

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 1 月 31 日 (31.01.2019)



(10) 国际公布号
WO 2019/019736 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01)

(21) 国际申请号: PCT/CN2018/084702

(22) 国际申请日: 2018 年 4 月 26 日 (26.04.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710633559.1 2017 年 7 月 28 日 (28.07.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 吴荣 (WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 甘露 (GAN, Lu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 张博 (ZHANG, Bo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong

518129 (CN)。 谭帅帅 (TAN, Shuaishuai); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

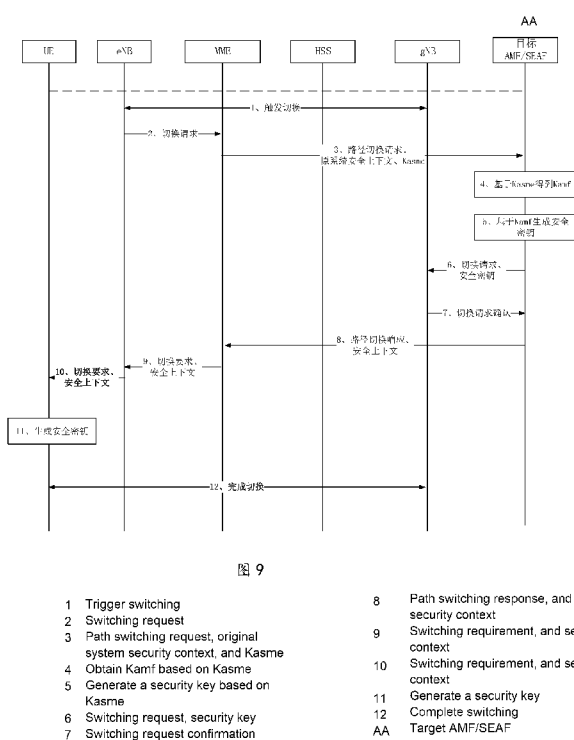
(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

(54) Title: SECURITY IMPLEMENTATION METHOD, AND RELATED APPARATUS AND SYSTEM

(54) 发明名称: 安全实现方法、相关装置以及系统



(57) Abstract: Disclosed are a security implementation method, and a related apparatus and system. The method comprises: a first network element receiving a communication request for switching a user equipment from a source access network device to a target access network device; the first network element obtaining a security key, wherein the security key is used for protecting, after the user equipment is switched from the source access network device to the target access network device, a communication between the user equipment and the target access network device; and the first network element sending the security key to the target access network device.

(57) 摘要: 本申请公开了安全实现方法、相关装置和系统, 该方法包括: 第一网元接收将用户设备从源接入网设备切换到目标接入网设备的通信的请求; 第一网元获得安全密钥; 所述安全密钥用于, 在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后, 对所述用户设备与所述目标接入网设备之间的通信进行保护; 第一网元向所述目标接入网设备发送所述安全密钥。

NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

- 包括国际检索报告(条约第21条(3))。
- 包括经修改的权利要求(条约第19条(1))。

安全实现方法、相关装置以及系统

技术领域

本申请涉及通信技术领域，尤其涉及安全实现方法、相关装置以及系统。

背景技术

现如今，用户设备（如手机）已经被广泛地应用，极大的方便了人们的生活。用户设备可以直接与基站建立通信连接，从而进行通信，利用网络提供的数据传输服务为用户呈现丰富的通信体验。在一些应用场景中，如果用户设备从一个基站小区移动到当前基站小区，需要将用户设备的网络连接从原基站切换到当前基站，才能继续保持通信。

未来移动通信架构（例如第 5 代通信系统 5G）同样要求网络满足用户设备的切换需求。目前，在现有的移动通信 3GPP 标准中，SA2 架构组已经提出了 5G 网络的大致架构，在该架构中，核心网的接入与管理网元 AMF 通常会部署在离基站较近的位置，所以当用户设备跨基站切换通信时，也可能造成跨 AMF 切换。

然而，目前的通信安全实现方法（可扩展的身份验证协议 EAP 方法）并不适用 5G 网络中跨 AMF 切换的安全保护，因此，如何建立基于未来的移动通信架构的安全机制，成为目前亟待解决的问题。

发明内容

本发明实施例提供了安全实现方法、相关装置以及系统，可实现跨 AMF 切换场景中的安全保护，提高未来的移动通信架构的安全性，满足用户需求。

第一方面，本发明实施例公开了一种安全实现方法，该方法包括：第一网元接收将用户设备从源接入网设备切换到目标接入网设备的通信的请求；所述第一网元获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标网络之间的通信进行保护，所述目标网络包括所述目标接入网设备和目标核心网设备，所述目标核心网设备包括所述第一网元；所述第一网元向所述目标接入网设备发送所述安全密钥。

其中，第二网元连接所述源接入网设备，第二网元和源接入网设备属于源侧的网络设备；第一网元连接目标接入网设备，第一网元和目标接入网设备属于目标侧的网络设备。

在具体实现中，所述第二网元可以是源 AMF、源 SEAF、源 SMF 等网络设备，第一网元为对应的目标 AMF、目标 SEAF、目标 SMF 等网络设备。

其中，所述请求可能携带有源侧的安全上下文，所述源侧安全上下文例如可以包括密钥的生存周期、密钥的索引、UE 的安全能力、完整性算法、完整性算法标识、加密算法、加密算法标识、与计算密钥相关的计数值中的一项或多项，所述请求例如可以为切换请求、路径切换请求等等。

在本发明实施例中，所述第一网元获得安全密钥，包括：所述第一网元获取第一中间密钥；所述第一中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；所述第一网元确定安全保护算法，基于所述安全保护算法和所述第一中间密

钥推导出所述安全密钥。

所述安全密钥可包括接入层 AS 密钥和非接入层 NAS 密钥，AS 密钥用于对用户设备与接入网设备之间的通信进行保护，NAS 密钥用于对用户设备与核心网设备（如 AMF/SEAF/SMF 等等）之间的通信进行保护。

其中，第一网元获取第一中间密钥的方式可以是多种多样的：

具体实施例中，第一网元获取第二网元基于第二中间密钥、网络参数推导出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推导下层的接入层和非接入层密钥，例如，第二中间密钥为原先已存在于第二网元的密钥 Kamf，该密钥 Kamf 在通过认证时由第二网元所获取。

具体实施例中，第一网元接收第二网元发送的第二中间密钥；所述第一网元基于所述第二中间密钥、网络参数推导出的所述第一中间密钥。

具体实施例中，在所述用户设备从所述源接入网设备切换到所述目标接入网设备、并且所述用户设备重新通过双向认证后，所述第一网元获得锚密钥 Kseaf；所述第一网元基于所述锚密钥、网络参数推导出的所述第一中间密钥。

其中，网络参数可包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项。

在本发明具体实施例中，第一网元还可以获取第二网元发送的下一跳密钥第一 NH、下一跳密钥关联计数第一 NCC；所述第一网元基于{第一 NH，第一 NCC}对得到{第二 NH，第二 NCC}对。后续步骤中第一网元可向目标接入网设备发送{第二 NH，第二 NCC}对，以及第二密钥、第三密钥，目标接入网设备基于{第二 NH，第二 NCC}对生成第一密钥。

在可能的实施例中，所述安全密钥包括第一密钥，第二密钥和第三密钥；所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥；所述第二密钥为 NAS 信令加密性保护密钥；所述第三密钥为 NAS 信令完整性保护密钥；

所述第一网元确定安全保护算法，基于所述安全保护算法和所述第一中间密钥推导出所述安全密钥，包括：所述安全保护算法包括 NAS 机密性算法标识和 NAS 完整性算法标识，所述第一网元基于第一参数推导出所述第一密钥，例如密钥 KgNB；其中，所述第一参数包括所述第一中间密钥、目标小区标识、频点、NAS 计数值、NAS 连接标识、计数值或随机码或序列码中的一项或多项；所述第一网元基于第二参数推导出所述第二密钥，例如密钥 Knasenc；其中，所述第二参数包括所述第一中间密钥、所述 NAS 机密性算法标识、计数值或随机码或序列码中的一项或多项；所述第一网元基于第三参数推导出所述第三密钥，例如 Knasint；其中，所述第三参数包括所述第一中间密钥、所述 NAS 完整性算法标识、计数值或随机码或序列码中的一项或多项；

所述第一网元向所述目标接入网设备发送所述安全密钥，包括：所述第一网元向所述目标接入网设备发送所述第一密钥。

在可能的实施例中，所述源接入网设备为第一通信系统的接入网设备；所述目标接入网设备为第二通信系统的接入网设备；所述第一网元为所述第二通信系统的网元；所述请求包括所述第一通信系统的安全上下文、第三中间密钥；所述第三中间密钥为在所述第一

通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；

所述第一网元获取第一中间密钥，包括：所述第一网元基于所述第一通信系统的安全上下文、所述第二通信系统的安全上下文以及所述第三中间密钥推衍出的所述第一中间密钥。

在可能的实施例中，所述第一网元包括目标接入和移动管理网元 AMF，所述第二网元包括源 AMF，所述目标 AMF 连接所述目标接入网设备，所述源 AMF 连接所述源接入网设备；或者，所述第一网元包括目标安全锚点 SEAF，所述第二网元包括源安全锚点 SEAF，所述目标 SEAF 连接所述目标接入网设备，所述源 SEAF 连接所述源接入网设备。

在可能的实施例中，所述网络参数包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值或随机码或序列码中的一项或多项。

在可能的实施例中，所述第一网元包括第一通信系统的移动性管理实体网元 MME；所述目标接入网设备为所述第一通信系统的接入网设备；所述源接入网设备为第二通信系统的接入网设备；

具体的，所述 MME 接收将用户设备从所述源接入网设备切换到所述目标接入网设备的通信的请求；所述请求包括所述第二通信系统的安全上下文；所述 MME 获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标接入网设备之间的通信进行保护；所述 MME 向所述目标接入网设备发送所述安全密钥。

在可能的实施例中，所述 MME 获取所述第一通信系统的归属签约用户服务器 HSS 基于第一加密密钥、第一完整性保护密钥、服务网络名称标识、序列号 SQN 推衍出的第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；所述 MME 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密钥。

在可能的实施例中，所述 MME 获取所述第二通信系统的 AMF 发送的第一中间密钥；所述第一中间密钥为所述第二通信系统中认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；所述 MME 基于所述第一中间密钥推衍出所述第三中间密钥；所述 MME 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密钥。

第二方面，本发明实施例提供了一种安全实现方法，其特征在于，包括：

目标接入网设备接收将用户设备从源无线节点切换到目标无线节点的通信的请求；所述目标接入网设备接收核心网设备发送的第一密钥；所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥；所述目标接入网设备基于所述中间密钥生成第二密钥；所述第二密钥为用户设备与所述目标无线节点之间进行安全保护的中间密钥；所述目标接入网设备向目标无线节点发送所述第二密钥，以便于所述目标无线节点基于所述第二密钥生成安全密钥；所述安全密钥用于，在将所述用户设备从源无线节点切换到目标无线节点后，对所述用户设备与所述目标无线节点之间的通信进行保护。

第三方面，本发明实施例提供了一种网元，该网元为第一网元，第一网元包括接收器、发射器、存储器和与存储器耦合的处理器。接收器、发射器、存储器、处理器可通过总线

或者其它方式连接。其中，发射器用于向外部发送数据、信令，接收器用于从外部接收数据、信令。存储器用于存储程序代码以及相关数据（如配置信息、安全上下文、密钥等等），处理器 1201 用于调用并运行存储于存储器中的程序代码，并执行第一方面所述方法的相关步骤。

第四方面，本发明实施例提供了一种目标接入网设备，该目标接入网设备包括接收器、发射器、存储器与与存储器耦合的处理器。接收器、发射器、存储器、处理器可通过总线或者其它方式连接。其中，发射器用于向外部发送数据、信令，接收器用于从外部接收数据、信令。存储器用于存储程序代码以及相关数据（如配置信息、安全上下文、密钥等等），处理器用于调用并运行存储于存储器中的程序代码，并执行第二方面所述方法的相关步骤。

第五方面，本发明实施例提供了一种网元，该网元包括接收模块，密钥处理模块，发送模块，该网元用于实现第一方面描述的方法。

第六方面，本发明实施例提供了一种计算机可读存储介质，用于存储第一方面或第二方面所述方法的实现代码。

第七方面，本发明实施例提供了一种计算机软件产品，当其在计算机中运行时，可用于实现第一方面或第二方面所述的方法。

实施本发明实施例，在跨网元（如跨 AMF 切换）的实施过程中，通信系统可相应生成安全密钥，使用安全网元（SEAF/AMF）来实现目标侧安全上下文和安全密钥的获取和传递。通过实施本发明实施例有利于实现在未来的移动通信架构（如 5G）中跨 AMF 切换的场景中的安全保护，提高未来的移动通信架构的安全性，满足用户需求。

附图说明

下面将对背景技术或者实施例所需要使用的附图作简单地介绍。

图 1 是本发明实施例公开的一种移动通信的系统架构示意图；

图 2 是本发明实施例公开的一种 LTE 系统的场景示意图；

图 3 是本发明实施例公开的一种 5G 系统的场景示意图；

图 4 是本发明实施例公开的一种安全实现方法的流程示意图；

图 5 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 6 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 7 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 8 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 9 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 10 是本发明实施例公开的又一种安全实现方法的流程示意图；

图 11 是本发明实施例公开的一种 5G 结合 WLAN 系统的场景示意图；

图 12 是本发明实施例公开的一种装置的结构示意图；

图 13 是本发明实施例公开的又一种装置的结构示意图。

具体实施方式

下面将结合附图对本发明实施例中的技术方案进行清楚地描述。

为便于方案理解，首先结合相关附图来举例介绍本申请实施例的方案可能应用到的网络架构。图 1 为未来的移动通信的网络架构，该网络架构包括用户设备、接入网设备和运营商网络（如 5G 等 3GPP 网络），运营商网络又包括核心网和数据网，用户设备通过接入网设备接入运营商网络。具体描述如下：

用户设备 (User Equipment, UE), UE 为逻辑实体，具体的，UE 可以是终端设备 (Terminal Equipment)、通信设备 (Communication Device)、物联网 (Internet of Things, IoT) 设备中的任意一种。其中，终端设备可以是智能手机 (smart phone)、智能手表 (smart watch)、智能平板 (smart tablet) 等等。通信设备可以是服务器、网关 (Gateway, GW)、控制器等等。物联网设备可以是传感器，电表以及水表等等。

接入网 (access network, AN)，在具体应用中又可称为无线接入网 (Radio Access Network, RAN)，RAN 由接入网设备组成，负责用户设备的接入。RAN 可以是基站（如 NB、eNB、gNB 等）、无线保真 (Wireless Fidelity, Wi-Fi) 接入点、以及蓝牙接入点等等。

数据网络 (Data network, DN)，DN 可以为运营商外部网络，也可以为运营商控制的网络，用于向用户提供业务服务。UE 可通过接入运营商网络来访问 DN，使用 DN 上的运营商或第三方提供的业务。

核心网 (core network, CN)，CN 作为承载网络提供到 DN 的接口，为 UE 提供通信连接、认证、管理、策略控制以及对数据业务完成承载等。其中，CN 又包括：接入和移动管理网元、会话管理网元，认证服务器网元、策略控制节点、应用功能网元、用户面节点等，相关描述具体如下：

接入与移动管理网元 (Access and Mobility Management Function, AMF)，由运营商提供的控制面网元，负责 UE 接入运营商网络的接入控制和移动性管理。作为 NAS 信令的终结点，处理网络信令；

安全锚点 (Security Anchor Function, SEAF)，SEAF 与 AMF 连接，作为安全认证功能的节点。在具体实施中，在物理位置上可以将 AMF 和 SEAF 集合部署在一起，也可以将 AMF 和 SEAF 分别独立设置。另外，在可能的实施中，可以将 AMF 和 SEAF 的功能分离部署不同的网元，也可以将 AMF 和 SEAF 的功能几种设置于同一个网元（比如 AMF 具备 SEAF 的功能）。

会话管理网元 (Session Management Function, SMF)，由运营商提供的控制面网元，负责管理 UE 的数据包的会话。

认证服务器网元 (Authentication Server Function, AUSF)，认证服务器功能网元 AUSF 是由运营商提供的控制面网元，用于 UE 的认证。AUSF 可以作为一个独立的逻辑功能实体单独部署，也可以集合在 AMF/SMF 等设备中。

统一数据管理网元 (Unified Data Manager, UDM)，由运营商提供的控制面网元，负责存储运营商网络的签约用户持久标识 (Subscriber Permanent Identifier, SUPI)、注册信息、信任状 (credential)、签约数据。这些数据用于 UE 接入运营商网络的认证和授权。

应用功能网元 (Application Function, AF)，用于存储业务安全需求，提供策略判定的信息。

用户面节点 (User Plane Function, UPF)，UPF 可以是网关、服务器、控制器、用户

面功能网元等。UPF 可以设置在运营网内部,也可以设置在运营网外部。UPF 是由运营商提供的用户面网元,是运营商网络与 DN 通信的网关。

策略控制节点(Policy control Function, PCF),所述 PCF 部署有策略控制的功能,所述策略控制的功能是指根据安全需求完成用户面保护机制的协商,确定网络中的用户面保护机制的功能。

需要说明的是,图 1 中体现的是各个网元之间的逻辑关系,在实际中,有些网元可以单独部署,也可以两两或多个网元集成部署在一个实体中。例如,AMF 和 SMF 可部署在一个实体中,或者 AMF 和 SMF 也可分别部署在不同的实体中。

图 2 示出了一种 LTE 通信系统中切换通信的应用场景。该 LTE 通信系统由演进分组核心网(Evolved Packet Core, EPC)、基站(Evolved Node B, eNode B)和用户设备 3 部分组成。其中,EPC 负责核心网部分,EPC 包括用于存储用户签约信息的归属签约用户服务器(Home Subscriber Server, HSS) 141,信令处理和移动管理的移动性管理实体(Mobility Management Entity, MME);基站负责接入网部分,基站与核心网连接,如图示中基站 121 连接 MME131,基站 122 连接 MME132;用户设备与基站之间通过 LTE 空口技术(如 Uu 接口)进行上行通信或下行通信。

在一具体的通信场景中,用户设备与基站 121 通信连接,如果用户设备从 111 处移动至 112 处,那么,用户设备可能就需要将通信连接从基站 121 切换至基站 122,在完成切换进程后,用户设备与基站 122 通信连接,进而才能继续进行通信。可以看出,在这一过程中,由于基站 121 和基站 122 分别连接于不同的 MME,所以,上述通信切换过程同样伴随着 MME 的通信切换。

图 3 示出了一种 5G 通信系统中切换通信的应用场景。该 5G 通信系统包括用户设备、接入网和核心网,可参考图 1 实施例的相关描述。其中,接入网包括 RAN 设备 221、RAN 设备 222,核心网包括核心网设备组 231 和核心网设备组 232,接入网设备与核心网设备连接,如图示中 RAN 设备 221 连接核心网设备 231 中的 AMF, RAN 设备组 222 连接核心网设备组 232 中的 AMF。用户设备与接入网设备之间通过 5G 空口技术进行上行通信或下行通信。

在一具体的通信场景中,用户设备与 RAN 设备 221 通信连接,如果用户设备从 211 处移动至 212 处,那么,用户设备可能就需要将通信连接从 RAN 设备 221 切换至 RAN 设备 222,在完成切换进程后,用户设备与 RAN 设备 222 通信连接,进而才能继续进行通信。可以看出,在这一过程中,由于 RAN 设备 221 和 RAN 设备 222 分别连接于不同核心网设备组的 AMF,所以,上述通信切换过程同样伴随着 AMF 的通信切换。

为了提高未来移动通信架构的网络安全性,实现跨 AMF 切换后网络侧和用户设备侧获得足够的安全保障,本发明实施例提供了一种安全实现方法,参见图 4,该方法包括但不限于以下步骤:

1、源接入网设备触发通信切换。

本发明实施例中,用户设备与源接入网设备通过接入技术建立通信连接。当用户设备需要从当前连接的源 RAN 切换到目标 RAN 时,源接入网设备触发通信切换。其中,接入技

