

课程编号: 3182121321

无线通信安全



第七讲 WCDMA安全技术

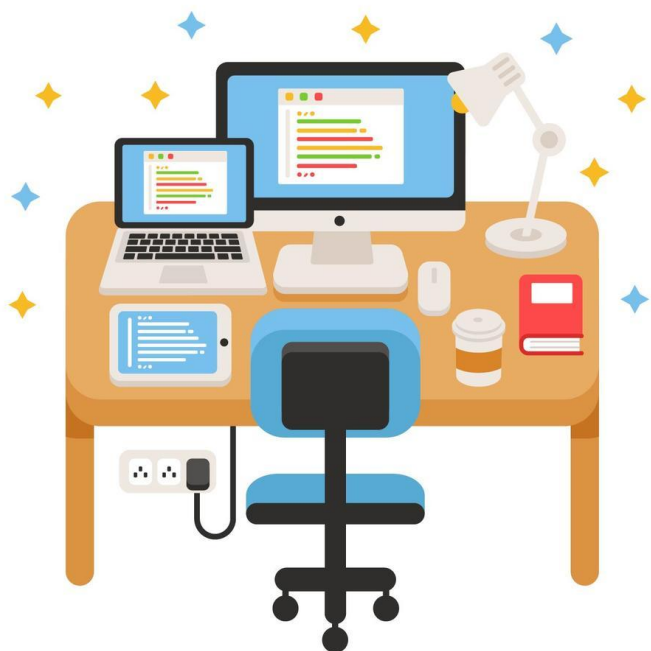
李晖

lihuill@bupt.edu.cn

监控厂商滥用权限追踪手机位置

- 4月23日，Citizen Lab发布报告，揭示：
- 两起间谍行动：监控厂商利用全球电信网络漏洞，追踪人们的手机位置。
- 伪装公司：相关监控厂商假装成合法运营商，借此进入网络并查询目标位置数据。
- 技术漏洞：
 - SS7协议(2G/3G)：缺乏认证和加密；
 - Diameter协议(4G/5G)：虽有改进，但部分运营商未完全落实防护措施。
- 新闻链接：[Surveillance vendors caught abusing access to telcos to track people's phone locations, researchers say | TechCrunch](#)



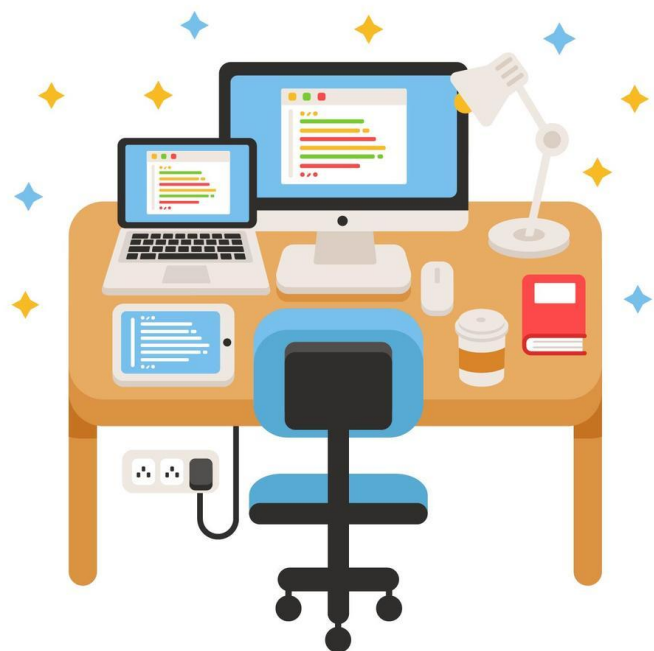


1. 3G通信技术简介
2. 安全原则和安全目标
3. 安全体系结构
4. 接入域安全
5. 网络域安全
6. 结论

1. 3G通信技术简介

3G通信技术

- 由2G向3G的演进
 - GSM → GPRS → **WCDMA** (3GPP, S3)
 - CDMA → CDMA20001x → **cdma2000** (3GPP2, WG4)
 - GSM → **TD-SCDMA**
- 3G主要特征
 - 宽带CDMA技术
 - 支持多路同步通话或数据传输
 - 提供2Mb/s的数据传输数率



1. 3G通信技术简介
- 2. 安全原则和安全目标**
3. 安全体系结构
4. 接入域安全
5. 网络域安全
6. 结论

2. 安全原则和安全目标

3G安全原则

- 建立在2G系统的安全基础之上。
 - 在GSM和其它2G系统中认为是必要的和稳健的安全特征，将在3G安全中采纳。
- 对现有2G系统的安全机制进行增强和改进，对2G系统中存在的潜在的安全缺陷进行改进。
- 根据3G提供的业务特点，将提供新的安全特征和安全服务。

2. 安全原则和安全目标

2G系统的安全特征及弱点

■ 安全特征

- 用户访问鉴权 ❌
- 无线接口加密 ❌
- 用户身份机密性 ❌
- 用户身份模块SIM ✔
- 安全独立于用户 ✔

安全弱点

- 认证方式简单
 - 仅单向实体认证，难防止中间人攻击和假基站攻击
- 密码算法不安全
 - 算法不公开，缺乏对安全性客观、公正的评估
 - 密钥长度不够
- 缺乏完整性保护
 - 用户数据和信令数据可被篡改
- 用户隐私泄露
 - 在无线信道上以明文发送安全参数IMSI
- 保护范围有限
 - 在固定网内无加密和认证措施
 - 不提供端到端的加密

2. 安全原则和安全目标

3G中的安全威胁

- 未授权访问敏感数据
 - 违反了信息的机密性（偷听，流量分析，泄密）
- 未授权操纵数据
 - 违反了完整性（信息可能被入侵者故意修改、插入、重复或删除）
- 扰乱网络服务或者滥用网络服务
 - 导致拒绝服务或者降低可用性
- 否认
 - 一个用户或者一个网络否认已经发生的操作
- 未授权访问服务
 - 用户可能通过滥用其访问权获得未授权访问服务

2. 安全原则和安全目标

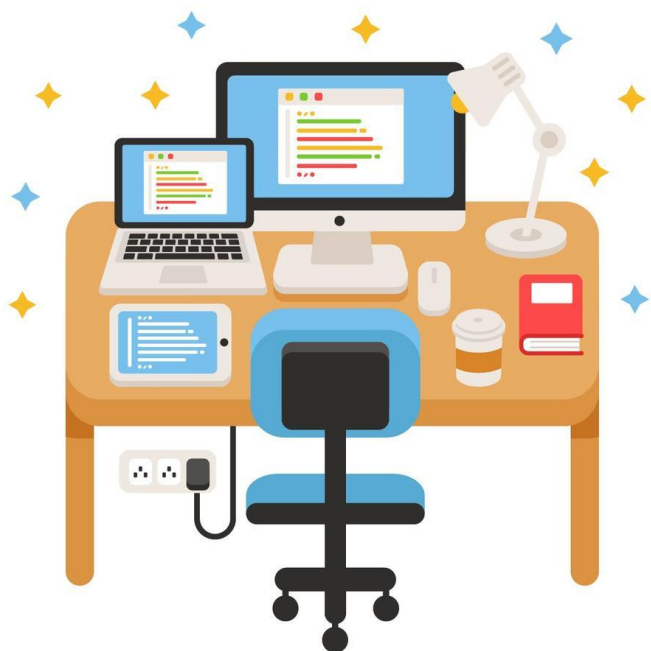
新的环境及业务特点

- 基于IP网络
- 运营商越来越多
- 业务提供商越来越多
- 非话音服务的多样性和重要性
- 将增强用户服务范围的控制和对其终端能力的控制
- 存在对用户的主动攻击
- 终端将用做电子商务应用和其它应用的平台

2. 安全原则和安全目标

3G安全目标

- 确保用户相关的信息安全，以防止滥用或盗用
- 确保服务网络和归属网提供的资源和业务得到足够的保护，以防止滥用和盗用。
- 确保安全特征的充分标准化，保证全世界范围内的漫游和互通能力
- 确保给用户和业务提供者提供的安全水平高于当前正在使用的固定网络和移动网络
- 确保3G安全特征的可扩展性，能够根据新的威胁和业务要求进行升级或更新



1. 3G通信技术简介
2. 安全原则和安全目标
- 3. 安全体系结构**
4. 接入域安全
5. 网络域安全
6. 结论

3. 安全体系结构

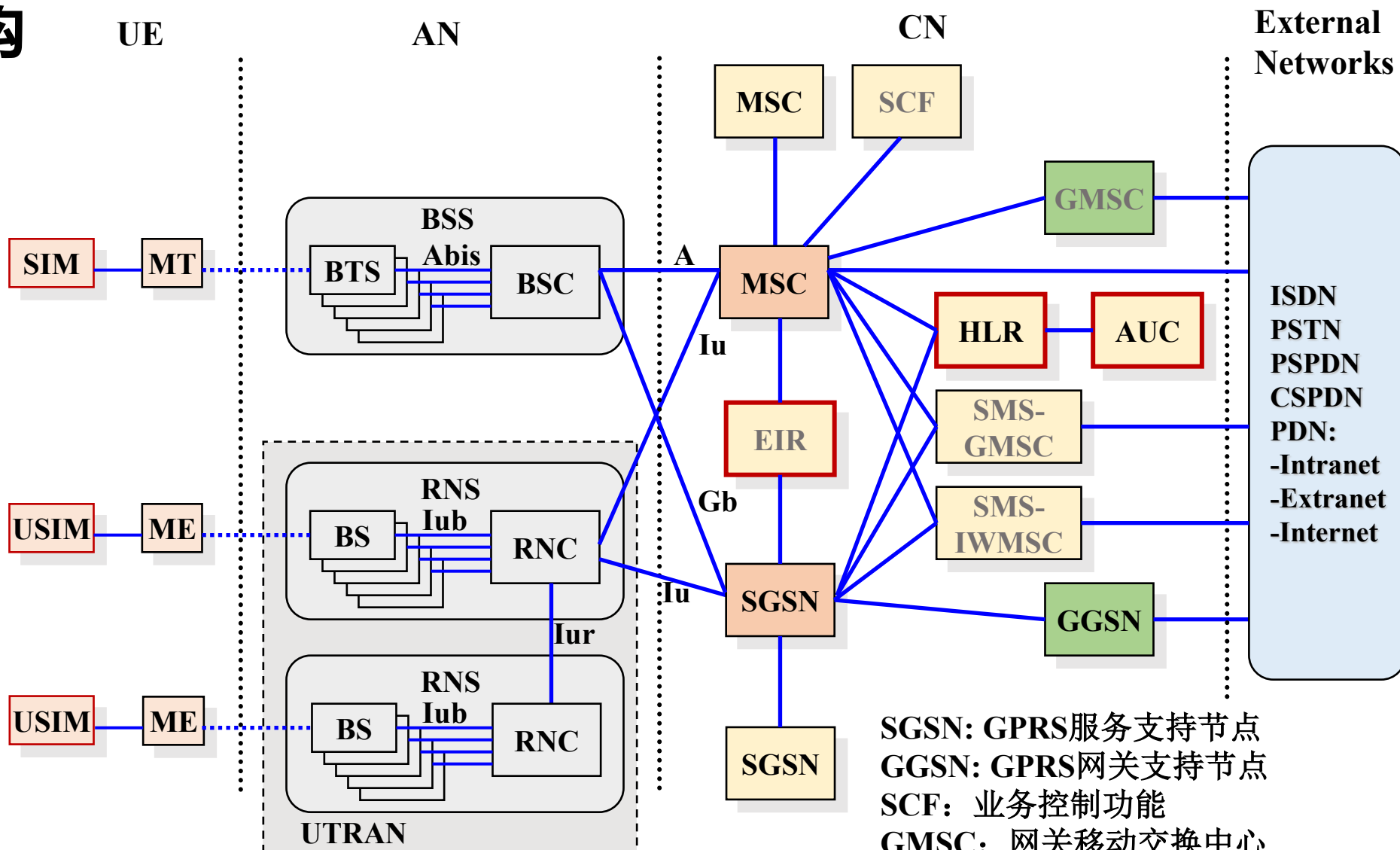
3G系统网络结构

分组交换域 (PS)

- 从**GPRS**域进化而来
- **SGSN**负责网络接入控制、路由选择和转发、移动性管理等
- **GGSN**负责数据包路由和封装以及与外部数据网的接口功能

电路交换域(CS)

- 从**GSM**进化而来
- **MSC**（移动交换中心）是重要的网元



SGSN: GPRS服务支持节点
GGSN: GPRS网关支持节点
SCF: 业务控制功能
GMSC: 网关移动交换中心
SMS-GMSC: 短信网关移动交换中心
SMS-IWMSC: 短信互通移动交换中心

