

课程编号: 3182121321

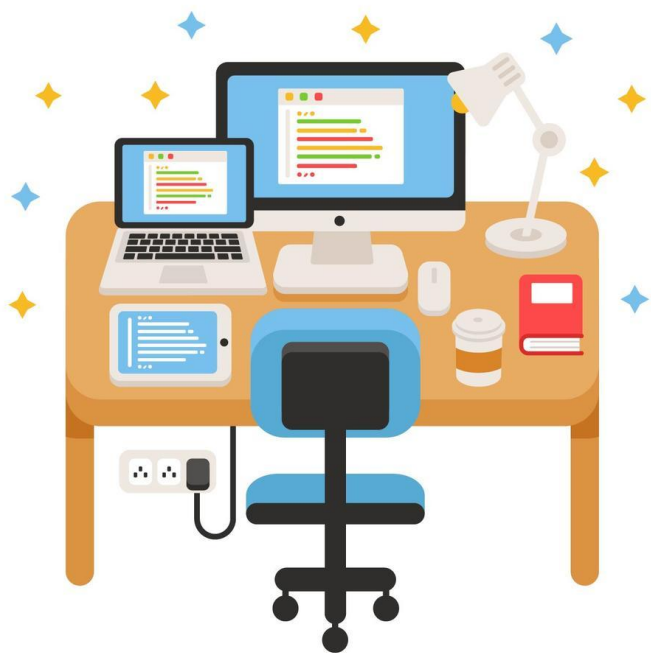
无线通信安全



第六讲 TETRA安全技术

李晖

lihuill@bupt.edu.cn



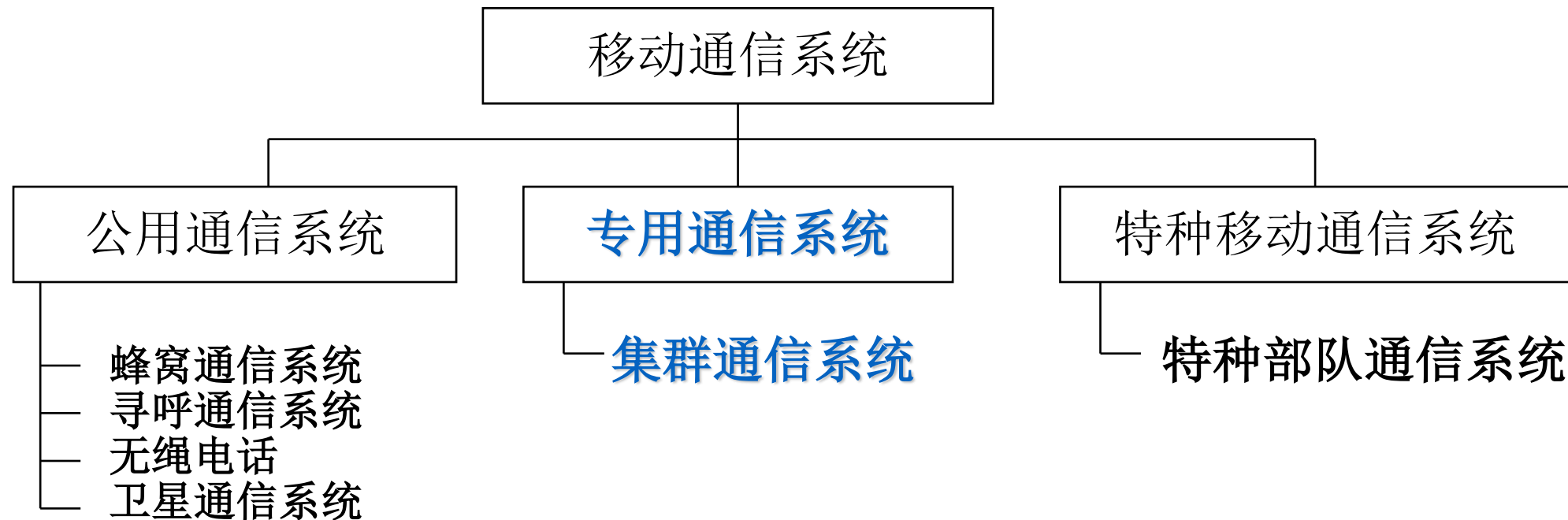
1. 数字集群系统及TETRA标准简介
2. TETRA系统面临的安全威胁
3. TETRA系统的安全技术
4. TETRA系统的安全技术之一：鉴权
5. TETRA系统的安全技术之二：空中接口加密
6. TETRA系统的安全技术之三：端到端加密

1. 数字集群系统及TETRA标准简介

什么是专业无线移动业务

- 专业无线移动业务（Professional Mobile Radio, PMR），是指长期以来为专业内部通信所提供的业务，主要用于警察、救护、公交等行业
- PMR大多或完全限制在内部沟通使用
- 最基本的功能需求是：
 - 群组通信（一人说话，其它人收听）
 - 调度通信，通常是控制中心内的调度员和在外人员的通话，一般会希望所有的现场工作人员都能听到该通话
- 呼叫及通话时间很短

1. 数字集群系统及TETRA标准简介



■ 集群通信系统定义：

- 多个用户（部门、群体）共用一组无线电信道，并动态使用这些信道的专用移动通信系统，主要用于指挥调度通信。

1. 数字集群系统及TETRA标准简介

主要数字集群标准

- 国外标准：
 - **TETRA (TErrestrial Trunked RAdio)**
 - **iDEN (integrated Digital Enhanced Network)**
 - **FHMA (Frequency Hopping Multiple Access)**
 - **TETRAPOL**
- 国内标准
 - **YDC030-2004 《基于GSM技术的数字集群系统总体技术要求》**
 - 华为公司开发的GT800系统
 - **YDC031-2004 《基于CDMA技术的数字集群系统总体技术要求》**
 - 中兴公司开发的GoTa

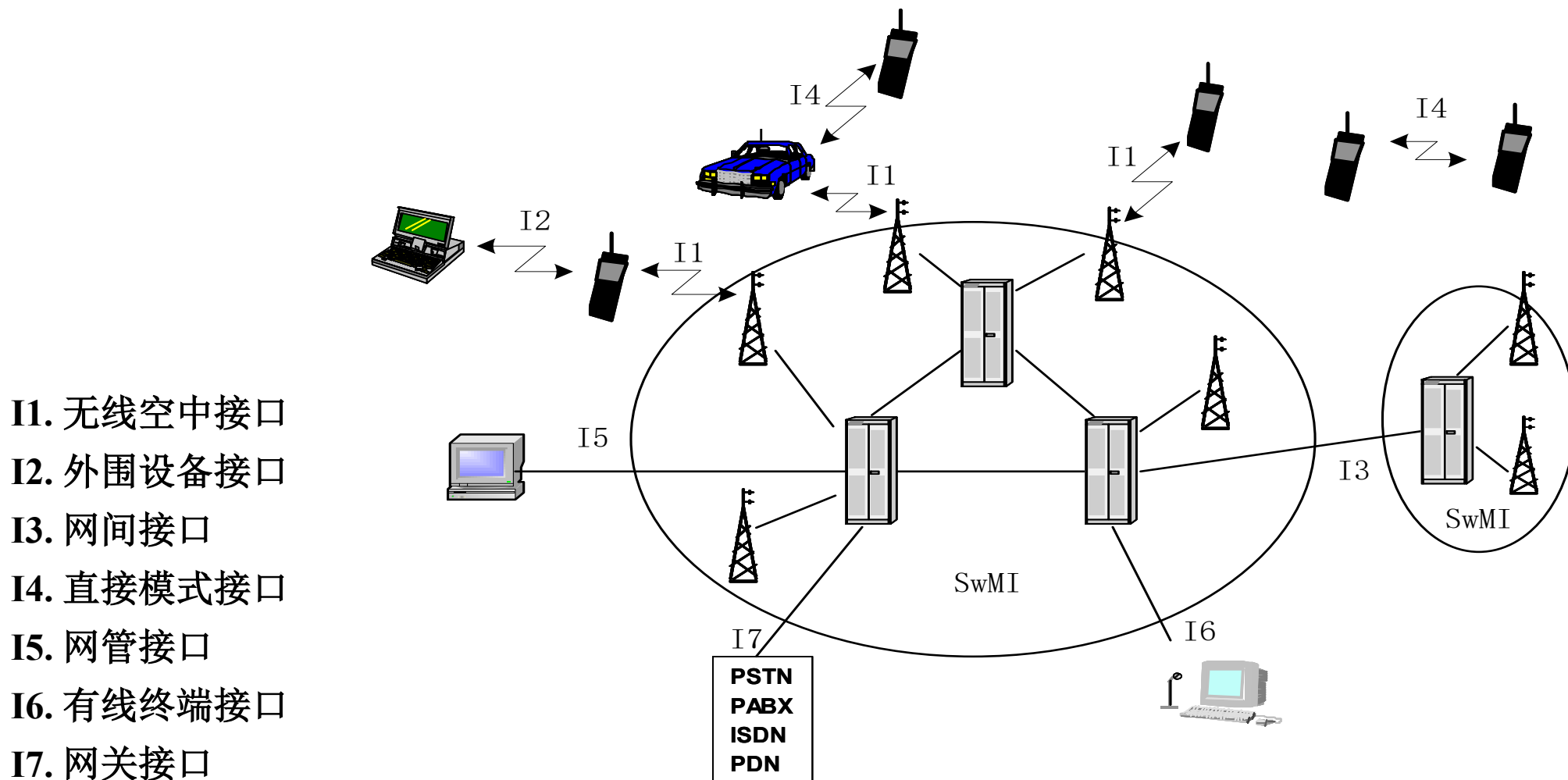
1. 数字集群系统及TETRA标准简介

TETRA简介

- TETRA是TErrestrial TRunked RAdio的缩写，直译为陆地无线集群系统
- ETSI制定的数字集群通信标准
ETSI — 欧洲电信标准协会
- 1988年—1997年，标准的绝大部分制定完成
- TETRA是唯一开放的专业数字移动无线系统的标准
- TETRA设备和终端在全球有多个厂家支持
- TETRA的标准性由一个由制造商、运营商、和其它相关团体联合组成的机构 — TETRA MoU来作监管协调

