

切换的处理方法和装置

5 本申请要求于 2019 年 04 月 29 日提交中国专利局、申请号为 201910356843.8、申请名称为“切换的处理方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10 本发明涉及通信领域，并且更具体地，涉及一种切换的处理方法和装置。

背景技术

在第五代（5th generation，5G）通信场景下，由于用户设备的移动会存在接入网设备切换场景，例如用户设备的位置发生变化导致为用户设备提供服务的接入网设备发生变化。目前通信协议中定义了两种接入网设备的切换，一种是 Xn 接口切换，一种是 N2 接口切换。Xn 接口切换指的是发生接入网设备切换前后的接入网设备之间存在 Xn 接口，接入网设备之间的切换基于该接口进行。N2 切换是指发生接入网设备切换基于接入网设备与核心网元接入管理功能（access and mobility management function，AMF）之间的 N2 接口进行。

20 现有的 N2 接口切换场景下，在接入网设备切换失败的时候，可能会存在切换流程中导致用户设备与第一 AMF 上的密钥不一致的情况，从而导致接入网设备切换失败之后用户设备无法重新与第一 AMF 建立连接。

发明内容

25 本申请公开了一种切换的处理方法和装置，通过第一 AMF 保存并恢复使用第一 NAS 安全上下文，保证在接入网设备切换失败的时候，用户设备与第一 AMF 上的安全上下文一致，进而保证了用户设备与第一 AMF 上的密钥一致。

30 第一方面，提供了一种切换的处理方法，包括：第一接入管理功能 AMF 接收第一接入网设备发送的切换请求消息；当确定需要进行密钥推演时，所述第一 AMF 保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下文为所述第一 AMF 与用户设备 UE 协商生成的 NAS 安全上下文；所述第一 AMF 恢复使用所述第一 NAS 安全上下文。

本申请实施例提供的切换的处理方法，通过第一 AMF 在需要密钥推演的情况下，保存第一 NAS 安全上下文，并在密钥推演之后，恢复使用第一 NAS 安全上下文，达到接入网设备切换失败的时候，用户设备与第一 AMF 上的密钥一致的目的。

35 应理解，本申请实施例第一 NAS 安全上下文还可以称为 UE 当前使用的 NAS 安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述第一 NAS 安全上下文中包括第一 NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计

数器 NAS COUNT。

本申请实施例提供的切换的处理方法，第一 NAS 安全上下文中包括第一 AMF 与用户设备 UE 协商使用的 AMF 密钥 Kamf1、第一 AMF 与用户设备 UE 协商生成的 NAS 密钥以及非接入层计数器 NAS COUNT。

- 5 结合第一方面，在第一方面的某些实现方式中，所述第一 AMF 恢复使用所述第一 NAS 安全上下文包括：所述第一 AMF 向第二 AMF 发起用户上下文创建服务请求之后，所述第一 AMF 恢复使用所述第一 NAS 安全上下文。

本申请实施例提供的切换的处理方法，第一 AMF 恢复使用所述第一 NAS 安全上下文可以是在第一 AMF 向第二 AMF 发起用户上下文创建服务请求之后；或者，在第一 AMF 向第二 AMF 发起用户上下文创建服务请求之前；或者，在第一 AMF 向第二 AMF 发起用户上下文创建服务请求的时候。

第二方面，提供了一种切换的处理方法，包括：用户设备 UE 接收第一接入网设备发送的切换命令消息，所述切换命令消息携带第二接入管理功能 AMF 选择的第二 NAS 安全算法和 AMF 密钥改变指示；当所述第二 NAS 安全算法与所述 UE 当前使用的第一 NAS 安全算法不一致和/或所述 AMF 密钥改变指示为预设值时，所述 UE 保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下文为所述 UE 和第一 AMF 协商生成的 NAS 安全上下文，当所述 UE 用户设备切换失败时，使用所述第一 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 保护；或者，当所述 UE 对非接入层容器 NASC 完整性校验失败时，所述 UE 继续使用所述第一 NAS 安全上下文，其中，所述 NASC 携带在所述切换命令消息中。

本申请实施例提供的切换的处理方法，通过使得 UE 接收到的切换命令消息中携带的第二 NAS 安全算法和/或 AMF 密钥改变指示为 1 时，UE 保存第一 NAS 安全上下文，并在 UE 用户设备切换失败使用所述第一 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 保护；或者，UE 在对 NASC 完整性校验失败时，继续使用当前的第一 NAS 安全上下文，达到用户设备与第一 AMF 上的密钥一致。

结合第二方面，在第二方面的某些实现方式中，所述第一 NAS 安全上下文中包括第一 NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计数器 NAS COUNT。

本申请实施例提供的切换的处理方法，第一 NAS 安全上下文中包括第一 AMF 与用户设备 UE 协商使用的 AMF 密钥 Kamf1、第一 AMF 与用户设备 UE 协商生成的 NAS 密钥以及非接入层计数器 NAS COUNT。

结合第二方面，在第二方面的某些实现方式中，所述 AMF 密钥改变指示为预设值包括：所述 AMF 密钥改变指示为 1。

本申请实施例提供的切换的处理方法，AMF 密钥改变指示为 1 的时候指示进行密钥推演。

第三方面，提供了一种切换的处理方法，包括：第一接入管理功能 AMF 接收第一接入网设备发送的切换请求消息；所述第一 AMF 根据本地策略进行密钥推演得到第二 AMF 密钥；所述第一 AMF 基于所述第二 AMF 密钥以及第一 NAS 安全算法生成第二 NAS 安全上下文，其中，所述第一 NAS 安全算法为所述第一 AMF 与用户设备 UE 协商的 NAS

安全算法；所述第一 AMF 使用所述第二 NAS 安全上下文与所述 UE 进行非接入层 NAS 保护。

本申请实施例提供的切换的处理方法，第一 AMF 进行密钥推演生成了第二 AMF 密钥的情况下，第一 AMF 可以基于第二 AMF 密钥以及与用户设备 UE 协商的第一 NAS 安全算法生成第二 NAS 安全上下文。

结合第三方面，在第三方面的某些实现方式中，所述第二 NAS 安全上下文中包括所述第一 NAS 安全算法、所述第二 AMF 密钥、第二非接入层 NAS 密钥以及第二非接入层计数器 NAS COUNT。

第四方面，提供了一种切换的处理方法，包括：用户设备 UE 接收第一接入网设备发送的切换命令消息，所述切换命令消息携带第二接入管理功能 AMF 选择的第二 NAS 安全算法和 AMF 密钥改变指示；当所述第二 NAS 安全算法与第一 NAS 安全算法不一致且所述 AMF 密钥改变指示为预设值时，所述 UE 保存第一 NAS 安全算法，以及进行密钥推演以获取第二 AMF 密钥；其中，所述第一 NAS 安全算法为所述 UE 与第一接入管理功能 AMF 协商的 NAS 安全算法。

本申请实施例提供的切换的处理方法，通过使得 UE 接收到的切换命令消息中携带的第二 NAS 安全算法和 AMF 密钥改变指示为 1 时，UE 保存第一 NAS 安全算法，并基于 AMF 密钥改变指示进行密钥推演得到第二 AMF 密钥。结合第四方面，在第四方面的某些实现方式中，所述 UE 利用所述第二 AMF 密钥以及所述第一 NAS 安全算法生成第二 NAS 安全上下文。

本申请实施例提供的切换的处理方法，UE 可以利用新生成的第二 AMF 密钥以及保存的第一 NAS 安全算法生成第二 NAS 安全上下文。

结合第四方面，在第四方面的某些实现方式中，当所述 UE 切换失败时，所述 UE 使用所述第二 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 安全保护。

本申请实施例提供的切换的处理方法，UE 切换失败时，UE 使用第二 NAS 安全上下文与第一 AMF 进行非接入层 NAS 安全保护。

结合第四方面，在第四方面的某些实现方式中，当所述 UE 切换失败时，所述 UE 利用所述第二 AMF 密钥以及所述第一 NAS 安全算法生成第二 NAS 安全上下文；所述 UE 使用所述第二 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 安全保护。

本申请实施例提供的切换的处理方法，UE 切换失败时，UE 首先利用新生成的第二 AMF 密钥以及保存的第一 NAS 安全算法生成第二 NAS 安全上下文，再利用第二 NAS 安全上下文与第一 AMF 进行非接入层 NAS 安全保护。

结合第四方面，在第四方面的某些实现方式中，所述 AMF 密钥改变指示为预设值包括：所述 AMF 密钥改变指示为 1。

本申请实施例提供的切换的处理方法，AMF 密钥改变指示为 1 的时候指示进行密钥推演。

第五方面，提供了一种切换的处理装置，该装置可以用来用于执行第一方面和第三方面以及第一方面和第三方面的任意可能的实现方式中的用户设备的操作。具体地，该切换的处理装置可以包括用于执行上述第一方面和第三方面以及第一方面和第三方面的任意可能的实现方式中所描述的步骤或功能相对应的部件（means）可以是第一方面和第三方面

面的用户设备或用户设备内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第六方面，提供了一种切换的处理装置，该装置可以用来用于执行第二方面和第四方面以及第二方面和第四方面的任意可能的实现方式中的第一 AMF 的操作。具体地，该切换的处理装置可以包括用于执行上述第二方面和第四方面以及第二方面和第四方面的任意可能的实现方式中所描述的步骤或功能相对应的部件（means）可以是第二方面和第四方面的第一 AMF 或第一 AMF 内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第七方面，提供了一种通信设备，包括，处理器，收发器，存储器，该存储器用于存储计算机程序，该收发器，用于执行第一至第四方面中任一种可能实现方式中的切换的处理装置方法中的收发步骤，该处理器用于从存储器中调用并运行该计算机程序，使得该通信设备执行第一至第四方面中任一种可能实现方式中的切换的处理装置方法。

