

通信方法及其装置

本申请要求于 2019 年 4 月 28 日提交中国专利局、申请号为 201910351464.X、申请名称为“通信方法及其装置”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

本申请实施例涉及通信技术领域，具有涉及一种通信方法及其装置。

背景技术

随着通信技术的发展，第五代移动通信（5th-generation, 5G）系统应运而生。在 5G 系统中除了沿用长期演进（long term evolution, LTE）系统中的用户面加密保护之外，还引入用户面完整性保护，用户面完整性保护即保护数据在用户面传输过程中的完整性。并且，5G 系统中的用户面加密保护和用户面完整性保护按照是否需要来确定是否开启。

5G 系统还提出一种区别于空闲（idle）态和连接（connected）态的新状态，inactive 态，又称为去活动态、第三态、非激活态或去激活态等。在空闲态时，用户设备（user equipment, UE）、基站和核心网都进入空闲态，UE 和基站之前使用的接入层（access stratum, AS）安全上下文都会被删除，基站会将 UE 的上下文信息删除，UE 的上下文信息包括 UE 使用的 AS 安全上下文。在连接时，UE、基站和核心网都处于连接态，此时 UE 和基站正在使用 AS 安全上下文。在 inactive 态下，UE 连接的基站会保存 UE 的上下文信息，该上下文信息包括 UE 的接入层（access stratum, AS）安全上下文。对于核心网而言，即使 UE 处于 inactive 态，也认为 UE 还是处于连接态。因此在 UE 从连接态进入 inactive 态之后，基站也进入 inactive 态，但是核心网还是连接态。UE 进入 inactive 态的好处在于，可以使 UE 快速恢复连接态，从而减少通信中断的时延。

inactive 场景可以涉及两个过程：UE 和基站可以从连接态进入 inactive 态，可以将该过程称为推迟（suspend）过程；UE 和基站可以从 inactive 态进入连接态，可以将该过程称为恢复（resume）过程。

虽然 5G 系统引入用户面安全保护，即用户面加密保护和用户面完整性保护，但是该用户面安全保护适应于连接态，在 inactive 场景下，并没有涉及用户面安全保护，更没有涉及用户面按需安全保护。因此，如何确保 inactive 场景下的用户面安全是亟待解决的技术问题。

发明内容

本申请实施例提供一种通信方法及其装置，可以确保 inactive 场景下的用户面安全，从而保证 inactive 场景下用户面数据传输的安全性。

本申请实施例第一方面提供一种通信方法，包括：

目标接入网设备在接收到来自用户终端的无线资源控制（radio resource control, RRC）恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与该用户终端之间的第一用户面安全保护方法；确定与该用户终端之间的第一用户面安全密钥；在接收到来自该用户终端的第一上行用户面数据时，根据该第一用户面安全密钥和第一用户面安全保护方

法对第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；发送该上行用户面数据，具体向核心网中的用户面功能发送该上行用户面数据。

其中，目标接入网设备为用户终端从第三态进入连接态的过程中，将与用户终端建立 RRC 连接的接入网设备，源接入网设备为使用户终端从连接态进入第三态，向用户终端发送 RRC 释放消息的接入网设备，即为进入第三态之前，与用户终端建立过 RRC 连接的接入网设备。

本申请实施例第一方面，目标接入网设备接收到 RRC 恢复消息时，表明用户终端将从第三态进入连接态，将与目标接入网设备建立 RRC 连接，此时，目标接入网设备根据上下文信息获取响应所携带的信息确定第一用户面安全保护方法，确定第一用户面安全密钥，根据第一用户面安全保护方法以及第一用户面安全密钥对第一上行用户面数据进行解安全保护，对下行用户面数据进行用户面安全保护，以确保 resume 过程中用户面数据传输的安全性。

在一种可能的实现方式中，上述上下文信息获取响应包括该用户终端的用户面安全策略，目标接入网设备直接根据该用户面安全策略确定与该用户终端之间的第一用户面安全保护方法，具体可根据该用户面安全策略以及目标接入网设备的自身情况确定该第一用户面安全保护方法。目标接入网设备可根据第一用户面安全保护方法激活用户面安全，第一用户面安全保护方法是根据该用户面安全策略和自身情况确定的，那么激活的用户面安全不仅满足用户面安全策略的需求，还满足当前环境需求。

在一种可能的实现方式中，上述上下文信息获取响应包括该用户终端的用户面安全策略和第一指示信息，该第一指示信息用于指示该用户终端与源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；目标接入网设备直接将该第一指示信息所指示的第二用户面安全保护方法确定为第一用户面安全保护方法，或在确定第二用户面安全保护方法可用的情况下，将第二用户面安全保护方法确定为第一用户面安全保护方法。第二用户面安全保护方法为从连接态进入第三态之前所使用的用户面安全保护方法，将该用户面安全保护方法作为目标接入网设备与用户终端之间的用户面安全保护方法，使得从连接态进入第三态之前与从第三态进入连接态之后，使用的用户面安全保护方法一致。

在一种可能的实现方式中，上述上下文信息获取响应包括该用户终端的用户面安全策略和第一指示信息，目标接入网设备在确定第二用户面安全保护方法不可用或不使用第二用户面安全保护方法的情况下，根据该用户面安全策略确定第一用户面安全保护方法，使得激活的用户面安全不仅满足用户面安全策略的需求，还满足当前环境需求。或者，在该情况下，目标接入网设备向用户终端发送 RRC 消息，该 RRC 消息用于触发用户终端重新建立与目标接入网设备之间的 RRC 连接，在建立 RRC 连接的过程中，目标接入网设备与用户终端重新协商用户面安全保护方法，以确定出第一用户面安全保护方法，这样可以最大限度的兼容现有技术。

在一种可能的实现方式中，目标接入网设备在激活用户安全之后，可将激活结果告知会话管理网元，以便会话管理网元获知所使用的第一用户面安全保护方法。

在一种可能的实现方式中，目标接入网设备在确定第一用户面安全保护方法之后，可根据该第一用户面安全保护方法确定与该用户终端之间的第一用户面安全密钥，以便目标

接入网设备根据第一用户面安全保护方法和第一用户面安全密钥对第一上行用户面数据进行解用户面安全保护，对下行用户面数据进行用户面安全保护。

在一种可能的实现方式中，目标接入网设备可通过 RRC 恢复消息向用户终端发送第二指示信息，即将第二指示信息携带在 RRC 恢复消息中，该第二指示信息用于指示目标接入网设备确定的第一用户面安全保护方法，以使用户终端根据第二指示信息激活用户面安全。

若目标接入网设备根据第一指示信息确定第一用户面安全保护方法，在用户终端在 suspend 过程中保存有第一指示信息的情况下，上述 RRC 恢复消息可不携带第二指示信息，用户终端直接根据第一指示信息激活用户面安全。

目标接入网设备可在发送 RRC 恢复消息之前或之后或同时激活用户面安全。

本申请实施例第二方面提供一种目标接入网设备，该目标接入网设备具有实现第一方面提供方法的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。

在一种可能实现的方式中，该目标接入网设备包括：收发单元和处理单元，处理单元，在收发单元接收到来自用户终端的 RRC 恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与该用户终端之间的第一用户面安全保护方法；确定与该用户终端之间的第一用户面安全密钥；在收发单元接收到来自该用户终端的第一上行用户面数据时，根据该第一用户面安全密钥和第一用户面安全保护方法对第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；收发单元，用于发送该上行用户面数据，具体向核心网中的用户面功能发送该上行用户面数据。

在一种可能实现的方式中，该目标接入网设备包括：处理器、收发器和存储器，其中，收发器用于接收和发送信息，存储器中存储计算机程序，计算机程序包括程序指令，处理器通过总线与存储器和收发器连接，处理器执行存储器中存储的程序指令，以使该用户终端执行以下操作：在收发器接收到来自用户终端的无线资源控制（radio resource control, RRC）恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与该用户终端之间的第一用户面安全保护方法；确定与该用户终端之间的第一用户面安全密钥；在收发器接收到来自该用户终端的第一上行用户面数据时，根据该第一用户面安全密钥和第一用户面安全保护方法对第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；控制收发器发送该上行用户面数据，具体向核心网中的用户面功能发送该上行用户面数据。

基于同一发明构思，由于该目标接入网设备解决问题的原理以及有益效果可以参见第一方面所述的方法以及所带来的有益效果，因此该装置的实施可以参见方法的实施，重复之处不再赘述。

本申请实施例第三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计算机程序，计算机程序包括程序指令，程序指令当被处理器执行时使得处理器执行上述第一方面所述的方法。

本申请实施例第四方面提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

本申请实施例第五方面提供一种通信方法，包括：

用户终端在向目标接入网设备发送 RRC 恢复请求之后，确定与该目标接入网设备之间

的第一用户面安全保护方法；确定与该目标接入网设备之间的第一用户面安全密钥；根据第一用户面安全保护方法和第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；向该目标接入网设备发送该第一用户面数据。

对于下行传输，用户终端在接收到来自该目标接入网设备的第一下行用户面数据时，根据第一用户面安全保护方法和第一用户面安全密钥，对第一下行用户面数据进行解用户面安全保护，获得下行用户面数据。

本申请实施例第五方面，用户终端在确定第一用户面安全保护方法以及第一用户面安全密钥之后，根据第一用户面安全保护方法和第一用户面安全密钥对上行用户面数据进行用户面安全保护，对下行用户面数据进行解用户面安全保护，以确保 resume 过程中用户面数据传输的安全性。

在一种可能的实现方式中，用户终端接收来自目标接入网设备的 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息，该第二指示信息用于指示第一用户面安全保护方法，用户终端直接根据第二指示信息确定与目标接入网设备之间的第一用户面安全保护方法，以便根据第一用户面安全保护方法激活用户面安全。

在一种可能的实现方式中，用户终端在接收到携带第二指示信息的 RRC 恢复消息之后，释放 RRC 连接。用户终端可通过向目标接入网设备报错的方式，来释放 RRC 连接，也可由目标接入网设备主动发起释放 RRC 连接的流程或发起重新建立 RRC 连接的流程。

在一种可能的实现方式中，用户终端在接收到来自目标接入网设备的 RRC 释放消息之后，用户终端从连接态进入第三态，并保存第一指示信息，该第一指示信息用于指示用户终端和源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法。用户终端保存第一指示信，以使用户终端从连接态进入第三态之前，与从第三态进入连接态之后，使用相同的用户面安全保护方法。

在一种可能的实现方式中，在用户终端保存了第一指示信息的情况下，用户终端可直接将第一指示信息指示的第二用户面安全保护方法确定为第一用户面安全保护方法，以使用户终端从连接态进入第三态之前，与从第三态进入连接态之后，使用相同的用户面安全保护方法。

在一种可能的实现方式中，用户终端接收来自目标接入网设备的 RRC 恢复消息，该 RRC 恢复消息不包括第二指示信息，该第二指示信息用于指示目标接入网设备确定的用户面安全保护方法。RRC 恢复消息不携带第二指示信息，默认用户终端和目标接入网设备根据第一指示信息确定第一用户面安全保护方法并激活用户面安全，在用户终端保存了第一指示信息的情况下，目标接入网设备无需告知用户终端，可节省信令开销。

在一种可能的实现方式中，用户终端在确定第一用户面安全保护方法的情况下，根据该第一用户面安全保护方法确定第一用户面安全密钥。可包括两种情况，一种为用户终端在发送 RRC 恢复请求之后，生成所有的用户面安全密钥，然后根据第一用户面安全保护方法从所有的用户面安全密钥中确定出第一用户面安全密钥；另一种为用户终端直接根据第一用户面安全保护方法确定第一用户面安全密钥。

在一种可能的实现方式中，用户终端在接收到来自目标接入网设备的 RRC 释放消息之后，保存第二用户面安全密钥，该第二用户面安全密钥为用户终端与源接入网设备从连接

态进入第三态之前，所使用的用户面安全密钥。用户终端保存第二用户面安全密钥，以便用户终端在发送 RRC 恢复请求之后，可立即或快速使用第二用户面安全密钥和第二用户面安全保护方法对上行用户面数据进行用户面安全保护。

在一种可能的实现方式中，在用户终端保存第二用户面安全密钥的情况下，在 resume 过程中确定第一用户面安全密钥之后，将第二用户面安全密钥删除，以避免用户终端不知道使用哪个用户面安全密钥。

在一种可能的实现方式中，用户终端在接收到来自目标接入网设备的 RRC 恢复消息之前，可激活用户面安全，向目标接入网设备发送第一上行用户面数据。该种方式下，用户终端可能使用第二用户面安全保护方法和第二用户面安全密钥对上行用户面数据进行用户面安全保护，使得用户终端在需要发送上行用户面数据时，可快速对用户面数据进行用户面安全保护。

在一种可能的实现方式中，用户终端在接收到来自目标接入网设备的 RRC 恢复消息之后，可激活用户面安全，向目标接入网设备发送第一上行用户面数据。该种方式下，用户终端可能使用新确定的用户安全保护方法和新确定的用户面安全密钥对上行用户面数据进行用户面安全保护。

本申请实施例第六方面提供一种用户终端，该用户终端具有实现第五方面提供方法的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块。

在一种可能实现的方式中，该用户终端包括：收发单元和处理单元，处理单元，用于在收发单元向目标接入网设备发送 RRC 恢复请求之后，确定与该目标接入网设备之间的第一用户面安全保护方法；确定与该目标接入网设备之间的第一用户面安全密钥；根据第一用户面安全保护方法和第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；收发单元，用于向该目标接入网设备发送该第一用户面数据。

在一种可能实现的方式中，该用户终端包括：处理器、收发器和存储器，其中，收发器用于接收和发送信息，存储器中存储计算机程序，计算机程序包括程序指令，处理器通过总线与存储器和收发器连接，处理器执行存储器中存储的程序指令，以使该用户终端执行以下操作：在控制收发器向目标接入网设备发送 RRC 恢复请求之后，确定与该目标接入网设备之间的第一用户面安全保护方法；确定与该目标接入网设备之间的第一用户面安全密钥；根据第一用户面安全保护方法和第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；控制收发器向该目标接入网设备发送该第一用户面数据。

基于同一发明构思，由于该用户终端解决问题的原理以及有益效果可以参见第五方面所述的方法以及所带来的有益效果，因此该装置的实施可以参见方法的实施，重复之处不再赘述。

本申请实施例第七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计算机程序，计算机程序包括程序指令，程序指令当被处理器执行时使得处理器执行上述第五方面所述的方法。

本申请实施例第八方面提供一种包含指令的计算机程序产品，当其在计算机上运行时，

使得计算机执行上述第五方面所述的方法。

本申请实施例第九方面提供一种通信系统，包括第一方面提供的目标接入网设备以及第二方面提供的用户终端。

附图说明

为了更清楚地说明本申请实施例或背景技术中的技术方案，下面将对本申请实施例或背景技术中所需要使用的附图进行说明。

图 1 为用户面按需安全过程的流程示意图；

图 2 为目前 suspend 过程的流程示意图；

图 3 为目前 resume 过程的流程示意图；

图 4 为应用本申请实施例的网络架构示意图；

图 5-1 为本申请实施例一提供的通信方法的流程示意图；

图 5-2 为本申请实施例二提供的通信方法的流程示意图；

图 6 为本申请实施例三提供的通信方法的流程示意图；

图 7-1 为本申请实施例四提供的通信方法的流程示意图；

图 7-2 为本申请实施例五提供的通信方法的流程示意图；

图 7-3 为本申请实施例六提供的通信方法的流程示意图；

图 8-1 为本申请实施例七提供的通信方法的流程示意图；

图 8-2 为本申请实施例八提供的通信方法的流程示意图；

图 9-1 为本申请实施例九提供的通信方法的流程示意图；

图 9-2 为本申请实施例十提供的通信方法的流程示意图；

图 10 为本申请实施例提供的路径切换流程的示意图；

图 11 为本申请实施例提供的通信装置的逻辑结构示意图；

图 12 为本申请实施例提供的通信装置的实体结构简化示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。其中，在本申请的描述中，除非另有说明，“/”表示前后关联的对象是一种“或”的关系，例如，A/B 可以表示 A 或 B；本申请中的“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。并且，在本申请的描述中，除非另有说明，“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。另外，为了便于清楚描述本申请实施例的技术方案，在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同。

此外，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。

下面将对本申请实施例涉及的名词或术语进行介绍：

用户面安全策略，包括用户面加密保护策略和用户面完整性保护策略。用户面加密保护策略存在三种可能的值，分别为 not needed、preferred 和 required，用户面完整性保护策略存在三种可能的值，分别为 not needed、preferred 和 required。其中，not needed 表示不需要开启，preferred 表示可以开启也可以不开启，required 表示必须开启。上述三种可能的值可以采用 2 比特（bit）来指示，例如 00 指示不需要开启，01 指示可以开启也可以不开启，11 指示必须开启。用户面加密保护策略和用户面完整性保护策略具体采用何种方式对三种可能的值进行指示，在本申请实施例中不作限定。

用户面加密保护即保护数据在传输过程中的机密性（因此又可以被称作用户面机密性保护），机密性是指无法被直接看出真实内容。用户面完整性保护即保护数据在用户面传输过程中的完整性，完整性是指数据是原始的没有被篡改的。

用户面安全保护方法，指的是用户终端侧或基站侧的用户面加密保护是否开启和/或用户面完整性保护是否开启。

安全算法，可以包括用户面安全算法（即用户面使用的安全算法）和信令面安全算法（即信令面使用的安全算法）。用户面使用的安全算法用于保护用户面数据，可以包括用户面加密算法和用户面完整性算法。信令面使用的安全算法用于保护信令，可以包括信令面加密算法和信令面完整性算法。用户面使用的安全算法与信令面使用的安全算法可以相同，也可以不相同。相同的具体含义是，如果用户面完整性保护开启，则用户面使用的完整性算法和信令面使用的完整性算法相同；如果用户面加密保护开启，则用户面使用的加密算法和信令面使用的加密算法相同。信令面使用的安全算法和用户面使用的安全算法有不一样的即不同，例如用户面使用加密算法为加密算法 A，信令面使用的加密算法为加密算法 B，但是用户面和信令面都使用完整性算法 C，此时用户面使用的安全算法和信令面使用的安全算法不相同。

