

课程编号：3182121321

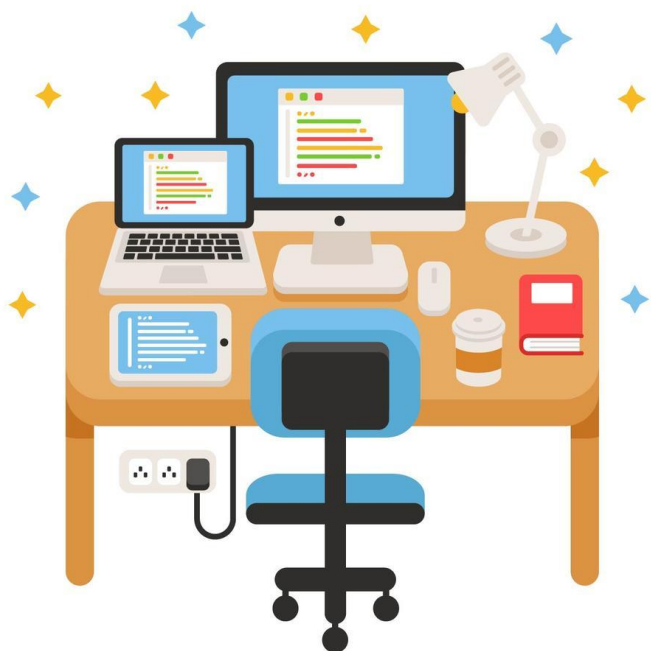
无线通信安全



第八讲 LTE安全

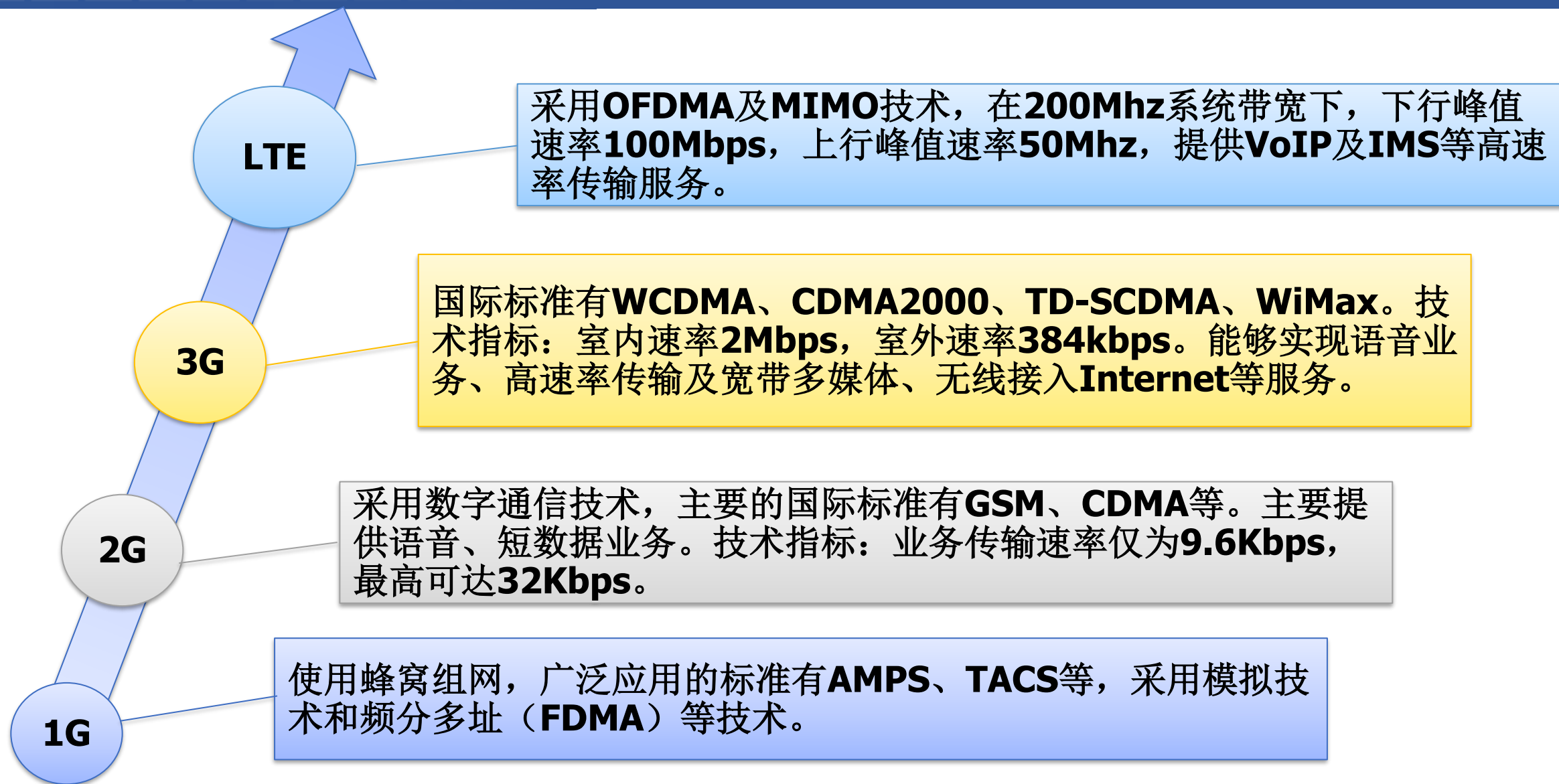
李晖

lihuill@bupt.edu.cn



1. LTE简介
2. LTE安全威胁
3. LTE安全架构
4. LTE安全机制
 - ✓ 匿名
 - ✓ 认证
 - ✓ 密钥管理
 - ✓ 传输安全机制

1. LTE简介：移动无线技术的演进路径



1. LTE简介

LTE简介

- 2005年开始由3GPP组织制定
- LTE(Long Term Evolution)长期演进项目
- SAE (System Architecture Evolution) 系统架构演进项目
- 主要特点
 - 支持1.25MHz~20MHz带宽
 - 峰值数据率：上行50Mb/s，下行100Mb/s
 - 支持增强的IMS (IP多媒体子系统)
 - 取消电路交换 (CS) 域，CS域业务在包交换 (PS) 域实现，如采用VoIP

1. LTE简介

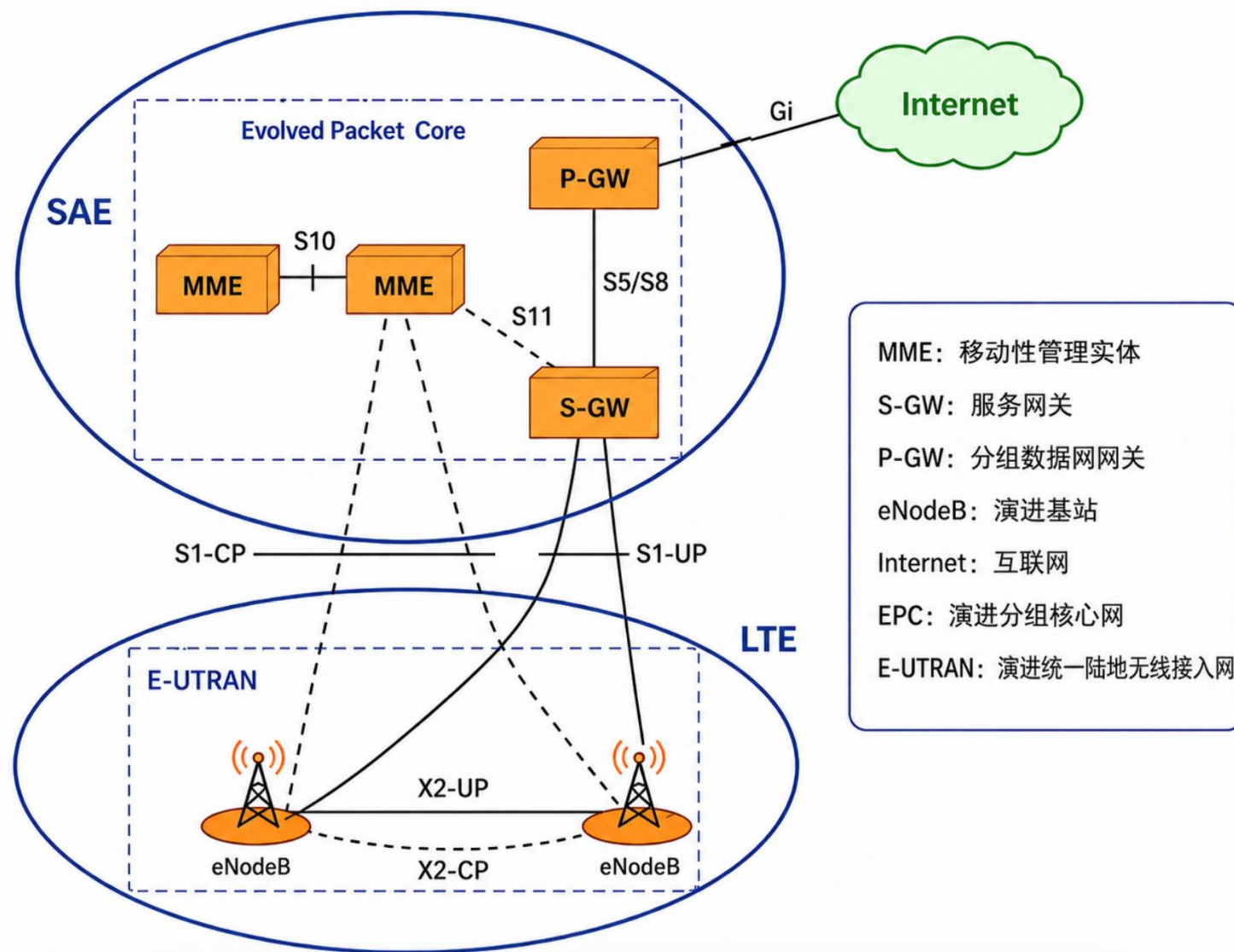
LTE网络

■ LTE接入网

- 由eNB组成
- eNB可以位于不完全可信的区域

■ SAE核心网

- 取消了CS域
- MME完成认证
- MME完成NAS信令的安全保护
- S-GW完成合法侦听功能、数据包的路由和前转等功能；
- P-GW完成基于用户的包过滤功能、合法侦听功能、UE的IP地址分配功能等。

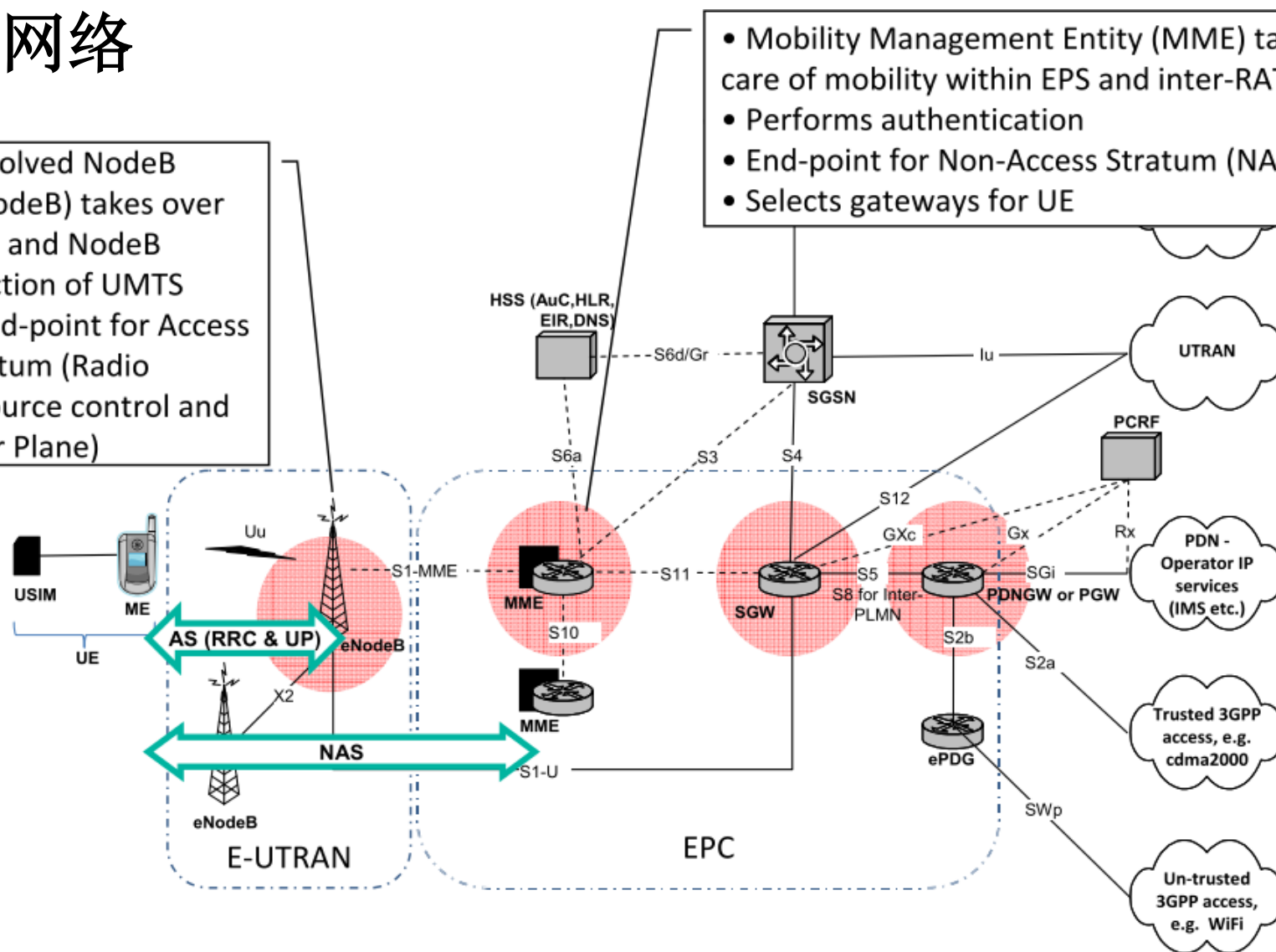


1. LTE简介

LTE网络

- evolved NodeB (eNodeB) takes over RNC and NodeB function of UMTS
- End-point for Access Stratum (Radio resource control and User Plane)

