(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 10 月 25 日 (25.10.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/192513 A1

(51) 国际专利分类号:
H04W 36/00 (2009.01)

(21) 国际申请号: PCT/CN2018/083474

(22) 国际申请日: 2018 年 4 月 18 日 (18.04.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710253561.6 2017年4月18日 (18.04.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 李秉肇 (LI, Bingzhao); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 熊新 (XIONG, Xin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王学龙 (WANG, Xuelong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 曹振臻 (CAO, Zhenzhen); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.); 中国北京市海淀区北清路68号院3号楼101, Beijing 100094 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) **Title:** COMMUNICATION METHOD AND DEVICE

(54) **发明名称:** 通信方法与设备

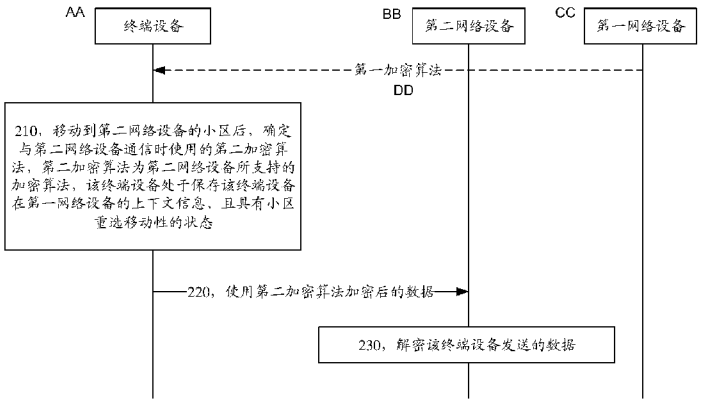

图 2

210 After moving to a cell of a second network device, determine a second encryption algorithm to be used when communicating with the second network device, the second encryption algorithm being an encryption algorithm supported by the second network device, the terminal device being in a state of saving the context information of the terminal device in a first network device and having cell re-selection mobility
220 Use data encrypted by the second encryption algorithm
230 Decrypt the data sent by the terminal device
AA Terminal device
BB Second network device
CC First network device
DD First encryption algorithm

(57) **Abstract:** Provided by the present application are a communication method and device, the communication method comprising: after a terminal device moves to a cell of a second network device, the terminal device determines a second encryption algorithm to be used when communicating with the second network device, the second encryption algorithm being an encryption algorithm supported by the second network device, the terminal device being in a state of saving the context information of the terminal device in a first network device and having cell re-selection mobility, and the first network device being different from the second network device; and

WO 2018/192513 A1

[见续页]

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

the terminal device sends data encrypted by using the second encryption algorithm to the second network device, which may effectively avoid the problem of a network device newly accessed by the terminal device in an inactive state not being able to decrypt data sent by the terminal device.

(57) 摘要：本申请提供一种通信方法与设备，该通信方法包括：终端设备移动到第二网络设备的小区后，该终端设备确定与该第二网络设备通信时使用的第二加密算法，该第二加密算法为该第二网络设备所支持的加密算法，该终端设备处于保存该终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，该第一网络设备不同于该第二网络设备；该终端设备向该第二网络设备发送使用该第二加密算法加密后的数据，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题。

通信方法与设备

本申请要求于2017年04月18日提交中国专利局、申请号为201710253561.6、申请名称为“通信方法与设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，并且更具体地，涉及一种通信方法与设备。

背景技术

终端设备的非激活态指的是，终端设备与无线接入网（Radio Access Network，RAN）设备断开RRC连接，但保留终端设备的上下文信息的状态。在非激活态下，当终端设备移动到新的RAN设备的小区时，可以基于之前保留的该终端设备的上下文，向新的RAN设备（也可称为切换后的RAN设备）发送上行数据。

当前技术中，终端设备与新的RAN设备通信时所使用的加密算法沿用的是该终端设备与之前归属的RAN设备通信时所采用的加密算法（记为第一加密算法）。但是，新的RAN设备不一定支持该第一加密算法，如果不支持，则无法解密终端设备发送的数据。

发明内容

本申请提供一种通信方法与设备，能够有效避免非激活态下的终端设备新接入的网络设备无法解密终端设备发送的数据的问题。

第一方面提供一种通信方法，所述通信方法包括：终端设备移动到第二网络设备的小区后，所述终端设备确定第二加密算法，所述第二加密算法为所述第二网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述第二网络设备；所述终端设备向所述第二网络设备发送使用所述第二加密算法加密后的数据。

所述终端设备处于的所述状态可以称为非激活态。换句话说，终端设备为进入非激活态的终端设备。具体地，第一网络设备可以通过向终端设备发送无线资源控制（Radio Resource Control，RRC）挂起消息，来通知终端设备进入非激活态。

在本申请提供的方案中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，所述加密后的数据是使用所述新的网络设备所支持的加密算法加密的。这样，可以保证所述终端设备向所述新的网络设备发送的数据能够被新的网络设备解密。因此，本申请提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

结合第一方面，在第一方面的一种可能的实现方式中，所述终端设备确定第二加密算法，包括：所述终端设备判断所述第二网络设备是否支持第一加密算法，所述第一加密算

法为所述第一网络设备为所述终端设备配置的加密算法；当所述第二网络设备支持所述第一加密算法时，所述终端设备将所述第一加密算法确定为所述第二加密算法。

可选地，所述第一加密算法为第一网络设备配置的用于终端设备在与第一网络设备通信时使用的加密算法。

可选地，所述第一加密算法为第一网络设备配置的用于终端设备在所述状态（即非激活态）下使用的加密算法。

具体地，第一网络设备可以在配置终端设备进入非激活态之前，向终端设备发送所述第一加密算法；或者，在配置终端设备进入非激活态之前向终端设备发送所述第一加密算法。

第二加密算法可能与第一加密算法相同，也有可能不同。具体地，当第二网络设备支持第一加密算法时，所述第二加密算法可以直接是第一加密算法。当第二网络设备不支持第一加密算法时，所述第二加密算法一定与第一加密算法不同。

可选地，作为一种实现方式，当所述终端设备判断所述第二网络设备不支持所述第一加密算法时，向所述第二网络设备发送 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识；所述终端设备接收所述第二网络设备发送的 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息；所述终端设备根据所述第二指示信息，获取所述第二加密算法。

在本申请提供的方案中，终端设备通过判断第二网络设备是否支持第一网络设备为终端设备配置的加密算法（即第一加密算法），进而采用第二网络设备支持的加密算法向第二网络设备发送数据，这样，可以保证所述终端设备发送的数据能够被所述第二网络设备解密。因此，本申请提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

结合第一方面，在第一方面的一种可能的实现方式中，所述终端设备判断所述第二网络设备是否支持所述第一加密算法，包括：所述终端设备接收所述第二网络设备发送的系统广播消息，所述系统广播消息中包括用于指示所述第二网络设备支持或不支持的加密算法的第一指示信息；所述终端设备根据所述第一指示信息，判断所述第二网络设备是否支持所述第一加密算法。

具体地，当根据所述系统广播消息中的第一指示信息，判断所述第二网络设备支持所述第一加密算法时，直接利用所述第一加密算法对向第二网络设备发送的数据进行加密。

具体地，当根据所述系统广播消息中的第一指示信息，判断所述第二网络设备不支持所述第一加密算法时，可以通过所述第一指示信息获取所述第二网络设备支持的加密算法，或者通过向第二网络设备发送 RRC 连接恢复请求来获取所述第二网络设备支持的加密算法。

在本申请提供的方案中，第二网络设备通过向终端设备发送用于指示第二网络设备支持的加密算法的系统广播消息，使得终端设备能够判断第二网络设备是否支持第一网络设备为终端设备配置的加密算法（即第一加密算法），进而采用第二网络设备支持的加密算法向第二网络设备发送数据，这样，可以保证所述终端设备发送的数据能够被所述第二网络设备解密。因此，本申请提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

结合第一方面，在第一方面的一种可能的实现方式中，所述通信方法还包括：所述终端设备接收所述第一网络设备发送的小区加密算法信息，所述小区加密算法信息用于指示所述第一网络设备的管理区域内的各个小区的加密算法相关信息；所述终端设备判断所述第二网络设备是否支持所述第一加密算法，包括：当所述第二网络设备的小区在所述管理区域内时，所述终端设备根据所述小区加密算法信息，判断所述第二网络设备是否支持所述第一加密算法。

可选地，所述第一网络设备可以在配置终端设备进入非激活态之前或同时，向终端设备发送所述小区加密算法信息。

具体地，所述小区加密算法信息用于指示所述第一网络设备的管理区域内的各个小区的加密算法相关信息。其中，小区的加密算法相关信息可以是下列信息中的任一种或多种：小区支持的加密算法，小区不支持的加密算法，小区支持第一加密算法，小区不支持第一加密算法，通知终端设备进入小区后使用的加密算法。其中，所述管理区域可以是第一网络设备的寻呼区或接入网位置跟踪区，终端设备在所述管理区域内移动时，无需通知第一网络设备，当移动出所述管理区域时需要通知第一网络设备。

