面向 B5G 网络的高效切换认证与安全密钥更新机制

崔琪楣[1,2]，赵文静[1]，顾晓阳[1]，朱增宝[1]，朱晓暄[3]，陶小峰[1,2]，倪巍[4]

（1. 北京邮电大学信息与通信工程学院，北京 100876；2. 鹏城实验室，广东 深圳 518055；
3. 中国科学技术交流中心，北京 100045；4. 澳大利亚联邦科学与工业研究组织，悉尼 2122）

摘 要：为了解决 5G 网络切换认证与密钥更新机制不具备前向安全性、易遭受旁路攻击、存在信令拥塞等问题，针对 5G 增强（B5G）网络，提出一种基于无证书的高效切换认证与安全密钥更新机制。在网络边缘侧引入基于无证书的密钥协商机制，使移动终端主动发起密钥更新请求，在空口侧完成无证书密钥更新全过程；在 eCK 安全模型下基于 Diffie-Hellman 困难问题，从理论上证明了该密钥更新机制的安全性。仿真评估表明，所提机制不仅满足了移动终端密钥管理的前向安全，与其他同类切换认证相比有更低的通信开销和计算开销。

关键词：切换认证；密钥更新；无证书密钥协商；eCK 安全模型

中图分类号：TN929.5

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021240

Efficient handover authentication and secure key-updating mechanism for B5G networks

CUI Qimei[1,2], ZHAO Wenjing[1], GU Xiaoyang[1], ZHU Zengbao[1], ZHU Xiaoxuan[3], TAO Xiaofeng[1,2], NI Wei[4]

1. School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Peng Cheng Laboratory, Shenzhen 518055, China
3. China Science and Technology Exchange Center, Beijing 100045, China
4. Commonwealth Scientific and Industrial Research Organization, Sydney 2122, Australia

Abstract: In order to solve the problems of 5G network handover authentication and key update mechanism, such as lacking of forward security, being vulnerable to bypass attack and having signaling congestion, for 5G enhanced (B5G) network, an efficient handover authentication and security key-updating mechanism based on no certificate was proposed.

The certificateless key agreement mechanism was introduced in the network edge side, which made the mobile terminals initiate the key-updating request actively and complete the whole certificateless key-updating process on the fly. The security of the key-updating mechanism was proved theoretically based on the Diffie-Hellman problem under the eCK security model. Simulation results demonstrate that the proposed mechanism not only meets the forward security of mobile terminal key management, but also has lower communication and computing overheads compared with other similar handoff authentication.

Keywords: handover authentication, key-updating, certificateless key agreement, eCK security model

1 引言

随着 3GPP R-16 版本机制的冻结和 R-17 版本机制的跟进，全球各主要国家正逐步加快推进 5G 网络落地与应用的进程。5G 以其高速率、大容量、低时延等卓越性能，正逐步支持增强移动带宽（eMBB, enhanced mobile broadband）、高可靠低时延通信（uRLLC, ultra-reliable low-latency communication）和大规模机器类型通信（mMTC, massive machine type communication）三大典型应用场景[1]，

收稿日期：2021−09−10；**修回日期**：2021−12−06

基金项目：国家自然科学基金资助项目（No.61941114, No.61941105）；中国移动研究院联合创新中心基金资助项目

Foundation Items: The National Natural Science Foundation of China (No.61941114, No.61941105), Telecommunications-China Mobile Research Institute Joint Innovation Center

在推动 AR/VR、自动驾驶、工业互联网、远程医疗等新领域快速发展的同时，也使其面临着网络安全与数据隐私保护等方面的新挑战。

移动通信网络通过升级鉴权认证与密钥协商体系实现 5G 接入侧数据加密性与完整性保护。与长期演进（LTE, long term evolution）网络采用的鉴权认证及密钥协商机制相比，5G 网络提出 5G-AKA（5G authentication and key management）和 EAP-AKA（extensible authentication protocol authentication and key management）这 2 种接入认证方式，沿用并升级以 AES（advanced encryption standard）、ZUC（Zu Chong）、SNOW 3G 为代表的加密算法，支持小区内切换和小区间切换场景下的密钥更新机制[2]，以防止攻击者非法获取用户身份凭证、终端节点伪造，通信数据遭泄露或篡改。然而，当前 5G 网络的切换认证不具备前向安全性，还存在密钥生命周期管理不够灵活，密钥协商过程信令交互低效等问题，具体描述如下。

1) 当前 5G 网络采用的切换密钥链模型的水平推演不具备前向安全性。具体地，当上一个接入层（AS, access stratum）密钥失陷时，攻击者可以中断失陷基站的链路计数值（NCC, next-hop chaining count）更新，通过操控链路计数值对核心网发起去同步攻击[3-4]，根据失陷的 AS 层密钥和公共参数推导出下一 AS 层的密钥，即破坏密钥前向的安全性。

2) 移动终端在小区内切换时，密钥更新信令由基站 gNB（next generation node base station）发起，低移动性终端只能被动等待更新。在工业物联网、远程医疗等 mMTC 应用场景中，大规模低移动性终端在完成密钥协商流程后长期沿用初次协商的密钥，攻击者可利用多次加密运算过程中泄露的功耗、能量等信息对终端发起旁路攻击[5]。

3) 移动终端在小区间切换时，密钥更新信令由核心网的接入和移动管理功能（AMF, access and mobility management function）发起，更新过程需要基站和核心网完成多次信令交互。例如在车联网、智慧交通等 mMTC 应用场景中，高移动性机器类设备在密集小区中会频繁切换，切换时每个终端都要访问位于核心网的身份认证服务器，增加了传输过程的额外时延，这导致了核心网的资源消耗和严重的信令拥塞[6]。

针对 5G 网络切换认证与密钥更新机制中的前向安全问题，文献[7]基于代理签名、预认证和密钥预分配增强了会话密钥的安全管理。文献[8]基于无证书签密提出一种密钥的自生成机制解决前向安全缺陷，但密钥更新效率低。文献[9]通过向合法用户颁发公钥基础设施简化传统身份验证，但是使用周期短，在切换过程需要进行重认证，存在密钥托管问题。

针对大规模低移动性终端的密钥安全性问题，文献[10-16]均采用群组认证与密钥管理方案，主要是利用本地群组内获得的临时密钥进行认证，不需要与远程归属网络频繁交互，有效降低机器类设备入网成本。但是，群组认证与密钥管理存在以下缺点：①难以找出群组中的非法用户[10-12]；②依赖于秘密共享[13]、中国剩余定理[14]等密码学原语，与 5G 标准不兼容；③群认证只适用于初次接入认证，不适合切换认证[10-16]。因此，群组认证与密钥管理方案难以适用于 mMTC 场景的切换密钥更新管理。文献[17]在超密集组网模式下提出了一种基于安全区域的快速认证密钥协商协议，但该协议需要将空口数据面加解密功能以分布式部署于安全区域内的所有基站，也无法适配 5G 网络架构。

针对高移动性终端密钥更新的时延与效率问题，文献[18]利用辅基站在切换过程中传输数据，以降低传统切换方式中数据传输中断所引起的时延。文献[19]基于双陷门变色龙散列函数提出一种高效的切换认证协议，允许陷门散列密钥持有实体接入网络，避免了切换测量、判决等流程。文献[20]采用椭圆曲线密码实现了认证匿名性和不可追踪性。然而，文献[18-20]的密钥更新机制需要多次访问位于核心网中的身份认证服务器，降低了网络切换信令交互效率。文献[21]提出了基于无证书的密钥隔离方案，克服传统公钥密码体制下复杂的证书管理问题，但该方案采用运算量较大的双线性映射，复杂度高，难以适用于 mMTC 场景。

基于上述分析，本文引入无双线性的无证书密钥协商协议，并与移动边缘计算（MEC, mobile edge computing）技术融合，提出一种基于无证书的高效切换认证与安全密钥更新机制，主要贡献如下。

1) 本文沿用 5G 标准现有的椭圆曲线密码，基于无双线性的无证书密钥协商，提出一种满足前向安全性的新型密钥更新机制，所提机制以移动终端为密钥更新流程的发起点，终端可在密钥使用期限内发起 AS 层密钥更新，以保障大规模低移动性设备的隐私与安全。

2) 本文在 eCK（extended canetti krawczyk）安全模型下基于离散对数困难问题，证明了攻击者无法在多项式时间内攻破机制，并从理论上分析了所提机制满足前向安全性、会话密钥不可控性、抗密钥泄露伪装、抗未知密钥共享等安全属性。

3) 本文提出在 MEC 服务器上增加可信第三方密钥生成中心（KGC, key generation center），负责在初次认证时根据通信实体的身份信息来生成部分私钥[22]。与核心网的认证、授权、计费（AAA, authentication authorization accounting）服务器相比，MEC 位于接入网的边缘，更接近终端，并且具有强大的存储空间[23]，通过 MEC 服务器作为认证服务器，更新机制在不增加核心网资源成本的情况下可以减少信息传输距离和更新时延。仿真结果表明，所提机制在提高安全性的同时，也提高了接入侧密钥更新的效率。

