南京郵電大學
Nanjing University of Posts and Telecommunications

无线蜂窝网4G安全-密钥管理

汇报人：陈浩南
汇报日期：4.1

目录 CONTNENTS

人 工 智 能 语 言 模 型

PART 01

引言

Work Summary

4G网络特点与安全挑战

高带宽与低延迟的双刃剑

4G网络的高带宽和低延迟为用户带来便捷，但同时也增加了数据传输的风险，数据在传输过程中更容易被窃取和篡改。无线通信的开放性使得网络容易受到伪基站攻击，攻击者可以利用这一特点进行中间人攻击，窃取用户隐私。

安全威胁场景与案例

2019年伪基站中间人攻击事件，攻击者利用密钥派生漏洞伪造基站，窃取用户短信与支付验证码，导致百万级用户隐私泄露。其他威胁还包括IMSI捕获、信令篡改、身份伪装等，这些威胁严重威胁了4G网络的安全性。

密钥的核心价值与作用

密钥在4G网络安全中起着至关重要的作用，它能够抵御伪基站攻击，保障数据的机密性与完整性。密钥通过加密、完整性保护和身份认证等功能，为4G网络提供了全方位的安全保障。

密钥的作用与重要性

01

加密与数据保护

密钥用于加密数据，防止数据在传输过程中被泄露，保护用户的隐私和敏感信息。

通过加密，即使数据被攻击者截获，也无法轻易获取其内容，从而有效防止数据泄露。

02

完整性保护与篡改防御

密钥用于生成消息认证码（MAC），对数据进行完整性保护，防止数据在传输过程中被篡改。

通过完整性保护，可以检测到数据是否被篡改，从而确保数据的完整性和可靠性。

03

身份认证与合法性验证

密钥用于双向验证终端与网络的合法性，确保只有合法的用户和设备能够接入网络。

身份认证可以防止身份伪装攻击，保护网络的安全性和稳定性。

人 工 智 能 语 言 模 型

PART 02

密钥介绍

Work Summary

各代密钥技术安全特征对比

2G密钥

单层平面结构，功能简单，仅支持接入层（AS）的加密，无完整性保护，密钥层次扁平，未区分控制面与用户面。

缺陷：

无完整性保护密钥，密钥衍生路径单一，易受重放攻击和中间人攻击。

3G密钥

分层雏形，引入完整性保护。首次区分加密与完整性保护，初步形成接入层（AS）与非接入层（NAS）的分层，但层次仍较简单。

进步：

双向鉴权（含 AUTN 防重放）、完整性保护（EIA 算法），但密钥层级较少，AS 与 NAS 密钥仍强耦合。

4G密钥

多层级树形架构，精细化分层。密钥层次深度分化，接入层进一步细分基站级与业务层密钥，支持跨层密钥衍生与动态更新

优势：

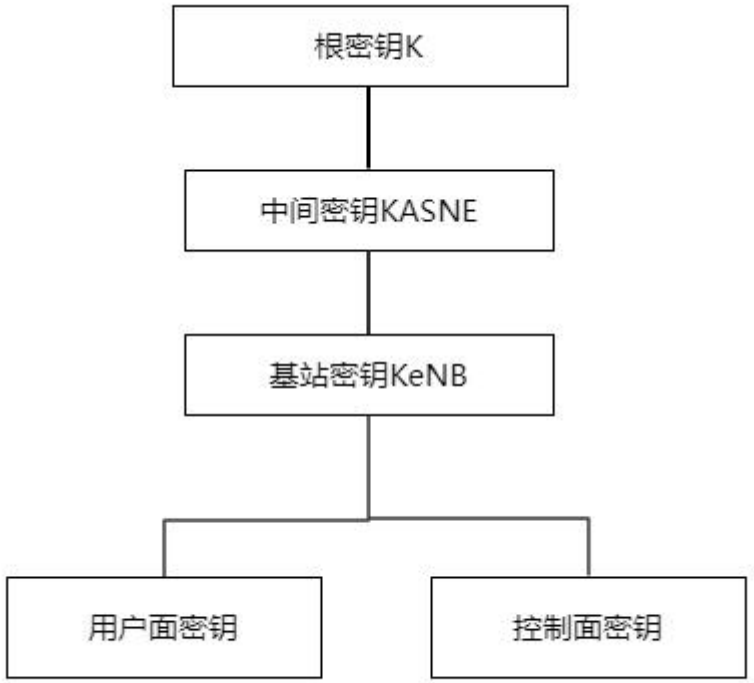
每层密钥独立作用域，通过密钥衍生函数（KDF）实现层级隔离，支持跨基站切换时的局部密钥更新，安全性与灵活性显著提升。

