

配置演进分组系统非接入层安全算法的方法及相关装置

本申请要求于 2021 年 02 月 10 日提交中国国家知识产权局、申请号为
5 202110183922.0、申请名称为“配置演进分组系统非接入层安全算法的方法及相关装置”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

本申请涉及通信技术领域，尤其涉及一种配置演进分组系统(evolved packet system,
10 EPS) 非接入层(non-access stratum, NAS) 安全算法的方法及相关装置。

背景技术

目前，在第五代移动通信(5th generation, 5G)网络支持 N26 接口、用户设备(user
equipment, UE)支持 S1 模式的情况下，UE 的注册流程中包括两次安全模式命令
15 (security mode command, SMC) 流程。

在 UE 的注册流程中，会出现第一次 SMC 流程正常，第二次 SMC 异常的情况，
这会导致注册成功后的 UE 中无 EPS NAS 安全算法，因此，如何确保为 UE 成功配置
EPS NAS 安全算法成为了亟需解决的问题。

20 发明内容

本申请提供了一种配置 EPS NAS 安全算法的方法及相关装置，确保了接入和移动
管理功能实体能够为终端设备成功配置 EPS NAS 安全算法。

第一方面，本申请提供一种配置 EPS NAS 安全算法的方法，所述方法包括：接入
和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法；所述接
25 入和移动管理功能实体向所述终端设备提供所述所选的 EPS NAS 安全算法。

本方法中，接入和移动管理功能实体在未成功为终端设备提供所选的 EPS NAS 安全
算法的情况下，向终端设备重新提供所选的 EPS NAS 安全算法，可以确保接入和移
动管理功能实体能够为终端设备成功配置所选的 EPS NAS 安全算法。

在一种可能的实现方式中，所述接入和移动管理功能实体确定没有成功为终端设
30 备提供所选的 EPS NAS 安全算法之前，所述方法还包括：所述接入和移动管理功能实
体向所述终端设备发送第一消息，所述第一消息包括所述所选的 EPS NAS 安全算法的
信元。

在一种可能的实现方式中，所述接入和移动管理功能实体确定没有成功为终端设
备提供所选的 EPS NAS 安全算法包括：所述接入和移动管理功能实体确定未收到第一
35 完成消息，所述第一完成消息用于表示所述终端设备已接收到所述第一消息。

在一种可能的实现方式中，所述接入和移动管理功能实体确定未收到第一完成消
息包括：所述接入和移动管理功能实体确定在预设时间内未收到所述第一完成消息。

该实现方式中，接入和移动管理功能实体通过在预设时间内未收到第一完成消息
来确定没有成功为终端设备提供所选的 EPS NAS 安全算法，提高了接入和移动管理功

能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法的准确度。

在一种可能的实现方式中，所述第一消息为安全模式命令 SMC 消息，所述第一完成消息为 SMC 完成消息。

在一种可能的实现方式中，所述方法包括：所述接入和移动管理功能实体将所述
5 所选的 EPS NAS 安全算法标记为无效。

该实现方式中，接入和移动管理功能实体在确定没有成功为终端设备提供所选的 EPS NAS 安全算法之后，将所选的 EPS NAS 安全算法标记为无效。接入和移动管理功能实体可以根据标记的所选的 EPS NAS 安全算法为无效的信息为终端设备重新提供所选的 EPS NAS 安全算法，确保了接入和移动管理功能实体能够成功为终端设备提供
10 所选的 EPS NAS 安全算法。

在一种可能的实现方式中，所述接入和移动管理功能实体向所述终端设备提供所述所选的 EPS NAS 安全算法之前，所述方法还包括：所述接入和移动管理功能实体接收来自所述终端设备的注册请求消息。

在一种可能的实现方式中，所述方法还包括：所述接入和移动管理功能实体确定
15 更新所选的 EPS NAS 安全算法；所述接入和移动管理功能实体向所述终端设备提供更新后的所选的 EPS NAS 安全算法。

在一种可能的实现方式中，所述方法还包括：所述接入和移动管理功能实体确定没有成功为所述终端设备提供更新后的所选的 EPS NAS 安全算法；所述接入和移动管理功能实体向所述终端设备提供所述更新后的所选的 EPS NAS 安全算法。

该实现方式中，接入和移动管理功能实体在确定没有成功为终端设备提供更新后的所选的 EPS NAS 安全算法后，向终端设备提供更新后的所选的 EPS NAS 安全算法，确保了接入和移动管理功能实体能够成功为终端设备配置更新的所选的 EPS NAS 安全算法，使得终端设备中的 EPS NAS 安全算法与接入和移动管理功能实体确定的更新的所选的 EPS NAS 安全算法一致。
20

在一种可能的实现方式中，所述接入和移动管理功能实体支持 N26 接口，所述终端设备支持 S1 模式。
25

在一种可能的实现方式中，所述接入和移动管理功能实体中存在所述终端设备指示的有效第五代移动通信 5G NAS 安全上下文。

第二方面，本申请提供一种配置 EPS NAS 安全算法的方法，所述方法包括：终端设备确定不存在第五代移动通信 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法；
30 所述终端设备删除所述 5G NAS 安全上下文；所述终端设备向接入和移动管理功能实体发送第二消息，所述第二消息用于请求所述 5G NAS 安全上下文；所述终端设备接收来自所述接入和移动管理功能实体的所述所选的 EPS NAS 安全算法的信元。

本方法中，在终端设备中已经存在 5G NAS 安全上下文的情况下，首先确定终端设备的 5G NAS 安全上下文中是否存在对应的所选的 EPS NAS 安全算法，若终端设备确定 5G NAS 安全上下文中不存在对应的所选的 EPS NAS 安全算法，则将 5G NAS 安全上下文删除，重新向接入和移动管理功能实体请求 5G NAS 安全上下文，接入和移动管理功能实体再次向终端设备发送 5G NAS 安全上下文和对应的所选的 EPS NAS 安全算法的信元，确保了终端设备能够成功配置 EPS NAS 安全算法。
35

在一种可能的实现方式中，所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法包括：所述终端设备确定没有接收来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。

在一种可能的实现方式中，所述终端设备确定没有接收来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元包括：所述终端设备在预设时间内没有接收到来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。

该实现方式中，通过在预设时间内没有接收到来自接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元来确定终端设备中不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法，提高了终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法的准确度。

在一种可能的实现方式中，所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法之前，所述方法还包括：所述终端设备接收所述接入和移动管理功能实体发送的第三消息，所述第三消息包括所述 5G NAS 安全上下文；所述终端设备向所述接入和移动管理功能实体发送第三完成消息，所述第三完成消息用于表示所述终端设备已接收到所述第三消息。

该实现方式中，终端设备通过接收接入和移动管理功能实体发送的携带有 5G NAS 安全上下文的第三消息激活了 5G NAS 安全上下文，并向接入和移动管理功能实体发送第三完成消息，确保了终端设备成功激活了 5G NAS 安全上下文。

在一种可能的实现方式中，所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法包括：确定下一代无线接入网密钥集标识 ngKSI 没有对应的所选的 EPS NAS 安全算法。

该实现方式中，通过确定下一代无线接入网密钥集标识 ngKSI 没有对应的所选的 EPS NAS 安全算法来确定终端设备中不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法，提高了终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法的准确度。

在一种可能的实现方式中，所述方法还包括：所述终端设备将所述 ngKSI 设为无效值。

该实现方式中，在终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法，终端设备将所述 ngKSI 设为无效值，以便在下一次注册请求中向接入和移动管理功能实体重新请求 5G NAS 安全上下文。

