

(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
2024 年 12 月 19 日 (19.12.2024)



(10) 国际公布号
WO 2024/254799 A1

(51) 国际专利分类号:

H04W 12/04 (2021.01)

(21) 国际申请号:

PCT/CN2023/100304

(22) 国际申请日:

2023 年 6 月 14 日 (14.06.2023)

(25) 申请语言:

中文

(26) 公布语言:

中文

(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: 王君 (**WANG, Jun**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 邢玮俊 (**XING, Weijun**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 习燕 (**XI, Yan**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王文会 (**WANG, Wenhui**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 彭

程晖 (**PENG, Chenghui**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 武绍芸 (**WU, Shaoyun**); 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: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路 81 号院二区 3 号楼 8 层 801-1 室, Beijing 100094 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) Title: NON-ACCESS STRATUM MESSAGE PROCESSING METHOD AND APPARATUS

(54) 发明名称: 一种非接入层消息处理方法和装置

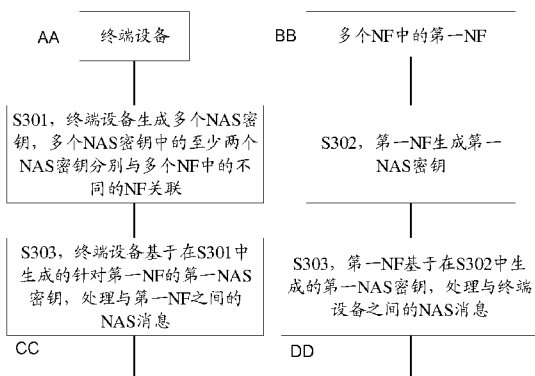


图 3

- S301 The terminal device generates a plurality of NAS keys, wherein at least two of the plurality of NAS keys are respectively associated with different NFs among a plurality of NFs
- S302 The first NF generates a first NAS key
- AA Terminal device
- BB First NF among a plurality of NFs
- CC S303, the terminal device processes an NAS message between the terminal device and a first NF on the basis of a first NAS key generated in S301 for the first NF
- DD S303, the first NF processes an NAS message between the first NF and a terminal device on the basis of the first NAS key generated in S302

(57) Abstract: The present application provides a non-access stratum (NAS) message processing method and apparatus. The method comprises: a terminal device generating a plurality of NAS keys, wherein at least two of the plurality of NAS keys are respectively associated with different NFs, and the plurality of NAS keys comprise a first NAS key for a first NF; the first NF generating a first NAS key, wherein the first NF is a non-anchor point function; the terminal device processing an NAS message between the terminal device and the first NF on the basis of the first NAS key generated by the terminal device; and the first NF processing an NAS message between the first NF and the terminal device on the basis of the first NAS key generated by the first NF. According to the embodiments of the present application, after an access network device is directly connected to a plurality of CN NFs, a terminal device can generate an NAS key associated with each of the plurality of CN NFs, and accordingly, each of the plurality of CN NFs can also generate an NAS key, such that an NAS message is processed.



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

(57) 摘要: 本申请提供了一种非接入层NAS消息处理方法和装置。该方法包括: 终端设备生成多个NAS密钥, 多个NAS密钥中的至少两个NAS密钥分别与不同的NF关联, 多个NAS密钥中包括针对第一NF的第一NAS密钥; 第一NF生成第一NAS密钥, 第一NF为非锚点功能; 终端设备基于终端设备生成的第一NAS密钥, 处理与第一NF的NAS消息; 第一NF基于第一NF生成的第一NAS密钥, 处理与终端设备的NAS消息。根据本申请实施例, 当接入网设备与多个CN NF进行直连之后, 终端设备可以生成与多个CN NF中每个CN NF关联的NAS密钥, 相应地多个CN NF中的每个CN NF也可以生成NAS密钥, 从而对NAS消息进行处理。

一种非接入层消息处理方法和装置

5 技术领域

本申请涉及通信领域，更具体地，涉及一种非接入层消息处理方法和装置。

背景技术

在第五代(5th generation, 5G)通信系统中，基站和接入与移动性管理功能(access and mobility management function, AMF)有直接连接(简称“直连”)，与其他控制面的核心网网络功能(core network network function, CN NF)没有直连，因此，其他控制面 CN NF 与基站之间的消息需要通过 AMF 进行传输，也就是说 AMF 是基站与其他控制面 CN NF 之间的代理。然而，这种架构会增加传输时延，因此对时延敏感类业务(例如，低时延高可靠(ultra-reliable low-latency communications, URLLC)业务)不友好。

15 为了降低传输时延，在未来的通信系统中，与基站有直连的 NF 可以包括多个。在此基础上，非接入层(non-access stratum, NAS)安全机制应该如何更新，以便适应未来的通信系统，是一个亟待解决的问题。

发明内容

20 本申请提供一种 NAS 消息处理方法和装置，用于对 NAS 安全机制进行更新，使其能够适用于未来的通信系统。

第一方面，提供一种 NAS 消息处理方法，包括：

25 终端设备生成多个非接入层 NAS 密钥，多个 NAS 密钥中的至少两个 NAS 密钥分别与多个网络功能 NF 中的不同的 NF 关联；所述终端设备基于所述多个 NAS 密钥，处理与
所述多个 NF 通信的 NAS 消息。

根据本申请实施例，当无线接入网设备与多个 CN NF 进行直连之后，终端设备可以生成与该多个 CN NF 中每个 CN NF 相关联的 NAS 密钥，从而对接收到的 NAS 消息进行处理(例如，进行加解密和/或完保)。

30 结合第一方面，在第一方面的某些实现方式中，所述终端设备生成多个 NAS 密钥，
包括：

所述终端设备根据第一 NF 的类型参数、所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值(count)、PDU 会话标识中的一项或多项，生成第一 NAS 密钥，其中所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

35 结合第一方面，在第一方面的某些实现方式中，所述终端设备生成多个 NAS 密钥，
包括：

所述终端设备根据第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值(count)，生成第一 NAS 密钥，其中所

述第一NF为所述多个NF中的一个,所述第一NAS密钥为所述多个NAS密钥中的一个。

结合第一方面,在第一方面的某些实现方式中,所述终端设备生成多个NAS密钥,包括:

5 所述终端设备根据第一NF的类型参数和/或所述第一NF的标识、所述第一NF选择的安全算法的标识、所述第一NF的NAS计数值、PDU会话标识,生成第一NAS密钥,所述第一NF为所述多个NF中的一个,所述第一NAS密钥为所述多个NAS密钥中的一个。

结合第一方面,在第一方面的某些实现方式中,所述终端设备生成多个NAS密钥,包括:

10 所述终端设备根据第一NF选择的安全算法的标识、所述第一NF的NAS计数值、PDU会话标识,生成第一NAS密钥,所述第一NF为所述多个NF中的一个,所述第一NAS密钥为所述多个NAS密钥中的一个。

结合第一方面,在第一方面的某些实现方式中,所述第一NF的NAS计数值从0开始计数;或者,所述第一NF的NAS计数值从锚点功能的初始NAS计数值开始计数。

15 示例性地,该锚点功能可以为AMF。

结合第一方面,在第一方面的某些实现方式中,所述终端设备生成多个NAS密钥,包括:

所述终端设备基于NAS根密钥,生成所述多个NAS密钥。

20 示例性地,NAS根密钥可以为 K_{SEAF} ,或者 K_{AMF} ,或者由 K_{SEAF} 派生的密钥(非 K_{AMF}),或者由 K_{AMF} 派生的密钥。

结合第一方面,在第一方面的某些实现方式中,所述方法还包括:

所述终端设备创建第一NF对应的NAS实体,所述第一NF为所述多个NF中的一个。

结合第一方面,在第一方面的某些实现方式中,所述终端设备创建所述第一NF对应的NAS实体,包括:

25 在所述终端设备首次接入核心网网络,并认证鉴权成功后,所述终端设备创建所述第一NF对应的NAS实体;或者,所述终端设备接收消息,并根据该消息创建所述第一NF对应的NAS实体。

结合第一方面,在第一方面的某些实现方式中,所述方法还包括:

30 所述终端设备暂停第一NF对应的NAS实体,并保存所述第一NF的安全上下文;其中,所述安全上下文包括所述第一NF的类型和/或所述第一NF的标识、所述第一NF的NAS计数值、所述第一NF选择的安全算法的标识,所述第一NF为所述多个NF中的一个。

结合第一方面,在第一方面的某些实现方式中,所述安全上下文还包括PDU会话标识。

35 结合第一方面,在第一方面的某些实现方式中,所述终端设备暂停所述第一NF对应的NAS实体,包括:

在所述终端设备进入空闲态或非激活态的情况下,所述终端设备暂停所述第一NF对应的NAS实体;或者,所述终端设备接收消息,并根据该消息暂停所述第一NF对应的NAS实体。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

所述终端设备删除第一 NF 对应的 NAS 实体，并删除所述第一 NF 的安全上下文，所述第一 NF 为所述多个 NF 中的一个。

5 结合第一方面，在第一方面的某些实现方式中，所述终端设备删除所述第一 NF 对应的 NAS 实体，包括：

在所述终端设备进入空闲态或非激活态的情况下，所述终端设备删除所述第一 NF 对应的 NAS 实体；或者，所述终端设备接收消息，并根据该消息删除所述第一 NF 对应的 NAS 实体。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

10 在创建与第一 NF 对应的 NAS 实体时，所述终端设备激活第一 NAS 密钥；或者，所述终端设备接收第一消息，并根据所述第一消息激活所述第一 NAS 密钥；其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

15 在暂停或者删除与第一 NF 对应的 NAS 实体时，所述终端设备去激活第一 NAS 密钥；或者，所述终端设备接收第二消息，并根据所述第二消息去激活所述第一 NAS 密钥；其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

20 在从连接态转入空闲态或非激活态时，所述终端设备保存第一 NF 的安全上下文，所述第一 NF 的安全上下文包括所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值；在从所述空闲态或所述非激活态转入所述连接态时，所述终端设备根据所述第一 NF 的安全上下文生成所述第一 NAS 密钥；其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

25 结合第一方面，在第一方面的某些实现方式中，所述第一 NF 的安全上下文还包括所述第一 NF 的类型、所述第一 NF 的标识、PDU 会话标识、终端设备的标识中的一项或多项。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

30 在从连接态转入空闲态或非激活态时，所述终端设备不保存所述第一 NF 的安全上下文；在从所述空闲态或所述非激活态转入所述连接态时，所述终端设备接收来自第二 NF 的所述第一 NF 的安全上下文，并根据所述第一 NF 的安全上下文生成所述第一 NAS 密钥，其中第二 NF 用于保存所述第一 NF 的安全上下文，其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

35 示例性地，第二 NF 可以为第一 NF，即，第一 NF 保存安全上下文。或者，第二 NF 可以与第一 NF 不同，即，由第二 NF 代替第一 NF 保存安全上下文。例如，第一 NF 为 SMF，第二 NF 为 AMF，SMF 可以向 AMF 发送安全上下文，由 AMF 代替 SMF 保存安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

在从连接态转入空闲态或非激活态时，所述终端设备不保存所述第一 NF 的 NAS 计数值；在从所述空闲态或所述非激活态转入所述连接态时，所述终端设备生成所述第一

NAS 密钥；其中，所述第一 NF 对应的 NAS 计数值从 0 开始计数；或者，所述第一 NF 对应的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数；所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：

- 5 所述终端设备接收来自第一 NF 的第三消息，并根据所述第三消息更新第一 NAS 密钥，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个；或者，所述终端设备接收来自锚点功能的第四消息，并根据所述第四消息更新所述多个 NAS 密钥。

示例性地，第一 NF 可以为 AMF、SMF、PCF、LMF 中的任一项。

- 10 结合第一方面，在第一方面的某些实现方式中，在所述终端设备从第一 NF 切换到第一目标 NF 的情况下，所述方法还包括：

所述终端设备接收来自所述第一目标 NF 的安全算法标识，所述第一 NF 为所述多个 NF 中的一个，所述第一 NF 为非锚点功能。

第二方面，提供一种 NAS 消息处理方法，包括：

- 15 第一网络功能 NF 生成第一非接入层 NAS 密钥；所述第一 NF 基于所述第一 NAS 密钥，处理与终端设备之间的 NAS 消息，第一 NF 为非锚点功能。

根据本申请实施例，当无线接入网设备与多个 CN NF 进行直连之后，该多个 CN NF 中的第一 NF（非锚点功能）也可以生成 NAS 密钥，从而对接收到的 NAS 消息进行处理（例如，进行加解密和/或完保）。

- 20 结合第二方面，在第二方面的某些实现方式中，所述第一 NF 生成第一 NAS 密钥，包括：

所述第一 NF 根据所述第一 NF 的类型参数、所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值（count）、PDU 会话标识中的一项或多项为，生成所述第一 NAS 密钥。

- 25 结合第二方面，在第二方面的某些实现方式中，所述第一 NF 生成第一 NAS 密钥，包括：

所述第一 NF 根据所述第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值（count），生成所述第一 NAS 密钥。

- 30 结合第二方面，在第二方面的某些实现方式中，所述第一 NF 生成第一 NAS 密钥，包括：

所述第一 NF 根据所述第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值、PDU 会话标识，生成所述第一 NAS 密钥。

- 35 结合第二方面，在第二方面的某些实现方式中，所述第一 NF 生成第一 NAS 密钥，包括：

所述第一 NF 根据所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值、PDU 会话标识，生成所述第一 NAS 密钥。

结合第二方面，在第二方面的某些实现方式中，所述第一 NF 维护的 NAS 计数值从 0

开始计数；或者，所述第一 NF 维护的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

结合第二方面，在第二方面的某些实现方式中，所述第一 NF 生成第一 NAS 密钥，包括：

- 5 所述第一 NF 从锚点功能获取 NAS 根密钥；所述第一 NF 基于所述 NAS 根密钥，生成所述第一 NAS 密钥。

示例性地，NAS 根密钥可以为 K_{SEAF} ，或者 K_{AMF} ，或者由 K_{SEAF} 派生的密钥（非 K_{AMF} ），或者由 K_{AMF} 派生的密钥。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

- 10 所述第一 NF 创建与所述第一 NF 对应的 NAS 实体。

结合第二方面，在第二方面的某些实现方式中，所述第一 NF 创建与所述第一 NF 对应的 NAS 实体，包括：

在成功对所述终端设备进行接入鉴权后，所述第一 NF 创建与所述第一 NF 对应的 NAS 实体；或者，所述第一 NF 接收消息，并根据该消息创建与所述第一 NF 对应的 NAS 实体。

- 15 结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

所述第一 NF 暂停与所述第一 NF 对应的 NAS 实体，并保存所述第一 NF 的安全上下文，所述安全上下文包括所述第一 NAS 计数值、所述第一 NF 选择的安全算法的标识、所述终端设备的标识。

- 20 结合第二方面，在第二方面的某些实现方式中，所述安全上下文还包括所述第一 NF 的类型、所述第一 NF 的标识、PDU 会话标识中的一项或多项。

结合第二方面，在第二方面的某些实现方式中，所述第一 NF 暂停与所述第一 NF 对应的 NAS 实体，包括：

所述第一 NF 接收消息，并根据该消息暂停与所述第一 NF 对应的 NAS 实体。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

- 25 所述第一 NF 删除与所述第一 NF 对应的 NAS 实体，并删除所述第一 NF 的安全上下文。

结合第二方面，在第二方面的某些实现方式中，所述第一 NF 删除与所述第一 NF 对应的 NAS 实体，包括：

所述第一 NF 接收消息，并根据该消息删除与所述第一 NF 对应的 NAS 实体。

- 30 结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

在创建与所述第一 NF 对应的 NAS 实体时，所述第一 NF 激活所述第一 NAS 密钥；或者，所述第一 NF 接收第五消息，并根据所述第五消息激活所述第一 NAS 密钥。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

- 35 所述第一 NF 接收激活成功信息，所述激活成功信息用于指示所述终端设备成功激活所述第一 NAS 密钥；所述第一 NF 根据所述激活成功信息，与所述终端设备进行 NAS 消息的传输。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

在暂停或者删除与所述第一 NF 对应的 NAS 实体时，所述第一 NF 去激活所述第一 NAS 密钥；或者，所述第一 NF 接收第六消息，并根据所述第六消息去激活所述第一 NAS

密钥。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

所述第一 NF 接收去激活成功信息，所述去激活成功信息用于指示所述终端设备成功去激活所述第一 NAS 密钥。

5 结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 保存所述终端设备的安全上下文，所述终端设备的安全上下文包括所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值、所述终端设备的标识；在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 根据所述终端设备的安全上下文生成所述第一 NAS 密钥。

10 结合第二方面，在第二方面的某些实现方式中，所述终端设备的安全上下文还包括所述第一 NF 的类型、所述第一 NF 的标识、PDU 会话标识中的一项或多项。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

15 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 不保存所述终端设备的安全上下文；在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 从第二 NF 获取所述终端设备的安全上下文，并根据所述终端设备的安全上下文生成所述第一 NAS 密钥。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

20 在所述终端设备从连接态转入空闲态或非激活态时，第二 NF 保存安全上下文，所述安全上下文包括所述终端设备的标识、所述第一 NF 的类型和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法标识、所述第一 NF 的 NAS 计数值；在所述终端设备从空闲态或非激活态转入连接态时，所述第二 NF 向所述第一 NF 和所述终端设备发送所述安全上下文。

25 可以理解的是，此时，第二 NF 与第一 NF 不同，例如，第一 NF 为 SMF、LMF 或者 PCF，第二 NF 为 AMF。

结合第二方面，在第二方面的某些实现方式中，所述安全上下文还包括 PDU 会话标识。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

30 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 不保存所述第一 NF 的 NAS 计数值；在所述终端设备从所述空闲态或所述非激活态转入连接态时，所述第一 NF 生成所述第一 NAS 密钥；其中，所述第一 NF 对应的 NAS 计数值从 0 开始计数；或者，所述第一 NF 对应的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

35 在预设条件满足的情况下，所述第一 NF 更新所述第一 NAS 密钥；所述第一 NF 发送第三消息，所述第三消息用于指示所述终端设备更新所述第一 NAS 密钥；或者，所述第一 NF 通知锚点功能：所述第一 NF 成功更新所述第一 NAS 密钥。

结合第二方面，在第二方面的某些实现方式中，所述方法还包括：

锚点功能接收来自第一 NF 的 NAS 密钥更新请求消息，与无线接入网设备直连的多个 NF 中包括所述第一 NF；所述锚点功能向与无线接入网设备直连的多个 NF 中除所述第

一 NF 和所述锚点功能之外的其他 NF 发送 NAS 密钥更新请求消息;所述锚点功能确定与无线接入网设备直连的多个 NF 中的每个 NF 均成功更新对应的 NAS 密钥;所述锚点功能向终端设备发送第四消息,所述第四消息用于指示所述终端设备更新与无线接入网设备直连的多个 NF 的 NAS 密钥。

5 结合第二方面,在第二方面的某些实现方式中,所述方法还包括:

所述第一 NF 接收来自锚点功能的消息,并根据该消息,在所述第一 NAS 密钥更新期间暂停与所述终端设备之间的 NAS 消息传输。

结合第二方面,在第二方面的某些实现方式中,所述方法还包括:

10 所述第一 NF 接收来自所述锚点功能的消息,并根据该消息,恢复与所述终端设备之间的 NAS 消息传输。

结合第二方面,在第二方面的某些实现方式中,在所述终端设备从所述第一 NF 切换到第一目标 NF 的情况下,所述方法还包括:

所述第一 NF 向所述第一目标 NF 发送所述终端设备的安全上下文,所述终端设备的安全上下文包括所述第一 NF 的 NAS 计数值。

15 结合第二方面,在第二方面的某些实现方式中,所述终端设备的安全上下文还包括以下中的一项或多项:

PDU 会话标识、所述终端设备的安全能力信息。

结合第二方面,在第二方面的某些实现方式中,所述第一 NF 向所述第一目标 NF 发送所述终端设备的安全上下文,包括:

20 所述第一 NF 直接向所述第一目标 NF 发送所述终端设备的安全上下文;或者,所述第一 NF 通过源锚点功能向所述第一目标 NF 发送所述终端设备的安全上下文;或者,所述第一 NF 通过源锚点功能和目标锚点功能,向所述第一目标 NF 发送所述终端设备的安全上下文。

25 结合第二方面,在第二方面的某些实现方式中,在所述终端设备从所述第一 NF 切换到第一目标 NF 的情况下,所述方法还包括:

源锚点功能向所述第一目标 NF 发送所述终端设备的安全能力信息。

结合第二方面,在第二方面的某些实现方式中,源锚点功能向所述第一目标 NF 发送所述终端设备的安全能力信息,包括:

30 所述源锚点功能直接向所述第一目标 NF 发送所述终端设备的安全能力信息;或者,所述源锚点功能通过目标锚点功能向所述第一目标 NF 发送所述终端设备的安全能力信息。

结合第二方面,在第二方面的某些实现方式中,在所述终端设备从所述第一 NF 切换到第一目标 NF 的情况下,所述方法还包括:

源锚点功能接收第一目标 NF 选择的安全算法标识;所述源锚点功能向终端设备发送第一目标 NF 选择的安全算法标识。

35 结合第二方面,在第二方面的某些实现方式中,源锚点功能接收第一目标 NF 选择的安全算法标识,包括:

所述源锚点功能从所述第一目标 NF 接收第一目标 NF 选择的安全算法标识;或者,所述源锚点功能从目标锚点功能接收第一目标 NF 选择的安全算法标识

第三方面,提供一种 NAS 消息处理方法,包括:

终端设备生成多个非接入层 NAS 密钥，所述多个 NAS 密钥中的至少两个 NAS 密钥分别与多个网络功能 NF 中的不同的 NF 关联，所述多个 NAS 密钥中包括针对第一 NF 的第一 NAS 密钥，所述第一 NF 为所述多个 NF 中的一个；第一 NF 生成第一 NAS 密钥，所述第一 NF 为非锚点功能；所述终端设备基于所述终端设备生成的第一 NAS 密钥，处理与
5 所述第一 NF 之间的 NAS 消息；所述第一 NF 基于所述第一 NF 生成的第一 NAS 密钥，处理与
所述终端设备之间的 NAS 消息。

在本申请实施例中，第一 NF 生成的第一 NAS 密钥与终端设备生成的针对第一 NF 的第一 NAS 密钥可以是相同的，也可以是不同的。

结合第三方面，在第三方面的某些实现方式中，所述终端设备和所述第一 NF 根据所述
10 所述第一 NF 的类型参数、所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述
所述第一 NF 的 NAS 计数值（count）、PDU 会话标识中的一项或多项，生成第一 NAS 密
钥，其中所述多个 NAS 密钥包括所述第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述终端设备和所述第一 NF 根据第
15 一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述
第一 NF 的 NAS 计数值，生成第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述终端设备和所述第一 NF 根据第
一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述
20 第一 NF 的 NAS 计数值、PDU 会话标识，生成第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述终端设备和所述第一 NF 根据所
述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值、PDU 会话标识，生成
25 第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述第一 NF 的 NAS 计数值从 0 开
始计数；或者，所述第一 NF 的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

结合第三方面，在第三方面的某些实现方式中，所述终端设备和所述第一 NF 基于
25 NAS 根密钥生成第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备创建与所述第一 NF 对应的 NAS 实体；所述第一 NF 创建与所述第一
NF 对应的 NAS 实体。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

30 所述终端设备暂停与所述第一 NF 对应的 NAS 实体；所述第一 NF 暂停与所述第一
NF 对应的 NAS 实体。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备删除与所述第一 NF 对应的 NAS 实体；所述第一 NF 删除与所述第一
NF 对应的 NAS 实体。

35 结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备激活所述终端设备生成的第一 NAS 密钥；所述第一 NF 激活所述第一
NF 生成的第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备发送激活成功信息，所述激活成功信息用于指示所述终端设备成功激活

所述终端设备生成的第一 NAS 密钥；所述第一 NF 接收所述激活成功信息；所述第一 NF 根据所述激活成功信息，与所述终端设备进行 NAS 消息的传输。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

5 所述终端设备去激活所述终端设备生成的第一 NAS 密钥；所述第一 NF 去激活所述第一 NF 生成的第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备发送去激活成功信息，所述去激活成功信息用于指示所述终端设备成功去激活所述终端设备生成的第一 NAS 密钥；所述第一 NF 接收所述去激活成功信息。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

10 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 和所述终端设备均保存安全上下文；在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 和所述终端设备分别根据保存的安全上下文生成第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

15 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 和所述终端设备均不保存安全上下文；在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 和所述终端设备分别从第二 NF 获取安全上下文，并分别根据获取到的安全上下文生成第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

20 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 和所述终端设备均不保存所述第一 NF 的 NAS 计数值；在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 和所述终端设备分别生成第一 NAS 密钥；其中，所述第一 NF 对应的 NAS 计数值从 0 开始计数；或者，所述第一 NF 对应的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

25 在预设条件满足的情况下，所述第一 NF 更新所述第一 NF 生成的第一 NAS 密钥；所述第一 NF 发送第三消息；所述终端设备接收所述第三消息，并根据所述第三消息更新所述终端设备生成的第一 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

30 在预设条件满足的情况下，与无线接入网设备直接连接的多个 NF 更新对应的所述多个 NAS 密钥；在所述多个 NF 均成功更新对应的所述多个 NAS 密钥的情况下，锚点功能发送第四消息；所述终端设备接收所述第四消息，并根据所述第四消息更新所述多个 NAS 密钥。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

35 所述终端设备和所述第一 NF 接收来自锚点功能的消息，并根据接收到的消息在第一 NAS 密钥更新期间暂停所述第一 NF 与所述终端设备之间的 NAS 消息传输。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：

所述终端设备和所述第一 NF 接收来自锚点功能的消息，并根据接收到的消息恢复所述第一 NF 与所述终端设备之间的 NAS 消息传输。

结合第三方面，在第三方面的某些实现方式中，在所述终端设备从所述第一 NF 切换

到第一目标 NF 的情况下，所述方法还包括：

所述第一 NF 发送所述终端设备的安全上下文；所述第一目标 NF 接收所述终端设备的安全上下文。

5 结合第三方面，在第三方面的某些实现方式中，所述终端设备的安全上下文中包括所述终端设备的安全能力信息，所述方法还包括：

所述第一目标 NF 根据所述终端设备的安全能力信息选择安全算法；所述第一目标 NF 发送所述第一目标 NF 选择的安全算法的标识；所述终端设备接收所述第一目标 NF 选择的安全算法的标识。

10 第四方面，提供一种通信装置，该通信装置可以为终端设备，也可以是终端设备中的装置（例如，芯片，或者芯片系统，或者电路），或者是能够和终端设备匹配使用的装置。

一种可能的实现中，该通信装置可以包括执行第一方面中所描述的方法/操作/步骤/动作所一一对应的模块或单元，该模块或单元可以是硬件电路，也可是软件，也可以是硬件电路结合软件实现。

15 第五方面，提供一种通信装置，该通信装置可以为第一 NF，也可以是第一 NF 中的装置（例如，芯片，或者芯片系统，或者电路），或者是能够 and 第一 NF 匹配使用的装置。

一种可能的实现中，该通信装置可以包括执行第二方面中与第一 NF 相关的方法/操作/步骤/动作所一一对应的模块或单元，该模块或单元可以是硬件电路，也可是软件，也可以是硬件电路结合软件实现。

20 第六方面，提供一种通信装置，包括通信接口和处理器，所述通信接口用于输出和/或输入信号，所述处理器用于执行存储器存储的计算机程序或指令，使得该通信装置执行第一方面或者第二方面中的方法。

可选地，该存储器可以包括在该通信装置中，作为一种方式，存储器可以与处理器分开设置；作为另一种方式，该存储器可以位于处理器中，与处理器集成在一起。

可选地，该存储器也可以在该通信装置之外，与处理器耦合。

25 第七方面，提供一种计算机可读存储介质，包括计算机程序，当计算机程序在计算机上运行时，使得计算机执行第一方面或者第二方面中任一种可能实现方式中的方法。

第八方面，提供一种芯片或芯片系统，芯片或芯片系统包括处理电路和输入输出接口，处理电路用于执行该第一方面或者第二方面中任一种可能实现方式中的方法。

30 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，使得计算机执行第一方面或者第二方面中任一种可能实现方式中的方法。

第十方面，提供一种通信系统，包括与基站直连的多个 NF 和终端设备。终端设备用于执行第一方面中任一种可能实现方式中的方法；与基站直连的多个 NF 中包括第一 NF，第一 NF 用于执行第二方面中任一种可能实现方式中的方法。

35

附图说明

图 1 示出了一种通信系统。

图 2 示出了另一种通信系统。

图 3 为本申请提出的 NAS 消息处理方法的流程示意图一。

图 4 为本申请提出的 NAS 消息处理方法的流程示意图二。

图 5 为暂停 NAS 实体的方法的流程示意图。

图 6 为删除 NAS 实体的方法的流程示意图。

图 7 为去激活 NAS 密钥的方法的流程示意图。

5 图 8 为终端设备转为连接态时的 NAS 密钥生成方法的流程示意图。

图 9 为终端设备与第一 NF 独立更新 NAS 密钥的方法的流程示意图。

图 10 为终端设备与多个 NF 统一更新 NAS 密钥的方法的流程示意图。

图 11 为切换场景下第一目标 NF 生成 NAS 密钥的方法的流程示意图。

图 12 为本申请提供的通信装置的一种示意性框图。

10 图 13 为本申请提供的通信装置的另一种示意性框图。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

15 在本申请的各个实施例中，如果没有特殊说明以及逻辑冲突，不同的实施例之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。

可以理解的是，在本申请中涉及的各种数字编号仅为描述方便进行的区分，并不用来限制本申请的范围。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。

20 可以理解的是，在本申请中涉及的各种数字编号仅为描述方便进行的区分，并不用来限制本申请的范围。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。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”以及其他各种术语标号等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

25 可以理解的是，在本申请中，“用于指示”可以包括直接指示和间接指示两种方式。

30 本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请提供的技术方案可以应用于各种通信系统，例如：5G 或新无线（new radio, NR）系统、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）系统等。本申请提供的技术方案还可以应用于未来的通信系统，如第六代（6th generation, 6G）移动通信系统。本申请提供的技术方案还可以应用于设备到设备（device to device, D2D）通信，车到万物（vehicle-to-everything, V2X）通信，机器到机器（machine to machine, M2M）通信，

35

机器类型通信 (machine type communication, MTC), 以及物联网 (internet of things, IoT) 通信系统或者其他通信系统。

为了方便理解, 下面对一些技术术语进行说明。

1、终端设备

5 本申请实施例中的终端设备, 可以是: 用户设备 (user equipment, UE)、移动台 (mobile station, MS)、移动终端 (mobile terminal, MT)、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等。

10 终端设备可以是一种向用户提供语音/数据连通性的设备, 例如, 具有无线连接功能的手持式设备、车载设备等。终端设备的举例为: 移动手机 (mobile phone)、平板电脑、笔记本电脑、掌上电脑、移动互联网设备 (mobile internet device, MID)、可穿戴设备、虚拟现实 (virtual reality, VR) 设备、增强现实 (augmented reality, AR) 设备、工业控制 (industrial control) 中的无线终端、无人驾驶 (self-driving or autopilot) 中的无线终端、远程手术 (remote medical surgery) 中的无线终端、智能电网 (smart grid) 中的无线终端、
15 运输安全 (transportation safety) 中的无线终端、智慧城市 (smart city) 中的无线终端、智慧家庭 (smart home) 中的无线终端、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 网络中的终端设备或者未来演进的
20 公用陆地移动通信网络 (public land mobile network, PLMN) 中的终端设备等, 本申请实施例对此并不限定。

作为示例而非限定, 在本申请实施例中, 该终端设备还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备, 是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称, 如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上,
25 或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备, 更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能, 例如: 智能手表或智能眼镜等, 以及只专注于某一类应用功能, 需要和其它设备如智能手机配合使用, 如各类进行体征监测的智能手环、智能首饰等。此外, 在本申请实施例中, 终端设备还可以是物联网
30 (internet of things, IoT) 系统中的终端设备。

2、网络功能 (networkfunction, NF)

本申请实施例中, NF 可以包括无线接入网 (radioaccessnetwork, RAN) 网络功能和核心网 (corenetwork, CN) 网络功能。并且, NF 可以为网络物理实体, 也可以为逻辑功能, 不予限制。网络功能也可以称为网元。

35 其中, 本申请实施例中的 RAN, 可以指代接入网, 也可以指接入网设备, 此处不作区分。接入网设备是一种为终端设备提供无线通信功能的设备, 也可以称为接入设备、网络设备或者无线接入网设备等。该接入网设备包括但不限于: 5G 系统中的下一代基站 (next generation node basestation, gNB)、LTE 系统中的演进型基站 (evolved node B, eNB)、无线网络控制器 (radio network controller, RNC)、节点 B (node B, NB)、基站控制器

(base station controller, BSC)、基站收发台(base transceiver station, BTS)、家庭基站(home evolved nodeB, 或 home node B, HNB)、基带单元(base band unit, BBU)、传输接收点(transmitting and receiving point, TRP)、发射点(transmitting point, TP)、小基站设备(pico)、移动交换中心, 或者未来网络中的网络设备等。可理解, 本申请对接入网设备的具体类型不作限定。采用不同无线接入技术的系统中, 具备接入网设备功能的设备的名称可能会有所不同。

可选的, 在接入设备的一些部署中, 接入设备可以包括集中式单元(central unit, CU)和分布式单元(distributed unit, DU)等。在接入设备的另一些部署中, CU还可以划分为CU-控制面(control plane, CP)和CU-用户面(user plan, UP)等。在接入设备的又一些部署中, 接入设备还可以是开放的无线接入网(open radio access network, ORAN)架构等, 本申请对于接入设备的具体部署方式不作限定。

下面以5G系统为例, 对控制面CN NF进行说明。在5G中控制面CN NF包括AMF, 会话管理功能(session management function, SMF), 策略控制功能(policy control function, PCF), 位置管理功能(location management function, LMF)等。可以理解的是, 5G系统中还包括其他类型的NF, 在此不再赘述。

(1) AMF

AMF可以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, 合法探测、或接入授权等功能, 此外还用于在终端设备与PCF之间传输用户策略。

此外, 本申请对AMF在未来通信系统中的名称不做限定。

(2) SMF

SMF可以用于会话管理、终端设备的网络互连协议(internet protocol, IP)地址分配和管理、选择和管理用户面功能(user plane function, UPF)网元、策略控制和收费功能接口的终结点以及下行数据通知等。

此外, 本申请对SMF在未来通信系统中的名称不做限定。

(3) PCF

PCF可以为控制平面功能网元(例如接入与移动性管理功能网元, 会话管理功能网元等)提供策略规则信息等。PCF主要负责针对会话、业务流级别进行计费、QoS带宽保障及移动性管理、终端设备策略决策等的策略控制。PCF既可以具备接入与移动性管理策略控制网元(policy control function for access and mobility control, AM PCF)的能力, 又可以具备会话管理策略控制网元(PCF for session management, SM PCF)的能力。其中, 在逻辑上, AM PCF和SM PCF可以理解为分别具备不同能力的不同的网络功能。在实际部署场景中, AM PCF和SM PCF可以是同一个策略控制网元实体, 也可以是两个不同的策略控制网元实体。

比如, AM PCF与AMF直接相连, AM PCF向AMF提供移动性、终端设备的接入选择相关策略。其中, 移动性策略包括例如服务区限制管理、无线电接入技术频率选择优先级(radio access technology frequency selection priority, RFSP)索引(index)管理。

此外, 本申请对PCF在未来通信系统中的名称不做限定。

(4) LMF

LMF 可以用于与 5G 核心网交互，完成终端的定位功能。此外，本申请对 LMF 在未来通信系统中的名称不做限定。

(5) 锚点功能

在本申请实施例中，锚点功能可以理解为产生 NAS 根密钥的网络功能。

- 5 在 5G 系统中，锚点功能可以为 AMF。本申请对未来通信系统中可以作为锚点功能的 NF 不作限定。例如，在未来通信系统中，锚点功能仍然可以为 AMF，当然也可以为其他的 NF，不予限制。

下面介绍本申请针对的技术问题。

- 10 如图 1 所示，在 5G 系统中，无线接入网设备与 AMF 有直接连接（简称“直连”），与其他控制面 CN NF（例如，SMF、PCF、LMF）没有直连，因此，其他 CN NF（与无线接入网设备没有直连的 NF）与无线接入网设备之间的消息（例如，Ng 消息和 NAS 消息）需要通过 AMF 进行传输，或者说 AMF 是无线接入网设备与其他 CN NF 之间的代理。这种架构会带来传输时延，因此对时延敏感类业务（例如，低时延高可靠（ultra-reliable low-latency communications, URLLC）业务）不友好。

- 15 如图 2 所示，作为一种实现方式，在未来通信系统中，无线接入网设备可以与多种类型的控制面 CN NF 进行直连，即，无线接入网设备可以与多种类型的控制面 CN NF 进行直接通信。例如，无线接入网设备除了与 AMF 进行直连，还可以与 SMF、PCF、LMF 中的一项或多项进行直连。基于图 2 所示的通信架构，可以降低传输时延。以 SMF 为例，在图 1 的架构中，终端设备与 SMF 之间的通信经过无线接入网设备和 AMF；在图 2 的架构中，终端设备与 SMF 之间的通信可以不经 AMF，从而降低传输时延。

可选地，作为另一种方式，在未来通信系统中，虽然无线接入网设备与多种类型的控制面 CN NF 进行直连，但是无线接入网设备也可以通过锚点功能与 CN NF 进行通信。

- 20 也就是说，未来的通信系统可以包括锚点功能和非锚点功能。例如，该锚点功能为 AMF，该非锚点功能包括 SMF、LMF、PCF 等。无线接入网设备可以通过 AMF 与 SMF、LMF、或者 PCF 进行通信。

当然，未来的通信系统也可以不包括锚点功能，本申请对此不予限制。

可以理解的是，随着技术的发展，现有的 NAS 安全机制并不适用于未来的无线接入网设备与多种类型的控制面 CN NF 进行直连之后的通信系统。

- 30 基于上述问题，本申请提出了方法 300。可以理解的是，该方法 300 适用于未来的通信系统（例如，图 2 所示的通信系统）。具体地，如图 3 所示，该方法 300 包括如下步骤。

S301，终端设备生成多个 NAS 密钥，多个 NAS 密钥中的至少两个 NAS 密钥分别与多个 NF 中的不同的 NF 关联。

关于终端设备生成多个 NAS 密钥的机制可以参考方法 400，这里先不展开说明。

- 35 例如，终端设备可以生成与 SMF 关联的密钥，记为 K_{SMF} 。进一步地，终端设备可以基于 K_{SMF} 生成用于 NAS 消息（即，终端设备与 SMF 之间的 NAS 消息）加解密的 NAS 密钥，记为 $K_{NASsmf-enc}$ ，以及用于 NAS 消息完整性保护（简称“完保”）的 NAS 密钥，记为 $K_{NASsmf-int}$ 。其中， $K_{NASsmf-enc}$ 以及 $K_{NASsmf-int}$ 也是与 SMF 关联的密钥。

可以理解的是，终端设备可以生成 K_{SMF} 、 $K_{NASsmf-enc}$ 、 $K_{NASsmf-int}$ 中的一项或多项。例如，当不需要开启终端设备与 SMF 之间的 NAS 消息的加解密功能时，终端设备可以不生

