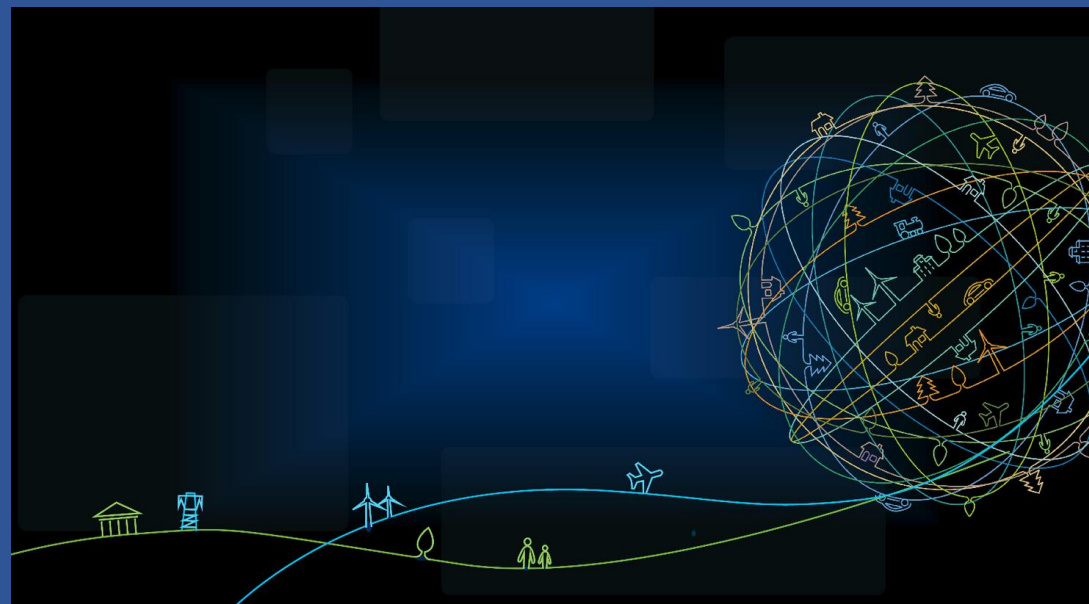


课程编号: 3182121321

无线通信安全



第五讲 数字保密通信与GSM安全

李晖

lihuill@bupt.edu.cn

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY
RESOURCE CENTER
CSRC

UPDATES

2026

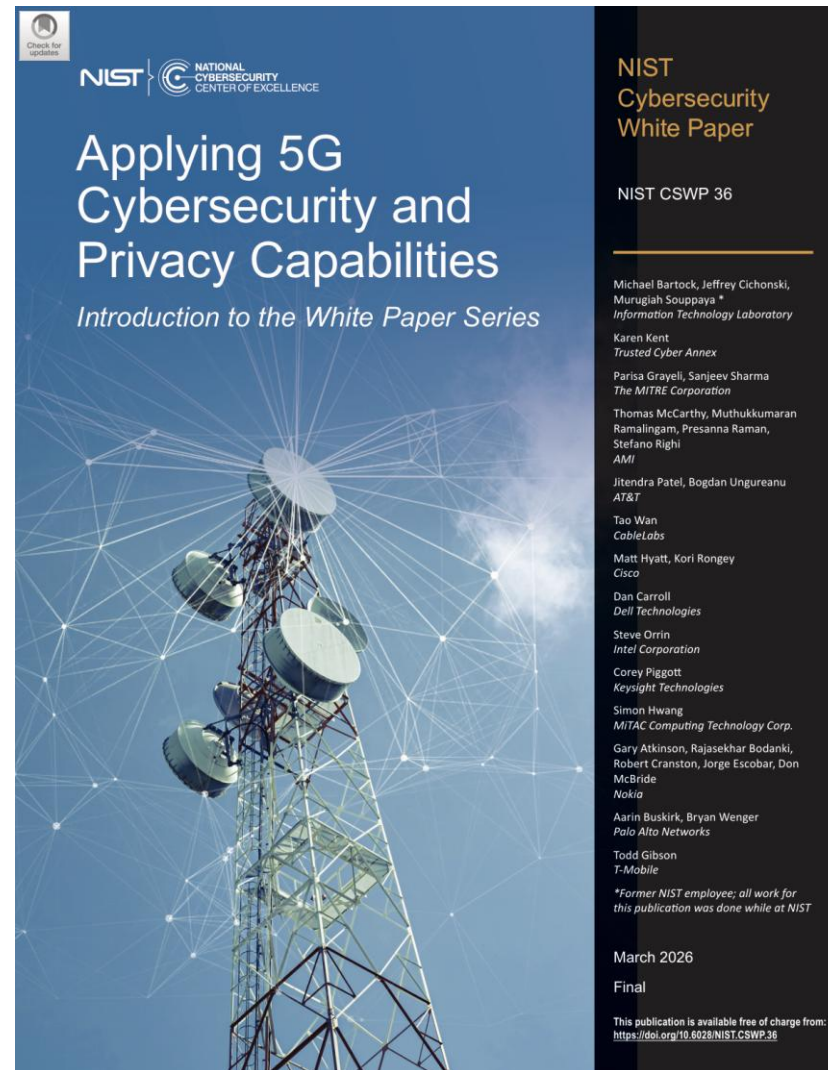
The NIST NCCoE releases "Applying 5G Cybersecurity and Privacy Capabilities" white paper series

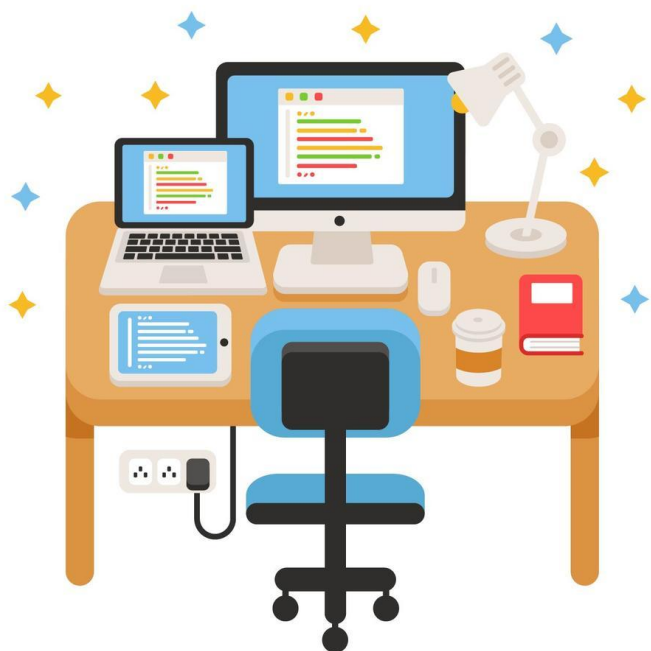
March 19, 2026

NIST公布5G网络安全与隐私能力白皮书

- **NIST CSWP 36: 5G 网络安全与隐私能力的应用**
- **NIST CSWP 36A: 利用用户加密标识（**SUCI**）保护用户标识**
- **NIST CSWP 36B: 利用硬件增强安全保障5G系统平台完整性**
- **NIST CSWP 36C: 临时身份标识的重新分配**
- **NIST CSWP 36D: 禁止基于**SUPI**的寻呼机制**
- **NIST CSWP 36E: 5G网络安全设计原则**

5G安全落地强调身份隐私、平台可信与网络架构安全





1. 数字保密通信
2. GSM简介
3. GSM系统安全目标
4. GSM系统安全机制
5. GSM系统安全缺陷

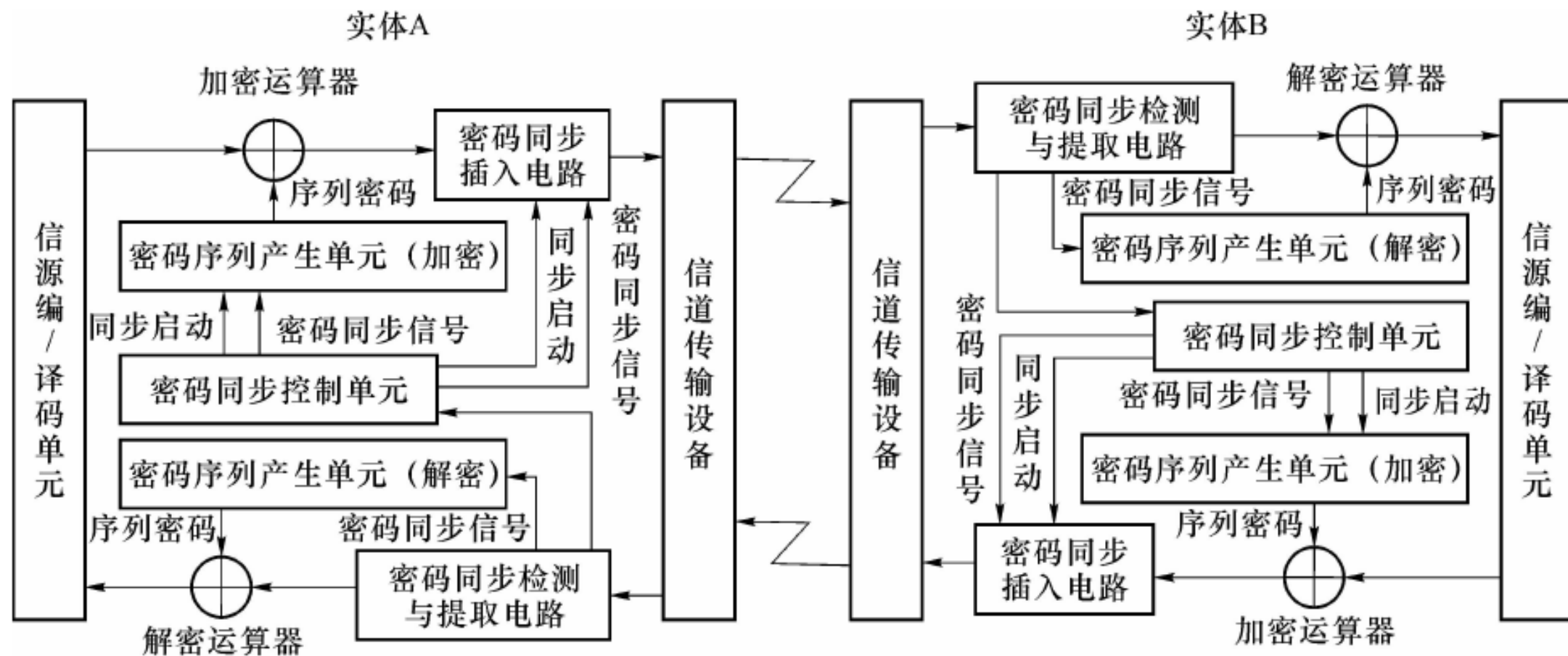
基本概念

- 数字保密通信系统：在一般数字通信系统基础上新增安全功能
- 目的：防止窃听、防止信息被篡改等
- 主要内容：
 - 通信实体的认证
 - 保密性
 - 完整性
 - 不可否认性
 - 密钥管理
 - 密码协议

关键技术

- 加解密技术是实现通信内容保密性的基本技术。
- 数字签名、散列函数、单向函数等都是实现通信内容的完整性和不可否认性的基本密码算法。
- 通信实体认证是对通信对象的确认过程，即身份认证，使用的主要密码算法包括散列函数、数字签名等。
- 密钥管理和分配技术是信息保密性、完整性、身份认证的核心，通常由认证中心（**CA**）、或分层的密钥管理思想来实现。这一般是通信安全中最易被攻击的环节。
- 密码协议与具体的密码应用紧密结合，为特定的密码应用提供安全规范。

