

一种切片隔离方法、装置及系统

技术领域

本申请涉及无线通信技术领域，尤其涉及一种切片隔离方法、装置及系统。

5 背景技术

全球移动通信系统协会（global system for mobile communications association，GSMA）定义了通用切片模板的共用属性，简称切片的属性，切片的属性用于描述切片能否与其他切片同时使用，即描述用户设备是否可以同时使用多个切片。多个切片之间可能会共享一些网络资源，如果没有进行适当的隔离，会存在互相泄露信息的风险。

- 10 现有第三代合作伙伴项目（3rd generation partnership project，3GPP）标准中允许用户设备可以先后分时接入不同的切片，当用户设备先后接入不同的切片时，用户设备有可能会使用同一个访问和移动管理功能（access and mobility management function，AMF），也可能使用不同的AMF。因此用户设备可能在某一时刻接入了切片1，使用并完成了切片1上的业务后，用户设备退出了切片1和网络，之后用户设备可能又接入了切片2，此时用户设备和网络中可能保留并使用着切片1对应的安全上下文，此时切片2可能获取并使用当前保存的安全上下文，就导致切片1的相关信息被切片2获取到，切片1的信息存在泄漏的风险。

发明内容

- 20 本申请实施例提供一种切片隔离方法、装置及系统，用以避免切片间的信息泄露，保证切片间的控制信令和数据安全。

- 第一方面，提供一种切片隔离方法，包括第一网络设备获取用户设备的第一切片的信息；若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

- 25 所述第二密钥为所述用户设备接入所述第二切片时，用户设备和网络所使用的密钥。所述第二密钥用于对所述第二切片的信息和/或所述用户设备接入所述第二切片时的信息进行安全保护。一种可能的理解，所述第二密钥为所述第一网络设备（如AMF）的密钥，示例性的，所述第二密钥为所述用户设备接入所述第二切片时，所述第一网络设备的密钥。30 另一种可能的理解，所述第二密钥为针对所述第二切片的密钥，或所述第二密钥为所述第二切片的密钥。

可以理解，本申请实施例中涉及到的“信息”包括但不限于切片相关的控制信令和用户数据。

- 35 通过上述方法，所述第一网络设备可以在当前保存的第一切片的信息和请求接入的第二切片的信息不匹配时，重新获取所述第二密钥，保证所述第二切片的信息通过所述第二密钥进行保护，仅能利用所述第二密钥正确解密，避免了利用其他密钥也可获取所述第二切片的信息，保证切片间的信息安全。

在一种可能的设计中，所述第一切片的信息包括所述第一切片的属性，所述第二切片

的信息包括第二切片的属性；若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥，包括：

若所述第一切片的属性与所述第二切片的属性不匹配，则所述第一网络设备获取所述第二密钥。

5 切片的属性可以用来描述该切片是否能够与其他切片共用，因此在切片的属性不匹配时，确定第一切片和第二切片不能被用户设备共用，从而将所述用户设备接入第一切片时所使用的密钥和所述用户设备接入第二切片时所使用的密钥进行区分，避免切片间的信息泄露。

在一种可能的设计中，所述第一网络设备获取第二密钥，包括：

10 所述第一网络设备根据第一密钥生成所述第二密钥，其中，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。

所述第一密钥为所述用户设备接入所述第一切片时，用户设备和网络所使用的密钥。所述第一密钥用于对所述切片的信息和/或所述用户设备接入所述第一切片时的信息进行安全保护。一种可能的理解，所述第一密钥为所述第一网络设备的密钥，示例性的，所述
15 第一密钥为所述用户设备接入所述第一切片时，所述第一网络设备的密钥。另一种可能的理解，所述第一密钥为针对所述第一切片的密钥，或所述第一密钥为所述第一切片的密钥。

在该设计中，根据所述第一密钥生成第二密钥，不仅可以保证切片间的信息安全，还可以减少用户设备与网络设备之间交互的数据量。

在一种可能的设计中，所述第一网络设备根据所述第一密钥生成所述第二密钥，包括：

20 若所述第一切片的隔离要求高于所述第二切片的隔离要求，所述第一网络设备根据所述第一密钥生成所述第二密钥。

根据切片隔离要求的不同，在之前接入的切片的隔离要求高于本次欲接入的切片的隔离要求，基于当前保存的密钥生成新的密钥，在保证切片间的信息安全的基础上，减少用户设备与网络设备之间交互的数据量。

25 在一种可能的设计中，所述第一网络设备获取第二密钥，包括：

所述第一网络设备对所述用户设备重新进行认证；

若第一网络设备对所述用户设备重新认证成功，则所述第一网络设备生成或者接收所述第二密钥。

所述第一网络设备通过对用户设备重新进行网络认证，从而可以保证切片间的信息安全。所述第二密钥可以由所述第一网络设备生成，也可以由其他网络设备生成。若所述第二密钥由其他网络设备生成，所述第一网络设备可以在所述其他网络设备中获取所述第二密钥，即所述第一网络设备接收来自所述其他网络设备的所述第二密钥。
30

在一种可能的设计中，所述第一网络设备对所述用户设备重新进行认证，包括：

35 若所述第一切片的隔离要求低于所述第二切片的隔离要求，所述第一网络设备对所述用户设备重新进行网络认证。

根据切片隔离要求的不同，在之前接入的切片的隔离要求低于本次欲接入的切片的隔离要求，重新进行网络认证再生成新的密钥，可以进一步提高切片间信息的安全。

在一种可能的设计中，所述第一切片的属性与所述第二切片的属性不匹配，包括：

所述第一切片的属性或第二切片的属性不允许与其他任意属性的切片共用；或者

40 所述第一切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第二切片的属性

的 SST 与所述第一切片的属性的 SST 不同；或者

所述第二切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第一切片的属性的 SST 与所述第二切片的属性的 SST 不同；或者

5 所述第一切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 不同；或者

所述第二切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 不同。

在一种可能的设计中，若所述第一切片的属性与所述第二切片的属性匹配，所述第一网络设备还可以向所述用户设备发送注册接受消息。

10 在所述第一切片的属性和所述第二切片的属性相匹配时，所述第一网络设备可以和所述用户设备继续完成注册过程。

在一种可能的设计中，所述第一切片的属性与所述第二切片的属性匹配，包括：

所述第一切片的属性或第二切片的属性允许与其他任意属性的切片共用；或者

15 所述第一切片的属性仅允许具有相同 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

所述第二切片的属性仅允许具有相同 SST 的切片共用，所述第一切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

所述第一切片的属性仅允许具有相同 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 相同；或者

20 所述第二切片的属性仅允许具有相同 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 相同；或者

所述第二切片和所述第一切片映射到同一单网络切片选择辅助信息 S-NSSAI。

在一种可能的设计中，所述第一切片的属性与所述第二切片的属性不匹配，包括所有不满足上述属性匹配的情况。

25 第二方面，提供一种切片隔离方法，包括用户设备向第一网络设备发送第一请求消息，所述第一请求消息用于请求接入第二切片；所述用户设备接收来自所述第一网络设备的第一指示消息，所述第一指示消息用于指示所述用户设备获取第二密钥；所述用户设备获取所述第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

30 通过上述方法，所述第一网络设备可以在当前保存的第一切片的信息和请求接入的第二切片的信息不匹配时，重新获取所述第二密钥，保证所述第二切片的信息通过所述第二密钥进行保护，仅能利用所述第二密钥正确解密，避免了利用其他密钥也可获取所述第二切片的信息，保证切片间的信息安全。

在一种可能的设计中，所述用户设备获取所述第二密钥，包括：

35 所述用户设备获取第一密钥，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护；

所述用户设备根据所述第一密钥生成所述第二密钥。

根据所述第一密钥生成第二密钥，不仅可以保证切片间的信息安全，还可以减少用户设备与网络设备之间交互的数据量。

40 在一种可能的设计中，所述用户设备获取所述第二密钥，包括：

所述用户设备与所述第一网络设备重新进行认证;

若所述用户设备与所述第一网络设备重新认证成功,则所述用户设备生成或接收所述第二密钥。

所述第一网络设备通过对用户设备重新进行网络认证,从而可以保证切片间的数据安全。所述第二密钥可以由所述用户设备生成,也可以由网络设备(如所述第一网络设备)生成。若所述第二密钥由网络设备生成,所述用户设备可以在所述网络设备中获取所述第二密钥,即所述用户设备接收来自所述网络设备的所述第二密钥。

在一种可能的设计中,所述用户设备还可以接收来自所述第一网络设备的注册接受消息。在所述第一切片的属性和所述第二切片的属性相匹配时,所述第一网络设备可以和所述用户设备继续完成注册过程。

第三方面,提供一种切片隔离方法,包括第一网络设备接收去注册请求消息,或者发送去注册请求消息,所述第一网络设备删除所述用户设备的第三密钥,所述第三密钥用于对第三切片的信息或/和所述用户设备接入所述第三切片时的信息进行安全保护,所述第三切片为所述用户设备最后接入的切片。

所述第三密钥为所述用户设备接入所述第三切片时,用户设备和网络所使用的密钥。所述第三密钥用于对所述第三切片的信息和/或所述用户设备接入所述第三切片时的信息进行安全保护。一种可能的理解,所述第三密钥为所述第一网络设备的密钥,示例性的,所述第三密钥为所述用户设备接入所述第三切片时,所述第一网络设备的密钥。另一种可能的理解,所述第三密钥为针对所述第三切片的密钥,或所述第三密钥为所述第三切片的密钥。

通过上述方法,第一网络设备删除去注册的用户设备的第三密钥,而为后续接入的切片重新生成密钥,从而避免切片间的信息泄露。

在一种可能的设计中,所述第一网络设备删除所述用户设备的第三密钥,包括:若所述第一网络设备确定所述第三切片属性不允许与任意属性切片共用,所述第一网络设备删除所述用户设备的第三密钥。通过对隔离要求高的专属切片删除密钥,避免后续接入的切片使用该专属密钥,从而保证切片间的数据安全。

在一种可能的设计中,若所述第一网络设备确定所述第三切片属性允许与其他属性切片共用,所述第一网络设备还可以向所述用户设备发送去注册接受消息。

在一种可能的设计中,若所述第一网络设备未获取到所述第三切片的切片属性,所述第一网络设备还可以向用户设备发送去注册接受消息。

第四方面,提供一种切片隔离方法,包括用户设备发送去注册请求消息,或者接收去注册请求消息,所述用户设备删除所述用户设备的第三密钥,所述第三切片为所述用户设备最后接入的切片,所述第三密钥用于对所述第三切片的信息或/和所述用户设备接入所述第三切片时的信息进行安全保护。通过上述方法,用户设备删除去注册的用户设备的第三密钥,而为后续接入的切片重新生成密钥,从而避免切片间的信息泄露。

在一种可能的设计中,所述用户设备删除所述用户设备的第三密钥,包括:若所述用户设备确定所述第三切片属性不允许与任意属性切片共用,所述用户设备删除所述用户设备的第三密钥。通过对隔离要求高的专属切片删除密钥,避免后续接入的切片使用该专属密钥,从而保证切片间的信息安全。

第五方面,提供一种切片隔离方法,包括:第二网络设备接收来自第一网络设备的重

定向信息,所述重定向信息包括用户设备的第四切片的信息和/或所述用户设备请求接入的第五切片的信息;

若所述第四切片的信息与所述第五切片的信息不匹配,且所述第五切片具有隔离要求,则所述第二网络设备对所述用户设备重新认证。

5 在请求接入的切片具有隔离要求时,第二网络设备对用户设备进行重新认证,生成新的密钥,避免了所述用户设备接入所述第四切片和所述用户设备接入所述第五切片时使用同一密钥造成的信息泄露,保证切片间的信息安全。

10 在一种可能的设计中,若所述第四切片的信息与所述第五切片的信息不匹配,且所述第五切片允许与其他任意属性切片共用,则所述第二网络设备继续对所述用户设备进行认证。

第六方面,提供一种通信装置,该装置具有实现上述任意方面或任意方面中的实现方法的功能。该功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

15 第七方面,提供一种通信装置,包括:处理器和存储器;该存储器用于存储计算机执行指令,当该装置运行时,该处理器执行该存储器存储的该计算机执行指令,以使该装置执行如上述任意方面或任意方面中的实现方法。

第八方面,提供一种通信装置,包括:包括用于执行以上任意方面各个步骤的单元或手段(means)。

20 第九方面,提供一种通信装置,包括处理器和接口电路,所述处理器用于通过接口电路与其它装置通信,并执行以上任意方面提供的任意方法。该处理器包括一个或多个。

第十方面,提供一种通信装置,包括处理器,用于与存储器相连,用于调用所述存储器中存储的程序,以执行上述任意方面的任意实现方式中的方法。该存储器可以位于该装置之内,也可以位于该装置之外。且该处理器包括一个或多个。

25 第十一方面,提供一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得处理器执行上述任意方面所述的方法。

第十二方面,提供一种包括指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述任意方面所述的方法。

第十三方面,提供一种芯片系统,包括:处理器,用于执行上述各方面所述的方法。

30 第十四方面,提供一种通信系统,包括用于执行上述第一方面或第一方面任一实现方法的第一网络设备、用于执行上述第二方面或第二方面任一实现方法的第二方面任一实现方法的用户设备。

第十五方面,提供一种通信系统,包括用于执行上述第三方面或第三方面任一实现方法的第一网络设备、用于执行上述第四方面或第四方面任一实现方法的用户设备。

35 第十六方面,提供一种通信系统,包括第一网络设备、用于执行上述第五方面或第五方面任一实现方法的第二网络设备及用户设备。

第十七方面,提供一种芯片系统,该芯片系统包括收发器用于实现上述任一方面的方法中网络设备或用户设备的功能,例如,例如接收或发送上述方法中所涉及的数据和/或信息。在一种可能的设计中,所述芯片系统还包括存储器,所述存储器,用于保存程序指令和/或数据。该芯片系统,可以由芯片构成,也可以包括芯片和其他分立器件。