维度	2G（GSM）	3G（UMTS）	4G（LTE）
密钥层数	1 层（Ki → Kc）	2-3 层（K → CK/IK/K NAS）	4-5 层（K → KASME → KgNB → KUPsec/KNASenc）
功能细分	仅加密，无完整性保护	加密 + 完整性保护，区分 AS/NAS	加密 + 完整性保护，细分用户面 / 控制面、基站级 / 业务层
衍生机制	简单算法（A8）直接生成 Kc	基于鉴权向量（CK/IK 同生）	多层级密钥衍生函数（KDF），支持动态参数输入（如基站 ID、时间戳）
跨层依赖	单层依赖，无层级隔离	AS 与 NAS 密钥弱关联	严格分层，下层密钥由上层派生，层级间通过 KDF 解耦
动态更新	不支持（密钥一次生成）	有限支持（鉴权时更新 CK/IK）	全面支持（周期性 / 事件触发，切换时局部更新 KgNB 及下层密钥）
安全能力	仅防窃听（弱加密）	防窃听 + 防篡改（完整性保护）	防窃听 + 防篡改 + 防重放 + 密钥时效管理（如序列号、计数器）

密钥层级

在无线蜂窝网 4G（LTE）的安全体系中，密钥管理通过分层结构保障通信安全，并在切换场景下通过密钥切换机制实现密钥的动态更新

层级	核心作用
根密钥	生成中间密钥，绑定用户身份
中间密钥	派生会话密钥，支持多基站服务
会话秘钥	基站级加密、完整性保护与切换安全



- **最小化泄露**：泄露不影响KASME）
- **前向安全性**：H密钥设计）
- **业务隔离**：密钥

人 工 智 能 语 言 模 型

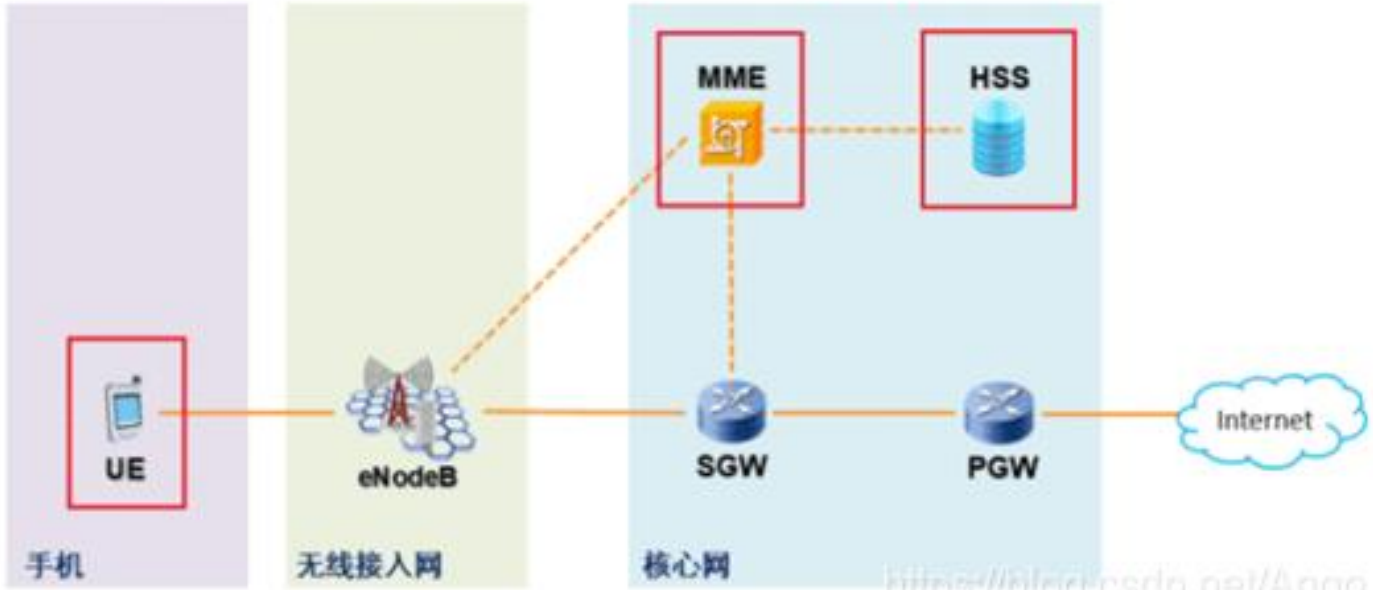
PART 03

密钥机制

Work Summary

密钥生成与分发机制

在 4G LTE 网络中，密钥生成和分发机制是EPS-AKA 鉴权的核心延伸，基于鉴权过程中生成的根密钥，通过层次化密钥结构衍生出多层密钥，实现接入层（AS）和非接入层（NAS）的安全保护。