基于序列密码的典型保密数字通信系统原理



采用的密码体制

■ 分组密码体制

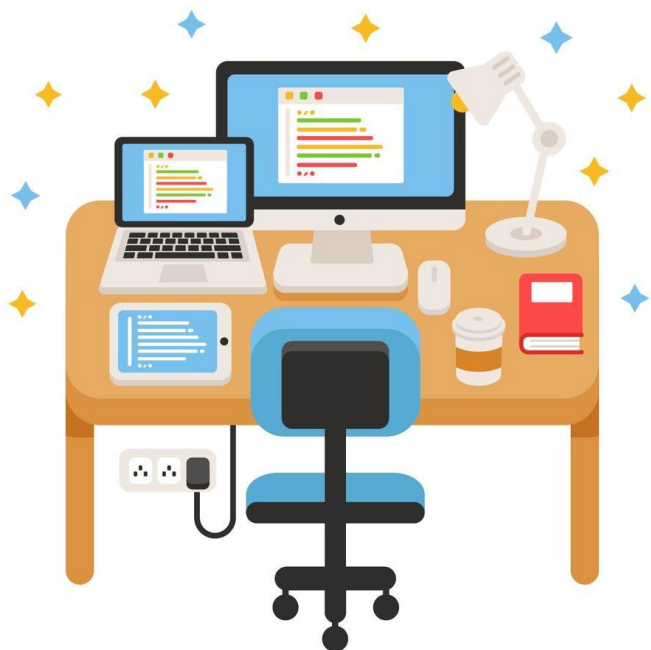
- 特点：存在误码扩散和一定的时延
- 一般应用于传输信道较好和具有数据重发功能的场合

■ 序列密码体制

- 特点：具有良好的低时延、无误码扩散

■ 非对称密码体制

- 特点：计算量大，难以满足实时性要求；对设备计算能力要求高
- 在计算机通信网络中应用广泛，其他数字通信系统中还没有广泛应用



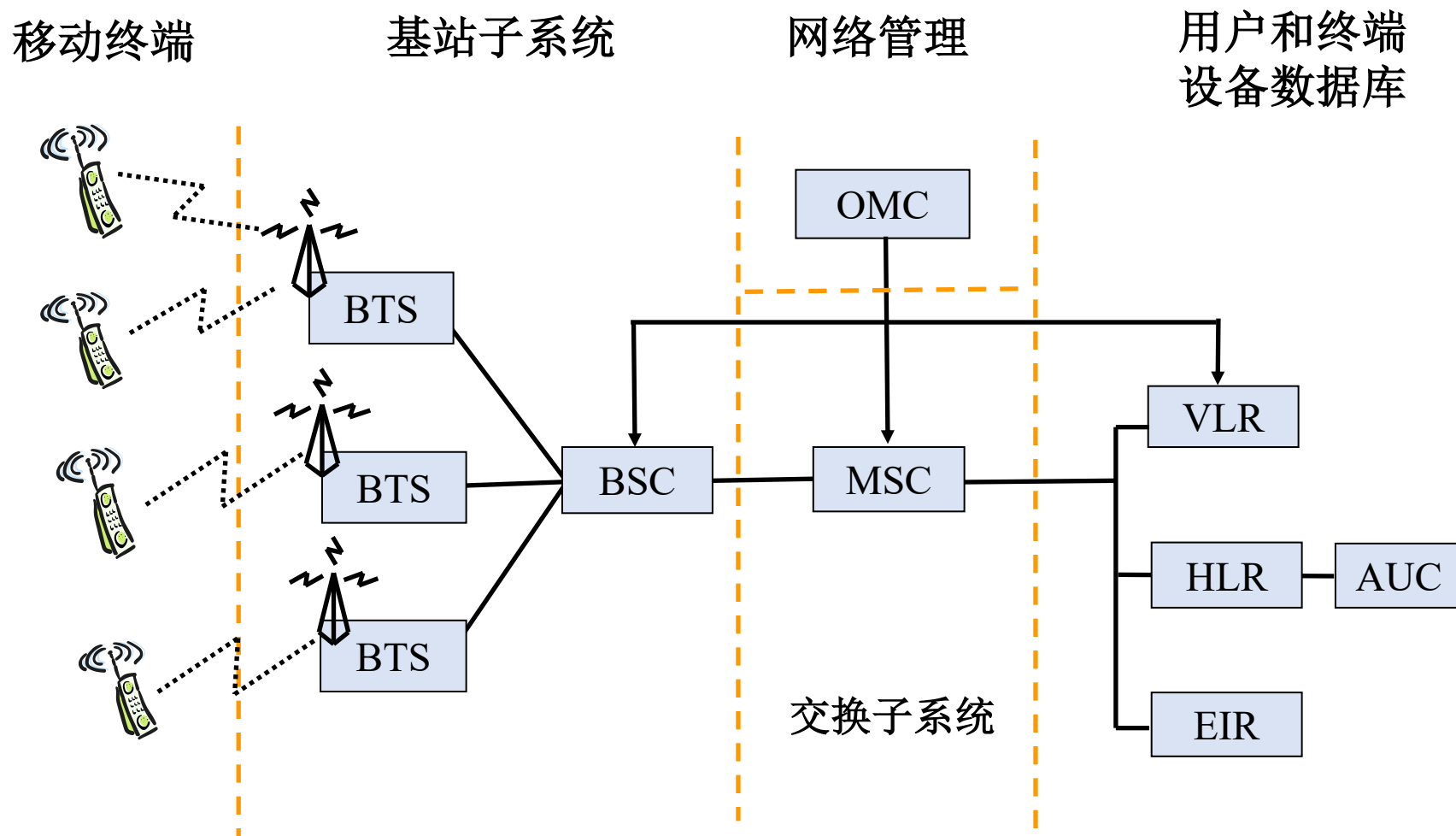
1. 数字保密通信
2. **GSM简介**
3. GSM系统安全目标
4. GSM系统安全机制
5. GSM系统安全缺陷

简介

- **Global System for Mobile Communications**
- 中文：全球移动通信系统
- 由ETSI制定的规范
- 采用数字蜂窝通信技术
- 高可移动性 (支持国际漫游)
- 服务
 - 基本服务：语音和短数据通信
 - 增值业务：呼叫等待，呼叫转移等
 - 承载业务：电路交换数据(包交换数据with GPRS)

2 GSM简介

GSM系统网络结构



网络数据库

- 用于认证和安全功能的相关数据库
 - **HLR**：保存每个GSM注册用户的所有管理信息和MS的位置信息
 - **VLR**：存储不在归属网络中的用户信息，从而使网络可以知道MS所在位置
 - **EIR**：存储一组MS的IMEI列表
 - 白名单- 允许连入网络名单
 - 灰名单-可疑用户名单
 - 黑名单- 不允许连入网络名单
 - **AUC**：存储用户关键安全信息
 - **IMSI**: International Mobile Subscriber Identity
 - **LAI**: Location Area Identity
 - **Ki**: Authentication Key

2 GSM简介

物理信道和逻辑信道

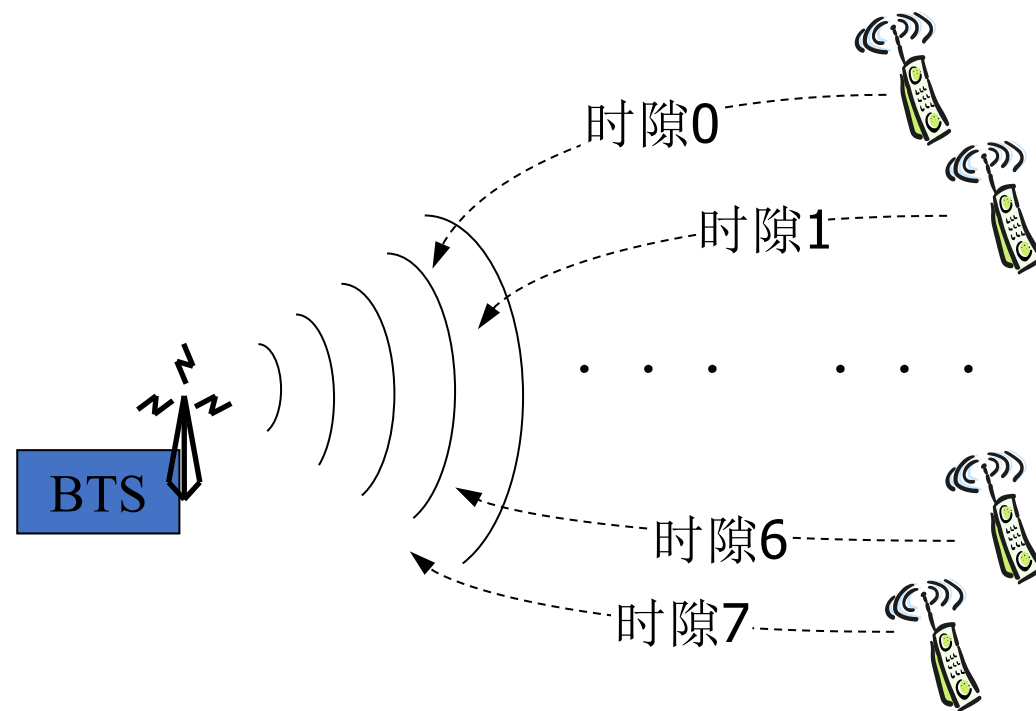
■ 物理信道

■ 频分多址接入 (FDMA)

- 在GSM900频段的上行（从MS到BTS）
890 ~915MHz或下行（从BTS 到MS）
935 ~960MHz频率范围内分配了124个载波频率，简称载波。
- 上行与下行载波是成对的，即是所谓的双工通信方式。
- 双工收发载频对的间隙为**45MHz**。

■ 时分多址接入 (TDMA)