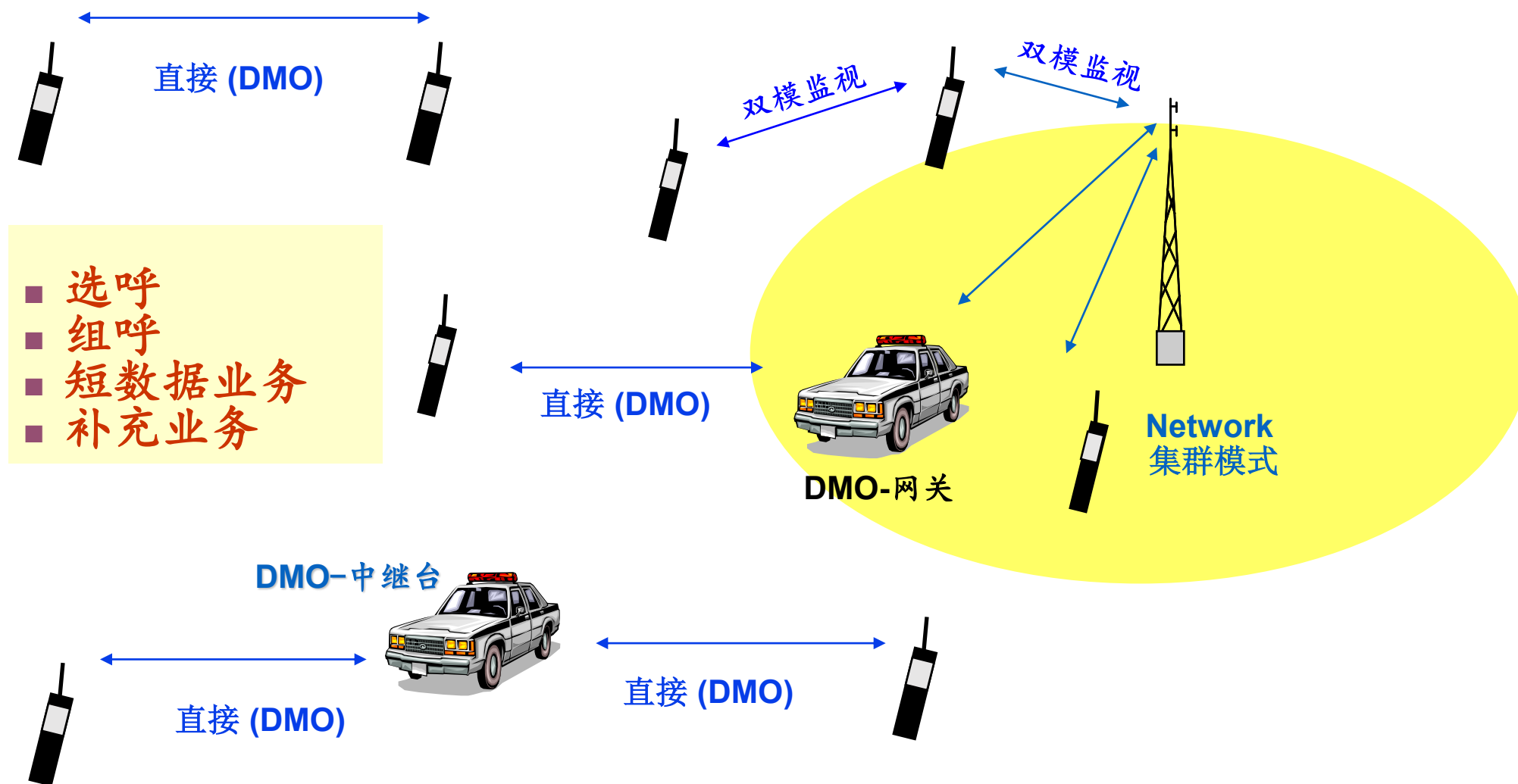
1. 数字集群系统及TETRA标准简介

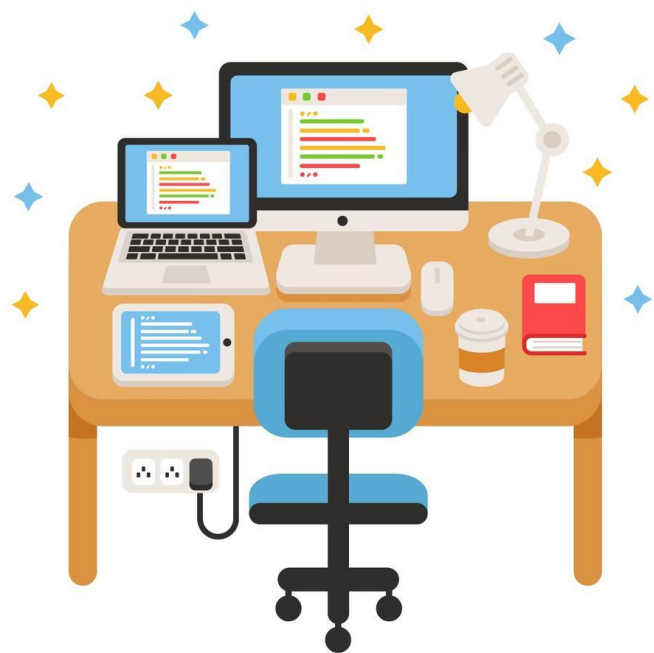
TETRA系统组成和标准接口



1. 数字集群系统及TETRA标准简介

独特的直接模式操作



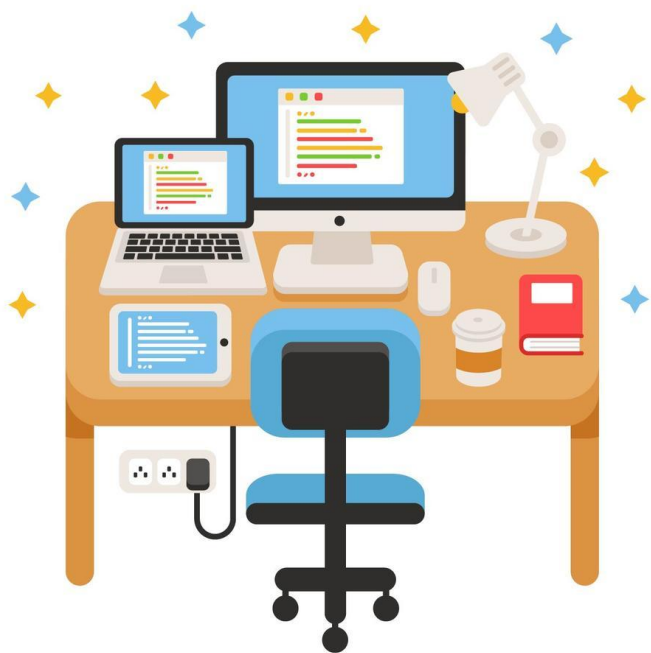


1. 数字集群系统及TETRA标准简介
- 2. TETRA系统面临的安全威胁**
3. TETRA系统的安全技术
4. TETRA系统的安全技术之一：鉴权
5. TETRA系统的安全技术之二：空中接口加密
6. TETRA系统的安全技术之三：端到端加密

2. TETRA系统面临的安全威胁

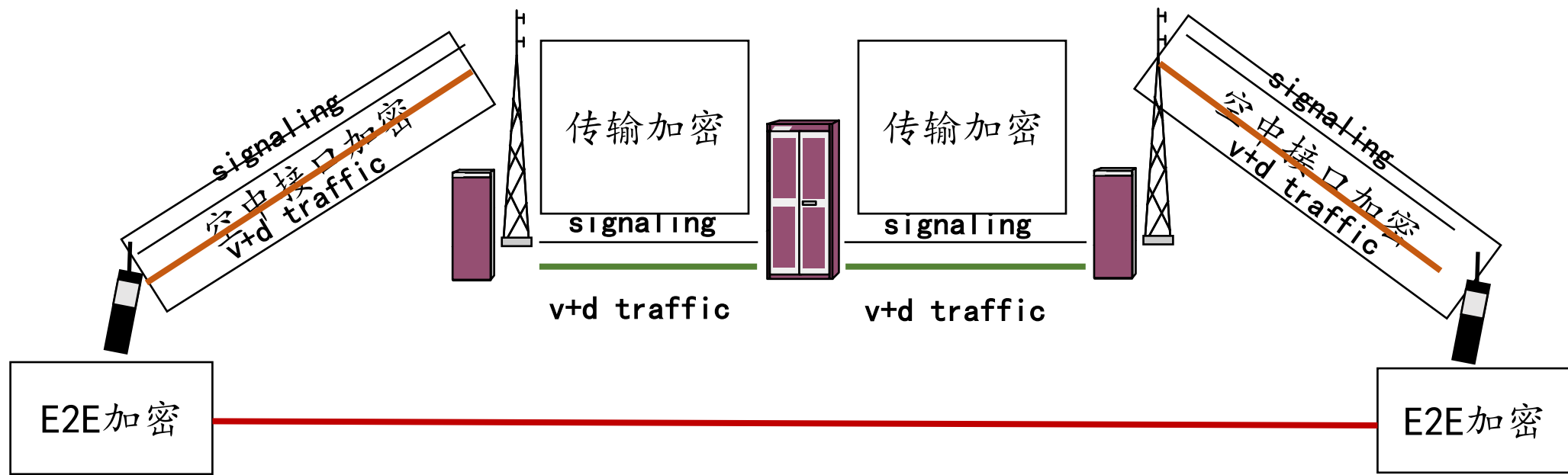
数字集群系统需要具有和移动通信公网相比更高的安全性，不仅要防范移动通信公网中存在的安全威胁，还需要达到以下安全要求：

- 调度台用户身份、组成员身份和连接链路的认证；
- 增强的通信机密性
- 增强的通信完整性
- 端到端的信息保密
- 增强的合法监视功能



1. 数字集群系统及TETRA标准简介
2. TETRA系统面临的安全威胁
- 3. TETRA系统的安全技术**
4. TETRA系统的安全技术之一：鉴权
5. TETRA系统的安全技术之二：空中接口加密
6. TETRA系统的安全技术之三：端到端加密

3. TETRA系统的安全技术



■ TETRA 标准定义

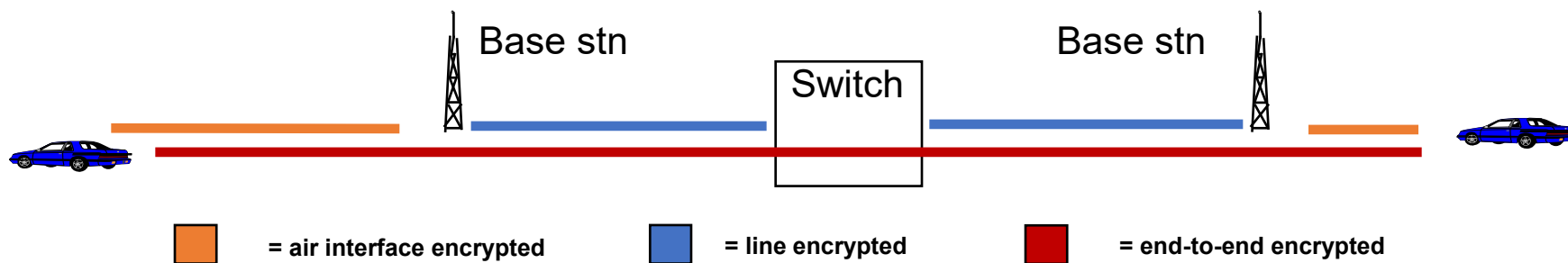
- 双向鉴权
- 空中接口加密

■ 用户定义和完善

- 传输加密
- 端对端加密

3. TETRA系统的安全技术

不同的加密机制适应不同的安全需求



空中接口加密 防止对空中无线信道的监听、分析和滥用

传输加密 防止对有线传输和微波链路的监听、分析和滥用

端到端加密 很好地防止监听，但不能防止分析和滥用

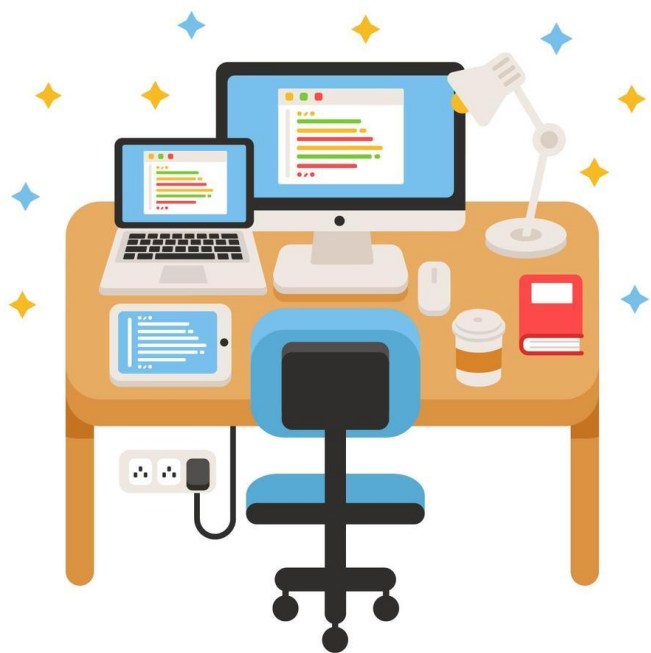
3. TETRA系统的安全技术

■TETRA 安全模式

CLASS 1	不使用加密
	可以使用鉴权
CLASS 2	必须使用 SCK 加密
	必须使用基于SCK的 ESI机制
	可以使用鉴权
CLASS 3	必须使用鉴权
	必须使用 DCK加密
	必须使用基于CCK的ESI机制