术可以为 CDMA2000、无线局域网 (WLAN)、固定接入 (Fixed access)、全球微波互联接入 (Worldwide Interoperability for Microwave Access, WiMAX)、长期演进 (Long Term Evolution, LTE)、5G 等技术。

具体应用场景中, 当 UE 跨 AMF 切换时, 即从源 AMF 切换至目标 AMF 时, 其源 AMF 下连接管理的源 RAN 也需要切换至目标 RAN。切换的原因可以是多种多样的, 例如, 源 RAN 与目标 RAN 没有 Xn 接口连接, 当 UE 从源 RAN 的通信小区向目标 RAN 的通信小区移动时, 需要将当前通信连接从源 RAN 切换至目标 RAN; 又比如, 在当前网络拥塞导致通信资源不足, 当前连接的源 RAN 需要将 UE 的通信连接请求切换至网络状况较好的目标 RAN; 又比如, 需要将当前通信系统 (如 LTE) 切换到另一个通信系统 (如 5G), 等等。

2、源接入网设备向第二网元发送第一请求; 第二网元向第一网元发送第二请求。

其中, 源接入网设备向第二网元发送的第一请求和第二网元向第一网元发送的第二请求可以是相同的请求, 也可能是不同的请求, 所述第一请求或第二请求可能携带有源侧的安全上下文, 所述源侧安全上下文例如可以包括密钥的生存周期、密钥的索引、UE 的安全能力、完整性算法、完整性算法标识、加密算法、加密算法标识、与计算密钥相关的计数值中的一项或多项, 所述第一请求例如为切换请求, 第二请求例如为路径切换请求。后文实施例中相关的请求可参考这里的描述, 后文将不再赘述。

其中, 第二网元连接所述源接入网设备, 第二网元和源接入网设备属于源侧的网络设备; 第一网元连接目标接入网设备, 第一网元和目标接入网设备属于目标侧的网络设备。

在具体实现中, 所述第二网元可以是源 AMF、源 SEAF、源 SMF 等网络设备, 第一网元为对应的目标 AMF、目标 SEAF、目标 SMF 等网络设备。

3、第一网元获得安全密钥。

其中, 所述安全密钥用于在将所述用户设备从源接入网设备切换到目标接入网设备后, 对用户设备与目标网络之间的通信进行保护, 所述目标网络包括所述目标接入网设备和目标核心网设备, 所述目标核心网设备包括所述第一网元。所述安全密钥可包括接入层 AS 密钥和非接入层 NAS 密钥, AS 密钥用于对用户设备与接入网设备之间的通信进行保护, NAS 密钥用于对用户设备与核心网设备 (如 AMF/SEAF/SMF 等等) 之间的通信进行保护。

第一网元获得安全密钥, 包括: 第一网元生成该安全密钥, 或者, 第一网元获取其他网元发送的安全密钥。

本发明实施例中, 第一网元可首先获取第一中间密钥, 其中, 第一中间密钥为认证后生成的上层的密钥, 用于推衍下层的接入层 AS 和非接入层 NAS 密钥, 例如, 第一中间密钥为新的 K_{amf} ; 然后, 第一网元确定安全保护算法, 包括具体的安全算法以及安全算法的标识, 标识可以用来指示具体的保护算法。然后第一网元基于所述安全保护算法和所述第一中间密钥推导出安全密钥, 所述安全保护算法可包括 NAS 层机密性算法标识和 NAS 层完整性算法标识、AS 层机密性算法标识和 AS 层完整性算法标识。

所述安全密钥包括第一密钥, 第二密钥和第三密钥; 所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥, 例如密钥 K_{gNB} ; 所述第二密钥为 NAS 信令加密性保护密钥, 例如密钥 K_{nasenc} ; 所述第三密钥为 NAS 信令完整性保护密钥, 例如 K_{nasint} 。

具体的，第一网元可基于第一参数推导出所述第一密钥，其中，所述第一参数包括所述第一中间密钥、目标小区标识、频点、NAS 计数值、NAS 连接标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项；基于第二参数推导出所述第二密钥，其中，所述第二参数包括所述第一中间密钥、NAS 机密性算法标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项；基于第三参数推导出所述第三密钥，其中，所述第三参数包括所述第一中间密钥、NAS 完整性算法标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项；第一网元可以保存所述第二密钥、第三密钥，并在后续的步骤中，将第一密钥发送给接入网设备。

其中，第一网元获取第一中间密钥的方式可以是多种多样的：

具体实施例中，第一网元获取第二网元基于第二中间密钥、网络参数推导出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推导下层的接入层和非接入层密钥，例如，第二中间密钥为原先已存在于第二网元的密钥 Kamf，该密钥 Kamf 在通过认证时由第二网元所获取。

具体实施例中，第一网元接收第二网元发送的第二中间密钥；所述第一网元基于所述第二中间密钥、网络参数推导出的所述第一中间密钥。

具体实施例中，在所述用户设备从所述源接入网设备切换到所述目标接入网设备、并且所述用户设备重新通过双向认证后，所述第一网元获得锚密钥 Kseaf；所述第一网元基于所述锚密钥、网络参数推导出的所述第一中间密钥。

其中，网络参数可包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项。

在本发明具体实施例中，第一网元还可以获取第二网元发送的下一跳密钥第一 NH、下一跳密钥关联计数第一 NCC；所述第一网元基于{第一 NH，第一 NCC}对得到{第二 NH，第二 NCC}对。后续步骤中第一网元可向目标接入网设备发送{第二 NH，第二 NCC}对，以及第二密钥、第三密钥，目标接入网设备基于{第二 NH，第二 NCC}对生成第一密钥。

4、第一网元向目标接入网设备发送安全密钥，所发送的安全密钥包括第一密钥。

5、第一网元通过第二网元、接入网设备向用户设备发送安全上下文，以便于用户设备可基于安全上下文生成安全密钥，其中，用户设备所接收到的安全上下文只需包括网络侧生成安全密钥相关的各个密钥时用户设备侧没有的参数，比如随机数 RAND、计数值 Nonce 或者 Counter、时间戳、相关的安全保护算法标识等。

6、用户设备基于安全上下文生成安全密钥。具体实施例中，用户设备可基于安全上下文、网络参数、预存在本地的中间密钥等生成安全密钥，这里的安全密钥包括 AS 密钥和 NAS 密钥。

7、用户设备与目标接入网设备完成后续的切换进程，最终，用户设备的通信连接从当前的源 RAN 切换到目标 RAN。

需要说明的是，本发明实施例以及后文描述的实施例中，源侧和目标侧之间、源侧和 UE 侧之间、目标侧与 UE 侧之间传递的与安全相关的消息（例如安全上下文、中间密钥、密钥请求、密钥响应等等）可能是通过以独立的消息形式进行传递，也可能携带于其他消

息（例如与切换相关的请求、响应等等）中进行传递，本发明在这里不做限定。

参见图 5，本发明实施例提供了又一种安全实现方法，在该方法的应用场景中，UE 在与网络认证后，UE 侧与网络侧（例如 SEAF）可配置有锚密钥 Kseaf。当 UE 需要从当前连接的源 RAN 切换到目标 RAN 时，可通过以下方法实现网络安全，该方法包括但不限于以下步骤：

1、源 RAN 触发通信切换。

本发明实施例中当 UE 跨 AMF 切换时，即从源 AMF 切换至目标 AMF 时，其源 AMF 下连接的源 RAN 也需要切换至目标 RAN。源 RAN 可触发该通信切换，切换的原因可以是多种多样的，例如，源 RAN 与目标 RAN 没有 Xn 接口连接，当 UE 从源 RAN 的通信小区向目标 RAN 的通信小区移动时，需要将当前通信连接从源 RAN 切换至目标 RAN；又比如，在当前网络拥塞导致通信资源不足，当前连接的源 RAN 需要将 UE 的通信连接请求切换至网络状况较好的目标 RAN，等等。

2、源 RAN 向源 AMF 发送切换请求。

源 RAN 发送切换请求（Handover Required）的消息到源 AMF，通知源 AMF 有用户要进行切换，所述切换请求携带 UE 的标识。其中，AMF 指定用来转发数据（消息）的承载。

3、源 AMF 向目标 AMF 发送路径切换请求。

为了实现通信切换，源 AMF 选择一个目标 AMF，并向该目标 AMF 发送路径切换请求（Forward Relocation Request），所述路径切换请求中可以包含源侧的安全上下文。

4、目标 AMF 向目标 RAN 发送切换请求。

目标 AMF 向目标 RAN 发送切换请求（Handover Request）的消息，用以请求目标 RAN 建立无线网络资源，在目标 RAN 创建 UE 的上下文。在 PDU 会话（PDU session）激活后，目标 AMF 还可为 PDU 会话分配了上行通信隧道的标识符和 IP 地址，并向目标 RAN 发送 PDU 会话。

5、目标 RAN 向目标 AMF 返回切换请求的确认消息。

目标 RAN 向目标 AMF 发送切换请求的确认消息，该确认消息中包括已经被目标 RAN 接受的 PDU 会话。目标 RAN 会分配下行通信隧道的标识符和 PDU 会话的 IP 地址，并向目标 AMF 发送 PDU 会话。

6、目标 AMF 向 SEAF 发送密钥请求。

在本发明实施例中，SEAF 作为安全认证和密钥配置的节点，AMF 和 SEAF 可以分离部署，也可以集合部署在一起。在 AMF 和 SEAF 分离部署时，SEAF 的数量可能是一个，也可能是多个，也就是说，在跨 AMF 切换时，源 AMF 与目标 AMF 可连接同一个 SEAF，也可能源 AMF 与目标 AMF 分别连接不同的 SEAF（源 AMF 连接源 SEAF，目标 AMF 连接目标 SEAF），此时跨 AMF 将伴随着跨 SEAF 切换；在 AMF 和 SEAF 集合部署时，AMF 和 SEAF 可以在物理位置上部署在一起，但仍然是两个功能不同的逻辑实体，则跨 AMF 的情况下，也将伴随着跨 SEAF 切换。

本发明实施例中，为了保障跨 AMF 切换后的网络通信安全，目标 AMF 向 SEAF 发送密钥请求，以便于获得用于生成安全密钥的中间密钥。

需要说明的是，步骤6与步骤4、5之间并没有必然的先后顺序，也就是说，具体实现中，步骤6也可以放在步骤3之后，还可以放在步骤4之后，本发明在这里不做限定。

还需要说明的是，本发明实施例并不限定密钥请求为单独的信令消息，在可能的实施方式中，步骤6中的密钥请求可以承载于目标AMF和SEAF之间的其他交互消息中。

7、SEAF 基于 Kseaf 和网络参数生成 Kamf。

其中，密钥 Kseaf 为锚密钥(anchor key)，所述锚密钥为认证后生成的密钥，属于服务网络中的上层密钥，锚密钥可用于推衍服务网络的下层密钥。

需要说明的是，在本发明实施例中，在 UE 与网络进行身份验证过后，SEAF 就具有密钥 Kseaf。该 Kseaf 可能是固定存储于 SEAF 中，也可能临时存储于 SEAF 中，在 Kseaf 生成网络中的下层密钥后就被删除。在后一种情况中，当 SEAF 收到目标 AMF 的密钥请求时，SEAF 可向 AUSF 发送请求，AUSF 基于该请求生成 Kseaf，并将该 Kseaf 发送给 SEAF。

SEAF 基于 Kseaf 和网络参数生成新的中间密钥 Kamf（第一中间密钥），Kamf 可用于推衍下层的接入层 AS 和非接入层 NAS 密钥。

其中，所述网络参数为网络侧的相关参数，该网络参数例如可以是目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、AMF 设置标识、计数值 Nonce 或 Counter 或随机码或序列码中的一项或多项，具体实现中，网络参数还会包括其他参数。下面简单说明上述网络参数。

目标侧标识：可以为目标侧服务网络标识、目标侧具体小区 ID、目标侧基站 ID 等可以唯一标识目标侧信息的标识。

切片标识：用来唯一性地标识网络切片的 ID。

网络接入标识符 (Network Access Identifier, NAI)：NAI 通常用于唯一标识移动节点。

网络切片选择辅助信息(network slice selection assistant information, NSSAI)：NSSAI 可包括切片各种标识、切片相关实体的标识。终端可通过提供 NSSAI 来选择和组建网络切片相关的实例，一条网络切片选择辅助信息可对应一个网络切片。

AMF 区域标识 (AMF Region ID)：用来区分 AMF 在哪个区域的标识。

AMF 设置标识 (AMF Set ID)：在一个 AMF 区域内唯一标识一个 AMF 集的标识。

AMF 指针 (AMF Pointer)：AMF 指针为唯一标识在一个 AMF 集下的 AMF 的标识。

AMF 全局唯一指示符 GUAMI：GUAMI 可以用来最终指示某个 AMF，具体可为：<GUAMI>=<MCC><MNC><AMF 区域标识><AMF 设置标识><AMF 指针>，其中，MCC 表示移动国家码(Mobile Country Code)，MNC 表示移动网络码 (Mobile Network Code)。

其他参数 (Other parameters)：本发明实施例中，其他的网络参数还可以为时间戳、注册类型 (registration type)、AMF ID、SEAF ID、NAS 计数 (NAS Count) 或安全算法标识、安全算法类型名称、序列号 SQN、AK，还可以这些参数或者前述某个关键参数的长度，等等，后文在描述生成相关密钥时所采用的“其他参数”均可以参考这里的描述，后文将不再赘述。

举例来说，在具体实施例中，SEAF 基于 Kseaf 和网络参数推导出中间密钥 Kamf：

$K_{amf} = KDF(K_{seaf}, \text{目标侧 ID}, \text{切片 ID}, \text{NAI}, \text{NSSAI}, \text{AMF 区域标识}, \text{GUAMI}, \text{AMF 指针}, \text{AMF 设置标识}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$, 其中, KDF 为密钥推导函数。

8、SEAF 向目标 AMF 发送 K_{amf} , 相应的, 目标 AMF 获得所述 K_{amf} 。

9、目标 AMF 基于 K_{amf} 生成安全密钥。

其中, 所述安全密钥用于在将 UE 从所述源 RAN 切换到目标 RAN 后, 对所述 UE 与所述目标 RAN 之间的通信进行保护。由于协议栈可以分为接入层 (Access Stratum, AS) 和非接入层 (Non-Access Stratum, NAS)。所以, 这里所生成的安全密钥需要包括 AS 层密钥和 NAS 层密钥。

在具体的实施例中, 目标 AMF 收到中间密钥 K_{amf} 后, 可以根据预设的规则确定密钥保护算法, 例如, 目标 AMF 中预设有算法优先级列表, 算法优先级列表中具有多种算法 ID, 该目标 AMF 查找算法优先级列表, 并根据算法优先级列表选择新的 NAS 算法, 获得 NAS 机密性算法 ID 和 NAS 完整性算法 ID。目标 AMF 也可能会选择新的 AS 算法, 获得 AS 机密性算法 ID 和 AS 完整性算法 ID。

对于 AS 层密钥, 目标 AMF 首先生成中间密钥 K_{gNB} , 所述 K_{gNB} 为在目标 RAN 侧使用的中间密钥, K_{gNB} 用于在目标 RAN 侧生成 AS 层相关的密钥 (如 K_{rrcenc} 、 K_{rrcint} 、 K_{upenc} 、 K_{upint} 等), 后续步骤中需要将 K_{gNB} 发送至目标接入网设备。

本发明实施例中, 目标 AMF 基于 K_{amf} 和第一参数推导出 K_{gNB} , 具体为:

$K_{gNB} = KDF(K_{amf}, \text{目标小区标识}, \text{频点}, \text{NAS 计数值}, \text{NAS 连接标识}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

其中, NAS 计数值 (NAS Count) 为 NAS 传输 NAS 消息的计数值或 NAS 数据包的计数值, 具体可以为上行 NAS 计数值或者下行 NAS 计数值。频点 (EARFCN-DL) 表示网络的下行通信频率。目标小区标识 (Target physical cell id) 用于唯一标识目标小区。

对于 NAS 层密钥, 目标 AMF 需要生成 K_{nasenc} 和 K_{nasint} , 其中, 这里的 K_{nasenc} 为网络侧的 NAS 信令加密保护密钥, 这里的 K_{nasint} 为网络侧的 NAS 信令完整性保护密钥。目标 AMF 保存 NAS 层密钥, 还可能根据需要向其他核心网设备发送 NAS 层密钥。

本发明实施例中, 目标 AMF 基于 K_{amf} 、重新确定的密钥保护算法和第二参数推导出 K_{nasenc} , 具体为:

$K_{nasenc} = KDF(K_{amf}, \text{NAS 机密性算法 ID}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

本发明实施例中, 目标 AMF 基于 K_{amf} 、重新确定的密钥保护算法和第三参数推导出 K_{nasint} , 具体为:

$K_{nasint} = KDF(K_{amf}, \text{NAS 完整性算法 ID}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

10、目标 AMF 向目标 RAN 发送安全密钥、安全上下文。相应的, 目标 RAN 获得安全密钥、安全上下文。其中, 这里的安全密钥包括 K_{gNB} 。

具体实施例中, 目标 AMF 也会将所选择的 NAS 算法 (也可能包括 AS 算法) 通知给目标 RAN, 以便于目标 RAN 确定安全保护算法。

在可能的实施例中，目标 AMF 还可能会向目标 RAN 发送安全上下文。所述安全上下文包含与网络安全相关的信息。具体的，所述安全上下文包括：密钥的生存周期、密钥的索引、UE 的安全能力、完整性算法、完整性算法标识、加密算法、加密算法标识、与计算密钥相关的计数值等，此外，也可能包括具体密钥。其中，所述 UE 安全能力可以为 UE 支持的加密和完整性算法列表，UE 所要求的密钥长度、密钥生存期等。

目标 RAN 获得安全密钥后，基于安全保护算法、中间密钥 KgNB 继续推导出 AS 层的具体密钥，包括密钥 Krrcenc、密钥 Krrcint、密钥 Kupenc、密钥 Kupint 等，其中，密钥 Krrcenc 为空口无线接入侧控制面信令加密密钥；密钥 Krrcint 为空口无线接入侧信令完整性保护密钥；密钥 Kupenc 为空口无线接入侧用户面加密保护密钥；密钥 Kupint 为空口无线接入侧用户面完整性保护密钥。

需要说明的是，如果前述步骤 6 放在步骤 3 之后，那么，在可能的实施例中，步骤 10 中的安全密钥、安全上下文还可以放在步骤 4 中切换请求的消息中去具体实现。

11、目标 RAN 向目标 AMF 发送响应，以通知目标 AMF 成功获得安全密钥。

12、目标 AMF 向源 AMF 发送路径切换响应、安全上下文。

具体的，为了响应步骤 3 中的路径切换请求，目标 AMF 向源 AMF 发送路径切换请求的确认消息，其中，所述路径切换请求的确认消息可以携带安全上下文。

13、源 AMF 向源 RAN 发送切换要求、安全上下文。

具体的，为了响应步骤 2 中的切换请求，源 AMF 向源 RAN 发送切换要求 (HO Command)，以向源 RAN 通知切换准备完成，其中，所述切换请求中可以携带安全上下文。

14、源 RAN 向 UE 发送切换要求、安全上下文。

具体的，源 RAN 向 UE 发送切换要求，向 UE 通知切换准备完成，促发 UE 完成后续的切换操作。其中，所述切换请求中可以携带安全上下文。

15、UE 基于 Kseaf、安全上下文生成安全密钥。

需要说明的是，UE 侧所接收到的安全上下文，只需包括网络侧生成各个密钥时 UE 侧没有的参数，比如随机数，时间戳，安全保护算法标识等，UE 可能在之前步骤中都已具备其他的用于生成密钥的参数。

由于 UE 原先在与网络认证后，就已经配置 Kseaf，此外，UE 还预先共享了网络侧的网络参数，所以，对 UE 来说，UE 同样可基于 Kseaf、网络参数、安全上下文生成新的 NAS 层密钥和 AS 层密钥。例如，UE 可先基于 Kseaf 生成 Kamf，再基于 Kamf、网络参数、安全上下文生成 AS 层密钥 (如 Krrcenc、Krrcint、Kupenc、Kupint 等) 和 NAS 层密钥 (如 Knasenc、Knasint 等)，具体过程类似参考步骤 7、步骤 9、步骤 10 中的相关描述，这里不再赘述。