可选地，作为一种实现方式，当终端设备当前归属的所述第二网络设备的小区在所述管理区域内时，且根据所述小区加密算法信息，判断所述第二网络设备支持所述第一加密算法时，直接将所述第一加密算法确定为第二加密算法，即在后续数据发送过程中，直接使用第一加密算法对数据加密。

可选地，作为一种实现方式，当终端设备当前归属的所述第二网络设备的小区在所述管理区域内时，且根据所述小区加密算法信息，判断所述第二网络设备不支持所述第一加密算法时，可以通过向第二网络设备发送 RRC 连接恢复请求，来获取第二网络设备支持的第二加密算法；或者也可以根据所述小区加密算法信息，获取所述第二加密算法。

可选地，作为一种实现方式，当所述终端设备确定当前归属的所述第二网络设备的小区不在所述管理区域内时，可以通过如下方式获取所述第二网络设备支持的加密算法：向所述第二网络设备发送 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识；所述终端设备接收所述第二网络设备发送的 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息；所述终端设备根据所述第二指示信息，获取所述第二加密算法。

在本申请提供的方案中，终端设备通过获知第一网络设备的管理区域内的小区加密算法信息，使得终端设备能够判断第二网络设备是否支持第一网络设备为终端设备配置的加密算法（即第一加密算法），进而采用第二网络设备支持的加密算法向第二网络设备发送数据，这样，可以保证所述终端设备发送的数据能够被所述第二网络设备解密。因此，本申请提供的方案能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

结合第一方面，在第一方面的一种可能的实现方式中，所述终端设备确定第二加密算法，包括：

所述终端设备向所述第二网络设备发送第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法；所述终端设备接收所述第二网络设备发送的加密算法更

新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法；所述终端设备根据所述加密算法更新命令，获取所述第二加密算法。

可选地，所述第一加密算法为第一网络设备配置的用于终端设备在与第一网络设备通信时使用的加密算法。

可选地，所述第一加密算法为第一网络设备配置的用于终端设备在所述状态（即非激活态）下使用的加密算法。

具体地，第一网络设备可以在配置终端设备进入非激活态之前，向终端设备发送所述第一加密算法；或者，在配置终端设备进入非激活态之前向终端设备发送所述第一加密算法。

结合第一方面，在第一方面的一种可能的实现方式中，所述终端设备向所述第二网络设备发送的使用所述第二加密算法加密的数据为所述第一数据。

结合第一方面，在第一方面的一种可能的实现方式中，在所述终端设备向所述第二网络设备发送使用所述第二加密算法加密后的所述第一数据之前，所述通信方法还包括：

所述终端设备接收所述第二网络设备发送的第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

在本申请提供的方案中，第二网络设备在判断第二网络设备不支持终端设备当前使用的加密算法（即第一加密算法）时，通知终端设备将加密算法更新为第二网络设备支持的第二加密算法，这样，可以保证所述终端设备发送的数据能够被所述第二网络设备解密。因此，本申请提供的方案能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

第二方面提供一种通信方法，所述通信方法包括：第二网络设备接收终端设备发送的使用第二加密算法加密后的数据，所述第二加密算法为所述第二网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述第二网络设备；所述第二网络设备基于所述第二加密算法，解密所述终端设备发送的数据。

在本申请提供的方案中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，所述加密后的数据是使用所述新的网络设备所支持的加密算法加密的。这样，可以保证所述终端设备向所述新的网络设备发送的数据能够被新的网络设备解密。因此，本申请提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

结合第二方面，在第二方面的一种可能的实现方式中，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括：所述第二网络设备向所述终端设备发送系统广播消息，所述系统广播消息中包括用于指示所述第二网络设备支持或不支持的加密算法的第一指示信息。

结合第二方面，在第二方面的一种可能的实现方式中，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括：所述第二网络设备接收所述终端设备发送的 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识；所述第二网络设备向所述终端设备发送 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息。

结合第二方面，在第二方面的一种可能的实现方式中，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括：

所述第二网络设备接收所述终端设备发送的第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法；所述第二网络设备基于所述终端设备的标识，向所述第一网络设备请求所述终端设备的上下文信息；所述第二网络设备根据所述上下文信息，获取所述第一加密算法；当所述第二网络设备不支持所述第一加密算法时，所述第二网络设备向所述终端设备发送加密算法更新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法。

结合第二方面，在第二方面的一种可能的实现方式中，所述第二网络设备接收的所述终端设备发送的使用所述第二加密算法加密后的数据为所述第一数据。

结合第二方面，在第二方面的一种可能的实现方式中，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括：

所述第二网络设备向所述终端设备发送第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

第三方面提供一种通信方法，所述通信方法包括：终端设备接收第一网络设备发送的通知消息，所述通知消息包括所述终端设备的标识；当发现无线链路失败，所述终端设备进行小区选择或者小区重选，确定当前服务小区；所述终端设备向所述当前服务小区对应的第二网络设备发送连接恢复请求，所述连接恢复请求中携带所述终端设备的标识。

具体地，所述无线链路失败是指所述终端设备与所述网络设备的通讯链路发送故障。

具体地，所述当前服务小区可以是所述网络设备的覆盖小区，也可以是其他网络设备的覆盖。

可选地，所述第一网络设备在与终端设备建立连接时，为所述终端设备分配所述终端设备的标识。

可选地，在所述终端设备切换到所述第一网络设备的小区时，所述第一网络设备为所述终端设备分配所述终端设备的标识。

具体地，所述终端设备的标识包括用于识别所述终端设备的标识以及之前归属的网络设备的标识。所述终端标识用于所述终端设备在无线链路失败后恢复连接使用，或者所述设备标识也可以用于所述终端设备在去激活态进行连接恢复时使用。

在本申请提供的方案中，通过网络设备预先为终端设备配置终端设备的标识，使得当终端设备发现无线链路失败时，可以基于终端设备的标识，及时进行连接恢复。

结合第三方面，在第三方面的一种可能的实现方式中，所述通知消息中还包括密钥信息。所述通信方法还包括，终端设备使用所述密钥信息生成完整性保护信息，并向所述服务网络设备发送所述完整性保护信息。

具体地，可以结合所述密钥信息与终端设备的连接恢复信息，计算得到所述完整性保护信息。或者，可以结合所述密钥信息与所述终端设备的标识，计算得到所述完整性保护信息。

在本申请提供的方案中，网络设备提前为终端设备配置密钥与终端设备的标识，能够使得终端设备发现无线链路失败时，及时、有效地进行连接恢复。

第四方面提供一种终端设备，所述终端设备用于执行上述第一方面或第一方面的任一可能的实现方式中的通信方法。具体地，所述终端设备可以包括用于执行第一方面或第一方面的任一可能的实现方式中的通信方法的模块。

第五方面提供一种终端设备，所述终端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存储的指令，并且对所述存储器中存储的指令的执行使得所述处理器执行第一方面或第一方面的任一可能的实现方式中的方法。

第六方面提供一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现第一方面或第一方面的任一可能的实现方式中的方法。

第七方面提供一种网络设备，所述网络设备用于执行上述第二方面或第二方面的任一可能的实现方式中的通信方法。具体地，所述网络设备可以包括用于执行第二方面或第二方面的任一可能的实现方式中的通信方法的模块。

第八方面提供一种网络设备，所述网络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存储的指令，并且对所述存储器中存储的指令的执行使得所述处理器执行第二方面或第二方面的任一可能的实现方式中的方法。

第九方面提供一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现第二方面或第二方面的任一可能的实现方式中的方法。种

附图说明

图 1 为本发明实施例的架构示意图。

图 2 为本发明实施例提供的通信方法的示意性流程图。

图 3 为本发明实施例提供的通信方法的另一示意性流程图。

图 4 为本发明实施例提供的通信方法的再一示意性流程图。

图 5 为本发明实施例提供的通信方法的再一示意性流程图。

图 6 为本发明实施例提供的通信方法的再一示意性流程图。

图 7 为本发明实施例提供的终端设备的示意性框图。

图 8 为本发明实施例提供的终端设备的另一示意性框图。

图 9 为本发明实施例提供的网络设备的示意性框图。

图 10 为本发明实施例提供的网络设备的另一示意性框图。

图 11 为本申请实施例提供的通信装置的示意性框图。

图 12 为本申请实施例提供的通信装置的另一示意性框图。

图 13 为本申请实施例提供的通信装置的再一示意性框图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

应理解，本发明实施例的技术方案可以应用于长期演进（Long Term Evolution，LTE）架构，还可以应用于通用移动通信系统（Universal Mobile Telecommunications System，UMTS）陆地无线接入网（UMTS Terrestrial Radio Access Network，UTRAN）架构，或者全球移动通信系统（Global System for Mobile Communication，GSM）/增强型数据速率 GSM 演进（Enhanced Data Rate for GSM Evolution，EDGE）系统的无线接入网(GSM EDGE Radio

Access Network，GERAN)架构。在 UTRAN 架构或/GERAN 架构中，MME 的功能由服务通用分组无线业务（General Packet Radio Service，GPRS）支持节点（Serving GPRS Support，SGSN）完成，SGW\PGW 的功能由网关 GPRS 支持节点（Gateway GPRS Support Node，GGSN）完成。本发明实施例的技术方案还可以应用于其他通信系统，例如公共陆地移动网络（Public Land Mobile Network，PLMN）系统，甚至未来的 5G 通信系统或 5G 之后的通信系统等，本发明实施例对此不作限定。

