北邮信息理论
与技术教研中心

BUPT Information Theory & Technology Center

第十九章
移动信息安全

主讲人: 牛 凯

niukai@bupt.edu.cn

本章内容

- 信息安全涉及内容很广，本章仅讨论移动通信中信息安全的两个核心问题：鉴权(也称认证)与加密，而且主要以空中接口即接入过程介绍为主。
- 本章共分六节：第一节为概述，第二节为保密学的基本原理，第三节讨论GSM中的鉴权与加密，第四节叙述IS-95中的鉴权与加密，第五节简介WCDMA与cdma2000中的鉴权与加密，第六节概述LTE、WiMax、5G系统中的鉴权与加密，最后总结移动通信中的信息安全方法。

§ 19.1 概述

- 随着移动通信的迅速普及和业务类型的与日俱增，特别是电子商务、电子贸易等数据业务的需求，使移动通信中的信息安全地位日益显著。

19.1.1移动通信中的安全需求

- 在上世纪八九十年代，模拟手机盗号问题给电信部门和用户带来巨大的经济损失，并增加了运营商与用户之间不必要的矛盾。
- 移动通信体制的数字化，为通信的安全保密，特别是鉴权与加密提供了理论与技术基础。
- 数据业务与多媒体业务的开展进一步促进了移动安全保密技术的发展。
- 移动台与手持设备的认证也推动了移动安全技术的发展。

19.1.2移动环境中的安全威胁及相应措施

- 目前，移动通信最有代表性的是第三代移动通信系统(3G) 安全体系结构如下

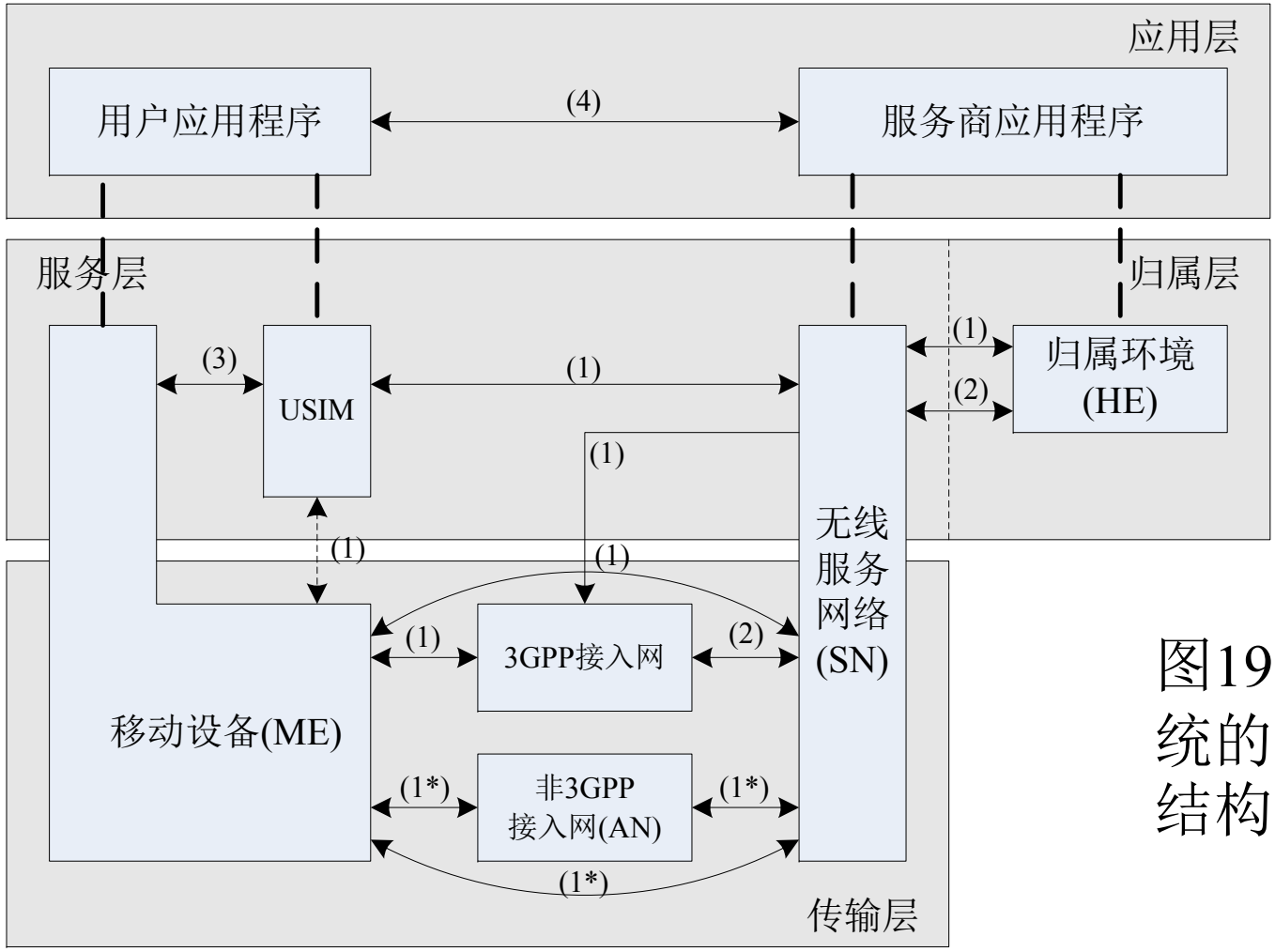


图19.1 3GPP系统的安全体系结构

19.1.2移动环境中的安全威胁及相应措施

- (1) 网络接入安全(等级1)：主要定义用户接入3GPP网络的安全特性，特别强调防止无线接入链路所受到的安全攻击，这个等级的安全机制包括USIM卡、移动设备(ME)、3GPP无线接入网(UTRAN/E-UTRAN)以及3GPP核心网(CN/EPC)之间的安全通信。
- (1*)非3GPP网络接入安全：主要定义ME、非3GPP接入网(例如WiMax、cdma2000与WLAN)与3GPP核心网(EPC)之间的安全通信。
- (2) 网络域安全(等级2)：定义3GPP接入网、无线服务网(SN)和归属环境(HE)之间传输信令和数据的安全特性，并对攻击有线网络进行保护。

19.1.2移动环境中的安全威胁及相应措施

- (3) 用户域的安全(等级3)：定义USIM与ME之间的安全特性，包括两者之间的相互认证。
- (4) 应用程序域安全(等级4)：定义用户应用程序与业务支撑平台之间交换数据的安全性，例如对于VoIP业务，IMS提供了该等级的安全框架。
- (5) 安全的可见度与可配置性：它定义了用户能够得知操作中是否安全，以及是否根据安全特性使用业务。

19.1.2移动环境中的安全威胁及相应措施

- 以空中接口为主体的安全威胁包括如下几类情况：
  - 窃听
  - 假冒
  - 重放
  - 数据完整性侵犯
  - 业务流分析
  - 跟踪
- 来自网络和数据库的安全威胁包括以下三类情况：
  - 网络内部攻击
  - 对数据库的非法访问
  - 对业务的否认

§19.2 保密学的基本原理

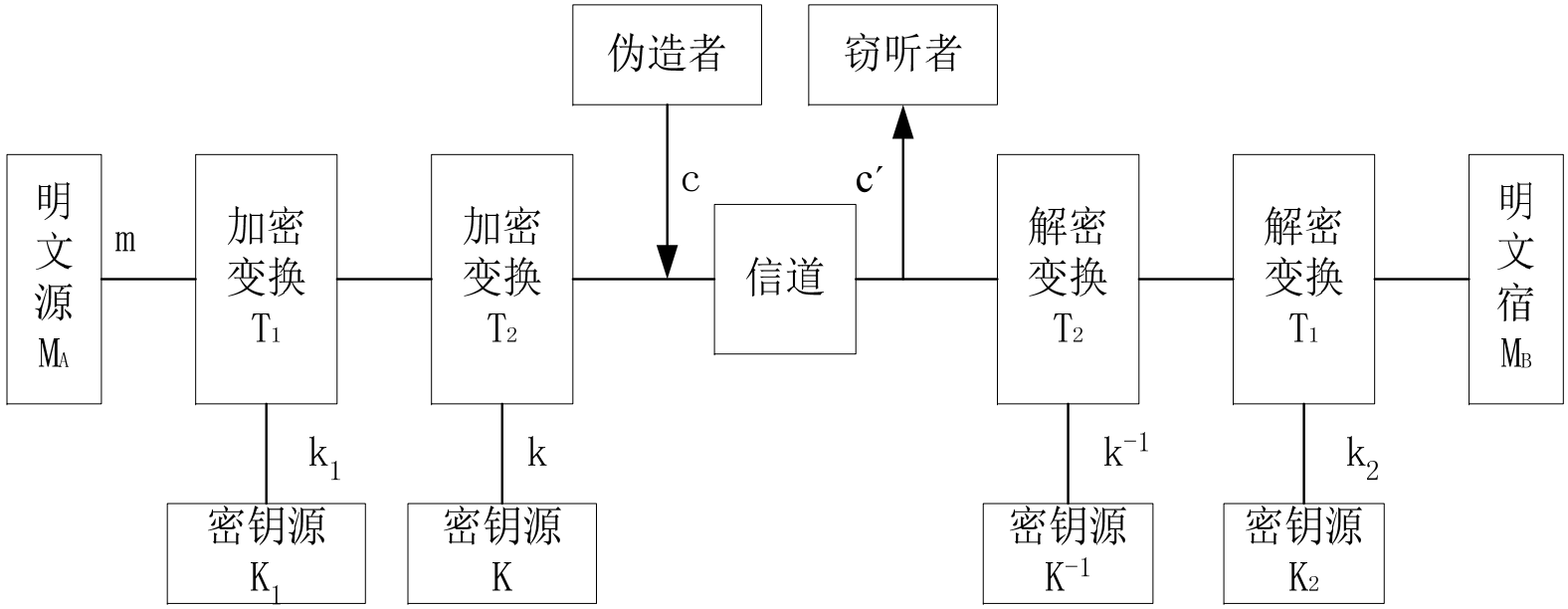
• 19.2.1引言

- 上世纪40年代以前它基本上是一门经验性、技术性学科。
- 四十年代末，C. E. Shannon发表了保密学的奠基性论文《保密系统的信息理论》[19.4]，从而创立统计保密学理论。
- 1976年，美国学者W. Differ与M. Hellman发表《保密学的新方向》[19.1]，首先提出双钥制与公开密钥理论，为现代密码学奠定了基础，从而为广义密码学、认证理论、数字签名等现代密码学及其在现代信息网中的应用开辟了新的方向。

19.2.2广义保密系统的物理、数学模型

- 保密系统是以信息系统的安全性为目的的专用通信系统。信息安全是针对通信系统中授权的合理用户而言，而未授权的非法用户既可以在接收端窃听，也可以在发送端主动攻击、非法伪造。
- 传统的保密学仅研究前者即非法窃听，又称为狭义保密学，而两者均研究的则称为广义保密学。

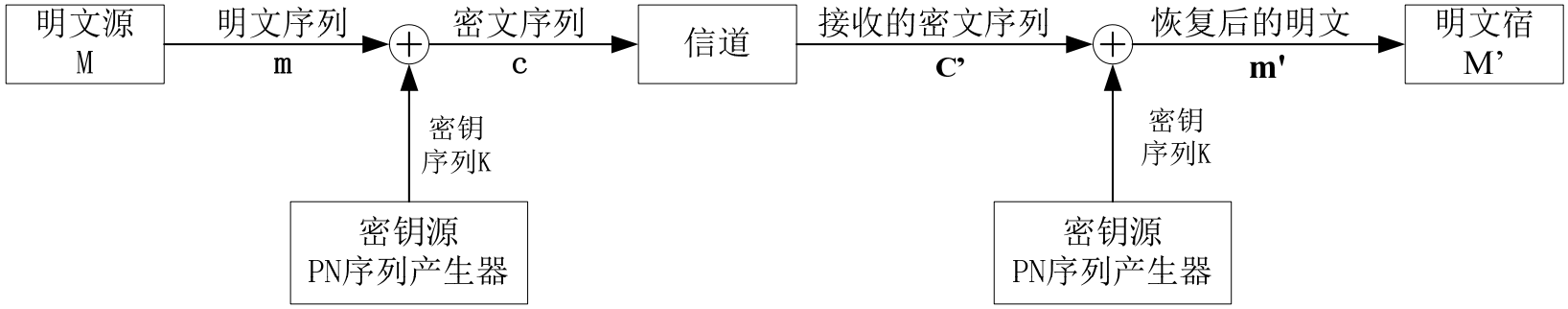
19.2.2广义保密系统的物理、数学模型



- 上图为一个典型广义保密通信系统。
- 一个广义保密系统 $S=\{M_A,K,C,(T_K,T_{K^{-1}}),(T_{K_1},T_{K_2})\}$ 。若上述系统中仅有 $(T_K,T_{K^{-1}})$，且 $T_K\cdot T_{K^{-1}}=1$，该保密系统退化为传统的狭义保密系统。
- 保密系统的核心是密钥和加、解密变换的实现算法。