3. 安全体系结构

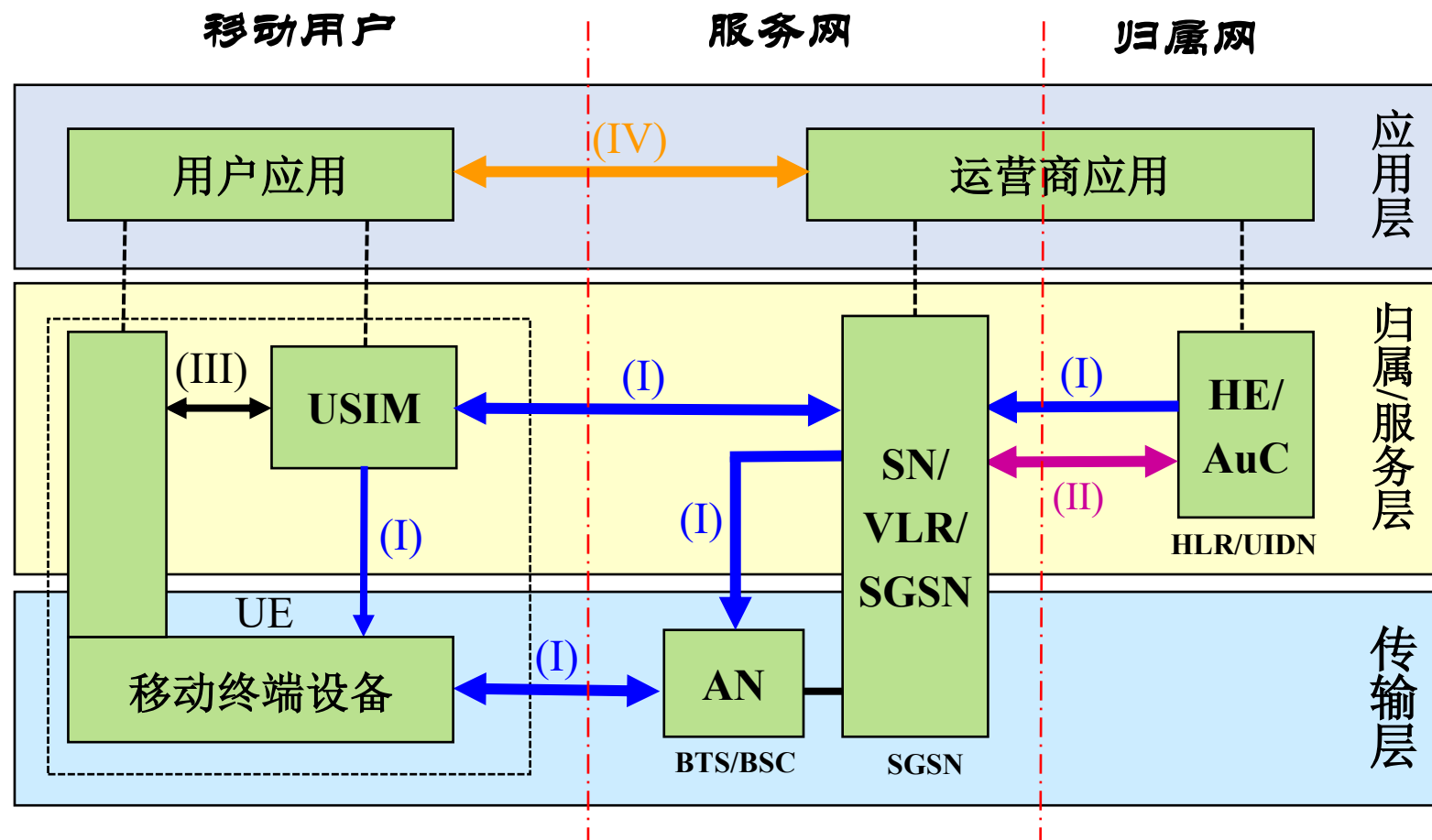
3G安全体系结构

三个层面

- 应用层面
- 归属及服务网络层面
- 传输层面

五个域

- 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



3. 安全体系结构

接入安全

- 作用
 - 提供用户安全接入3G提供的业务，防止在无线信道上的攻击。
- 内容
 - 用户身份的机密性、用户位置的机密性、用户不可跟踪性、用户身份认证、加密算法和完整性算法的协商、加密密钥和完整性密钥的协商、用户数据和信令数据的机密性和完整性保护等。

网络域安全

- 作用

- 运营商网络领域内的节点之间安全的交换信令数据，主要防止在固定有线网内部的攻击

- 内容

- 网络实体之间的相互认证、信息加密、信息的完整性保护和欺骗信息的收集

3. 安全体系结构

用户域安全

- 作用
 - 用户安全使用移动终端
- 内容
 - 1.用户和智能卡(USIM)之间的认证
 - 2.智能卡和终端设备之间的认证
 - 3.智能卡和终端设备之间链路的保护

3. 安全体系结构

应用安全

- 作用
 - 用户和网络运营商或应用提供商之间的应用能够安全的交换信息
- 内容
 - 随应用的不同而不同

3. 安全体系结构

安全的可视性和可配置性

- 作用

- 使用户得知一个安全特征是否在使用，并且业务的使用和提供是否依赖于该安全特征

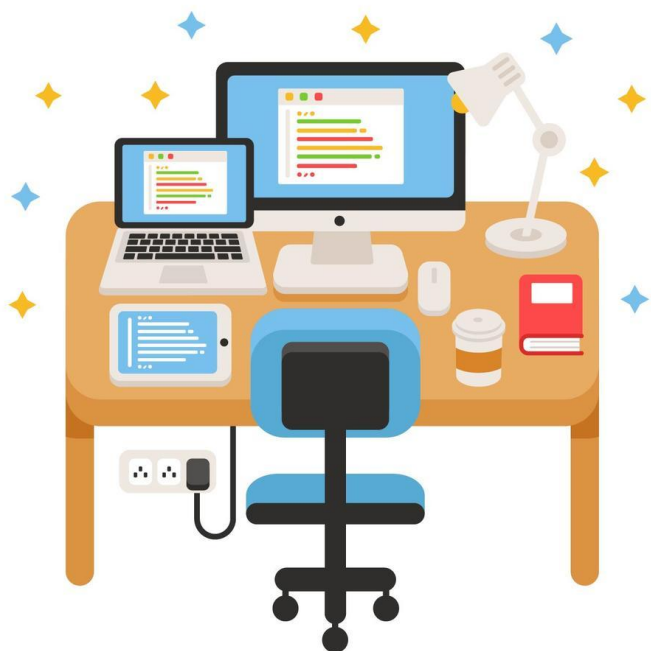
- 内容

- 可视性

- 提示用户接入网络加密
 - 提示用户安全的级别

- 可配置性

- 是否采用用户和**USIM**卡之间的认证
 - 接受/拒绝非加密方式的被叫
 - 设置或不设置非加密方式的呼叫
 - 接受/拒绝使用某一特定加密算法



1. 3G通信技术简介
2. 安全原则和安全目标
3. 安全体系结构
- 4. 接入域安全**
5. 网络域安全
6. 结论

4. 接入域安全

身份标识机制

- 通过临时身份进行识别（P-TMSI/TMSI）
 - 需要附加位置区域识别码（Location Area Identification, LAI），或路由算法识别码（Routing Area Identification, RAI）
- 通过永久身份进行识别（IMSI）
 - 用户第一次在服务网络注册或服务网络不能从临时移动用户身份TMSI重新得到永久用户身份IMSI时
 - 属于对提供用户身份机密性的一种安全漏洞

4. 接入域安全

临时移动用户身份TMSI的再分配



- (TMSI, LAI) 在无线访问链上识别用户
- TMSI再分配规程应该在初始化加密之后执行

4. 接入域安全

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)
- 生成完整性密钥(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

4. 接入域安全

AKA中用到的变量和函数

- K = 由USIM和AuC共享的主密钥
- $RAND = f_0$, 由AuC产生的随机数, 认证时的挑战 (Challenge)
- $XRES = f_{2_K}(RAND)$, 由AuC计算的期望响应
- $RES = f_{2_K}(RAND)$, 由USIM计算出的响应
- $CK = f_{3_K}(RAND)$, 空中接口加密密钥
- $IK = f_{4_K}(RAND)$, 空中接口完整性保护密钥
- $AK = f_{5_K}(RAND)$, 匿名密钥 (Anonymity Key)
- SQN = 序列号
- AMF = 认证管理域 (Authentication Management Field)
- $MAC = f_{1_K}(SQN \parallel RAND \parallel AMF)$, 网络侧消息认证码
- $AUTN = SQN \oplus AK \parallel AMF \parallel MAC$, 网络认证令牌
- $AV = (RAND, XRES, CK, IK, AUTN)$, 认证五元组或认证向量