- Mobility Management Entity (MME) takes care of mobility within EPS and inter-RAT
- Performs authentication
- End-point for Non-Access Stratum (NAS)
- Selects gateways for UE



AS: 接入层

NAS: 非接入层

RRC: 无线资源控制

UP: 用户层

eNodeB: 演进型基站

MME: 移动性管理实体

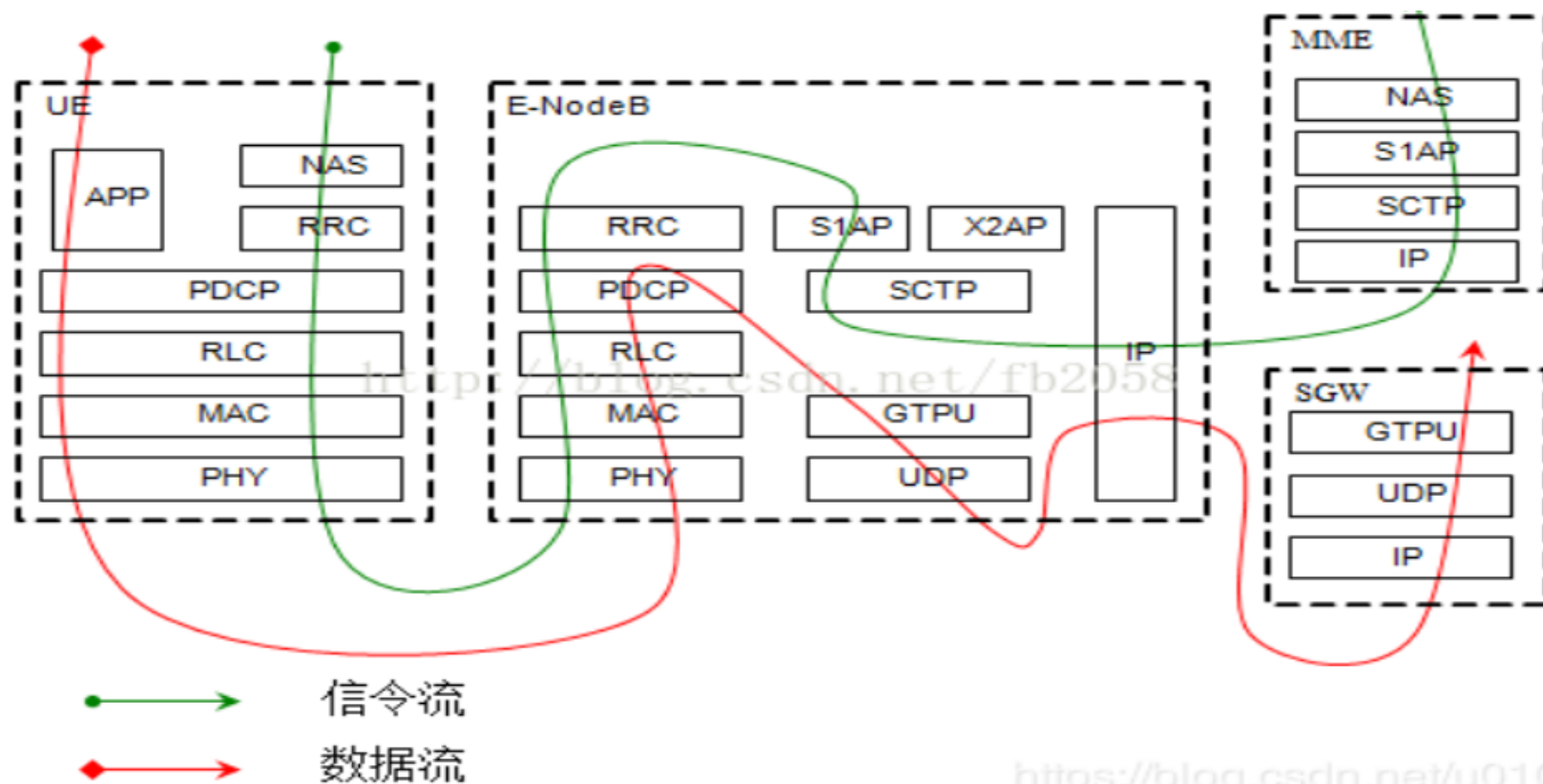
SGW: 服务网关

PDNGW: 分组数据网网关

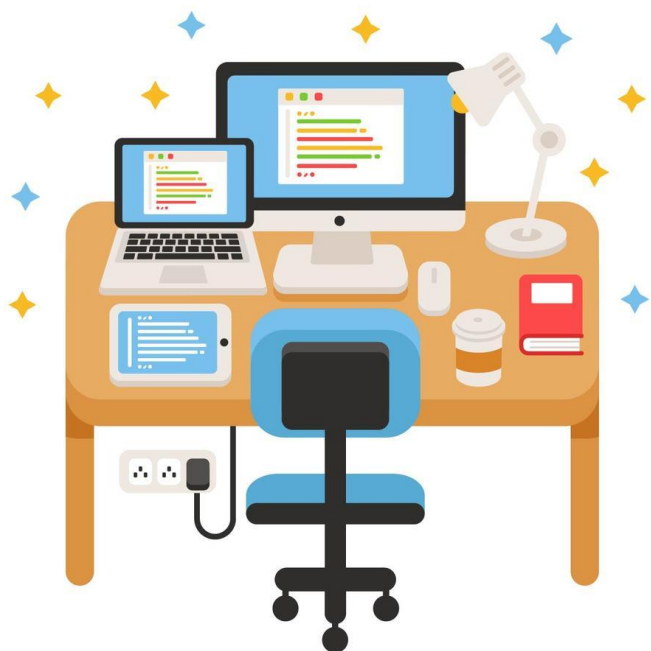
HSS: 原籍用户服务器

1. LTE简介

LTE协议栈



PDCP(Packet Data Convergence Protocol)分组数据汇聚协议, 压缩和解压IP头、传输用户数据和信令



1. LTE简介
2. **LTE安全威胁**
3. LTE安全架构
4. LTE安全机制
 - ✓ 匿名
 - ✓ 认证
 - ✓ 密钥管理
 - ✓ 传输安全机制

2. LTE安全威胁

LTE安全威胁

- 3G网络面临的安全威胁同样存在
- 与3G网络相比最大的不同来源于eNB
 - eNB体积小、成本低，部署在不安全的地点，与核心网连接所使用的传输链路不安全。
 - 对 eNB（尤其是 home eNB）的物理攻击是可能的
 - 对 eNB的网络攻击是可能的

2. LTE安全威胁

- 基本安全要求
 - 继续使用USIM
 - 安全性要不低于或高于UMTS的安全性
- 具体要求
 - UE与网络之间要有双向认证
 - 无线链路的机密性可选
 - RRC与NAS要有强制完整性保护机制
 - 用户层面的数据完整性保护可选
 - 要保护用户标识
 - 网元之间要进行双向认证
 - 网络域之间是否需要机密性或完整性保护由运营商来决定
 - 对演进基站的安全性要求增多（下页）

2. LTE安全威胁

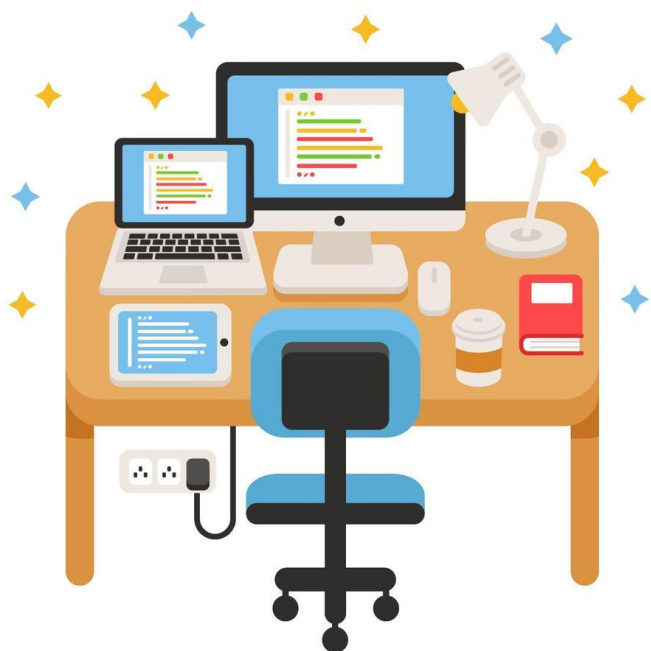
■ 具体要求

■ 对演进基站的安全性要求增多

- 使用授权的数据、软件
- 安全加载或启动
- 在授权情况下方可改变数据和软件
- 密钥要保存在安全环境中

■ 对密钥管理的要求

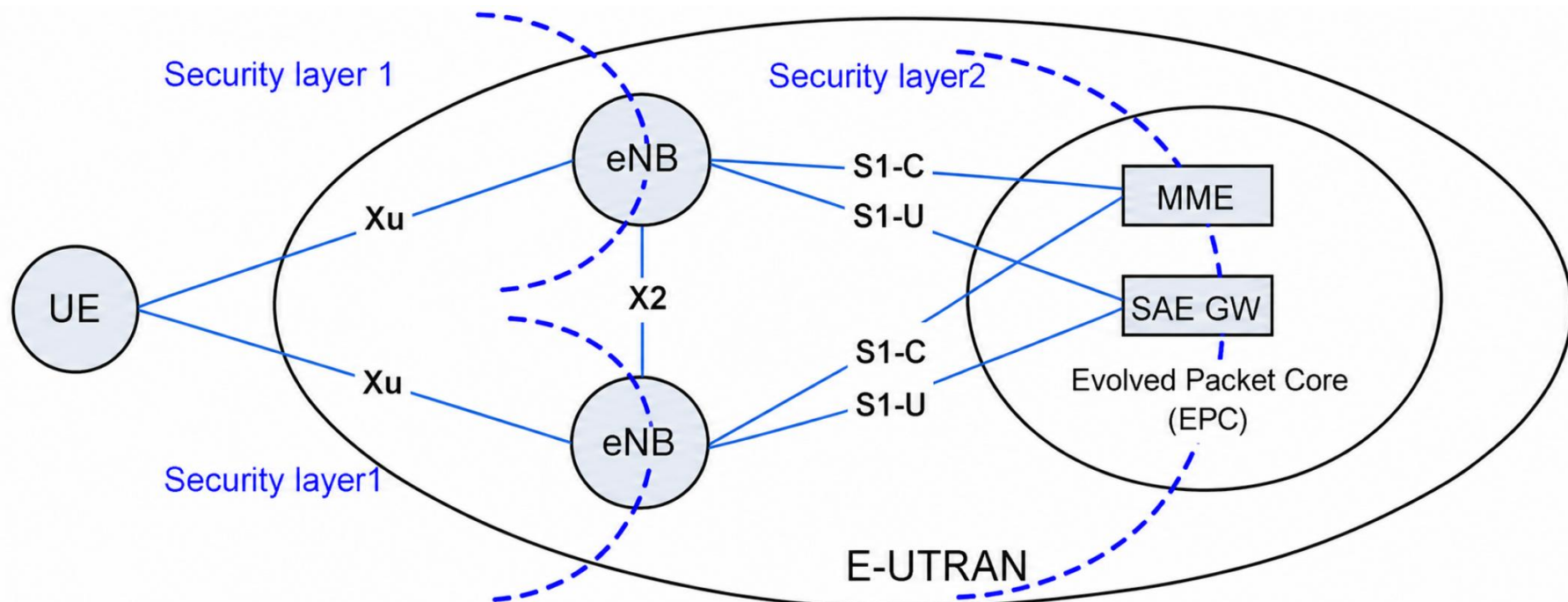
- 由于仍然使用流密码加密信息，避免密钥流重用，还要避免经常执行AKA协议，因为AKA协议在USIM中完成密钥计算需要数百ms的计算时间
- 需要在不执行AKA的情况下提供一套密钥更新机制