- 每个载频上按时间分为8个时间段，每一个时隙段称为一个时隙（slot）
- 这样的时隙叫做信道，或物理信道。



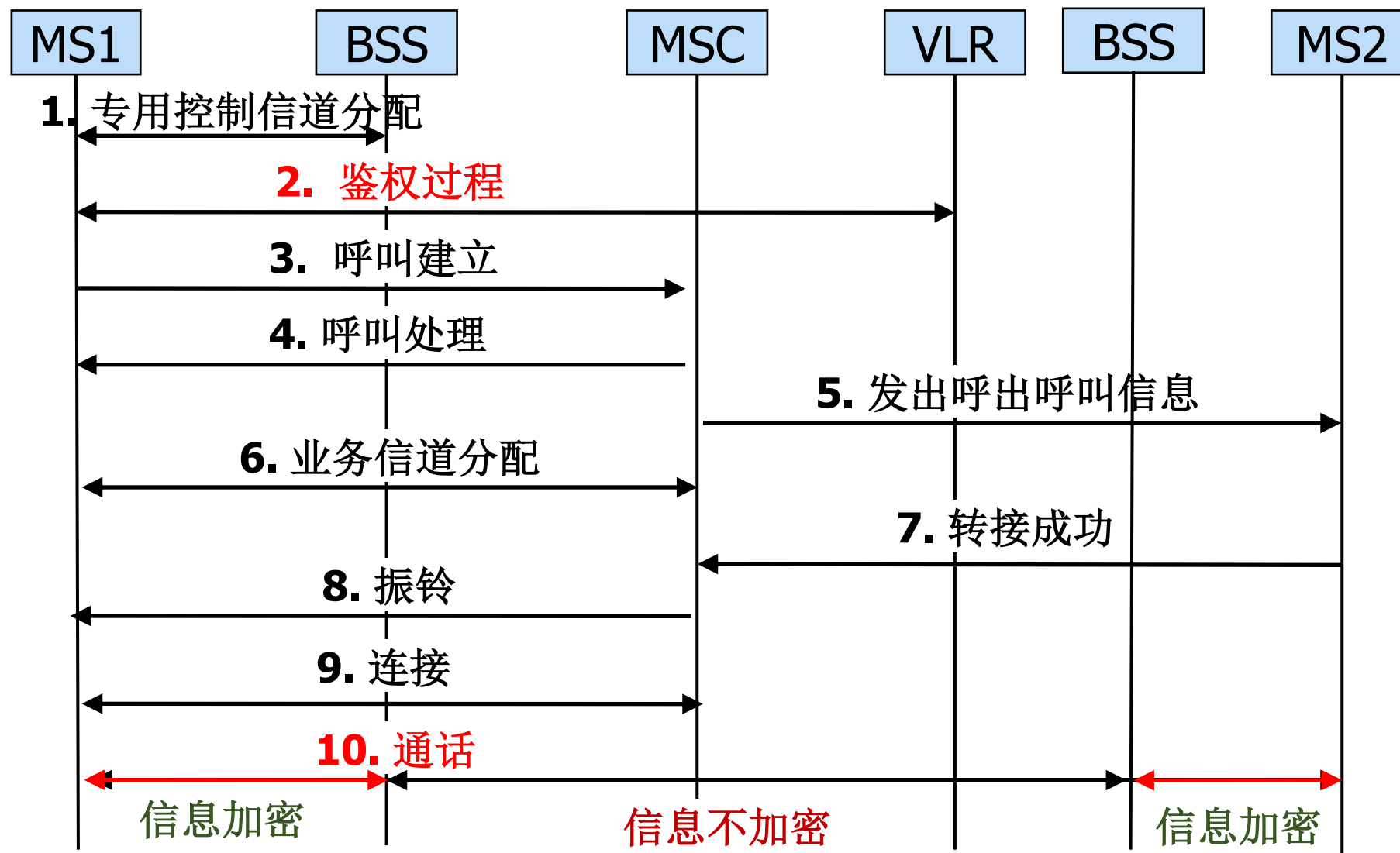
2 GSM简介

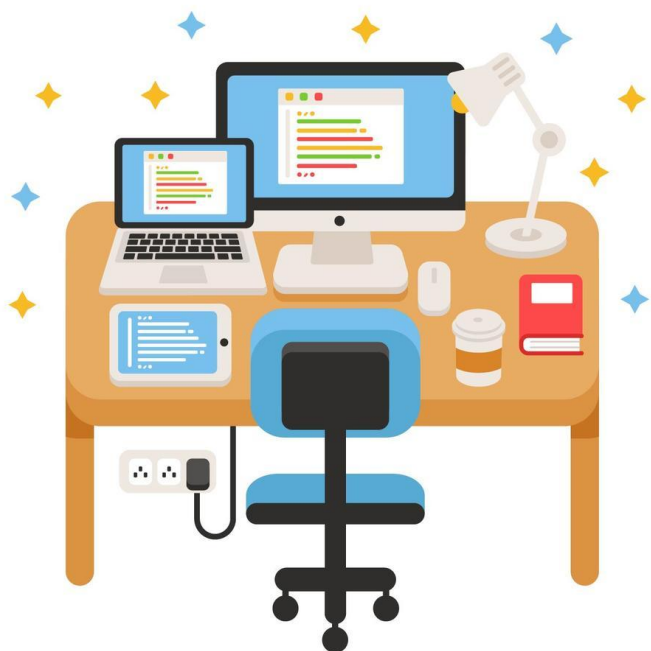
物理信道和逻辑信道

- **逻辑信道：** 依据物理信道传输的内容划分的逻辑上的信道
 - **公共信道**
 - **广播信道：** 传送基站向移动台广播消息
 - 频率校正信道、同步信道、广播控制信道
 - **公共控制信道：** 传送业务交换中心与移动台之间建立连接所需的双向信号
 - 寻呼信道、随机接入信道、接入允许信道
 - **专用信道**
 - **专用控制信道：** 传送一些用于控制某个用户的控制信息
 - 独立专用控制信道、慢速随路信道、快速信道
 - **业务信道：** 传送用户语音或数据业务
 - 全速率信道、半速率信道、增强型全速率信道

2 GSM简介

呼叫过程

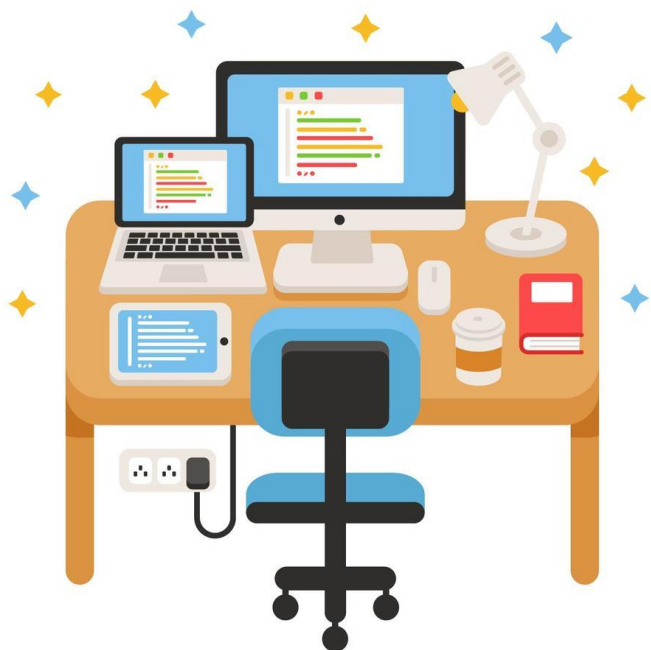




1. 数字保密通信
2. GSM简介
3. **GSM系统安全目标**
4. GSM系统安全机制
5. GSM系统安全缺陷

安全目标

- 防止未经授权的用户接入网络
- 保护用户的隐私权



1. 数字保密通信
2. GSM简介
3. GSM系统安全目标
- 4. GSM系统安全机制**
5. GSM系统安全缺陷

4 GSM安全机制

安全机制简介

- **PIN码：** **SIM**卡鉴权—终端的本地安全机制，防止别人盗用**SIM**卡
 - 存储在SIM卡内部，当移动终端开机时提示用户输入
 - 如果用户连续3次输入了错误的PIN 码，则需要输入正确的更长的个人解锁密钥PUK。
 - 如果连续输入10 次错误的 PUK ，则SIM卡被锁，需要运营商更换新SIM卡。
- **用户鉴权：**网络发起，网络和终端共同完成
- **加密：** 对在空中接口传输的信息进行加密
- **匿名：** 在空中接口使用**TMSI**，而不是**IMSI**

4 GSM安全机制

GSM中的标识码

- **IMEI**: 国际移动台设备识别码
- **MSISDN**: 国际移动用户电话号码

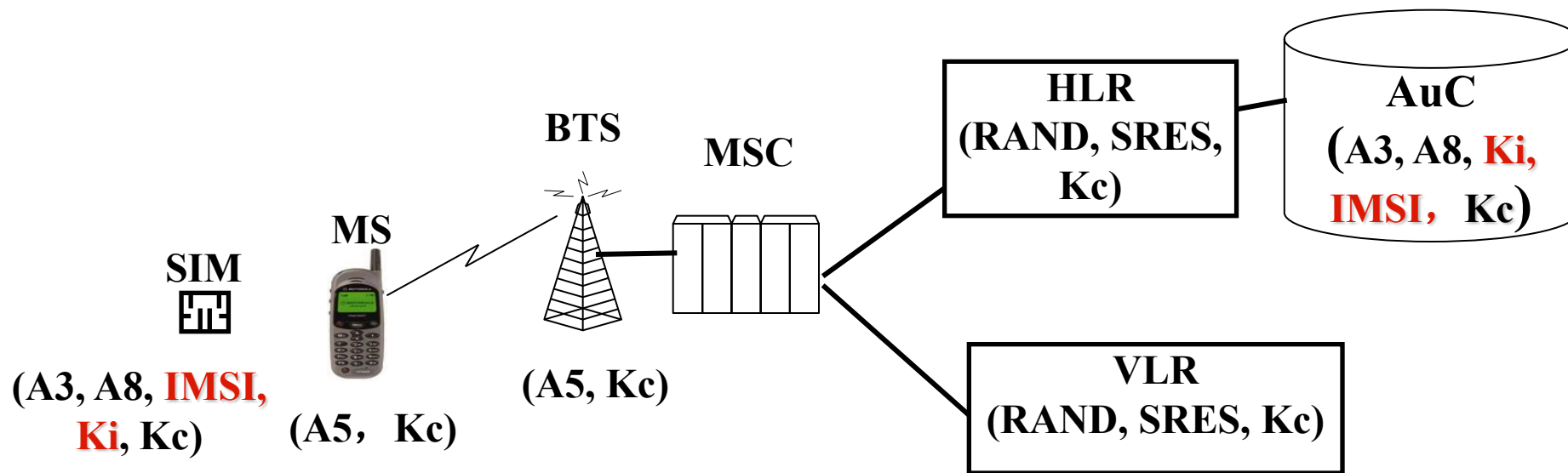
CC	NDC	HLR识别码	SN
----	-----	--------	----

- **IMSI**: 国际移动用户标识

MCC	MNC	MSIN
-----	-----	------

4 GSM安全机制

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, 归属位置寄存器
MSC: Mobile Switch Center, 移动交换中心
AuC: Authentication Center, 认证中心
RAND: Random, 随机数
SRES: Signed Response, 期待响应值