安全密钥，可以包括用户面安全密钥和信令面安全密钥。其中，用户面安全密钥用于保护用户面数据，可以包括用户面加密密钥和用户面完整性保护密钥。信令面安全密钥用于保护信令，例如可以是保护无线资源控制（radio resource control, RRC）信令的密钥，即 RRC 密钥，RRC 密钥可以包括 RRC 加密密钥和 RRC 完整性保护密钥。

安全保护，对于执行安全功能的节点而言，用户面/信令面安全算法和用户面/信令面安全密钥一起用于保护用户面数据。具体地，使用加密密钥和加密算法对用户面/信令面数据进行加密保护；使用完整性保护密钥和完整性保护算法对用户面/信令面数据进行完整性保护。本申请实施例不限定加密保护和完整性保护的顺序关系，即可以先对用户面/信令面数据进行加密保护，再做完整性保护；也可以先对用户面/信令面进行完整性保护，再对用户面/信令面数据进行加密保护。当然，用户面和信令面可以不使用相同的执行顺序。

解密安全保护，对于执行安全功能的节点而言，用户面/信令面安全算法和用户面/信令面安全密钥一起用于获得原始的用户面数据。具体地，使用加密密钥和加密算法对加密的用

户面/信令面数据进行解密；使用完整性保护密钥和完整性保护算法对用户面数据进行完整性保护验证。本发明实施例不限定解密和验证完整性保护的顺序。但需要理解的是，如果是用户面/信令面数据先被加密保护，再被完整性保护，则解安全保护是先验证完整性保护、再对加密后的用户面数据进行解密；如果用户面/信令面数据先被完整性保护，再被加密，则解安全保护的顺序为先解密加密后的数据，再进行完整性保护验证。

激活用户面/信令面安全，指的是在确定出用户面/信令面安全保护方法的情况下，可以开始使用用户面/信令面安全算法和用户面/信令面安全密钥来激活该用户面/信令面安全，即可以开始使用用户面/信令面安全保护方法、用户面/信令面安全算法和用户面/信令面安全密钥来对将要传输的用户面数据/信令进行安全保护。例如，确定的用户面安全保护方法为开启用户面加密保护+不开启用户面完整性保护，用户面加密算法为加密算法 A，用户面加密密钥为密钥 K，则对于将要传输的用户面数据，采用加密算法 A 和密钥 K 对该用户面数据进行用户面加密保护。激活用户面安全保护方法可以达到的效果是执行激活用户面安全的节点可以开始对用户面数据进行安全保护和开始对用户面数据进行解安全保护。需要理解的是，安全保护和解安全保护这两个动作可能是进一步分开激活的。比如基站在发送安全激活消息后，则基站激活解安全保护；基站再收到安全激活确认消息后，基站激活安全保护。

请参见图 1，为用户面按需安全过程的流程示意图，可以包括如下步骤：

步骤 101，UE 向基站发送协议数据单元（protocol data unit，PDU）会话建立请求消息。相应的，基站接收来自 UE 的 PDU 会话建立请求消息。

其中，PDU 会话建立请求消息包括 PDU 会话标识（identity，ID）、数据网络名称（data network name，DNN）和网络切片选择辅助信息（network slice select auxiliary information，NSSAI）等信息。

步骤 102，基站通过接入和移动性管理功能（access and mobility management function，AMF）向会话管理功能（session management function，SMF）发送 PDU 会话建立请求。

具体的，基站先向 AMF 发送 PDU 会话建立请求，然后 AMF 向 SMF 发送 PDU 会话建立请求。图 1 中省略了基站与 SMF 之间的 AMF。

步骤 103，SMF 获取用户面安全策略。

SMF 可以从统一数据管理（unified data management，UDM）中获得用户面安全策略，也可以从 SMF 的本地配置信息中获得用户面安全策略。

其中，SMF 获取的用户面安全策略为 UE 的用户面安全策略，具体可以为针对该 PDU 会话的用户面安全策略。

步骤 104，SMF 向基站发送用户面安全策略，即 SMF 将其获取的用户面安全策略发送至基站。相应的，基站接收来自 SMF 的用户面安全策略。

SMF 将用户面安全策略发送给 AMF，AMF 可通过 N2 消息向基站发送用户面安全策略，即将用户面安全策略携带在 N2 消息中。

基站在接收到该用户面安全策略时，可对其进行保存。基站在保存该用户面安全策略时，还保存该用户面安全策略对应的 PDU 会话标识，即 PDU 会话 ID。

步骤 105，基站根据用户面安全策略激活用户面安全。

基站根据用户面安全策略激活基站与 UE 之间的用户面安全。例如，用户面安全策略所包括的用户面加密保护策略为 **required**，用户面完整性保护策略为 **required**，则基站开启用户面加密保护和用户面完整性保护，并采用用户面加密密钥、用户面完整性保护密钥以及用户面安全算法对与 UE 之间的用户面数据进行加密保护和完整性保护，或进行解密和验证。再例如，用户面安全策略所包括的用户面加密保护策略为 **required**，用户面完整性保护策略为 **not needed**，则基站开启用户面加密保护，不开启用户面完整性保护，并采用用户面加密密钥以及用户面安全算法对与 UE 之间的用户面数据进行加密保护或解密。

在用户面加密保护策略或用户面完整性保护策略是 **preferred** 的情况下，可选的，基站将用户面安全激活结果（**security result**）发送给 SMF。若基站生成 **security result**，则基站保存 **security result**。

步骤 106，基站向 UE 发送 RRC 连接重配置消息。相应的，UE 接收来自基站的 RRC 连接重配置消息。

其中，RRC 连接重配置消息包括用户面激活指示信息，该用户面激活指示信息包括用户面加密保护激活指示信息和/或用户面完整性保护激活指示信息，用户面加密保护激活指示信息用于指示是否开启用户面加密保护，用户面完整性保护激活指示信息用于指示是否开启用户面完整性保护。具体地，若用户面激活指示信息包括的用户面完整性保护激活指示信息为 **enable**，不包括用户面加密保护激活指示信息，则 UE 可确定开启用户面加密保护，开启用户面完整性保护。若用户面激活指示信息包括的用户面加密保护激活指示信息为 **disable**，不包括用户面完整性保护激活指示信息，则 UE 可确定不开启用户面加密保护，不开启用户面完整性保护。若用户面激活指示信息包括的用户面完整性保护激活指示信息为 **enable**，用户面加密保护激活指示信息为 **disable**，则 UE 可确定不开启用户面加密保护，开启用户面完整性保护。若用户面激活指示信息不包括用户面完整性保护激活指示信息，也不包括用户面加密保护激活指示信息，则 UE 可确定不开启用户面完整性保护，开启用户面加密保护。

步骤 107，UE 激活用户面安全。UE 根据步骤 6 所携带的用户面激活指示信息激活 UE 与基站之间的用户面安全，以便对与基站之间的用户面数据进行安全保护或解安全保护。

步骤 108，UE 向基站发送 RRC 连接重配置确认（**ack**）消息。相应的，基站接收来自 UE 的 RRC 连接重配置确认消息。

在图 1 所示的流程中，在连接态场景下，基站从 SMF 获取用户面安全策略，激活与 UE 之间的用户面安全，向 UE 发送指示，以便 UE 根据指示激活与基站之间的用户面安全，从而保证 UE 与基站之间的用户面数据的机密性和完整性。

请参见图 2，为目前 **suspend** 过程的流程示意图，可包括如下步骤：

步骤 201，基站获取并保存 UE 的用户面安全策略。步骤 201 获取并保存的 UE 的用户面安全策略，可以为基站在建立 PDU 会话的过程中，从 SMF 获取的针对该 PDU 会话的用户面安全策略，即为图 1 所示流程中步骤 104 中传输的用户面安全策略。也可以为基站从切换流程中获得的。

可选的，基站还保存 **security result**。**security result** 的作用是，表示用户面安全策略中的用户面加密保护策略和/或用户面完整性保护策略为 **preferred** 的时候，是否执行了用户面

安全策略 (3GPP TS 38.413 版本 f30 原文: indicates whether the security policy indicated as "preferred" in the Security Indication IE is performed or not.)。security result 的生成和使用都是可选的: 用户面安全策略中的用户面加密保护策略和/或用户面完整性保护策略为 preferred 的时候才需要生成; security result 可选的在一些流程中使用, 比如需要基站发送 security result 给 SMF, 或者在切换流程中发送给目标基站, 因此 security result 保存是可选的。security result 包括用户面完整性保护结果 (integrity protection result) 和用户面加密保护结果 (confidentiality protection result)。其值域为: ENUMERATED (performed, not performed, ...)。其作用是指示当前的 PDU 连接有没有执行用户面加密保护和有没有执行用户面完整性保护。

步骤 202, 基站向 UE 发送 RRC 释放 (release) 消息。相应的, UE 接收来自基站的 RRC 释放消息。

当基站和 UE 需要从连接态进入 inactive 态时, 基站向 UE 发送 RRC 释放消息。RRC 释放消息包括一个指示信息, 该指示信息用于指示 UE 释放 RRC 连接, 但不进入空闲态, 而是进入 inactive 态。这个指示信息就是 suspend 配置信息。RRC 释放消息还包括第三态无线网络临时标识 (inactive-radio network temporary identifier, I-RNTI) 和下一跳链路级数 (next hop chaining counter parameter, NCC) 值。I-RNTI 用于在基站侧标识 inactive 态的 UE, 以便 UE 从 inactive 态进入连接态时, 可以根据 I-RNTI 查找 UE 的上下文信息。NCC 值用于在 UE 回到连接态的过程中生成新的 KgNB*。

步骤 203, 基站在发送 RRC 释放消息之后, 删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥, 保存 RRC 完整性保护密钥。换言之, 基站在发送 RRC 释放消息之后, 删除用户面安全密钥和 RRC 加密密钥, 只保存 RRC 完整性保护密钥。

同时, 基站还保存 RRC 释放消息所包括的 I-RNTI, 以便 UE 从 inactive 进入连接态时, 基站可以根据 I-RNTI 查找 UE 的上下文信息。基站也会保存用户面安全策略。可选的保存 security result。

步骤 204, UE 在接收到 RRC 释放消息之后, 对 RRC 释放消息的完整性保护进行验证, UE 采用 RRC 完整性保护密钥对 RRC 释放消息进行验证, 若验证成功, 则 UE 存储 RRC 释放消息所包括的 NCC 值, 并删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥, 只保存 RRC 完整性保护密钥。换言之, UE 在验证成功的情况下, 删除用户面安全密钥和 RRC 加密密钥, 只保存 RRC 完整性保护密钥。UE 会根据 NCC 的值, 确定是否保留当前使用的 KgNB。具体确定方法与本申请实施例无关, 因此在这里不做过多阐述。

同时, UE 还保存 RRC 释放消息所包括的 I-RNTI。

图 2 所示的目前 suspend 过程涉及对安全密钥的处理, 在基站侧涉及用户面安全保护方法的处理并不是很清晰, security result 的生成、使用和保存是可选的; 在 UE 侧并未涉及对用户面安全保护方法的处理, 并且该过程中基站和 UE 均删除了用户面加密密钥和用户面完整保护密钥。鉴于此, 本申请实施例明确 suspend 过程中如何对用户面安全保护方法进行处理, 具体可参见实施例一至实施例三。

请参见图 3, 为目前 resume 过程的流程示意图。UE 在 suspend 过程所涉及的基站, 与 UE 在 resume 过程中建立 RRC 连接的基站可能是同一个基站, 也可能是不同的基站。图 3

以不同的基站为例，假设 UE 从连接态进入 inactive 态所涉及的基站是源基站，从 inactive 态进入连接态，与 UE 建立 RRC 连接的基站是目标基站。图 3 所述的流程可包括如下步骤：

步骤 301，UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume 消息认证代码标识（message authentication code-identify，MAC-I）。

步骤 302，UE 向目标基站发送 RRC 恢复（resume）请求（request）。相应的，目标基站接收来自 UE 的 RRC 恢复请求。

其中，RRC 恢复请求包括 I-RNTI 和 resume MAC-I。I-RNTI 可以是 UE 在 suspend 过程所保存的 I-RNTI。

UE 在发送 RRC 恢复请求之后，生成新的 KgNB*，并用新的 KgNB*生成 RRC 密钥，RRC 密钥包括 RRC 加密密钥和 RRC 完整性保护密钥。可选的，UE 还生成用户面安全密钥，用户面安全密钥包括用户面加密密钥和用户面完整性保护密钥。这里需要说明的是，现有技术中说明用户面安全密钥是可选生成，既没有说什么情况下生成，也没有说什么情况下使用。

步骤 303，目标基站在接收到 RRC 恢复请求之后，发起 Xn-应用层（application protocol，AP）恢复（retrieve）流程，向源基站发送上下文信息获取请求，用于请求获取 UE 的上下文信息。相应的，源基站接收来自目标基站的上下文信息获取请求。Xn 为基站之间的接口。

其中，上下文信息获取请求包括 I-RNTI、resume MAC-I 和目标小区标识（identity，ID）。I-RNTI 和 resume MAC-I 为 UE 向目标基站发送的。目标小区标识为目标基站下的，将为 UE 提供服务的小区的标识。

源基站在接收到该上下文信息获取请求之后，根据 I-RNTI 查找 UE 的上下文信息，并利用 suspend 过程保存的 RRC 完整性保护密钥计算 resume MAC-I，若源基站计算得到的 resume MAC-I 与 UE 发送的 resume MAC-I 相同，则源基站生成新的 KgNB*。

步骤 304，源基站向目标基站发送上下文信息获取响应。相应的，目标基站接收来自源基站的上下文信息获取响应。

其中，上下文信息获取响应包括源基站生成的新的 KgNB*、与该 KgNB*对应的 NCC 值、UE 的 5G 安全能力、源小区使用的加密算法和完整性保护算法、用户面安全策略，以及可选的 security result。

步骤 305，若目标基站支持源小区使用的加密算法和完整性保护算法，则使用上下文信息获取响应所包括的 KgNB*生成 RRC 密钥和用户面安全密钥。

其中，RRC 密钥包括 RRC 加密密钥和 RRC 完整性保护密钥，用户面安全密钥包括用户面加密密钥和用户面完整性保护密钥。

步骤 306，目标基站向 UE 发送 RRC resume 消息。相应的，UE 接收来自目标基站的 RRC resume 消息。

其中，RRC resume 消息被目标基站新生成的 RRC 密钥进行加密保护和完整性保护，即被新生成的 RRC 加密密钥和 RRC 完整性保护密钥进行加密保护和完整性保护。

步骤 307，UE 使用其新生成的 RRC 密钥验证 RRC resume 消息，即 UE 使用其在步骤 302 生成的 RRC 加密密钥和 RRC 完整性保护密钥对 RRC resume 消息进行解密和验证，若成功解码且验证成功，则 UE 删除 suspend 过程中保存的 RRC 完整性保护密钥。

步骤 308, UE 向目标基站发送 RRC resume 完成消息。相应的, 目标基站接收来自 UE 的 RRC resume 完成消息。

UE 采用其新生成的 RRC 密钥对 RRC resume 完成消息进行加密保护和完整性保护。

步骤 309, 目标基站与目标 AMF 进行路径切换 (path switch) 流程。

若 UE 从 inactive 态进入连接态, 与 UE 建立 RRC 连接的基站是源基站, 则可省略图 3 中的步骤 303-步骤 304, 该种情况下可包括: UE 直接向源基站发送 RRC resume 请求; 源基站根据 I-RNTI 查找 UE 的上下文信息, 并利用 suspend 过程保存的 RRC 完整性保护密钥计算 resume MAC-I, 若源基站计算得到的 resume MAC-I 与 UE 发送的 resume MAC-I 相同, 则源基站生成新的 KgNB*, 根据新的 KgNB* 生成 RRC 密钥和用户面安全密钥; 源基站采用新生成的 RRC 密钥对 RRC resume 消息进行加密保护和完整性保护, 并向 UE 发送保护后的 RRC resume 消息; UE 采用其新生成的 RRC 密钥对 RRC resume 消息进行解密保护, 向源基站发送 RRC resume 完成消息, 该 RRC resume 完成消息被 RRC 密钥保护。

图 3 所示的目前 resume 过程虽然涉及了用户面安全密钥, 但是并未涉及何时以及如何使用用户面安全密钥。鉴于此, 本申请实施例明确 resume 过程中何时以及如何使用用户面安全密钥, 以及何时发送用户面数据。

图 2 和图 3 的流程是 3GPP 标准 TS 33.501 版本 F30 的总结。更多细节可以进一步参考相关内容。

请参见图 4, 为应用本申请实施例的网络架构示意图, 包括用户终端 10 和源接入网设备 20。

其中, 用户终端 10 可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备; 还可以包括 UE、用户单元 (subscriber unit)、蜂窝电话 (cellular phone)、智能电话 (smart phone)、无线数据卡、个人数字助理 (personal digital assistant, PDA) 电脑、平板型电脑、无线调制解调器 (modem)、手持设备 (handheld)、膝上型电脑 (laptop computer)、无绳电话 (cordless phone) 或者无线本地环路 (wireless local loop, WLL) 台、机器类型通信 (machine type communication, MTC) 终端、UE, 移动台 (mobile station, MS), 终端设备 (terminal device) 或者中继用户设备等。其中, 中继用户设备例如可以是 5G 家庭网关 (residential gateway, RG)。为方便描述, 本申请实施例中, 上面提到的设备统称为用户终端, 用户终端以 UE 为例进行介绍。

接入网设备可以是长期演进 (long term evolution, LTE) 系统中的演进型基站节点 (evolved Node Basestation, eNB 或 eNodeB), 升级后的 eNB, 即下一代演进型基站节点 (next generation eNodeB, ng-eNB), 第五代移动通信 (5th-generation, 5G) 系统中的下一代基站节点 (next generation Node Basestation, gNB) 等接入网设备, 还可以是未来通信系统中的接入网设备。

应用在本申请实施例中, 将用户终端 10 从连接态进入 inactive 态的 suspend 过程所涉及的基站作为源接入网设备 20, 源接入网设备 20 可以是图 2 中的基站。该基站可以是 5G 基站, 也可以是 4G 基站, 还可以是未来进一步演进的基站。若该基站是 4G 基站, 那么前文所述的现有技术应该是 4G 对应的 RRC suspend 和 RRC Resume 流程。本申请实施例以

