

课程编号：3182121321

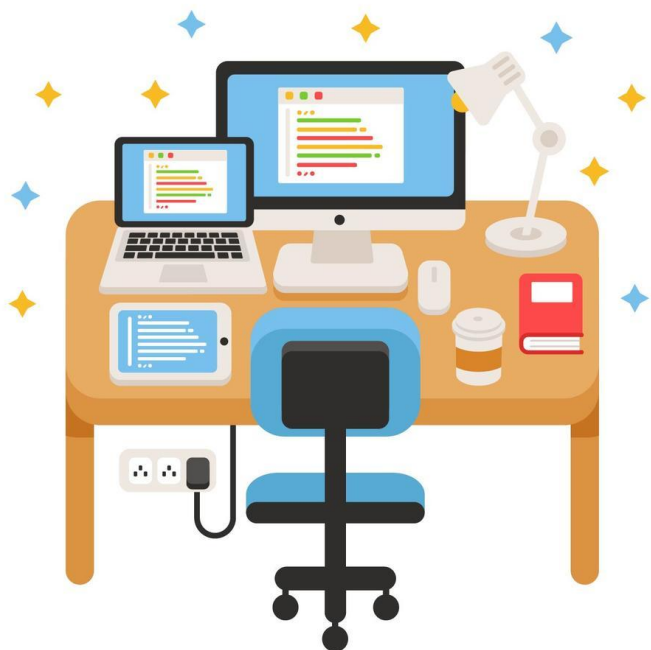
# 无线通信安全



课程总结、未来无线安全技术展望

李晖

lihuill@bupt.edu.cn



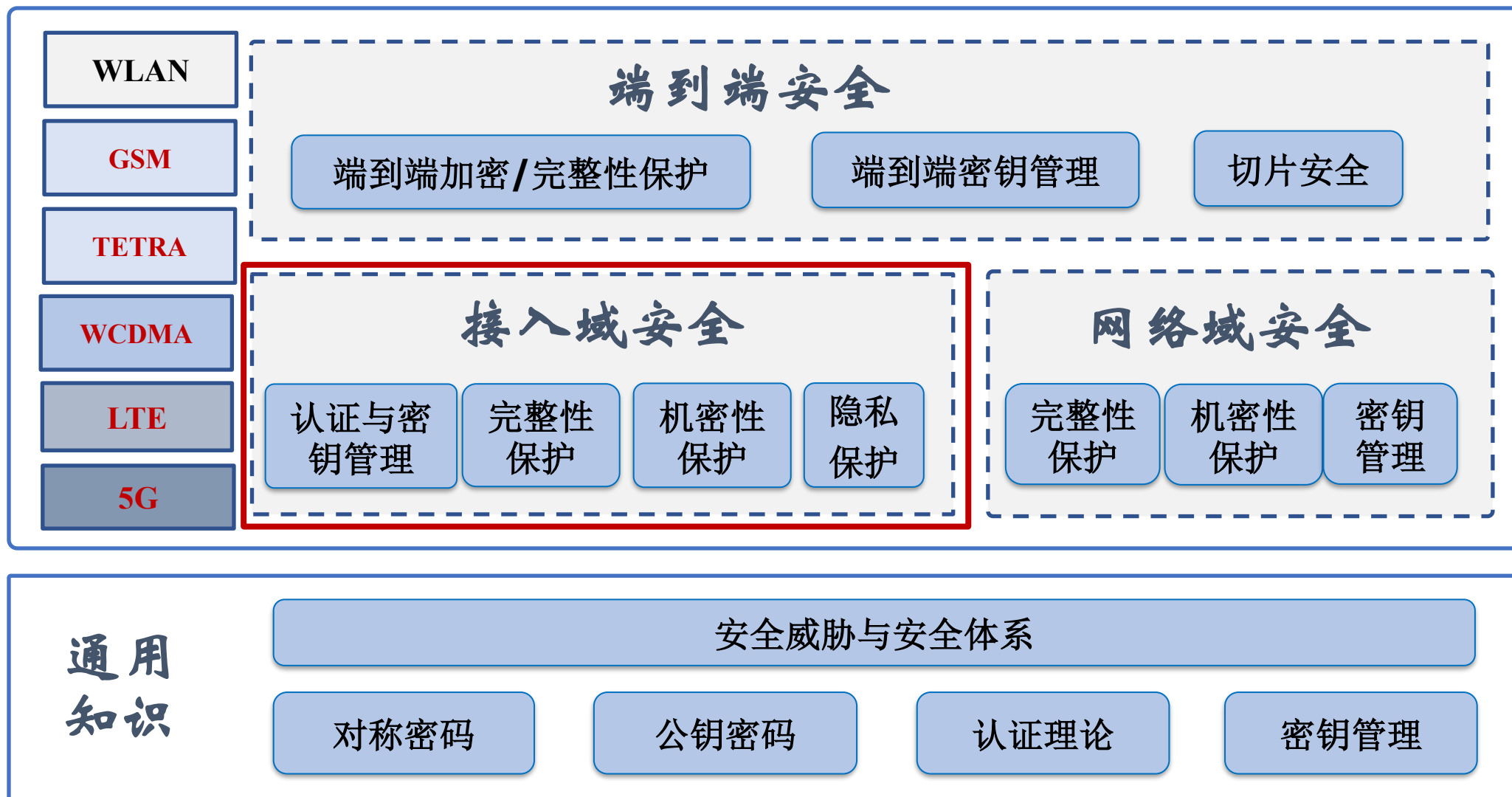
## 1. 课程总结

- ✓ 课程内容架构
- ✓ 核心课程内容

## 2. 未来无线安全技术展望

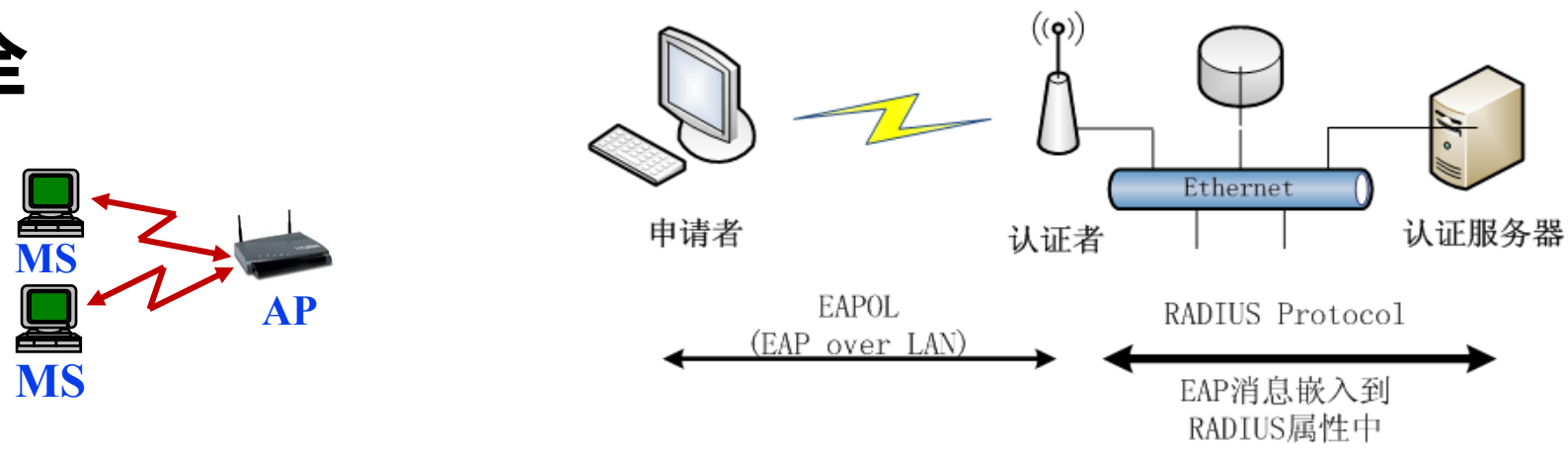
- ✓ 未来移动网络
- ✓ 未来移动网络安全

## 2. 课程总结—课程内容架构



## 2. 课程总结—核心课程内容

### WLAN安全



#### 802.11

#### 802.1x

#### WPA

#### 802.11i/WPA2

#### WPA3

- WEP协议
- 基于共享密钥认证
- 基于RC4算法的机密性保护
- 基于CRC校验码的完整性保护

- EAP协议
- 动态密钥管理（四步握手协商）

- 预共享密钥认证(WPA 个人)
- 802.1X 服务器认证(WPA 企业)
- 基于128比特RC4流密码
- TKIP（临时密钥完整性协议）

- 使用802.1x中的认证
- TKIP
- CCMP(AES的CCM)
- WRAP(AES的OCB)

- 192位的CNSA算法
- 对等实体同时认证(SAE)

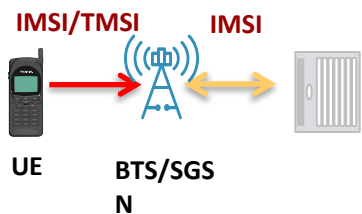
#### WAPI

- 基于公钥证书的认证与密钥协商协议（身份认证、单播密钥更新、组播密钥更新）
- 密钥管理、完整性保护、机密性保护

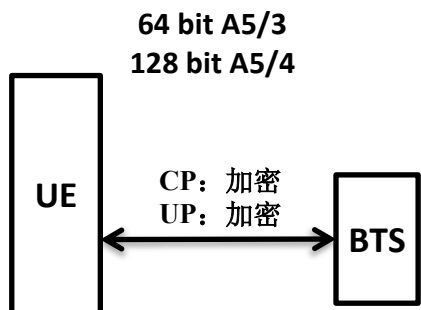
# 1. 课程总结—核心课程内容

## 2/3/4/5G标准的接入域安全演进

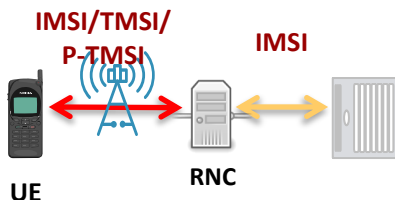
2G/2.5G



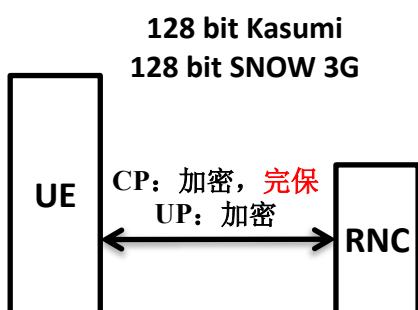
- 2G AKA: 仅有网络对UE的单向鉴权
- 数据和信令机密性保护
- 数据加密终结点: BTS或SGSN