本发明实施例涉及终端设备。终端设备可以为包含无线收发功能、且可以与网络设备配合为用户提供通讯服务的设备。具体地，终端设备可以指用户设备（User Equipment，UE）、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。例如，终端设备可以是蜂窝电话、无绳电话、会话启动协议（Session Initiation Protocol，SIP）电话、无线本地环路（Wireless Local Loop，WLL）站、个人数字处理（Personal Digital Assistant，PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，未来 5G 网络或 5G 之后的网络中的终端设备等，本发明实施例对此不作限定。

本发明实施例还涉及网络设备。网络设备可以是用于与终端设备进行通信的设备，例如，可以是 GSM 系统或 CDMA 中的基站（Base Transceiver Station，BTS），也可以是 WCDMA 系统中的基站（NodeB，NB），还可以是 LTE 系统中的演进型基站（Evolutional Node B，eNB 或 eNodeB），或者该网络设备可以为中继站、接入点、车载设备、可穿戴设备以及未来 5G 网络或 5G 之后的网络中的网络侧设备或未来演进的 PLMN 网络中的网络设备等。

本发明实施例中涉及的网络设备也可称为无线接入网（Radio Access Network，RAN）设备。RAN 设备与终端设备连接，用于接收终端设备的数据并发送给核心网设备。RAN 设备在不同通信系统中对应不同的设备，例如，在 2G 系统中对应基站与基站控制器，在 3G 系统中对应基站与无线网络控制器（Radio Network Controller，RNC），在 4G 系统中对应演进型基站（Evolutional Node B，eNB），在 5G 系统中对应 5G 系统，如新无线接入系统(New Radio Access Technology，NR)中的接入网设备（例如 gNB，CU，DU）。

本发明实施例还涉及核心网（Core Network，CN）设备。CN 设备在不同的通信系统中对应不同的设备，例如，在 3G 系统中对应服务 GPRS 支持节点（Serving GPRS Support Node，SGSN）或网关 GPRS 支持节点（Gateway GPRS Support Node，GGSN），在 4G 系统中对应移动管理实体（Mobility Management Entity，MME）或服务网关（Serving GateWay，S-GW），在 5G 系统中对应 5G 系统的核心网相关设备（例如 NG-Core）。

为了便于理解本申请，首先在此介绍本申请的描述中会引入的几个要素：

连接（Connected）态，终端设备与无线接入网（Radio Access Network，RAN）设备之间建立了无线资源控制（Radio Resource Control，RRC）连接。当终端设备处于连接态时终端设备保存自身的上下文信息，可以执行基于 RAN 控制的小区切换。

空闲（Idle）态，终端设备与 RAN 设备之间没有 RRC 连接，且终端设备与 RAN 设备中不再保存上下文信息。当终端设备处于空闲态时终端设备释放自身的上下文信息，可以执行基于小区的重选。

第三态，终端设备保存其自身的上下文信息并且可以执行基于小区的重选操作，同时，

终端设备的连接信息保存在锚点 RAN 设备，终端设备的连接信息包括终端设备的上下文信息以及核心网连接。在终端设备处于第三态时，终端设备保存一个锚点 RAN 设备配置的管理区域信息，终端设备移动出该管理区域信息对应的管理区域时需要通知锚点 RAN 设备。

第三态还可以称为非激活态，轻连接（Light connection）态，挂起（Suspend）态，去激活态，低开销状态等。管理区域也可以叫做寻呼区（Paging Area），接入网位置跟踪区等。

在终端设备处于第三态时，可以通过恢复（Resume）消息恢复终端设备与 RAN 设备间的 RRC 连接，可选地，还可以恢复终端设备与 RAN 设备间的用于传输数据的数据无线承载（Data Radio Bearer，DRB）。该终端设备的 S1 接口会锚定在一个 RAN 设备（可以称之为锚点 RAN 设备），然后可以执行小区重选移动性，在一个预定的区域（如，称之为“基于 RAN 的寻呼区”，或“无线接入网区”）内移动时不需要通知锚点 RAN 设备，而一旦出了基于 RAN 的寻呼区，则需要向锚点 RAN 设备通知其位置，这个过程称为基于 RAN 的寻呼区更新（Paging Area Update）。本发明实施例中提及的“非激活态”只是用于描述这种状态，而非任何限定。

需要说明的是，本文中提及的以下术语：非激活态，锚点 RAN 设备，无线接入网区（或基于 RAN 的寻呼区）更新，仅为描述方便进行的区分，并不用来限制本发明实施例的范围。

上下文信息，RAN 设备与终端设备建立 RRC 连接之后，RAN 设备为终端设备分配上下文信息，RAN 设备与终端设备基于上下文信息进行通信。

具体地，上下文信息包括终端设备的标识信息、终端设备的安全上下文信息、终端设备的签约信息、终端设备的无线承载的配置信息，逻辑信道信息，以及 Network Slicing Info，Network Slicing Info 中包含当前终端设备在哪些 Network Slicing 内注册，以及每个 Network Slicing 内的 CP Function 的地址，其中，终端设备的无线承载的配置信息包括以下至少一项：分组数据汇聚协议 PDCP 的配置参数，无线链路层控制协议 RLC 的配置参数，媒体接入控制 MAC 的配置参数和/或物理层 PHY 的配置参数，分组数据汇聚协议 PDCP 的变量、计数器和/或定时器的取值，无线链路层控制协议 RLC 的变量、计数器和/或定时器的取值，媒体接入控制 MAC 的变量、计数器和/或定时器的取值和/或物理层 PHY 的变量、计数器和/或定时器的取值，比如，PDCP 包的 COUNT, PDCP 包的 SN。

终端设备的标识，表示能够唯一标识终端设备的标识，可以是由 RAN 设备为终端设备分配的标识，也可以为控制面设备（CP Function）为该终端设备分配的标识。

图 1 为本发明实施例的系统架构示意图。终端设备 110 初始与第一网络设备 120 建立 RRC 连接，即终端设备 110 进入连接态。在连接态，第一网络设备 120 为终端设备 110 分配上下文信息。在连接态，终端设备基于 RRC 连接与第一网络设备 120 进行通信，例如通过第一网络设备 120 访问核心网 140。然后，终端设备 110 断开与第一网络设备 120 的 RRC 连接，但保留终端设备 110 在第一网络设备 120 的上下文信息（即第一网络设备 120 为终端设备 110 分配的上下文信息），即终端设备 110 进入非激活态。在非激活态，终端设备 110 向第二网络设备 130 移动，当移动到第二网络设备 130 的小区内时，终端设备 110 基于之前保留的上下文信息，与第二网络设备 130 进行通信传输，例如通过第一网

络设备 120 访问核心网 140。

图 2 为本发明实施例提供的通信方法 200 的示意性流程图。图 2 中描述的终端设备、第一网络设备、第二网络设备可以分别对应于图 1 中所示的终端设备 110、第一网络设备 120 与第二网络设备 130。如图 2 所示，该通信方法 200 包括:

210，终端设备移动到第二网络设备的小区后，终端设备确定第二加密算法，第二加密算法为第二网络设备所支持的加密算法，终端设备处于保存终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，第一网络设备不同于第二网络设备。

具体地，终端设备所处的状态可以称为非激活态。

该第二加密算法为该第二网络设备所支持的加密算法指的是，第二网络设备能够解密使用该第二加密算法加密后的数据。

220，该终端设备向该第二网络设备发送使用该第二加密算法加密后的数据。

具体地，该终端设备向第二网络设备发送的加密后的数据是使用密钥与该第二加密算法加密的。其中，该密钥可以是该第一网络配置给该终端设备使用的密钥。应理解，该第一网络设备为该终端设备配置该密钥后，在该终端设备配置的上下文信息（即该终端设备在该第一网络设备下的上下文信息）中包括该密钥。该第二网络设备可以通过向该第一网络设备请求该上下文信息，获取该密钥。

应理解，该终端设备在向该第二网络设备发送使用第二加密算法加密后的数据的同时，也会发送该终端设备的标识，该终端设备的标识用于该第二网络设备识别接收到的数据来自于哪个设备。

具体地，该终端设备的标识包括用于识别该终端设备的标识。第二网络设备接收到该终端设备的标识后，能够获知接收到的数据来自于该终端设备。

可选地，该终端设备的标识除了可以包括用于识别该终端设备的标识，还可以包括用于识别该第一网络设备的标识。第二网络设备接收到该终端设备的标识后，能够获知接收到的数据来自于该终端设备，还能够获知该终端设备之前归属的网络设备是该第一网络设备。

进一步地，该终端设备的标识包括的用于识别该终端设备的标识具体可以是用于在该第一网络设备内识别该终端设备的标识。

具体地，该终端设备的标识可以是该第一网络设备为连接态下的终端设备分配的标识。

230，该第二网络设备基于该第二加密算法，解密该终端设备发送的数据。

具体地，该第二网络设备使用该加密算法对应的解密算法解密该数据。

在步骤 220 中已经提及，终端发送的数据是使用密钥与第二加密算法加密的。该第二网络设备可以向该第一网络设备请求该终端设备的上下文信息，从而获取该密钥，进而可以基于该密钥与对应的解密算法解密终端设备发送的数据。

