM网络的VLR中，它用于在一定时间内代替用户的真实身份。
- 只有在用户开机或者VLR数据丢失的时候IMSI才被发送，平时仅在无线信道上发送移动用户相应的TMSI。
- TMSI会定期更新。



GSM鉴权和加密

(1)鉴权与加密的重要特征

- 客户的鉴权与加密是通过系统提供的客户三参数组来完成的。

- 每个客户在签约（注册登记)时，就被分配一个客户号码(客户电话号码)，客户识别码(IMSI)、 客户鉴权键Ki，它被分别存储在客户SIM卡和AUC（鉴权中心）中。

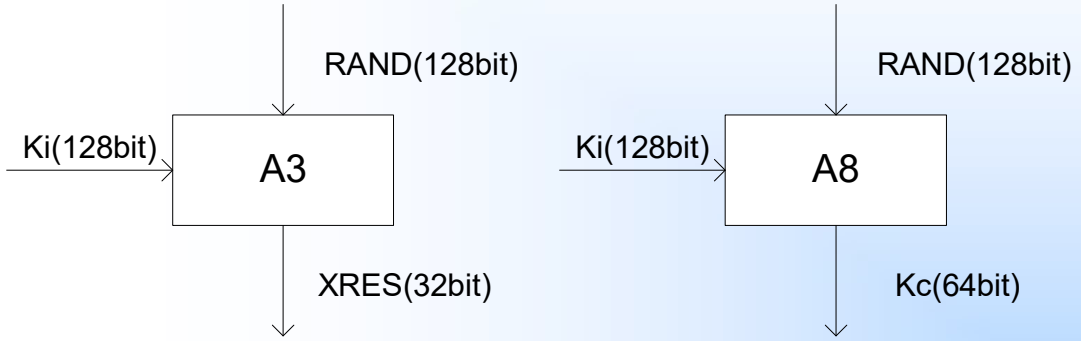
- AUC (Authentication Center)中还有个伪随机码发生器，用于产生一个不可预测的伪随机数 (RAND，16字节)。

GSM系统中的鉴权认证过程

（1）AuC产生一个随机数RAND，通过（AuC中的）A3、A8算法产生认证（鉴权）向量组（RAND，XRES，Kc）。

（2）VLR/MSC收到鉴权三元组以后存储起来。当移动台注册到该VLR时，VLR/MSC选择一个认证向量，并将其中的随机数RAND发送给移动台。

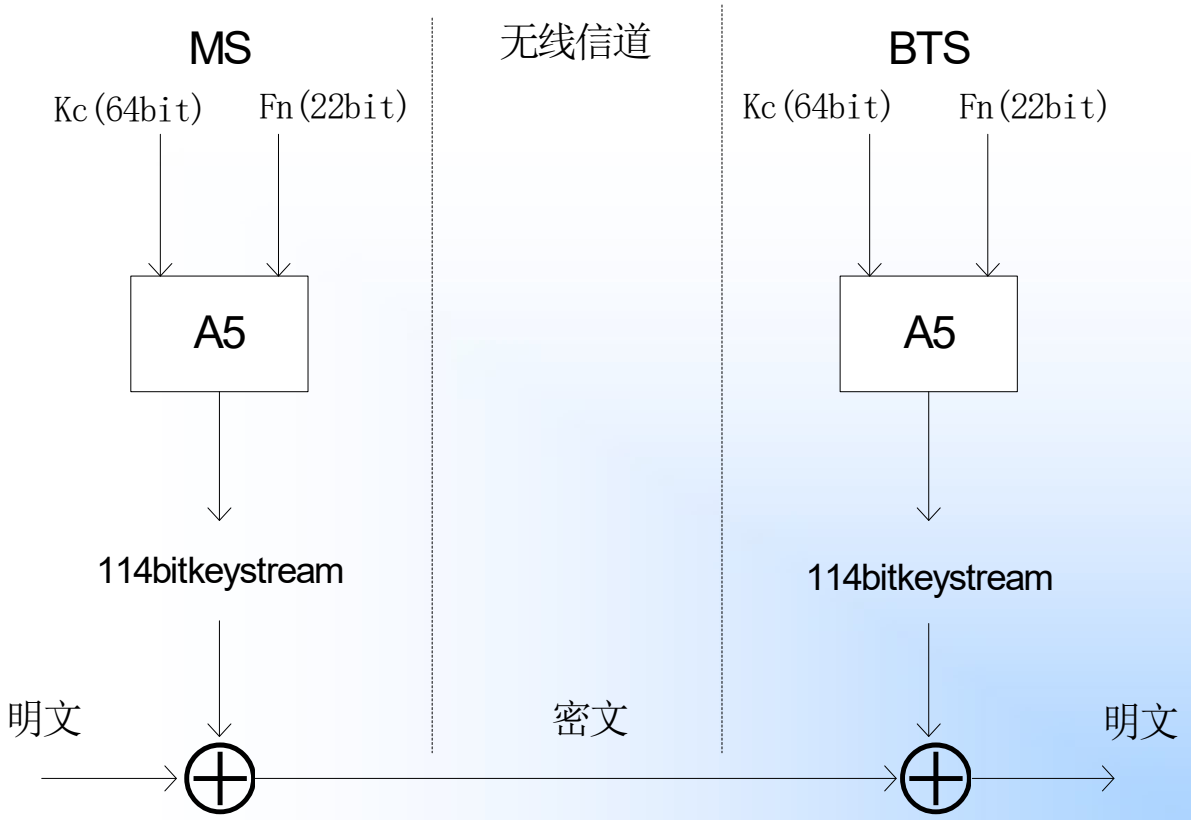
（3）移动台收到RAND以后，利用存储在SIM卡中的A3、A8算法，计算出SRES和Kc。移动台将SRES发送给VLR/MSC，如果SRES等于VLR/MSC发送给用户的RAND所在的鉴权三元组中的XRES，移动台就完成了向VLR/MSC验证自己身份的过程。