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

■ 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

4 GSM安全机制

用户鉴权协议

✓ 认证成功

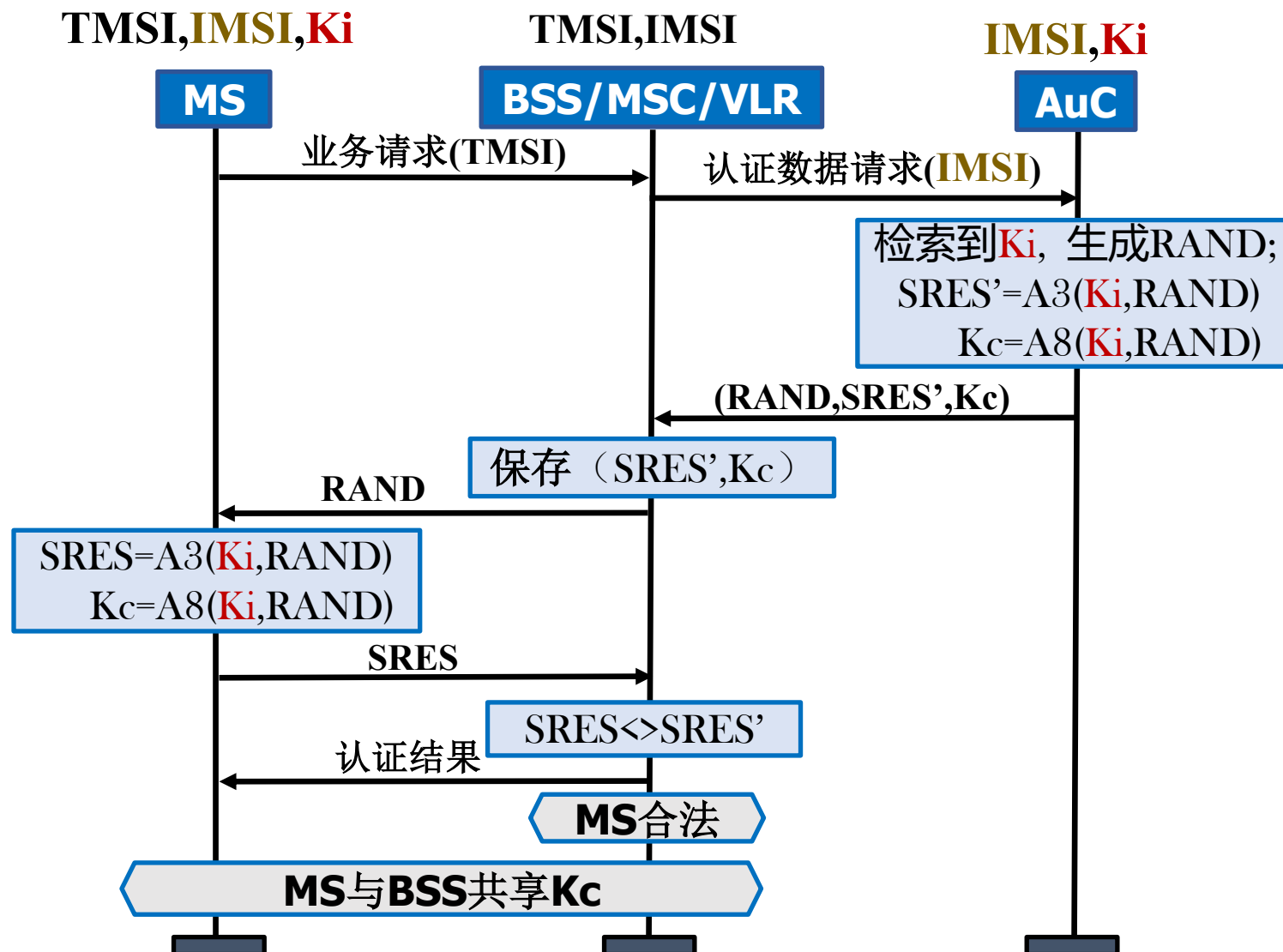
SIM卡和**AuC**共享密钥
Ki及算法**A3**

✓ **Kc**的一致性

认证成功及**A8**的一致性

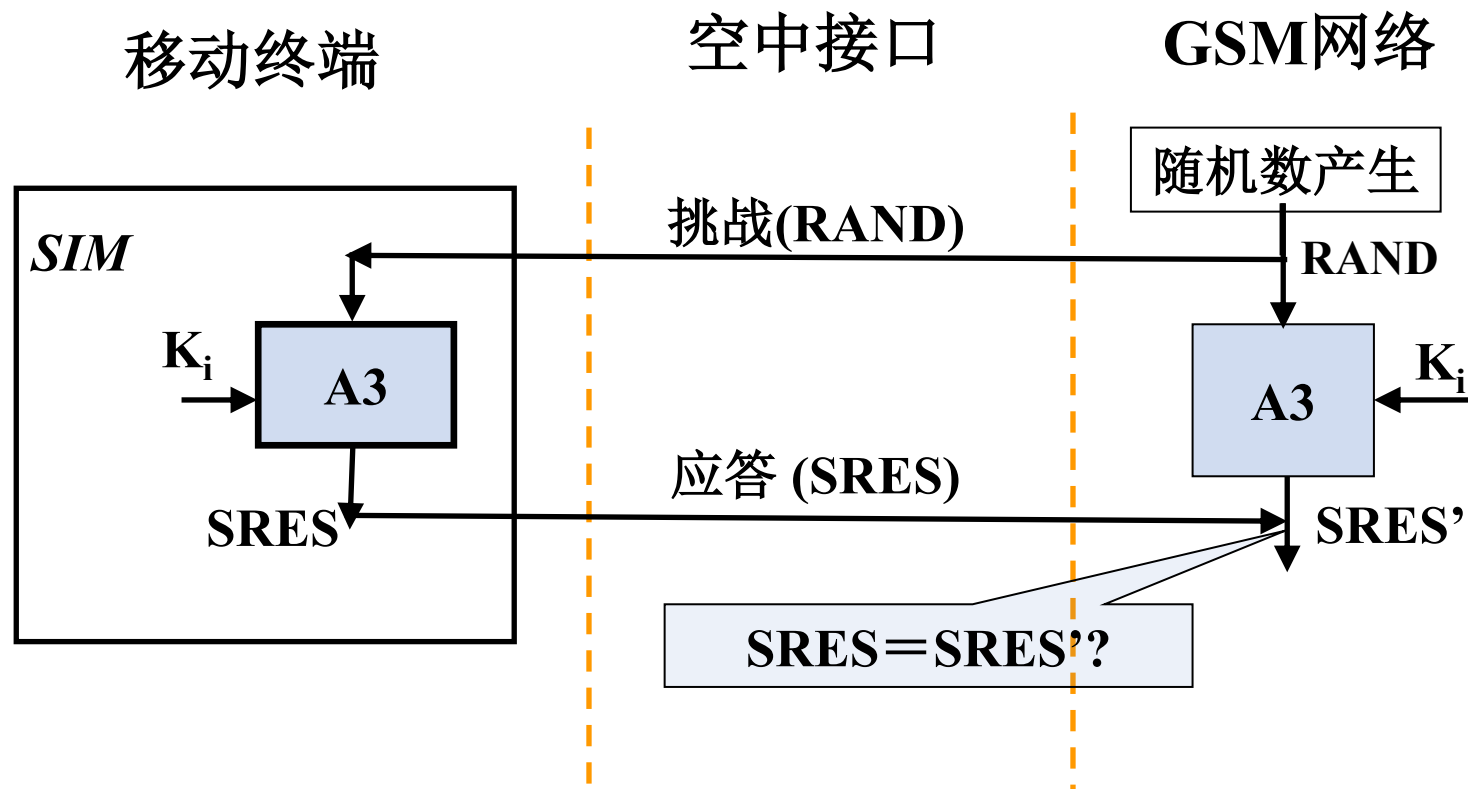
✓ **Kc**的排它性

Kc不会在空中传输



4 GSM安全机制

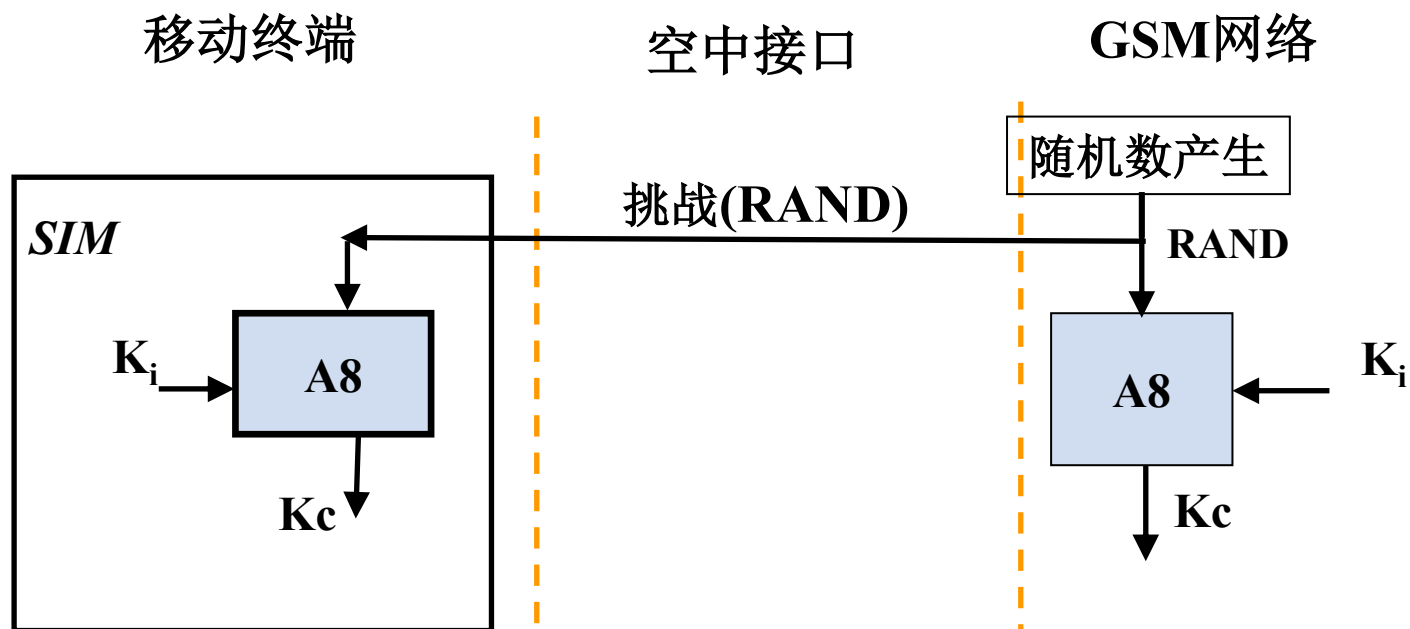
用户鉴权过程



认证的前提是终端中的SIM卡和网络共享密钥 K_i 及认证算法A3

4 GSM安全机制

GSM加密密钥生成

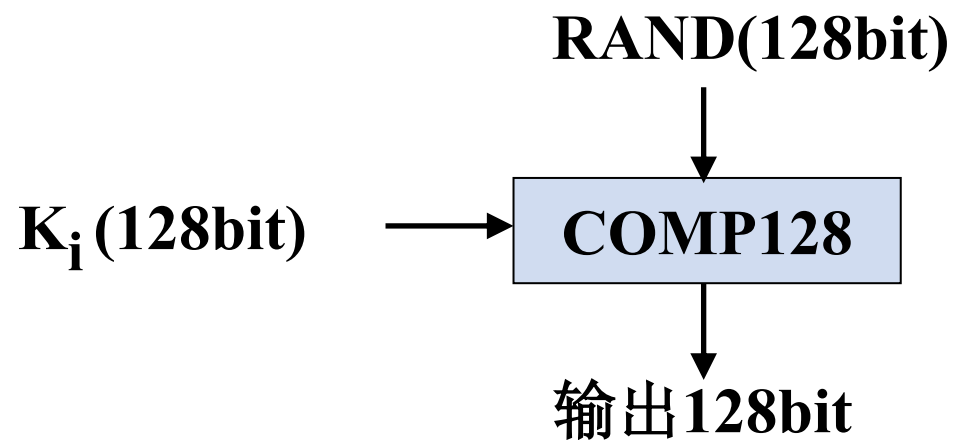


- 认证成功及**A8**算法的一致性能够保证两边生成的会话密钥**Kc**的一致性。
- **Kc**不会在空中传输。

4 GSM安全机制

A3和A8算法的实现

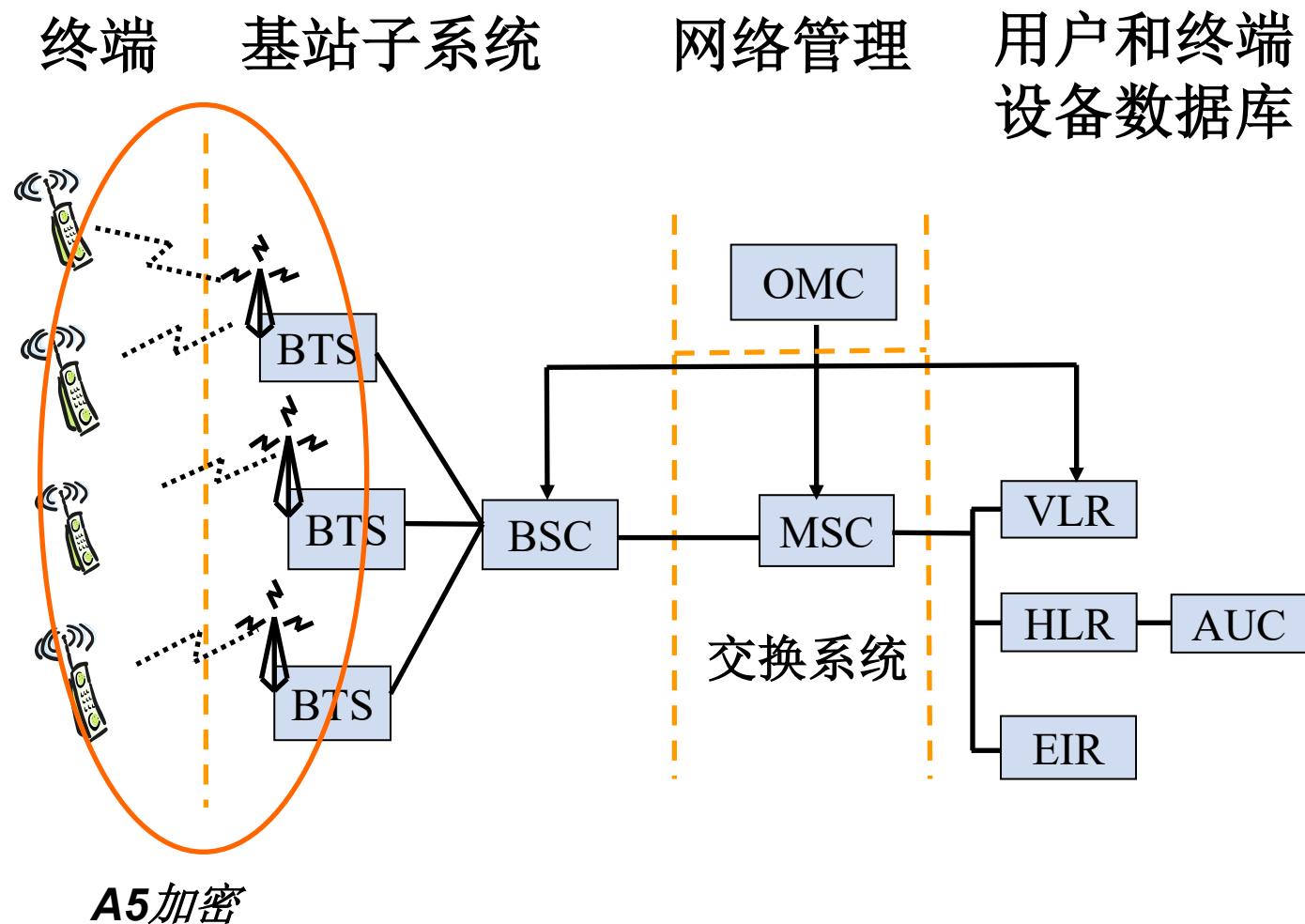
- A3和A8算法都在SIM卡和AuC中实现
- A3和A8算法在SIM卡中的运算时 K_i 不出卡
- 算法的具体实现由运营商决定
- 大部分的GSM网络运营商都选用COMP128作为A3和A8算法的实现
- COMP128是一个带密钥的散列函数。