可选地，处理器为一个或多个，存储器为一个或多个。

可选地，存储器可以与处理器集成在一起，或者存储器与处理器分离设置。

可选的，收发器包括，发射机（发射器）和接收机（接收器）。

第八方面，提供了一种系统，系统包括第五方面至第六方面提供的切换的处理装置。

第九方面，提供了一种计算机程序产品，计算机程序产品包括：计算机程序（也可以称为代码，或指令），当计算机程序被运行时，使得计算机执行上述第一至第四方面中任一种可能实现方式中的方法。

第十方面，提供了一种计算机可读介质，计算机可读介质存储有计算机程序（也可以称为代码，或指令）当其在计算机上运行时，使得计算机执行上述第一至第四方面中任一种可能实现方式中的方法。

第十一方面，提供了一种芯片系统，包括存储器和处理器，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得安装有该芯片系统的通信设备执行上述第一至第四方面中任一种可能实现方式中的方法。

附图说明

图 1 是适用于本申请实施例的网络架构。

图 2 是一种切换失败流程示意图。

图 3 是另一种切换失败流程示意图。

图 4 是本申请实施例提供的一种切换的处理方法的流程示意图。

图 5 是本申请实施例提供的另一种切换的处理方法的流程示意图。

图 6 为本申请实施例提供的切换的处理装置 10 的示意图。

图 7 是适用于本申请实施例的用户设备 20 的结构示意图。

图 8 为本申请实施例提供的切换的处理装置 30 的示意图。

图 9 是适用于本申请实施例的第一 AMF 40 的结构示意图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

图 1 是适用于本申请实施例的网络架构。如图 1 所示，下面对该网络架构中涉及各个部分分别进行说明。

1、用户设备 110：可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备，以及各种形式的终端，移动台（mobile station, MS），终端（terminal），用户设备（user equipment, UE），软终端等等。例如，水表、电表、传感器等。

2、（无线）接入网络（radio access network, (R)AN）网元 120：用于为特定区域的授权用户设备提供入网功能，并能够根据用户设备的级别，业务的需求等使用不同质量的传输隧道。

10 (R)AN 网元能够管理无线资源，为用户设备提供接入服务，进而完成控制信号和用户设备数据在用户设备和核心网之间的转发，(R)AN 网元也可以理解为传统网络中的基站。

3、用户面网元 130：用于分组路由和转发以及用户面数据的服务质量（quality of service, QoS）处理等。

15 在 5G 通信系统中，该用户面网元可以是用户面功能（user plane function, UPF）网元。在未来通信系统中，用户面网元仍可以是 UPF 网元，或者，还可以有其它的名称，本申请不做限定。

4、数据网络网元 140：用于提供传输数据的网络。

20 在 5G 通信系统中，该数据网络网元可以是数据网络（data network, DN）网元。在未来通信系统中，数据网络网元仍可以是 DN 网元，或者，还可以有其它的名称，本申请不做限定。

5、接入管理网元 150：主要用于移动性管理和接入管理等，可以用于实现移动性管理实体（mobility management entity, MME）功能中除会话管理之外的其它功能，例如，合法监听以及接入授权/鉴权等功能。

25 在 5G 通信系统中，该接入管理网元可以是接入管理功能（access and mobility management function, AMF）网元。在未来通信系统中，接入管理网元仍可以是 AMF，或者，还可以有其它的名称，本申请不做限定。

6、会话管理网元 160：主要用于会话管理、用户设备的网络互连协议（internet protocol, IP）地址分配和管理、选择可管理用户平面功能、策略控制和收费功能接口的终结点以及下行数据通知等。

30 在 5G 通信系统中，该会话管理网元可以是会话管理功能（session management function, SMF）网元。在未来通信系统中，会话管理网元仍可以是 SMF 网元，或者，还可以有其它的名称，本申请不做限定。

7、策略控制网元 170：用于指导网络行为的统一策略框架，为控制面功能网元（例如 AMF, SMF 网元等）提供策略规则信息等。

35 在 4G 通信系统中，该策略控制网元可以是策略和计费规则功能（policy and charging rules function, PCRF）网元。在 5G 通信系统中，该策略控制网元可以是策略控制功能（policy control function, PCF）网元。在未来通信系统中，策略控制网元仍可以是 PCF 网元，或者，还可以有其它的名称，本申请不做限定。

8、认证服务器 180：用于鉴权服务、产生密钥实现对用户设备的双向鉴权，支持统

一的鉴权框架。

在 5G 通信系统中，该认证服务器可以是认证服务器功能（authentication server function, AUSF）网元。在未来通信系统中，认证服务器功能网元仍可以是 AUSF 网元，或者，还可以有其它的名称，本申请不做限定。

5 9、数据管理网元 190：用于处理用户设备标识，接入鉴权，注册以及移动性管理等。

在 5G 通信系统中，该数据管理网元可以是统一数据管理（unified data management, UDM）网元；在 4G 通信系统中，该数据管理网元可以是归属用户服务器（home subscriber server, HSS）网元。在未来通信系统中，统一数据管理仍可以是 UDM 网元，或者，还可以有其它的名称，本申请不做限定。

10 10、应用网元 1100：用于进行应用影响的数据路由，接入网络开放功能网元，与策略框架交互进行策略控制等。

在 5G 通信系统中，该应用网元可以是应用功能（application function, AF）网元。在未来通信系统中，应用网元仍可以是 AF 网元，或者，还可以有其它的名称，本申请不做限定。

15 11、网络存储网元：用于维护网络中所有网络功能服务的实时信息。

在 5G 通信系统中，该网络存储网元可以是网络注册功能（network repository function, NRF）网元。在未来通信系统中，网络存储网元仍可以是 NRF 网元，或者，还可以有其它的名称，本申请不做限定。

可以理解的是，上述网元或者功能既可以是硬件设备中的网络元件，也可以是在专用
20 硬件上运行软件功能，或者是平台（例如，云平台）上实例化的虚拟化功能。为方便说明，本申请后续，以接入管理网元为 AMF，数据管理网元为 UDM 网元，会话管理网元为 SMF 网元，用户面网元为 UPF 网元为例进行说明。

进一步地，将 AMF 简称为 AMF，UDM 网元简称为 UDM，SMF 网元简称为 SMF，UPF 网元简称为 UPF。即本申请后续所描述的 AMF 均可替换为接入管理网元，UDM 均可
25 替换为数据管理网元，SMF 均可替换为会话管理网元，UPF 均可替换为用户面网元。

为方便说明，本申请实施例中以装置为 AMF 实体、UDM 实体为例，对用于会话建立的方法进行说明，对于装置为 AMF 实体内的芯片、UDM 实体内的芯片的实现方法，可参考装置分别为 AMF 实体、UDM 实体的具体说明，不再重复介绍。

在图 1 所示的网络架构中，用户设备通过 N1 接口与 AMF 连接，(R)AN 通过 N2 接口
30 与 AMF 连接，(R)AN 通过 N3 接口与 UPF 连接。UPF 之间通过 N9 接口连接，UPF 通过 N6 接口 DN 互联。SMF 通过 N4 接口控制 UPF。AMF 通过 N11 接口与 SMF 接口。AMF 通过 N8 接口从 UDM 单元获取用户设备签约数据，SMF 通过 N10 接口从 UDM 单元获取用户设备签约数据。

应理解，上述应用于本申请实施例的网络架构仅是一种举例说明，适用本申请实施例
35 的网络架构并不局限于此，任何能够实现上述各个网元的功能的网络架构都适用于本申请实施例。

例如，在某些网络架构中，AMF、SMF 网元、PCF 网元、BSF 网元以及 UDM 网元等网络功能网元实体都称为网络功能（network function, NF）网元；或者，在另一些网络架构中，AMF、SMF 网元、PCF 网元、BSF 网元、UDM 网元等网元的集合都可以称为控

制面功能网元。

本申请实施例的技术方案可以应用于各种通信系统，例如：全球移动通信（global system for mobile communications, GSM）系统、码分多址（code division multiple access, CDMA）系统、宽带码分多址（wideband code division multiple access, WCDMA）系统、通用分组无线业务（general packet radio service, GPRS）、长期演进（long term evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、未来的第五代（5th generation, 5G）系统或新无线（new radio, NR）等。

本申请实施例中的用户设备可以指用户设备、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。用户设备还可以是蜂窝电话、无绳电话、会话启动协议（session initiation protocol, SIP）电话、无线本地环路（wireless local loop, WLL）站、个人数字助理（personal digital assistant, PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，未来 5G 网络中的用户设备或者未来演进的公用陆地移动通信网络（public land mobile network, PLMN）中的用户设备等，本申请实施例对此并不限定。

本申请实施例中的网络设备可以是用于与用户设备通信的设备，该网络设备可以是全球移动通信（global system for mobile communications, GSM）系统或码分多址（code division multiple access, CDMA）中的基站（base t(R)ANsceiver station, BTS），也可以是宽带码分多址（wideband code division multiple access, WCDMA）系统中的基站（NodeB, NB），还可以是 LTE 系统中的演进型基站（evolved NodeB, eNB 或 eNodeB），还可以是云无线接入网络（cloud radio access network, C(R)AN）场景下的无线控制器，或者该网络设备可以为中继站、接入点、车载设备、可穿戴设备以及未来 5G 网络中的网络设备或者未来演进的 PLMN 网络中的网络设备等，本申请实施例并不限定。

在本申请实施例中，用户设备或网络设备包括硬件层、运行在硬件层之上的操作系统层，以及运行在操作系统层上的应用层。该硬件层包括中央处理器（central processing unit, CPU）、内存管理单元（memory management unit, MMU）和内存（也称为主存）等硬件。该操作系统可以是任意一种或多种通过进程（process）实现业务处理的计算机操作系统，例如，Linux 操作系统、Unix 操作系统、Android 操作系统、iOS 操作系统或 windows 操作系统等。该应用层包含浏览器、通讯录、文字处理软件、即时通信软件等应用。并且，本申请实施例并未对本申请实施例提供的方法的执行主体的具体结构特别限定，只要能够通过运行记录有本申请实施例的提供的方法的代码的程序，以根据本申请实施例提供的方法进行通信即可，例如，本申请实施例提供的方法的执行主体可以是用户设备或网络设备，或者，是用户设备或网络设备中能够调用程序并执行程序的功能模块。