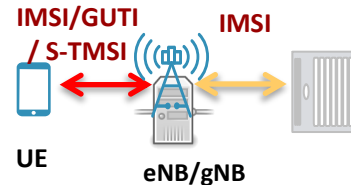
3G



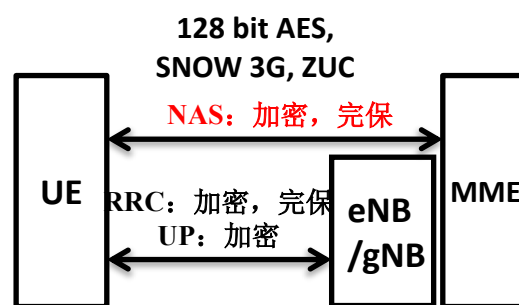
- 3G AKA: **双向鉴权**
- 数据&信令的机密性保护
- **信令完整性保护**
- 数据加密终结点: RNC



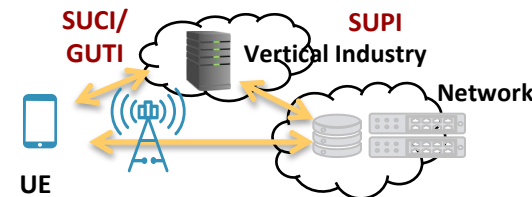
4G/5G(NSA)



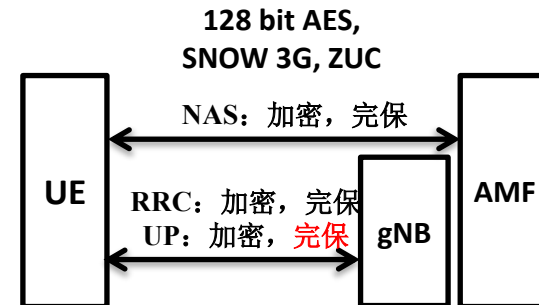
- 4G AKA: 双向鉴权
- 数据&信令的机密/完整性保护
- **NAS信令机密性和完整性保护**
- **快速切换的密钥管理**
- 数据加密终结点: eNB/gNB
- RRC加密与完保终结点: eNB/gNB
- NAS加密与完保终结点: MME



5G Standalone



- 保持4G安全特性
- 针对垂直行业的增强
- 统一认证框架
- 5G AKA: **增强的双向鉴权**
- **UP面完整性保护**



# 1. 课程总结—核心课程内容

## 2/3/4/5G对基站切换的支持

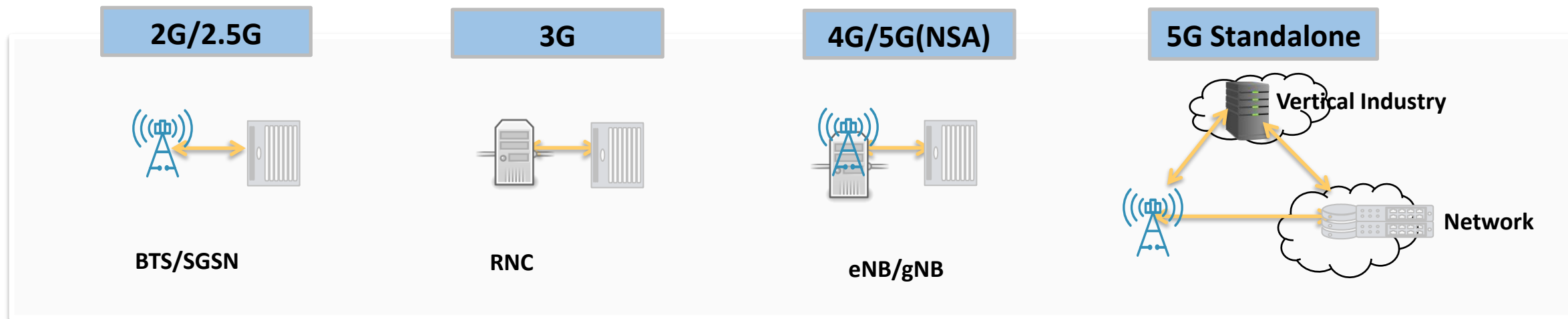
- **重新认证**：为了继续保障通信机密性和完整性，防止继续使用失效或被泄露的密钥
  - **2G**：一般需要重新认证
  - **3G**：根据情况来选择是否重新认证

| 场景                                                 | 是否重认证 | 说明                                   |
|----------------------------------------------------|-------|--------------------------------------|
| 同域内普通切换                                            | 否     | 可上下文转移（通过 <b>Iur</b> 接口），保留密钥        |
| <b>PS ⇌ CS</b> 域切换                                 | 是     | 不同域使用独立安全上下文                         |
| 区域变更(从一个 <b>VLR/SGSN</b> 切换到另外一个 <b>VLR/SGSN</b> ) | 是     | 核心网可能无法识别 <b>UE</b>                  |
| 上下文失效                                              | 是     | 终端能力限制或核心网上下文丢失，导致密钥失效，需重建           |
| 安全策略或网络策略要求重新认证                                    | 是     | 设定了“切换次数达到上限后必须重新认证”或“跨特定区域时刷新密钥”的策略 |

- **4G/5G**：定义了完整的密钥派生策略（课程难点）

# 1. 课程总结—核心课程内容

## 2/3/4/5G标准的网络域安全演进



- 无安全机制

- 针对IP: IPsec
- 针对MAP: MAPsec

- IMS安全
- TLS安全

- TLS安全
- Oauth认证

# 1. 课程总结— 核心课程内容

## 安全威胁与安全体系

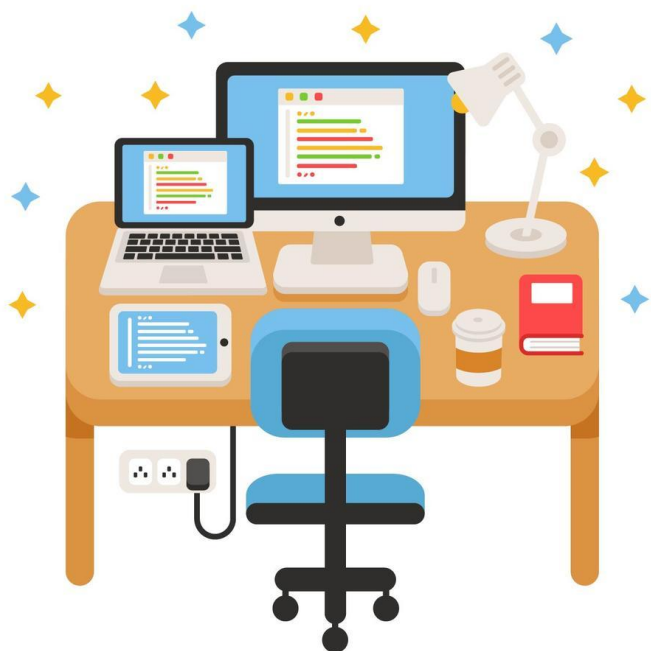
- 通信网面临的安全威胁有哪些？
- 哪些是无线通信网特有的安全威胁？
- 安全体系模型？

# 1. 课程总结— 核心课程内容

## 无线通信系统安全技术

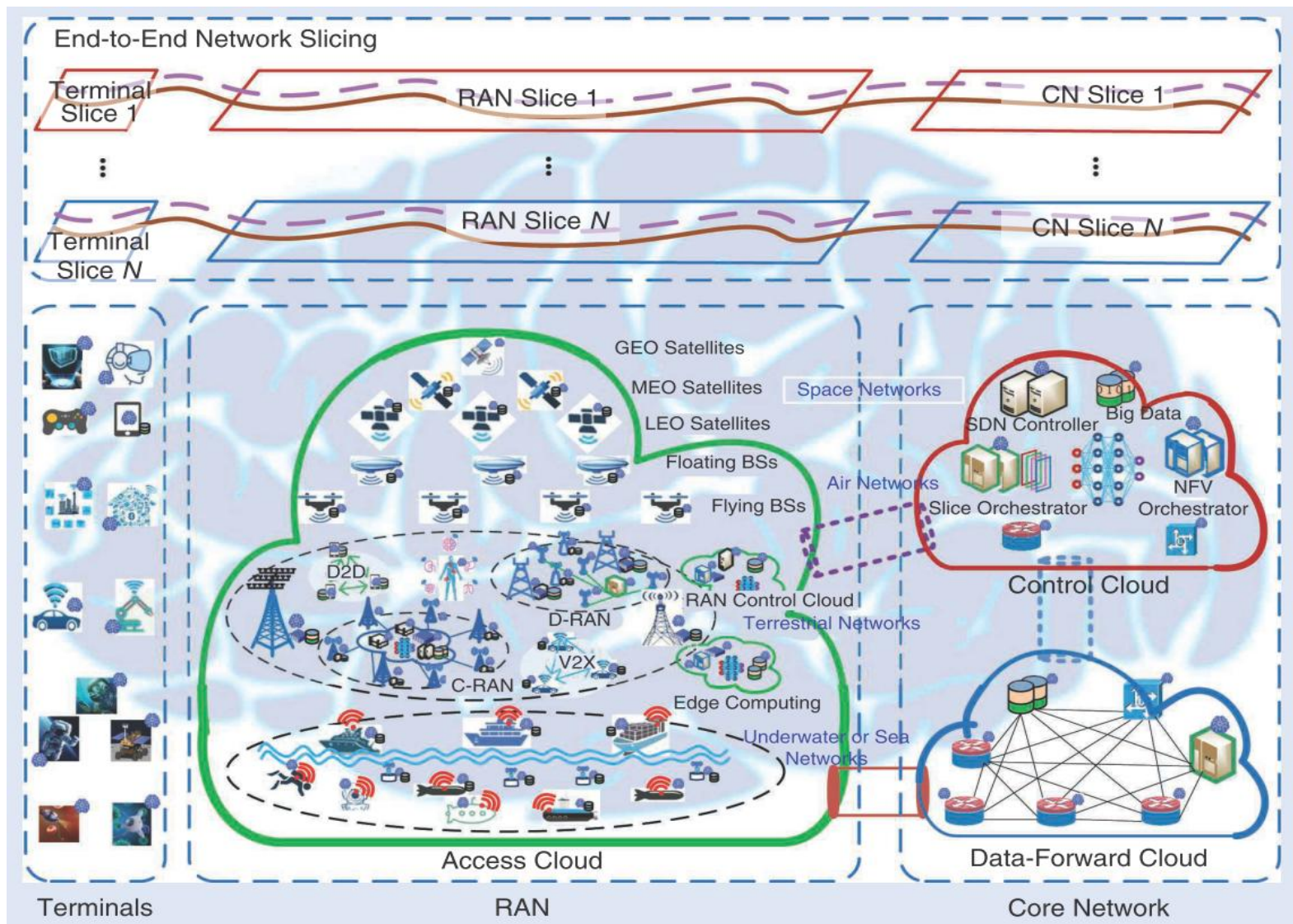
- 安全要求是什么？
- 如何对用户进行标识？
- 如何保护用户身份？
- 如何进行认证？
- 如何保证信息传输的机密性、完整性？
- 如何管理密钥？
- 有哪些特殊安全要求？ 如何实现的？