1. LTE简介
2. LTE安全威胁
3. **LTE安全架构**
4. LTE安全机制
 - ✓ 匿名
 - ✓ 认证
 - ✓ 密钥管理
 - ✓ 传输安全机制

3. LTE安全架构

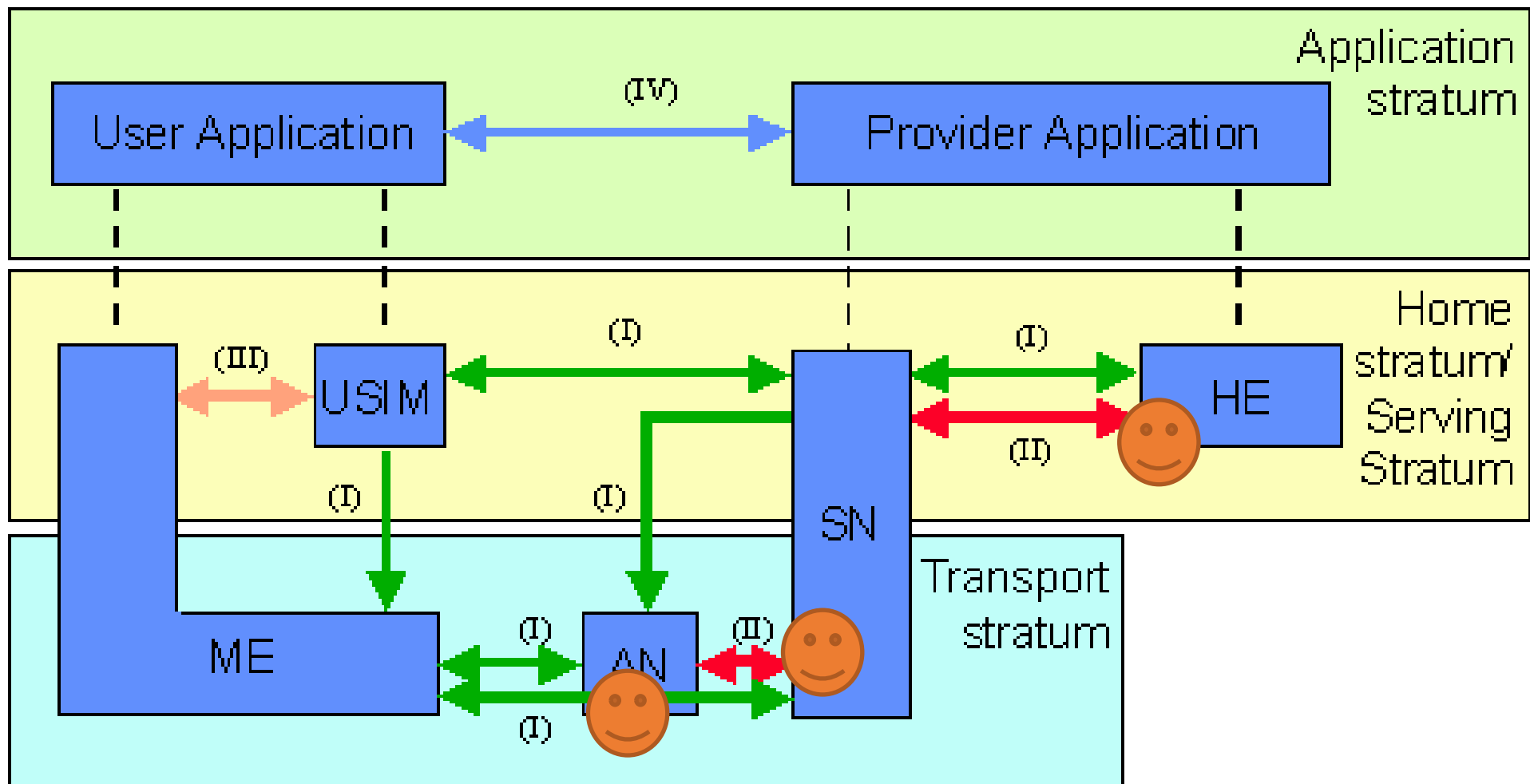
安全层次

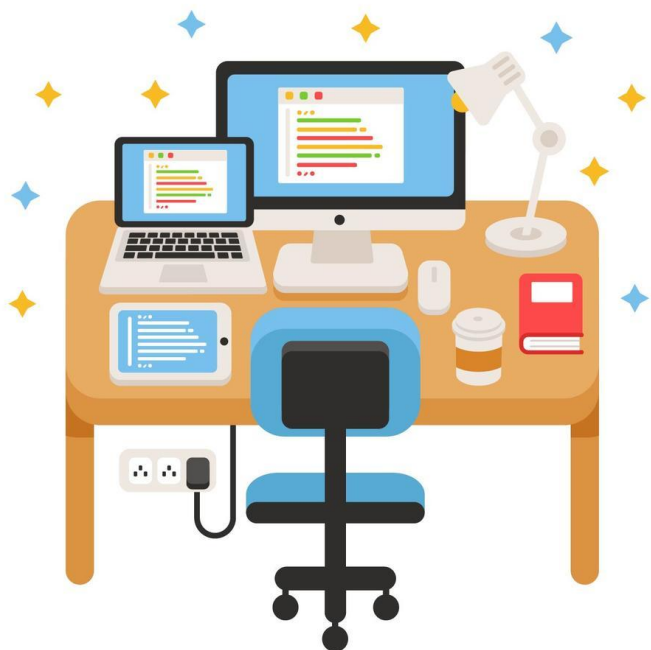


- 由于eNB处于一个不完全信任区域，因此LTE/SAE的安全包括**两个层次**：
 - **接入层 (AS) 安全**：UE与eNB之间的安全，主要执行AS信令的加密和完整性保护，用户面UP的机密性保护。
 - **非接入层 (NAS) 安全**：UE与MME之间的安全，主要执行NAS信令的加密和完整性保护。

3. LTE安全架构

LTE安全架构





1. LTE简介
2. LTE安全威胁
3. LTE安全架构
4. **LTE安全机制**
 - ✓ 匿名
 - ✓ 认证
 - ✓ 密钥管理
 - ✓ 传输安全机制

4. LTE安全机制

匿名与认证

■ 匿名

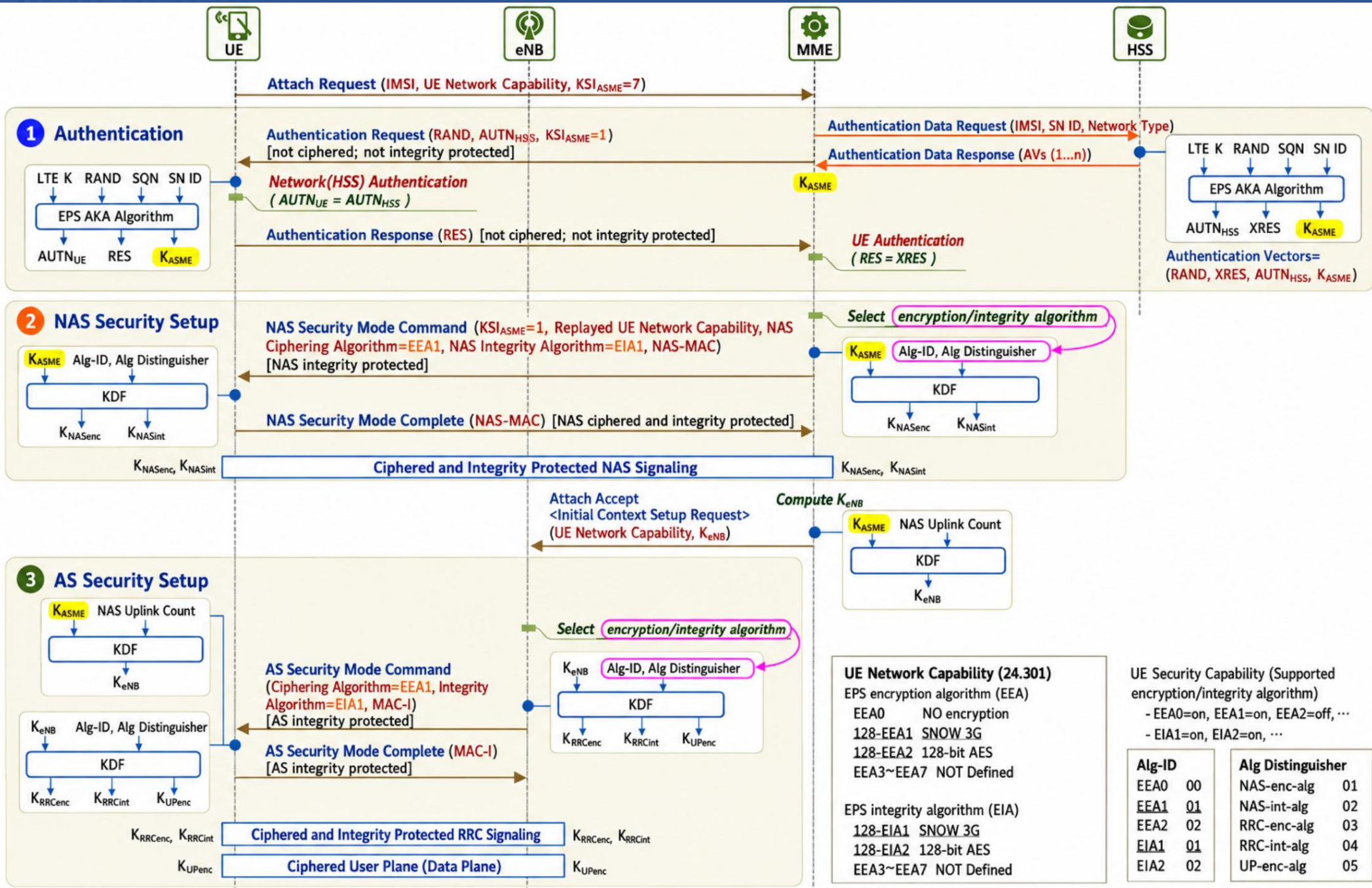
- 定义了一个明确的UE临时标识GUTI，以隐藏UE或用户永久身份。
- GUTI的完整格式为<GUTI> = <MCC><MNC><MMEGI><MMEC><M-TMSI>
- S-TMSI是GUTI的缩简形式，以达到更高效的无线信令交互程序，如用在寻呼和服务请求中来识别移动终端。
- <S-TMSI> = <MMEC><M-TMSI>