40 上述第六方面至第十七方面中任一方面及其任一方面中任意一种可能的实现可以达

到的技术效果，请参照上述任意方面可以带来的技术效果描述，这里不再重复赘述。

附图说明

图 1 为本申请实施例的一种可能的网络架构示意图；

5 图 2A、图 2B 为一种切片接入场景示意图；

图 3、图 4、图 5、图 6、图 7、图 8、图 9、图 10 为本申请实施例的一种切片隔离流程示意图；

图 11、图 12 为本申请实施例的一种通信装置示意图。

10 具体实施方式

下面将结合附图对本申请作进一步地详细描述。

本申请将围绕可包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所有设备、组件、模块等。此外，还可以使用这些方案的组合。

15 另外，在本申请实施例中，“示例的”一词用于表示作例子、例证或说明。本申请中被描述为“示例”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用示例的一词旨在以具体方式呈现概念。

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制，本领域普通技术人员可知，
20 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。

以下对本申请实施例的部分用语进行解释说明，以便于本领域技术人员理解。

1) 用户设备 (user equipment, UE)，也称终端设备，是一种具有无线收发功能的设备，
25 可以经无线接入网 (radio access network, RAN) 中的接入网设备 (或者也可以称为接入设备) 与一个或多个核心网 (core network, CN) 设备 (或者也可以称为核心设备) 进行通信。

用户设备也可称为接入终端、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、用户代理或用户装置等。用户设备可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上 (如轮船等)；还可以部署在空中 (例如飞机、气球和卫星上等)。用户设备可以是蜂窝电话 (cellular phone)、无绳电话、会话启动协议 (session initiation protocol, SIP) 电话、智能电话 (smart phone)、手机 (mobile phone)、无线本地环路 (wireless local loop, WLL) 站、个人数字处理 (personal digital assistant, PDA) 等。或者，用户设备还可以是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设备、车载设备、可穿戴设备、无人机设备或物联网、车联网中的终端、
35 第五代移动通信 (5th-generation, 5G) 网络以及未来网络中的任意形态的终端、中继用户设备或者未来演进的 PLMN 中的终端等。其中，中继用户设备例如可以是 5G 家庭网关 (residential gateway, RG)。例如用户设备可以是虚拟现实 (virtual reality, VR) 终端、增强现实 (augmented reality, AR) 终端、工业控制 (industrial control) 中的无线终端、无人驾驶 (self driving) 中的无线终端、远程医疗 (remote medical) 中的无线终端、智能电

网 (smart grid) 中的无线终端、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) 中的无线终端等。本申请实施例对终端设备的类型或种类等并不限定。

2) 网络设备, 指可以为终端提供无线接入功能的设备。其中, 网络设备可以支持至少一种无线通信技术, 例如长期演进 (long term evolution, LTE)、新无线 (new radio, NR)、宽带码分多址 (wideband code division multiple access, WCDMA) 等。

例如网络设备可以包括接入网设备。示例的, 网络设备包括但不限于: 5G 网络中的下一代基站或下一代节点 B (generation nodeB, gNB)、演进型节点 B (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 (例如, home evolved node B、或 home node B, HNB)、基带单元 (baseband unit, BBU)、收发点 (transmitting and receiving point, TRP)、发射点 (transmitting point, TP)、移动交换中心、小站、微型站等。网络设备还可以是云无线接入网络 (cloud radio access network, CRAN) 场景下的无线控制器、集中单元 (centralized unit, CU)、和/或分布单元 (distributed unit, DU), 或者网络设备可以为中继站、接入点、车载设备、终端、可穿戴设备以及未来移动通信中的网络设备或者未来演进的公共移动陆地网络 (public land mobile network, PLMN) 中的网络设备等。

又如, 网络设备可以包括核心网 (CN) 设备, 核心网设备例如包括 AMF 等。

本申请中的“和/或”, 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。字符“/”一般表示前后关联对象是一种“或”的关系。

本申请中所涉及的多个, 是指两个或两个以上。

另外, 需要理解的是, 在本申请的描述中, “第一”、“第二”等词汇, 仅用于区分描述的目的, 而不能理解为指示或暗示相对重要性, 也不能理解为指示或暗示顺序。

本申请实施例的技术方案可以应用于各种通信系统。一个通信系统中, 由运营者运营的部分可称为公共陆地移动网络 (public land mobile network, PLMN) (也可以称为运营商网络等)。PLMN 是由政府或其所批准的经营者, 为公众提供陆地移动通信业务目的而建立和经营的网络, 主要是移动网络运营商 (mobile network operator, MNO) 为用户提供移动宽带接入服务的公共网络。本申请实施例中所描述的 PLMN, 具体可为符合 3GPP 标准要求的网络, 简称 3GPP 网络。3GPP 网络通常包括但不限于 5G、第四代移动通信 (4th-generation, 4G) 网络等。为了方便描述, 本申请实施例中将 PLMN 为例进行说明。或者, 本申请实施例提供的技术方案还可以应用于 LTE 系统、LTE 频分双工 (frequency division duplex, FDD) 系统、LTE 时分双工 (time division duplex, TDD)、通用移动通信系统 (universal mobile telecommunication system, UMTS)、全球互联微波接入 (worldwide interoperability for microwave access, WiMAX) 通信系统、5G 通信系统或 NR 以及未来的其他通信系统如 6G 等。

随着移动带宽接入服务的扩展, 移动网络也会随之发展以便更好地支持多样化的商业模式, 满足更加多样化的应用业务以及更多行业的需求。为了给更多的行业提供更好、更完善的服务, 5G 网络相对于 4G 网络也做了网络架构调整。例如, 5G 网络将 4G 网络中的

移动管理实体 (mobility management entity, MME) 进行拆分, 拆分为包括 AMF 和会话管理功能 (session management function, SMF) 等多个网络功能。

为了便于理解本申请实施例, 以图 1 所示的 5G 网络架构为例对本申请使用的应用场景进行说明。图 1 为 3GPP 标准化过程中定义的非漫游场景下基于服务化架构的 5G 网络架构。所述网络架构中可以包括: 终端设备 (也可以称为用户设备) 部分、PLMN 部分和数据网络 (data network, DN) 部分。

PLMN 可以包括: 网络开放功能 (network exposure function, NEF) 131、网络存储功能 (network function repository function, NRF) 132、策略控制功能 (policy control function, PCF) 133、统一数据管理功能 (unified data management, UDM) 134、认证服务器功能 (authentication server function, AUSF) 136、AMF 137、会话管理功能 (session management function, SMF) 138、用户面功能 (user plane function, UPF) 139、接入网 (access network, AN) 140、网络切片选择功能 (network slice selection function, NSSF) 141、网络切片认证授权功能 (network slice specific authentication and authorization function, NSSAAF) 142 等。上述 PLMN 中, 除接入网 140 部分之外的部分可以称为核心网部分。

数据网络 DN 120, 也可以称为分组数据网络 (packet data network, PDN), 通常可以部署在 PLMN 之外, 例如第三方网络。示例性的, PLMN 可以接入多个数据网络 DN 120, 数据网络 DN 120 上可部署多种业务, 从而为终端设备 110 提供数据和/或语音等服务。例如, 数据网络 DN 120 可以是某智能工厂的私有网络, 智能工厂安装在车间的传感器可为终端设备 110, 数据网络 DN 120 中部署了传感器的控制服务器, 控制服务器可为传感器提供服务。传感器可与控制服务器通信, 获取控制服务器的指令, 根据指令将采集的传感器数据传送给控制服务器等。又例如, 数据网络 DN 120 可以是某公司的内部办公网络, 该公司员工的手机或者电脑可为终端设备 110, 员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。终端设备 110 可通过 PLMN 提供的接口 (例如图 1 中的 N1 接口等) 与 PLMN 建立连接, 使用 PLMN 提供的数据和/或语音等服务。终端设备 110 还可通过 PLMN 访问数据网络 DN 120, 使用数据网络 DN 120 上部署的运营商业务, 和/或第三方提供的业务。其中, 上述第三方可为 PLMN 和终端设备 110 之外的服务方, 可为终端设备 110 提供其他数据和/或语音等服务。其中, 上述第三方的具体表现形式, 具体可根据实际应用场景确定, 在此不做限制。

应用功能 (application function, AF) 135 可以隶属于 PLMN, 也可以不隶属于 PLMN。不过通常情况下, AF 隶属于第三方而不属于 PLMN, 但同 PLMN 有协议关系。AF 用于支持通过应用来影响数据路由的功能以及接入网络开放功能 NEF、与策略框架交互进行策略控制等。

示例性的, 下面对 PLMN 中的网络功能进行简要介绍。

AN 140, 也称无线 (Radio) AN, 是 PLMN 的子网络, 是 PLMN 中业务节点 (或网络功能) 与终端设备 110 之间的实施系统。终端设备 110 要接入 PLMN, 首先是经过 AN 140, 进而通过 AN 140 与 PLMN 中的业务节点连接。本申请实施例中的 AN 140, 可以指代接入网本身, 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 110 提供无线通信功能的设备, 也可以称为接入设备、(R) AN 设备或网络设备等。该接入网设备包括但不限于: 5G 系统中的 gNB、LTE 系统中的 eNB、RNC、NB、基站控制器 BSC、BTS、HNB、BBU、TRP、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。

5 可选的,在接入设备的一些部署中,接入设备可以包括 CU 和 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, O-RAN 或 Open RAN)架构等,本申请对于接入设备的具体部署方式不作限定。

网络开放功能 NEF(也可以称为网络开放功能实体)131 是由运营商提供的控制面功能。网络开放功能 NEF 131 以安全的方式对第三方开放网络的能力的对外双向接口。在其他网络功能(如应用功能 AF135 等)需要与第三方的网络通信时,NEF 网络功能 131 可作为与第三方的网络实体进行通信的中继。NEF 网络功能 131 还可作为签约用户的标识信息的翻译,以及第三方的网络功能的标识信息的翻译。比如,NEF 网络功能 131 将签约用户的用户永久标识符(subscriber permanent identifier, SUPI)从 PLMN 发送到第三方时,可以将 SUPI 翻译成其对应的外部公开使用的签约标识(generic public subscription identifier, GPSI)。反之,NEF 网络功能 131 将外部信息转发发送到 PLMN 网络,防止 PLMN 内部的其他网络功能与外部直接接触。

网络存储功能 NRF 132,是由运营商提供的控制面功能,可用于维护网络中所有网络功能服务的实时信息。

策略控制功能 PCF 133 是由运营商提供的控制面功能,它支持统一的策略框架来治理网络行为、向其他控制功能提供策略规则、策略决策相关的签约信息等。

20 统一数据管理 UDM 134 是由运营商提供的控制面功能,负责存储 PLMN 中签约用户的 SUPI、安全上下文(security context)、签约数据等信息。上述 PLMN 的签约用户具体可为使用 PLMN 提供的业务的用户,例如使用中国电信的终端设备芯卡的用户,或者使用中国移动的终端设备芯卡的用户等。示例性的,签约用户的 SUPI 可为终端设备芯卡的号码等。上述安全上下文可以为存储在本地终端设备(例如手机)上的数据(cookie)或者令牌(token)等。上述签约用户的签约数据可以为该终端设备芯卡的配套业务,例如该手机芯卡的流量套餐等。

认证服务器功能 AUSF 136 是由运营商提供的控制面功能,通常用于一级认证,即终端设备 110(签约用户)与 PLMN 之间的网络认证。

30 接入与移动性管理功能 AMF 137 是由 PLMN 提供的控制面网络功能,负责终端设备 110 接入 PLMN 的接入控制和移动性管理,例如包括移动状态管理,分配用户临时身份标识,认证和授权用户等功能。

会话管理功能 SMF 138 是由 PLMN 提供的控制面网络功能,负责管理终端设备 110 的协议数据单元(protocol data unit, PDU)会话。PDU 会话是一个用于传输 PDU 的通道,终端设备需要通过 PDU 会话与 DN 120 互相传输数据。PDU 会话可以由 SMF 138 负责建立、维护和删除等。SMF 138 包括会话管理(如会话建立、修改和释放,包含 UPF 139 和 AN 140 之间的隧道维护等)、UPF 139 的选择和控制、业务和会话连续性(service and session continuity, SSC)模式选择、漫游等会话相关的功能。

40 用户面功能 UPF 139 是由运营商提供的网关,是 PLMN 与 DN 120 通信的网关。UPF 139 包括数据包路由和传输、包检测、业务用量上报、服务质量(quality of service, QoS)处

理、合法监听、上行包检测、下行数据包存储等用户面相关的功能。

网络切片选择功能（network slice selection function, NSSF）141，是由 PLMN 提供的控制面网络功能，用于负责确定网络切片实例，选择 AMF 网络功能 137 等。

网络切片认证授权功能（network slice specific authentication and authorization function, NSSAAF）142，是由 PLMN 提供的控制面网络功能，用于支持终端设备 110 与 DN 进行的切片认证。

图 1 所示的 PLMN 中的网络功能还可以包括统一数据存储（unified data repository, UDR）等（图中未示出），本申请实施例对于 PLMN 中包括的其他网络功能不作限定。

图 1 中 Nnef、Nausf、Nnrf、Npcf、Nudm、Naf、Namf、Nsmf、Nnssf、Nnssaaf、N1、N2、N3、N4，以及 N6 为接口序列号。示例性的，上述接口序列号的含义可参见 3GPP 标准协议中定义的含义，本申请对于上述接口序列号的含义不做限制。需要说明的是，图 1 中仅以终端设备 110 为 UE 作出了示例性说明，图 1 中的各个网络功能之间的接口名称也仅仅是一个示例，在具体实现中，该系统架构的接口名称还可能为其他名称，本申请对此不作限定。