NTS 支持
Class 1 和
Class 3 终端

注： ESI (Encrypted short identity，加密短标识) $xESI=TA61_{CCK\ or\ SCK} (xSSI)$



1. 数字集群系统及TETRA标准简介
2. TETRA系统面临的安全威胁
3. TETRA系统的安全技术
4. **TETRA系统的安全技术之一：鉴权**
5. TETRA系统的安全技术之二：空中接口加密
6. TETRA系统的安全技术之三：端到端加密

4. TETRA系统的安全技术之一：鉴权

TETRA系统的识别码

识别码	号码位数	描述
ITSI	48	Individual TETRA Subscriber Identity, TETRA个人用户识别码
ISSI	24	Individual Short Subscriber Identity, TETRA短用户识别码
GTSI	48	Group TETRA Subscriber Identity, TETRA群组用户识别码
GSSI	24	Group Short Subscriber Identity, TETRA群组短用户识别码

4. TETRA系统的安全技术之一：鉴权

TETRA用户识别码结构

移动国家代码(MCC) (CCITT X.121规定)	移动网络代(MNC) (国际授权)	网络专用短用户识别码(SSSI)
10位	14位	24位

ITSI由MCC、MNC、ISSI三部分构成：

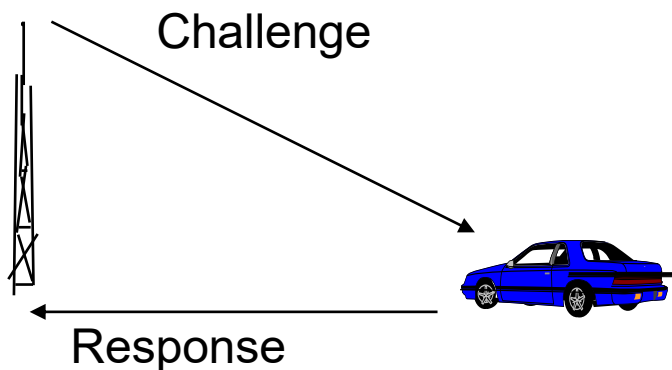
- MCC：国家代码，由ETSI规定，对应于国家名称
- MNC：网络代码，由网络内部规定，一般由国家统一规划。
 - 也是GTSI号码和位置信息的一部分，储存在DXT的数据库里，取值范围是0-16383。
- ISSI： 是一个TETRA系统中用户的唯一识别号。
 - 24位的SSSI号被直接转为十进制格式

4. TETRA系统的安全技术之一：鉴权

TETRA安全技术 - - 鉴权

■ 鉴权目的

- 检查终端/**SmartCard**的合法性
- 保护网络免受非授权使用
- 检查网络的合法性
- 防止用户接入虚假网络
- 建立会话密钥



4. TETRA系统的安全技术之一：鉴权

TETRA安全技术 - - 鉴权

■ 鉴权方案

- 通过ITSI(个人身份识别码)识别用户
- 基于鉴权密钥K(存储在MS和SwMI中)，主密秘密钥；
- 假设只有合法的MS和合法的SwMI知道正确的密钥K，验证方需要证明自己知道密钥K；
- 既要证明自己知道密钥K，又要保证密钥K不以任何形式在空中接口和SwMI内部进行传输；
- 采用挑战一应答协议

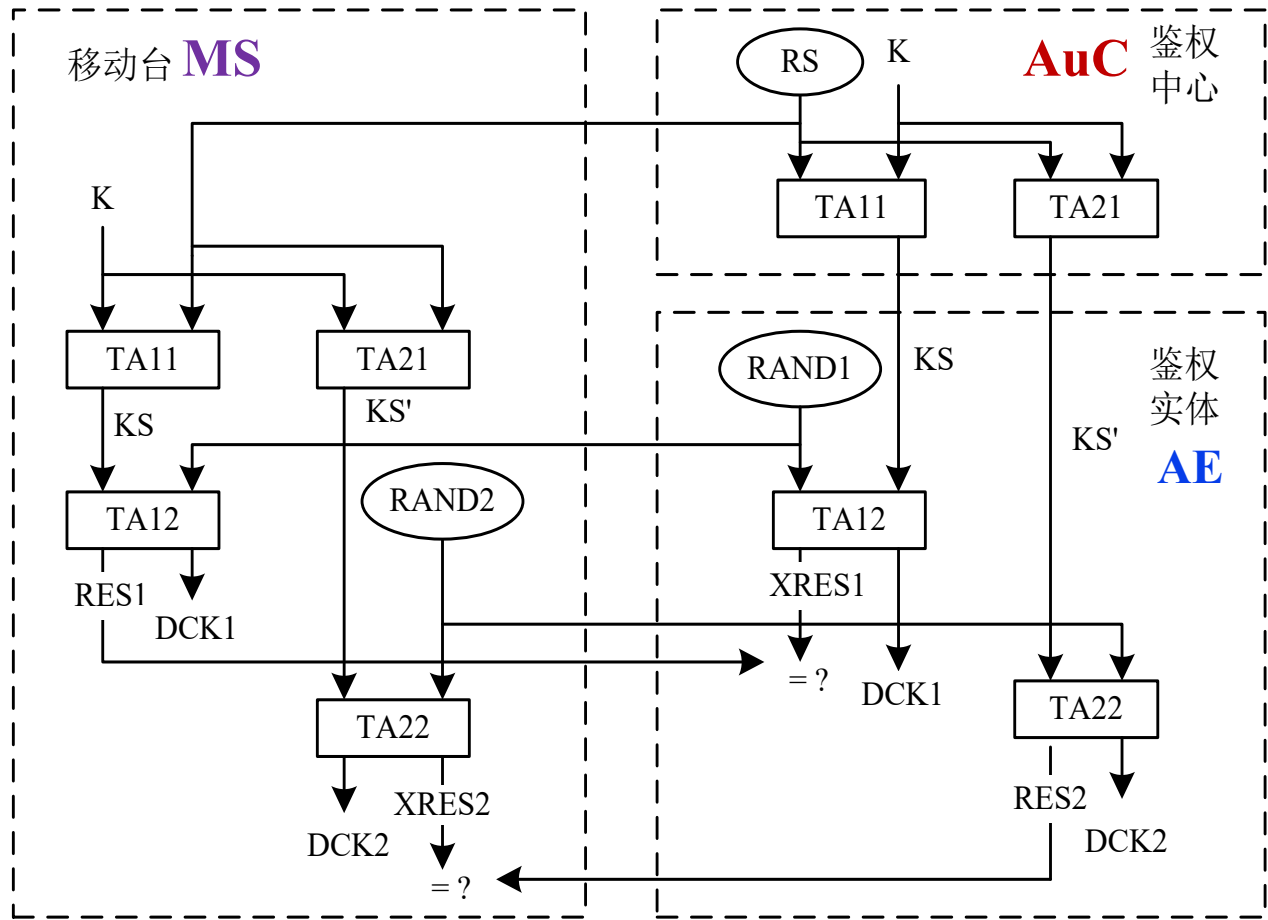
4. TETRA系统的安全技术之一：鉴权

TETRA安全技术 - - 鉴权

- MS对SwMI的鉴权
- SwMI对MS的鉴权
- 由MS发起的MS和SwMI之间的双向鉴权
- 由SwMI发起的MS和SwMI之间的双向鉴权

4. TETRA系统的安全技术之一：鉴权

TETRA 系统的双向鉴权过程



SwMI发起的双向鉴权结构

鉴权协议

$AuC \rightarrow AE: RS, KS, KS'$

$AE \rightarrow MS: RS, RAND1$

$MS \rightarrow AE: RES1, RAND2$

$AE \rightarrow MS: R1, RES2$

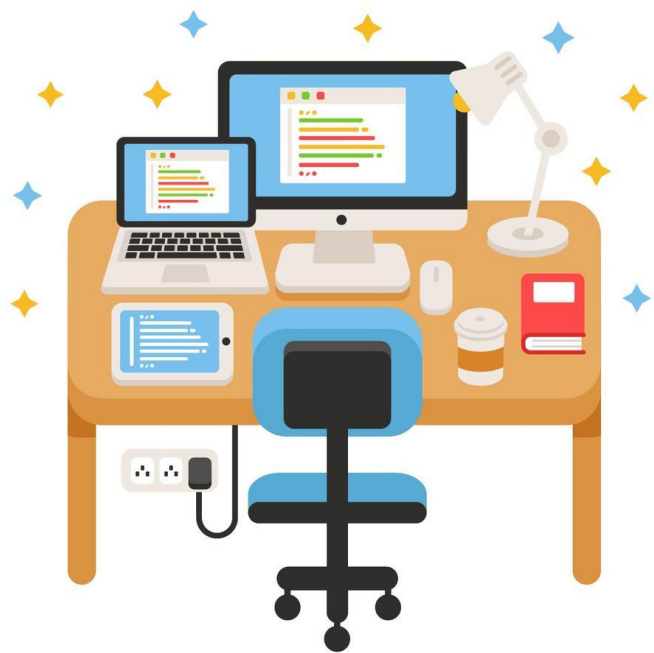
$MS \rightarrow AE: R2$

4. TETRA系统的安全技术之一：鉴权

TETRA鉴权协议分析

- 双向鉴权：防止虚假终端和虚假基站
- 防止重放攻击：三个随机数，有效防止重放攻击
- 主密钥更新：不提供主密钥**K**的更新机制
- 密钥确认：不提供显式的密钥确认
- 抵御中间人攻击：从理论上无法抵御中间人攻击
- 防止恶意破坏和干扰：没有校验和或签名保护
- 仲裁机构：无，不能防范抵赖攻击。
- 协议效率：较低

4. TETRA系统的安全技术之一：鉴权



1. 数字集群系统及TETRA标准简介
2. TETRA系统面临的安全威胁
3. TETRA系统的安全技术
4. TETRA系统的安全技术之一：鉴权
- 5. TETRA系统的安全技术之二：空中接口加密**
6. TETRA系统的安全技术之三：端到端加密

5. TETRA系统的安全技术之二：空中接口加密

- 由基础设施 (SwMI)控制
- 在登记过程中协商加密技术(包括安全级别和采用的加密算法等)
- 采用的密钥
 - 静态加密密钥 (**SCK**) ----级别**2&DMO**方式
 - 在鉴权的过程中产生动态/导出密钥 (**DCK**)----级别**3**
 - 通用加密密钥 (**CCK**) ----级别**3**