成 $K_{NASsmf-enc}$ 。例如，当不需要开启终端设备与 SMF 之间的 NAS 消息的完保功能时，终端设备可以不生成 $K_{NASsmf-int}$ 。例如，当不需要开启终端设备与 SMF 之间的 NAS 消息的加解密功能以及完保功能时，终端设备可以生成 K_{SMF} ，不生成 $K_{NASsmf-enc}$ 和 $K_{NASsmf-int}$ 。

此外，可选地，对于同一个终端设备而言，不同的 PDU 会话对应的 SMF 实体可能不同，因此，终端设备在生成 K_{SMF} ， $K_{NASsmf-enc}$ 以及 $K_{NASsmf-int}$ 时，可以以 PDU 会话为粒度生成这些密钥。例如，针对 PDU 会话#1，终端设备可以生成 $K_{SMF\#1}$ ， $K_{NASsmf-enc\#1}$ 以及 $K_{NASsmf-int\#1}$ 中的一项或多项；可选地，如果还有其他的 PDU 会话，例如 PDU 会话#2，终端设备可以生成 $K_{SMF\#2}$ ， $K_{NASsmf-enc\#2}$ 以及 $K_{NASsmf-int\#2}$ 中的一项或多项。

可以理解的是，PDU 会话与 SMF 实体是相关联的，PDU 会话相关联的 SMF 实体会随着终端设备执行的切换流程发生变化。例如，在切换前，PDU 会话#1 与 SMF#1 关联，PDU 会话#2 与 SMF#2 关联，在切换后 PDU 会话#1 和 PDU 会话#2 均与 SMF#3 关联，如果以 SMF 为粒度生成 NAS 密钥，那么在切换后 PDU 会话#1 和 PDU 会话#2 的 NAS 密钥可能是相同的，从而造成冲突。因此，终端设备以 PDU 会话为粒度生成 NAS 密钥，在发生切换场景下更为灵活，从而减少冲突概率。

终端设备还可以生成与 LMF 关联的密钥，记为 K_{LMF} 。进一步地，终端设备可以基于 K_{LMF} 生成用于 NAS 消息（即，终端设备与 LMF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASlmf-enc}$ ，以及用于 NAS 消息完保的密钥，记为 $K_{NASlmf-int}$ 。其中， $K_{NASlmf-enc}$ 以及 $K_{NASlmf-int}$ 也是与 LMF 关联的密钥。

可以理解的是，终端设备可以生成 K_{LMF} 、 $K_{NASlmf-enc}$ 、 $K_{NASlmf-int}$ 中的一项或多项。例如，当不需要开启终端设备与 LMF 之间的 NAS 消息的加解密功能时，终端设备可以不生成 $K_{NASlmf-enc}$ 。例如，当不需要开启终端设备与 LMF 之间的 NAS 消息的完保功能时，终端设备可以不生成 $K_{NASlmf-int}$ 。例如，当不需要开启终端设备与 LMF 之间的 NAS 消息的加解密功能以及完保功能时，终端设备可以生成 K_{LMF} ，不生成 $K_{NASlmf-enc}$ 和 $K_{NASlmf-int}$ 。

终端设备还可以生成与 PCF 关联的密钥，记为 K_{PCF} 。进一步地，终端设备可以基于 K_{PCF} 生成用于 NAS 消息（即，终端设备与 PCF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASpcf-enc}$ ，以及用于 NAS 消息完保的密钥，记为 $K_{NASpcf-int}$ 。其中， $K_{NASpcf-enc}$ 以及 $K_{NASpcf-int}$ 也是与 PCF 关联的密钥。

可以理解的是，终端设备可以生成 K_{PCF} 、 $K_{NASpcf-enc}$ 、 $K_{NASpcf-int}$ 中的一项或多项。例如，当不需要开启终端设备与 PCF 之间的 NAS 消息的加解密功能时，终端设备可以不生成 $K_{NASpcf-enc}$ 。例如，当不需要开启终端设备与 PCF 之间的 NAS 消息的完保功能时，终端设备可以不生成 $K_{NASpcf-int}$ 。例如，当不需要开启终端设备与 PCF 之间的 NAS 消息的加解密功能以及完保功能时，终端设备可以生成 K_{PCF} ，不生成 $K_{NASpcf-enc}$ 和 $K_{NASpcf-int}$ 。

终端设备还可以生成与 AMF 关联的密钥，记为 K_{AMF} 。进一步地，终端设备可以基于 K_{AMF} 生成用于 NAS 消息（即，终端设备与 AMF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASamf-enc}$ ，以及用于 NAS 消息完保的密钥，记为 $K_{NASamf-int}$ 。其中， $K_{NASamf-enc}$ 以及 $K_{NASamf-int}$ 也是与 AMF 关联的密钥。

可以理解的是，终端设备可以生成 K_{AMF} 、 $K_{NASamf-enc}$ 、 $K_{NASamf-int}$ 中的一项或多项。例如，当不需要开启终端设备与 AMF 之间的 NAS 消息的加解密功能时，终端设备可以不生成 $K_{NASamf-enc}$ 。例如，当不需要开启终端设备与 AMF 之间的 NAS 消息的完保功能时，终

端设备可以不生成 $K_{NASmf-int}$ 。例如，当不需要开启终端设备与 AMF 之间的 NAS 消息的加解密功能以及完保功能时，终端设备可以生成 K_{AMF} ，不生成 $K_{NASmf-enc}$ 和 $K_{NASmf-int}$ 。

下面通过几个例子对“多个密钥中的至少两个密钥分别与不同的网络功能关联”进行说明。

5 例 1:

终端设备生成的多个密钥中包括 K_{AMF} 和 K_{PCF} ，其中， K_{AMF} 与 AMF 关联， K_{PCF} 与 PCF 关联。也就是说， K_{AMF} 和 K_{PCF} 分别与不同的 NF 关联。

例 2:

10 终端设备生成的多个密钥中包括 K_{AMF} 、针对 PDU 会话#1 的 $K_{SMF\#1}$ 和针对 PDU 会话#2 的 $K_{SMF\#2}$ ，其中， K_{AMF} 与 AMF 关联， $K_{SMF\#1}$ 和 $K_{SMF\#2}$ 与同一 SMF 关联。也就是说， K_{AMF} 和 $K_{SMF\#1}$ 分别与不同的 NF 关联， K_{AMF} 和 $K_{SMF\#2}$ 分别与不同的 NF 关联。

例 3:

终端设备生成的多个密钥中包括 K_{AMF} 、 K_{PCF} 和 K_{LMF} ，其中， K_{AMF} 与 AMF 关联， K_{PCF} 与 PCF 关联， K_{LMF} 与 LMF 关联。也就是说， K_{AMF} 、 K_{PCF} 和 K_{LMF} 分别与不同的 NF 关联。

15 例 4:

终端设备生成的多个密钥中包括 K_{AMF} 、 K_{PCF} 、 K_{LMF} 和 K_{SMF} ，其中， K_{AMF} 与 AMF 关联， K_{PCF} 与 PCF 关联， K_{LMF} 与 LMF 关联， K_{SMF} 与 SMF 关联。也就是说， K_{AMF} 、 K_{PCF} 、 K_{LMF} 和 K_{SMF} 分别与不同的 NF 关联。

20 在本申请实施例中，从网络侧来说，与无线接入网设备直连的多个 NF 均生成相应的 NAS 密钥，例如，与无线接入网设备直连的多个 NF 包括 NF#1、NF#2 和 NF#3。NF#1 生成 NAS 密钥#1，NF#2 生成 NAS 密钥#2，NF#3 生成 NAS 密钥#3。下面以第一 NF 生成第一 NAS 密钥为例进行说明，第一 NF 为该多个 NF 中的一个。

S302，第一 NF 生成第一 NAS 密钥。

第一 NF 为终端设备生成的多个 NAS 密钥所对应的多个 NF 中的任意一个 NF。

25 可以理解的是，该多个 NF 为与无线接入网设备直连的 NF。该第一 NF 可以具有锚点功能（即，第一 NF 为锚点功能），也可以不具有锚点功能（即，第一 NF 为非锚点功能）。

关于第一 NF 生成第一 NAS 密钥的机制可以参考方法 400，这里先不展开说明。

30 例如，第一 NF 为 SMF，SMF 可以生成 K_{SMF} 。可选地，SMF 可以基于 K_{SMF} 生成用于 NAS 消息（即，终端设备与 SMF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASsmf-enc}$ ，和/或，基于 K_{SMF} 生成用于 NAS 消息完保的密钥，记为 $K_{NASsmf-int}$ 。

可以理解的是，第一 NF 根据是否要开启 NAS 消息加解密功能，决定是否生成与加解密相关的 NAS 密钥。类似地，第一 NF 根据是否要开启 NAS 消息完保功能，决定是否生成与完保相关的 NAS 密钥。

35 与终端设备类似，可选地，SMF 可以以 PDU 会话为粒度生成 K_{SMF} ， $K_{NASsmf-enc}$ 以及 $K_{NASsmf-int}$ 中的一项或多项。根据本申请实施例，SMF 以 PDU 会话为粒度生成 NAS 密钥，可以避免不同 SMF 针对同一终端设备生成的 NAS 密钥相同的情况，从而减少冲突概率。

又例如，第一 NF 为 LMF，LMF 可以生成 K_{LMF} 。可选地，LMF 可以基于 K_{LMF} 生成用于 NAS 消息（即，终端设备与 LMF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASlmf-enc}$ ，和/或，基于 K_{LMF} 生成用于 NAS 消息完保的密钥，记为 $K_{NASlmf-int}$ 。

又例如，第一 NF 为 PCF，PCF 可以生成 K_{PCF} 。可选地，PCF 可以基于 K_{PCF} 生成用于 NAS 消息（即，终端设备与 PCF 之间的 NAS 消息）加解密的密钥，记为 $K_{NASpcf-enc}$ ，和/或，基于 K_{PCF} 生成用于 NAS 消息完保的密钥，记为 $K_{NASpcf-int}$ 。

又例如，第一 NF 为 AMF，AMF 可以生成 K_{AMF} 。可选地，第一 NF 可以基于 K_{AMF} 生成 $K_{NASamf-enc}$ ，和/或， $K_{NASamf-int}$ 。

S303，第一 NF 基于在 S302 中生成的第一 NAS 密钥，处理与终端设备之间的 NAS 消息。相应地，终端设备基于在 S301 中生成的针对第一 NF 的第一 NAS 密钥，处理与第一 NF 之间的 NAS 消息。

以下行传输为例：

第一 NF 可以基于在 S302 中生成的第一 NAS 密钥对 NAS 消息进行加密，并发送 NAS 消息。相应地，终端设备可以接收 NAS 消息，并根据在 S301 中生成的第一 NAS 密钥对 NAS 消息进行解密。

例如，SMF 可以基于 $K_{NASsmf-enc}$ 对与一个终端设备通信的 NAS 消息进行加密，并向该终端设备发送 NAS 消息#1。相应地，该终端设备可以接收 NAS 消息#1，并根据 $K_{NASsmf-enc}$ 对 NAS 消息#1 进行解密。

又例如，LMF 可以基于 $K_{NASlmf-enc}$ 对与一个终端设备通信的 NAS 消息进行加密，并向该终端设备发送 NAS 消息#2。相应地，该终端设备可以接收 NAS 消息#2，并根据 $K_{NASlmf-enc}$ 对 NAS 消息#2 进行解密。

又例如，PCF 可以基于 $K_{NASpcf-enc}$ 对与一个终端设备通信的 NAS 消息进行加密，并向该终端设备发送 NAS 消息#3。相应地，该终端设备可以接收 NAS 消息#3，并根据 $K_{NASpcf-enc}$ 对 NAS 消息#3 进行解密。

以上行传输为例：

终端设备可以基于在 S301 中生成的第一 NAS 密钥对 NAS 消息进行加密，并发送 NAS 消息。相应地，第一 NF 可以接收 NAS 消息，并根据在 S302 中生成的第一 NAS 密钥对 NAS 消息进行解密。

例如，终端设备可以基于 $K_{NASsmf-enc}$ 对与一个 SMF 通信的 NAS 消息进行加密，并向该 SMF 发送 NAS 消息#a。相应地，该 SMF 可以接收 NAS 消息#a，并根据 $K_{NASsmf-enc}$ 对 NAS 消息#a 进行解密。

又例如，终端设备可以基于 $K_{NASlmf-enc}$ 对与一个 LMF 通信的 NAS 消息进行加密，并向该 LMF 发送 NAS 消息#b。相应地，该 LMF 可以接收 NAS 消息#b，并根据 $K_{NASlmf-enc}$ 对 NAS 消息#b 进行解密。

又例如，终端设备可以基于 $K_{NASpcf-enc}$ 对与一个 PCF 通信的 NAS 消息进行加密，并向该 PCF 发送 NAS 消息#c。相应地，该 PCF 可以接收 NAS 消息#c，并根据 $K_{NASpcf-enc}$ 对 NAS 消息#c 进行解密。

此外，作为一种情况，S302 中第一 NF 生成的第一 NAS 密钥与 S301 中终端设备针对该第一 NF 生成的第一 NAS 密钥可以是相同的。

例如，在对称加密场景中，SMF 可以基于 $K_{NASsmf-enc}$ 对 NAS 消息进行加密，并发送 NAS 消息，终端设备接收到该 NAS 消息后可以基于同样的 NAS 密钥 $K_{NASsmf-enc}$ 对 NAS 消息进行解密。

作为另一种情况, S302 中第一 NF 生成的第一 NAS 密钥与 S301 中终端设备针对该第一 NF 生成的第一 NAS 密钥可以是不同的。

例如, 在非对称加密场景中, 有两种密钥, 分别为私钥和公钥。SMF 可以基于公钥 $K_{NASsmf-enc}$ 对 NAS 消息进行加密, 并发送 NAS 消息, 终端设备接收到该 NAS 消息后可以
5 基于私钥 $K_{NASsmf-enc}$ 对 NAS 消息进行解密。

根据本申请实施例, 当无线接入网设备与多个控制面 CN NF 进行直连之后, 终端设备可以生成与该多个 CN NF 中每个 CN NF 相关联的一个或多个 NAS 密钥, 相应地该多个 CN NF 中的每个 CN NF 也可以生成 NAS 密钥, 从而对 NAS 消息进行处理 (例如, 进行加解密和/或完保)。

10 为了更好地理解本申请提出的方法 300, 下面结合方法 400, 以第一 NF 为例对上述方法 300 进行详细说明。可以理解的是, 该第一 NF 为与无线接入网设备直连的多个 NF 中的任意一个。具体地, 该方法 400 包括如下步骤。

S401, 终端设备向第一 NF 发送终端设备的安全能力信息。相应地, 第一 NF 接收来自终端设备的安全能力信息。

15 例如, 该第一 NF 可以具有锚点功能 (即, 第一 NF 为锚点功能), 也可以不具有锚点功能 (即, 第一 NF 为非锚点功能)。例如, 第一 NF 可以为 AMF、SMF、LMF、PCF 中的任一项。

下面介绍第一 NF 获取终端设备的安全能力信息的几种方式。

方式 1:

20 终端设备直接向第一 NF 发送终端设备的安全能力信息。

示例性地, 终端设备可以直接向第一 NF 发送 NAS 消息, 该 NAS 消息中包括终端设备的安全能力信息。

方式 2:

25 终端设备向无线接入网设备发送安全能力信息。进一步地, 无线接入网设备向第一 NF 发送终端设备的安全能力信息。

例如, 第一 NF 为 SMF, 终端设备可以向无线接入网设备发送该终端设备的安全能力信息, 进一步地, 无线接入网设备向 SMF 发送终端设备的安全能力信息。

30 作为另一种情况, 终端设备可以向无线接入网设备发送 NAS 消息, 该 NAS 消息中包括终端设备的安全能力信息。无线接入网设备不对该 NAS 消息进行解析。进一步地, 无线接入网设备向第一 NF 发送该 NAS 消息。即, 该 NAS 消息在无线接入网设备处是透传的。

方式 3:

35 终端设备向锚点功能 (例如, AMF) 发送安全能力信息。进一步地, 锚点功能向第一 NF 发送终端设备的安全能力信息。在该方式 3 中, 第一 NF 不为锚点功能, 或者说第一 NF 为非锚点功能。

例如, 第一 NF 为 LMF, 终端设备可以向 AMF 发送该终端设备的安全能力信息, 进一步地, AMF 向 LMF 发送终端设备的安全能力信息。

作为一种情况, 终端设备可以向锚点功能发送 NAS 消息, 该 NAS 消息中包括终端设备的安全能力信息, 进一步地, 锚点功能可以向第一 NF 发送该 NAS 消息。即, 该 NAS

消息在锚点功能处是透传的。

方式 4:

终端设备可以向无线接入网设备发送该终端设备的安全能力信息。进一步地，无线接入网设备向锚点功能（例如，AMF）发送终端设备的安全能力信息。进一步地，锚点功能向第一 NF 发送终端设备的安全能力信息。

可以理解的是，在该方式 4 中，该第一 NF 不为锚点功能。

例如，第一 NF 为 SMF，终端设备可以通过无线接入网设备、AMF 向 SMF 发送终端设备的安全能力信息。

作为一种情况，终端设备可以向无线接入网设备发送 NAS 消息，该 NAS 消息中包括终端设备的安全能力信息。进一步地，无线接入网设备向锚点功能发送该 NAS 消息。进一步地，锚点功能可以向第一 NF 发送该 NAS 消息。即，该 NAS 消息在锚点功能和无线接入网设备处是透传的。

S402，第一 NF 根据终端设备的安全能力信息以及第一 NF 的安全能力信息，选择安全算法。

S403，第一 NF 发送安全算法的信息。相应地，终端设备接收该安全算法的信息。

该安全算法的信息用于指示第一 NF 在 S402 中选择的安全算法。示例性地，该安全算法的信息为安全算法的标识。

下面介绍终端设备获取该安全算法的信息的几种方式。

方式 1:

第一 NF 向锚点功能（例如，AMF）发送该安全算法的信息。进一步地，锚点功能向终端设备发送该安全算法的信息。

可以理解的是，在该方式 1 中，第一 NF 不为锚点功能，或者说第一 NF 为非锚点功能。

例如，第一 NF 为 SMF，SMF 在选择了安全算法之后，可以将其选择的安全算法的标识通过 AMF 发送给终端设备。

作为一种情况，第一 NF 可以向锚点功能发送 NAS 消息，该 NAS 消息中包括安全算法的信息，进一步地，锚点功能向终端设备发送该 NAS 消息。即，该 NAS 消息在锚点功能处是透传的。

方式 2:

第一 NF 直接向终端设备发送该安全算法的信息。

作为一种情况，第一 NF 可以向终端设备发送 NAS 消息，该 NAS 消息中包括安全算法的信息。

方式 3:

第一 NF 向无线接入网设备发送该安全算法的信息。进一步地，无线接入网设备向终端设备发送该安全算法的信息。

例如，第一 NF 为 PCF，PCF 在选择了安全算法之后，可以将其选择的安全算法的标识通过无线接入网设备发送给终端设备。

作为一种情况，第一 NF 可以向无线接入网设备发送 NAS 消息，该 NAS 消息中包括安全算法的信息。进一步地，无线接入网设备可以向终端设备发送该 NAS 消息。即，该

NAS 消息在无线接入网设备处是透传的。

方式 4:

第一 NF 可以向锚点功能（例如，AMF）发送安全算法的信息。进一步地，锚点功能向无线接入网设备发送该安全算法的信息。进一步地，无线接入网设备向终端设备发送该安全算法的信息。