在一种可能的实现方式中，所述终端设备与长期演进 LTE 系统断开连接，所述第二消息用于请求注册至新无线 NR 系统。

在一种可能的实现方式中，所述终端设备确定所述接入和移动管理功能实体支持 N26 接口。

在一种可能的实现方式中，所述接入和移动管理功能实体支持 N26 接口，所述终端设备支持 S1 模式。

第三方面，本申请提供一种配置 EPS NAS 安全算法的装置，所述装置可以包括用于实现第一方面中的方法的各个模块，这些模块可以通过软件和/或硬件的方式实现。

第四方面，本申请提供一种配置 EPS NAS 安全算法的装置，所述装置可以包括用

于实现第二方面中的方法的各个模块，这些模块可以通过软件和/或硬件的方式实现。

第五方面，本申请提供一种配置 EPS NAS 安全算法的装置。该装置可以包括与存储器耦合的处理器。其中，该存储器用于存储程序代码，该处理器用于执行该存储器中的程序代码，以实现第一方面或第二方面或其中任意一种实现方式中的方法。

5 可选地，该装置还可以包括该存储器。

第六方面，本申请提供一种芯片，包括至少一个处理器和通信接口，所述通信接口和所述至少一个处理器通过线路互联，所述至少一个处理器用于运行计算机程序或指令，以执行如第一方面或第二方面或其中任意一种可能的实现方式所述的方法。

10 第七方面，本申请提供一种计算机可读介质，该计算机可读介质存储用于设备执行的程序代码，该程序代码包括用于执行如第一方面或第二方面或其中任意一种可能的实现方式所述的方法。

第八方面，本申请提供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，使得计算机执行如第一方面或第二方面或其中任意一种可能的实现方式所述的方法。

15 第九方面，本申请提供一种接入和移动管理功能实体，包括至少一个处理器和通信接口，所述通信接口和所述至少一个处理器通过线路互联，所述通信接口与目标系统通信，所述至少一个处理器用于运行计算机程序或指令，以执行如第一方面或其中任意一种可能的实现方式所述的方法。

20 第十方面，本申请提供一种终端设备，包括至少一个处理器和通信接口，所述通信接口和所述至少一个处理器通过线路互联，所述通信接口与目标系统通信，所述至少一个处理器用于运行计算机程序或指令，以执行如第二方面或其中任意一种可能的实现方式所述的方法。

25 第十一方面，本申请提供一种通信系统，包括至少一个处理器和通信接口，所述通信接口和所述至少一个处理器通过线路互联，所述通信接口与目标系统通信，所述至少一个处理器用于运行计算机程序或指令，以执行如第一方面或第二方面或其中任意一种可能的实现方式所述的方法。

附图说明

- 图 1 为本申请的实施例的一种 5G 网络架构的示意图；
- 30 图 2 为本申请的实施例的另一种 5G 网络架构的示意图；
- 图 3 为本申请的实施例的一种配置 EPS NAS 安全算法的方法的流程示意图；
- 图 4 为本申请一个实施例的配置 EPS NAS 安全算法的方法的流程示意图；
- 图 5 为本申请另一个实施例的配置 EPS NAS 安全算法的方法的流程示意图；
- 图 6 为本申请的实施例的另一种配置 EPS NAS 安全算法的方法的流程示意图；
- 35 图 7 为本申请又一个实施例的配置 EPS NAS 安全算法的方法的流程示意图；
- 图 8 为本申请又一个实施例的配置 EPS NAS 安全算法的方法的流程示意图；
- 图 9 为本申请一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图；
- 图 10 为本申请另一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图；

图 11 为本申请又一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图。

具体实施方式

5 图 1 为本申请一个实施例的 5G 网络架构的示意图，5G 系统也称为新无线通信系统、新接入技术（new radio, NR）或者下一代移动通信系统。

如图 1 所示，该网络架构包括 UE、接入网（access network, AN）、核心网和数据网络（data network, DN）。其中，接入网主要用于实现无线物理层功能、资源调度和无线资源管理、无线接入控制以及移动性管理等功能；核心网可以包含管理设备
10 和网关设备，管理设备主要用于终端设备的设备注册、安全认证、移动性管理和位置管理等，网关设备主要用于与终端设备间建立通道，在该通道上转发终端设备和外部数据网络之间的数据包；数据网络可以包含网络设备（如：服务器、路由器等设备），数据网络主要用于为终端设备提供多种数据业务服务。需要说明的是，图 1 仅为示例性架构图，除图 1 中所示功能单元之外，该网络架构还可以包括其他功能单元，本申请
15 实施例对此不进行限定。

5G 系统中的接入网可以是无线接入网（radio access network, (R)AN），5G 系统中的(R)AN 设备可以由多个 5G-(R)AN 节点组成，该 5G-(R)AN 节点可以包括：非 3GPP 的接入网络如 WiFi 网络的接入点（access point, AP）、下一代基站（可统称为新一代无线接入网节点 NG-RAN node），其中，下一代基站包括新空口基站（NR nodeB, gNB）、新一代演进型基站（NG-eNB）、中心单元（central unit, CU）和分布式单元（distributed unit, DU）分离形态的 gNB 等）、收发点（transmission receive point, TRP）、传输点（transmission point, TP）或其它节点。
20

如图 1 所示，核心网可以包括接入和移动性管理功能（access and mobility management function, AMF）网元、会话管理功能（session management function, SMF）
25 网元、用户面功能（user plane function, UPF）网元、鉴权服务器功能（authentication server function, AUSF）网元、策略控制功能（policy control function, PCF）网元、应用功能（application function, AF）网元、统一数据管理功能（unified data management, UDM）网元、网络切片选择功能（network slice selection function, NSSF）网元等多个功能单元。

30 AMF 网元主要负责移动性管理、接入管理等服务。SMF 网元主要负责会话管理、UE 地址管理和分配、动态主机配置协议功能、用户面功能的选择和控制等。UPF 主要负责对外连接到数据网络（data network, DN）以及用户面的数据包路由转发、报文过滤、执行服务质量（quality of service, QoS）控制相关功能等。AUSF 主要负责对终端设备的认证功能等。PCF 网元主要负责为网络行为管理提供统一的策略框架、提供控制面功能的策略规则、获取与策略决策相关的注册信息等。需要说明的是，这些
35 功能单元可以独立工作，也可以组合在一起实现某些控制功能，如对终端设备的接入鉴权、安全加密、位置注册等接入控制和移动性管理功能，以及用户面传输路径的建立、释放和更改等会话管理功能。

5G 网络中各功能单元之间可以通过下一代网络（next generation, NG）接口进行

通信，如：UE 可以通过 NG 接口 1（简称 N1）与 AMF 网元进行控制面消息的传输，RAN 设备可以通过 NG 接口 3（简称 N3）与 UPF 建立用户面数据传输通道，AN/RAN 设备可以通过 NG 接口 2（简称 N2）与 AMF 网元建立控制面信令连接，UPF 可以通过 NG 接口 4（简称 N4）与 SMF 网元进行信息交互，UPF 可以通过 NG 接口 6（简称 N6）与数据网络 DN 交互用户面数据，AMF 网元可以通过 NG 接口 11（简称 N11）与 SMF 网元进行信息交互，SMF 网元可以通过 NG 接口 7（简称 N7）与 PCF 网元进行信息交互，AMF 网元可以通过 NG 接口 12（简称 N12）与 AUSF 进行信息交互。

图 1 所示网络架构为基于参考点网络架构，且该网络架构为非漫游场景下的网络架构，当然本申请的方法也可以应用在漫游场景下，并且网络架构也不限于基于参考点的网络架构，也可以采用基于服务化接口的网络架构。

图 2 为本申请另一个实施例的 5G 网络架构的示意图。如图 2 所示，该网络架构主要是基于服务化接口的网络架构。该网络架构与图 1 所示的网络架构相比较而言，核心网还包括 NEF 和 NRF 网元。

基于服务化接口的场景下，核心网中的部分网元通过总线方式连接。如图 2 所示，AUSF 网元、AMF 网元、SMF 网元、AF 网元、UDM、PCF 网元、网络存储功能（network repository function, NRF）网元、网络开放功能（network exposure function, NEF）网元和 NSSF 网元通过总线互连，所述网元在通过总线互连时，采用服务化接口，例如，AUSF 网元通过 Nausf 接口连接到总线上，AMF 网元采用 Namf 接口连接到总线上，SMF 网元通过 Nsmf 接口连接到总线上，AF 网元采用 NAF 网元接口连接到总线上，UDM 采用 Nudm 接口连接到总线上，PCF 网元通过 NPCF 网元接口连接到总线上，NRF 通过 Nnrf 接口连接到总线上，NEF 通过 Nnef 接口连接到总线上，NSSF 通过 Nnssf 接口连接到总线上。