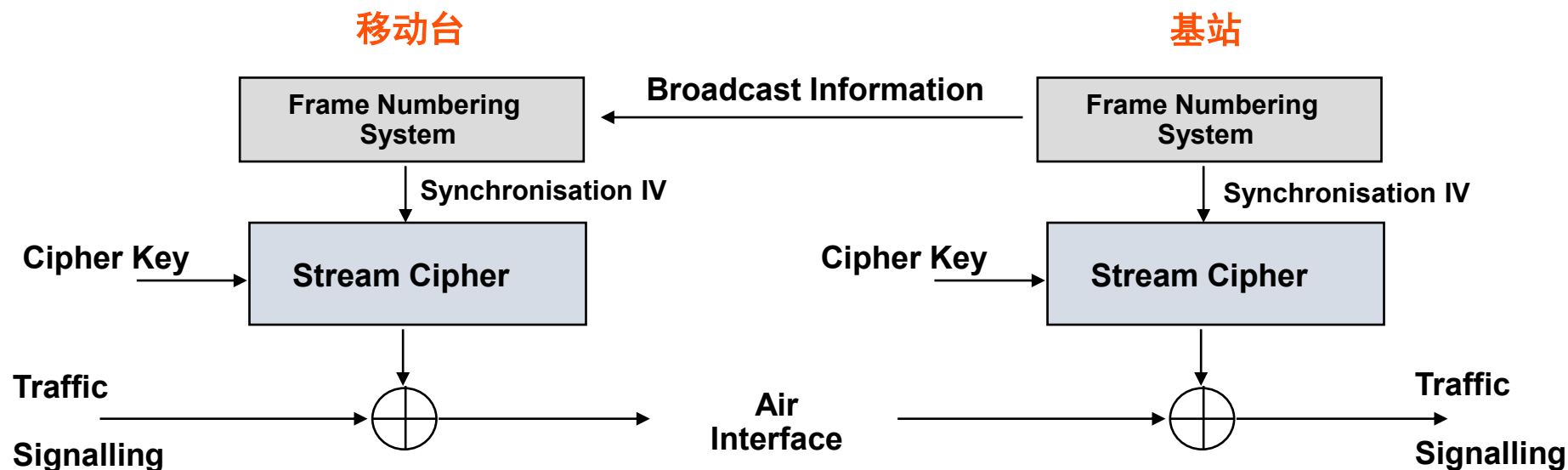
5. TETRA系统的安全技术之二：空中接口加密

为什么需要空中接口加密？

- 防止TETRA 系统中的个呼和组呼在空中接口被监听；
- 在空中接口，防止重放攻击和干扰/操纵用户的控制/业务信息；
- 在空中接口保护用户身份信息，防止某些特殊组织对该用户的信息进行监视或流量分析；

5. TETRA系统的安全技术之二：空中接口加密

流密码的同步

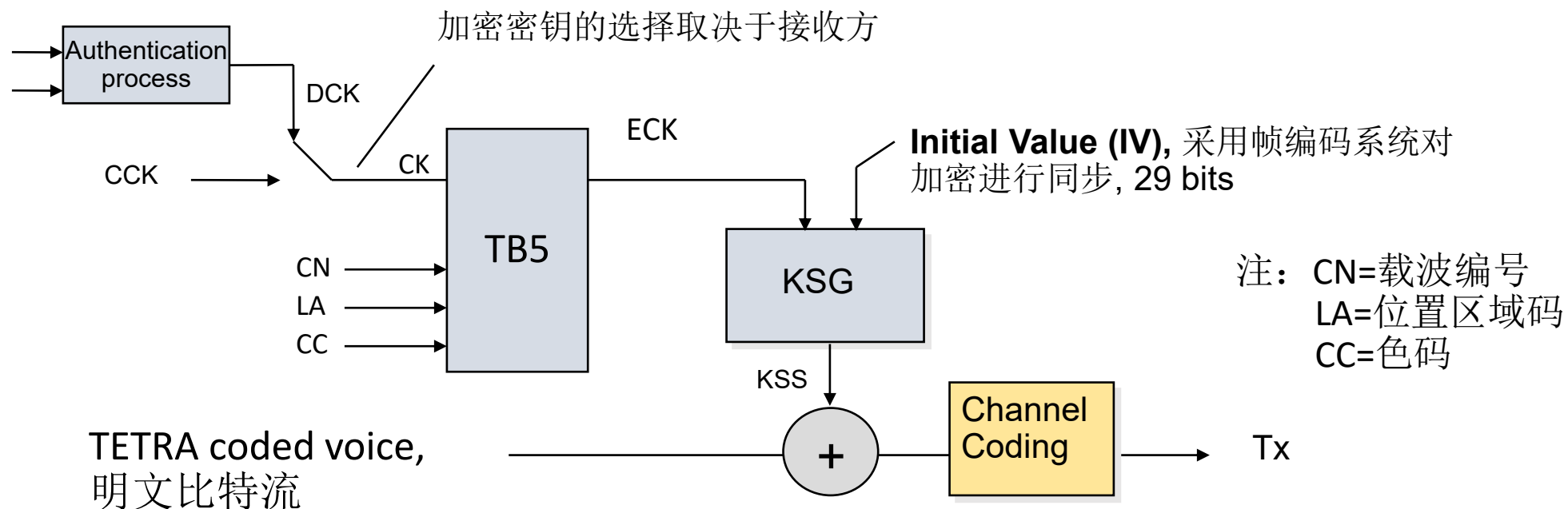


- 由SwMI维护并通过同步控制(SYNC)和系统消息(SYSINFO) PDU进行广播来产生用于同步的初始向量(IV, Initial Vector)
- 移动台和基站分别通过同步帧系统生成IV

5. TETRA系统的安全技术之二：空中接口加密

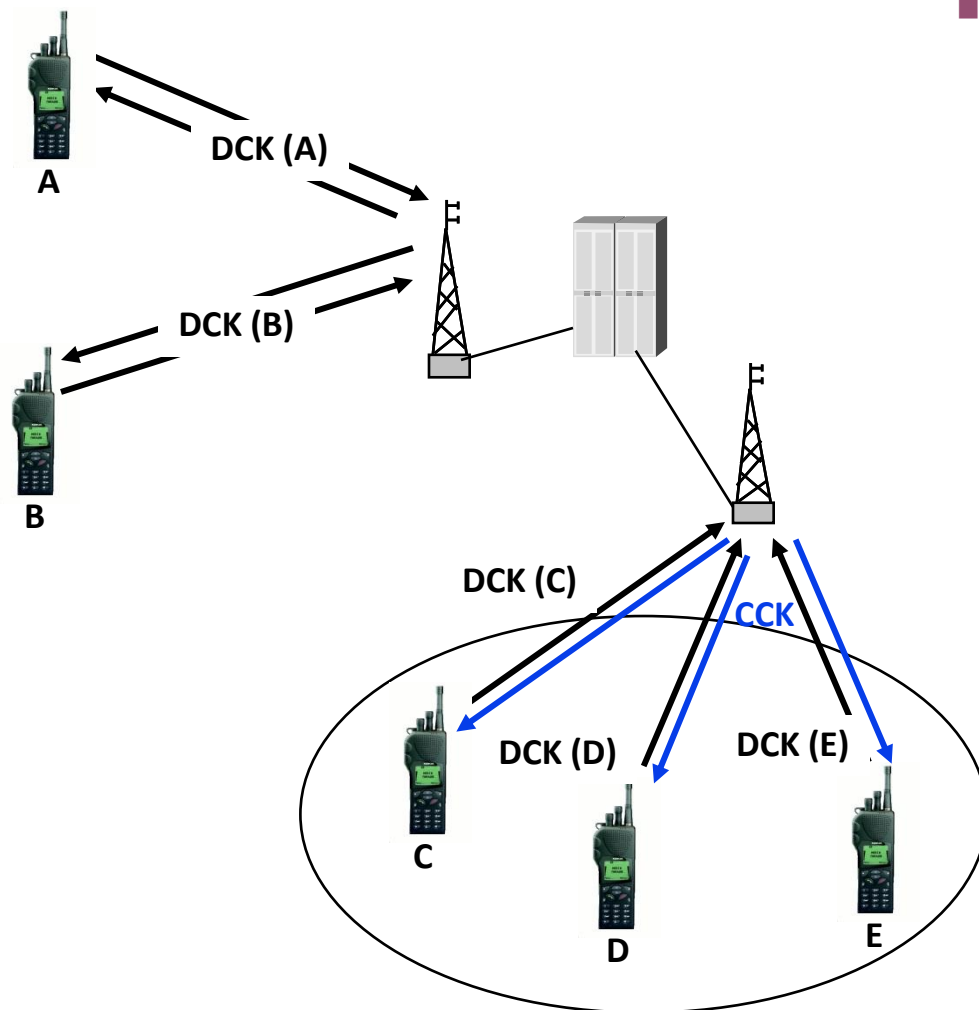
空中接口加密方法

- 空中接口加密的实现：密钥流发生器KSG的流密码方法
- 密钥流发生器KSG中的密码算法 (TEA1, TEA2 ...)
- 每个时隙均采用密钥流Key Stream Segment (KSS) 进行加密

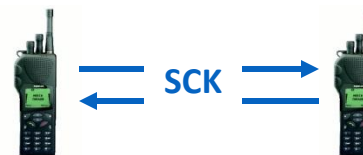


5. TETRA系统的安全技术之二：空中接口加密

空中接口加密（级别3） – 密钥

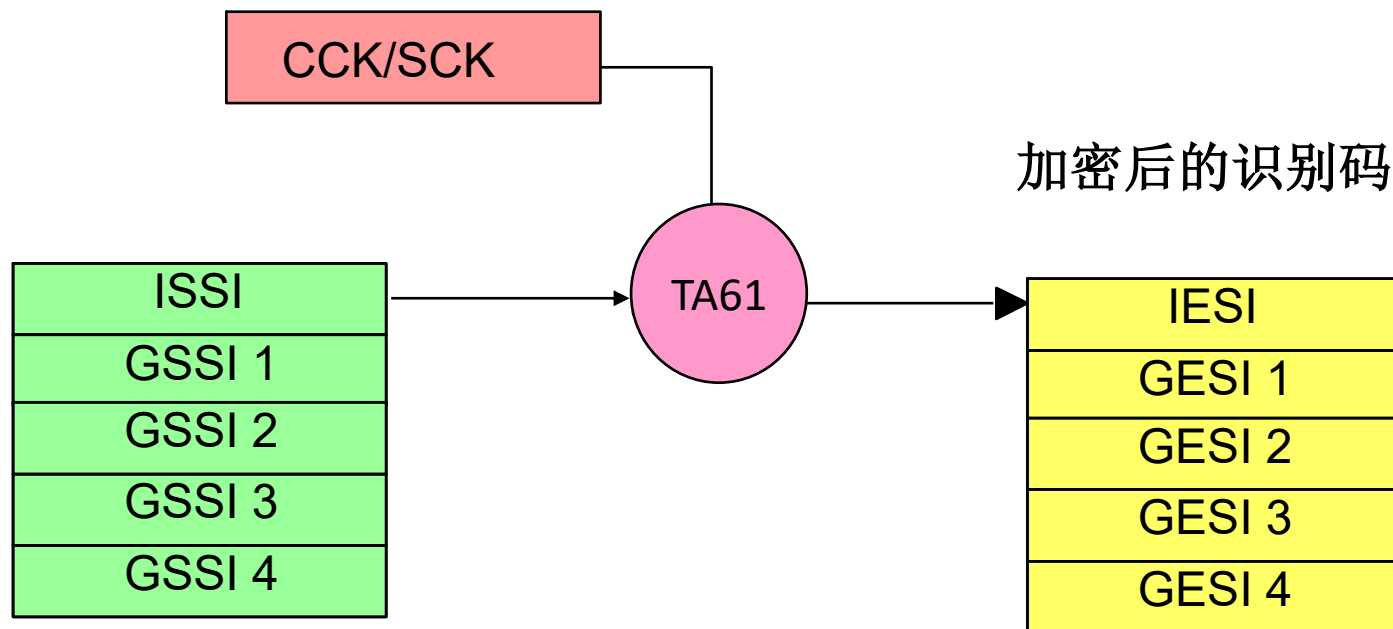


- DCK (Derived Cipher Key)
 - 个呼
 - 组呼的上行链路
- CCK (Common Cipher Key)
 - 组呼的下行链路
 - 加密ISSI或GSSI
- SCK (Static Cipher Key)
 - 直通模式加密
 - 最多 32 SCKs/MS