16、UE 和目标 RAN 完成后续的切换进程。

UE 和目标 RAN 还会继续完成后续的切换进程，例如，UE 跟目标小区成功同步后，发送切换确认消息给目标 RAN。目标 RAN 发送切换通知给目标 AMF，通知目标 AMF 该 UE 已经位于目标小区。目标 AMF 发送切换路径重换完成消息给源 AMF。源 AMF 再回复一个响应给目标 AMF。源 AMF 发送 UE 上下文释放的消息通知源 RAN 释放与 UE 相关的资源。源 RAN 返回释放确认消息给源 AMF，等等。最终，UE 的通信连接从源 RAN 切换到目标 RAN。

需要说明的是，在本发明实施例中，通信系统在进行 AMF 切换时，不同的 AMF 对应的

SMF 可能不同，所以在上述过程中也可能发生 SMF 切换。在这种情况下，也需要考虑 PDU 会话的安全保护。

在具体实现中，在步骤 7 中 SEAF 生成 Kamf 时，在目标侧需要考虑 PDU 会话密钥的更新。则在 SEAF 生成 Kamf 时，即为 SEAF 向 AUSF 发送指示信息，触发 AUSF 生成新的 PDU 会话密钥。具体的，AUSF 预先保存有密钥 Left K，那么，AUSF 可基于 Left K、以及源 AMF 所发送过来的 UE 的相关信息及会话信息（比如会话 ID、切片信息等等），生成新的 PDU 会话密钥 Ksmf，具体为：

$Ksmf = KDF(Left\ K, NAI, NSSAI, \text{切片 ID}, AMF \text{ 相关参数}, SMF \text{ 相关参数}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

然后，AUSF 将 Ksmf 发送至 SEAF 或目标 AMF，SEAF 或目标 AMF 将 Ksmf 转发至目标 SMF 和 UE，目标 SMF/UE 使用 Ksmf 更新 PDU 会话密钥。

可以看出，实施本发明实施例，在跨 AMF 切换的实施过程中，通信系统可相应生成安全密钥，使用安全网元 SEAF/AMF 等来实现目标侧安全上下文和安全密钥的获取和传递。对于网络而言，由于目标侧的安全密钥由目标侧的网元（如 SEAF/目标 AMF）生成，目标 RAN 不能获得源 RAN 使用的安全密钥，无法破解源 RAN 与 UE 之间的通信信息，实现了网络通信的后向安全；源 RAN 不能获得目标 RAN 使用的安全密钥，不能破解目标 RAN 与 UE 之间的通信信息，实现了网络通信的前向安全。

参见图 6，本发明实施例提供了又一种安全实现方法，在该方法的应用场景中，UE 在与网络认证后，UE 侧与网络侧（例如源 AMF/源 SEAF）可配置有第一 Kamf。当 UE 需要从当前连接的源 RAN 切换到目标 RAN 时，可通过以下方法实现网络安全，该方法包括但不限于以下步骤：

- 1、源 RAN 触发通信切换，可参考图 5 步骤 1 的描述。
- 2、源 RAN 向源 AMF/源 SEAF 发送切换请求。

在本发明实施例中，SEAF 作为安全认证和密钥配置的节点，源 AMF 和源 SEAF 可以分离部署，也可以集合部署在一起。在源 AMF 和源 SEAF 分离部署时，源 AMF 连接源 SEAF，此时跨 AMF 将伴随着跨 SEAF 切换；在源 AMF 和源 SEAF 集合部署时，源 AMF 和源 SEAF 可以在物理位置上部署在一起，但仍然是两个功能不同的逻辑实体，则跨 AMF 的情况下，也将伴随着跨 SEAF 切换。

- 3、源 AMF/源 SEAF 基于第一 Kamf 推导出第二 Kamf。

在源 AMF/SEAF 收到来自于源 RAN 发送的切换请求后，源 SEAF/AMF 基于预先存储的第一中间密钥 Kamf（简称第一 Kamf）、网络参数生成第二中间密钥 Kamf（简称第二 Kamf）。该网络参数例如可以是目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 全局唯一指示符 GUAMI、AMF 指针、AMF 集合标识、Nonce 计数值或随机码或序列码中的一项或多项，具体实现中，网络参数还会包括其他参数。

具体实施例中，源 SEAF/AMF 基于预先存储的第一 Kamf、网络参数推导出第二 Kamf，具体为：

$第二\ Kamf = KDF(第一\ Kamf, \text{目标侧 ID}, \text{切片 ID}, NAI, NSSAI, AMF \text{ 区域标识}, GUAMI, AMF$

指针, AMF 设置标识, 计数值 Nonce 或 Counter 或者 随机码 Random 或者序列码 Sequence number, 其他参数)。

需要说明的是, 在源 AMF 和源 SEAF 分离的情况下, 源 AMF/源 SEAF 基于第一 Kamf 推导出第二 Kamf, 可能包含以下情况:

情况一: 源 AMF 基于预设的第一 Kamf 推导出第二 Kamf;

情况二: 源 SEAF 基于预设的第一 Kamf 推导出第二 Kamf, 并将第二 Kamf 发送给源 AMF。

4、源 AMF/源 SEAF 向目标 AMF/目标 SEAF 发送路径切换请求、第二 Kamf。

在本发明实施例中, 目标 AMF 和目标 SEAF 可以分离部署, 也可以集合部署在一起。在目标 AMF 和目标 SEAF 分离部署时, 目标 AMF 连接目标 SEAF, 此时跨 AMF 将伴随着跨 SEAF 切换; 在目标 AMF 和目标 SEAF 集合部署时, 目标 AMF 和目标 SEAF 可以在物理位置上部署在一起, 但仍然是两个功能不同的逻辑实体, 则跨 AMF 的情况下, 也将伴随着跨 SEAF 切换。

在一具体实施例中, 源 AMF/源 SEAF 向目标 AMF/目标 SEAF 发送路径切换请求, 所述路径切换请求中携带有该第二 Kamf。

在另一具体实施例中, 源 AMF/源 SEAF 分别向目标 AMF/目标 SEAF 发送路径切换请求和第二 Kamf。

5、目标 AMF/目标 SEAF 向目标 RAN 发送切换请求。

6、目标 RAN 向目标 AMF/目标 SEAF 反馈切换请求的确认消息。

7、目标 AMF/目标 SEAF 基于第二 Kamf 生成安全密钥。

其中, 所述安全密钥用于在将 UE 从所述源 RAN 切换到目标 RAN 后, 对所述 UE 与所述目标 RAN 之间的通信进行保护。这里所生成的安全密钥包括 AS 层密钥和 NAS 层密钥。

本发明实施例中, 目标 AMF/目标 SEAF 收到中间密钥 Kamf 后, 可以根据预设的规则确定 NAS 机密性算法 ID 和 NAS 完整性算法 ID, 目标 AMF/目标 SEAF 基于第一 Kamf 和第一参数推导出 KgNB, 基于第一 Kamf、密钥保护算法和第二参数推导出 Knasenc, 基于第一 Kamf、密钥保护算法和第三参数推导出 Knasint, 目标 AMF/目标 SEAF 可保存所述 Knasenc 和 Knasint。具体操作可类似参考图 5 实施例步骤 9, 这里不再赘述。

需要说明的是, 步骤 7 与步骤 5、6 之间并没有必然的先后顺序, 也就是说, 具体实现中, 步骤 6 也可以放在步骤 4 之后, 还可以放在步骤 5 之后, 本发明在这里不做限定。

还需要说明的是, 在目标 AMF 和目标 SEAF 分离的情况下, 目标 AMF/目标 SEAF 第二 Kamf 生成安全密钥, 可能包含以下情况:

情况一: 目标 AMF 基于预设的第二 Kamf 推导出安全密钥;

情况二: 目标 SEAF 基于预设的第二 Kamf 推导出安全密钥, 并将安全密钥发送给目标 AMF。

8、目标 AMF/目标 SEAF 向目标 RAN 发送安全密钥、安全上下文。其中, 所发送的安全密钥包括 KgNB。具体操作可类似参考图 5 实施例步骤 10, 这里不再赘述。

9、目标 RAN 向目标 AMF/目标 SEAF 反馈响应, 以通知目标 AMF/目标 SEAF 成功获得安全密钥。

10、目标 AMF/目标 SEAF 向源 AMF/源 SEAF 反馈路径切换响应、安全上下文。

具体的, 为了响应步骤 4 中的路径切换请求, 目标 AMF 向源 AMF 发送路径切换请求的

确认消息，其中，所述路径切换请求的确认消息可以携带安全上下文。

11、源 AMF/源 SEAF 向源 RAN 反馈切换要求、安全上下文。具体的，为了响应步骤 2 中的切换请求，源 AMF 向源 RAN 发送切换要求 (HO Command)，以向源 RAN 通知切换准备完成，其中，所述切换请求中可以携带安全上下文。

12、源 RAN 向 UE 发送切换要求、安全上下文。

具体的，源 RAN 向 UE 发送切换要求，向 UE 通知切换准备完成，促发 UE 完成后续的切换操作。其中，所述切换请求中可以携带安全上下文。

13、UE 基于第一 Kamf、安全上下文生成安全密钥。

需要说明的是，UE 侧所接收到的安全上下文，只需包括网络侧生成各个密钥时 UE 侧没有的参数，比如随机数，时间戳等，安全保护算法标识等，UE 可能在之前步骤中都已具备其他的用于生成密钥的参数。

由于 UE 原先在与网络认证后，就已经配置第一 Kamf，此外，UE 还预先共享了网络侧的网络参数，所以，可以理解的，对 UE 来说，UE 同样可基于第一 Kamf、网络参数、安全上下文生成新的 NAS 层密钥和 AS 层密钥。UE 和目标 RAN 完成后续的切换进程。

需要说明的是，对于上述图 6 实施例，在一种可能的实施方式中，可以取消步骤 3，而在步骤 4 中，源 AMF/源 SEAF 将第一 Kamf 发送给到目标 AMF/目标 SEAF，在步骤 4 之后，目标 AMF/目标 SEAF 基于第一 Kamf 生成第二 Kamf。

还需要说明的是，在本发明实施例中，通信系统在进行 AMF 切换时，不同的 AMF 对应的 SMF 可能不同，所以在上述过程中也可能发生 SMF 切换。在这种情况下，也需要考虑 PDU 会话的安全保护。在具体实现中，在步骤 7 中目标 AMF/目标 SEAF 基于第二 Kamf 生成安全密钥时，在目标侧需要考虑 PDU 会话密钥的更新。例如目标 AMF/目标 SEAF 向 AUSF 发送指示信息，触发 AUSF 生成新的 PDU 会话密钥。具体的，AUSF 预先保存有密钥 Left K，那么，AUSF 可基于 Left K、以及源 AMF/源 SEAF 所发送过来的 UE 的相关信息及会话信息（比如会话 ID、切片信息等等），生成新的 PDU 会话密钥 Ksmf。

可以看出，实施本发明实施例，在跨 AMF 切换的实施过程中，通信系统可相应生成安全密钥，使用安全网元 SEAF/AMF 等来实现目标侧安全上下文和安全密钥的获取和传递。由于下层的密钥推衍来自于源 AMF/源 SEAF 的第一中间密钥 Kamf 的推衍，源 AMF/源 SEAF 侧生成并传递目标侧安全上下文，对于网络而言，目标 RAN 无法破解源 RAN 与 UE 之间的通信信息，实现了网络通信的后向安全。

参见图 7，本发明实施例提供了又一种安全实现方法，当 UE 需要从当前连接的源 RAN 切换到目标 RAN 时，可通过以下方法实现网络安全，该方法包括但不限于以下步骤：

- 1、源 RAN 触发通信切换。
- 2、源 RAN 向源 AMF/源 SEAF 发送切换请求。
- 3、源 AMF/源 SEAF 向目标 AMF/目标 SEAF 发送路径切换请求。
- 4、目标 AMF/目标 SEAF 向目标 RAN 发送切换请求。
- 5、目标 RAN 向目标 AMF/目标 SEAF 反馈切换请求的确认消息。
- 6、目标 AMF/目标 SEAF 确定本地安全策略。

其中, 所述安全策略可预设于本地缓存中, 也可以存储于其他安全网元中 (例如 PCF、UDM、AUSF 等), 所述安全策略指示确定该 UE 切换到目标 RAN 是否需要重新认证, 目标 AMF/目标 SEAF 从本地缓存中查询该安全策略, 或者从其他安全网元中查询该安全策略。

举例来说, 该安全策略可依据下列实施条件确定: 源 AMF/源 SEAF 侧的密钥已经到期或者不再安全, 或者, 需要重新获取 UE 的安全能力而不是通过源 AMF/源 SEAF 侧传递的安全上下文。那么, 在当前状况符合该安全策略所指示的实施条件时, 目标 AMF/目标 SEAF 确定本地安全策略指示了该 UE 切换到目标 RAN 需要重新认证, 故目标 AMF/目标 SEAF 将继续执行后续步骤。

7、目标 AMF/目标 SEAF 向源 AMF/源 SEAF 反馈路径切换响应, 所述路径切换响应不携带安全上下文。

8、源 AMF/源 SEAF 向源 RAN 反馈切换要求, 所述切换要求不携带安全上下文。

9、源 RAN 向 UE 发送切换要求, 所述切换要求不携带安全上下文。

10、UE 和目标 RAN 完成后续的切换进程。

11、UE 与 AUSF 或 UDM 进行双向认证。

在 UE 的通信连接从源 RAN 切换到目标 RAN 后, UE 与认证网元进行双向认证, 以验证 UE 身份合法性, 认证网元可能是 AUSF, 也可能是 UDM。在通过该双向认证后, UE 侧和目标 AMF/目标 SEAF 侧都获得了新的锚密钥 Kseaf。

12、目标 AMF/目标 SEAF 基于新的 Kseaf 生成安全密钥。

可以理解的, 目标 AMF/目标 SEAF 基于新的 Kseaf、预先共享的网络参数、安全上下文生成安全密钥 (用于生成 AS 层密钥的 KgNB 和 NAS 层密钥), 并保存该 NAS 层密钥。详细过程可参考图 5 实施例步骤 7、步骤 9、步骤 10 中的相关描述, 这里不再赘述。

需要说明的是, 这里的安全上下文可以是基于从源 AMF/源 SEAF 侧传递过来的安全上下文并结合目标 AMF/目标 SEAF 侧自身的安全上下文取交集的结果, 比如最终得到安全上下文包括: 加密性算法 ID 和完整性算法 ID、用户设备的安全能力, 等等。

13、目标 AMF/目标 SEAF 向目标 RAN 发送安全密钥, 其中, 所发送的安全密钥包括 KgNB。

14、UE 基于新的 Kseaf 生成安全密钥, 本步骤和步骤 12、步骤 13 并无必然先后顺序。

可以理解的, UE 也可基于新的 Kseaf、预先共享的网络参数、安全上下文生成安全密钥, 详细过程可参考图 5 实施例步骤 7、步骤 9、步骤 10 中的相关描述, 这里不再赘述。

需要说明的是, 图 7 实施例中沒有详细描述的步骤, 均可以类似参考图 5 和图 6 实施例的相关描述。

还需要说明的是, 在本发明实施例中, 通信系统在进行 AMF 切换时, 不同的 AMF 对应的 SMF 可能不同, 所以在上述过程中也可能发生 SMF 切换。在这种情况下, 也需要考虑 PDU 会话的安全保护。具体的, 在通过步骤 11 所描述的双向认证后, AUSF 同样获得新的密钥 Left K, AUSF 可生成新的 PDU 会话密钥 Ksmf 并发送给 SMF, 这里不再赘述。

目标侧重新认证获取新的保护密钥, 满足前后向安全。不需要源侧传递密钥, 或者基于已有密钥生成。

可以看出, 实施本发明实施例, 在跨 AMF 切换结束后, 通信系统可在重新双向认证之后获得新的保护密钥, 不需要源网络侧传递中间密钥, 也不需要基于原有的密钥生成中

间密钥。对于网络而言，目标 RAN 不能获得源 RAN 使用的安全密钥，无法破解源 RAN 与 UE 之间的通信信息，实现了网络通信的后向安全；源 RAN 不能获得目标 RAN 使用的安全密钥，不能破解目标 RAN 与 UE 之间的通信信息，实现了网络通信的前向安全。

参见图 8，本发明实施例提供了又一种安全实现方法，在该方法的应用场景中，UE 在与网络认证后，UE 侧与源 AMF/源 SEAF 可配置有第一密钥 Kamf，源 RAN 侧配置有第一 KgNB。当 UE 需要从当前连接的源 RAN 切换到目标 RAN 时，可通过以下方法实现网络安全，该方法包括但不限于以下步骤：

1、源 RAN 触发通信切换。

2、源 RAN 向源 AMF/源 SEAF 发送切换请求。

3、源 AMF/源 SEAF 基于第一 Kamf 推导出第二 Kamf，详细推导过程可参考图 6 实施例步骤 3 的描述。

4、源 AMF/源 SEAF 向目标 AMF/目标 SEAF 发送路径切换请求、第二 Kamf、第一 NH、第一 NCC。

在本发明实施例中，密钥 KeNB 和 NH 参数、NCC 参数相关联，其中，NH 表示下一跳密钥 (Next hop)，NCC 表示下一跳密钥关联计数 (Next Chain Counter)。KeNB 和 NH 都可以从其他中间密钥 (例如 Kasme) 推导而来。初始建立过程中，KeNB 直接从 Kasme 推导产生，NCC 值为 0。后续 KeNB 需要更新时，可以依据 {NH, NCC} 对进行更新。

在一具体实施例中，源 AMF/源 SEAF 确定 {第一 NH, 第一 NCC} 对，分别将 {第一 NH, 第一 NCC, 第二 Kamf}、路径切换请求发送给目标 AMF/目标 SEAF。

另一具体实施例中，源 AMF/源 SEAF 确定 {第一 NH, 第一 NCC} 对，并将 {第一 NH, 第一 NCC} 对、第二 Kamf 通过路径切换请求发送给目标 AMF/目标 SEAF。

5、目标 AMF/目标 SEAF 基于第二 Kamf、第一 NH、第一 NCC 生成第一安全密钥。

具体实现中，目标 AMF/目标 SEAF 保存收到的 {第一 NH, 第一 NCC} 对，并基于 {第一 NH, 第一 NCC} 对和第二 Kamf 推导出 {第二 NH, 第二 NCC} 对，具体推导过程如下：

第二 NH=KDF(第二 Kamf, 第一 NH)；

第二 NCC=第一 NCC+1；

另外，目标 AMF/目标 SEAF 还将基于第二 Kamf、重新确定的密钥保护算法和第二参数推导出 Knasenc，具体为：

$\text{Knasenc}=\text{KDF}(\text{第二 Kamf}, \text{NAS 机密性算法 ID}, \text{计数值 Nonce 或 Counter 或者随机码 Random 或者序列码 Sequence number}, \text{其他参数})$ 。

目标 AMF/目标 SEAF 还将 Kamf、密钥保护算法和第三参数推导出 Knasint，具体为：

$\text{Knasint}=\text{KDF}(\text{第二 Kamf}, \text{NAS 完整性算法 ID}, \text{计数值 Nonce 或 Counter 或者随机码 Random 或者序列码 Sequence number}, \text{其他参数})$ 。

可以理解的，所述第一安全密钥包括上述 {第二 NH, 第二 NCC} 对、密钥 Knasenc、密钥 Knasint。后续目标 AMF/目标 SEAF 保存密钥 Knasenc、密钥 Knasint，将 {第二 NH, 第二 NCC} 对发送至接入网。

6、目标 AMF/目标 SEAF 向目标 RAN 发送切换请求、第一安全密钥中的 {第二 NH, 第二

NCC} 对, 相应的, 目标 RAN 获得并保存 {第二 NH, 第二 NCC} 对。

7、目标 RAN 向目标 AMF/目标 SEAF 发送切换请求的确认消息, 通知目标 AMF/目标 SEAF 以成功获得该第一安全密钥中的 {第二 NH, 第二 NCC} 对。