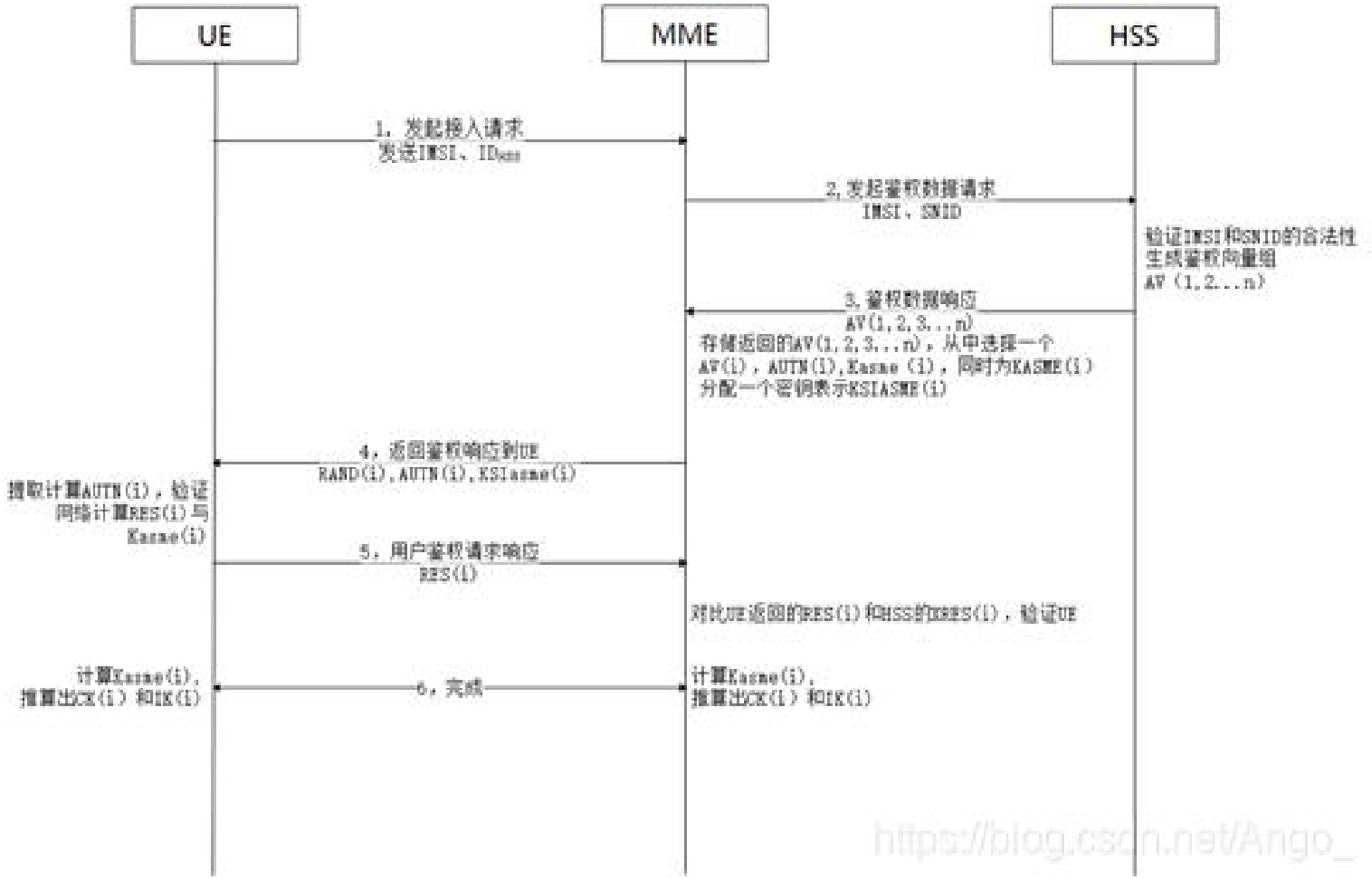
LTE基本结构

四元组鉴权向量

鉴权向量由 AUC 基于用户根密钥 K 与随机数算法生成：

- **RAND（随机数）：**由 HSS （归属签约用户服务器）生成的 128 位随机数，作为鉴权过程的输入之一，用于触发用户设备（UE）和网络侧的鉴权计算。
- **AUTN（鉴权令牌）：**UE 通过解析 AUTN 验证网络是否为合法服务方，并检查消息新鲜性。
- **XRES（期望响应值）：**AUC 通过加密算法（如 Milenage）计算的理论响应值，用于验证用户合法性；
- **KASME（接入层密钥）：**由 HSS 通过密钥（K）和 RAND 生成的 256 位密钥，是后续生成接入层密钥（如 K-eNB）和会话密钥的基础。