5. TETRA系统的安全技术之二：空中接口加密

个人识别码 (ISSI) 和组织识别码 (GSSI) 采用CCK加密



5. TETRA系统的安全技术之二：空中接口加密

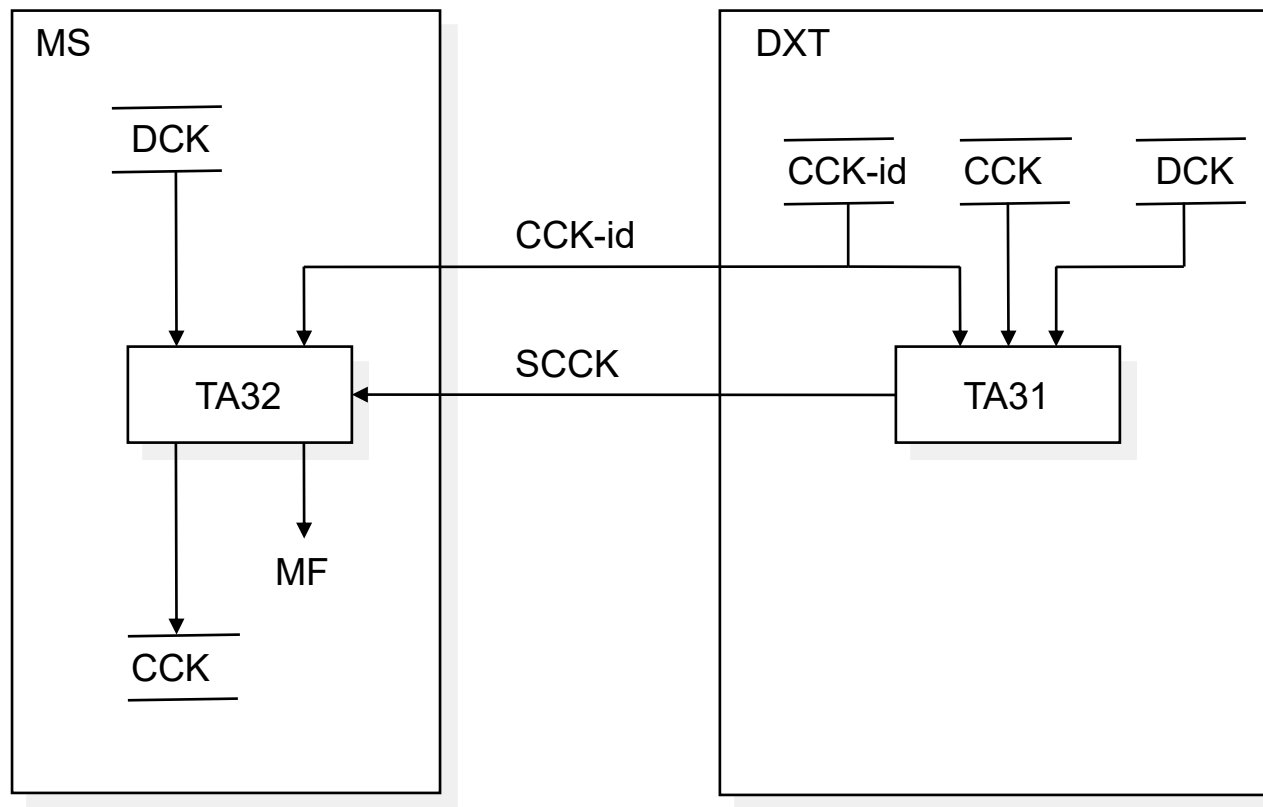
空中接口密钥管理： CCK 的改变

- CCK 在DXT中生成。
- CCK 在BS 的启动过程中进行更新。
- 除了在BS启动时，采用“广播更改”方式更改CCK。
- 当SwMI 在广播消息中通知MS需要更改CCK时，MS 激活更新CCK操作。
- 当MS发现在当前的小区中CCK-id变化了，且MS不知道这个LA的新的CCK 时，MS 激活更新CCK操作。
- 采用OTAR协议以加密形式向MS传输密钥
- 密钥的更新可采用人工方式或定期地激活
- 参数： CCK更换的时间间隔-缺省值为21天

5. TETRA系统的安全技术之二：空中接口加密

■空中接口密钥管理： CCK OTAR

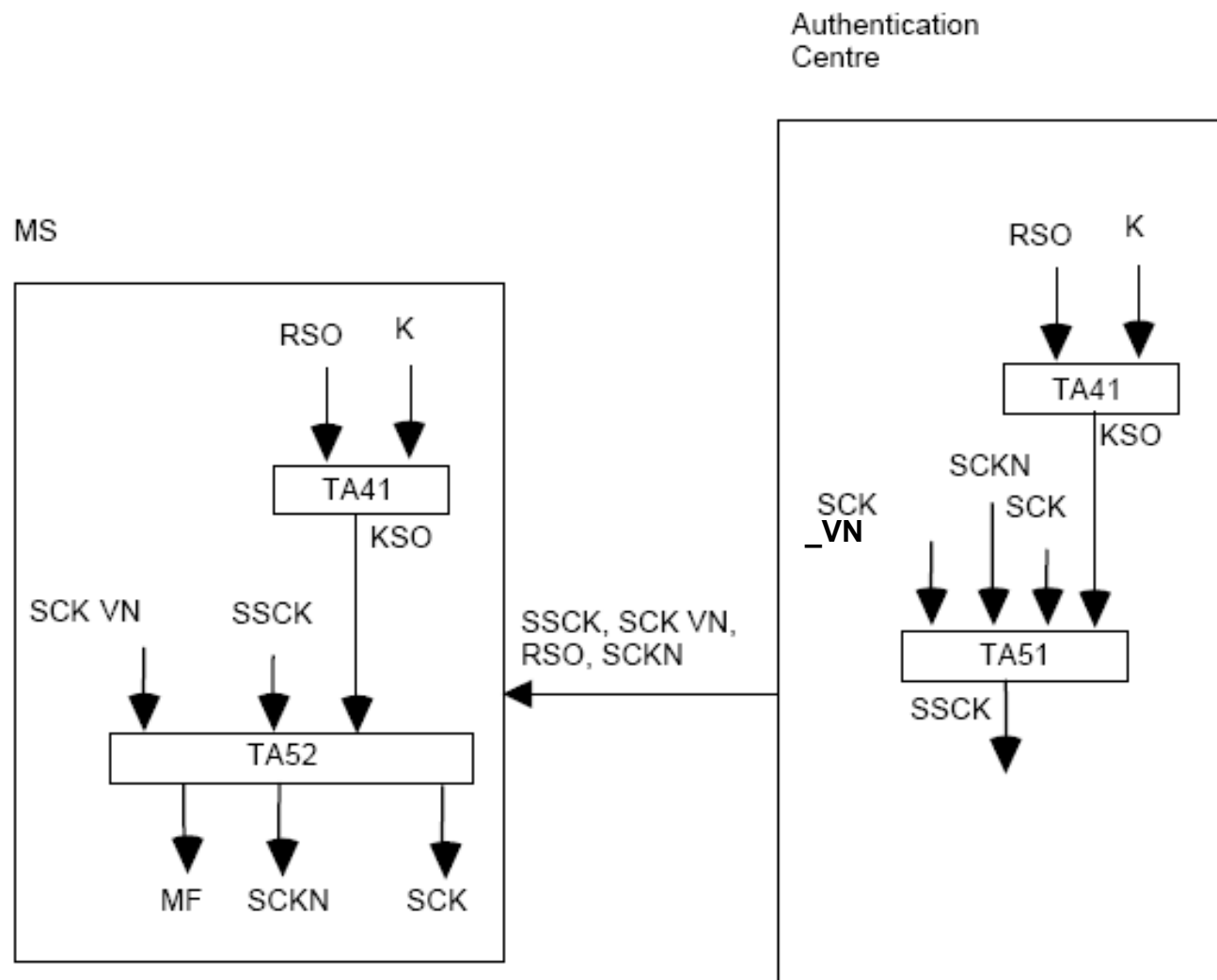
- 从SwMI 到 MS通过空中传送 CCK的机制
- 传送消息使用个人地址
- 密钥采用加密封装传送
- 采用DCK作为CCK的加密密钥
- CCK-id: CCK密钥的标识
- 只有收到正确的CCK-id, 才能解密出正确的CCK



5. TETRA系统的安全技术之二：空中接口加密

空中接口密钥管理：SCK分发

- 鉴权中心向某个MS下发SCK
- SCK用于等级2和DMO方式
- KSO: 由RSO(随机种子)和K通过TA41产生，减少密钥K的使用。
- SCKN: SCK编号，标识该密钥在这32个SCK密钥中的位置
- SCK_VN: SCK版本号，防止重放攻击。



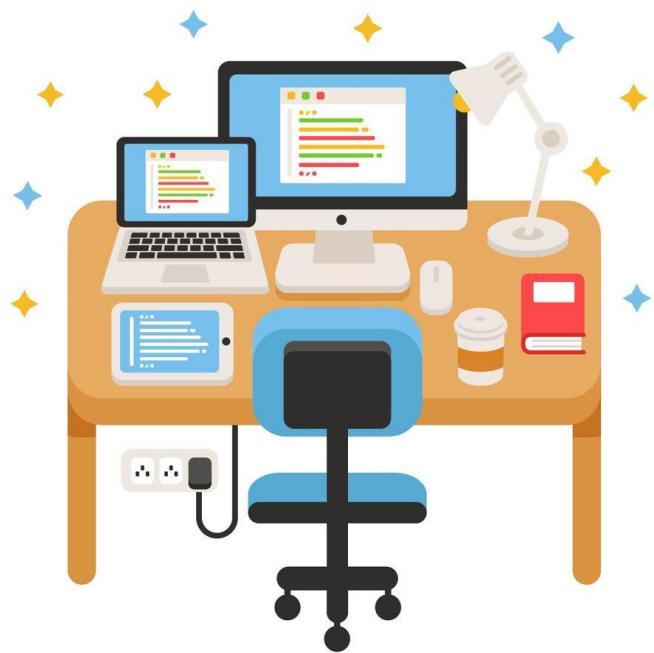
鉴权中心向某个MS下发SCK

5. TETRA系统的安全技术之二：空中接口加密

标准 AI 加密算法

	Algorithm	Distribution
Authentication	TAA1	free to most countries in the world
General Encryption	TEA1	free to most countries in the world
European Police Encryption	TEA2	European public safety and security users (restricted use)
General Police Encryption	TEA3	Public safety and security users outside Europe