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

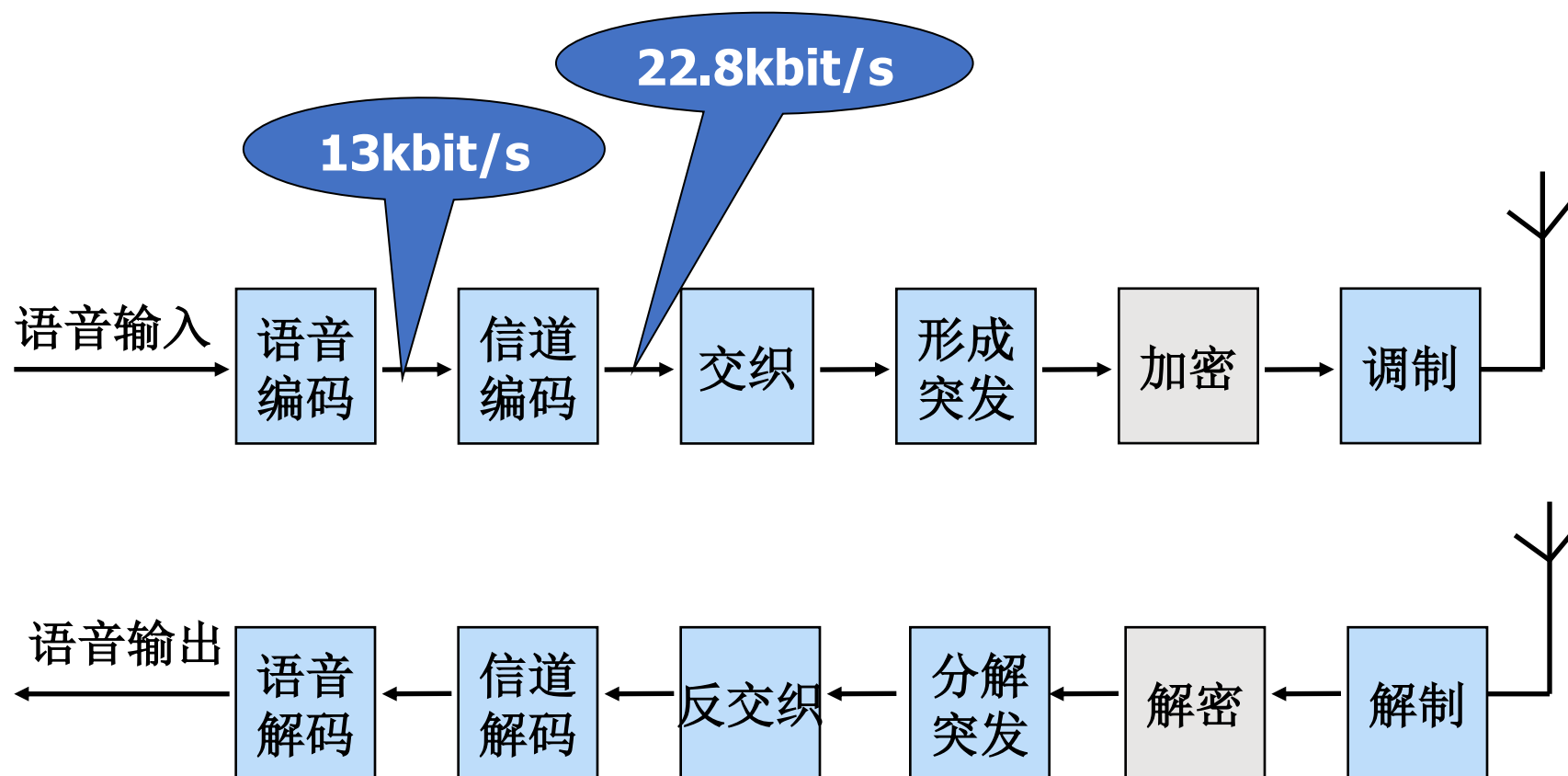
4 GSM安全机制

GSM系统空中接口加密



4 GSM安全机制

GSM系统中语音处理的一般过程



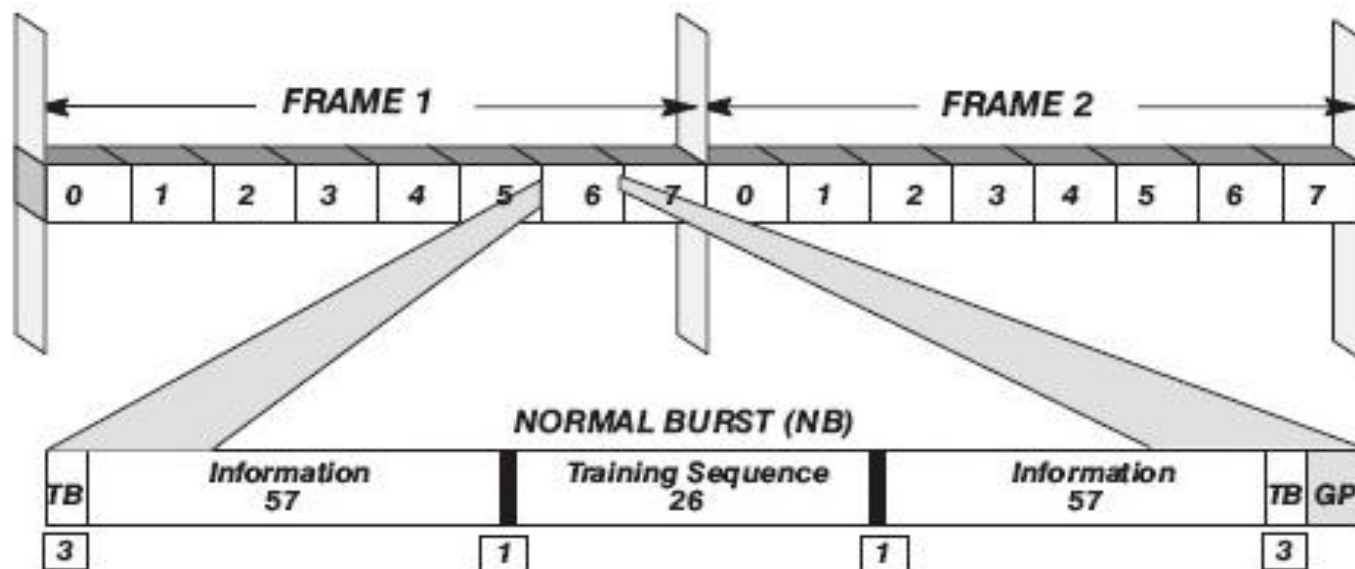
突发脉冲

- 是以不同的信息格式携带不同的逻辑信道，在一个时隙内传输的，由**100**多个调制比特组成的脉冲序列。
- 分类

类型	逻辑信道	携带信息
普通突发脉冲	TCH及除RACHA、SCH、FCCH和空闲突发脉冲以外的控制信道	业务信息和控制信息
频率校正突发脉冲	频率校正信道（FCCH）	频率校正信息
同步突发脉冲	同步信道（SYCH）	系统同步信息
接入突发脉冲	随机接入信道（RACH）	随机接入信息
空闲突发脉冲	控制信道	无

4 GSM安全机制

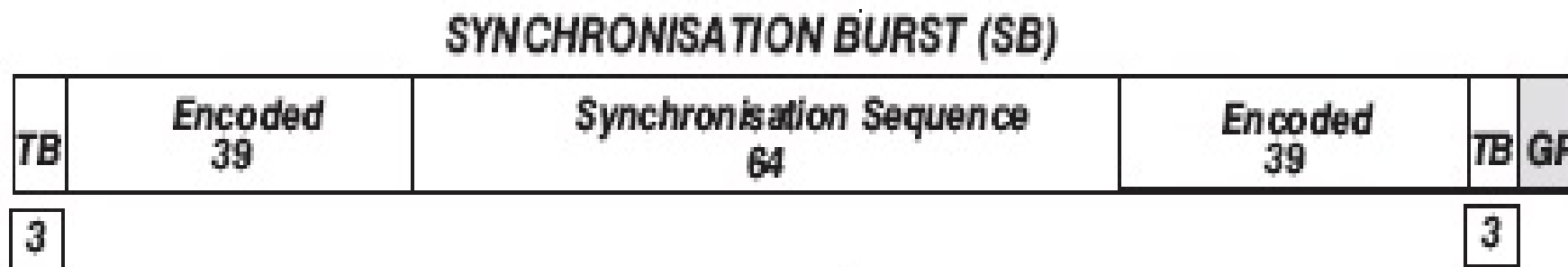
普通突发脉冲的结构



- 尾位TB (2*3bit) :总是000, 标记突发脉冲的开始与结束
- 信息 (2*57bit) :语音、数据或控制信息 (可进行加密)
- 训练序列 (26bit) : 一串已知比特, 供信道均衡用
- 保护时间GP: 防止由于定时误差而造成突发脉冲间的重叠