在本发明实施例中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，该加密后的数据是使用该新的网络设备所支持的加密算法加密的。这样，可以保证该终端设备向该新的网络设备发送的数据能够被新的网络设备解密。因此，本发明实施例提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

本发明实施例中的该终端设备为处于非激活下的终端设备。该终端设备进入非激活态的流程可以为：该终端设备接收第一网络设备发送的RRC挂起消息，该RRC挂起消息用于指示该终端设备进入非激活态；该终端设备接收到该RRC挂起消息后，保存该终端设备在该第一网络设备的上下文信息，可以向其他网络设备移动，并可以自主接入临近的小区。其中，该RRC挂起消息具体可以为RRC释放消息，RRC重配置消息或者RRC去激活消息。

具体地，在步骤210中，可选地，作为一种实施例，该终端设备确定第二加密算法，包括：该终端设备判断该第二网络设备是否支持第一加密算法，该第一加密算法为第一网络设备为终端设备配置的加密算法；当该终端设备判断该第二网络设备支持该第一加密算法时，将该第一加密算法确定为该第二加密算法。

可选地，该第一加密算法为第一网络设备配置的用于终端设备在与第一网络设备通信时使用的加密算法。

可选地，该第一加密算法为第一网络设备配置的用于终端设备在该状态（即非激活态）下使用的加密算法。

具体地，终端设备从第一网络设备获取该第一加密算法。可选地，第一网络设备可以在配置终端设备进入非激活态之前，向终端设备发送该第一加密算法；也可以在配置终端设备进入非激活态的同时向终端设备发送该第一加密算法。例如，第一网络设备可以在用于配置终端设备进入非激活态的RRC挂起消息中携带该第一加密算法的信息；或者，可以在向终端设备发送RRC挂起消息之前，向终端设备发送该第一加密算法的信息。其中，该第一加密算法的信息指的是用于指示该第一加密算法的指示信息，该指示信息例如为该第一加密算法的编号或标识。例如，系统预定义多种加密算法，并为每种加密算法分别分配唯一的编号，在后续通信过程中，可以利用加密算法的编号来表示对应的加密算法。

第二加密算法可能与第一加密算法相同，也有可能不同。具体地，当第二网络设备支持第一加密算法时，该第二加密算法可以直接是第一加密算法。当第二网络设备不支持第一加密算法时，该第二加密算法一定与第一加密算法不同。

本文采用“第一加密算法”表示该终端设备之前归属的网络设备（即第一网络设备）为该终端设备配置的加密算法，仅用于在描述上与第二网络设备支持的第二加密算法作区分，并不限定本发明实施例的保护范围。

具体地，当该终端设备判断该第二网络设备支持该第一加密算法时，将该第一加密算法确定为该第二加密算法。即在步骤220中，终端设备直接使用该第一加密算法对将要向第二网络设备发送的数据进行加密。

具体地，当该终端设备判断该第二网络设备不支持该第一加密算法时，可以通过如下方式获取该第二加密算法：向该第二网络设备发送RRC连接恢复请求，该RRC连接恢复请求中包括该终端设备的标识；该第二网络设备接收到RRC连接恢复请求后，向该终端设备发送RRC连接恢复响应，该RRC连接恢复响应中包括用于指示该第二网络设备支持的加密算法的第二指示信息；该终端设备根据该第二指示信息，获取该第二加密算法。

具体地，该第二指示信息例如可以是该第二网络设备支持的加密算法的编号或标识。换句话说，该终端社设备根据该第二指示信息可以获知该第二网络设备支持的加密算法具体是哪个加密算法。

在本发明实施例中，终端设备通过判断第二网络设备是否支持终端设备之前归属的第一网络设备配置的加密算法（即第一加密算法），确定出该第二网络设备所支持的加密算法，从而可以基于该第二网络设备所支持的加密算法向该第二网络设备发送加密后的数据，这样，可以保证该终端设备发送的数据能够被该第二网络设备解密。因此，本发明实施例提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

具体地，该终端设备可以采用多种不同的方式来判断该第二网络设备是否支持第一加密算法。

可选地，作为一种可选实施例，该终端设备判断该第二网络设备是否支持该第一加密算法，包括：该终端设备接收该第二网络设备发送的系统广播消息，该系统广播消息中包括用于指示该第二网络设备支持或不支持的加密算法的第一指示信息；该终端设备根据该第一指示信息，判断该第二网络设备是否支持该第一加密算法。

具体地，该第二网络设备向小区内的设备发送系统广播消息，该系统广播消息中包括用于指示该第二网络设备支持或不支持的加密算法的第一指示信息；处于非激活态的该终端设备移动到该第二网络设备的小区后，接收该第二网络设备的系统广播消息，然后，基于该第一指示信息可以获知该第二网络设备支持哪种或哪几种加密算法，或者不支持哪一种或哪几种加密算法，进而可以获知该第二网络设备是否支持该第一加密算法。

可选地，该第一指示信息可以为第二网络设备支持的加密算法的编号。

例如，系统预定义 10 种加密算法，且分别为这 10 种加密算法定义编号为 1-10。例如该第一指示信息为 1,5,7，则表明该第二网络设备支持的加密算法为编号分别为 1,5 与 7 的加密算法。如果该第一加密算法的编号为 1，则可知第二网络设备支持该第一加密算法；如果该第一加密算法的编号为 9，则可知第二网络设备不支持该第一加密算法。

具体地，在本实施例中，当根据该系统广播消息中的第一指示信息判断该第二网络设备支持该第一加密算法时，直接利用该第一加密算法对向第二网络设备发送的数据进行加密。

具体地，在本实施例中，当根据该系统广播消息中的第一指示信息判断该第二网络设备不支持该第一加密算法时，可以通过该第一指示信息获取该第二网络设备支持的加密算法，或者通过向第二网络设备发送 RRC 连接恢复请求来获取该第二网络设备支持的加密算法。

例如，当该第一指示信息仅指示第二网络设备支持的一种加密算法时，可以直接将该第一指示信息所指示的加密算法确定为第二加密算法。

例如，当该第一指示信息指示第二网络设备支持的多种加密算法时，由于终端设备并不知道第二网络设备当前使用的加密算法是哪种，因此，在这种情形下，终端设备可以向网络设备发送 RRC 连接恢复请求来获知第二网络设备当前使用的加密算法。具体地，终端设备向该第二网络设备发送 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识；该第二网络设备接收到 RRC 连接恢复请求后，向该终端设备发送 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示该第二网络设备当前使用的加密算法的第二指示信息；该终端设备根据该第二指示信息，获取该第二加密算法。

可选地，当该第一指示信息指示第二网络设备支持的多种加密算法时，虽然终端设备

并不知道第二网络设备当前使用的加密算法是哪种，但是第一指示信息所指示的多种加密算法均是第二网络设备所支持的加密算法。因此，终端设备可以选择该多种加密算法中的一种加密算法加密确定为该第二加密算法，并在向第二网络设备发送使用该第二加密算法加密的数据的同时还发送用于指示该第二加密算法的指示信息。对应地，第二网络设备可以根据该第二加密算法的指示信息，确定出用于对终端设备发送的数据进行解密的加密算法。

为了便于更好地理解本发明实施例提供的通信方法，下文结合图 3 详细描述一些具体实施例。图 3 为本发明实施例提供的通信方法 300 的示意性流程图，该通信方法 300 包括:

301，第一网络设备向终端设备发送 RRC 挂起消息。

具体地，在接收到该 RRC 挂起消息之前，终端设备已经从第一网络设备获取到第一加密算法。或者，该 RRC 挂起消息中携带用于指示第一加密算法的信息，终端设备通过该 RRC 挂起消息，获知该第一加密算法。其中，具体地，该 RRC 挂起消息可以是 RRC 释放消息，RRC 去激活消息或 RRC 重配置消息。

可选地，该 RRC 挂起消息还可包括第一网络设备为该终端设备配置的终端设备的标识。

可选地，该 RRC 挂起消息还可包括第一网络设备为该终端设备配置的寻呼区域，终端设备在该寻呼区域内移动时，无需通知第一网络设备。该寻呼区域也可称为管理区域。

302，终端设备接收 RRC 挂起消息后，进入非激活态。

303，终端设备（非激活态的终端设备）移动到第二网络设备的小区后，接收第二网络设备的系统广播消息，该系统广播消息中包括用于指示第二网络设备支持的加密算法的指示信息。

304，终端设备基于该系统广播消息，判断第二网络设备是否支持第一加密算法，若是，转到步骤 305，若否，转到步骤 306。

305，终端设备向第二网络设备发送使用第一加密算法加密后的数据。

306，终端设备向第二网络设备发送 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识。

307，第二网络设备接收 RRC 连接恢复请求后，向终端设备发送 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示第二网络设备支持的加密算法的信息。