可以理解的是，在该方式 4 中，第一 NF 不为锚点功能。

例如，第一 NF 为 SMF，SMF 可以将其选择的安全算法的标识通过 AMF 和无线接入网设备发送给终端设备。

作为一种情况，第一 NF 可以向锚点功能发送 NAS 消息，该 NAS 消息中包括安全算法的信息。进一步地，锚点功能可以向无线接入网设备发送该 NAS 消息。进一步地，无线接入网设备可以向终端设备发送该 NAS 消息。即，该 NAS 消息在锚点功能和无线接入网设备处是透传的。

S404，第一 NF 创建（或者说，建立）NAS 实体。

可以理解的是，该 NAS 实体可以用于生成 NAS 消息，对 NAS 消息进行加密，对 NAS 消息进行解密，对 NAS 消息进行完整性保护，维护 NAS 安全上下文。

下面分情况对第一 NF 创建 NAS 实体的触发条件进行说明。

情况 1:

在成功对终端设备进行接入鉴权后，第一 NF 创建第一 NF 对应的 NAS 实体。

例如，该第一 NF 为 PCF。在 PCF 成功对终端设备进行接入鉴权的情况下，PCF 创建 PCF 对应的 NAS 实体，记为 NASpcf 实体。

情况 2:

第一 NF 接收消息#A，并根据消息#A 创建第一 NF 对应的 NAS 实体。可以理解的是，该消息#A 可以来自终端设备、无线接入网设备、AMF（此时，第一 NF 不为 AMF）、增强的服务移动定位中心（enhanced serving mobile location centre, E-SMLC）、安全的用户面定位（secure user plane location, SUPL）定位平台（SUPL location platform, SLP）中的任一项。

例如，该第一 NF 为 SMF。示例性地，该消息#A 可以显式指示 SMF 创建 SMF 对应的 NAS 实体，记为 NASsmf 实体。例如，该消息#A 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#A 指示 SMF 创建 NASsmf 实体。

或者，该消息#A 可以隐式指示 SMF 创建 NASsmf 实体（例如，该消息#A 为 PDU 会话创建消息（PDU session create 消息））。即，可以复用 PDU 会话创建消息隐式指示 SMF 创建 NASsmf 实体。

例如，该第一 NF 为 LMF。示例性地，该消息#A 可以显式指示 LMF 创建 LMF 对应的 NAS 实体，记为 NASlmf 实体。例如，该消息#A 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#A 指示 LMF 创建 NASlmf 实体。

或者，该消息#A 可以隐式指示 LMF 创建 NASlmf 实体（例如，该消息#A 为定位业务启动消息）。即，可以复用定位业务启动消息隐式指示 LMF 创建 NASlmf 实体。

例如，该第一 NF 为 PCF。示例性地，该消息#A 可以显式指示 PCF 创建 NASpcf 实体。例如，该消息#A 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#A 指示

PCF 创建 NASpcf 实体。

或者, 该消息#A 可以隐式指示 PCF 创建 NASpcf 实体。例如, 该消息#A 可以为 AMF 向 PCF 发送的 AM policy association establishment 消息, 或者 AM policy association modification 消息, 或者, UE policy association establishment 消息等。即, 可以复用现有的消息隐式指示 PCF 创建 NASpcf 实体。

S405, 第一 NF 生成第一 NAS 密钥。

可以理解的是, 本申请对 S404 和 S405 的执行顺序不作限定。例如, S404 可以在 S405 之前执行, 也可以在 S405 之后执行。

具体而言, 第一 NF 可以获取 NAS 根密钥, 并基于 NAS 根密钥, 生成第一 NAS 密钥。可以理解的是, 如果第一 NF 为锚点功能, 则第一 NF 可以生成 NAS 根密钥。如果第一 NF 不为锚点功能, 第一 NF 可以从锚点功能 (例如, AMF) 获取 NAS 根密钥, 例如, SMF、PCF、LMF 等 NF 可以从 AMF 获取 NAS 根密钥。

示例性地, NAS 根密钥为安全锚定功能对应的密钥, 记为 K_{SEAF} , 或者 NAS 根密钥为接入和移动性管理功能对应的密钥, 记为 K_{AMF} , 或者, NAS 根密钥为基于 K_{SEAF} 派生的密钥 (但不是 K_{AMF} , 或者说与 K_{AMF} 不同), 或者, NAS 根密钥为基于 K_{AMF} 派生的密钥。

下面以 NAS 根密钥为 K_{SEAF} 或者 K_{AMF} 为例, 对第一 NF 生成第一 NAS 密钥的过程进行说明。

(1) NAS 根密钥为 K_{SEAF} 。

该第一 NF 为 SMF, SMF 基于 K_{SEAF} 生成 K_{SMF} , 可选地, SMF 可以基于 K_{SMF} 生成 $K_{NASsmf-enc}$, 和/或, $K_{NASsmf-int}$ 。

或者, 该第一 NF 为 LMF, LMF 基于 K_{SEAF} 生成 K_{LMF} , 可选地, LMF 可以基于 K_{LMF} 生成 $K_{NASlmf-enc}$, 和/或, $K_{NASlmf-int}$ 。

或者, 该第一 NF 为 PCF, PCF 基于 K_{SEAF} 生成 K_{PCF} , 可选地, PCF 可以基于 K_{PCF} 生成 $K_{NASpcf-enc}$, 和/或, $K_{NASpcf-int}$ 。

或者, 该第一 NF 为 AMF, AMF 基于 K_{SEAF} 生成 K_{AMF} , 可选地, AMF 可以基于 K_{AMF} 生成用于 NAS 消息 (即, 终端设备与 AMF 之间的 NAS 消息) 加解密的密钥, 记为 $K_{NASamf-enc}$, 和/或, 用于 NAS 消息完保的密钥, 记为 $K_{NASamf-int}$ 。

(2) NAS 根密钥为 K_{AMF} 。

该第一 NF 为 SMF, SMF 基于 K_{AMF} 生成 K_{SMF} , 可选地, SMF 可以基于 K_{SMF} 生成 $K_{NASsmf-enc}$, 和/或, $K_{NASsmf-int}$ 。

或者, 该第一 NF 为 LMF, LMF 基于 K_{AMF} 生成 K_{LMF} , 可选地, LMF 可以基于 K_{LMF} 生成 $K_{NASlmf-enc}$, 和/或, $K_{NASlmf-int}$ 。

或者, 该第一 NF 为 PCF, PCF 基于 K_{AMF} 生成 K_{PCF} , 可选地, PCF 可以基于 K_{PCF} 生成 $K_{NASpcf-enc}$, 和/或, $K_{NASpcf-int}$ 。

或者, 该第一 NF 为 AMF, 可选地, AMF 可以基于 K_{AMF} 生成 $K_{NASamf-enc}$, 和/或, $K_{NASamf-int}$ 。

接下来对生成第一 NAS 密钥时的输入参数进行说明。

在本申请实施例中, 第一 NF 可以将第一 NF 的类型参数、第一 NF 的标识、第一 NF

的 NAS count、安全算法标识、PDU 会话标识中的一项或多项作为输入参数。其中，第一 NF 的 NAS count 可以是第一 NF 维护的。本申请对输入参数的组合形式不作限定，下面对输入参数的几种可能的情况进行说明。可以理解的是，下述几种情况仅仅是示例性地。

情况 1:

- 5 第一 NF 可以将第一 NF 的类型参数和/或第一 NF 的标识、第一 NF 维护的 NAS count、安全算法标识（即，在 S402 中选择的安全算法的标识）作为输入参数，并将输入参数输入到相应的算法中。

在本申请实施例中，“第一 NF 的类型参数和/或第一 NF 的标识”可以包括三种可选的情况，即：“第一 NF 的类型参数”、“第一 NF 的标识”以及“第一 NF 的类型参数和第一 NF 的标识”。关于此，下文不再赘述。

10 示例性地，第一 NF 可以将输入参数输入到下一代加密算法（next generation encryption algorithm, NEA）中，例如，128-NEA1，或者，128-NEA2，或者 128-NEA3 中。关于此，下文不再赘述。

例如，第一 NF 为 PCF，PCF 在生成 K_{PCF} 时，可以将 PCF 的类型参数和/或 PCF 的标识、PCF 维护的 NAS count、PCF 在 S402 选择的安全算法标识作为输入参数。

例如，第一 NF 为 LMF，LMF 在生成 K_{LMF} 时，可以将 LMF 的类型参数和/或 LMF 的标识、LMF 维护的 NAS count、LMF 在 S402 选择的安全算法标识作为输入参数。

情况 2:

- 20 第一 NF 可以将第一 NF 的类型参数和/或第一 NF 的标识、第一 NF 维护的 NAS count、安全算法标识（即，在 S402 中选择的安全算法的标识）、PDU 会话标识（PDU session id）作为输入参数。

例如，第一 NF 为 SMF，SMF 在生成 K_{SMF} 时，可以将 SMF 的类型参数、SMF 维护的 NAS count、SMF 在 S402 选择的安全算法标识、PDU 会话标识作为输入参数。

情况 3:

- 25 第一 NF 可以将第一 NF 维护的 NAS count、安全算法标识（即，在 S402 中选择的安全算法的标识）、PDU 会话标识作为输入参数。

例如，第一 NF 为 SMF，SMF 在生成 K_{SMF} 时，可以将 SMF 维护的 NAS count、SMF 在 S402 选择的安全算法标识、PDU 会话标识作为输入参数。

- 30 由上述情况 1 至情况 3 可知，在本申请实施例中，与无线接入网设备直连的多个 NF 中的每个 NF 可以分别维护 NAS count。

作为一种方式，与无线接入网设备直连的多个 NF 维护的 NAS count 可以从 0 开始计数。

- 35 作为另一种方式，与无线接入网设备直连的多个 NF 维护的 NAS count 可以从锚点功能（例如，AMF）的初始 NAS count 开始计数。以该多个 NF 中的第一 NF 为例，可以理解的是，如果第一 NF 不为锚点功能，此时，第一 NF（例如，SMF、PCF 或者 LMF）可以从锚点功能获取锚点功能的初始 NAS count。

可以理解的是，在上述情况 1 至情况 3 中，通过将多个参数作为输入参数，生成的 NAS 密钥发生冲突的概率较小。

情况 4:

第一 NF 可以只将第一 NF 的类型参数、第一 NF 的标识、第一 NF 维护的 NAS count、安全算法标识、PDU 会话标识中的一项作为输入参数。

例如，第一 NF 可以只将第一 NF 的类型参数作为输入参数，生成 NAS 密钥。

可以理解的是，通过将一个参数作为输入参数，可以简化 NAS 密钥生成机制，降低 NAS 密钥生成算法的复杂度。

S406，第一 NF 激活第一 NAS 密钥。

该 S406 为可选的步骤。可以理解的是，如果激活了第一 NAS 密钥，第一 NF 可以对 NAS 消息进行加解密和/或完整性保护。如果不激活第一 NAS 密钥，第一 NF 与终端设备之间也可以传输 NAS 消息。

下面介绍第一 NF 激活第一 NAS 密钥的触发条件。

情况 1:

在创建第一 NF 对应的 NAS 实体时，第一 NF 激活第一 NAS 密钥。

例如，PCF 可以在创建 NASpcf 实体时激活 K_{PCF} ，LMF 可以在创建 NASlmf 实体时激活 K_{LMF} ，SMF 可以在创建 NASsmf 实体时激活 K_{SMF} 。

情况 2:

第一 NF 接收消息#B（即，第五消息），并根据消息#B 激活第一 NAS 密钥。

示例性地，该消息#B 可以来自终端设备、无线接入网设备、AMF（此时，第一 NF 不为 AMF）、E-SMLC、SLP 中的任一项。

例如，该第一 NF 为 SMF，SMF 收到了 PDU 会话创建消息（消息#B 的一个例子），该 PDU 会话创建消息可以隐式指示 SMF 创建 NAS 实体，生成并激活 NAS 密钥。

S407，终端设备创建 NAS 实体。

下面分情况对终端设备创建 NAS 实体的触发条件进行说明。

情况 1:

在终端设备首次接入核心网网络，并认证鉴权成功后，终端设备创建第一 NF 对应的 NAS 实体。

例如，在终端设备首次接入核心网网络，并且认证鉴权成功后，终端设备创建 NASamf 实体、NASpcf 实体、NASsmf 实体、NASlmf 实体中的一项或多项。

情况 2:

终端设备接收消息#C，并根据消息#C 创建第一 NF 对应的 NAS 实体。可选地，消息#C 用于指示需要创建的 NAS 实体标识。

作为一种实现方式，该消息#C 可以显式指示终端设备创建 NAS 实体。例如，该消息#C 为 NAS 安全模式命令（securitymodecommand，SMC）消息。该 NAS SMC 消息中包括一个或多个比特，该一个或多个比特可以用于指示终端设备创建 NASamf 实体、NASpcf 实体、NASsmf 实体、NASlmf 实体中的一项或多项。

例如，AMF 可以向终端设备发送 NAS SMC 消息。可选地，SMF、PCF、LMF 也可以向终端设备发送 NAS SMC 消息。

作为另一种实现方式，该消息#C 可以隐式指示终端设备创建 NAS 实体。

例如，终端设备可以向网络侧发送 PDU 会话创建请求消息（PDU session create request 消息），终端设备可以接收来自网络侧的 PDU 会话创建接受消息（PDU session create accept 消息）。

消息), 终端设备在收到该 PDU 会话创建接受消息后, 可以针对每个 PDU 会话建立 1 个 NASsmf 实体。

又例如, AMF 可以向终端设备发送定位业务开启消息, 终端设备在收到该定位业务开启消息后创建 NASlmf 实体。

5 又例如, LMF 可以向 UE 发送 LTE 定位协议(LTE positioning protocol, LPP)请求定位信息 (requestlocationinformation) 消息, 终端设备基于该消息创建 NASlmf 实体。

S408, 终端设备生成多个 NAS 密钥。该多个 NAS 密钥中的至少两个 NAS 密钥分别与多个 NF 中的不同的 NF 关联。

可以理解的是, 本申请对 S407 和 S408 的执行顺序不作限定。例如, S407 可以在 S408
10 之前执行, 也可以在 S408 之后执行。

具体而言, 终端设备可以基于 NAS 根密钥, 生成 NAS 密钥。与网络侧不同的是, 终端设备可以生成 NAS 根密钥。例如, 终端设备可以生成 K_{AMF} 或者 K_{SEAF} 。关于该 NAS 根密钥可以参考上文。

下面以 NAS 根密钥为 K_{SEAF} 或者 K_{AMF} 为例, 介绍终端设备生成多个 NAS 密钥的过程。
15

(1) NAS 根密钥为 K_{SEAF} 。

终端设备可以基于 K_{SEAF} 生成 K_{SMF} 。可选地, 终端设备可以基于 K_{SMF} 生成 $K_{NASsmf-enc}$, 和/或, $K_{NASsmf-int}$ 。

终端设备可以基于 K_{SEAF} 生成 K_{LMF} 。可选地, 终端设备可以基于 K_{LMF} 生成 $K_{NASlmf-enc}$,
20 和/或, $K_{NASlmf-int}$ 。

终端设备可以基于 K_{SEAF} 生成 K_{PCF} 。可选地, 终端设备可以基于 K_{PCF} 生成 $K_{NASpcf-enc}$, 和/或, $K_{NASpcf-int}$ 。

终端设备可以基于 K_{SEAF} 生成 K_{AMF} 。可选地, 终端设备可以基于 K_{AMF} 生成 $K_{NASamf-enc}$, 和/或, $K_{NASamf-int}$ 。

25 (2) NAS 根密钥为 K_{AMF} 。

终端设备可以基于 K_{AMF} 生成 K_{SMF} 。可选地, 终端设备可以基于 K_{SMF} 生成 $K_{NASsmf-enc}$, 和/或, $K_{NASsmf-int}$ 。

终端设备可以基于 K_{AMF} 生成 K_{LMF} 。可选地, 终端设备可以基于 K_{LMF} 生成 $K_{NASlmf-enc}$, 和/或, $K_{NASlmf-int}$ 。

30 终端设备可以基于 K_{AMF} 生成 K_{PCF} 。可选地, 终端设备可以基于 K_{PCF} 生成 $K_{NASpcf-enc}$, 和/或, $K_{NASpcf-int}$ 。

可选地, 终端设备可以基于 K_{AMF} 生成 $K_{NASamf-enc}$, 和/或, $K_{NASamf-int}$ 。

终端设备生成的多个 NAS 密钥中包括终端设备针对第一 NF 生成的第一密钥。接下来以第一 NF 为例, 对终端设备生成针对第一 NF 的第一 NAS 密钥时的输入参数进行说明。

35 示例性地, 终端设备可以将输入参数输入到 NEA 中, 例如, 128-NEA1, 或者, 128-NEA2, 或者 128-NEA3 中。

在本申请实施例中, 终端设备可以将第一 NF 的类型参数、第一 NF 的标识、第一 NF 的 NAS count、安全算法标识、PDU 会话标识中的一项或多项作为输入参数。其中, 第一 NF 的 NAS count 可以是终端设备维护的, 也可以是从其他 NF 处获取的。本申请对输入

参数的组合形式不作限定，下面对输入参数的几种可能的情况进行说明。可以理解的是，下述几种情况仅仅是示例性地。

情况 A:

5 终端设备可以将第一 NF 的类型参数和/或第一 NF 的标识、第一 NF 的 NAS count、安全算法标识（即，在 S403 中接收到的来自第一 NF 的安全算法的标识）作为输入参数。

例如，第一 NF 为 PCF，终端设备在生成 K_{PCF} 时，可以将 PCF 的类型参数、终端设备维护的 PCF 的 NAS count、在 S403 中接收到的来自 PCF 的安全算法标识作为输入参数。

10 例如，第一 NF 为 LMF，终端设备在生成 K_{LMF} 时，可以将 LMF 的类型参数、终端设备维护的 LMF 的 NAS count、在 S403 中接收到的来自 LMF 的安全算法标识作为输入参数。

情况 B:

终端设备可以将第一 NF 的类型参数和/或第一 NF 的标识、第一 NF 的 NAS count、安全算法标识（即，在 S403 中接收到的来自第一 NF 的安全算法的标识）、PDU 会话标识作为输入参数。

15 例如，第一 NF 为 SMF，终端设备在生成 K_{SMF} 时，可以将 SMF 的类型参数、终端设备维护的 SMF 的 NAS count、在 S403 中接收到的来自 SMF 的安全算法标识、PDU 会话标识作为输入参数。

情况 C:

20 终端设备可以将第一 NF 的 NAS count，安全算法标识（即，在 S403 中接收到的安全算法的标识）、PDU 会话标识（PDU session id）作为输入参数。

例如，第一 NF 为 SMF，终端设备在生成 K_{SMF} 时，可以将终端设备维护的 SMF 的 NAS count、安全算法标识和 PDU 会话标识作为输入参数。

由情况 A 至情况 C 可知，在多个 NF 分别与无线接入网设备直接连接的情况下，终端设备可以维护该多个 NF 的 NAS count。

25 作为一种方式，该多个 NF 中的各个 NF 的 NAS count 可以从 0 开始计数。

作为另一种方式，该多个 NF 中的各个 NF 的 NAS count 可以从锚点功能（例如，AMF）的初始 NAS count 开始计数，此时，终端设备可以从锚点功能获取锚点功能的初始 NAS count。

S409，终端设备激活在 S408 中生成的多个 NAS 密钥。

30 下面以第一 NF 为例，对终端设备激活第一 NAS 密钥的触发条件进行说明。其中，该第一 NAS 密钥为终端设备针对第一 NF 生成的 NAS 密钥。

该 S409 为可选的步骤。可以理解的是，如果激活了第一 NAS 密钥，终端设备可以对 NAS 消息进行加解密和/或完整性保护。如果不激活第一 NAS 密钥，第一 NF 与终端设备之间也可以传输 NAS 消息。

35 情况 1:

在创建第一 NF 对应的 NAS 实体时，终端设备激活第一 NAS 密钥。

例如，第一 NF 为 SMF，终端设备在创建 SMF 对应的 NAS 实体时，终端设备激活 K_{SMF} ， $K_{NASsmf-enc}$ 以及 $K_{NASsmf-int}$ 。

情况 2:

终端设备接收消息#D（即，第一消息），并根据消息#D 激活第一 NAS 密钥。

例如，AMF 可以向终端设备发送消息#D（示例性地，该消息#D 可以是加密的），终端设备可以根据该消息#D 激活 AMF 相关的 NAS 密钥。

又例如，SMF 可以向终端设备发送消息#D（示例性地，该消息#D 可以不加密），终端设备可以根据该消息#D 激活 SMF 关联的 NAS 密钥。

又例如，PCF 可以向终端设备发送消息#D（示例性地，该消息#D 可以不加密），终端设备可以根据该消息#D 激活 PCF 关联的 NAS 密钥。

又例如，LMF 可以向终端设备发送消息#D（示例性地，该消息#D 可以不加密），终端设备可以根据该消息#D 激活 LMF 关联的 NAS 密钥。

10 可选地，在终端设备成功激活第一 NAS 密钥之后，终端设备可以发送激活成功信息。相应地，第一 NF 接收激活成功信息。该激活成功信息指示终端设备成功激活第一 NAS 密钥。

示例性地，终端设备可以直接向第一 NF 发送激活成功信息。

或者，终端设备可以通过无线接入网设备向第一 NF 发送激活成功信息。

15 或者，终端设备可以通过无线接入网设备、锚点功能（例如，AMF）向第一 NF 发送激活成功信息。可以理解的是，此时第一 NF 不为锚点功能。

应理解，基于该激活成功信息，第一 NF 可以获知终端设备成功激活第一 NAS 密钥，在此之后，第一 NF 向终端设备发送 NAS 消息。基于此，可以避免第一 NF 发送了 NAS 消息，但是由于终端设备未激活第一 NAS 密钥，导致终端设备不能处理该 NAS 消息的情况（例如，终端设备不能对该 NAS 消息进行解密）。

20 可选地，第一 NF 可以默认终端设备成功激活第一 NAS 密钥。此时，终端设备无需向第一 NF 发送上述激活成功信息。

S410，第一 NF 基于在 S405 中生成的第一 NAS 密钥，处理与终端设备之间的 NAS 消息。相应地，终端设备基于在 S408 中生成的针对第一 NF 的第一 NAS 密钥，处理与第一 NF 之间的 NAS 消息。

此外，作为一种情况，S405 中第一 NF 生成的第一 NAS 密钥与 S408 中终端设备针对该第一 NF 生成的第一 NAS 密钥可以是相同的。作为一种情况，S405 中第一 NF 生成的第一 NAS 密钥与 S408 中终端设备针对该第一 NF 生成的第一 NAS 密钥可以是不同的。关于此，可以参考上文，不再赘述。

30 关于该过程可以参考 S303 中的描述。

可选地，在上述方法 400 中，S401 至 S403、S404 至 S406、S407 至 S409 可以是相互独立的。换句话说，S404 至 S406 可以不依赖 S401 至 S403 的执行（或者说，可以不在 S401 至 S403 的基础上执行），S407 至 S409 也可以不依赖 S401 至 S403 的执行，S407 至 S409 也可以不依赖 S404 至 S406 的执行。

35 可选地，S404 至 S409 中的每一项可以是相互独立的。即，S404 至 S409 中的每一项可以独立执行，相互之间不具有依赖关系。

根据本申请实施例，当无线接入网设备与多个 CN NF 进行直连之后，终端设备可以生成与该多个 CN NF 中每个 NF 相关联的 NAS 密钥，相应地该多个 CN NF 中的每个 CN NF 也可以生成 NAS 密钥，从而终端设备和该多个 CN NF 可以对 NAS 消息进行处理（例

如，进行加解密和/或完保）。

本申请还提出了 NAS 安全机制中的 NAS 实体的暂停 (suspend) 机制。图 5 示出了本申请提出的方法 500，可以理解的是，作为一种实现方式，方法 500 可以在方法 400 的基础上执行。具体地，该方法 500 包括如下步骤。

5 S501，第一 NF 暂停 NAS 实体，并保存第一 NF 的安全上下文。

第一 NF 的安全上下文包括第一 NF 的 NAS count、第一 NF 选择的安全算法标识、终端设备的标识、第一 NF 的类型、第一 NF 的标识、PDU 会话标识中的一项或多项。

例如，第一 NF 的安全上下文包括第一 NF 的 NAS count、第一 NF 选择的安全算法标识、终端设备的标识。可选的，第一 NF 的安全上下文还包括第一 NF 的类型、第一 NF 的标识、PDU 会话标识中的一项或多项。

也就是说，在本申请实施例中，与无线接入网设备直连的各个 NF 会维护 NAS count。例如，SMF 可以以 PDU 会话为粒度维护 NAS count。AMF 可以维护 AMF 的 NAS count。LMF 可以维护 LMF 的 NAS count。PCF 可以维护 PCF 的 NAS count。

作为一种实现方式，第一 NF 接收消息#E，并根据消息#E 暂停第一 NF 对应的 NAS 实体。示例性地，该消息#E 可以是终端设备、无线接入网设备、或者其他 CN NF 发送的。

例 1:

第一 NF 为 PCF。AMF 可以向 PCF 发送消息#E1，该消息#E1 用于指示 PCF 暂停 NASpcf 实体。

示例性地，该消息#E1 可以显式指示 PCF 暂停 NASpcf 实体。例如，该消息#E1 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#E1 指示 PCF 暂停 NASpcf 实体。

或者，该消息#E1 可以隐式指示 PCF 暂停 NASpcf 实体。例如，可以复用某一消息，通过该消息的消息类型隐式地指示 PCF 暂停 NASpcf 实体。

例 2:

第一 NF 为 SMF。AMF 可以向 SMF 发送消息#E2，该消息#E2 用于指示 SMF 暂停 NASsmf 实体。

示例性地，该消息#E2 可以显式指示 SMF 暂停 NASsmf 实体。例如，该消息#E2 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#E2 指示 SMF 暂停 NASsmf 实体。

或者，该消息#E2 可以隐式指示 SMF 暂停 NASsmf 实体（例如，该消息#E2 为 PDU 会话删除（PDU session delete）消息）。即，可以复用 PDU 会话删除消息隐式指示 SMF 暂停 NASsmf 实体。

例 3:

第一 NF 为 LMF。AMF 可以向 LMF 发送消息#E3，并根据该消息#E3 暂停 NASlmf 实体。

示例性地，该消息#E3 可以显式指示 LMF 暂停 NASlmf 实体。例如，该消息#E3 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#E3 指示 LMF 暂停 NASlmf 实体。

或者，该消息#E3 可以隐式指示 LMF 暂停 NASlmf 实体（例如，该消息#E3 为定位业务删除消息）。即，可以复用定位业务删除消息隐式指示 LMF 暂停 NASlmf 实体。

S502，终端设备暂停第一 NF 对应的 NAS 实体，并保存第一 NF 的安全上下文。

第一 NF 的安全上下文包括第一 NF 的类型、第一 NF 的标识、第一 NF 的 NAS count，

第一 NF 选择的安全算法标识、PDU 会话标识、终端设备的标识中的一项或多项。

例如，第一 NF 的安全上下文包括第一 NF 的类型和/或第一 NF 的标识、第一 NF 的 NAS count，第一 NF 选择的安全算法标识。可选的，第一 NF 的安全上下文还可以包括 PDU 会话标识、终端设备的标识中的一项或多项。

- 5 在本申请实施例中，终端设备可以维护多种 NAS count。例如，终端设备可以以 PDU 会话为粒度维护 SMF 的 NAS count。终端设备可以维护 AMF 的 NAS count。终端设备可以维护 LMF 的 NAS count。终端设备可以维护 PCF 的 NAS count。

下面对该 S502 的触发条件进行说明。

情况 1:

- 10 在终端设备进入空闲态或非激活态的情况下，终端设备暂停第一 NF 对应的 NAS 实体，并保存第一 NF 的安全上下文。

例如，在终端设备进入空闲态或非激活态的情况下，终端设备暂停 NASmf 实体和/或 NASpcf 实体。

情况 2:

- 15 终端设备接收消息#F，并根据消息#F 暂停第一 NF 对应的 NAS 实体。

例如，该消息#F 可以为 RRC 释放(release)消息，或者 NAS 去注册(NAS de-registration)消息，终端设备收到该消息#F 后，暂停 NASmf 实体和/或 NASpcf 实体。

例如，该消息#F 可以为 PDU 会话释放消息(PDU sessionrelease 消息)，终端设备收到该消息#F 后，暂停 NASsmf 实体。

- 20 例如，该消息#F 可以为定位业务释放消息，终端设备收到该消息#F 后，暂停 NASlmf 实体。

可以理解的是，如果第一 NF 和终端设备暂停 NAS 实体时保存了安全上下文，在后续恢复 NAS 实体时第一 NF 和终端设备可以无需从其他网元获取安全上下文，从而减少信令交互，提高恢复 NAS 实体的效率。

- 25 本申请还提出了 NAS 安全机制中的 NAS 实体的删除(delete)机制。图 6 示出了本申请提出的方法 600，可以理解的是，作为一种实现方式，方法 600 可以在方法 400，或者方法 400 和方法 500 的基础上执行。具体地，该方法 600 包括如下步骤。

S601，第一 NF 删除 NAS 实体，并删除第一 NF 的安全上下文。

- 30 作为一种实现方式，第一 NF 可以接收消息#G，并根据消息#G 删除第一 NF 对应的 NAS 实体，并删除第一 NF 的安全上下文。

例 1:

第一 NF 为 PCF。AMF 可以向 PCF 发送消息#G1，该消息#G1 用于指示 PCF 删除 NASpcf 实体。

- 35 示例性地，该消息#G1 可以显式指示 PCF 删除 NASpcf 实体。例如，该消息#G1 中可以包括 1 个比特，当该比特的取值为“1”时，该消息#G1 指示 PCF 删除 NASpcf 实体。

或者，该消息#G1 可以隐式指示 PCF 删除 NASpcf 实体。例如，可以复用某一消息，通过该消息的消息类型隐式地指示 PCF 删除 NASpcf 实体。

例 2:

第一 NF 为 SMF。AMF 可以向 SMF 发送消息#G2，该消息#G2 用于指示 SMF 删除

NASsmf 实体。

示例性地，该消息#G2 可以显式指示 SMF 删除 NASsmf 实体。例如，该消息# G2 中可以包括 1 个比特，当该比特的取值为“1”时，该消息# G2 指示 SMF 删除 NASsmf 实体。

5 或者，该消息#G2 可以隐式指示 SMF 删除 NASsmf 实体（例如，该消息#G2 为 PDU 会话删除（PDU session delete）消息）。即，可以复用 PDU 会话删除消息隐式指示 SMF 删除 NASsmf 实体。

例 3:

第一 NF 为 LMF。LMF 可以接收消息#G3，并根据该消息#G3 删除 NASlmf 实体。

10 示例性地，该消息#G3 可以显式指示 LMF 删除 NASlmf 实体。例如，该消息# G3 中可以包括 1 个比特，当该比特的取值为“1”时，该消息# G3 指示 LMF 删除 NASlmf 实体。

或者，该消息#G3 可以隐式指示 LMF 删除 NASlmf 实体（例如，该消息#G3 为定位业务删除消息）。即，可以复用定位业务删除消息隐式指示 LMF 删除 NASlmf 实体。

S602，终端设备删除第一 NF 对应的 NAS 实体，并删除第一 NF 的安全上下文。

下面对该 S602 的触发条件进行说明。

15 情况 1:

在终端设备进入空闲态或非激活态的情况下，终端设备删除第一 NF 对应的 NAS 实体，并删除第一 NF 的安全上下文。

例如，在终端设备进入空闲态或非激活态的情况下，终端设备删除 NASamf 实体和/或 NASpcf 实体。

20 情况 2:

终端设备接收消息#H，并根据消息#H 删除第一 NF 对应的 NAS 实体。

类似的，该消息#H 可以显示或隐式指示终端设备删除第一 NF 对应的 NAS 实体。

例如，该消息#H 可以为 RRC 释放（release）消息，或者 NAS de-registration 消息，终端设备收到该消息#H 后，删除 NASamf 实体和/或 NASpcf 实体。

25 例如，该消息#H 可以为 PDU 会话释放消息（PDU sessionrelease 消息），终端设备收到该消息#H 后，删除 NASsmf 实体。

例如，该消息#H 可以为定位业务释放消息，终端设备收到该消息#H 后，删除 NASlmf 实体。

30 可以理解的是，在删除 NAS 实体的同时删除安全上下文，可以节省终端设备和第一 NF 的存储空间。

本申请还提出了 NAS 安全机制中的 NAS 密钥的去激活（deactivate）机制。具体地，图 7 示出了本申请提出的方法 700，可以理解的是，作为一种实现方式，方法 700 可以在方法 400 的基础上执行。具体地，该方法 700 包括如下步骤。

S701，第一 NF 去激活第一 NAS 密钥。

35 下面介绍 S701 的触发条件。

情况 1:

在暂停或者删除第一 NF 对应的 NAS 实体时，第一 NF 去激活第一 NAS 密钥。

情况 2:

第一 NF 接收消息#I（即，第六消息），并根据消息#I 去激活第一 NAS 密钥。

类似的, 该消息#I 可以显示或隐式指示第一 NF 去激活第一 NAS 密钥。

例如, 第一 NF 为 AMF, 无线接入网设备可以向 AMF 发送 UE 上下文释放请求 (UE context release request) 消息 (消息#I 的一个例子), AMF 可以根据该消息去激活 AMF 相关的 NAS 密钥。或者, AMF 可以在向无线接入网设备发送 UE 上下文释放命令 (UE context release command) 之后, 去激活 AMF 相关的 NAS 密钥。

又例如, 第一 NF 为 SMF, 无线接入网设备可以向 SMF 发送 UE 上下文释放请求消息, SMF 可以根据该消息去激活 SMF 相关的 NAS 密钥。或者, SMF 可以在向无线接入网设备发送 UE 上下文释放命令之后, 去激活 SMF 相关的 NAS 密钥。

S702, 终端设备去激活针对第一 NF 生成的第一 NAS 密钥。

下面介绍 S702 的触发条件。

情况 1:

在暂停或者删除第一 NF 对应的 NAS 实体时, 终端设备去激活第一 NAS 密钥。

情况 2:

终端设备接收消息#J (即, 第二消息), 并根据消息#J 去激活第一 NAS 密钥。

类似的, 该消息#J 可以显示或隐式指示终端设备去激活第一 NAS 密钥。

例如, 终端设备可以在接收到无线接入网设备发送的接入网连接释放 (AN connection release) 消息 (消息#J 的一个例子) 后, 去激活第一 NAS 密钥。

又例如, 终端设备可以在向无线接入网设备发送 AN connection release 消息后, 去激活第一 NAS 密钥。

可选地, 在终端设备成功去激活第一 NAS 密钥之后, 终端设备可以发送去激活成功信息。相应地, 第一 NF 接收来自终端设备的去激活成功信息。该去激活成功信息用于指示终端设备成功去激活第一 NAS 密钥。

具体地, 终端设备可以通过无线接入网设备向第一 NF 发送去激活成功信息。

或者, 终端设备可以通过无线接入网设备、锚点功能 (例如, AMF) 向第一 NF 发送去激活成功信息。可以理解的是, 此时第一 NF 不为锚点功能。

可选地, 本申请还提出了终端设备从空闲态 (idle) 或者非激活态 (inactive) 转为连接态 (connected) 时的 NAS 安全机制。

图 8 示出了本申请提出的方法 800, 可以理解的是, 作为一种实现方式, 方法 800 可以在方法 400 的基础上执行。具体地, 该方法 800 包括 4 种并列的情况, 分别为 S801、S802、S803 和 S804。

S801, 终端设备从连接态转为空闲态或非激活态时, 第一 NF 和终端设备均保存安全上下文。在终端设备重新从空闲态或非激活态转入连接态时, 第一 NF 和终端设备分别根据保存的安全上下文生成第一 NAS 密钥。

如前文所述, 可以理解的是, 第一 NF 生成的第一 NAS 密钥与终端设备生成的针对第一 NF 的第一 NAS 密钥可以是相同的, 也可以是不同的。不再赘述。

该安全上下文包括第一 NF 的类型、第一 NF 的标识、终端设备的标识、第一 NF 选择的安全算法的标识, 第一 NF 的 NAS count、PDU 会话标识中的一项或多项。

例如, 终端设备保存的安全上下文包括第一 NF 的类型和/或第一 NF 的标识、第一 NF 选择的安全算法的标识, 第一 NF 的 NAS count。可选的, 该安全上下文还包括 PDU

会话标识、终端设备的标识中的一项或多项。

又例如，第一 NF 保存的安全上下文包括终端设备的标识、第一 NF 选择的安全算法的标识，第一 NF 的 NAS count。可选的，该安全上下文还包括 PDU 会话标识、第一 NF 的类型、第一 NF 的标识中的一项或多项。

- 5 可以理解的是，在终端设备从连接态转为空闲态或非激活态时，第一 NF 和终端设备均保存安全上下文，在后续终端设备重新从空闲态或非激活态转入连接态时，第一 NF 和终端设备无需再从其他网元获取安全上下文，从而减少信令交互。

- 此外，终端设备从连接态转为空闲态或非激活态时，第一 NF 可以暂停 NAS 实体，终端设备也暂停 NAS 实体。在终端设备从空闲态或非激活态转入连接态时，第一 NF 重新激活（或者说，恢复）NAS 实体，终端设备也重新激活 NAS 实体。

S802，在终端设备从连接态转入空闲态或非激活态时，第一 NF 和终端设备均不保存安全上下文。在终端设备重新从空闲态或非激活态转入连接态时，第一 NF 和终端设备分别接收来自第二 NF 的安全上下文，并分别根据接收到的安全上下文生成第一 NAS 密钥。

- 15 如前文所述，可以理解的是，第一 NF 生成的第一 NAS 密钥与终端设备生成的针对第一 NF 的第一 NAS 密钥可以是相同的，也可以是不同的。不再赘述。

其中，该第二 NF 用于保存安全上下文。例如，第二 NF 可以为 AMF，当然第二 NF 还可以为其他 NF。该安全上下文中包括终端设备的标识、第一 NF 的类型、第一 NF 的标识、第一 NF 选择的安全算法标识、第一 NF 的 NAS 计数值、PDU 会话标识中的一项或多项。

- 20 例如，该安全上下文中包括终端设备的标识、第一 NF 的类型和/或第一 NF 的标识、第一 NF 选择的安全算法标识、第一 NF 的 NAS 计数值。可选地，该安全上下文还包括 PDU 会话标识。

- 也就是说，作为一种实现方式，在终端设备从连接态转入空闲态或非激活态时，第二 NF 可以代替第一 NF 和终端设备保存安全上下文，从而节省第一 NF 和终端设备的存储空间。例如，第一 NF 可以将上述安全上下文发送给第二 NF，和/或，终端设备可以将上述安全上下文发送给第二 NF。

- 此外，在上述 S802 中，终端设备和第一 NF 未保存安全上下文，终端设备从连接态转为空闲态或非激活态时，第一 NF 可以删除 NAS 实体，终端设备也删除 NAS 实体。在终端设备从空闲态或非激活态转入连接态时，第一 NF 重新新建 NAS 实体，终端设备也重新新建 NAS 实体。