2　相关研究

2.1　5G 网络的切换认证与密钥更新机制

5G 网络有 2 种切换更新机制：小区内切换和小区间切换。如图 1 所示，切换密钥链模型又分为式(1)所示的水平切换和式(2)所示的垂直切换。

$$K^{*}_{\text{NG-RAN}}=\text{KDF}\left(K_{\text{gNB}},\text{PCI,EARFCN-DL}\right) \quad (1)$$

$$K^{*}_{\text{NG-RAN}}=\text{KDF}\left(\text{NH}_{\text{NCC}},\text{PCI,EARFCN-DL}\right) \quad (2)$$

其中，PCI（physical cell ID）为目标小区的物理小区标识，EARFCN-DL（E-UTRAN absolute radio frequency channel number-down link）为下行链路绝对频率信道值，NCC 为链路计数值，NH（next-hop key）为下一跳密钥，NH_{NCC} 为 NCC 对应的下一跳密钥，如式(3)~式(5)所示。

$$\text{NH}_0=\text{KDF}\left\{K_{\text{AMF}},\text{NAS uplink COUNT}\right\} \quad (3)$$

$$\text{NH}_1=\text{KDF}\left\{K_{\text{AMF}},\text{NH}_0\right\} \quad (4)$$

$$\text{NH}_{\text{NCC}}=\text{KDF}\left\{K_{\text{AMF}},\text{NH}_{\text{NCC}-1}\right\} \quad (5)$$

2.1.1　小区内切换

5G 基站分为集中式单元（CU, centralized unit）和分布式单元（DU，distributed unit）两部分，当用户设备（UE, user equipment）从同一 gNB 内的一个 gNB-DU 切换到另一个 gNB-DU 时，这种切换被称为小区内切换，如图 2 所示。

1) gNB 选择切换的目标 UE，在切换命令中将 NCC 值发送给目标 UE。

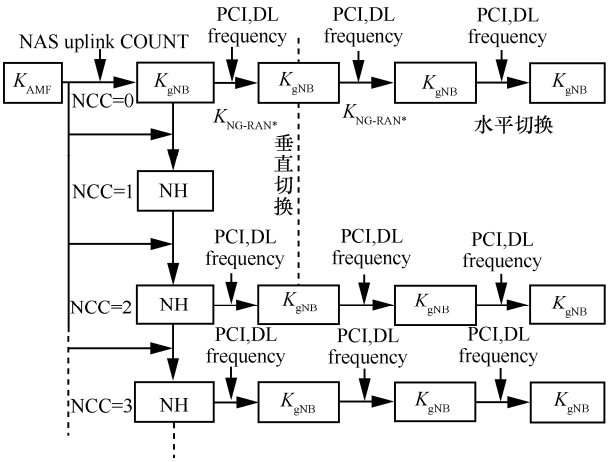


图 1　切换密钥链模型

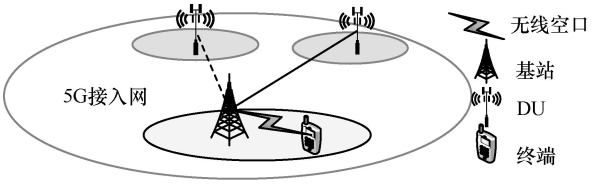


图 2　小区内切换场景

2) gNB 和 UE 将使用目标 PCI 和 EARFCN-DL 来执行切换密钥链：如果 gNB 中存在未使用的 {NH,NCC} 对，执行垂直切换，否则执行水平切换。

3) 在切换后，UE 决定是否更新当前密钥 K_{gNB}，若更新则令 $K_{\text{gNB}}=K^{*}_{\text{NG-RAN}}$，否则保留当前 K_{gNB}。

2.1.2　小区间切换

5G 网络有 2 种小区间切换类型[1]：Xn 切换和 N2 切换，这是以切换时信令传输经由的接口命名的。如图 3 所示，当 UE 移动时，可能会通过 Xn 接口从源 gNB 切换到同一个 AMF 管理下的目标 gNB，这种切换被称为 Xn 切换，具体流程如图 4 所示。

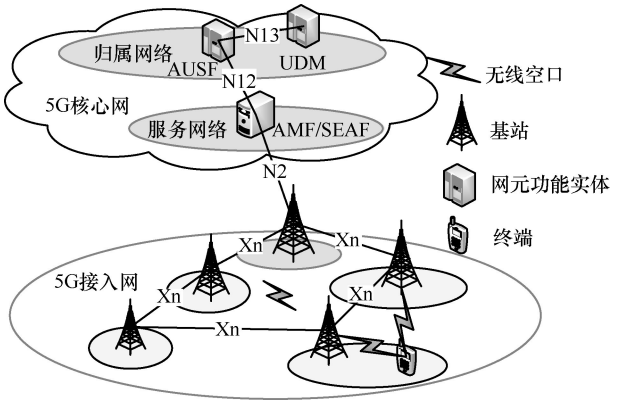


图 3　Xn 切换场景

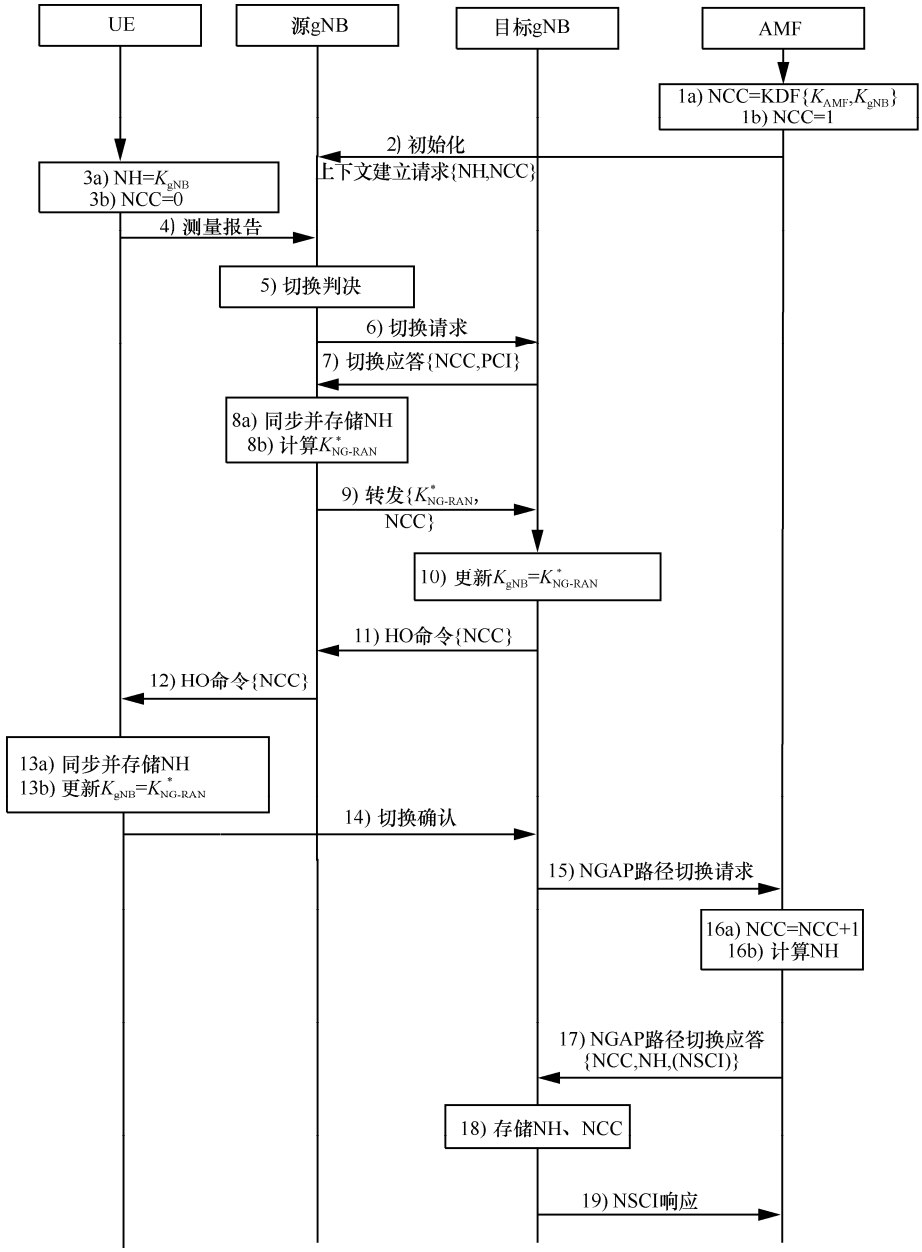


图 4　Xn 切换的密钥更新流程

1)~3)初始化上下文建立请求：当 UE 从源 gNB 移动到同一个 AMF 管理下的目标 gNB 时，AMF 向源 gNB 发送初始化上下文建立请求，包含安全参数 {NH, NCC}，UE 设置 NH = K_{gNB} 、NCC = 0，完成下一跳密钥的初始化工作。

4)～7)更新请求：UE 通过无线链路向源 gNB 发送测量报告，源 gNB 根据测量报告做出切换判决后向目标 gNB 发起切换请求，目标 gNB 返回包含安全参数 $\{\text{NH, NCC}\}$ 的切换应答。

8)～10)目标 gNB 更新下一跳密钥：若源 gNB 接收到的 NCC 比当前使用的 K_{gNB} 的 NCC 大，则同步 {NH, NCC} 后，根据式(2)进行垂直推演；否则根据式(1)进行水平推演。