19.2.3序列密码

- 序列加密又称为流加密，属于串行逐位加密，即通过明文序列与密钥序列逐位模二加来生成对应的密文序列。
- 序列密码实质上是仿效理想保密体制中的“一次一密”体制，从而牺牲了部分的理想性能，而换取了易于产生、易于同步的优点，且密钥的管理、分配具有工程可实现性。
- 序列密码的原理如下图所示：



19.2.3序列密码

- **1.m序列非线性前馈加密算法**
- 序列密码要求密钥具有较大的线性复杂度，并且除了在整体上具有伪随机特性以外，还必须进一步具有抗统计攻击的局部随机性。
- m序列虽然能完全满足Golomb随机性公设，但是它的线性复杂度很低，因此不能直接用作序列密钥。
- 为了改善m序列的线性复杂度，最简单的方法是在m序列产生器上附加一个非线性前馈滤波器。选取非线性前馈函数的标准是既保留m序列的伪随机特性与优点，又要设法提高线性复杂度。

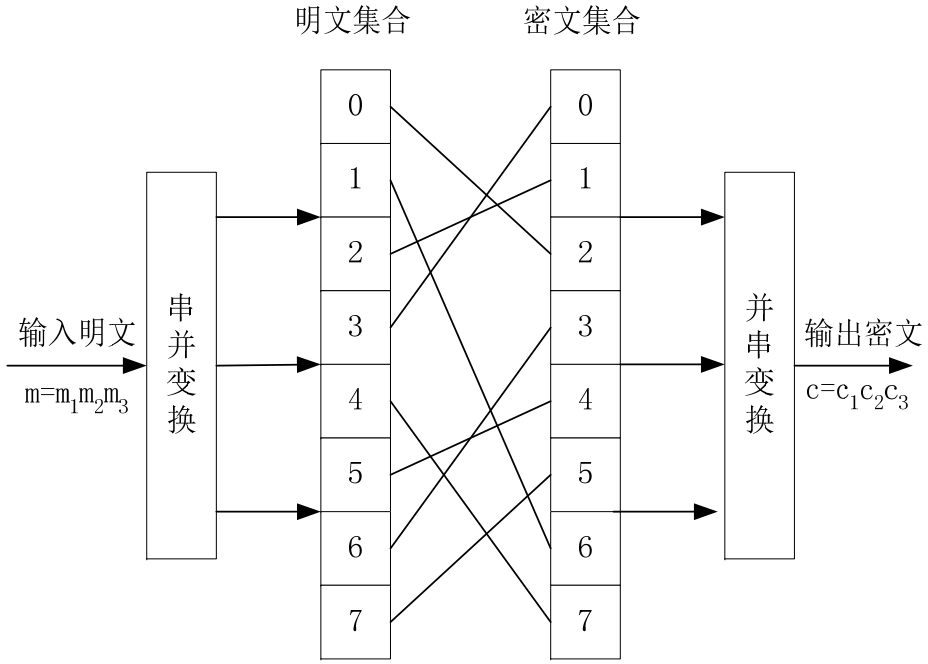
19.2.3序列密码

- **2. RC算法**
- RC系列算法是密钥长度可变的序列加密算法，其中最流行的是RC4算法，可以使用高达2048位的密钥，该算法的速度可以达到DES加密的10倍左右。RC4算法的原理是“搅乱”，包括初始化模块和伪随机子密码生成模块两大部分。
- 初始化过程将一个256字节的数列进行随机搅乱，经过伪随机子密码生成模块处理后得到不同的子密钥序列，子密钥序列和明文进行异或运算(XOR)后，得到密文。
- 由于RC4算法加密采用的是异或，所以，一旦子密钥序列出现了重复，密文就有可能被破解。但是目前还没有发现密钥长度达到128位的RC4有重复的可能性，所以，RC4是目前最安全的加密算法之一。

19.2.4分组密码

- 分组密码是对明文信息进行分组加解密，由于处理需要一定时延，因此适合于非实时加密。本节重点介绍分组加密基本原理与分组加密标准DES。

- 下面举一个最简单的例子，令分组长度n＝3，明文与密文各有8种不同组合，明文m与密文c以及密钥k(联线)的对应关系可以直观表示如右图所示。



19.2.4分组密码

- 加密、解密方程与逻辑真值表如右：

输入				输出			
m	M_1	m_2	m_3	c_1	c_2	c_3	c
0	0	0	0	0	1	0	2
1	0	0	1	1	1	0	6
2	0	1	0	0	0	1	1
3	0	1	1	0	0	0	0
4	1	0	0	1	1	1	7
5	1	0	1	1	0	0	4
6	1	1	0	0	1	1	3
7	1	1	1	1	0	1	5

- 加密方程为：

$$\left.\begin{aligned} c_1 &= f_{k_1}(m_1m_2m_3) = \overline{m_1}\,\overline{m_2}m_3 \cup m_1\overline{m_2}\,\overline{m_3} \cup m_1\overline{m_2}m_3 \cup m_1m_2m_3 \\ c_2 &= f_{k_2}(m_1m_2m_3) = \overline{m_1}\,\overline{m_2}\,\overline{m_3} \cup \overline{m_1}\,\overline{m_2}m_3 \cup m_1\overline{m_2}\,\overline{m_3} \cup m_1m_2\overline{m_3} \\ c_3 &= f_{k_3}(m_1m_2m_3) = \overline{m_1}m_2\overline{m_3} \cup m_1\overline{m_2}\,\overline{m_3} \cup m_1m_2\overline{m_3} \cup m_1m_2m_3 \end{aligned}\right\}$$

- 解密方程为：

$$\left.\begin{aligned} m_1 &= g_{k_1}(c_1c_2c_3) = c_1c_2c_3 \cup c_1\overline{c_2}\,\overline{c_3} \cup \overline{c_1}c_2c_3 \cup c_1\overline{c_2}c_3 \\ m_1 &= g_{k_1}(c_1c_2c_3) = \overline{c_1}\,\overline{c_2}c_3 \cup \overline{c_1}c_2\overline{c_3} \cup \overline{c_1}c_2c_3 \cup c_1\overline{c_2}c_3 \\ m_1 &= g_{k_1}(c_1c_2c_3) = c_1c_2\overline{c_3} \cup \overline{c_1}c_2\overline{c_3} \cup c_1\overline{c_2}\,\overline{c_3} \cup c_1\overline{c_2}c_3 \end{aligned}\right\}$$

19.2.4分组密码

- 将上述加、解密方程写成矩阵形式$\mathbf{C} = \mathbf{K} \cdot \mathbf{M}$
- 即：

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

- 同理有：$\mathbf{M} = \mathbf{K}^{-1} \cdot \mathbf{C}$
- 即：

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

19.2.4分组密码

1. DES算法

DES是由IBM研制，并由美国国家安全局NSA认证安全。目前该标准已被广泛应用于全世界的数据加密中。DES可以构成分组(块)加密和序列(流)加密两种不同形式，但主要用于分组(块)加密，两者的唯一差别是密钥不同。

DES算法把64位明文输入块变为64位密文输出块，它所使用密钥也是64位(56位密钥加8比特校验)。DES是一种Feistel结构的加密算法，即每次迭代分为左右两半，进行交叉加密操作。

Horst Feistel(1915-1990)是德国物理学家和密码学家，在IBM工作期间提出了以其名字命名的加密技术，是DES标准的发明人之一。

19.2.4分组密码

- DES算法安全性很高，到目前为止，除了用穷举搜索法对DES算法进行攻击外，还没有发现更有效的办法。
- TripleDES算法又称3-DES，是DES算法改进，使用两个密钥对明文运行 DES算法三次，得到 112 位有效密钥，主要用于解决DES56位密钥的抵抗破解强度随着计算机运算速度加快而日益减弱的问题。

19.2.4分组密码

- **2. Kasumi算法**
- Kasumi算法也是一种Feistel结构的分组密码，数据长度64比特，密钥长度128比特，经过8次迭代得到密文输出。
- Kasumi算法设计的关键与DES相同，也在于选择压缩S运算，这些映射专门针对差分与线性密码分析进行了优化，因此具有很高的非线性度。
- Kasumi算法的运算非常简单，可以在任意软硬件设备实现，既可以应用于分组加密，也可以应用于序列加密。
- Kasumi算法已经应用于GSM A5/3、GPRS GAE3加密算法，以及3GPP的加密(f8)和完整性保护(f9)算法中。

19.2.4分组密码

- **3. AES算法**
- 为了应对计算机技术特别是互联网计算能力的快速增长导致的密码分析能力的迅猛发展，2000年底，美国国家标准技术局NIST决定采用新的高级加密标准AES逐步替代DES。AES的设计基于替代重排结构，不采用Feistel结构。
- AES的数据长度为128比特，密钥长度128、192或256比特，核心运算都基于Rijndael算法。

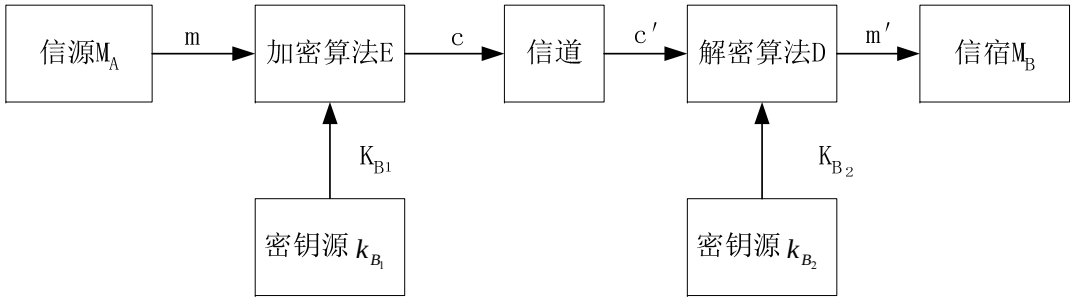
19.2.5公开密钥密码

- 公开密钥打破了传统的单钥制对密码学的垄断，奠定了双钥制公开密钥的新思路，为现代密码学的发展奠定了基础。本节介绍公开密钥基本原理和RSA算法。

19.2.5公开密钥密码

1. 公开密钥的基本原理

- 公开密钥采用发收不对称的两个密钥，且将发端加密密钥公开，而仅把解密密钥作为保密的私钥。
- 公开密钥的双钥制物理与数学模型如下所示：



- 在上面公开密钥通信系统中，每个用户都有一对加、解密密钥 (K_{B_1}, K_{B_2})，比如用户B的加解密密钥为(K_{B_1}, K_{B_2})，其中K_{B_1}是加密密钥是公开的，可查找的，称为公钥，而 K_{B_2}是解密密钥是秘密的，它仅为用户B私有，称为私钥。

19.2.5公开密钥密码

- 任何一个其它用户比如用户A若想要与用户B进行保密通信，可以首先查找到用户B的公钥K_{B_1}进行下列加密运算：$C = E_{K_{B_1}}(m)$。
- 在接收端，仅有合法用户B掌握属于自己的私钥，因此可以进行正常解密运算，并恢复原来明文m：

$$m' = D_{K_{B_2}}[c'] = D_{K_{B_2}}[c] = D_{K_{B_2}} E_{K_{B1}}(m) = m$$

- 对于其它非法用户，虽然也能窃获密文c'，但是由于不掌握B用户私钥，故无法解密。在公开密钥系统中，加密与解密的密钥是两个分别为公钥K_1和私钥K_2，且$K_1 \neq K_2$是非对称的，因此又称为非对称密钥体制。

19.2.5公开密钥密码

- 对每个单程保密信道有一对加解密变换：$(T_{K_1}, T_{K_2}) = (E_{K_1}, D_{K_2})$ 其中加密密钥和加密变换(算法)是公开的、可查找的，而解密密钥与解密变换(算法)是秘密的，必须存在有效地产生 E_{K_1} 与 D_{K_2} 的简单可行方法，来实现公开密钥体制。
- 为了满足上述要求，公开密钥提出者建议采用一类单向陷门函数作为加、解密变换的算法。
- 若函数 $y = f(x)$ 为单向函数，则它应满足：对每个 $x \in X$，计算 $y = f(x)$ 很容易实现；而若由y计算x是极其困难的(NP问题)。若函数f进一步满足存在某个陷门函数k，当k未知时，为单向函数，但是若k已知时，则从 $y = f(x)$ 中已知y求解x是可以办得到的(P类问题)。
- 目前已找到的单向陷门函数有：RSA体制、背包体制、McEliece体制、二次剩余等等。