本申请中的移动性管理网络功能可以是图 1 所示的 AMF 137，也可以是未来通信系统中的具有上述接入与移动性管理功能 AMF 137 的其他网络功能。或者，本申请中的移动性管理网络功能还可以是 LTE 系统中的移动管理实体（mobility management entity, MME）等。

为方便说明，本申请实施例中将接入与移动性管理功能 AMF 137 简称为 AMF，将统一数据管理 UDM 134 简称为 UDM，将终端设备 110 称为用户设备或 UE，即本申请实施例中后文所描述的 AMF 均可替换为移动性管理网络功能，UDM 均可替换为统一数据管理，用户设备或 UE 均可替换为终端设备。可理解，其他未示出的网络功能同样适用该替换方法。

图 1 中示出的网络架构（例如 5G 网络架构）采用基于服务的架构和通用接口，传统网元功能基于网络功能虚拟化（network function virtualization, NFV）技术拆分成若干个自包含、自管理、可重用的网络功能服务模块，通过灵活定义服务模块集合，可以实现定制化的网络功能重构，对外通过统一的服务调用接口组成业务流程。图 1 中示出的网络架构示意图可以理解作为一种非漫游场景下基于服务的 5G 网络架构示意图。在该架构中，根据特定场景需求，将不同网络功能按需有序组合，可以实现网络的能力与服务的定制化，从而为不同业务部署专用网络，实现 5G 网络切片（network slicing）。网络切片技术可以使运营商能够更加灵活、快速地响应客户需求，支持网络资源的灵活分配。

下面先对网络设备中的切片进行说明。

切片（slice）即网络切片，简单理解就是将运营商的物理网络切割成多个虚拟的端到端的网络，每个虚拟网络之间（包括网络内的设备、接入网、传输网和核心网）是逻辑独立的，任何一个虚拟网络发生故障都不会影响到其它虚拟网络。为了满足多样性需求和切片间的隔离，需要业务间相对独立的管理和运维，并提供量身定做的业务功能和分析能力。不同业务类型的实例可以部署在不同的网络切片上，相同业务类型的不同实例也可部署在不同的网络切片上。切片可以由一组网络功能（network function, NF）和/或子网络等构成。比如，图 1 中的子网络 AN 140、AMF 137、SMF 138、UPF 139 可以组成一个切片。可理

解，图 1 中的每种网络功能只示意性地画出了一个，而在实际网络部署中，每种网络功能或子网络可以有多个、数十个或上百个。PLMN 中可以部署很多切片，每个切片可以有不同的性能来满足不同应用、不同垂直行业的需求。运营商可以根据不同垂直行业客户的需求，“量身定做”一个切片。运营商也可以允许一些行业客户享有较大的自主权，参与切片的部分管理、控制功能。其中，切片级的认证就是由行业客户有限参与的一种网络控制功能，即对终端设备接入切片进行认证和授权，即“切片级认证”，也可称为“二级认证”、“二次认证”等，本申请简称为“切片认证”。

终端设备在被允许接入网络或切片之前，需要与网络和/或切片进行双向认证并得到该网络和/或切片的授权。一般的，网络需要对终端设备经过一次或者两次的认证与授权才能接入网络或切片。首先，PLMN 要基于终端设备所使用的与 PLMN 签约的 SUPI 进行认证，这种认证被称为一级认证（primary authentication）。其次，PLMN 要基于终端设备所使用的与 DN 的签约标识进行认证，即切片认证或二级认证等。

如以图 1 为例，当核心网中部署了切片，UE 110 需要接入到某个切片时，UE 110 可以提供请求的切片给核心网。其中，UE 110 请求的切片可以包括请求的网络切片选择辅助信息集合（requested network slice selection assistance information, requested NSSAI）。该 NSSAI 可以包括一个或多个单网络切片选择辅助信息（single network slice selection assistance information, S-NSSAI），一个 S-NSSAI 用于标识一个网络切片类型，也可以理解为，S-NSSAI 用于标识切片，或者可以理解为 S-NSSAI 是切片的标识信息。可理解，本申请中切片还可以称为网络切片、网络切片实例或 S-NSSAI 等，本申请对于该切片的名称不作限定。为方便理解，在后文的描述中，本申请对切片或 S-NSSAI 等不做严格区分，二者可以同样适用。

在 3GPP 标准中，S-NSSAI 的格式至少包括两个部分：

1、切片类型或业务类型（slice/service type, SST）。

SST 用来区分切片在特征、业务等方面的所预期的不同特性；目前，3GPP 标准定义了 4 种切片标准类型，即增强的移动宽带（enhanced mobile broadband, eMBB）、高可靠超低时延通信（ultra-reliable low-latency communication, URLLC）、大规模物联网（massive internet of things, MIoT）、车联网（vehicle to everything, V2X）。

2、切片差异化因素（slice differentiator, SD）。

SD 指的是细分的可选特征，用于进一步区别不同的切片。

SST 和 SD 都可以有非标准化的、PLMN 自定义的类型。

进一步的，UE 110 向网络发送注册请求后，核心网网络功能（如 AMF 网络功能或 NSSF 网络功能）根据 UE 110 的签约数据、UE 110 请求的网络切片、漫游协议以及本地配置等信息，为 UE 110 选择允许接入的网络切片集合。其中，允许接入的网络切片集合可以用允许的（allowed）NSSAI 来表示，允许的 NSSAI 中包括的 S-NSSAI 可以为当前 PLMN 允许该 UE 110 接入的 S-NSSAI。

举例说明一级认证和二级认证，示例性的，随着垂直行业和物联网的发展，PLMN 之外的数据网络 DN 120（如服务于垂直行业的 DN），对于接入到该 DN 120 的 UE 110 同样有认证与授权的需求。比如，某商业公司提供了游戏平台，通过 PLMN 为游戏玩家提供游戏服务。一方面，由于玩家使用的 UE 110 是通过 PLMN 接入游戏平台，因此 PLMN 需要对该 UE 110 的身份（SUPI）进行认证或授权等，即一级认证。游戏玩家是商业公司的客

户，该商业公司也需要对游戏玩家的身份进行认证或授权。如对游戏玩家的身份进行认证或授权，这种认证可以是基于切片的认证，或者说认证是以切片为单位。该情况下，这种认证可以被称为切片认证（slice authentication），或称为基于网络切片的认证（network slice-specific authentication and authorization, NSSAA）。需要说明的是，切片认证的实际含义如可以是：终端设备与第三方网络（如 DN 或其认证服务器）之间执行的认证。切片认证结果将会决定 PLMN 是否授权终端设备接入该 PLMN 提供的切片。还应理解，本申请中应用于切片认证的方法也同样适用于基于会话的二次认证（secondary authentication）或基于切片的二次认证等场景，在此不再详述。

下面对通用切片模板（generic network slice template, GST）进行说明。

GSMA 定义了 GST 的概念，GST 的主要作用是制定一套标准的网络切片模板，以便运营商在保证互联互通基础上，按需裁剪所需建立、使用、运营的网络切片，既方便互联互通、又提高效率及安全性。3GPP 标准组织针对该通用切片模板，正在制定相关标准，以便 5G 网络可以通过演进系统架构、流程，更好的支持并满足通用切片模板所规定的对切片特性、切片性能的要求。

GSMA 目前定义了通用切片模板的许多属性（GST Attributes，或简称 GST 属性），其中的一种 GST 属性是本申请实施例所关心的，也是 3GPP 标准组织中正在研究制定相关标准的 GST 属性。这类 GST 属性称为共用属性，或可被同时使用的网络切片（simultaneous use of the network slice），也可称为专属属性、互斥属性等。该属性主要描述该切片是否能与其他切片同时使用。在本申请实施例中所涉及的切片的属性，也称切片属性，指 GST 属性，包括共用属性。因为网络通常会同时部署各种类型、各种属性的切片，而 UE 是否可以同时使用多个切片是在通信过程中需要考虑的安全问题，因此该共用属性的实质也可以看作是切片间的隔离问题。

多个切片之间有可能会共享一些网络资源以提高网络资源的使用效率。这些网络资源如网元或 NF 等，如果没有进行适当的隔离，会存在互相泄露信息的风险。这个问题对于拥有较高敏感性的数据、或对网络安全隐私要求比较高的用户/行业比较重要，通常希望其切片能够做到不同时与其他切片被 UE 使用，以防止切片间信息泄露。相反，对于一些普通业务数据，现有网络切片所提供的安全性足以满足需求，而不需要额外增加安全机制、费用，来增强切片间的隔离。

GSMA 对 GST 共用属性还进一步给出了属性细分的建议。例如在本申请实施例中，共用属性可以存在以下划分：

- 共用属性取值为 0 时：可以与其他任意切片共用（简称“普通切片”）；
- 共用属性取值为 1 时：仅可与具有相同 SST 类型的切片共用（简称“1 型切片”）；
- 共用属性取值为 2 时：仅可与具有相同 SD 的切片共用（简称“2 型切片”）；
- 共用属性取值为 3 时：不允许与其他任意切片共用（简称“专属切片”）；
- 共用属性取值为 4-15 时：运营商自定义（简称“自定义切片”）。

需要说明的是，本申请实施例主要针对 GST 属性中的共用属性为例来进行描述。为了方便起见，下述描述中并不严格区分“属性”和“共用属性”，他们可以互换。

本申请实施例主要研究切片间资源共享和安全隔离的问题，对于上述 GST 属性的具体划分不作限制。现有 3GPP 标准中存在以下切片的接入规则：

规则 1: 允许 UE 同时接入多个切片: UE 在同一个 PLMN 中, 可以同时接入至多 8 个切片。当 UE 接入同一个 PLMN 中的 2-8 个切片时, 这些切片需要共享同一个 AMF。

规则 2: 允许 UE 可以先后 (分时) 接入不同切片: 当 UE 先后接入不同的切片时, UE 有可能会使用同一个 AMF, 也可能使用不同的 AMF, 取决于许多因素, 如 UE 的运动位置、AMF 的负载程度等等。

对于“专属切片”而言, 现有 3GPP 标准不定义统一的专属切片隔离方法, 而是留给运营商在部署切片时, 进行自定义, 自行考虑实现。例如, 一种简单的方法是, 对于部署专属切片的情况, 运营商可以采用私有策略, 禁止 UE 接入多切片。当然, 这种方法是牺牲了网络切片原有的灵活部署及 UE 的便利性。

目前 3GPP 正在研究制定的标准中, 正在探讨如何通过对网络、对 UE 进行配置, 从而网络进行自动化的判断、避免出现一个 UE 同时接入专属切片 (GST 公用属性值=3) 和其他切片 (任意公用属性值) 的情况, 或如何做到完全符合 GST 共用属性的限定要求。

GST 专用切片属性的核心安全问题是保证切片间的安全隔离。

实际通信场景中, 存在 UE 同时接入多个切片的场景 (上述规则 1), 也存在先后 (非同时) 接入多个切片的场景 (上述规则 2)。在现有 3GPP 仅针对上述规则 1 所述的场景进行讨论, 而实际上述规则 2 所述的场景也需要保证切片间的安全隔离。

下面对上述规则 2 所述的场景可能存在的切片间信息泄露问题进行简单描述。需要说明的是, 切片间的信息可以包括切片间的控制信令、用户数据等。以下述 2 个典型的场景为例。

场景 A: 共享 AMF: UE 先后接入不同 (或相同) 的切片。

例如, UE 在某一个时刻接入了切片 1, 使用并完成了切片 1 上的业务后, UE 退出了切片 1 和网络, 完成了与网络间的去注册 (de-registration) 流程。一段时间之后, UE 需要使用切片 2 的业务, 通过所述网络又接入了切片 2。

切片的核心网部分通常主要包括 AMF、SMF 和 UPF 等网络功能。在现有 3GPP 标准中, 通常的实现方法是切片 1 和切片 2 使用不同的 SMF、UPF, 但切片 1 和切片 2 会使用同一个 AMF (如上述规则 1 描述)。如图 2A 所示, 切片 1 使用 SMF1 和 UPF1, 切片 2 使用 SMF2 和 UPF2, 但是切片 1 和切片 2 使用了同一个 AMF。并且, 虽然 UE 使用切片 1 和切片 2 之间相隔一段时间 (非同时), 而且 UE 中间还完成了去注册, 但是 UE 和网络仍会保留并使用同一套安全上下文, 如包括: AMF 密钥 Kamf, 用于推演加密/完整性保护的密钥。这是由于网络通过重复使用安全上下文, 可优化网络性能。

由此可见, 虽然 UE 非同时接入 2 个不同切片, 但使用的仍然是同一套安全上下文。如果其中一个切片是要求与其他切片隔离的切片, 则该切片的信息仍然存在泄露的风险, 因为其安全上下文与另一个切片的安全上下文是相同的, 使用另一个切片的安全上下文也可以获取到该切片的信息。因此, 对于非同时接入不同切片的场景, 也应该进行切片间的安全隔离 (如密钥隔离)。

场景 B: 不共享 AMF: UE 先后接入不同 (或相同) 的切片, 或者发生了 AMF 重定向。

例如, UE 在某一个时刻通过 AMF1 接入了切片 1, 使用并完成了切片 1 上的业务后, UE 退出了切片 1 和网络, 完成了与网络间的去注册 (de-registration) 流程。UE 通过 AMF2 重新注册到网络并接入切片 2。虽然 UE 接入的是 AMF2, 但是由于网络性能优化的需求,

网络通常会要求 AMF1 保存 UE 的安全上下文，如密钥 Kamf，并传递给 AMF2。也就是说即使 UE 在非同时、非共享 AMF 的情况下接入了不同的切片，但是使用的安全上下文仍可以是相同的，切片 1 和切片 2 之间同样没有进行密钥层面的安全隔离。