源 gNB 向目标 gNB 发送 $\{K^*_{gNB}, \text{NCC}\}$，在目标 gNB 侧更新 AS 层密钥 $K_{gNB} = K^*_{NG\text{-}RAN}$。

11)~13)UE 更新下一跳密钥：由于 UE 还未与目标 gNB 建立安全通信，源 gNB 在收到 HO 切换指令后转发 $\{\text{NCC, PCI, EARFCN-DL}\}$。若 UE 接收到的 NCC 大于本地存储的 NCC，则根据式(5)同步并存储 NH，再根据式(2)进行垂直推演；否则根据式(1)进行水平推演。在 UE 侧更新密钥 $K_{gNB} = K^*_{NG\text{-}RAN}$。

14)～19)为下一次切换提供密钥材料：UE 向目标 gNB 发送切换确认，与目标 gNB 建立安全通信；gNB 向 AMF 发送路径切换请求，AMF 同步 NH，设置 NCC=NCC+1，更新数据路由。

根据上述流程，分析当前 5G 系统的切换密钥管理机制存在以下问题：①当终端与失陷基站连接时，攻击者可以中断失陷基站的链路计数值 NCC 更新，使失陷基站 {NH,NCC} 无法同步，只能通过 $\mathrm{NH}_{\mathrm{NCC}}$ 进行水平切换[24]，无法达到完美的前向隔离；②小区内切换密钥更新指令由 gNB 发起，gNB 决定目标 UE 后发送切换命令，UE 更新数据链路值 NCC、同步并存储下一跳密钥 NH，这会导致大规模低移动性设备只能被动的等待切换更新；③小区间切换更新过程 gNB 需要和核心网进行四次信令交互，并且在每次同步 {NH,NCC} 要存储对应的 $\mathrm{NH}_{\mathrm{NCC}}$ 值，高移动性机器类设备在密集小区中会频繁切换，导致核心网的资源消耗和严重的信令拥塞。

2.2 相关知识

困难问题 令 P 是阶为 q 的循环群 G 的一个生成元。计算性 Diffie-Hellman（CDH）：已知 $P, aP, bP \in G$，CDH 问题的目标是计算 abP，任意多项时间内解决 CDH 问题的优势 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}}$ 是可忽略的。决策性 Diffie-Hellman（DDH）：已知 $P, aP, bP, cP \in G$，DDH 问题的目标是等式 $abP = cP$ 是否成立。

敌手模型 $\mathcal{A}$ 类敌手不能得到系统的主密钥，但能通过公钥替换攻击机制；$\mathcal{A}$ 类敌手能得到系统的主密钥，但是不能通过公钥替换攻击机制。

eCK 安全模型 本节参考文献[25]所定义的 eCK 安全模型，通过挑战者和敌手 $\mathcal{A}$ 的游戏定义密钥协商协议的安全性。$\pi_{i,j}^{S}$ 代表 i 向 j 发起的第 S 次会话，拥有相同会话 id 的称为匹配会话；当计算出会话密钥 $\mathrm{sk}_{i,j}^{S}$ 时，$\pi_{i,j}^{S}$ 变为 accepted 状态，会话可能会在没有进入 accepted 状态的情况下终止。构造解决 CDH 困难问题的模拟器 τ，$\mathcal{A}$ 可以通过以下随机预言机查询。

Create(i)：参与者 i 生成公私钥对。

RevealMasterKey：τ 返回主密钥。

RevealSessionKey($\pi_{i,j}^{S}$)：若会话 $\pi_{i,j}^{S}$ 没有被接受，τ 返回 $\perp$；否则返回会话密钥 sk。

RevealPartialPrivateKey(i)：τ 返回参与者 i 的部分私钥。

RevealSecretValue(i)：τ 返回参与者 i 的私钥。

RevealEphemeralKey($\prod_{i,j}^{t}$)：τ 返回参与者 i 的临时密钥。

ReplacePublicKey(i)：替换参与者 i 的公钥。

Send($\pi_{i,j}^{S}, m$)：τ 向 $\pi_{i,j}^{S}$ 发送消息 m，根据协议得到响应。

Test($\pi_{i,j}^{S}$)：在游戏某一时刻可以向新鲜会话 $\pi_{i,j}^{S}$（新鲜性定义见后文）进行 Test 询问，随机选择 $b \in \{0,1\}$，若 $b=0$ 返回协商得到的 sk，否则返回会话空间 $\{0,1\}^k$ 上的随机值。

在游戏最后输出 b' 作为对 b 的猜测，若 $b'=b$，称敌手赢得游戏。

新鲜性 令 $\pi_{i,j}^{S}$ 为已接受会话。如果下列条件都不成立，则称 $\pi_{i,j}^{S}$ 是新鲜的。

1) 询问了 $\pi_{i,j}^{S}$ 或匹配会话（如果存在的话）的会话密钥。

2) 匹配会话 $\pi_{j,i}^{T}$ 存在时，$\mathcal{A}$ 询问了 i 的部分私钥和 $\pi_{i,j}^{S}$ 的临时私钥，或询问了 j 的部分私钥和 $\pi_{j,i}^{T}$ 的临时私钥。

3) 匹配会话 $\pi_{j,i}^{T}$ 不存在，$\mathcal{A}$ 询问了 i 的部分私钥和 $\pi_{i,j}^{S}$ 的临时私钥，或询问了 j 的部分私钥。

安全性 如果下列条件被满足，则称密钥协商协议是安全的。

1) 参与者协商了相同的会话密钥，并且该会话密钥在密钥空间上满足均匀分布。

2) 在任意的多项式时间 t 内敌手 $\mathcal{A}$（$\mathcal{A}_1, \mathcal{A}_2$）在上述游戏中获胜的优势 $\mathrm{Adv}_{\mathcal{A}}(k)$ 是可忽略的。

3 基于无证书的切换认证与密钥更新机制

3.1 设计目标

针对上述问题，本文设计一种基于无证书的切换认证与密钥更新机制，如图 5 所示。①终端可以在小区内切换状态内主动发起更新，保障 5G 网络新场景下用户的隐私与安全。②新密钥的生成不依赖核心网的控制，终端和接入点在 5G-RAN 侧完成无证书密钥协商全过程，减少核心网资源消耗和信息传输距离。③更新过程保证较小的流量负担和信令交互，降低基站的传输负载。

3.2 切换认证与密钥更新机制

系统初始化阶段 通过无证书密钥协商机制，

终端和基站只在完成初次认证时与 MEC 服务器建立连接，MEC 服务器将 KGC 根据身份标识生成的部分私钥通过安全信道分别发送给 UE 和 gNB，完成系统初始化。

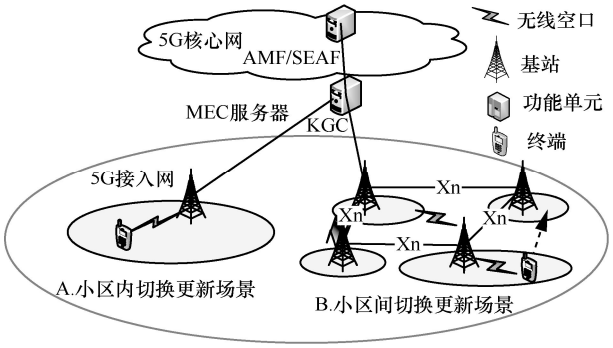


图 5　基于无证书的切换密钥更新场景

步骤 1　KGC 根据主密钥 $s \in Z_q^*$，计算 $P_{\mathrm{KGC}} = sP$，得到公开参数 $\mathrm{params} = \{q, F_p, E/F_p, G, P, P_{\mathrm{KGC}}, H_1, H_2\}$，其中 q 是满足 $q > 2^k$（k 是安全参数）的大素数，F_q 是有限域，E/F_q 是有限域上的椭圆曲线，群 G 是 E/F_q 上的 q 阶加法循环群，P 是群 G 的一个生成元，$H_1: \{0,1\}^* \times G \times G \to Z_q^*$，$H_2: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \to Z_q^*$，$H_3: G \to Z_q^*$ 是单向抗碰撞哈希函数。

步骤 2　UE 随机选择秘密值 $x_{\mathrm{UE}} \in Z_q^*$，计算 UE 的部分公钥 $X_{\mathrm{UE}} = x_{\mathrm{UE}} P$，发送用户隐藏标识符（SUCI, subscription concealed identifier）给 KGC。同理计算出 gNB 的部分公钥 X_{gNB} 并公开，发送物理小区标识 PCI 给 KGC。

步骤 3　KGC 随机选择秘密值 $r_{\mathrm{UE}} \in Z_q^*$，计算 UE 的部分公钥 $Y_{\mathrm{UE}} = r_{\mathrm{UE}} P$，根据 SUCI 生成 UE 部分私钥 $y_{\mathrm{UE}} = r_{\mathrm{UE}} + sH_1(\mathrm{SUCI}, X_{\mathrm{UE}}, Y_{\mathrm{UE}})$，通过安全信道把 y_{UE} 传给 UE；同理计算出 gNB 的部分公钥 $Y_{\mathrm{gNB}} = r_{\mathrm{gNB}} P$ 并公开，根据 PCI 生成 gNB 部分私钥 $y_{\mathrm{gNB}} = r_{\mathrm{gNB}} + sH_1(\mathrm{PCI}, X_{\mathrm{gNB}}, Y_{\mathrm{gNB}})$，通过安全信道把 y_{gNB} 传给 gNB。