目前，在 5G 网络支持 N26 接口、终端设备支持 S1 模式的情况下，UE 的注册流程中可以包括两次 SMC 流程。在 UE 的注册流程中，会出现第一次 SMC 流程正常，第二次 SMC 异常的情况。在这种情况下，当 UE 再次发起注册请求时，由于第一次 SMC 流程正常，即 UE 和网络之间的 5G NAS 安全上下文正常，因此网络可能不再重新执行第二次 SMC 流程。但是，EPS NAS 安全算法的配置信息是网络在第二次 SMC 流程中向 UE 下发的，这会导致注册成功后的 UE 中无 EPS NAS 安全算法，从而导致 UE 后续切换至长期演进（long term evolution, LTE）时会出现切换失败、业务中断和/或业务功能不连续等问题。

针对上述问题，本申请提出了新的技术方案。本申请提出的技术方案可以确保接入和移动管理功能实体能够为终端设备成功配置 EPS NAS 安全算法。

图 3 为本申请的实施例的一种配置 EPS NAS 安全算法的方法的流程示意图。如图 3 所示，该方法至少包括 S301 至 S302。

S301，接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法。

本实施例中，接入和移动管理功能实体为终端设备提供所选的 EPS NAS 安全算法可以是接入和移动管理功能实体在终端设备没有有效 EPS NAS 安全算法的场景下为该终端设备选择的 EPS NAS 安全算法；或者，接入和移动管理功能实体为终端设备提

供所选的 EPS NAS 安全算法可以是终端设备上已有有效 EPS NAS 安全算法的场景下，接入和移动管理功能实体为终端设备重新选择的 EPS NAS 安全算法。

接入和移动管理功能实体为终端设备提供所选的 EPS NAS 安全算法的一种实现方式为：接入和移动管理功能实体向终端设备发送第一消息，第一消息包括接入和移动管理功能实体为终端设备所选的 EPS NAS 安全算法的信元(information element, IE)。其中，第一消息的一种示例为 SMC 消息。

本实施例中的 NAS 安全算法的信元可以指示用于加密和完整性保护的算法，EPS NAS 安全算法的信元可以指示 EPS 中用于加密和完整性保护的算法。本实施例中的信元也可以替换为信息。其中该信元可以是所选的 EPS NAS 安全算法本身，也可以是用于指示所选的 EPS NAS 安全算法的信息，例如，可以是用于指示所选的 EPS NAS 安全算法的有效值。示例性的，本实施例中的信元的具体形式可以是比特位。

该实现方式中，接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法的一种示例包括：接入和移动管理功能实体确定没有接收到来自终端设备的第一完成消息，第一完成消息用于表示终端设备已接收到接入和移动管理功能实体为其选择的 EPS NAS 安全算法的信元。例如，接入和移动管理功能实体在预设时长内没有接收到来自终端设备的第一完成消息时，可以确定没有成功为终端设备提供所选的 EPS NAS。其中，第一完成消息的一种示例为 SMC 完成消息。

接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法的另一种示例包括：终端设备在预设时间内没有接收到来自接入和移动管理功能实体的第一消息，则向接入和移动管理功能实体发送第一指示消息，第一指示消息用于指示终端设备没有成功接收 EPS NAS 安全算法的信元的消息；接入和移动管理功能实体接收到第一指示消息之后，确定没有成功为终端设备提供所选的 EPS NAS 安全算法。

本实施例的一些实现方式中，接入和移动管理功能实体支持 N26 接口，终端设备支持 S1 模式。其中，N26 接口为第四代移动通信（4th generation, 4G）核心网与 5G 核心网之间的接口，即移动管理节点功能（mobility management entity, MME）网元与 AMF 网元之间的接口，用于 4G 与 5G 的互操作。终端设备支持 S1 模式表示该终端设备支持连接至 LTE 网络。

本实施例中的一些实现方式中，在接入和移动管理功能实体确定是否成功向终端设备提供所选的 EPS NAS 安全算法之前，或者在接入和移动管理功能实体向终端提供所选的 EPS NAS 安全算法之前，接入和移动管理功能实体可以接收来自终端设备的注册请求（Registration Request）消息。

作为一个示例，接入和移动管理功能实体接收来自终端设备的注册请求消息之后，响应于该注册请求消息可以判断接入和移动管理功能实体上是否存在终端设备指示的有效 5G NAS 安全上下文；若存在，则进一步判断接入和移动管理功能实体是否成功向终端设备提供过所选的 EPS NAS 安全算法；若不存在，则向终端设备下发 SMC 流程，以激活终端设备指示的有效 5G NAS 安全上下文。

其中，接入和移动管理功能实体上不存在终端设备指示的有效 5G NAS 安全上下文的情况下，若终端设备支持 S1 模式且接入和移动管理功能实体支持 N26 接口，则接入和移动管理功能实体向终端设备下发第一次 SMC 流程之后，还可以向终端设备再

次下发 SMC 流程并携带为终端设备所选的 EPS NAS 安全算法；接入和移动管理功能实体上不存在终端设备指示的有效 5G NAS 安全上下文的情况下，若终端设备不支持 S1 模式和/或接入和移动管理功能实体不支持 N26 接口，则接入和移动管理功能实体向终端设备下发第一次 SMC 流程之后，可以不用向终端设备再次下发 SMC 流程并携带为终端设备所选的 EPS NAS 安全算法的信元。

本实施例中，可选的，接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法后，可以标记未成功为终端设备配置所选的 EPS NAS 安全算法的标记信息。

示例性的，接入和移动管理功能实体可以为 5G 网络中的 AMF 网元，也可以为 6G 网络中具有接入和移动性管理功能的网元。

S302，接入和移动管理功能实体向终端设备提供所选的 EPS NAS 安全算法。

也就是说，在接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法之后，向终端设备重新提供所选的 EPS NAS 安全算法。

例如，若接入和移动管理功能实体向终端设备发送第一消息之后，（在预设时间内）没有接收到来自终端设备的第一完成消息，则接入和移动管理功能实体可以确定没有成功为终端设备提供所选的 EPS NAS 安全算法，因此向终端设备重新发送第一消息。

又如，若接入和移动管理功能实体向终端设备发送第一消息之后，（在预设时间内）没有接收到来自终端设备的第一完成消息，则接入和移动管理功能实体可以确定没有成功为终端设备提供所选的 EPS NAS 安全算法，并将所选的 EPS NAS 安全算法标记为无效值，然后在接入和移动管理功能实体接收到来自终端设备的注册请求消息之后，在接入和移动管理功能实体上存在终端设备的有效 5G 安全上下文的情况下，因为所选的 EPS NAS 安全算法标记为无效值而向终端设备重新发送第一消息。该示例的一种实现方式可以参考图 4 所示的实施例。

再如，接入和移动管理功能实体向终端设备更新所选的 EPS NAS 安全算法，且确定没有成功为终端设备提供该更新的 EPS NAS 安全算法时，可以生成所选的 EPS NAS 安全算法更新的指示信息；并在接收到来自终端设备的初始接入请求消息（例如注册请求消息）时，基于该指示信息重新向终端设备提供该更新的 EPS NAS 安全算法。该示例的一种实现方式可以参考图 5 所示的实施例。

作为一种示例，接入和移动管理功能实体选择在 EPS 中使用的加密算法和完整性算法，并通过所选的 EPS NAS 安全算法的信元向终端设备指示所选的算法，例如通过向终端设备发送 SMC 消息，该 SMC 消息包括所选的 EPS NAS 安全算法的信元的方式向终端设备指示所选的算法。