8、目标 RAN 基于第一安全密钥生成第二安全密钥。

具体实现中, 目标 RAN 基于 {第二 NH, 第二 NCC} 对、以及目标 RAN 的物理标识等参数生成第二 KgNB, 具体为:

第二 KgNB=KDF(第二 NH, 物理标识, 其他参数)。

可以理解的, 目标 RAN 得到第二 KgNB 后, 可基于安全保护算法、第二 KgNB 继续推导出密钥 Krrcenc、密钥 Krrcint、密钥 Kupenc、密钥 Kupint 等 AS 层的具体密钥。

9、目标 AMF/目标 SEAF 向源 AMF/源 SEAF 反馈路径切换响应、安全上下文。

10、源 AMF/源 SEAF 向源 RAN 反馈切换要求、安全上下文。

11、源 RAN 向 UE 反馈切换要求、安全上下文。

12、UE 基于第一 Kamf 和安全上下文生成安全密钥。

需要说明的是, UE 侧所接收到的安全上下文, 只需包括网络侧生成各个密钥时 UE 侧没有的参数, 比如随机数, 时间戳等, 安全保护算法标识, {第一 NH, 第一 NCC}, 等等, UE 可能在之前步骤中都已具备其他的用于生成密钥的参数。

可以理解的, 由于 UE 原先在与网络认证后, 就已经配置第一 Kamf, UE 还预先共享了网络侧的网络参数, 所以 UE 可以基于第一 Kamf、网络参数、安全上下文生成 NAS 层密钥。另外, UE 还可以基于 {第一 NH, 第一 NCC}、第一 Kamf 得到 {第二 NH, 第二 NCC}, 并基于 {第二 NH, 第二 NCC}、以及目标 RAN 的物理标识等参数生成第二 KgNB, 再基于第二 KgNB 推导出具体的 AS 层密钥。

13、UE 和目标 RAN 完成后续的切换进程。

可以看出, 实施本发明实施例, 在跨 AMF 切换的实施过程中, 目标侧 (目标 RAN、目标 AMF/目标 SEAF 等) 基于源侧 (源 RAN、源 AMF/源 SEAF 等) 的密钥 KgNB、Kamf 生成目标侧的安全密钥, 对于网络而言, 目标 RAN 不能获得源 RAN 使用的安全密钥, 无法破解源 RAN 与 UE 之间的通信信息, 实现了网络通信的后向安全。

需要说明的是, 在本发明上述一些实施例中, 通信系统在进行 AMF 切换时, 不同的 AMF 对应的 SMF 可能不同, 所以在上述过程中也可能发生 SMF 切换。在这种情况下, 也需要考虑 PDU 会话的安全保护。

进行 AMF 切换的流程中, 在目标侧需要考虑 PDU 会话密钥的更新。在具体实现中, 目标 AMF/目标 SEAF 向 AUSF 发送指示信息, 触发 AUSF 生成新的 PDU 会话密钥。具体的, AUSF 预先保存有密钥 Left K, 那么, AUSF 可基于 Left K、以及目标 AMF/目标 SEAF 所发送过来的 UE 的相关信息及会话信息 (比如会话 ID、切片信息等等), 生成新的 PDU 会话密钥 Ksmf, 具体为:

$K_{smf} = \text{KDF}(\text{Left K}, \text{NAI}, \text{NSSAI}, \text{切片 ID}, \text{AMF 相关参数}, \text{SMF 相关参数}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

然后, AUSF 将 Ksmf 发送至 SEAF 或目标 AMF, SEAF 或目标 AMF 将 Ksmf 转发至目标 SMF

和 UE，目标 SMF/UE 使用 Ksmf 更新 PDU 会话密钥。

在本发明实施例提供的安全实现方法不仅可以应用于同一个通信系统中跨 RAN/跨 AMF 切换的场景，还可以应用于不同的通信系统中跨基站（eNB 和 gNB）/跨接入管理网元（MME 和 AMF）的场景，参见图 9，本发明实施例提供了又一种安全实现方法，该方法可应用于不同通信系统的切换过程中，例如，UE 原先在第一通信系统中建立通信连接，后来 UE 基于用户需求或者当前网络状况，需要将通信连接切换到第二通信系统（比如手机从 LTE 通信系统切换到 5G 通信系统）。在一种可能的实施方式中，第一通信系统（LTE 通信系统）包括：处于接入网的 eNB、处于核心网的 MME、HSS 等，第二通信系统（5G 通信系统）包括：处于接入网的 gNB，处于核心网的目标 AMF/目标 SEAF、AUSF 等，当 UE 需要从当前连接的 eNB 切换到 gNB 时，可通过以下方法实现网络安全，该方法包括但不限于以下步骤：

1、 eNB 触发通信切换。

具体的， eNB 可基于 UE 的需求、UE 的移动、当前网络状况等因素触发通信切换。

2、 eNB 向 MME 发送切换请求。

eNB 发送切换请求（Handover Required）的消息到 MME，通知 MME 有用户要进行切换，所述切换请求携带 UE 的标识。

3、 MME 向目标 AMF/目标 SEAF 发送路径切换请求、原系统安全上下文、中间密钥 Ksme。

其中，所述原系统安全上下文即为第一通信系统的安全上下文，第一通信系统的安全上下文例如包括：第一通信系统中与安全相关的密钥的生存周期、密钥的索引、UE 的安全能力、完整性算法、完整性算法标识、加密算法、加密算法标识、与计算密钥相关的计数值等，也可能包括具体密钥。其中，UE 安全能力可以为 UE 支持的加密和完整性算法列表，UE 所要求的密钥长度、密钥生存期等。

其中，中间密钥 Ksme 为第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥。

在一具体实施例中，在 MME 到目标侧 AMF/SEAF 的路径切换请求中携带有第一通信系统的安全上下文，中间密钥 Ksme。

在又一具体实施例中，MME 将路径切换请求、第一通信系统的安全上下文和中间密钥 Ksme 分别发送至目标 AMF/SEAF。

4、 目标 AMF/目标 SEAF 基于 Ksme 得到 Kamf。

具体实施例中，AMF/SEAF 中间密钥 Ksme、网络参数推导出 Kamf，例如：

$Kamf = KDF(Ksme, \text{目标侧 ID}, \text{切片 ID}, \text{NAI}, \text{NSSAI}, \text{AMF 区域标识}, \text{GUAMI}, \text{AMF 指针}, \text{AMF 设置标识}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{其他参数})$ 。

此外，具体实现中，AMF/SEAF 还可以使用 Ksme、第一通信系统的安全上下文（例如利用 UE 的安全能力）、网络参数等推导出该 Kamf。

5、 目标 AMF/目标 SEAF 基于 Kamf 生成安全密钥。

在具体的实施例中，目标 AMF/目标 SEAF 可以根据预设的规则确定第二通信系统的密

钥保护算法,例如,目标 AMF/目标 SEAF 中预设有 5G 的算法优先级列表,算法优先级列表中具有多种算法 ID,该目标 AMF 查找该算法优先级列表,并根据算法优先级列表选择 5G 的 NAS 算法,获得 NAS 机密性算法 ID 和 NAS 完整性算法 ID。

可以理解的,目标 AMF/目标 SEAF 可基于 Kamf 推导出 AS 层密钥和 NAS 层的相关密钥:如 KgNB, Knasenc, Knasint 等,目标 AMF/目标 SEAF 保存所述 Knasenc, Knasint。详细过程可参考图 5 步骤 9 的描述,这里不再赘述。

6、目标 AMF/目标 SEAF 向 gNB 发送切换请求、安全密钥,这里所发送的安全密钥包括 KgNB。相应的,gNB 获取 KgNB。

具体实施例中,目标 AMF/目标 SEAF 向 gNB 发送切换请求,该切换请求中携带密钥 KgNB。

需要说明的是,如果在前述步骤 4 和步骤 5 中生成密钥的过程中使用了计数值 Nonce 或 Counter,则该切换请求还会携带该计数值 Nonce 或 Counter,以便于 UE 侧能够正确的生成密钥。

在本发明实施例中,当第二通信系统支持用户面完整性保护时,gNB 需要判断是否需要生成和启用用户面完保密钥,具体的,gNB 可以根据预存的策略进行判断,或者,gNB 还可以与 SMF 或 AMF 等网元进行协商从而进行判断,或者,gNB 可以根据第二通信系统的安全上下文来进行判断,该安全上下文包括完整性是否开启的指示信息。当判断支持用户面保护时,gNB 基于 KgNB 继续生成后续的密钥 Krrcenc、密钥 Krrcint、密钥 Kupenc、密钥 Kupint 等 AS 层密钥。

7、gNB 向目标 AMF/目标 SEAF 发送切换请求的确认消息。

8、目标 AMF/目标 SEAF 向 MME 发送路径切换请求、安全上下文。

如果在前述生成密钥的过程中使用了计数值 Nonce 或 Counter,则安全上下文包括计数值 Nonce 或 Counter。

9、MME 向 eNB 发送切换要求、安全上下文。

10、eNB 向 UE 发送切换要求、安全上下文。

11、UE 生成安全密钥。

需要说明的是,UE 侧所接收到的安全上下文,只需包括网络侧生成各个密钥时 UE 侧没有的参数,比如随机数(计数值 Nonce 或 Counter),时间戳等,5G 相关的安全保护算法标识等,UE 可能在之前步骤中都已具备其他的用于生成密钥的参数。

由于 UE 可以从第一通信系统获得 Ksme,所以,对 UE 来说,UE 同样可基于 Ksme、网络参数、安全上下文等生成新的 NAS 层密钥和 AS 层密钥。例如,UE 可先基于 Ksme 生成 Kamf,再基于 Kamf、网络参数、安全上下文生成 AS 层密钥(如 Krrcenc、Krrcint、Kupenc、Kupint 等)和 NAS 层密钥(如 Knasenc、Knasint 等),这里不再赘述。

12、UE 与 gNB 完成后续的切换进程,最终,UE 的通信连接从 eNB 切换到 gNB。

需要说明的是,对于上述图 9 实施例,在可能的实施方式中,可以不在步骤 3 中传递 Ksme,并取消步骤 4,那么,在步骤 5 之前,AUSF 会根据目标侧的 CK/IK 和 MME 传递过来的原系统安全上下文生成目标侧新的 Kseaf,并发送至目标 AMF/目标 SEAF,目标 AMF/目标 SEAF 再根据新的 Kseaf、第一通信系统(如 5G)安全保护算法生成后续的 Kamf 等密钥。

还需要说明的是,在可能的实施方式中,可以不在步骤 3 中传递 Ksme,并取消步骤 4,

那么,在步骤5之前,HSS基于自身的CK/IK和NONCE等参数计算密钥Klte,并将Klte传递给AUSF,AUSF再基于Klte生成Kseaf和Left K,具体的,Kseaf=KDF(Klte,服务网络名称标识,计数值Nonce或Counter或者随机码Random或者序列码Sequence number,其他参数)。AUSF发送Kseaf至目标AMF/目标SEAF,目标AMF/目标SEAF再根据Kseaf、第一通信系统(如5G)安全保护算法生成后续的Kamf等密钥。

可以看出,实施本发明实施例,在跨通信系统切换的实施过程中,目标侧的通信系统可利用源侧的通信系统的中间密钥和安全上下文相应生成安全密钥,从而对切换后的通信系统中的通信进行安全保护。对于网络而言,目标侧的通信系统不能获得源侧的通信系统使用的安全密钥,无法破解源侧的通信系统与UE之间的通信信息,实现了网络通信的后向安全。

参见图10,本发明实施例提供了又一种安全实现方法,该方法可应用于不同通信系统的切换过程中,例如,UE原先在第二通信系统中建立通信连接,后来UE基于用户需求或者当前网络状况,需要将通信连接切换到第一通信系统(比如手机从5G通信系统切换到LTE通信系统)。在一种可能的实施方式中,第一通信系统(LTE通信系统)包括:处于接入网的eNB、处于核心网的MME、HSS等,第二通信系统(5G通信系统)包括:处于接入网的gNB,处于核心网的目标AMF/目标SEAF、AUSF等,当UE需要从当前连接的gNB切换到eNB时,可通过以下方法实现网络安全,该方法包括但不限于以下步骤:

1、gNB触发通信切换。

具体的,eNB可基于UE的需求、UE的移动、当前网络状况等因素触发通信切换。

2、gNB向源AMF/源SEAF发送切换请求,通知向源AMF/源SEAF有用户要进行切换。

3、源AMF/源SEAF向MME发送路径切换请求、原系统的安全上下文;MME向HSS发送切换请求、源系统的安全上下文。

其中,所述原系统安全上下文即为第二通信系统的安全上下文,第二通信系统的安全上下文例如包括:第二通信系统中与安全相关的密钥的生存周期、密钥的索引、UE的安全能力、完整性算法、完整性算法标识、加密算法、加密算法标识、与计算密钥相关的计数值等,也可能包括具体密钥、完整性是否开启的指示信息等。

具体实施例中,源AMF/源SEAF向MME发送的路径切换请求中携带所述安全上下文。

4、HSS向MME反馈路径切换请求响应;MME向源AMF/源SEAF反馈路径切换请求响应。

5、AUSF向HSS发送CK、IK。

本发明具体实施例中,为了满足切换后的LTE系统的安全需求,AUSF可用于生成HSS所需的完整性密钥(Integrity Key,IK)和加密性密钥CK(Cipher Key,CK),并将所述CK、IK发送至HSS。

6、HSS向AUSF发送响应,以通知AUSF成功收到CK、IK。

7、HSS基于CK、IK生成Kasme。

具体实施例中,HSS基于所获取的CK、IK进一步推导出适合第一通信系统的中间密钥Kasme,具体可以为:

Kasme=KDF(CK,IK,服务网络名称标识,序列号SQN,其他参数)。

8、HSS 向 MME 发送生成 K_{asme}，相应的，MME 获取该 K_{asme}。

9、MME 基于 K_{asme} 和安全上下文生成安全密钥。

具体实施例中，MME 可基于 K_{asme}、UE 的安全能力，网络侧的安全能力等参数生成安全密钥（包括密钥 KeNB 和 NAS 密钥），MME 可保存所述 NAS 密钥。其中，UE 安全能力例如可以为 UE 支持的加密和完整性算法列表、UE 所要求的密钥长度、密钥生存期等；网络侧安全能力例如可以为网络侧的网络设备中预配置的网络支持的加密和完整性算法列表，运营商支持的加密和完整性算法优先级列表，网络设备/运营商支持的密钥长度、密钥生存期等。

在具体实现中，该密钥 KeNB 的生成过程可能为：

$\text{KeNB} = \text{KDF}(\text{新的 NAS 计数值}, \text{NAS 计数值的长度}, \text{算法标识}, \text{其他参数})$ 。

10、MME 向 eNB 发送 S1 路径切换请求、安全密钥，所发送的安全密钥包括 KeNB。

其中，其中 S1 接口是 eNB 和 MME 之间的接口。具体实施例中，MME 通过 S1 接口向 eNB 发送路径切换请求，该路径切换请求可携带 KeNB；另一具体实施例中，MME 通过 S1 接口分别向 eNB 发送路径切换请求和 KeNB。

11、eNB 向 MME 反馈 S1 路径响应，通知 MME 成功收到消息。

12、eNB 不计算用户面完整性密钥。

在本发明实施例中，当第一通信系统（LTE）不支持用户面完整性保护时，eNB 判断不需要生成和启用用户面完保密钥。这种情况下，如果所接收到的安全密钥里面包括用户面完整性保护密钥，则 eNB 将不启用该密钥；另外，在 eNB 基于所接收到的密钥 KeNB 生成 AS 密钥过程中，不再生成 AS 的用户面完整性保护密钥。

13、源 AMF/源 SEAF 向 gNB 反馈切换要求、安全上下文。

14、gNB 向 UE 发送切换要求、安全上下文。

15、UE 生成安全密钥。

需要说明的是，UE 侧所接收到的安全上下文，只需包括网络侧生成各个密钥时 UE 侧没有的参数，比如随机数（计数值 Nonce 或 Counter），时间戳等，LTE 相关的安全保护算法标识等，UE 可能在之前步骤中都已具备其他的用于生成密钥的参数。UE 可基于预设的 Kamf 推导出 K_{asme}，进而基于 K_{asme}、网络参数，安全上下文等得到相应的 AS 层密钥和 NAS 层密钥。

16、UE 与 eNB 完成后续的切换进程，最终，UE 的通信连接从 gNB 切换到 eNB。

需要说明的是，对于上述图 10 实施例，在可能的实施方式中，还可以取消步骤 5 和步骤 6，而在步骤 7 中，HSS 可根据预存的 CK/IK、以及所接收的原系统（第二系统）安全上下文生成中间密钥 K_{asme}，在步骤 9 中，MME 可基于 K_{asme}、第一系统（如 5G）安全保护算法生成 KeNB 和 NAS 密钥。

还需要说明的是，在又一种可能的实施方式中，AMF 可发送 Kamf 给 MME，MME 基于 Kamf 经过推导得到 K_{asme}，方式可能有：

第一次推导： $\text{Kasme} = \text{KDF}(\text{Kamf}, \text{目标侧 ID}, \text{服务网络名称标识}, \text{计数值 Nonce 或 Counter 或者 随机码 Random 或者 序列码 Sequence number}, \text{NAS COUNT})$ ；

第二次 $\text{Kasme} = \text{KDF}(\text{Kamf}, \text{第一次推导的 Kasme}, \text{其他参数})$ 。

可以看出, 实施本发明实施例, 在跨通信系统切换的实施过程中, 目标侧的通信系统可利用源侧的通信系统的中间密钥和安全上下文相应生成安全密钥, 从而对切换后的通信系统中的通信进行安全保护。对于网络而言, 目标侧的通信系统不能获得源侧的通信系统使用的安全密钥, 无法破解源侧的通信系统与 UE 之间的通信信息, 实现了网络通信的后向安全。

参见图 11, 基于同一发明构思, 本发明实施例提供了一种 5G 网络结合 WLAN 网络而成的通信系统中切换通信的应用场景。其中, 该 5G 网络包括接入网和核心网, 接入网包括 RAN 设备 331、RAN 设备 332, 核心网包括核心网设备组 341, 接入网设备分别通过 N2 接口与核心网设备连接。WLAN 网络包括无线节点 321、无线节点 322, 以及与无线节点 (无线节点也可以视为接入网的一部分) 建立通信连接的用户设备, 其中无线节点可分别与 RAN 设备 331 和 RAN 设备 332 通过 Xw 接口连接。用户设备与无线节点之间通过 WLAN 技术进行上行通信或下行通信。

在一具体的通信场景中, 用户设备与无线节点 321 通信连接, 如果用户设备从 311 处移动至 312 处, 那么, 用户设备可能就需要将通信连接从无线节点 321 切换至无线节点 322, 在完成切换进程后, 用户设备与无线节点 322 通信连接, 进而才能继续进行通信, 在这一过程中, 上述通信切换过程可能会伴随着 RAN 设备的通信切换。

在这种场景中, 同样可应用本发明实施例提供的安全实现方法对切换后的通信进行安全保护。具体可以包括以下步骤:

1、RAN 设备 332 接收将用户设备从无线节点 321 切换到无线节点 322 的通信的请求;

本发明实施例中, 无线节点例如可以是 WLAN 端点 (WLAN Termination)、无线接入点 AP、无线路由等等。RAN 设备例如可以 gNB 等基站设备。

2、RAN 设备 332 获得主密钥;

具体实施例中, RAN 设备 332 可通过以下方式获得主密钥:

核心网设备组 341 生成中间密钥 KgNB, 并将 KgNB 发送至 RAN 设备 332。

RAN 设备 332 基于 KgNB 生成主密钥, 例如, 当无线节点为 WLAN 端点 (WLAN Termination)。

RAN 设备 332g 基于 KgNB 和 WLAN 端点计数值 (WT Counter) 推导出主密钥 S-Kwt, 具体为: $S-Kwt = KDF(KgNB, WT Counter, \text{其他参数})$ 。