# 本讲目录



1. GPS安全
2. 课程总结
  - ✓ 课程内容架构
  - ✓ 核心课程内容
3. 未来无线安全技术展望
  - ✓ 未来移动网络
  - ✓ 未来移动网络安全

## 2. 展望 — 未来移动网络



### 未来通信网络:

#### 1. 终端形式多样:

传统终端、智能车、小型的飞行器等

#### 2. 异构接入网络:

- a. 涵盖了海陆空多种接入设备
- b. 卫星与地面系统有机融合
- c. 多种的无线通信模式

#### 3. 核心网虚拟化:

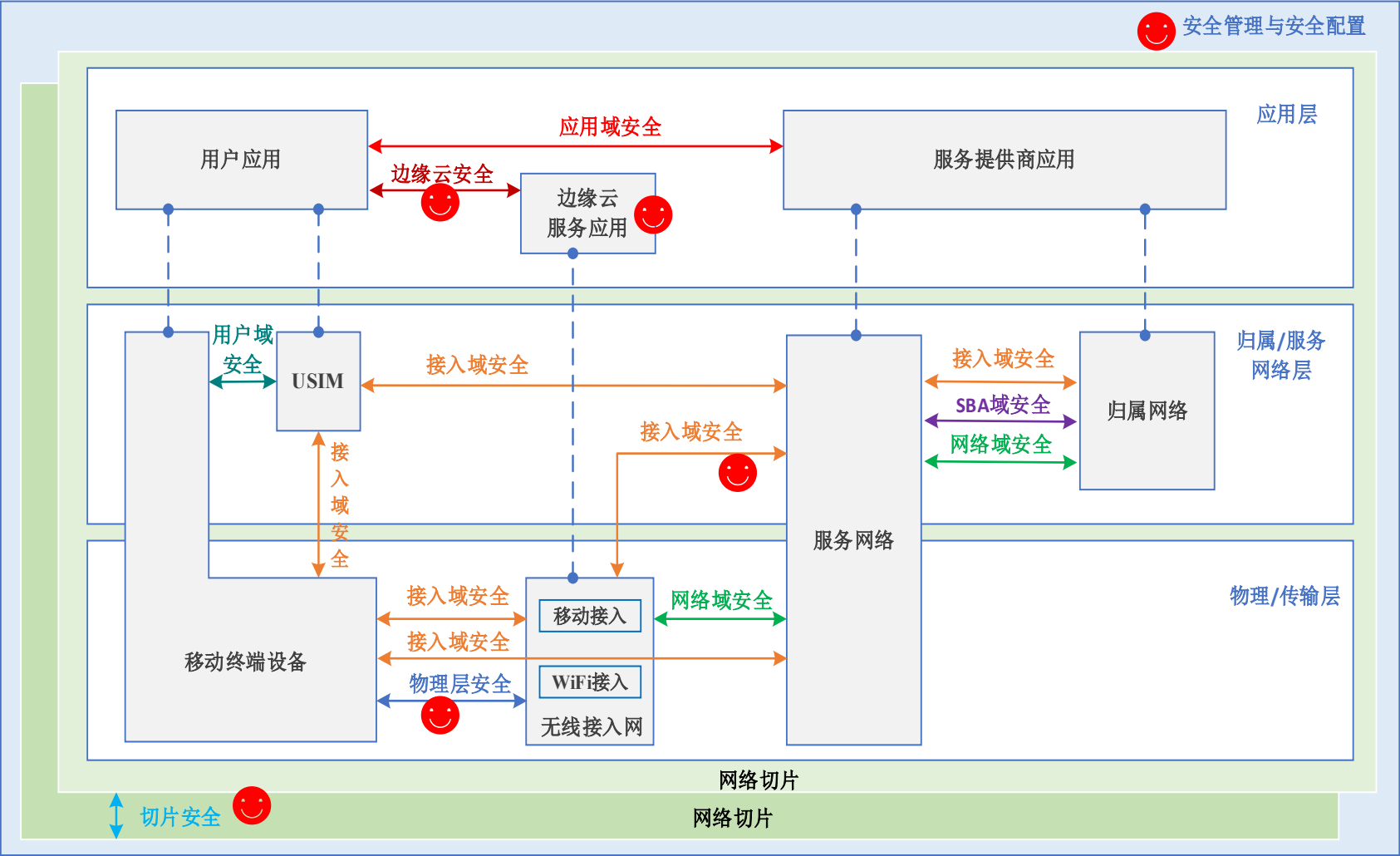
- a. 基于SBA架构
- b. 控制功能下放到网络边缘
- c. 支持虚拟化设备
- d. 支持多种交换方式
- e. 多种服务设备

#### 4. E2E网络切片:

- a. 网络切片服务

# 2. 展望 — 未来移动网络安全

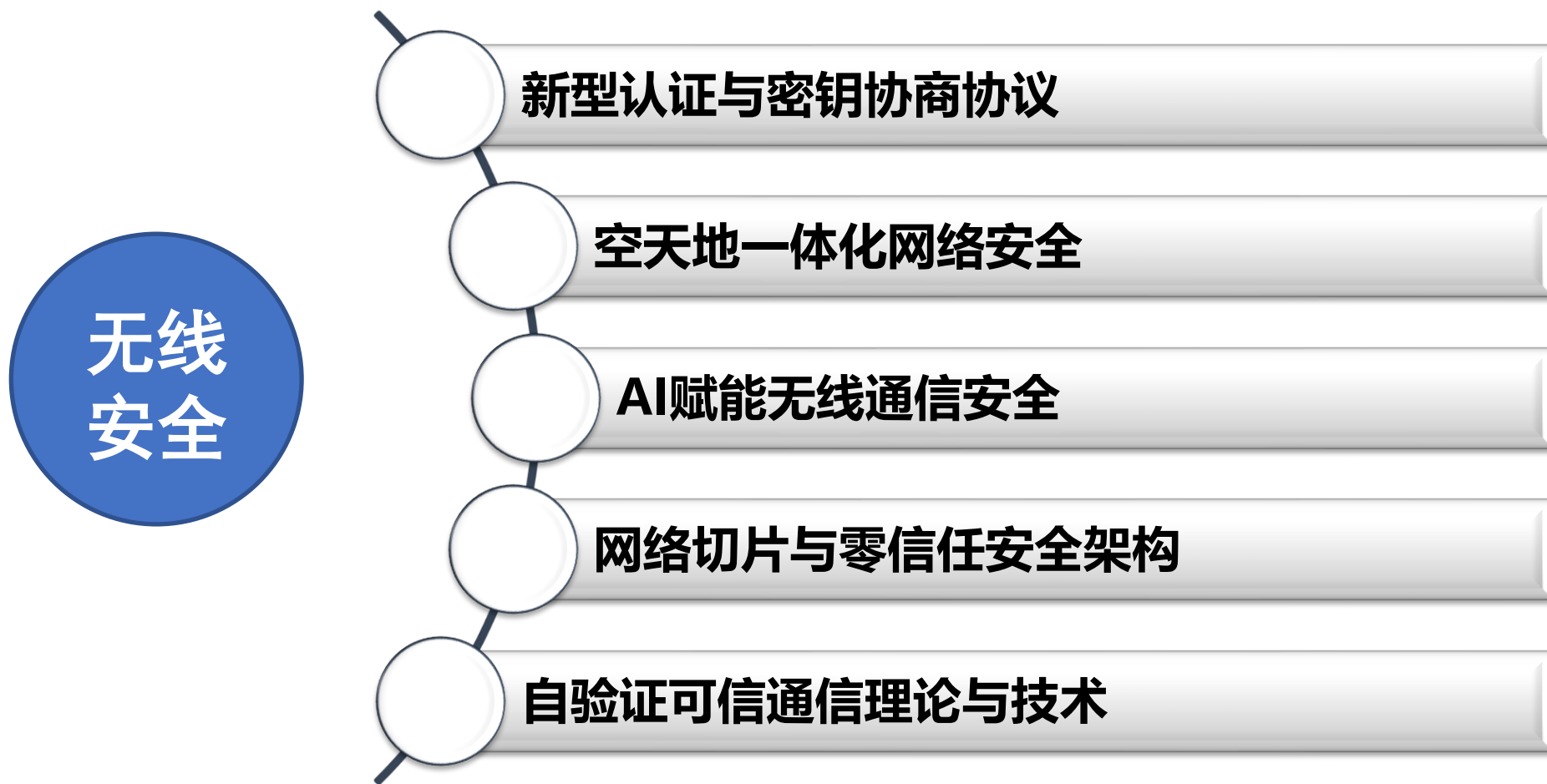
## 未来移动网络安全架构



- I. 接入域安全
- II. 网络域安全
- III. SBA域安全
- IV. 物理层安全
- V. 用户域安全
- VI. 应用域安全
- VII. 边缘云安全
- VIII. 切片安全
- IX. 安全管理与安全配置