19.2.5公开密钥密码

2. RSA体制

- RSA是美国麻省理工MIT三位教授Rivest、Shamir和Adleman于1978年提出，后人以他们三人字头RSA命名，它是迄今为止最为成功的公开密钥体制。

- RSA体制是建立在数论和计算复杂度的基础上，采用离散指数的同余运算来构造加、解密算法。加密时：将明文m自乘e次幂，除以模数n，余数则构成密文c。即：$c = m^e \bmod n$。解密时：将密文c自乘d次幂，再除以模数n，其余数为待解的明文m。即：$m = c^d \bmod n$。

19.2.5公开密钥密码

- RSA具体算法步骤为：每个用户选取两个大素数p_1和p_2，计算其积$n = p_1 \cdot p_2$和欧拉函数$\phi(n) = (p_1 - 1)(p_2 - 1)$，并选择一个任意整数e，使它满足$(e, \phi(n)) = 1$，即e与$\phi(n)$互素，且$1 < e < \phi(n)$。一般选 p_1、p_2 为不小于40位的十进制数。
- 按加密方程(算法)构成密文c并送出：$c = E_{K_1}(m) = m^e \bmod n$。由下列同余方程求出解密指数幂次d：$e \cdot d \equiv 1 \bmod \phi(n)$ 。且$1 < d < \phi(n)$，只要用欧几里德算法进行$2\log\phi(n)$次运算即可求出d值。
- 按下列解密方程求解明文m：

$$m = D_{K_2}(c) = D_{K_2}\left[E_{K_1}(m)\right] = c^d \bmod n = (m^e)^d \bmod n = m \bmod n$$

19.2.5公开密钥密码

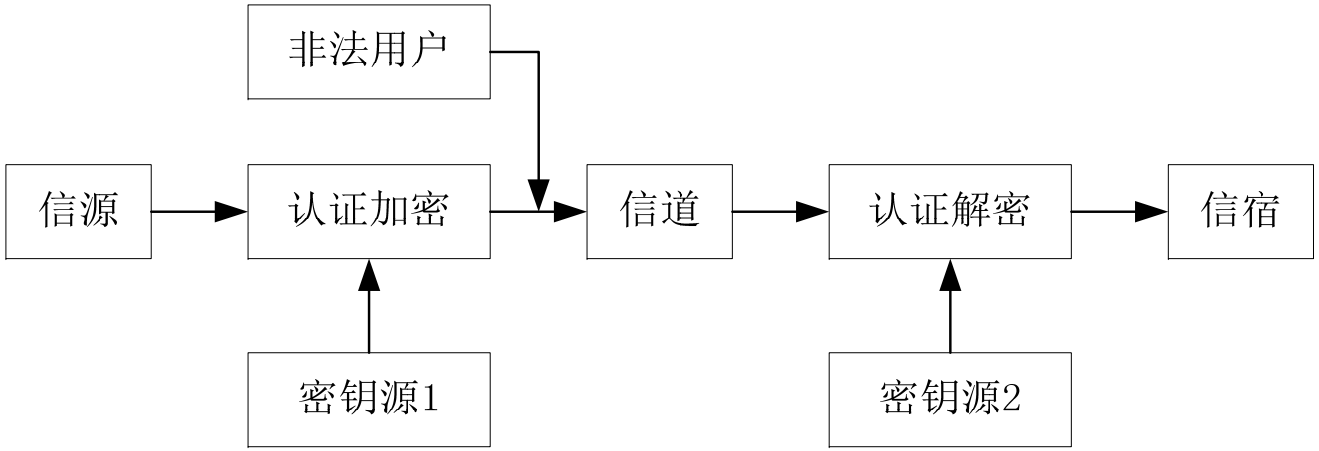
- 下面举一简单例子说明RSA体制。
- 设 $p_1=17$，$p_2=31$，明文m=2，则 $n=p_1\times p_2=17\times 31=527$ 有 $\phi(n)=(p_1-1)(p_2-1)=16\times 30=480$，选加密指数幂指数e=7，再选解密指数幂指数满足 ，且 $e\bullet d=1 \bmod \phi(n)$，则 $1<d<\phi(n)$，或 。因此求解出d=343，按加密方程求密文 ，按解密方程可以求得明文：

$$c=m^e \bmod n=2^7 \bmod 527=128$$

$$m=c^d \bmod n=128^{343} \bmod 527=128^{256}\cdot 128^{64}\cdot 128^{16}\cdot 128^{4}\cdot 128^{2}\cdot 128 \bmod 527$$
$$=35\times 256\times 35\times 101\times 47\times 128 \bmod 527=2 \bmod 527$$

19.2.6认证系统

- 信息服务中还存在另一类信息安全问题，即来自发送端非法用户的主动攻击，包含非法用户的伪造篡改、删除、重放，甚至是来自合法用户的抵赖与篡改等。这类来自发送端的非法攻击的防范措施通称为认证技术，在移动通信中称为鉴权技术。
- 认证系统的基本原理如下图所示：



19.2.6认证系统

1. 消息认证

- 一个消息认证系统是由明文M、密钥K、密文C和认证函数 $f(m,k)$ 以及认证码集合 $A(m,k)$ 组成的。

- 2G、3G和4G移动通信系统中对合法用户的鉴权都属于身份认证。GSM系统中用户识别码IMSI存储在SIM卡与AuC中；IS-95系统中用户序列号ESN存储在移动台或UIM卡与AC中；UMTS/cdma2000系统中，用户识别码IMSI存储在USIM卡与AuC中。

19.2.6认证系统

2. 数据完整性保护

在3G以后的移动通信系统中，为了防止数据传输的中间截获攻击，数据完整性保护得到了更多重视。在发送端，使用加密算法对发送数据进行计算，得到一小段附加消息。

这一小段数据与发送数据每一位都相关。然后将其与原数据一起通过信道发送。在接收端，根据接收到的数据重新计算附加消息，并与接收到的附加消息比较，用它可判断原数据的内容是否被改变，出处是否真实。单向杂凑Hash函数，是一种用于数据完整性保护的典型技术，下面简要介绍其原理。

Hash函数是一类单向函数，也可称作消息摘要(Message Digest)函数，主要用于鉴权认证和数字签名。它以长度可变的消息M为输入并将其变换成长度固定的消息摘要函数H(M)作为输出，且一般，例如H(M)可以是16、64或128比特，而M则为兆字节或更长。

19.2.6认证系统

Hash函数具有下列主要性质：(1)H(M)适用于任何变长输入消息的数据块；(2)H(M)本身是定长输出；(3)H(M)应按用户特殊保密要求对给定的M进行计算。

根据指定消息摘要H(M)求得消息M至少在计算上是极其困难的。对于任意给定的消息M要找到另一个消息，使在计算上也是不可行的，换言之，要找到映射到同一个消息摘要的两个不同的M与在计算上是不可行的，满足这一性质的Hash函数称为抗碰撞的Hash函数。

反之，如果找到一对消息，具有相同的摘要，则称为产生一次碰撞。一般的，碰撞分为“强无碰撞”和“弱无碰撞”。强无碰撞无法产生有实际意义的原文，也就无法篡改和伪造出有意义的明文。而弱无碰撞则指根据消息摘要可以构造另一个有实际意义的原文，从而可以篡改和伪造数据。

19.2.6认证系统

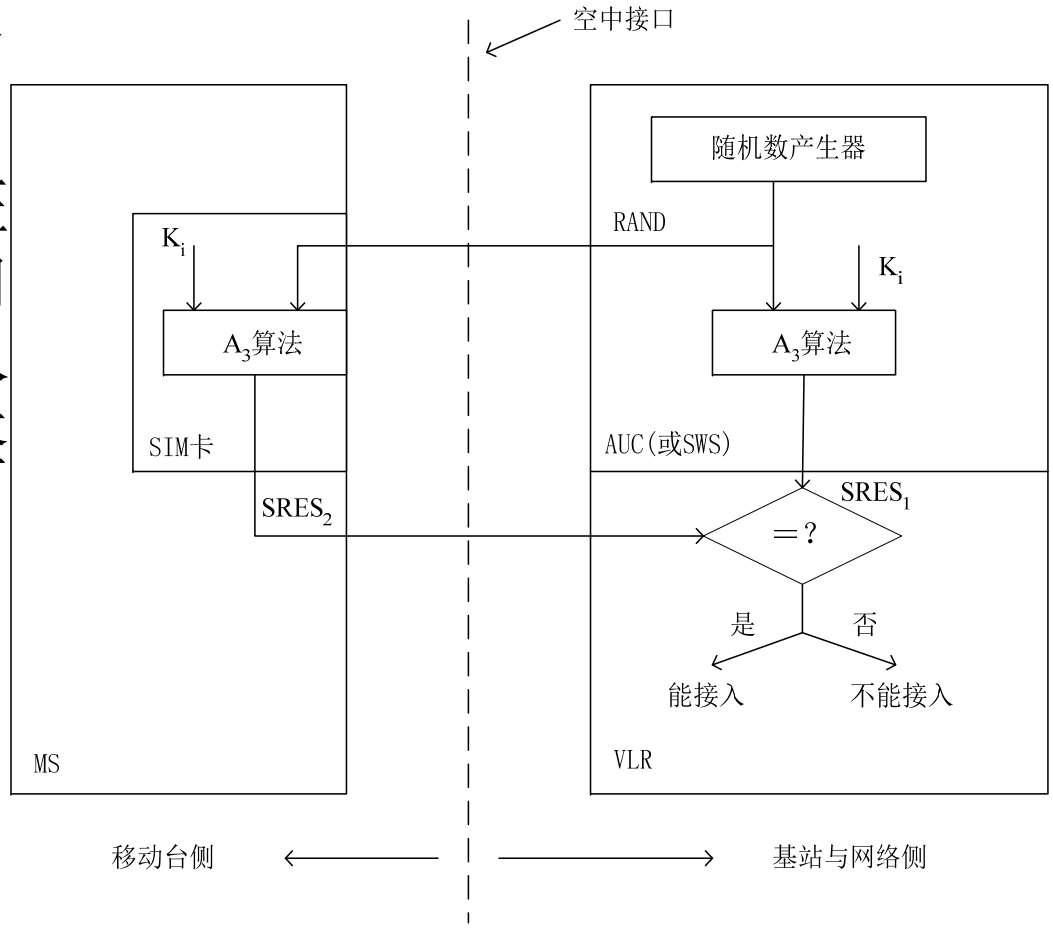
- 值得指出的是，在Crypto’2004年会上，我国学者王小云等人成功找到MD4、MD5、HAVAL-128和RIPEMD等四种消息摘要算法的强无碰撞，后来又找到了SHA-1算法的强无碰撞，这是密码学界的一个重大突破。
- 尽管这些结果只具有理论意义，还不是弱无碰撞，但它表明现有的消息摘要算法都存在缺陷，我们需要重新审视这些算法的安全性。

§19.3 GSM系统的鉴权与加密

- 为了保障GSM系统的安全保密性能，在系统设计中采用了很多安全、保密措施，其中最主要的有以下四类：
  - 防止未授权的非法用户接入的鉴权(认证)技术
  - 防止空中接口非法用户窃听的加、解密技术
  - 防止非法用户窃取用户身份码和位置信息的临时移动用户身份码TMSI更新技术
  - 防止未经登记的非法用户接入和防止合法用户过期终端(手机)在网中继续使用的设备认证技术