另外，本申请的各个方面或特征可以实现成方法、装置或使用标准编程和/或工程技术的制品。本申请中使用的术语“制品”涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。例如，计算机可读介质可以包括，但不限于：磁存储器件（例如，硬盘、软盘或磁带等），光盘（例如，压缩盘（compact disc, CD）、数字通用盘（digital versatile

disc, DVD)等), 智能卡和闪存器件(例如, 可擦写可编程只读存储器(erasable programmable read-only memory, EPROM)、卡、棒或钥匙驱动器等)。另外, 本文描述的各种存储介质可代表用于存储信息的一个或多个设备和/或其它机器可读介质。术语“机器可读介质”可包括但不限于, 无线信道和能够存储、包含和/或承载指令和/或数据的各种其它介质。

5 本申请实施例中主要涉及到图 1 所示的网络架构中的 AMF、UE 以及(R)AN。其中, 针对 AMF 本申请中涉及到第一 AMF (或称为源 AMF (source AMF)) 和第二 AMF (或称为目标 AMF (target AMF)); 针对(R)AN 网元本申请中涉及到第一(R)AN (或称为源(R)AN (source (R)AN)) 网元和第二(R)AN (或称为目标(R)AN (target (R)AN)) 网元。

10 具体地, 本申请中所涉及的第一 AMF 指的是发生切换之前为 UE 提供核心网服务的 AMF; 本申请中所涉及的第二 AMF 指的是发生切换之后选择为 UE 提供核心网服务的 AMF。本申请中所涉及的第一(R)AN 网元指的是第一 AMF 切换之前为 UE 提供接入网服务的(R)AN 网元; 本申请中所涉及的第二(R)AN 网元指的是第二 AMF 切换之后选择为 UE 提供接入网服务的(R)AN 网元。进一步地, 本申请中还可能涉及到 AUSF/UDM, 15 AUSF/UDM 主要用于进行认证。例如, 实现 UE 与网络设备之间的认证。应理解, 本申请主要涉及到切换流程, 对于认证流程并不限制, 下面不再对 UE 与网络设备之间的认证进行描述。

 具体地, 本申请实施例中为了便于描述, 可以将第一(R)AN 网元简称为第一(R)AN、第二(R)AN 网元简称为第二(R)AN。本申请实施例中涉及的切换指的是为 UE 提供接入网服务的(R)AN 网元从第一(R)AN 切换至与第二(R)AN, 而第一(R)AN 与第二(R)AN 之间 20 无法直接建立连接进行信令交互, 第一(R)AN 由第一 AMF 管理、第二(R)AN 由第二 AMF 管理, 则为 UE 提供接入网服务的(R)AN 网元从第一(R)AN 切换至与第二(R)AN 过程中需要经由第一 AMF 和第二 AMF 传递相关的信令。当为 UE 提供接入网服务的(R)AN 网元从第一(R)AN 切换至与第二(R)AN 失败的时候, 一般情况下第一(R)AN 会继续为 UE 提供接入网服务。本申请中将为 UE 提供接入网服务的(R)AN 网元从第一(R)AN 切换至与第二(R)AN 简称为切换, 将为 UE 提供接入网服务的(R)AN 网元从第一(R)AN 切换至与第二(R)AN 失败的情况简称为切换失败。

 进一步地, 在进行切换之前, UE 与网络设备完成认证之后, UE 和第一 AMF 得到相同的 AMF 密钥, 本申请实施例中为了便于描述, 将 UE 与第一 AMF 得到的 AMF 密钥记 30 为 Kamf, Kamf 也可以称为第一 AMF 密钥或者 Kamf1。然后, UE 和第一 AMF 分别基于该 Kamf 以及 UE 与第一 AMF 之间协商的非接入层 (non-access stratum, NAS) 完整性保护算法生成用于 NAS 消息保护的完整性保护密钥; UE 和第一 AMF 基于该 Kamf 以及 UE 与第一 AMF 之间协商的非接入层 (non-access stratum, NAS) 机密性保护算法, 生成用于 NAS 消息保护的机密性保护密钥, 其中, 用于 NAS 消息保护的完整性保护密钥和机密性保护密钥可以统称为 NAS Key。本申请实施例中为了便于描述, 将 UE 与第一 AMF 生成用于 NAS 消息保护的完整性保护密钥记为 Knasint; 将 UE 与第一 AMF 生成用于 NAS 消息保护的机密性保护密钥记为 Knasenc, 可以将 UE 和第一 AMF 基于 Kamf 以及 UE 与第一 AMF 之间协商的 NAS 完整性保护算法和机密性保护算法, 生成用于 NAS 消息保护的完整性保护密钥和机密性保护密钥称为第一 NAS Key; 可以将 UE 与第一 AMF 之间协

商的 NAS 完整性保护算法和机密性保护算法称为第一 NAS 安全算法。

应理解,本申请中对于 UE 与第一 AMF 之间如何协商 NAS 完整性保护算法和机密性保护算法并不限制,可以是现有协议中规定的协商方案。

为了保证切换的业务连续性,在发生上述的切换的时候,第一 AMF 会将与 UE 之间的 UE 的安全上下文传递给第二 AMF。UE 的安全上下文包括上述的 Kamf 或上述 Kamf 经过密钥推演之后的 Kamf' (也可以称为 Kamf2 或第二 AMF 密钥)、第一 AMF 与 UE 之间协商的第一 NAS 安全算法、下行非接入层计数 (downlink non-access stratum count, DL NAS COUNT) 以及 UE 支持的 NAS 安全算法列表等。应理解,第一 AMF 将与 UE 之间的 UE 的安全上下文传递给第二 AMF 为现有协议中切换流程中规定的步骤,本申请对此步骤并不做改进,也就是说第一 AMF 向第二 AMF 发送的 UE 的安全上下文包括的内容可以参考现有协议的规定,这里只做简单的描述。

第二 AMF 利用第一 AMF 所传递的 UE 的安全上下文中包括的 AMF 密钥,以及第二 AMF 与 UE 之间协商的第二 NAS 安全算法生成第三 NAS 安全上下文。第三 NAS 安全上下文包括 Kamf2、Knasint2、Knasenc2 以及 DL NAS COUNT2 等。具体地,第二 AMF 与 UE 之间协商第二 NAS 安全算法包括第二 AMF 从第一 AMF 接收到的 UE 的安全上下文中包括的 UE 支持的 NAS 安全算法列表中选择一个第二 NAS 安全算法,基于选择的第二 NAS 安全算法与接收到的 UE 的安全上下文中包括的密钥 Kamf 或 Kamf' 生成上述新的 NAS 安全上下文。不做特别说明的情况下,本申请中涉及的第二 NAS 安全算法与上述的第一 NAS 安全算法相异。

应理解,与上述的第一 NAS 安全算法类似,第二 NAS 安全算法包括第二 NAS 完整性保护算法和第二 NAS 机密性保护算法,NAS 完整性保护算法用于生成第二完整性保护密钥、NAS 机密性保护算法用于生成第二机密性保护密钥。

具体地,由上述可知第一 AMF 向第二 AMF 发送的 UE 的安全上下文包括以下两种可能的形式:

形式一:第一 AMF 未对 Kamf 进行推演。UE 的安全上下文包括:Kamf、DL NAS COUNT、第一 AMF 与 UE 之间协商的第一 NAS 安全算法以及 UE 支持的 NAS 安全算法列表;

形式二:第一 AMF 对 Kamf 进行了密钥推演,生成了第二 AMF 密钥 Kamf'。UE 的安全上下文包括:Kamf'、DL NAS COUNT、第一 AMF 与 UE 之间协商的第一 NAS 安全算法、UE 支持的 NAS 安全算法列表以及推演指示信息,该推演指示信息用于指示第一 AMF 进行了 AMF 密钥的水平推演。

在形式二下第一 AMF 在将第一 AMF 与 UE 之间的安全上下文传递给第二 AMF 之前,第一 AMF 根据第一 AMF 本地的策略对上述的 Kamf 进行密钥推演,生成密钥推演之后的密钥 Kamf'。应理解,本申请实施例中涉及到对密钥进行密钥推演生成第二密钥所使用的密钥推演的机制和参数不做限制,只限制生成的第二密钥不能进行密钥推演得到被推演的密钥;或者,可以称第二密钥和被推演的密钥之间是隔离的。

作为一种可能的实现方式,本申请中所述的密钥推演可以为现有协议中定义的水平密钥推演;

例如,Kamf 经过水平密钥推演生成为 Kamf' 的方式为:

$Kamf' = \text{HMAC-SHA-256}(\text{Key}, S);$
 $FC = 0x72;$
 $P0 = 0x01;$
 $L0 = \text{length of } P0 \text{ (i.e. } 0x00 \text{ } 0x01);$
5 $P1 = \text{DL NAS COUNT};$
 $L1 = \text{length of } P1 \text{ (i.e. } 0x00 \text{ } 0x04);$
 $\text{KEY} = \text{Kamf};$
 $S = FC || P0 || L0 || P1 || L1.$

作为另一种可能的实现方式，本申请中所述的密钥推演可以为不同的网元之间约定的
 10 密钥推演方式。例如，第一 AMF 和第二 AMF 之间约定密钥推演方式为预设的密钥推演
 方式，只要第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括上述的推演指示信息，
 第二 AMF 能够确定接收到的 UE 的安全上下文中的密钥是第一 AMF 通过预设的密钥推演
 方式进行密钥推演得到的。

具体地，由上述可知第二 AMF 利用第一 AMF 所传递的 UE 的安全上下文，以及第二
 15 AMF 与 UE 之间协商第二 NAS 安全算法生成新的 NAS 安全上下文包括以下两种可能的
 形式：

形式一：对应于上述的形式一第一 AMF 未对 Kamf 进行推演。新的 NAS 安全上下文
 包括：Kamf2、Knasint2、Knasenc2 以及 DL NAS COUNT2，其中，Kamf2 为上述的 Kamf。