## 2. 展望 — 未来移动网络安全

### 未来无线安全的研究热点

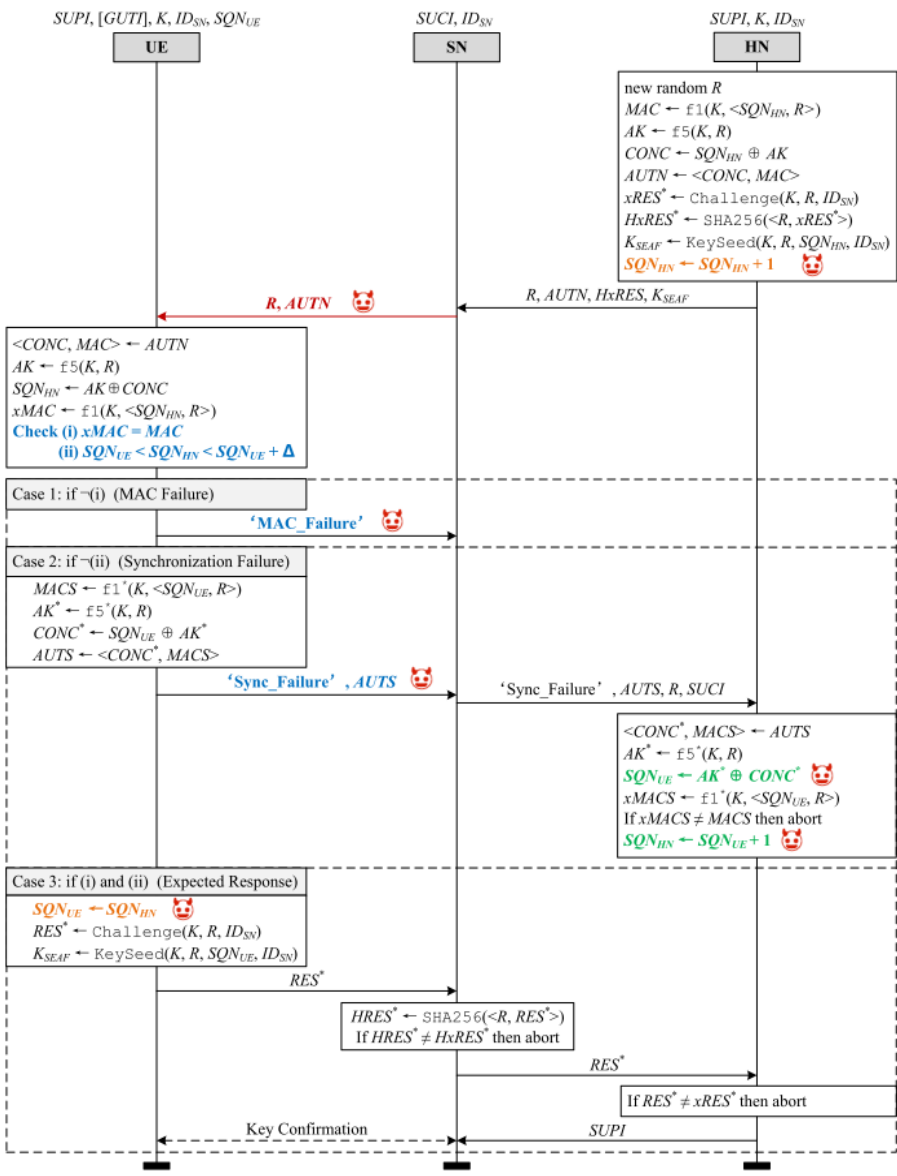
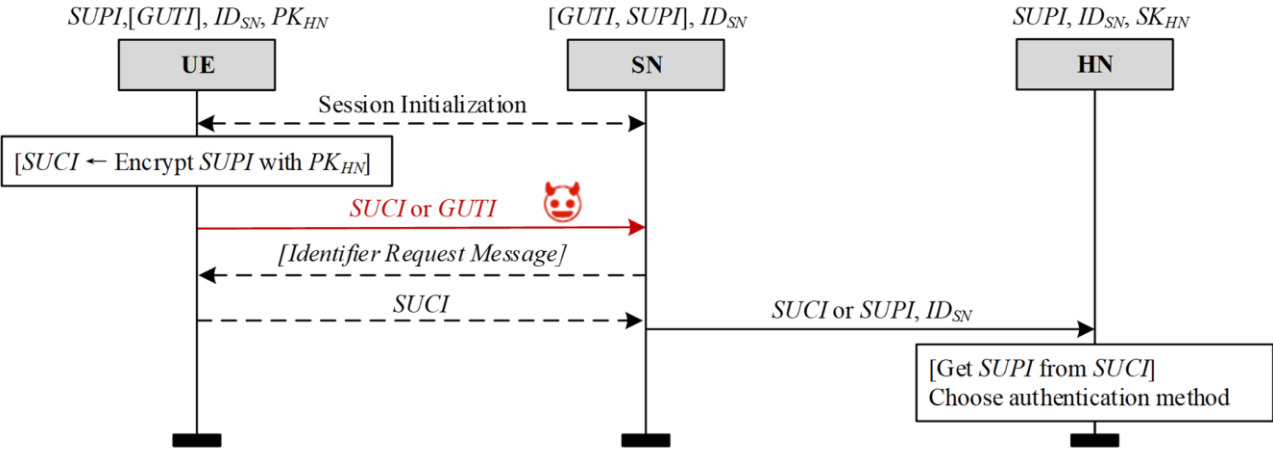


# 2. 展望 — 未来移动网络安全

## 新型认证与密钥协商协议

- 设计新的AKA协议
- 问题：如何抵御现有攻击？
- 问题：如何保持高效性？
- 问题：如何评估安全性？

## 5G-AKA协议流程



[1] H. Li, et al., "5G-RNAKA: A Random Number-based Authentication and Key Agreement Protocol for 5G Systems," *Proc. ACM CCS (CCF A)*, 2025.

## 2. 展望 — 未来移动网络安全

### 可链接攻击

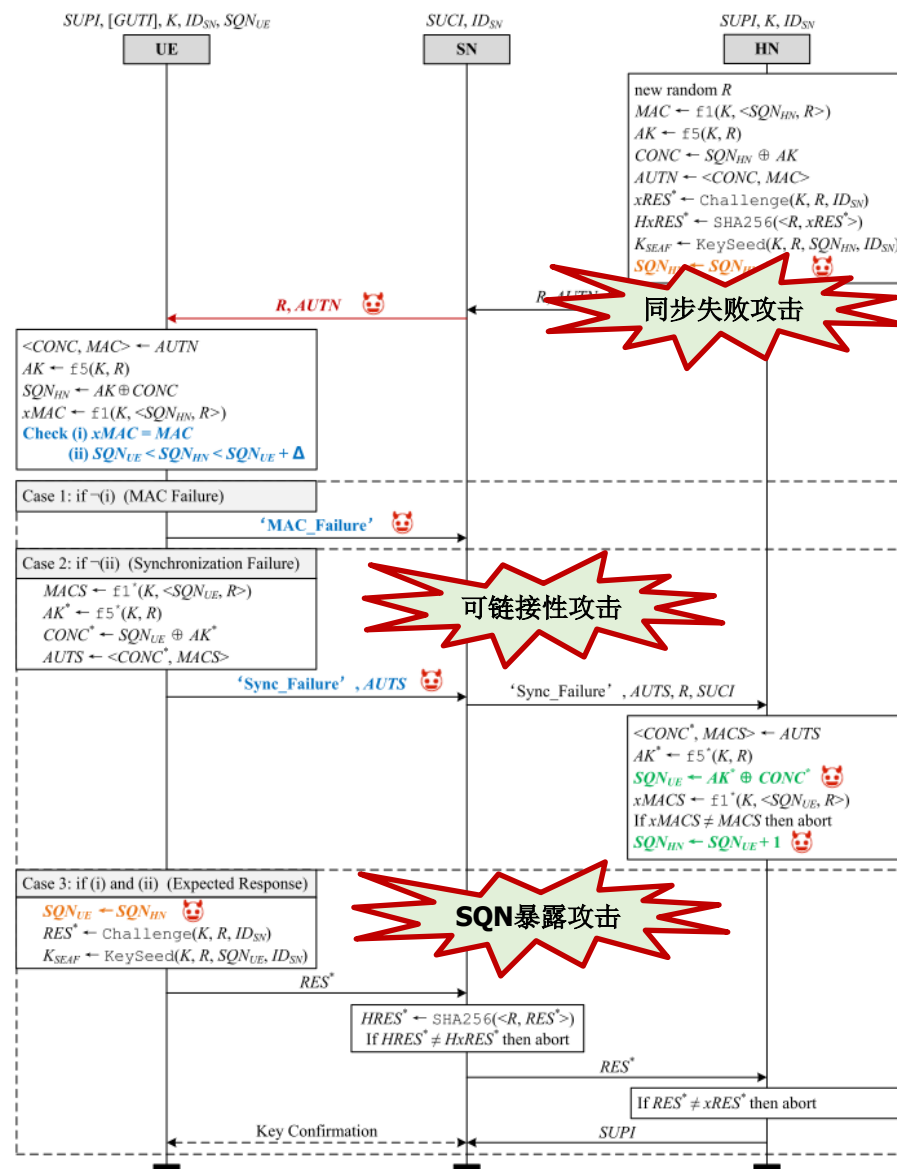
- 攻击者重放  $\langle SUCI \text{ or } GUTI \rangle$  或  $\langle R, AUTN \rangle$ 
  - 目标UE将回复Sync\_Failure
  - 非目标UE回复MAC\_Failure
- 导致攻击者能够区分和跟踪目标UE

### 同步失败攻击

- 攻击者多次重放 $\langle SUCI \text{ or } GUTI \rangle$ 
  - $SQN_{HN}$  不断增加（与 $SQN_{UE}$ 不一致）
  - UE验证 $SQN_{HN}$  失败
- 导致目标UE服务中断

### SQN泄露攻击

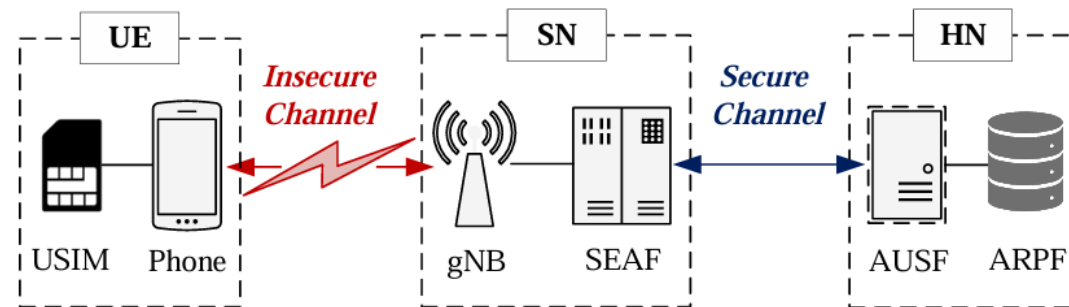
- 攻击者多次重放 $\langle R, AUTN \rangle$ 
  - 目标UE回复多个重同步向量  $AUTS1, AUTS2, \dots$
  - 攻击者监听后可以分析出 SQN的部分信息
- 进一步可以分析出用户使用的一些典型服务