密钥生成与分发流程



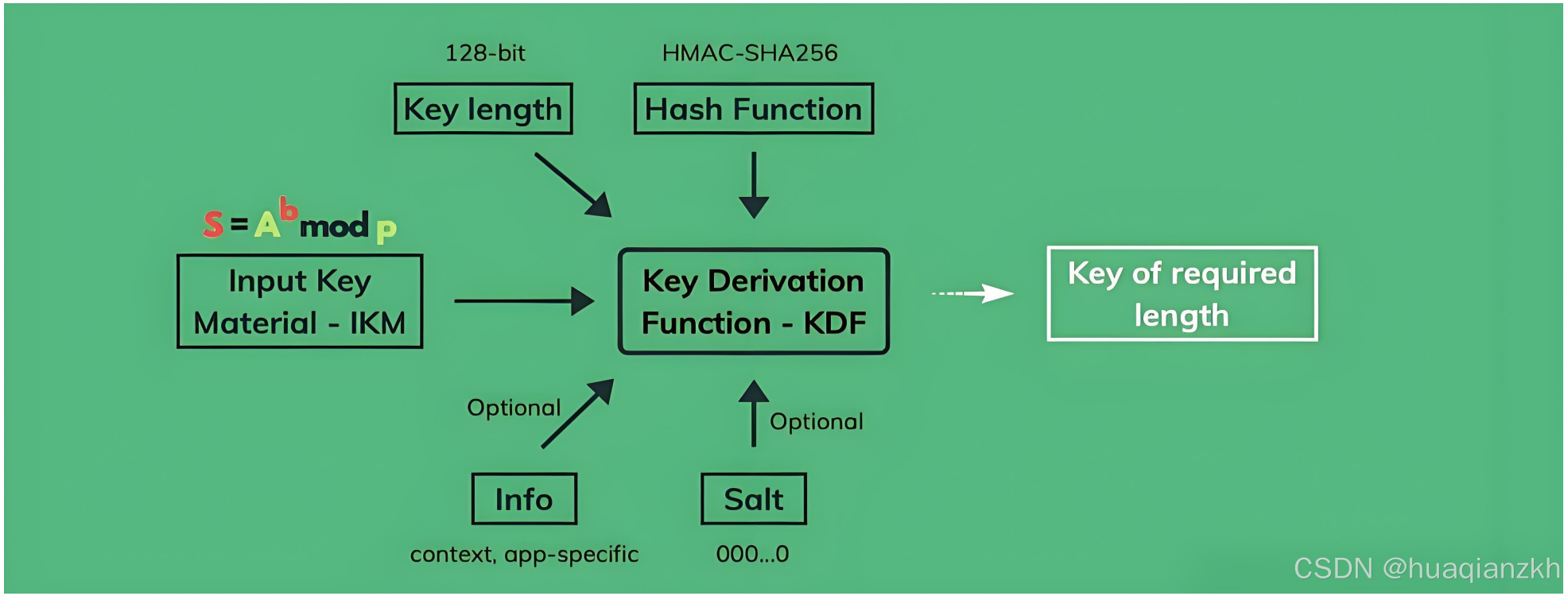
密钥生成与分发机制

核心优势

- 最小化密钥暴露风险：通过层次化推导，仅必要网元持有对应密钥，降低单一节点泄露的影响。
- 高效密钥协商：鉴权后无需额外信令交互，直接通过本地算法生成下层密钥，减少信令开销。
- 兼容性与扩展性：支持 2G/3G 网络漫游，并为 5G 的密钥机制奠定分层设计基础。

密钥派生函数（KDF）机制

密钥派生函数（KDF）：是一种从初始密钥材料（如根密钥、密码、随机数等）安全派生出多个目标密钥的算法，核心作用是将“短密钥”或“弱密钥”转换为满足特定安全需求（如长度、用途）的“强密钥”，并通过添加盐值、迭代次数等参数增强抗攻击性。它是现代密码学和网络安全中密钥管理的关键组件，尤其在层次化密钥体系（如 4G/5G 网络）中不可或缺。