一种可能的实现方式是，第二 AMF 与 UE 之间协商的 NAS 完整性保护算法和机密性
 20 保护算法，与第一 AMF 与 UE 之间协商的 NAS 完整性保护算法和机密性保护算法一致，
 则第二 AMF 基于该 Kamf 以及 UE 与第二 AMF 之间协商的 NAS 完整性保护算法和机密
 性保护算法，生成用于 NAS 消息保护的完整性保护密钥和机密性保护密钥 Knasint2 和
 Knasenc2 为上述的 Knasint 和 Knasenc；

另一种可能的实现方式是，第二 AMF 与 UE 之间协商的 NAS 完整性保护算法和机密
 25 性保护算法，与第一 AMF 与 UE 之间协商的 NAS 完整性保护算法和机密性保护算法不一
 致，则第二 AMF 基于该 Kamf 以及 UE 与第二 AMF 之间协商的 NAS 完整性保护算法和
 机密性保护算法，生成用于 NAS 消息保护的完整性保护密钥和机密性保护密钥 Knasint2
 和 Knasenc2 与上述的 Knasint 和 Knasenc 不同。

形式二：对应于上述的形式二第一 AMF 对 Kamf 进行了推演。新的 NAS 安全上下文
 30 包括：Kamf'、Knasint2、Knasenc2、DL NAS COUNT 以及推演指示信息，该推演指示信
 息用于指示 Kamf' 为经过推演之后的 AMF 密钥。

其中，Knasint2 和 Knasenc2 为第二 AMF 基于 Kamf' 以及 UE 与第二 AMF 之间协商
 的 NAS 完整性保护算法和机密性保护算法，生成用于 NAS 消息保护的完整性保护密钥和
 机密性保护密钥。

35 在形式二下第二 AMF 收到了推演指示信息，也会向 UE 发送该推演指示信息，该推
 演指示信息用于指示 UE 对 Kamf 进行推演，保证 UE 和网络侧的 Kamf' 保持一致。

应理解，第二 AMF 在收到第一 AMF 发送的 Kamf 或 Kamf' 之后，结合第二 AMF 与
 UE 之间的算法协商，根据自身选择的 NAS 安全算法（包括完整性保护算法和机密性保护
 算法）以及收到的 Kamf 或 Kamf'，生成第二 AMF 与 UE 之间的 NAS Key（Knasenc2 和

Knasint2)。UE 侧也会进行相同的计算,最终 UE 侧和第二 AMF 侧的 AMF 密钥以及 NAS Key 达成一致。

当上述的切换失败的情况下,只能保证 UE 和第二 AMF 上的 AMF 密钥以及 NAS Key 达成一致,不能保证在发生切换失败的时候,UE 和第一 AMF 上的 NAS Key 是一致的。

- 5 下面结合图 2 和图 3 分别简单介绍切换失败过程中上述第一 AMF 对 Kamf 进行推演和第一 AMF 不对 Kamf 进行推演,但是第一 AMF 与第二 AMF 支持的 NAS 安全算法不一致时,UE 和第一 AMF 上的 AMF 密钥以及 NAS Key 不一致的情况。

图 2 是一种切换失败流程示意图。包括 UE、第一 AMF、第二 AMF、第一(R)AN、第二(R)AN 以及 S1-S11。下面详细介绍图 2 所示的方法流程。

- 10 在进行切换之前 UE 和第一 AMF 上的 AMF 密钥以及 NAS Key 为 Kamf、Knasenc 和 Knasint, DL NAS COUNT=X。

S1, 第一(R)AN 向第一 AMF 发送切换请求消息。

- 该切换请求消息用于指示需要进行接入网设备切换。其中,切换请求消息可以称为 handover required。应理解,本申请中对于第一(R)AN 向第一 AMF 发送的切换请求消息并不做改进,参照现有协议中对于切换请求消息的规定即可。
- 15

S2, 第一 AMF 进行密钥推演。

图 2 所示的切换失败流程中,第一 AMF 在接收到第一(R)AN 发送的切换请求消息之后,确定需要进行接入网设备切换。第一 AMF 对本地的第一 AMF 密钥 Kamf 进行密钥推演得到第二 AMF 密钥 Kamf'。

- 20 应理解,第一 AMF 执行 S2 之后,第一 AMF 上的 AMF 密钥以及 NAS Key 为 Kamf'、Knasenc 和 Knasint。

S3, 第一 AMF 向第二 AMF 发送 UE 的安全上下文。

- UE 的安全上下文中包括上述的 Kamf'、Knasenc 和 Knasint 以及 DL NAS COUNT=X+1。其中,第一 AMF 向第二 AMF 发送 UE 的安全上下文可以是第一 AMF 向第二 AMF 发起 UE 上下文创建服务请求,该 UE 上下文创建服务请求可以称为 create UE context request。应理解,本申请中对于第一 AMF 向第二 AMF 发送 UE 的安全上下文并不做改进,参照现有协议中对于第一 AMF 向第二 AMF 发送 UE 的安全上下文的规定即可。
- 25

S4, 第二 AMF 生成新的 NAS 安全上下文。

- 新的 NAS 安全上下文包括上述的第二 AMF 接收到的 Kamf'、第二 AMF 结合第二 AMF 与 UE 之间协商的第二 NAS 安全算法,生成第二 AMF 与 UE 之间的 NAS Key (Knasenc2 和 Knasint2) 和 DL NAS COUNT=0,其中,Knasenc2 和 Knasint2 与 Knasenc 和 Knasint 相异。
- 30

S5, 第二 AMF 向第二(R)AN 发送切换请求。

- 该切换请求用于获取第二(R)AN 的相关信息。其中,该切换请求可以称为 handover request。应理解,本申请中对于第二 AMF 向第二(R)AN 发送切换请求并不做改进,参照现有协议中对于第二 AMF 向第二(R)AN 发送切换请求的规定即可。
- 35

S6, 第二(R)AN 向第二 AMF 发送切换请求响应。

该切换请求响应用于通知第二 AMF,该第二(R)AN 的相关信息。其中,该切换请求响应可以称为 handover request acknowledge。应理解,本申请中对于第二(R)AN 向第二 AMF

发送切换请求响应并不做改进，参照现有协议中对于第二(R)AN 向第二 AMF 发送切换请求响应的规定即可。

S7，第二 AMF 向第一 AMF 发送 UE 上下文创建服务请求响应。

该 UE 上下文创建服务请求响应用于通知第一 AMF 第二(R)AN 的相关信息。其中，
5 该 UE 上下文创建服务请求响应可以称为 create UE context response。应理解，本申请中对于第二 AMF 向第一 AMF 发送 UE 上下文创建服务请求响应并不做改进，参照现有协议中对于第二 AMF 向第一 AMF 发送 UE 上下文创建服务请求响应的规定即可。

S8，第一 AMF 向第一(R)AN 发送切换命令消息。

该切换命令消息用于通知第一(R)AN，第二(R)AN 的相关信息。其中，该切换命令消息
10 可以称为 handover command。应理解，本申请中对于第一 AMF 向第一(R)AN 发送切换命令消息并不做改进，参照现有协议中对于第一 AMF 向第一(R)AN 发送切换命令消息的规定即可。

S9，第一(R)AN 向 UE 发送切换命令消息。

该切换命令消息用于通知 UE 第二(R)AN 的相关信息。其中，该切换命令消息可以称
15 为 handover command。应理解，本申请中对于第一(R)AN 向 UE 发送切换命令消息并不做改进，参照现有协议中对于第一(R)AN 向 UE 发送切换命令消息的规定即可。

S10，UE 生成新的 NAS 安全上下文。

新的 NAS 安全上下文包括上述的 K_{amf}^* 、UE 结合第二 AMF 与 UE 之间协商的第二 NAS 安全算法生成第二 AMF 与 UE 之间的 NAS Key ($K_{nasenc2}$ 和 $K_{nasint2}$)，DL NAS
20 COUNT=0。

UE 执行 S10 之后，UE 上的 AMF 密钥以及 NAS Key 为 K_{amf}^* 、 $K_{nasenc2}$ 和 $K_{nasint2}$ 。

当 UE 因为某些原因导致切换失败（比如第二(R)AN 信号变差，或者，UE 对接收到的 NASC 完整性校验失败）发生 S11，切换失败的情况时，此时 UE 需要回到第一 AMF 处进行服务。但是如果在切换阶段，第一 AMF 进行了 K_{amf} 的推演，由于 UE 上的 NAS Key
25 和第一 AMF 上的 NAS Key 不一致，导致后续 UE 与第一 AMF 的 NAS 消息无法进行安全保护。

图 3 是另一种切换失败流程示意图。包括 UE、第一 AMF、第二 AMF、第一(R)AN、第二(R)AN 以及 S20-S29。下面详细介绍图 3 所示的方法流程。

在进行切换之前 UE 和第一 AMF 上的 AMF 密钥以及 NAS Key 为 K_{amf} 、 K_{nasenc} 和
30 K_{nasint} ，DL NAS COUNT=X。

S20，第一(R)AN 向第一 AMF 发送切换请求消息。

该切换请求消息用于指示需要进行切换。与图 2 中所示的第一(R)AN 向第一 AMF 发送的切换请求消息类似，这里不再赘述。

S21，第一 AMF 向第二 AMF 发送 UE 的安全上下文。

UE 的安全上下文中包括上述的 K_{amf} 、 K_{nasenc} 和 K_{nasint} 以及 DL NAS
35 COUNT=X+1。

S22，第二 AMF 确定新的 NAS 安全上下文。

新的 NAS 安全上下文包括上述的第二 AMF 接收到的 K_{amf} 、第二 AMF 结合第二 AMF 与 UE 之间协商的第二 NAS 安全算法，生成第二 AMF 与 UE 之间的 NAS Key ($K_{nasenc2}$

和 Knasint2) 和 $\text{DL NAS COUNT} = X+1$, 其中, Knasenc2 和 Knasint2 与 Knasenc 和 Knasint 相异。