5G 基站为例进行介绍。若用户终端 10 从 inactive 态进入连接态，与用户终端 10 建立 RRC 连接的基站不为源接入网设备 20，则图 4 所示的网络架构还包括目标接入网设备 30，目标接入网设备 30 为用户终端 10 从 inactive 进入连接态，与用户终端 10 建立 RRC 连接的基站，该种情况下，源接入网设备 20 可以是图 3 中的源基站，目标接入网设备可以是图 3 中的目标基站。需要说明的是，源接入网设备、目标接入网设备这两个名词并不构成对本申请实施例的限定，例如源接入网设备也可以称为源基站或源接入网设备等，目标接入网设备也可以称为目标基站或目标接入网设备等。本申请实施例在介绍 resume 过程时，以 suspend 过程所涉及的接入网设备与在 resume 过程中与 UE 建立 RRC 连接的接入网设备为不同接入网设备为例，即以图 4 所示的网络架构包括用户终端、源接入网设备和目标接入网设备为例。

下面将对本申请实施例提供的通信方法进行具体阐述。实施例中各名称与权利要求书中各名称的对应关系可包括：权利要求书中的第一用户面安全保护方法即为实施例中的新的用户面安全保护方法，第二用户面安全保护方法即为实施例中的旧的用户面安全保护方法或第一指示信息所指示的用户面安全保护方法，第一用户面安全密钥即为实施例中的新的用户面安全密钥或要使用的用户面安全密钥，第二用户面安全密钥即为实施例中旧的用户面安全密钥或 suspend 过程保存的用户面安全密钥。

需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体限定。

请参见图 5-1，为本申请实施例一提供的通信方法的流程示意图，该实施例主要介绍 suspend 过程中如何处理用户面安全策略。图 5-1 所示实施例在图 2 所示流程示意的基础上，增加步骤 505-1，源接入网设备保存第一指示信息。图 5-1 所示实施例可以包括但不限于如下步骤：

步骤 501-1，源接入网设备获取并保存 UE 的用户面安全策略。

源接入网设备获取并保存 UE 的用户面安全策略，即源接入网设备处于连接态时，从 SMF 获取并保存的针对 UE 的用户面安全策略或者在切换流程中从其他基站获取的用户面安全策略。源接入网设备保存该用户面安全策略的好处在于，便于源接入网设备确定与 UE 之间的用户面安全保护方法。在源接入网设备未执行步骤 505-1 的情况下，源接入网设备可以根据该用户面安全策略确定与 UE 之间的用户面安全保护方法。

源接入网设备在保存该用户面安全策略时，还可以保存该用户面安全策略对应的粒度信息。粒度信息指的是用户面安全保护方法适用的范围。粒度信息可以是 PDU 会话 ID，即不同 PDU 会话对应的用户面安全策略可以不同，还可以是无线承载标识(data radio bearer identity, DRB ID)、网络切片标识或数据网络名称等，例如不同的 DRB 对应的用户面安全策略可以不同。粒度信息还可以包括 PDU 会话 ID、DRB ID、网络切片标识或数据网络名称等中的多种，例如包括 PDU 会话 ID 和 DRB ID。需要说明的是，上述粒度信息与用户面安全策略绑定时，对应关系可以是一对一，也可以是一对多。例如一个 PDU 会话对应一个用户面安全策略，多个 PDU 会话可以对应同一个用户面安全策略。再例如，一个 DRB ID 对应一个用户面安全策略，多个 DRB ID 对应同一个用户面安全策略，目前一个 PDU 会话对应多个 DRB ID，该 PDU 会话对应的多个 DRB ID 可以对应同一个用户面安全策略，即

该 PDU 会话对应的用户面安全策略。

源接入网设备保存用户面安全策略以及对应的粒度信息的好处在于，当源接入网设备从 inactive 态进入连接态时，在获知 UE 发送的上行用户面数据的粒度信息的情况下，源接入网设备可以根据该粒度信息确定对应的用户面安全策略，进而确定用户面安全保护方法，进而对该上行用户面数据进行解安全保护。

如果源接入网设备生成并使用了用户面安全激活结果 (security result)，则保存 security result。

步骤 502-1，源接入网设备向 UE 发送 RRC 释放消息。相应的，UE 接收来自源接入网设备的 RRC 释放消息。

步骤 503-1，源接入网设备在发送 RRC 释放消息之后，删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥；保存 I-RNTI。

进一步的，源接入网设备去激活用户面安全。用户面安全的激活与去激活与用户面密钥是相关联的。因为源接入网设备删除了用户面安全密钥，因此源接入网设备要去激活用户面安全。具体的实施方法在这里不做限制。也就是说，也可能因为源接入网设备决定去激活用户面安全导致源接入网设备删除用户面安全密钥。

步骤 504-1，UE 在接收到 RRC 释放消息之后，对 RRC 释放消息的完整性保护进行验证，若验证成功，则 UE 存储 NCC 值，并删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥。

步骤 502-1 至步骤 504-1 的实现过程可参见图 2 所示流程中步骤 202-步骤 204 的具体描述，在此不再赘述。

这里需要额外强调的是，UE 去激活用户面安全。具体地，UE 的用户面安全激活状态与 UE 的用户面安全密钥是绑定的。因为 UE 删除了用户面密钥，因此 UE 去激活用户面安全。具体的实施方法在这里不做限制。也就是说，也可能因为 UE 决定去激活用户面安全导致 UE 删除用户面安全密钥。

步骤 505-1，源接入网设备保存第一指示信息，第一指示信息包括用户面安全激活方法指示信息和/或用户面安全保护方法指示信息。

其中，用户面安全激活方法指示信息用于指示是否开启用户面加密保护以及是否开启用户面完整性保护，为 UE 和源接入网设备处于连接态时，源接入网设备通过 RRC 消息发送给 UE 的，用于指示激活何种用户面安全保护方法，具体指示视源接入网设备和 UE 处于连接态时源接入网设备所激活的用户面安全保护方法而定。该用户面安全激活方法指示信息可以是图 1 步骤 106 中 RRC 连接重配置消息所携带的用户面激活指示信息。源接入网设备保存用户面安全激活方法指示信息，以便源接入网设备在 resume 过程中可以使用。

其中，用户面安全保护方法指示信息，指的是源接入网设备根据 UE 当前保护数据所使用的用户面安全保护方法新生成的指示信息，用于指示用户面加密保护是否开启以及用户面完整性保护是否开启。源接入网设备保存用户面安全保护方法指示信息，以便源接入网设备在 resume 过程中可以使用。

第一指示信息，还可以是 security result 的增强。在现有技术中，security result 是可选生成，可选使用。其可能在用户面安全策略含有 preferred 的情况下才会生成。本申请实施

例可以进一步规定不管用户面安全策略是否有 preferred 的, security result 必须生成。其格式可以继续使用现有格式,也可以更新为 ENUMERATED (enabled, disabled ...)。

上述用户面安全激活方法指示信息和用户面安全保护方法指示信息,都可以指示源接入网设备在进入 inactive 态时,源接入网设备和 UE 在从连接态进入 inactive 态之前所使用的用户面安全保护方法。用户面安全激活方法指示信息是接入网设备传递给 UE 的指示信息,可以理解为 UE 不需要生成,只需要接收。该用户面安全激活方法指示信息在 RRC 消息中传递,具体在 RRC 连接重配置消息中传递(可参考步骤 106)。而用户面安全保护方法指示信息不需要传递,是需要接入网设备和 UE 分别生成的一种指示信息。

源接入网设备保存第一指示信息的好处在于,可以确保源接入网设备在从连接态进入 inactive 态之前,与从连接态进入 inactive 态之后,所使用的用户面安全保护方法一致。

在一种可能的实现方式中,源接入网设备在保存第一指示信息时,还保存第一指示信息对应的粒度信息。粒度信息指的是用户面安全保护方法适用的范围。粒度信息可以是 PDU 会话 ID,即不同 PDU 会话对应的第一指示信息可以不同,还可以是 DRB ID、网络切片标识或数据网络名称等,例如不同的 DRB 对应的第一指示信息可以不同。粒度信息还可以包括 PDU 会话 ID、DRB ID、网络切片标识或数据网络名称等中的多种,例如包括 PDU 会话 ID 和 DRB ID。

需要说明的是,上述粒度信息与第一指示信息绑定时,对应关系可以是一对一,也可以是一对多。例如一个 PDU 会话对应一个第一指示信息,多个 PDU 会话可以对应同一个第一指示信息。再例如,一个 DRB ID 对应一个第一指示信息,多个 DRB ID 对应同一个第一指示信息,目前一个 PDU 会话对应多个 DRB ID,该 PDU 会话对应的多个 DRB ID 可以对应同一个第一指示信息,即该 PDU 会话对应的第一指示信息。

源接入网设备保存第一指示信息以及第一指示信息对应的粒度信息的好处在于,当源接入网设备从 inactive 态进入连接态时,在获知 UE 发送的上行用户面数据的粒度信息的情况下,源接入网设备可以根据该粒度信息确定对应的用户面安全保护方法,进而对该上行用户面数据进行解安全保护。

需要说明的是,步骤 505-1 可以在步骤 503-1 之后执行,也可以在步骤 502-1 与步骤 503-1 之间执行,还可以在步骤 503-1 的过程中执行。图 5-1 所示实施例以步骤 505-1 在步骤 503-1 之后执行为例进行介绍,并不构成对本申请实施例的限定。

在图 5-1 所示的实施例中,源接入网设备在发送 RRC 释放消息之后保存第一指示信息,可以确保源接入网设备在从连接态进入 inactive 态之前,与从连接态进入 inactive 态之后,所使用的用户面安全保护方法一致。还可以便于源接入网设备根据第一指示信息确定是否保存用户面安全密钥,具体将在图 6 所示的实施例中介绍。源接入网设备保存第一指示信息,而 UE 不保存第一指示信息,在 UE 发送 RRC 恢复请求消息后,源接入网设备可在确定用户面安全保护方法之后,通过第二指示信息将所确定的用户面安全保护方法告知 UE。

进一步的,在用户面安全策略不包括 preferred 的情况下,即用户面加密保护策略不为 preferred,或用户面完整性保护策略不为 preferred,或用户面加密保护策略和用户面完整性保护策略均不为 preferred,源接入网设备可只保存用户面安全策略,即只执行步骤 501-1。在用户面安全策略包括 preferred 的情况下,即用户面加密保护策略为 preferred,或用户面

完整性保护策略为 preferred，或用户面加密保护策略和用户面完整性保护策略均为 preferred，源接入网设备需要保存用户面安全策略和第一指示信息，即执行步骤 501-1 和步骤 505-1，这样便于在 resume 过程中，在接入网设备根据用户面安全策略包括 preferred 的情况下无法准确确定出与 UE 之间的用户面安全保护方法的情况下，可以根据第一指示信息确定出与 UE 之间用户面安全保护方法。其中，该接入网设备为 UE 恢复 RRC 连接的基站，可以为源接入网设备，也可以为目标接入网设备。

请参见图 5-2，为本申请实施例二提供的通信方法的流程示意图，该实施例主要介绍 suspend 过程中如何处理用户面安全策略。图 5-2 所示实施例在图 5-1 所示实施例的基础上，增加步骤 506-2，UE 保存第一指示信息，换言之，图 5-2 所示实施例中，UE 和源接入网设备均保存第一指示信息，而图 5-1 所示实施例只有源接入网设备保存第一指示信息。图 5-2 所示的实施例可以包括但不限于如下步骤：

步骤 501-2，源接入网设备获取并保存 UE 的用户面安全策略。

步骤 502-2，源接入网设备向 UE 发送 RRC 释放消息。相应的，UE 接收来自源接入网设备的 RRC 释放消息。

步骤 503-2，源接入网设备在发送 RRC 释放消息之后，删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥；保存 I-RNTI。

步骤 504-2，UE 在接收到 RRC 释放消息之后，对 RRC 释放消息的完整性保护进行验证，若验证成功，则 UE 存储 NCC 值，并删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥。

步骤 505-2，源接入网设备保存第一指示信息，第一指示信息包括用户面安全激活方法指示信息和/或用户面安全保护方法指示信息。

其中，步骤 501-2 和步骤 505-2 可参见图 5-1 所示实施例中步骤 501-1 和步骤 505-1 的具体描述，步骤 502-2 至步骤 504-2 的实现过程可参见图 2 所示流程中步骤 202-步骤 204 的具体描述和图 5-1 所示流程中步骤 502-1 至步骤 504-1 的具体描述，在此不再赘述。

步骤 506-2，UE 保存第一指示信息，第一指示信息包括用户面安全激活方法指示信息和/或用户面安全保护方法指示信息。

其中，用户面安全激活方法指示信息，指的是 UE 与源接入网设备处于连接态时，源接入网设备在图 1 步骤 106 中所携带的用户面激活指示信息。例如，图 1 步骤 106 的 RRC 连接重配置消息包括用户面完整性保护激活指示信息为 enable，不包括用户面加密保护激活指示信息，则 UE 可确定开启用户面加密保护，开启用户面完整性保护。在 UE 接收到 RRC 释放消息之后，UE 记录用户面完整性保护为 enable，该记录表示开启用户面完整性保护，同时开启用户面加密保护。该种情况下，UE 所保存的用户面激活方法指示信息用于指示开启用户面加密保护和开启用户面完整性保护。再例如，图 1 步骤 106 的 RRC 连接重配置消息包括用户面加密保护激活指示信息为 disable，不包括用户面完整性保护激活指示信息，则 UE 可确定不开启用户面加密保护，不开启用户面完整性保护。在 UE 接收到 RRC 释放消息之后，UE 记录用户面完整性保护为 disable，该记录表示不开启用户面完整性保护，不开启用户面加密保护。该种情况下，UE 所保存的用户面激活方法指示信息用于指示不开启用户面加密保护和不开启用户面完整性保护。再例如，图 1 步骤 106 的 RRC 连接重配置

消息包括用户面完整性保护激活指示信息为 enable，用户面加密保护激活指示信息为 disable，则 UE 可确定不开启用户面加密保护，开启用户面完整性保护。在 UE 接收到 RRC 释放消息之后，UE 记录用户面完整性保护为 enable，用户面加密保护为 disable，该记录表示开启用户面完整性保护，不开启用户面加密保护。该种情况下，UE 所保存的用户面激活方法指示信息用于指示不开启用户面加密保护和开启用户面完整性保护。

上述三个例子中，UE 所记录的信息表示用户面安全激活方法指示信息，例如 UE 记录的信息为用户面完整性保护为 enable，用户面加密保护为 disable，所表示的用户面安全激活方法指示信息用于指示不开启用户面加密保护和开启用户面完整性保护。再例如，UE 记录的信息为用户面加密保护为 disabled，所表示的用户面安全激活方法指示信息用于指示用户面加密保护和用户面完整性保护都不开启。除了这种记录方式外，还可以采用两个比特来记录或表示用户面安全激活方法指示信息，例如“01”表示用户面加密保护开，用户面完整性保护关。具体 UE 如何记录以及用户面安全激活方法指示信息采用何种方式指示，在本申请实施例中不作限定。

用户面安全保护方法指示信息，指的是 UE 根据其当前保护数据所使用的用户面安全保护方法生成的指示信息，或 UE 根据其从连接态进入 inactive 态前保护数据所使用的用户面安全保护方法生成的指示信息。换言之，用户面安全保护方法指示信息，用于指示 UE 当前所使用的用户面安全保护方法，或指示 UE 从连接态进入 inactive 态前所使用的用户面安全保护方法。该用户面安全保护方法指示信息的具体表现形式，可以参考 UE 记录的信息表示用户面安全激活方法指示信息的保存形式。该指示信息可以通过显示的方法保存在源接入网设备侧；也可以通过保存 DRB 配置信息隐式的体现。即，第一指示信息可以是相关的 DRB 配置信息。接入网设备可以根据 DRB 配置信息知晓使用什么样的用户面安全保护方法。

UE 保存第一指示信息的好处在于，可以确保 UE 在从连接态进入 inactive 态之前，与从连接态进入 inactive 态之后，所使用的用户面安全保护方法一致。

在一种可能的实现方式中，UE 在保存第一指示信息时，还保存第一指示信息对应的粒度信息。该过程与步骤 505-1 中源接入网设备保存第一指示信息以及第一指示信息对应的粒度信息相同。UE 保存第一指示信息以及第一指示信息对应的粒度信息的好处在于，当 UE 从 inactive 态进入连接态之后，在需要发送上行用户面数据时，可根据要发送的上行用户面数据的粒度信息确定其对应的用户面安全保护方法，然后根据该用户面安全保护方法对该上行用户面数据进行安全保护。

需要说明的是，步骤 506-2 可以在步骤 504-2 之后执行，也可以在步骤 502-2 与 504-2 之间执行，还可以在步骤 504-2 的过程中执行。图 5-2 所示实施例以步骤 505-2 在步骤 504-2 之后执行为例进行介绍，并不构成对本申请实施例的限定。

在图 5-2 所示的实施例中，UE 和源接入网设备均保存第一指示信息，可以确保 UE 和源接入网设备在从连接态进入 inactive 态之前，与从连接态进入 inactive 态之后，所使用的用户面安全保护方法一致。还可以便于源接入网设备和 UE 根据第一指示信息确定是否保存用户面安全密钥，具体将在图 6 所示的实施例中介绍。

在 UE 和源接入网设备均保存第一指示信息的情况下，UE 和源接入网设备可以采用不

同方式保存用户面安全保护方法。意味着，步骤 506-2 与步骤 505-2 保存的第一指示信息可能相同，也可能不同。比如步骤 506-2 保存的是步骤 106 中的用户面激活指示信息，但步骤 505-2 中保存的是增强的 security result。因此，本实施例的主要目的是说明 UE 侧也会保存一个具有与第一指示信息功能相同的指示信息。具体 UE 和源接入网设备保存的指示信息的内容，可能相同，也可能不同。本发明不做限定。例如，UE 保存的是用户面安全激活方法指示信息，源接入网设备保存的是用户面安全保护方法指示信息。也可以采用相同方式保存用户面安全保护方法。