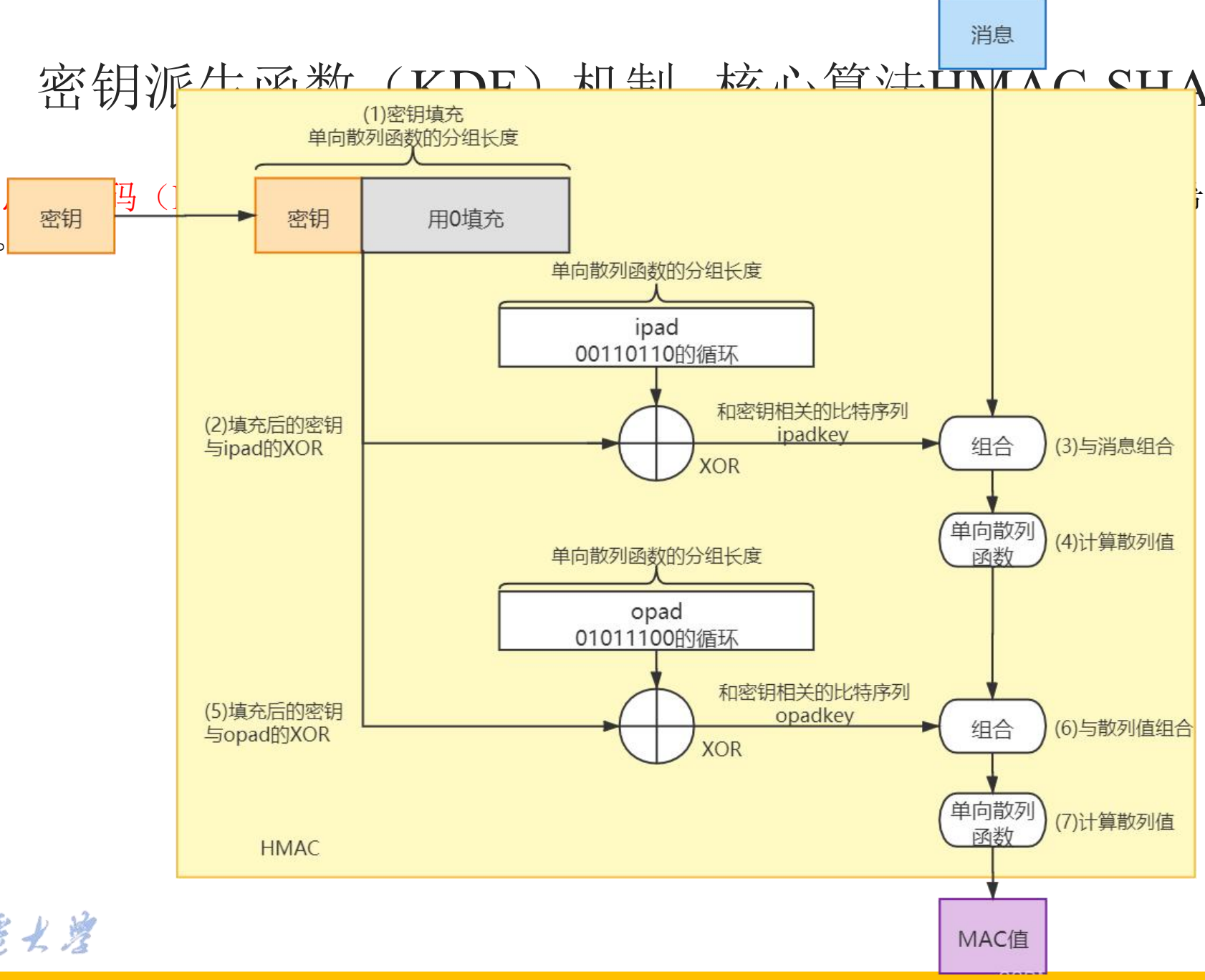
密钥派生函数（KDF）机制

核心作用：

- 分层隔离：避免上层密钥（如根密钥 K）直接参与业务加密，通过“中间密钥”（如 KASME）派生下层密钥，缩小风险暴露范围；
- 动态唯一性：每次派生时加入随机参数，确保同一主密钥生成的目标密钥不同（如不同基站、不同时间的密钥不重复）；
- 算法兼容性：支持多种加密 / 完整性算法，通过参数输入适配不同安全需求。

密钥派生函数（KDF）机制 核心算法HMAC-SHA-256

基于 哈希消 码（ ，生成固定长度的目标密钥。



密钥派生函数（KDF）机制--核心算法HMAC-SHA-256

基于 哈希消息认证码（HMAC） 与 SHA-256 哈希算法，将 “主密钥 + 上下文参数” 混合哈希，生成固定长度的目标密钥。

优势：

- 抗碰撞性：SHA-256 的输出长度（256-bit）确保极难找到不同输入生成相同哈希值；
- 密钥相关性：HMAC 要求主密钥作为 “密钥输入”，避免单纯哈希导致的密钥泄露风险；
- 灵活性：通过调整输入参数顺序与组合，适配不同层次的密钥派生需求（如从 KASME 派生 KgNB 或 KUPsec）。

动态密钥更新与跨基站切换机制

为应对长期会话中的密钥泄露风险，4G 支持 **周期性或事件触发的** 密钥更新：

- 周期性更新：按预设时间间隔（如数分钟）重新协商密钥，降低密钥被破解概率；
- 事件触发：当用户移动性状态变化（如跨基站切换）或检测到安全威胁时，强制更新密钥。