■ 认证

- LTE/SAE的AKA过程继承于UTMS的AKA过程，认证过程基本一致，认证向量的产生方法也一样，只是认证向量中CK，IK变为 K_{ASME} 。

4. LTE安全

LTE安全 链接建立 过程



4. LTE安全机制

LTE认证过程

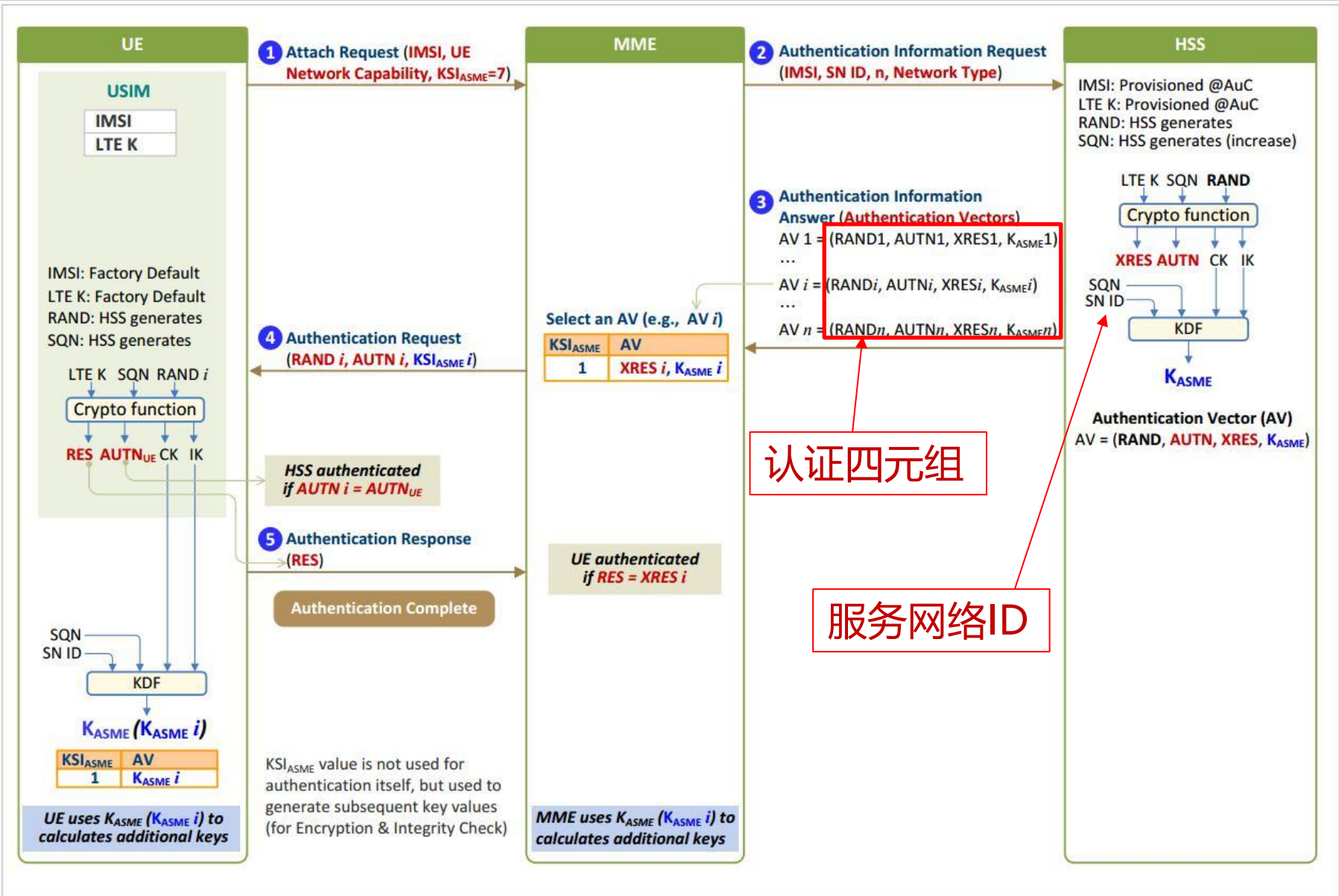
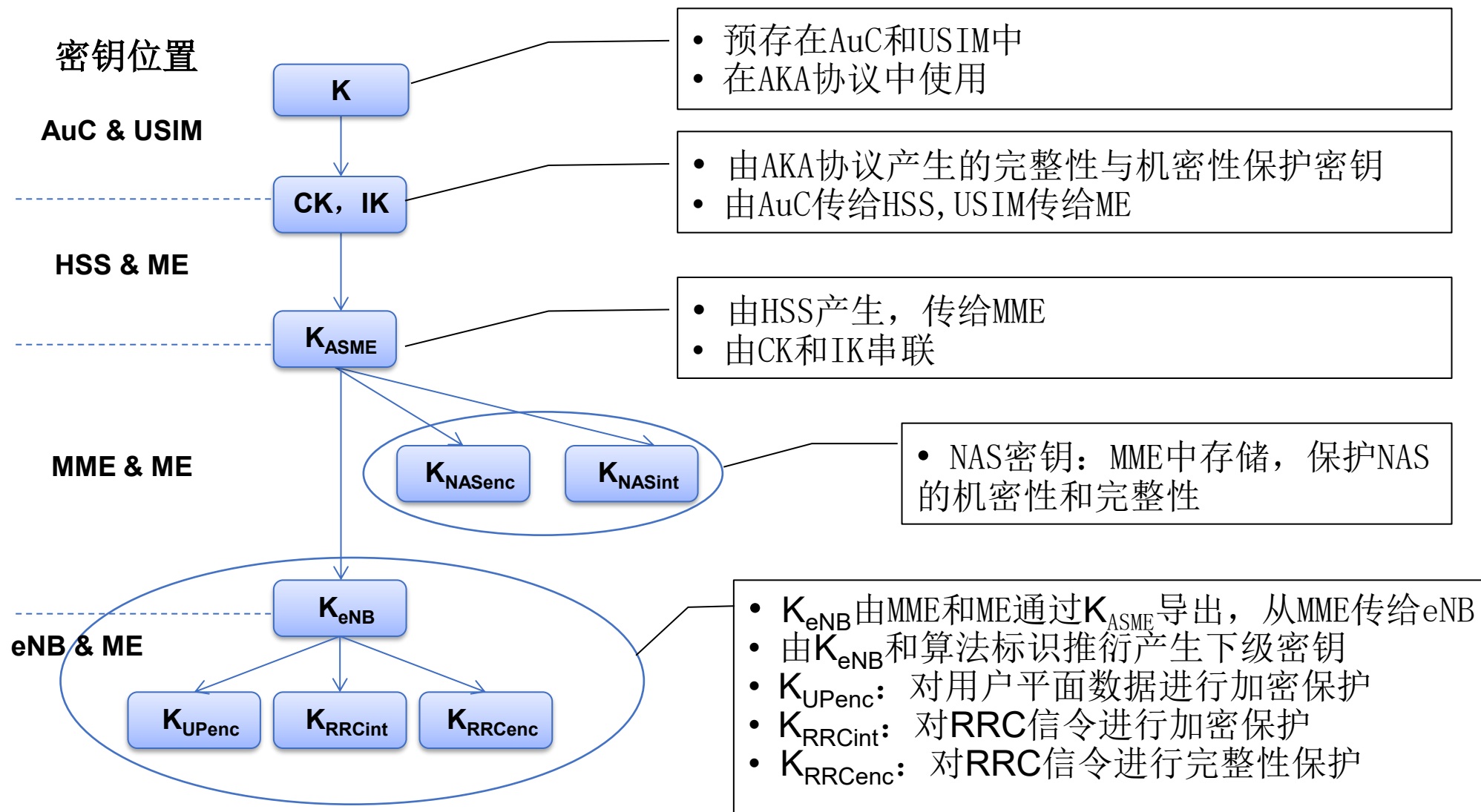