4. 接入域安全

认证和密钥协商过程

$$XRES = f2_K (RAND)$$

$$CK = f3_K (RAND)$$

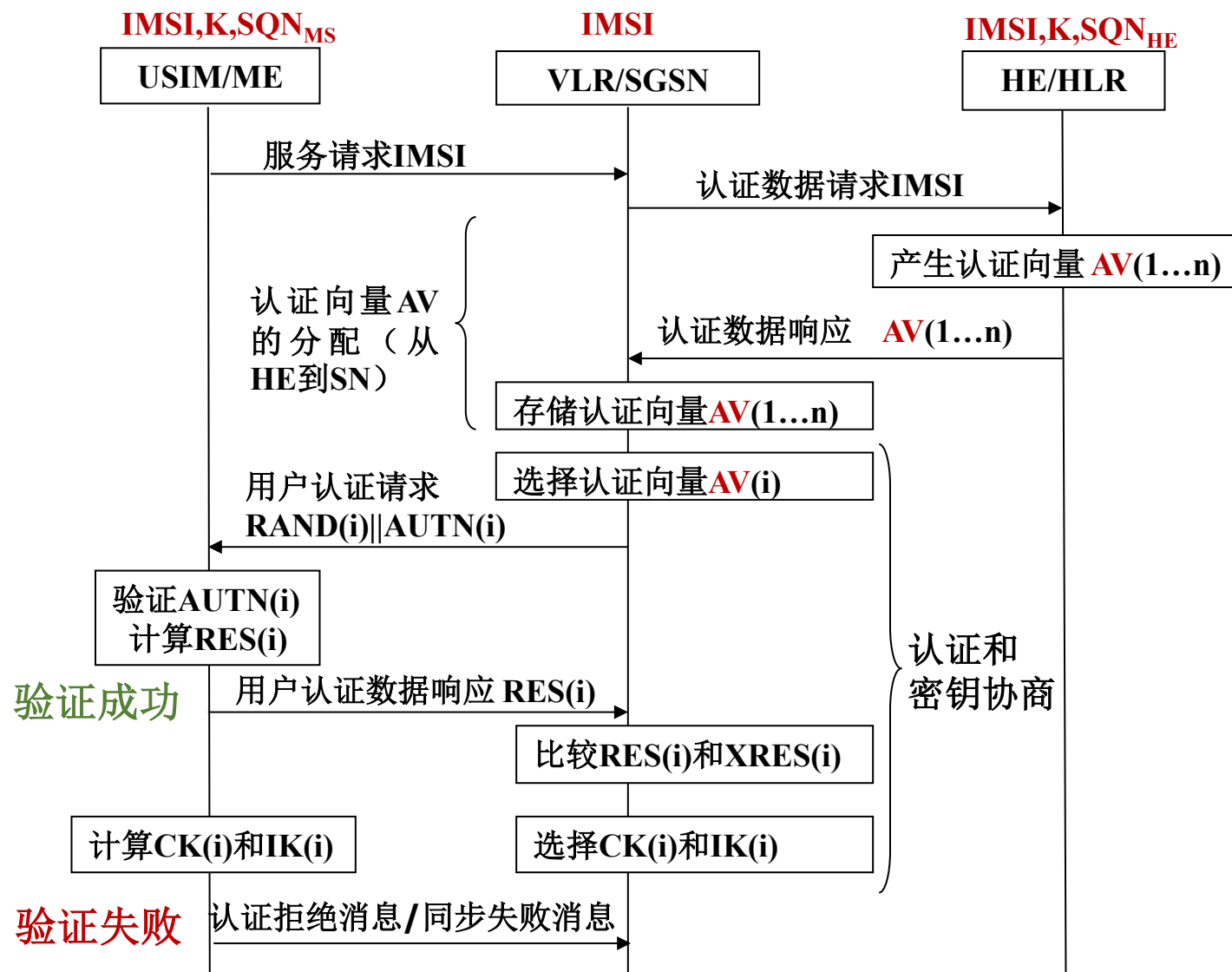
$$IK = f4_K (RAND)$$

$$AK = f5_K (RAND)$$

$$MAC = f1_K (SQN || RAND || AMF)$$

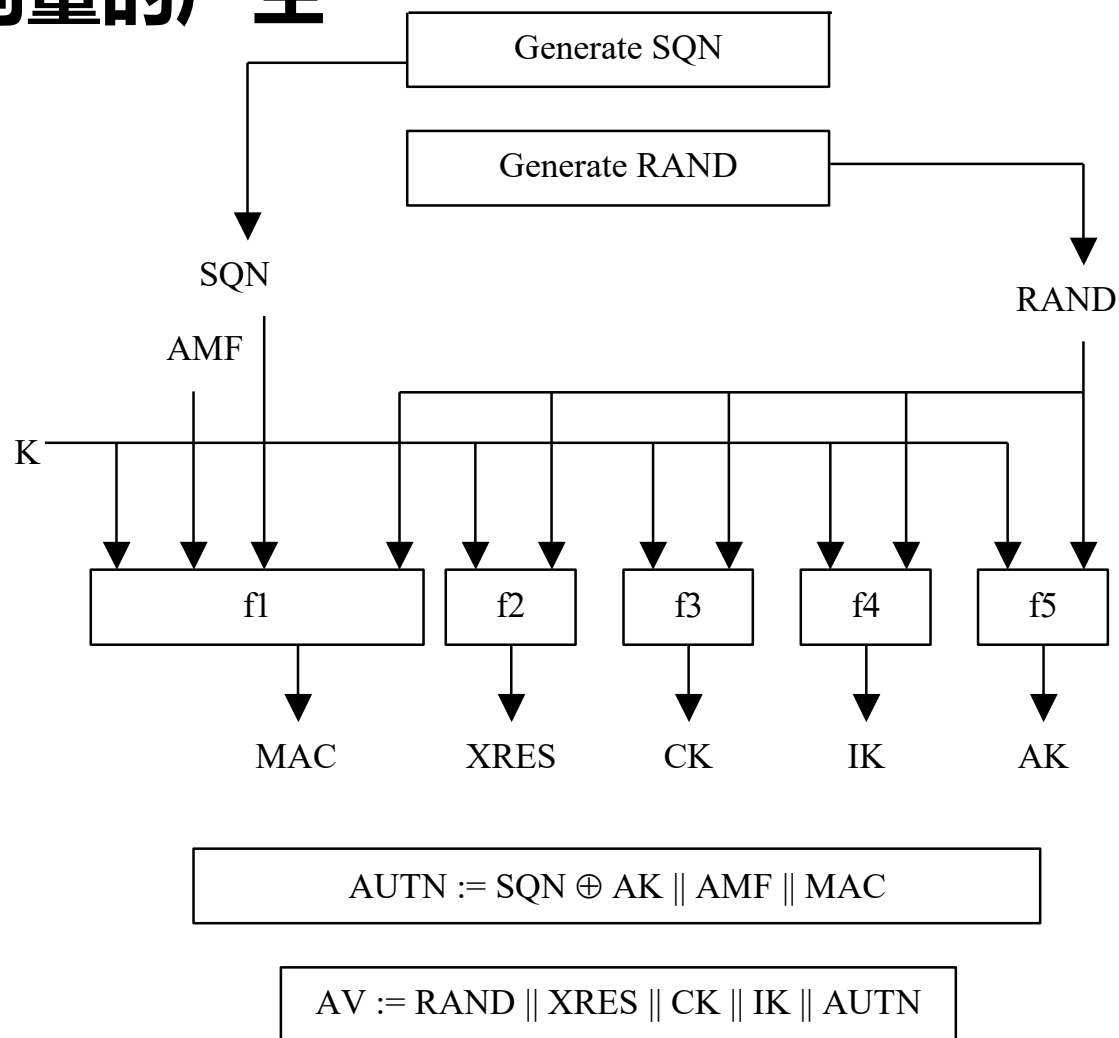
$$AUTN = SQN \oplus AK || AMF || MAC$$

$$AV = (RAND, XRES, CK, IK, AUTN)$$



4. 接入域安全

AuC中认证向量的产生



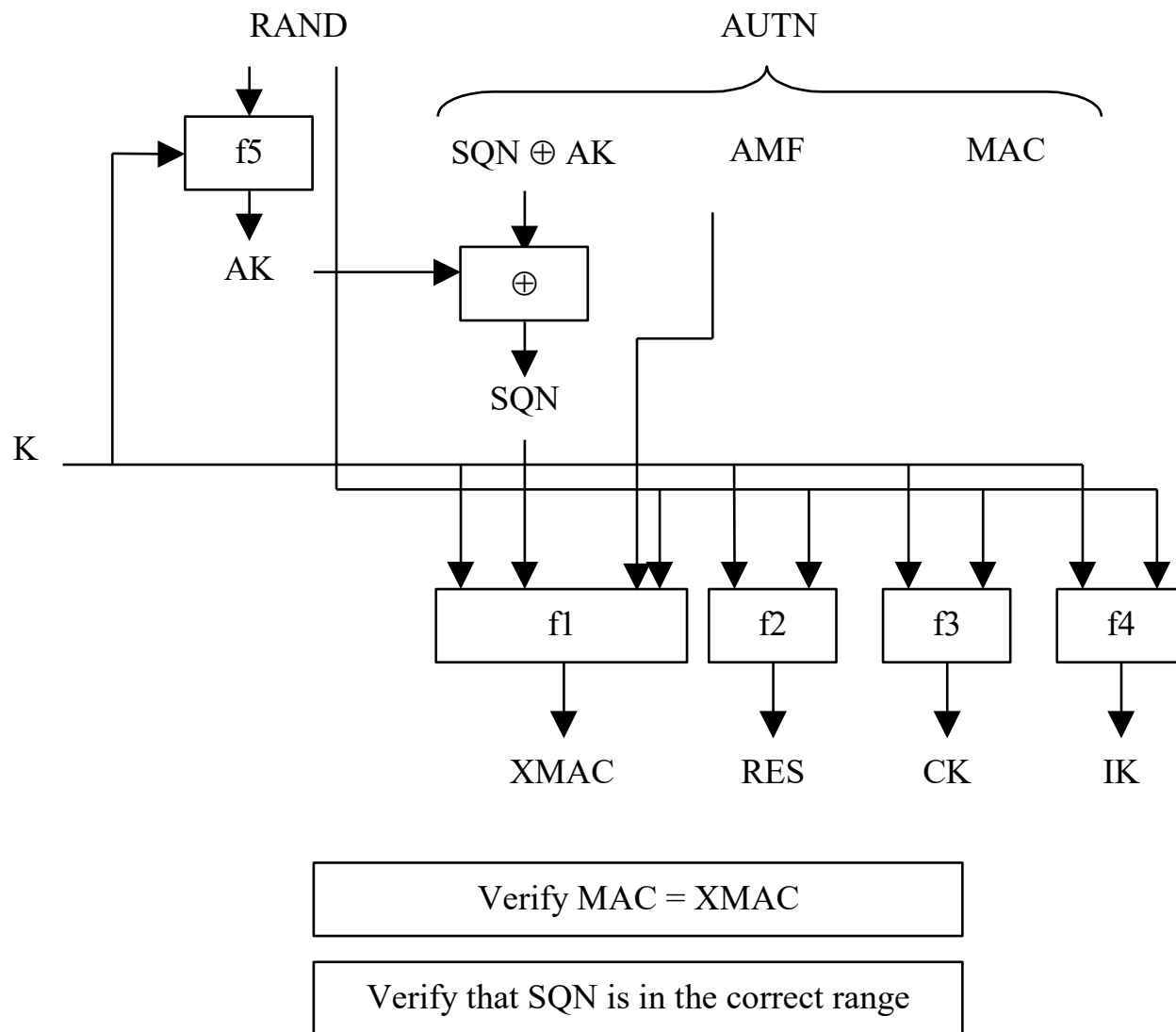
各变量和参数的长度:

- **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

4. 接入域安全

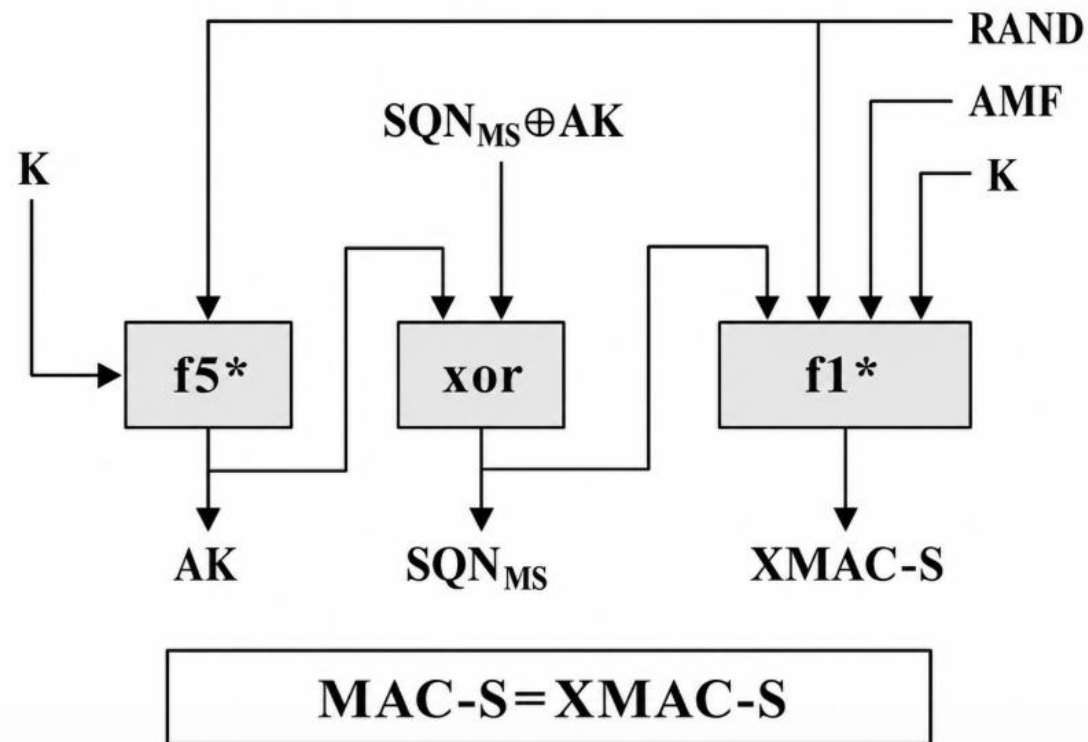
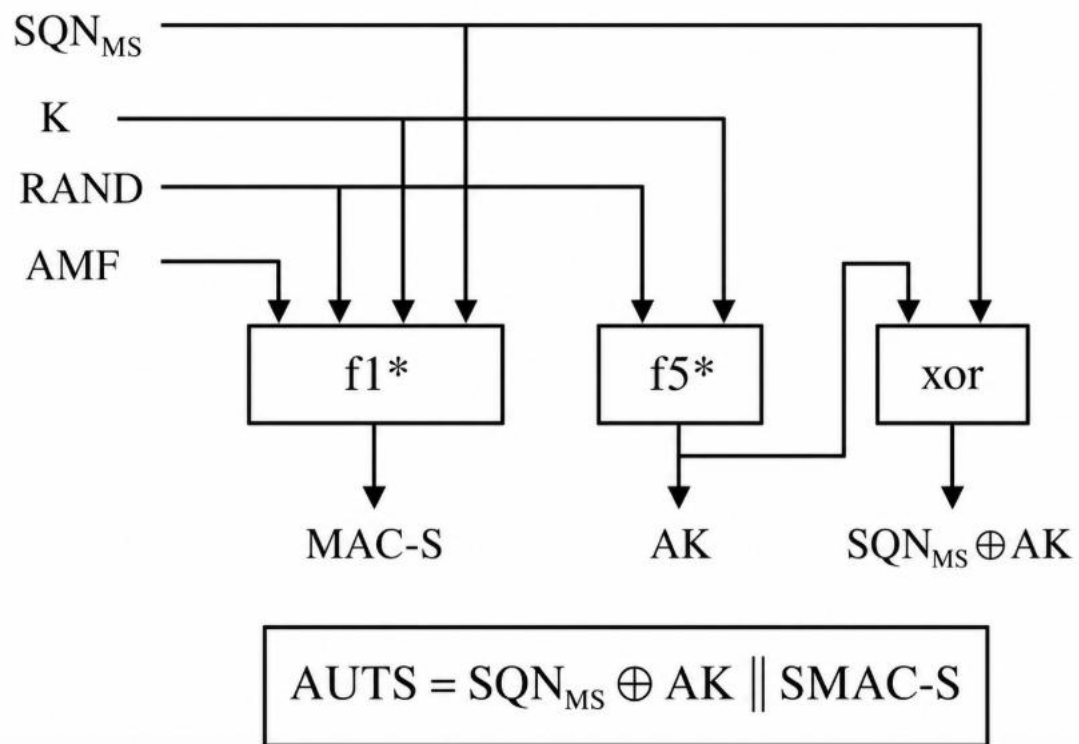
USIM卡中的认证功能

- USIM卡接收到用户认证请求数据 $RAND||AUTN$ 。
- 把 $RAND$ 和 K 输入 $f5$, 产生匿名密钥, 然后得到 $SEQN$ 。
- 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。
- 检查 $SEQN$ 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。



4. 接入域安全

USIM和HLR/AuC的再同步



MS→HLR/AuC: 同步失败指示和一个 (AUTS, RAND) 对

4. 接入域安全

AKA算法要求

- 算法功能要求（f0~f5, f1*,f5*）
- 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）和侧信道（side channel）攻击

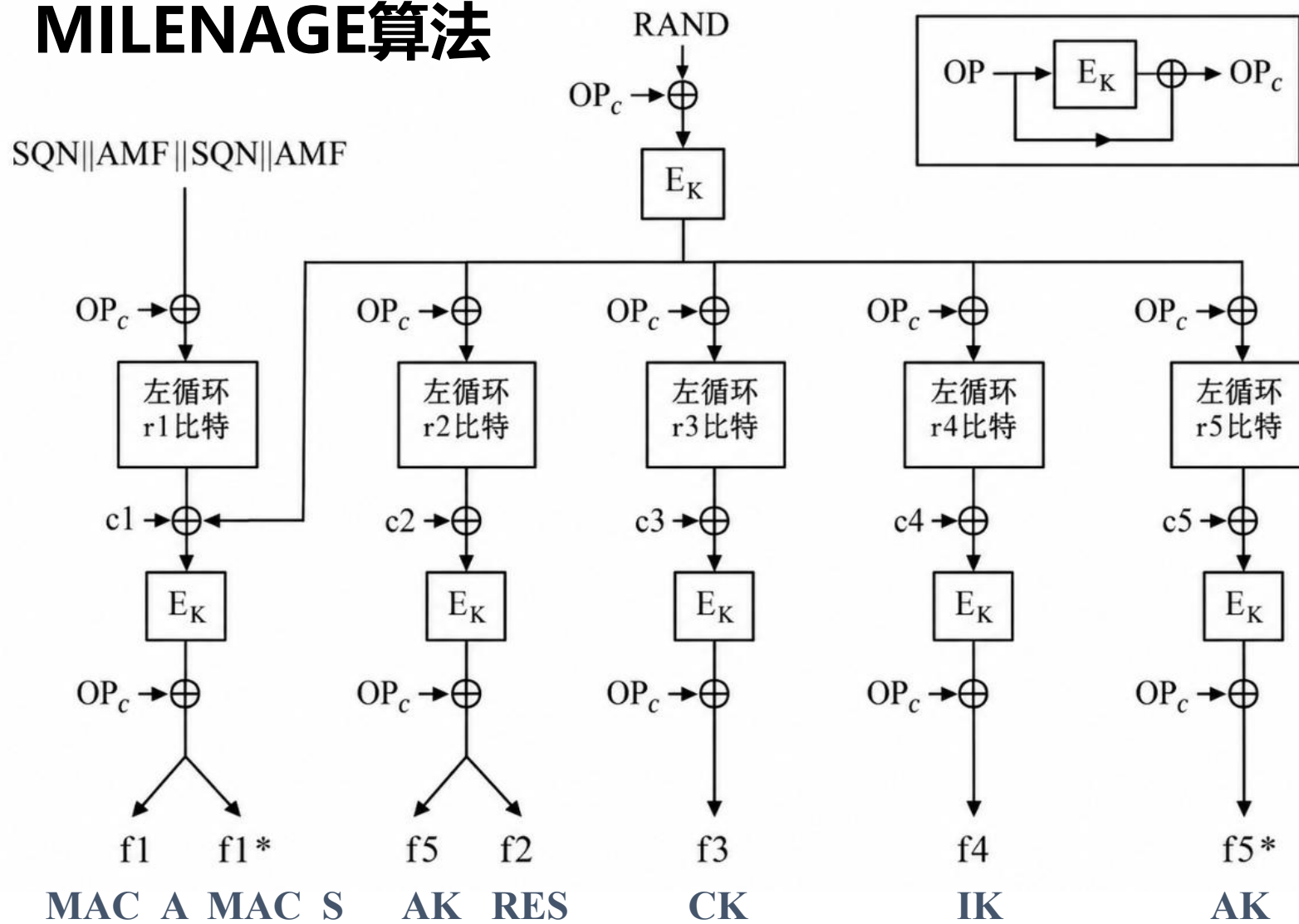
4. 接入域安全

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。

4. 接入域安全

MILENAGE算法



4. 接入域安全

MILENAGE输出值

- 设 $TEMP := E_K[RAND \oplus OPc]$, 则输出值为:
 - ✓ $OUT1 = E_K[TEMP \oplus \text{rot}(IN1 \oplus OPc, r1) \oplus c1] \oplus OPc$
 - ✓ $OUT2 = E_K[\text{rot}(TEMP \oplus OPc, r2) \oplus c2] \oplus OPc$
 - ✓ $OUT3 = E_K[\text{rot}(TEMP \oplus OPc, r3) \oplus c3] \oplus OPc$
 - ✓ $OUT4 = E_K[\text{rot}(TEMP \oplus OPc, r4) \oplus c4] \oplus OPc$
 - ✓ $OUT5 = E_K[\text{rot}(TEMP \oplus OPc, r5) \oplus c5] \oplus OPc$