4 GSM安全机制

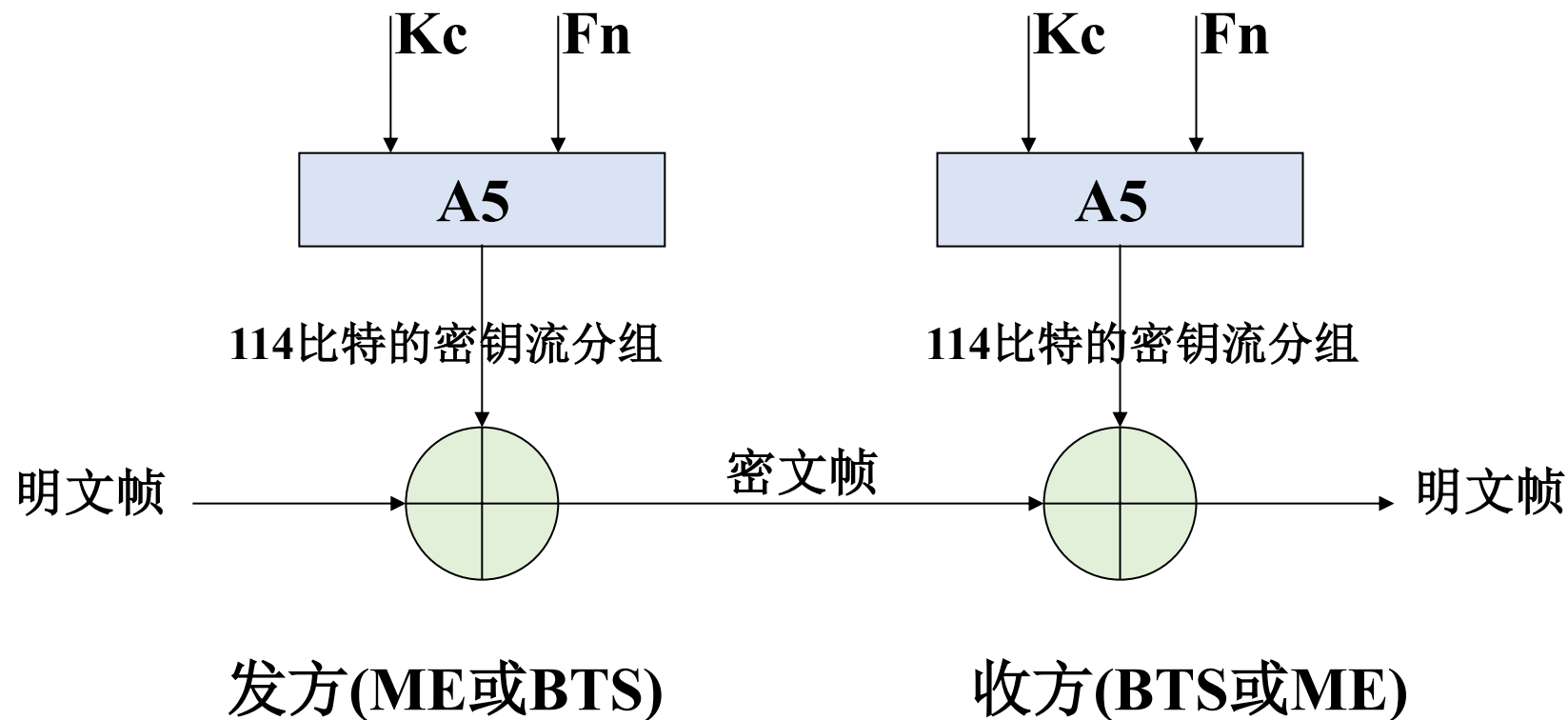
同步突发脉冲



- 39个编码比特： **TDMA帧号（TN）** 以及基站识别码(BSIC)
- 信息长同步序列： 易被检测

4 GSM安全机制

GSM系统加密



Kc: 64比特

Fn: 22比特

4 GSM安全机制

A5算法

- A5是一个序列密码算法
 - 可以在硬件上高效实现
 - 该算法的设计没有公开
 - 但最终还是泄漏出去了
- 算法的变种
 - A5/1 – 较强的版本
 - A5/2 – 较弱的版本
 - A5/3
 - GSM联盟安全组和3GPP设计
 - 基于3GPP中使用的Kasumi算法

A5/1 概述

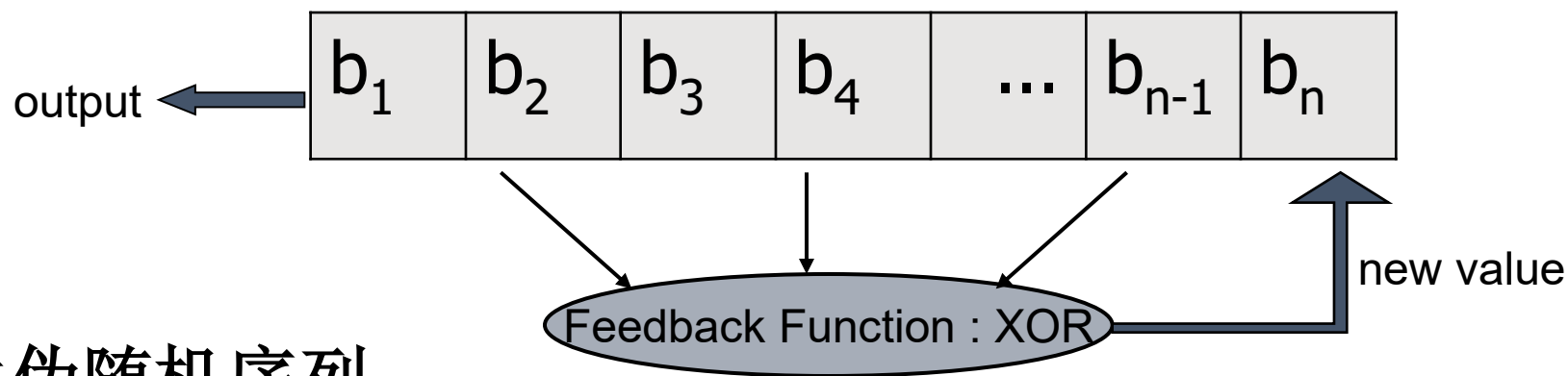
“Cryptography is a mixture of mathematics and muddle, and without the muddle the mathematics can be used against you.”

- Ian Cassells, a former Bletchly Park cryptanalyst.

- A5/1 是一个流密码算法，每发送一帧都会重新初始化。
- 由3个长度为19、22、23位的LFSR组成。
- 三个寄存器使用多数规则的时钟停/走方式计算反馈值。

4 GSM安全机制

LFSR 结构



- 目的：产生伪随机序列
- 包括两部分：
 - 移位寄存器：产生比特序列
 - 反馈函数：一般是**XOR**，产生反馈值
- 抽头序列：
 - 移位寄存器中被作为反馈函数的输入端的比特位

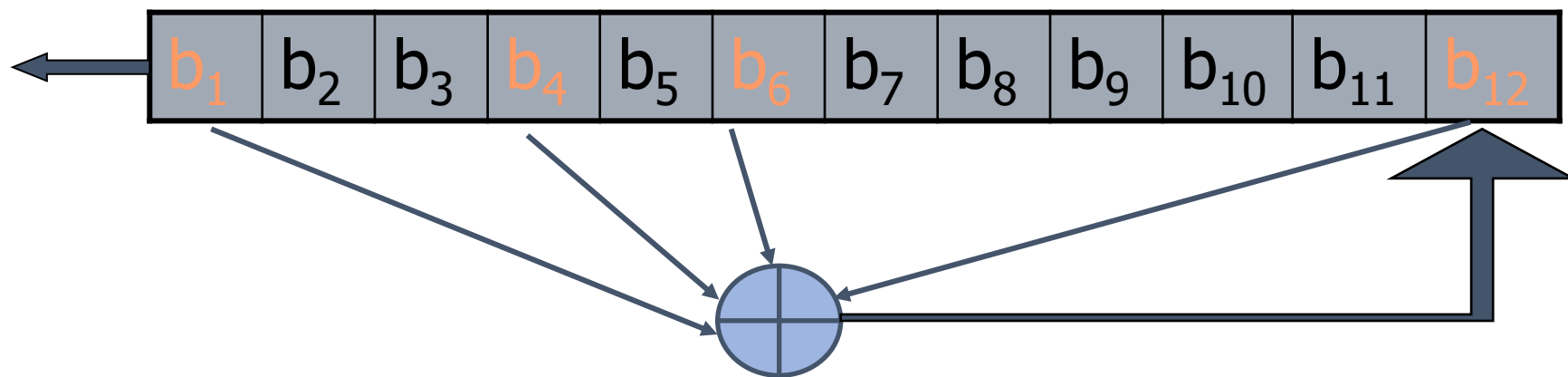
LFSR Features

- LFSR 周期： 输出序列开始自身重复之前的长度。
- n-bit LFSR 可以处于 2^n-1 内部状态
 - ➔ 最大周期为 2^n-1
- 抽头序列决定了LFSR的周期大小
- 为达到最大周期，由抽头序列加1构成的多项式（特征多项式）必须是本原多项式（mod 2）

4 GSM安全机制

LFSR

- 例如: $x^{12}+x^9+x^7+x+1$ 对应长度为12的LFSR



4 GSM安全机制

A5/1 LFSRs

3个不同长度的LFSR组成

■ 19 bits

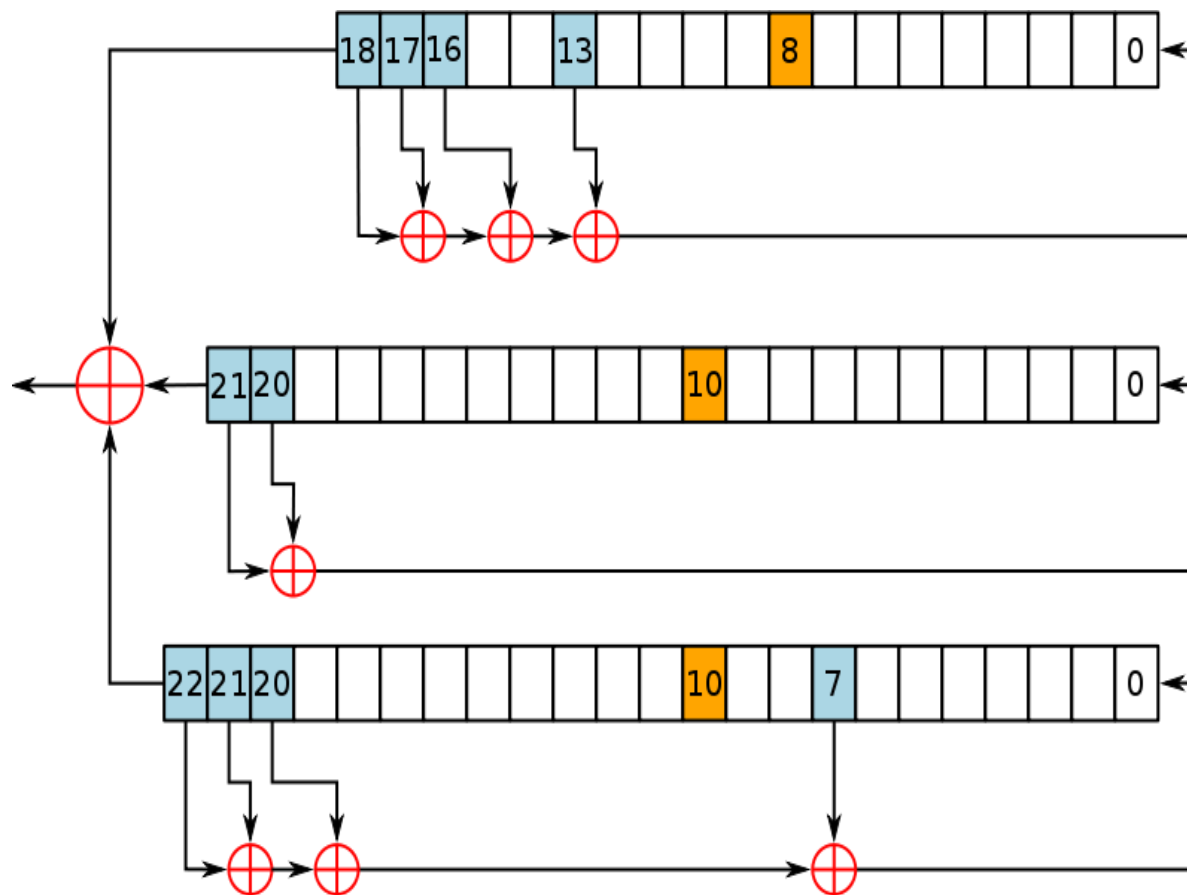
- $x^{19} + x^{18} + x^{17} + x^{14} + 1$
- clock bit 8
- tapped bits: 13, 16, 17, 18

■ 22 bits

- $x^{22} + x^{21} + 1$
- clock bit 10
- tapped bits 20, 21

■ 23 bits

- $x^{23} + x^{22} + x^{21} + x^8 + 1$
- clock bit 10
- tapped bits 7, 20, 21, 22