基于图 5-2 所示的实施例的另一种实现源接入网设备和 UE 保存用户面安全保护方法的实现方法为，源接入网设备和 UE 协商用户面安全保护方法。协商的用户面安全保护方法用于当 UE 和源接入网设备再次进入连接态或进入连接态的过程中，应该使用什么样的用户面安全保护方法。协商的用户面安全保护方法，可以与当前的用户面安全保护方法相同，也可以不同。

一种可行的实施方法为，步骤 502-2 中的 RRC 释放消息可以携带新的用户面安全激活方法指示信息和/或用途指示信息。该新的用户面安全激活方法指示信息指示 UE 再次进入连接态的时候应该使用什么样的用户面安全保护方法。该用途指示信息指示 UE 在什么情况下才可以使用步骤 502-2 中指示的用户面安全保护方法。在步骤 502-2 中没有新的用户面安全激活方法指示信息的情况下，UE 可以使用进入 inactive 态前的用户面安全保护方法保护早期数据传送（early data transfer），或者 UE 可以使用从核心网获取的用户面安全保护方法保护早期数据传送。

其中，携带的新的用户面安全激活方法指示信息的具体内容可以参考用户面安全激活方法指示信息。用途指示信息可以指示该 UE 从 inactive 态进入连接态后，用户面安全保护方法是只可以用于保护早期数据传送，还是只可以用于在进入连接态后才可以用于保护传递用户面数据，还是既可以用于保护早期数据传送，又可以用于在进入连接态后才可以用于保护传递用户面数据。比如，可以用枚举型的消息格式传递这个信息。因此，步骤 504-2 和步骤 506-2 中，源接入网设备和 UE 分别只需要根据新协商的用户面安全保护方法确定保存第一指示信息。

图 5-2 所示实施例为 UE 和源接入网设备均保存了第一指示信息，在一种特殊的情况下，源接入网设备和 UE 均不保存第一指示信息，源接入网设备和 UE 从连接态进入 inactive 态的过程中，存在一种固定的用户面安全保护方法，那么接入网设备和 UE 从连接态进入 inactive 态时，可直接使用该固定的用户面安全保护方法。例如，固定的用户面安全保护方法为不开启用户面加密保护，开启用户面完整性保护。在这种方法下，源接入网设备可以保存从 SMF 获取的用户面安全策略，以便于 UE 回到连接态后，源接入网设备可根据用户面安全策略激活和 UE 之间的用户面安全。

请参见图 6，为本申请实施例三提供的通信方法的流程示意图，该实施例主要介绍 suspend 过程中如何处理用户面安全策略。图 6 所示实施例在图 2 所示流程的基础上，增加源接入网设备和/或 UE 确定是否保存用户面安全密钥的步骤，换言之，图 6 所示实施例中需确定是否删除用户面加密密钥以及是否删除用户面完整性保护密钥，而图 2 所示流程中源接入网设备和 UE 直接删除用户面加密密钥和用户面完整性保护密钥。图 6 所示的实

例可以包括但不限于如下步骤:

步骤 601, 源接入网设备获取并保存 UE 的用户面安全策略。步骤 601 的实现过程可参见图 5-1 所示实施例中步骤 501-1 的具体描述, 在此不再赘述。

步骤 602, 源接入网设备向 UE 发送 RRC 释放消息。相应的, UE 接收来自源接入网设备的 RRC 释放消息。步骤 602 的实现过程可参见图 2 所示流程中步骤 202 的具体描述, 在此不再赘述。

步骤 603, 源接入网设备在发送 RRC 释放消息之后, 删除 RRC 加密密钥, 保存 RRC 完整性保护密钥, 保存 I-RNTI。

步骤 604, 源接入网设备确定是否保存用户面安全密钥, 即确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥。

源接入网设备可通过如下几种方式来确定是否保存用户面安全密钥。

方式一, 若源接入网设备和 UE 通过 resume 消息进入连接态后, 采用的是固定的用户面安全保护方法, 则源接入网设备在 suspend 过程中, 确定保存与其方法相对应的用户面安全密钥。固定的用户面安全保护方法可以是只做用户面完整性保护、或者只做用户面加密保护、或者既做用户面加密保护又做用户面完整性保护。相应的, 源接入网设备采用只保存用户面完整性密钥, 或者只保存用户面加密密钥, 或者既保存用户面完整性密钥又保存用户面加密密钥。相应的, 在 UE 通过 RRC resume 消息进入连接态后, 源接入网设备只使用户面完整性保护、或者只使用用户面加密保护、或者既使用用户面加密保护又使用用户面完整性保护的密钥对收到的用户面消息进行解保护。

方式二, 在源接入网设备只保存用户面安全策略的情况下, 即按照图 2 所示流程执行的情况下, 源接入网设备除了保存该用户面安全策略外, 还保存当前使用的用户面安全密钥, 以便源接入网设备在进入连接态后更好地确定用户面安全保护方法。这种方法好处在于, 在该用户面安全策略所包括的用户面加密保护策略和用户面完整性保护策略均为 preferred 时, 直接根据该用户面安全策略确定出之前使用的用户面安全保护方法存在困难, 因此在保存该用户面安全策略的同时保存当前使用的用户面安全密钥, 可以使源接入网设备知晓之前的用户面安全保护方法。源接入网设备当前使用的用户面安全密钥, 指的是源接入网设备在发送 RRC 释放消息之前, 源接入网设备和 UE 保护用户面安全所使用的用户面安全密钥。

方式三, 在源接入网设备保存第一指示信息的情况下, 即执行步骤 505-1 或步骤 505-2 的情况下, 源接入网设备根据第一指示信息确定是否保存用户面安全密钥, 即根据第一指示信息所指示的用户面安全保护方法确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥。例如, 第一指示信息指示开启用户面加密保护, 不开启用户面完整性保护, 则源接入网设备保存用户面加密密钥, 删除用户面完整性保护。

方式四, 在源接入网设备保存了某个粒度信息相关的用户面资源的情况下, 源接入网设备可根据该用户面资源对应的用户面安全保护方法确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥。

方式五, 若源接入网设备与 UE 新协商了用户面安全保护方法, 则源接入网设备可根据新协商的用户面安全保护方法, 确定是否保存用户面加密密钥以及是否保存用户面完整

性保护密钥。

因为源接入网设备保存了用户面安全密钥，因此源接入网设备会保留用户面安全激活方法的相关 DRB 配置信息。可以理解为源接入网设备将用户面安全激活方法的相关 DRB 配置信息和用户面安全密钥一起保存在源接入网设备。

步骤 605，UE 在接收到 RRC 释放消息之后，对 RRC 释放消息的完整性保护进行验证，若验证成功，则 UE 存储 NCC 值，并删除 RRC 加密密钥、保存 RRC 完整性保护密钥。

步骤 606，UE 确定是否保存用户面安全密钥，即确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥。

UE 可通过如下几种方式来确定是否保存用户面安全密钥。

方式一，不管进入 inactive 态前使用何种用户面安全密钥，UE 都保存该用户面安全密钥。在此方式下，UE 会在 RRC resume 流程中重新激活用户面安全保护方法，新激活的用户面安全保护方法使用的用户面安全密钥可能与进入 inactive 态前的相同也可能不同。

方式二，UE 可以确定只保存用户面加密密钥、或者只保存用户面完整性保护密钥、或者既保存用户面加密密钥又保存用户面完整性保护密钥。并且保存的内容与源接入网设备侧一致。例如，UE 和源接入网设备均只保存用户面加密密钥。该方式下保存的用户面安全密钥可以用于保护早期数据传送。

方式三，UE 可以根据当前的用户面安全保护方法确定需要保存的密钥。例如，若 UE 在进入 inactive 态前，只开启了用户面加密保护，则需要保存用户面加密密钥，用户面完整性保护密钥可以删除也可以保存；若只开启了用户面完整性保护，则需要保存用户面完整性保护密钥，用户面加密密钥可以保存也可以删除；若既开启了用户面完整性保护，又开启了用户面加密保护，则需要既保存用户面加密密钥，又保存用户面完整性保护密钥。

方式四，在 UE 保存第一指示信息的情况下，即执行步骤 506-2 的情况下，UE 根据第一指示信息确定需要保存的用户面安全密钥。例如，第一指示信息指示只开启了用户面加密保护，则需要保存用户面加密密钥，用户面完整性保护密钥可以删除也可以保存；若用户面安全激活方法指示信息和/或用户面安全保护方法指示信息只开启了用户面完整性保护，则需要保存用户面完整性保护密钥，用户面加密密钥可以保存也可以删除；若用户面安全激活方法指示信息和/或用户面安全保护方法指示信息既开启了用户面完整性保护，又开启了用户面加密保护，则需要既保存用户面加密密钥，又保存用户面完整性保护密钥。

对于方式四，保存第一指示信息与确定是否保存用户面安全密钥可以同时执行；也可以先保存第一指示信息，再确定是否保存用户面安全密钥；还可以先确定是否保存用户面安全密钥，再保存第一指示信息。

若保存第一指示信息与确定是否保存用户安全密钥同时执行，则 UE 根据图 1 步骤 106 所携带的用户面激活指示信息，或根据当前所使用的用户面安全保护方法，或根据从连接态进入 inactive 态时所使用的用户面安全保护方法，确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥，同时生成并保存用户面安全激活指示信息和/或用户面安全保护方法指示信息。这里的同时，是指确定用户面安全密钥与生成并保存用户面安全激活指示信息和/或用户面安全保护方法指示信息无直接关系。

若先保存第一指示信息，再确定是否保存用户安全密钥，那么 UE 根据图 1 步骤 106

所携带的用户面激活指示信息生成并保存用户面安全激活指示信息；根据当前所使用的用户面安全保护方法，或根据从连接态进入 inactive 态时所使用的用户面安全保护方法生成并保存用户面安全保护方法指示信息；然后 UE 根据用户面安全激活指示信息和/或用户面安全保护方法指示信息确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥。可以看出，此时 UE 根据用户面安全保护方法生成并保存用户面安全保护方法指示信息确定需要保护的的用户面安全密钥。

若先确定是否保存用户安全密钥，再保存第一指示信息，那么 UE 根据图 1 步骤 106 所携带的用户面激活指示信息，或根据当前所使用的用户面安全保护方法，或根据从连接态回到 inactive 态时所使用的用户面安全保护方法，确定是否保存用户面加密密钥以及是否保存用户面完整性保护密钥；然后再根据确定的保存的用户面安全密钥，进一步生成并保存用户面安全激活指示信息和/或用户面安全保护方法指示信息。可以看出，此时 UE 先确定需要保存的用户面安全密钥，再根据保存的密钥进一步生成并保存用户面安全保护方法指示信息确定需要保护的的用户面安全密钥。

因为 UE 保存了用户面安全密钥，因此 UE 会保留用户面安全激活方法的相关 DRB 配置信息。可以理解为 UE 将用户面安全激活方法的相关 DRB 配置信息和用户面安全密钥一起保存在 UE。

需要说明的是，本申请实施例不限定步骤 605 与步骤 606 执行的先后顺序，可以同时执行，也可以先执行步骤 605 再执行步骤 606，还可以先执行步骤 606 再执行步骤 605。

需要说明的是，源接入网设备与 UE 确定是否保存用户面安全密钥可以是同步的，即执行步骤 604 和步骤 606，或不执行步骤 604 和步骤 606。也可以是不同步的，即执行步骤 604 不执行步骤 606，源接入网设备保存而 UE 不保存；或执行步骤 606 不执行步骤 604，UE 保存而源接入网设备不保存。不同步，更好的考虑 UE 和基站的后向兼容性，实现最小程度的改动。

在图 6 所示的实施例中，在 suspend 过程中，增加 UE 和/源接入网设备确定是否保存用户面安全密钥的步骤，以便在 resume 过程中，可以快速对用户面数据进行安全保护、解安全保护。

在图 6 所示的实施例中，是否保存用户面安全密钥的步骤可在图 2 的基础上增加，也可在图 5-1 或图 5-2 的基础上增加，例如 UE 根据保存的第一指示信息确定是否保存用户面安全密钥。

图 5-1、图 5-2 以及图 6 所示的实施例针对 suspend 过程，下面将对 resume 过程进行介绍。本申请实施例中，在 suspend 过程中保存用户面安全密钥的情况下，将保存的用户面安全密钥称为旧的用户面安全密钥，将 resume 过程中生成的用户面安全密钥称为新的用户面安全密钥，将 suspend 过程中涉及的用户面安全保护方法称为旧的用户面安全保护方法，将 resume 过程中重新确定的用户面安全保护方法称为新的用户面安全保护方法。

请参见图 7-1，为本申请实施例四提供的通信方法的流程示意图，该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 7-1 所示实施例基于图 2 所示流程，即在 suspend 过程中 UE 和源接入网设备均未保存第一指示信息。图 7-1 所示的实施例可以包括但不限于如下步骤：

步骤 701-1, UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 702-1, UE 向目标接入网设备发送 RRC 恢复请求。相应的, 目标基站接收来自 UE 的 RRC 恢复请求。

UE 在发送 RRC 恢复请求之后, 生成新的 KgNB*, 用新的 KgNB* 生成新的 RRC 密钥, 新的 RRC 密钥包括新的 RRC 加密密钥和新的 RRC 完整性保护密钥。

一种可能的实现方式, UE 在发送 RRC 恢复请求之后, 没有生成用户面安全密钥, 即图 7-1 所示, 不生成用户面安全密钥。

另一种可能的实现方式, UE 在发送 RRC 恢复请求之后, 生成新的用户面安全密钥, 具体将在图 8-1 所示的步骤 802-1a 进行介绍。

步骤 701-1 至步骤 702-1 的实现过程可参见图 3 所示实施例中步骤 301 至步骤 302 的具体描述, 不过步骤 702-1 中只生成 RRC 密钥, 未生成用户面安全密钥。

步骤 703-1, 目标接入网设备向源接入网设备发送上下文信息获取请求。相应的, 源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 704-1, 源接入网设备向目标接入网设备发送上下文信息获取响应。相应的, 目标接入网设备接收来自源接入网设备的上下文信息获取响应。

步骤 703-1 至步骤 704-1 的实现过程可参见图 3 所示实施例中步骤 303 至步骤 304 的具体描述。

步骤 705-1, 若目标接入网设备支持源小区使用的加密算法和完整性保护算法, 则使用 KgNB* 生成新的 RRC 密钥 (包括新的 RRC 加密密钥和 RRC 完整性保护密钥), 根据用户面安全策略确定用户面安全保护方法, 并根据该用户面安全保护方法确定要使用的用户面安全密钥。

目标接入网设备根据用户面安全策略以及自身情况, 确定与 UE 之间的用户面安全保护方法。其中, 自身情况可以包括但不限于是否支持开启用户面加密保护、是否支持开启用户面完整性保护、当前资源使用情况、当前负荷情况、UE 当前支持的速率等。例如, 用户面安全策略中用户面加密保护策略为 required, 用户面完整性保护为 preferred, 但是目标接入网设备不支持开启用户面完整性保护, 则目标接入网设备确定的与 UE 之间的用户面安全保护方法为开启用户面加密保护, 不开启用户面完整性保护。相应的, 根据该用户面安全保护方法确定要使用的用户面安全密钥包括用户面加密密钥, 不包括用户面完整性保护密钥。

目标接入网设备的确定用户面安全密钥可以先与用户面安全激活结合在一起, 也可以分开。如果结合在一起, 则目标接入网设备根据该用户面安全保护方法和 KgNB* 生成新的用户面安全密钥, 使用新的用户面安全保护方法和新的用户面安全密钥激活用户面安全, 新的用户面安全密钥即为要使用的用户面安全密钥。例如, 第一指示信息所指示的用户面安全保护方法为开启用户面完整性保护, 但是目标接入网设备不支持开启用户面完整性保护, 那么重新确定的用户面安全保护方法包括不开启用户面完整性保护, 相应的, 新的用户面安全密钥不包括用户面完整性保护密钥。如果是分开的, 则目标接入网设备可以在用户面安全激活之前或之后生成所有用户面安全密钥, 再根据用户面安全激活方法确定要使用哪种用户面安全密钥。例如, 如果用户面安全激活时只激活了用户面加密保护, 没有激

活用户面完整性保护，则目标接入网设备只使用用户面加密密钥，不使用用户面完整性保护密钥。此时用户面完整性保护密钥可以删除也可以保留，本申请实施例不做规定。目标接入网设备在确定用户面安全保护方法以及要使用的用户面安全密钥的情况下，可以使用该用户面安全保护方法、该用户面安全密钥以及用户面安全算法对上行用户面数据进行解安全保护，对下行用户面数据进行安全保护。

目标接入网设备在确定用户面安全保护方法之后，可使用该用户面安全保护方法激活用户面安全，可在向 UE 发送 RRC 恢复消息之前激活用户面安全，也可以在向 UE 发送 RRC 恢复消息之后激活用户面安全，例如在步骤 706-1 与步骤 708-1 之间激活用户面安全，或在步骤 708-1 之后激活用户面安全。

可选的，目标接入网设备在确定的用户面安全保护方法之后，向 SMF 发送用户面安全激活结果。该用户面安全激活结果，可以通过 Pathswitch 流程中的消息进行发送，也可以通过其他的流程的消息发送，比如通过切换请求确认传输（handover request acknowledge transfer）消息。具体的承载消息本发明不做限制。

步骤 706-1，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

其中，第二指示信息用于指示目标接入网设备所确定的用户面安全保护方法，具体指示是否开启用户面加密保护以及是否开启用户面完整性保护，包括用户面加密保护激活指示信息和/或用户面完整性保护激活指示信息。在一种可能的实现方式中，例如，第二指示信息所包括的用户面完整性保护激活指示信息为 enable，不包括用户面加密保护激活指示信息，那么用于指示开启用户面完整性保护，同时开启用户面加密保护。再例如，第二指示信息所包括的用户面完整性保护激活指示信息为 disable，不包括用户面加密保护激活指示信息，那么用于指示不开启用户面完整性保护，不开启用户面加密保护。在另一种可能的实现方式中，例如，第二指示信息所包括的用户面完整性保护激活指示信息为 enable，用户面加密保护激活指示信息为 enable，那么用于指示开启用户面完整性保护，同时开启用户面加密保护。再例如，第二指示信息所包括的用户面完整性保护激活指示信息为 disable，用户面加密保护激活指示信息为 disable，那么用于指示不开启用户面完整性保护，不开启用户面加密保护。除了上述对第二指示信息的指示方式外，还可以采用两个比特来记录或表示第二指示信息，例如“01”表示用户面加密保护开，用户面完整性保护关。具体 UE 如何记录以及第二指示信息采用何种方式指示，在本申请实施例中不限定。