3、RAN 设备 332 通过 Xw 接口向无线节点 322 发送主密钥, 所述 S-Kwt 该 WLAN 的空口保护密钥, 无线节点 322 基于主密钥 S-Kwt 和 IEEE 802.11 规范生成最终的安全密钥, 所述安全密钥用于, 在将用户设备从无线节点 321 切换到无线节点 322 后, 对所述用户设备与无线节点 322 之间的通信进行保护。

4、RAN 设备 332 会通过 UE 之间的空口消息如 RRC 信令消息将 WLAN 端点计数值 (WT Counter) 发送给用户设备, 使得用户设备也能计算出对应的 S-Kwt, 继而基于 S-Kwt 和 IEEE 规范生成安全密钥。

上文详细阐述了本发明实施例的方法, 为了便于更好地实施本发明实施例的上述方案, 下面提供了本发明实施例的相关装置。

参见图 12，本发明实施例提供了一种装置 1200，该装置 1200 包括处理器 1201、存储器 1202 和发射器 1203 以及接收器 1204，所述处理器 1201、存储器 1202 和发射器 1203 以及接收器 1204 相连接（如通过总线相互连接）。

存储器 1202 包括但不限于是随机存储记忆体（Random Access Memory, RAM）、只读存储器（Read-Only Memory, ROM）、可擦除可编程只读存储器（Erasable Programmable Read Only Memory, EPROM）、或便携式只读存储器（Compact Disc Read-Only Memory, CD-ROM），该存储器 1202 用于存储相关指令及数据。

发射器 1203 用于发射数据，接收器 1204 用于接收数据。

处理器 1201 可以是一个或多个中央处理器 1201（Central Processing Unit, CPU），在处理器 1201 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

该处理器 1201 用于读取所述存储器 1202 中存储的程序代码，以实现图 3 实施例中的所述认证网元的功能。

当装置 1200 为第一网元时，存储器 1202 中存储的程序代码具体用于实现图 4 实施例中的所述第一网元的功能。具体描述如下：

所述接收器 1204 用于接收将用户设备从源接入网设备切换到目标接入网设备的通信的请求；

所述处理器 1201 用于获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标网络之间的通信进行保护，所述目标网络包括所述目标接入网设备和目标核心网设备，所述目标核心网设备包括所述第一网元；

所述发射器 1203 用于向所述目标接入网设备发送所述安全密钥。

具体的实施例中，所述处理器 1201 用于获得安全密钥，包括：

所述处理器 1201 用于获取第一中间密钥；所述第一中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；

所述处理器 1201 用于确定安全保护算法，基于所述安全保护算法和所述第一中间密钥推导出所述安全密钥。

具体的实施例中，所述处理器 1201 用于获取第一中间密钥，包括：

所述处理器 1201 用于通过所述接收器 1204 获取安全锚点 SEAF 基于锚密钥、网络参数推衍出的所述第一中间密钥。

具体的实施例中，所述处理器 1201 用于获取第一中间密钥，包括：

所述处理器 1201 用于通过所述接收器 1204 获取第二网元基于第二中间密钥、网络参数推衍出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层和非接入层密钥。

具体的实施例中，所述处理器 1201 用于获取第一中间密钥，包括：

所述处理器 1201 用于通过所述接收器 1204 接收第二网元发送的第二中间密钥；

所述处理器 1201 用于基于所述第二中间密钥、网络参数推衍出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层和非接入层密钥。

具体的实施例中,所述处理器 1201 用于获取第一中间密钥,包括:

在所述用户设备从所述源接入网设备切换到所述目标接入网设备、并且所述用户设备重新通过双向认证后,所述处理器 1201 获得锚密钥;

所述处理器 1201 用于基于所述锚密钥、网络参数推衍出的所述第一中间密钥。

具体的实施例中,所述接收器 1204 还用于接收第二网元发送的下一跳密钥第一 NH、下一跳密钥关联计数第一 NCC;所述处理器 1201 还用于基于所述第一 NH 和第一 NCC 得到第二 NH 和第二 NCC;所述发射器 1203 还用于向所述目标接入网设备发送所述第二 NH 和所述第二 NCC。

具体的实施例中,所述安全密钥包括第一密钥,第二密钥和第三密钥;所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥;所述第二密钥为 NAS 信令加密性保护密钥;所述第三密钥为 NAS 信令完整性保护密钥;

所述处理器 1201 用于确定安全保护算法,基于所述安全保护算法和所述第一中间密钥推衍出所述安全密钥,包括:

所述安全保护算法包括 NAS 机密性算法标识和 NAS 完整性算法标识。

所述处理器 1201 用于基于第一参数推衍出所述第一密钥;其中,所述第一参数包括所述第一中间密钥、目标小区标识、频点、NAS 计数值、NAS 连接标识、计数值或随机码或序列码中的一项或多项;

所述处理器 1201 用于基于第二参数推衍出所述第二密钥;其中,所述第二参数包括所述第一中间密钥、所述 NAS 机密性算法标识、计数值或随机码或序列码中的一项或多项;

所述处理器 1201 用于基于第三参数推衍出所述第三密钥;其中,所述第三参数包括所述第一中间密钥、所述 NAS 完整性算法标识、计数值或随机码或序列码中的一项或多项;

所述发射器 1203 用于向所述目标接入网设备发送所述安全密钥,包括:

所述发射器 1203 用于向所述目标接入网设备发送所述第一密钥。

具体的实施例中,所述源接入网设备为第一通信系统的接入网设备;所述目标接入网设备为第二通信系统的接入网设备;所述第一网元为所述第二通信系统的网元;所述请求包括所述第一通信系统的安全上下文、第三中间密钥;所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥,用于推衍下层的接入层和非接入层的密钥;

所述处理器 1201 用于获取第一中间密钥,包括:

所述处理器 1201 用于基于所述第一通信系统的安全上下文、所述第二通信系统的安全上下文以及所述第三中间密钥推衍出的所述第一中间密钥。

具体的实施例中,所述第一网元包括目标接入和移动管理网元 AMF,所述第二网元包括源 AMF,所述目标 AMF 连接所述目标接入网设备,所述源 AMF 连接所述源接入网设备;或者,所述第一网元包括目标安全锚点 SEAF,所述第二网元包括源安全锚点 SEAF,所述目标 SEAF 连接所述目标接入网设备,所述源 SEAF 连接所述源接入网设备。

具体的实施例中,所述网络参数包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值或随机码或序列码中的一项或多项。

具体的实施例中,所述第一网元包括第一通信系统的移动性管理实体网元 MME;所述

目标接入网设备为所述第一通信系统的接入网设备；所述源接入网设备为第二通信系统的接入网设备；

所述 MME 的接收器 1204 用于接收将用户设备从所述源接入网设备切换到所述目标接入网设备的通信的请求；所述请求包括所述第二通信系统的安全上下文；

所述 MME 的处理器 1201 用于获得安全密钥；

所述 MME 的发射器 1203 用于向所述目标接入网设备发送所述安全密钥。

具体的实施例中，所述 MME 的处理器 1201 用于通过所述 MME 的接收器 1204 接收所述第一通信系统的归属签约用户服务器 HSS 基于第一加密密钥、第一完整性保护密钥、服务网络名称标识、序列号 SQN 推导出的第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推导下层的接入层和非接入层的密钥；

所述 MME 的处理器 1201 用于基于所述第二通信系统的安全上下文、所述第三中间密钥推导出所述安全密钥。

具体的实施例中，所述 MME 的处理器 1201 用于获得安全密钥，包括：

所述 MME 的处理器 1201 用于通过所述 MME 的接收器 1204 接收所述第二通信系统的 AMF 发送的第一中间密钥；所述第一中间密钥为所述第二通信系统中认证后生成的上层的密钥，用于推导下层的接入层 AS 和非接入层 NAS 密钥；

所述 MME 的处理器 1201 用于基于所述第一中间密钥推导出所述第三中间密钥；

所述 MME 的处理器 1201 用于基于所述第二通信系统的安全上下文、所述第三中间密钥推导出所述安全密钥。

需要说明的是，当装置 1200 为第一网元时，处理器 1201 执行的步骤以及处理器 1201 涉及的其他技术特征还可以参照图 5-图 10 所示的方法实施例的相应描述，这里不再赘述。

当装置 1200 为目标接入网设备时，存储器 1202 中存储的程序代码具体用于实现图 11 实施例中的所述 RAN 设备 332 的功能。具体描述如下：

所述接收器 1204 用于接收将用户设备从源无线节点切换到目标无线节点的通信的请求；

所述接收器 1204 还用于接收核心网设备发送的第一密钥（例如 KeNB 或 KgNB）；所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥；

所述处理器 1201 用于基于所述中间密钥生成第二密钥（主密钥）；所述第二密钥为用户设备与所述目标无线节点之间进行安全保护的中间密钥；

所述发射器 1203 用于向目标无线节点发送所述第二密钥，以便于所述目标无线节点基于所述第二密钥生成安全密钥；所述安全密钥用于，在将所述用户设备从源无线节点切换到目标无线节点后，对所述用户设备与所述目标无线节点之间的通信进行保护。

需要说明的是，当装置 1200 为第一网元时，处理器 1201 执行的步骤以及处理器 1201 涉及的其他技术特征还可以参照图 11 所示的方法实施例的相应描述，这里不再赘述。

参见图 13，基于同一发明构思，本发明实施例提供了又一种装置 1300，装置 1300 为第一网元，具体包括：接收模块 1301，密钥处理模块 1302，发送模块 1303，描述如下：

接收模块 1301 用于接收将用户设备从源接入网设备切换到目标接入网设备的通信的请求；

密钥处理模块 1302 用于获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标网络之间的通信进行保护，所述目标网络包括所述目标接入网设备和目标核心网设备，所述目标核心网设备包括所述第一网元；

发送模块 1303 用于向所述目标接入网设备发送所述安全密钥。

具体实施例中，密钥处理模块 1302 获取第一中间密钥；所述第一中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；

密钥处理模块 1302 确定安全保护算法，基于所述安全保护算法和所述第一中间密钥推导出所述安全密钥。

具体实施例中，所述第一网元获取第一中间密钥，包括：

密钥处理模块 1302 通过接收模块 1301 获取安全锚点 SEAF 基于锚密钥、网络参数推衍出的所述第一中间密钥。

具体实施例中，密钥处理模块 1302 获取第一中间密钥，包括：

密钥处理模块 1302 通过接收模块 1301 获取第二网元基于第二中间密钥、网络参数推衍出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层和非接入层密钥。

具体实施例中，密钥处理模块 1302 获取第一中间密钥，包括：

接收模块 1301 接收第二网元发送的第二中间密钥；

密钥处理模块 1302 基于所述第二中间密钥、网络参数推衍出的所述第一中间密钥；其中，第二中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层和非接入层密钥。

具体实施例中，密钥处理模块 1302 获取第一中间密钥，包括：

在所述用户设备从所述源接入网设备切换到所述目标接入网设备、并且所述用户设备重新通过双向认证后，密钥处理模块 1302 获得锚密钥；

密钥处理模块 1302 基于所述锚密钥、网络参数推衍出的所述第一中间密钥。

具体实施例中，密钥处理模块 1302 通过接收模块 1301 还获取第二网元发送的下一跳密钥第一 NH、下一跳密钥关联计数第一 NCC；

密钥处理模块 1302 基于所述第一 NH 和第一 NCC 得到第二 NH 和第二 NCC；

发送模块 1303 向所述目标接入网设备发送所述第二 NH 和所述第二 NCC。

具体实施例中，所述安全密钥包括第一密钥，第二密钥和第三密钥；所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥；所述第二密钥为 NAS 信令加密性保护密钥；所述第三密钥为 NAS 信令完整性保护密钥；

密钥处理模块 1302 确定安全保护算法，基于所述安全保护算法和所述第一中间密钥推导出所述安全密钥，包括：

所述安全保护算法包括 NAS 机密性算法标识和 NAS 完整性算法标识

密钥处理模块 1302 基于第一参数推导出所述第一密钥；其中，所述第一参数包括所述第一中间密钥、目标小区标识、频点、NAS 计数值、NAS 连接标识、计数值或随机码或序列

码中的一项或多项；

密钥处理模块 1302 基于第二参数推导出所述第二密钥；其中，所述第二参数包括所述第一中间密钥、所述 NAS 机密性算法标识、计数值或随机码或序列码中的一项或多项；

密钥处理模块 1302 基于第三参数推导出所述第三密钥；其中，所述第三参数包括所述第一中间密钥、所述 NAS 完整性算法标识、计数值或随机码或序列码中的一项或多项；

发送模块 1303 向所述目标接入网设备发送所述安全密钥，包括：

所述发送向所述目标接入网设备发送所述第一密钥。

具体实施例中，所述源接入网设备为第一通信系统的接入网设备；所述目标接入网设备为第二通信系统的接入网设备；所述第一网元为所述第二通信系统的网元；所述请求包括所述第一通信系统的安全上下文、第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；

密钥处理模块 1302 获取第一中间密钥，包括：

密钥处理模块 1302 基于所述第一通信系统的安全上下文、所述第二通信系统的安全上下文以及所述第三中间密钥推衍出的所述第一中间密钥。

具体实施例中，所述第一网元包括目标接入和移动管理网元 AMF，所述第二网元包括源 AMF，所述目标 AMF 连接所述目标接入网设备，所述源 AMF 连接所述源接入网设备；或者，所述第一网元包括目标安全锚点 SEAF，所述第二网元包括源安全锚点 SEAF，所述目标 SEAF 连接所述目标接入网设备，所述源 SEAF 连接所述源接入网设备。

具体实施例中，所述网络参数包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值或随机码或序列码中的一项或多项。

具体实施例中，所述第一网元包括第一通信系统的移动性管理实体网元 MME；所述目标接入网设备为所述第一通信系统的接入网设备；所述源接入网设备为第二通信系统的接入网设备；

密钥处理模块 1302 通过接收模块 1301 接收将用户设备从所述源接入网设备切换到所述目标接入网设备的通信的请求；所述请求包括所述第二通信系统的安全上下文；

密钥处理模块 1302 获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标网络之间的通信进行保护；

发送模块 1303 向所述目标接入网设备发送所述安全密钥。

具体实施例中，所述 MME 获得安全密钥，包括：

密钥处理模块 1302 通过接收模块 1301 获取所述第一通信系统的归属签约用户服务器 HSS 基于第一加密密钥、第一完整性保护密钥、服务网络名称标识、序列号 SQN 推衍出的第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；

密钥处理模块 1302 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密钥。

具体实施例中，密钥处理模块 1302 获取安全密钥，包括：密钥处理模块 1302 通过接

收模块 1301 获取所述第二通信系统的 AMF 发送的第一中间密钥；所述第一中间密钥为所述第二通信系统中认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；

密钥处理模块 1302 基于所述第一中间密钥推衍出所述第三中间密钥；

密钥处理模块 1302 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密钥。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者任意组合来实现。当使用软件实现时，可以全部或者部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令，在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络或其他可编程装置。所述计算机指令可存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网络站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线）或无线（例如红外、微波等）方式向另一个网络站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质，也可以是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如软盘、硬盘、磁带等）、光介质（例如 DVD 等）、或者半导体介质（例如固态硬盘）等等。

在上述实施例中，对各个实施例的描述各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

权利要求

1、一种安全实现方法，其特征在于，所述方法包括：

第五代通信系统中的接入与管理网元 AMF 接收第四代通信系统中的移动性管理实体网元 MME 发送的路径切换请求，所述路径切换请求中包括中间密钥 K_{asme}；

所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}；

所述 AMF 基于所述 K_{amf} 生成安全密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述网络参数包括下行非接入层消息对应的计数值；

所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}，包括：

所述 AMF 基于所述下行非接入层消息对应的计数值和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述 AMF 基于所述 K_{amf} 生成安全密钥，包括：

所述 AMF 基于所述 K_{amf} 生成基站密钥 K_{gNB}。

4、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

所述 AMF 向基站 gNB 发送第一切换请求，所述切换请求中包括所述 K_{gNB}；以使得所述 gNB 基于所述 K_{gNB} 生成接入层密钥。

5、一种安全实现方法，其特征在于，所述方法包括：

当接收到接收第四代通信系统中的基站发送的切换请求时，用户设备 UE 根据中间密钥 K_{asme} 以及网络参数获得第五代通信系统中的密钥 K_{amf}；

所述 UE 根据所述 K_{amf} 生成安全密钥。

6、根据权利要求 5 所述的方法，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

7、根据权利要求 5 或 6 所述的方法，其特征在于，所述 UE 根据所述 K_{amf} 生成安全密钥之后，所述方法还包括：

所述 UE 与所述第五代通信系统中的基站进行交互以完成所述 UE 从所述第四代通信系统的基站到所述第五代通信系统基站的切换。

8、根据权利要求 5 所述的方法，其特征在于，所述切换请求中包括安全上下文；

所述 UE 根据所述 K_{amf} 生成安全密钥，包括：

所述 UE 根据网络参数、接收到的所述安全上下文以及所述 K_{amf} 生成接入层密钥和非接入层密钥。

9、一种装置，其特征在于，所述装置包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器和接收器执行以下操作：

所述接收器，用于第四代通信系统中的移动性管理实体网元 MME 发送的路径切换请求，所述路径切换请求中包括中间密钥 K_{asme}；

所述处理器，用于所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}；以及基于所述 K_{amf} 生成安全密钥。

10、根据权利要求 9 所述的装置，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

11、根据权利要求 9 或 10 所述的装置，其特征在于，所述基于所述 K_{amf} 生成安全密钥，包括：

基于所述 K_{amf} 生成基站密钥 K_{gNB}。

12、根据权利要求 9 所述的装置，其特征在于，所述装置还包括发射器；

所述发射器，用于向基站 gNB 发送第一切换请求，所述切换请求中包括所述 K_{gNB}；以使得所述 gNB 基于所述 K_{gNB} 生成接入层密钥。

13、一种用户设备，其特征在于，所述用户设备包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行以下操作：

当接收到接收第四代通信系统中的基站发送的切换请求时，根据中间密钥 K_{asme} 以及网络参数获得第五代通信系统中的密钥 K_{amf}；以及

根据所述 K_{amf} 生成安全密钥。

14、根据权利要求 13 所述的用户设备，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

15、根据权利要求 13 或 14 所述的用户设备，其特征在于，所述处理器还用于执行以下操作：

所述第五代通信系统中的基站进行交互以完成所述 UE 从所述第四代通信系统的基站到所述第五代通信系统基站的切换。

16、根据权利要求 13 所述的用户设备，其特征在于，所述切换请求中包括安全上下文；所述根据所述 K_{amf} 生成安全密钥，包括：

根据网络参数、接收到的所述安全上下文以及所述 K_{amf} 生成接入层密钥和非接入层密钥。

1、一种安全实现方法，其特征在于，所述方法包括：

第五代通信系统中的接入与管理网元 AMF 接收第四代通信系统中的移动性管理实体网元 MME 发送的路径切换请求，所述路径切换请求中包括中间密钥 K_{asme}；

所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}；

所述 AMF 基于所述 K_{amf} 生成安全密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述网络参数包括下行非接入层消息对应的计数值；

所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}，包括：

所述 AMF 基于所述下行非接入层消息对应的计数值和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述 AMF 基于所述 K_{amf} 生成安全密钥，包括：

所述 AMF 基于所述 K_{amf} 生成基站密钥 K_{gNB}。

4、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

所述 AMF 向基站 gNB 发送第一切换请求，所述切换请求中包括所述 K_{gNB}；以使得所述 gNB 基于所述 K_{gNB} 生成接入层密钥。

5、一种安全实现方法，其特征在于，所述方法包括：

当接收到接收第四代通信系统中的基站发送的切换请求时，用户设备 UE 根据中间密钥 K_{asme} 以及网络参数获得第五代通信系统中的密钥 K_{amf}；

所述 UE 根据所述 K_{amf} 生成安全密钥。

6、根据权利要求 5 所述的方法，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

7、根据权利要求 5 或 6 所述的方法，其特征在于，所述 UE 根据所述 K_{amf} 生成安全密钥之后，所述方法还包括：

所述 UE 与所述第五代通信系统中的基站进行交互以完成所述 UE 从所述第四代通信系统的基站到所述第五代通信系统基站的切换。

8、根据权利要求 5 所述的方法，其特征在于，所述切换请求中包括安全上下文；

所述 UE 根据所述 K_{amf} 生成安全密钥，包括：

所述 UE 根据网络参数、接收到的所述安全上下文以及所述 K_{amf} 生成接入层密钥和非接入层密钥。

9、一种装置，其特征在于，所述装置包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器和接收器执行以下操作：