19.3.1防止未授权非法用户接入鉴权(认证)技术

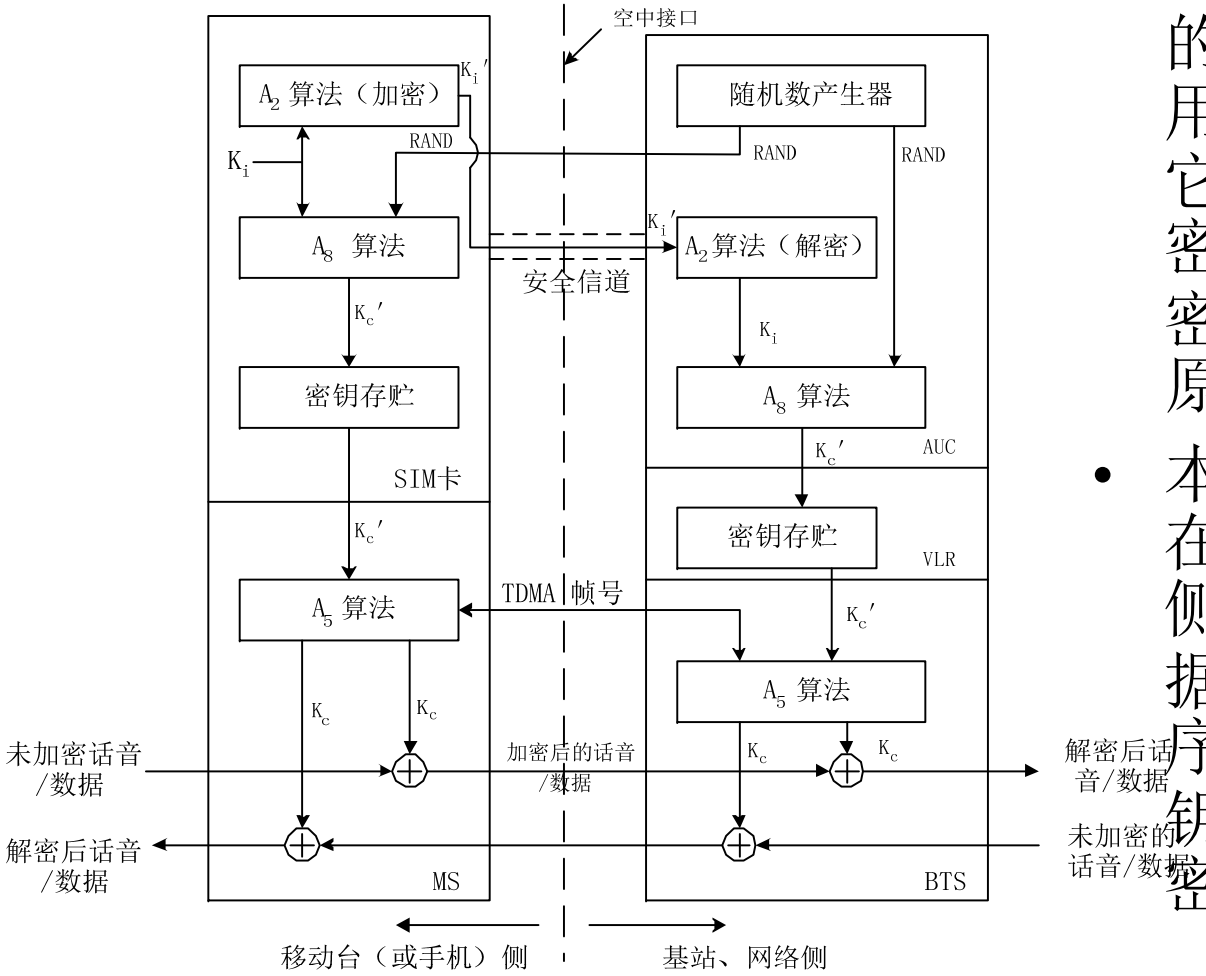
- 鉴权(认证)目的是防止未授权的非法用户接入GSM系统。其基本原理是利用认证技术在移动网端访问寄存器VLR时，对入网用户的身份进行鉴别。
- GSM系统中鉴权的原理图如右所示。



19.3.1防止未授权非法用户接入鉴权(认证)技术

- 本方案的核心思想是在移动台与网络两侧各产生一个供鉴权(认证)用鉴别响应符号SRES1和SRES2，然后送至网络侧VLR中进行鉴权(认证)比较，通过鉴权的用户是合理用户可以入网，通不过鉴权的用户则是非法(未授权)用户，不能入网。
- 在移动台的用户识别卡SIM中，分别给出一对IMSI和个人用户密码Ki。在SIM卡中利用个人密码Ki与从网络侧鉴权中心AUC和安全工作站SWS并经VLR传送至移动台SIM卡中的一组随机数RAND通过A3算法产生输出的鉴权响应符号SRES2。
- 在网络侧，也分为鉴权响应符号SRES1的产生与鉴权比较两部分。

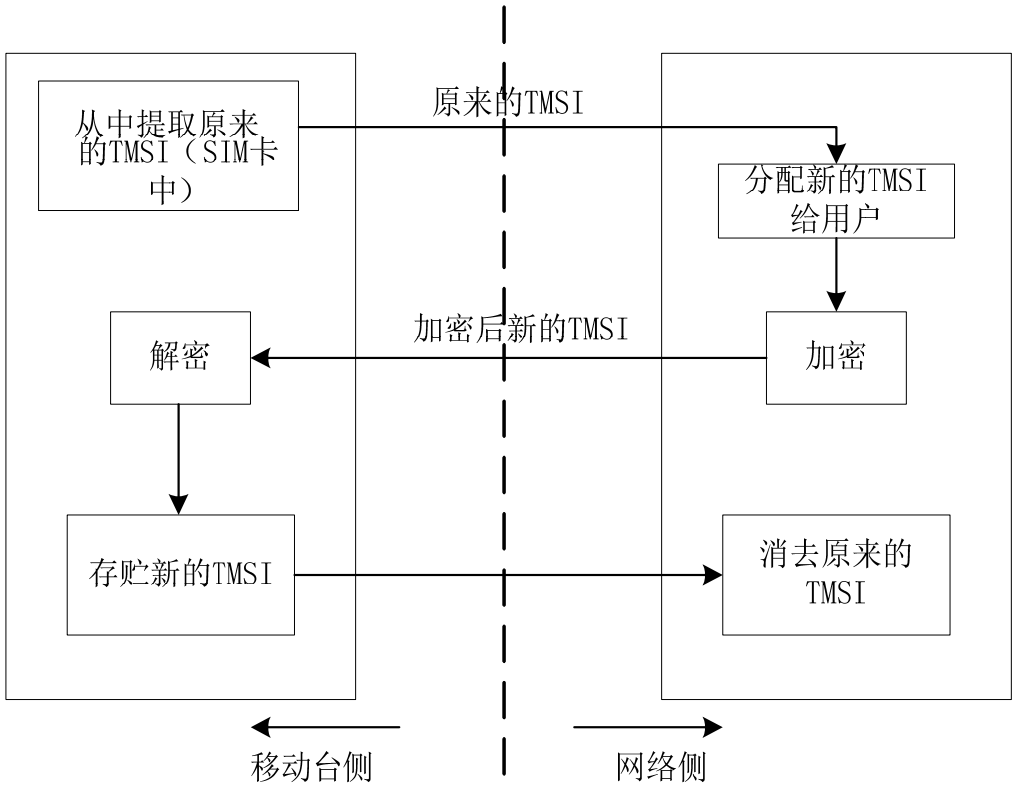
19.3.2 防止空中接口窃听的加解密技术



- 这种技术的加密目的是防止非法窃听用户的机密信息，它的基本原理遵循密码学中序列(流)加密原理。其加解密原理框图如左所示。
- 本方案基本思路是在移动台以及网络侧分别提供话音/数据业务加、解密用序列(流)加、解密密钥，以供用户加解密用。

19.3.3临时移动用户身份码TMSI更新技术

- 为了保证移动用户身份的隐私权，防止非法窃取用户身份码和相应的位置信息，可以采用不断更新临时移动用户身份码TMSI取代每个用户唯一的国际移动用户身份码IMSI。



- TMSI的具体更新过程原理如上图所示，由移动台侧与网络侧双方配合进行。

19.3.4 防止非法或过期设备接入的用户识别寄存器(EIR)

- 这项技术的目的是防止非法用户接入移动网，同时也防止已老化的过期手机接入移动网。
- 在网络端采用一个专门用于用户设备识别的寄存器EIR，它实质上是一个专用数据库。负责存储每个手机唯一的国际移动设备号码IMEI。
- 根据运营者的要求，MSC/VLR能够触发检查IMEI的操作。

19.3.5 GSM安全性能分析

- 尽管GSM系统成功引入了鉴权与加密技术，但随着GSM系统在全球大规模商用化，暴露出诸多安全缺陷，可以总结为六方面的技术漏洞。
- **1.SIM/MS接口翻录**
- SIM-ME之间的接口不受保护，因此当合法用户的SIM卡被插入仿真的非法移动设备中时，SIM卡和MS接口间的消息都可以被截获和翻录。
- **2.A3/A8算法破解**
- GSM系统中采用Comp128算法实现A3和A8。但Wagnner和Gold berg等人指出如果收集160000个RAND-SRES对，可以获取Ki。因此如果获取合法用户的SIM卡，大约只要花10个小时，就可以破解Comp128算法。

19.3.5 GSM安全性能分析

•3.A5算法漏洞

•Biryukov和Shamir[19.16]以及Wagner[19.17]等人发现了A5算法的分析方法。这种方法首先建立算法状态和密钥流对应的数据库，然后通过对截获数据的匹配搜索，即可以轻易获得Kc密码。文献指出，一定条件下，只要耗时2分钟，甚至2秒钟，就可以破解A5/1和A5/2算法。

•4.SIM卡攻击

•由于SIM只是一个简单集成电路，可以采用逆向工程方法，直接从卡中解析IMSI和Ki等安全数据。另外，IBM研究人员指出，采用分割攻击方法，也能够快速克隆SIM卡。这说明，SIM的物理安全性亟待加强。

19.3.5 GSM安全性能分析

- **19.网络伪装攻击**
- 更为严重的问题是GSM只提供了单向认证，即网络对用户的认证。因此可以采用伪装的网络单元，如伪基站对MS发起攻击，获取MS的IMSI、Ki与Kc。并且这种方法要比直接破解鉴权与加密算法更方便。
- **6.网络数据明文传输**
- 另一个严重问题是在GSM网络侧，所有用户数据与信令都是明文传输，因此如果在网络侧进行监听与截获，则能够比空中接口更容易获取所需信息。

§19.4 IS-95系统的鉴权与加密

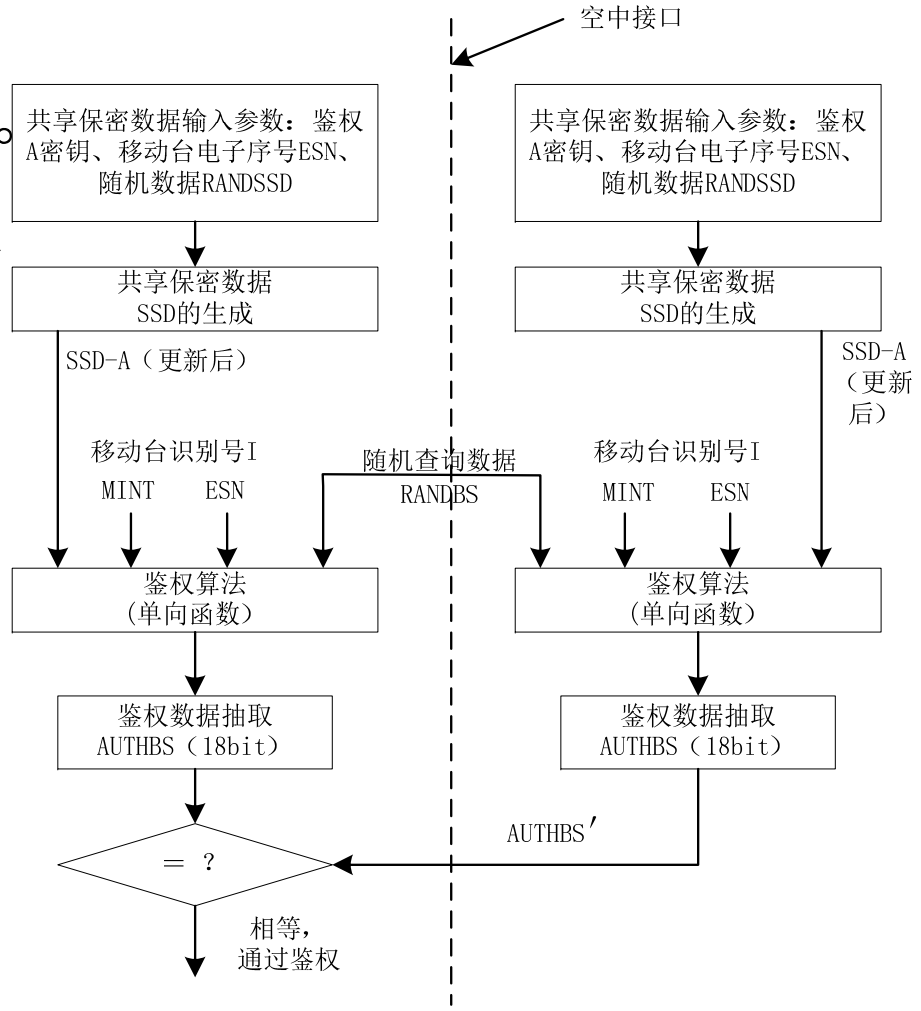
- IS-95中的信息安全主要包含鉴权(认证)与加密两个方面的问题，而且主要是针对数据用户，以确保用户的数据完整性和保密性。
- 鉴权(认证)技术的目的：确认移动台的合理身份、保证数据用户的完整性、防止错误数据的插入和防止正确数据被篡改。
- 加密技术的目的是防止非法用户从信道中窃取合法用户正在传送的机密信息，它包括：信令加密、话音加密、数据加密 。