- 受控算法，由ETSI/SAGE (Security Algorithms Group of Experts)开发
- 在MS, TBS 和 DXT中算法得到有效保护
- 每个MS在登记时协商所采用的算法



1. 数字集群系统及TETRA标准简介
2. TETRA系统面临的安全威胁
3. TETRA系统的安全技术
4. TETRA系统的安全技术之一：鉴权
5. TETRA系统的安全技术之二：空中接口加密
6. TETRA系统的安全技术之三：端到端加密

6. TETRA系统的安全技术之三：端到端加密

空中接口安全 <> 端到端安全

- 除端到端安全外还需要鉴权和空中接口安全来提供以下功能：
 - 在终端和网络之间的双向鉴权
 - 保护信令
 - 用户的匿名性
 - 安全的使能功能
 - 安全并灵活地创建和关闭通话组

6. TETRA系统的安全技术之三：端到端加密

E2EE 用户需求

- E2EE 主要是终端特性
- SwMI 主要充当的是透明的传输介质，有些用户不希望SwMI对传输的信息进行任何干涉。
- 如果需要加密调度功能，调度台需要具有端到端加密功能。
- 可能需要定义只使用端到端加密呼叫的组。
- 一些权威机构可能限制端到端加密的使用。
- 使用了E2EE后，很难实施录音、监听
- 防篡改

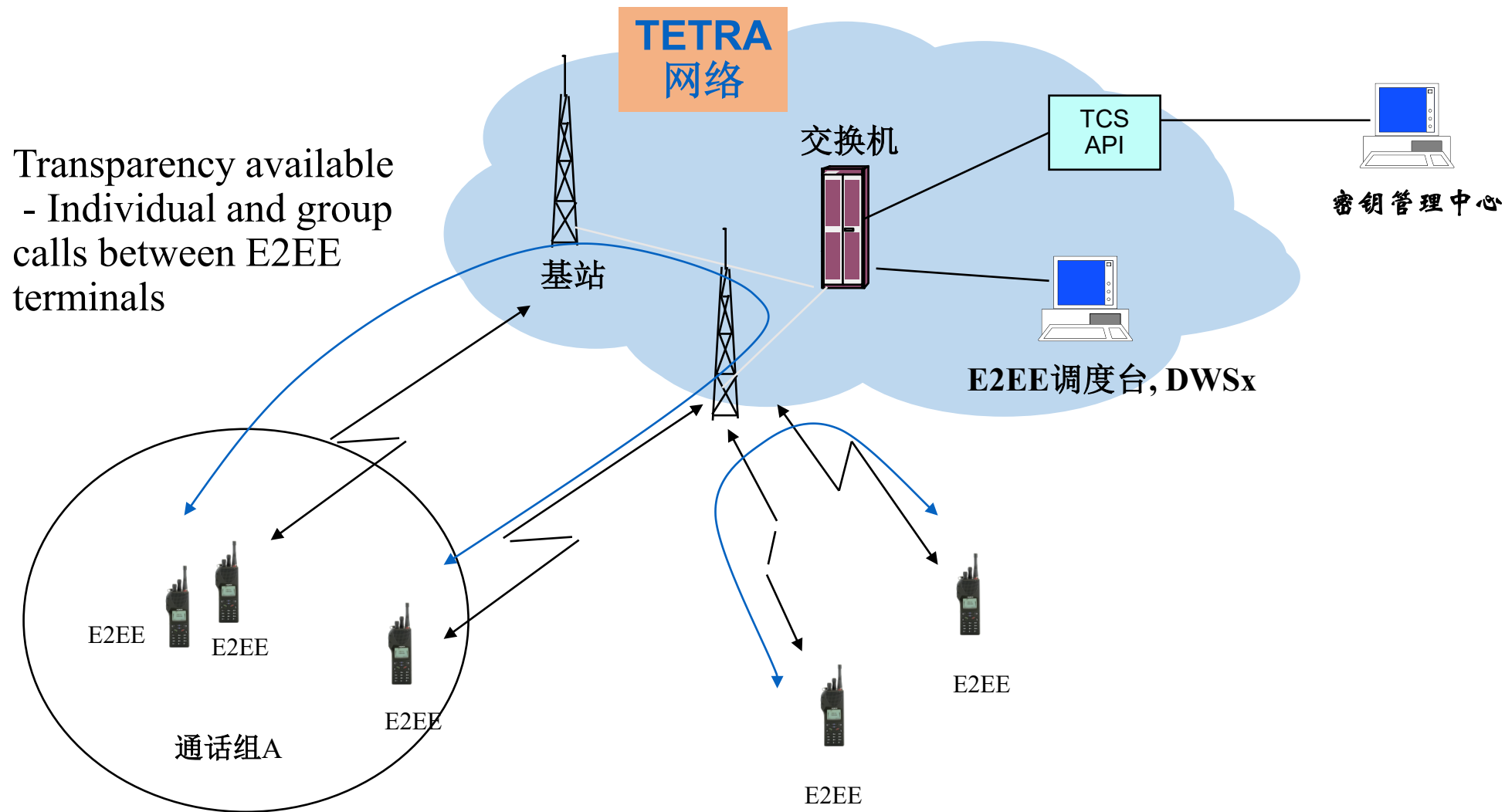
6. TETRA系统的安全技术之三：端到端加密

E2EE 信令

- E2EE服务的标识——是一个指示E2E加密呼叫和E2E加密语音项的flag。所有响应该呼叫的终端都知道这是一个端到端加密的呼叫。
- 每个终端在请求传输时指出它的加密模式。在呼叫建立时，不管所包含的信息是什么，都可选择进行加密。
- 迟到进入广播用来反映正在进行的语音的正确状态信息（是否为加密通信）。

6. TETRA系统的安全技术之三：端到端加密

TETRA系统的端到端加密方案

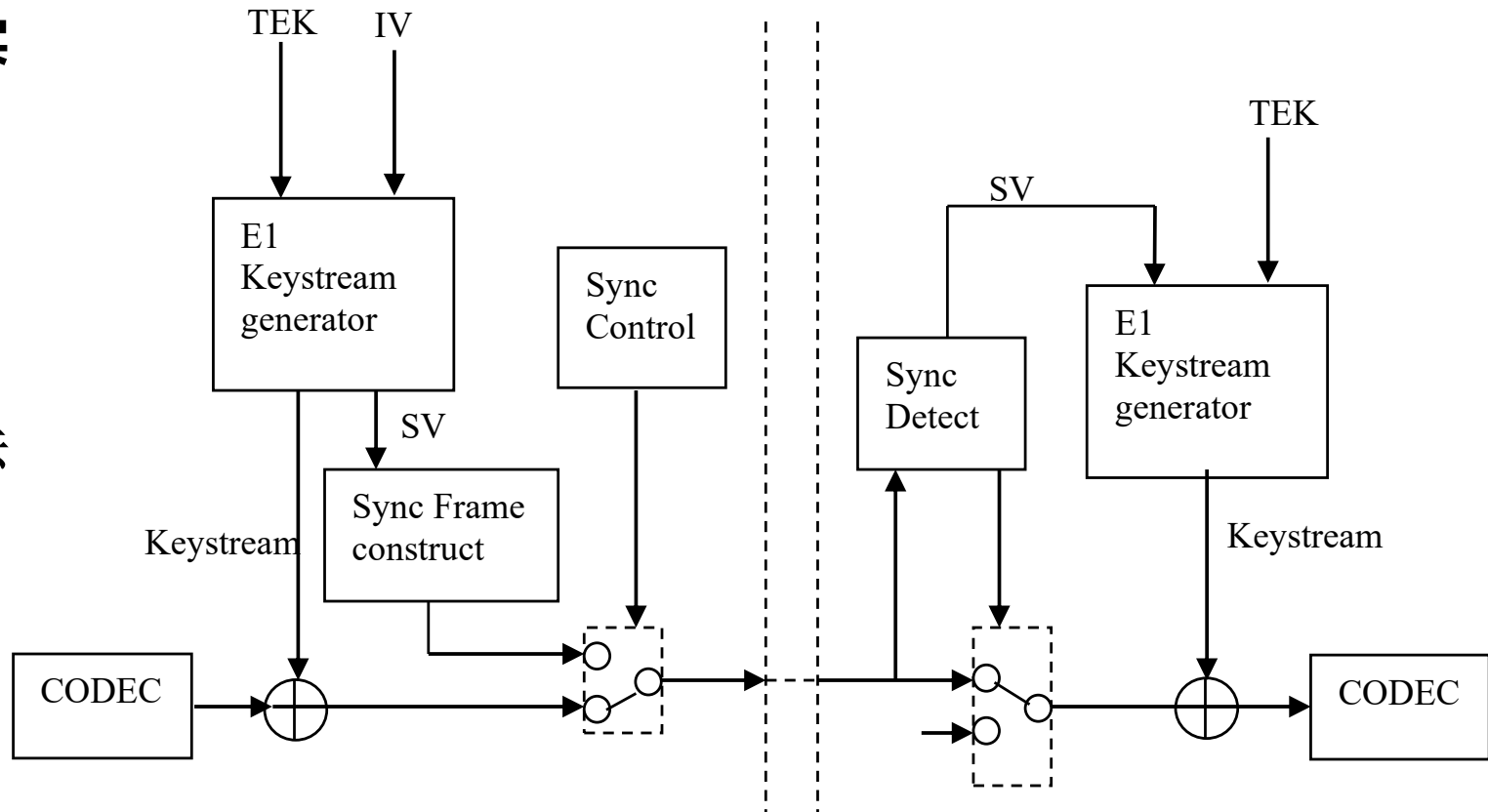


6. TETRA系统的安全技术之三：端到端加密

加密和同步

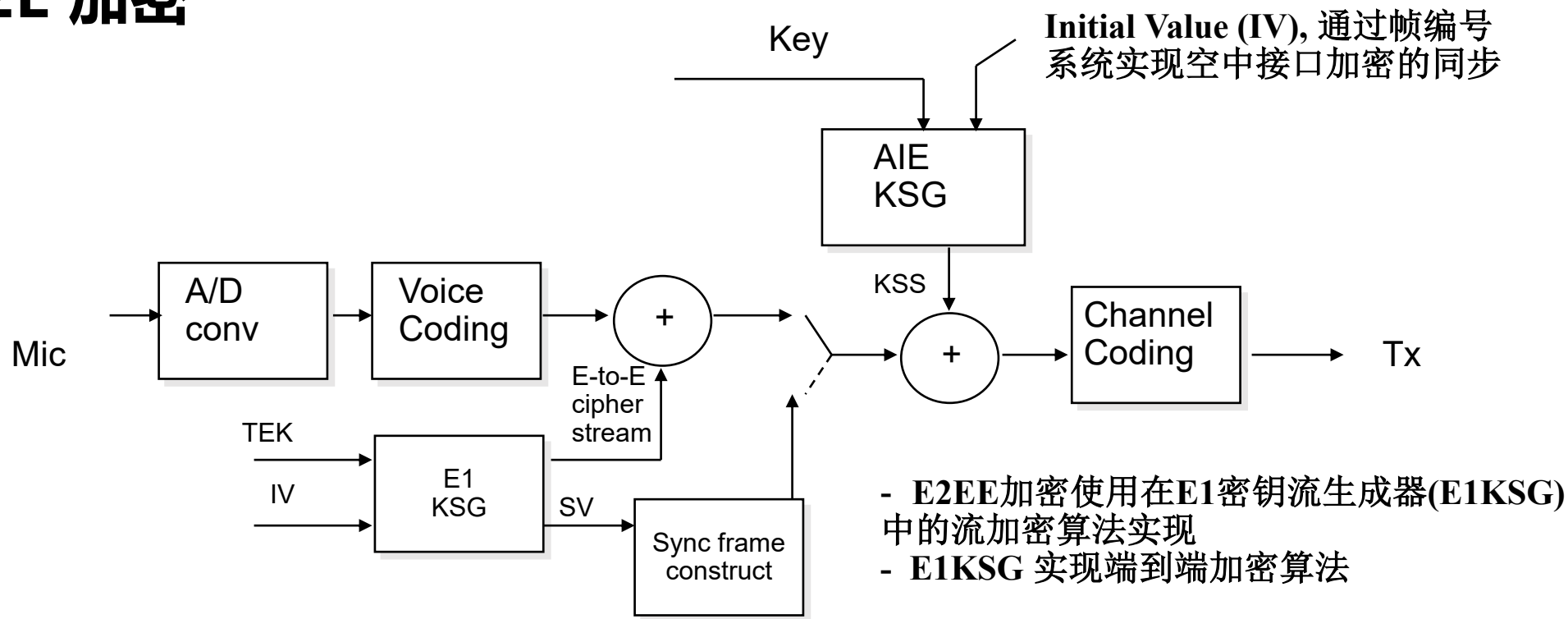
通过在U-面上窃取半个时隙的语音帧实现同步帧的传输，用于保证接收端与发送端的密钥流同步；