## 2. 展望 — 未来移动网络安全

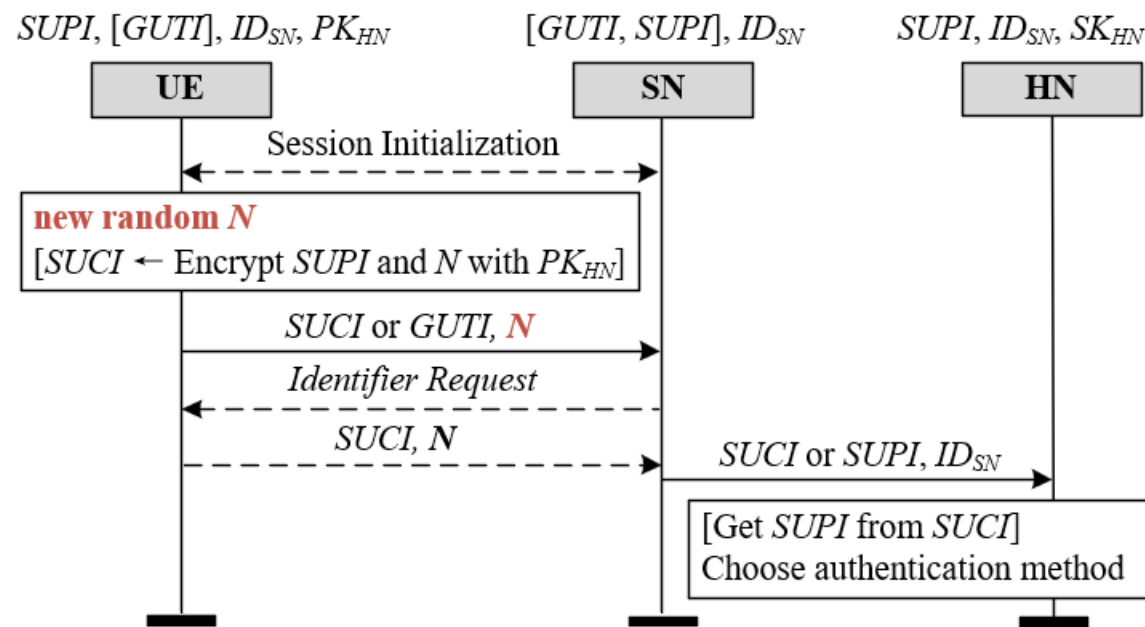
## 协议架构

- 与5G-AKA架构相同，未引入新的实体
- USIM具有产生随机数的能力
- USIM支持非对称随机加密
  - 确保SUCI的随机性和新鲜性



## 初始阶段

- 引入随机数  $N$  (由USIM产生)
  - $N$  被发送至SN
- SN保存 $N$ , 并用于计算  $SNMAC$



## 挑战应答阶段

## 2. 展望 — 未来移动网络安全

### 5G-RNAKA协议

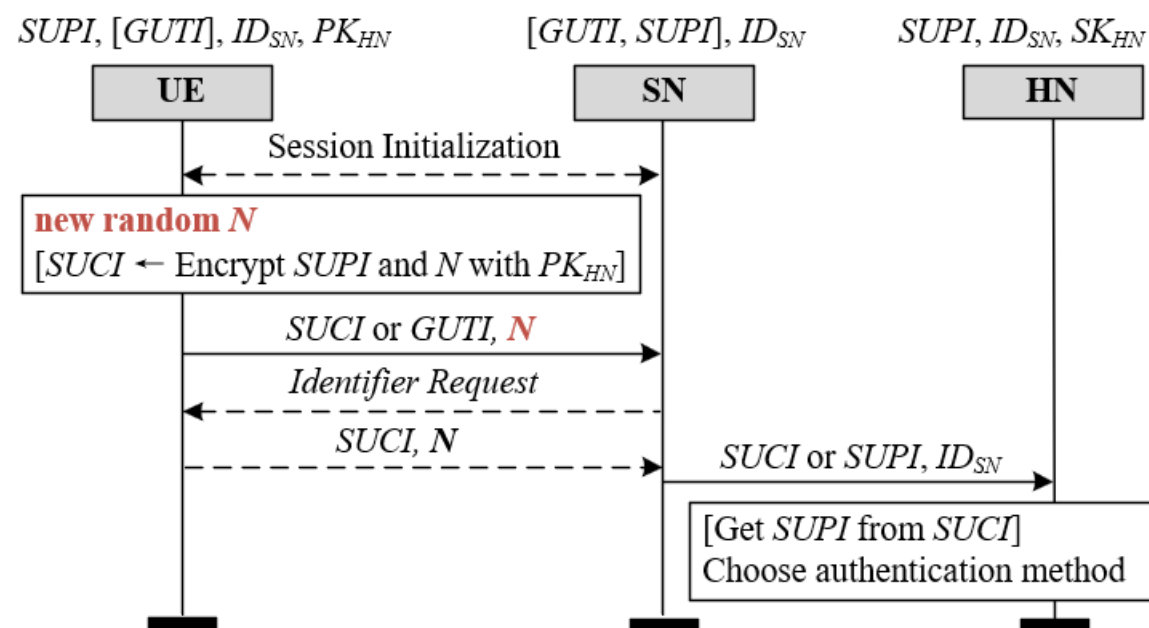
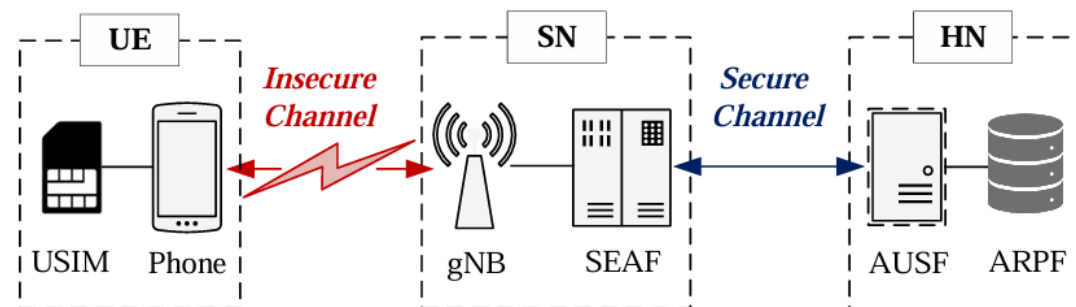
#### 协议架构

- 与5G-AKA架构相同，未引入新的实体
- USIM具有产生随机数的能力
- USIM支持非对称随机加密
  - 确保SUCI的随机性和新鲜性

#### 初始阶段

- 引入随机数  $N$  (由USIM产生)
  - $N$  被发送至SN
- SN保存 $N$ , 并用于计算  $SNMAC$

#### 挑战应答阶段



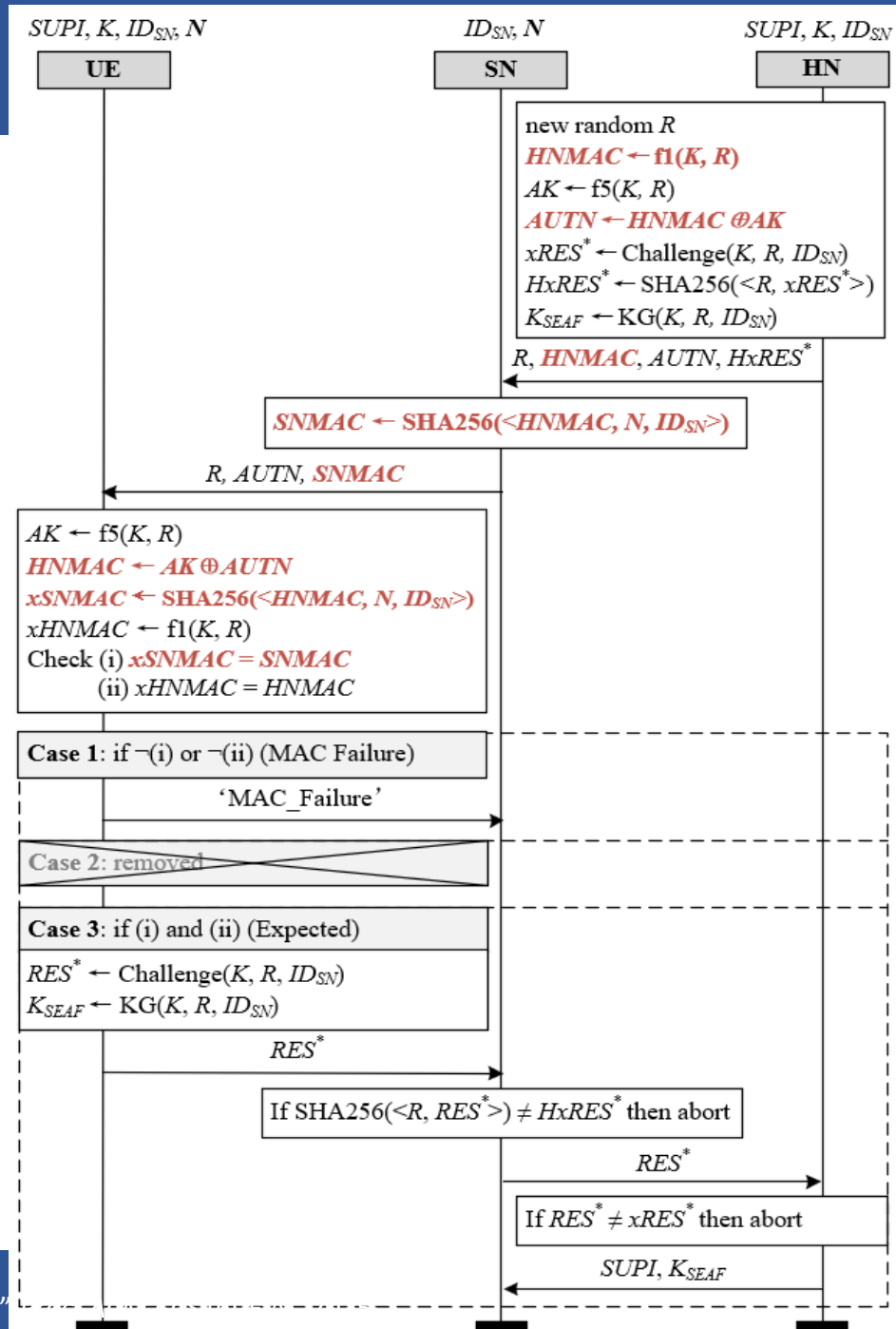
## 2. 展望 — 未来移动网络安全

### 5G-RNAKA协议

初始化阶段

挑战应答阶段

- 删除了与SQN相关的操作
  - UE中的SQN比较过程
  - UE和HN中的重同步过程 (case 2)
- SN利用 $N, ID_{SN}, HNMAC$ 计算 $SNMAC$ 
  - $N$  用来防 $\langle R, AUTN, SNMAC \rangle$ 消息被重放
  - $HNMAC$ 用来防止攻击者生成虚假的  $SNMAC$
  - $ID_{SN}$  确保UE认证SN.
- UE 验证 $SNMAC$  和 $HNMAC$ 来验证SN和HN
- HN对UE的认证原理与5G-AKA相同
- 认证成功后, UE和SN将获得一致的锚定密钥 $K_{SEAF}$



## 2. 展望 — 未来移动网络安全

### 5G-RNAKA协议的形式化分析结果

#### 5G-RNAKA和5G-AKA的对比

- 可实现UE与HN关于 $ID_{SN}$ 达成NI (A3)
  - UE通过验证SNMAC来认证SN
- 无需密钥确认实现UE与HN关于 $K_{SEAF}$ 达成I (A5)
  - UE通过SNMAC验证嵌入到 $K_{SEAF}$ 的 $ID_{SN}$
- 可实现UE不可区分性 (P2)
  - 无法通过观察是否收到失败消息区分用户