S23, 第二 AMF 向第二(R)AN 发送切换请求。

该切换请求用于获取第二(R)AN 的相关信息。

5 S24, 第二(R)AN 向第二 AMF 发送切换请求响应。

该切换请求响应用于通知第二 AMF, 该第二(R)AN 的相关信息。

S25, 第二 AMF 向第一 AMF 发送 UE 上下文创建服务请求响应。

该 UE 上下文创建服务请求响应用于通知第一 AMF 第二(R)AN 的相关信息。

S26, 第一 AMF 向第一(R)AN 发送切换命令消息。

10 该切换命令消息用于通知第一(R)AN, 第二(R)AN 的相关信息。

S27, 第一(R)AN 向 UE 发送切换命令消息。

该切换命令消息用于通知 UE 第二(R)AN 的相关信息。

S28, UE 生成新的 NAS 安全上下文。

新的 NAS 安全上下文包括上述的 Kamf 、UE 结合第二 AMF 与 UE 之间协商的第二
15 NAS 安全算法生成第二 AMF 与 UE 之间的 NAS Key (Knasenc2 和 Knasint2), $\text{DL NAS COUNT} = X+1$ 。

UE 执行 S28 之后, UE 上的 AMF 密钥以及 NAS Key 为 Kamf 、 Knasenc2 和 Knasint2 。

当 UE 因为某些原因导致切换失败 (比如第二(R)AN 信号变差) 发生 S29, 切换失败的情况时, 此时 UE 需要回到第一 AMF 处进行服务。但是如果在切换阶段, 第二(R)AN
20 选择与上述第一 NAS 安全算法相异的第二 NAS 安全算法, UE 基于 Kamf 和第二 NAS 安全算法生成的 Knasenc2 和 Knasint2 与上述的 Knasenc 和 Knasint 相异, 则 UE 上的 NAS Key 和第一 AMF 上的 NAS Key 不一致, 导致后续 UE 与第一 AMF 的 NAS 消息无法进行安全保护。

为了避免图 2 和图 3 所示的方法流程中出现的 UE 上的 NAS Key 和第一 AMF 上的
25 NAS Key 不一致, 本申请提出一种切换的处理方法, 通过保证 UE 与第一 AMF 上采用的 NAS 安全上下文一致, 使得 UE 上的 NAS Key 和第一 AMF 上的 NAS Key 一致。下面结合图 4 和图 5 详细介绍本申请实施例提供的切换的处理方法。

图 4 是本申请实施例提供的一种切换的处理方法的流程示意图。该示意图包括 UE、
30 第一 AMF、第二 AMF、第一(R)AN、第二(R)AN 以及 S110-S140。下面详细介绍图 4 所示的方法流程。

在进行切换之前 UE 和第一 AMF 上的 NAS 安全上下文包括上述的 Kamf (第一 AMF 密钥 Kamf1)、 Knasenc 、 Knasint (Knasenc 和 Knasint 统称为第一非接入层 NAS 密钥)、
35 $\text{DL NAS COUNT} = X$ (第一非接入层计数器 NAS COUNT) 以及 UE 与第一 AMF 之间协商的 NAS 安全算法 (第一 NAS 安全算法) 等。图 4 所示的实施例中称切换之前 UE 和第一 AMF 上的 NAS 安全上下文为第一 NAS 安全上下文。

S110, 第一 AMF 确定需要进行密钥推演, 保存第一 NAS 安全上下文。

一种可能的实现方式, 第一 AMF 进行密钥推演之前保存第一 NAS 安全上下文;

另一种可能的实现方式, 第一 AMF 进行密钥推演之后保存第一 NAS 安全上下文;

本申请中对于第一 AMF 进行密钥推演和第一 AMF 保存第一 NAS 安全上下文的先后

关系不做严格的限制。具体地，第一 AMF 在执行 S110 之前，图 4 所示的实施例还包括 S111，第一(R)AN 向第一 AMF 发送切换请求消息。图 4 所示的实施例中，第一(R)AN 向第一 AMF 发送切换请求消息与图 2 中 S1 类似，这里不再赘述。

具体地，图 4 所示的实施例中第一 AMF 接收到切换请求消息之后，保存第一 NAS 安全上下文包括以下两种可能：

可能一：第一 AMF 不对第一 NAS 安全上下文中包括的密钥 Kamf 进行密钥推演，则第一 AMF 确定保存第一 NAS 安全上下文，与现有图 2 所示的流程一致。

可能二：第一 AMF 根据本地策略确定需要对第一 NAS 安全上下文中包括的密钥 Kamf 进行密钥推演，图 4 所示的实施例中还包括 S112，第一 AMF 进行密钥推演。

具体地，第一 AMF 将第一 NAS 安全上下文保存之后，第一 AMF 进行密钥推演将第一密钥 Kamf 进行密钥推演得到第二密钥 Kamf'。应理解，本申请实施例中对于第一 AMF 进行密钥推演的过程并不限制，可以是现有协议中规定的第一 AMF 进行密钥推演的流程。第一 AMF 进行密钥推演生成推演之后的 Kamf'，图 4 所示的实施例中称之为第一密钥。图 4 所示的实施例中主要介绍与现有流程不一致的可能二，对于与现有流程一致的可能一只进行简单描述。

S113，第一 AMF 向第二 AMF 发送 UE 的安全上下文。

具体地，第一 AMF 将 UE 的安全上下文发送给第二 AMF 可以是第一 AMF 向第二 AMF 发起 UE 上下文创建服务请求。对应于 S110 中的可能一和可能二，第一 AMF 向第二 AMF 发送的 UE 的安全上下文也包括以下两种可能：

可能一：第一 AMF 不对第一 NAS 安全上下文中包括的第一密钥 Kamf 进行密钥推演，则第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括 Kamf、DL NAS COUNT=X+1、UE 与第一 AMF 之间协商的 NAS 安全算法和 UE 支持的 NAS 安全算法列表；

可能二：第一 AMF 对第一 NAS 安全上下文中包括的第一密钥 Kamf 进行密钥推演，则第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括 Kamf'、DL NAS COUNT=X+1、UE 与第一 AMF 之间协商的 NAS 安全算法、UE 支持的 NAS 安全算法列表以及密钥推演指示，该密钥推演指示用于指示第一 AMF 向第二 AMF 发送的 UE 的安全上下文中的密钥为第一 AMF 经过密钥推演得到的。其中，密钥推演指示可以称为 K_AMF_change_flag，具体地 K_AMF_change_flag 的值为 1 表示指示第一 AMF 向第二 AMF 发送的 UE 的安全上下文中的密钥为第一 AMF 经过密钥推演得到。

图 4 所示的实施例中，第二 AMF 接收到第一 AMF 发送的 UE 的安全上下文之后，执行 S114，第二 AMF 生成第三 NAS 安全上下文。对应于 S113 中的可能一和可能二，第二 AMF 生成第三 NAS 安全上下文也包括以下两种可能：

可能一：第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括的密钥为 Kamf。

第二 AMF 基于接收到第一 AMF 发送的 UE 的安全上下文中的密钥 Kamf 以及从 UE 支持的 NAS 安全算法列表中选择一种 NAS 安全算法，生成用于 NAS 消息保护的完整性保护密钥和机密性保护密钥 Knasint2 和 Knasenc2。第二 AMF 生成第三 NAS 安全上下文中包括 Kamf、Knasint2、Knasenc2、DL NAS COUNT=X+1、UE 与第二 AMF 之间协商的 NAS 安全算法。

一种可能的实现方式，第二 AMF 从 UE 支持的 NAS 安全算法列表中选择的一种 NAS

安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法相同, 则 Knasint2、Knasenc2 与上述的 Knasint、Knasenc 相同, 在该实现方式下, 不会发生切换失败时, UE 和第一 AMF 上的 AMF 密钥和 NSA Key 不一致的情况。

另一种可能的实现方式, 第二 AMF 从 UE 支持的 NAS 安全算法列表中选择的一种 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法不同, 则 Knasint2、Knasenc2 与上述的 Knasint、Knasenc 不同, 在该实现方式为图 3 中所示的情况, UE 和第一 AMF 上的 NSA Key 不一致。

可能二: 第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括的密钥为 Kamf'。

第二 AMF 基于接收到第一 AMF 发送的 UE 的安全上下文中的密钥 Kamf' 以及从 UE 支持的 NAS 安全算法列表中选择一种 NAS 安全算法, 生成用于 NAS 消息保护的完整性保护密钥和机密性保护密钥 Knasint2 和 Knasenc2。第二 AMF 生成第三 NAS 安全上下文中包括 Kamf'、Knasint2、Knasenc2、DL NAS COUNT=X+1 或 DL NAS COUNT=0、UE 与第二 AMF 之间协商的 NAS 安全算法以及上述密钥推演指示。

一种可能的实现方式, 第二 AMF 从 UE 支持的 NAS 安全算法列表中选择的一种 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法相同, 由于密钥不一致, 则 Knasint2、Knasenc2 与上述的 Knasint、Knasenc 仍然不同, 在该实现方式为图 2 中所示的情况, UE 和第一 AMF 上的 AMF 密钥和 NSA Key 不一致。

另一种可能的实现方式, 第二 AMF 从 UE 支持的 NAS 安全算法列表中选择的一种 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法不同, 由于密钥和 NAS 安全算法均不一致, 则 Knasint2、Knasenc2 与上述的 Knasint、Knasenc 不同, 在该实现方式为图 2 中所示的情况, UE 和第一 AMF 上的 AMF 密钥和 NSA Key 不一致。

进一步地, 第二 AMF 生成第三 NAS 安全上下文之后, 基于该第三 NAS 安全上下文确定非接入层容器 NASC (non-access stratum container, NASC), 即图 4 所示的实施例还包括 S115, 第二 AMF 确定 NASC。对应于 S114 中的可能一和可能二, 第二 AMF 确定 NASC 也包括以下两种可能:

可能一: 第三 NAS 安全上下文中包括 Kamf'、Knasint2、Knasenc2、DL NAS COUNT=X+1、UE 与第二 AMF 之间协商的 NAS 安全算法。则 NASC 中包括 COUNT=X+1 以及 UE 与第二 AMF 之间协商的 NAS 安全算法。