19.4.1 鉴权认证技术

- 在IS-95标准中，定义了下列两个鉴权过程：全局查询鉴权和唯一查询鉴权。
- 鉴权基本原理是要在通信双方都产生一组鉴权认证参数，这组数据必须满足下列特性：
  - 通信双方、移动台与网络端均能独立产生这组鉴权认证数据
  - 必须具有被认证的移动台用户的特征信息
  - 具有很强的保密性能，不易被窃取，不易被复制
  - 具有更新的功能
  - 产生方法应具有通用性和可操作性，以保证认证双方和不同认证场合，产生规律的一致性

19.4.1 鉴权认证技术

- 满足上述五点特性的具体产生过程如右图所示。
- IS-95系统的鉴权认证过程涉及到以下几项关键技术：
  - ➢共享保密数据SSD的产生
  - ➢鉴权认证算法
  - ➢共享保密数据SSD的更新

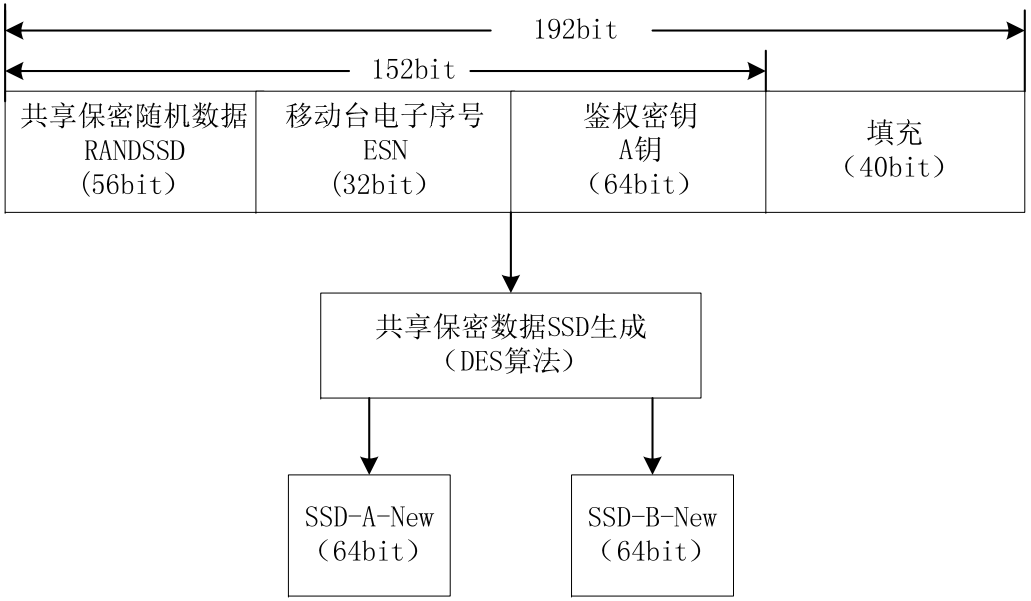


19.4.1 鉴权认证技术

1. SSD的产生

- SSD是存贮在移动台用户识别UIM卡中半永久性128bit的共享加密数据，其产生框图如下所示。

- SSD的输入参数组有三部分：共享保密的随机数据RANDSSD、移动台电子序号ESN、鉴权密钥(A钥)、填充。



- SSD输出两组数据：SSD-A-New是供鉴权用的共享加密数据；SSD-B-New是供加密用的共享加密数据。

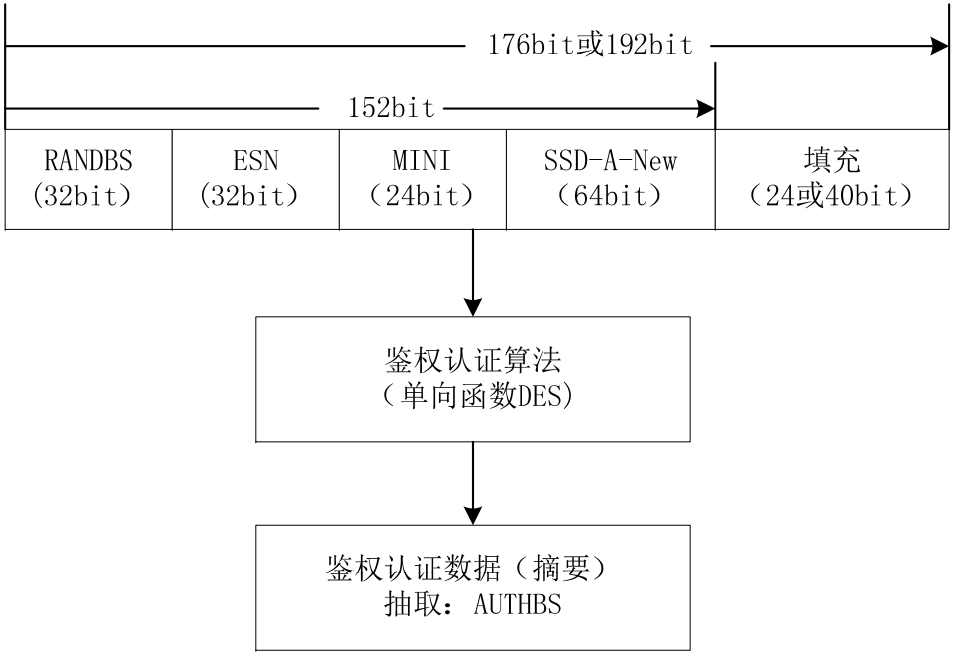
19.4.1 鉴权认证技术

2. 鉴权认证算法

- 这一部分是鉴权认证的核心，鉴权认证输入参数组含有5组参数：随机查询数据RANDBS；移动台电子序号ESN；移动台识别号第一部分；更新后的共享保密数据SSD-A-New；填充。
- 鉴权核心算法：包含以下两步：

➢利用单向Hash函数，产生鉴权所需的候选数据组

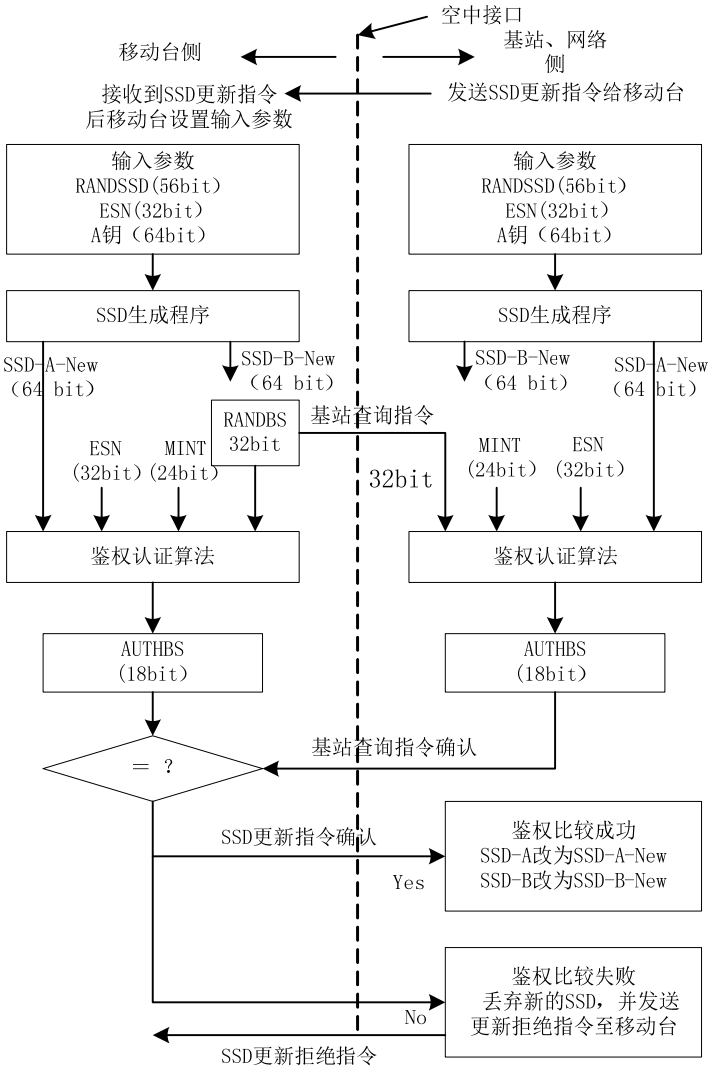
➢从鉴权认证的后选数据组中摘要抽取正式鉴权认证数据AUTHR，供鉴权认证比较用



19.4.1 鉴权认证技术

3. SSD的更新

- 为了使鉴权认证数据AUTHBS具有不断随用户变化的特性，要求共享保密数据应具有不断更新的功能。SSD更新框图如右图所示。



19.4.2 加密技术

- IS-95系统可以对下列不同业务类型进行加密：
  - 信令消息加密
  - 话音消息加密
  - 数据消息加密
- IS-95系统就业务而言，可以分为信令、话音与数据，但是就加密模式而言，则可分为两大类型：
  - 信源消息加密：其中外部加密方式和内部加密方式。
  - 信道输入信号加密

§19.5 3G系统的信息安全

- 本节主要简介WCDMA系统的鉴权与认证
- 3G安全体系目标为：
  - ➢确保用户信息不被窃听或盗用
  - ➢确保网络提供的资源信息不被滥用或盗用
  - ➢确保安全特征应充份标准化，且至少有一种加密算法是全球标准化
  - ➢安全特征的标准化，以确保全球范围内不同服务网之间的相互操作和漫游
  - ➢安全等级高于目前的移动网或固定网的安全等级(包括GSM)
  - ➢安全特征具有可扩展性

19.5.1 WCDMA系统的鉴权与加密

为了克服GSM系统的安全缺陷，WCDMA系统采用了双向认证技术，建立了完整的认证与密钥协商机制(AKA)。

1. UMTS安全体系结构与AKA过程

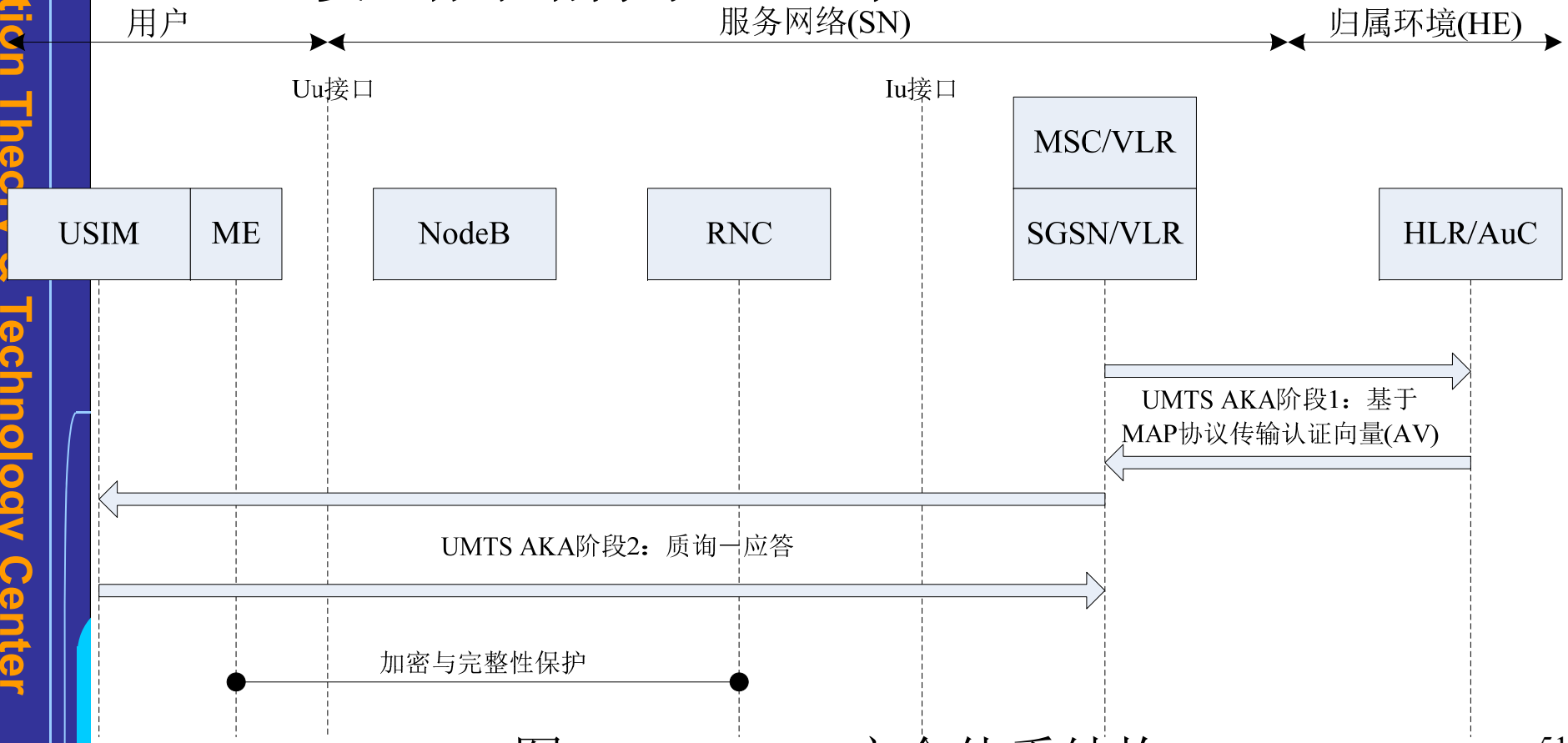


图19.16 UMTS安全体系结构

19.5.1 WCDMA系统的鉴权与加密

1. UMTS安全体系结构与AKA过程

- UMTS安全体系主要涉及到USIM、ME、RNC、MSC/SGSN/VLR、HLR/AuC等网络单元。所采用的AKA过程分为两个阶段。
- 阶段1是HE与SN之间的安全通信，认证向量AV通过SS7信令的MAP协议传输。
- 由于MAP协议本身没有安全功能，因此3GPP定义了扩展MAP安全协议，称为MAPsec，用于传输认证矢量AV=(RAND(随机数)，XRES(期望应答)，CK(加密密钥)，IK(完整性密钥)，AUTH(认证令牌))。