4. 接入域安全

AKA中各密码学函数的输出值

- 函数f1的输出: $\text{MAC-A} = \text{OUT1}[0] \parallel \text{OUT1}[1] \parallel \dots \parallel \text{OUT1}[63]$
- 函数f1* 的输出: $\text{MAC-S} = \text{OUT1}[64] \parallel \text{OUT1}[65] \parallel \dots \parallel \text{OUT1}[127]$
- 函数f2的输出: $\text{RES} = \text{OUT2}[64] \parallel \text{OUT2}[65] \parallel \dots \parallel \text{OUT2}[127]$
- 函数f3的输出: $\text{CK} = \text{OUT3}[0] \parallel \text{OUT3}[1] \parallel \dots \parallel \text{OUT3}[127]$
- 函数f4的输出: $\text{IK} = \text{OUT4}[0] \parallel \text{OUT4}[1] \parallel \dots \parallel \text{OUT4}[127]$
- 函数f5的输出: $\text{AK} = \text{OUT2}[0] \parallel \text{OUT2}[1] \parallel \dots \parallel \text{OUT2}[47]$
- 函数f5*的输出: $\text{AK} = \text{OUT5}[0] \parallel \text{OUT5}[1] \parallel \dots \parallel \text{OUT5}[47]$

4. 接入域安全

MILENAGE的特点

- 使用OP的推导值OPc，从而USIM不需要存储OP值，增加了OP值的机密性；
- 使用旋转常数r1~r5和附加常量c1~c5，确保区分所有的加密函数。
- 结构的合理性
 - f1和f1*结构本质上与应用于输入块RAND和IN1的标准CBC MAC模式大致相同，此结构的正确性已经被证明；
 - f2、f3、f4、f5函数被定义为一种对随机质询进行的双重加密，在第二次加密之前要经历旋转并使用附加常量参与运算，是一种较为普遍的操作模式，已被证明在某种攻击下安全；
- 选用了分组加密Rijndael算法作为内核
- 用户选项：
 - 由运营商可以自由选择OP和可移植的内核算法
 - 由运营商可以在某些条件下选择自己的常量和旋转值

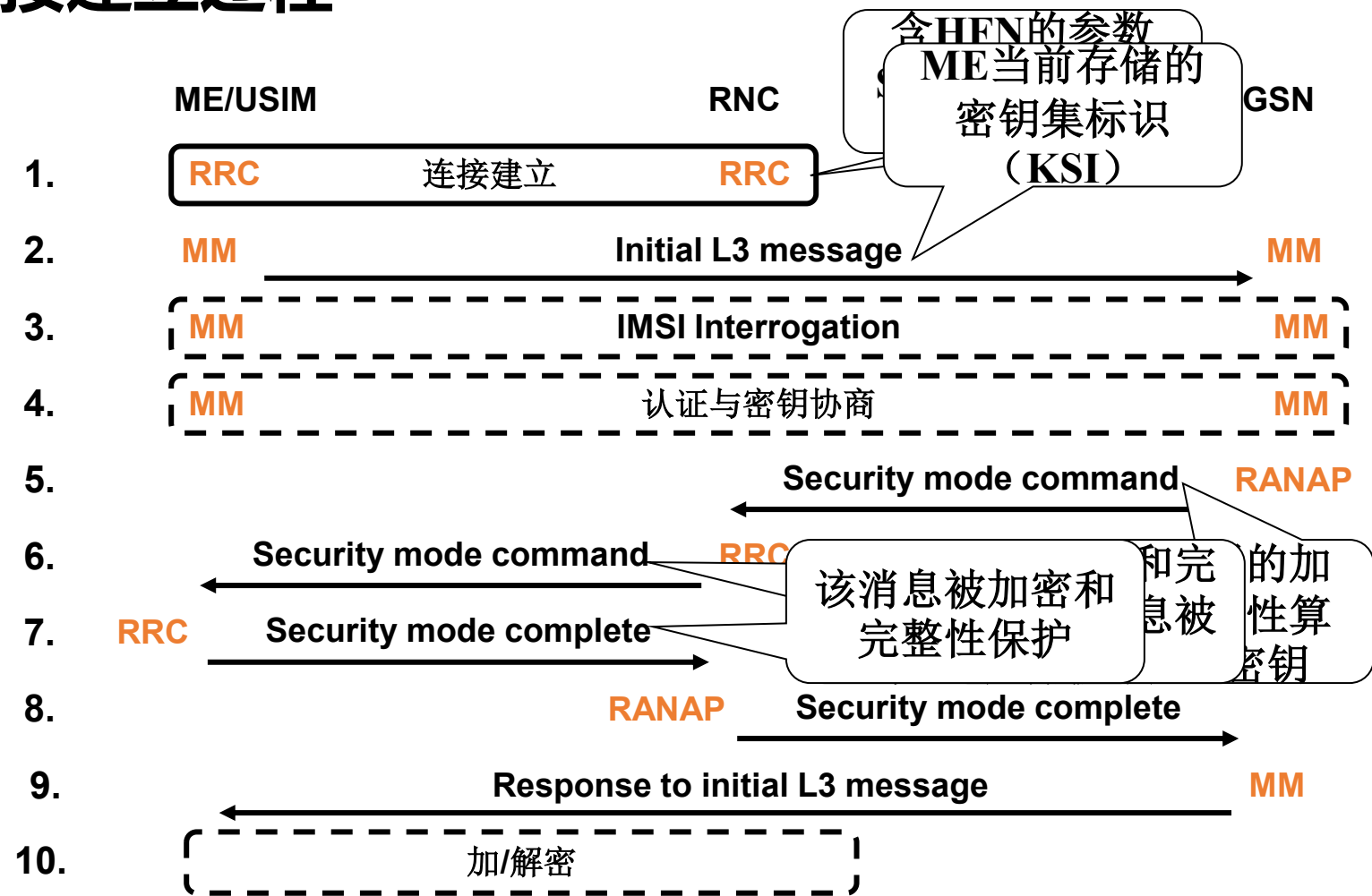
4. 接入域安全

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)

4. 接入域安全

安全连接建立过程

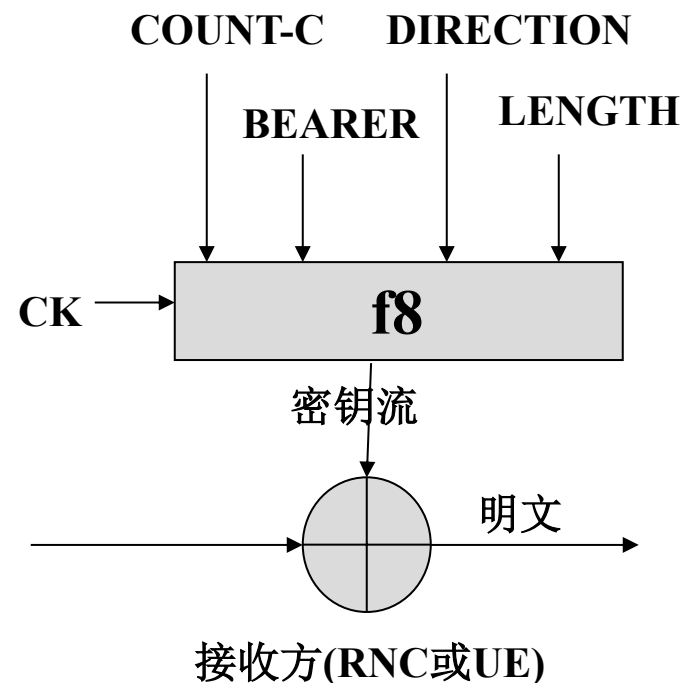
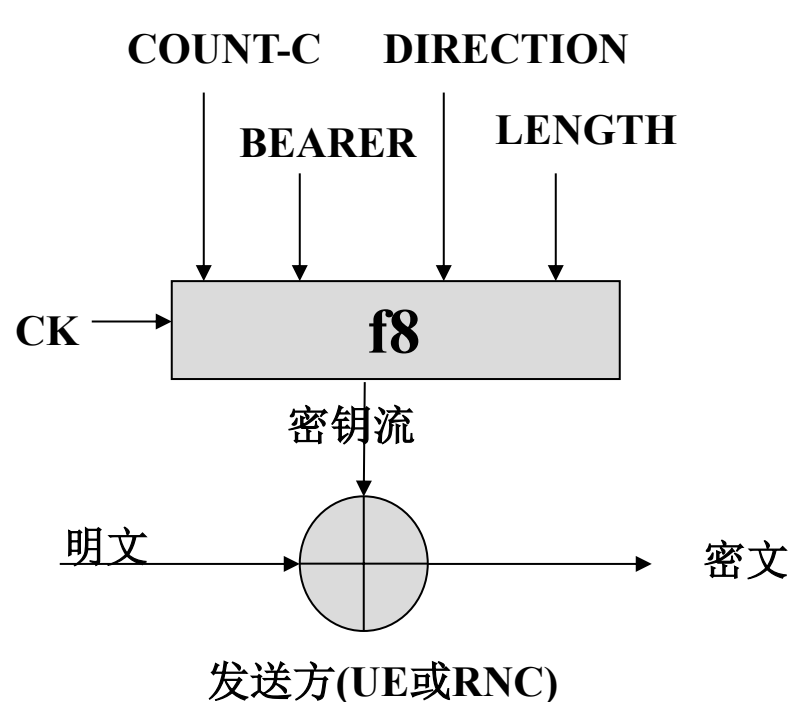


RRC: Radio Resource Control
HFN: HyperFrame Number
KSI: Key Set Identifier
MM: Mobility Management
RANAP: Radio Access Network Application Part

4. 接入域安全

空口加解密机制

- 适用于所有用户业务信息和关键信令信息的加密
- 采用序列密码f8，在终端和RNC中实现；
- 有不同的算法可以选择，算法标识符占4位：
 - “0000”，UEA0，不加密
 - “0001”，UEA1，基于Kasumi算法



CK(加密密钥)	128比特	COUNT-C(加密计数器)	32比特
BEARER(无线信道指示器)	5比特	DIRECTION(方向标识)	1比特
LENGTH(密钥流长度)	16比特		

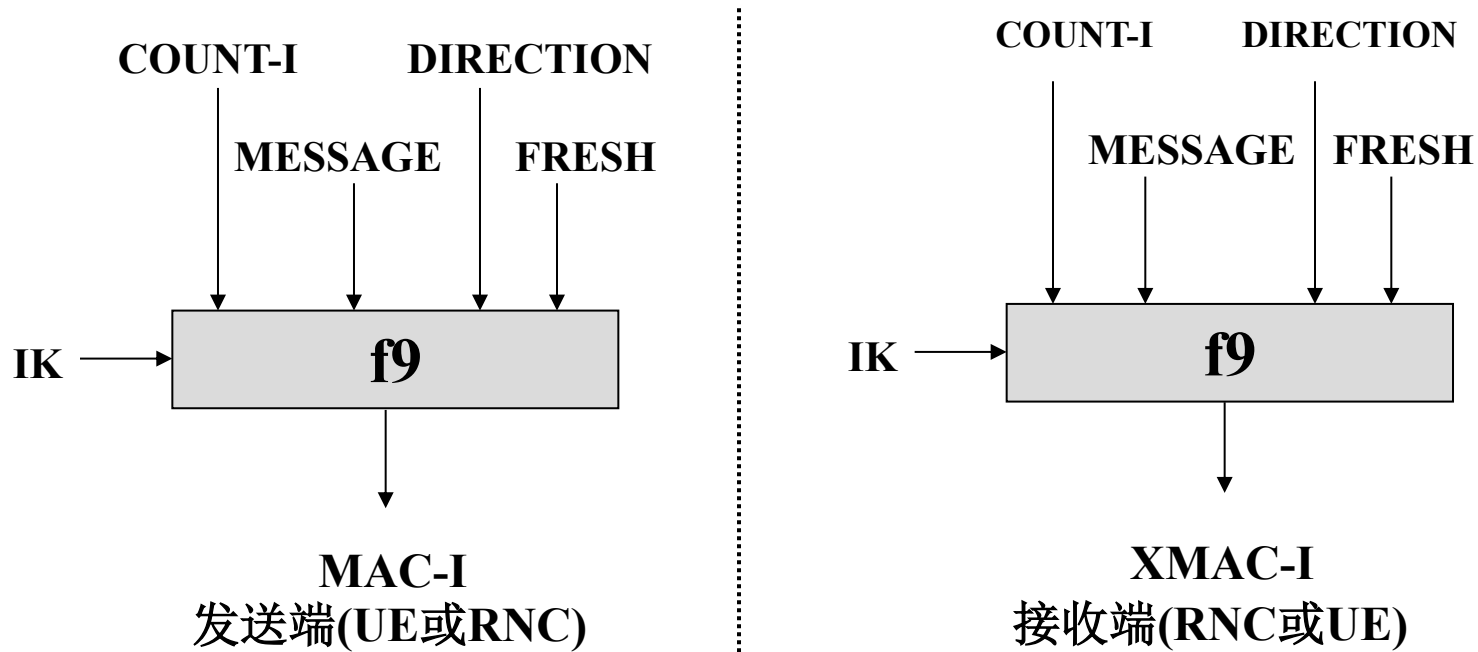
4. 接入域安全

空口的完整性机制

- 除12种信令信息外，其它信令信息都需要完整性保护
 - 完全切换到UTRAN。
 - 寻呼类型1。
 - 物理共享信道分配
 - RRC连接请求
 - RRC连接建立
 - RRC连接建立完成
 - . . .
- 完整性保护机制是基于消息认证码概念，完整性算法f9是由IK控制下的一个单向函数；
- 采用与加密算法同样的核心算法实现。
- 在终端和RNC中实现
 - “0001”，UIA1，基于Kasumi算法

4. 接入域安全

空口的完整性机制



IK (完整性密钥): 128比特
FRESH (新鲜值): 32比特
MESSAGE (信令消息): 消息长度
MAC-I/XMAC-I: 32比特

COUNT-I (完整性计数器): 32比特
DIRECTION (方向标识): 1比特

4. 接入域安全

Kasumi算法介绍

- 由日本三菱公司开发
- 在MISTY的基础上
- 分组密码（分组长度：64bit；密钥长度：128bit）
- 在不改变已证实的安全性的前提下，增加了额外的功能以使得密码分析更复杂
- 通过改进，简化了硬件实现，提高了计算速度