步骤 4　UE 判断等式 $y_{\mathrm{UE}} P = Y_{\mathrm{UE}} + P_{\mathrm{KGC}} h_{\mathrm{UE}}$ 来验证部分私钥有效性。若等式成立，表示密钥有效，设置公钥为 $\mathrm{PK}_{\mathrm{UE}} = < X_{\mathrm{UE}}, Y_{\mathrm{UE}} >$，设置私钥为 $\mathrm{SK}_{\mathrm{UE}} = < x_{\mathrm{UE}}, y_{\mathrm{UE}} >$；否则返回步骤 1。同理在 gNB 判断密钥的有效性。

密钥更新阶段　引入了无证书密钥体制和密钥隔离技术方案，具体流程如图 6 所示。

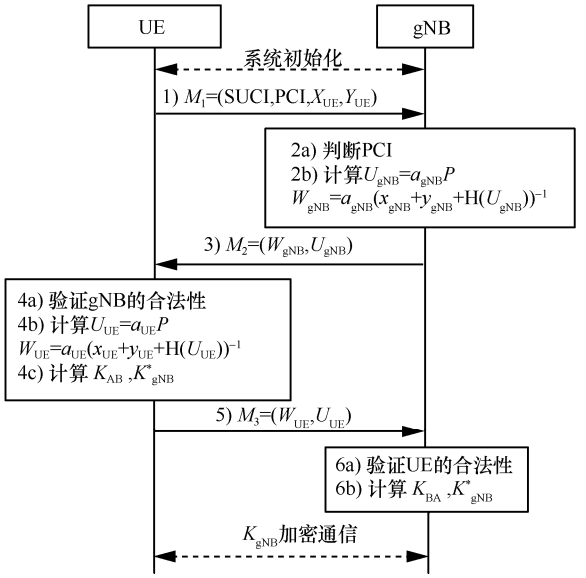


图 6　基于无证书的切换认证与密钥更新流程

步骤 1　UE 发起更新请求给 gNB，包含验证消息 $M_1 = (\mathrm{SUCI}, \mathrm{PCI}, X_{\mathrm{UE}}, Y_{\mathrm{UE}})$，在小区间切换时发送 $\mathrm{PCI} = \mathrm{PCI}_{\mathrm{gNB}_1}$ 与目标基站建立通信，在小区内切换时发送 $\mathrm{PCI} = \mathrm{PCI}_{\mathrm{gNB}_0}$ 与源基站建立通信。

步骤 2　gNB 首先对比接收到的 PCI 与自己的 PCI 是否相等，若相等则随机选择 $a_{\mathrm{gNB}} \in Z_q^*$，依次计算式(6)、式(7)；否则将 M_1 通过安全信道发送给目标 gNB，目标 gNB 执行式(6)和式(7)并与 UE 建立通信。

$$U_{\mathrm{gNB}} = a_{\mathrm{gNB}} P \tag{6}$$

$$W_{\mathrm{gNB}} = a_{\mathrm{gNB}} (x_{\mathrm{gNB}} + y_{\mathrm{gNB}} + H_3(U_{\mathrm{gNB}}))^{-1} \tag{7}$$

步骤 3　gNB 返回验证消息 $M_2 = (W_{\mathrm{gNB}}, U_{\mathrm{gNB}})$ 给 UE。

步骤 4　UE 在收到 M_2 后计算 $P_{\mathrm{UE}}^1 = W_{\mathrm{gNB}}(X_{\mathrm{gNB}} + H_3(U_{\mathrm{gNB}})P + Y_{\mathrm{gNB}} + P_{\mathrm{KGC}} h_{\mathrm{gNB}})$，其中 $h_{\mathrm{gNB}} = H_1(\mathrm{PCI}, X_{\mathrm{gNB}}, Y_{\mathrm{gNB}})$。判断等式 $U_{\mathrm{gNB}} = P_{\mathrm{UE}}^1$ 来验证 gNB 的合法性，如果相等，表示 gNB 通过了 UE 对它的合法性验证；否则终止更新，此步骤防止了伪基站攻击。

UE 随机选择 $a_{\mathrm{UE}} \in Z_q^*$，分别计算

$$U_{\mathrm{UE}} = a_{\mathrm{UE}} P \tag{8}$$

$$W_{\mathrm{UE}} = a_{\mathrm{UE}} (x_{\mathrm{UE}} + y_{\mathrm{UE}} + H_3(U_{\mathrm{UE}}))^{-1} \tag{9}$$

然后 UE 依次计算

$$K_{\mathrm{AB}}^{1}=(a_{\mathrm{UE}}+y_{\mathrm{UE}})(U_{\mathrm{gNB}}+Y_{\mathrm{gNB}}+P_{\mathrm{KGC}}+h_{\mathrm{gNB}}) \quad (10)$$

$$K_{\mathrm{AB}}=H_2\left(\mathrm{SUCI}\|\mathrm{PCI}\|U_{\mathrm{UE}}\|U_{\mathrm{gNB}}\|K_{\mathrm{AB}}^{1}\right) \quad (11)$$

将协商出的密钥 K_{AB} 和原密钥 K_{gNB} 作为输入，使用 HMAC-SHA-256 算法推演出下一个 AS 层密钥 K_{gNB}^{*}，如图 7 所示，在小区间切换时根据目标 $\mathrm{PCI}_{\mathrm{gNB}_1}$ 进行垂直推演，在小区内切换时根据源 $\mathrm{PCI}_{\mathrm{gNB}_0}$ 进行水平推演。由当前时段协商出的密钥与前一时段的临时密钥，共同生成下一时段的临时密钥，达到前向隔离。

$$K_{\mathrm{gNB}}^{*}=\mathrm{KDF}\left(K_{\mathrm{gNB}},K_{\mathrm{AB}},\mathrm{SUCI},\mathrm{PCI},\mathrm{EARFCN\text{-}DL}\right)=$$
$$\text{HMAC-SHA-256}\left(K_{\mathrm{gNB}},S\right)=$$
$$\mathrm{Hash}\left(K_{\mathrm{gNB}}\oplus\mathrm{opad},\mathrm{Hash}\left(K_{\mathrm{gNB}}\oplus\mathrm{ipad},S\right)\right) \quad (12)$$

其中，ipad 为 64 个 0x36，opad 为 64 个 0x5c，String $S=\mathrm{FC}\|K_{\mathrm{AB}}\|\mathrm{SUCI}\|\mathrm{PCI}\|\mathrm{EARFCN}\|L_n$，FC 用于区分不同的算法，$L_n$ 是相应输入参数的长度。

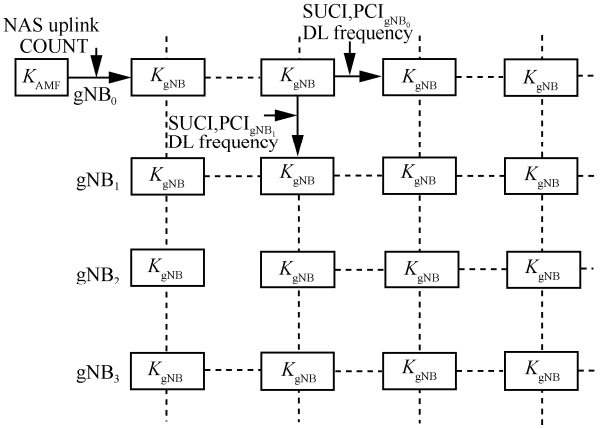


图 7 新型密钥更新机制的密钥推演流程

步骤 5 UE 返回验证消息 $M_3=(W_{\mathrm{UE}},U_{\mathrm{UE}})$ 给 gNB。

步骤 6 gNB 计算 $P_{\mathrm{gNB}}^{1}=W_{\mathrm{UE}}(X_{\mathrm{UE}}+H_3(U_{\mathrm{UE}})P+Y_{\mathrm{UE}}+P_{\mathrm{KGC}}h_{\mathrm{UE}})$，其中 $h_{\mathrm{UE}}=H_1\left(\mathrm{SUCI},X_{\mathrm{UE}},Y_{\mathrm{UE}}\right)$，判断等式 $U_{\mathrm{UE}}=P_{\mathrm{gNB}}^{1}$ 来验证 UE 的合法性，如果相等，表示 UE 通过了 gNB 对它的合法性验证；否则终止更新，此步骤防止了恶意用户攻击。

最后 gNB 依次计算

$$K_{\mathrm{BA}}^{1}=(a_{\mathrm{gNB}}+y_{\mathrm{gNB}})(U_{\mathrm{UE}}+Y_{\mathrm{UE}}+P_{\mathrm{KGC}}h_{\mathrm{UE}}) \quad (13)$$

$$K_{\mathrm{BA}}=H_2(\mathrm{SUCI}\|\mathrm{PCI}\|U_{\mathrm{UE}}\|U_{\mathrm{gNB}}\|K_{\mathrm{BA}}^{1}) \quad (14)$$