目标接入网设备在 RRC 恢复消息中携带第二指示信息，以便 UE 根据第二指示信息激活用户面安全。

RRC 恢复消息被目标接入网设备生成的新的 RRC 密钥进行加密保护和完整性保护，即进行信令面保护。

步骤 707-1，UE 根据第二指示信息激活用户面安全，并确定要使用的用户面安全密钥。

UE 在接收到 RRC 恢复消息时，对 RRC 恢复消息的信令面安全进行验证，并在验证成功后，生成所有的用户面安全密钥，然后根据用户面安全激活情况或第二指示信息进一步确定使用哪种用户面安全密钥。该用户面安全激活情况指的是 UE 从连接态进入第三态之前如何激活用户面安全的。比如，UE 生成用户面加密密钥和用户名完整性保护密钥，然后

用户面安全激活情况或第二指示信息指示的是开启用户面加密保护，关闭用户面完整性保护，那么 UE 只使用用户面加密密钥。用户面完整性保护密钥可以删除也可以保留，本申请实施例不做限定。UE 也可以直接根据用户面安全激活情况或者第二指示信息确定要使用的用户面安全密钥。比如，用户面安全激活情况或者第二指示信息指示的是用户面加密开，用户面完整性保护关，则目标接入网设备只需要生成用户面加密密钥，不需要生成用户面完整性保护密钥。

若 UE 在发送 RRC 恢复请求之后，生成新的用户面安全密钥，即执行了步骤 802-1a，则相应地需执行步骤 807-1。

步骤 708-1，UE 向目标接入网设备发送 RRC 恢复完成消息。相应的，目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

其中，RRC 恢复完成消息被步骤 702-1 生成的 RRC 密钥进行加密保护和完整性保护，即进行信令面保护。

步骤 709-1，UE 向目标接入网设备发送第一上行用户面数据。相应的，目标接入网设备接收来自 UE 的第一上行用户面数据。

UE 使用根据第二指示信息所确定的用户面安全保护方法、新的用户面安全密钥和用户面安全算法对上行用户面数据进行安全保护，得到第一上行用户面数据。换言之，第一上行用户面数据为被新的用户面安全密钥保护。这样，目标接入网设备在接收到第一上行用户面数据时，使用用户面安全保护方法、新的用户面安全密钥和用户面安全算法对第一上行用户面数据进行解安全保护，得到上行用户面数据。

其中，用户面安全算法可以是在 suspend 过程中保存的，也可以是 UE 和目标接入网设备在 resume 过程中协商的用户面安全算法，具体使用哪个过程中的用户面安全算法，图 7-1 所示的实施例以及后续实施例不作限定，后续实施例的介绍过程中省略了用户面安全算法，实际对上行用户面数据进行安全保护需要使用用户面安全保护方法、用户面安全密钥和用户面安全算法。其中，UE 和目标接入网设备在 resume 过程中可以协商信令面安全算法和/或用户面安全算法，或者协商的安全算法既可以用于信令面，也可以用于用户面。

步骤 709-1 是上行传输，对于下行传输，目标接入网设备在接收到下行用户面数据时，使用用户面安全保护方法、新的用户面安全密钥以及用户面安全算法对下行用户面数据进行安全保护，得到第一下行用户面数据，向 UE 发送第一下行用户面数据。UE 在接收到第一下行用户面数据时，使用用户面安全保护方法、新的用户面安全密钥以及用户面安全算法对第一下行用户面数据进行解安全保护，得到下行用户面数据。

在图 7-1 所示的实施例中，UE 和源接入网设备在 suspend 过程均未保存第一指示信息，也未确定是否保存用户面安全密钥的情况下，目标接入网设备根据用户面安全策略确定用户面安全保护方法，生成新的用户面安全密钥，通过 RRC 恢复消息向 UE 发送第二指示信息，以便 UE 生成新的用户面安全密钥，并激活用户面安全。该实施例明确 UE 在接收到第二指示信息时，激活用户面安全，并发送上行用户面数据，目标接入网设备在接收到用户面安全策略之后，可激活用户面安全，从而保证 resume 过程中用户面数据传输的安全性。

可以理解的是，目标接入网设备根据用户面安全策略确定的用户面安全保护方法是新的用户面安全保护方法，与第一指示信息指示的用户面安全保护方法可能相同，可能不相

同。在后续实施例的介绍过程中，将第一指示信息指示的用户面安全保护方法称为旧的用户面安全保护方法，将目标接入网设备不根据第一指示信息确定的用户面安全保护方法称为新的用户面安全保护方法。

请参见图 7-2，为本申请实施例五提供的通信方法的流程示意图，该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 7-2 所示实施例基于图 5-1 所示实施例，即在 suspend 过程中源接入网设备保存了第一指示信息。也可以基于图 2 所示流程，即使源接入网设备未保存第一指示信息，源接入网设备也可以确定出第一指示信息，例如源接入网设备根据进入 inactive 态前用户面数据的保护方式确定用户面安全保护方法，进而确定第一指示信息。

图 7-2 所示的实施例可以包括但不限于如下步骤：

步骤 701-2，UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 702-2，UE 向目标接入网设备发送 RRC 恢复请求。相应的，目标基站接收来自 UE 的 RRC 恢复请求。

UE 在发送 RRC 恢复请求之后，生成新的 KgNB*，用新的 KgNB*生成新的 RRC 密钥，新的 RRC 密钥包括新的 RRC 加密密钥和新的 RRC 完整性保护密钥。

步骤 701-2 至步骤 702-2 的实现过程可参见图 3 所示实施例中步骤 301 至步骤 302 的具体描述，或参见步骤 701-1 至步骤 702-1 的具体描述。

步骤 703-2，目标接入网设备向源接入网设备发送上下文信息获取请求。相应的，源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 704-2，源接入网设备向目标接入网设备发送上下文信息获取响应。相应的，目标接入网设备接收来自源接入网设备的上下文信息获取响应。

步骤 703-2 至步骤 704-2 的实现过程可参见图 3 所示实施例中步骤 303 至步骤 304 的具体描述，不过步骤 704-2 中上下文信息获取响应除包括步骤 304 中上下文信息获取响应所包括的内容外，还包括第一指示信息，第一指示信息即为源接入网设备在图 5-1 所示实施例中步骤 501-1 所包括的指示信息。

在一种可能的实现方式中，源接入网设备可以判断是否要携带第一指示信息。例如，如果发生了基站变换，那么源接入网设备可以不发送第一指示信息。此时参考步骤 304 的描述。

步骤 705-2，若目标接入网设备支持源小区使用的加密算法和完整性保护算法，则使用 KgNB*生成新的 RRC 密钥（包括新的 RRC 加密密钥和 RRC 完整性保护密钥），确定要使用的用户面安全密钥。

在一种可能的实现方式中，目标接入网设备根据判断第一指示信息所指示的用户面安全保护方法是否可用，若不可用则目标接入网设备根据用户面安全策略重新确定与 UE 之间的用户面安全保护方法，并激活用户面安全；或者目标接入网设备通过发送 RRC 消息使 UE 和目标接入网设备重新建立 RRC 连接的方法重新确定与 UE 之间的用户面安全保护方法，并激活用户面安全。目标接入网设备向 UE 发送 RRC 消息，该 RRC 消息用于触发 UE 重新接入、重新建立 PDU 会话，以重新建立 RRC 连接。在重新建立 RRC 连接的过程中，目标接入网设备与 UE 可按照现有 UE 与基站协商用户面安全保护方法的方式协商用户面安

全保护方法。换言之，重新建立 RRC 连接意味着 UE 要重新入网、重新建立 PDU 会话连接。因此可以重新协商用户面安全保护方法。这样做虽然降低了接入的效率，但是可以实现对现有技术最好的兼容。其中，目标接入网设备根据用户面安全策略重新确定用户面安全保护方法可参见步骤 705-1 中的描述。目标接入网设备根据激活的用户面安全确定要使用的用户面安全密钥。

在一种可能的实现方式中，目标接入网设备忽略第一指示信息，直接根据用户面安全策略确定用户面安全保护方法，并激活用户面安全。目标接入网设备根据激活的用户面安全确定要使用的用户面安全密钥。

在一种可能的实现方式中，如果源接入网设备经过判断没有携带第一指示信息，则目标接入网设备根据用户面安全策略确定用户面安全保护方法，并激活用户面安全。目标接入网设备根据激活的用户面安全确定要使用的用户面安全密钥。

在一种可能的实现方式中，目标接入网设备直接根据第一指示信息和 KgNB*生成新的用户面安全密钥，使用第一指示信息所指示的用户面安全保护方法和新的用户面安全密钥激活用户面安全。由于图 7-2 针对图 5-1，UE 未保存第一指示信息，因此在该方式中，目标接入网设备通过在 RRC 恢复消息中携带第二指示信息来告知 UE，以便 UE 确定用户面安全保护方法，并激活用户面安全。目标接入网设备可在向 UE 发送 RRC 恢复消息之前激活用户面安全，也可以在向 UE 发送 RRC 恢复消息之后激活用户面安全，例如在步骤 706-2 与步骤 708-2 之间激活用户面安全，或在步骤 708-2 之后激活用户面安全。

步骤 706-2，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

步骤 707-2，UE 根据第二指示信息激活用户面安全，并确定要使用的用户面安全密钥。

步骤 708-2，UE 向目标接入网设备发送 RRC 恢复完成消息。相应的，目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

步骤 706-2 至步骤 708-2 的实现过程可参见图 7-1 中步骤 706-1 至步骤 708-1 的具体描述，在此不再赘述。

在图 7-2 所示的实施例，源接入网设备在 suspend 过程中保存第一指示信息，而 UE 未保存第一指示信息的情况下，目标接入网设备在判断出第一指示信息所指示的用户面安全保护方法不可用时，根据用户面安全策略重新确定用户面安全保护方法并激活用户面安全；或目标接入网设备直接根据第一指示信息所指示的用户面安全保护方法激活用户面安全。该实施例明确 UE 在接收到第二指示信息时，激活用户面安全，并发送上行用户面数据，目标接入网设备在接收到用户面安全策略和第一指示信息之后，可激活用户面安全，从而保证 resume 过程中用户面数据传输的安全性。

请参见图 7-3，为本申请实施例六提供的通信方法的流程示意图，该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 7-3 所示实施例基于图 5-2 所示实施例，即在 suspend 过程中源接入网设备和 UE 均保存第一指示信息。也可以基于图 2 所示流程，即使源接入网设备未保存第一指示信息，源接入网设备也可以确定出第一指示信息。图 7-3 所示的实施例可以包括但不限于如下步骤：

步骤 701-3，UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 702-3, UE 向目标接入网设备发送 RRC 恢复请求。相应的, 目标基站接收来自 UE 的 RRC 恢复请求。

UE 在发送 RRC 恢复请求之后, 生成新的 KgNB*, 用新的 KgNB* 生成 RRC 密钥, RRC 密钥包括 RRC 加密密钥和 RRC 完整性保护密钥。

步骤 701-3 至步骤 702-3 的实现过程可参见图 3 所示实施例中步骤 301 至步骤 302 的具体描述, 或参见步骤 701-1 至步骤 702-1 的具体描述。

步骤 703-3, 目标接入网设备向源接入网设备发送上下文信息获取请求。相应的, 源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 704-3, 源接入网设备向目标接入网设备发送上下文信息获取响应。相应的, 目标接入网设备接收来自源接入网设备的上下文信息获取响应。其中, 上下文信息获取响应包括用户面安全策略和第一指示信息, 具体可参见步骤 704-2 中对其的具体描述。

步骤 705-3, 若目标接入网设备支持源小区使用的加密算法和完整性保护算法, 则使用 KgNB* 生成新的 RRC 密钥 (包括新的 RRC 加密密钥和 RRC 完整性保护密钥), 根据第一指示信息确定要使用的用户面安全密钥。其过程可以参考步骤 705-2 中根据第一指示信息确定要使用的用户面安全密钥的具体描述。

目标接入网设备可在向 UE 发送 RRC 恢复消息之前激活用户面安全, 也可以在向 UE 发送 RRC 恢复消息之后激活用户面安全, 例如在步骤 706-3 与步骤 708-3 之间激活用户面安全, 或在步骤 708-3 之后激活用户面安全。

步骤 706-3, 目标接入网设备向 UE 发送 RRC 恢复消息。相应的, UE 接收来自目标接入网设备的 RRC 恢复消息。

步骤 707-3, UE 根据第一指示信息激活用户面安全, 并确定要使用的用户面安全密钥。

UE 在接收到 RRC 恢复消息时, 对 RRC 恢复消息的信令面安全进行验证, 并在验证成功后, 生成所有的用户面安全密钥, 然后根据用户面安全激活情况或第一指示信息进一步确定使用哪种用户面安全密钥。该用户面安全激活情况指的是 UE 从连接态进入第三态之前如何激活用户面安全的。比如, UE 生成用户面加密密钥和用户面完整性保护密钥, 然后用户面安全激活情况或第一指示信息指示的是开启用户面加密保护, 关闭用户面完整性保护, 那么 UE 只使用用户面加密密钥。用户面完整性保护密钥可以删除也可以保留, 本申请实施例不做限定。UE 也可以直接根据用户面安全激活情况或者第一指示信息确定要使用的用户面安全密钥。比如, 用户面安全激活情况或者第一指示信息指示的是用户面加密开, 用户面完整性保护关, 则目标接入网设备只需要生成用户面加密密钥, 不需要生成用户面完整性保护密钥。UE 根据第一指示信息生成新的用户面安全密钥并激活用户面安全的步骤可在接收到 RRC 恢复消息之后执行, 即步骤 707-3 在步骤 706-3 之后执行; 也可在 UE 向目标接入网设备发送 RRC 恢复请求之后执行, 即步骤 707-3 在步骤 702-3 之后执行。如果在步骤 706-3 之后执行, 若步骤 706-3 中携带了第二指示信息, 则 UE 需要释放 RRC 连接。这是因为如果步骤 706-3 携带了第二指示信息, 那么意味着 UE 要根据第二指示信息重新确定用户面安全保护方法。重新确定用户面安全保护方法, 可能导致 UE 无法继续使用之前的用户面安全保护方法, 因此 UE 需要释放 RRC 连接。可选的, UE 可以向目标接入网设备报告错误, 使得目标接入网设备主动发起 RRC 连接释放或者发起 RRC 连接重建流程。

步骤 708-3, UE 向目标接入网设备发送 RRC 恢复完成消息。相应的, 目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

图 7-3 与图 7-2 的不同之处在于, 步骤 705-3 中目标接入网设备直接根据第一指示信息生成新的用户面安全密钥, 并激活用户面安全, 由于 UE 保存有第一指示信息, 那么目标接入网设备无需在 RRC 恢复消息中携带第二指示信息, 使得 UE 和源接入网设备在从连接态进入 inactive 态之前, 与从连接态进入 inactive 态之后, 所使用的用户面安全保护方法一致, UE 和源接入网设备可快速对用户面数据进行安全保护或解安全保护。

若目标接入网设备根据用户面安全策略确定新的用户面安全保护方法, 则 RRC 恢复消息中需携带第二指示信息, 用于指示目标接入网设备确定的用户面安全保护方法, UE 根据第二指示信息确定用户面安全保护方法并激活相应的用户面安全。

在图 7-3 所示的实施例中, UE 和源接入网设备在 suspend 过程均保存了第一指示信息, 均可根据第一指示信息生成新的用户面安全密钥, UE 可在接收到 RRC 恢复消息之前或之后生成新的用户面安全密钥并激活用户面安全, 目标接入网设备可在发送 RRC 恢复消息之后生成新的用户面安全密钥并激活用户面安全, 从而保证 resume 过程中用户面数据传输的安全性。

图 7-1、图 7-2 以及图 7-3 中, UE 在发送 RRC 恢复请求之后, 并没有立即生成用户面安全密钥。下面图 8-1 至图 8-2 中, UE 在发送 RRC 恢复请求之后, 立即生成用户面安全密钥。

请参见图 8-1, 为本申请实施例七提供的通信方法的流程示意图, 该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 8-1 所示实施例基于图 5-1 所示实施例, 也可以基于图 2 所示流程。图 7-2 也是基于图 5-1, 不过图 7-2 步骤 702-2 中不生成用户面安全密钥, 而图 8-1 步骤 802-1 中生成新的用户面安全密钥。图 8-1 所示的实施例可以包括但不限于如下步骤:

步骤 801-1, UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 802-1, UE 向目标接入网设备发送 RRC 恢复请求。相应的, 目标基站接收来自 UE 的 RRC 恢复请求。

UE 在发送 RRC 恢复请求之后, 生成新的 KgNB*, 用新的 KgNB* 生成新的 RRC 密钥, 新的 RRC 密钥包括新的 RRC 加密密钥和新的 RRC 完整性保护密钥。UE 在发送 RRC 恢复请求之后, 还生成新的用户面安全密钥, 将 UE 生成新的用户面安全密钥作为步骤 802-1a。

在步骤 802-1a 中, UE 生成的新的用户面安全密钥为用户面加密密钥, 或用户面完整性保护密钥, 或用户面加密密钥和用户面完整性保护密钥。可以理解的是, 该新的用户面安全密钥为一种已经确定的用户面安全密钥。

在一种可能的实现方式中, UE 直接根据新的 KgNB* 生成新的用户面安全密钥, 即新的用户面加密密钥和新的用户面完整性保护密钥。该方式即为图 3 步骤 302 中可选的。

在一种可能的实现方式中, 在图 5-2 所示实施例中 UE 和源接入网设备均保存第一指示信息的情况下, UE 根据新的 KgNB*, 以及保存的第一指示信息, 生成新的用户面安全密钥。此时生成的是新的用户面加密密钥和/或新的用户面完整性保护密钥。举例来说, 第一指示信息指示不开启用户面加密保护, 开启用户面完整性保护, 那么 UE 根据新的 KgNB*