可能二: 第三 NAS 安全上下文中包括 Kamf'、Knasint2、Knasenc2、DL NAS COUNT=X+1 或 DL NAS COUNT=0、UE 与第二 AMF 之间协商的 NAS 安全算法以及上述密钥推演指示。则 NASC 中包括 DL NAS COUNT=X+1 或 DL NAS COUNT=0、UE 与第二 AMF 之间协商的 NAS 安全算法以及上述密钥推演指示。

应理解, 第二 AMF 需要将上述的 NASC 发送给 UE, 具体地发送给 UE 需要经由第二(R)AN、第一 AMF 以及第一(R)AN 的转发, 本申请实施例中对于上述的 NASC 如何发送至 UE 并不限制, 参照现有协议中的规定即可, 例如, 图 4 所示的实施例还包括:

S116, 第二 AMF 向第二(R)AN 发送切换请求。

该切换请求用于获取第二(R)AN 的相关信息。

S117, 第二(R)AN 向第二 AMF 发送切换请求响应。

该切换请求响应用于通知第二 AMF, 该第二(R)AN 的相关信息。

S118, 第二 AMF 向第一 AMF 发送 UE 上下文创建服务请求响应。

UE 上下文创建服务请求响应中携带上述的 NASC。

S119, 第一 AMF 向第一(R)AN 发送切换命令消息。

该切换命令消息中携带上述的 NASC。

5 S1191, 第一(R)AN 向 UE 发送切换命令消息。

该切换命令消息中携带上述的 NASC。

可选地, 图 4 所示的实施例中还包括 S120, 第一 AMF 恢复使用第一 NAS 安全上下文。

一种可能的实现方式, 第一 AMF 收到 S110 中所示的切换请求消息后, 对应于 S110
10 中的可能二, 第一 AMF 进行了密钥推演, 在第一 AMF 将水平推演后的 Kamf 发送给第二 AMF 上述 UE 的上下文之后的任意时刻第一 AMF 删除第二 Kamf, 恢复使用第一 NAS 安全上下文;

另一种可能的实现方式, 第一 AMF 执行上述的 S110 保存了第一 NAS 安全上下文之后, 并且进行密钥推演生成了第四 NAS 安全上下文之后, 第一 AMF 设置标识位区分第一
15 NAS 安全上下文和第四 NAS 安全上下文, 也就是说第一 AMF 可以在发送给第二 AMF 上述 UE 的上下文之前或者同时恢复使用第一 NAS 安全上下文。

S130, UE 保存第一 NAS 安全上下文。

UE 收到第一(R)AN 发送的切换命令消息, 获取到 NASC 之后, UE 对该 NASC 进行完整性验证, NASC 的完整性验证通过之后, 若 NASC 中的 UE 与第二 AMF 之间协商的
20 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法不一致, 和/或, NASC 中携带 K_AMF_change_flag=1, 则 UE 保存第一 NAS 安全上下文, K_AMF_change_flag 可以称为 AMF 密钥改变指示或密钥推演指示。

UE 保存了第一 NAS 安全上下文之后, 基于 NASC 中的信息更新第一 NAS 安全上下文得到第三 NAS 安全上下文, 执行 S131。

25 S140, UE 恢复使用第一 NAS 安全上下文。

在 UE 发现切换失败时, UE 恢复 S130 保存的第一 NAS 安全上下文。

可选地, UE 删除第三 NAS 安全上下文。

作为另一种可能的实现方式, UE 不执行上述的 S130、S131 和 S140。而是执行 S132, 继续使用第一 NAS 安全上下文。

30 UE 收到第一(R)AN 发送的切换命令消息, 获取到 NASC 之后, UE 对该 NASC 进行完整性验证, NASC 的完整性验证失败之后, UE 继续使用当前使用的第一 NAS 安全上下文。

本申请实施例中涉及的 NAS 安全上下文主要包括: 密钥标识符 ngKSI、AMF 密钥、NAS Key、DL NAS count、UL NAS count 以及 NAS 安全算法等。其中, 密钥标识符用来
35 指示 AMF 密钥, DL NAS count 和 UL NAS count 分别是下行和上下 NAS 计数器。上述描述的 NAS 安全上下文中包括的内容只是简单的描述, 并不能以此限制本申请的保护范围。

综上所述, 图 4 所示的实施例中, 在切换失败的情况下, UE 和第一 AMF 均退回到使用第一 NAS 安全上下文进行 NAS 安全保护, 进而到达 UE 和第一 AMF 使用的 AMF 密钥和 NAS 密钥一致的目的。

图 5 是本申请实施例提供的另一种切换的处理方法的流程示意图。该示意图包括 UE、第一 AMF、第二 AMF、第一(R)AN、第二(R)AN 以及 S210-S240。下面详细介绍图 5 所示的方法流程。

在进行切换之前 UE 和第一 AMF 上的 NAS 安全上下文包括上述的 Kamf、Knasenc、Knasint、DL NAS COUNT=X 以及 UE 与第一 AMF 之间协商的 NAS 安全算法等。图 4 所示的实施例中称切换之前 UE 和第一 AMF 上的 NAS 安全上下文为第一 NAS 安全上下文。

S211, 第一(R)AN 向第一 AMF 发送切换请求消息。

图 5 所示的实施例中, 第一(R)AN 向第一 AMF 发送切换请求消息与图 2 中 S1 类似, 这里不再赘述。

10 S212, 第一 AMF 向第二 AMF 发送 UE 的安全上下文。

具体地, 第一 AMF 将 UE 的安全上下文发送给第二 AMF 可以是第一 AMF 向第二 AMF 发起 UE 上下文创建服务请求。包括以下两种可能:

可能一: 第一 AMF 不对第一 NAS 安全上下文中包括的密钥 Kamf 进行密钥推演, 则第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括 Kamf、DL NAS COUNT=X+1、
15 UE 与第一 AMF 之间协商的 NAS 安全算法和 UE 支持的 NAS 安全算法列表;

可能二: 第一 AMF 对第一 NAS 安全上下文中包括的密钥 Kamf 进行密钥推演, 则第一 AMF 向第二 AMF 发送的 UE 的安全上下文中包括 Kamf'、DL NAS COUNT=X+1、UE 与第一 AMF 之间协商的 NAS 安全算法、UE 支持的 NAS 安全算法列表以及密钥推演指示, 该密钥推演指示用于指示第一 AMF 向第二 AMF 发送的 UE 的安全上下文中的密钥为
20 第一 AMF 经过密钥推演得到的。其中, 密钥推演指示可以称为 K_AMF_change_flag, 具体地 K_AMF_change_flag 的值为 1 表示指示第一 AMF 向第二 AMF 发送的 UE 的安全上下文中的密钥为第一 AMF 经过密钥推演得到。

图 5 所示的实施例中, 第二 AMF 接收到第一 AMF 发送的 UE 的安全上下文之后, 执行 S213, 第二 AMF 生成第三 NAS 安全上下文。具体地, 图 5 所示的实施例中, 第二 AMF
25 生成第三 NAS 安全上下文与图 4 所示的实施例中第二 AMF 生成第三 NAS 安全上下文类似, 这里不再赘述。

进一步地, 第二 AMF 生成第三 NAS 安全上下文之后, 基于该新的 NAS 安全上下文确定 NASC, 即图 5 所示的实施例还包括 S214, 第二 AMF 确定 NASC。具体地, 图 5 所示的实施例中, 第二 AMF 确定 NASC 与图 4 所示的实施例中第二 AMF 确定 NASC 类似,
30 这里不再赘述。

应理解, 第二 AMF 需要将上述的 NASC 发送给 UE, 具体地发送给 UE 需要经由第二(R)AN、第一 AMF 以及第一(R)AN 的转发, 本申请实施例中对于上述的 NASC 如何发送至 UE 并不限制, 参照现有协议中的规定即可, 与图 4 所示的实施例中第二 AMF 将上述的 NASC 发送给 UE 类似, 这里不再赘述。

35 S210, UE 保存第一 NAS 安全上下文。

UE 收到第一(R)AN 发送的切换命令消息, 获取到 NASC 之后, UE 首先保存第一 NAS 安全上下文之后, 再基于 NASC 中的信息更新第一 NAS 安全上下文得到第三 NAS 安全上下文, 执行 S211。

S220, UE 生成第二 NAS 安全上下文。

UE 在发现切换失败时，UE 生成第三 NAS 安全上下文包括以下几种可能：

可能一： NASC 中的 UE 与第二 AMF 之间协商的 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法不一致且 NASC 中携带 K_AMF_change_flag=1。NASC 中携带 K_AMF_change_flag=1 指的是 UE 需要进行密钥推演得到 Kamf'。

5 UE 对 Kamf 进行密钥推演，得到 Kamf'。进一步地 UE 根据第二密钥 Kamf' 和保存的第一 NAS 安全上下文中 UE 与第一 AMF 之间的 NAS 安全算法，生成第二 NAS 安全上下文。然后删除第一 NAS 安全上下文以及与 S211 中生成的第三 NAS 安全上下文，开始使用第二 NAS 安全上下文与第一 AMF 进行 NAS 保护。

10 可能二： NASC 中的 UE 与第二 AMF 之间协商的 NAS 安全算法与 UE 与第一 AMF 之间协商的 NAS 安全算法不一致。

UE 使用第一 NAS 安全上下文与第一 AMF 进行 NAS 保护，与图 4 所示的实施例类似。

可能三： NASC 中携带 K_AMF_change_flag=1。

15 UE 对 Kamf 进行密钥推演，得到 Kamf'。进一步地 UE 根据第二密钥 Kamf' 和保存的第一 NAS 安全上下文中 UE 与第一 AMF 之间的 NAS 安全算法，生成第二 NAS 安全上下文。然后删除第一 NAS 安全上下文以及与 S211 中生成的第三 NAS 安全上下文，开始使用第二 NAS 安全上下文与第一 AMF 进行 NAS 保护。

进一步地，UE 发现切换失败之后，需要经由第一(R)AN 通知第一 AMF 取消切换，则图 5 所示的方法流程中，还包括 S221，第一(R)AN 向第一 AMF 发送切换取消请求。