可选地，作为一种情况，如果终端设备或者第一 NF 发起该终端设备的去注册流程，则终端设备和第一 NF 可以均删除相应的 NAS 实体。

- S803，在终端设备从连接态转入空闲态或非激活态时，第一 NF 和终端设备均不保存第一 NF 的 NAS count。在终端设备从空闲态或非激活态转入连接态时，第一 NF 和终端设备分别生成第一 NAS 密钥，并且第一 NF 对应的 NAScount 从锚点功能（例如，AMF）的 NAScount 开始计数。

如前文所述，可以理解的是，第一 NF 生成的第一 NAS 密钥与终端设备生成的针对第一 NF 的第一 NAS 密钥可以是相同的，也可以是不同的。不再赘述。

可以理解的是，在 S803 中，第一 NF 不为锚点功能，或者说第一 NF 为非锚点功能。

在 S803 中, 第一 NF 和终端设备虽然未保存第一 NF 的 NAS count, 但是可以保存安全上下文中的其他信息, 例如, 可以保存第一 NF 的类型、第一 NF 的标识、第一 NF 选择的安全算法的标识、PDU 会话标识、终端设备的标识中的一项或多项。

也就是说, 在该 S803 中, 在终端设备从连接态转入空闲态或非激活态时, 终端设备和第一 NF 不保存第一 NF 的 NAS count, 在终端设备从空闲态或非激活态转入连接态时, 第一 NF 和终端设备分别从锚点功能获取锚点功能的 NAS count, 由于 AMF 的 NAS count 有随机性, 从而可以提升后续生成第一 NAS 密钥的安全等级。

S804, 在终端设备从连接态转入空闲态或非激活态时, 第一 NF 和终端设备均不保存第一 NF 的 NAS count。在终端设备从空闲态或非激活态转入连接态时, 第一 NF 和终端设备分别生成第一 NAS 密钥, 第一 NF 对应的 NAS count 从 0 开始计数。

如前文所述, 可以理解的是, 第一 NF 生成的第一 NAS 密钥与终端设备生成的针对第一 NF 的第一 NAS 密钥可以是相同的, 也可以是不同的。不再赘述。

可以理解的是, 与 S803 类似, 在 S804 中, 第一 NF 和终端设备虽然未保存第一 NF 的 NAS count, 但是可以保存安全上下文中的其他信息, 例如, 可以保存第一 NF 的类型、第一 NF 的标识、第一 NF 选择的安全算法的标识、PDU 会话标识、终端设备的标识中的一项或多项。

也就是说, 在该 S804 中, 在终端设备从连接态转入空闲态或非激活态时, 终端设备和第一 NF 不保存第一 NF 的 NAS count, 也不维护锚点功能(例如, AMF)的 NAS count, 从而简化终端设备和第一 NF 的 NAS 安全机制。

由上文可知, 在未来的通信系统, 与无线接入网设备直连的多个 NF 中的每个 NF 都有相对应的 NAS 密钥, 在一些情况中, 终端设备和 NF 的 NAS 密钥需要同步更新(rekeying)。因此, 可选地, 本申请还提出了 NAS 安全机制中的 NAS 密钥更新机制。下面分两种情况, 对 NAS 密钥更新机制进行说明。

情况 1:

在生成 NAS 密钥时, 以 K_{SEAF} 为根密钥。与无线接入网设备直连的多个 NF 中的第一 NF 的 NAS 密钥更新时, 该第一 NF 可以对终端设备进行独立的 NAS 密钥更新流程。图 9 示出了本申请提出的方法 900, 可以理解的是, 作为一种实现方式, 方法 900 可以在方法 400 的基础上执行。该方法 900 包括如下步骤。

S901, 在预设条件满足的情况下, 第一 NF 更新第一 NAS 密钥。

例如, 该预设条件可以为第一 NF 对应的 NAS count 的值达到了最大值。

S902, 第一 NF 发送消息#K (即, 第三消息)。相应地, 终端设备接收来自第一 NF 的消息#K。

该消息#K 用于指示终端设备更新第一 NAS 密钥。示例性地, 该消息#K 可以为 NAS 消息。

可选地, 作为一种方式, 第一 NF 可以向无线接入网设备发送 NAS 消息, 该 NAS 消息中包括指示终端设备更新第一 NAS 密钥的信息, 无线接入网设备再向终端设备发送该 NAS 消息。即, 该 NAS 消息在无线接入网设备处是透传的。

S903, 终端设备根据消息#K, 更新针对第一 NF 生成的第一 NAS 密钥。

例如, 第一 NF 为 SMF, 终端设备可以根据消息#K 更新 K_{SMF} , $K_{NASsmf-enc}$ 以及 $K_{NASsmf-int}$ 。

当然，该第一 NF 还可以为 PCF、LMF、AMF 等。

可以理解的是，上述 S901 至 S903 是由第一 NF 触发的 NAS 密钥同步更新，作为另一种方式，可以由终端设备触发 NAS 密钥同步更新。例如，在预设条件满足的情况下，终端设备可以更新第一 NAS 密钥，并且终端设备可以向第一 NF 发送指示信息，指示第一 NF 更新 NAS 密钥，第一 NF 可以根据终端设备的指示信息更新 NAS 密钥。

例如，终端设备可以直接向第一 NF 发送指示信息。

或者，终端设备可以向锚点功能（例如，AMF）发送指示信息，进一步地，锚点功能可以指示第一 NF 更新 NAS 密钥。此时，第一 NF 不为锚点功能，或者说，第一 NF 为非锚点功能。

可以理解的是，在 NAS count 值达到最大值的情况下，第一 NF 和终端设备同步更新 NAS 密钥，可以避免第三方的攻击重放，从而提高安全性。

可选的，如果第一 NF 不为锚点功能，或者说，第一 NF 为非锚点功能，该方法 900 还包括 S904 至 S907。

S904，锚点功能向第一 NF 和终端设备发送消息#L。相应地，第一 NF 和终端设备接收消息#L。

该消息#L 用于指示在第一 NAS 密钥更新期间，第一 NF 与终端设备之间暂停 NAS 消息传输。

可以理解的是，本申请对 S904 和 S901 的执行顺序不作限定，作为一种情况，S904 还可以在 S901 之前执行。

S905，第一 NF 和终端设备根据消息#L，在第一 NAS 密钥更新期间，暂停 NAS 消息传输。

可以理解的是，在 NAS 密钥更新期间，可能出现旧 NAS 密钥失效，但是 NAS 新密钥还未成功启用的情况，因此，在 NAS 密钥更新期间，第一 NF 和终端设备可以暂停 NAS 消息传输，降低 NAS 消息解析出错的概率。

S906，锚点功能向第一 NF 和终端设备发送消息#M。相应地，第一 NF 和终端设备接收消息#M。

该消息#M 用于指示第一 NF 与终端设备之间恢复 NAS 消息传输。

作为一种实现方式，在锚点功能发送消息#L 之后，锚点功能可以开启定时器，例如，该定时器的预设时长大于或等于进行 NAS 密钥更新所需的时长，在定时器超时之后，锚点功能发送该消息#M。

作为另一种实现方式，第一 NF 在成功更新第一 NAS 密钥之后，可以通知锚点功能该第一 NF 成功更新第一 NAS 密钥。类似地，终端设备在成功更新第一 NAS 密钥之后，可以通知锚点功能该终端设备成功更新第一 NAS 密钥。在此基础上，锚点功能可以发送消息#M。

S907，第一 NF 和终端设备根据消息#M，重新开启 NAS 消息传输。

与 S904 至 S907 类似，可选地，如果第一 NF 为锚点功能，则第一 NF 可以向终端设备发送消息#L，指示终端设备在第一 NAS 密钥更新期间，暂停与第一 NF 之间的 NAS 消息传输。第一 NF 也可以在第一 NAS 密钥更新期间，暂停与终端设备之间的 NAS 消息传输。后续，第一 NF 可以向终端设备发送消息#M，指示终端设备恢复与第一 NF 之间的

NAS 消息传输。相应地，第一 NF 也可以恢复与终端设备之间的 NAS 消息传输。

情况 2:

生成 NAS 密钥时，以 K_{AMF} 为根密钥。如果 K_{AMF} 更新，则与无线接入网设备直连的多个 NF 中的每个 NF 的 NAS 密钥均需要更新。相应地，终端设备也需要更新该多个 NF 中每个 NF 对应的 NAS 密钥。图 10 示出了本申请提出的方法 1000，可以理解的是，作为一种实现方式，方法 1000 可以在方法 400 的基础上执行。该方法 1000 包括如下步骤。

S1001，在预设条件满足的情况下，与无线接入网设备直连的多个 NF 中的每个 NF 更新 NAS 密钥。

示例性地，与无线接入网设备直连的多个 NF 中的某一 NF（例如，第一 NF）的 NAS count 达到了最大值。如果第一 NF 不为锚点功能，该第一 NF 可以向锚点功能发送 NAS 密钥更新请求消息，进一步地，锚点功能可以向该多个 NF 中的除第一 NF 和锚点功能之外的其他 NF 均发送 NAS 密钥更新请求消息，从而与无线接入网设备直连的多个 NF 中的每个 NF 均更新 NAS 密钥；如果第一 NF 为锚点功能，第一 NF 可以向该多个 NF 中的除第一 NF 之外的其他 NF 均发送 NAS 密钥更新请求消息，从而与无线接入网设备直连的多个 NF 中的每个 NF 均更新 NAS 密钥。

S1002，与无线接入网设备直连的多个 NF 向锚点功能发送 NAS 密钥更新成功的指示信息。相应地，锚点功能接收来自多个 NF 的 NAS 密钥更新成功的指示信息。

可以理解的是，该 S1002 为可选的步骤。作为另一种方式，锚点功能可以默认与无线接入网设备直连的多个 NF 均成功更新相对应的 NAS 密钥。

S1003，锚点功能确定与无线接入网设备直连的多个 NF 中的每个 NF 均成功更新 NAS 密钥。

例如，与无线接入网设备直连的多个 NF 包括 AMF、SMF、PCF、LMF，锚点功能为 AMF。AMF 可以确定 AMF、SMF、PCF 和 LMF 均成功更新对应的 NAS 密钥。

S1004，锚点功能向终端设备发送消息#N（即，第四消息）。相应地，终端设备接收来自锚点功能的消息#N。

该消息#N 用于指示终端设备更新与无线接入网设备直连的多个 NF 中每个 NF 所对应的 NAS 密钥。示例性地，该消息#N 可以为 NAS 消息。

可选地，作为一种方式，锚点功能可以向无线接入网设备发送 NAS 消息，该 NAS 消息中包括指示终端设备更新多个 NF 中每个 NF 所对应的 NAS 密钥的信息，无线接入网设备再向终端设备发送该 NAS 消息。即，该 NAS 消息在无线接入网设备处是透传的。

S1005，终端设备根据消息#N，更新与无线接入网设备直连的多个 NF 中每个 NF 所对应的 NAS 密钥。

例如，与无线接入网设备直连的多个 NF 包括 AMF、SMF、PCF、LMF，终端设备可以根据该消息#N，更新 AMF 对应的 NAS 密钥、SMF 对应的 NAS 密钥、PCF 对应的 NAS 密钥以及 LMF 对应的 NAS 密钥。

可以理解的是，上述 S1001 至 S1005 是由网络侧发起的 NAS 密钥统一更新，作为另一种情况，还可以由终端设备发起 NAS 密钥统一更新。例如，与无线接入网设备直连的多个 NF 中的某一 NF 的 NAS count 达到了最大值，则终端设备更新该多个 NF 中每个 NF 对应的 NAS 密钥，进一步地，终端设备向该多个 NF 发送指示信息，使得该多个 NF 中的

每个 NF 更新对应的 NAS 密钥。例如，终端设备可以直接向该多个 NF 发送指示消息。或者，终端设备可以向锚点功能发送指示消息，进一步地，锚点功能可以指示该多个 NF 中除锚点功能之外的其他 CN NF 更新 NAS 密钥。

- 5 可以理解的是，在 NAS count 值达到最大值的情况下，与无线接入网设备直连的多个 NF 和终端设备同步更新 NAS 密钥，可以避免第三方的攻击重放，从而提高安全性。

可选地，该方法 1000 还包括 S1006 至 S1009。

S1006，锚点功能向与无线接入网设备直连的多个 NF 和终端设备发送消息#P。相应地，第一 NF 和终端设备接收消息#P。

该消息#P 用于指示在 NAS 密钥更新期间，暂停 NAS 消息传输。

- 10 S1007，与无线接入网设备直连的多个 NF 和终端设备根据消息#P，在 NAS 密钥更新期间，暂停 NAS 消息传输。

可以理解的是，在 NAS 密钥更新期间，可能出现旧 NAS 密钥失效，但是新 NAS 密钥还未成功启用的情况，因此，在 NAS 密钥更新期间，与无线接入网设备直连的多个 NF 和终端设备可以暂停 NAS 消息传输，降低 NAS 消息解析出错的概率。

- 15 S1008，锚点功能向与无线接入网设备直连的多个 NF 和终端设备发送消息#Q。相应地，第一 NF 和终端设备接收消息#Q。

该消息#Q 用于指示恢复 NAS 消息传输。

关于该消息#Q 的触发机制，可以参考 S906。

- 20 S1009，与无线接入网设备直连的多个 NF 和终端设备根据消息#Q，重新开启 NAS 消息传输。

可选的，在一些情况下，为终端设备提供服务的 NF 会发生改变，即，从源 NF 变为目标 NF。因此，本申请还提出了终端设备发生切换（handover）时的 NAS 安全机制。图 11 示出了本申请提出的方法 1100，可以理解的是，作为一种实现方式，方法 1100 可以在方法 400 的基础上执行。该方法 1100 包括如下步骤。

- 25 S1101，第一 NF 发送终端设备的安全上下文。相应地，第一目标 NF 接收终端设备的安全上下文。

该安全上下文包括第一 NF 维护的 NAS count。可选的，该安全上下文还包括 PDU 会话标识，终端设备安全能力信息中的一项或多项。

下面介绍第一目标 NF 接收该安全上下文的方式。

- 30 方式 1:

第一 NF 向锚点功能发送该安全上下文。进一步地，锚点功能向第一目标 NF 发送该安全上下文。

可以理解的是，在该方式 1 中，第一 NF 不为锚点功能，或者说，第一 NF 为非锚点功能。

- 35 例如，第一 NF 为源 SMF，锚点功能为 AMF，第一目标 NF 为目标 SMF，源 SMF 可以通过 AMF 向目标 SMF 发送安全上下文。

又例如，第一 NF 为源 PCF，锚点功能为 AMF，第一目标 NF 为目标 PCF，源 PCF 可以通过 AMF 向目标 PCF 发送安全上下文。

又例如，第一 NF 为源 LMF，锚点功能为 AMF，第一目标 NF 为目标 LMF，源 LMF

可以通过 AMF 向目标 LMF 发送安全上下文。

可以理解的是，如果锚点功能也发生了切换，即，从源锚点功能切换到了目标锚点功能，则第一 NF 可以通过源锚点功能（例如，源 AMF）以及目标锚点功能（例如，目标 AMF）向第一目标 NF 发送安全上下文。

5 方式 2:

第一 NF 直接向第一目标 NF 发送安全上下文。

例如，第一 NF 为源 SMF，第一目标 NF 为目标 SMF，源 SMF 可以直接向目标 SMF 发送安全上下文。

10 又例如，第一 NF 为源 PCF，第一目标 NF 为目标 PCF，源 PCF 可以直接向目标 PCF 发送安全上下文。

又例如，第一 NF 为源 LMF，第一目标 NF 为目标 LMF，源 LMF 可以直接向目标 LMF 发送安全上下文。

又例如，第一 NF 为源 AMF，第一目标 NF 为目标 AMF，源 AMF 可以直接向目标 AMF 发送安全上下文。

15 方式 3:

以锚点功能为 AMF 为例，AMF 也可以将 AMF 维护的终端设备安全能力信息发送给第一目标 NF。

20 例如，第一目标 NF 为目标 SMF，则 AMF 可以向目标 SMF 发送终端设备安全能力信息。又例如，第一目标 NF 为目标 PCF，则 AMF 可以向目标 PCF 发送终端设备安全能力信息。又例如，第一目标 NF 为目标 LMF，则 AMF 可以向目标 LMF 发送终端设备安全能力信息。

可以理解的是，如果锚点功能也发生了切换，即，从源锚点功能切换到了目标锚点功能，则源锚点功能（例如，源 AMF）可以通过目标锚点功能（例如，目标 AMF）向第一目标 NF 发送终端设备安全能力信息。

25 S1102，第一目标 NF 根据终端设备的安全上下文，生成 NAS 密钥。

可以理解的是，第一目标 NF 可以根据终端设备安全能力信息选择安全算法，并生成 NAS 密钥。

此外，第一目标 NF 可以将该第一目标 NF 选择的安全算法的信息发送给终端设备。示例性地，第一目标 NF 可以通过以下几种方式向终端设备发送安全算法的信息。

30 方式 1:

第一目标 NF 直接向终端设备发送安全算法的信息。

示例性地，第一目标 NF 向终端设备发送 NAS 消息，该 NAS 消息中包括安全算法的信息。

方式 2:

35 第一目标 NF 可以将安全算法的信息通过锚点功能（例如，AMF）发送给终端设备。

可以理解的是，在该方式 2 中，第一目标 NF 不为锚点功能，或者说，第一目标 NF 为非锚点功能。

例如，第一目标 NF 为目标 SMF，目标 SMF 可以通过 AMF 向终端设备发送目标 SMF 选择的安全算法的标识。

例如,第一目标 NF 为目标 LMF,目标 LMF 可以通过 AMF 向终端设备发送目标 LMF 选择的安全算法的标识。

例如,第一目标 NF 为目标 PCF,目标 PCF 可以通过 AMF 向终端设备发送目标 PCF 选择的安全算法的标识。

- 5 可以理解的是,如果锚点功能也发生了切换,即,从源锚点功能切换到了目标锚点功能,则第一目标 NF 可以通过目标锚点功能(例如,目标 AMF)、源锚点功能(例如,源 AMF)向终端设备发送安全算法的信息。

方式 3:

第一目标 NF 可以通过第一 NF 向终端设备发送安全算法的信息。

- 10 例如,第一目标 SMF 可以通过第一 SMF 向终端设备发送安全算法的信息。

方式 4:

第一目标 NF 可以通过锚点功能以及第一 NF,向终端设备发送安全算法的信息。

可以理解的是,在该方式 4 中,第一目标 NF 和第一 NF 不为锚点功能,或者说,第一目标 NF 和第一 NF 为非锚点功能。

- 15 例如,第一目标 SMF 可以通过 AMF、第一 SMF,向终端设备发送安全算法的信息。

根据本申请实施例,终端设备可以从源 SMF 切换到目标 SMF、从源 LMF 切换到目标 LMF、从源 AMF 切换到目标 AMF、从源 PCF 切换到目标 PCF。源 NF 可以将终端设备的安全上下文发送给目标 NF,从而节省信令开销(例如,终端设备无需再向目标 NF 发送终端设备自身的安全能力信息),使得目标 NF 可以根据终端设备的安全上下文生成 NAS 密钥,处理与终端设备之间的 NAS 消息。

以上介绍了本申请提出的方法。图 12 为本申请实施例提供的一种通信装置,该通信装置包括收发单元和处理单元。

其中,收发单元可以用于实现相应的信息收发功能。收发单元还可以称为通信接口或通信单元。处理单元可以用于进行处理操作。

- 25 示例性地,该装置还包括存储单元,该存储单元可以用于存储指令和/或数据,处理单元可以读取存储单元中的指令和/或数据,以使得装置实现前述各个方法实施例中的装置的动作。