（4）存储在MS 和AuC 内的Kc 都是由Ki 和一个随机数通过A8算法运算得出的。密钥Ki 以加密形式存储在SIM 卡和AuC 中。

当移动台第一次到达一个新的MSC时，MSC会向移动台发出一个随机号码RAND，发起一个鉴权认证过程。

将密钥Kc（64比特）和当前帧的序列号（22比特）作为参数，使用A5算法，得到114比特流；此比特流与需要加密的114比特信息异或，得到密文；



A5算法使用Kc加密后的TMSI（32bit）派送给移动电话。

GSM安全性分析

主要针对语音业务：

（1）TMSI的安全新问题

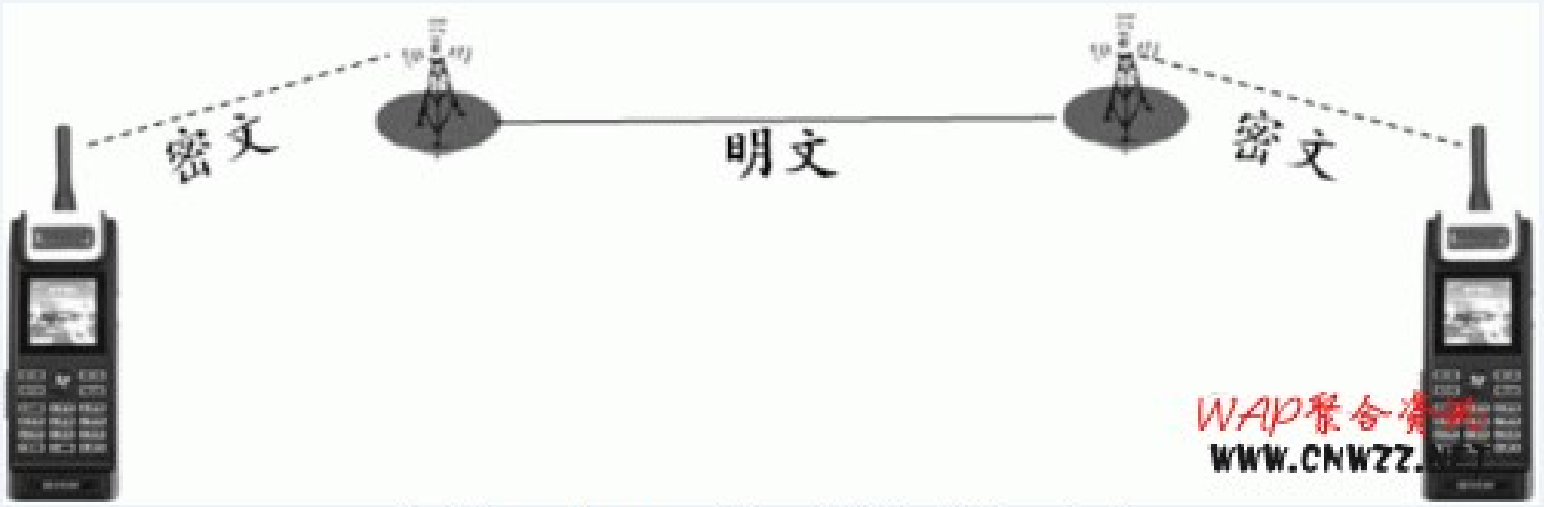
- 但移动用户第一次注册和漫游时，会以明文方式发送IMSI给MSC/VLR，此时容易被窃听；

（2）认证方案缺陷

- 单向认证。因此可以伪造合法基站，向用户发送查询消息，获得用户的IMSI等信息；
- 需要网络端必须事先保护用户密钥Ki，在数据库中明文保存密钥，一旦泄露。。。。
- 无第三方仲裁功能，当网络各实体间出现费用纠纷时无法提交给第三方进行仲裁；