20 S230，第一 AMF 生成第二 NAS 安全上下文。

第一 AMF 侧在收到切换取消请求后，生成第二 NAS 安全上下文包括以下两种可能：

可能一：第一 AMF 在 S212 之前对 Kamf 进行了密钥推演，得到了第二密钥 Kamf'。则第一 AMF 侧在收到切换取消请求后根据 Kamf' 以及第一 NAS 安全上下文中 UE 与第一 AMF 之间的 NAS 安全算法，生成第二 NAS 安全上下文。然后利用第二 NAS 安全上下文与 UE 进行 NAS 安全保护。图 5 所示的实施例主要考虑可能一，第一 AMF 生成了第二 NAS 安全上下文。

可能二：第一 AMF 在 S212 之前未对 Kamf 进行了密钥推演。则第一 AMF 侧在收到切换取消请求后使用第一 NAS 安全上下文与第一 AMF 进行 NAS 保护，与图 4 所示的实施例类似。

30 综上所述，图 5 所示的实施例中，在切换失败的情况下，UE 和第一 AMF 均使用第二 NAS 安全上下文进行 NAS 安全保护，进而到达 UE 和第一 AMF 使用的 NAS 密钥一致的目的。

35 应理解，上述各个方法实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

还应理解本申请中的“第一”、“第二”仅用于区分说明，而不应对本申请构成任何限定。其中，第一 NAS 安全上下文、第二 NAS 安全上下文只是用于区分不同的 NAS 安全上下文。

上面结合图 4 和图 5 详细介绍了本申请实施例提供的切换的处理方法，下面结合图

6-图 9 详细介绍本申请实施例提供的切换的处理装置。

参见图 6，图 6 是本申请提出的切换的处理装置 10 的示意图。如图 6 所示，装置 10 包括接收单元 110 和处理单元 120。

接收单元 110，用于接收第一接入网设备发送的切换命令消息，所述切换命令消息携带第二接入管理功能 AMF 选择的第二 NAS 安全算法和 AMF 密钥改变指示；

处理单元 120，用于当所述第二 NAS 安全算法与所述 UE 当前使用的第一 NAS 安全算法不一致和/或所述 AMF 密钥改变指示为 1 时，所述 UE 保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下文为所述 UE 和第一 AMF 协商生成的 NAS 安全上下文；

所述处理单元 120，还用于切换失败时，使用所述第一 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 保护。

装置 10 和方法实施例中的用户设备完全对应，装置 10 可以是方法实施例中的用户设备，或者方法实施例中的用户设备内部的芯片或功能模块。装置 10 的相应单元用于执行图 4 和图 5 所示的方法实施例中由用户设备执行的相应步骤。

其中，装置 10 中的接收单元 110 执行方法实施例中用户设备接收的步骤。例如，执行图 4 中接收第一(R)AN 发送切换命令消息的步骤 1191、执行图 5 中接收第一(R)AN 发送切换命令消息的步骤 219。

处理单元 120 执行方法实施例中用户设备内部实现或处理的步骤。例如，执行图 4 中保存第一 NAS 安全上下文的步骤 130、执行图 4 中生成第三 NAS 安全上下文的步骤 131、执行图 4 中恢复使用第一 NAS 安全上下文的步骤 140、或者，执行图 4 中继续使用第一 NAS 安全上下文的步骤 132、执行图 5 中保存第一 NAS 安全上下文的步骤 210、执行图 5 中生成第三 NAS 安全上下文的步骤 211、执行图 5 中生成第二 NAS 安全上下文的步骤 220。

装置 10 中所示的切换的处理装置还可能包括发送单元（图 6 中并未示出），发送单元用于执行向其他设备发送消息的功能，接收单元 110 和发送单元可以组成收发单元，同时具有接收和发送的功能。其中，处理单元 120 可以是处理器。发送单元可以是接收器。接收单元 110 可以是发射器。接收器和发射器可以集成在一起组成收发器。

参见图 7，图 7 是适用于本申请实施例的用户设备 20 的结构示意图。该用户设备 20 可应用于图 1 所示出的系统中。为了便于说明，图 7 仅示出了用户设备的主要部件。如图 7 所示，用户设备 20 包括处理器、存储器、控制电路、天线以及输入输出装置。处理器用于控制天线以及输入输出装置收发信号，存储器用于存储计算机程序，处理器用于从存储器中调用并运行该计算机程序，以执行本申请提出的切换的处理方法中由用户设备执行的相应流程和/或操作。此处不再赘述。

本领域技术人员可以理解，为了便于说明，图 7 仅示出了一个存储器和处理器。在实际的用户设备中，可以存在多个处理器和存储器。存储器也可以称为存储介质或者存储设备等，本申请实施例对此不做限制。

参见图 8，图 8 是本申请提出的切换的处理装置 30 的示意图。如图 8 所示，装置 30 包括接收单元 310、处理单元 320 和发送单元 330。

接收单元 310，用于接收第一接入网设备发送的切换请求消息；

处理单元 320，用于根据本地策略确定需要进行密钥推演；

处理单元 320，还用于保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下

文为所述第一 AMF 与用户设备 UE 协商生成的 NAS 安全上下文;

发送单元 330, 用于向第二 AMF 发送用户设备 UE 的安全上下文;

处理单元 320, 还用于恢复使用所述第一 NAS 安全上下文。

装置 30 和方法实施例中的第一 AMF 完全对应, 装置 30 可以是方法实施例中的第一
5 AMF, 或者方法实施例中的第一 AMF 内部的芯片或功能模块。装置 30 的相应单元用于
执行图 4 和图 5 所示的方法实施例中由第一 AMF 执行的相应步骤。

其中, 装置 30 中的接收单元 310 执行方法实施例中第一 AMF 接收的步骤。例如, 执
行图 4 中接收第一(R)AN 发送切换请求消息的步骤 111、执行图 4 中接收第二 AMF 发送
UE 上下文创建服务请求响应的步骤 118、执行图 5 中接收第一(R)AN 发送切换请求消息
10 的步骤 211、执行图 5 中接收第二 AMF 发送 UE 上下文创建服务请求响应的步骤 217。

处理单元 320 执行方法实施例中第一 AMF 内部实现或处理的步骤。例如, 执行图 4
中保存第一 NAS 安全上下文的步骤 110、执行图 4 中进行密钥推演的步骤 112、执行图 4
中恢复使用第一 NAS 安全上下文的步骤 120、执行图 5 中生成第二 NAS 安全上下文的步
骤 230。

发送单元 330 执行方法实施例中第一 AMF 发送的步骤。例如, 执行图 4 中向第二 AMF
发送 UE 的安全上下文的步骤 113、执行图 4 中向第一(R)AN 发送切换命令消息的步骤 119、
执行图 5 中向第二 AMF 发送 UE 的安全上下文的步骤 212、执行图 5 中向第一(R)AN 发
送切换命令消息的步骤 218。

接收单元 310 和发送单元 330 可以组成收发单元, 同时具有接收和发送的功能。其中,
20 处理单元 320 可以是处理器。发送单元 330 可以是接收器。接收单元 310 可以是发射器。
接收器和发射器可以集成在一起组成收发器。

如图 9 所示, 本申请实施例还提供了一种第一 AMF 40, 该第一 AMF 40 包括处理器
410, 存储器 420 与收发器 430, 其中, 存储器 420 中存储指令或程序, 处理器 430 用于
执行存储器 420 中存储的指令或程序。存储器 420 中存储的指令或程序被执行时, 收发器
25 430 用于执行图 8 所示的装置 30 中的接收单元 310 与发送单元 330 执行的操作。

本申请一实施例还提供了一种计算机可读存储介质, 该计算机可读存储介质中存储有
指令, 当该指令在计算机上运行时, 使得计算机执行上述如图 4 和图 5 所示的方法中第一
AMF 执行的各个步骤。

本申请一实施例还提供了一种计算机可读存储介质, 该计算机可读存储介质中存储有
30 指令, 当该指令在计算机上运行时, 使得计算机执行上述如图 4 和图 5 所示的方法中用户
设备执行的各个步骤。

本申请一实施例还提供了一种包含指令的计算机程序产品, 当该计算机程序产品在计
算机上运行时, 使得计算机执行如图 4 和图 5 所示的方法中第一 AMF 执行的各个步骤。

本申请一实施例还提供了一种包含指令的计算机程序产品, 当该计算机程序产品在计
35 算机上运行时, 使得计算机执行如图 4 和图 5 所示的方法中用户设备执行的各个步骤。

本申请一实施例还提供一种芯片, 包括处理器。该处理器用于读取并运行存储器中存
储的计算机程序, 以执行本申请提供的切换的处理方法中由用户设备执行的相应操作和/
或流程。可选地, 该芯片还包括存储器, 该存储器与该处理器通过电路或电线与存储器连
接, 处理器用于读取并执行该存储器中的计算机程序。进一步可选地, 该芯片还包括通信

接口，处理器与该通信接口连接。通信接口用于接收需要处理的数据和/或信息，处理器从该通信接口获取该数据和/或信息，并对该数据和/或信息进行处理。该通信接口可以是输入输出接口。

本申请还提供一种芯片，包括处理器。该处理器用于调用并运行存储器中存储的计算机程序，以执行本申请提供的切换的处理方法中由第一 AMF 执行的相应操作和/或流程。可选地，该芯片还包括存储器，该存储器与该处理器通过电路或电线与存储器连接，处理器用于读取并执行该存储器中的计算机程序。进一步可选地，该芯片还包括通信接口，处理器与该通信接口连接。通信接口用于接收需要处理的数据和/或信息，处理器从该通信接口获取该数据和/或信息，并对该数据和/或信息进行处理。该通信接口可以是输入输出接口。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