所述接收器，用于第四代通信系统中的移动性管理实体网元 MME 发送的路径切换请求，所述路径切换请求中包括中间密钥 K_{asme}；

所述处理器，用于所述 AMF 基于网络参数和所述 K_{asme} 获得第五代通信系统中的密钥 K_{amf}；以及基于所述 K_{amf} 生成安全密钥。

10、根据权利要求 9 所述的装置，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

11、根据权利要求 9 或 10 所述的装置，其特征在于，所述基于所述 K_{amf} 生成安全密钥，包括：

基于所述 K_{amf} 生成基站密钥 K_{gNB}。

12、根据权利要求 9 所述的装置，其特征在于，所述装置还包括发射器；

所述发射器，用于向基站 gNB 发送第一切换请求，所述切换请求中包括所述 K_{gNB}；以使得所述 gNB 基于所述 K_{gNB} 生成接入层密钥。

13、一种用户设备，其特征在于，所述用户设备包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行以下操作：

当接收到接收第四代通信系统中的基站发送的切换请求时，根据中间密钥 K_{asme} 以及网络参数获得第五代通信系统中的密钥 K_{amf}；以及

根据所述 K_{amf} 生成安全密钥。

14、根据权利要求 13 所述的用户设备，其特征在于，所述网络参数包括下行非接入层消息对应的计数值。

15、根据权利要求 13 或 14 所述的用户设备，其特征在于，所述处理器还用于执行以下操作：

所述第五代通信系统中的基站进行交互以完成所述 UE 从所述第四代通信系统的基站到所述第五代通信系统基站的切换。

16、根据权利要求 13 所述的用户设备，其特征在于，所述切换请求中包括安全上下文；所述根据所述 K_{amf} 生成安全密钥，包括：

根据网络参数、接收到的所述安全上下文以及所述 K_{amf} 生成接入层密钥和非接入层密钥。

17、一种接入与管理网元，其特征在于，所述接入与管理网元用于执行权利要求 1 至 4 任一所述的方法。

18、一种用户设备，其特征在于，所述用户设备用于执行权利要求 5 至 8 任一所述的方法。

19、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 1 至 4 任一所述的方法会被运行。

20、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 5 至 8 任一所述的方法会被运行。

21、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 1 至 4 任一所述的方法会被运行。

22、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算

机指令，当所述计算机指令被运行时，所述权利要求 5 至 8 任一所述的方法会被运行。

23、一种密钥推演的方法，其特征在于，所述方法包括：

第五代通信系统中的接入与管理网元 AMF 接收第四代通信系统中的接入与管理网元 MME 发送的第一中间密钥 K_{asme}；

所述 AMF 根据第一中间密钥 K_{asme} 生成第二中间密钥 K_{amf}；

所述 AMF 根据所述第二中间密钥 K_{amf} 生成安全密钥；以及

所述 AMF 向基站发送所述安全密钥。

24、根据权利要求 23 所述的方法，其特征在于，所述 AMF 根据第一中间密钥生成第二中间密钥，包括：

所述 AMF 根据第一中间密钥和网络参数推演第二中间密钥。

25、根据权利要求 23 所述的方法，其特征在于，所述方法还包括：

所述 AMF 接收所述 MME 发送的第四代通信系统的安全上下文；

所述 AMF 根据第一中间密钥生成第二中间密钥，包括：

所述 AMF 根据第一中间密钥、所述第四代通信系统的安全上下文以及网络参数生成第二中间密钥。

26、根据权利要求 23 至 25 任一所述的方法，其特征在于，所述安全密钥包括接入层密钥；所述 AMF 根据所述第二中间密钥生成安全密钥，包括：

所述 AMF 根据所述第二中间密钥和上行非接入层计数值生成接入层密钥。

27、根据权利要求 23 至 26 任一所述的方法，其特征在于，所述第一中间密钥为所述第四代通信系统中认证后生成的上层的密钥，用于推衍第四代通信系统的下层的接入层和非接入层的密钥。

28、一种密钥推演的方法，其特征在于，所述方法包括：

用户设备接收第四代通信系统中的无线接入网络发送的切换请求，所述切换请求中包括安全上下文；

所述用户设备根据第一中间密钥 K_{asme} 和所述安全上下文生成安全密钥，其中，所述第一中间密钥 k_{asme} 为所述第四代通信系统中认证后生成的上层的密钥，用于推衍第四代通信系统的下层的接入层和非接入层的密钥；

所述用户设备从所述第四代通信系统中的无线接入网络切换至第五代通信系统中的无线接入网络。

29、根据权利要求 28 所述的方法，其特征在于，所述用户设备根据第一中间密钥和所述安全上下文生成安全密钥，包括：

所述用户设备根据第一中间密钥 K_{asme} 生成第二中间密钥 K_{amf}；

所述用户设备根据所述第二中间密钥 K_{amf} 和所述安全上下文生成安全密钥。

30、根据权利要求 29 所述的方法，其特征在于，所述用户设备根据第一中间密 K_{asme} 生成第二中间密钥 K_{amf}，包括：

所述用户设备根据第一中间密钥和网络参数推演第二中间密钥。

31、根据权利要求 29 或 30 所述的方法，其特征在于，所述安全密钥包括接入层密钥和非接入层密钥；

所述用户设备根据所述第二中间密钥和所述安全上下文生成安全密钥，包括：

所述用户设备根据所述第二中间密钥和上行非接入层计数值获取接入层中间密钥 KgNB，并基于所述接入层中间密钥 KgNB 获取接入层密钥；以及

所述用户设备根据所述第二中间密钥和非接入层的算法标识获取非接入层密钥。

32、根据权利要求 28 所述的方法，其特征在于，所述用户设备根据第一中间密钥和所述安全上下文生成安全密钥，包括：

所述 AMF 根据所述第一中间密钥、所述安全上下文以及网络参数生成第二中间密钥；

所述用户设备根据所述第二中间密钥 Kamf 和所述安全上下文生成安全密钥。

33、一种密钥推演的方法，其特征在于，所述方法包括：

第五代通信系统中的源接入与管理网元接收源无线接入网络发送的切换请求；

响应于所述切换请求，所述源接入与管理网元根据第一中间密钥生成第二中间密钥；

所述源接入与管理网元向目标接入与管理网元发送下一跳密钥、下一跳密钥关联计数值以及所述第二中间密钥。

34、根据权利要求 33 所述的方法，其特征在于，所述源接入与管理网元根据第一中间密钥生成第二中间密钥，包括：

所述源接入与管理网元根据第一中间密钥和网络参数生成第二中间密钥。

35、根据权利要求 34 所述的方法，其特征在于，所述网络参数为下行非接入层计数值。

36、根据权利要求 33 至 35 任一所述的方法，其特征在于，所述下一跳密钥和下一跳密钥关联计数值是根据所述第二中间密钥生成的。

37、根据权利要求 33 至 34 任一所述的方法，其特征在于，所述第一中间密钥为用户设备与源网络认证成功之后配置在源接入与管理网元的密钥。

38、一种密钥推演的方法，其特征在于，所述方法包括：

用户设备接收第五代通信系统中的基站 gNB 发送的切换请求，所述切换请求中包括安全上下文；

所述用户设备根据第五代通信系统中的中间密钥 Kamf 推演第四代通信系统的中间密钥 Kasme；

所述用户设备根据网络参数，所述 Kasme、所述安全上下文获取接入层层密钥和非接入层密钥。

39、根据权利要求 38 所述的方法，其特征在于，所述安全上下文包括安全保护算法标识。

40、根据权利要求 39 所述的方法，其特征在于，所述网络参数包括所述安全保护算法标识的长度。

41、根据权利要求 38 至 40 任一所述的方法，其特征在于，所述用户设备根据网络参数，所述 Kasme、所述安全上下文获取接入层层密钥和非接入层密钥之后，所述方法还包括：

所述用户设备从所述所述基站 gNB 切换到第四代通信系统中的基站 eNB。

42、根据权利要求 41 所述的方法，其特征在于，所述用户设备根据第五代通信系统中的中间密钥 Kamf 推演第四代通信系统的中间密钥 Kasme，包括：

所述用户设备根据第五代通信系统中的中间密钥 K_{amf} 和非接入层下行计数值推演第四代通信系统的中间密钥 K_{asme} ;

所述用户设备从所述所述基站 gNB 切换到第四代通信系统中的基站 eNB。

43、一种密钥推演的方法，其特征在于，所述方法包括：

第五代通信系统中的源接入与管理网元 AMF 接收第五代通信系统中的源无线接入网络 RAN 发送的切换请求；

响应于所述切换请求，所述源 AMF 根据第一中间密钥生成第二中间密钥；所述第一中间密钥为用户设备与源网络认证成功之后配置在源网络侧的密钥；

所述源 AMF 向第五代通信系统中的目标 AMF 发送所述第二中间密钥以使得所述目标 AMF 基于所述第二中间密钥生成安全密钥。

44、根据权利要求 43 所述的方法，其特征在于，所述源 AMF 根据第一中间密钥生成第二中间密钥，包括：

所述源 AMF 根据所述第一中间密钥和网络参数生成所述第二中间密钥。

45、根据权利要求 44 所述的方法，其特征在于，所述网络参数包括非接入层计数值。

46、根据权利要求 45 所述的方法，其特征在于，所述非接入层计数值为下行非接入层计数值。

47、根据权利要求 46 所述的方法，其特征在于，所述网络参数还包括所述非接入层计数值的长度。

48、根据权利要求 43 至 47 任一项所述的方法，其特征在于，所述方法还包括：

所述源 AMF 接收所述目标 AMF 发送的路径切换响应消息；以及

所述源 AMF 向所述源 RAN 发送切换要求以向源 RAN 通知切换准备完成。

49、一种密钥推演的方法，其特征在于，所述方法包括：

用户设备接收第五代通信系统中的源无线接入网络发送的切换请求，所述切换请求包括安全上下文；

所述用户设备根据第一中间密钥和所述安全上下文生成安全密钥，其中，所述第一中间密钥为所述用户设备与源网络认证成功之后配置在所述用户设备上的密钥。

50、根据权利要求 49 所述的方法，其特征在于，所述用户设备根据第一中间密钥和所述安全上下文生成安全密钥，包括：

所述用户设备根据所述第一中间密钥生成第二中间密钥；

所述用户设备根据所述第二中间密钥和所述安全上下文生成所述安全密钥。

51、根据权利要求 50 所述的方法，其特征在于，所述用户设备根据所述第一中间密钥生成第二中间密钥，包括：

所述用户设备根据所述第一中间密钥和网络参数生成所述第二中间密钥。

52、根据权利要求 51 所述的方法，其特征在于，所述网络参数包括非接入层计数值。

53、根据权利要求 52 所述的方法，其特征在于，所述非接入层计数值为下行非接入层计数值。

54、根据权利要求 53 所述的方法，其特征在于，所述网络参数还包括所述下行非接入层计数值的长度。

55、根据权利要求 49 至 54 任一所述的方法，其特征在于，所述安全密钥包括非接入层加密密钥和非接入层完整性保护密钥；所述安全上下文包括非接入层加密算法标识和非接入层完整性保护算法标识；

所述用户设备根据所述第二中间密钥和所述安全上下文生成安全密钥，包括：

所述用户设备根据所述第二中间密钥和所述非接入层加密算法标识获取所述非接入层加密密钥；

所述用户设备根据所述第二中间密钥和所述非接入层完整性保护算法标识获取所述非接入层完整性保护密钥。

56、一种接入与管理网元，其特征在于，所述接入与管理网元包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 23 至 27 任一所述的方法。

57、一种用户设备，其特征在于，所述用户设备包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 28 至 32 任一所述的方法。

58、一种接入与管理网元，其特征在于，所述接入与管理网元包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 33 至 37 任一所述的方法。

59、一种用户设备，其特征在于，所述用户设备包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 38 至 42 任一所述的方法。

60、一种接入与管理网元，其特征在于，所述接入与管理网元包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 43 至 48 任一所述的方法。

61、一种用户设备，其特征在于，所述用户设备包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 49 至 55 任一所述的方法。

62、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 23 至 27 任一所述的方法会被运行。

63、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 28 至 32 任一所述的方法会被运行。

64、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 33 至 37 任一所述的方法会被运行。

65、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 38 至 42 任一所述的方法会被运行。

66、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 43 至 48 任一所述的方法会被运行。

67、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指

令，当所述计算机软件指令被运行时，所述权利要求 49 至 55 任一所述的方法会被运行。

68、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 23 至 27 任一所述的方法会被运行。

69、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 28 至 32 任一所述的方法会被运行。

70、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 33 至 37 任一所述的方法会被运行。

71、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 38 至 42 任一所述的方法会被运行。

72、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 43 至 48 任一所述的方法会被运行。

73、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 49 至 55 任一所述的方法会被运行。

74、一种接入与管理网元，其特征在于，所述接入与管理网元用于执行权利要求 23 至 27 任一所述的方法。

75、一种用户设备，其特征在于，所述用户设备用于执行权利要求 28 至 32 任一所述的方法。

76、一种接入与管理网元，其特征在于，所述接入与管理网元用于执行权利要求 33 至 37 任一所述的方法。

77、一种用户设备，其特征在于，所述用户设备用于执行权利要求 38 至 42 任一所述的方法。

78、一种接入与管理网元，其特征在于，所述接入与管理网元用于执行权利要求 43 至 48 任一所述的方法。

79、一种用户设备，其特征在于，所述用户设备用于执行权利要求 49 至 55 任一所述的方法。

80、一种安全实现方法，其特征在于，包括：

第一网元接收将用户设备从源接入网设备切换到目标接入网设备的通信的请求；

所述第一网元获得安全密钥；所述安全密钥用于，在将所述用户设备从所述源接入网设备切换到所述目标接入网设备后，对所述用户设备与所述目标网络之间的通信进行保护，所述目标网络包括所述目标接入网设备和目标核心网设备，所述目标核心网设备包括所述第一网元；

所述第一网元向所述目标接入网设备发送所述安全密钥。

81、根据权利要求 80 所述的方法，其特征在于，所述第一网元获得安全密钥，包括：

所述第一网元获取第一中间密钥；所述第一中间密钥为认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；

所述第一网元确定安全保护算法，基于所述安全保护算法和所述第一中间密钥推导出所述安全密钥。

82、根据权利要求 81 所述的方法，其特征在于，所述第一网元获取第一中间密钥，包

括:

所述第一网元获取安全锚点 SEAF 基于锚密钥、网络参数推衍出的所述第一中间密钥。

83、根据权利要求 81 所述的方法,其特征在于,所述第一网元获取第一中间密钥,包括:

所述第一网元获取第二网元基于第二中间密钥、网络参数推衍出的所述第一中间密钥;其中,第二中间密钥为认证后生成的上层的密钥,用于推衍下层的接入层和非接入层密钥。

84、根据权利要求 81 所述的方法,其特征在于,所述第一网元获取第一中间密钥,包括:

所述第一网元接收第二网元发送的第二中间密钥;

所述第一网元基于所述第二中间密钥、网络参数推衍出的所述第一中间密钥;其中,第二中间密钥为认证后生成的上层的密钥,用于推衍下层的接入层和非接入层密钥。

85、根据权利要求 81 所述的方法,其特征在于,所述第一网元获取第一中间密钥,包括:

在所述用户设备从所述源接入网设备切换到所述目标接入网设备、并且所述用户设备重新通过双向认证后,所述第一网元获得锚密钥;

所述第一网元基于所述锚密钥、网络参数推衍出的所述第一中间密钥。

86、根据权利要求 83 所述的方法,其特征在于,所述方法还包括:

所述第一网元还获取第二网元发送的下一跳密钥第一 NH、下一跳密钥关联计数第一 NCC;

所述第一网元基于所述第一 NH 和第一 NCC 得到第二 NH 和第二 NCC;

所述第一网元向所述目标接入网设备发送所述第二 NH 和所述第二 NCC。

87、根据权利要求 81 至 86 任一项所述的方法,其特征在于,所述安全密钥包括第一密钥,第二密钥和第三密钥;所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥;所述第二密钥为 NAS 信令加密性保护密钥;所述第三密钥为 NAS 信令完整性保护密钥;

所述第一网元确定安全保护算法,基于所述安全保护算法和所述第一中间密钥推衍出所述安全密钥,包括:

所述安全保护算法包括 NAS 机密性算法标识和 NAS 完整性算法标识;

所述第一网元基于第一参数推衍出所述第一密钥;其中,所述第一参数包括所述第一中间密钥、目标小区标识、频点、NAS 计数值、NAS 连接标识、计数值或随机码或序列码中的一项或多项;

所述第一网元基于第二参数推衍出所述第二密钥;其中,所述第二参数包括所述第一中间密钥、所述 NAS 机密性算法标识、计数值或随机码或序列码中的一项或多项;

所述第一网元基于第三参数推衍出所述第三密钥;其中,所述第三参数包括所述第一中间密钥、所述 NAS 完整性算法标识、计数值或随机码或序列码中的一项或多项;

所述第一网元向所述目标接入网设备发送所述安全密钥,包括:

所述第一网元向所述目标接入网设备发送所述第一密钥。

88、根据权利要求 81 所述的方法,其特征在于,所述方法还包括:所述源接入网设备

为第一通信系统的接入网设备；所述目标接入网设备为第二通信系统的接入网设备；所述第一网元为所述第二通信系统的网元；所述请求包括所述第一通信系统的安全上下文、第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；

所述第一网元获取第一中间密钥，包括：

所述第一网元基于所述第一通信系统的安全上下文、所述第二通信系统的安全上下文以及所述第三中间密钥推衍出的所述第一中间密钥。

89、根据权利要求 79 至 88 任一项所述的方法，其特征在于，

所述第一网元包括目标接入和移动管理网元 AMF，所述第二网元包括源 AMF，所述目标 AMF 连接所述目标接入网设备，所述源 AMF 连接所述源接入网设备；

或者，

所述第一网元包括目标安全锚点 SEAF，所述第二网元包括源安全锚点 SEAF，所述目标 SEAF 连接所述目标接入网设备，所述源 SEAF 连接所述源接入网设备。

90、根据权利要求 82 至 89 任一项所述的方法，其特征在于，所述网络参数包括目标侧标识、切片标识、网络接入标识符 NAI、网络切片选择辅助信息 NSSAI、AMF 区域标识、AMF 设置标识、AMF 全局唯一指示符 GUAMI、AMF 指针 pointer、AMF 集合标识、计数值或随机码或序列码中的一项或多项。

91、根据权利要求 79 所述的方法，其特征在于，所述第一网元包括第一通信系统的移动性管理实体网元 MME；所述目标接入网设备为所述第一通信系统的接入网设备；所述源接入网设备为第二通信系统的接入网设备；

所述方法包括：

所述 MME 接收将用户设备从所述源接入网设备切换到所述目标接入网设备的通信的请求；所述请求包括所述第二通信系统的安全上下文；

所述 MME 获得安全密钥；

所述 MME 向所述目标接入网设备发送所述安全密钥。

92、根据权利要求 91 所述的方法，其特征在于，所述 MME 获得安全密钥，包括：

所述 MME 获取所述第一通信系统的归属签约用户服务器 HSS 基于第一加密密钥、第一完整性保护密钥、服务网络名称标识、序列号 SQN 推衍出的第三中间密钥；所述第三中间密钥为在所述第一通信系统中认证后生成的上层的密钥，用于推衍下层的接入层和非接入层的密钥；

所述 MME 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密钥。

93、根据权利要求 92 所述的方法，其特征在于，所述 MME 获取安全密钥，包括：

所述 MME 获取所述第二通信系统的 AMF 发送的第一中间密钥；所述第一中间密钥为所述第二通信系统中认证后生成的上层的密钥，用于推衍下层的接入层 AS 和非接入层 NAS 密钥；