（3）加密方案的缺陷

- 不是端到端加密
- 没考虑到数据完整性保护
- 密钥过短，Kc64比特



图片1现有GSM网络仅支持空中接口加密

（4）加密算法是不公开的

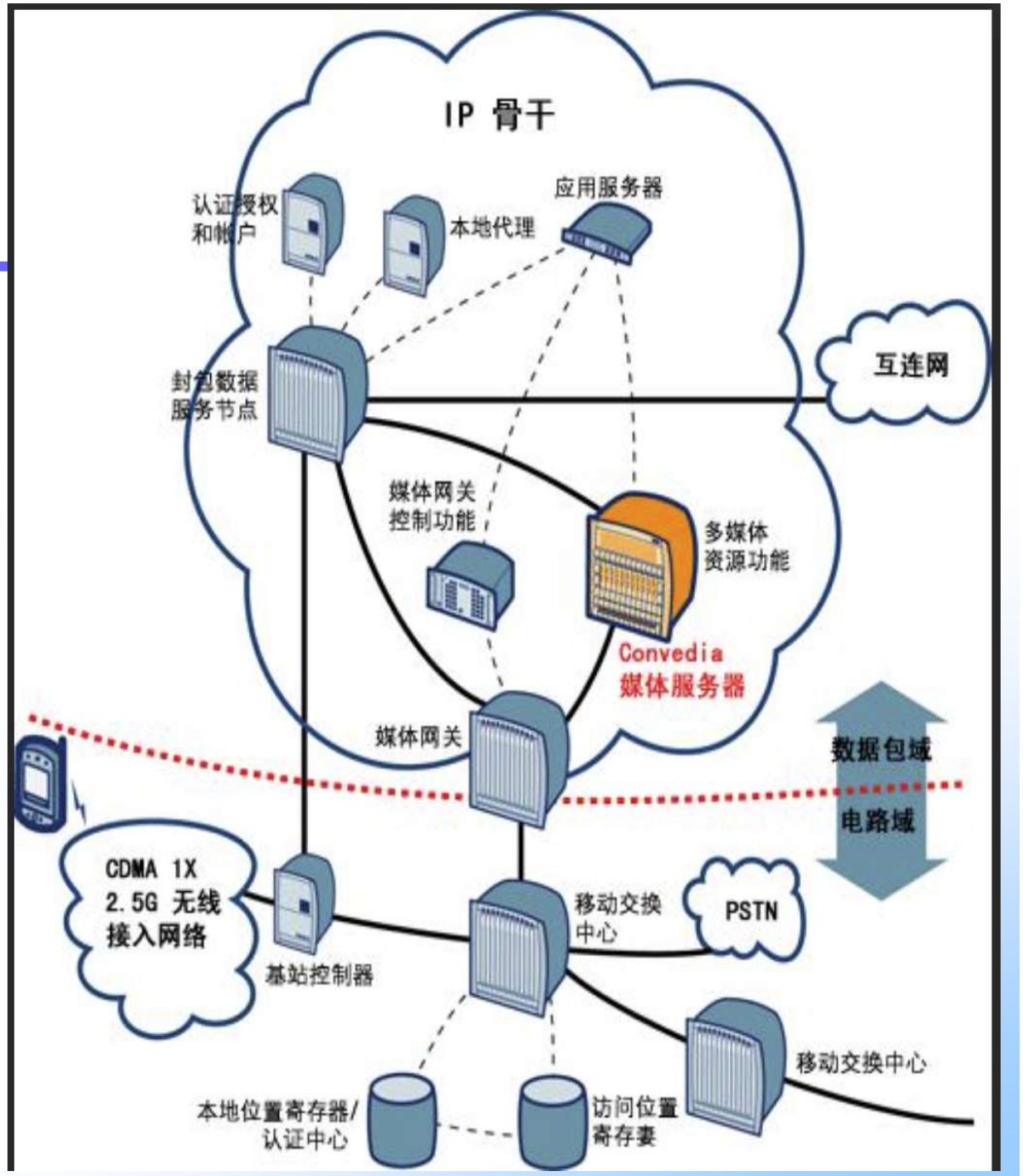
这些密码算法的安全性不能得到客观的评价，在实际中，也受到了很多攻击。

（5）加密算法是固定不变的

没有更多的密钥算法可供选择，缺乏算法协商和加密密钥协商的过程。

4.3 3G安全

- 3G时代又被称为“图片时代”
- 3G成就移动互联网



3G安全威胁

（1）对敏感数据的非法获取：

- 侦听
- 伪装
- 流量分析：攻击者对链路中消息的时间、速率、源及目的地等信息进行分析从而判断用户位置或了解重要的商业交易是否正在进行；
- 浏览：攻击者对敏感信息的存储位置进行搜索；
- 泄露：攻击者利用合法接入进程获取敏感信息；
- 试探：攻击者通过向系统发送一信号来观察系统反应。

3G安全威胁

（2）对敏感数据的非法操作：对消息的篡改、插入、重放或删除。

（3）对网络服务的干扰或滥用：

●干扰：攻击者通过阻塞用户业务、信令或控制数据使合法用户无法使用网络资源；

●资源耗尽：用户或服务网络利用其特权非法获取非授权信息；

●服务滥用：攻击者通过滥用某些系统服务从而获取好处或者导致系统崩溃。

（4）否认：主要指用户或网络否认曾经发生的动作。

（5）对服务的非法访问：

●攻击者伪造成网络和用户实体对系统服务进行非法访问；

●用户或网络通过滥用访问权利非法获取未授权服务

- 第三代手机卡
  USIM: Universal Subscriber Identity Module（全球用户识别卡）

  - 在安全性方面对算法进行了升级，并增加了卡对网络的认证功能，这种**双向认证**可以有效防止黑客对卡片的攻击，，**“伪基站”就不灵光了。**

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	算法	f8
	密钥	Kc:64bit	密钥	CK:128bit
	算法灵活性	固定的加密算法	算法灵活性	用户可以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安全措施：安全原则和安全目标

- 3G的安全将建立在第二代系统的安全之上
- 3G的安全要确定和校正第二代系统中的实时的和已认识到的缺点；
- 3G的安全要提供新的安全特征，并保护3G提供的新的业务。

3G安全措施

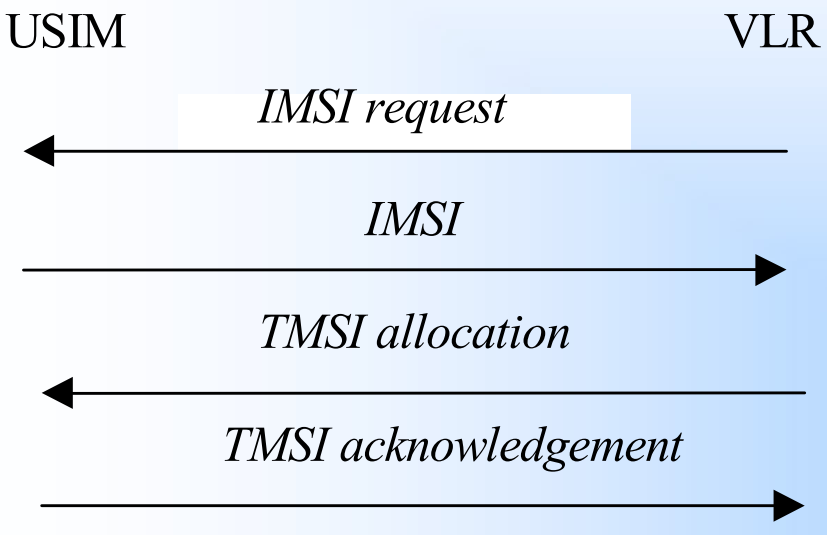
安全措施分为5类：

- 身份保密：对USIM（用户业务识别模:块）身份信息进行认证；
- 用户与服务网间身份认证（UIC）；
- 认证与密钥分配：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；
- 数据加密（DC）：
- 数据完整性（DI）：用于对交互消息的完整性、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分别实现DC和DI标准算法。f6、f7用于实现身份保密。认证与密钥分配由f0~f5实现。