又如，UE 进行 AMF 重定向（AMF re-allocation）的场景。这种场景发生在 UE 处于连接状态或没有去注册的情况下。如图 2B 所示，当 UE 向网络注册时，网络设备先由源（Source）AMF 处理 UE 的请求，并发起网络认证的流程，在认证完成并获取了 UE 请求接入的切片信息（如 NSSAI）后，确定使用目标（target）AMF 继续处理 UE 请求接入的切片。这个过程称为 UE 的重定向流程。重定向流程也可以因为 UE 位置的移动而触发。

在重定向流程中，UE 刚开始接入网络使用的是源 AMF，并在源 AMF 中保存 UE 的信息（包括 UE 的安全上下文）。需要说明的是，此时 UE 可以是已经接入了切片 1 或者可以是还没有接入切片 1。当网络决定转换使用目标 AMF 来为 UE 继续服务时，存储在源 AMF 的安全上下文可以被转移到目标 AMF。也就是说，UE 虽然没有同时接入切片 1 和切片 2，但是 UE 在切片 2 所使用的安全上下文却可以在两个 AMF 中都获取到。因此切片 2 和切片 1 并没有实现密钥层面的安全隔离。

根据场景 A 和场景 B 的描述可知，在 UE 非同时接入多切片时，切片间可能存在信息泄露的风险。

鉴于此，本申请提出一种切片隔离方法来避免切片间的信息泄露。在注册过程中，第一网络设备获取用户的第一切片的信息，若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，所述第一网络设备可以获取第二密钥，所述第二密钥用于对所述第二切片的信息和/或所述用户设备的信息进行安全保护。这里可以保证用户设备接入了待请求接入的第二切片之后，网络和用户设备所使用的密钥（即第二密钥）与用户设备接入其他切片（如，第一切片）时网络和用户所使用的密钥不同，避免了切片间的信息泄露。或者在去注册过程中，第一网络设备接收来自用户设备的去注册请求消息，所述第一网络设备删除第三密钥，所述第三密钥是用户设备接入第三切片时，网络和用户设备所使用的密钥，所述第三切片为所述用户设备最后一次接入的切片。这里通过删除用户设备之前用于接入其他切片时使用的密钥，可以保证网络和用户设备在后续接入的切片中所使用的密钥与先前接入其他切片时所使用的密钥不同，避免了切片间的信息泄露。或者在 AMF 重定向过程中，所述第一网络设备向其他网络设备发送用户设备的重定向消息，若所述第一网络设备获取到的切片的信息和用户设备请求接入的切片的信息不匹配，所述第一网络设备可以对所述用户设备发起重新认证。这里在 AMF 重定向过程中对用户设备重新发起认证流程，重新生成密钥，重新生成的密钥与源 AMF 中保存的密钥不同，从而避免了接入不同切片时使用相同的密钥，避免了切片间的信息泄露。

本申请实施例提供的切片隔离方法可以应用于图 1 所示的通信系统中。

注册过程中提供的切片隔离过程如图 3 所示，该过程包括：

S301：用户设备向第一网络设备发送第一请求消息，所述第一网络设备接收所述第一请求消息，所述第一请求消息用于请求接入第二切片。

示例性的，第一网络设备为 AMF。

所述第一请求消息可以为注册请求（Registration Request）消息。所述第一请求消息包括所述用户设备的标识信息和所述第二切片的信息。

所述用户设备的标识信息为所述用户设备的身份识别符，如用户设备的全球唯一临时标识符（globally unique temporary identifier, GUTI），和/或用户设备的隐藏标识符（subscription concealed identifier, SUCI），所述 SUCI 可以是对所述 SUPI 进行隐私保护处理（如加密处理）而得到的。

5 所述第二切片的信息包括所述第二切片的标识信息，可选的，所述第二切片的信息还可以包括所述第二切片的属性。所述第二切片的标识信息包括 S-NSSAI 或 NSSAI，所述 NSSAI 为切片标识集合，可以包括多个切片的标识（即多个 S-NSSAI），所述第二切片可以是所述多个 S-NSSAI 中的任意一个 S-NSSAI 所标识的切片。所述第二切片的属性可以通过共用属性值确定。例如共用属性值为 0 时，所述第二切片为普通切片，共用属性值为 10 1 时，所述第二切片为 1 型切片，共用属性值为 2 时，所述第二切片为 2 型切片，共用属性值为 3 时，所述第二切片为专属切片。

一种可能的示例中，所述第一网络设备接收到所述第一请求消息后，可以检查是否存在所述用户设备的安全上下文或上下文（包括安全上下文）。如所述第一网络设备确定所述用户设备之前是否接入过网络（如判断用户的身份标识符是否为 GUTI）。如果确定所述 15 用户设备之前未接入过网络设备，所述第一网络设备确定所述用户设备的上下文不存在，所述第一网络设备可以对所述用户设备进行网络认证，使得所述用户设备接入网络。如果确定所述用户设备之前曾接入过网络，所述第一网络设备还确定所述用户设备之前接入网络时通过哪个网络设备或哪个网络功能接入网络（如通过 GUTI 可以确定之前接入的网络设备，其中 GUTI 的内容包括了网络标识和网络功能（AMF）标识）。

20 S302: 第一网络设备获取用户设备的第一切片的信息。

如果所述用户设备最近一次通过所述第一网络设备接入网络，所述第一网络设备直接在所述第一网络设备中获取所述用户设备的第一切片的信息；如果所述用户设备最近一次 25 通过其他网络设备（非所述第一网络设备）接入网络，所述第一网络设备在其他网络设备中获取所述用户设备的第一切片的信息。可选的，所述用户设备的上下文或者安全上下文中包括所述第一切片的信息。以及可选的，所述用户设备的上下文或者安全上下文中包括所述第一切片的属性和/或第一密钥（如 Kamf），所述第一密钥为所述用户设备接入所述第一切片时，所述用户设备和网络所使用的密钥。

所述用户设备的第一切片为所述用户设备签约的一个或多个切片中的任一切片，或者所述第一切片为所述用户设备之前接入过或最近接入过的或当前接入的切片。所述第一切片 30 的信息包括所述第一切片的标识信息，可选的，所述第一切片的信息还可以包括以下至少一种：所述第一切片的属性，所述第一切片的安全上下文，和/或第一密钥，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。

在一种可能的示例中，所述第一网络设备可以在获取到所述用户设备的上下文或者安全上下文时，获取第一切片的信息。可选的，所述用户设备的上下文或者安全上下文包括 35 所述第一切片的信息，所述第一网络设备在所述用户设备的上下文或者安全上下文中获取所述第一切片的信息。或者可选的，所述第一网络设备在所述第一网络设备或其他网络设备中获取所述第一切片的信息。

S303: 若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则 40 所述第一网络设备获取第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户

设备接入所述第二切片时的信息进行安全保护。

所述第二密钥为所述用户设备接入所述第二切片时，所述用户设备和网络所使用的密钥。

若所述第一切片的信息包括所述第一切片的属性，所述第二切片的信息包括所述第二切片的属性，则在 S303 中，若所述第一切片的属性与所述第二切片属性不匹配，则所述第一网络设备获取所述第二密钥。

其中所述第一切片的属性与所述第二切片的属性不匹配，包括所述第一切片的属性与所述第二切片的属性不相容，或者所述第一切片的属性与所述第二切片的属性互斥。

所述第一切片的属性与所述第二切片的属性不匹配/不相容/互斥，包括以下至少一种：
11) 所述第一切片的共用属性和/或第二切片的共用属性不允许与其他任意属性的切片共用。

示例性的，所述第一切片和/或所述第二切片为专属切片。例如，所述第一切片为专属切片，所述第二切片为任意属性的切片。又如，所述第二切片为专属切片，所述第一切片为任意属性的切片。又如，所述第一切片为专属切片，所述第二切片为专属切片，所述第一切片和所述第二切片为不同的专属切片。

12) 所述第一切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 不同。

13) 所述第二切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第一切片的属性的 SST 与所述第二切片的属性的 SST 不同。

14) 所述第一切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 不同。

15) 所述第二切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 不同。

其中 12) 和 14) 中所述第一切片非专属切片，但与所述第二切片的共用属性不相容，例如所述第一切片的属性为 1 型切片，所述第二切片的属性为 2 型切片，或者所述第一切片的属性为 2 型切片，所述第二切片的属性为 1 型切片。13) 和 15) 中所述第二切片非专属切片，但与所述第一切片的共用属性不相容，例如所述第二切片的属性为 1 型切片，所述第一切片的属性为 2 型切片，或者所述第二切片的属性为 2 型切片，所述第一切片的属性为 1 型切片。

在一种可能的示例中，所述第一网络设备获取所述第二密钥时，所述第一网络设备根据所述第一密钥生成所述第二密钥，其中，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。例如，第一网络设备是 AMF，AMF 根据 Kamf(用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护)生成第二切片密钥。

在另一种可能的示例中，所述第一网络设备获取所述第二密钥时，所述第一网络设备对所述用户设备重新发起网络认证或者发起切片认证；若第一网络设备对所述用户设备重新发起的认证成功或者发起的切片认证成功，则所述第一网络设备生成或者收到所述第二密钥。例如，第一网络设备是 AMF，AMF 中包括了安全锚点功能(SECURITY ANCHOR FUNCTION 或 SEAF)。网络认证成功时，安全锚点功能 SEAF 生成第二密钥。又例如，AMF 中不包括 SEAF 功能，即 AMF 与 SEAF 分开部署在不同的网络设备中。网络认证成功时，安全

锚点功能 SEAF 生成第二密钥后, 将第二密钥发送给 AMF。这个流程确保第二密钥与第一密钥是独立的, 无法基于第二密钥获取到第一密钥, 也不能基于第一密钥获取到第二密钥。

在又一种可能的示例中, 可以根据不同的共用属性, 设置对应的隔离要求, 在本申请实施例中对不同共用属性对应的隔离要求不做限制。例如, 共用属性值越大, 隔离要求越高, 如所述专属切片的隔离要求最高, 所述 2 型切片的隔离要求次之, 所述 1 型切片的隔离要求较所述 2 型切片的隔离要求低, 所述普通切片的隔离要求最低。

在该示例中, 所述第一网络设备获取所述第二密钥时, 若所述第一切片的隔离要求高于所述第二切片的隔离要求, 所述第一网络设备根据所述第一密钥生成所述第二密钥; 若所述第一切片的隔离要求低于所述第二切片的隔离要求, 所述第一网络设备对所述用户设备重新进行网络认证, 若重新认证成功, 所述第一网络设备生成或收到所述第二密钥。

其中, 相比于重新认证, 根据所述第一密钥生成所述第二密钥的过程简单, 执行步骤少, 所述用户设备与网络交互也少。

S304: 所述第一网络设备向所述用户设备发送第一指示信息, 所述用户设备接收所述第一指示信息, 所述第一指示信息用于指示所述用户设备获取第二密钥。

所述第一指示信息可以用于指示所述用户设备根据所述第一密钥生成所述第二密钥。

在一种实现方式中, 第一指示消息可以是非接入层 (non access stratum, NAS) 安全模式命令 (security mode command, SMC) 信令。

步骤 S304 为可选步骤, 如果所述第一网络设备对所述用户设备发起重新进行网络认证, 则不必执行步骤 S304。需要说明的是, 在所述第一网络设备发起的对所述用户设备重新进行网络认证的过程中, 所述第一网络设备 (如包括 AMF 和 SEAF) 会发送其他一条或多条消息, 如认证请求消息等, 而所述用户设备也会回复一条或多条消息, 这里不作限定。

S305: 所述用户设备获取所述第二密钥。

在一种可能的示例中, 在该 S305 中, 所述用户设备获取第一密钥, 所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护; 所述用户设备根据所述第一密钥生成所述第二密钥。

所述用户设备中可以保存有所述第一密钥。

在另一种可能的示例中, 所述用户设备与所述第一网络设备进行重新认证; 若所述用户设备与所述第一网络设备重新认证成功, 则所述用户设备生成所述第二密钥, 该密钥与第一密钥不能相互推演获得。

需要注意的是, 所述第一网络设备和所述用户设备采用相同的方式获取 (包括使用相同参数生成) 所述第二密钥, 以保证后续所述第一网络设备和所述用户设备采用相同的密钥对通信信息进行安全保护。

在该注册过程中, 若所述第一切片的属性与所述第二切片的属性匹配, 所述第一网络设备还可以向所述用户设备发送注册接受消息, 所述用户设备接收所述注册接受消息。

其中所述第一切片的属性与所述第二切片的属性匹配, 包括所述第一切片的属性与所述第二切片的属性相容, 或者所述第一切片的属性与所述第二切片的属性不互斥。

所述第一切片的属性与所述第二切片的属性匹配/相容/不互斥, 包括以下至少一种:

21) 所述第一切片的属性或第二切片的属性允许与其他任意属性的切片共用。

示例性的, 所述第一切片和/或所述第二切片为普通切片。

22) 所述第一切片的属性仅允许具有相同 SST 的切片共用, 所述第二切片的属性的

SST 与所述第一切片的属性的 SST 相同。

例如所述第一切片和所述第二切片均为 1 型切片，且 SST 相同。

23) 所述第二切片的属性仅允许具有相同 SST 的切片共用，所述第一切片的属性的 SST 与所述第一切片的属性的 SST 相同。

5 例如所述第一切片和所述第二切片均为 1 型切片，且 SST 相同。

24) 所述第一切片的属性仅允许具有相同 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 相同。

例如所述第一切片和所述第二切片均为 2 型切片，且具有相同 SD。

10 25) 所述第二切片的属性仅允许具有相同 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 相同。

例如所述第一切片和所述第二切片均为 2 型切片，且具有相同 SD。

26) 所述第二切片和所述第一切片映射到同一单网络切片选择辅助信息 S-NSSAI。

15 所述第一切片和所述第二切片可以映射到归属网络 (Home PLMN) 中相同的 S-NSSAI 切片。所述第一切片和所述第二切片在各自的 PLMN 中可以有不同的切片标识 S-NSSAI 或不同的 SST 类型、SD。