4. 接入域安全

Kasumi算法

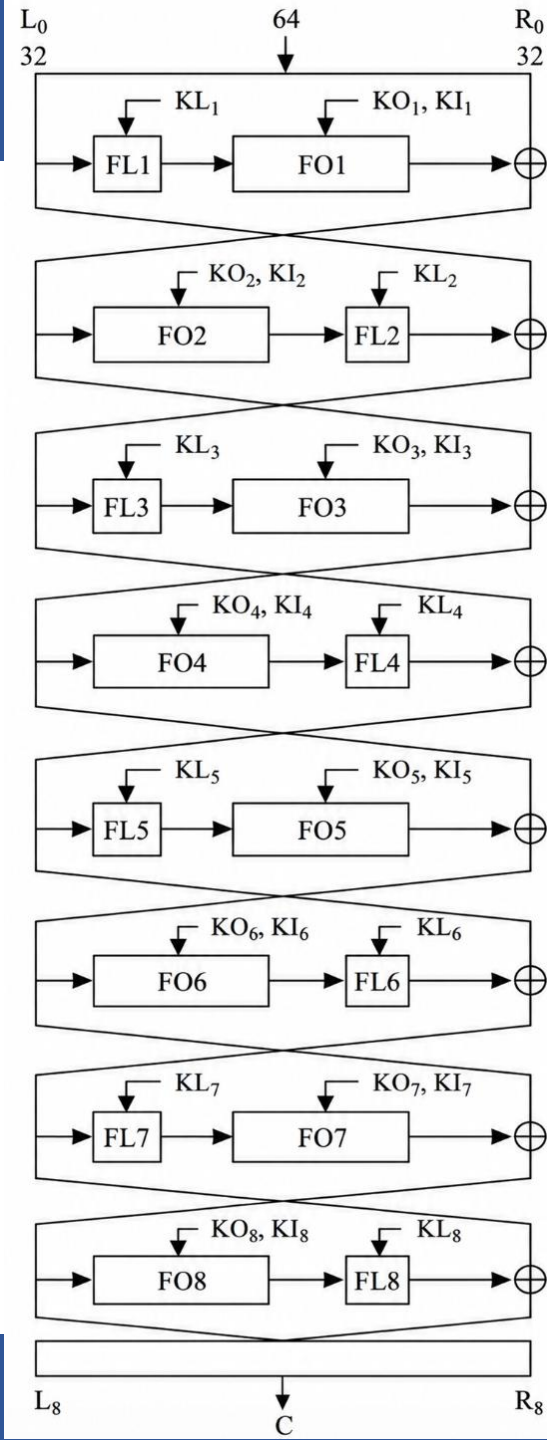
■ 变换原理:

第一步: 输入I被分为两个32比特序列 L_0 和 R_0 , 即 $I=L_0\parallel R_0$

第二步: 进入轮变换, 对每个 i , $1\leq i\leq 8$, 轮变换如下:

$$R_i=L_{i-1}; \quad L_i=R_{i-1}\oplus f_i(L_{i-1},RK_i)$$

第三步: 输出是8轮变换后的64比特的输出 $L_8\parallel R_8$ 。



4. 接入域安全

Kasumi算法流程

KASUMI算法轮函数fi

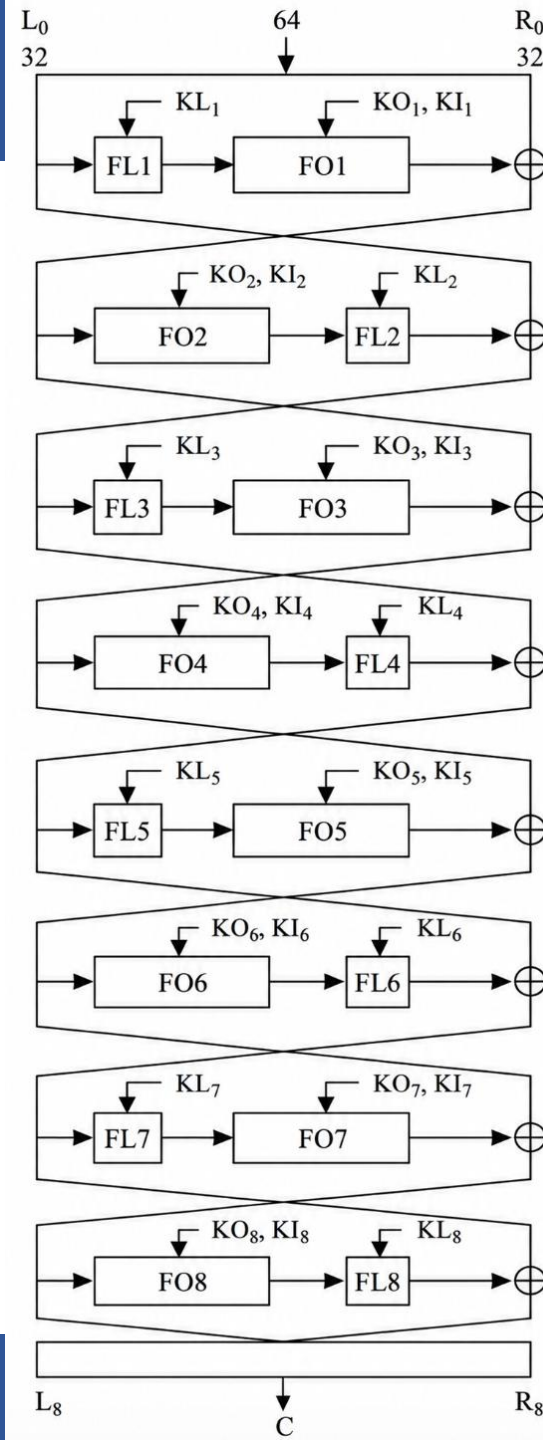
变化顺序为:

- 在第1、3、5、7轮，轮函数的变换顺序为:

$$fi(I, RK_i) = FO_i(FL_i(I, KL_i), KO_i, KI_i)$$

- 在第2、4、6、8轮，轮函数的变换顺序为:

$$fi(I, RK_i) = FL_i(FO_i(I, KO_i, KI_i), KL_i)$$



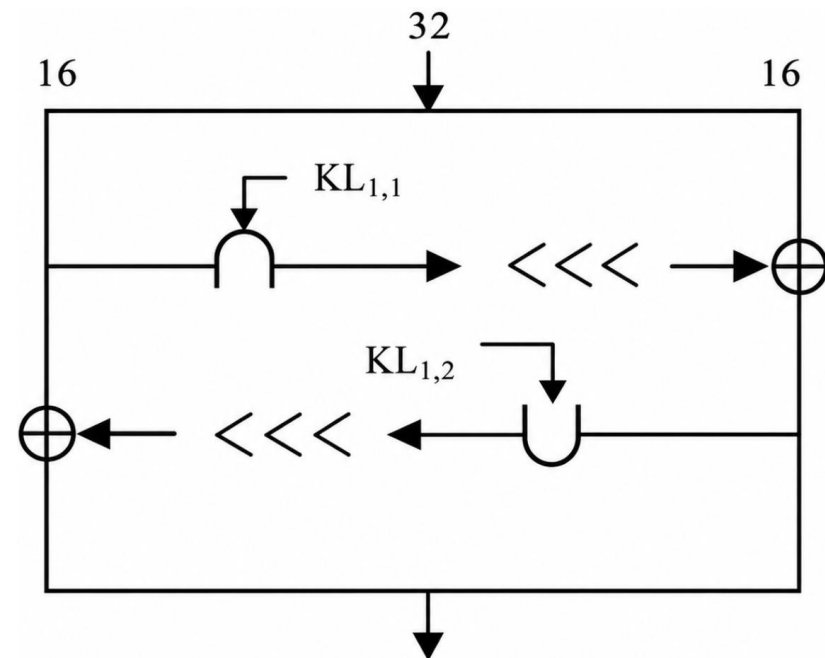
4. 接入域安全

KASUMI算法中子函数FL

- 设32比特的输入I分成两半即 $I := L || R$;
- 子密钥 KL_i 也分成两半,即 $KL_i := KL_{i,1} || KL_{i,2}$.
- 子函数FL的变换为:
 - $R' = R \oplus \text{ROL}(L \cap KL_{i,1})$
 - $L' = L \oplus \text{ROL}(R' \cup KL_{i,2})$

其中:

- $\text{ROL}(D)$: 数据块D向左旋转一位。
- $D1 \cup D2$: 数据块D1和D2按位或操作。
- $D1 \cap D2$: 数据块D1和D2按位与操作。



比特“与”操作



比特“或”操作



1比特的左循环

FL函数

4. 接入域安全

KASUMI算法中的子函数FO

变换原理:

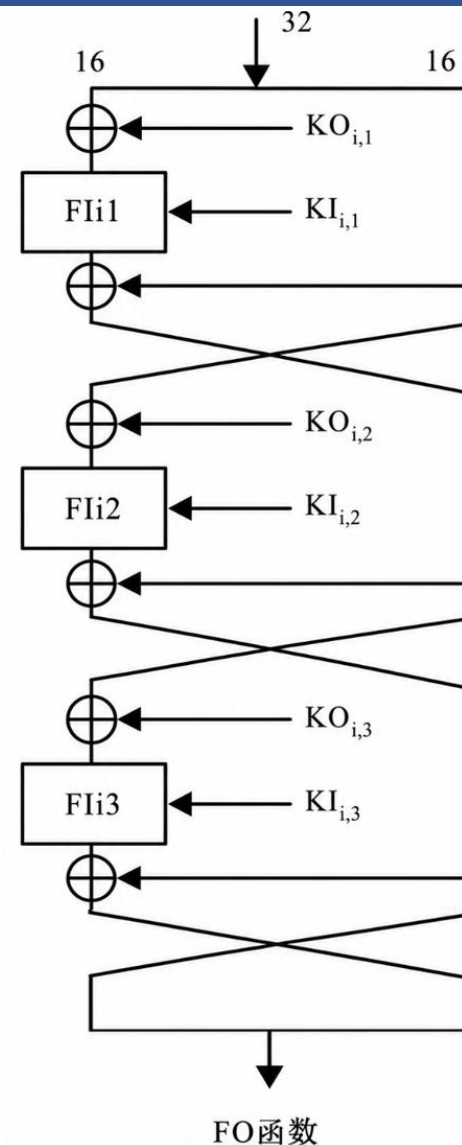
■ For(int j=1,j<=3,j++)

$$R_j = Fli_j(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$$

$$L_j = R_{j-1}$$

■ 其中输入I和子密钥 KO_i 和 KI_i 分为:

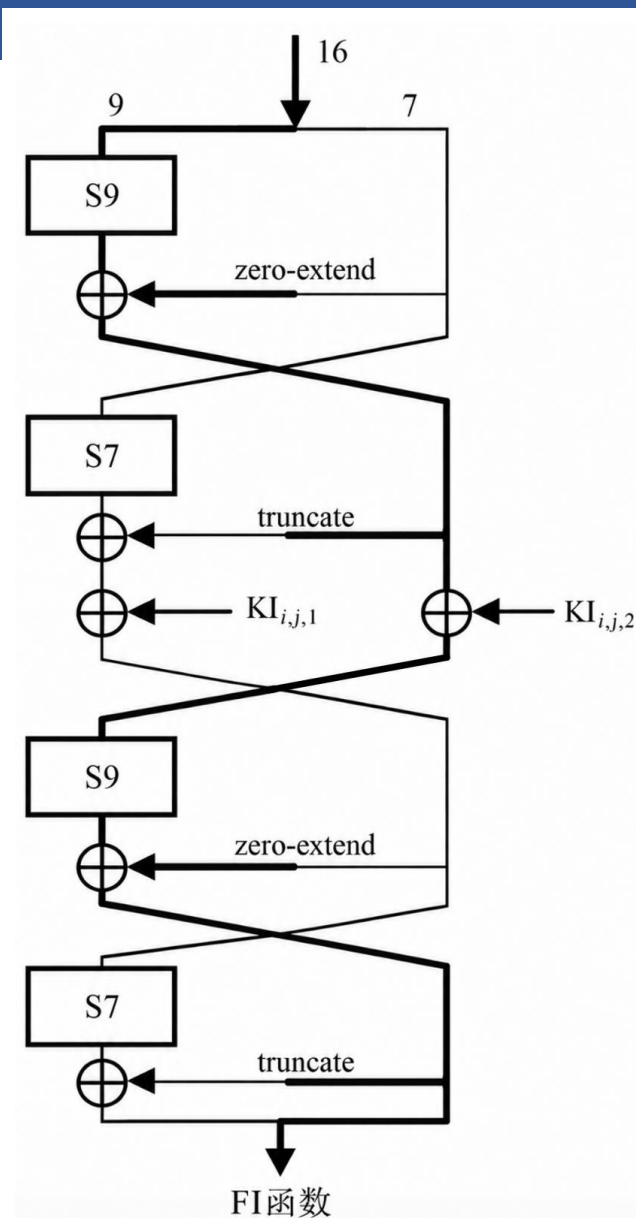
- $I := L_0 || R_0$
- $KO_i = KO_{i,1} || KO_{i,2} || KO_{i,3}$
- $KI_i = KI_{i,1} || KI_{i,2} || KI_{i,3}$



4. 接入域安全

KASUMI算法中的子函数FI

- 输入:16比特的I分成不相等的两部分,左边为9比特,右边为7比特,即 $I:=L_0\|R_0$.
- S9盒和S7盒
- 扩展函数ZE()和截短函数TR()
 - ZE(x):把长度为7比特的值x的最高位加上00序列转换成长度为9比特的值;
 - TR(x):去掉长度为9比特的值x的最高两比特序列转换成长度为7比特的值;



4. 接入域安全

KASUMI算法密钥扩展方案

- 128比特的密钥K分成8个16比特的密钥组:

$$K=K1\parallel K2\parallel K3\parallel K4\parallel K5\parallel K6\parallel K7\parallel K8$$

- K_i 与一个固定常数 C_i 异或, 即:

$$k_i'=k_i\oplus C_i, \text{ 从而得到 } K':$$

$$K'=K1'\parallel K2'\parallel K3'\parallel K4'\parallel K5'\parallel K6'\parallel K7'\parallel K8'$$

其中:

- $C1=0x0123, C2=0x4567, C3=0x89AB, C4=0Xcedf,$
- $C5=0Xfedc, C6=0xBA98, C7=0x7654, C8=0x3210$