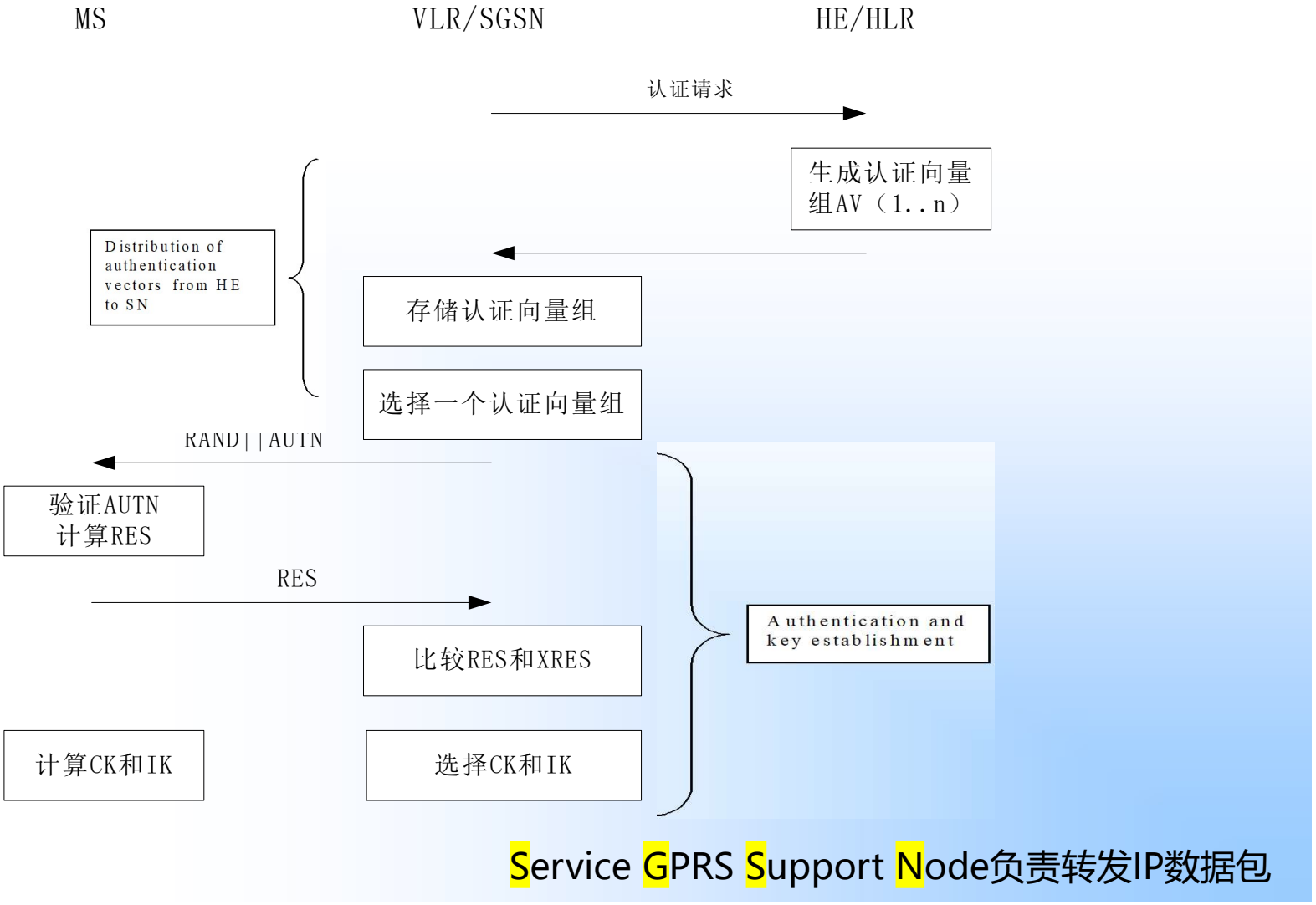
3G安全措施(1):身份保密

- User Confidentiality



Advanced Network Technology

3G安全措施(2):3G鉴权认证过程



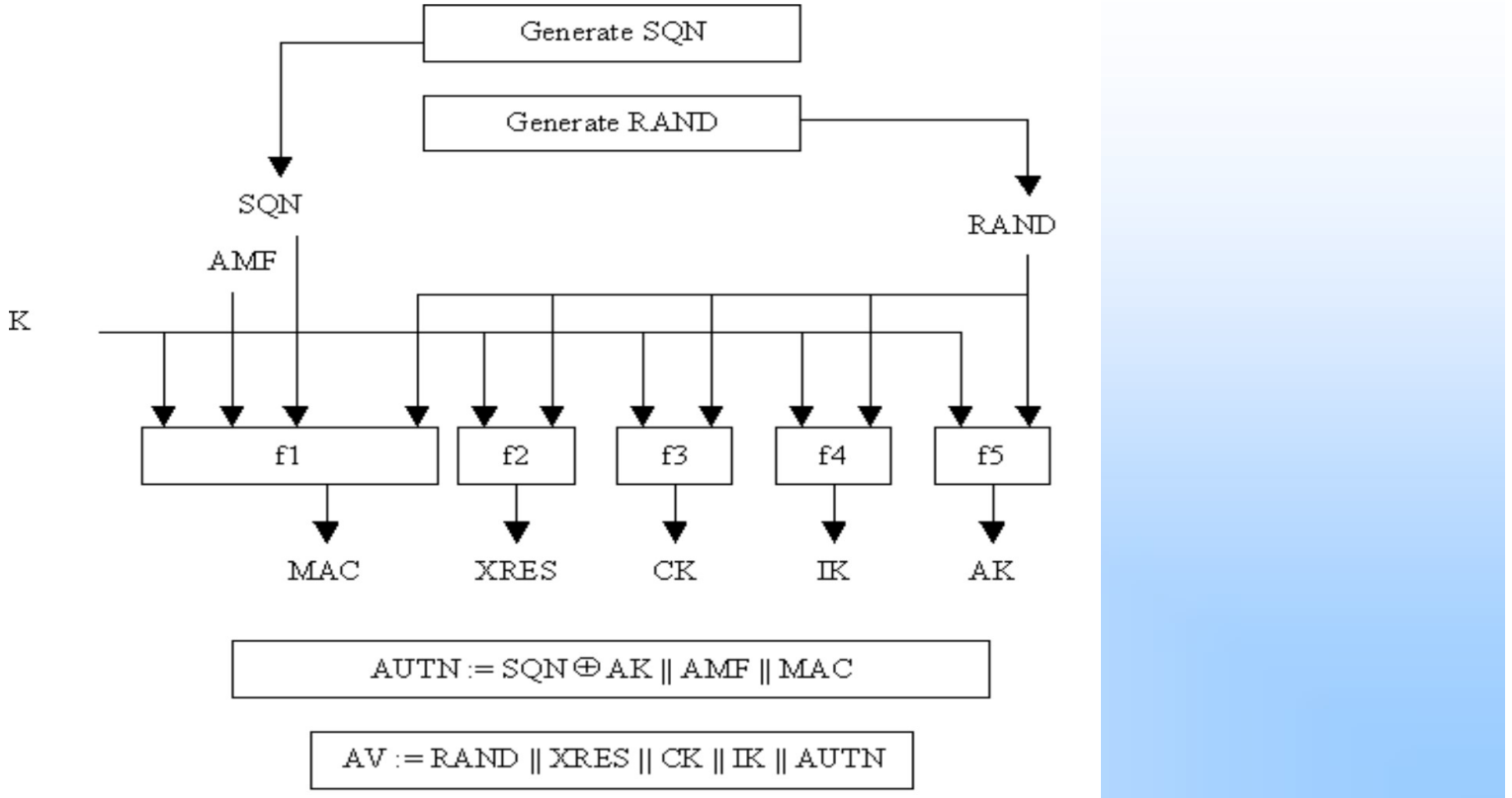
Service GPRS Support Node负责转发IP数据包