- 在每个传输开始时，由发送方MS生成一个随机的初始向量IV；
- 发送同步帧（包括初始向量IV，算法标识和密钥标识）；
- 接收端同步密钥流；
- 传输期间，E1生成不间断的密钥流；
- 周期性发送同步帧（1~4 SV/s）用于保持同步，以便完成解密。



6. TETRA系统的安全技术之三：端到端加密

A/I + E2E 加密



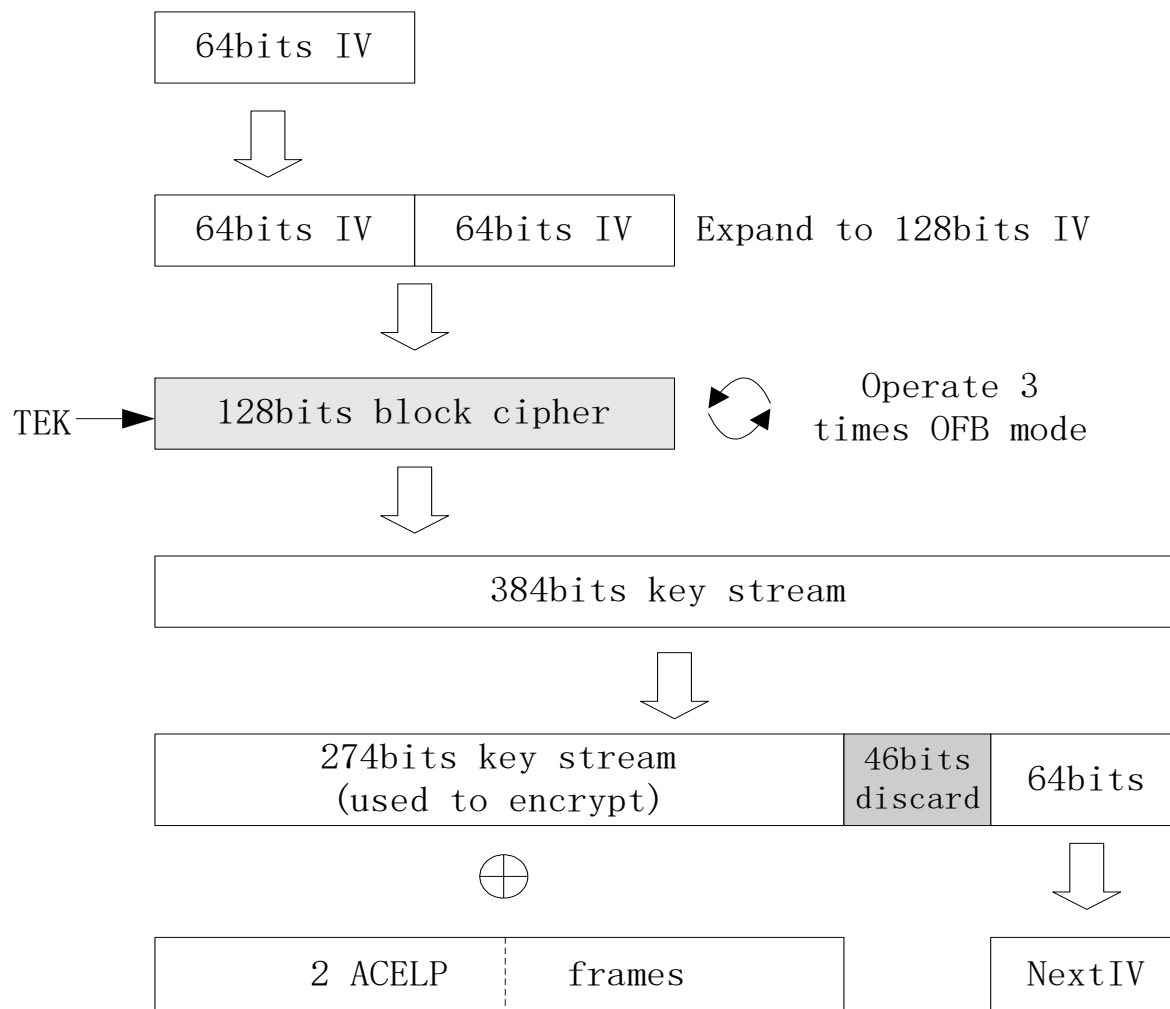
- AI-加密使用在密钥流生成器(KSG)中的流加密算法实现
- 在AIE KSG中使用加密算法 (TEA1,TEA2.....)
- 每个时隙都采用密钥流进行加密 (KSS), KSS是密钥比特流的序列

6. TETRA系统的安全技术之三：端到端加密

E1算法：完成密钥流的生成

- 核心算法：**128**位的分组加密算法

1. 64bits的IV扩展
2. 采用OFB(输出反馈模式)运行三圈后得到384bits的输出数据
3. 前274bits作为密钥流用来和语音编码后的2个语音帧进行异或
4. 最后的64bits作为下一轮的E1算法的IV，用来产生后面的密钥流



6. TETRA系统的安全技术之三：端到端加密

E3算法

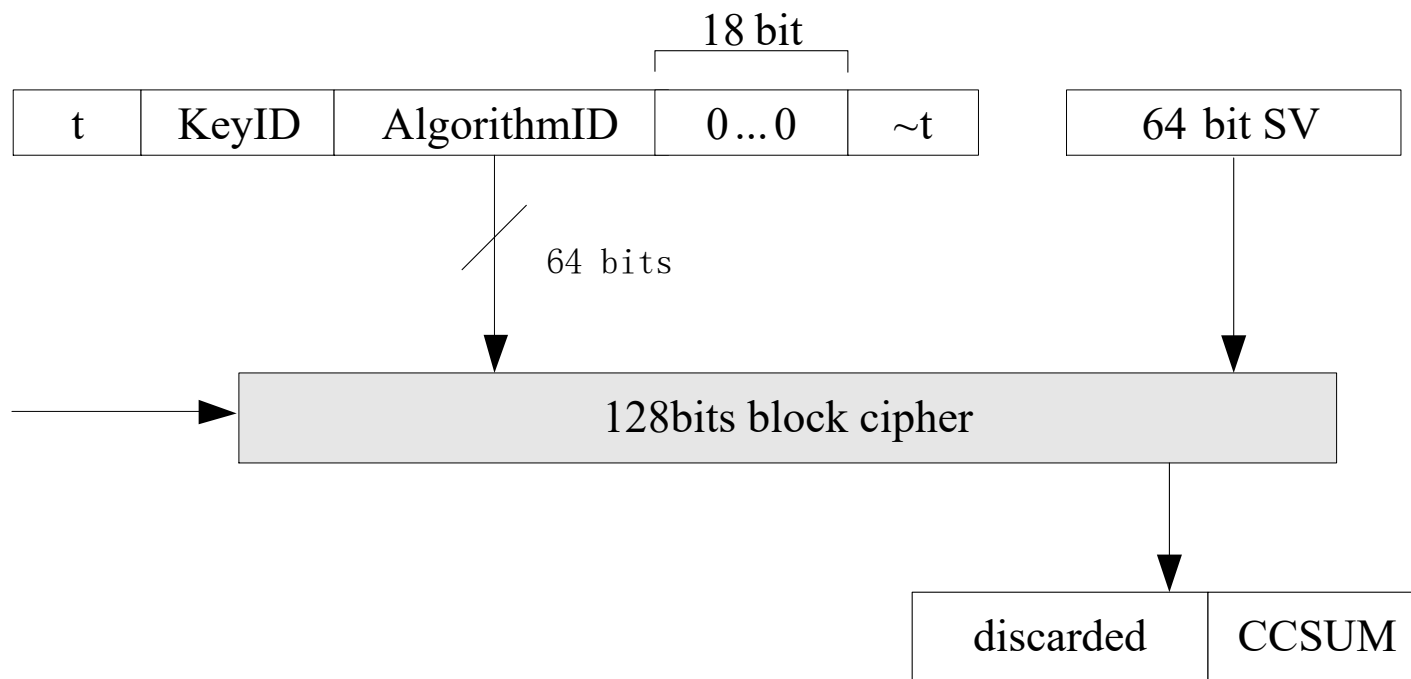
■ 同步帧



- 算法标识：接收方选择正确的算法
- 密钥标识：接收方选择正确的密钥
- 同步向量SV：用于进行收发两端的密钥流同步；
- 同步帧校验和，防篡改：  TEK

■ 区分IV和SV

- **IV**用于生成密钥流，**SV**用于同步；
- **SV**是**IV**的“传输形式”



6. TETRA系统的安全技术之三：端到端加密

TETRA E2EE的密钥管理

- 主要思路
 - 预共享密钥体系
 - 终端接收密钥管理消息，存储通信密钥
 - 通信时，直接使用存储的通信密钥进行通信
 - 集中的密钥管理系统
 - 负责密钥生成、分发、更新等
 - 采用三级密钥管理
 - 主密钥
 - 密钥管理密钥
 - 通信密钥

6. TETRA系统的安全技术之三：端到端加密

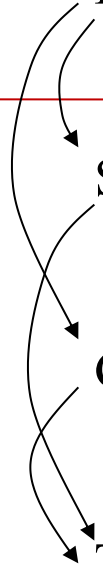
TETRA E2EE的密钥管理

- E2EE密钥种类
 - 主密钥
 - KEK (Key Encryption Key) 主加密密钥
 - 用于加密GEK或SEK;
 - 管理密钥
 - GEK (Group Encryption Key) 组加密密钥
 - 用于加密TEK, 也可以用KEK代替GEK;
 - SEK (Signaling Encryption Key) 消息加密密钥
 - 用于加密OTAK消息, 也可以用GEK或KEK来代替SEK;
 - 通信密钥
 - TEK (Traffic Encryption Key) 通信加密密钥
 - 用于所有的端到端用户通信数据的加密。