#### 结论

- 5G-RNAKA在认证性和隐私性方面优于5G-AKA

| Security goals                  | 5G-AKA | 5G-RNAKA [time (s)] |
|---------------------------------|--------|---------------------|
| A1: UE Weak agreement with HN   | ●      | ● [ 54.64]          |
| A2: HN Weak agreement with UE   | ●      | ● [ 137.48]         |
| A3: UE NI on $ID_{SN}$ with HN  | ○      | ● [ 9.57]           |
| A4: HN NI on $ID_{SN}$ with UE  | ●      | ● [ 11.51]          |
| A5: UE I on $K_{SEAF}$ with HN  | ◐      | ● [ 112.35]         |
| A6: HN I on $K_{SEAF}$ with UE  | ●      | ● [ 9.90]           |
| A7: UE Weak agreement with SN   | ◐      | ◐ [ 114.18]         |
| A8: SN Weak agreement with UE   | ●      | ● [ 8.61]           |
| A9: UE I on $K_{SEAF}$ with SN  | ◐      | ◐ [ 34.33]          |
| A10: SN I on $K_{SEAF}$ with UE | ●      | ● [ 37.97]          |
| A11: SN NI on $SUPI$ with HN    | ●      | ● [ 7.31]           |
| A12: SN I on $K_{SEAF}$ with HN | ●      | ● [ 17.84]          |
| A13: HN I on $K_{SEAF}$ with SN | ○      | ○ [ 20.50]          |
| S1: Keep $K$ secret             | ●      | ● [ 15.65]          |
| S2: Keep $K_{SEAF}$ secret      | ●      | ● [ 42.08]          |
| P1: Keep $SUPI$ secret          | ●      | ● [ 44.71]          |
| P2: UE Indistinguishability     | ○      | ● [9465.56]         |

NI: 非单射一致性      I: 单射一致性

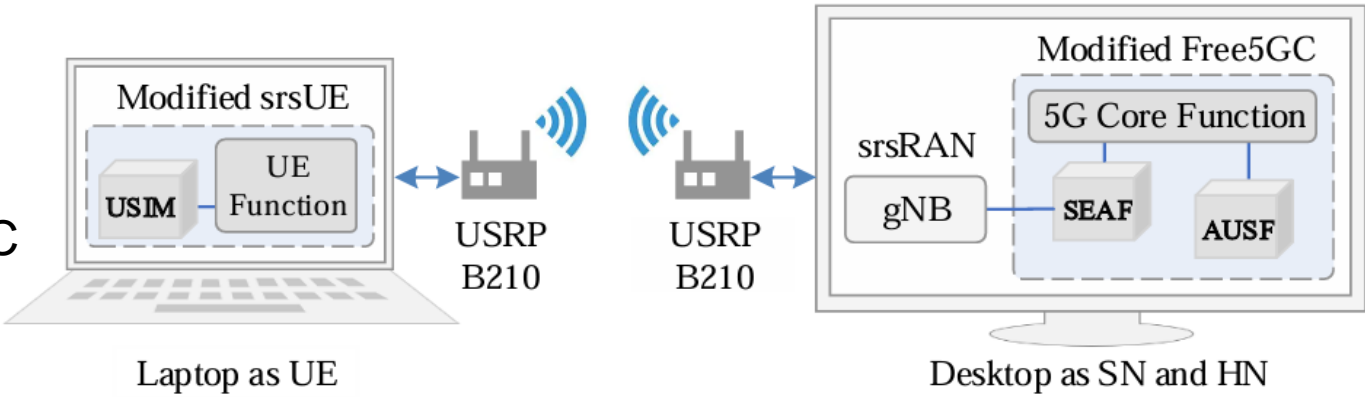
[1] H. Li, et al., “5G-RNAKA: A Random Number-based Authentication and Key Agreement Protocol for 5G Systems,” *Proc. ACM CCS (CCF A)*, 2025.

## 2. 展望 — 未来移动网络安全

### 5G-RNAKA协议的实现与性能分析

#### 验证环境

- UE: 笔记本电脑+修改后的SrsUE
- SN+HN: 台式机+srsRAN+修改后的Free5GC
- 无线通信: 两台USRP B210



#### 性能评估

- 计算开销: 减少了39.99%
- 存储开销: 减少了3.15%
- 通信开销: 减少了37.95%
- 端到端开销: 节省了重同步时间 (Case 2) → 其他情况 (Case1&3) 时间亦有减少

端到端开销(单位: 秒)

| Stage | 5G-AKA   |          |          | 5G-RNAKA |        |          |
|-------|----------|----------|----------|----------|--------|----------|
|       | Case 1   | Case 2   | Case 3   | Case 1   | Case 2 | Case 3   |
| S1-S0 | 0.482167 | 0.625720 | 0.572963 | 0.417251 | -      | 0.470587 |
| S2-S1 | 0.000023 | 0.000047 | 0.000032 | 0.000026 | -      | 0.000045 |
| S3-S2 | -        | 0.060721 | -        | -        | -      | -        |
| S4-S3 | -        | 0.000022 | -        | -        | -      | -        |
| S5-S4 | -        | 0.058987 | 0.085316 | -        | -      | 0.048126 |
| Total | 0.48219  | 0.745497 | 0.658311 | 0.417277 | -      | 0.518758 |

[1] H. Li, et al., “5G-RNAKA: A Random Number-based Authentication and Key Agreement Protocol for 5G Systems,” *Proc. ACM CCS (CCF A)*, 2025.

## 2. 展望 — 未来移动网络安全

### 空天地一体化网络安全

#### • 物理通信环境复杂

- 多空口：星地、星星、用户-卫星
- 开放信道易遭受多种等恶意攻击
- 太空轨道中多种干扰并存
- 误码率高、时延大

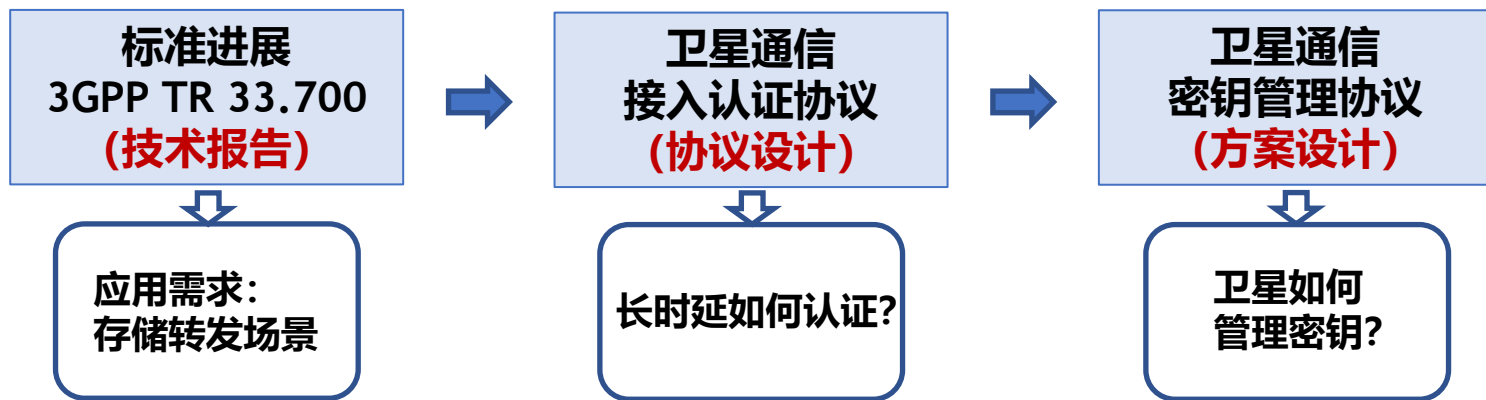
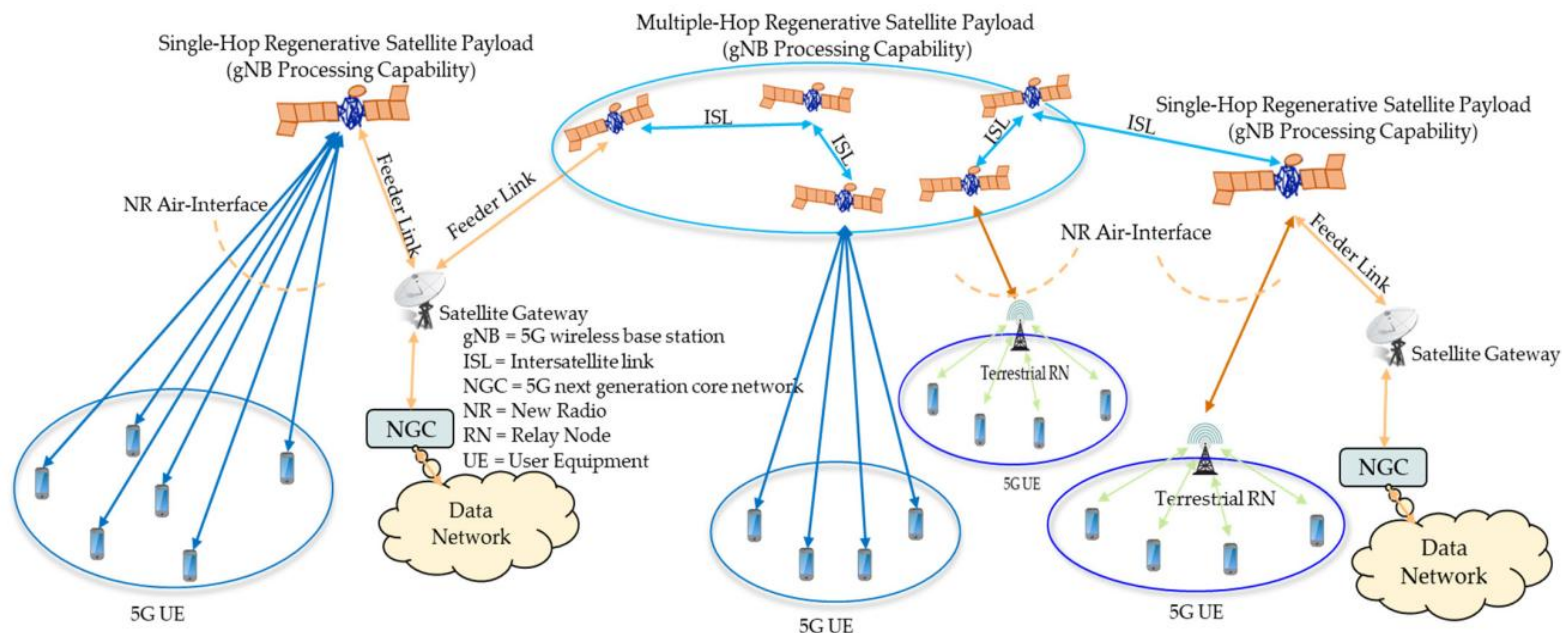
#### • 卫星节点能力受限