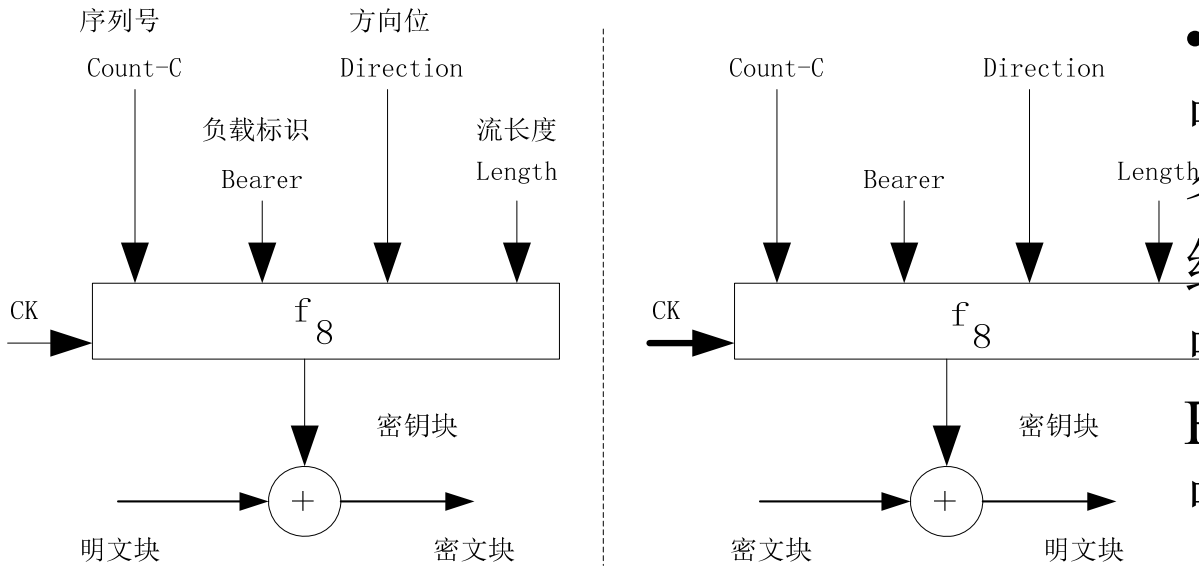
19.5.1 WCDMA系统的鉴权与加密

1. UMTS安全体系结构与AKA过程

- 阶段2是SN和用户之间的安全通信，采用一次处理方式，在USIM与SGSN/VLR之间进行质询-应答处理。
- 实现用户和网络的双向认证。UMTS在ME与RNC之间实现加密和完整性保护，对于业务数据和信令，都进行加密，为了降低处理时延，只对信令进行完整性保护。

- 为了满足不同制造商设备(手机、基站)之间的互连互通，必须要求3G空中接口安全算法标准化，目前定义的标准算法是Kasami算法，它同时适用于数据加密和接入链路数据完整性的f8与f9算法。

1. 数据加密算法

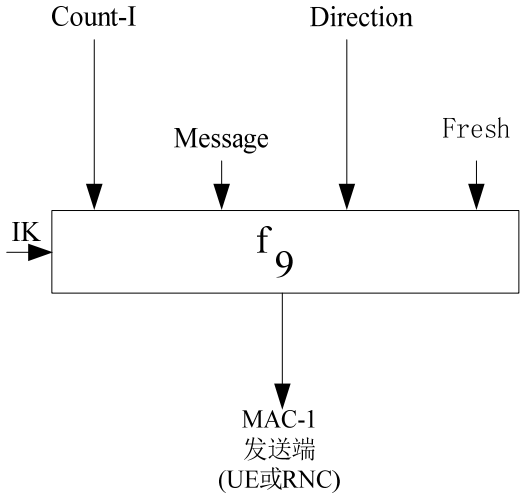


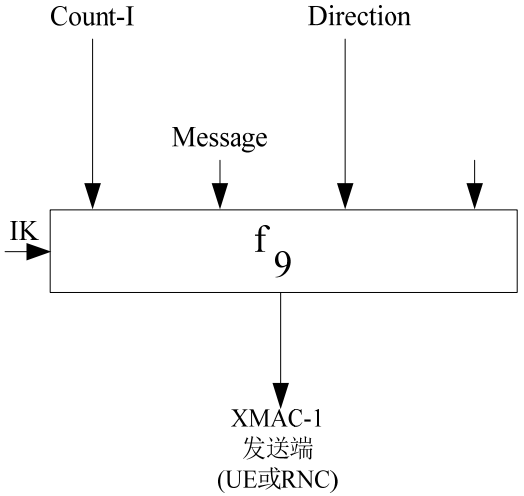
- f8算法在3G中用户终端设备UE与无线网络控制器RNC中链路层RLC/MAC层中实施。

- WCDMA系统数据加密原理如上所示。

2. 接入链路数据完整性保护

- f9算法为数据完整性保护算法，在UE与RNC之间实施，可以选用16种不同算法，应该采用标准化算法。



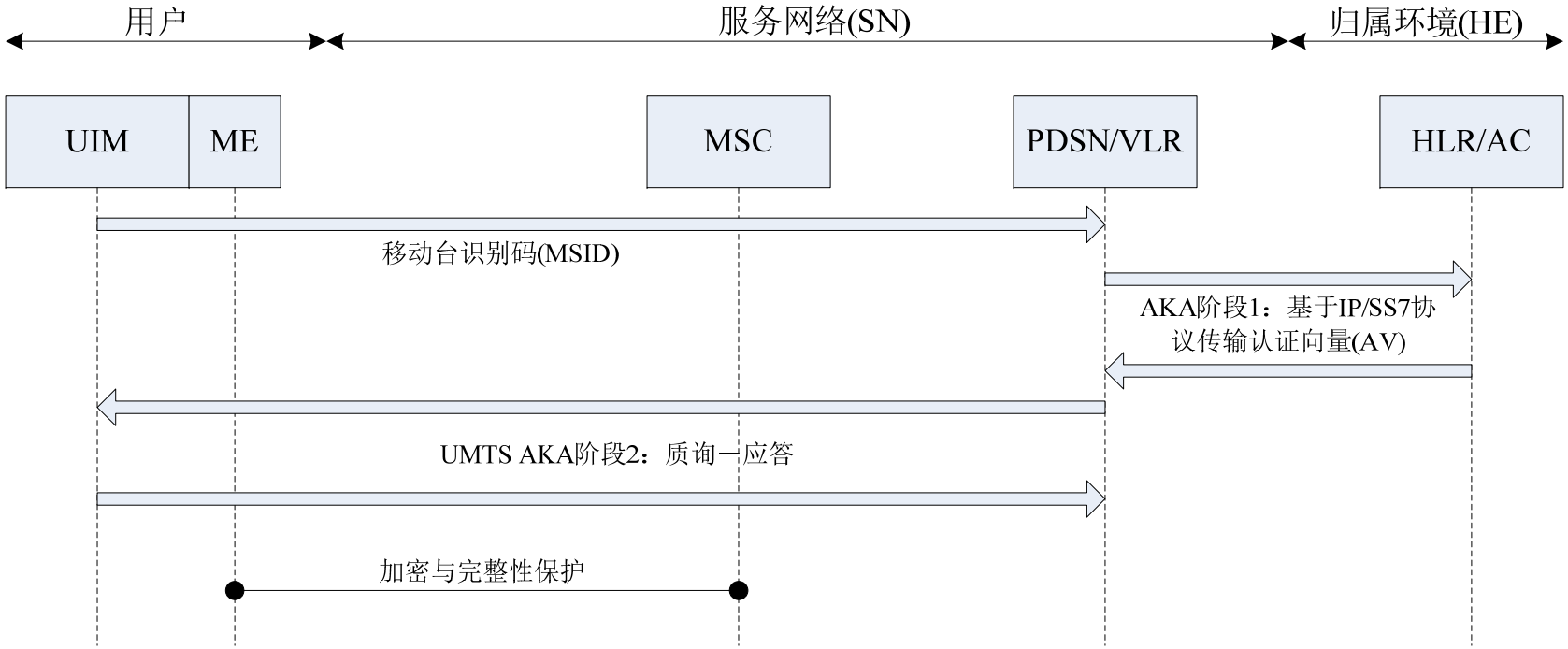


- WCDMA系统中消息认证码MAC-1或XMAC-1产生原理图如上所示。

- **4. UMTS安全性能总结**
- UMTS的接入安全机制要远好于GSM，质询—应答机制提供了用户与网络的双向认证，消除了伪基站的安全威胁。UMTS系统中采用的认证算法集合也比GSM系统中的A3/A8安全性能更好。
- UMTS中的加密算法性能远好于GSM中的A5算法。Kasumi算法自从提出以来，仍然被认为非常安全，预计能够有20年的安全期。并且随着技术的进展，可以将加密算法升级为更安全的版本。
- 数据完整性保护是UMTS新引入的安全技术，独立于加密保护，应用于不允许加密或者无法加密的场合，可以防止非法用户的中间截获与发端攻击。但由于运行速度的问题，UMTS系统中只针对信令进行完整性保护。

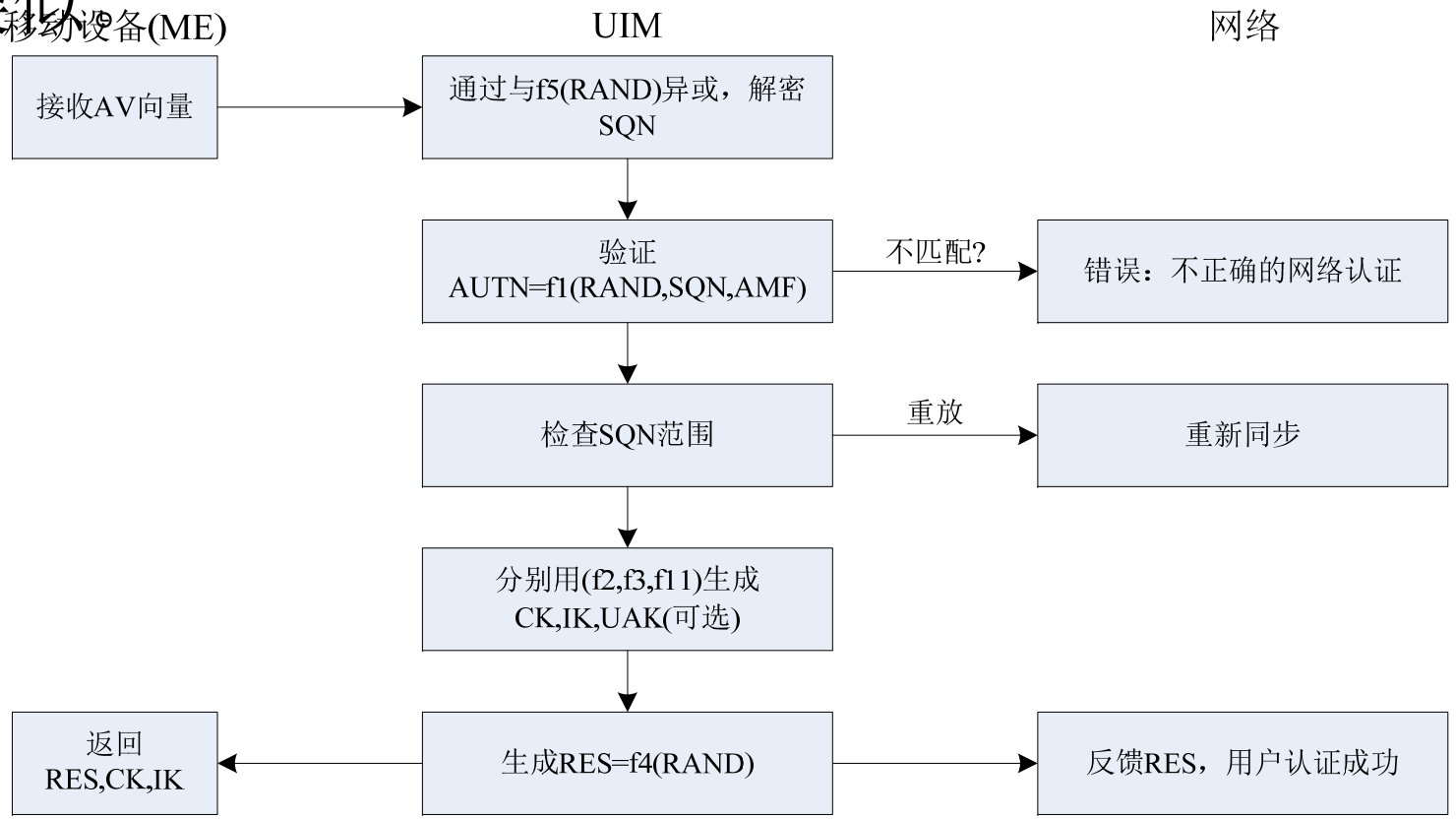
19.5.2 cdma2000系统的鉴权与加密

- 与WCDMA类似，cdma2000系统也采用了双向认证技术与认证与密钥协商机制(AKA)。
- **1. cdma2000安全体系结构**
- cdma2000的安全体系结构与UMTS类似，也采用两阶段AKA过程，涉及到UIM/ME、MSC、PDSN/VLR和HLR/AC等网络单元。