将协商出的密钥 K_{BA} 和原密钥 K_{gNB} 作为输入，用 HMAC-SHA-256 算法推演出下一个 AS 层密钥 K_{gNB}^{*}。其中，String $S=\mathrm{FC}\|K_{\mathrm{BA}}\|\mathrm{SUCI}\|\mathrm{PCI}\|\mathrm{EARFCN}\|L_n$。

$$K_{\mathrm{gNB}}^{*}=\mathrm{KDF}\left(K_{\mathrm{gNB}},K_{\mathrm{BA}},\mathrm{SUCI},\mathrm{PCI},\mathrm{EARFCN\text{-}DL}\right)=$$
$$\text{HMAC-SHA-256}\left(K_{\mathrm{gNB}},S\right)=$$
$$\mathrm{Hash}\left(K_{\mathrm{gNB}}\oplus\mathrm{opad},\mathrm{Hash}\left(K_{\mathrm{gNB}}\oplus\mathrm{ipad},S\right)\right) \quad (15)$$

4 讨论

4.1 正确性分析

密钥有效性。已知 $h_{\mathrm{UE}}=H_1(\mathrm{SUCI},X_{\mathrm{UE}},Y_{\mathrm{UE}})$、$y_{\mathrm{UE}}=r_{\mathrm{UE}}+sh_{\mathrm{UE}}$，通过验证式(16)判断部分私钥的有效性。

$$y_{\mathrm{UE}}P=\left(r_{\mathrm{UE}}+sh_{\mathrm{UE}}\right)P=$$
$$Y_{\mathrm{UE}}+P_{\mathrm{KGC}}H_1\left(\mathrm{SUCI},X_{\mathrm{UE}},Y_{\mathrm{UE}}\right) \quad (16)$$

身份合法性。以 UE 验证 gNB 的身份合法性为例进行分析，同理 gNB 可验证 UE 的身份合法性。

$$P_{\mathrm{UE}}^{1}=W_{\mathrm{gNB}}\left(X_{\mathrm{gNB}}+Y_{\mathrm{gNB}}+H_3(U_{\mathrm{gNB}})P+P_{\mathrm{KGC}}h_{\mathrm{gNB}}\right)=$$
$$a_{\mathrm{gNB}}\left(x_{\mathrm{gNB}}+y_{\mathrm{gNB}}\right)^{-1}\cdot$$
$$\left(x_{\mathrm{gNB}}P+H_3(U_{\mathrm{gNB}})P+r_{\mathrm{gNB}}P+sPh_{\mathrm{gNB}}\right)=$$
$$a_{\mathrm{gNB}}P=U_{\mathrm{gNB}} \quad (17)$$

密钥一致性。以 K_{AB}^{1} 为例进行分析，则 UE 和 gNB 两端更新后的 AS 层密钥 K_{gNB}^{*} 相等。

$$K_{\mathrm{AB}}^{1}=(a_{\mathrm{UE}}+y_{\mathrm{UE}})\left(U_{\mathrm{gNB}}+Y_{\mathrm{gNB}}+P_{\mathrm{KGC}}h_{\mathrm{gNB}}\right)=$$
$$(a_{\mathrm{UE}}+y_{\mathrm{UE}})(a_{\mathrm{gNB}}+y_{\mathrm{gNB}})P=$$
$$\left(a_{\mathrm{gNB}}+y_{\mathrm{gNB}}\right)\left(U_{\mathrm{UE}}+Y_{\mathrm{UE}}+P_{\mathrm{KGC}}h_{\mathrm{UE}}\right)=K_{\mathrm{BA}}^{1} \quad (18)$$

4.2 安全性分析

本节参考第 2 节所定义的 eCK 安全模型和随机预言模型，证明所提机制在 eCK 模型下的安全性；再根据文献[26]定义的安全属性对本文所提机制进行安全性评价。

1) 安全性证明

本节将证明所提协议满足上述安全属性，主要考虑 $\mathcal{A}_1$ 类敌手的攻击，$\mathcal{A}$ 类敌手证明同理。

声明 1 i、j 协商了相同的会话密钥 sk，sk 在密钥空间上满足均匀分布。

证明 1　由 4.1 节正确性分析可知 i、j 协商了相同的会话密钥，且参数的随机性确保了会话密钥在密钥空间上满足均匀分布。

声明 2　敌手 $\mathcal{A}_1$ 在多项式时间 t 内获胜的优势 $\mathrm{Adv}_{\mathcal{A}_1}(k)$ 可忽略。

证明 2　敌手 $\mathcal{A}_1$ 可以通过以下 3 种攻击情形区分真实会话密钥和随机值。

猜测攻击：猜测会话密钥。

密钥复制攻击：$\mathcal{A}_1$ 迫使 Test 会话的一个非匹配会话拥有与 Test 相同的会话密钥。

伪造攻击：敌手 $\mathcal{A}_1$ 在某时刻成功计算出 K 并通过随机预言机查询到 SK 。

由文献[27]可知，前 2 种攻击成功概率可以忽略不计，主要考虑伪造攻击。

按照新鲜性定义，考虑如下 2 种子情形：存在诚实实体拥有 Test 会话的匹配会话；无诚实的参与者拥有 Test 会话的匹配会话。

情形 1　存在诚实实体拥有 Test 会话的匹配会话，此情形又可以被分为以下 4 种子情形：既不能查询 I 的临时私钥，也不能查询 J 的部分私钥；既不能查询 J 的临时私钥，也不能查询 I 的部分私钥；既不能查询 I 的部分私钥，也不能查询 J 的部分私钥；既不能查询 I 的临时私钥，也不能查询 J 的临时私钥。

情形 1.1　既不能查询 I 的临时私钥，也不能查询 J 的部分私钥。

构造解决 CDH 困难问题的模拟器 τ，其输入是 $P\in G, M=mP, N=nP$，目标是计算 mnP。τ 首先选择 $P_o\in G$ 作为 P_{KGC}，发送系统参数 $\mathrm{params}=\{q,\ F_p, E/F_p, G, P, P_{\mathrm{KGC}}, H_1, H_2\}$ 给 $\mathcal{A}_1$。τ 随机选择 $S\in\{1,2,\cdots,n_0\}$ 和 2 个参与者 $I,J\in\{1,2,\cdots,n_1\}$，n_0、n_1、n_2 分别为最多的密钥协商次数、最大诚实实体数、H_2 询问次数。

询问阶段　初始值为空的列表 L_C、L_{H_1}、L_{H_2}、L_S 分别用于跟踪 Create、H_1、H_2、Send 询问。

Create(i)：若 $i=J$，τ 选取随机值 $h_i, x_i\in Z_q^*$，计算 $Y_i=M-h_iP_0$，$X_i=x_iP$，设置 $H_1(\mathrm{ID}_i, X_i, Y_i)\leftarrow h_1$，将 $(\mathrm{ID}_i, \perp, Y_i, x_i, X_i)$ 和 $(\mathrm{ID}_i, X_i, Y_i)$ 分别存入 L_C 和 L_{H_1} 中；否则，τ 选取随机值 $h_i, x_i, y_i\in Z_q^*$，计算 $Y_i=y_iP-h_iP_{\mathrm{KGC}}$，$X_i=x_iP$，设置 $H_1(\mathrm{ID}_i, X_i, Y_i)\leftarrow h_1$，将 $(\mathrm{ID}_i, y_i, Y_i, x_i, X_i)$ 和 $(\mathrm{ID}_i, X_i, Y_i)$ 分别存入 L_C 和 L_{H_1} 中。

$H_1(\mathrm{ID}_i, X_i, Y_i)$：若 $(\mathrm{ID}_i, X_i, Y_i)\in L_{H_1}$，返回 h_i；否则，τ 选取随机数 $h_i\in Z_q^*$，将 $(\mathrm{ID}_i, X_i, Y_i)$ 存入 L_{H_1}，并返回 h_i。

$H_2(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$：令 $Z_1=K_{\mathrm{AB}}^1$，$\mathrm{sk}=K_{\mathrm{AB}}$，若 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})\in L_{H_2}$，返回 sk；否则 τ 判断以下是否成立。

①若 $i=J$，τ 在 L_s 查询 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, *)$。若 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, *)\in L_s$，$\tau$ 计算 $\overline{Z_1}=Z_1-s_I(U_J+M)$，当输入元组 $(Y_i+H_1(\mathrm{ID}_i, X_i, Y_i), U_j, \overline{Z_1})$ 时，通过检查预言机 DDH(*,*,*) 的输出来判断 Z_1 是否正确。若正确，将 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$ 存入 L_{H_2} 中，其中 sk 来自 L_s；若 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, *)\notin L_s$，$\tau$ 选择随机值 $\mathrm{sk}\in\{0,1\}^k$，将 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$ 存入 L_{H_2} 中。

②否则，进行 Send 询问。若 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, *)\in L_s$，将 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$ 存入 L_{H_2} 中，其中 sk 来自 L_s；否则，τ 选择随机值 $\mathrm{sk}\in\{0,1\}^k$，将 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$ 存入 L_{H_2} 中。

RevealPartialPrivateKey(i)：若 $\mathrm{ID}_i=\mathrm{ID}_J$，终止模拟；否则返回私钥 y_i。

RevealSecretValue(i)：若 $(\mathrm{ID}_i, *, *, *, *)\in L_c$，返回 x_i；否则执行 Create(i) 再返回 x_i。