生成新的用户面完整性保护密钥，不必生成新的用户面加密密钥。

若 UE 在 suspend 过程中保存了用户面安全密钥，例如在图 6 所示实施例中 UE 确定保存用户面安全密钥，那么 UE 在生成新的用户面安全密钥的情况下，并且没有早期数据传送（early data transfer）发生的情况下，删除 suspend 过程所保存的用户面安全密钥。本申请实施例将 suspend 过程保存的用户面安全密钥称为旧的用户面安全密钥，将 resume 过程新生成的用户面安全密钥称为新的用户面安全密钥，那么在生成新的用户面安全密钥的情况下，并且没有早期数据传送发生的情况下，删除旧的用户面安全密钥。在有早期数据传送的情况下，则选取合适时机删除旧的用户面安全密钥。例如 UE 在接收到 RRC 恢复消息后删除，再例如 UE 在确定早期数据发送成功后删除。图 8-1 所示的实施例，不管 UE 在 suspend 过程是否保存旧的用户面安全密钥，在接收到 RRC 恢复消息之后都使用新的用户面安全密钥；或者 UE 在 suspend 过程未保存旧的用户面安全密钥，则使用新的用户面安全密钥保护和验证接收到 RRC 恢复消息之后的上下行用户面数据。

UE 在生成新的用户面安全密钥的情况下，可以立即激活用户面安全，也可以不立即激活用户面安全，即激活用户面安全可以在步骤 802-1a 执行，也可以在步骤 802-1a 之后执行。立即激活的好处在于：用户面安全有利于 UE 可以立即发送上行用户面数据，并且上行用户面数据可以被新的用户面安全密钥进行安全保护。不立即激活的好处在于：UE 可以确定 resume 过程中，在 UE 确定成功接入目标接入网设备或源接入网设备后再发送上行用户面数据。若 UE 没有确定接入成功就发送上行用户面数据，那么发送的上行用户面数据可能因为 resume 过程的不成功而需要再次发送。同时，若不立即激活，则 UE 无法立即发送上行用户面数据，或者发送的上行用户面数据是没有安全保护的。图 8-1 所示实施例以激活用户面安全在步骤 806-1 之后执行为例。

在步骤 802-1a 是否激活用户面安全，可以由 UE 根据是否需要立即发送上行用户面数据确定，例如，UE 需要立即发送上行用户面数据，那么可以在生成新的用户面安全密钥之后，立即激活用户面安全。在步骤 802-1a 是否激活用户面安全，也可以由 UE 根据 UE 和接入网设备预先约定的流程激活。例如，根据标准规定，UE 和接入网设备在接入网设备发送 RRC 恢复消息（即步骤 806-1）之后，激活用户面安全，那么 UE 在生成新的用户面安全密钥之后，不立即激活用户面安全，即不在步骤 802-1a 激活用户面安全。换言之，该例中激活用户面安全与生成用户面安全密钥是解耦的。再例如，标准规定，UE 可以在其发送 RRC 恢复请求之后或之前激活用户面安全，那么 UE 可以先激活用户面安全，再根据激活的用户面安全生成新的用户面安全密钥；或者 UE 先生成所有的用户面安全密钥，再根据需激活的用户面安全确定要使用的用户面安全密钥，即确定新的用户面安全密钥（此时步骤 802-1a 生成用户面加密密钥和用户面完整性保护密钥，然后 UE 在步骤 807-1 确定要使用哪个密钥，具体在图 8-2 所示实施例中介绍）。

在 UE 保存有旧的用户面安全密钥的情况下，在有早期数据传送的情况下，UE 和接入网设备可能发生 2 次用户面安全激活。即发送早期数据前，UE 先激活用户面安全，此时用户面安全保护方法可以是 UE 在进入 inactive 前的用户面安全保护方法（按需的用户面安全保护方法），也可以是标准规定好的固定的用户面安全保护方法（固定的用户面安全保护方法，比如只开启完整性保护）。接入网设备会与 UE 执行相同的处理，即当接入网设备收到

早期数据时，先激活用户面安全，此时用户面安全保护方法可以是 UE 在进入 inactive 前的用户面安全保护方法（按需的用户面安全保护方法），也可以是标准规定好的固定的用户面安全保护方法（固定的用户面安全保护方法，比如只开启完整性保护）。在早期数据发送后，UE 和接入网设备可以再次激活用户面安全。此时的激活的用户面安全用于 UE 和接入网设备进入连接态后使用。其用户面安全保护方法可以与第一次的相同，也可以不同。当然，一种可行的优化方法是，若接入网设备判断可以继续使用第一次激活的用户面安全保护方法，则接入网和 UE 继续使用之前的用户面安全保护方法。此时可以在步骤 806-1 中显示的告知，比如通过传递第二指示信息告知；也可以通过隐式的告知，即不传递任何指示信息，UE 和接入网设备默认继续使用已经激活的用户面安全保护方法。在这种情况下，UE 和接入网设备可以继续使用保存的旧的用户面安全密钥，也可以使用新生成的用户面安全密钥。使用旧的用户面安全密钥的好处是，不需要占用资源额外生成一个。使用新的用户面安全密钥的好处是，与现有用户面安全保护方法的兼容性好。

其中，UE 激活用户面安全，指的是 UE 激活与目标接入网设备之间的用户面安全保护方法，可以开启使用该用户面安全保护方法对上行用户面数据进行安全保护。若不存在目标接入网设备，那么 UE 激活与源接入网设备之间的用户面安全保护方法。

步骤 803-1，目标接入网设备向源接入网设备发送上下文信息获取请求。相应的，源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 804-1，源接入网设备向目标接入网设备发送上下文信息获取响应。相应的，目标接入网设备接收来自源接入网设备的上下文信息获取响应。

步骤 803-1 至步骤 804-1 的实现过程可参见图 3 所示实施例中步骤 303 至步骤 304 的具体描述，不过步骤 804-1 中上下文信息获取响应除包括步骤 304 中上下文信息获取响应所包括的内容外，可选的还包括第一指示信息，该第一指示信息即为源接入网设备在图 5-1 所示实施例中步骤 505-1 所保存的指示信息。另一种可能实现的方式为，在第一指示信息生成的情况下，源接入网设备可以进一步判断是否发送第一指示信息。若源接入网设备将 resume 流程使用的安全上下文发给目标接入网设备，则不发送第一指示信息。

步骤 805-1，若目标接入网设备支持源小区使用的加密算法和完整性保护算法，则使用 KgNB*生成新的 RRC 密钥（包括新的 RRC 加密密钥和 RRC 完整性保护密钥），确定要使用的用户面安全密钥。

在一种可能的实现方式中，若上下文信息获取响应只包括用户面安全策略，则目标接入网设备根据用户面安全策略激活用户面安全，并根据激活的用户面安全确定要使用的用户面安全密钥，具体可参见图 7-1 中步骤 705-1 的描述。作为步骤 705-1 的一种可能实现方式的补充，图 8-2 中步骤 807-2 的描述也可以进行参考。

在一种可能的实现方式中，若上下文信息获取响应包括用户面安全策略和第一指示信息，则目标接入网设备可在判断出第一指示信息所指示的用户面安全保护方法不可用的情况下，根据用户面安全策略激活用户面安全，相应的，根据激活的用户面安全确定要使用的用户面安全密钥。目标接入网设备可在判断出第一指示信息所指示的用户面安全保护方法可用的情况下，根据第一指示信息激活用户面安全；相应的，目标接入网根据激活的用户面安全确定要使用的用户面安全密钥。具体可参见图 7-1 中步骤 705-1 的描述，或图 8-2

中步骤 807-2 的描述。或目标接入网设备直接根据第一指示信息确定要使用的用户面安全密钥。具体可参见图 7-2 中步骤 705-2 的描述。

特别的，若不存在目标接入网设备，即 UE 向源接入网设备发送 RRC 恢复请求，那么源接入网设备生成用户面安全密钥与激活用户面安全可能不同步，即源接入网设备可以先生成所有的用户面安全密钥，再根据要激活的用户面安全确定使用哪个用户面安全密钥。源接入网设备也可以确定继续使用保存的旧的用户面安全密钥，若继续使用旧的用户面安全密钥，那么源接入网设备可通过在 RRC 恢复消息中携带指示信息，该指示信息用于指示继续使用旧的用户面安全密钥。此时，UE 不执行步骤 802-1a，即不生成新的用户面安全密钥，或者执行 802-1a，不过在步骤 807-1 中删除新的用户面安全密钥。

在另一种可能的实现方式中，若不存在目标接入网设备，则源接入网设备根据第一指示信息激活用户面安全。然后向 UE 发送第二指示信息。UE 根据第二指示信息激活用户面安全，并确定使用哪种用户面安全密钥。

但是当存在目标接入网设备的情况下，UE 和目标接入网设备只能使用新的用户面安全密钥。因此 UE 在接收到 RRC 恢复消息后，需确定是否存在目标接入网设备，若存在目标接入网设备，则 UE 需要删除保存的旧的用户面安全密钥，开始使用新的用户面安全密钥。因为目标接入网设备没有旧的用户面安全密钥，因此目标接入网设备只能使用新的用户面安全密钥。在这个情况下，源接入网设备删除旧的用户面安全密钥。源接入网设备删除旧的用户面安全密钥，例如可在步骤 804-1 之后删除。

步骤 806-1，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

步骤 807-1，UE 根据第二指示信息激活用户面安全。

与步骤 707-1 以及步骤 707-2 的不同之处在于，步骤 807-1 中直接根据第二指示信息激活用户面安全，即可以使用新的用户面安全密钥和第二指示信息所指示的用户面安全保护方法对上行用户面数据进行安全保护，对下行用户面数据进行解安全保护。在激活用户面安全后，因为步骤 802-1a 已经生成了新的用户面安全密钥，因此步骤 807-1 可根据用户面安全激活情况，直接使用新的用户面安全密钥即可。而步骤 707-1 以及步骤 707-2 为，根据第二指示信息确定与目标接入网设备之间的用户面安全保护方法，激活用户面安全。换言之，步骤 707-1 以及步骤 707-2 中，新的用户面安全密钥与第二指示信息相关，而步骤 807-1 中，新的用户面安全密钥与第二指示信息无关。

若 UE 保存有旧的用户面安全密钥，那么 UE 在使用新的用户面安全密钥激活用户面安全之后，删除旧的用户面安全密钥。

步骤 808-1，UE 向目标接入网设备发送 RRC 恢复完成消息。相应的，目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

步骤 809-1，UE 向目标接入网设备发送第一上行用户面数据。相应的，目标接入网设备接收来自 UE 的第一上行用户面数据。

步骤 808-1 至步骤 809-1 的实现过程可参见步骤 708-1 至步骤 709-1 的具体描述。

在图 8-1 所示的实施例，源接入网设备在 suspend 过程保存第一指示信息，而 UE 未保存第一指示信息的情况下，目标接入网设备在确定出用户面安全保护方法之后将其告知

UE。该实施例明确 UE 在接收到第二指示信息时，激活用户面安全，并发送上行用户面数据，目标接入网设备在接收到用户面安全策略和第一指示信息之后，可激活用户面安全，从而保证 resume 过程中用户面数据传输的安全性。

若 UE 在 suspend 过程保存了第一指示信息，即图 5-2 所示实施例，那么在步骤 802-1a 中 UE 根据第一指示信息生成新的用户面安全密钥，在步骤 805-1 中目标接入网设备根据第一指示信息生成新的用户面安全密钥并激活用户面安全，在步骤 806-1 中 RRC 恢复消息不携带第二指示信息，在步骤 808-1 中 UE 根据第一指示信息激活用户面安全，步骤 809-1 中 UE 使用第一指示信息指示的用户面安全保护方法以及新的用户面安全密钥对上行用户面数据进行安全保护，得到第一上行用户面数据。

请参见图 8-2，为本申请实施例八提供的通信方法的流程示意图，该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 8-2 所示实施例基于图 5-1 所示实施例，也可以基于图 2 所示流程。图 8-2 也是基于图 5-1，不过图 8-2 步骤 802-2a 中生成所有的用户面安全密钥，而图 8-1 步骤 802-1a 中生成新的用户面安全密钥，一种确定的用户面安全密钥。图 8-2 所示实施例与图 8-1 所示实施例相同的部分可参见图 8-1 的具体描述。图 8-2 所示的实施例可以包括但不限于如下步骤：

步骤 801-2，UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 802-2，UE 向目标接入网设备发送 RRC 恢复请求。相应的，目标基站接收来自 UE 的 RRC 恢复请求。

步骤 802-2a，UE 生成所有的用户面安全密钥，所有的用户面安全密钥包括用户面加密密钥和用户面完整性保护密钥，以便 UE 根据需要激活的用户面安全确定要使用的用户面安全密钥，即确定新的用户面安全密钥。UE 可以在接收到 RRC 恢复消息之后，根据第二指示信息确定要使用的用户面安全密钥。UE 也可以在 UE 保存第一指示信息的情况下，根据第一指示信息确定要使用的用户面安全密钥。图 8-2 所示实施例以 UE 在接收到 RRC 恢复消息之后，根据第二指示信息确定要使用的用户面安全密钥。

步骤 803-2，目标接入网设备向源接入网设备发送上下文信息获取请求。相应的，源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 804-2，源接入网设备向目标接入网设备发送上下文信息获取响应。相应的，目标接入网设备接收来自源接入网设备的上下文信息获取响应。

步骤 805-2，若目标接入网设备支持源小区使用的加密算法和完整性保护算法，则使用 KgNB*生成新的 RRC 密钥（包括新的 RRC 加密密钥和 RRC 完整性保护密钥），确定要使用的用户面安全密钥。步骤 805-2 的实现过程可参见步骤 805-1 的具体描述。

步骤 806-2，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

步骤 807-2，UE 根据第二指示信息确定要使用的用户面安全密钥并激活用户面安全。

UE 根据第二指示信息从步骤 802-2a 生成的所有用户面安全密钥中确定要使用的用户面安全密钥。例如，第二指示信息指示开启用户面加密保护，不开启用户面完整性保护，步骤 802-2a 生成了用户面加密密钥和用户面完整性保护密钥，则确定的要使用的用户面安全密钥为用户面加密密钥。对于不使用的用户面安全密钥，可以删除也可以保留。

UE 在确定新的用户面安全密钥之后,可以使用第二指示信息所指示的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护,对下行用户面数据进行解安全保护。

步骤 808-2, UE 向目标接入网设备发送 RRC 恢复完成消息。相应的,目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

步骤 809-2, UE 向目标接入网设备发送第一上行用户面数据。相应的,目标接入网设备接收来自 UE 的第一上行用户面数据。

在图 8-1 所示的实施例中,源接入网设备在 suspend 过程保存第一指示信息,而 UE 未保存第一指示信息的情况下,UE 先生成所有的用户面安全密钥,在接收到 RRC 恢复消息之后确定需要使用的用户面安全密钥并激活用户面安全;目标接入网设备在确定出用户面安全保护方法之后将其告知 UE。该实施例明确 UE 在接收到第二指示信息时,激活用户面安全,并发送上行用户面数据,目标接入网设备在接收到用户面安全策略和第一指示信息之后,可激活用户面安全,从而保证 resume 过程中用户面数据传输的安全性。

若 UE 在 suspend 过程保存了第一指示信息,即图 5-2 所示实施例,那么在步骤 805-2 中目标接入网设备根据第一指示信息确定要使用的用户面安全密钥,在步骤 806-2 中 RRC 恢复消息不携带第二指示信息,在步骤 807-2 中 UE 根据第一指示信息确定需要使用的用户面安全密钥并激活用户面安全,步骤 809-2 中 UE 使用第一指示信息指示的用户面安全保护方法以及新的用户面安全密钥对上行用户面数据进行安全保护,得到第一上行用户面数据。

请参见图 9-1,为本申请实施例九提供的通信方法的流程示意图,该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 9-1 所示实施例基于图 5-1 所示实施例,也可以基于图 2 所示流程。图 9-1 所示实施例与图 8-1 所示实施例相同的部分可参见图 8-1 的具体描述。图 9-1 所示的实施例可以包括但不限于如下步骤:

步骤 901-1, UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 902-1, UE 向目标接入网设备发送 RRC 恢复请求。相应的,目标基站接收来自 UE 的 RRC 恢复请求。

步骤 902-1a, UE 生成新的用户面安全密钥并激活用户面安全。

步骤 902-1b, UE 向目标接入网设备发送第一上行用户面数据。相应的,目标接入网设备接收来自 UE 的第一上行用户面数据。

UE 使用第一指示信息所指示的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护,得到第一上行用户面数据。换言之,UE 使用旧的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护,得到第一上行用户面数据。

步骤 903-1,目标接入网设备向源接入网设备发送上下文信息获取请求。相应的,源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 904-1,源接入网设备向目标接入网设备发送上下文信息获取响应。相应的,目标接入网设备接收来自源接入网设备的上下文信息获取响应。

步骤 905-1,若目标接入网设备支持源小区使用的加密算法和完整性保护算法,则使用 KgNB*生成新的 RRC 密钥(包括新的 RRC 加密密钥和 RRC 完整性保护密钥),根据第一指示信息确定要使用的用户面安全密钥。

目标接入网设备根据第一指示信息激活用户面安全，根据激活的用户面安全确定要使用的用户面安全密钥。步骤 905-1 的实现过程可参见步骤 705-3 的具体描述。

步骤 905-1a，目标接入网设备对第一上行用户面数据进行解安全保护，得到上行用户面数据。

目标接入网设备使用旧的用户面安全保护方法和新的用户面安全密钥对第一上行用户面数据进行解安全保护，得到上行用户面数据。

步骤 905-1b，目标接入网设备向核心网发送上行用户面数据，具体向用户面功能（user plane function，UPF）发送上行用户面数据。

步骤 905-1c，目标接入网设备确定不使用旧的用户面安全保护方法，根据用户面安全策略确定新的用户面安全保护方法。

目标接入网设备根据用户面安全策略确定新的用户面安全保护方法可参见图 7-1 中步骤 705-1 的具体描述。

步骤 906-1，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

其中，第二指示信息用于指示目标接入网设备确定的新的用户面安全保护方法。

步骤 907-1，UE 根据第二指示信息重新激活用户面安全。

UE 使用新的用户面安全保护方法和新的用户面安全密钥重新激活用户面安全，即可以使用新的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护。