19.5.2 cdma2000系统的鉴权与加密

- **2. UIM认证流程**
- cdma2000中的UIM卡存储用户的身份信息与认证参数，其功能与GSM中的SIM卡、UMTS中的USIM卡功能类似



19.5.2 cdma2000系统的鉴权与加密

- **3. cdma2000与UMTS安全技术比较**
- cdma2000与UMTS具有类似的安全体系，都能够满足3G系统的安全目标，但由于两个系统的技术参数、系统架构与实现细节的差异，导致两者的安全技术有所不同。

§19.6 B3G与4G系统的信息安全

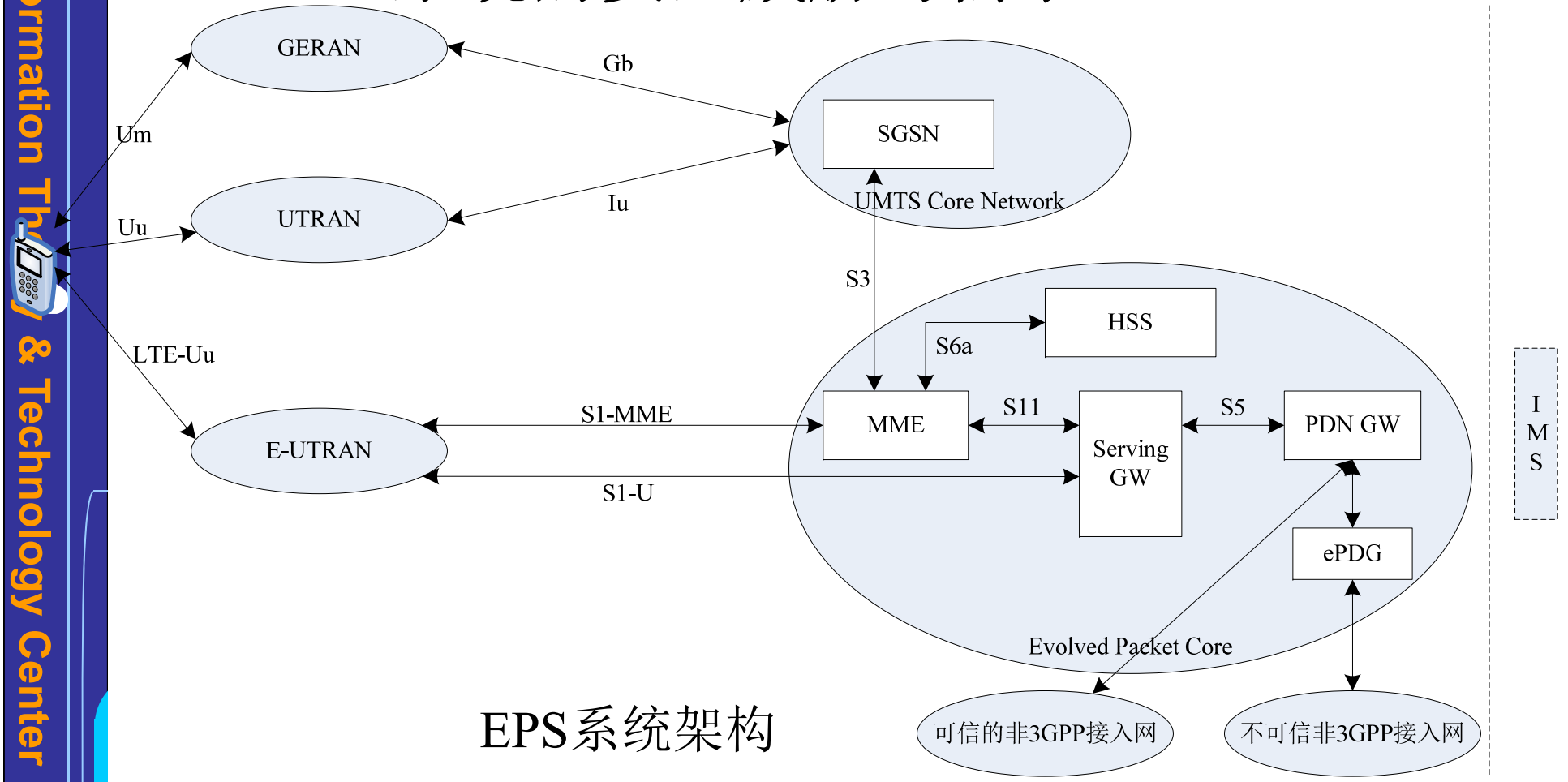
- 以LTE为代表的4G移动通信系统，继承了3G系统的安全体系设计理念，在结构完善和功能增强方面都有新的进展。本节重点介绍LTE系统的信息安全，并简要介绍WLAN系统的安全缺陷，以及WiMax的鉴权与加密。

19.6.1 LTE系统的信息安全

- 3GPP长期演进/系统架构演进(LTE/SAE)是面向4G的宽带移动通信体制，主要目标是为移动用户提供更高的带宽、更好的频谱效率、更安全的移动业务，通过更好融合其它无线接入网络，使用户享受完美的业务体验。
- GSM系统主要关注无线链路的安全特性，UMTS系统增强了无线接入安全，并开始关注网络功能的安全。
- 未来网络将基于全IP结构，尽管具备提供高效灵活业务的能力，但IP机制也意味着面临更多的安全威胁和隐患。因此演进分组系统(EPS)需要更加强健的安全体系，处理各种网络架构的差别，提高安全机制的健壮性。

19.6.1 LTE系统的信息安全

- 1. EPS系统的安全威胁与需求



EPS系统架构

19.6.1 LTE系统的信息安全

- **1. EPS系统的安全威胁与需求**
- 非法使用移动设备ME和用户的识别码接入网络；
- 根据用户设备(UE)的临时识别码、信令消息等跟踪用户；
- 非法使用安全过程中的密钥接入网络；
- 修改UE参数，使正常工作的手机永久或长期闭锁；
- 篡改E-UTRAN网络广播的系统信息；
- 监听和非法修改IP数据包内容；
- 通过重放攻击数据与信令的完整性。

19.6.1 LTE系统的信息安全

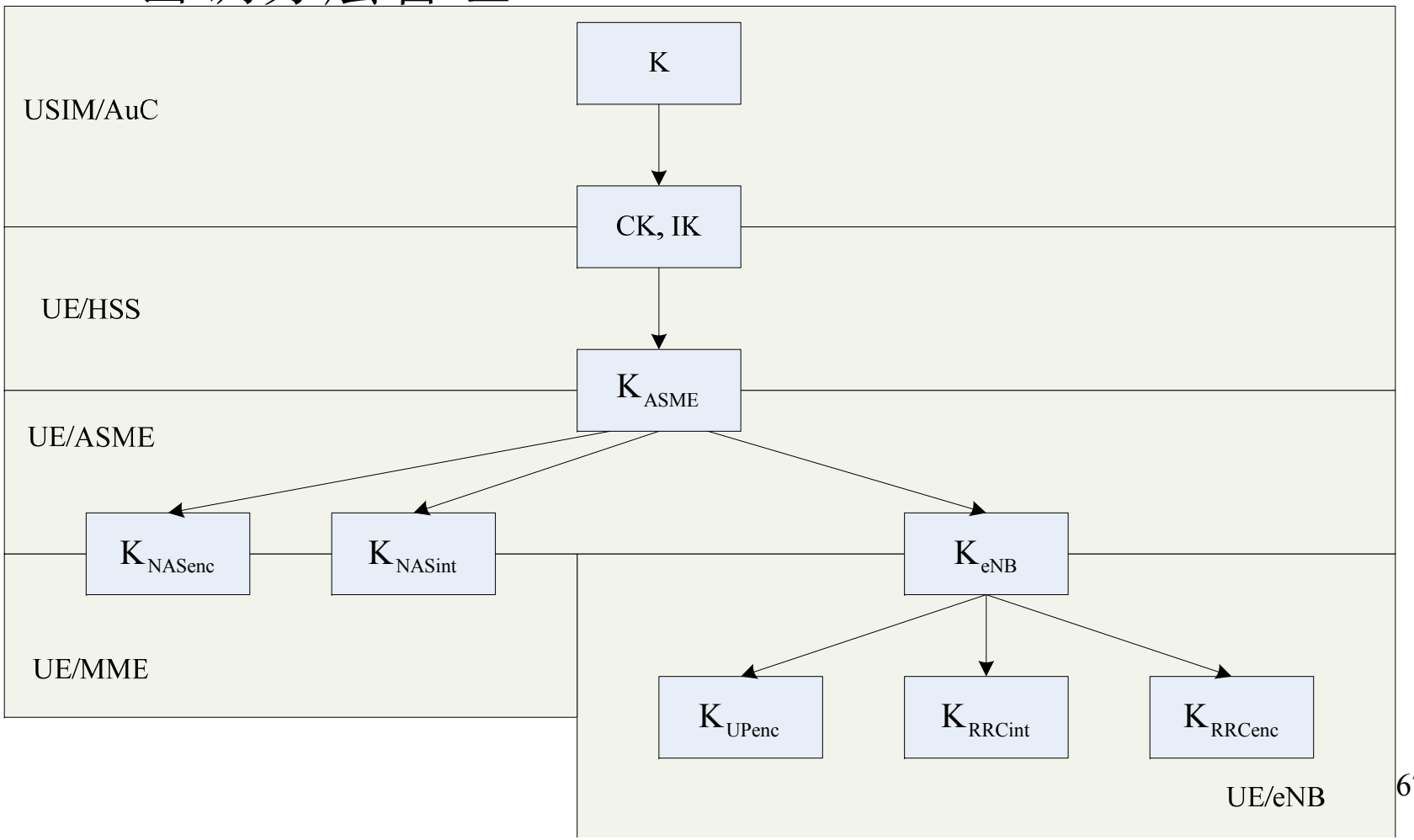
- **1. EPS系统的安全威胁与需求**
- EPS系统的安全要求总结如下。
- 提供比UMTS更强壮的安全性——增加新的安全功能和安全措施；
- 用户身份加密——消除任何非法鉴别与跟踪用户的手段；
- 用户和网络相互认证——保证网络中的通信双方是安全互信；
- 数据加密——确保无法在传输过程中窃取业务数据；
- 数据完整性保护——保证任何网络实体收到的数据都未被篡改；
- 与GERAN和UTRAN互操作——在网络互操作条件下，保证安全性低的接入网不会对LTE/SAE产生威胁；
- 重放保护——确保入侵者不能重放已经发送的信令消息。

19.6.1 LTE系统的信息安全

- **2. EPS的安全体系与密钥管理**
- EPS系统的安全体系的特点总结如下。
- 非接入层(NAS)引入安全机制，包括加密与完整性保护。由于EPC支持非3GPP网络接入，因此需要采用移动IP机制。为了提高系统安全的健壮性，NAS层的所有信令都要进行加密和完整性保护。
- 使用临时用户识别码，在UE接入网络初始附着时，强制进行AKA双向认证。
- 使用加密技术，保证用户数据和信令的安全，使用完整性技术，保证网络信息的安全。
- 采用动态密钥分配与管理机制，增加抽象层，对密钥进行分层管理，保护各级密钥。
- 在IP传输层，采用IPSec协议保护传输数据。
- 增加3GPP与非3GPP接入网之间的安全互操作机制。