本申请提出的技术方案中，接入和移动管理功能实体在未成功为终端设备提供所选的 EPS NAS 安全算法的情况下，向终端设备重新提供所选的 EPS NAS 安全算法，可以确保接入和移动管理功能实体能够为终端设备成功配置所选的 EPS NAS 安全算法。

需要说明的是，本申请实施例提供的方法中接入和移动管理功能实体重新发送的不限于是接入和移动管理功能实体所选的 EPS NAS 安全算法，也可以是未来支持 5G

和/或 6G 网络的终端设备向 6G 网络注册时获取的关于 5G 的安全算法, 该 5G 的安全算法可以用于终端设备后续生成 5G NAS 安全上下文。

也就是说, 只要是接入和移动管理功能实体在确定没有成功为终端设备提供的用于终端设备后续生成 NAS 安全上下文的情况下, 向终端设备发送该 NAS 安全上下文的方法都可纳入本申请技术方案的保护范围。

图 4 为本申请一个实施例的配置 EPS NAS 安全算法的方法的流程示意图。如图 4 所示, 该方法至少包括 S401 至 S414。在本实施例中, 接入和移动管理功能实体为 AMF 网元。

S401, UE 向 AMF 网元发送注册请求消息, 该注册请求消息中携带 ngKSI 的值为 7。为了便于描述, 该注册请求消息可以称为第一注册请求消息。

此时 UE 侧无 5G NAS 安全上下文, 故在 UE 向 AMF 网元发起的第一注册请求信息中携带的下一代无线接入网密钥集标识 (key set identifier for next generation radio access network, ngKSI) 的值为 7, 7 表示 UE 侧无 5G NAS 安全上下文。

S402, AMF 网元向 UE 发送身份认证请求 (identity request) 消息。

S403, UE 向 AMF 网元发送身份认证回复 (identity response) 消息。

S404, AMF 网元向 UE 发送鉴权认证请求 (authentication request) 消息。

可选的, UE 在接收到来自 AMF 网元发送的鉴权认证请求 (authentication request) 消息之后, 可以根据该鉴权认证请求 (authentication request) 消息生成未激活的 5G NAS 安全上下文。

S405, UE 向 AMF 网元发送鉴权认证回复 (authentication response) 消息。

S402 至 S405 为 UE 与 AMF 网元进行身份认证和鉴权认证的过程, 当 UE 通过了 AMF 网元的身份认证和鉴权认证后, AMF 网元会与 UE 进行下面的注册流程。

S406, AMF 网元向 UE 发送 SMC 消息, 该 SMC 消息中携带 ngKSI 的有效值。该 SMC 消息可以称为第一 SMC 消息。

当 UE 通过了 AMF 网元的身份认证和鉴权认证之后, AMF 网元向 UE 发送第一 SMC 消息, 第一 SMC 消息中携带 ngKSI 的有效值, 用来激活 UE 中的 5G NAS 安全上下文, 此时 UE 中会存在与第一 SMC 消息中携带的 ngKSI 的有效值对应的当前安全上下文 (current security context)。其中, ngKSI 的有效值可以为 0 至 6 中任意一个整数值, 每个整数值对应一套 5G NAS 安全上下文。

S407, UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第一 SMC 完成消息。

当 UE 成功接收 AMF 网元发送的第一 SMC 消息, 并且根据第一 SMC 消息中携带的 ngKSI 的有效值成功激活了 5G NAS 安全上下文后, 向 AMF 网元发送第一 SMC 完成消息, 表示 UE 已经成功配置了 ngKSI 的有效值对应的 5G NAS 安全上下文。

S408, AMF 网元向 UE 发送 SMC 消息, 该 SMC 消息中携带所选的 EPS NAS 安全算法的信元。该 SMC 消息称为第二 SMC 消息。

当 AMF 网元接收到 UE 发送的第一 SMC 完成消息后, 向 UE 发送第二 SMC 消息, 第二 SMC 消息中携带所选的 EPS NAS 安全算法的信元, 用来为 UE 配置所选的 EPS NAS 安全算法的信元对应的 EPS NAS 安全算法。其中, EPS NAS 安全算法的信元可

以为 0 至 7 中任意一个整数值，每个整数值对应一个 EPS NAS 安全算法。

可以理解的是，本实施例中的 UE 支持 S1 模式，且 AMF 网元支持 N26 接口。

S409，AMF 网元没有接收到 UE 响应于第二 SMC 消息发送的 SMC 完成消息，将所选的 EPS NAS 安全算法标记为无效。该 SMC 完成消息称为第二 SMC 完成消息。

- 5 当 AMF 网元向 UE 发送第二 SMC 消息后，AMF 网元没有接收到 UE 发送的第二 SMC 完成消息，则表示 UE 没有成功配置 AMF 在第二 SMC 消息中携带的所选的 EPS NAS 安全算法的信元对应的所选的 EPS NAS 安全算法。

一种可能的实现方式，由于网络信号异常等因素，UE 没有接收到 AMF 网元发送的携带有所选的 EPS NAS 安全算法的信元的第二 SMC 消息。

- 10 另一种可能的实现方式，UE 接收到了 AMF 网元发送的携带有所选的 EPS NAS 安全算法的信元的第二 SMC 消息，但未能根据所选的 EPS NAS 安全算法的信元成功配置对应的所选的 EPS NAS 安全算法。

上述 S401 至 S409 可以称为第一次注册流程；下面描述的注册流程可以称为第二次注册流程。

- 15 S410，UE 向 AMF 网元发送注册请求消息，该注册请求信息中携带 ngKSI 的有效值。该注册请求消息可以称为第二注册请求消息。

- UE 经过第一次注册流程，已经根据 AMF 网元在第一 SMC 消息中携带的 ngKSI 的有效值成功激活了对应的 5G NAS 安全上下文。UE 向 AMF 网元发起第二注册请求消息时，第二注册请求消息中携带的 ngKSI 的值为与 UE 中的 5G NAS 安全上下文对应的 ngKSI 的有效值。也就是说，UE 在第二注册请求消息中携带的 ngKSI 的有效值与 AMF 网元在第一次注册流程中的第一 SMC 消息中携带的 ngKSI 的有效值相同。
- 20

S411，AMF 网元对第二注册请求消息进行检查。

- AMF 网元对第二注册请求消息的检查包括对第二注册请求消息进行完整性检查和判断 AMF 网元是否能够对第二注册请求消息中的 NAS 信息箱 (NAS message container) 解密成功。
- 25

S412，AMF 网元向 UE 发送 SMC 消息，该 SMC 消息中携带 ngKSI 的有效值和所选的 EPS NAS 安全算法的信元。该 SMC 消息可以称为第三 SMC 消息。

具体地，AMF 网元检查终端设备的 ngKSI 对应的安全上下文中是否存在有效的 EPS NAS 安全算法，若不存在，则通过 SMC 流程提供所选的 EPS NAS 安全算法。

- 30 本实施例中，因为在 S409 中，AMF 网元将当前的安全上下文中的 ngKSI 对应的所选的 EPS NAS 安全算法标记为无效，所以 AMF 网元向 UE 发送第三 SMC 消息。

- 示例性的，第三 SMC 消息中携带 ngKSI 的有效值与 UE 在第二注册请求信息中携带的 ngKSI 的有效值和 AMF 网元在第一注册请求流程中的第一 SMC 消息中携带的 ngKSI 的有效值相同；第三 SMC 消息中携带的所选的 EPS NAS 安全算法的信元与 AMF 网元在第二 SMC 消息中携带的 EPS NAS 安全算法的信元相同，终端设备根据第三 SMC 消息中携带的所选的 EPS NAS 安全算法的信元配置所选的 EPS NAS 安全算法。
- 35