- 硬件处理能力较低
- 对于已有系统的修改比较困难

#### • 网络动态性变化

- 网络拓扑：无中心、自组织
- 地面终端：移动性、可扩展性、种类多
- 信任关系：不断变化

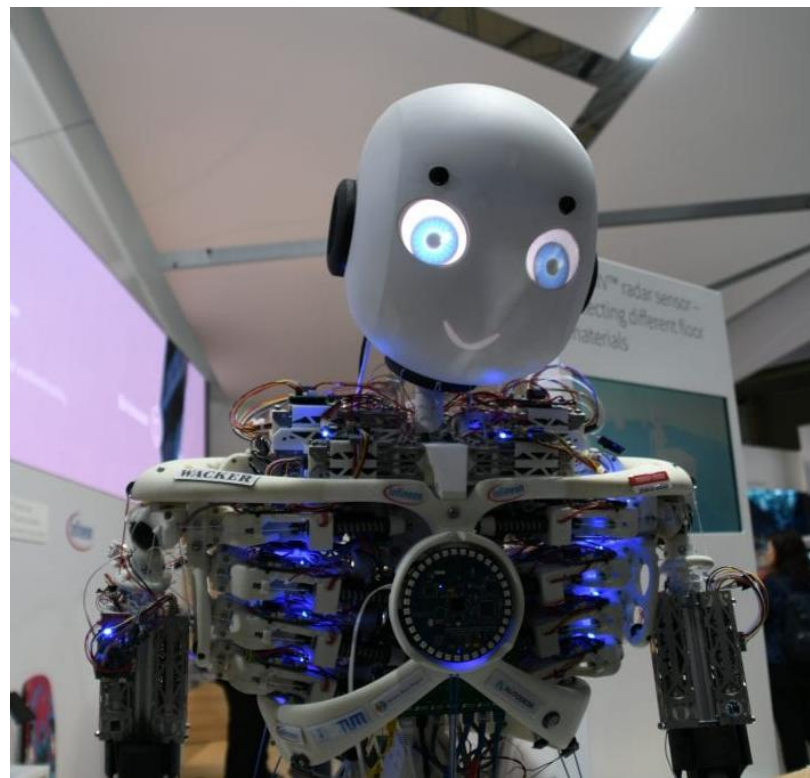
身份认证、密钥管理、访问控制难度大



## 2. 展望 — 未来移动网络安全

### AI赋能无线通信安全

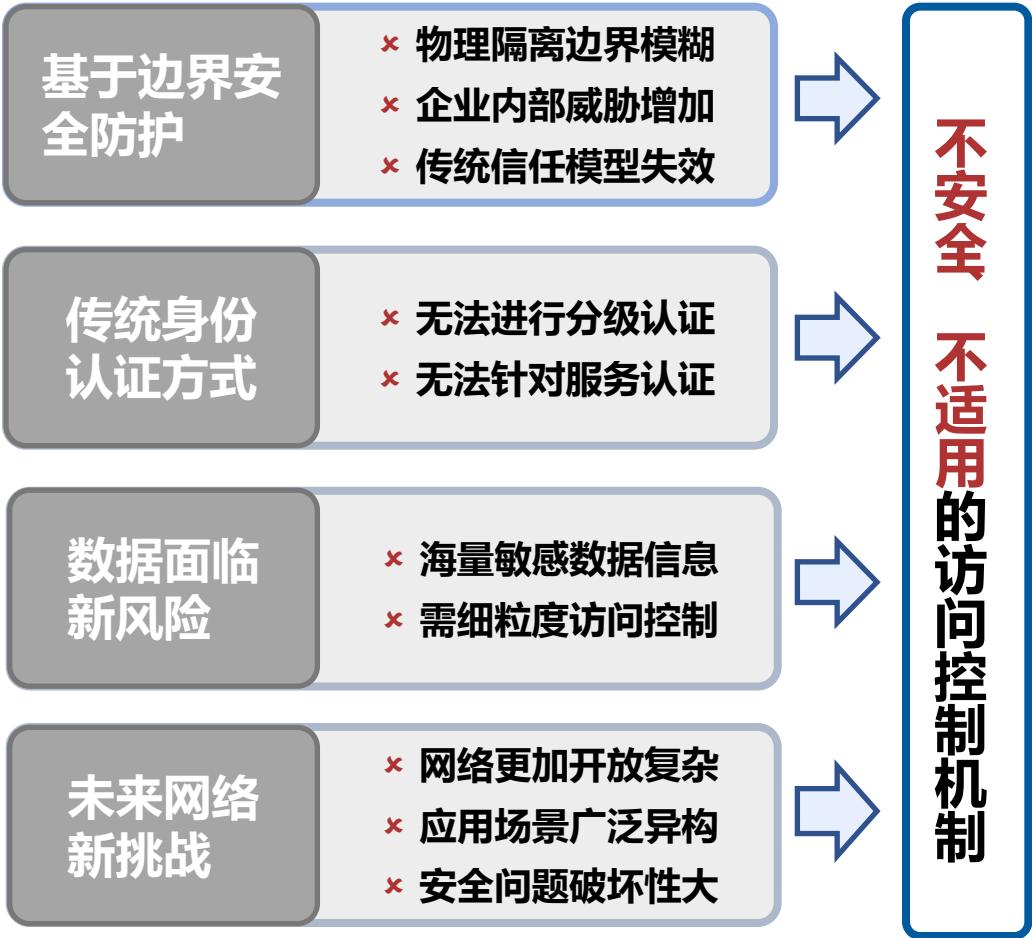
- **AI辅助伪基站检测：**利用无线信号特征和小区标识等自动识别伪基站；
- **AI辅助异常接入检测：**利用AI识别异常认证行为和异常位置更新；
- **AI核心网入侵检测：**检测DoS、信令风暴、异常流量等；
- **AI辅助切片安全：**监测Slice异常和跨Slice访问；
- **AI赋能无线资源安全：**AI辅助抗干扰和频谱感知；
- **AI赋能协议安全分析：**利用AI自动提取协议流程和安全目标、生成形式化模型、分析协议漏洞等；



<https://edwinhernandez.com/2020/01/04/artificial-intelligence/>

## 2. 展望 — 未来移动网络安全

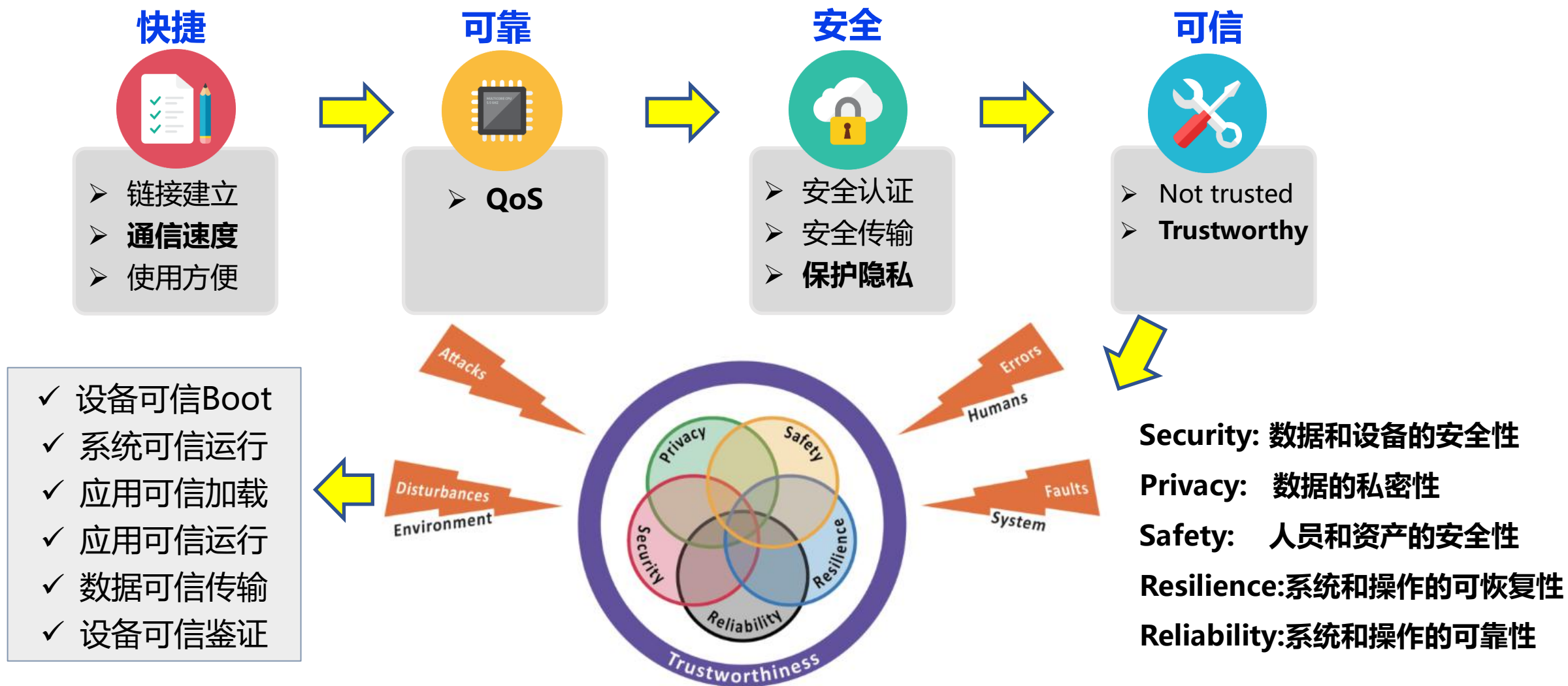
### 网络切片与零信任网络安全架构



- 零信任网络安全架构——
- ① 身份作为访问控制基础;
  - ② 仅授予所需最小权限;
  - ③ 实时计算访问控制;
  - ④ 资源受控安全访问;
  - ⑤ 信任等级持续评估。