27) 多个类型的切片，但切片的属性可以相容的其他可能。

20 若所述第一切片的信息中未标识所述第一切片的属性，则可以认为所述第一切片的属性允许与其他任意属性的切片共用。例如，可以认为所述第一切片为普通切片。或者若所述第一切片的信息中未标识所述第二切片的属性，则可以认为所述第二切片的属性允许与其他任意属性的切片共用。例如，可以认为所述第二切片为普通切片。

25 若所述第一切片的信息中未标识所述第一切片的属性，或者所述第二切片的信息中未标识所述第二切片的属性，则用户设备为 legacy 设备即原有设备。例如 5G 标准有 R15 版本、R16 版本、R17 版本。如果 GST 共用属性是 R17 版本中新引入的，则 R15、R16 版本的设备可以被称为 legacy 设备。为了“向后兼容”性，legacy 设备仍可以在网络中使用，legacy 设备接入的切片可以被看作是普通切片。

下面以两个具体的实施例对图 3 所示的切片隔离过程进一步说明。

用户设备最近一次接入网络时通过第一 AMF 接入网络，切片隔离过程参见图 4 (分时共享 AMF)，包括以下步骤：

30 S401: 用户设备向第一 AMF 发送注册请求。

所述注册请求包括所述用户设备的身份标识符 (如 GUTI 或者 SUCI 等) 和请求接入的第二切片的标识信息 (如 S-NSSAI, 可以是请求接入的 NSSAI 中的任意一个 S-NSSAI)。可选的，所述注册请求包括所述第二切片的属性。

S402: 第一 AMF 确定是否存储了所述用户设备的安全上下文 (security context)。

35 例如，所述第一 AMF 根据所述用户设备的身份标识符 GUTI，确定是否在所述第一 AMF 中保存了所述用户的有效的安全上下文，如果有，跳过 S403，执行 S404，如果没有，执行 S403。

40 所述安全上下文为有效的安全上下文，指所述第一 AMF 使用所述安全上下文 (如第一密钥 Kamf) 可以验证成功所述注册请求消息中的消息认证码 (message authentication code, MAC)。

可选的步骤 S403: AMF 发起所述用户设备与所述第一 AMF、UDM 进行网络认证或一级认证 (Primary Authentication)。

在执行所述 S403 之后, 跳过 S404-S409, 执行 S410, 执行现有标准流程中的其他注册步骤。

5 可选的步骤 S404: 所述第一 AMF 获取用户设备签约的切片的信息, 即获取、检索签约信息 (subscription information)。

所述第一 AMF 从本地(所述第一 AMF 自身的存储单元)或 UDM(也可以为其他 NF) 中获取所述用户设备签约的切片的信息 (如切片标识 NSSAI, 可以包括一个或多个 S-NSSAI)。例如, 所述第一 AMF 先在本地查找是否存在所述用户设备签约的切片的信息, 10 如果存在, 所述第一 AMF 在本地获取所述用户设备签约的切片的信息, 如果不存在, 所述第一 AMF 向所述 UDM 发送请求消息, 在所述 UDM 获取所述用户设备签约的切片的信息。

所述第一 AMF 在获取的所述用户设备签约的切片的信息中, 检索、获取所述签约的切片的共用属性信息。

15 可选的步骤 S405: 所述第一 AMF 检查所述签约的切片的属性。

例如可选的, 检查所述签约的切片的信息中是否包括所述签约的切片的属性信息。所述签约的切片可以是一个或多个切片, 所述一个或多个切片分别对应一个或多个切片属性, 也就是说, 每个切片分别对应一个切片的属性信息。

若所述签约的切片只包含了单一的切片属性, 所述第一 AMF 跳过 S406-S409, 执行 20 S410。

若所述签约的切片信息中包括多于一个切片属性, 且所述多于一个的切片属性为相容的属性, 所述第一 AMF 跳过 S406-S409, 执行 S410, 或者所述第一 AMF 也可以执行 S407。

其余情况所述第一 AMF 执行 S406。

25 可选的步骤 S406: 所述第一 AMF 获取第一切片信息 (即第一切片的信息), 比较所述第一切片的属性和请求接入的所述第二切片的属性。

所述第一 AMF 从本地(所述第一 AMF 自身的存储单元)或 UDM(也可以为其他 NF) 中获取所述第一切片信息。所述第一切片信息为保存在所述用户设备的上下文中的切片信息。所述第一切片信息包括一个或多个 S-NSSAI, 用来表示所述用户设备正在接入或曾经接入的所述一个或多个 S-NSSAI 指示的切片。所述第一切片信息还包括所述第一切片 (对 30 应于一个或多个 S-NSSAI) 的属性信息。一种可选的方式, 若根据所述第一切片的属性和所述第二切片的属性, 确定所述第一切片的属性和所述第二切片的属性不匹配, 且所述第一切片的隔离要求高于或不低于所述第二切片的隔离要求, 所述第一 AMF 返回执行 S403。

一种可选的方式, 若根据所述第一切片的属性和所述第二切片的属性, 确定所述第一切片的属性和所述第二切片的属性不匹配, 所述第一 AMF 返回执行 S403。

35 一种可选的方式, 若根据所述第一切片的属性和所述第二切片的属性, 确定所述第一切片的属性和所述第二切片的属性不匹配, 且所述第一切片的隔离要求低于或者不高于所述第二切片的隔离要求, 所述第一 AMF 执行 S407。

一种可选的方式, 若根据所述第一切片的属性和所述第二切片的属性, 确定所述第一切片的属性和所述第二切片的属性不匹配, 所述第一 AMF 执行 S407。若根据所述第一切 40 片的属性和所述第二切片的属性, 确定所述第一切片的属性和所述第二切片的属性匹配,

所述第一 AMF 跳过 S407-S409, 执行 S410。

需要说明的是, 获取到的所述第一切片的属性可以为一份或多份, 获取到的所述第二切片的属性可以为一份或多份, 所述第一切片 (S-NSSAI) 的数量和所述第二切片 (S-NSSAI) 的数量可以相同或不同。每份切片的属性分别对应一个切片 (S-NSSAI), 即每个切片 (S-NSSAI) 都对应一个属性。例如, 所述用户设备上一次接入 2 个切片, 标识分别为 S-NSSAI-1 和 S-NSSAI-2, 切片 S-NSSAI-1 的属性值为 0, 即普通切片, 切片 S-NSSAI-2 的属性值为 2, 即仅允许相同 SD 值共用的切片 (这 2 个切片上一次被所述用户设备共用, 隐含了切片 S-NSSAI-1 的 SD 值与切片 S-NSSAI-2 的 SD 值相同)。所述 AMF 中对应所述用户设备的上下文中保存有切片 S-NSSAI-1 和切片 S-NSSAI-2 的标识以及属性值, 还保存共用的密钥 Kamf。如所述用户设备本次请求接入另一个切片 S-NSSAI-3, 切片 S-NSSAI-3 的属性值为 3, 即专属切片。在这个例子中, 所述第一 AMF 可以获取到 2 个第一切片的属性, 以及 1 个第二切片的属性。

对于属性值为 “0” - “3” 的场景, 由于属性 “3” 不可以与其他属性共存 (即不相容), 而属性 “0” 可以与所有属性相容, 因此对于多份 S-NSSAI 的场景, 包括了 4 个可能单一属性 (1 种属性时) + 3 个可能的相容属性 (2 种属性时) + 1 个可能的相容属性 (3 种属性时) = 8 种可能的相容属性组合。对于分别包括多份 S-NSSAI 的第一切片属性信息和第二切片属性信息中, 两处切片信息的组合就会有 $8 \times 8 = 64$ 种可能的属性组合。为了便于描述, 在本申请实施例, 以保存有 1 个第一切片的信息, 以及所述用户设备请求接入 1 个第二切片的场景为例进行说明, 对于多个切片或多种属性值的情况, 可以参照该场景所示的情况, 不一一进行说明。具体可以归纳为以下情况:

31) 请求接入的第二切片的专属性要求高于第一切片的专属性, 即所述第二切片的隔离要求高于所述第一切片的隔离要求。

如所述第二切片的属性为专属切片 (属性值为 3), 所述第一切片的属性为非专属性切片 (属性值为 0 或 1 或 2)。

又如, 所述第二切片的属性值为 1 或 2, 所述第一切片的属性为普通切片 (属性值为 0)。

32) 请求接入的第二切片的专属性要求低于第一切片的专属性, 即所述第二切片的隔离要求低于所述第一切片的隔离要求。

如所述第一切片的属性为专属切片 (属性值为 3), 所述第二切片的属性为非专属性切片 (属性值为 0 或 1 或 2)。

又如, 所述第一切片的属性值为 1 或 2, 所述第二切片的属性为普通切片 (属性值为 0)。

33) 请求接入的第二切片与所述第一切片不相容的其他情况。

其中 33) 包括 31) 和 32) 所示的情况, 其余情况可以参见图 3 中的相关描述, 在此不一一列出。

34) 请求接入的第二切片与所述第一切片可以被同时使用。

如所述第二切片和所述第一切片为同一个专属切片。又如所述第二切片和所述第一切片为普通切片。以及所述第二切片和所述第一切片属性相容的其他情况, 其他情况可以参见图 3 中的相关描述, 在此不一一列出。

针对 31) 和 33), 所述第一 AMF 返回执行 S403, 采用较强的隔离方式, 保证切片间

信息的安全性。在另一种可选实现方式中，所述第一 AMF 执行 S407，即与 32) 采用同样执行方法。

针对 32)，所述第一 AMF 执行 S407，采用代价较小的隔离方式，保证切片间信息的安全性。在另一种可选实现方式中，所述第一 AMF 执行 S40，即与 31) 和 33) 采用同样执行方法。

针对 34)，所述第一 AMF 跳过 S407-S409，执行 S410，切片之间无需隔离。

可选的步骤 S407: 所述第一 AMF 启动密钥更新流程来更新存储在 AMF 处的密钥 Kamf。

在该 S407 中，所述第一 AMF 根据第一密钥（如密钥 Kamf）生成所述第二密钥（更新的密钥 Kamf）。

可选的步骤 S408: 所述第一 AMF 通知所述用户设备更新第一密钥 Kamf，并将所需的密钥更新参数发送给所述用户设备。该 S408 发送的消息可以是“非接入层”（non access stratum, NAS）安全模式命令（security mode command, SMC）消息。可选的步骤 S409: 所述用户设备根据收到的密钥更新参数，更新存储的第一密钥 Kamf 生成第二密钥 Kamf（即原本存储的 Kamf 密钥为第一密钥，更新后的 Kamf 密钥为第二密钥）。

S410: 所述用户设备完成注册流程中的其他子流程，可参加相关标准流程，此处不详细介绍。

S411: 所述第一 AMF 向所述用户设备发送注册接受消息。

另一种可能的方式中，所述 S406 可以简化为所述第一 AMF 检查所述第二切片是否需要隔离，如果需要就重新返回执行 S403，或重新执行返回 S707（执行 S707-S709），如果不需要，所述第一 AMF 执行 S410。

用户设备最近一次接入网络时通过第二 AMF 接入网络，所述用户设备本次接入网络通过第一网络设备接入，切片隔离过程参见图 5（非共享 AMF），包括以下步骤：

S501 的过程参见上述 S401。

S502: 所述第一 AMF 确定所述用户设备曾经接入过网络（如通过注册请求中包括 GUTI），且曾经通过第二 AMF 接入网络（如 GUTI 包括所述 AMF 的 ID）。即所述用户设备之前接入的 AMF 已经发生了改变（第二 AMF 与第一 AMF 不是同一个 AMF）。

所述第一 AMF 可以看作是新（new）AMF，或目标（target）AMF。所述第二 AMF 可以看作是旧（old）AMF，或源/初始（Source/Initial）AMF。

S503: 所述第一 AMF 向所述第二 AMF 发送请求消息（如用户终端上下文转换请求消息 UE context transfer request），获取所述第二 AMF 存储的第一切片的信息。

所述请求消息中可以包括所述用户设备请求接入的第二切片的信息。

S504: 所述第二 AMF 比较保存的所述第一切片的属性和请求接入的所述第二切片的属性。在一种可选实现方式中，S504 为可选执行，即第二 AMF 不执行该比较。

S505: 所述第二 AMF 向所述第一 AMF 发送响应消息（如用户终端上下文转换响应消息 UE context transfer response）。

所述第二 AMF 可以根据所述 S504 的比较结果，确定在 S505 的响应消息中携带哪些信息。

例如，所述第一切片的属性和所述第二切片的属性匹配，所述响应消息中可以包括所述第一切片的安全上下文（如包括第一密钥 Kamf）等。

又如，所述第一切片的属性和所述第二切片的属性不匹配，所述响应消息中可以包括

非安全的上下文，而不包括安全上下文（如第一密钥 Kamf）。或者所述响应消息中可以包括不影响切片隔离的上下文（安全或非安全的上下文均可以，如所述用户设备的 SUPI 等），而不包括影响切片隔离的上下文（如第一密钥 Kamf）。可选的，所述响应消息中包括所述第一切片的标识信息（NSSAI）及属性。可选的，所述响应消息包括指示信息，告知所述第一 AMF 所述用户设备已经通过了安全认证，所述用户设备的安全上下文存在但与第二切片的属性不匹配，不能发送所述安全上下文（如第一密钥 Kamf），指示所述第一 AMF 重新进行认证（网络认证或切片认证，其中网络认证包括一级认证和可选的切片认证）。又或者所述第二 AMF 先更新第一密钥 Kamf，（更新后为第二密钥 Kamf）或进行重新认证，然后将更新后的安全上下文（如第二密钥 Kamf 以及更新密钥所需参数，可选的还包括密钥指示信息，用来指示该密钥已经更新或者指示该密钥为第二密钥）携带在所述响应消息中发送给所述第一 AMF，可能的所述第一 AMF 为了切片隔离，还会更新密钥或进行重新认证。