S413，UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第三 SMC 完成消息。

当 UE 成功配置 AMF 网元在第三 SMC 消息中携带的所选的 EPS NAS 安全算法的

信元对应的所选的 EPS NAS 安全算法后，向 AMF 网元发送第三 SMC 完成消息。

S414, AMF 网元向 UE 发送注册成功消息。

当 UE 根据第二注册请求消息注册成功后，AMF 网元向 UE 发送注册成功消息。

本申请提出的技术方案中，UE 在无 5G NAS 安全上下文时向 AMF 网元发起注册
5 请求消息，UE 支持 S1 模式，网络支持 N26 接口时，UE 在第一次注册过程中只成功
收到第一 SMC 消息，并激活了 5G NAS 安全上下文；AMF 网元未收到来自 UE 的第
二 SMC 完成消息时，AMF 网络标记所选的 EPS NAS 安全算法未配置成功，并在 UE
发起第二次注册请求消息时，AMF 网元根据标记的所选的 EPS NAS 安全算法未配置
成功的信息，再次为 UE 提供所选的 EPS NAS 安全算法，确保了 AMF 网元能够成功
10 为 UE 配置所选的 EPS NAS 安全算法。

图 5 为本申请另一个实施例的配置 EPS NAS 安全算法的方法的流程示意图。如图
5 所示，该方法至少包括 S501 至 S507。在本实施例中，接入和移动管理功能实体为
AMF 网元。

S501, UE 向 AMF 网元发送业务请求消息或注册请求消息。该业务请求消息可以
15 称为第一业务请求消息，该注册请求消息可以称为第一注册请求消息。

UE 通过向 AMF 发送第一业务请求消息或第一注册请求消息等初始接入流程消息，
触发链路建立后进入连接态。

在本实施例中，UE 存在有效的 EPS NAS 安全算法。

S502, AMF 网元向 UE 发送 SMC 消息，该 SMC 消息中携带更新的所选的 EPS NAS
20 安全算法的信元。该 SMC 消息可以称为第一 SMC 消息。

AMF 网元将要向 UE 中已经存在的 EPS NAS 安全算法进行修改，故 AMF 网元在
向 UE 发送的第一 SMC 消息中携带了将要为 UE 配置的更新的所选的 EPS NAS 安全
算法的信元。

S503, AMF 网元未收到 UE 发送的 SMC 完成消息，标记更新的所选的 EPS NAS
25 安全算法配置失败，释放链路。该 SMC 完成消息可以称为第一 SMC 完成消息。

若 AMF 网元未收到第一 SMC 完成消息，将导致此次业务请求或注册请求等初始
接入流程终止，此时 AMF 网元需要标记用于表示更新的所选的 EPS NAS 安全算法配
置失败的标记信息，并释放链路资源。

S504, UE 再次向 AMF 网元发送业务请求消息或注册请求消息。该业务请求消息
30 可以称为第二业务请求消息，该注册请求消息可以称为第二注册请求消息。

UE 通过向 AMF 网元发送第二业务请求消息或第二注册请求消息等初始接入流程
消息，再次触发链路建立后进入连接态。

S505, AMF 网元确认存在更新的所选的 EPS NAS 安全算法配置失败的标识信息。

当 AMF 网元接收到 UE 发送的第二业务请求消息或第二注册请求消息等初始接入
35 流程消息后，需要确认是否存在用于表示更新的所选的 EPS NAS 安全算法配置失败的
标识信息。若 AMF 网元中存在更新的所选的 EPS NAS 安全算法配置失败的标识信息，
则需要再次向 UE 发送携带更新的所选的 EPS NAS 安全算法的信元的 SMC 消息。

S506, AMF 网元向 UE 发送 SMC 消息，该 SMC 消息中携带更新的所选的 EPS NAS
安全算法的信元。该 SMC 消息可以称为第二 SMC 消息。

AMF 网元向 UE 发送第二 SMC 消息，第二 SMC 消息中携带了将要为 UE 配置的更新的所选的 EPS NAS 安全算法的信元。

- 可选的，第二 SMC 消息中携带的更新的所选的 EPS NAS 安全算法的信元可以与第一 SMC 消息中携带的更新的所选的 EPS NAS 安全算法的信元相同，也可以与第一 SMC 消息中携带的更新的所选的 EPS NAS 安全算法的信元不同。

S507, UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第二 SMC 完成消息。

- 当 UE 成功配置了 AMF 网元在第二 SMC 消息中携带的更新的所选的 EPS NAS 安全算法的信元对应的更新的所选的 EPS NAS 安全算法后，向 AMF 网元发送第二 SMC 完成消息，此时 UE 中的 EPS NAS 安全算法与 AMF 网元中的更新的所选的 EPS NAS 安全算法一致。

- 本申请提出的技术方案中，UE 中存在 EPS NAS 安全算法，AMF 网元希望改变 UE 中的 EPS NAS 安全算法，当 UE 处于连接态时，AMF 网元向 UE 发送携带更新的所选的 EPS NAS 安全算法的信元的 SMC 消息，但是 AMF 网元未收到 UE 发送的 SMC 完成消息的回复时，AMF 网元标记更新的所选的 EPS NAS 安全算法未修改成功的信息，当 UE 再一次处于连接态时，AMF 网元根据标记的更新的所选的 EPS NAS 安全算法未修改成功的信息，为 UE 重新下发更新的所选的 EPS NAS 安全算法的信元的 SMC 消息，确保了 AMF 网元能够成功为 UE 配置更新的所选的 EPS NAS 安全算法，使得 UE 中 EPS NAS 安全算法与 AMF 网元中的一致。

- 图 6 为本申请的实施例的另一种配置 EPS NAS 安全算法的方法的流程示意图。如图 6 所示，该方法至少包括 S601 至 S604。

S601, 终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法。

本实施例中，终端设备中已经存在 5G NAS 安全上下文，但不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法。

- 终端设备激活 5G NAS 安全上下文的一种实现方式为：终端设备向接入和移动管理功能实体发送注册请求消息后；接入和移动管理功能实体向终端设备发送第三消息，第三消息中包括 5G NAS 安全上下文；终端设备接收第三消息并根据第三消息成功激活 5G NAS 安全上下文后，向接入和移动管理功能实体发送第三完成消息，第三完成消息用于表示终端设备已接收到第三消息；接入和移动管理功能实体接收到来自终端设备的第三完成消息后，向终端设备提供所选的 EPS NAS 安全算法。其中，第三消息的一种示例为 SMC 消息，第三完成消息的一种示例为 SMC 完成消息。

- 该实现方式中，终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法的一种示例包括：终端设备确定没有接收来自接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。例如，终端设备在预设时间内没有接收来自接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元，可以确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法。

在该种可能的实现方式中，接入和移动管理功能实体支持 N26 接口，终端设备支持 S1 模式。

终端设备激活 5G NAS 安全上下文的另一种实现方式为：终端设备连接在 LTE 网

络时向 NR 系统中的 AMF 网元请求注册并完成注册流程,终端设备在该注册流程中激活了 5G NAS 安全上下文。在完成该注册流程之后,终端设备与 LTE 网络断开连接,再次向 NR 系统中的 AMF 网元请求注册。

- 该实现方式中,终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法的一种示例包括:终端设备的 ngKSI 中没有对应的所选的 EPS NAS 安全算法,可以确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法。

在该种可能的实现方式中,终端设备支持 SI 模式,并且终端设备可以确定 AMF 网元支持 N26 接口。

S602,终端设备删除 5G NAS 安全上下文。

- 10 若终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法,则删除已经激活的 5G NAS 安全上下文。

可选的,若终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法,将 ngKSI 设为无效值,即将 ngKSI 的值设置为 7。

- 15 S603,终端设备向接入和移动管理功能实体发送第二消息,第二消息用于请求 5G NAS 安全上下文。

作为一种示例,终端设备向接入和移动管理功能实体发送第二消息时,第二消息中携带 ngKSI 的值为 7,7 表示终端设备中不存在 5G NAS 安全上下文。

- 20 可选的,当接入和移动管理功能实体接收到来自终端设备的携带有 ngKSI 的值为 7 的第二消息后,接入和移动管理功能实体向终端设备发送第四消息,第四消息中包括一个 ngKSI 的有效值,ngKSI 的有效值可以为 0 至 6 中任意一个整数值,每个整数值对应一套 5G NAS 安全上下文。其中,第四消息的一个示例为 SMC 消息。