308，终端设备接收 RRC 连接恢复响应后，确定第二加密算法。

309，终端设备向第二网络设备发送使用第二加密算法加密的数据。

可选地，第二网络设备的系统广播消息还包括用于指示第二网络设备当前使用的加密算法的信息。这种情形下，当在步骤 304 中，终端设备判断第二网络设备不支持第一加密算法时，可以根据系统广播消息中用于指示第二网络设备当前使用的加密算法的信息，将第二网络设备当前使用的加密算法确定为该第二加密算法。

在本发明实施例中，第二网络设备通过向终端设备发送用于指示第二网络设备支持的加密算法的系统广播消息，使得终端设备能够判断第二网络设备是否支持第一网络设备为终端设备配置的加密算法（即第一加密算法），进而采用第二网络设备支持的加密算法向第二网络设备发送数据，这样，可以保证该终端设备发送的数据能够被该第二网络设备解密。因此，本发明实施例提供的方案，能够有效避免非激活态下的终端设备新接入的网络

设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

可选地，作为另一种可选实施例，该通信方法200还包括：该终端设备接收该第一网络设备发送的小区加密算法信息，该小区加密算法信息用于指示该第一网络设备的管理区域内的各个小区的加密算法相关信息；该终端设备判断该第二网络设备是否支持该第一加密算法，包括：当确定当前归属的该第二网络设备的小区在该管理区域内时，该终端设备根据该小区加密算法信息，判断该第二网络设备是否支持该第一加密算法。

具体地，终端设备在进入非激活态之前或同时，接收该第一网络设备发送的小区加密算法信息。该小区加密算法信息用于指示该第一网络设备的管理区域内的各个小区的加密算法相关信息。

其中，小区的加密算法相关信息可以是下列信息中的任一种或多种：小区支持的加密算法，小区不支持的加密算法，小区支持第一加密算法，小区不支持第一加密算法，通知终端设备进入小区后使用的加密算法。

其中，该管理区域可以是第一网络设备的寻呼区或接入网位置跟踪区，终端设备在该管理区域内移动时，无需通知第一网络设备，当移动出该管理区域时需要通知第一网络设备。

可选地，在本实施例中，当终端设备当前归属的该第二网络设备的小区在该管理区域内时，且根据该小区加密算法信息，判断该第二网络设备支持该第一加密算法时，直接将该第一加密算法确定为第二加密算法，即在后续数据发送过程中，直接使用第一加密算法对数据加密。

可选地，在本实施例中，当终端设备当前归属的该第二网络设备的小区在该管理区域内时，且根据该小区加密算法信息，判断该第二网络设备不支持该第一加密算法时，可以通过向第二网络设备发送RRC连接恢复请求，来获取第二网络设备支持的第二加密算法；或者也可以根据该小区加密算法信息，获取该第二加密算法。

例如，终端设备向该第二网络设备发送RRC连接恢复请求，该RRC连接恢复请求中包括该终端设备的标识；该终端设备接收该第二网络设备发送的RRC连接恢复响应，该RRC连接恢复响应中包括用于指示该第二网络设备支持的加密算法的第二指示信息；该终端设备根据该第二指示信息，获取该第二加密算法。

再例如，终端设备基于该小区加密算法信息，获知当前归属的第二网络设备的小区所支持的加密算法，然后从中选择一种加密算法作为该第二加密算法。优选地，在向第二网络设备发送使用该第二加密算法加密后的数据的同时，可以向第二网络设备发送该第二加密算法的信息，例如，该第二加密算法的编号。

可选地，在本实施例中，当该终端设备确定当前归属的该第二网络设备的小区不在该管理区域内时，可以通过如下方式获取该第二网络设备支持的加密算法：向该第二网络设备发送RRC连接恢复请求，该RRC连接恢复请求中包括该终端设备的标识；该终端设备接收该第二网络设备发送的RRC连接恢复响应，该RRC连接恢复响应中包括用于指示该第二网络设备支持的加密算法的第二指示信息；该终端设备根据该第二指示信息，获取该第二加密算法。

为了便于更好地理解本发明实施例提供的通信方法，下文结合图4详细描述一些具体实施例。图4为本发明实施例提供的通信方法400的示意性流程图，该通信方法400包括：

401，第一网络设备向终端设备发送 RRC 挂起消息，该 RRC 挂起消息用于指示终端设备进入非激活态，该 RRC 挂起消息中还包括小区加密算法信息，该小区加密算法信息用于指示该第一网络设备的管理区域内的各个小区的加密算法相关信息。

具体地，该加密算法相关信息可以是下列信息中的任一种或多种：小区支持的加密算法，小区不支持的加密算法，小区支持第一加密算法，小区不支持第一加密算法，通知终端设备进入小区后使用的加密算法。

可选地，第一网络设备也可以在发送该 RRC 挂起消息之前，向终端设备发送该小区加密算法信息。

具体地，在接收到该 RRC 挂起消息之前，终端设备已经从第一网络设备获取到第一加密算法。或者，该 RRC 挂起消息中携带用于指示第一加密算法的信息，终端设备通过该 RRC 挂起消息，获知该第一加密算法。

可选地，该 RRC 挂起消息还可包括第一网络设备为该终端设备配置的终端设备的标识。

可选地，该 RRC 挂起消息还可包括第一网络设备为该终端设备配置的寻呼区域（即该管理区域），终端设备在该寻呼区域内移动时，无需通知第一网络设备。

其中，具体地，该 RRC 挂起消息可以是 RRC 释放消息，RRC 去激活消息或 RRC 重配置消息。

402，终端设备接收 RRC 挂起消息后，进入非激活态。

403，终端设备（非激活态的终端设备）移动到第二网络设备的小区后，判断当前归属的第二网络设备的小区是否在该管理区域内，若是，转到步骤 404，若否，转到步骤 406。

404，终端设备基于该小区加密算法信息，判断第二网络设备是否支持第一加密算法，若是，转到步骤 405，若否，转到步骤 406。

405，终端设备向第二网络设备发送使用第一加密算法加密后的数据。

406，终端设备向第二网络设备发送 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识。

407，第二网络设备接收 RRC 连接恢复请求后，向终端设备发送 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示第二网络设备支持的加密算法。

408，终端设备接收 RRC 连接恢复响应后，确定第二加密算法。

409，终端设备向第二网络设备发送使用第二加密算法加密的数据。

可选地，在步骤 404 中，若基于该小区加密算法信息，判断第二网络设备不支持第一加密算法的情况下，还可以基于该小区加密算法信息，确定该第二加密算法。具体地，首先通过该小区加密算法信息包括的各个小区的加密算法相关信息，获取到当前归属的第二网络设备的小区所支持的加密算法，然后从中选择一种加密算法作为该第二加密算法。在本实施例中，优选地，在向第二网络设备发送使用该第二加密算法加密后的数据的同时，可以向第二网络设备发送该第二加密算法的信息，例如，该第二加密算法的编号。

在本发明实施例中，终端设备通过获知第一网络设备的管理区域内的小区加密算法信息，使得终端设备能够判断第二网络设备是否支持第一网络设备为终端设备配置的加密算法（即第一加密算法），进而采用第二网络设备支持的加密算法向第二网络设备发送数据，这样，可以保证该终端设备发送的数据能够被该第二网络设备解密。因此，本发明实施例

提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

在上文描述的某些实施例中，由终端设备判断第二网络设备是否支持终端设备当前使用的加密算法（即第一加密算法），然后根据判断结果，采用对应的手段获取第二网络设备支持的加密算法。本发明实施例并非限定于此，还可以由第二网络设备来判断第二网络设备是否支持终端设备当前使用的第一加密算法。

具体地，在步骤 210 中，可选地，作为另一种实施例，该终端设备确定第二加密算法，包括：该终端设备向该第二网络设备发送第一消息，该第一消息包括该终端设备的标识，以及使用第一加密算法加密后的第一数据，该第一加密算法为第一网络设备为终端设备配置的加密算法；该第二网络设备接收该终端设备发送的第一消息后，基于该终端设备的标识，向该第一网络设备请求该终端设备的上下文信息；该第二网络设备根据该上下文信息，获取该第一加密算法；当该第二网络设备确定该第二网络设备不支持该第一加密算法时，向该终端设备发送加密算法更新命令，该加密算法更新命令用于指示将该第一加密算法更新为该第二加密算法；该终端设备根据该加密算法更新命令，获取该第二加密算法。

可选地，该第一加密算法为第一网络设备配置的用于终端设备在与第一网络设备通信时使用的加密算法。

可选地，该第一加密算法为第一网络设备配置的用于终端设备在该状态（即非激活态）下使用的加密算法。

具体地，终端设备从第一网络设备获取该第一加密算法。可选地，第一网络设备可以在配置终端设备进入非激活态之前，向终端设备发送该第一加密算法；也可以在配置终端设备进入非激活态的同时向终端设备发送该第一加密算法。例如，第一网络设备可以在用于配置终端设备进入非激活态的 RRC 挂起消息中携带该第一加密算法的信息；或者，可以在向终端设备发送 RRC 挂起消息之前，向终端设备发送该第一加密算法的信息。其中，该第一加密算法的信息指的是用于指示该第一加密算法的指示信息，该指示信息例如为该第一加密算法的编号或标识。例如，系统预定义多种加密算法，并为每种加密算法分别分配唯一的编号，在后续通信过程中，可以利用加密算法的编号来表示对应的加密算法。