4. 接入域安全

KASUMI算法密钥扩展方案(续)

- 轮密钥按如下表格取密钥值：
- 其中 $D \lll n$ 表示数据D向左旋转n位

	1	2	3	4	5	6	7	8
$KL_{i,1}$	$K1 \lll 1$	$K2 \lll 1$	$K3 \lll 1$	$K4 \lll 1$	$K5 \lll 1$	$K6 \lll 1$	$K7 \lll 1$	$K8 \lll 1$
$KL_{i,2}$	$K3'$	$K4'$	$K5'$	$K6'$	$K7'$	$K8'$	$K1'$	$K2'$
$KO_{i,1}$	$K2 \lll 5$	$K3 \lll 5$	$K4 \lll 5$	$K5 \lll 5$	$K6 \lll 5$	$K7 \lll 5$	$K8 \lll 5$	$K1 \lll 5$
$KO_{i,2}$	$K6 \lll 8$	$K7 \lll 8$	$K8 \lll 8$	$K1 \lll 8$	$K2 \lll 8$	$K3 \lll 8$	$K4 \lll 8$	$K5 \lll 8$
$KO_{i,3}$	$K7 \lll 13$	$K8 \lll 13$	$K1 \lll 13$	$K2 \lll 13$	$K3 \lll 13$	$K4 \lll 13$	$K5 \lll 13$	$K6 \lll 13$
$Kl_{i,1}$	$K5'$	$K6'$	$K7'$	$K8'$	$K1'$	$K2'$	$K3'$	$K4'$
$Kl_{i,2}$	$K4'$	$K5'$	$K6'$	$K7'$	$K8'$	$K1'$	$K2'$	$K3'$
$Kl_{i,3}$	$K8'$	$K1'$	$K2'$	$K3'$	$K4'$	$K5'$	$K6'$	$K7'$

4. 接入域安全

KASUMI的数学分析

■ 组件属性

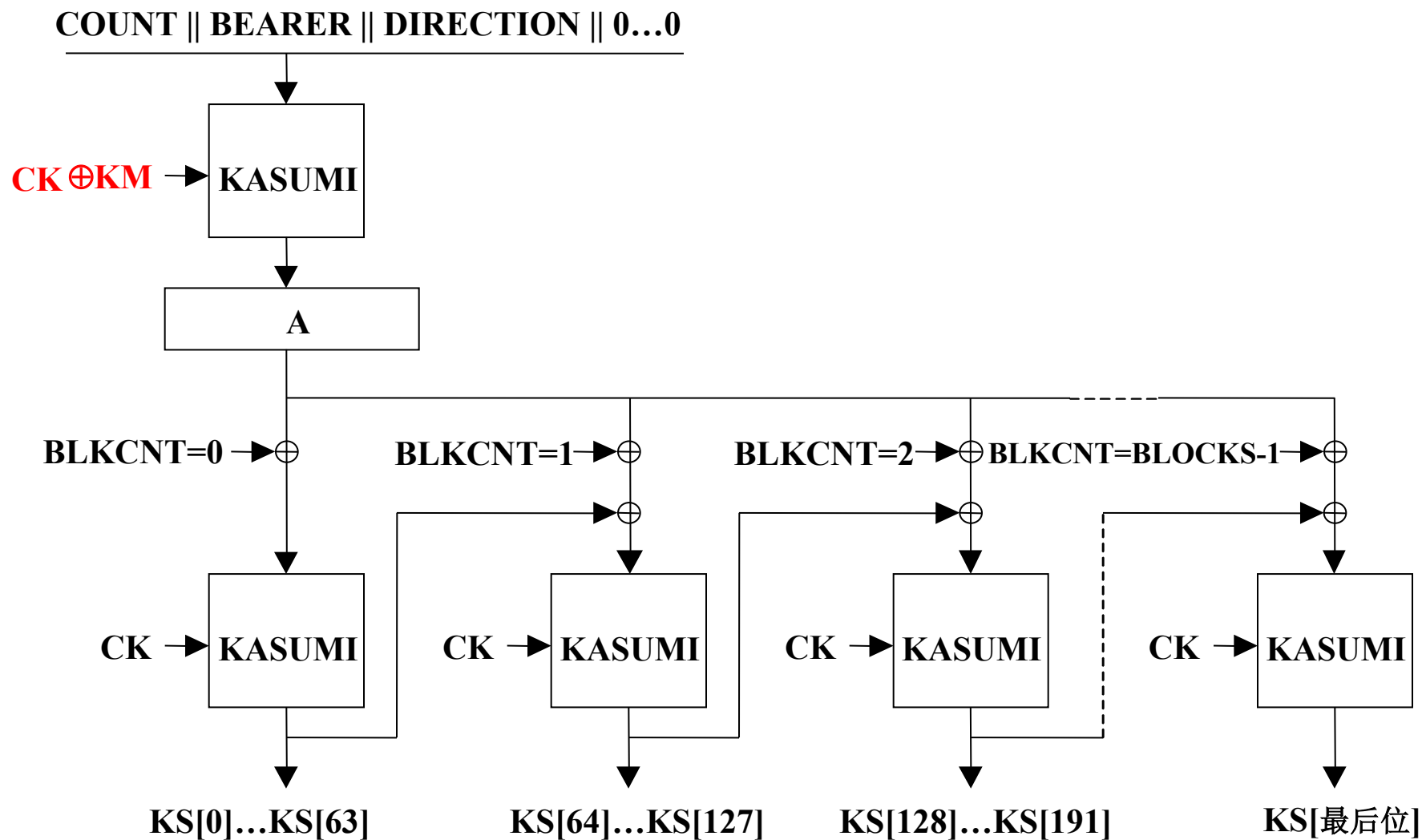
- FL函数是一个线性函数，输入微小变化在输出端也只引起微小的变化，目的是使单个的比特位在转换过程中更难被追踪。
- FI函数是KASUMI的基本随机函数，由两个非线性S-box S7和S9的4次循环结构组成。S7和S9的使用避免了FI中出现线性结构；
- FO的作用和FI一样，通过在函数中增加循环来改善它的耗散特性，从而通过在复杂性和功率消费上的开销来提高KASUMI算法的总体安全系数。
- S7和S9使算法获得非线性特征，从而抵抗线性/差分攻击。
- 密钥安排简单，且没有发现会产生任何实际的漏洞；其中使用的常量C1~C8,使得连续的循环密钥之间没有固定重复的关系，可用来防范选择明文攻击。

KASUMI的数学分析（续）

- 密码分析
 - 差分选择明文攻击
 - 相关密码差分攻击
 - 不可差分
 - 截短差分
 - 线性密码分析
 - 高阶差分攻击

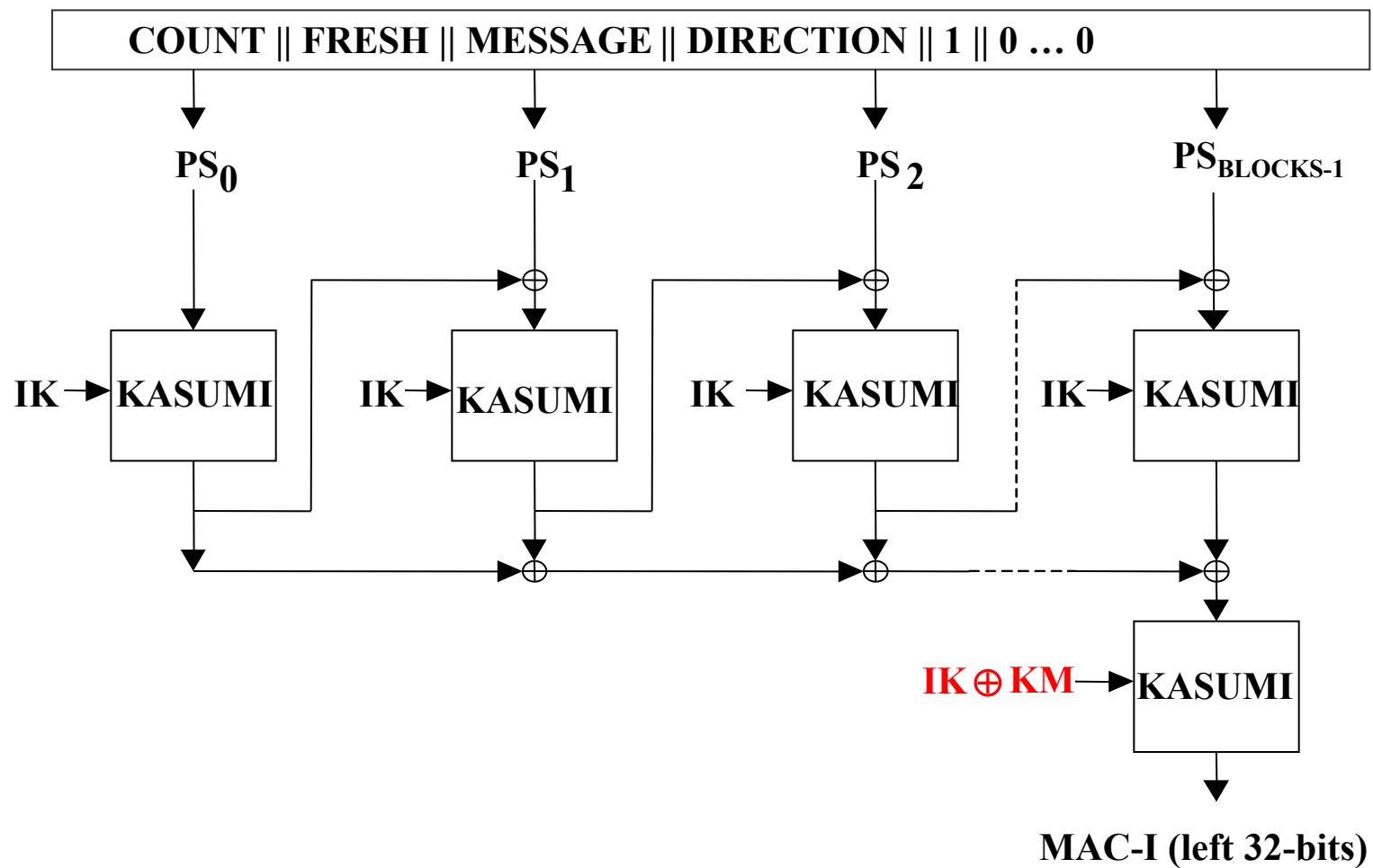
4. 接入域安全

基于Kasumi的f8算法



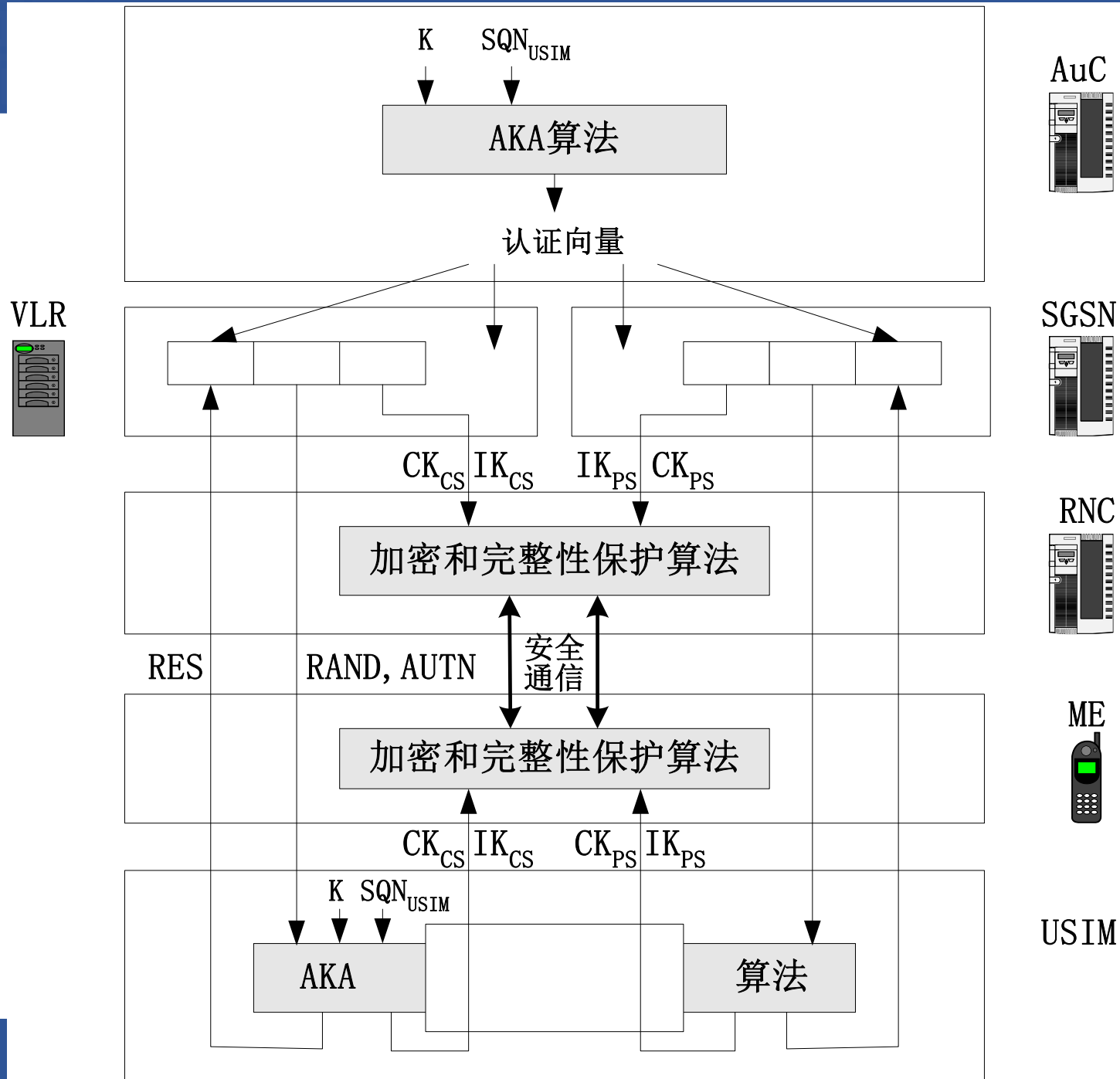
4. 接入域安全

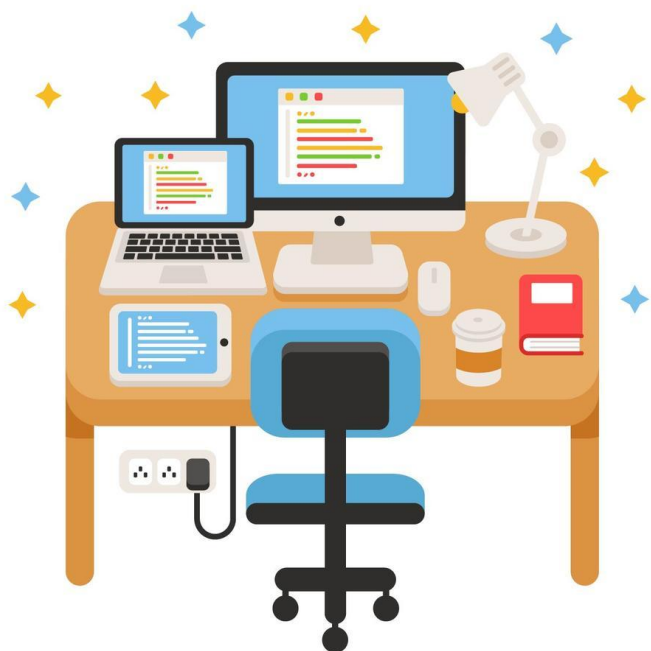
基于Kasumi的f9算法



4. 接入域安全

小结





1. 3G通信技术简介
2. 安全原则和安全目标
3. 安全体系结构
4. 接入域安全
- 5. 网络域安全**
6. 结论

什么是网络域安全

- 网络域内的安全主要指的是在AN、SN及CN中的网络实体之间的信令、数据的安全传输
 - 不包括用户设备
 - 网元可能处于同一个网络下，被统一的移动网络管理系统所管理；也可能分属于不同的网络