Figure 3. LTE authentication procedure

4. LTE安全机制

密钥结构

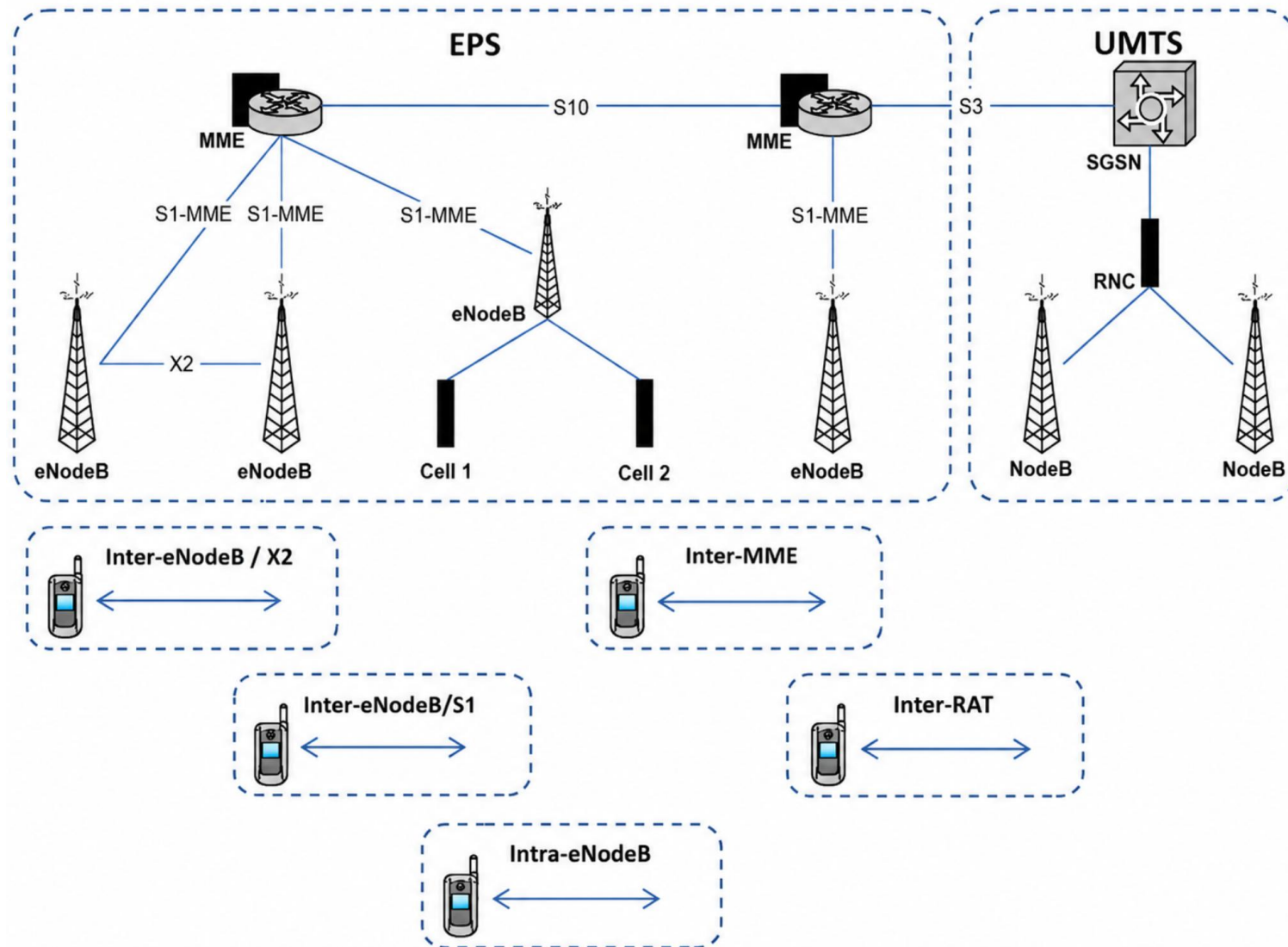


4. LTE安全机制

LTE中的切换安全

包含

- 网间切换
 - 网内切换
 - 基于X2的切换
 - 基于S1的切换
 - eNB内切换



4. LTE安全机制

LTE中的切换安全

- 切换安全原则

- 后向安全（backward security）：

- 目标eNB不能破解源eNB与UE之前的信息
 - 目标eNB不能获得源eNB使用的密钥

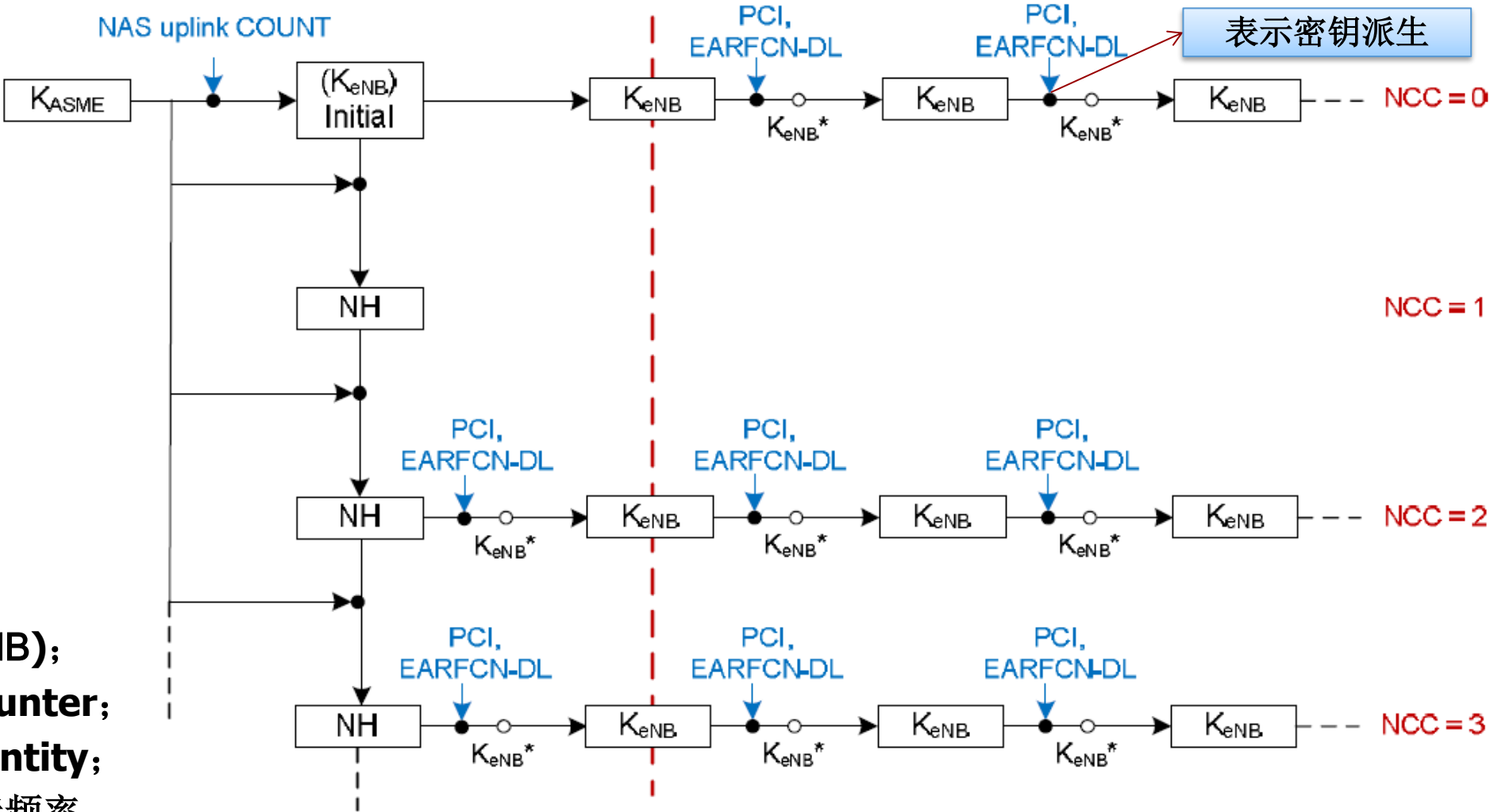
- 前向安全（forward security）：

- 源eNB不能破解目标eNB与UE之后的信息
 - 源eNB不能获得目标eNB使用的密钥

4. LTE安全机制

切换安全

NH: Next Hop
(MME派生, 发给eNB);
NCC: NH Chaining Counter;
PCI: Physical Cell Identity;
EARFCN-DL: 小区下行频率



4. LTE安全机制

LTE中的切换安全

■ 初始化阶段

- 当UE和eNB 建立AS安全链接时，MME和UE要从 K_{ASME} 导出 K_{eNB} 和NH。NH不能由eNB求出。
- NCC与每个 K_{eNB} 和NH关联。
- 在初始化阶段NCC=0
- 在初始化阶段MME不给eNB发NH

■ 横向派生

- K_{eNB}^* 从当前的 K_{eNB} 导出

■ 纵向派生

- K_{eNB}^* 从NH导出

■ 密钥导出时还引入了PCI和EARFCN-DL

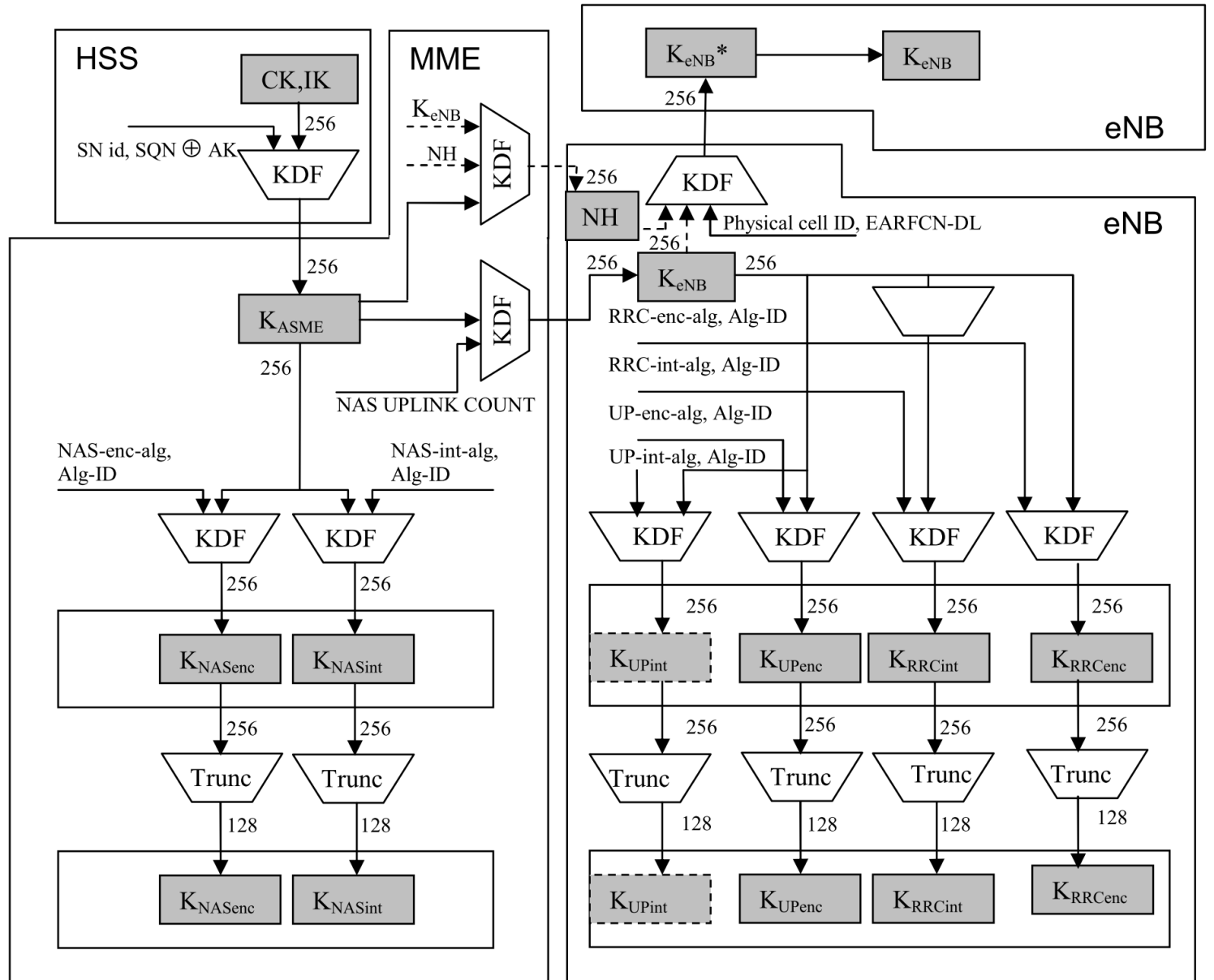
4. LTE安全机制

LTE中的切换安全

- $\{NH, NCC\}$ $NCC=1$, 不能用来派生密钥, 原因是初始化时的NH没有下发给eNB, 此外, 在X2切换中NH不能由源eNB传给目的eNB。
- eNB内切换
 - 如果有 $\{NH, NCC\}$ 可用, 则用 $\{NH, NCC\}$ 导出密钥, 否则用当前的 K_{eNB} 导出密钥;
- X2切换
 - 源eNB如果存在未使用的 $\{NH, NCC\}$ 对, 则通过纵向方式, 导出 $\{K_{eNB}^*, NCC\}$, 并发给目标eNB, 否则通过横向衍生产生密钥;
 - 目标eNB在设置 K_{eNB}^* 为 K_{eNB} 后, 发送消息给MME, MME发送新的 $\{NH, NCC\}$ 给目标eNB, 并立即启动eNB内切换流程;
- S1切换
 - 源MME计算新的 $\{NH, NCC\}$, 连同 K_{ASME} 一起发给目标MME, 目标MME存储并转发收到的 $\{NH, NCC\}$ 给目标eNB, 目标eNB计算 K_{eNB}