又如，如果所述第二 AMF 无法判断所述第一切片的属性和所述第二切片的属性是否匹配，如所述第二 AMF 没有存储所述第一切片的属性，或者所述第一 AMF 发送的请求消息中不包括所述第二切片的属性等情况，此时所述第二 AMF 可以认为所述第一切片的属性和所述第二切片的属性不匹配。

在一种可选方式中，如果第二 AMF 不执行 S504，即第二 AMF 认为第一切片属性和第二切片属性相匹配（相容），S505 可以按照现有流程执行。

在一种可选方式中，第二 AMF 在 S505 消息中包括指示信息，指示第一 AMF 重新进行一级认证（即不基于第一密钥而生成第二密钥），或者进行 Kamf 密钥更新（即发送第一密钥，指示第一 AMF 基于第一密钥生成第二密钥）。

S506：所述第一 AMF 对所述响应消息进行处理。

所述第一 AMF 根据所述响应消息，决定并执行后续的流程。

如果所述响应消息包括所述第一密钥或/和第二密钥、第一切片标识信息及属性，比较所述所述第一切片的属性和请求接入的第二切片的属性。

一种可选的方式，若根据所述第一切片的属性和所述第二切片的属性，确定所述第一切片的属性和所述第二切片的属性不匹配，且所述第一切片的隔离要求高于或不低于所述第二切片的隔离要求，所述第一 AMF 执行 S507。

一种可选的方式，若根据所述第一切片的属性和所述第二切片的属性，确定所述第一切片的属性和所述第二切片的属性不匹配，且所述第一切片的隔离要求低于或者不高于所述第二切片的隔离要求，所述第一 AMF 执行 S508。

一种可选的方式，若根据所述第一切片的属性和所述第二切片的属性，确定所述第一切片的属性和所述第二切片的属性不匹配，所述第一 AMF 执行 S507。

一种可选的方式，若根据所述第一切片的属性和所述第二切片的属性，确定所述第一切片的属性和所述第二切片的属性不匹配，所述第一 AMF 执行 S508。

若根据所述第一切片的属性和所述第二切片的属性，确定所述第一切片的属性和所述第二切片的属性匹配，所述第一 AMF 跳过 S507-S508，执行 S509。

一种可选的方式，如果所述响应消息包括所述第二密钥 Kamf 以及更新密钥所需参数，所述第一 AMF 执行 S508。

在一种可选方式中，第一 AMF 根据 S505 消息中包括的指示信息执行。即，如果指示

第一 AMF 重新进行一级认证, 则执行 S507; 或者如果指示第一 AMF 进行 Kamf 密钥更新则执行 S508。

S507 的过程参见上述 S403。

所述第一 AMF 发起所述用户设备与网络进行一级认证 (Primary Authentication)。

5 在执行所述 S507 之后, 执行现有标准流程生成所述第二密钥 (跳过 S508 中的密钥更新流程), 执行 S509, 执行现有标准流程中的其他注册步骤。

S508 的过程参见上述 S407-S409。

S509-S510 的过程参见上述 S410-S411。

10 可选的, S504 和 S506 可以择一执行, 或者都执行。需要说明的是, 上述 S506 中所述第一 AMF 可以独立于所述第二 AMF (S504) 重新进行了判断。是因为所述第一 AMF 和所述第二 AMF 有可能处于不同的 PLMN 或不同的安全域, 或者所述第一 AMF 不一定完全信任所述第二 AMF 的判断结果。

15 另外, 所述第一 AMF 也可以通过其他 NF (非第二 AMF, 如非结构化数据存储功能 (unstructured data storage function, UDSF)) 获取所述第一切片的信息。所述第一 AMF 也可以通过其他 NF (如 UDSF) 与所述第二 AMF 间接交互, 这里对此不做限制。

去注册过程中提供的切片隔离过程如图 6 所示, 该过程包括:

S601a: 用户设备向第一网络设备发送去注册请求消息, 所述第一网络设备接收所述去注册请求消息。

20 在该 S601a 中, 去注册过程由所述用户设备发起。

S601b: 第一网络设备向用户设备发送去注册请求消息, 所述用户设备接收所述去注册请求消息。

在该 S601b 中, 去注册过程由所述第一网络设备发起。

可以理解, 所述 S601a 和 S601b 可以择一执行。

25 S602: 所述第一网络设备删除本地 (即第一网络设备) 存储的所述用户设备上下文中的第三密钥, 所述第三密钥用于对第三切片的信息或者所述用户设备接入第三切片时的信息进行安全保护, 所述第三切片为所述用户设备最后接入的一个切片 (对应于一 S-NSSAI 标识) 或多个切片 (对应于多个 S-NSSAI 标识或包括多个 S-NSSAI 的 NSSAI) 中的任意/每一个切片 (当允许同时接入多切片时, 这些切片属性默认是相容的, 可以共用一套密钥)。

30 在 S602 中, 所述第一网络设备可以确定所述第三切片的属性不允许与其他任意属性切片共用 (即所述第三切片为专属切片, 属性值为 3), 所述第一网络设备删除本地存储的所述用户设备的上下文中的所述第三密钥。

35 可选的, 在 S602 中, 所述第一网络设备可以确定所述用户设备签约了多个属性的切片 (如本地存储的用户签约信息或向 UDM 获取的所述用户的用户签约信息), 其中存在与第三切片属性不相容的切片, 所述第一网络设备删除本地存储的所述用户设备的上下文中的所述第三密钥。

40 可选的, 在 S602 中, 所述第一网络设备可以确定所述第三切片的属性不允许与其他任意属性切片共用 (即所述第三切片为专属切片, 属性值为 3), 且所述第一网络设备可以确定所述用户设备仅签约该切片 (如本地存储的用户签约信息或向 UDM 获取的所述用户的用户签约信息), 所述第一网络设备保留 (即不删除) 本地存储的所述用户设备的上下

文中的所述第三密钥。

所述第三切片的属性不允许与其他任意属性切片共用（即所述第三切片为专属切片，属性值为3），所述第一网络设备删除本地存储的所述用户设备的上下文中的所述第三密钥。

5 可选的，所述第一网络设备向其他网络设备或网络功能（如UDM、其他AMF等）发送指示信息，指示所述网络设备或网络功能删除存储的所述用户设备的上下文中的所述第三密钥。

可选的，所述第一网络设备向所述用户设备发送指示信息，指示所述用户设备删除存储的所述第三密钥。

S603：所述用户设备删除所述第三密钥。

10 可选的，所述S602和S603的执行先后顺序不做限定。

在一种可能的示例中，在该S603中，所述用户设备可以确定所述第三切片的属性不允许与其他任意属性的切片共用，所述用户设备删除所述第三密钥。

在另一种可能的示例中，在该S603中，所述用户设备接收来自所述第一网络设备的指示信息，所述用户设备删除所述第三密钥。

15 在该去注册过程中，若所述第三切片的属性允许与其他属性的切片共用或未获取所述第三切片的属性，当所述用户设备发起去注册流程时，所述第一网络设备还可以向所述用户设备发送去注册接受消息，所述用户设备接收所述去注册接受消息；或者当所述第一网络设备发起去注册流程时，所述用户设备还可以向所述第一网络设备发送去注册接受消息，所述第一网络设备接收所述去注册接受消息。

20 可以理解，所述S602和S603可以在去注册过程之前、去注册的过程中、或者去注册过程之后执行。

需要说明的是，在去注册过程完整之后，如果所述用户设备接入专属切片，所述用户设备需要和网络重新进行一次认证（可选的，和切片认证），生成新的密钥以便接入所述专属密。

25 在实施例中通过删除敏感/重要的安全上下文，可以避免这类安全上下文被重复使用，保证切片间信息的安全性。

下面以两个具体的实施例对图6所示的切片隔离过程进一步说明。

用户设备发起去注册流程，切片隔离过程参见图7所示，包括以下步骤：

30 S701：所述用户设备向AMF发送去注册请求消息（Deregistration Request），所述AMF接收所述去注册请求消息。

S702：所述AMF确认存储的所述用户设备的上下文中第三切片的属性。所述第三切片为所述用户设备最后接入的一个切片（对应于一S-NSSAI标识），或者多个切片（对应于多个S-NSSAI标识或包括多个S-NSSAI的NSSAI）中的任意/每一个切片（当允许同时接入多切片时，表明这些切片属性是相容的，可以共用一套密钥）。

35 所述AMF可以在本地或UDM（也可以为其他NF）中获取第三切片的属性。例如所述AMF先确定本地存储的所述用户设备的上下文中是否存在第三切片的属性，如果存在，所述AMF在所述用户设备的上下文中获取所述第三切片的属性，如果不存在，所述AMF在所述UDM中获取所述第三切片的属性。

40 S703：进行PDU会话释放、N4会话释放（N4 session release）、中止策略（policy termination）等流程。

S704: 所述 AMF 发送去注册接受消息 (Deregistration Accept), 所述用户设备接收所述去注册接受消息。

S705a: 所述 AMF 检查所述第三切片的属性。

S705b: 所述用户设备检查所述第三切片的属性。

5 若仅签约了属性相容的切片 (如所述第三切片的属性为普通切片, 允许与其他属性的切片共用), 或者未获取到所述第三切片的属性, 所述 AMF 和所述用户设备保留所述第三密钥, 执行 S706。

若签约了属性不相容的切片 (如所述第三切片的属性为专属切片, 不允许与任意属性的切片共用), 所述 AMF 和所述用户设备删除所述第三密钥, 执行 S706。

10 S706: 所述用户设备和所述 AMF 释放信号连接。

需要说明的是, S702 也可以在 S703 (有多条交互消息) 的执行过程中执行, 或通过 S703 中的现有消息执行 (如通过增加信息元 (information elements) 的方式), 而不必须新增单独的交互消息。

15 另外, S705a 和 S705b 的执行先后顺序不做说明, 并且 S705a、S705b 可以在 S704 之前执行, 或者可以在 S706 之后执行。

网络设备发起去注册流程, 切片隔离过程参见图 8 所示, 包括以下步骤:

可选的步骤 S801: UDM 发送去注册通知消息, 所述 AMF 接收所述去注册通知消息。

在 S801 中, UDM 发起去注册流程。

20 可选的, 所述去注册通知消息可以包括第三切片的属性或者包括用户设备所有签约的切片的属性。可选的, 所述去注册通知消息还可以包括指示信息, 指示所述 AMF 删除第三密钥。即 UDM 根据所述第三切片的信息或者用户设备签约的切片的消息判断安全敏感性或隔离要求。

S802: 所述 AMF 向用户设备发送去注册请求消息, 所述用户设备接收所述去注册请求消息。

25 所述 AMF 也可以自行发起去注册流程。

所述去注册请求消息为可选的消息, 即所述去注册流程可以通知所述用户设备, 也可以不通知所述用户设备。如果发送所述去注册请求消息, 可选的, 所述 AMF 还可以指示所述用户设备删除所述第三密钥。这里所述 AMF 根据所述 UDM 发送的所述第三切片的属性, 判断是否删除所述第三密钥 (可以参见上述 S705a), 或者所述 AMF 根据所述 UDM 的指示信息, 确定是否删除所述第三密钥。

S803 的过程可以参见上述 S703。

S804: 所述用户设备发送去注册接受消息, 所述 AMF 接收所述去注册接受消息。

S805a: 所述 AMF 检查所述第三切片的属性。

参见上述 S702 及 S802 或上述 S705a 获取、检查第三切片的属性。

35 S805b: 所述用户设备检查所述第三切片的属性。

参见上述 S705b。

S806 的过程可以参见上述 S706。

所述 S805a 可以在任何一个步骤执行 (包括在步骤 S801 之前, 因此 AMF 可以自行发起去注册流程)。所述 S805b 可以在 S802 之后的任何一个步骤执行。

40 所述图 7 和图 8 所示的切片隔离方法既适用于分时共享 AMF, 又适用于非共享 AMF。

AMF 重定向过程中提供的切片隔离过程如图 9 所示, 该过程包括:

S901: 第一网络设备向第二网络设备发送重定向消息, 所述第二网络设备接收所述重定向消息。

5 所述第一网络设备在 AMF 重定向过程中, 可以理解为源网络设备, 所述第二网络设备在 AMF 重定向过程, 可以理解为目标网络设备。

所述重定向消息包括用户设备的第四切片的信息和/或所述用户设备请求接入的第五切片的信息。所述第四切片为当前保存的用户之前接入或当前已接入的切片。

10 所述第四切片的信息包括所述第四切片的标识信息, 以及可选的包括第四密钥和/或所述第四切片的属性, 所述第四密钥用于对所述第四切片的信息或/和所述用户设备接入所述第四切片时的信息进行安全保护。所述第五切片的信息包括所述第五切片的标识信息, 以及可选的所述第五切片的属性。

AMF 重定向的一个典型场景为: 用户设备已经和所述第一网络设备完成了网络级认证 (一级认证), 并生成了安全上下文 (如第四密钥 kamf)。所述第一网络设备决定由另一个合适的第二 AMF 服务所述用户设备。这时所述用户设备与所述第一网络设备的交互就转换为所述用户设备与所述第二网络设备的交互。

15 在 S901 之前, 所述第一网络设备还可以检查当前保存的所述用户设备的安全上下文是否已经用于对切片 (如第四切片) 的信息进行安全保护或者是否有第四切片的信息。如果否, 即不存在第四切片, 所述第一网络设备可以假设 (不存在的) 第四切片的属性为可以与任何切片匹配的普通切片, 然后执行 S901。如果是, 则存在所述第四切片。

若所述第四切片的信息与所述第五切片的信息匹配 (类似地, 如果不存在第五切片信息, 则视为可以与任何切片匹配的普通切片), 所述第一网络设备执行 S901;