作为一种实现方式,该装置可以是前述实施例中的终端设备,也可以是终端设备的组成部件(如芯片)。其中,收发单元和处理单元,可以用于实现终端设备的相关操作。

- 30 例如,收发单元可用于执行 S401。处理单元可用于执行 S407、S408、S409、S410。

又例如,处理单元可用于执行 S502。

又例如,处理单元可用于执行 S602。

又例如,处理单元可用于执行 S702。

又例如,处理单元可用于执行 S801 至 S804 中的任一项。

- 35 又例如,处理单元可用于执行 S903、S905、S907。

又例如,处理单元可用于执行 S1005、S1007、S1009。

作为另一种实现方式,该装置可以是前述实施例中的第一 NF,也可以是第一 NF 的组成部件(如芯片)。其中,收发单元和处理单元,可以用于实现第一 NF 的相关操作。

例如,收发单元可用于执行 S403。处理单元可用于执行 S402、S404、S405、S406。

又例如，处理单元可用于执行 S501。

又例如，处理单元可用于执行 S601。

又例如，处理单元可用于执行 S701。

又例如，处理单元可用于执行 S801 至 S804 中的任一项。

5 又例如，处理单元可用于执行 S901、S905、S907。

又例如，处理单元可用于执行 S1001、S1007、S1009。

可以理解的是，各单元执行上述相应步骤的具体过程在上述各方法实施例中已经详细说明，为了简洁，在此不再赘述。

收发单元可以由收发机替代（例如，收发单元中的发送单元可以由发送机替代，收发
10 单元中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

此外，上述收发单元还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。

图 13 为本申请实施例提供的另一种通信装置，该通信装置包括：处理器和通信接口。
15 处理器用于执行存储器中存储的程序或指令，或读取存储器中存储的数据，以执行上文各方法实施例中的相关动作。示例性地，处理器可以为一个或多个。通信接口用于信号的接收和/或发送。

示例性地，该通信装置还可以包括存储器，存储器用于存储计算机程序或指令和/或数据。该存储器可以与处理器集成在一起，或者也可以分离设置。当然，该通信装置中还可以不包括存储器，存储器可以设置在该通信装置之外。示例性地，存储器可以为一个或多个。
20

示例性地，处理器、通信接口以及存储器通过总线相互连接；总线可以是外设部件互连标准(peripheral component interconnect, PCI)总线或扩展工业标准结构(extended industry standard architecture, EISA)总线等。上述总线可以分为地址总线、数据总线和控制总线等。为便于表示，图 13 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。
25

可以理解的是，本申请实施例中提及的处理器可以是中央处理单元(central processing unit, CPU)，网络处理器(network processor, NP)，或者 CPU 和 NP 的组合。处理器还可以进一步包括硬件芯片。上述硬件芯片可以是应用特有集成电路(application specific integrated circuit, ASIC)，可编程逻辑器件(programmable logic device, PLD)。上述 PLD 可以是复杂可编程逻辑器件(complex programmable logic device, CPLD)，现场可编程逻辑门阵列(field-programmable gate array, FPGA)，通用阵列逻辑(generic array logic, GAL)或其任意组合。
30

还可以理解的是，本申请实施例中提及的存储器可以是易失性存储器或非易失性存储器，
35 或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(read-only memory, ROM)、可编程只读存储器(programmable ROM, PROM)、可擦除可编程只读存储器(erasable PROM, EPROM)、电可擦除可编程只读存储器(electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory, RAM)，其用作外部高速缓存。

可以理解的是，如果以软件的形式实现本申请的实施例，并作为独立的产品销售或使用时，可以将相应的程序（也可以称为代码，或指令）存储在可读取存储介质中。因此，本申请还提供一种可读存储介质，包括程序，当程序在设备或计算机上运行时，使得设备或计算机执行上述方案中任一种可能的实现。

5 可读取存储介质包括：U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

本申请的技术方案可以以软件产品的形式体现出来。因此，本申请还提供了一种程序产品，该程序产品包括：程序，当该程序被运行时，使得设备或计算机执行上述方案中任一种可能的实现。

10 此外，本申请实施例还提供一种芯片系统（或者说芯片）。该芯片系统包括处理器以及接口电路，接口电路用于为所述处理器提供数据、指令或者信息的发送和/或接收，处理器用于执行上述方案中任一种可能的实现。

15 以上，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权利要求的保护范围为准。

权利要求书

1. 一种非接入层 NAS 消息处理方法，其特征在于，包括：

5 终端设备生成多个 NAS 密钥，多个 NAS 密钥中的至少两个 NAS 密钥分别与多个网络功能 NF 中的不同的 NF 关联；

所述终端设备基于所述多个 NAS 密钥，处理与所述多个 NF 通信的 NAS 消息。

2. 根据权利要求 1 所述的方法，其特征在于，所述终端设备生成多个 NAS 密钥，包括：

10 所述终端设备根据第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值，生成第一 NAS 密钥，其中所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

3. 根据权利要求 1 所述的方法，其特征在于，所述终端设备生成多个 NAS 密钥，包括：

15 所述终端设备根据第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值、PDU 会话标识，生成第一 NAS 密钥，其中所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

4. 根据权利要求 1 所述的方法，其特征在于，所述终端设备生成多个 NAS 密钥，包括：

20 所述终端设备根据第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值、PDU 会话标识，生成第一 NAS 密钥，其中所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

5. 根据权利要求 2-4 中任一项所述的方法，其特征在于，

所述第一 NF 的 NAS 计数值从 0 开始计数；或者，

25 所述第一 NF 的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

6. 根据权利要求 1-5 中任一项所述的方法，其特征在于，所述终端设备生成多个 NAS 密钥，包括：

所述终端设备基于 NAS 根密钥，生成所述多个 NAS 密钥。

7. 根据权利要求 1-6 中任一项所述的方法，其特征在于，所述方法还包括：

30 在创建与第一 NF 对应的 NAS 实体时，所述终端设备激活第一 NAS 密钥；

或者，所述终端设备接收第一消息，并根据所述第一消息激活第一 NAS 密钥；

其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

8. 根据权利要求 1-7 中任一项所述的方法，其特征在于，所述方法还包括：

35 在暂停或者删除与第一 NF 对应的 NAS 实体时，所述终端设备去激活第一 NAS 密钥；

或者，所述终端设备接收第二消息，并根据所述第二消息去激活第一 NAS 密钥；

其中，所述第一 NF 为所述多个 NF 中的一个，所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

9. 根据权利要求 1-8 中任一项所述的方法, 其特征在于, 所述方法还包括:

在从连接态转入空闲态或非激活态时, 所述终端设备保存第一 NF 的安全上下文, 所述第一 NF 的安全上下文包括所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值;

5 在从所述空闲态或所述非激活态转入所述连接态时, 所述终端设备根据所述第一 NF 的安全上下文生成第一 NAS 密钥;

其中, 所述第一 NF 为所述多个 NF 中的一个, 所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

10. 根据权利要求 1-8 中任一项所述的方法, 其特征在于, 所述方法还包括:

10 在从连接态转入空闲态或非激活态时, 所述终端设备不保存第一 NF 的安全上下文;

在从所述空闲态或所述非激活态转入所述连接态时, 所述终端设备从第二 NF 获取所述第一 NF 的安全上下文, 并根据所述第一 NF 的安全上下文生成第一 NAS 密钥;

其中, 所述第一 NF 为所述多个 NF 中的一个, 所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

15 11. 根据权利要求 1-8 中任一项所述的方法, 其特征在于, 所述方法还包括:

在从连接态转入空闲态或非激活态时, 所述终端设备不保存第一 NF 的 NAS 计数值;

在从所述空闲态或所述非激活态转入所述连接态时, 所述终端设备生成第一 NAS 密钥;

20 其中, 所述第一 NF 对应的 NAS 计数值从 0 开始计数; 或者, 所述第一 NF 对应的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数;

所述第一 NF 为所述多个 NF 中的一个, 所述第一 NAS 密钥为所述多个 NAS 密钥中的一个。

12. 根据权利要求 1-11 中任一项所述的方法, 其特征在于, 所述方法还包括:

25 所述终端设备接收来自第一 NF 的第三消息, 并根据所述第三消息更新第一 NAS 密钥, 所述第一 NF 为所述多个 NF 中的一个, 所述第一 NAS 密钥为所述多个 NAS 密钥中的一个; 或者,

所述终端设备接收来自锚点功能的第四消息, 并根据所述第四消息更新所述多个 NAS 密钥。

13. 一种非接入层 NAS 消息处理方法, 其特征在于, 包括:

30 第一网络功能 NF 生成第一 NAS 密钥;

所述第一 NF 基于所述第一 NAS 密钥, 处理与终端设备之间的 NAS 消息, 第一 NF 为非锚点功能。

14. 根据权利要求 13 所述的方法, 其特征在于, 所述第一 NF 生成第一 NAS 密钥, 包括:

35 所述第一 NF 根据所述第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值, 生成所述第一 NAS 密钥。

15. 根据权利要求 13 所述的方法, 其特征在于, 所述第一 NF 生成第一 NAS 密钥, 包括:

所述第一 NF 根据所述第一 NF 的类型参数和/或所述第一 NF 的标识、所述第一 NF

选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值、PDU 会话标识，生成所述第一 NAS 密钥。

16. 根据权利要求 13 所述的方法，其特征在于，所述第一 NF 生成第一 NAS 密钥，包括：

5 所述第一 NF 根据所述第一 NF 选择的安全算法的标识、所述第一 NF 维护的 NAS 计数值、PDU 会话标识，生成所述第一 NAS 密钥。

17. 根据权利要求 14-16 中任一项所述的方法，其特征在于，
所述第一 NF 维护的 NAS 计数值从 0 开始计数；或者，
所述第一 NF 维护的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

10 18. 根据权利要求 13-17 中任一项所述的方法，其特征在于，所述第一 NF 生成第一 NAS 密钥，包括：

所述第一 NF 从锚点功能获取 NAS 根密钥；
所述第一 NF 基于所述 NAS 根密钥，生成所述第一 NAS 密钥。

15 19. 根据权利要求 13-18 中任一项所述的方法，其特征在于，所述方法还包括：
在创建与所述第一 NF 对应的 NAS 实体时，所述第一 NF 激活所述第一 NAS 密钥；
或者，所述第一 NF 接收第五消息，并根据所述第五消息激活所述第一 NAS 密钥。

20. 根据权利要求 13-19 中任一项所述的方法，其特征在于，所述方法还包括：
在暂停或者删除与所述第一 NF 对应的 NAS 实体时，所述第一 NF 去激活所述第一 NAS 密钥；

20 或者，所述第一 NF 接收第六消息，并根据所述第六消息去激活所述第一 NAS 密钥。

21. 根据权利要求 13-20 中任一项所述的方法，其特征在于，所述方法还包括：
在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 保存所述终端设备的安全上下文，所述终端设备的安全上下文包括所述第一 NF 选择的安全算法的标识、所述第一 NF 的 NAS 计数值、所述终端设备的标识；

25 在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 根据所述终端设备的安全上下文生成所述第一 NAS 密钥。

22. 根据权利要求 13-20 中任一项所述的方法，其特征在于，所述方法还包括：

在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 不保存所述终端设备的安全上下文；

30 在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 从第二 NF 获取所述终端设备的安全上下文，并根据所述终端设备的安全上下文生成所述第一 NAS 密钥。

23. 根据权利要求 13-20 中任一项所述的方法，其特征在于，所述方法还包括：

35 在所述终端设备从连接态转入空闲态或非激活态时，所述第一 NF 不保存所述第一 NF 的 NAS 计数值；

在所述终端设备从所述空闲态或所述非激活态转入所述连接态时，所述第一 NF 生成所述第一 NAS 密钥；

其中，所述第一 NF 对应的 NAS 计数值从 0 开始计数；或者，
所述第一 NF 对应的 NAS 计数值从锚点功能的初始 NAS 计数值开始计数。

24. 根据权利要求 13-23 中任一项所述的方法, 其特征在于, 所述方法还包括:
在预设条件满足的情况下, 所述第一 NF 更新所述第一 NAS 密钥;

所述第一 NF 发送第三消息, 所述第三消息用于指示所述终端设备更新所述第一 NAS 密钥。

5 25. 一种非接入层 NAS 消息处理方法, 其特征在于, 包括:

终端设备生成多个 NAS 密钥, 所述多个 NAS 密钥中的至少两个 NAS 密钥分别与多个网络功能 NF 中的不同的 NF 关联, 所述多个 NAS 密钥中包括针对第一 NF 的第一 NAS 密钥, 所述第一 NF 为所述多个 NF 中的一个;

第一 NF 生成第一 NAS 密钥, 所述第一 NF 为非锚点功能;

10 所述终端设备基于所述终端设备生成的第一 NAS 密钥, 处理与所述第一 NF 之间的 NAS 消息;

所述第一 NF 基于所述第一 NF 生成的第一 NAS 密钥, 处理与所述终端设备之间的 NAS 消息。

15 26. 一种通信装置, 其特征在于, 包括用于执行权利要求 1-12 中任一项方法的单元, 或者包括用于执行权利要求 13-24 中任一项方法的单元。

27. 一种通信装置, 其特征在于, 包括: 通信接口和处理器, 所述处理器用于执行计算机程序或指令, 使得所述通信设备执行如权利要求 1-12 中任一项所述的方法, 或者, 使得所述通信设备执行如权利要求 13-24 中任一项所述的方法。

28. 一种通信系统, 其特征在于, 所述通信系统包括终端设备和第一 NF;

20 所述终端设备用于执行如权利要求 1-12 中任一项所述的方法, 所述第一 NF 用于执行如权利要求 13-24 中任一项所述的方法。

29. 一种计算机可读存储介质, 其特征在于, 包括计算机程序或指令, 当所述计算机程序或所述指令在计算机上运行时, 使得所述计算机执行如权利要求 1-12 中任意一项所述的方法, 或者, 使得所述计算机执行如权利要求 13-24 中任意一项所述的方法。

25 30. 一种计算机程序产品, 其特征在于, 包含指令, 当所述指令在计算机上运行时, 使得所述计算机执行如权利要求 1-12 中任意一项所述的方法, 或者, 使得所述计算机执行如权利要求 13-24 中任意一项所述的方法。