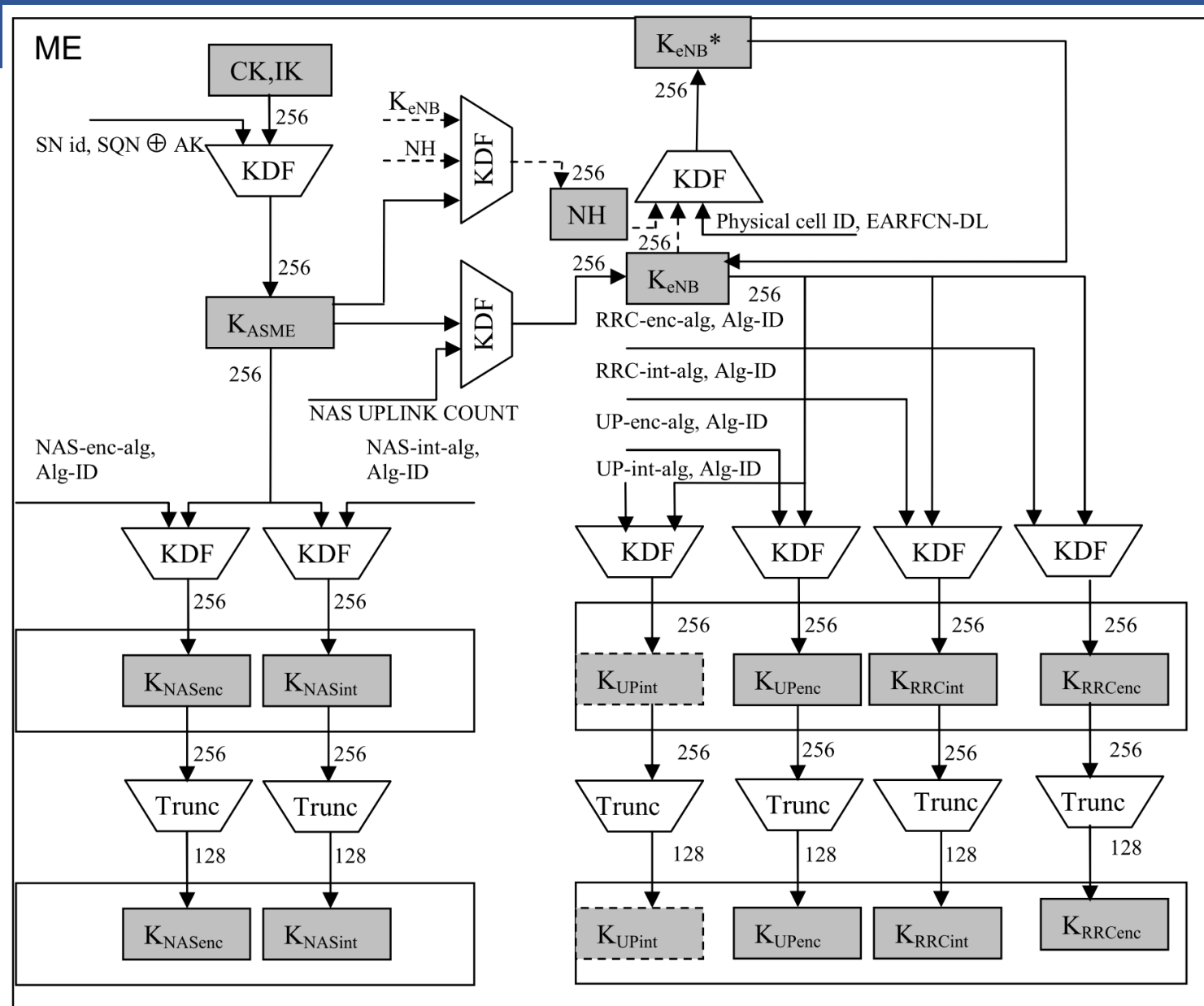
4. LTE安全机制

LTE系统中网络节点的 密钥分发和推衍方案



4. LTE安全机制

LTE系统中ME的 密钥分发和推导方案



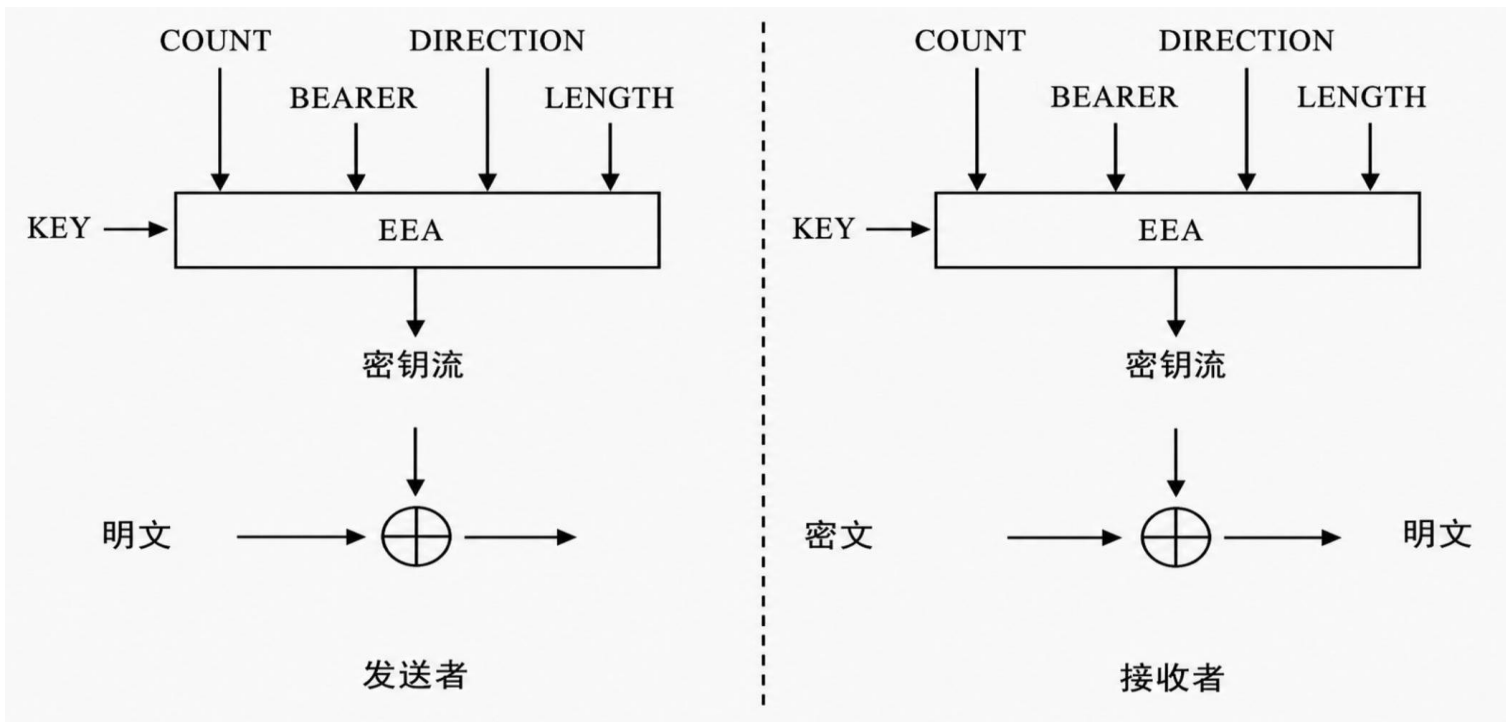
4. LTE安全机制

算法标识符

- 算法标识符 加密算法 算法描述
 - (0000)₂ EEA0 不加密
 - (0001)₂ 128-EEA1 基于SNOW 3G的加密算法
 - (0010)₂ 128-EEA2 基于AES的加密算法剩下的标识符为保留值，供将来使用。
- 完整性保护算法标识符应包括：
- 算法标识符 完整性算法 算法描述
 - (0000)₂ EIA0 无完整性保护(仅用于紧急呼叫)
 - (0001)₂ 128-EIA1 基于SNOW 3G的完整性算法
 - (0010)₂ 128-EIA2 基于AES的完整性算法剩下的标识符为保留值，供将来使用。
- 注： (XXXX)₂代表二进制

4. LTE安全机制

加密算法



参数:

- **Key:** 128位的加密密钥; **COUNT:** 32位计数器值;
- **BEARER:** 5位承载标识符;
- **DIRECTION:** 1位方向标识, 0表示上行/1表示下行链路;
- **LENGTH:** 密钥流长度。影响密钥流的长度, 不影响实际比特位。

4. LTE安全机制

加密算法

- 由于专利收费原因，Kasumi 不再成为 EPS 中安全算法。
- EEA1和EIA1：SNOW 3G的核心算法是一种流密码算法，由snow 2.0演变而来，虽然snow 2.0已有已知漏洞，但是SNOW 3G与其主要不同在于第二个S盒抗未来可能的代数攻击能带来附加安全强度。
- EEA1和EIA1：AES算法。
- EEA3和EIA3：我国自主研发的 ZUC 算法在 3GPP SA3#55 次会议上首次提出并通过，**2011年9月**成为 3GPP 标准的加密/完整性算法。

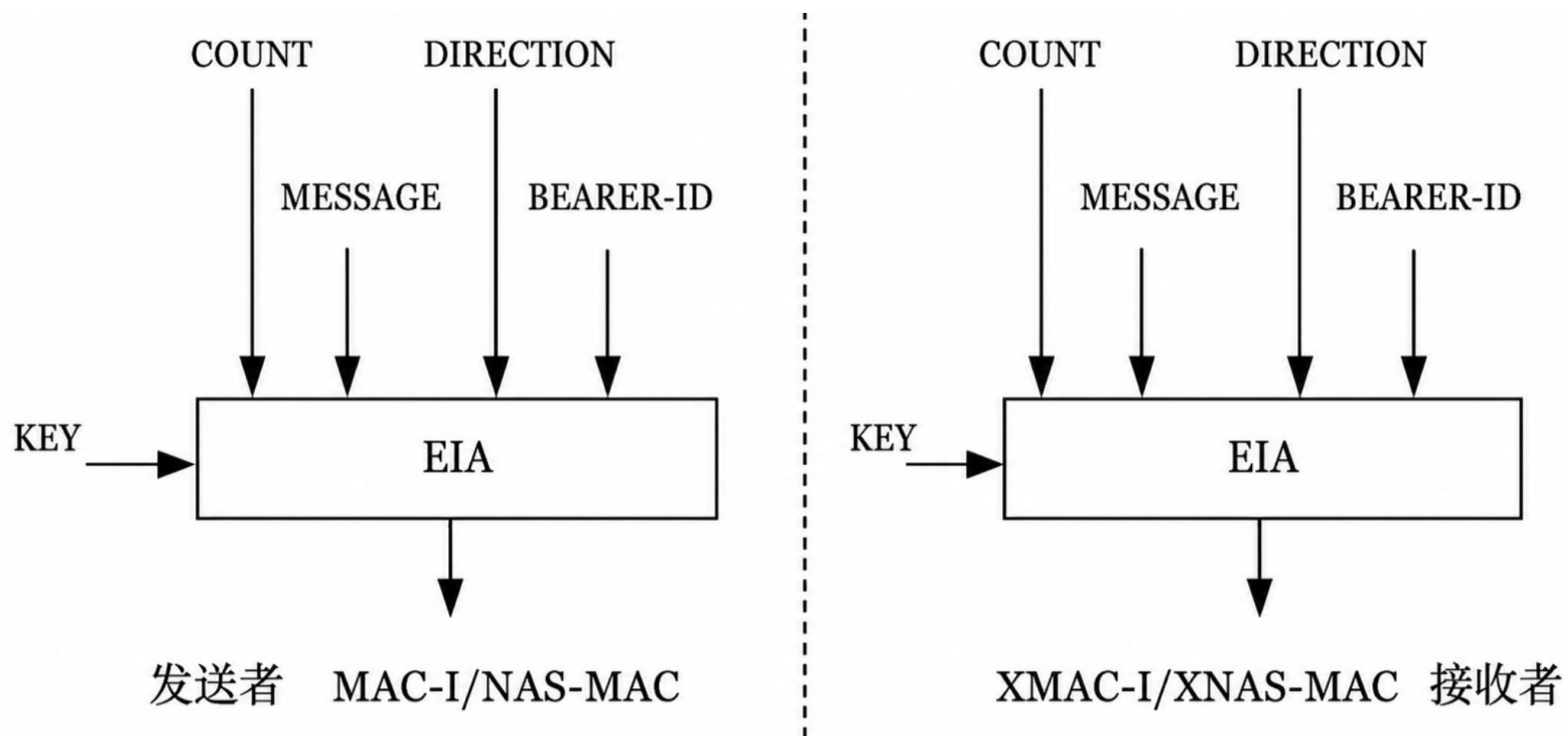
4. LTE安全机制

128-EEA2

- 128-EEA2基于128位的AES CTR模式的算法。
- CTR所需的128位计数器的序列号T1, T2, ..., Ti, ...将按如下规则构造：
 - T1的最高64位：
$$\text{COUNT}[0] \dots \text{COUNT}[31] \mid \text{BEARER}[0] \dots \text{BEARER}[4] \mid \text{DIRECTION} \mid 0_{26}$$
 - 从左至右为最高有效位至最低有效位排列，如COUNT[0]是T1的最高有效位。
 - T1的最低64位全为0。
 - 后续计数器块通过标准整数增加功能对先前的计数值的低64位模 2^{64} 运算来获得。

4. LTE安全机制

128位完整性算法



参数:

- **KEY**: 128位的完整性密钥, **COUNT**: 32位的计数值
- **BEARER**: 5位的承载标识, **DIRECTION**: 1位方向标识
- **MESSAGE**: 消息。

4. LTE安全机制

128-EIA2

- 128-EIA2基于128位AES CMAC模式。
- CMAC模式的输入为Mlen长度的位串M，M包含以下内容：
 - $M0 \dots M31 = \text{COUNT}[0] \dots \text{COUNT}[31]$
 - $M32 \dots M36 = \text{BEARER}[0] \dots \text{BEARER}[4]$
 - $M37 = \text{DIRECTION}$
 - $M38 \dots M63 = 0 \quad 26$ (i.e. 26 zero bits)
 - $M64 \dots \text{MBLENGTH}+63 = \text{MESSAGE}[0] \dots \text{MESSAGE}[\text{BLENGTH}-1]$
- $\text{Mlen} = \text{BLENGTH} + 64$.
- AES CMAC模式使用这些输入参数产生一个长度Tlen=32的消息认证码T。T直接用于128-EIA2的输出MACT[0] .. MACT[31]，其中MACT[0]为T的最高有效位。