Step1：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）只存放于AuC中，用于生成RAND。

3G认证向量中有一个“认证令牌”AUTN，包含了一个序列号，使得用户可以避免受到重传攻击。

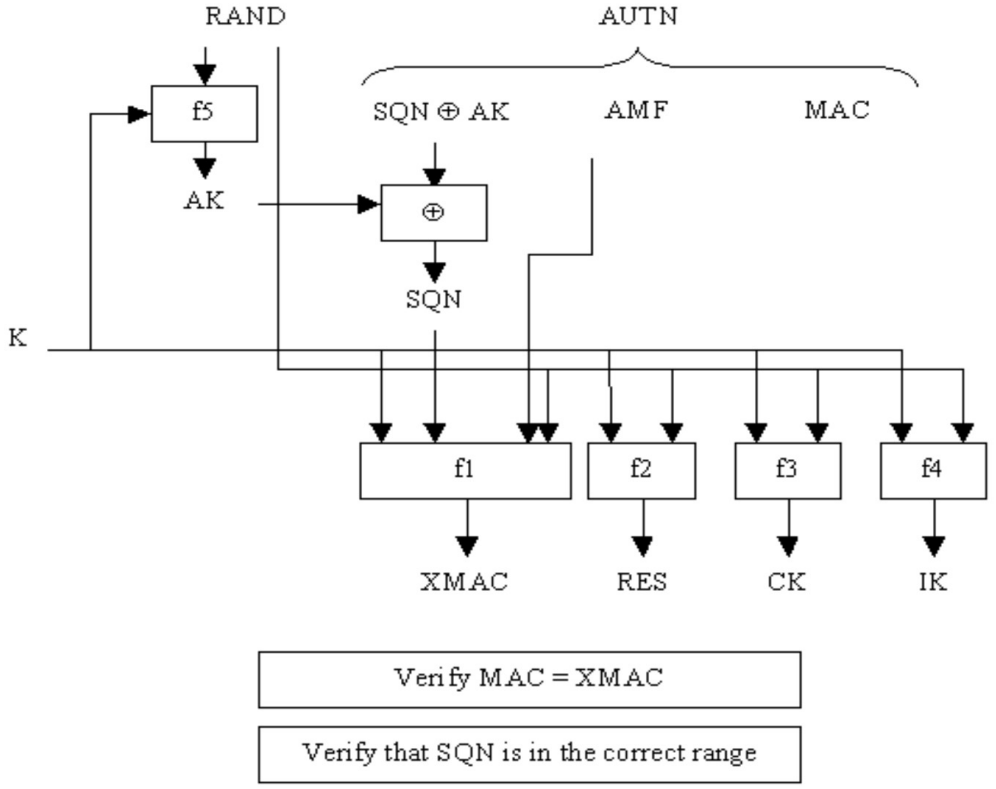
其中AK是用来在AUTN中隐藏序列号，因为序列号可能会暴露用户的身份和位置信息。AMF：认证与密钥管理字段