- 25 若终端设备根据接入和移动管理功能实体发送的携带有 ngKSI 的有效值的第四消息成功激活了 5G NAS 安全上下文,则终端设备向接入和移动管理功能实体发送第四完成消息,第四完成消息用于表示终端设备已接收到接入和移动管理功能实体发送的 ngKSI 的有效值,并根据 ngKSI 的有效值成功激活了该 ngKSI 的有效值对应的 5G NAS 安全上下文。其中,第四完成消息的一个示例为 SMC 完成消息。

可选的,能够使接入和移动管理功能实体获知向终端设备提供 5G NAS 安全上下文的消息都可以称为本申请实施例中的第二消息。

- 30 例如,第二消息可以是注册请求消息,接入和移动管理功能实体可以根据注册请求消息中携带的 ngKSI 的值来判断终端设备中是否存在 5G NAS 安全上下文,若注册请求消息中携带的 ngKSI 的值为 7,表示终端设备中不存在 5G NAS 安全上下文,接入和移动管理功能实体需要为终端设备提供 5G NAS 安全上下文。

S604,终端设备接收来自接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。

- 35 作为一个示例,终端设备在重新激活了 5G NAS 安全上下文之后,能够接收 5G NAS 安全上下文发送的第五消息,第五消息中包括 5G NAS 安全上下文确定的所选的 EPS NAS 安全算法的信元,所选的 EPS NAS 安全算法的信元可以为 0 至 7 中任意一个整数值,每个整数值对应一个所选的 EPS NAS 安全算法。其中,第五消息的一个示例为 SMC 消息。

本申请提出的技术方案中,在终端设备中已经存在 5G NAS 安全上下文的情况下,首先确定终端设备的 5G NAS 安全上下文中是否存在对应的所选的 EPS NAS 安全算法,若终端设备确定 5G NAS 安全上下文中不存在对应的所选的 EPS NAS 安全算法,则将 5G NAS 安全上下文删除,重新向接入和移动管理功能实体请求 5G NAS 安全上下文,接入和移动管理功能实体再次向终端设备发送 5G NAS 安全上下文和对应的所选的 EPS NAS 安全算法的信元,确保了终端设备能够成功配置 EPS NAS 安全算法。

图 7 为本申请又一个实施例的配置 EPS NAS 安全算法的方法的流程示意图。如图 7 所示,该方法至少包括 S701 至 S719。在本实施例中,接入和移动管理功能实体为 AMF 网元。

10 S701, UE 向 AMF 网元发送注册请求消息,该注册请求消息中携带 ngKSI 的值为 7。为了便于描述,该注册请求消息可以称为第一注册请求消息。

S702, AMF 网元向 UE 发送申请认证请求(identity request)消息。

S703, UE 向 AMF 网元发送身份认证回复(identity response)消息。

S704, AMF 网元向 UE 发送鉴权认证请求(authentication request)消息。

15 S705, UE 向 AMF 网元发送鉴权认证回复(authentication response)消息。

S706, AMF 网元向 UE 发送 SMC 消息,该 SMC 消息中携带 ngKSI 的有效值。该 SMC 消息可以称为第一 SMC 消息。

S707, UE 向 AMF 网元发送 SMC 完成信息。该 SMC 完成消息可以称为第一 SMC 完成消息。

20 本实施例中的 S701 至 S707 可以参考 S401 至 S407,此处不再进行赘述。

S708, AMF 网元向 UE 发送 SMC 消息,该 SMC 消息中携带所选的 EPS NAS 安全算法的信元。该 SMC 消息称为第二 SMC 消息。

S709, UE 没有接收到 AMF 网元发送的第二 SMC 消息,删除 5G NAS 安全上下文。

25 本实施例中,UE 没有接收到 AMF 网元发送的第二 SMC 消息的一种可能的原因为第一次注册流程中断导致第二 SMC 消息没有成功到达 UE;另一种可能的原因为 AMF 网元并没有执行 S708,即 AMF 网元并没有向 UE 发送所选的 EPS NAS 安全算法的信元。由此可知,本实施例中的 S708 是可选的,即不是必须执行的步骤。

30 在 S707 中,UE 向 AMF 网元发送了第一 SMC 完成消息,表示 UE 已经成功激活了第一 SMC 消息中携带的 ngKSI 的有效值对应的 5G NAS 安全上下文。但 UE 没有接收到 AMF 网元发送的第二 SMC 消息,表示 UE 中不存在第二 SMC 消息中携带的所选的 EPS NAS 安全算法的信元对应的所选的 EPS NAS 安全算法,此时 UE 需要删除已经激活的 5G NAS 安全上下文,并向 AMF 网元再次发起注册请求,用于请求 5G NAS 安全上下文。

35 上述 S701 至 S709 可以称为第一次注册流程;下面描述的注册流程可以称为第二次注册流程。

S710, UE 向 AMF 网元发送注册请求消息,该注册请求消息中携带 ngKSI 的值为 7。该注册请求消息可以称为第二注册请求消息。

由于在 S709 中,UE 删除了 5G NAS 安全上下文,故在 UE 向 AMF 网元发送的第

二注册请求消息中携带的 ngKSI 的值为 7, 7 表示 UE 中无 5G NAS 安全上下文。

S711, AMF 网元向 UE 发送身份认证请求 (identity request) 消息。

S712, UE 向 AMF 网元发送身份认证回复 (identity response) 消息。

S713, AMF 网元向 UE 发送鉴权请求 (authentication request) 消息。

5 S714, UE 向 AMF 网元发送鉴权回复 (authentication response) 消息。

需要说明的是, S711 至 S714 可以参考 S402 至 S405, 此处不再进行赘述。

S715, AMF 网元向 UE 发送 SMC 消息, 该 SMC 消息中携带 ngKSI 的有效值。该 SMC 消息可以称为第三 SMC 消息。

10 当 UE 通过了 AMF 网元的身份认证和鉴权认证之后, AMF 网元向 UE 发送第三 SMC 消息, 第三 SMC 消息中携带 ngKSI 的有效值, 用来激活 UE 中的 5G NAS 安全上下文。

可选的, 第三 SMC 消息中携带 ngKSI 的有效值与第一次 SMC 流程信息中携带 ngKSI 的有效值相同。

15 S716, UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第三 SMC 消息。

20 当 UE 成功接收 AMF 发送的第三 SMC 消息, 并且根据第三 SMC 消息中携带的 ngKSI 的有效值成功激活了 5G NAS 安全上下文后, 向 AMF 网元发送第三 SMC 完成消息, 表示 UE 已经成功配置了 ngKSI 的有效值对应的 5G NAS 安全上下文。其中, ngKSI 的有效值可以为 0 至 6 中任意一个整数值, 每个整数值对应一个 5G NAS 安全上下文。

S717, AMF 网元向 UE 发送 SMC 消息, 该 SMC 消息中携带所选的 EPS NAS 安全算法的信元。该 SMC 消息可以称为第四 SMC 消息。

25 当 AMF 网元接收到 UE 发送的第三 SMC 完成消息后, 向 UE 发送第四 SMC 消息, 第四 SMC 消息中携带所选的 EPS NAS 安全算法的信元, 用来为 UE 配置所选的 EPS NAS 安全算法的信元对应的所选的 EPS NAS 安全算法。

可选的, 第四 SMC 消息中携带的所选的 EPS NAS 安全算法的信元与第二 SMC 消息中携带的所选的 EPS NAS 安全算法的信元相同。

S718, UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第四 SMC 消息。

30 当 UE 成功配置 AMF 网元在第四 SMC 消息中携带的所选的 EPS NAS 安全算法的信元对应的所选的 EPS NAS 安全算法后, 向 AMF 网元发送第四 SMC 完成消息。