5. 网络域安全

网络域安全的必要性

- 过去
 - 网络域内无可用的安全机制
 - 基于全球**7**号信令网的封闭性
- 现在
 - 运营商和业务商需要互连互通
 - 基于**IP**的网络代替了基于**7**号信令的网络
 - 核心网络中的重要信息
 - 密钥和认证数据

5. 网络域安全

网络域安全的主要机制

■ MAPsec

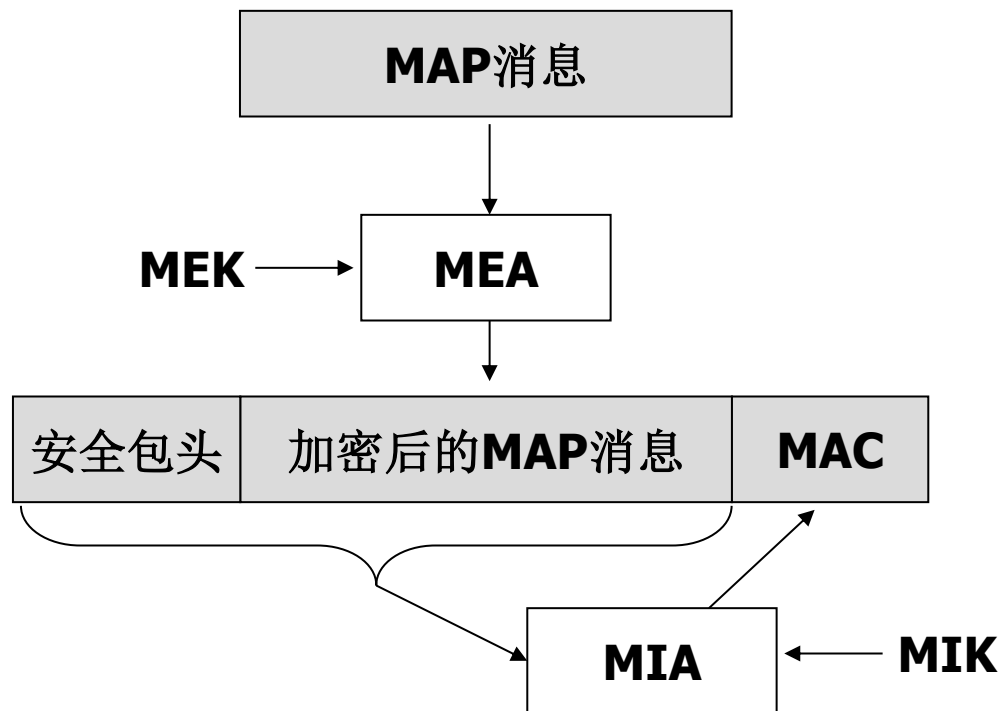
- MAP (Mobile Application Part) 移动应用部分：是SS7信令中专述移动通信的部分
- 对一个明文的MAP消息进行保护

■ IPsec

- 通过对IP层进行保护来实现对敏感信息的安全传输
- 能够保护更低层的消息头

MAPsec基本原理

- 加密算法
 - MEA, 计数器模式下的AES算法
 - MIA, CBC-MAC模式下的AES算法
- 保护模式
- 密钥管理



5. 网络域安全

MAPsec基本原理

■ MAPsec的三种保护模式

- 模式0：不提供保护
- 模式1：提供完整性保护
- 模式2：不但提供完整性保护而且提供加密

■ 安全包头结构：

SPI	Original component ID	TVP	NE-ID	Prop
------------	------------------------------	------------	--------------	-------------

- **SPI**（安全参数索引），与目标**PLMN ID**一起指向一个唯一的**MAPsec安全关联**；
- **OriginalcomponentID**：原始MAP消息的类型，以便接收方能够正确处理MAP消息
- **TVP**（时变参数）：是一个32比特的时间戳，用来抵御重放攻击
- **NE-ID**：网元标识，用于在同一时间戳内不同的网元可以产生不同的IV
- **Prop**：所有权域，用于在同一时间戳内在加密不同的Map消息时产生不同的IV

安全关联（**Security Association, SA**）是通信双方之间建立的一组安全参数和状态信息，用于定义安全通信所采用的加密算法、完整性算法、密钥及相关安全属性。

5. 网络域安全

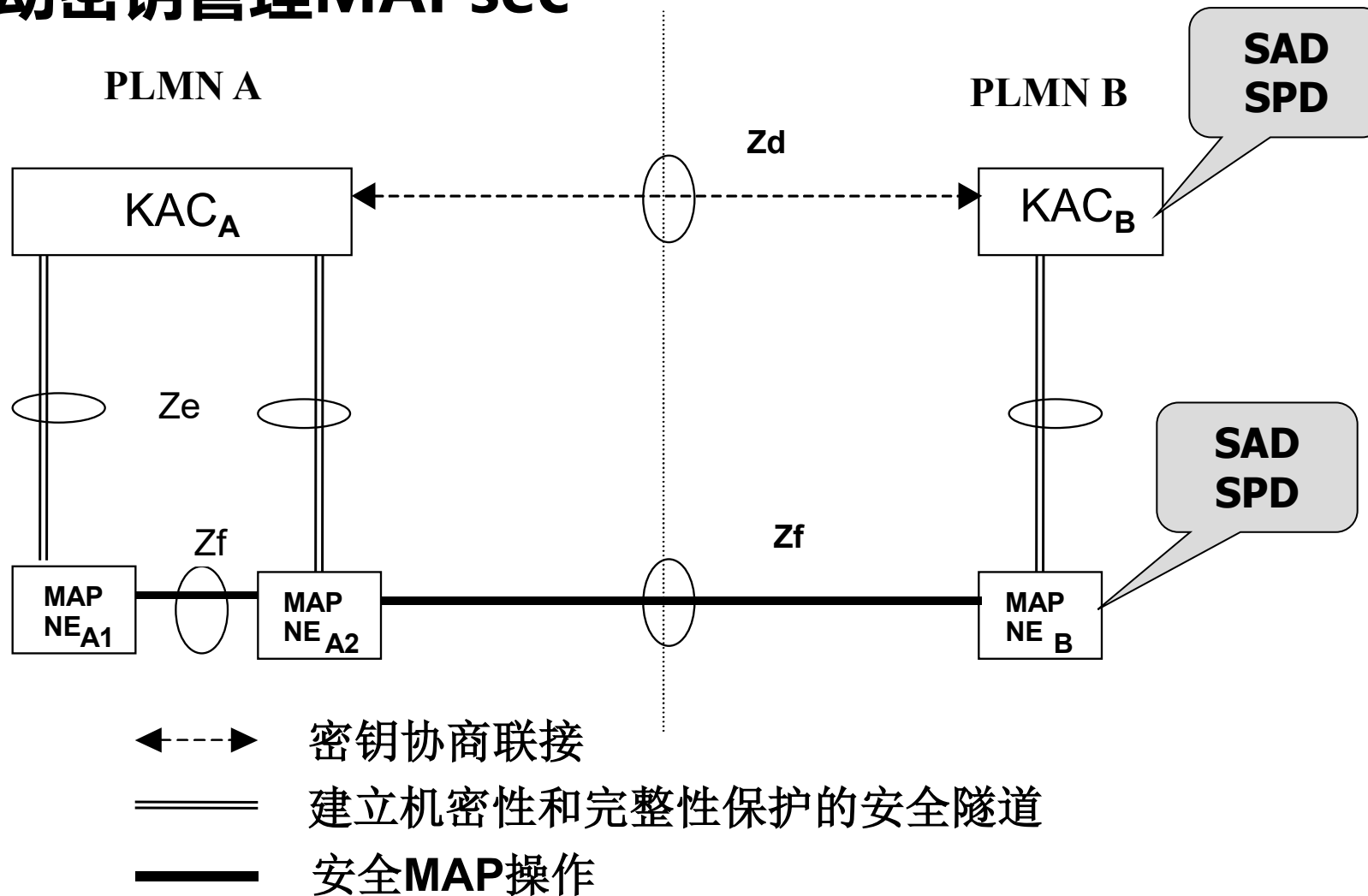
MAPsec基本原理

■ 安全关联（SA）

- 目的PLMN ID：目标公众陆地移动通信网标识，接收网络的国家代码MCC|网络代码MNC；
- 安全参数索引（SPI）：与目标PLMNID一起指向一个唯一的MAPsec安全关联；
- 发送PLMN ID：发送公众陆地移动通信网标识，发送网络的国家代码MCC|网络代码MNC；
- MAP加密密钥（MEK）
- MAP加密算法标识（MEA）
- MAP完整性密钥（MIK）
- MAP完整性算法标识（MIA）
- 保护轮廓ID(PPI)：用于标识 MAPsec 所采用的安全保护轮廓，即具体的安全机制和算法组合；
- 保护轮廓修订ID(PPRI)：用于标识该保护轮廓的修订版本；
- 软有效时间：SA针对出站流量的软失效时间。到达该时间后，SA 仍可暂时使用，但应协商新SA；
- 硬有效时间：SA的实际失效时间。到达该时间后，必须停止通信或重新协商新SA；