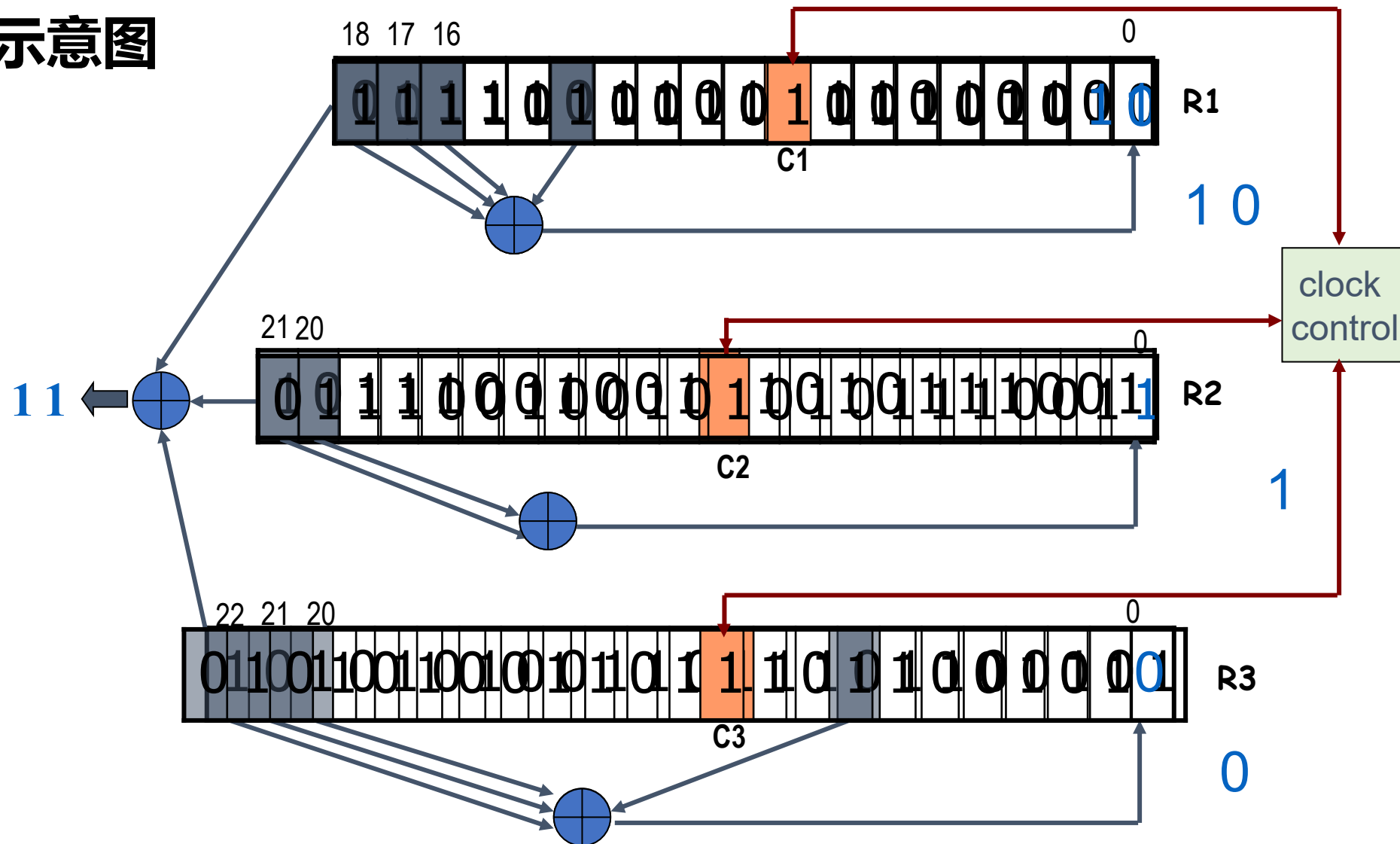


➤三个LFSR的生成多项式均为本原多项式

➤移位是由时钟控制的，且遵循“服从多数”的原则。

4 GSM安全机制

A5/1算法示意图

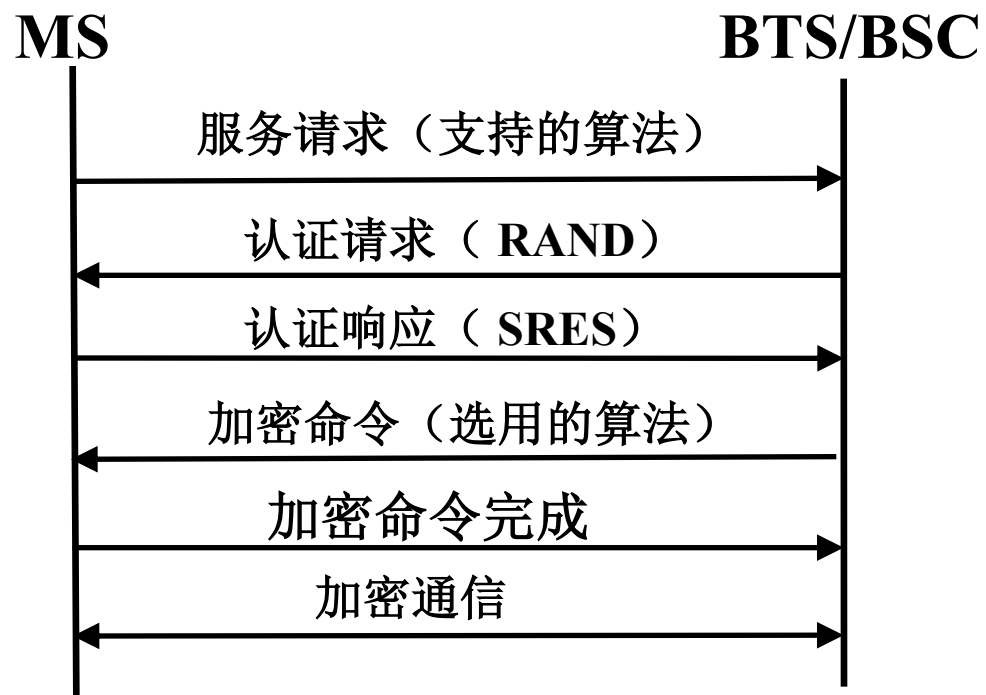


A5/1 : Operation

- 先将R1、R2、R3清零
- 把64比特会话密钥Kc注入LFSR作为其初始值
- 再将22比特帧数Fn与LFSR的反馈值做模2加注入LFSR
- 开启LFSR的“服从多数”停走钟控功能，对寄存器进行移位，使密钥和帧号进行充分混合，这样便可以产生密钥流。
- 注意：在每获得114比特的密钥流之前，要舍去产生的100比特输出。
- 一次运算产生2个114比特，共计228比特的密钥流。