30

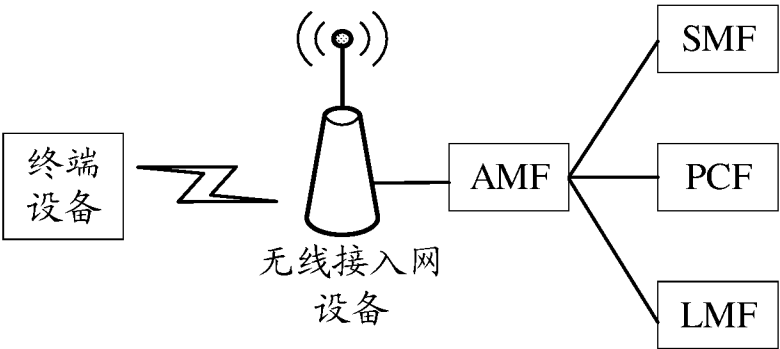


图 1

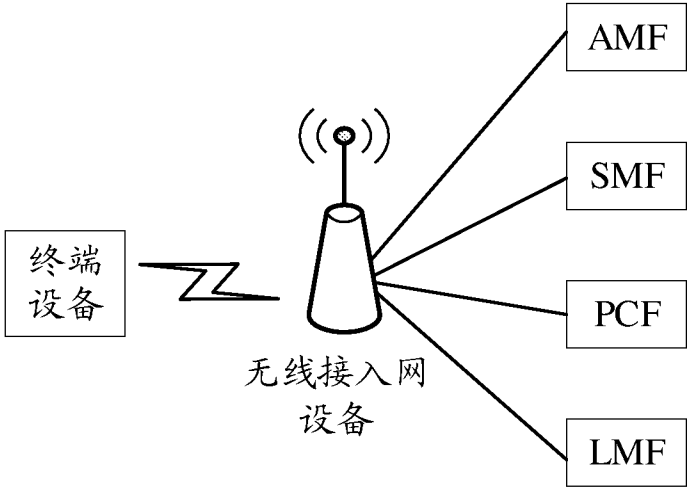


图 2

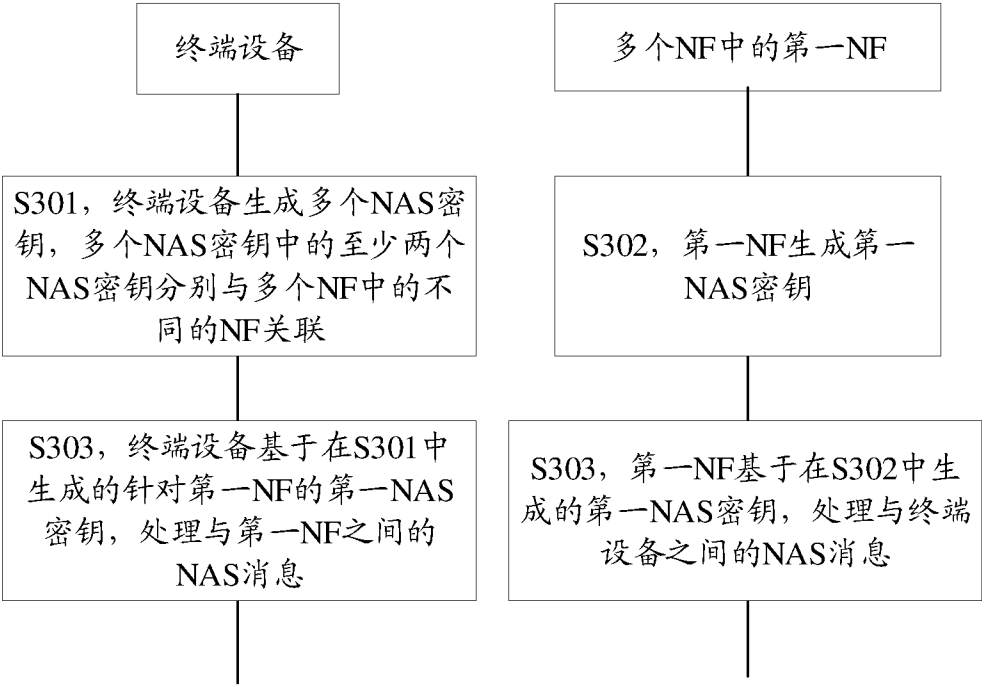


图 3

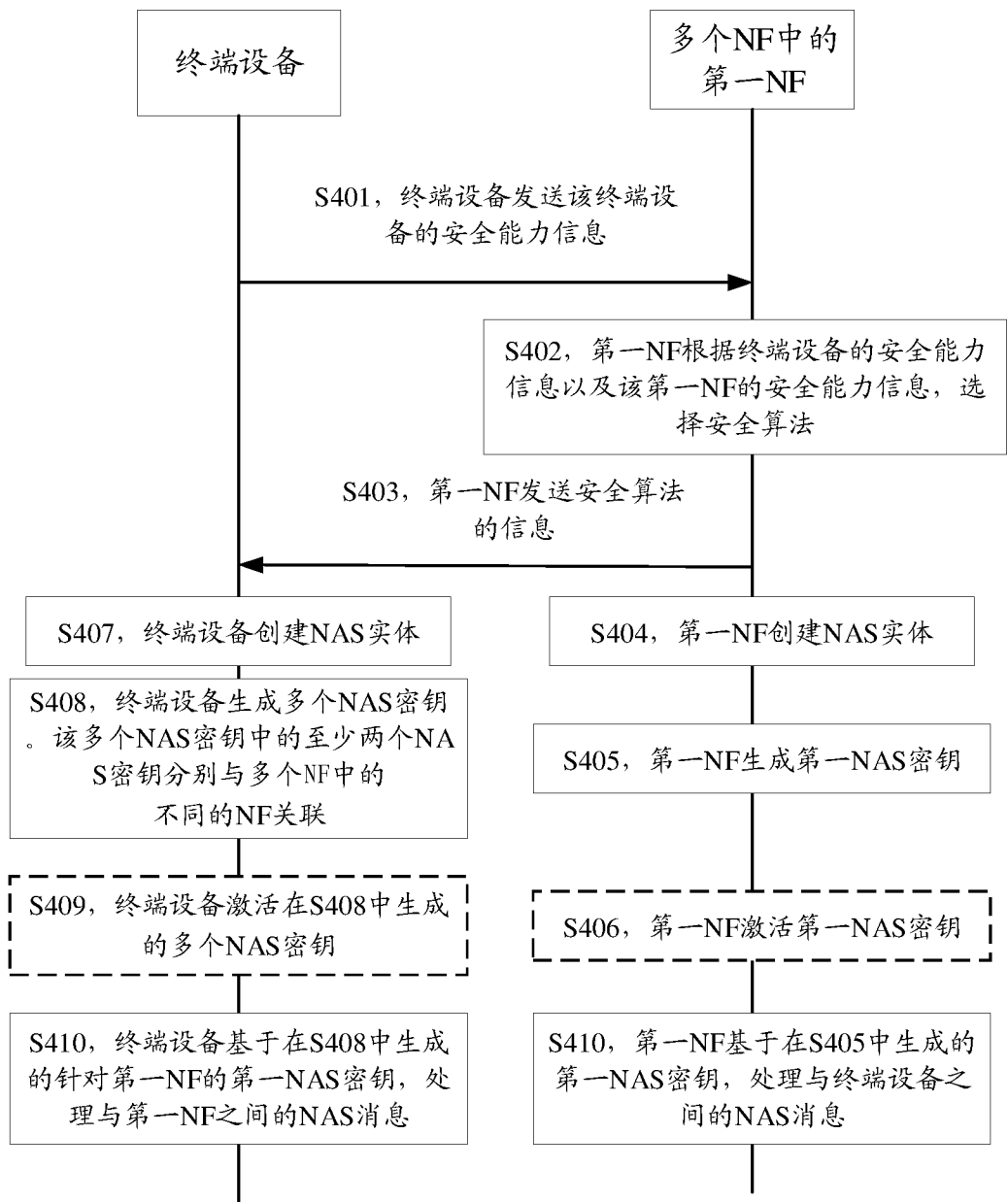


图 4

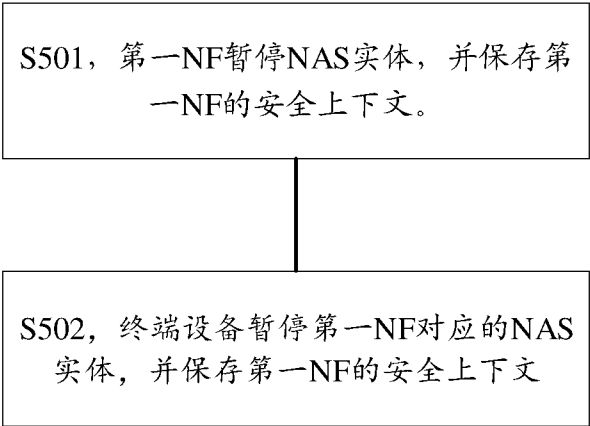


图 5

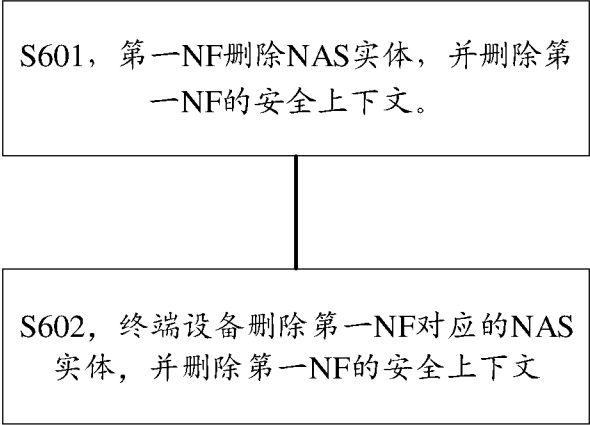


图 6

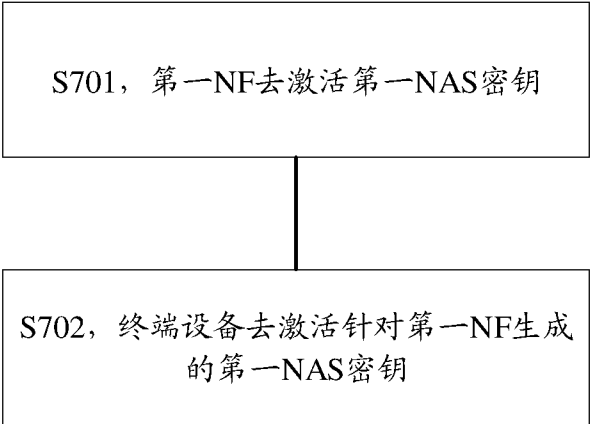


图 7

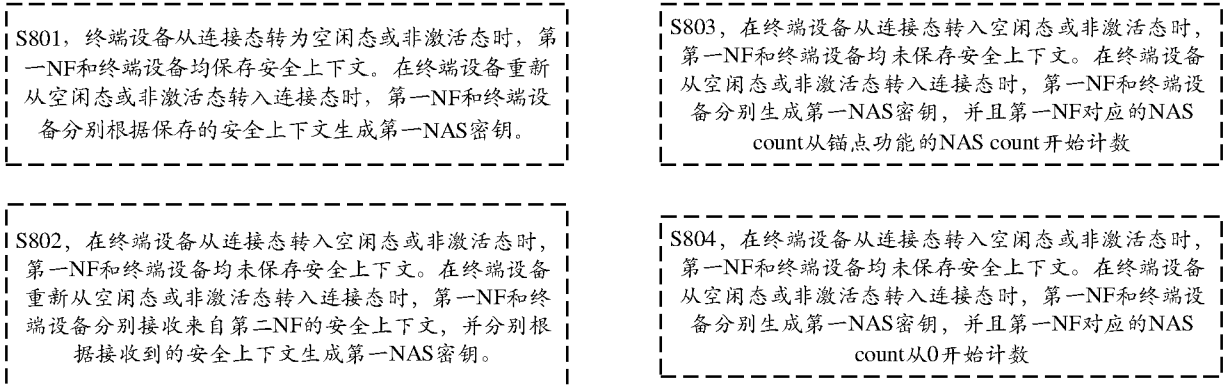


图 8

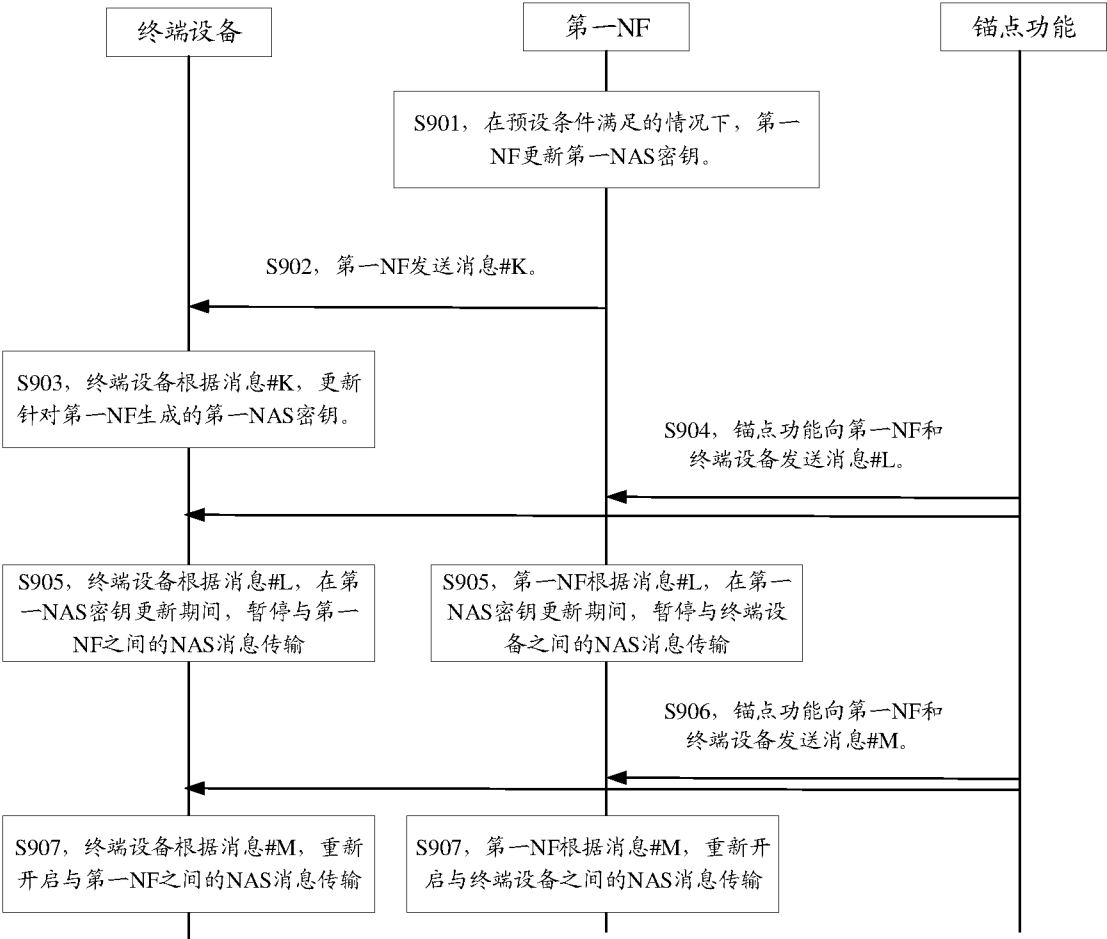


图 9

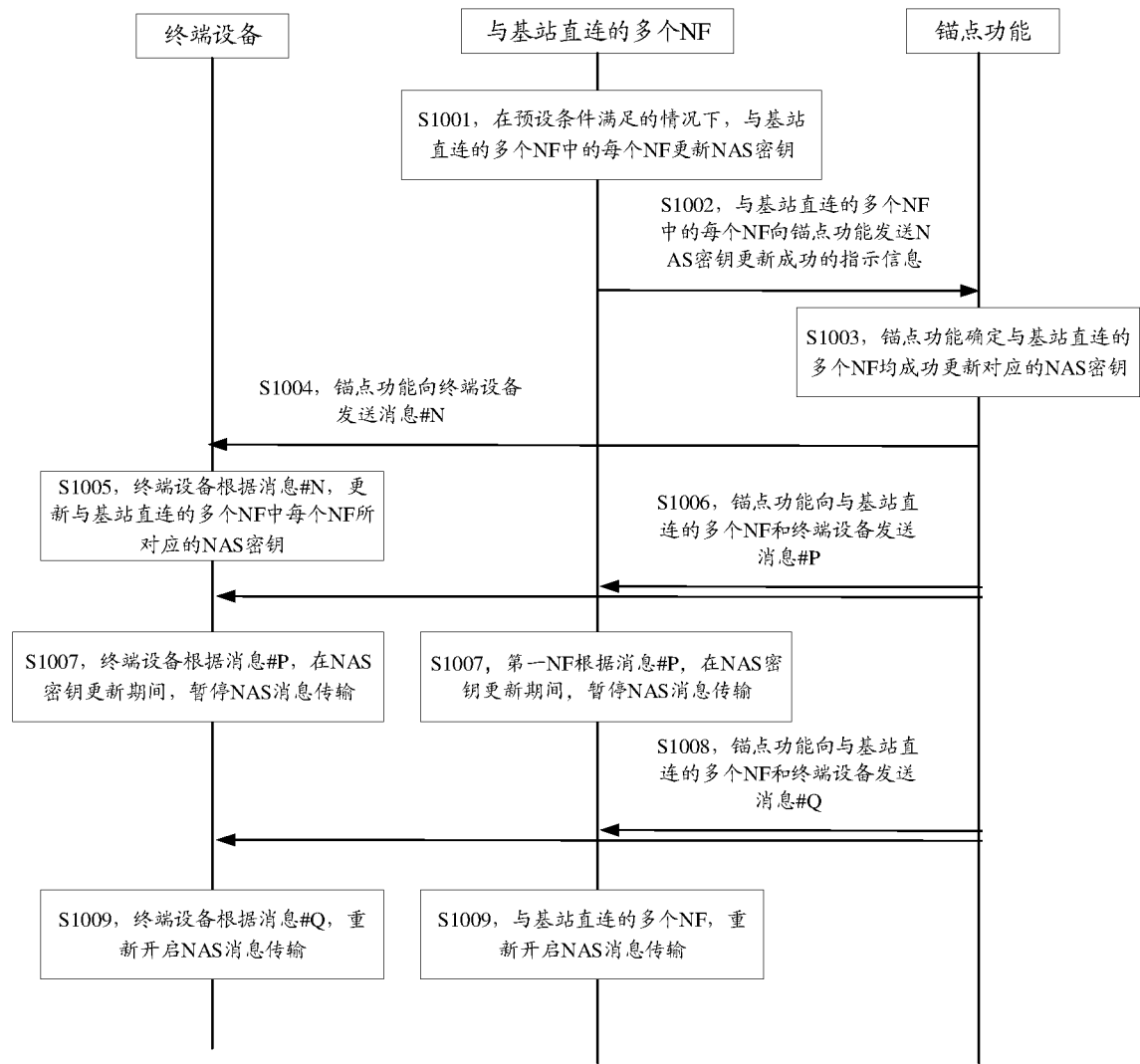


图 10

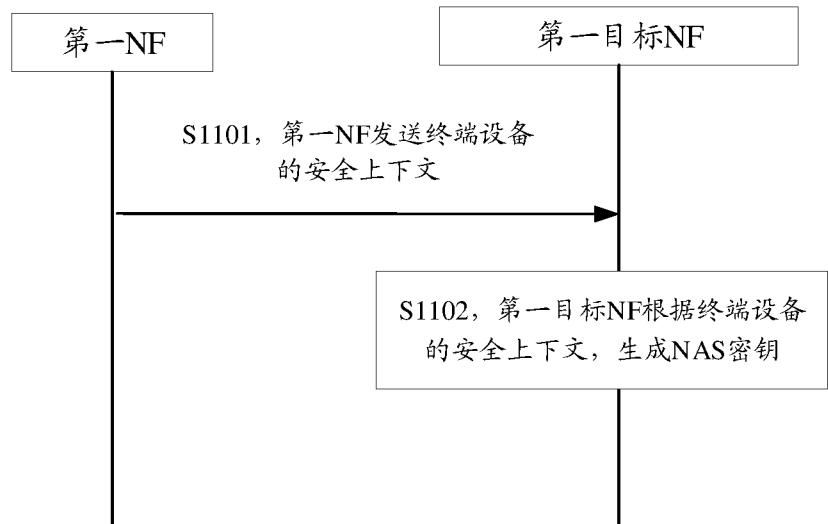


图 11

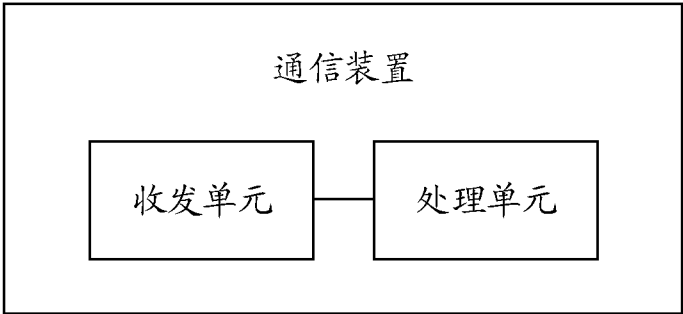


图 12

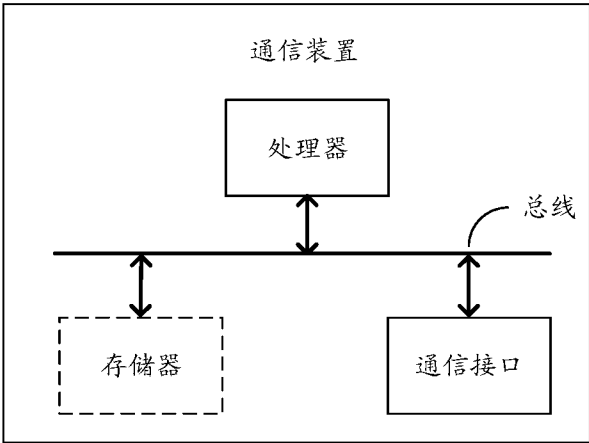


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/100304

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/04(2021.01)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)

IPC: H04W H04B H04Q

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)

CNTXT, ENTXTC, WPABS, VEN, ENTXT, CNKI, 3GPP: 非接入层, 秘钥, 密钥, 多, 两, 不同, 各, 网络功能, NAS, key, multi+, two, different, each, NF, LMF, PCF, AMF, SMF

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111386720 A (NEC CORP.) 07 July 2020 (2020-07-07) claims 1-25, and description, paragraphs [0078]-[0271]	1-30
A	WO 2023055342 A1 (NOKIA TECHNOLOGIES OY et al.) 06 April 2023 (2023-04-06) entire document	1-30
A	US 2020021993 A1 (APPLE INC.) 16 January 2020 (2020-01-16) entire document	1-30
A	NOKIA. "pCR to 33.899: Security solution for SMS over NAS" 3GPP TSG SA WG3 (Security) Meeting #88, S3-171815, 11 August 2017 (2017-08-11), entire document	1-30



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

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

11 September 2023

Date of mailing of the international search report

15 September 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/100304

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111386720	A	07 July 2020	JP	2022101688	A	06 July 2022
				US	2020280849	A1	03 September 2020
				JPWO	2019065897	A1	06 August 2020
				WO	2019065897	A1	04 April 2019
				EP	3691317	A1	05 August 2020
				JP	2021057921	A	08 April 2021
WO	2023055342	A1	06 April 2023	None			
US	2020021993	A1	16 January 2020	WO	2020010515	A1	16 January 2020
				US	2022086642	A1	17 March 2022

国际检索报告

国际申请号

PCT/CN2023/100304

A. 主题的分类

H04W12/04 (2021.01) 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)

IPC: H04W H04B H04Q

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))

CNTXT, ENTXT, WPABS, VEN, ENTXT, CNKI, 3GPP: 非接入层, 秘钥, 密钥, 多, 两, 不同, 各, 网络功能, NAS, key, multi+, two, different, each, NF, LMF, PCF, AMF, SMF

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 111386720 A (日本电气株式会社) 2020年7月7日 (2020 - 07 - 07) 权利要求1-25, 说明书第[0078]-[0271]段	1-30
A	WO 2023055342 A1 (NOKIA TECHNOLOGIES OY等) 2023年4月6日 (2023 - 04 - 06) 全文	1-30
A	US 2020021993 A1 (APPLE INC.) 2020年1月16日 (2020 - 01 - 16) 全文	1-30
A	NOKIA. "pCR to 33.899: Security solution for SMS over NAS" 3GPP TSG SA WG3 (Security) Meeting #88 S3-171815, 2017年8月11日 (2017 - 08 - 11), 全文	1-30

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2023年9月11日

国际检索报告邮寄日期

2023年9月15日

ISA/CN的名称和邮寄地址

中国国家知识产权局

中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

王怡轩

电话号码 (+86) 010-53961621

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2023/100304

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	111386720	A	2020年7月7日	JP	2022101688	A	2022年7月6日
				US	2020280849	A1	2020年9月3日
				JPWO	2019065897	A1	2020年8月6日
				WO	2019065897	A1	2019年4月4日
				EP	3691317	A1	2020年8月5日
				JP	2021057921	A	2021年4月8日
WO	2023055342	A1	2023年4月6日	无			
US	2020021993	A1	2020年1月16日	WO	2020010515	A1	2020年1月16日
				US	2022086642	A1	2022年3月17日