ReplacePublicKey(i)：若 $(\mathrm{ID}_i, *, *, *, *)\in L_c$，用 x_i' 和 $X_i'=x_i'P$ 代替 x_i 和 X_i；否则执行 Create(i) 再进行上述替代。

RevealEphemeralKey($\prod_{i,j}^t$)：若 $\prod_{i,j}^t=\prod_{I,J}^T$，终止模拟；否则，返回 i 的临时私钥。

RevealMasterKey：τ 终止模拟。

RevealSessionKey($\pi_{i,j}^t$)：若 $\prod_{i,j}^t=\prod_{I,J}^T$ 或 $\prod_{i,j}^t=\prod_{J,I}^L$，终止模拟；否则返回 sk。

Send($\pi_{i,j}^t, m$)：τ 判断以下是否成立。

①若 $\prod_{i,j}^t=\prod_{I,J}^S$，返回 $U_i=N$。

②若 $\mathrm{ID}_i=\mathrm{ID}_J$，$\tau$ 选取随机值 $a_i\in Z_q^*$，计算 $\overline{Z_1}=Z_1-a_i(U_j+Y_j+h_jP_{\mathrm{KGC}})-y_j(Y_j+h_jP_{\mathrm{KGC}})$，当输入元组 $(Y_i+H_1(\mathrm{ID}_i, X_i, Y_i), U_j, \overline{Z_1})$ 时，通过检查预言机 DDH(*,*,*) 来判断 Z_1 是否正确。若正确，将 $(\mathrm{ID}_i, \mathrm{ID}_j, U_i, U_j, Z_1, \mathrm{sk})$ 存入 L_{H_2} 中，其中 sk 来自 L_s；否则，τ 选择随机值 $\mathrm{sk}\in\{0,1\}^k$，将

$(\mathrm{ID}_i,\mathrm{ID}_j,U_i,U_j,Z_1,\mathrm{sk})$ 存入 L_{H_2} 中。

③否则，根据协议规范回应。

$\mathrm{Test}(\pi_{i,j}^S)$：若 $\prod_{i,j}^t \neq \prod_{I,J}^S$，终止模拟；否则随机选取会话空间 $\{0,1\}^k$ 上的随机值，并返回给 $\mathcal{A}_\mathrm{I}$。

伪造阶段 当 $\mathcal{A}_\mathrm{I}$ 发起伪造攻击，假设它以不可忽略的概率成功攻击了 Test 会话，那么它一定向 H_2 查询了形如 $Z_1=(a_I+y_I)(U_J+Y_J+H_1(\mathrm{ID}_J,X_J,Y_J)P_{\mathrm{KGC}})=(a_I+y_I)(U_J+M)$ 的值。为了求解 CDH (M,N) 问题，τ 以 $1/n_o n_1^2$ 的概率随机选择一个会话 $\prod_{I,J}^S$；对于 L_{H_2} 中的所有条目，τ 以 $1/n_2$ 的概率随机选择一个条目，然后进行以下步骤。

计算 $\overline{Z_1}=Z_1-s_I(U_J+M)$，又由于 $\overline{Z_1}=\mathrm{CDH}(U_I,U_J)+\mathrm{CDH}(M,N)$，因此 $\mathrm{CDH}(M,N)=\overline{Z_1}-\mathrm{CDH}(U_I,U_J)=\overline{Z_1}-a_I U_J$。

解决 CDH 问题的优势为

$$\mathrm{Adv}_\tau^{\mathrm{CDH}}(k)\geqslant\frac{1}{n_0 n_1^2 n_2}\mathrm{Adv}_{\mathcal{A}_\mathrm{I}}(k) \tag{19}$$

假设 $\mathrm{Adv}_{\mathcal{A}_\mathrm{I}}(k)$ 是不可忽略的，那么 $\mathrm{Adv}_\tau^{\mathrm{CDH}}(k)$ 也不可忽略，这与 CDH 是困难问题相矛盾。因此，敌手 $\mathcal{A}_\mathrm{I}$ 在多项式时间内攻破协议的优势 $\mathrm{Adv}_{\mathcal{A}_\mathrm{I}}(k)$ 可忽略。

情形 1.2 既不能查询 J 的临时私钥，也不能查询 I 的部分私钥。

交换 I 和 J，与情形 1.1 类似，不再赘述。

情形 1.3 既不能查询 I 的部分私钥，也不能查询 J 的部分私钥。

除下述询问，其余均与情形 1.1 相同。

$\mathrm{Create}(i)$：若 $i=I$，τ 选取随机值 $h_i,x_i\in Z_q^*$，计算 $Y_i=M-h_iP_0$，$X_i=x_iP$；若 $i=J$，τ 选取随机值 $h_i,x_i\in Z_q^*$，计算 $Y_i=N-h_iP_{\mathrm{KGC}}$，$X_i=x_iP$，上述 2 种情况都设置 $H_1(\mathrm{ID}_i,X_i,Y_i)\leftarrow h_\mathrm{I}$，并将 $(\mathrm{ID}_i,\perp,Y_i,x_i,X_i)$ 和 (ID_i,X_i,Y_i) 分别存入 L_C 和 L_{H_I} 中；否则，τ 选取随机值 $h_i,x_i,y_i\in Z_q^*$，计算 $Y_i=y_iP-h_iP_{\mathrm{KGC}}$，$X_i=x_iP$，设置 $H_1(\mathrm{ID}_i,X_i,Y_i)\leftarrow h_\mathrm{I}$，将 $(\mathrm{ID}_i,y_i,Y_i,x_i,X_i)$ 和 (ID_i,X_i,Y_i) 分别存入 L_C 和 L_{H_I} 中。

$H_2(\mathrm{ID}_i,\mathrm{ID}_j,U_i,U_j,Z_1,\mathrm{sk})$：若 $(\mathrm{ID}_i,\mathrm{ID}_j,U_i,U_j,Z_1,\mathrm{sk})\in L_{H_2}$，返回 sk；否则判断①若 $i=I$ 或 $i=J$，按情形 1.1 中 H_2 询问方式模拟，其中 $\overline{Z_1}=Z_1-a_i\cdot(U_j+Y_j+h_jP_{\mathrm{KGC}})-y_j(Y_j+h_jP_{\mathrm{KGC}})$；②否则，按 H_2 询问方式②模拟。

$\mathrm{RevealPartialPrivateKey}(i)$：若 $i=I$ 或 $i=J$，终止模拟；否则返回私钥 y_i。

$\mathrm{Send}(\pi_{i,j}^t,m)$：$\tau$ 判断①若 $i=I$ 或 $i=J$，按情形 1.1 中 Send 询问方式②模拟；②否则，根据协议规范回应。

当 $\mathcal{A}_\mathrm{I}$ 发起伪造攻击，假设它以不可忽略的概率成功攻击了 Test 会话，那么它一定向 H_2 查询了形如 $Z_1=(a_I+y_I)(U_J+Y_J+H_1(\mathrm{ID}_J,X_J,Y_J)P_{\mathrm{KGC}})=(a_I+y_I)(U_J+N)$ 的值。可计算 $\mathrm{CDH}(M,N)=Z_1-a_I(U_J+N)-a_JM$，解决 CDH 问题的优势同上述分析。

情形 1.4 既不能查询 I 的临时私钥，也不能查询 J 的临时私钥。

除下述询问，其余均与情形 1.1 相同。

$\mathrm{Create}(i)$：τ 选取随机值 $h_i,x_i,y_i\in Z_q^*$，计算 $Y_i=y_iP-h_iP_{\mathrm{KGC}}$，$X_i=x_iP$，设置 $H_1(\mathrm{ID}_i,X_i,Y_i)\leftarrow h_\mathrm{I}$，将 $(\mathrm{ID}_i,y_i,Y_i,x_i,X_i)$ 和 (ID_i,X_i,Y_i) 分别存入 L_C 和 L_{H_I} 中。

$H_2(\mathrm{ID}_i,\mathrm{ID}_j,U_i,U_j,Z_1,\mathrm{sk})$：若 $(\mathrm{ID}_i,\mathrm{ID}_j,U_i,U_j,Z_1,\mathrm{sk})\in L_{H_2}$，返回 sk；否则 τ 按情形 1.1 中 H_2 询问方式①模拟，其中 $\overline{Z_1}=Z_1-y_i(U_j+Y_j+h_jP_{\mathrm{KGC}})-y_jU_i$。

$\mathrm{RevealPartialPrivateKey}(i)$：查询 L_c 并返回 i 的私钥 y_i。

$\mathrm{RevealEphemeralKey}(\prod_{i,j}^t)$：若 $\prod_{i,j}^t=\prod_{I,J}^T$ 或 $\prod_{i,j}^t=\prod_{J,I}^L$，终止模拟；否则，返回 i 的临时私钥。

$\mathrm{Send}(\pi_{i,j}^t,m)$：$\tau$ 判断①若 $\prod_{i,j}^t=\prod_{I,J}^T$，返回 $U_i=M$；②若 $\prod_{i,j}^t=\prod_{J,I}^L$，返回 $U_i=N$；③否则，根据协议规范回应。