S719, AMF 网元向 UE 发送注册成功消息。

35 当 UE 根据第二注册请求消息注册成功后, AMF 网元向 UE 发送注册成功消息。此时 UE 通过第二注册请求消息成功激活了 5G NAS 安全上下文, 并成功配置了所选的 EPS NAS 安全算法。

本申请提出的技术方案中, UE 在无 5G NAS 安全上下文时向 AMF 发起注册请求消息, 当 UE 只接收到第一 SMC 消息, 未接收到配置 EPS NAS 安全算法的第二 SMC 消息时, UE 主动删除已经激活的 5G NAS 安全上下文, 并在再次向 AMF 网元发起的注册请求消息中, 向 AMF 网元请求 5G NAS 安全上下文, AMF 网元再次向终端设备

发送 5G NAS 安全上下文和所选的 EPS NAS 安全算法的信元，确保了终端设备能够成功配置 EPS NAS 安全算法。

图 8 为本申请又一个实施例的配置 EPS NAS 安全算法的方法的流程示意图。本实施例适用于终端设备已经在 LTE 系统完成与 NR 系统的注册流程，并成功激活了 5G NAS 安全上下文时，与 LTE 系统断开连接并再次向 NR 系统请求注册的场景。如图 8 所示，该方法至少包括 S801 至 S811。在本实施例中，接入和移动管理功能实体为 AMF 网元。

S801，UE 确定当前的安全上下文中没有 EPS NAS 安全算法，删除当前的安全上下文。

10 UE 在向 NR 系统发起注册请求之前，需要确定 UE 中当前的安全上下文中是否存在 ngKSI 对应的有效的 EPS NAS 安全算法。若 UE 中当前的安全上下文中不存在 ngKSI 对应的有效的 EPS NAS 安全算法，则将 UE 中当前的安全上下文删除，即将 ngKSI 中的 NAS 密钥集标识符的值改为 7，7 表示 UE 中不存在 5G NAS 安全上下文。

15 S802，UE 向 AMF 网元发送注册请求消息，该注册请求消息中携带 ngKSI 的值为 7。

S803，AMF 网元向 UE 发送申请认证请求（identity request）消息。

S804，UE 向 AMF 网元发送身份认证回复（identity response）消息。

S805，AMF 网元向 UE 发送鉴权认证请求（authentication request）消息。

S806，UE 向 AMF 网元发送鉴权认证回复（authentication response）消息。

20 S807，AMF 网元向 UE 发送 SMC 消息，该 SMC 消息中携带 ngKSI 的有效值。该 SMC 消息可以称为第一 SMC 消息。

S808，UE 向 AMF 网元发送 SMC 完成消息。该 SMC 完成消息可以称为第一 SMC 完成消息。

25 S809，AMF 网元向 UE 发送 SMC 消息，该 SMC 消息中携带所选的 EPS NAS 安全算法的信元。该 SMC 消息称为第二 SMC 消息。

S810，UE 向 AMF 网元发送 SMC 完成消息。

S811，AMF 网元向 UE 发送注册完成信息。该 SMC 完成消息称为第二 SMC 完成消息。

本实施例中的 S802 至 S811 可以参考 S710 至 S719，此处不再进行赘述。

30 本申请提出的技术方案中，UE 在连接至 LTE 系统时完成与 NR 系统的注册流程，已经成功激活了 5G NAS 安全上下文，与 LTE 网络断开连接后，再次向 NR 系统发起注册请求时，首先判断 UE 中的 5G NAS 安全上下文中是否存在 EPS NAS 安全算法，若 UE 中的 5G NAS 安全上下文中不存在 EPS NAS 安全算法，则删除 UE 中的 5G NAS 安全上下文，并在注册请求中向 AMF 网元重新请求 5G NAS 安全上下文，AMF 网元
35 再次向 UE 发送 5G NAS 安全上下文和所选的 EPS NAS 安全算法的信元，确保了 UE 能够成功配置 EPS NAS 安全算法。

图 9 为本申请一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图。如图 9 所示，装置 900 可以包括处理模块 901 和发送模块 902。装置 900 可以用于实现图 3 至图 5 中任意一个所示的实施例中由接入和移动管理功能实体或 AMF 网元实

现的操作。

在一种可能的实现方式中，装置 900 可以用于实现上述图 3 所示的方法。例如，处理模块 901 用于实现 S301，发送模块 902 用于实现 S302。

在另一种可能的实现方式中，装置 900 还可以包括接收模块。该实现方式中的装置 900 可以用于实现上述图 4 所示的方法。例如，处理模块 901 用于实现 S409 和 S411，发送模块 902 用于实现 S402、S404、S406、S408、S412 和 S414，接收模块用于实现 S401、S403、S405、S407、S410 和 S413。

在又一种可能的实现方式中，装置 900 还可以包括接收模块。该实现方式中的装置 900 可以用于实现上述图 5 所示的方法。例如，处理模块 901 用于实现 S503 和 S505，发送模块 902 用于实现 S502 和 S506，接收模块用于实现 S501、S504 和 S507。

图 10 为本申请另一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图。如图 10 所示，装置 1000 可以包括处理模块 1001、发送模块 1002 和接收模块 1003。装置 1000 可以用于实现图 6 至图 8 中任意一个所示的实施例中由终端设备实现的操作。

在一种可能的实现方式中，装置 1000 可以用于实现上述图 6 所示的方法。例如，处理模块 1001 用于实现 S601 和 S602，发送模块 1002 用于实现 S603，接收模块 1003 用于实现 S604。

在另一种可能的实现方式中，装置 1000 可以用于实现上述图 7 所示的方法。例如，处理模块 1001 用于实现 S709，发送模块 1002 用于实现 S701、S703、S705、S707、S710、S712、S714、S716 和 S718，接收模块 1003 用于实现 S702、S704、S706、S708、S711、S713、S715、S717 和 S719。

在又一种可能的实现方式中，装置 1000 可以用于实现上述图 8 所示的方法。例如，处理模块 1001 用于实现 S801，发送模块 1002 用于实现 S802、S804、S806、S808 和 S810，接收模块 1003 用于实现 S803、S805、S807、S809 和 S811。

图 11 为本申请又一个实施例的一种配置 EPS NAS 安全算法的装置的示意性结构图。图 11 所示的装置 1100 可以用于执行图 3 至图 5 中任意一个所示的实施例中由接入和移动管理功能实体或 AMF 网元实现的方法或可以用于执行图 6 至图 8 中任意一个所示的实施例中由终端设备实现的方法。

如图 11 所示，本实施例的装置 1100 包括：存储器 1101、处理器 1102、通信接口 1103 以及总线 1104。其中，存储器 1101、处理器 1102、通信接口 1103 通过总线 1104 实现彼此之间的通信连接。

存储器 1101 可以是只读存储器（read only memory, ROM），静态存储设备，动态存储设备或者随机存取存储器（random access memory, RAM）。存储器 1101 可以存储程序，当存储器 1101 中存储的程序被处理器 1102 执行时，处理器 1102 可以用于执行图 3 至图 8 所示的方法的各个步骤。

处理器 1102 可以采用通用的中央处理器（central processing unit, CPU），微处理器，应用专用集成电路（application specific integrated circuit, ASIC），或者一个或多个集成电路，用于执行相关程序，以实现本申请方法实施例的配置 EPS NAS 安全算法的方法。

处理器 1102 还可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，

本申请各个实施例的方法的各个步骤可以通过处理器 1102 中的硬件的集成逻辑电路或者软件形式的指令完成。

上述处理器 1102 还可以是通用处理器、数字信号处理器(digital signal processing, DSP)、专用集成电路(ASIC)、现成可编程门阵列(field programmable gate array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成, 或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器, 闪存、只读存储器, 可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1101, 处理器 1102 读取存储器 1101 中的信息, 结合其硬件完成本申请实施例中各个方法所需执行的功能, 例如, 可以执行图 3 至图 8 所示实施例的各个步骤/功能。