25 若所述第四切片的信息与所述第五切片的信息不匹配, 且所述第四切片的隔离要求高于或不低于所述第五切片的隔离要求 (例如第四切片存在隔离要求 (非普通切片) 而第五切片为普通切片), 所述第一网络设备根据所述第四密钥生成所述第五密钥, 然后执行 S901;

若所述第四切片的信息与所述第五切片的信息不匹配, 且所述第四切片的隔离要求低于或者不高于所述第五切片的隔离要求 (例如第四切片不存在隔离要求的普通切片而第五切片为专属切片), 所述第一网络设备执行 S901。

30 一种可选的方式, 若所述第四切片的信息与所述第五切片的信息不匹配, 所述第一网络设备根据所述第四密钥生成所述第五密钥, 然后执行 S901。

S902: 若所述第四切片的信息与所述第五切片的信息不匹配, 且所述第五切片具有隔离要求, 则所述第二网络设备对所述用户设备重新认证。

若所述第二网络设备对所述用户设备重新认证成功, 所述第二网络设备生成所述第五密钥。

35 若所述第四切片的信息与所述第五切片的信息匹配, 所述第二网络设备继续对所述用户设备进行注册。

若所述第四切片的信息与所述第五切片的信息不匹配, 且所述第四切片不具有隔离要求 (即允许与其他任意属性切片共用), 所述第二网络设备继续对所述用户设备进行注册。

40 需要说明的是, 所述第一网络设备可以对所述第四切片的信息与所述第五切片的信息进行比较, 和/或所述第二网络设备也可以对所述第四切片的信息与所述第五切片的信息进

行比较,并分别在比较的切片信息不匹配时,执行 S902 重新认证生成第五密钥(不基于第四密钥)或根据第四密钥生成第五密钥。

下面以一个具体的实施例对图 9 所示的切片隔离过程进一步说明。

5 切片隔离过程参见图 10 所示,主要适用于非共享 AMF,包括以下步骤:

S1001: 用户设备向接入网设备发送注册请求消息。

所述注册请求消息用于请求接入第五切片。

S1002: 所述接入网设备向初始/源 (Initial/Source) AMF 发送初始消息 (Initial UE message)。所述初始/源 (Initial/Source) AMF 可以为第一网络设备。

10 所述初始消息包括所述注册请求消息。

S1003: 所述源 AMF 发起与所述用户设备的网络认证 (图 10 中未示出),并建立所述用户设备的安全上下文 (包括密钥 Kamf),用来安全保护所述用户设备与网络间交互的消息 (如对 NAS 消息进行加密和完整性保护)。所述源 AMF 确定需要进行 AMF 重定向,由目标 (target) AMF 来服务所述用户设备。所述目标 (target) AMF 可以为第二网络设备。
15 所述源 AMF 比较当前保存的第四切片的信息和用户请求接入的第五切片的信息。

若所述第四切片的信息与所述第五切片的信息匹配 (如果不存在第五切片信息,则视为可以与任何切片匹配的普通切片),所述第一网络设备执行 S1004,若所述第四切片的信息与所述第五切片的信息不匹配,且所述第四切片存在隔离要求 (非普通切片),所述第一网络设备根据所述第四密钥生成所述第五密钥,然后执行 S1004;若所述第四切片的信息与所述第五切片的信息不匹配,且所述第四切片不存在隔离要求 (普通切片),所述第一网络设备执行 S1004。
20

一种可选的方式,若所述第四切片的信息与所述第五切片的信息不匹配,且所述第四切片的隔离要求高于或不低于所述第五切片的隔离要求 (例如第四切片存在隔离要求 (非普通切片)而第五切片为普通切片),所述第一网络设备 (初始 AMF) 根据所述第四密钥生成所述第五密钥,然后执行 S1004;
25

一种可选的方式,若所述第四切片的信息与所述第五切片的信息不匹配,且所述第四切片的隔离要求低于或者不高于所述第五切片的隔离要求 (例如第四切片不存在隔离要求的普通切片而第五切片为专属切片),所述第一网络设备 (初始 AMF) 执行 S1004。

一种可选的方式,若所述第四切片的信息与所述第五切片的信息不匹配,所述第一网络设备 (初始 AMF) 根据所述第四密钥生成所述第五密钥,然后执行 S1004。
30

S1004: 所述源 AMF 向所述目标 AMF 发送重定向消息 (Rerouted message)。

所述重定向消息包括所述第四切片的信息和/或所述第五切片的消息。所述第四切片的信息包括所述第四切片的标识信息,以及可选的包括所述第四密钥和/或所述第四切片的属性。所述第四密钥用于对所述第四切片的信息或/和所述用户设备接入所述第四切片时的信息进行安全保护。所述第五切片的信息包括所述第五切片的标识信息,以及可选的所述第五切片的属性。
35

可选的,所述源 AMF 可以经过所述接入网设备转发所述重定向消息。(如 S1004a 和 S1004b 所示)。如果经过所述接入网设备转发,S1004b 的重定向消息与所述 S1004 的重定向消息可以不同。

40 S1005: 所述目标 AMF 比较当前保存的第四切片的信息和用户请求接入的第五切片的

信息。

若所述第四切片的信息与所述第五切片的信息不匹配，且所述第五切片具有隔离要求，则所述第二网络设备先对所述用户设备重新认证并生成第五密钥，然后进行执行 S1006。该重新认证的过程与 S1003 的相似，区别在于由所述目标 AMF 发起与所述用户设备的网络认证。

一种可选的方式，若所述第四切片的信息与所述第五切片的信息不匹配，且所述第四切片的隔离要求高于或不低于所述第五切片的隔离要求（例如第四切片存在隔离要求（非普通切片）而第五切片为普通切片），所述目标 AMF 根据所述第四密钥生成所述第五密钥，然后执行 S1006；

一种可选的方式，若所述第四切片的信息与所述第五切片的信息不匹配，且所述第四切片的隔离要求低于或者不高于所述第五切片的隔离要求（例如第四切片不存在隔离要求的普通切片而第五切片为专属切片），所述目标 AMF 执行 S1006。

一种可选的方式，若所述第四切片的信息与所述第五切片的信息不匹配，所述目标 AMF 根据所述第四密钥生成所述第五密钥，然后执行 S1006。

一种可选的方式，若所述第四切片的信息与所述第五切片的信息不匹配，所述目标 AMF 发起与用户设备的网络认证（一级认证）并生成第五密钥（不基于第四密钥），然后执行 S1006。若所述第四切片的信息与所述第五切片的信息匹配，所述第二网络设备，执行 S1006。

若所述第四切片的信息与所述第五切片的信息不匹配，且所述第四切片不具有隔离要求（即允许与其他任意属性切片共用），所述第二网络设备，执行 S1006。

S1006：所述第二网络设备继续对所述用户设备进行注册。

S1003 和 S1005 的比较过程可以都执行，也可以择一执行。

结合上述各实施例，可知本申请实施例提供的切片隔离适用于下述表 1 所示的场景。

表 1

流程场景	AMF 是否共享	说明
注册（registration）	分时共享 AMF	参见图 4
注册	非共享 AMF	参见图 5
去注册（deregistration）	分时共享 AMF/非共享 AMF	用户设备发起，参见图 7
去注册	分时共享 AMF/非共享 AMF	网络设备发起，参见图 8
注册中的 AMF 重定向 Re-Allocation	非共享 AMF	参见图 10

基于上述实施例可知，本申请实施例提供的切片隔离方法能够保证切片间的安全隔离，避免切片间的信息泄露。本申请实施例可以保证共享网络基础设施下场景的安全，也可以保证局部网络的安全。

可以理解的是，本申请提供的各实施例之间可以单独使用，也可以结合使用。

如图 11 所示，为本申请所涉及的通信装置的一种可能的示例性框图，该通信装置 1100 可以以软件或硬件的形式存在。通信装置 1100 可以包括：处理单元 1102 和收发单元 1103。作为一种实现方式，该收发单元 1103 可以包括接收单元和发送单元。处理单元 1102 用于对通信装置 1100 的动作进行控制管理。收发单元 1103 用于支持通信装置 1100 与其他网络

实体的通信。通信装置 1100 还可以包括存储单元 1101，用于存储通信装置 1100 的程序代码和数据。

其中，处理单元 1102 可以是处理器或控制器，例如可以是 CPU，通用处理器，DSP，ASIC，FPGA 或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包括一个或多个微处理器组合，DSP 和微处理器的组合等等。存储单元 1101 可以是存储器。收发单元 1103 是一种该装置的接口电路，用于从其它装置接收信号。例如，当该装置以芯片的方式实现时，该收发单元 1103 是该芯片用于从其它芯片或装置接收信号的接口电路，或者，是该芯片用于向其它芯片或装置发送信号的接口电路。

该通信装置 1100 可以为上述任一实施例中的用户设备和/或网络设备，还可以为用于用户设备和/或网络设备的芯片。例如，当通信装置 1100 为用户设备和/或网络设备时，该处理单元 1102 例如可以是处理器，该收发单元 1103 例如可以是收发器。可选的，该收发器可以包括射频电路，该存储单元例如可以是存储器。例如，当通信装置 1100 为用于用户设备和/或网络设备的芯片时，该处理单元 1102 例如可以是处理器，该收发单元 1103 例如可以是输入/输出接口、管脚或电路等。该处理单元 1102 可执行存储单元存储的计算机执行指令，可选地，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是该用户设备和/或网络设备内的位于该芯片外部的存储单元，如 ROM 或可存储静态信息和指令的其他类型的静态存储设备，RAM 等。

在第一个实施例中，该通信装置 1100 可以应用于第一网络设备。

具体的，所述收发单元 1103，用于获取用户设备的第一切片的信息；

所述处理单元 1102，用于若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则获取第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

在一个实现方式中，所述第一切片的信息包括所述第一切片的属性，所述第二切片的信息包括第二切片的属性；

所述处理单元 1102 在若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥时，具体用于若所述第一切片的属性与所述第二切片的属性不匹配，则获取所述第二密钥。

在一个实现方式中，所述处理单元 1102 在获取第二密钥时，具体用于根据所述第一密钥生成所述第二密钥，其中，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。

在一个实现方式中，所述处理单元 1102 在根据所述第一密钥生成所述第二密钥时，具体用于若所述第一切片的隔离要求高于所述第二切片的隔离要求，根据所述第一密钥生成所述第二密钥。

在一个实现方式中，所述处理单元 1102 在获取第二密钥时，具体用于：对所述用户设备重新进行认证；若对所述用户设备重新认证成功，则生成所述第二密钥。

在一个实现方式中，所述处理单元 1102 在对所述用户设备进行重新认证时，具体用于若所述第一切片的隔离要求低于所述第二切片的隔离要求，对所述用户设备重新进行网络认证。

在一个实现方式中, 所述第一切片的属性与所述第二切片的属性不匹配, 包括:

所述第一切片的属性或第二切片的属性不允许与其他任意属性的切片共用; 或者

所述第一切片的属性仅允许具有相同业务类型 SST 的切片共用, 所述第二切片的属性的 SST 与所述第一切片的属性的 SST 不同; 或者

5 所述第二切片的属性仅允许具有相同业务类型 SST 的切片共用, 所述第一切片的属性的 SST 与所述第二切片的属性的 SST 不同; 或者

所述第一切片的属性仅允许具有相同切片差异化因素 SD 的切片共用, 所述第二切片的属性的 SD 与所述第一切片的属性的 SD 不同; 或者

10 所述第二切片的属性仅允许具有相同切片差异化因素 SD 的切片共用, 所述第一切片的属性的 SD 与所述第二切片的属性的 SD 不同。

在一个实现方式中, 所述收发单元 1103, 还用于若所述第一切片的属性与所述第二切片的属性匹配, 向所述用户设备发送注册接受消息。

在一个实现方式中, 所述第一切片的属性与所述第二切片的属性匹配, 包括:

所述第一切片的属性或第二切片的属性允许与其他任意属性的切片共用; 或者

15 所述第一切片的属性仅允许具有相同 SST 的切片共用, 所述第二切片的属性的 SST 与所述第一切片的属性的 SST 相同; 或者

所述第二切片的属性仅允许具有相同 SST 的切片共用, 所述第一切片的属性的 SST 与所述第一切片的属性的 SST 相同; 或者

20 所述第一切片的属性仅允许具有相同 SD 的切片共用, 所述第二切片的属性的 SD 与所述第一切片的属性的 SD 相同; 或者

所述第二切片的属性仅允许具有相同 SD 的切片共用, 所述第一切片的属性的 SD 与所述第二切片的属性的 SD 相同; 或者

所述第二切片和所述第一切片映射到同一单网络切片选择辅助信息 S-NSSAI。

该通信装置 1100 可以应用于用户设备。

25 具体的, 所述收发单元 1103, 用于向第一网络设备发送第一请求消息, 所述第一请求消息用于请求接入第二切片; 接收来自所述第一网络设备的第一指示消息, 所述第一指示消息用于指示所述用户设备获取第二密钥;

所述处理单元 1102, 用于获取所述第二密钥, 所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

30 在一个实现方式中, 所述处理单元 1102 在获取所述第二密钥时, 具体用于获取第一密钥, 所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护; 根据所述第一密钥生成所述第二密钥。

35 在一个实现方式中, 所述处理单元 1102 在获取所述第二密钥时, 具体用于与所述第一网络设备重新进行认证; 若与所述第一网络设备重新认证成功, 则所述用户设备生成所述第二密钥。

在一个实现方式中, 所述收发单元 1103, 还用于接收来自所述第一网络设备的注册接受消息。

在第二个实施例中, 该通信装置 1100 可以应用于第一网络设备。

具体的, 所述收发单元 1103, 用于接收去注册请求消息, 或者发送去注册请求消息;