当 $\mathcal{A}_\mathrm{I}$ 发起伪造攻击，假设它以不可忽略的概率成功攻击了 Test 会话，那么它一定向 H_2 查询了形如 $Z_1=(a_I+y_I)(U_J+Y_J+H_1(\mathrm{ID}_J,X_J,Y_J)P_{\mathrm{KGC}})=(a_I+x_I)(U_J+X_J)$ 的值。可计算 $\mathrm{CDH}(M,N)=a_IU_J$，解决 CDH 问题的优势同上述分析。

情形 2 无诚实的参与者拥有 Test 会话的匹配会话，此情形又被分为 2 种子情形。在某时刻，参与者的长期私钥被敌手获得（敌手 $\mathcal{A}_\mathrm{I}$ 不能查询 Test 会话的临时私钥）；在某时刻，参与者的长期

私钥没有泄露（敌手 $\mathcal{A}_1$ 可以查询 Test 会话的临时私钥）。

该情形证明与上述类似，不再赘述。证毕。

综上所述，本文所提机制可以满足在 eCK 模型下的安全属性，可以看作安全的密钥协商机制。

2) 安全性评价

前向安全性。假设攻击者得到某一跳密钥，但是在未知 HMAC-SHA-256 算法另一参数 String$S$=FC||K_{AB}||SUCI||PCI||EARFCN-DL||Ln 的情况下，无法推导下一跳密钥；并且每一次更新过程 UE 和 gNB 分别会选择新的临时秘密值 a_i，在未知 a_i 的情况下，无法有效计算出 K_{AB}^1。

会话密钥的安全性。UE 和 gNB 两方不可以独立地生成下一跳密钥 K_{gNB}，必须要通过密钥协商过程生成临时秘密值来推导下一跳密钥。

抗密钥泄露伪装。假设攻击者已知 gNB 的长期私钥，通过公钥替换来模仿 UE 与 gNB 进行密钥协商，但是在攻击者未知 UE 临时私钥情况下，无法有效计算出 K_{AB}^1，满足抗密钥泄露伪装。

抗未知密钥共享。攻击者企图在通信双方共享密钥过程中截获密钥，但 AS 层密钥 K_{gNB}^* 是在 UE 和 gNB 两端分别生成的，独立存在 UE 和 gNB，满足抗未知密钥共享。

表 1 给出了本文所提机制和现有更新机制的比较分析。本文所提机制在更新过程中实现了前向安全性，保护了通信实体的隐私，解决了密钥泄露伪装问题。

表 1 本文所提机制和现有更新机制的比较分析

机制	前向安全性	会话密钥的安全性	抗密钥泄露伪装	抗未知密钥共享
5G 机制	×	√	×	√
文献[19]	×	√	×	√
文献[20]	√	√	√	√
文献[21]	√	√	√	√
本文所提机制	√	√	√	√

4.3 效率分析

本节参考相关文献[14-16]对本文所提机制进行仿真以评估更新效率。仿真场景参考 3GPP TR 38.801 标准和 3GPP TS 22.261 标准，仿真的实验参数根据文献[16]进行假设：工作频段为 3.4~3.5 GHz，频宽为 100 MHz，基站覆盖半径为 2.4 km，核心网覆盖半径为 100 km。表 2 列出了加密函数的标准运行时间和传输负载大小[19]。

表 2 加密函数的标准运行时间和传输负载大小

参数	含义	大小
L_q /bit	椭圆曲线阶数	160
L_p /bit	基数	1 024
L_{time} /bit	当前和到期时间	32
L_{id} /bit	通信实体标识	32
L_{hash} /bit	Hash 长度	160
L_{NCC} /bit	链路计数值长度	3
L_{NH} /bit	下一跳密钥长度	128
L_{NSCI} /bit	密钥数据路由长度	128
T_{BP} /ms	双线性配对运算	38.376
T_{PM} /ms	点乘运算	1.537
T_{ME} /ms	模幂运算	1.698
T_{RV} /ms	RSA 验证	0.957
T_{hash} /ms	Hash 散列函数	0.035 6
T_{mul} /ms	乘法运算	0.013 2
T_{AO} /ms	算术运算	0.009 4
T_{SM} /ms	同时点乘运算	1.799
T_{EV} /ms	椭圆曲线签名验证	1.875
$T_{\text{UE-gNB}}$ /ms	终端到基站最小传输时延	1
$T_{\text{gNB-Net}}$ /ms	基站到核心网最小传输时延	4
$T_{\text{gNB-gNB}}$ /ms	基站间最小传输时延	0.024

本文比较了进行一次小区间切换更新所需的计算开销和通信开销，在计算传输时延时忽略包长并假设每次通信能达到理论最小传输时延，结果如表 3 所示。与 5G 机制相比，本文所提机制具有较低的传输时延 Tc，更新过程不需要核心网参与；与其他同类切换认证相比，本文所提机制具有最低的传输负载 Lc、传输时延 Tc 和计算耗时 Ts。

随着移动速度的增大，小区间切换密钥更新次数增大，5G 需要执行公钥加密操作来保护身份，这会导致更多的通信成本和计算成本。因此本文分别仿真了不同更新机制中终端移动速率对传输负载、传输时延、计算耗时的影响。

图 8 给出了不同更新机制中终端移动速度与传输负载的关系。仿真表明，5G 机制具有最低的传输负载，这是因为 5G 机制是基于 128 bit 的对称密码学，而本文所提机制是基于 160 bit 的 ECC，与 1 024 bit RSA 有相同安全等级[19]，提供了更高

表 3 本文所提机制和现有更新机制的通信开销与计算开销比较

机制	传输负载 Lc/B	传输时延 Tc/ms	计算耗时 Ts/ms
5G 机制	$3L_{id}+7L_{NCC}+3L_{NH}+2L_{NSCI}+L_{hash}=115$	$3T_{UE\text{-}gNB}+4T_{gNB\text{-}gNB}+4T_{gNB\text{-}Net}=19.096$	$4T_{hash}+5T_{AO}=0.189$
文献[19]	$2L_q+4L_p+4L_{time}+2L_{id}+3L_{hash}=636$	$3T_{UE\text{-}gNB}+T_{gNB\text{-}gNB}+3T_{gNB\text{-}Net}=16.024$	$4T_{ME}+T_{RV}+3T_{hash}+4T_{mul}+2T_{AO}=7.891$
文献[20]	$6L_q+4L_p+4L_{time}+2L_{id}+2L_{hash}=692$	$3T_{UE\text{-}gNB}+T_{gNB\text{-}gNB}\,2T_{gNB\text{-}Net}=11.024$	$T_{PM}+2T_{SM}+T_{EV}+3T_{hash}+T_{mul}+2T_{AO}=8.092$
文献[21]	$6L_q+4L_{time}+2L_{id}+4L_{hash}=912$	$3T_{UE\text{-}gNB}+T_{gNB\text{-}gNB}+2T_{gNB\text{-}Net}=11.024$	$T_{BP}+2T_{PM}+4T_{hash}+2T_{mul}+2T_{AO}=41.638$
本文所提机制	$2L_q+4L_p+2L_{id}=540$	$3T_{UE\text{-}gNB}+T_{gNB\text{-}gNB}=3.024$	$5T_{PM}+3T_{hash}+4T_{AO}+T_{mul}=7.842$

的安全保障。与其他同类切换认证相比，在不同终端移动速度下，本文所提机制都具有较低的传输负载，这是因为本文所提机制采用了无证书密钥协商协议，保证了较小的流量负担和信令交互。

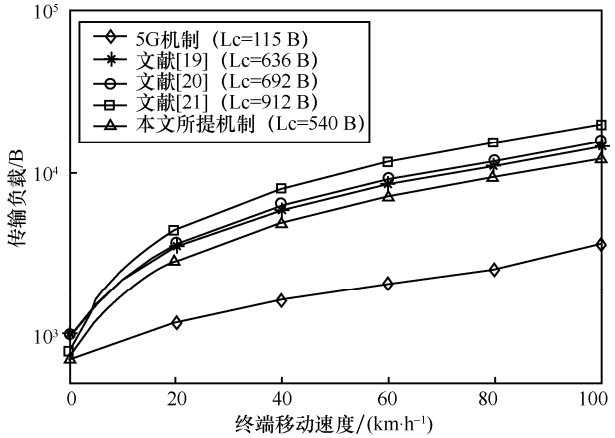


图 8 不同更新机制中终端移动速度与传输负载的关系

图 9 给出了不同更新机制中终端移动速度与传输时延的关系。仿真表明，在不同终端移动速度下本文所提更新机制具有最低的传输时延。这是因为制约通信时延的主要是基站到核心网的远距离传输时延，而本文所提机制中终端和接入点能够在无线 5G-RAN 侧完成 AS 层密钥更新的全流程。