更新过程通过控制面信令实现，利用上层密钥（如 KASME）派生新的业务层密钥，避免全链路密钥重新生成的开销。

动态密钥更新与跨基站切换机制

当用户终端在不同基站（eNodeB）间切换时，密钥协商需兼顾效率与安全性：

1. 源基站（Source eNodeB） 向核心网（MME）发送切换请求，携带当前密钥状态（如 KASME 有效时间）；

2. MME 触发密钥更新：若当前 KgNB（基站与终端之间的密钥） 未过期，可直接由 KASME（中间密钥） 派生新基站的 KgNB，避免与 HLR/AUC 重新鉴权；

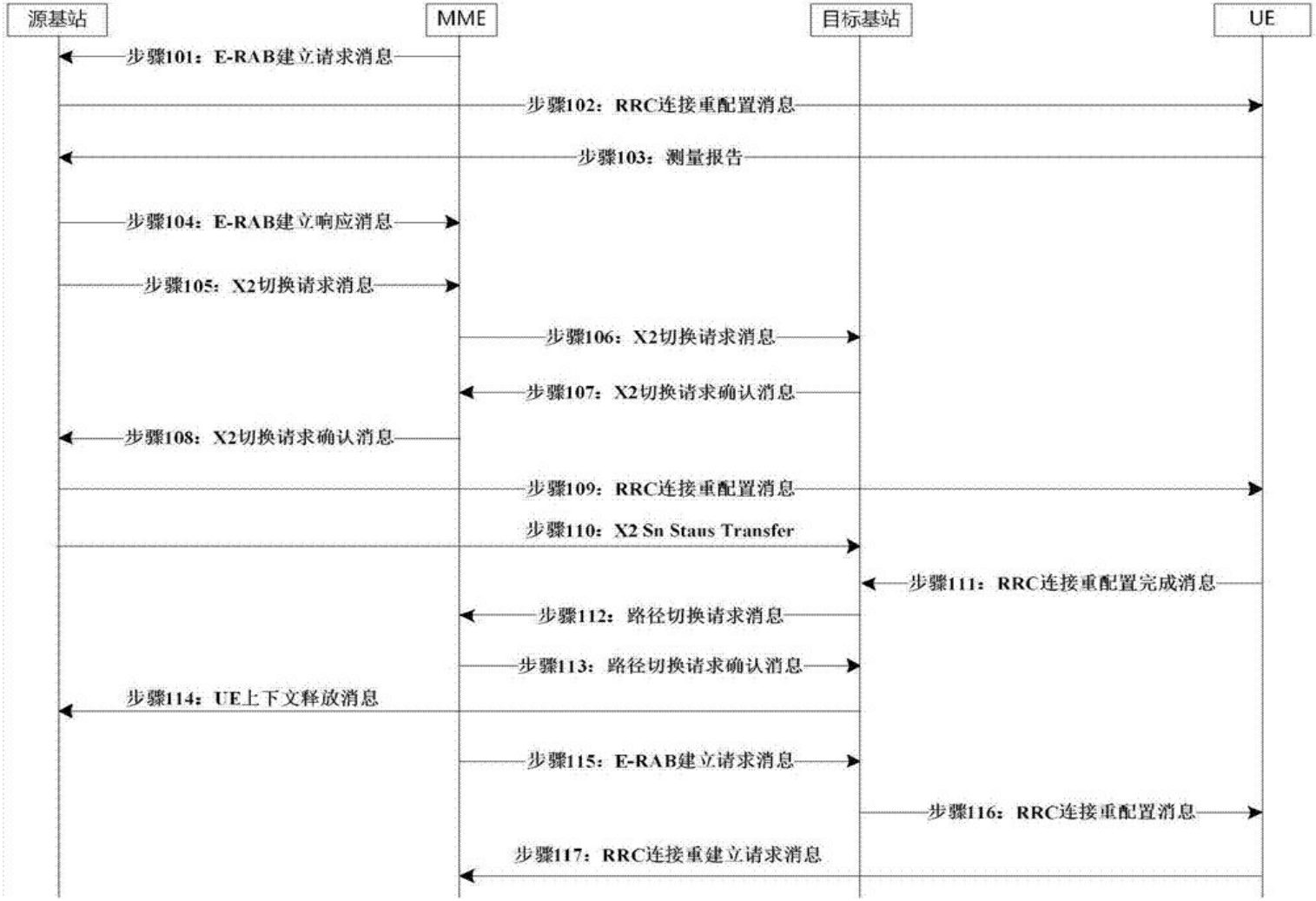
3. 目标基站（Target eNodeB） 与终端通过安全通道同步新 KgNB，并生成 KUPsec/KNASenc；

4. 切换完成后：旧基站密钥失效，新密钥仅在目标基站覆盖范围内生效，防止跨区域密钥滥用。

5. 该机制通过 密钥重用与局部更新，在保障安全的同时减少信令开销，提升切换效率。

KUPsec：是由移动设备（ME）和基站（gNB）从基站密钥（KgNB）派生的密钥，仅应用于使用特定加密算法保护 ME 和 gNB 之间的用户面（UP）通信流量，为用户数据提供机密性保护。
KNASenc：是由 ME 和接入与移动性管理功能（AMF）从 AMF 的密钥（KAMF）派生的密钥，仅应用于使用特定加密算法保护非接入层（NAS）信令，为 NAS 信令提供机密性保护。

跨基站切换机制


源基站
MME
目标基站
UE
步骤101：E-RAB建立请求消息
步骤102：RRC连接重配置消息
步骤103：测量报告
步骤104：E-RAB建立响应消息
步骤105：X2切换请求消息
步骤106：X2切换请求消息
步骤107：X2切换请求确认消息
步骤108：X2切换请求确认消息
步骤109：RRC连接重配置消息
步骤110：X2 Sn Staus Transfer
步骤111：RRC连接重配置完成消息
步骤112：路径切换请求消息
步骤113：路径切换请求确认消息
步骤114：UE上下文释放消息
步骤115：E-RAB建立请求消息
步骤116：RRC连接重配置消息
步骤117：RRC连接重建立请求消息

密钥切换优势

01

防历史破解(前向性安全)