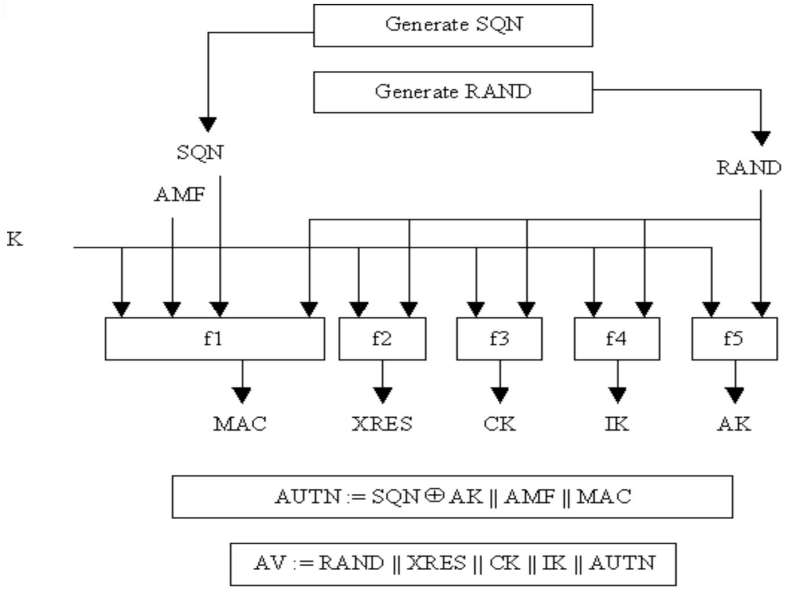
f0是一个伪随机数生成函数，只存放于AuC中，用于生成随机数RAND。



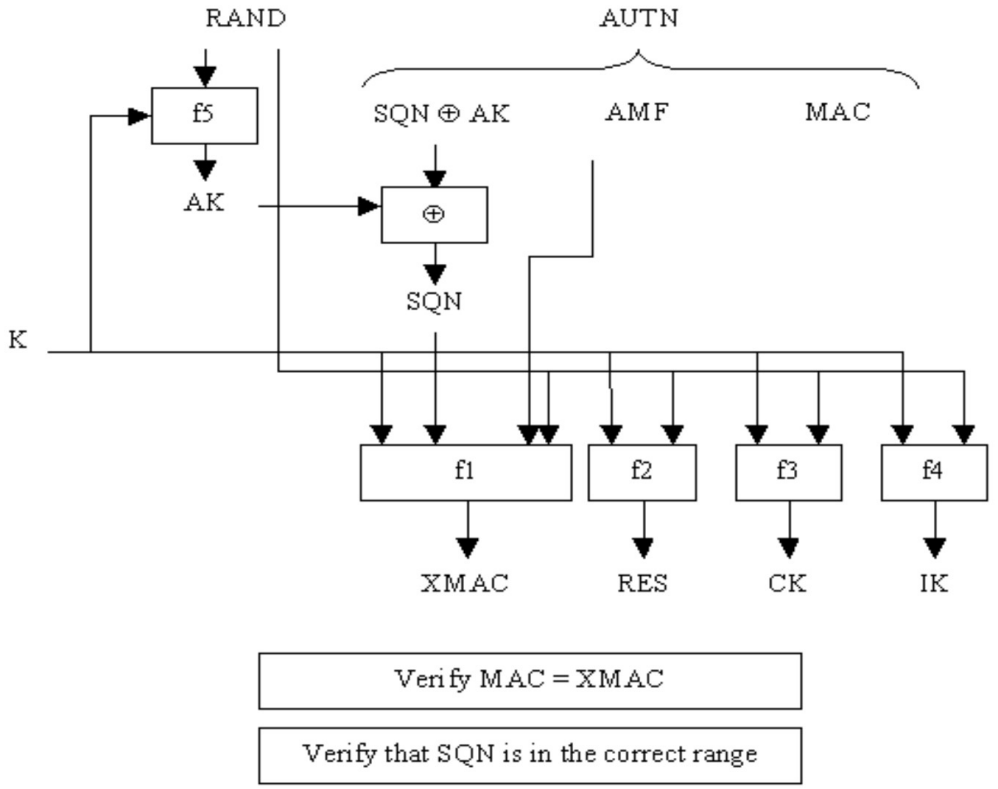
Step2： 当认证中心收到VLR/SGSN的认证请求，发送N个认证向量组给VLR/SGSN。在VLR/SGSN中，每个用户的N个认证向量组，按照“先入先出”（FIFO）的规则发送给移动台，用于鉴权认证。

Step3：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。





发送方行为



Step4：

① 首先计算AK并从AUTN中将序列号恢复出来SQN=(SQN⊕AK)⊕AK；

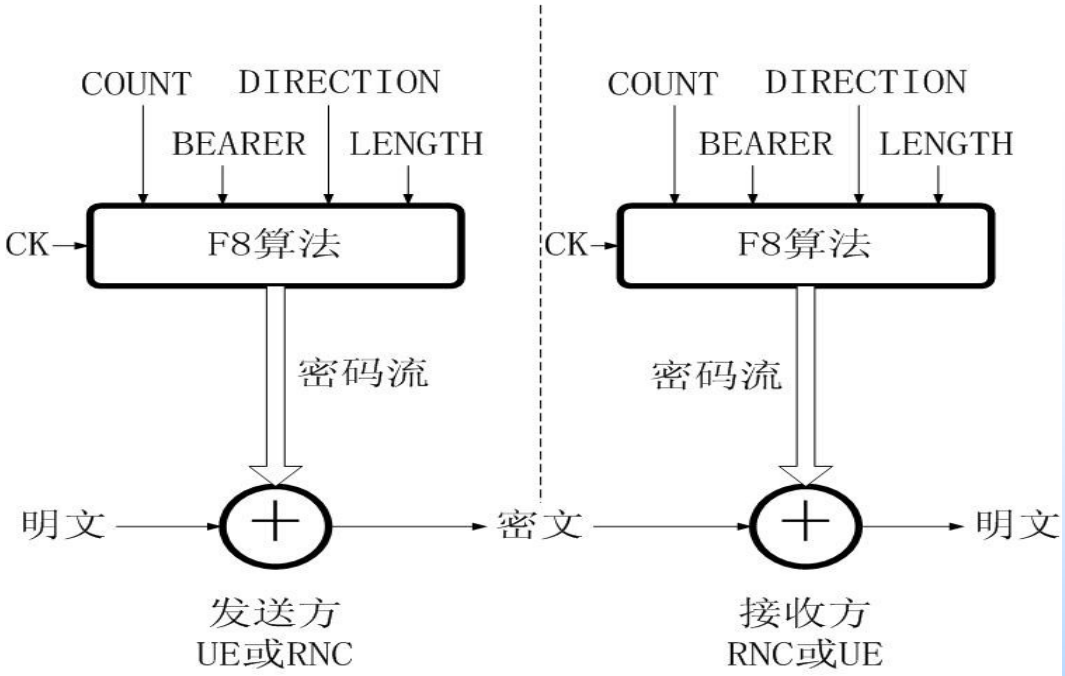
② USIM计算出XMAC，将它与AUTN中的MAC值进行比较。如果不同，用户发送一个“用户认证拒绝” 。VLR/SGSN向HLR发起一个“认证失败报告”。然后由VLR/SGSN决定是否重新向用户发起一个认证过程。

③ 用户比较收到的SQN是否在正确范围内：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。

④ 用户计算出加密密钥CK=f3(RAND，K)，完整性密钥IK=f4(RAND，K)