19.6.1 LTE系统的信息安全

- **2. EPS的安全体系与密钥管理**
- EPS密钥分层管理

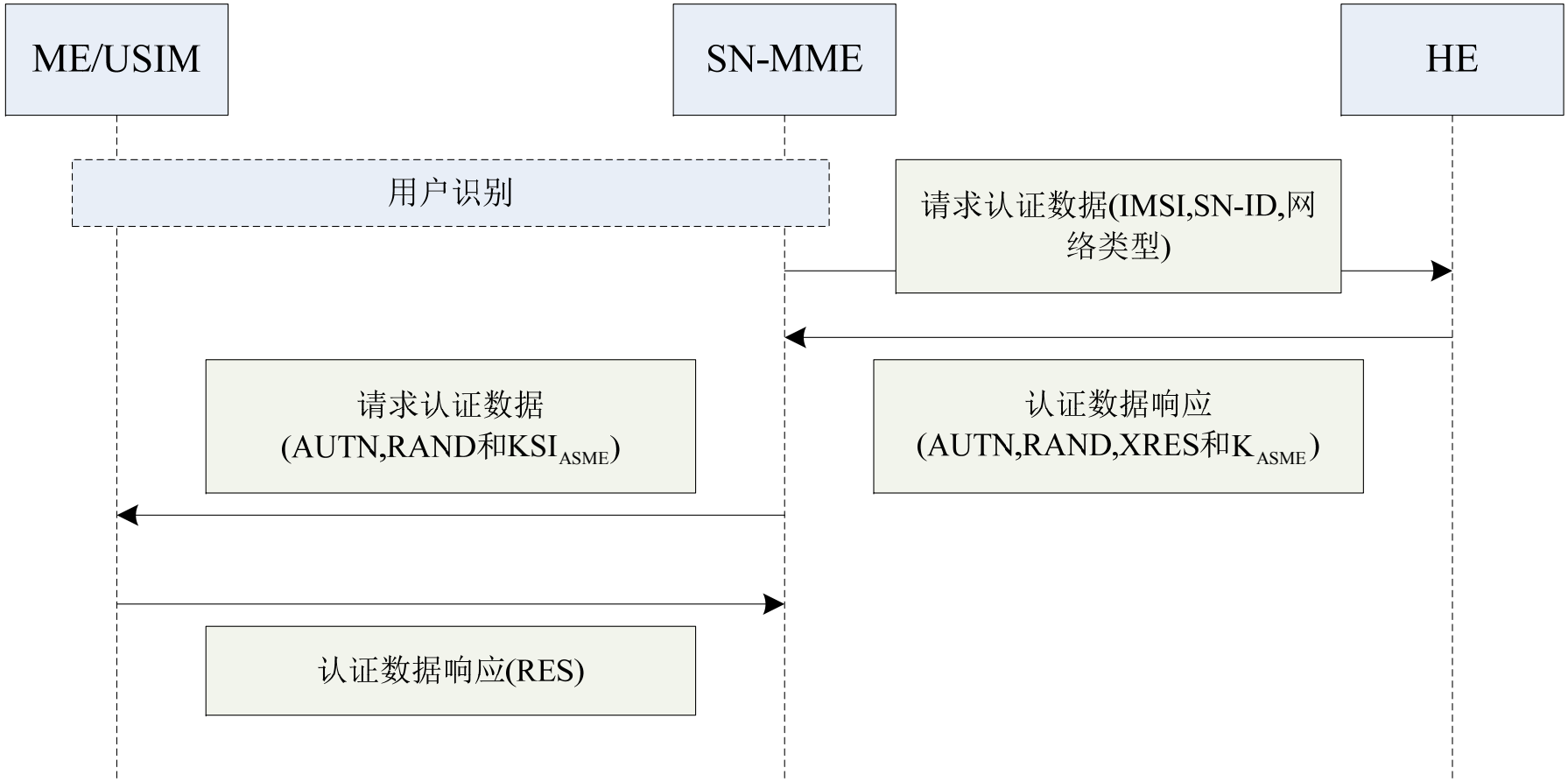


19.6.1 LTE系统的信息安全

- K、CK与IK，K是主密钥，位于USIM与AuC中，基于KDF生成CK，用于加密，生成IK用于完整性保护，CK与IK位于UE和HSS中。
- KASME，由CK与IK派生，位于UE与ASME(接入安全管理实体，位于MME)中，用于生成AS(接入层)与NAS的各种会话密钥，进行加密和完整性保护。
- KeNB，当UE在连接状态，由UE和MME从KASME派生；当UE在切换状态，由UE和目标eNodeB派生。
- KNASint与 KNASenc，分别用于NAS数据完整性保护和数据加密算法的密钥，由UE和MME从KASME派生。
- KUPenc、KRRCint和KRRCenc，分别用于AS层上行业务数据加密、RRC数据完整性和加密的密钥，由UE和eNodeB从KeNB派生。

19.6.1 LTE系统的信息安全

- EPS AKA流程



19.6.1 LTE系统的信息安全

- 与UMTS相比，EPS主要在以下三方面进行了安全性增强。
- AS与NAS双层安全功能
- EPS在AS安全功能层上引入了NAS层的安全机制。主要目的是防止不安全接入网对EPC的侵入。EPS对NAS层的所有信令都进行两次加密和完整性保护，从而提高了整个系统的健壮性。NAS比AS的安全参数具有更长的生命期。
- 网络互操作接口的安全保护
- 在网络侧，为了保护基于IP的EPC网络互操作接口，采用了IPsec对数据和信令进行保护。
- AKA机制增强
- UMTS中，CK与IK由AuC计算并反馈给SN。而EPS中，当SN请求时，CK和IK由归属网络的HSS计算，并不反馈回SN，仅当UE被网络认证后，才用反馈KASME代替。这样可以用KASME明确区分SN和UE的识别。

19.6.1 LTE系统的信息安全

- **3. EPS安全机制**
- EPS的安全机制主要包括用户身份保护、用户与网络双向认证以及数据保护三方面措施
- **(1)用户身份保护**
- 与GSM/UMTS类似，EPS主要采用临时识别码更新保护用户身份。这些临时识别码包括：M-TMSI，S-TMSI，GUTI，S-TMSI。除此以外，永久性识别码IMSI和IMEI需要被安全存储。用户身份保护存在一个漏洞，如果MME质询UE的IMSI，则即使通信不安全，UE也需要发送。

19.6.1 LTE系统的信息安全

- **(2)用户与网络双向认证**
- AKA机制保证了SN对UE的认证，同时也允许UE通过AUTN验证网络。KASME、CK与IK被抽象为密钥集合KSIASME。
- MME向UE发送KSIASME、AUTN和RAND，UE以SN-ID作为参数计算KASME，从而对网络进行认证。需要注意的是，这些认证向量必须随时更新，保证它们的安全性。

19.6.1 LTE系统的信息安全

- **(3)数据保护**
- 当UE和网络完成相互认证，则可以启动安全通信。EPS的数据保护包括数据加密和完整性保护，包括两次的加密和完整性保护过程。
- EPS的数据加密采用序列密码技术。对于信息数据，NAS和AS层都要进行序列加密，而对于业务数据，则只在AS层进行序列加密。
- EPS的完整性保护有效防止了中间截获攻击，对于所有信令数据，NAS和AS层都要进行完整性保护，由于完整性算法增加数据包开销，降低有效数据速率，因此业务数据不进行完整性保护。

19.6.2 WLAN系统安全缺陷

- IEEE 802.11标准采用WEP协议作为安全算法，但由于错误使用RC4算法，使得WLAN系统在算法密钥、数据完整性与密钥管理分配方面存在严重缺陷
- **1.加密算法漏洞**
- WEP协议采用RC4对称加密算法，密钥长度为40比特或128比特。但由于IV向量是公开的，因此根据IV复用情况有可能检测出密钥。更为严重的是IV向量仅有24比特，因此最大组合为2^{24}，只要发送5000个数据包，约几分钟时间就会产生周期性重复，从而极大降低了RC4算法安全性，导致WEP安全性极差。

19.6.2 WLAN系统安全缺陷

- **2.数据完整性缺陷**
- WEP协议采用CRC-32的校验和检查数据完整性，但这是一个错误方法。CRC-32可以发现信道传输差错，但由于CRC和RC4都是线性变换，因此无法通过异或这种线性操作，发现数据的篡改。因此WEP的完整性保护完全无效。

19.6.2 WLAN系统安全缺陷

- **3.密钥管理局限**
- WLAN利用AP标识进行接入控制，但如果无线网卡的ESSID设定为“ANY”时(这是目前绝大多数无线网卡、无线AP的默认ESSID标识)，就能自动搜寻在信号范围内所有的AP并试图建立连接，由此一来，无线网络的安全性形同虚设。

19.6.2 WLAN系统安全缺陷

- 正是看到了安全方面的不足，IEEE 802.11工作组开发了更安全的802.11i加密标准。
- 我国提出的WAPI(WLAN Authentication and Privacy Infrastructure)标准，具有比802.11i更好的安全性能。
- 它采用公开密钥体制，在网络和终端之间进行双向身份认证。
- 2009年6月，在日本东京召开的ISO/IEC JTC1/SC6全会上，WAPI获得包括美、英、法等10余个与会国家成员体一致同意，正式成为无线局域网的国际标准，掀开了新的篇章。

19.6.3 WiMax系统的鉴权与加密

- WiMax系统(802.16d/e)安全机制的核心是MAC层中的安全子层，提供鉴权、安全密钥交换和加密功能，定义了加密封装协议、私用密钥管理(PKM)协议，提供多种信令和数据的加密算法和密钥，并提供用户和设备两种认证方式。
- 另外WiMax可以自由地选取更高层(如网络层、传输层、会话层等)上的安全机制，这些机制包括IPSec协议、传输层安全(TLS)协议和无线传输层安全(WTLS)协议。

19.6.4 5GNR系统的信息安全

- 5G NR系统的安全机制设计沿用了LTE的基本思路。但由于5G引入了三大场景，支持大规模IoT节点、D2D通信、V2X通信、SDN/NFV等功能，因此在安全机制上带来了很多新的挑战。
- **(1)5G接入与切换的安全保障**
- 5G网络可以支持海量用户与多种类型的移动设备安全接入网络。为此，与无线接入相关的安全技术包括：多域条件下的超短时间鉴权与认证技术、异构网络安全通信以及无缝安全漫游与切换技术等。
- **(2)IoT安全保障**
- 3GPP组织已经设计了多种IoT标准，海量IoT设备并发安全接入、不同类型IoT设备的差异化安全接入、隐私保护以及轻量级安全机制等。

19.6.4 5GNR系统的信息安全

- **(3)D2D安全保障**
- 终端直连(D2D)通信是5G新引入的通信方式，移动蜂窝网络与无线自组织网络混合组网，使得5G网络面临多种安全威胁与隐私泄漏风险，还需要进一步研究。
- **(4)V2X安全保障**
- 5G V2X具有多种技术优势，例如大范围覆盖、预先部署的基础设施、确定的安全性与QoS保障，以及更稳健的灵活性。但是，还有一些安全机制需要进一步提高。
- **(5)网络切片安全保障**
- 在网络切片框架下，传统网络下的安全机制无法应对，需要在安全策略、可信网络管理等方面进一步改进。

§19.7 本章小结

- 本章讨论移动通信中的信息安全问题。首先对移动通信的安全性威胁和措施概要介绍。
- 然后简要介绍了保密学基本原理：狭义/广义保密学、单/双密钥、序列(流)加密、分组(块)加密、公开密钥等。
- 第三重点讨论移动通信鉴权与加密方案，包含两大类型方案：GSM/GPRS/WCDMA、IS-95/CDMA2000系列的鉴权与加密方案与措施。
- 最后，简要介绍了LTE/WiMax/5G等宽带移动通信系统的安全技术，并分析了WLAN的安全缺陷。

参考文献

[19.1] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inform. Theory, Vol. IT-22, Nov. 1976.

[19.2] X. J. Lai and J. Massey, “A Proposal for a new block encryption standard,” Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 389-404, 1991.

[19.3] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

[19.4] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., Vol. 28, pp. 656-715, Oct. 1949.

[19.5] X. W. Wang et. al., “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD,” Crypto 2004

[19.6] 吴伟陵，《信息处理与编码(修订本)》，人民邮电出版社，2003.7

[19.7] D. R. Stinson, Cryptography Theory and Practice，(2nd)，CRC Press LLC 2002.

[19.8] M. Y. Rhee, CDMA Cellular Mobile Communications and Network Security, Prentice Hall, 1998.

[19.9] 杨义先等，现代密码新理论，科学出版社，2002.8

[19.10] 3GPP TS 33.102 3G Security：Security Architecture

[19.11] 3G TS 33.105 3G Security：Cryptographic Algorithm Requirements

谢谢！