- 1、一种切换的处理方法，其特征在于，包括：
第一接入管理功能 AMF 接收第一接入网设备发送的切换请求消息；
- 5 当确定需要进行密钥推演时，所述第一 AMF 保存第一非接入层 NAS 安全上下文，所述
第一 NAS 安全上下文为所述第一 AMF 与用户设备 UE 协商生成的 NAS 安全上下文；
所述第一 AMF 恢复使用所述第一 NAS 安全上下文。
- 2、根据权利要求 1 所述的方法，其特征在于，所述第一 NAS 安全上下文中包括第一
NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计数
10 器 NAS COUNT。
- 3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一 AMF 恢复使用所述第一
NAS 安全上下文包括：
所述第一 AMF 向第二 AMF 发起用户上下文创建服务请求之后，所述第一 AMF 恢复
使用所述第一 NAS 安全上下文。
- 15 4、一种切换的处理方法，其特征在于，包括：
用户设备 UE 接收第一接入网设备发送的切换命令消息，所述切换命令消息携带第二
接入管理功能 AMF 选择的第二 NAS 安全算法和 AMF 密钥改变指示；
当所述第二 NAS 安全算法与第一 NAS 安全算法不一致和/或所述 AMF 密钥改变指示
为预设值时，所述 UE 保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下文为
20 所述 UE 和第一 AMF 协商生成的 NAS 安全上下文；
当所述 UE 用户设备切换失败时，使用所述第一 NAS 安全上下文与所述第一 AMF 进
行非接入层 NAS 保护；或者，
当所述 UE 对非接入层容器 NASC 完整性校验失败时，所述 UE 继续使用所述第一
NAS 安全上下文，其中，所述 NASC 携带在所述切换命令消息中。
- 25 5、根据权利要求 4 所述的方法，其特征在于，所述第一 NAS 安全上下文中包括第一
NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计数
器 NAS COUNT。
- 6、根据权利要求 4 或 5 所述的方法，其特征在于，所述 AMF 密钥改变指示为预设值
包括：
30 所述 AMF 密钥改变指示为 1。
- 7、一种切换的处理装置，其特征在于，包括：
接收单元，用于接收第一接入网设备发送的切换请求消息；
处理单元，用于当确定需要进行密钥推演时，第一非接入层 NAS 安全上下文，所述
第一 NAS 安全上下文为所述处理单元与用户设备 UE 协商生成的 NAS 安全上下文；
35 所述处理单元，还用于恢复使用所述第一 NAS 安全上下文。
- 8、根据权利要求 7 所述的装置，其特征在于，所述第一 NAS 安全上下文中包括第一
NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计数
器 NAS COUNT。

9、根据权利要求 7 或 8 所述的装置，其特征在于，所述处理单元恢复使用所述第一 NAS 安全上下文包括：

发送单元向第二 AMF 发起用户上下文创建服务请求之后，所述处理单元恢复使用所述第一 NAS 安全上下文。

5 10、一种切换的处理装置，其特征在于，包括：

接收单元，用于接收第一接入网设备发送的切换命令消息，所述切换命令消息携带第二接入管理功能 AMF 选择的第二 NAS 安全算法和 AMF 密钥改变指示；

10 处理单元，用于当所述第二 NAS 安全算法与第一 NAS 安全算法不一致和/或所述 AMF 密钥改变指示为预设值时，保存第一非接入层 NAS 安全上下文，所述第一 NAS 安全上下文为所述处理单元和第一 AMF 协商生成的 NAS 安全上下文；

所述处理单元，还用于当切换失败时，使用所述第一 NAS 安全上下文与所述第一 AMF 进行非接入层 NAS 保护；或者，

当所述处理单元对非接入层容器 NASC 完整性校验失败时，所述处理单元继续使用所述第一 NAS 安全上下文，其中，所述 NASC 携带在所述切换命令消息中。

15 11、根据权利要求 10 所述的装置，其特征在于，所述第一 NAS 安全上下文中包括第一 NAS 安全算法、第一 AMF 密钥 Kamf1、第一非接入层 NAS 密钥以及第一非接入层计数器 NAS COUNT。

12、根据权利要求 10 或 11 所述的装置，其特征在于，所述 AMF 密钥改变指示为预设值包括：

20 所述 AMF 密钥改变指示为 1。

13、一种通信设备，其特征在于，包括：

存储器，所述存储器用于存储计算机程序；

收发器，所述收发器用于执行收发步骤；

25 处理器，所述处理器用于从所述存储器中调用并运行所述计算机程序，使得所述通信设备执行权利要求 1-6 中任一项所述的方法。

14、一种计算机可读存储介质，其特征在于，包括：所述计算机可读介质存储有计算机程序；所述计算机程序在计算机上运行时，使得计算机执行权利要求 1-6 中任一项所述的方法。

15、一种通信系统，其特征在于，包括：

30 权利要求 7-9 中任一项所述的切换的处理装置、权利要求 10-12 中任一项所述的切换的处理装置。

16、一种切换的处理方法，其特征在于，所述方法应用于用户设备 UE 从第一接入管理网元 AMF 向第二 AMF 切换的场景，所述方法包括：

35 用户设备 UE 接收来自第一接入网设备的切换命令消息，所述切换命令消息携带非接入层容器 NASC；

所述 UE 对所述 NASC 进行完整性验证；

若对所述 NASC 的完整性验证失败，所述 UE 继续使用第一非接入层 NAS 安全上下文；其中，所述第一 NAS 安全上下文为所述 UE 与所述第一 AMF 之间的安全上下文。

17、根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

若所述 NASC 包括密钥推演指示且所述密钥推演指示的值为 1, 则所述 UE 根据所述第一 NAS 安全上下文获取第三 NAS 安全上下文。

18、根据权利要求 17 所述的方法, 其特征在于, 所述第一安全上下文包括第一密钥 Kamf; 所述用户设备根据所述第一安全上下文获取第三安全上下文, 包括:

5 所述用户设备根据所述第一 Kamf 获取第二 Kamf。

19、根据权利要求 17 或 18 所述的方法, 其特征在于, 所述方法还包括:

若对所述 NASC 的完整性验证失败, 则删除所述第三安全上下文。

20、根据权利要求 17 或 18 所述的方法, 其特征在于, 所述方法还包括:

10 若对所述 NASC 的完整性验证成功, 则使用所述第三安全上下文对所述 UE 与所述第二 AMF 之间的信息进行安全保护。

21、根据权利要求 16 所述的方法, 其特征在于, 所述 UE 继续使用第一非接入层 NAS 安全上下文, 包括:

所述 UE 使用第一 NAS 安全上下文对所述 UE 与所述第一 AMF 之间的信息进行安全保护。

15 22、根据权利要求 16 所述的方法, 其特征在于, 所述方法还包括:

若所述 NASC 包括密钥推演指示且所述密钥推演指示的值为 1, 则所述 UE 保存所述第一 NAS 安全上下文。

23、根据权利要求 16 所述的方法, 其特征在于, 所述方法还包括:

20 若对所述 NASC 的完整性验证失败, 所述 UE 通过第一接入网设备向所述第一 AMF 发送切换取消请求。

24、一种切换的处理装置, 其特征在于, 包括:

接收单元, 用于接收来自第一接入网设备的切换命令消息, 所述切换命令消息携带非接入层容器 NASC;

25 处理单元, 用于对所述 NASC 进行完整性验证; 若对所述 NASC 的完整性验证失败, 则继续使用第一非接入层 NAS 安全上下文; 其中, 所述第一 NAS 安全上下文为所述 UE 与所述第一 AMF 之间的安全上下文。

25、根据权利要求 24 所述的处理装置, 其特征在于,

所述处理单元, 还用于若所述 NASC 包括密钥推演指示且所述密钥推演指示的值为 1, 则所述 UE 根据所述第一 NAS 安全上下文获取第三 NAS 安全上下文。

30 26、根据权利要求 25 所述的处理装置, 其特征在于, 所述第一安全上下文包括第一密钥 Kamf; 所述处理单元, 还用于根据所述第一 Kamf 获取第二 Kamf。

27、根据权利要求 25 或 26 所述的处理装置, 其特征在于, 所述处理单元, 还用于若对所述 NASC 的完整性验证失败, 则删除所述第三安全上下文。

35 28、根据权利要求 25 或 26 所述的处理装置, 其特征在于, 所述处理单元, 还用于若对所述 NASC 的完整性验证成功, 则使用所述第三安全上下文对所述 UE 与所述第二 AMF 之间的信息进行安全保护。

29 根据权利要求 24 所述的处理装置, 其特征在于, 所述处理单元, 具体用于使用第一 NAS 安全上下文对所述 UE 与所述第一 AMF 之间的信息进行安全保护。

30、根据权利要求 24 所述的处理装置, 其特征在于, 所述处理单元, 还用于若所述

NASC 包括密钥推演指示且所述密钥推演指示的值为 1, 则保存所述第一 NAS 安全上下文。

31、根据权利要求 24 所述的处理装置, 其特征在于, 所述处理装置还包括发送单元, 所述发送单元用于若对所述 NASC 的完整性验证失败, 则通过第一接入网设备向所述第一 AMF 发送切换取消请求。

5 32、一种通信设备, 其特征在于, 包括:

存储器, 用于存储计算机程序;

收发器, 用于执行收发步骤;

处理器, 所述处理器与所述存储器、收发器耦合, 所述存储器中的所述计算机程序被所述处理器执行时, 权利要求 16 至 23 任一项所述的方法会被运行。

10 33、一种计算机可读存储介质, 其特征在于, 所述计算机可读介质存储有计算机程序; 所述计算机程序在计算机上运行时, 权利要求 16 至 23 中任一项所述的方法会被处理器运行。

34、一种芯片, 其特征在于, 所述芯片包括处理器, 所述处理器用于读取并运行存储器中存储的计算机程序, 以执行权利要求 16 至 23 任一所述的方法。

15 35、根据权利要求 34 所述的芯片, 其特征在于, 所述芯片还包括所述存储器, 所述存储器与所述处理器通过电路或电线存储器连接, 处理器用于读取并执行该存储器中的计算机程序。

20 36、根据权利要求 34 或 35 所述的芯片, 其特征在于, 所述芯片还包括通信接口, 所述处理器与所述通信接口连接; 通信接口用于接收需要处理的数据和/或信息, 所述处理器从所述通信接口获取所述数据和/或信息, 并对所述数据和/或信息进行处理。