40 所述处理单元 1102, 用于删除所述用户设备的第三密钥, 所述第三切片为所述用户设

备最后接入的切片,所述第三密钥用于对所述第三切片的信息或/和所述用户设备接入所述第三切片时的信息进行安全保护。

在一个实现方式中,所述处理单元 1102 在删除所述用户设备的第三密钥时,具体用于若确定所述第三切片属性不允许与任意属性切片共用,删除所述用户设备的第三密钥。

5 在一个实现方式中,所述收发单元 1103,还用于若确定所述第三切片属性允许与其他属性切片共用,向所述用户设备发送去注册接受消息。

在一个实现方式中,所述收发单元 1103,还用于若未获取到所述第三切片的切片属性,向所述用户设备发送去注册接受消息。

该通信装置 1100 可以应用于用户设备。

10 具体的,所述收发单元 1103,用于发送去注册请求消息,或者接收去注册请求消息;所述处理单元 1102,用于删除所述用户设备的第三密钥,所述第三切片为所述用户设备最后接入的切片,所述第三密钥用于对所述第三切片的信息或/和所述用户设备接入所述第三切片时的信息进行安全保护。

15 在一个实现方式中,所述处理单元 1102 在删除所述用户设备的第三密钥时,具体用于若确定所述第三切片不允许与任意属性切片共用,删除所述用户设备的第三密钥。

在第三个实施例中,该通信装置 1100 可以应用于第二网络设备。

具体的,所述收发单元 1103,用于接收来自第一网络设备的重定向信息,所述重定向信息包括用户设备的第四切片的信息和/或所述用户设备请求接入的第五切片的信息;

20 所述处理单元 1102,用于若所述第四切片的信息与所述第五切片的信息不匹配,且所述第五切片具有隔离要求,对所述用户设备重新认证。

在一个实现方式中,所述处理单元 1102,还用于若所述第四切片的信息与所述第五切片的信息不匹配,且所述第五切片允许与其他任意属性切片共用,继续对所述用户设备进行认证。

25 可以理解的是,该通信装置用于上述切片隔离方法时的具体实现过程以及相应的有益效果,可以参考前述方法实施例中的相关描述,这里不再赘述。

如图 12 所示,为本申请提供的一种通信装置示意图,该通信装置可以是上述移动性管理网元、或终端设备。该通信装置 1200 包括:处理器 1202、通信接口 1203、存储器 1201。可选的,通信装置 1200 还可以包括通信线路 1204。其中,通信接口 1203、处理器 1202 以及存储器 1201 可以通过通信线路 1204 相互连接;通信线路 1204 可以是外设部件互连标准(peripheral component interconnect,简称 PCI)总线或扩展工业标准结构(extended industry standard architecture,简称 EISA)总线等。所述通信线路 1204 可以分为地址总线、数据总线、控制总线等。为便于表示,图 12 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。

35 处理器 1202 可以是一个 CPU,微处理器,ASIC,或一个或多个用于控制本申请方案程序执行的集成电路。

通信接口 1203,使用任何收发器一类的装置,用于与其他设备或通信网络通信,如以太网,RAN,无线局域网(wireless local area networks, WLAN),有线接入网等。

40 存储器 1201 可以是 ROM 或可存储静态信息和指令的其他类型的静态存储设备,RAM 或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(electrically erasable programmable read-only memory, EEPROM)、只读光盘(compact disc

read-only memory, CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过通信线路 1204 与处理器相连接。存储器也可以和处理器集成在一起。

其中,存储器 1201 用于存储执行本申请方案的计算机执行指令,并由处理器 1202 来控制执行。处理器 1202 用于执行存储器 1201 中存储的计算机执行指令,从而实现本申请上述实施例提供的终端设备的注册方法。

可选的,本申请实施例中的计算机执行指令也可以称之为应用程序代码,本申请实施例对此不作具体限定。

本申请实施例还提供了一种计算机存储介质,存储有计算机程序,该计算机程序被计算机执行时,可以使得所述计算机用于执行上述切片隔离方法。

本申请实施例还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机可以执行上述提供的切片隔离方法。

本申请实施例还提供了一种通信系统,所述通信系统包括第一网络设备和用户设备。可选的所述通信系统还包括第二网络设备。

本领域普通技术人员可以理解:本申请中涉及的第一、第二等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实施例的范围,也表示先后顺序。“和/或”,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。字符“/”一般表示前后关联对象是一种“或”的关系。“至少一个”是指一个或者多个。至少两个是指两个或者多个。“至少一个”、“任意一个”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、种),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。“多个”是指两个或两个以上,其它量词与之类似。此外,对于单数形式“a”,“an”和“the”出现的元素(element),除非上下文另有明确规定,否则其不意味着“一个或仅一个”,而是意味着“一个或多于一个”。例如,“a device”意味着对一个或多个这样的 device。

在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,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。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。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(例如同轴电缆、光纤、数字用户线(DSL))或无线(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括一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘(Solid State Disk, SSD))等。

本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器,数字信

号处理器，专用集成电路（ASIC），现场可编程门阵列（FPGA）或其它可编程逻辑装置，离散门或晶体管逻辑，离散硬件部件，或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器，可选地，该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现，例如数字信号处理器和微处理器，多个微处理器，一个或多个微处理器联合一个数字信号处理器核，或任何其它类似的配置来实现。

本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示例性地，存储媒介可以与处理器连接，以使得处理器可以从存储媒介中读取信息，并可以向存储媒介存写信息。可选地，存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于ASIC中。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管结合具体特征及其实施例对本申请进行了描述，显而易见的，在不脱离本申请的精神和范围的情况下，可对其进行各种修改和组合。相应地，本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明，且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包括这些改动和变型在内。

权利要求

1、一种切片隔离方法，其特征在于，包括：

第一网络设备获取用户设备的第一切片的信息；

5 若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

2、如权利要求 1 所述的方法，其特征在于，所述第一切片的信息包括所述第一切片的属性，所述第二切片的信息包括第二切片的属性；

10 若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥，包括：

若所述第一切片的属性与所述第二切片的属性不匹配，则所述第一网络设备获取所述第二密钥。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述第一网络设备获取第二密钥，包括：

15 所述第一网络设备根据所述第一密钥生成所述第二密钥，其中，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。

4、如权利要求 3 所述的方法，其特征在于，所述第一网络设备根据所述第一密钥生成所述第二密钥，包括：

20 若所述第一切片的隔离要求高于所述第二切片的隔离要求，所述第一网络设备根据所述第一密钥生成所述第二密钥。

5、如权利要求 1 或 2 所述的方法，其特征在于，所述第一网络设备获取第二密钥，包括：

所述第一网络设备对所述用户设备重新进行认证；

25 若第一网络设备对所述用户设备重新认证成功，则所述第一网络设备生成所述第二密钥。

6、如权利要求 5 所述的方法，其特征在于，所述第一网络设备对所述用户设备进行重新认证，包括：

若所述第一切片的隔离要求低于所述第二切片的隔离要求，所述第一网络设备对所述用户设备重新进行网络认证。

30 7、如权利要求 2-6 任一项所述的方法，其特征在于，所述第一切片的属性与所述第二切片的属性不匹配，包括：

所述第一切片的属性或第二切片的属性不允许与其他任意属性的切片共用；或者

所述第一切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 不同；或者

35 所述第二切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第一切片的属性的 SST 与所述第二切片的属性的 SST 不同；或者

所述第一切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 不同；或者

所述第二切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 不同。

8、如权利要求 2-7 任一项所述的方法，其特征在于，还包括：

5 若所述第一切片的属性与所述第二切片的属性匹配，所述第一网络设备向所述用户设备发送注册接受消息。

9、如权利要求 8 所述的方法，其特征在于，所述第一切片的属性与所述第二切片的属性匹配，包括：

所述第一切片的属性或第二切片的属性允许与其他任意属性的切片共用；或者

10 所述第一切片的属性仅允许具有相同 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

所述第二切片的属性仅允许具有相同 SST 的切片共用，所述第一切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

所述第一切片的属性仅允许具有相同 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 相同；或者

15 所述第二切片的属性仅允许具有相同 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 相同；或者

所述第二切片和所述第一切片映射到同一单网络切片选择辅助信息 S-NSSAI。

10、一种切片隔离方法，其特征在于，包括：

20 用户设备向第一网络设备发送第一请求消息，所述第一请求消息用于请求接入第二切片；

所述用户设备接收来自所述第一网络设备的第一指示消息，所述第一指示消息用于指示所述用户设备获取第二密钥；

所述用户设备获取所述第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备接入所述第二切片时的信息进行安全保护。

25 11、如权利要求 10 所述的方法，其特征在于，所述用户设备获取所述第二密钥，包括：

所述用户设备获取第一密钥，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护；

所述用户设备根据所述第一密钥生成所述第二密钥。

30 12、如权利要求 10 所述的方法，其特征在于，所述用户设备获取所述第二密钥，包括：

所述用户设备与所述第一网络设备重新进行认证；

若所述用户设备与所述第一网络设备重新认证成功，则所述用户设备生成所述第二密钥。

13、如权利要求 10-12 任一项所述的方法，其特征在于，还包括：

35 所述用户设备接收来自所述第一网络设备的注册接受消息。

14、一种通信装置，其特征在于，包括收发单元和处理单元；

所述收发单元，用于获取用户设备的第一切片的信息；

40 所述处理单元，用于若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则获取第二密钥，所述第二密钥用于对所述第二切片的信息或/和所述用户设备

接入所述第二切片时的信息进行安全保护。

15、如权利要求 14 所述的装置，其特征在于，所述第一切片的信息包括所述第一切片的属性，所述第二切片的信息包括第二切片的属性；

5 所述处理单元在若所述第一切片的信息与所述用户设备请求接入的第二切片的信息不匹配，则所述第一网络设备获取第二密钥时，具体用于若所述第一切片的属性与所述第二切片的属性不匹配，则获取所述第二密钥。

16、如权利要求 14 或 15 所述的装置，其特征在于，所述处理单元在获取第二密钥时，具体用于根据所述第一密钥生成所述第二密钥，其中，所述第一密钥用于对所述第一切片的信息或/和所述用户设备接入所述第一切片时的信息进行安全保护。

10 17、如权利要求 16 所述的装置，其特征在于，所述处理单元在根据所述第一密钥生成所述第二密钥时，具体用于若所述第一切片的隔离要求高于所述第二切片的隔离要求，根据所述第一密钥生成所述第二密钥。

15 18、如权利要求 14 或 15 所述的装置，其特征在于，所述处理单元在获取第二密钥时，具体用于：对所述用户设备重新进行认证；若对所述用户设备重新认证成功，则生成所述第二密钥。

19、如权利要求 18 所述的装置，其特征在于，所述处理单元在对所述用户设备进行重新认证时，具体用于若所述第一切片的隔离要求低于所述第二切片的隔离要求，对所述用户设备重新进行网络认证。

20 20、如权利要求 15-19 任一项所述的装置，其特征在于，所述第一切片的属性与所述第二切片的属性不匹配，包括：

所述第一切片的属性或第二切片的属性不允许与其他任意属性的切片共用；或者

所述第一切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 不同；或者

25 所述第二切片的属性仅允许具有相同业务类型 SST 的切片共用，所述第一切片的属性的 SST 与所述第二切片的属性的 SST 不同；或者

所述第一切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 不同；或者

所述第二切片的属性仅允许具有相同切片差异化因素 SD 的切片共用，所述第一切片的属性的 SD 与所述第二切片的属性的 SD 不同。

30 21、如权利要求 15-20 任一项所述的装置，其特征在于，所述收发单元，还用于若所述第一切片的属性与所述第二切片的属性匹配，向所述用户设备发送注册接受消息。

22、如权利要求 21 所述的装置，其特征在于，所述第一切片的属性与所述第二切片的属性匹配，包括：

所述第一切片的属性或第二切片的属性允许与其他任意属性的切片共用；或者

35 所述第一切片的属性仅允许具有相同 SST 的切片共用，所述第二切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

所述第二切片的属性仅允许具有相同 SST 的切片共用，所述第一切片的属性的 SST 与所述第一切片的属性的 SST 相同；或者

40 所述第一切片的属性仅允许具有相同 SD 的切片共用，所述第二切片的属性的 SD 与所述第一切片的属性的 SD 相同；或者

所述第二切片的属性仅允许具有相同 SD 的切片共用，所述第一切片的属性的 SD 与
所述第二切片的属性的 SD 相同；或者

所述第二切片和所述第一切片映射到同一单网络切片选择辅助信息 S-NSSAI。

23、一种通信装置，其特征在于，包括收发单元和处理单元；

5 所述收发单元，用于向第一网络设备发送第一请求消息，所述第一请求消息用于请求
接入第二切片；接收来自所述第一网络设备的第一指示消息，所述第一指示消息用于指示
所述用户设备获取第二密钥；

所述处理单元，用于获取所述第二密钥，所述第二密钥用于对所述第二切片的信息或
/和所述用户设备接入所述第二切片时的信息进行安全保护。

10 24、如权利要求 23 所述的装置，其特征在于，所述处理单元在获取所述第二密钥时，
具体用于获取第一密钥，所述第一密钥用于对所述第一切片的信息进行安全保护；根据所
述第一密钥生成所述第二密钥。

25、如权利要求 23 所述的装置，其特征在于，所述处理单元在获取所述第二密钥时，
具体用于与所述第一网络设备重新进行认证；若与所述第一网络设备重新认证成功，则所
15 述用户设备生成所述第二密钥。

26、如权利要求 23-25 任一项所述的装置，其特征在于，所述收发单元，还用于接收
来自所述第一网络设备的注册接受消息。

27、一种计算机可读存储介质，其特征在于，包括程序或指令，当所述程序或指令在
计算机上运行时，如权利要求 1-9 任一项所述的方法或者如权利要求 10-13 任一项所述
20 的方法被执行。

28、一种通信系统，其特征在于，所述通信系统包括执行如权利要求 1-9 任一项所述
方法的第一网络设备，以及执行如权利要求 10-13 任一项所述方法的设备。

25