具体地，非激活态的终端设备移动到第二网络设备的小区后，如果需要发送数据时，向第二网络设备发送使用第一加密算法加密后的数据，同时还发送终端设备的标识；第二网络设备接收到终端设备发送到的加密数据后，根据该终端设备的标识向第一网络设备请求该终端设备的上下文信息，然后基于该上下文信息获得该第一加密算法，如果第二网络设备不支持该第一加密算法，则向终端设备发送加密算法更新命令，该加密算法更新命令用于指示将该第一加密算法更新为该第二加密算法，该第二加密算法可以为第二网络设备当前使用的加密算法；该终端设备根据该加密算法更新命令，获取该第二加密算法。

应理解，在本实施例中，如果第二网络设备支持该第一加密算法时，则可以直接使用该第一加密算法对应的解密算法，解密终端设备发送的数据，而无非发送该加密算法更新命令了。

可选地，在本实施例中，当终端设备根据加密算法更新命令获取该第二加密算法后，可以向第二网络设备重发之前使用第一加密算法加密的第一数据，即步骤 220 中，该终端设备向该第二网络设备发送使用该第二加密算法加密后的数据为该第一数据。

优选地，在本实施例中，第二网络设备在向终端设备发送加密算法更新命令的同时或者之后，还可以向终端设备发送第三指示信息，该第三指示信息用于指示将使用该第一加密算法发送的数据进行重传；该终端设备根据该第三指示信息，向第二网络设备重发之前使用第一加密算法加密的第一数据。

为了便于更好地理解本发明实施例提供的通信方法，下文结合图 5 详细描述一些具体实施例。图 5 为本发明实施例提供的通信方法 500 的示意性流程图，该通信方法 500 包括：

501，第一网络设备向终端设备发送 RRC 挂起消息。

步骤 501 同步骤 301，具体描述参见上文，这里不再赘述。

502，终端设备接收 RRC 挂起消息后，进入非激活态。

503，终端设备（非激活态的终端设备）移动到第二网络设备的小区后，需要发送数据时，向第二网络设备发送第一消息，该第一消息包括终端设备的标识，以及使用第一加密算法加密后的第一数据。

504，第二网络设备接收到第一消息后，向第一网络设备发送终端设备的标识，用于请求终端设备的上下文信息。

505，第一网络设备接收到终端设备的标识后，向第二网络设备发送终端设备的上下文信息。

506，第二网络设备根据终端设备的上下文信息，获取该第一加密算法，并判断是否支持该第一加密算法，若是，转到步骤 507，若否，转到步骤 509。

507，第二网络设备向该终端设备发送加密算法更新命令，该加密算法更新命令用于指示将该第一加密算法更新为该第二加密算法。

508，终端设备根据该加密算法更新命令，向第二网络设备发送使用第二加密算法加密后的数据。

可选地，终端设备使用第二加密算法，向第二网络设备重发之前使用第一加密算法加密后的数据，例如步骤 503 中发送的第一数据。

可选地，在步骤 507 之后，或者在步骤 507 中，第二网络设备向该终端设备发送用于指示重发之前使用第一加密算法发送的数据。

509，第二网络设备使用第一加密算法对应的解密算法，解密终端设备发送的第一数据。

在本发明实施例中，第二网络设备在判断第二网络设备不支持终端设备当前使用的加密算法（即第一加密算法）时，通知终端设备将加密算法更新为第二网络设备支持的第二加密算法，这样，可以保证该终端设备发送的数据能够被该第二网络设备解密。因此，本发明实施例提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

综上该，在本发明实施例中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，该加密后的数据是使用该新的网络设备所支持的加密算法加密的。这样，可以保证该终端设备向该新的网络设备发送的数据能够被新的网络设备解密。因此，本发明实施例提供的方案，能够有效避免非激活态下的终端设备新接入的网络设备无法解密该终端设备发送的数据的问题，从而可以提高数据传输的有效性。

如图 6 所示，本发明实施例还提供一种通信方法 600，该通信方法 600 包括：

610，第一网络设备向终端设备发送通知消息，该通知消息包括该终端设备的标识。

可选地，该第一网络设备在与终端设备建立连接时，为该终端设备分配该终端设备的标识。

具体地，该第一网络设备为该终端设备建立 RRC 连接的同时，为终端设备分配终端设备的标识，并可以通过 RRC 连接建立消息向终端设备通知该终端设备的标识。即该通知消息为 RRC 连接建立消息。

可选地，在该终端设备切换到该第一网络设备的小区时，该第一网络设备为该终端设备分配该终端设备的标识。

具体地，在终端设备向第一网络设备切换时，该第一网络设备为终端设备分配该终端设备的标识，并通过切换命令向终端设备通知该终端设备的标识。即该通知消息为切换命令。

具体地，该终端设备的标识包括用于识别该终端设备的标识以及之前归属的网络设备的标识。该终端标识用于该终端设备在无线链路失败后恢复连接使用，或者该设备标识也可以用于该终端设备在去激活态进行连接恢复时使用。

例如，在本实施例中，第一网络设备为终端设备分配的终端设备的标识，包括用于识别该终端设备的标识，还包括用于识别该第一网络设备的标识。进一步地，用于识别该终端设备的标识具体可以是用于在该第一网络设备内识别该终端设备的标识。

620，终端设备根据网络设备发送的通知消息，获取该终端设备的标识。

630，当终端设备发现无线链路失败时，进行小区选择或者小区重选，确定当前服务小区。

具体地，该无线链路失败是指该终端设备与该网络设备的通讯链路发送故障，具体触发原因包括下列原因中的任一种或多种:

该终端设备与该网络设备的通讯链路质量不满足阈值，或

该终端设备解密数据失败或者完整性校验失败，或者

该终端设备的无线链路层控制协议(Radio Link Control，RLC)实体产生故障。

具体地，该当前服务小区可以是该网络设备的覆盖小区，也可以是其他网络设备的覆盖

640，终端设备向该当前服务小区对应的第二网络设备发送连接恢复请求，该连接恢复请求中携带该终端设备的标识。

应理解，本发明实施例中的第二网络设备与第一网络设备可能相同，可能不同。

具体地，该第二网络设备可以根据该终端标识获知该终端之前归属的网络设备为第一网络设备，并向第一网络设备请求终端设备的上下文信息；第一网络设备向第二网络设备发送该终端设备的上下文信息；第二网络设备根据该终端设备的上下文信息为该终端设备恢复连接。

可选地，该连接恢复消息还携带连接恢复的原因，例如该原因为无线链路失败。

在本发明实施例中，通过网络设备预先为终端设备配置终端设备的标识，使得当终端设备发现无线链路失败时，可以基于终端设备的标识，及时进行连接恢复。

可选地，作为一种可选实施例，在步骤 610 中，该通知消息中还包括密钥信息。该通信方法 600 还包括，终端设备使用该密钥信息生成完整性保护信息，并向该服务网络设备

发送该完整性保护信息。

具体地，可以结合该密钥信息与终端设备的连接恢复信息，计算得到该完整性保护信息。或者，可以结合该密钥信息与该终端设备的标识，计算得到该完整性保护信息。

在本发明实施例中，网络设备提前为终端设备配置密钥与终端设备的标识，能够使得终端设备发现无线链路失败时，及时、有效地进行连接恢复。

应理解，本发明实施例中提及的 RRC 连接恢复消息表示用于终端设备和网络设备恢复连接的消息，该消息的具体名称并不对本发明实施例的保护范围作限定。具体地，该 RRC 连接恢复消息还可以表示具有相似功能的消息，包括但不限定于：RRC 连接激活消息，RRC 连接重激活消息，或 RRC 连接重建立消息等。

上文描述了本发明实施例提供的通信方法，下文将描述本发明实施例提供的终端设备与网络设备。

图 7 为本发明实施例提供的终端设备 700 的示意性框图，终端设备 700 包括：

处理模块 710，用于在该终端设备移动到第二网络设备的小区后，确定第二加密算法，该第二加密算法为该第二网络设备所支持的加密算法，该终端设备处于保存该终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，该第一网络设备不同于该第二网络设备；

收发模块 720，用于向该第二网络设备发送使用该第二加密算法加密后的数据。

在本发明实施例中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，所述加密后的数据是使用所述新的网络设备所支持的加密算法加密的。这样，可以保证所述终端设备向所述新的网络设备发送的数据能够被新的网络设备解密。因此，本发明实施例能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

可选地，作为一个实施例，该处理模块 710 用于确定第二加密算法，包括：

该处理模块 710 用于，判断该第二网络设备是否支持第一加密算法，该第一加密算法为该第一网络设备为该终端设备配置的加密算法；当该第二网络设备支持该第一加密算法时，将该第一加密算法确定为该第二加密算法。

可选地，作为一个实施例，该收发模块 720 还用于，接收该第二网络设备发送的系统广播消息，该系统广播消息中包括用于指示该第二网络设备支持或不支持的加密算法的第一指示信息；

该处理模块 710 用于判断该第二网络设备是否支持该第一加密算法，包括：

该处理模块 710 用于，根据该第一指示信息，判断该第二网络设备是否支持该第一加密算法。

可选地，作为一个实施例，该收发模块 720 还用于，接收该第一网络设备发送的小区加密算法信息，该小区加密算法信息用于指示该第一网络设备的管理区域内的各个小区的加密算法相关信息；