所述 MME 基于所述第一中间密钥推衍出所述第三中间密钥；

所述 MME 基于所述第二通信系统的安全上下文、所述第三中间密钥推衍出所述安全密

钥。

94、一种安全实现方法，其特征在于，包括：

目标接入网设备接收将用户设备从源无线节点切换到目标无线节点的通信的请求；

所述目标接入网设备接收核心网设备发送的第一密钥；所述第一密钥为用户设备与所述目标接入网设备之间进行安全保护的中间密钥；

所述目标接入网设备基于所述中间密钥生成第二密钥；所述第二密钥为用户设备与所述目标无线节点之间进行安全保护的中间密钥；

所述目标接入网设备向目标无线节点发送所述第二密钥，以便于所述目标无线节点基于所述第二密钥生成安全密钥；所述安全密钥用于，在将所述用户设备从源无线节点切换到目标无线节点后，对所述用户设备与所述目标无线节点之间的通信进行保护。

95、一种接入与管理网元，其特征在于，所述接入与管理网元包括处理器、存储器、发射器以及接收器；所述存储器中存储有程序代码，当所述程序代码被运行时，所述处理器执行权利要求 79 至 93 任一所述的方法。

96、一种接入与管理网元，其特征在于，所述接入与管理网元用于执行权利要求 94 所述的方法。

97、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 79 至 93 任一所述的方法会被运行。

98、一种计算机存储介质，其特征在于，所述计算机存储介质中存储有计算机软件指令，当所述计算机软件指令被运行时，所述权利要求 94 所述的方法会被运行。

99、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 79 至 93 任一所述的方法会被运行。

100、一种计算机程序产品，其特征在于，所述计算机程序产品中包括一个或多个计算机指令，当所述计算机指令被运行时，所述权利要求 94 所述的方法会被运行。

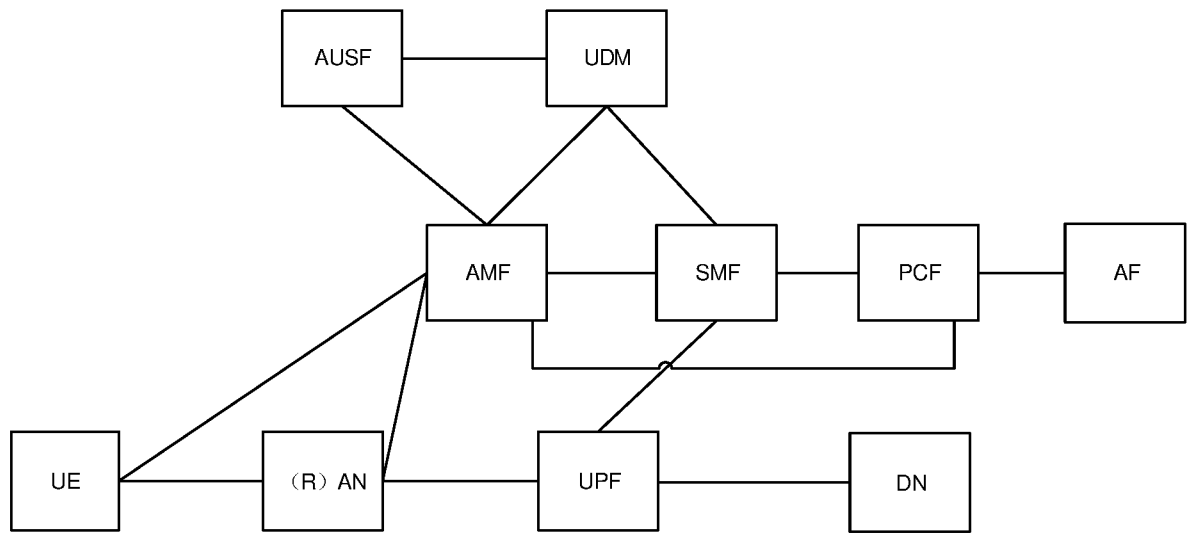


图 1

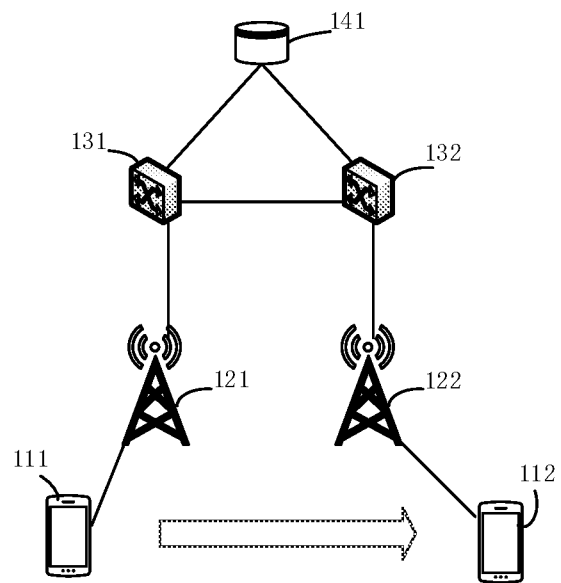


图 2

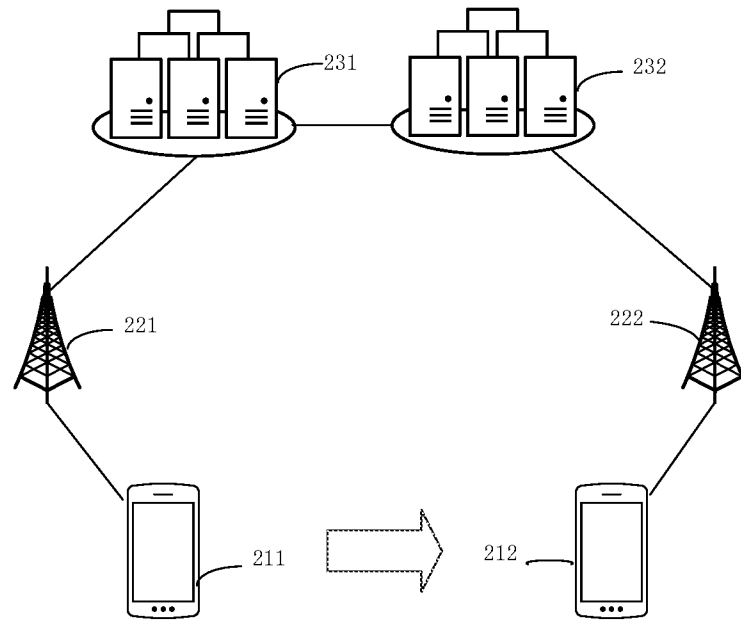


图 3

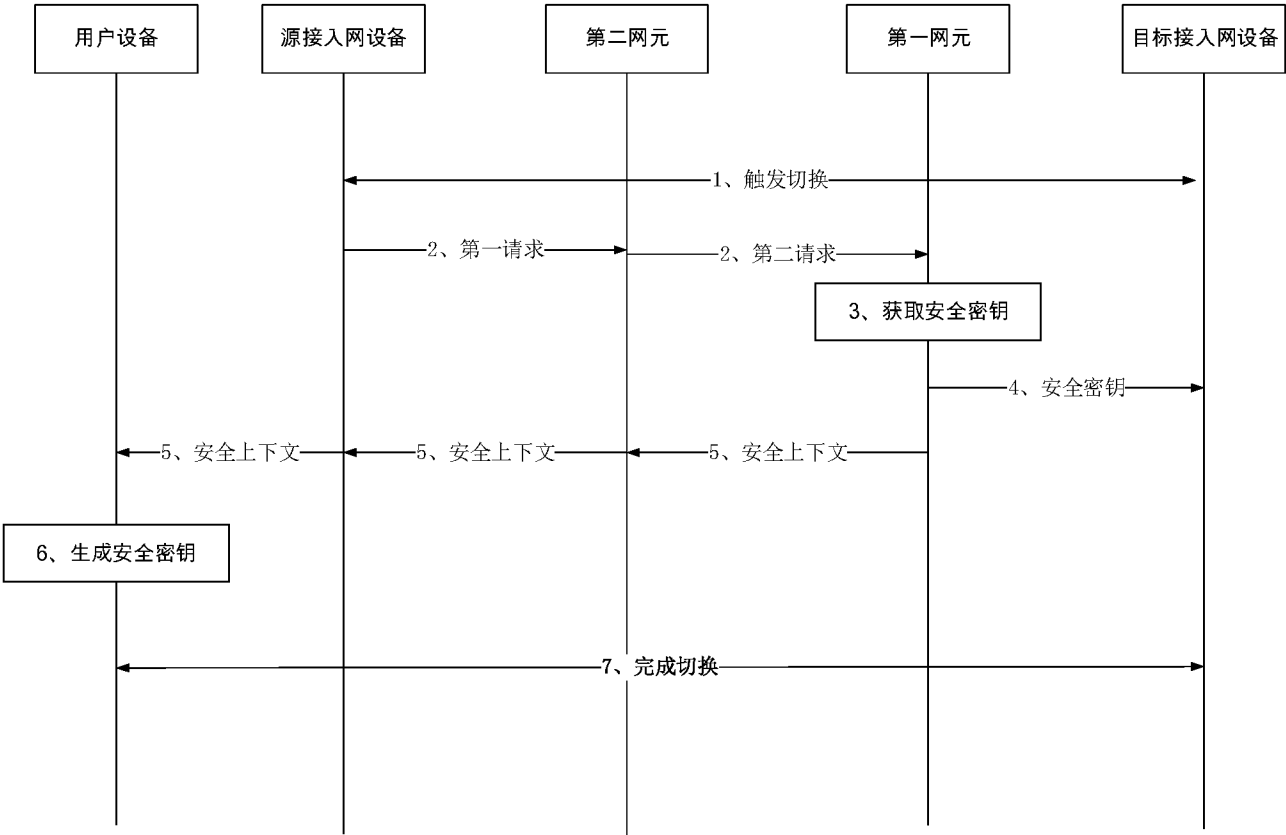


图 4

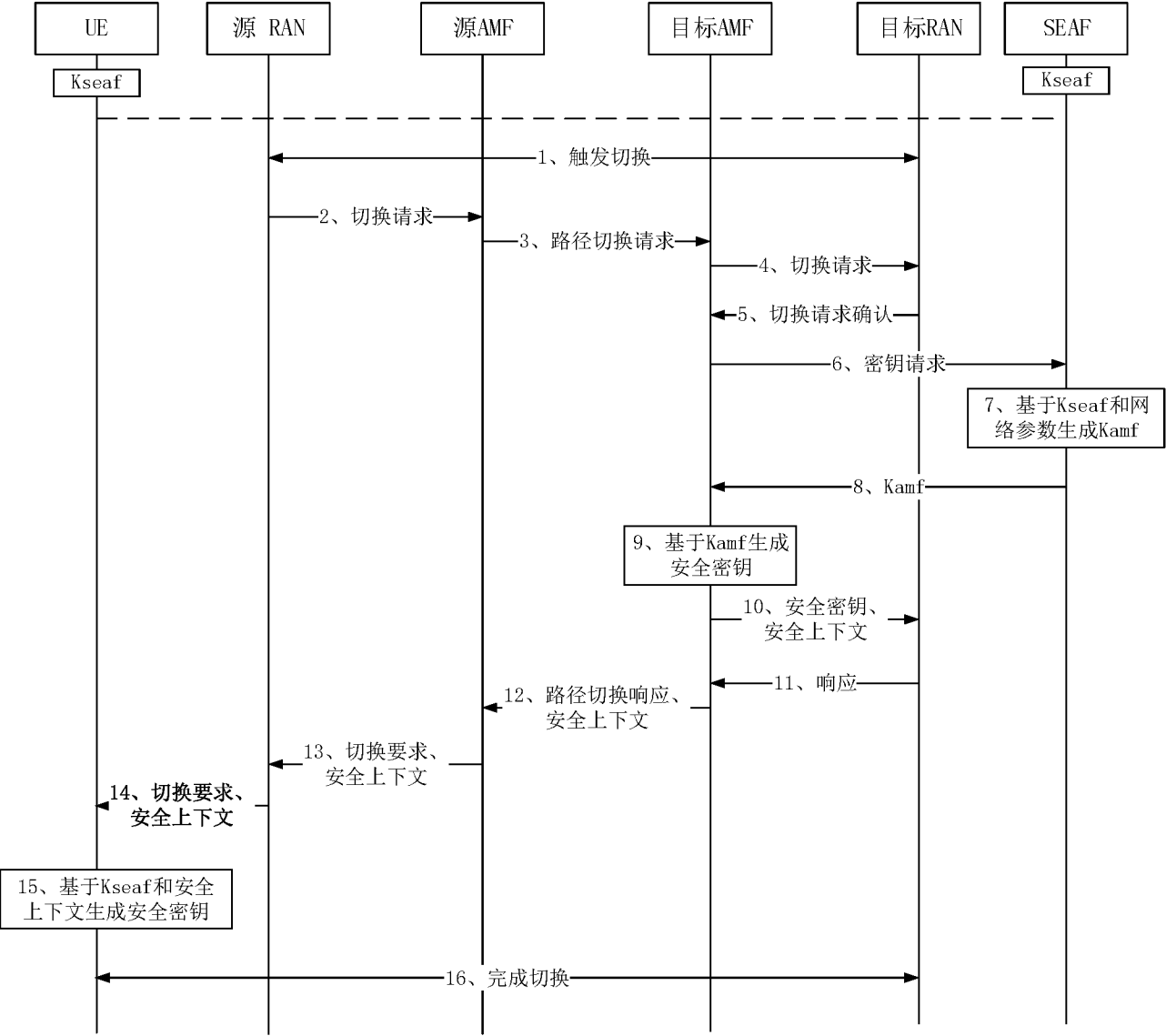


图 5

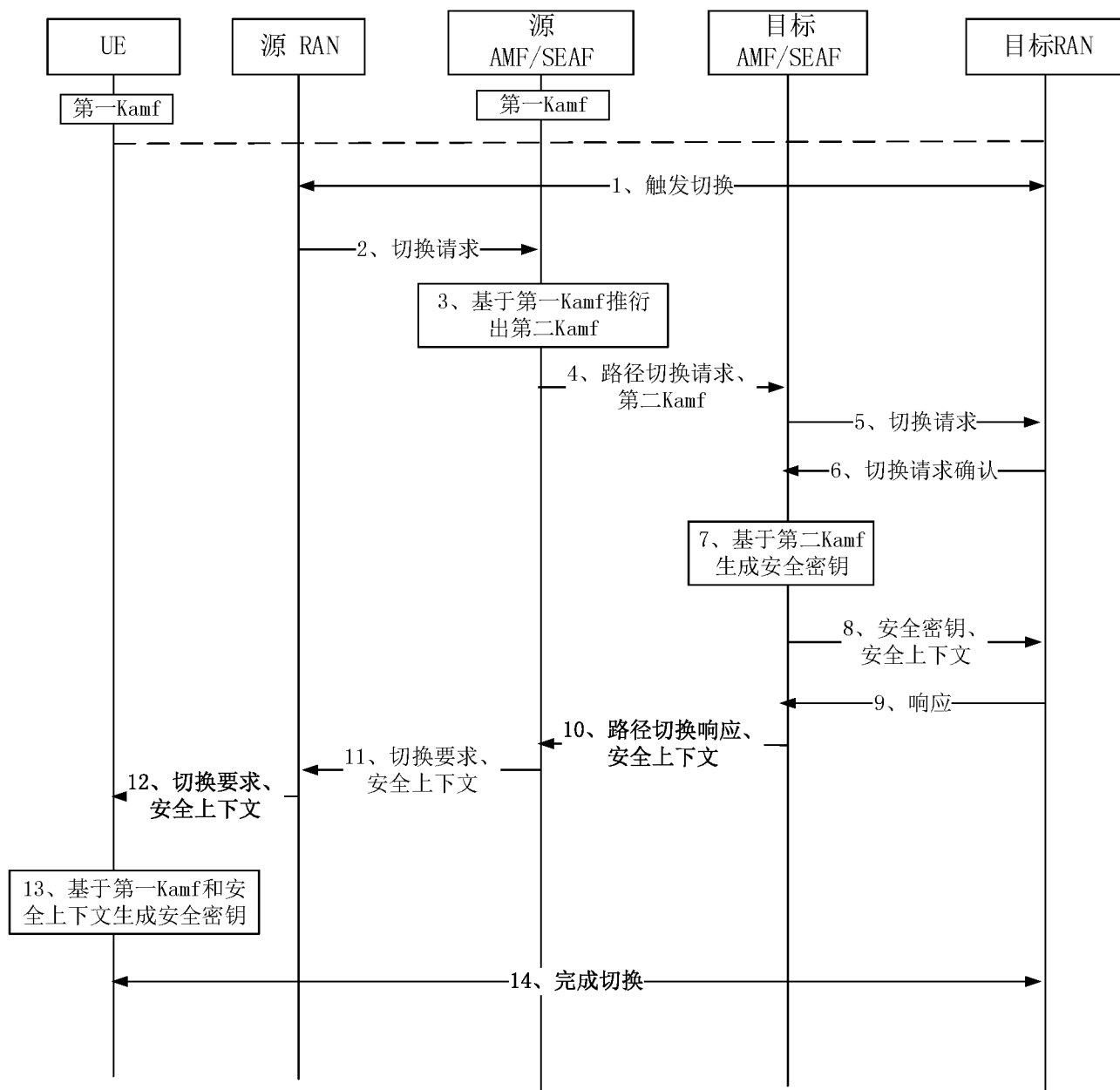


图 6

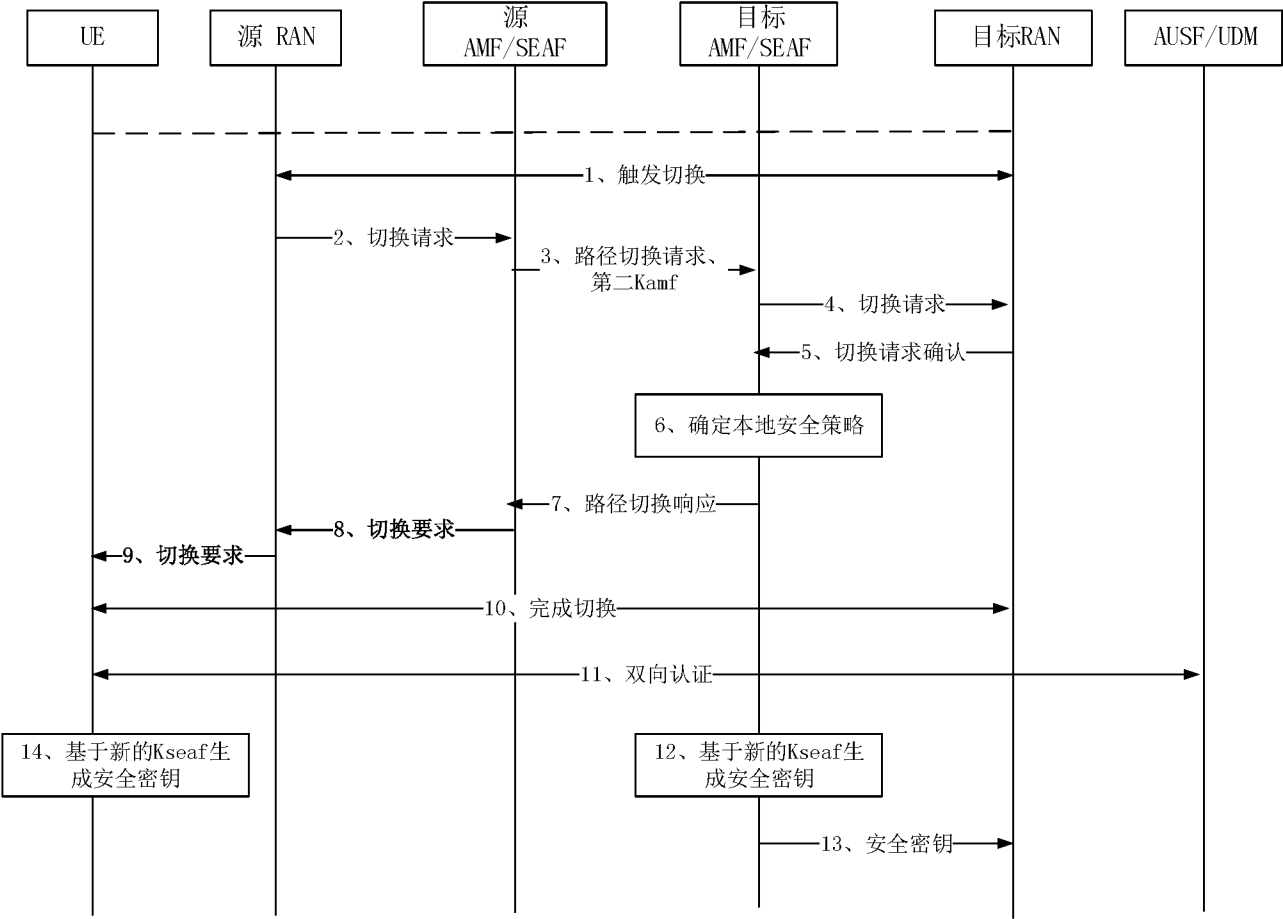


图 7

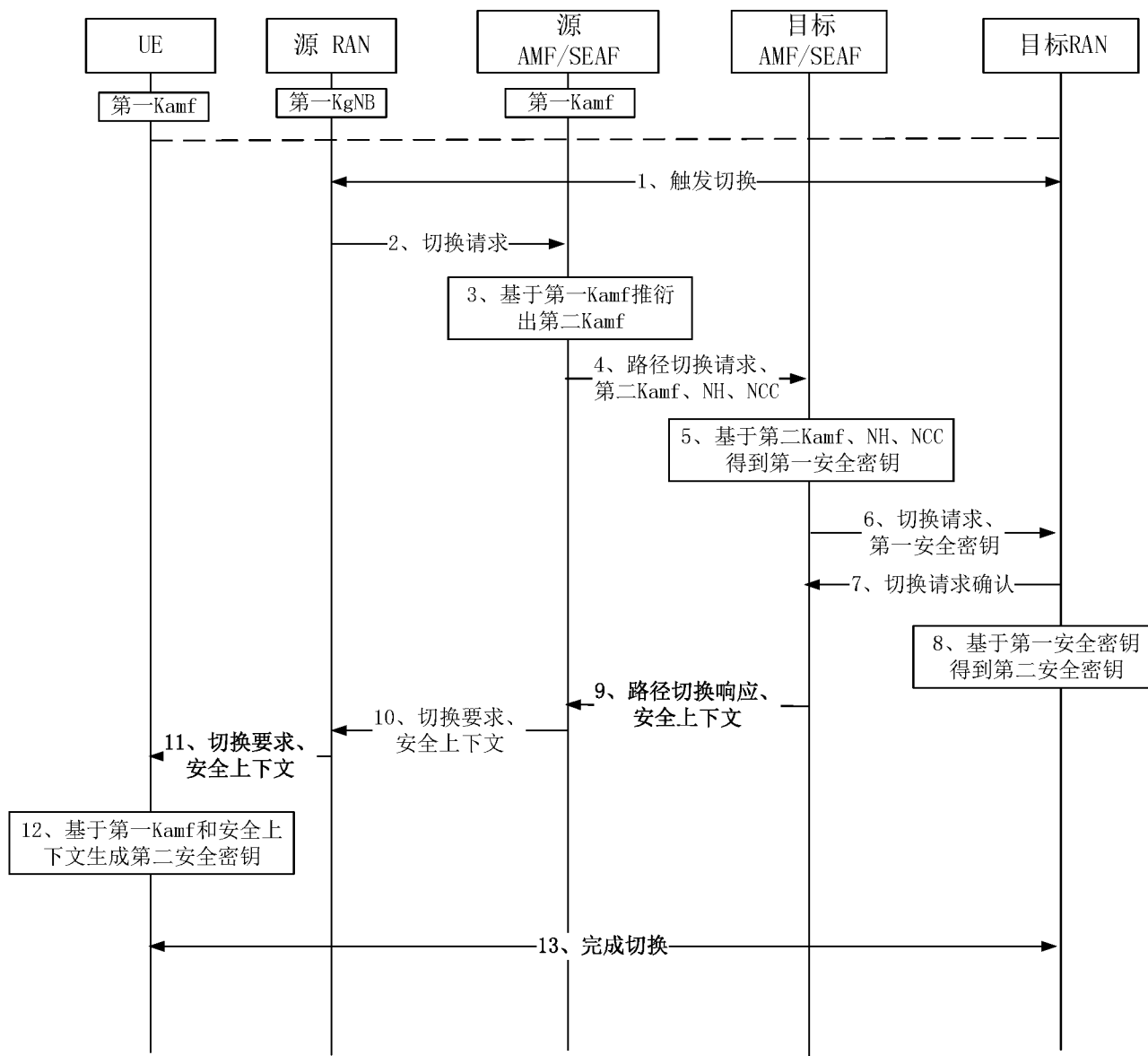


图 8

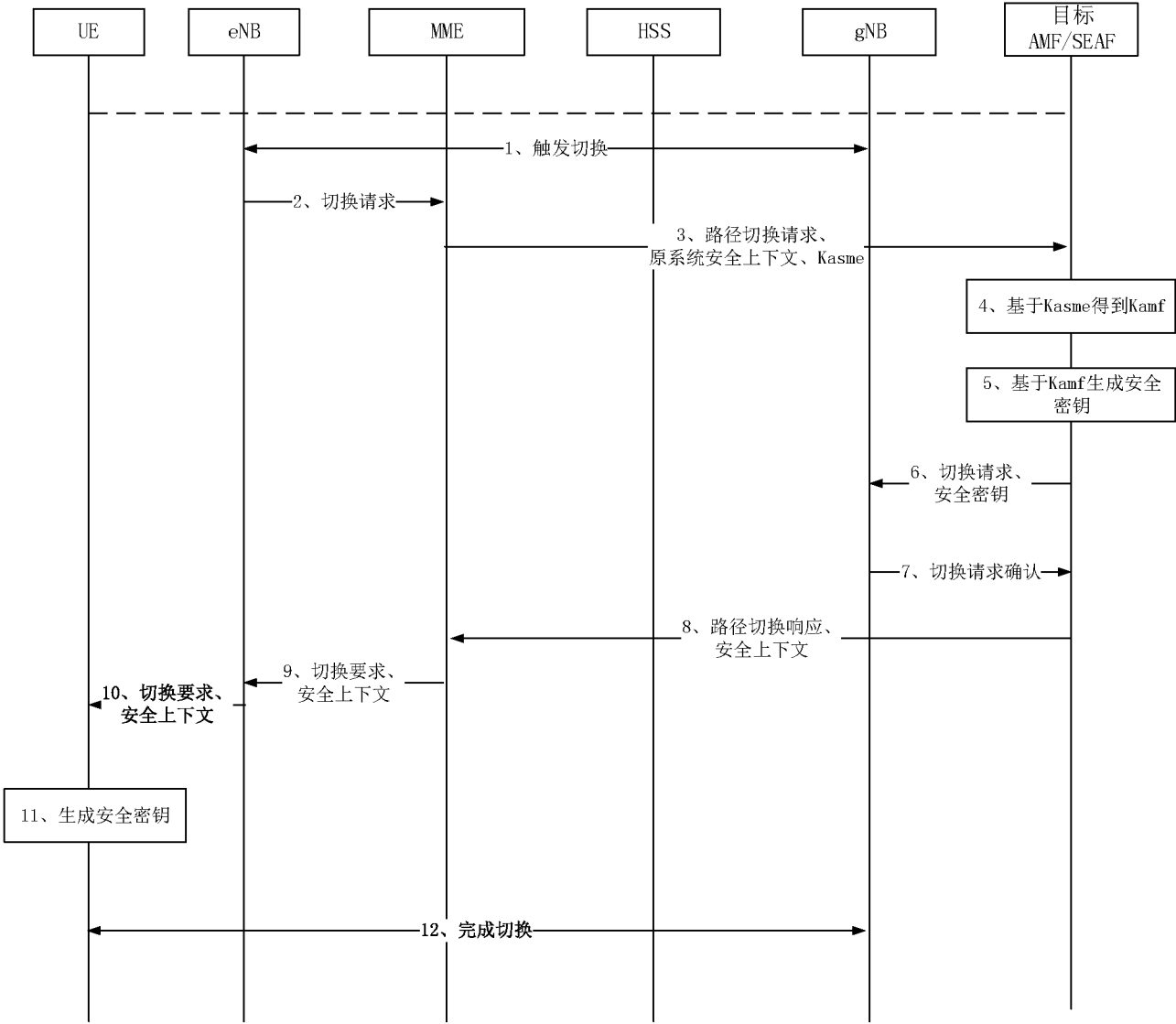


图 9

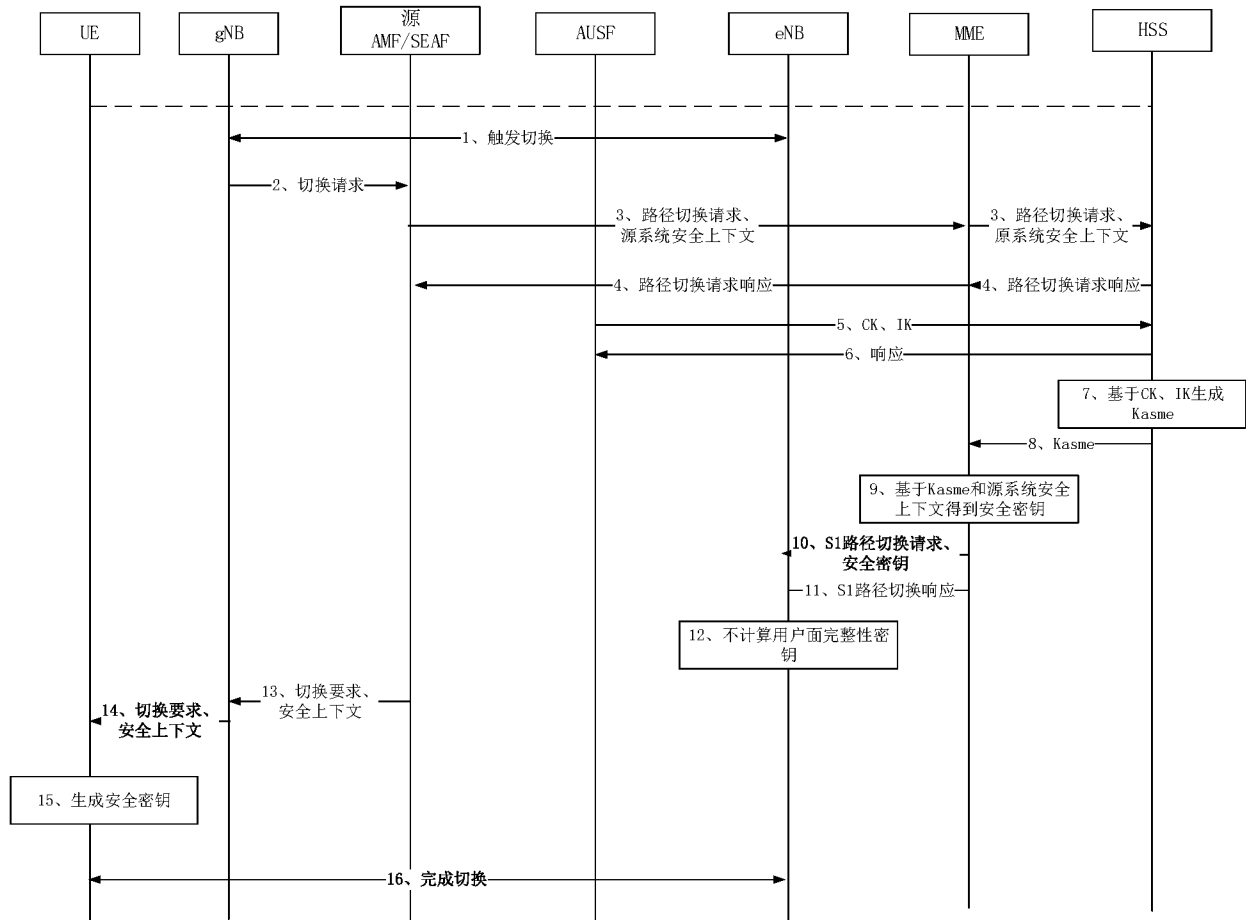


图 10

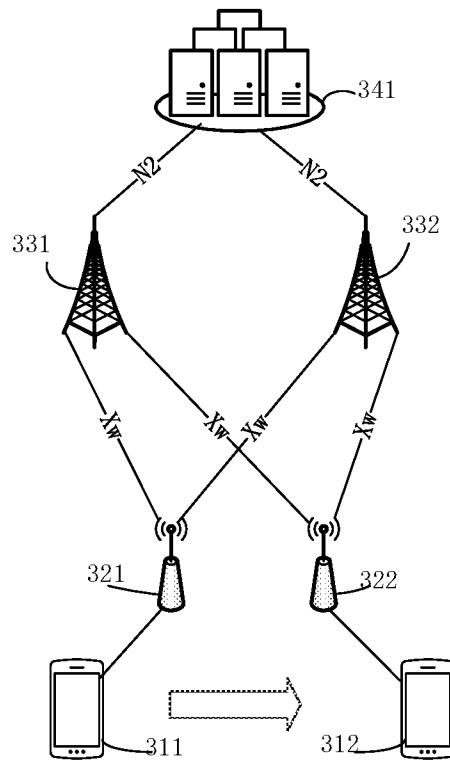


图 11

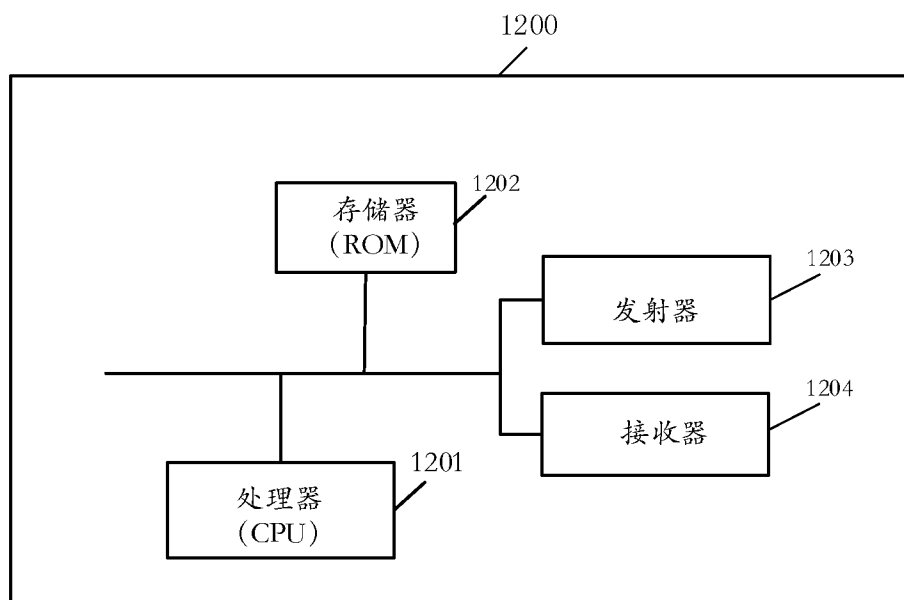


图 12

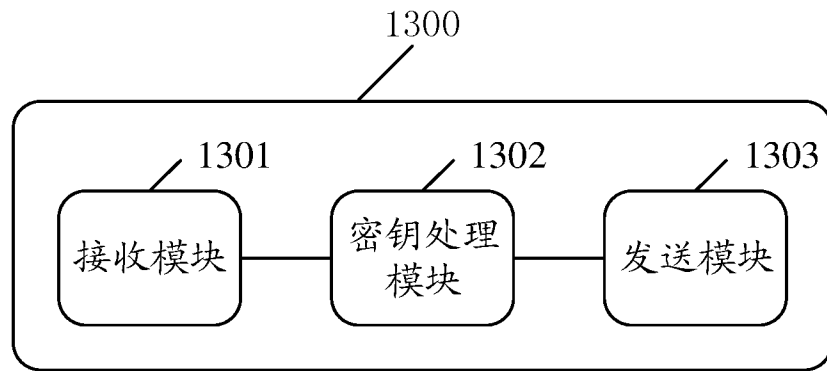


图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/084702

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; VEN; CNKI: 安全, 接入与管理网元, 移动性管理实体网元, 路径, 切换, 密钥, 网络参数, AFM, MME, key, safety, path, route, exchange, network parameter, switch, 4G, 5G

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103781069 A (HUAWEI TECHNOLOGIES CO., LTD.) 07 May 2014 (07.05.2014), claims 1-15	1-16
A	CN 103379490 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 October 2013 (30.10.2013), entire document	1-16
A	WO 2016166529 A1 (VODAFONE IP LICENSING LIMITED) 20 October 2016 (20.10.2016), entire document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	“&” document member of the same patent family

Date of the actual completion of the international search 11 July 2018	Date of mailing of the international search report 18 July 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer XU, Gang Telephone No. (86-10) 62411238

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/084702

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103781069 A	07 May 2014	CN 103781069 B	22 February 2017