每次切换生成新密钥，即使当前密钥泄露，历史通信仍安全。

02

防基站窃听

密钥与基站绑定，切换后旧基站无法解密新通信。

03

限时防护

缩短密钥有效期，降低被暴力破解风险。

人 工 智 能 语 言 模 型

PART 01

实际案例

Work Summary

密钥安全威胁与防护--典型攻击面分析

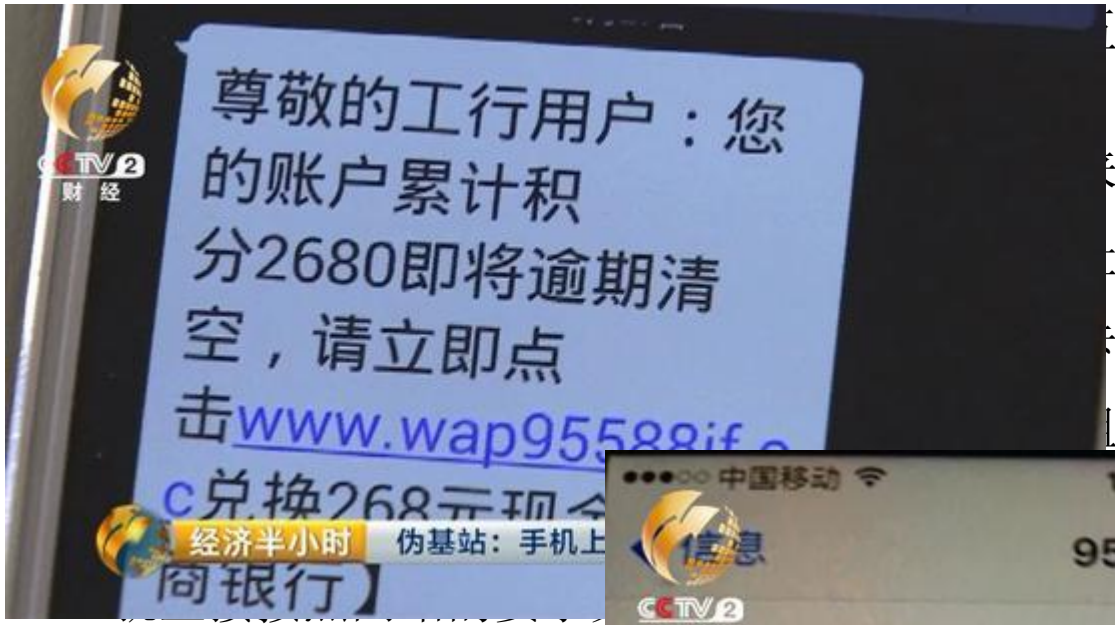
密钥泄露风险（存储 / 传输环节）：

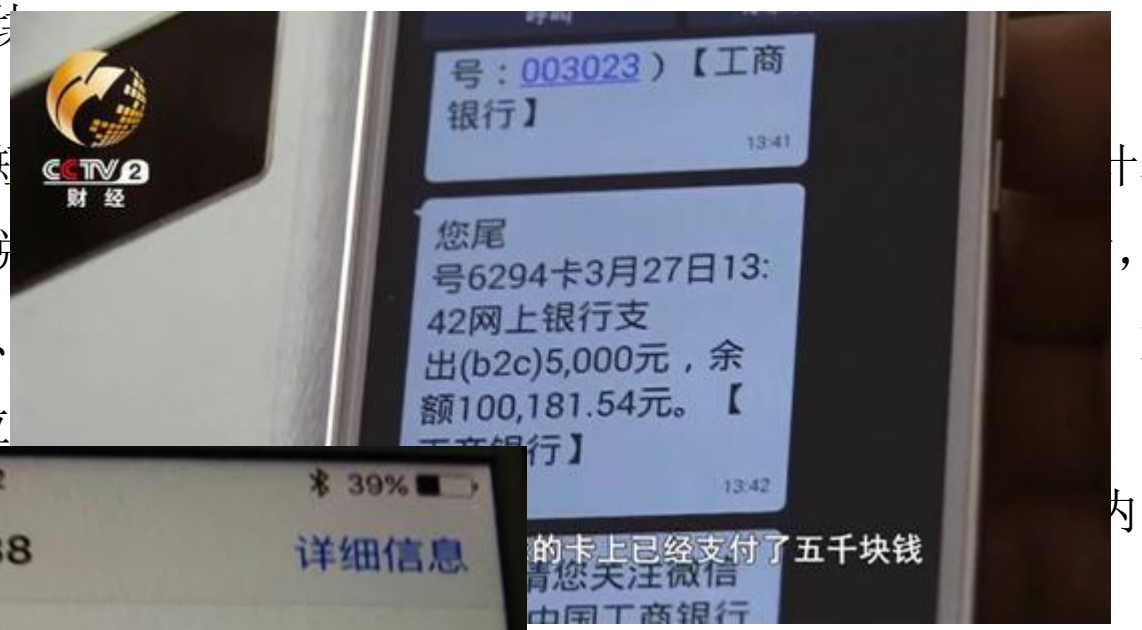
存储环节中，若密钥以明文形式存储或存储介质缺乏安全防护（如未使用硬件安全模块），攻击者可直接获取密钥；传输时若未采用加密协议（如未启用 TLS/IPsec），密钥可能被截获。