6. TETRA系统的安全技术之三：端到端加密

■ E2EE密钥种类

<i>Distribution method</i>	<i>Key type</i>	<i>Keys / terminal</i>	<i>Lifetime</i>
OOB	KEK (Key Encryption Key)	1	Long
OTAK	SEK (Signalling Encryption Key) - optional (OTAK)	1	Intermediate
	GEK (Group Encryption Key)	group num	Intermediate
	TEK (Traffic Encryption key)	n (< 4096) - different versions	Short



6. TETRA系统的安全技术之三：端到端加密

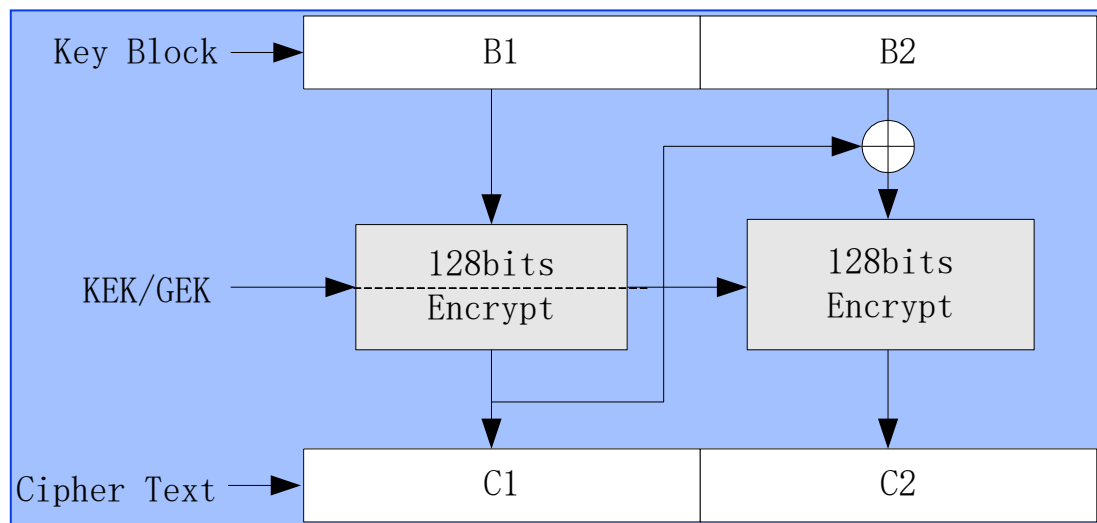
密钥管理方法

- **OOB(Out Of Band)带外密钥管理**
 - 通过适当软硬件工具直接将密钥下载到TETRA终端；
- **OTAK(Over The Air Keying)密钥管理， TETRA MoU 推荐02中详细描述**
 - 通过空中接口传送或管理TETRA终端的密钥；
 - 采用OTAK 消息 (SDS消息)管理终端中的密钥
 - 所有的OTAK 消息 (除了Registration消息)都采用E4算法和SEK、 GEK 或 KEK加密
 - OTAK消息按照个人地址发给某个终端或按照组地址广播给一组终端

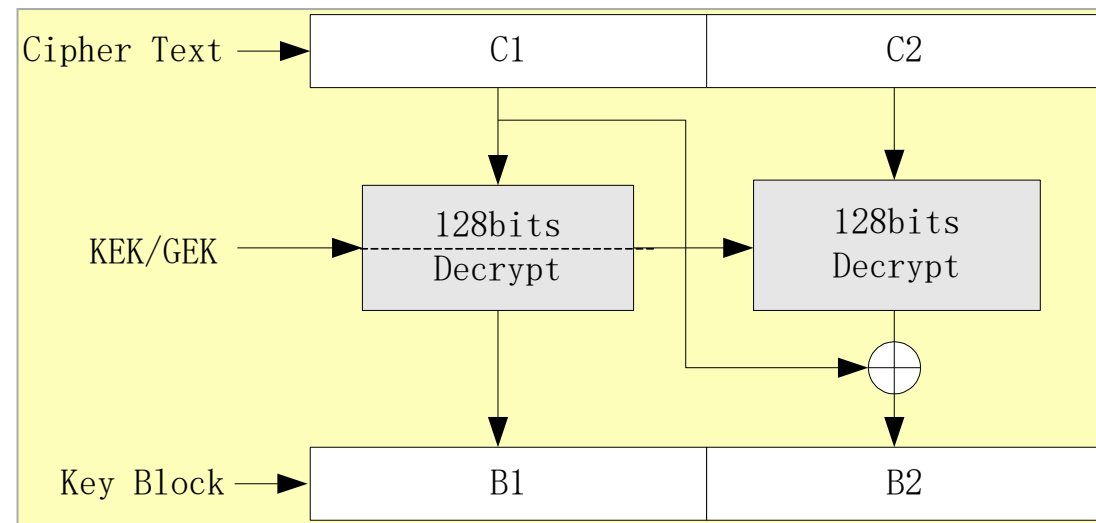
6. TETRA系统的安全技术之三：端到端加密

E2算法

■ 加密密钥算法



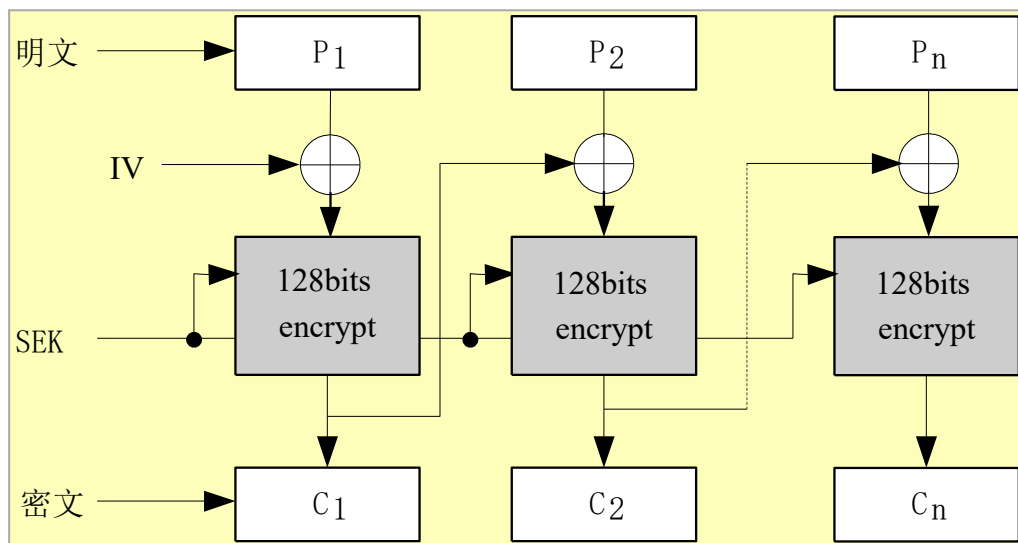
■ 解密密钥算法



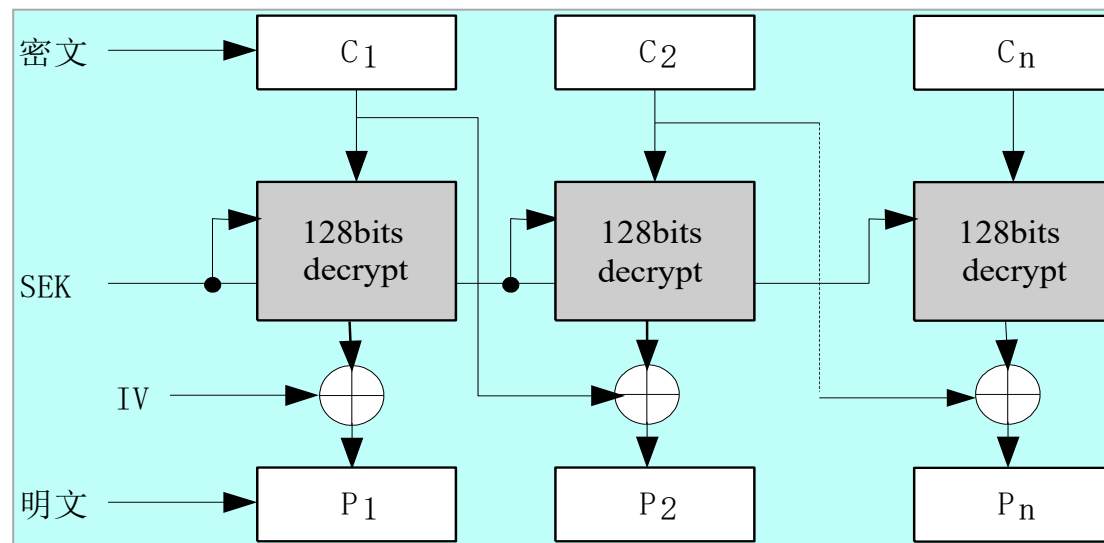
6. TETRA系统的安全技术之三：端到端加密

E4算法

■ OTAK消息加密算法



■ OTAK消息解密算法



6. TETRA系统的安全技术之三：端到端加密

算法总结

算法名称	用途	分组算法运行模式
E1	用于语音的密钥流生成	OFB
E2	密钥加/解密	CBC
E3	计算校验和	ECB
E4	OTAK消息加/解密	CBC
E5	用于SDS的密钥流生成	OFB
E6	用于SDS的消息完整性算法	CBC

6. TETRA系统的安全技术之三：端到端加密

TETRA E2EE具体实施的建议

- 需要采用有足够强度、符合国家相关规定的算法；
- 通过适当的安全工程设计MS和保护MS中敏感的密钥；
- 为防止OTAK消息被重放或被分析并修改，对OTAK消息进行密码保护；
- 为了保证KEK安全，尽量减少KEK的使用，使用SEK或GEK保护OTAK消息；
- 为了防止重放攻击或通过删除/插入方式破坏同步向量SV，建议在同步帧中嵌入时间戳和密码校验和；
- 为了防止OTAK消息的重放攻击，在OTAK消息中嵌入序列数；
- 为了防止假冒消息删除或更改E2EE密钥，需指定OTAK密钥管理中心的地址；
- 带外设置关键安全参数，包括自身的KEK，KMC的ITSI以及SEK。

- 基本安全机制：
 - 鉴权
 - 空中接口安全
- 增强安全机制：
 - 端到端安全
- 关键：
 - 算法、协议、密钥管理
- 网址：
 - <http://www.etsi.org>
 - <http://www.tetramou.com>

1. 请比较GSM接入认证方法与TETRA接入认证方法的相同点和不同点。
2. 请比较下面三种信息加密方式：
 - GSM空口加密
 - TETRA空口加密
 - TETRA端到端加密

在端到端加密中：

1. 加密模块的功能范畴？

- 生成密钥流 $\leftrightarrow$ 生成密钥流 + 异或

2. 如何检验终端的加密模块没有旁路？

- 语音是否加密？
- 是否采用生成的密钥流加密的？

- **ETR 086-3 (1994). Trans European Trunked Radio (TETRA) system; Technical requirements specification Part 3: Security aspects**
- **ETS 300 392-1. Radio Equipment and Systems(RES); TETRA; Voice plus Data (V + D); Part 1 : General network design**
- **ETS 300 392-2. Radio Equipment and Systems(RES); TETRA; Voice plus Data (V + D); Part 2 :Air Interface (AI)**
- **ETS 300 392-7.Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security**
- **ETS 300 396-2. TETRA; Technical requirements for Direct Mode Operation (DMO); Part 2: Radio aspects**
- **ETS 300 396-3. TETRA; Technical requirements for Direct Mode Operation (DMO) ; Part 3 : Mobile Station to Mobile Station (MS - MS) Air Interface (AI) protocol**

谢谢！