4. LTE安全机制

NAS加密建立过程

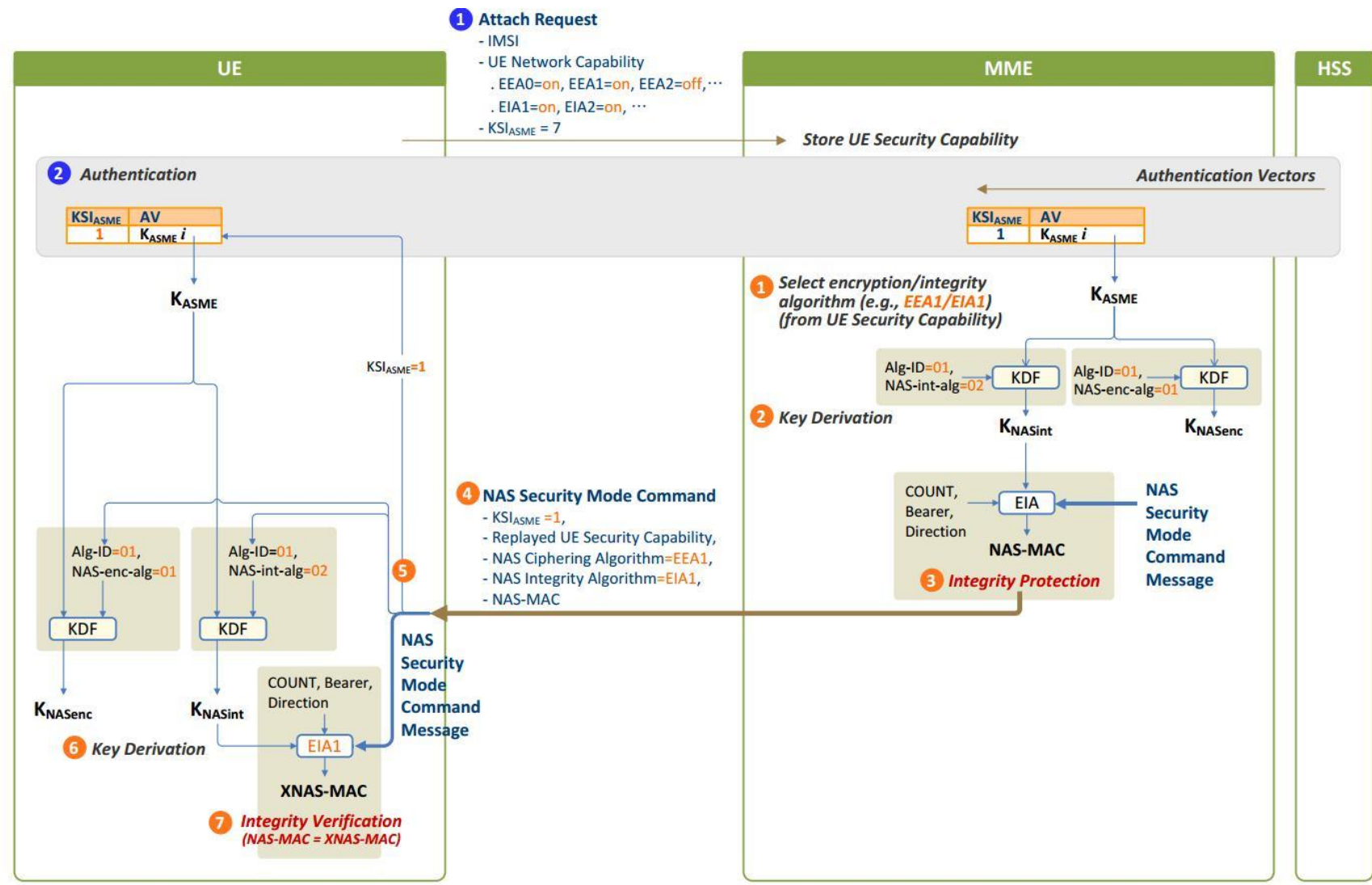


Figure 2. NAS security setup: Delivery of a Security Mode Command message

4. LTE安全机制

NAS加密 建立过程

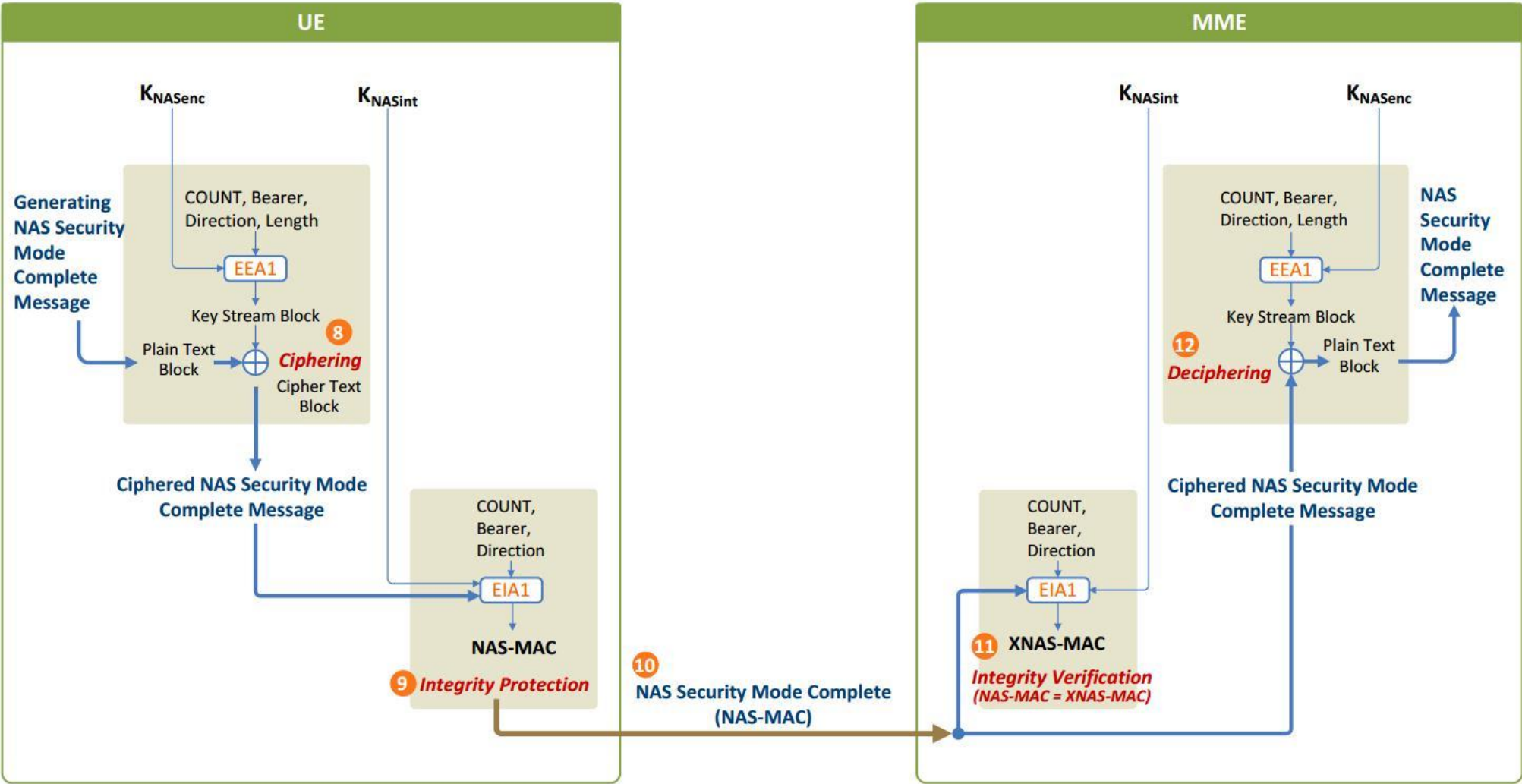


Figure 5. NAS security setup: Delivery of a Security Mode Complete message

4. LTE安全机制

NAS机密性和完整性保护

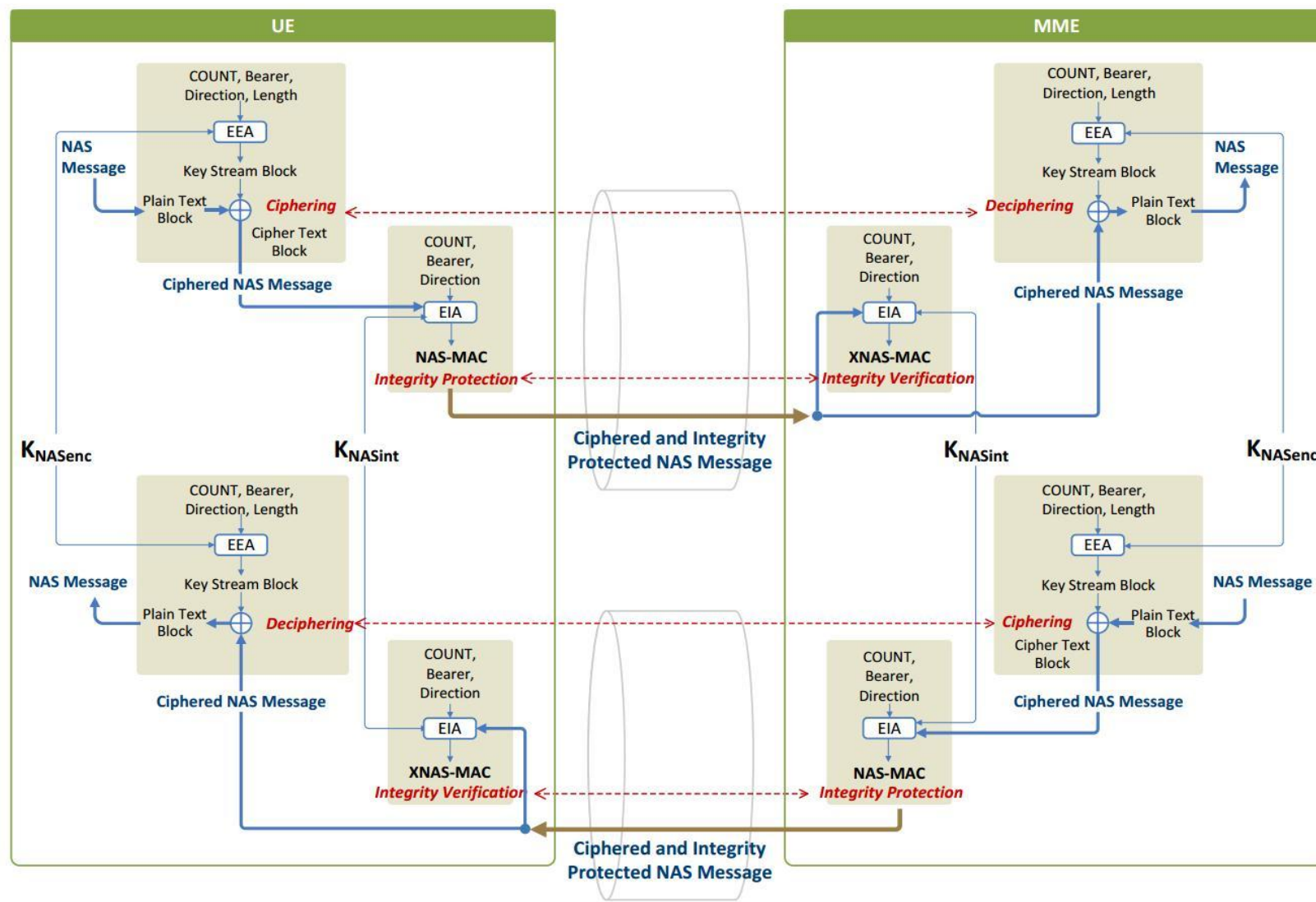


Figure 8. Ciphering and integrity protection of the NAS Messages after the NAS security setup

4. LTE安全机制

AS安全建立过程

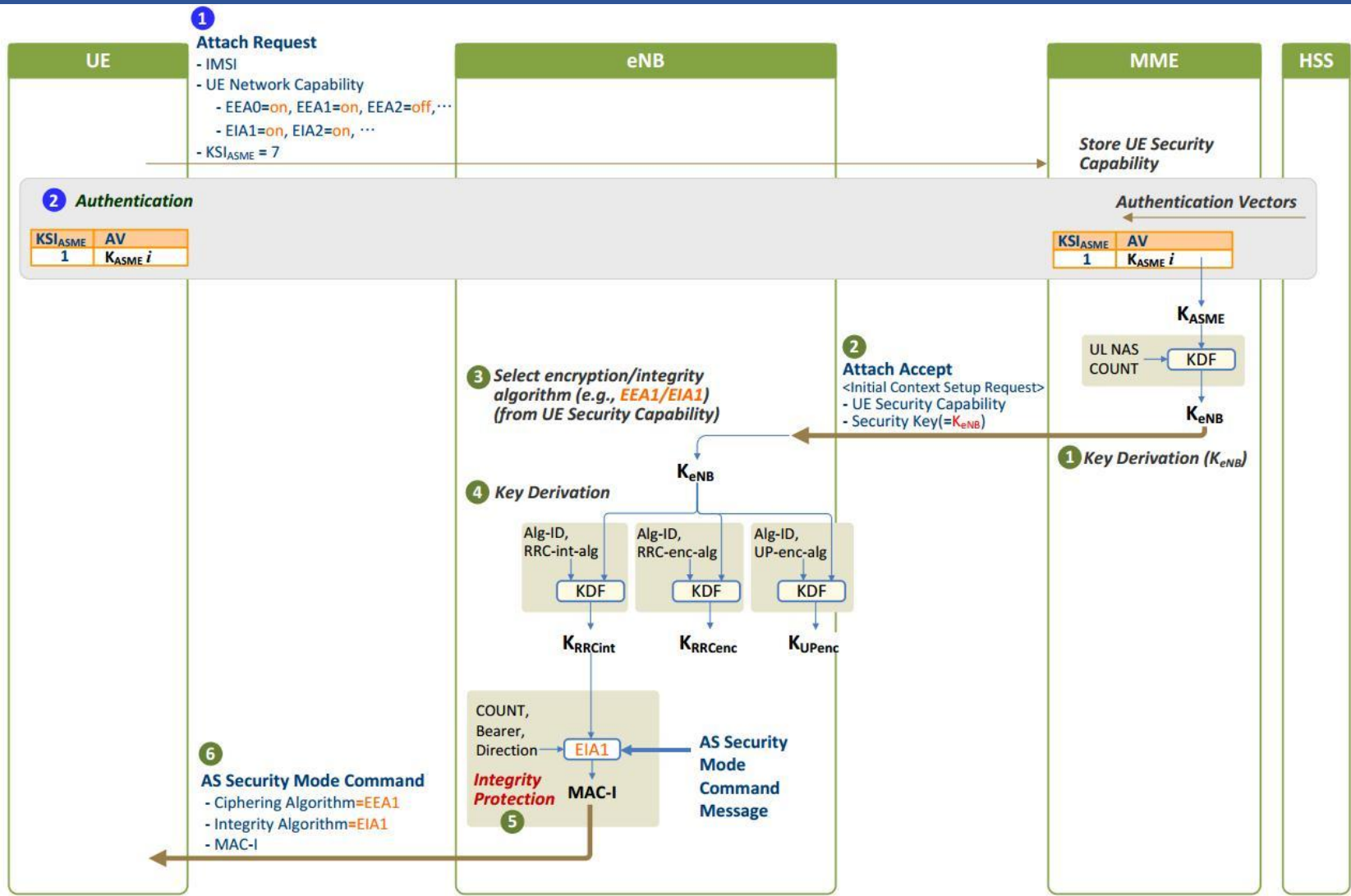


Figure 9. AS security setup: Generating and sending a Security Mode Command message