步骤 908-1，UE 向目标接入网设备发送 RRC 恢复完成消息。相应的，目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

步骤 909-1，UE 向目标接入网设备发送第二上行用户面数据。相应的，目标接入网设备接收来自 UE 的第二上行用户面数据。

UE 使用第二指示信息所指示的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护，即使用新的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护，得到第二上行用户面数据。

在图 9-1 所示的实施例，存在两次用户面安全激活，一次是在 UE 发送 RRC 恢复请求之后，使用新的用户面安全密钥和旧的用户面安全保护方法，一次是在 UE 接收到第二指示信息之后，使用新的用户面安全密钥和新的用户面安全保护方法。若步骤 905-1c 中确定继续使用旧的用户面安全保护方法，则步骤 706 的 RRC 恢复消息中不携带第二指示信息，不执行步骤 907-1 和步骤 909-1。

请参见图 9-2，为本申请实施例十提供的通信方法的流程示意图，该实施例主要介绍 resume 过程中如何对用户面数据进行安全保护。图 9-1 所示实施例基于图 6 所示实施例，UE 和源接入网设备保存用户面安全密钥，将 suspend 过程保存的用户面安全密钥称为旧的用户面安全密钥。图 9-2 所示的实施例可以包括但不限于如下步骤：

步骤 901-2，UE 使用 suspend 过程所保存的 RRC 完整性保护密钥计算 resume MAC-I。

步骤 902-2，UE 向目标接入网设备发送 RRC 恢复请求。相应的，目标基站接收来自 UE 的 RRC 恢复请求。

步骤 902-2a，UE 向目标接入网设备发送第一上行用户面数据。相应的，目标接入网设

备接收来自 UE 的第一上行用户面数据。

UE 使用第一指示信息所指示的用户面安全保护方法和旧的用户面安全密钥对上行用户面数据进行安全保护，得到第一上行用户面数据。换言之，UE 使用旧的用户面安全保护方法和旧的用户面安全密钥对上行用户面数据进行安全保护，得到第一上行用户面数据。

步骤 903-2，目标接入网设备向源接入网设备发送上下文信息获取请求。相应的，源接入网设备接收来自目标接入网设备的上下文信息获取请求。

步骤 904-2，源接入网设备向目标接入网设备发送上下文信息获取响应。相应的，目标接入网设备接收来自源接入网设备的上下文信息获取响应。

其中，上下文信息获取响应包括用户面安全策略和第一指示信息，还包括旧的用户面安全密钥。

步骤 905-2a，目标接入网设备对第一上行用户面数据进行解安全保护，得到上行用户面数据。

目标接入网设备使用旧的用户面安全保护方法和旧的用户面安全密钥对第一上行用户面数据进行解安全保护，得到上行用户面数据。

步骤 905-2b，目标接入网设备向核心网发送上行用户面数据，具体向 UPF 发送上行用户面数据。

步骤 905-2，若目标接入网设备支持源小区使用的加密算法和完整性保护算法，则使用 K_{gNB} 生成新的 RRC 密钥（包括新的 RRC 加密密钥和 RRC 完整性保护密钥），确定要使用的用户面安全密钥。

步骤 906-2，目标接入网设备向 UE 发送 RRC 恢复消息，该 RRC 恢复消息包括第二指示信息。相应的，UE 接收来自目标接入网设备的 RRC 恢复消息。

步骤 907-2，UE 根据第二指示信息重新激活用户面安全，并确定要使用的用户面安全密钥。

UE 在生成新的用户面安全密钥之后，删除旧的用户面安全密钥。

步骤 908-2，UE 向目标接入网设备发送 RRC 恢复完成消息。相应的，目标接入网设备接收来自 UE 的 RRC 恢复完成消息。

步骤 905-2 至步骤 908-2 的实现过程可参见图 7-2 所示实施例中步骤 705-2 至 708-2 的具体描述。

步骤 909-2，UE 向目标接入网设备发送第二上行用户面数据。相应的，目标接入网设备接收来自 UE 的第二上行用户面数据。

UE 使用第二指示信息所指示的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护，即使用新的用户面安全保护方法和新的用户面安全密钥对上行用户面数据进行安全保护，得到第二上行用户面数据。

在图 9-2 所示的实施例中，存在两次用户面安全激活，一次是在 UE 发送 RRC 恢复请求之后，使用旧的用户面安全密钥和旧的用户面安全保护方法，一次是在 UE 接收到第二指示信息之后，使用新的用户面安全密钥和新的用户面安全保护方法。

请参见图 10，为本申请实施例提供的路径切换流程的示意图，该路径切换流程可与实施例一至实施例十结合，以图 7-1 为例，该路径切换流程可在步骤 704-1 之后执行，也可在

步骤 704-1 与步骤 705-1 之间执行，还可以在步骤 709-1 之后执行。

图 10 所示的实施例可以包括但不限于如下步骤：

步骤 1001，目标接入网设备向 AMF 发送路径切换请求。相应的，AMF 接收来自目标接入网设备的路径切换请求。

其中，路径切换请求可以是 path switch request，路径切换请求包括用户面安全策略，该用户面安全策略为源接入网设备向目标接入网设备发送的。可选的，该路径切换请求还包括该用户面安全策略对应的粒度信息。

步骤 1002，AMF 向 SMF 发送会话管理（session management，SM）消息。相应的，SMF 接收来自 AMF 的 SM 消息。

其中，该 SM 消息包括用户面安全策略，可选的，还包括该用户面安全策略对应的粒度信息。

步骤 1001 与步骤 1002 为目标接入网设备通过 AMF 向 SMF 发送用户面安全策略，可选的，发送该用户面安全策略对应的粒度信息。

步骤 1003，SMF 判断其保存的用户面安全策略与路径切换请求携带的用户面安全策略是否一致。

若切换请求包括用户面安全策略以及该用户面安全策略对应的粒度信息，那么 SMF 根据该粒度信息查找该粒度信息对应的用户面安全策略，并判断查找到的用户面安全策略与切换请求所携带用户面安全策略是否一致。

若切换请求不包括用户面安全策略对应的粒度信息，切换请求还可以包括 UE 的标识，SMF 保存有 UE 的标识对应的用户面安全策略，SMF 判断 UE 的标识对应的用户面安全策略与切换请求所携带用户面安全策略是否一致。

步骤 1004，若不一致，则 SMF 向 AMF 发送 SM 确认（ack）消息。相应的，AMF 接收来自 SMF 的 SM 确认消息。

其中，该 SM 确认消息包括 SMF 保存的用户面安全策略。

步骤 1005，AMF 向目标接入网设备发送路径切换响应。相应地，目标接入网设备接收来自 AMF 的路径切换响应。

其中，路径切换响应可以是 path switch request，路径切换响应包括 SMF 保存的用户面安全策略。

步骤 1004-步骤 1005 为 SMF 通过 AMF 向目标接入网设备发送 SMF 保存的用户面安全策略。

步骤 1006，目标接入网设备重新确定用户面安全保护方法，与 UE 执行切换流程，该切换流程可以是 intra-gNB-集中单元（centralized unit，CU）切换（handover，HO）流程，使得 UE 和目标接入网设备重新确定用户面安全保护方法并激活用户面安全。

若路径切换流程在步骤 704-1 之后执行，或在步骤 704-1 与步骤 705-1 之间执行，那么可不执行步骤 1006，步骤 705-1 中根据从 SMF 获取的用户面安全策略确定用户面安全保护方法，这样可缩短时延。若路径切换流程在步骤 709-1 之后执行，那么需执行步骤 1006，UE 与目标接入网设备重新确定用户面安全保护方法，以纠正之前确定的用户面安全保护方法。

上述详细阐述了本申请实施例的方法，下面提供了本申请实施例的装置。

请参见图 11，是本申请实施例提供的通信装置的逻辑结构示意图，该通信装置 60 可以包括收发单元 601 和处理单元 602。该通信装置 60 可以是用户终端，也可以是目标接入网设备，还可以是源接入网设备。

针对该通信装置 60 为用户终端的情况：

处理单元 602，用于在收发单元 601 向目标接入网设备发送 RRC 恢复请求之后，确定与该目标接入网设备之间的第一用户面安全保护方法；确定与该目标接入网设备之间的第一用户面安全密钥；根据第一用户面安全保护方法和第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；

收发单元 601，用于向该目标接入网设备发送该第一用户面数据。

该通信装置 60 为用户终端时，可以实现实施例一至实施例十中 UE 的功能，该通信装置 60 中各个单元执行详细过程可以参见实施例一至实施例十中 UE 的执行步骤，此处不再赘述。

针对该通信装置 60 为目标接入网设备的情况：

处理单元 602，在收发单元 601 接收到来自用户终端的 RRC 恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与该用户终端之间的第一用户面安全保护方法；确定与该用户终端之间的第一用户面安全密钥；在收发单元 601 接收到来自该用户终端的第一上行用户面数据时，根据该第一用户面安全密钥和第一用户面安全保护方法对第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；

收发单元 601，用于发送该上行用户面数据，具体向核心网中的用户面功能发送该上行用户面数据。

该通信装置 60 为目标接入网设备时，可以实现实施例一至实施例十中目标接入网设备的功能，该通信装置 60 中各个单元执行详细过程可以参见实施例一至实施例十中目标接入网设备的执行步骤，此处不再赘述。

该通信装置 60 为源接入网设备时，可以实现实施例一至实施例十中源接入网设备的功能，该通信装置 60 中各个单元执行详细过程可以参见实施例一至实施例十中源接入网设备的执行步骤，此处不再赘述。

请参见图 12，是本申请实施例提供的通信装置的实体结构简化示意图。该通信装置 70 可以是用户终端，也可以是目标接入网设备，还可以是源接入网设备。

该通信装置 70 包括收发器 701、处理器 702 和存储器 703。收发器 701、处理器 702 和存储器 703 可以通过总线 704 相互连接，也可以通过其它方式相连接。图 11 所示的收发单元 601 所实现的相关功能可以由收发器 701 来实现。图 11 所示的处理单元 602 所实现的相关功能可以通过一个或多个处理器 702 来实现。

存储器 703 包括但不限于是随机存储记忆体（random access memory，RAM）、只读存储器（read-only memory，ROM）、可擦除可编程只读存储器（erasable programmable read only memory，EPROM）、或便携式只读存储器（compact disc read-only memory，CD-ROM），该存储器 703 用于相关指令及数据。

收发器 701 用于发送数据和/或信令，以及接收数据和/或信令。

若该通信装置 70 是实施例一至实施例十中的 UE，则收发器 701 可用于与源接入网设备和目标接入网设备进行通信，例如执行图 7-2 所示实施例中的步骤 702-2、步骤 706-2、步骤 708-2 以及步骤 709-2。

若该通信装置 70 是实施例一至实施例十中的目标接入网设备，则收发器 701 可用于与 UE、源接入网设备和 AMF 进行通信，例如执行图 7-2 所示实施例中的步骤 702-2、步骤 703-2、步骤 704-2、步骤 706-2、步骤 708-2 和步骤 709-2。

若该通信装置 70 是实施例一至实施例十中的源接入网设备，则收发器 701 可用于与目标接入网设备和 UE 进行通信，例如执行图 7-2 所示实施例中的步骤 703-2 和步骤 704-2。

处理器 702 可以包括是一个或多个处理器，例如包括一个或多个中央处理器（central processing unit, CPU），在处理器 702 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

若该通信装置 70 是实施例一至实施例十中的 UE，则处理器 702 可用于执行控制 UE 的操作，例如执行图 7-2 所示实施例中的步骤 701-2 和步骤 707-2。

若该通信装置 70 是实施例一至实施例十中的目标接入网设备，则处理器 702 可用于执行控制目标接入网设备的操作，例如执行图 7-2 所示实施例中的步骤 705-2。

若该通信装置 70 是实施例一至实施例十中的源接入网设备，则处理器 702 可用于执行控制源接入网设备的操作。

存储器 703 用于存储通信装置 70 的程序代码和数据。

关于处理器 702 和收发器 701 所执行的步骤，具体可参见实施例一至实施例十的描述，在此不再赘述。

可以理解的是，图 12 仅仅示出了通信装置的简化设计。在实际应用中，通信装置还可以分别包含必要的其他元件，包含但不限于任意数量的收发器、处理器、控制器、存储器、通信单元等，而所有可以实现本申请的设备都在本申请的保护范围之内。

本申请实施例还提供一种通信系统，可以包括用户终端和目标接入网设备，该用户终端和目标接入网设备可以用于实现实施例一至实施例十中 UE 和目标接入网设备的功能，具体可参见实施例一至实施例十中 UE 和目标接入网设备的具体实现过程。

该通信系统还可以包括源接入网设备，该源接入网设备可以用于实现实施例一至实施例十中源接入网设备的功能，具体可参见实施例一至实施例十中源接入网设备的具体实现过程。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，该流程可以由计算机程序来指令相关的硬件完成，该程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法实施例的流程。而前述的存储介质包括：ROM 或随机存储记忆体 RAM、磁碟或者光盘等各种可存储程序代码的介质。因此，本申请又一实施例提供了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，使得计算机执行上述各方面所述的方法。

本申请又一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，使得计算机执行上述各方面所述的方法。

本领域普通技术人员可以意识到，结合本申请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。

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发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者通过所述计算机可读存储介质进行传输。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（digital subscriber line, 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含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘（solid state disk，SSD））等。

权 利 要 求

1、一种通信方法，其特征在于，包括：

目标接入网设备接收来自用户终端 UE 的无线资源控制 RRC 恢复请求之后，获取第一指示信息；其中，所述第一指示信息用于指示所述 UE 在从连接态进入非激活态之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启；

在所述第一指示信息所指示的用户面安全保护方法可用的情况下，所述目标接入网设备使用所述第一指示信息所指示的用户面安全保护方法激活与所述 UE 之间的用户面安全。

2、根据权利要求 1 所述的方法，其特征在于，所述还包括：

在所述第一指示信息所指示的用户面安全保护方法不可用的情况下，所述目标接入网设备向所述 UE 发送 RRC 消息，所述 RRC 消息用于触发所述用户终端重新建立与所述目标接入网设备之间的 RRC 连接。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述获取第一指示信息，包括：

所述目标接入网设备向源接入网设备发送上下文信息获取请求；

所述目标接入网设备接收来自所述源接入网设备的上下文信息获取响应，其中，所述上下文信息获取响应包括第一指示信息。

4、根据权利要求 3 所述的方法，其特征在于，所述上下文信息获取响应还包括所述源接入网设备使用的加密算法、完整性保护算法以及所述源接入网设备生成的新的接入层密钥 KgNB*；所述方法还包括：

在所述目标接入网设备支持所述源接入网设备使用的加密算法和完整性保护算法的情况下，所述目标接入网设备根据所述 KgNB*确定与所述 UE 之间的第一用户面安全密钥。

5、根据权利要求 1、3 或 4 所述的方法，其特征在于，所述方法还包括：

所述目标接入网设备在接收到来自所述 UE 的第一上行用户面数据时，对所述第一上行用户面数据进行解用户面安全保护，得到上行用户面数据。

6、根据权利要求 1-5 任一所述的方法，其特征在于，所述上下文信息获取响应还包括所述 UE 的用户面安全策略，所述用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。

7、一种通信方法，其特征在于，包括：

源接入网设备向用户终端 UE 发送无线资源控制 RRC 释放消息，所述 RRC 释放消息用于指示所述 UE 进入非激活态；

所述源接入网设备删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥和第一指示信息；其中，所述第一指示信息用于指示所述源接入网设备和所述 UE 在从连接态进入非激活之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启。

8、根据权利要求 7 所述的方法，其特征在于，所述方法还包括：

所述源接入网设备接收来自目标接入网设备的上下文信息获取请求；

所述源接入网设备根据所述上下文信息获取请求，获取所述第一指示信息；

所述源接入网设备向所述目标接入网设备发送上下文信息获取响应，其中，所述上下文信息获取响应包括所述第一指示信息。

9、根据权利要求7或8所述的方法，其特征在于，所述上下文信息获取响应还包括所述UE的用户面安全策略，所述用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。

10、一种通信方法，其特征在于，包括：

用户终端UE接收无线资源控制RRC释放消息，所述RRC释放消息用于指示所述UE进入非激活态；

保存第一指示信息，所述第一指示信息用于指示所述UE从连接态进入非激活态之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述UE向目标接入网设备发送的RRC恢复请求；

所述UE接收所述目标接入网设备发送的RRC恢复消息；

所述UE使用所述第一指示信息所指示的用户面安全保护方法激活与所述目标接入网设备之间的用户面安全。

11、根据权利要求10所述的方法，其特征在于，所述方法还包括：

所述UE确定与所述目标接入网设备之间的第一用户面安全密钥；

所述UE根据所述用户面安全保护方法和所述第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；

所述UE向所述目标接入网设备发送所述第一上行用户面数据。

12、根据权利要求11所述的方法，其特征在于，所述UE确定与所述目标接入网设备之间的第一用户面安全密钥，包括：

所述UE根据所述用户面安全保护方法，确定与所述目标接入网设备之间的第一用户面安全密钥。

13、根据权利要求10-12任一所述的方法，其特征在于，所述UE接收无线资源控制RRC释放消息，包括：

所述UE接收来自源接入网设备发送的无线资源控制RRC释放消息。

14、一种通信系统，其特征在于，包括：目标接入网设备和源接入网设备；其中，

所述目标接入网设备，用于接收来自用户终端UE的无线资源控制RRC恢复请求；向所述源接入网设备发送上下文信息获取请求；

所述源接入网设备，用于接收所述目标接入网设备发送的所述上下文信息获取请求；根据所述上下文信息获取请求，获取第一指示信息，所述第一指示信息用于指示所述源接入网设备和所述UE在从连接态进入非激活之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启；向所述目标接入网设备发送上下文信息获取响应，所述上下文信息获取响应包括所述第一指示信息；

所述目标接入网设备，用于接收所述源接入网设备发送的所述上下文信息获取响应；在所述第一指示信息所指示的用户面安全保护方法可用的情况下，使用所述第一指示信息

所指示的用户面安全保护方法激活与所述 UE 之间的用户面安全。

15、根据权利要求 14 所述的系统，其特征在于，所述目标接入网设备，还用于在所述第一指示信息所指示的用户面安全保护方法不可用的情况下，向所述 UE 发送 RRC 消息，所述 RRC 消息用于触发所述用户终端重新建立与所述目标接入网设备之间的 RRC 连接。