安全措施(3):数据机密性

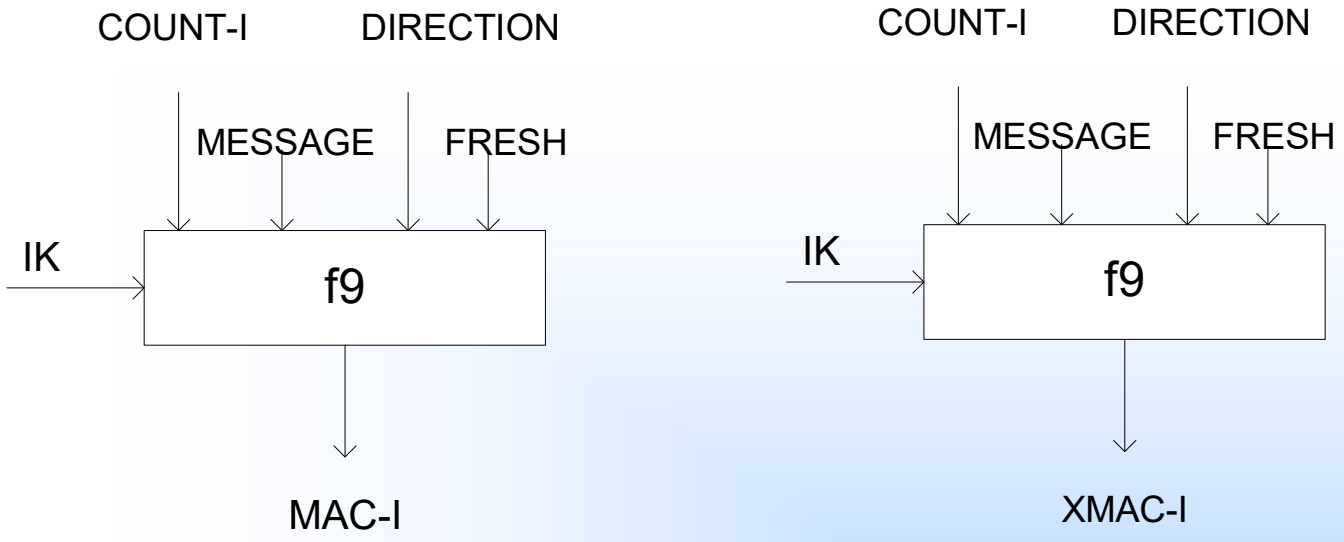
加密密钥CK，进行加解密。



COUNT：密钥序列号，32bit； BEARER：链路身份指示，5bit
DIRECTORY：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

安全措施(4):信息完整性

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。



UE　　RNC

COUNT-I：密钥序列号，**32bit**

MESSAGE：消息

DIRECTORY：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

安全措施(5):密钥协商机制

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），但是网络规定要使用加密连接，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）如果移动台和服务网络有相同版本的UIA，由服务网络选择一种可接受的算法版本，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，不同的运营上之间只要支持一种相同的UEA/UIA，就可以跨网通信。

AKA概念

- AKA全称是第三代移动通讯网络的认证与密钥协商协议，是国际移动电信组织3GPP(The Third Generation Partnership Project）在研究2G安全脆弱性的基础上，针对3G接入域安全需求提出的安全规范。

3G安全分析

- 1）3G鉴权认证过程中虽然增加了终端对网络的认证，但仅对归属地网络HLR进行认证，并没有认证拜访地网络VLR，利用这一漏洞攻击者就可以在空口截获合法的IMSI进行攻击。
- 2)3G网络没有对网络内部的通信链路进行保护，攻击者在VLR和HLR之间的通信链路上嗅探鉴权向量AV，从而获得CK和IK。
- 3）3G AKA也暴露出一些隐私问题，如攻击者通过重放预先截获某用户的认证令牌(AUTN)，借助3G AKA对消息鉴权码(MAC)校验失败和同步失败的提示不同，判断该特定用户是否在当前小区内。
- 总之，3G系统的安全性有一个前提：整个网络内部是可信的。