通信接口 1103 可以使用但不限于收发器一类的收发装置, 来实现装置 1100 与其他设备或通信网络之间的通信。

总线 1104 可以包括在装置 1100 各个部件(例如, 存储器 1101、处理器 1102、通信接口 1103)之间传递信息的通路。

应理解, 本申请实施例所示的装置 1100 可以是电子设备, 或者, 也可以是配置于电子设备中的芯片。

应理解, 本申请实施例中的处理器可以为中央处理单元(central processing unit, CPU), 该处理器还可以是其他通用处理器、数字信号处理器(digital signal processor, DSP)、专用集成电路(application specific integrated circuit, ASIC)、现成可编程门阵列(field programmable gate array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

还应理解, 本申请实施例中的存储器可以是易失性存储器或非易失性存储器, 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。通过示例性但不是限制性说明, 许多形式的随机存取存储器(random access memory, RAM)可用, 例如静态随机存取存储器(static RAM, SRAM)、动态随机存取存储器(DRAM)、同步动态随机存取存储器(synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(synchlink DRAM, SLDRAM)和直接内存总线随机存取存储器(direct rambus RAM, DR RAM)。

上述实施例, 可以全部或部分地通过软件、硬件、固件或其他任意组合来实现。当使用软件实现时, 上述实施例可以全部或部分地以计算机程序产品的形式实现。所

述计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质。半导体介质可以是固态硬盘。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况，其中A、B可以是单数或者复数。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系，但也可能表示的是一种“和/或”的关系，具体可参考前后文进行理解。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a、b、或c中的至少一项(个)，可以表示：a、b、c、a-b、a-c、b-c、或a-b-c，其中a、b、c可以是单个，也可以是多个。

应理解，在本申请的各种实施例中，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，而不对本申请实施例的实施过程构成任何限定。

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。

5 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，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）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、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

10 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权利要求的保护范围为准。

权 利 要 求 书

1. 一种配置演进分组系统 EPS 非接入层 NAS 安全算法的方法，其特征在于，所述方法包括：

5 接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法；

所述接入和移动管理功能实体向所述终端设备提供所述所选的 EPS NAS 安全算法。

2. 根据权利要求 1 所述的方法，其特征在于，所述接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法之前，所述方法还包括：

10 所述接入和移动管理功能实体向所述终端设备发送第一消息，所述第一消息包括所述所选的 EPS NAS 安全算法的信元。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述接入和移动管理功能实体确定没有成功为终端设备提供所选的 EPS NAS 安全算法包括：

15 所述接入和移动管理功能实体确定未收到第一完成消息，所述第一完成消息用于表示所述终端设备已接收到所述第一消息。

4. 根据权利要求 3 所述的方法，其特征在于，所述接入和移动管理功能实体确定未收到第一完成消息包括：

所述接入和移动管理功能实体确定在预设时间内未收到所述第一完成消息。

20 5. 根据权利要求 3 或 4 所述的方法，其特征在于，所述第一消息为安全模式命令 SMC 消息，所述第一完成消息为 SMC 完成消息。

6. 根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述接入和移动管理功能实体向所述终端设备提供所述所选的 EPS NAS 安全算法包括：

所述接入和移动管理功能实体向所述终端设备发送所述所选的 EPS NAS 安全算法的信元。

25 7. 根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述方法还包括：所述接入和移动管理功能实体将所述所选的 EPS NAS 安全算法标记为无效。

8. 根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述接入和移动管理功能实体向所述终端设备提供所述所选的 EPS NAS 安全算法之前，所述方法还包括：所述接入和移动管理功能实体接收来自所述终端设备的注册请求消息。

30 9. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述接入和移动管理功能实体确定更新所选的 EPS NAS 安全算法；

所述接入和移动管理功能实体向所述终端设备提供更新后的所选的 EPS NAS 安全算法。

10. 根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

35 所述接入和移动管理功能实体确定没有成功为所述终端设备提供更新后的所选的 EPS NAS 安全算法；

所述接入和移动管理功能实体向所述终端设备提供所述更新后的所选的 EPS NAS 安全算法。

11. 根据权利要求 1 至 10 中任一项所述的方法，其特征在于，所述接入和移动管

理功能实体支持 N27 接口, 所述终端设备支持 S1 模式。

12. 根据权利要求 1 至 11 中任一项所述的方法, 其特征在于, 所述接入和移动管理功能实体中存在所述终端设备指示的有效第五代移动通信 5G NAS 安全上下文。

13. 一种配置演进分组系统 EPS 非接入层 NAS 安全算法的方法, 其特征在于, 5 所述方法包括:
终端设备确定不存在第五代移动通信 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法;

所述终端设备删除所述 5G NAS 安全上下文;

10 所述终端设备向接入和移动管理功能实体发送第二消息, 所述第二消息用于请求所述 5G 安全上下文;

所述终端设备接收来自所述接入和移动管理功能实体的所述所选的 EPS NAS 安全算法的信元。

14. 根据权利要求 13 所述的方法, 其特征在于, 所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法包括:

15 所述终端设备确定没有接收来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。

15. 根据权利要求 14 所述的方法, 其特征在于, 所述终端设备确定没有接收来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元包括:

20 所述终端设备在预设时间内没有接收到来自所述接入和移动管理功能实体的所选的 EPS NAS 安全算法的信元。

16. 根据权利要求 13 至 15 中任一项所述的方法, 其特征在于, 所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法之前, 所述方法还包括:

所述终端设备接收所述接入和移动管理功能实体发送的第三消息, 所述第三消息包括所述 5G NAS 安全上下文;

25 所述终端设备向所述接入和移动管理功能实体发送第三完成消息, 所述第三完成消息用于表示所述终端设备已接收到所述第三消息。

17. 根据权利要求 13 至 16 中任一项所述的方法, 其特征在于, 所述终端设备确定不存在 5G NAS 安全上下文对应的所选的 EPS NAS 安全算法包括:

确定下一代无线接入网密钥集标识 ngKSI 没有对应的所选的 EPS NAS 安全算法。

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

所述终端设备将所述 ngKSI 设为无效值。

19. 根据权利要求 17 或 18 所述的方法, 其特征在于, 所述终端设备与长期演进 LTE 系统断开连接, 所述第二消息用于请求注册至新无线 NR 系统。

35 20. 根据权利要求 19 所述的方法, 其特征在于, 所述终端设备确定所述接入和移动管理功能实体支持 N27 接口。

21. 根据权利要求 13 至 20 中任一项所述的方法, 其特征在于, 所述接入和移动管理功能实体支持 N27 接口, 所述终端设备支持 S1 模式。

22. 一种配置演进分组系统 EPS 非接入层 NAS 安全算法的装置, 其特征在于, 包括用于实现权利要求 1 至 12 中任一项所述的方法的各个功能模块。

23. 一种配置演进分组系统 EPS 非接入层 NAS 安全算法的装置，其特征在于，包括用于实现权利要求 13 至 21 中任一项所述的方法的各个功能模块。

24. 一种配置演进分组系统 EPS 非接入层 NAS 安全算法的装置，其特征在于，包括：存储器和处理器；

5 所述存储器用于存储程序指令；

 所述处理器用于调用所述存储器中的程序指令执行如权利要求 1 至 12 中任一项所述的方法或权利要求 13 至 21 中任一项所述的方法。

25. 一种芯片，其特征在于，包括至少一个处理器和通信接口，所述通信接口和所述至少一个处理器通过线路互联，所述至少一个处理器用于运行计算机程序或指令，
10 以执行如权利要求 1 至 12 中任一项所述的方法或权利要求 13 至 21 中任一项所述的方法。

26. 一种计算机可读介质，其特征在于，所述计算机可读介质存储用于计算机执行的程序代码，该程序代码包括用于执行如权利要求 1 至 12 中任一项所述的方法或权利要求 13 至 21 中任一项所述的方法的指令。

15 27. 一种计算机程序产品，其特征在于，所述计算机程序产品包括指令，当所述指令被执行时，使得计算机执行权利要求 1 至 12 中任一项所述的方法或权利要求 13 至 21 中任一项所述的方法。