4. LTE安全机制

AS安全建立过程

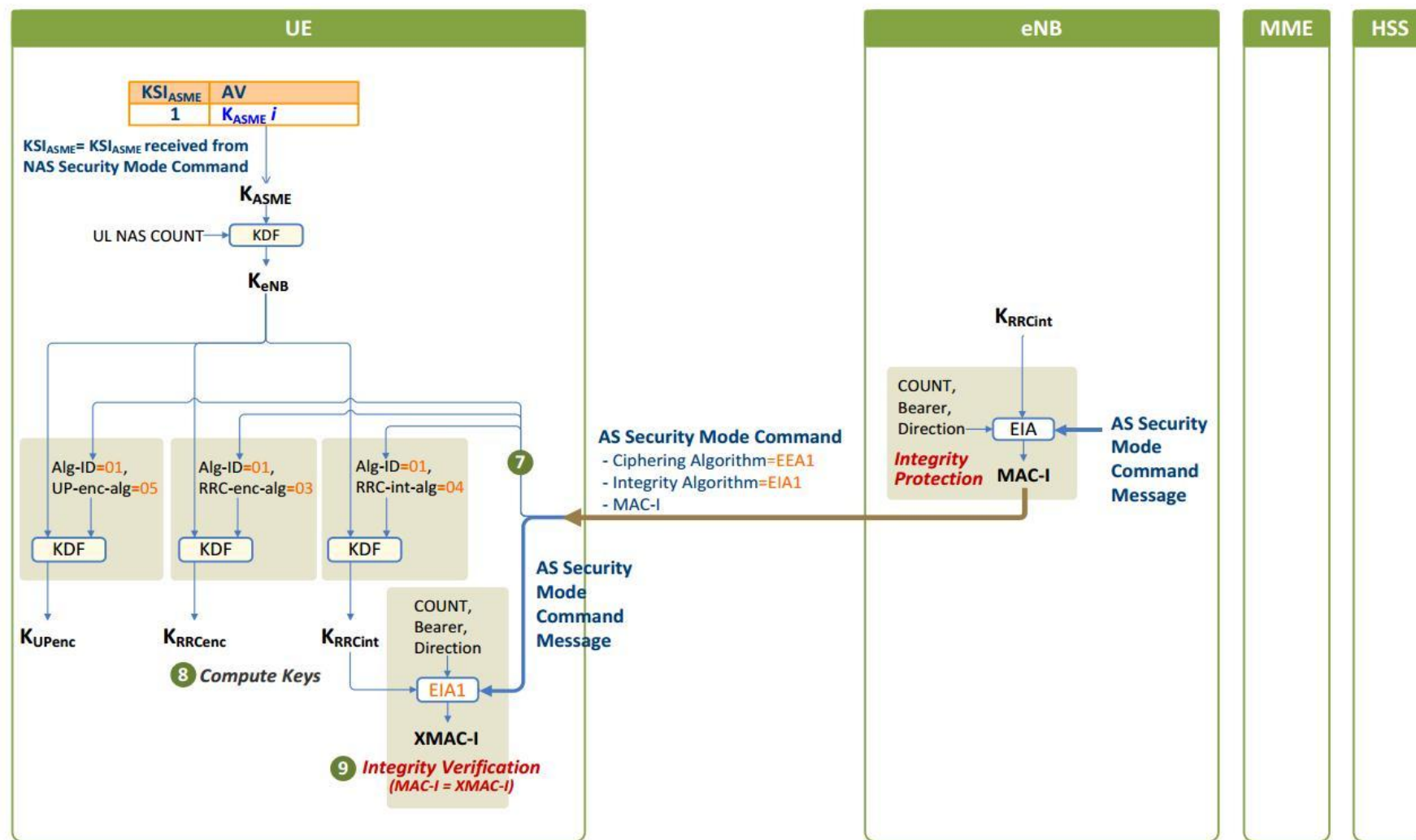


Figure 10. AS security setup: Receiving a Security Mode Command message

4. LTE安全机制

AS安全建立过程（续2）

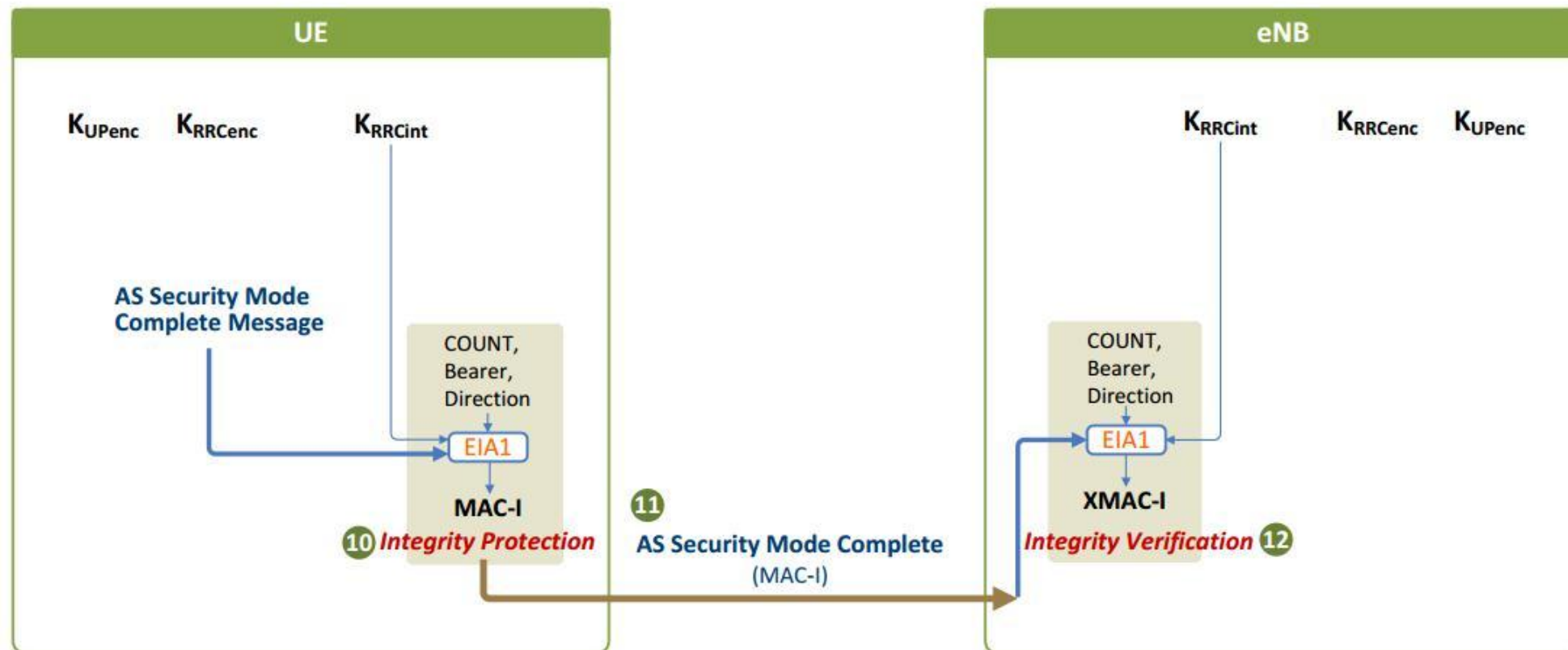


Figure 11. AS security setup: Delivery of a Security Mode Complete message

4. LTE安全机制

AS安全： RRC消息安全和 用户数据加密

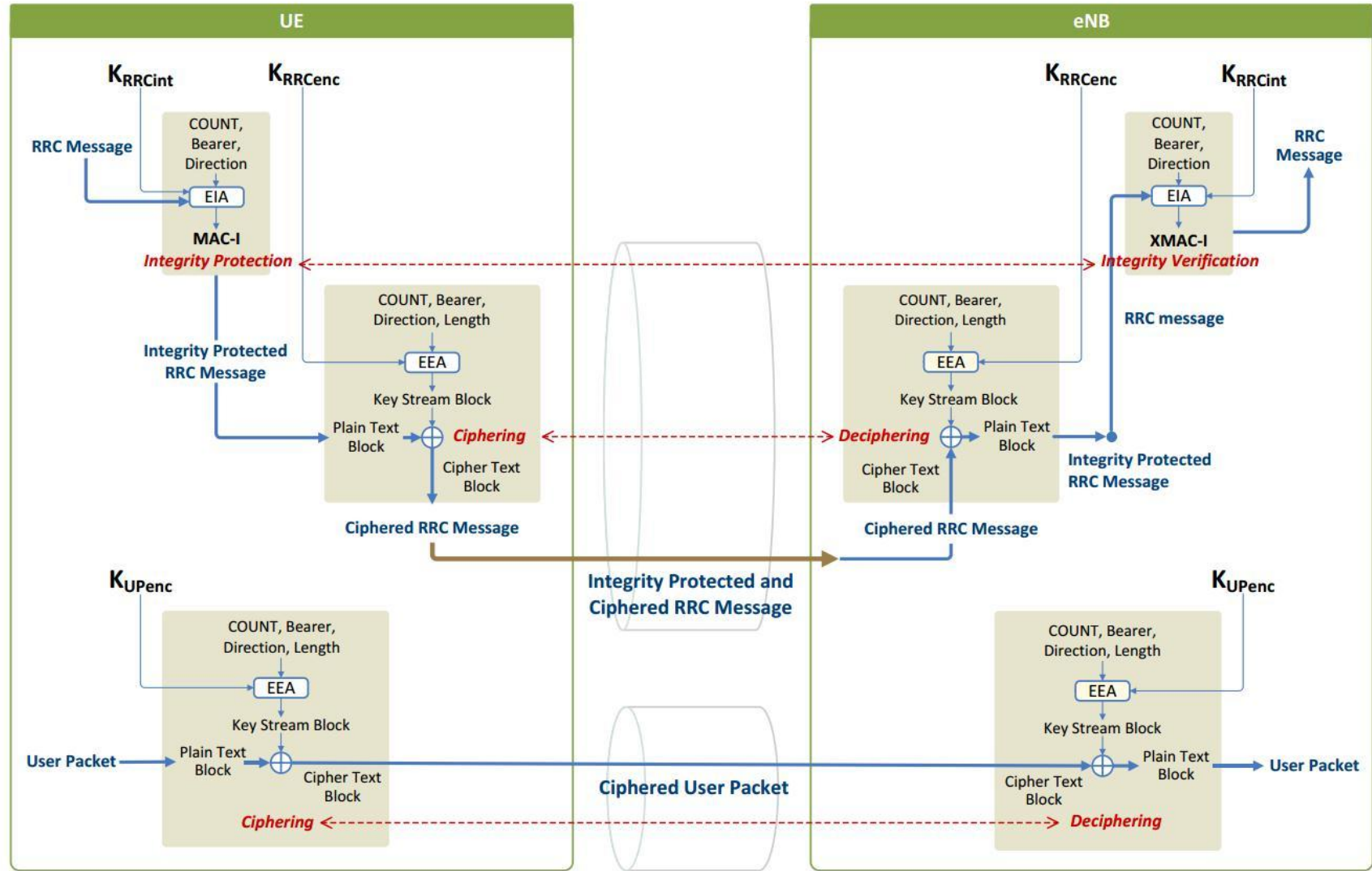


Figure 12. Integrity protection and ciphering of RRC messages and ciphering of user packets after the AS security setup

- 与**WCDMA**相比，增强了：
 - 安全传输的粒度更细：区分**NAS**层和**AS**层
 - 快速切换的密钥管理
- **LTE**安全缺陷
 - **IMSI**泄露
 - **SQN**重同步导致攻击
 - 用户面数据完整性保护可选将导致攻击
 - 降级攻击

1. 请画图给出基于X2接口进行基站切换的密钥更新过程，并分析该过程是否能够满足前向安全和后向安全目标。

1. **3GPP TS 33.401 V8.6.0 (2009-12)Security architecture**
2. **2018-NDSS-LTEInspector: A systematic Approach for Adversarial Testing of 4G LTE**
3. **2019-S&P(Oakland)-Breaking LTE on Layer Two**
4. **2020-NDSS-IMP4GT: IMPersonation Attacks in 4G NeTworks**
5. **NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".**

谢谢！