该处理模块 710 用于判断该第二网络设备是否支持该第一加密算法，包括：

该处理模块 710 用于，当该第二网络设备的小区在该管理区域内时，根据该小区加密算法信息，判断该第二网络设备是否支持该第一加密算法。

可选地，作为一个实施例，该收发模块 720 还用于，当该第二网络设备不支持该第一

加密算法时，向该第二网络设备发送无线资源控制 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识；

该收发模块 720 还用于，接收该第二网络设备发送的 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示该第二网络设备支持的加密算法的第二指示信息；

该处理模块 710 用于确定第二加密算法，包括：

该处理模块 710 用于，根据该收发模块 720 接收的该第二指示信息，获取该第二加密算法。

可选地，作为一个实施例，该系统广播消息中包括用于指示该第二网络设备支持的加密算法的该第一指示信息；

该处理模块 710 用于确定第二加密算法，包括：

该处理模块 710 用于，当该第二网络设备不支持该第一加密算法时，基于该第一指示信息指示的该第二网络设备支持的加密算法，获取该第二加密算法。

可选地，作为一个实施例，该收发模块 720 还用于，当该第二网络设备的小区不在该管理区域内时，向该第二网络设备发送 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识；接收该第二网络设备发送的 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示该第二网络设备支持的加密算法的第二指示信息；

该处理模块 710 用于确定第二加密算法，包括：

该处理模块 710 用于，根据该第二指示信息，获取该第二加密算法。

可选地，作为一个实施例，该收发模块 720 还用于，向该第二网络设备发送第一消息，该第一消息包括该终端设备的标识，以及使用第一加密算法加密后的第一数据，该第一加密算法为该第一网络设备为该终端设备配置的加密算法；接收该第二网络设备发送的加密算法更新命令，该加密算法更新命令用于指示将该第一加密算法更新为该第二加密算法；

该处理模块 710 用于确定第二加密算法，包括：

该处理模块 710 用于，根据该加密算法更新命令，获取该第二加密算法。

可选地，作为一个实施例，该终端设备向该第二网络设备发送的使用该第二加密算法加密的数据为该第一数据。

可选地，作为一个实施例，该收发模块 720 还用于，在向该第二网络设备发送使用该第二加密算法加密后的该第一数据之前，接收该第二网络设备发送的第三指示信息，该第三指示信息用于指示将使用该第一加密算法发送的数据进行重传。

应理解，本发明实施例中的处理模块 710 可以由处理器或处理器相关电路组件实现，收发模块 720 可以由收发器或收发器相关电路组件实现。

如图 8 所示，本发明实施例还提供一种终端设备 800，该终端设备 800 包括处理器 810，存储器 820 与收发器 830，其中，存储器 820 中存储指令或程序，处理器 810 用于执行存储器 820 中存储的指令或程序。存储器 820 中存储的指令或程序被执行时，该处理器 810 用于执行上述实施例中处理模块 710 执行的操作，收发器 830 用于执行上述实施例中收发模块 720 执行的操作。

应理解，根据本发明实施例的终端设备 700 或终端设备 800 可对应于本发明实施例的通信方法 200 至 500 中的终端设备，并且终端设备 700 或终端设备 800 中的各个模块的操作和/或功能分别为了实现图 2 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘

述。

图 9 为本发明实施例提供的网络设备 900 的示意性流程图，该网络设备 900 包括:

收发模块 910，用于接收终端设备发送的使用第二加密算法加密后的数据，该第二加密算法为该网络设备所支持的加密算法，该终端设备处于保存该终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，该第一网络设备不同于该网络设备;

处理模块 920，用于基于该第二加密算法，解密该终端设备发送的数据。

在本发明实施例中，非激活态的终端设备向新的网络设备（即第二网络设备）发送加密后的数据，所述加密后的数据是使用所述新的网络设备所支持的加密算法加密的。这样，可以保证所述终端设备向所述新的网络设备发送的数据能够被新的网络设备解密。因此，本发明实施例能够有效避免非激活态下的终端设备新接入的网络设备无法解密所述终端设备发送的数据的问题，从而可以提高数据传输的有效性。

可选地，作为一个实施例，该收发模块 910 还用于，在接收该终端设备发送的使用第二加密算法加密后的数据之前，向该终端设备发送系统广播消息，该系统广播消息中包括用于指示该网络设备支持或不支持的加密算法的第一指示信息。

可选地，作为一个实施例，该收发模块 910 还用于，在接收该终端设备发送的使用第二加密算法加密后的数据之前，接收该终端设备发送的无线资源控制 RRC 连接恢复请求，该 RRC 连接恢复请求中包括该终端设备的标识;

该收发模块 910 还用于，向该终端设备发送 RRC 连接恢复响应，该 RRC 连接恢复响应中包括用于指示该网络设备支持的加密算法的第二指示信息。

可选地，作为一个实施例，该收发模块 910 还用于，在接收该终端设备发送的使用第二加密算法加密后的数据之前，接收该终端设备发送的第一消息，该第一消息包括该终端设备的标识，以及使用第一加密算法加密后的第一数据，该第一加密算法为该第一网络设备为该终端设备配置的加密算法;

该处理模块 920 还用于，基于该收发模块 910 接收的该终端设备的标识，向该第一网络设备请求该终端设备的上下文信息;

该处理模块 920 还用于，根据该上下文信息，获取该第一加密算法;

该收发模块 910 还用于，当该网络设备不支持该第一加密算法时，该终端设备发送加密算法更新命令，该加密算法更新命令用于指示将该第一加密算法更新为该第二加密算法。

可选地，作为一个实施例，该网络设备接收的该终端设备发送的使用该第二加密算法加密后的数据为该第一数据。

可选地，作为一个实施例，该收发模块 910 还用于，在接收终端设备发送的使用第二加密算法加密后的数据之前，向该终端设备发送第三指示信息，该第三指示信息用于指示将使用该第一加密算法发送的数据进行重传。

应理解，本发明实施例中的处理模块 920 可以由处理器或处理器相关电路组件实现，收发模块 910 可以由收发器或收发器相关电路组件实现。

如图 10 所示，本发明实施例还提供一种网络设备 1000，该网络设备 1000 包括处理器 1010，存储器 1020 与收发器 1030，其中，存储器 1020 中存储指令或程序，处理器 1010 用于执行存储器 1020 中存储的指令或程序。存储器 1020 中存储的指令或程序被执行时，

该处理器 1010 用于执行上述实施例中处理模块 920 执行的操作，收发器 1030 用于执行上述实施例中收发模块 910 执行的操作。

应理解，根据本发明实施例的网络设备 900 或网络设备 1000 可对应于本发明实施例的通信方法 200 至 500 中的网络设备，并且网络设备 900 或网络设备 1000 中的各个模块的操作和/或功能分别为了实现图 2 至图 5 中的各个方法的相应流程，为了简洁，在此不再赘述。

本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时可以实现上述方法实施例提供的通信方法 200 中与终端设备相关的流程。

本发明实施例还提供计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时可以实现上述方法实施例提供的通信方法 200 中与第二网络设备相关的流程。

本发明实施例还提供一种终端设备，该终端设备包括:

收发模块，用于接收第一网络设备发送的通知消息，该通知消息包括该终端设备的标识;

处理模块，用于在发现无线链路失败时，进行小区选择或者小区重选，确定当前服务小区;

该收发模块还用于，向该当前服务小区对应的第二网络设备发送连接恢复请求，该连接恢复请求中携带该终端设备的标识。

在本发明实施例中，通过网络设备预先为终端设备配置终端设备的标识，使得当终端设备发现无线链路失败时，可以基于终端设备的标识，及时进行连接恢复。

可选地，作为一个实施例，该通知消息中还包括密钥信息；该处理模块还用于，使用该密钥信息生成完整性保护信息；该收发模块还用于，向该服务网络设备发送该完整性保护信息。

在本发明实施例中，网络设备提前为终端设备配置密钥与终端设备的标识，能够使得终端设备发现无线链路失败时，及时、有效地进行连接恢复。

应理解，上述实施例中的处理模块可以由处理器或处理器相关电路组件实现，收发模块可以由收发器或收发器相关电路组件实现。

还应理解，根据本发明实施例的终端设备可对应于本发明实施例的通信方法 600 中的终端设备，并且该终端设备中的各个模块的操作和/或功能分别为了实现图 6 中的相应流程，为了简洁，在此不再赘述。

本发明实施例还提供一种网络设备，该网络设备包括:

处理模块，用于确定终端设备的标识。

收发模块，用于向该终端设备发送通知消息，该通知消息包括该终端设备的标识，以便于该终端设备在发现无线链路失败时，进行连接恢复。

在本发明实施例中，通过网络设备预先为终端设备配置终端设备的标识，使得当终端设备发现无线链路失败时，可以基于终端设备的标识，及时进行连接恢复。

可选地，作为一个实施例，该通知消息中还包括密钥信息，以便于该终端设备根据该密钥信息生成完整性保护信息。

应理解，上述实施例中的处理模块可以由处理器或处理器相关电路组件实现，收发模块可以由收发器或收发器相关电路组件实现。

还应理解，根据本发明实施例的网络设备可对应于本发明实施例的通信方法 600 中的网络设备，并且该网络设备中的各个模块的操作和/或功能分别为了实现图 6 中的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供一种通信装置，该通信装置可以是终端设备也可以是电路。该通信装置可以用于执行上述方法实施例中由终端设备所执行的动作。