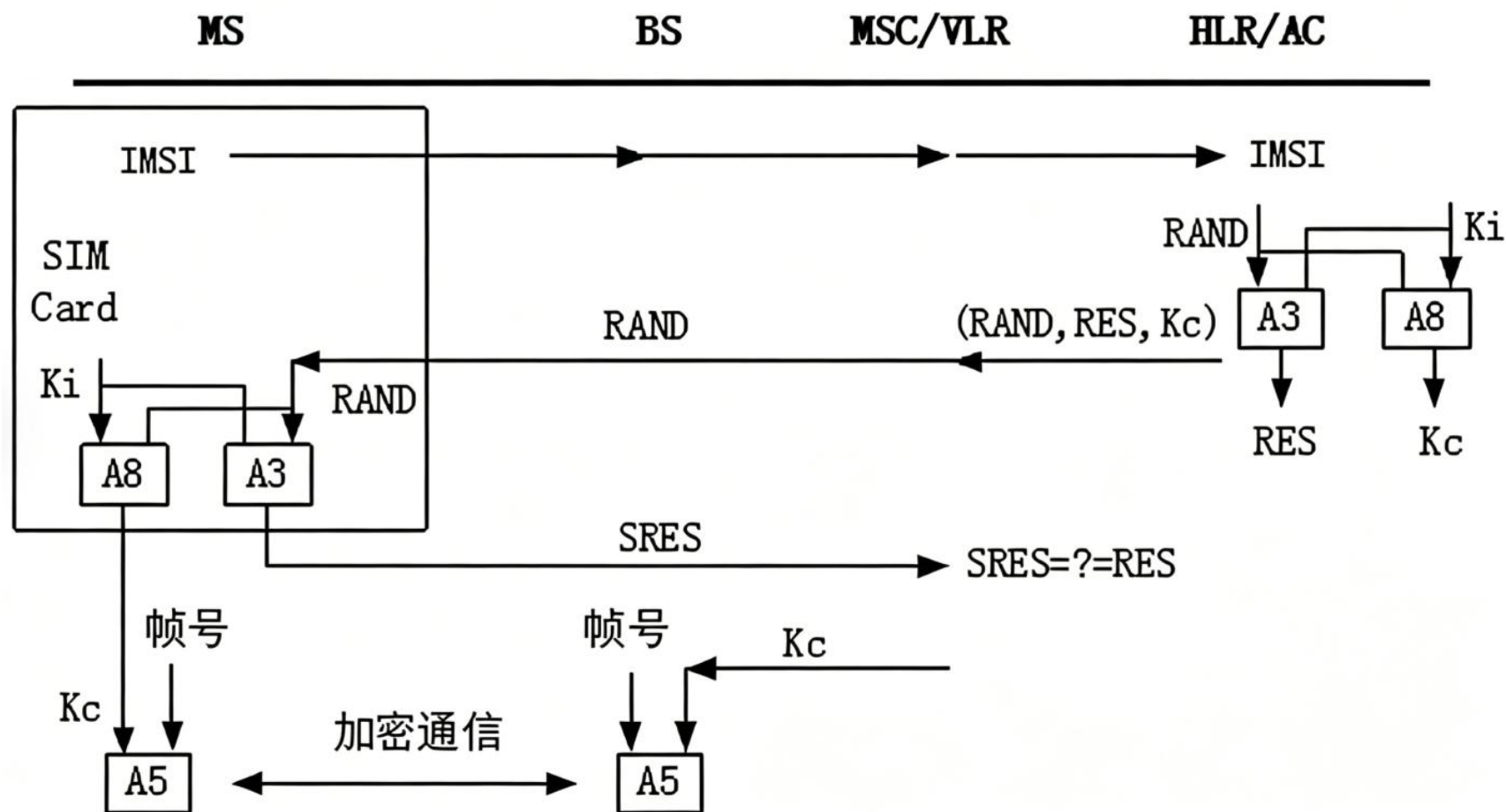
4 GSM安全机制

加密算法协商



4 GSM安全机制

GSM鉴权和空口加密小结

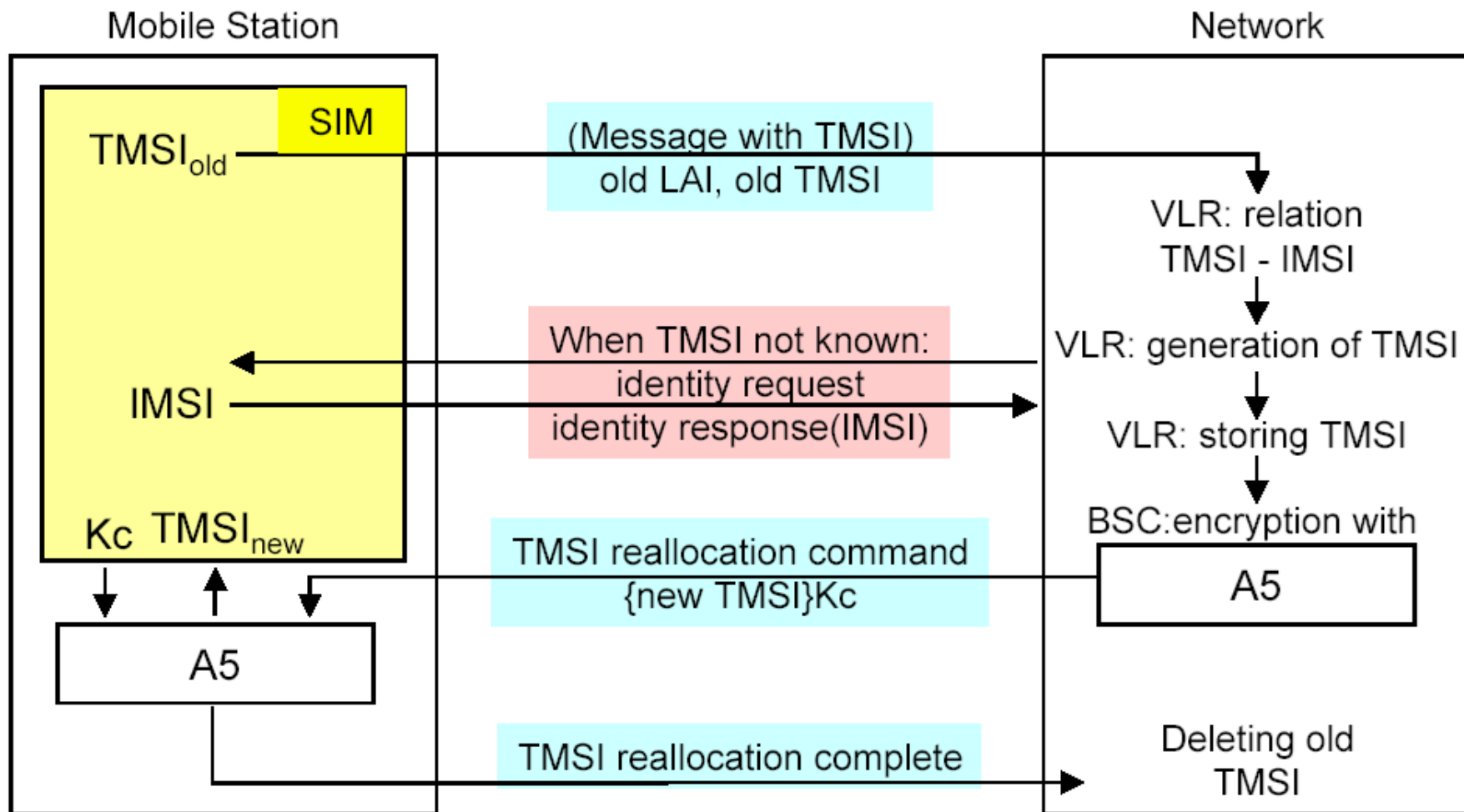


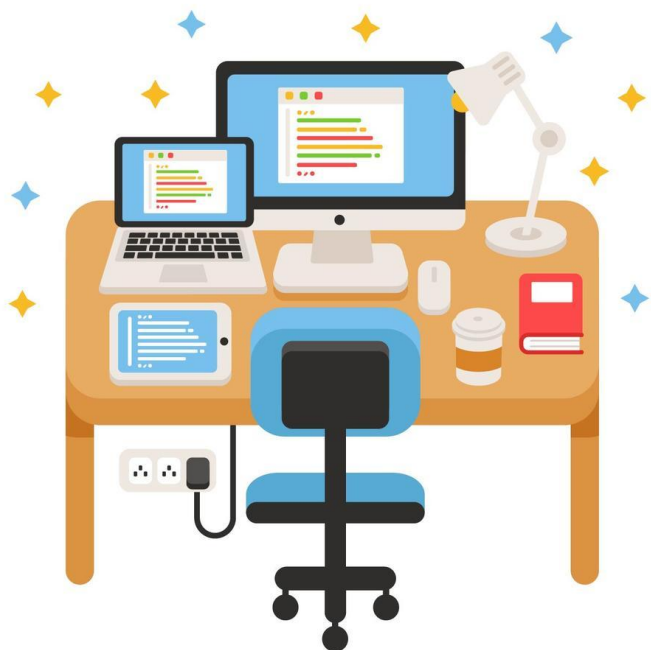
用户身份保密

- **IMSI – International Mobile Subscriber Identity**
- **TMSI – Temporary Mobile Subscriber Identity**
- TMSI在空中接口代替用户的IMSI身份，以防止通过窃听识别用户的身份。
- TMSI用于在无线链路上识别用户，如寻呼请求、位置更新请求、**attach** 请求、**detach**请求、业务请求、连接重新建立请求等。
- TMSI由MS所在区域的VLR/SGSN分配
- 每次发生位置更新时都由网络给MS分配一个新的TMSI。
- MS关机时TMSI存储在SIM卡中，等待下次使用。

4 GSM安全机制

用户身份保密 - 用TMSI代替IMSI





1. 数字保密通信
2. GSM简介
3. GSM系统安全目标
4. GSM系统安全机制
- 5. GSM系统安全缺陷**

5. GSM系统安全缺陷

针对GSM系统的攻击类型

- **伪基站攻击**：冒充合法基站，诱导用户接入，获取**IMSI**，实施跟踪、欺骗或拒绝服务等攻击。
- **弱加密算法攻击**：针对**A5/1**、**A5/2**等算法进行攻击，恢复密钥、窃听通信。
- **降级攻击**：强制终端使用无加密或弱加密模式，降低通信安全级别。
- **重放与信令滥用**：利用认证和信令机制缺陷进行重放、身份追踪或位置分析。
- **核心网信令攻击**：借助**SS7**等互联信令漏洞实施短信拦截、定位和业务劫持。
- **实现漏洞攻击**：针对基带、协议栈或网络设备实现缺陷发起攻击。



伪基站攻击

- “伪基站”即假基站，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搜集一定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。

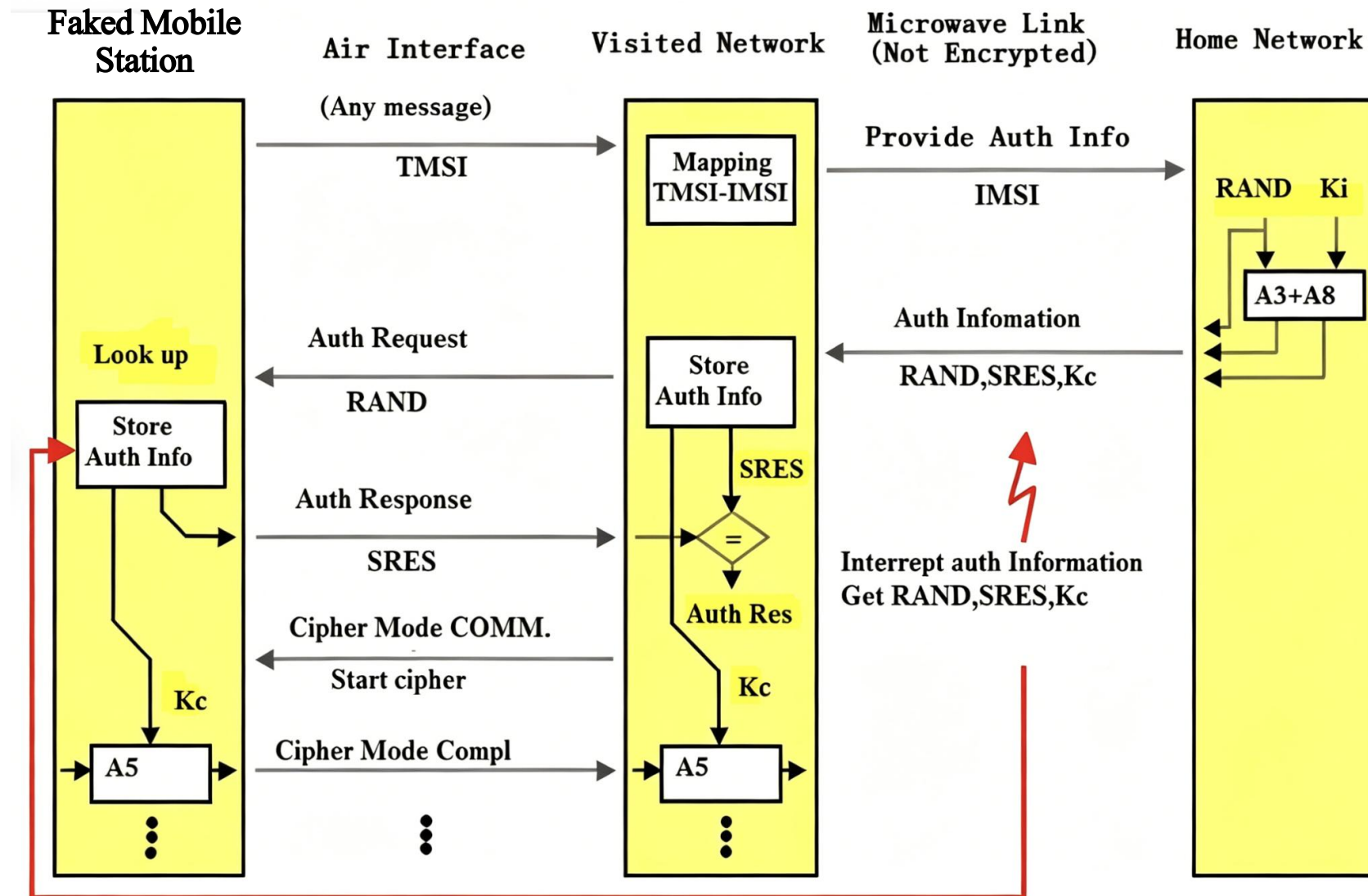


伪基站攻击（续）

- 伪基站攻击的特点
 - **发现难**：伪基站可以很隐蔽，很难检测
 - **抓获难**：伪基站流动性强，难以抓获
 - **定罪难**：其对用户、通信的伤害难以估计，定罪周期较长
- 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

5. GSM系统安全缺陷

核心网络攻击



5. GSM系统安全缺陷

对GSM的实际攻击

- 1998年，智能卡开发协会(SDA) 采用侧信道/查询攻击方法**攻破SIM卡中的COMP128算法**，可在数小时内恢复用户密钥Ki，可**实现SIM卡克隆**。
- 2002年，IBM研究人员提出对**COMP128**的改进攻击方法，可通过对SIM卡的查询在较短时间内恢复Ki。
- 2000年前后，Biryukov, Shamir和Wagner提出针对**A5/1的时间-存储权衡攻击**，通过大规模存储预计算表实施攻击，表明该算法在预计算条件下可被有效破解。
- 2003年，Barkan, Biham和Keller**攻破A5/2**，极短时间内恢复密钥，促使其被废。
- 2008年，在硬件辅助下，**A5/1**可在数小时内**被破解**，降低了GSM被动窃听门槛。
- 2010年代，**SS7 攻击**大规模暴露，GSM 用户定位与短信拦截风险凸显。

5. GSM系统安全缺陷

总结

- 保护范围
 - 只是在空中接口实施了鉴权和加密，在固定网内无加密和认证措施
 - 不提供端到端的加密。
 - 认证向量三元组有可能在固定网内被攻击者窃取，可以冒充网络单元进行认证，进而可以控制用户的加解密模式。
- 认证方式
 - 只有单向实体认证，很难防止中间人攻击和假基站攻击。
 - 缺乏数据完整性认证

5. GSM系统安全缺陷

总结

- 密钥管理及密码算法
 - 算法不公开，其安全性如何得不到客观、公正的评估。
 - 密钥长度
 - Ki一般固定不变，易破译
- 完整性保护
 - 用户数据和信令数据缺乏完整性保护机制
- IMSI的安全性
 - 在认证过程中，有可能在无线信道上以明文发送安全参数IMSI。
 - 用户第一次入网时
 - VLR中与用户有关数据丢失时

- GSM加强了移动通信网络安全
 - PIN码保护/单向用户鉴权/空中接口加密/匿名;
 - 具有较好的合理的安全通信框架;
 - 安全模型对通信及设备厂商的影响最小;
 - SIM- keys,A3,A8,etcSIM
 - ME – A5
- 还需加强
 - 固定网络安全
 - 端到端安全
 - 算法公开
 - 双向鉴权
 - 安全的可配置性
 - SIM卡安全

本讲作业

1. GSM系统中对IMSI进行匿名的方法有效吗？请说明原因
2. 什么是伪基站攻击？请设计针对GSM网络的伪基站攻击方案，并分析在GSM网络中可以实施这种攻击的原因。
3. 分析A5算法中Fn的作用，并计算如果一直保持通话，多长时间需要重新鉴权。

- <http://www.etsi.org> 中GSM相关标准
- <http://www.iol.ie/~kooltek/a3a8.txt>
- www.nettwerked.net 中'The GSM Security Technical Whitepaper for 2002'

Thank You !