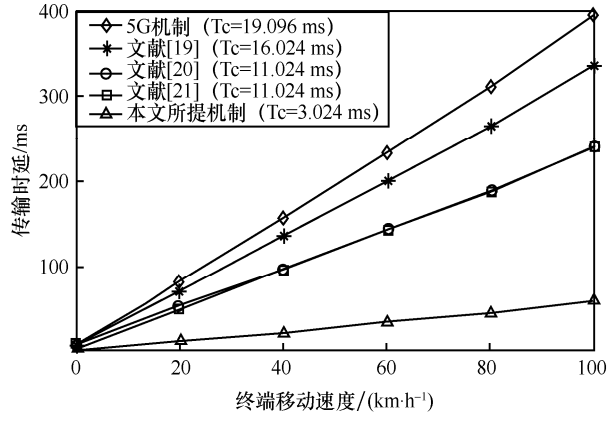


图 9 不同更新机制中终端移动速度与传输时延的关系

图 10 给出了不同更新机制中终端移动速度与计算耗时的关系。仿真表明，5G 机制具有最低的计算耗时，但是随着移动速度的增大，小区间切换密钥更新次数增大，5G 机制需要通过路径转换过程初始化 NCC 或执行公钥操作更新 K_{AMF} 来保护身份，这会导致更多的计算成本，而本文所提机制使用了无双线性映射的无证书密钥协商机制，支持身份隐私保护机制，不存在额外的计算开销。

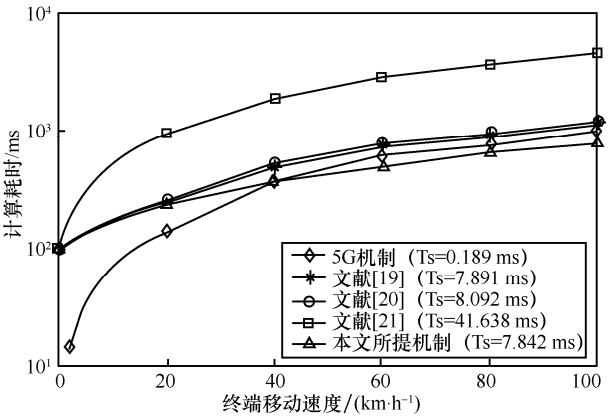


图 10 不同更新机制中终端移动速度与计算耗时的关系

5 结束语

本文在现有 5G 密钥管理的基础上，通过引入无双线性映射的无证书密钥协商机制，使移动终端能够主动发起密钥更新请求，在 MEC 服务器上增加可信第三方密钥生成中心 KGC，并在空口侧完成无证书密钥协商全过程。

针对所提机制，本文在 eCK 安全模型下基于离散对数困难问题，证明了攻击者无法在多项式时间内攻破机制，并从理论上分析了所提机制满足前向/后向安全性、会话密钥不可控性、抗密钥泄露伪装等安全属性。所提机制提高了切换认证的安全性，与其他同类切换认证相比有更低的通信开销和计

算开销。

本文提出的切换认证与密钥更新机制获得了较好的效果，如何满足 5G 业务场景差异化的安全需求，为多元化终端提供安全、轻量化的网络服务，这一问题还有待在身份管理、认证鉴权等方面做进一步研究。

参考文献：

[1] 3GPP. System architecture for the 5G system: TS23.501 V17.0.0[S]. 2021.

[2] 3GPP. Security architecture and procedures for 5G system: TS33.501 V17.0.0[S]. 2020.

[3] KONG Q L, LU R X, MA M D, et al. A privacy-preserving and verifiable querying scheme in vehicular fog data dissemination[J]. IEEE Transactions on Vehicular Technology, 2019, 68(2): 1877-1887.

[4] HUANG S Y, WANG X Y, XU G W, et al. Conditional cube attack on reduced-round keccak sponge function[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2017: 259-288.

[5] HUSSAIN S R, ECHEVERRIA M, CHOWDHURY O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information[C]//Proceedings 2019 Network and Distributed System Security Symposium. Reston: Internet Society, 2019: 24-27.

[6] HAN K H, MA M D, LI X H, et al. An efficient handover authentication mechanism for 5G wireless network[C]//Proceedings of 2019 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2019: 1-8.

[7] GUPTA S, PARNE B L, CHAUDHARI N S. Security vulnerabilities in handover authentication mechanism of 5G network[C]//Proceedings of 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). Piscataway: IEEE Press, 2018: 369-374.

[8] 张文波, 黄文华, 冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021, 42(7): 128-136.
ZHANG W B, HUANG W H, FENG J Y. Secure communication mechanism for VSN based on certificateless signcryptiont[J]. Journal on Communications, 2021, 42(7): 128-136.

[9] ERISSI Y E H, ZAHID N, JEDRA M. An efficient authentication protocol for 5G heterogeneous networks[C]//International Symposium on Ubiquitous Networking. Berlin: Springer, 2017: 496-508.

[10] HARN L. Group authentication[J]. IEEE Transactions on Computers, 2013, 62(9): 1893-1898.

[11] AYDIN Y, KURT G K, OZDEMIR E, et al. A flexible and lightweight group authentication scheme[J]. IEEE Internet of Things Journal, 2020, 7(10): 10277-10287.

[12] BASUDAN S. LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5G networks[J]. Journal of Communications and Information Networks, 2020, 5(4): 457-466.

[13] LI J G, WEN M, ZHANG T. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks[J]. IEEE Internet of Things Journal, 2016, 3(3): 408-417.

[14] CAO J, YAN Z, MA R H, et al. LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks[J]. IEEE Internet of Things Journal, 2020, 7(6): 5329-5344.

[15] SUN Y Q, CAO J, MA M D, et al. EAP-DDBA: efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G HetNet[J]. IEEE Transactions on Dependable and Secure Computing, 2020, PP(99): 1.

[16] LAI C Z, LI H, LI X Q, et al. A novel group access authentication and key agreement protocol for machine-type communication[J]. Transactions on Emerging Telecommunications Technologies, 2015, 26(3): 414-431.

[17] FAN C N, HUANG J J, ZHONG M Z, et al. ReHand: secure region-based fast handover with user anonymity for small cell networks in mobile communications[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 927-942.

[18] 裴旭明, 贾建鑫, 钱骅, 等. 5G 双连接场景下的低传输时延切换机制[J]. 通信学报, 2019, 40(4): 212-222.
PEI X M, JIA J X, QIAN H, et al. Low latency handover scheme for 5G dual-connectivity scenario[J]. Journal on Communications, 2019, 40(4): 212-222.

[19] GUPTA S, PARNE B L, CHAUDHARI N S. An efficient handover AKA protocol for wireless network using Chameleon Hash function[C]//Proceedings of 2018 4th International Conference on Recent Advances in Information Technology (RAIT). Piscataway: IEEE Press, 2018: 1-7.

[20] ZHANG Y H, CHEN X F, LI H, et al. Identity-based construction for secure and efficient handoff authentication schemes in wireless networks[J]. Security and Communication Networks, 2012, 5(10): 1121-1130.

[21] ZHANG Y H, CHEN X F, LI J, et al. Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks[J]. Computer Networks, 2014, 75: 192-211.

[22] KUMAR P, KUMARI S, SHARMA V, et al. A certificateless aggregate signature scheme for healthcare wireless sensor network[J]. Sustainable Computing: Informatics and Systems, 2018, 18: 80-89.

[23] SABELLA D, VAILLANT A, KUURE P, et al. Mobile-edge computing architecture: the role of MEC in the Internet of things[J]. IEEE Consumer Electronics Magazine, 2016, 5(4): 84-91.

[24] 张伟, 田丽萍, 梁玉, 等. 面向车联网多点协作联合传输的安全认证与密钥更新方法[J]. 中国公路学报, 2019, 32(6): 308-318.
ZHANG W, TIAN L P, LIANG Y, et al. Key management scheme to secure coordinated multi-point joint transmission for vehicular networks[J]. China Journal of Highway and Transport, 2019, 32(6): 308-318.

[25] LIPPOLD G, BOYD C, NIETO J G. Strongly secure certificateless key agreement[C]//International Conference on Pairing-Based Cryptography. Berlin: Springer, 2009: 206-230.

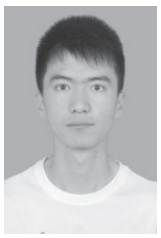
[26] CHENG Z H, NISTAZAKIS M, COMLEY R, et al. On the indistinguishability-based security model of key agreement protocols-simple cases[J]. IACR Cryptology ePrint Archive, 2005, 129: 1-39.

[27] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]//International Conference on Provable Security. Berlin: Springer, 2007: 1-16.

[作者简介]

崔琪楣（1979– ），女，河南驻马店人，博士，北京邮电大学教授、博士生导师，主要研究方向为宽带移动通信网络的新理论及技术、无线大数据基础理论研究等。

赵文静（1998– ），女，贵州安顺人，北京邮电大学硕士生，主要研究方向为无线通信网络安全、形式化分析与研究等。

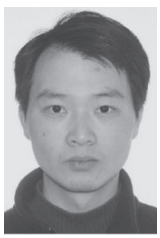


顾晓阳（1996– ），男，宁夏吴忠人，北京邮电大学硕士生，主要研究方向为 5G 网络安全、云虚拟化网络技术等。

朱增宝（1998– ），男，安徽六安人，北京邮电大学博士生，主要研究方向为无线通信网络安全等。

朱晓暄（1983– ），女，湖北荆州人，博士，中国科学技术交流中心副研究员，主要研究方向为无线网络传输、科技创新合作政策等。

陶小峰（1970– ），男，湖北黄冈人，博士，北京邮电大学教授、博士生导师，主要研究方向为 5G 网络技术与移动网络技术等。



倪巍（1977– ），男，上海人，博士，澳大利亚联邦科学与工业研究组织研究员、悉尼科技大学教授，主要研究方向为随机优化、博弈论和图论等。