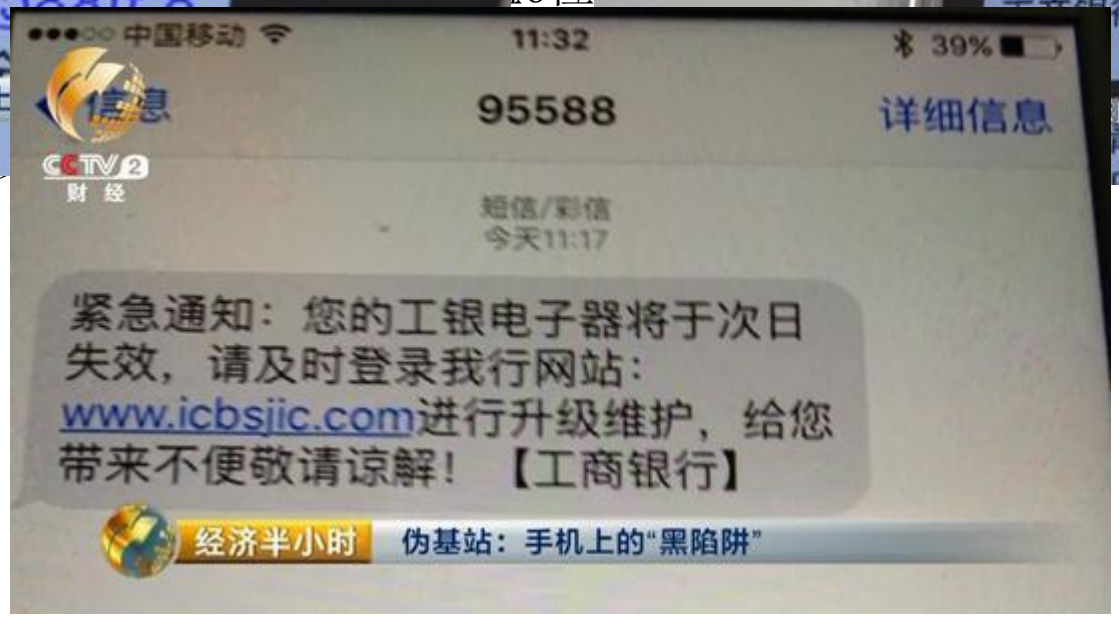
重放攻击与 SQN 同步问题：

重放攻击中，攻击者截获含旧密钥的信令并重新发送，试图绕过认证或解密数据。SQN（序列号）用于防重放，若网络侧与 UE 的 SQN 不同步（如 UE 未及时更新 SQN），可能导致合法信令被拒或接受重放信令。

密钥安全威胁与防护--实际案例







密钥安全威胁与防护--实际案例

中间人攻击：快递员调包包裹

攻击者如同心怀不轨的“快递员”，伪造通信双方身份获取密钥，解密通信内容。


抖音
抖音号: fengqiaojing38
停
警察
新型
网络wifi 诈骗

人 工 智 能 语 言 模 型

PART 05

安全挑战

Work Summary

4G密钥安全挑战

01

密钥层次的脆弱性

KASME 是 4G 接入层主密钥，下层密钥（如 KgNB、KUPsec）均由其派生。若 KASME 泄露，攻击者可推算出全链路密钥，导致用户数据、信令的机密性与完整性丧失。例如，攻击者获取 KASME 后，能解密用户通话内容、篡改短信等。

02

密钥转换的性能开销

在高铁等场景中，用户终端频繁切换基站。每次切换需重新派生密钥（如从旧 KgNB 转换为新 KgNB），终端与网络侧需执行 KDF 运算（如 HMAC - SHA - 256），消耗 CPU、内存等资源，可能导致终端发热、续航缩短，或网络侧处理延迟增加。

03

量子攻击下的密钥体系风险

现有 4G 密钥依赖传统密码学，量子计算机若运行 Shor 算法等后量子算法，可快速破解现有密钥生成逻辑，使 KASME 等密钥失去安全性。

3.参考文献

[1]陈胜宇.移动自组网密钥管理机制研究[D].西安电子科技大学,2019.DOI:10.27389/d.cnki.gxadu.2019.001556.
[2]蔡旻甫.计算机网络安全中信息保密技术研究[J].电脑知识与技术,2014,10(33):7838-7839+7846.DOI:10.14004/j.cnki.ckt.2014.0856.
[3]白媛,王倩,贾其兰,等.一种高效安全的EPS AKA协议[J].北京邮电大学学报,2015,38(S1):10-14.DOI:10.13190/j.jbupt.2015.s1.003.
[4]许书彬,吴巍,杨国瑞.基于CPK的IMS认证与密钥协商协议[J].现代电子技术,2011,34(13):117-119.DOI:10.16652/j.issn.1004-373x.2011.13.045.
[5]朱国超.无线局域网的构建及安全防范技术研究[J].计算机安全,2010,(04):66-68.
[6]周磊.面向3G/4G移动网络保密终端安全通信技术研究[D].东南大学,2016.
[7]丁源.4G通信系统中协作通信存在的安全缺陷及处理[J].通讯世界,2015,(07):27-28.
[8]李娜,王盛,李鸥.4G移动通信系统中协作通信的安全缺陷分析[J].电讯技术,2013,53(11):1500-1505.
[9]胡海翔,林斌.基于4G通信技术的无线网络安全通信研究[J].数字通信世界,2018,(07):89.
[10]王宁瑀.4G网络现状分析与安全对策研究[J].中国新通信,2015,17(10):21.

谢谢！

计算机学院 软件学院
网络空间安全学院
School of Computer Science