		WO 2014059947 A1	24 April 2014
CN 103379490 A	30 October 2013	WO 2013152740 A1	17 October 2013
		EP 2827628 A1	21 January 2015
		US 2015026787 A1	22 January 2015
		EP 2827628 A4	18 March 2015
WO 2016166529 A1	20 October 2016	GB 201506256 D0	27 May 2015
		GB 2537377 A	19 October 2016
		US 2018083782 A1	22 March 2018
		CN 107683616 A	09 February 2018
		EP 3284276 A1	21 February 2018

国际检索报告

国际申请号

PCT/CN2018/084702

A. 主题的分类 H04W 12/04 (2009.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类														
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CPRSABS; CNTXT; VEN; CNKI: 安全, 接入与管理网元, 移动性管理实体网元, 路径, 切换, 密钥, 网络参数, AFM, MME, key, safety, path, route, exchange, network parameter, switch, 4G, 5G														
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 103781069 A (华为技术有限公司) 2014年 5月 7日 (2014 - 05 - 07) 权利要求1-15</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 103379490 A (华为技术有限公司) 2013年 10月 30日 (2013 - 10 - 30) 全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>WO 2016166529 A1 (沃达方 IP 许可有限公司) 2016年 10月 20日 (2016 - 10 - 20) 全文</td> <td>1-16</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 103781069 A (华为技术有限公司) 2014年 5月 7日 (2014 - 05 - 07) 权利要求1-15	1-16	A	CN 103379490 A (华为技术有限公司) 2013年 10月 30日 (2013 - 10 - 30) 全文	1-16	A	WO 2016166529 A1 (沃达方 IP 许可有限公司) 2016年 10月 20日 (2016 - 10 - 20) 全文	1-16
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
A	CN 103781069 A (华为技术有限公司) 2014年 5月 7日 (2014 - 05 - 07) 权利要求1-15	1-16												
A	CN 103379490 A (华为技术有限公司) 2013年 10月 30日 (2013 - 10 - 30) 全文	1-16												
A	WO 2016166529 A1 (沃达方 IP 许可有限公司) 2016年 10月 20日 (2016 - 10 - 20) 全文	1-16												
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。														
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件														
国际检索实际完成的日期 2018年 7月 11日		国际检索报告邮寄日期 2018年 7月 18日												
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 徐刚 电话号码 86-(010)-62411238												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/084702

检索报告引用的专利文件				公布日 (年/月/日)		同族专利		公布日 (年/月/日)	
CN	103781069	A	2014年 5月 7日	CN	103781069	B	2017年 2月 22日		
				WO	2014059947	A1	2014年 4月 24日		
CN	103379490	A	2013年 10月 30日	WO	2013152740	A1	2013年 10月 17日		
				EP	2827628	A1	2015年 1月 21日		
				US	2015026787	A1	2015年 1月 22日		
				EP	2827628	A4	2015年 3月 18日		
WO	2016166529	A1	2016年 10月 20日	GB	201506256	D0	2015年 5月 27日		
				GB	2537377	A	2016年 10月 19日		
				US	2018083782	A1	2018年 3月 22日		
				CN	107683616	A	2018年 2月 9日		
				EP	3284276	A1	2018年 2月 21日		