16、根据权利要求 14 所述的系统，其特征在于，所述上下文信息获取响应还包括所述源接入网设备使用的加密算法、完整性保护算法以及所述源接入网设备生成的新的接入层密钥 KgNB*；

所述目标接入网设备，还用于在所述目标接入网设备支持所述源接入网设备使用的加密算法和完整性保护算法的情况下，根据所述 KgNB*确定与所述 UE 之间的第一用户面安全密钥。

17、根据权利要求 14 或 16 所述的系统，其特征在于，所述目标接入网设备，还用于在接收到来自所述用户终端的第一上行用户面数据时，对所述第一上行用户面数据进行解用户面安全保护，得到上行用户面数据。

18、根据权利要求 14-17 任一所述的系统，其特征在于，所述上下文信息获取响应还包括所述用户终端的用户面安全策略，所述用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。

19、根据权利要求 14-18 任一所述的系统，其特征在于，所述源接入网设备，用于向所述 UE 发送 RRC 释放消息，所述 RRC 释放消息用于指示所述 UE 进入所述非激活态；保存所述第一指示信息。

20、一种目标接入网设备，其特征在于，包括处理单元和收发单元；

所述收发单元，用于在接收来自用户终端 UE 的无线资源控制 RRC 恢复请求之后，获取第一指示信息；其中，所述第一指示信息用于指示所述 UE 在从连接态进入非激活态之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述处理单元，用于在所述第一指示信息所指示的用户面安全保护方法可用的情况下，使用所述第一指示信息所指示的用户面安全保护方法激活与所述 UE 之间的用户面安全。

21、根据权利要求 20 所述的目标接入网设备，其特征在于，

所述收发单元，还用于在所述第一指示信息所指示的用户面安全保护方法不可用的情况下，向所述 UE 发送 RRC 消息，所述 RRC 消息用于触发所述用户终端重新建立与所述目标接入网设备之间的 RRC 连接。

22、根据权利要求 20 或 21 所述的目标接入网设备，其特征在于，所述收发单元用于获取第一指示信息时，具体用于向源接入网设备发送上下文信息获取请求；接收来自所述源接入网设备的上下文信息获取响应，其中，所述上下文信息获取响应包括第一指示信息。

23、根据权利要求 22 所述的目标接入网设备，其特征在于，所述上下文信息获取响应还包括所述源接入网设备使用的加密算法、完整性保护算法以及所述源接入网设备生成的新的接入层密钥 KgNB*；

所述处理单元，还用于在所述目标接入网设备支持所述源接入网设备使用的加密算法和完整性保护算法的情况下，所述目标接入网设备根据所述 KgNB*确定与所述 UE 之间的

第一用户面安全密钥。

24、根据权利要求 20、22 或 23 所述的目标接入网设备，其特征在于，

所述处理单元，还用于在所述收发单元接收到来自所述 UE 的第一上行用户面数据时，对所述第一上行用户面数据进行解用户面安全保护，得到上行用户面数据。

25、根据权利要求 20-24 任一所述的目标接入网设备，其特征在于，所述上下文信息获取响应还包括所述 UE 的用户面安全策略，所述用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。

26、一种源接入网设备，其特征在于，包括处理单元和存储单元；

所述收发单元，用于向用户终端 UE 发送无线资源控制 RRC 释放消息，所述 RRC 释放消息用于指示所述 UE 进入非激活态；

所述存储单元，用于删除 RRC 加密密钥、用户面加密密钥和用户面完整性保护密钥，保存 RRC 完整性保护密钥和第一指示信息；其中，所述第一指示信息用于指示所述源接入网设备和所述 UE 在从连接态进入非激活之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启。

27、根据权利要求 26 所述的源接入网设备，其特征在于，

所述收发单元，还用于接收来自目标接入网设备的上下文信息获取请求；根据所述上下文信息获取请求，获取所述第一指示信息；向所述目标接入网设备发送上下文信息获取响应，其中，所述上下文信息获取响应包括所述第一指示信息。

28、根据权利要求 26 或 27 所述的源接入网设备，其特征在于，所述上下文信息获取响应还包括所述 UE 的用户面安全策略，所述用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。

29、一种用户终端，其特征在于，包括收发单元、存储单元和处理单元；

所述收发单元，用于接收无线资源控制 RRC 释放消息，所述 RRC 释放消息用于指示所述 UE 进入非激活态；

所述存储单元，用于保存第一指示信息，所述第一指示信息用于指示所述 UE 从连接态进入非激活态之前所使用的用户面安全保护方法；所述用户面安全保护方法用于指示用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述收发单元，还用于向目标接入网设备发送的 RRC 恢复请求；接收所述目标接入网设备发送的 RRC 恢复消息；

所述处理单元，用于使用所述第一指示信息所指示的用户面安全保护方法激活与所述目标接入网设备之间的用户面安全。

30、根据权利要求 29 所述的用户终端，其特征在于，

所述处理单元，还用于确定与所述目标接入网设备之间的第一用户面安全密钥；根据所述用户面安全保护方法和所述第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；

所述收发单元，还用于向所述目标接入网设备发送所述第一上行用户面数据。

31、根据权利要求 30 所述的用户终端，其特征在于，所述处理单元，具体用于根据所述用户面安全保护方法，确定与所述目标接入网设备之间的第一用户面安全密钥。

32、根据权利要求 29-31 任一所述的用户终端，其特征在于，所述收发单元，具体用于接收来自源接入网设备发送的无线资源控制 RRC 释放消息。

33、一种目标接入网设备，其特征在于，所述目标接入网设备包括存储器和处理器，所述存储器用于存储指令，所述处理器用于执行所述存储器中的指令，使得如权利要求 1-6 任一项所述的方法被实现。

34、一种源接入网设备，其特征在于，所述源接入网设备包括存储器和处理器，所述存储器用于存储指令，所述处理器用于执行所述存储器中的指令，使得如权利要求 7-9 任一项所述的方法被实现。

35、一种用户终端，其特征在于，所述用户终端包括存储器和处理器，所述存储器用于存储指令，所述处理器用于执行所述存储器中的指令，使得如权利要求 10-13 任一项所述的方法被实现。

36、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质包括指令，当所述指令在计算机上运行时，使得计算机执行如权利要求 1-6 任一项所述的方法；或如权利要求 7-9 任一项所述的方法；或如权利要求 10-13 任一项所述的方法。

37、一种包含指令的计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1-6 任一项所述的方法；或如权利要求 7-9 任一项所述的方法；或如权利要求 10-13 任一项所述的方法。

38、一种计算机芯片，其特征在于，所述芯片与存储器相连，所述芯片用于读取并执行所述存储器中存储的软件程序，执行如权利要求 1-6 任一项所述的方法。

39、一种计算机芯片，其特征在于，所述芯片与存储器相连，所述芯片用于读取并执行所述存储器中存储的软件程序，执行如权利要求 7-9 任一项所述的方法。

40、一种计算机芯片，其特征在于，所述芯片与存储器相连，所述芯片用于读取并执行所述存储器中存储的软件程序，执行如权利要求 10-13 任一项所述的方法。

41、一种通信方法，其特征在于，包括：

目标接入网设备在接收到来自用户终端的 RRC 恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与所述用户终端之间的第一用户面安全保护方法；所述第一用户面安全保护方法用于指示所述目标接入网设备和所述用户终端之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述目标接入网设备确定与所述用户终端之间的第一用户面安全密钥；

所述目标接入网设备在接收到来自所述用户终端的第一上行用户面数据时，根据所述第一用户面安全密钥和所述第一用户面安全保护方法对所述第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；

所述目标接入网设备发送所述上行用户面数据。

42、根据权利要求 41 所述的方法，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略；

所述目标接入网设备根据来自源接入网设备的上下文信息获取响应确定与所述用户终端之间的第一用户面安全保护方法，包括：

所述目标接入网设备根据来自源接入网设备的所述用户面安全策略，确定与所述用户

终端之间的第一用户面安全保护方法。

43、根据权利要求 41 所述的方法，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略和第一指示信息，所述第一指示信息用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；其中，所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述目标接入网设备根据来自源接入网设备的上下文信息获取响应确定与所述用户终端之间的第一用户面安全保护方法，包括：

所述目标接入网设备根据来自源接入网设备的所述第一指示信息，将所述第二用户面安全保护方法确定为与所述用户终端之间的第一用户面安全保护方法。

44、根据权利要求 41 所述的方法，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略和第一指示信息，所述第一指示信息用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；其中，所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述目标接入网设备根据来自源接入网设备的上下文信息获取响应确定与所述用户终端之间的第一用户面安全保护方法，包括：

所述目标接入网设备在确定出所述第二用户面安全保护方法不可用或不使用所述第二用户面安全保护方法时，根据所述用户面安全策略，确定与所述用户终端之间的第一用户面安全保护方法；或者

所述目标接入网设备在确定出所述第二用户面安全保护方法不可用或不使用所述第二用户面安全保护方法时，所述目标接入网设备向所述用户终端发送 RRC 消息，所述 RRC 消息用于触发所述用户终端重新建立与所述目标接入网设备之间的 RRC 连接；

所述目标接入网设备在建立所述 RRC 连接的过程中，确定与所述用户终端之间的第一用户面安全保护方法。

45、根据权利要求 41-44 任一项所述的方法，其特征在于，所述目标接入网设备确定与所述用户终端之间的第一用户面安全密钥，包括：

所述目标接入网设备根据所述第一用户面安全保护方法确定与所述用户终端之间的第一用户面安全密钥。

46、根据权利要求 41-44 任一项所述的方法，其特征在于，所述方法还包括：

所述目标接入网设备向所述用户终端发送 RRC 恢复消息，所述 RRC 恢复消息包括第二指示信息，所述第二指示信息用于指示所述第一用户面安全保护方法。

47、一种通信方法，其特征在于，包括：

用户终端在向目标接入网设备发送 RRC 恢复请求之后，确定与所述目标接入网设备之间的第一用户面安全保护方法；所述第一用户面安全保护方法用于指示所述目标接入网设备和所述用户终端之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述用户终端确定与所述目标接入网设备之间的第一用户面安全密钥；

所述用户终端根据所述第一用户面安全保护方法和所述第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；

所述用户终端向所述目标接入网设备发送所述第一上行用户面数据。

48、根据权利要求 47 所述的方法，其特征在于，所述用户终端确定与所述目标接入网设备之间的第一用户面安全保护方法，包括：

所述用户终端接收来自所述目标接入网设备的 RRC 恢复消息，所述 RRC 恢复消息包括第二指示信息，所述第二指示信息用于指示所述第一用户面安全保护方法；

所述用户终端根据所述第二指示信息确定与所述目标接入网设备之间的第一用户面安全保护方法。

49、根据权利要求 48 所述的方法，其特征在于，所述方法还包括：

所述用户终端在接收到所述 RRC 恢复消息之后，释放 RRC 连接。

50、根据权利要求 47 所述的方法，其特征在于，所述方法还包括：

所述用户终端在接收到来自所述目标接入网设备的 RRC 释放消息之后，保存第一指示信息，所述第一指示信息用于指示所述用户终端与源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启。

51、根据权利要求 50 所述的方法，其特征在于，所述用户终端确定与所述目标接入网设备之间的第一用户面安全保护方法，包括：

所述用户终端将所述第一指示信息指示的所述第二用户面安全保护方法确定为与所述目标接入网设备之间的第一用户面安全保护方法。

52、根据权利要求 51 所述方法，其特征在于，所述用户终端将所述第一指示信息指示的所述第二用户面安全保护方法确定为与所述目标接入网设备之间的第一用户面安全保护方法之前，还包括：

所述用户终端接收来自所述目标接入网设备的 RRC 恢复消息，所述 RRC 恢复消息不包括第二指示信息，所述第二指示信息用于指示所述目标接入网设备确定的用户面安全保护方法；

所述用户终端执行将所述第一指示信息指示的所述第二用户面安全保护方法确定为与所述目标接入网设备之间的第一用户面安全保护方法的步骤。

53、根据权利要求 48 或 51 所述的方法，其特征在于，所述用户终端确定与所述目标接入网设备之间的第一用户面安全密钥，包括：

所述用户终端根据所述第一用户面安全保护方法，确定与所述目标接入网设备之间的第一用户面安全密钥。

54、根据权利要求 47 所述的方法，其特征在于，所述方法还包括：

所述用户终端在接收到来自所述目标接入网设备的 RRC 释放消息之后，保存第二用户面安全密钥，所述第二用户面安全密钥为所述用户终端与源接入网设备从连接态进入第三态之前，所使用的用户面安全密钥。

55、一种目标接入网设备，其特征在于，包括处理单元和收发单元；

所述处理单元，用于在所述收发单元接收到来自用户终端的 RRC 恢复消息之后，根据来自源接入网设备的上下文信息获取响应确定与所述用户终端之间的第一用户面安全保护方法；所述第一用户面安全保护方法用于指示所述目标接入网设备和所述用户终端之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；确定与所述用户终端之间的第一用户面安全密钥；在所述收发单元接收到来自所述用户终端的第一上行用户面数据时，根据所述第一用户面安全密钥和所述第一用户面安全保护方法对所述第一上行用户面数据进行解用户面安全保护，得到上行用户面数据；

所述收发单元，用于发送所述上行用户面数据。

56、根据权利要求 55 所述的目标接入网设备，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略；所述处理单元，具体用于根据来自源接入网设备的所述用户面安全策略，确定与所述用户终端之间的第一用户面安全保护方法。

57、根据权利要求 55 所述的目标接入网设备，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略和第一指示信息，所述第一指示信息用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；其中，所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述处理单元，具体用于根据来自源接入网设备的所述第一指示信息，将所述第二用户面安全保护方法确定为与所述用户终端之间的第一用户面安全保护方法。

58、根据权利要求 55 所述的目标接入网设备，其特征在于，所述上下文信息获取响应包括所述用户终端的用户面安全策略和第一指示信息，所述第一指示信息用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护方法；其中，所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；

所述处理单元，具体用于在确定出所述第二用户面安全保护方法不可用或不使用所述第二用户面安全保护方法时，根据所述用户面安全策略，确定与所述用户终端之间的第一用户面安全保护方法；或者在确定出所述第二用户面安全保护方法不可用或不使用所述第二用户面安全保护方法时，控制所述收发单元向所述用户终端发送 RRC 消息，所述 RRC 消息用于触发所述用户终端重新建立与所述目标接入网设备之间的 RRC 连接；在建立所述 RRC 连接的过程中，确定与所述用户终端之间的第一用户面安全保护方法。

59、根据权利要求 55-58 任一项所述的目标接入网设备，其特征在于，所述处理单元，具体用于根据所述第一用户面安全保护方法确定与所述用户终端之间的第一用户面安全密钥。

60、根据权利要求 55-58 任一项所述的目标接入网设备，其特征在于，

所述收发单元，还用于向所述用户终端发送 RRC 恢复消息，所述 RRC 恢复消息包括第二指示信息，所述第二指示信息用于指示所述第一用户面安全保护方法。

61、一种用户终端，其特征在于，包括处理单元和收发单元；

所述处理单元，用于在所述收发单元向目标接入网设备发送 RRC 恢复请求之后，确定与所述目标接入网设备之间的第一用户面安全保护方法；所述第一用户面安全保护方法用于指示所述目标接入网设备和所述用户终端之间的用户面加密保护是否开启和/或用户面完整性保护是否开启；确定与所述目标接入网设备之间的第一用户面安全密钥；根据所述第一用户面安全保护方法和所述第一用户面安全密钥，对上行用户面数据进行用户面安全保护，得到第一上行用户面数据；

所述收发单元，用于向所述目标接入网设备发送所述第一上行用户面数据。

62、根据权利要求 61 所述的用户终端，其特征在于，所述处理单元，具体用于控制所述收发单元接收来自所述目标接入网设备的 RRC 恢复消息，所述 RRC 恢复消息包括第二指示信息，所述第二指示信息用于指示所述第一用户面安全保护用户终端；根据所述第二指示信息确定与所述目标接入网设备之间的第一用户面安全保护用户终端。

63、根据权利要求 62 所述的用户终端，其特征在于，所述处理单元，还用于在所述收发单元接收到所述 RRC 恢复消息之后，释放 RRC 连接。

64、根据权利要求 62 所述的用户终端，其特征在于，所述用户终端还包括存储单元，所述存储单元，用于在所述收发单元接收到来自所述目标接入网设备的 RRC 释放消息之后，保存第一指示信息，所述第一指示信息用于指示所述用户终端与源接入网设备从连接态进入第三态之前，所使用的第二用户面安全保护用户终端；所述第二用户面安全保护方法用于指示所述用户终端与所述源接入网设备从连接态进入第三态之前，所述用户终端与所述源接入网设备之间的用户面加密保护是否开启和/或用户面完整性保护是否开启。

65、根据权利要求 64 所述的用户终端，其特征在于，所述处理单元，具体用于将所述第一指示信息指示的所述第二用户面安全保护用户终端确定为与所述目标接入网设备之间的第一用户面安全保护用户终端。

66、根据权利要求 65 所述的用户终端，其特征在于，所述收发单元，还用于接收来自所述目标接入网设备的 RRC 恢复消息，所述 RRC 恢复消息不包括第二指示信息，所述第二指示信息用于指示所述目标接入网设备确定的用户面安全保护用户终端；所述处理单元执行将所述第一指示信息指示的所述第二用户面安全保护用户终端确定为与所述目标接入网设备之间的第一用户面安全保护用户终端的步骤。

67、根据权利要求 62 或 65 所述的用户终端，其特征在于，所述处理单元，具体用于根据所述第一用户面安全保护用户终端，确定与所述目标接入网设备之间的第一用户面安全密钥。

68、根据权利要求 61 所述的用户终端，其特征在于，所述用户终端还包括存储单元，所述存储单元，用于在所述收发单元接收到来自所述目标接入网设备的 RRC 释放消息之后，保存第二用户面安全密钥，所述第二用户面安全密钥为所述用户终端与源接入网设备从连接态进入第三态之前，所使用的用户面安全密钥。