4.4 4G

- 4G通信技术基于3G通信技术基础上不断优化升级、以WLAN技术为发展重点。4G通信技术的创新使其与3G通信技术相比具有更大的竞争优势。

（1）首先，4G通信在图片、视频传输上能够实现原图、原视频高清传输，其传输质量与电脑画质不相上下；

（2）利用4G通信技术，在软件、文件、图片、音视频下载上其速度最高可达到最高每秒几十兆，这是3G通信技术无法实现的；

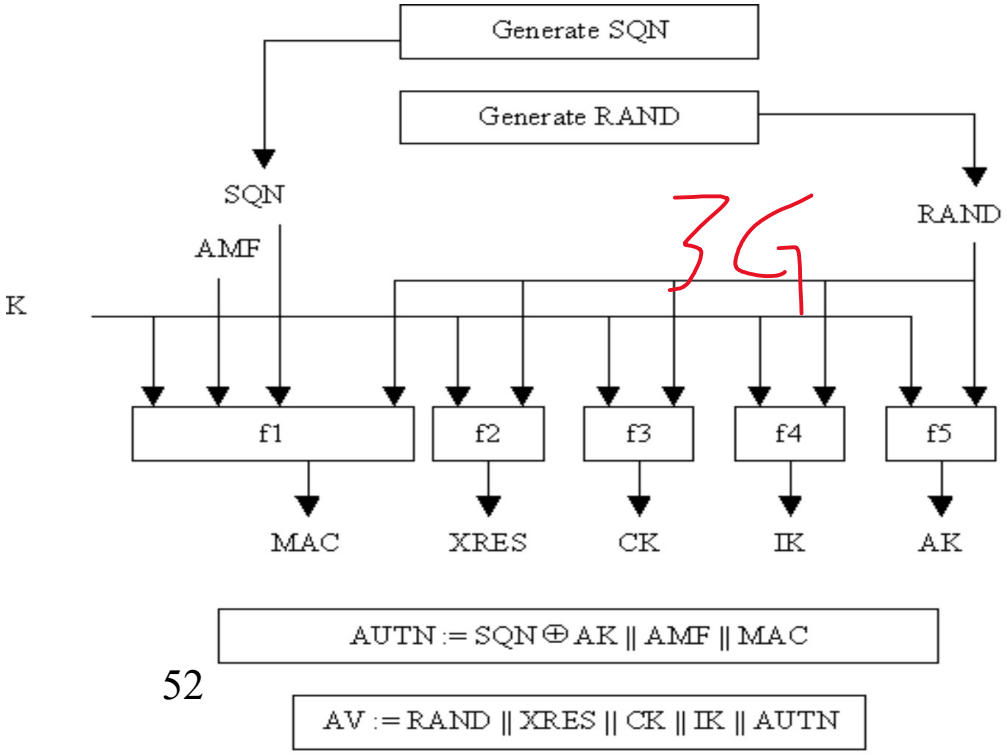
（3）安全层次和密钥管理机制相比3G系统有了很大改进；

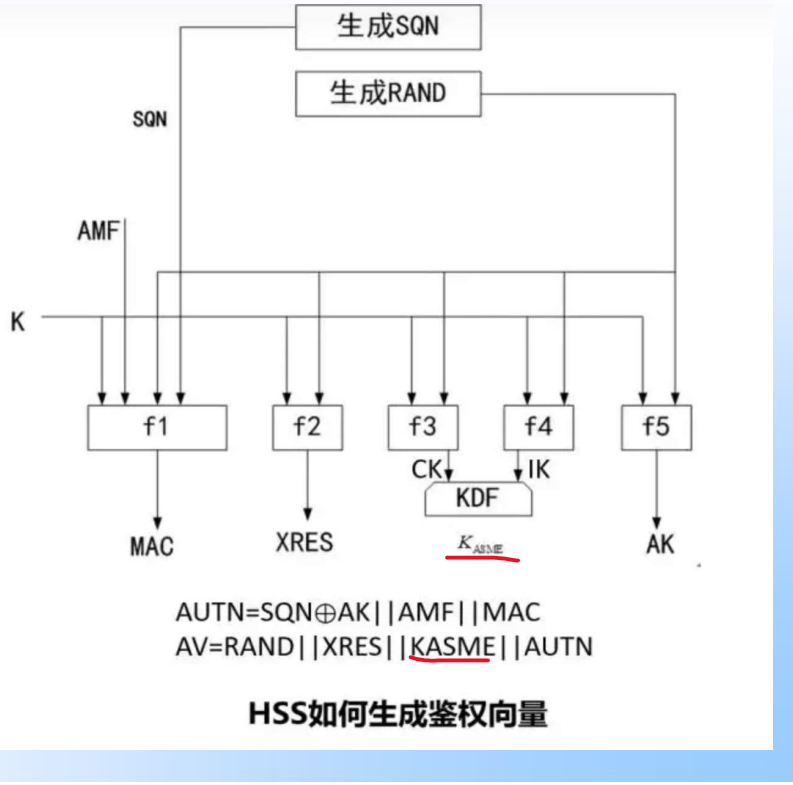
LTE

- “Long term Evolution”，直译“长程演进”。它是3G的演进，是3G与4G技术之间的一个过渡，是3.9G的全球标准。但是由于不断的在继续改善升级，所以后续版本已经成为了真正的4G。
- 4G和LTE并不是一回事，不过一般而言，LTE网络都能满足4G网络的标准(下行100Mbps)，而4G时代又以LTE网络为主，所以通常把二者结合在一起，统称为4G LTE。
- 4G LTE最大的数据传输速率超过100Mbps，这个速率是移动电话数据传输速率的1万倍，也是3G移动电话速率的50倍。

LTE鉴权

- 4G LTE对用户的鉴权过程与3G并没有本质的区别，采用的都是AKA机制，改变的部分是将HSS返回原有的五元组变成了四元组.
- 归属签约用户服务器（Home Subscriber Server，HSS）





LTE鉴权（自阅）

- LTE鉴权是一个基于四元组的鉴权：Kasme 、AUTN、RAND以及XRES。
  （1）UE向NAS层MMS发起鉴权请求；
  （2）MME则向HSS索要鉴权向量；
  （3）HSS 返回一套或多套EPS 鉴权向量{RAND,AUTN,XRES, Kasme}给MME，其中包含AMF分隔符，” 1”代表 LTE/SAE,”0”代表非LTE/SAE,如GSM,UMTS；
- （4）MME收到后保存XRES、 Kasme并将随机数RAND和鉴权令牌AUTN发送给UE；
- （5）UE通过AUTN对网络进行鉴权，并根据AUTN&RAND计算出RES&CK/IK，进一步计算出Kasme；
  （6）UE与MME根据Kasme推导出NAS层与AS层所需的加密密钥和完整性保护密钥。
- 当UE从ACTIVE到IDLE态时，将删除这些密钥；

4.5 5G

- 在以往的通信系统中，主要满足的是人与人之间的通信，而5G网络需要满足人与物以及物与物之间的通信，因此5G需要支持多种网络的接入，如无线局域网络(WLAN，wireless local areanetworks)、LTE、固定网络、物联网(IoT，Intemet ofthings)、卫星接入、车联网等，而不同的网络所使用的接入技术不同，因此有不同的安全需求和接入认证机制。

- 再者，由于各种智能穿戴设备的兴起，一个用户可能携带多个终端，而一个终端也可能同时支持多种接入方式，有些场景可能需要同一个终端在不同接入方式之间进行切换，或者用户在使用不同终端进行同一个业务时，要求能进行快速认证以保持业务的延续性从而获得流畅的用户体验 。

- 多种设备接入必然导致不同类型设备计算能力的差异；而有些能力低的终端设备，甚至没有特定的硬件来安全存储身份标识（IP地址、Mac地址）及认证凭证；

总之，5G网络需要构建一个统一的身份管理系统，使得其能够支持不同的认证方式、认证凭证和身份标识。

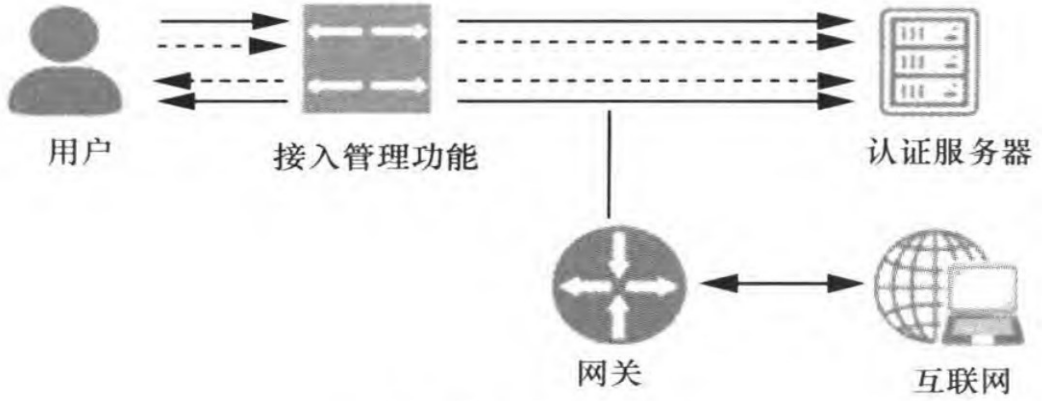


图 9　统一认证框架

5G安全 自阅

- 5G AKA流程
- 胡鑫鑫, 刘彩霞, 刘树新,等. 移动通信网鉴权认证综述[J]. 网络与信息安全学报, 2018, 4(12):15.

THANK YOU !