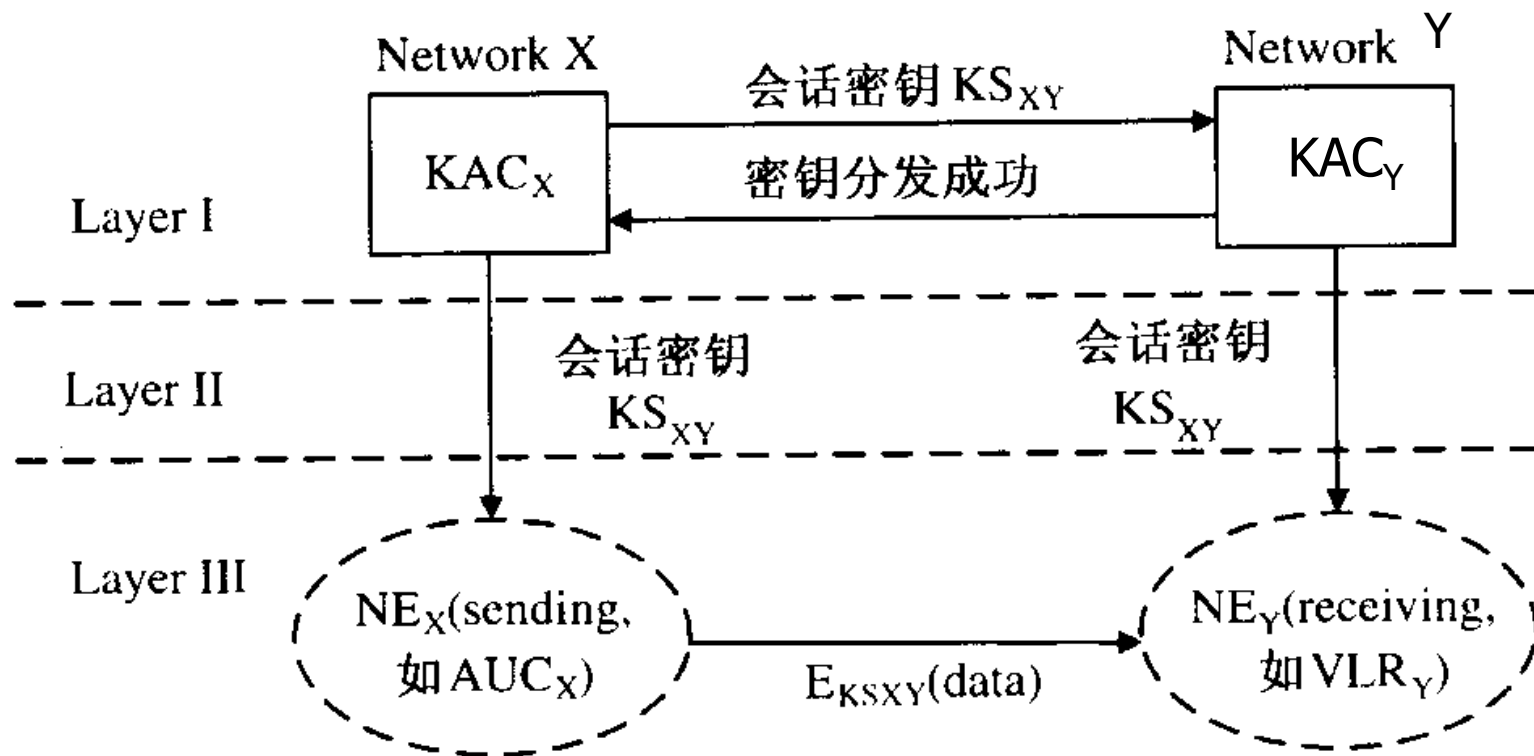
5. 网络域安全

3G网络域自动密钥管理MAPsec



5. 网络域安全

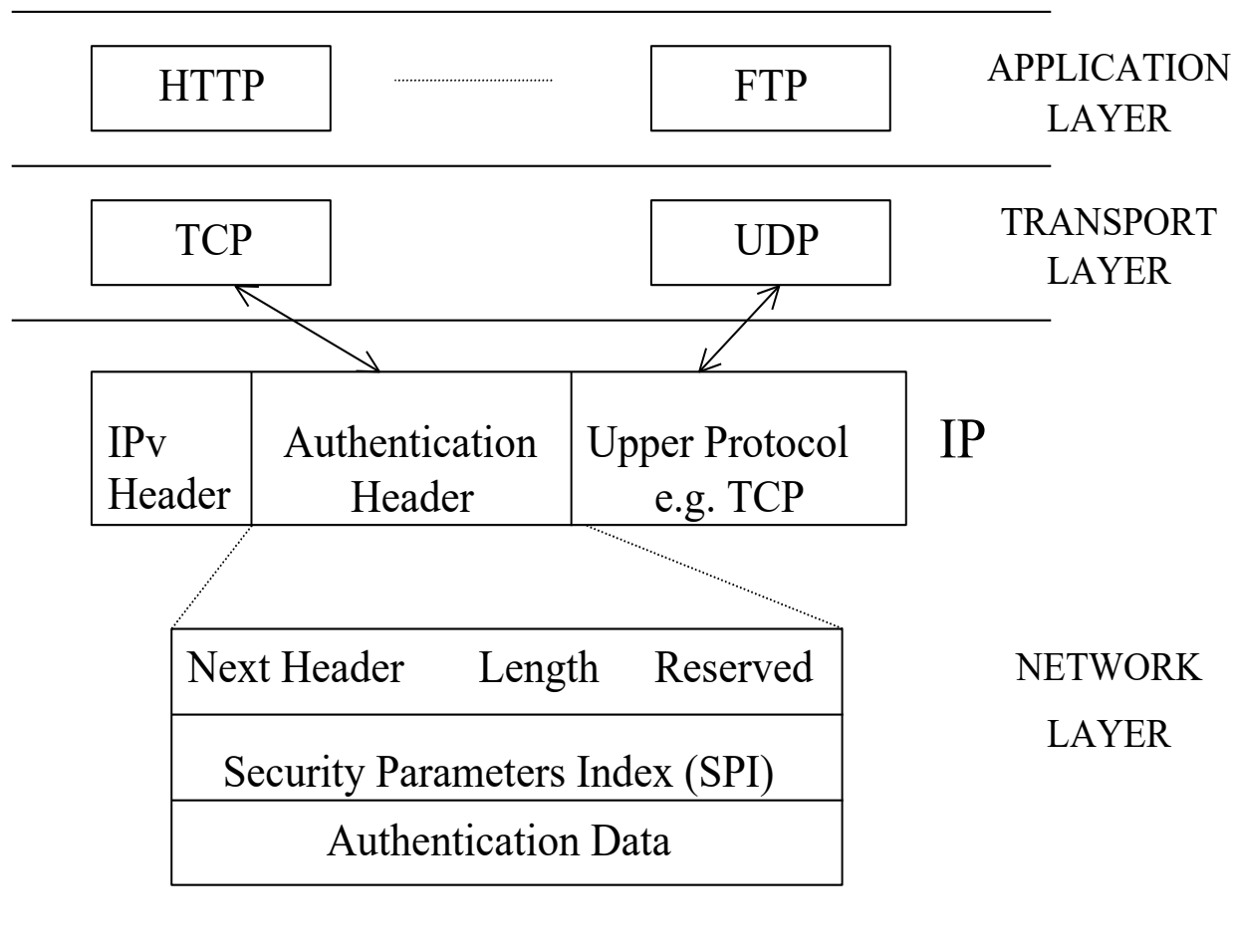
MAPsec机制的安全模型



5. 网络域安全

IPsec机制概述

- 在IP层上对通信进行保护
- IPsec的工作方式
 - 认证头 (AH)
 - 封装安全性负载 (ESP)
- 安全关联
 - 认证算法 (AH/ESP中)
 - 加密算法 (ESP中)
 - 加密和认证密钥
 - 加密密钥的生存时间
 - 安全关联本身的生存时间
 - 重放攻击序列号
- 密钥协商
 - IKE (密钥交换协议)



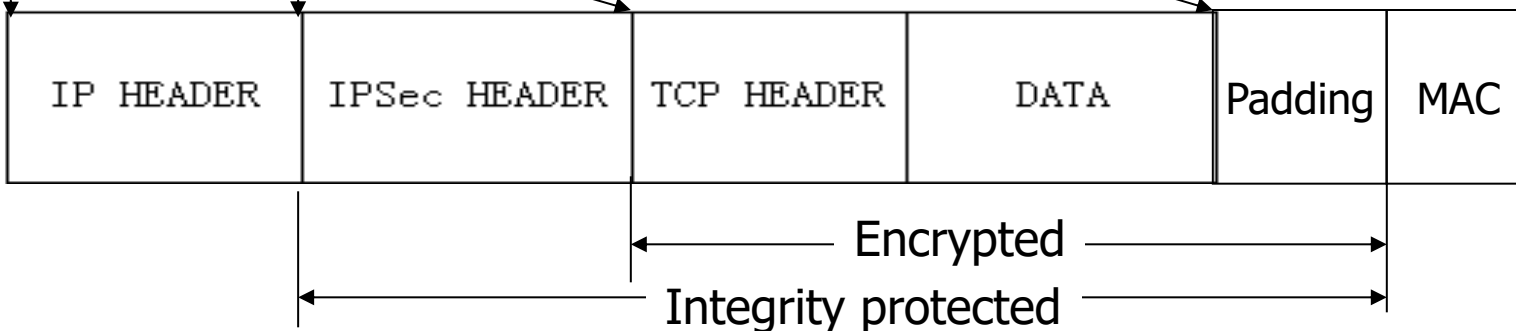
5. 网络域安全

封装安全性负载 (ESP) 协议

原始IP包



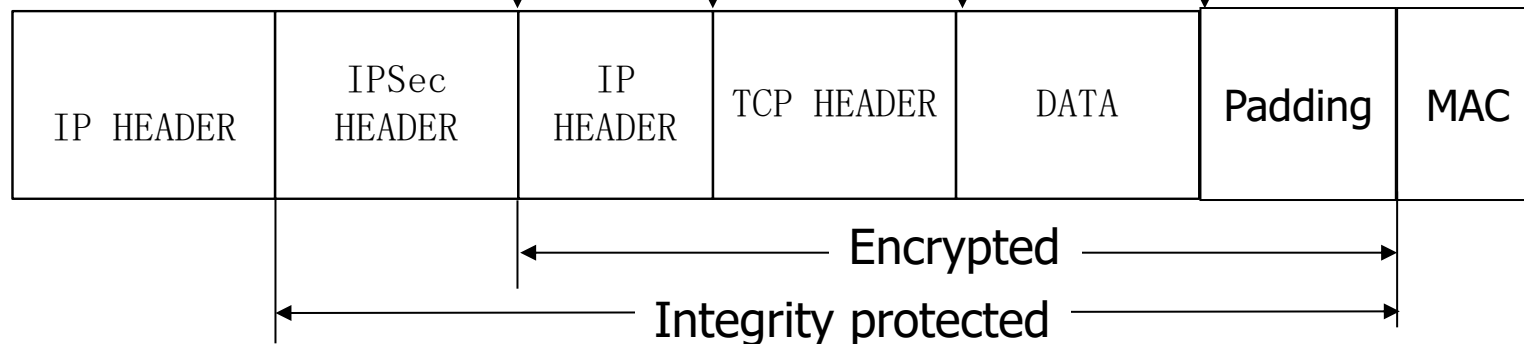
传输模式
IPSec包



原始IP包

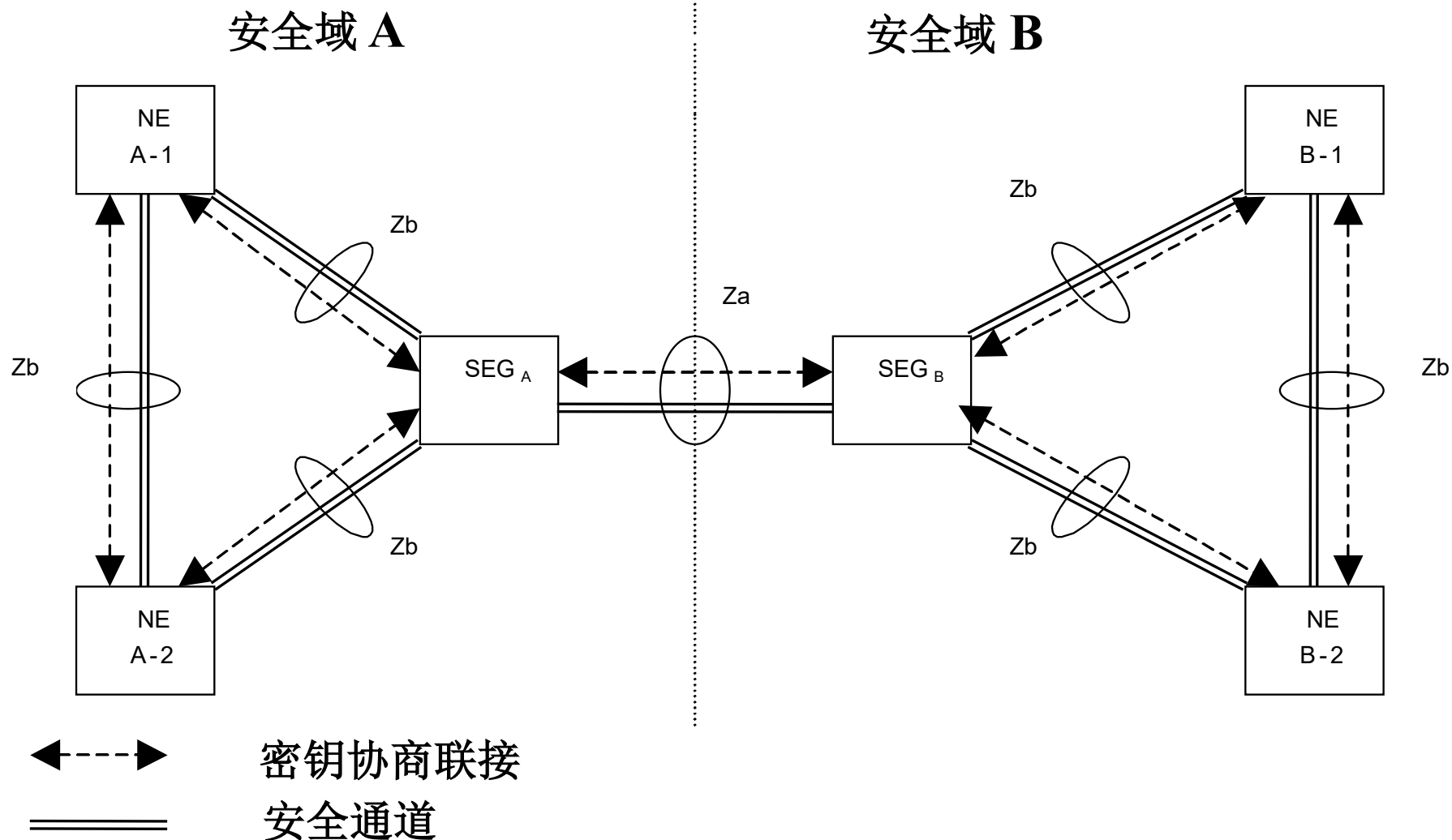


隧道模式
IPSec包



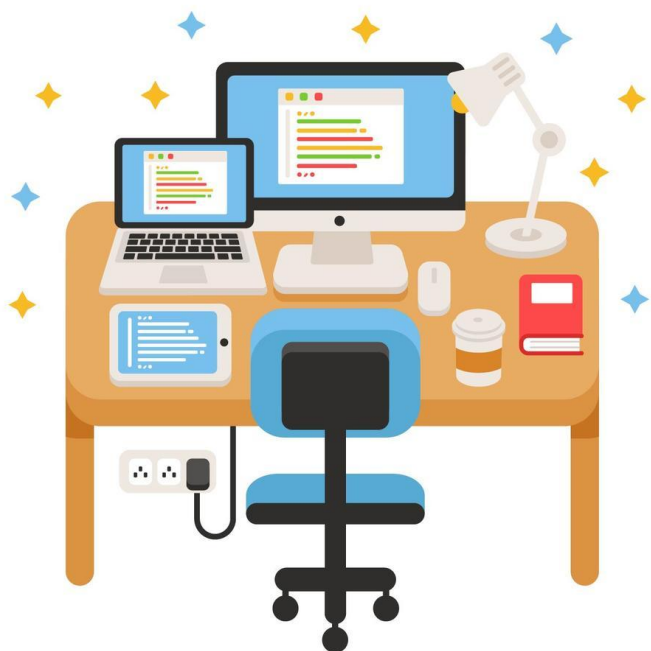
5. 网络域安全

3G网络域安全 IP核心网



其它的网络域安全技术

- 公共密钥基础设施PKI
- AAA
- 防火墙技术



1. 3G通信技术简介
2. 安全原则和安全目标
3. 安全体系结构
4. 接入域安全
5. 网络域安全
- 6. 结论**

6. 结论

- 与GSM系统相比：
 - 双向身份认证
 - 算法经过公开评估
 - 密钥长度增加，可以采用高强度的加密算法和完整性算法
 - 提出了保护核心网络节点之间通信的机制
 - 3G提供了比2G系统更高的安全特征
- 缺陷
 - IMSI泄露
 - 用户数据缺乏完整性保护
 - 缺少端到端的安全保护方法

1. 描述AKA协议，列出其安全目标，并分析其安全目标是否可以达到？
2. 描述WCDMA系统在接入域中如何保证信息传输的机密性和完整性的。
3. 举例解释下面名词：
 - 安全域
 - 安全关联

3G移动通信安全相关标准

- **TR 33.900 A Guide to 3rd Generation security**
- **TS 33.120 Security principles and objectives**
- **TS 21.133 Security threats and requirements**
- **TS 33.102 Security architecture**
- **TS 33.103 Integration guidelines**
- **TS 33.105 Cryptographic algorithm requirement**
- **TS 35.201 f8 and f9 specification**
- **TS 35.202 KASUMI specification**
- **TS 35.203 Implementors' Test data**
- **TS 35.204 Design conformance test data**
- **TR 33.909 Report on evaluation of 3GPP algorithm**

Thank You !