## 2. 展望 — 未来移动网络安全

### 自验证可信通信理论与技术

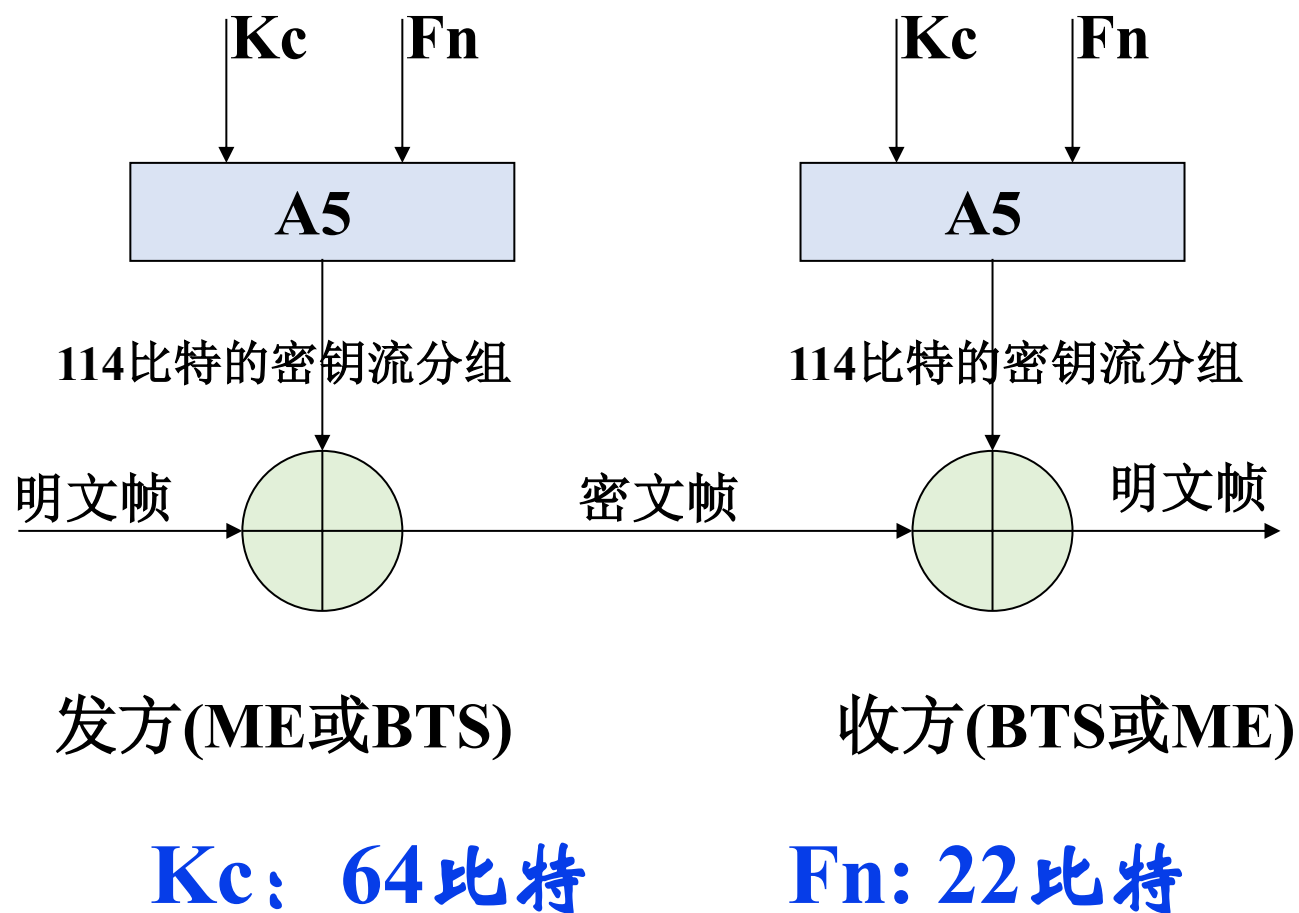


## 作业

1. 第一讲（概述）
2. 第二讲（密码学基础）
3. 第四讲（WLAN安全）
4. 第五讲（GSM安全）
5. 第六讲（TETRA安全）
6. 第七讲（WCDMA安全）
7. 第八讲（LTE安全）

# 作业讲解(GSM安全)

题目：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？



**Fn 的作用:**

- 保证每帧产生不同密钥流，防止密钥流重用
- 为发送端和接收端提供同步信息

**重新鉴权时间 (每帧延时4.615ms)**

$$N = 2^{22} = 4194304$$

$$T = 4194304 \times 4.615 \times 10^{-3}$$

$$T \approx 5.37h$$

**GSM帧号周期是一个hyperframe, 包含:**

$$2048 \times 26 \times 51 = 2715648 \text{ 个TDMA帧。}$$

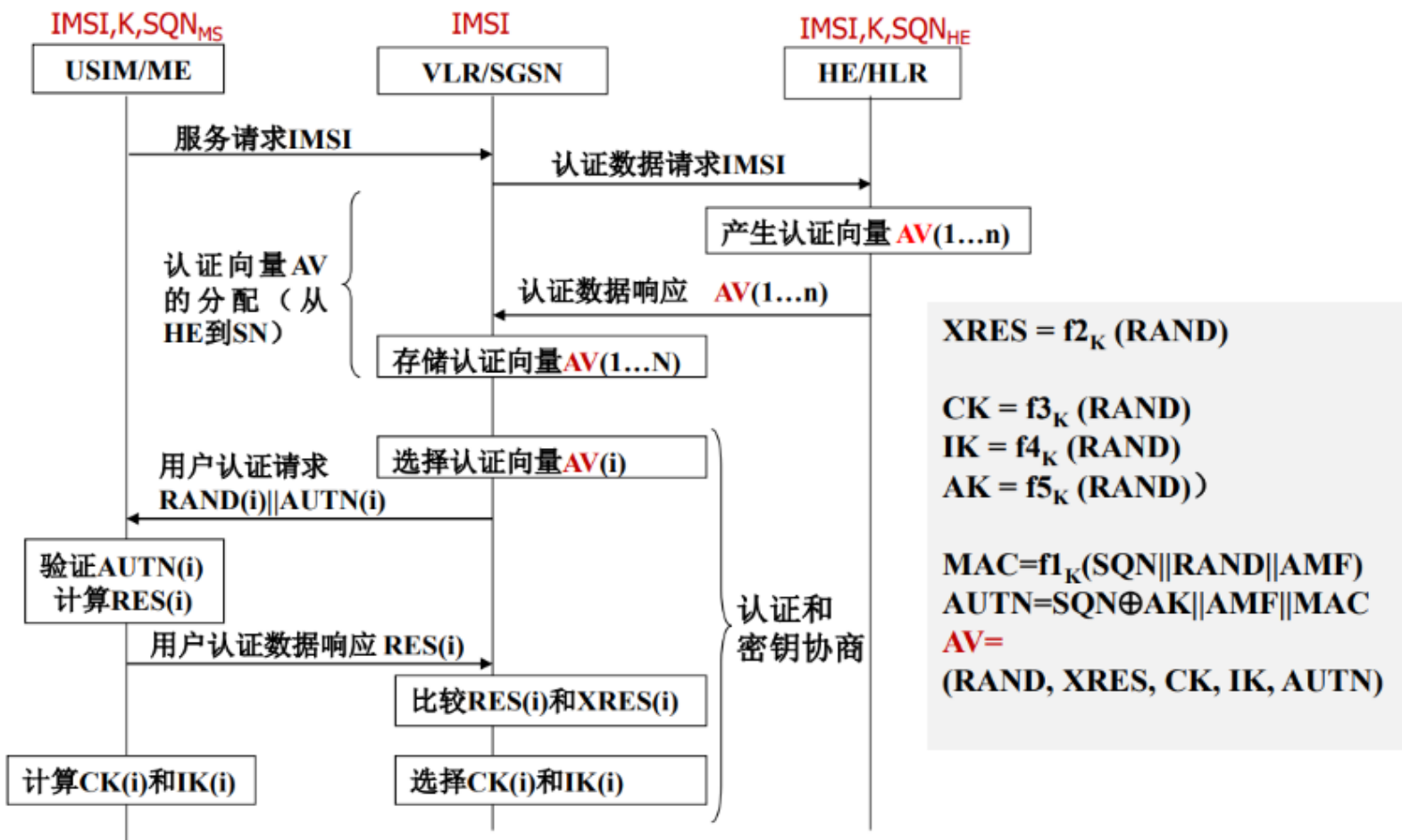
**Fn实际取值范围是: 0 ~ 2715647**

$$T = 2715648 \times 4.615 \times 10^{-3}$$

$$\approx 3.28 h$$

# 作业讲解 (WCDMA安全)

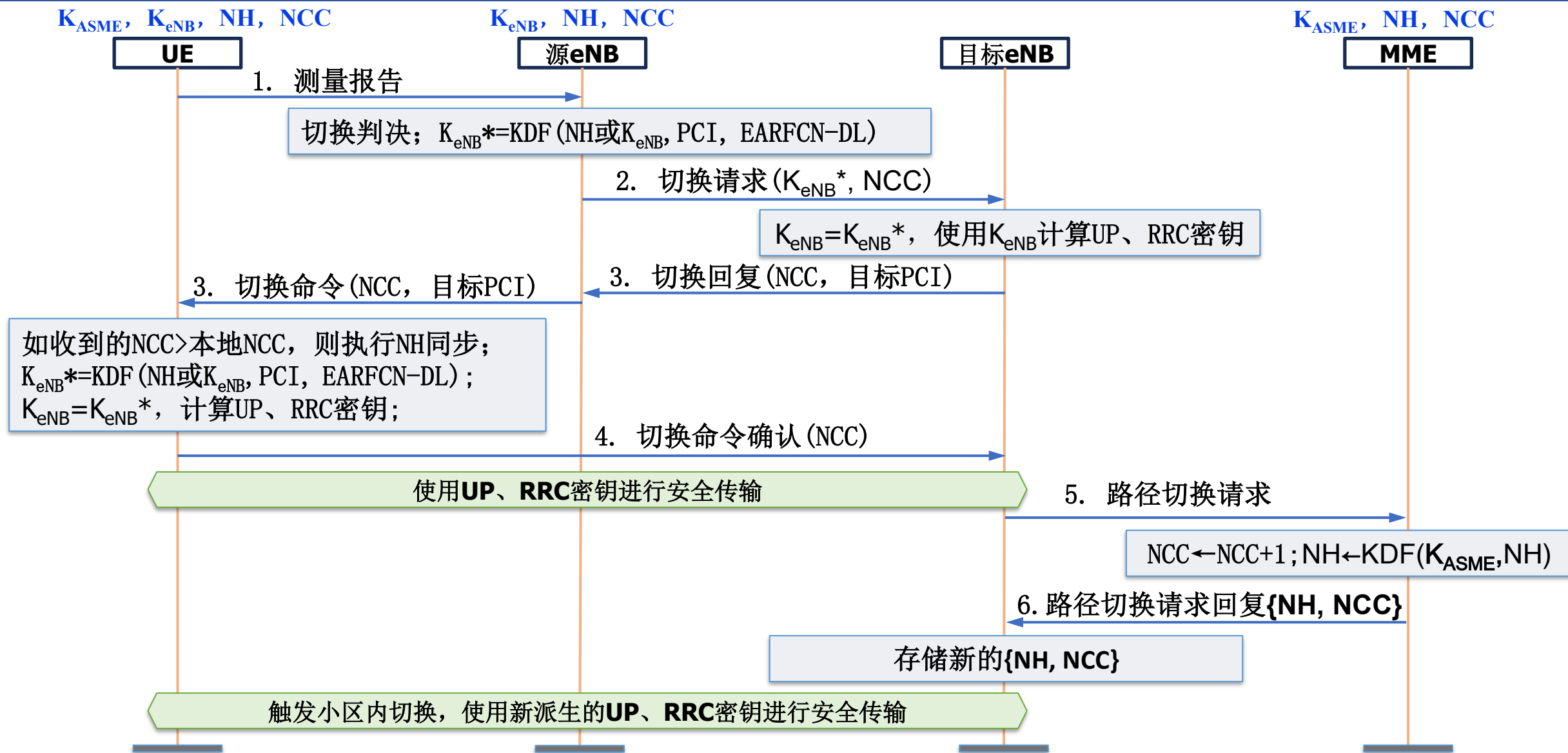
题目：描述WCDMA系统中的AKA协议，给出其安全目标，并分析其正确性。



## 安全目标:

- 双向认证
  - UE认证网络
  - 网络认证UE
- 产生一致且新鲜的密钥
  - CK一致、新鲜、排它
  - IK一致、新鲜、排它

# 作业讲解(LTE安全)



预祝大家  
学业有成！  
前程似锦！