当该通信装置为终端设备时，图 11 示出了一种简化的终端设备的结构示意图。便于理解和图示方便，图 11 中，终端设备以手机作为例子。如图 11 所示，终端设备包括处理器、存储器、射频电路、天线以及输入输出装置。处理器主要用于对通信协议以及通信数据进行处理，以及对终端设备进行控制，执行软件程序，处理软件程序的数据等。存储器主要用于存储软件程序和数据。射频电路主要用于基带信号与射频信号的转换以及对射频信号的处理。天线主要用于收发电磁波形式的射频信号。输入输出装置，例如触摸屏、显示屏，键盘等主要用于接收用户输入的数据以及对用户输出数据。需要说明的是，有些种类的终端设备可以不具有输入输出装置。

当需要发送数据时，处理器对待发送的数据进行基带处理后，输出基带信号至射频电路，射频电路将基带信号进行射频处理后将射频信号通过天线以电磁波的形式向外发送。当有数据发送到终端设备时，射频电路通过天线接收到射频信号，将射频信号转换为基带信号，并将基带信号输出至处理器，处理器将基带信号转换为数据并对该数据进行处理。为便于说明，图 11 中仅示出了一个存储器和处理器。在实际的终端设备产品中，可以存在一个或多个处理器和一个或多个存储器。存储器也可以称为存储介质或者存储设备等。存储器可以是独立于处理器设置，也可以是与处理器集成在一起，本申请实施例对此不做限制。

在本申请实施例中，可以将具有收发功能的天线和射频电路视为终端设备的收发单元，将具有处理功能的处理器视为终端设备的处理单元。如图 11 所示，终端设备包括收发单元 1110 和处理单元 1120。收发单元也可以称为收发器、收发机、收发装置等。处理单元也可以称为处理器，处理单板，处理模块、处理装置等。可选的，可以将收发单元 1110 中用于实现接收功能的器件视为接收单元，将收发单元 1110 中用于实现发送功能的器件视为发送单元，即收发单元 1110 包括接收单元和发送单元。收发单元有时也可以称为收发机、收发器、或收发电路等。接收单元有时也可以称为接收机、接收器、或接收电路等。发送单元有时也可以称为发射机、发射器或者发射电路等。

应理解，收发单元 1110 用于执行上述方法实施例中终端设备侧的发送操作和接收操作，处理单元 1120 用于执行上述方法实施例中终端设备上除了收发操作之外的其他操作。

例如，在一种实现方式中，收发单元 1110 用于执行图 2 中的步骤 220 中终端设备侧的发送操作，和/或收发单元 1110 还用于执行本申请实施例中终端设备侧的其他收发步骤。处理单元 1120，用于执行图 2 中的步骤 210，和/或处理单元 1120 还用于执行本申请实施例中终端设备侧的其他处理步骤。

再例如，在另一种实现方式中，收发单元 1110 用于执行图 3 中步骤 301、步骤 303 与步骤 307 中终端设备侧的接收操作或步骤 305、步骤 306 与步骤 309 中终端设备侧的发送操作，和/或收发单元 1120 还用于执行本申请实施例中终端设备侧的其他收发步骤。处理单元 1120 用于执行图 3 中的步骤 302、步骤 304、与步骤 308，和/或处理单元 1120 还

用于执行本申请实施例中终端设备侧的其他处理步骤。

又例如，在再一种实现方式中，收发单元 1110 用于执行图 4 中步骤 401 和步骤 407 中终端设备侧的接收操作或步骤 407 与步骤 405、步骤 406 与步骤 409 中终端设备侧的发送操作，和/或收发单元 1110 还用于执行本申请实施例中终端设备侧的其他收发步骤。处理单元 1120，用于执行图 4 中的步骤 402、步骤 403、步骤 404、和步骤 408，和/或处理单元 1120 还用于执行本申请实施例中终端设备侧的其他处理步骤。

又例如，在再一种实现方式中，收发单元 1110 用于执行图 5 中步骤 501 和步骤 508 中终端设备侧的接收操作或步骤 503 和步骤 509 中终端设备侧的发送操作，和/或收发单元 1110 还用于执行本申请实施例中终端设备侧的其他收发步骤。处理单元 1120，用于执行图 5 中的步骤 502，和/或处理单元 1120 还用于执行本申请实施例中终端设备侧的其他处理步骤。

又例如，在再一种实现方式中，收发单元 1110 用于执行图 6 中步骤 610 中终端设备侧的接收操作或步骤 640 中终端设备侧的发送操作，和/或收发单元 1110 还用于执行本申请实施例中终端设备侧的其他收发步骤。处理单元 1120，用于执行图 6 中的步骤 620 和步骤 630，和/或处理单元 1120 还用于执行本申请实施例中终端设备侧的其他处理步骤。

当该通信装置为芯片时，该芯片包括收发单元和处理单元。其中，收发单元可以是输入输出电路、通信接口；处理单元为该芯片上集成的处理器或者微处理器或者集成电路。

本实施例中的通信装置为终端设备时，可以参照图 12 所示的设备。作为一个例子，该设备可以完成类似于图 8 中处理器 810 的功能。在图 12 中，该设备包括处理器 1210，发送数据处理器 1220，接收数据处理器 1230。上述实施例中的处理模块 710 可以是图 12 中的该处理器 1210，并完成相应的功能。上述实施例中的收发模块 720 可以是图 12 中的发送数据处理器 1220，和/或接收数据处理器 1230。虽然图 12 中示出了信道编码器、信道解码器，但是可以理解这些模块并不对本实施例构成限制性说明，仅是示意性的。

图 13 示出本实施例的另一种形式。处理装置 1300 中包括调制子系统、中央处理子系统、周边子系统等模块。本实施例中的通信装置可以作为其中的调制子系统。具体的，该调制子系统可以包括处理器 1303，接口 1304。其中处理器 1303 完成上述处理模块 710 的功能，接口 1304 完成上述收发模块 720 的功能。作为另一种变形，该调制子系统包括存储器 1306、处理器 1303 及存储在存储器 1306 上并可在处理器上运行的程序，该处理器 1303 执行该程序时实现上述方法实施例中终端设备侧的方法。需要注意的是，所述存储器 1306 可以是非易失性的，也可以是易失性的，其位置可以位于调制子系统内部，也可以位于处理装置 1300 中，只要该存储器 1306 可以连接到所述处理器 1303 即可。

作为本实施例的另一种形式，提供一种计算机可读存储介质，其上存储有指令，该指令被执行时执行上述方法实施例中终端设备侧的方法。

作为本实施例的另一种形式，提供一种包含指令的计算机程序产品，该指令被执行时执行上述方法实施例中终端设备侧的方法。

应理解，本发明实施例中提及的处理器可以是中央处理单元（Central Processing Unit，CPU），还可以是其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（Field Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、

分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

还应理解，本发明实施例中提及的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（Synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）。

需要说明的是，当处理器为通用处理器、DSP、ASIC、FPGA 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件时，存储器（存储模块）集成在处理器中。

应注意，本文描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

还应理解，本文中涉及的第一、第二、第三、第四以及各种数字编号仅为描述方便进行的区分，并不用来限制本申请的范围。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

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

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

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

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

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的

部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

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

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

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

1、一种终端设备，其特征在于，包括:

处理模块，用于在所述终端设备移动到第二网络设备的小区后，确定第二加密算法，所述第二加密算法为所述第二网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述第二网络设备;

收发模块，用于向所述第二网络设备发送使用所述第二加密算法加密后的数据。

2、根据权利要求 1 所述的终端设备，其特征在于，所述处理模块用于确定第二加密算法，包括:

所述处理模块用于，判断所述第二网络设备是否支持第一加密算法，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法; 当所述第二网络设备支持所述第一加密算法时，将所述第一加密算法确定为所述第二加密算法。

3、根据权利要求 2 所述的终端设备，其特征在于，所述收发模块还用于，接收所述第二网络设备发送的系统广播消息，所述系统广播消息中包括用于指示所述第二网络设备支持或不支持的加密算法的第一指示信息;

所述处理模块用于判断所述第二网络设备是否支持所述第一加密算法，包括:

所述处理模块用于，根据所述第一指示信息，判断所述第二网络设备是否支持所述第一加密算法。

4、根据权利要求 2 所述的终端设备，其特征在于，所述收发模块还用于，接收所述第一网络设备发送的小区加密算法信息，所述小区加密算法信息用于指示所述第一网络设备的管理区域内的各个小区的加密算法相关信息;

所述处理模块用于判断所述第二网络设备是否支持所述第一加密算法，包括:

所述处理模块用于，当所述第二网络设备的小区在所述管理区域内时，根据所述小区加密算法信息，判断所述第二网络设备是否支持所述第一加密算法。

5、根据权利要求 2 至 4 中任一项所述的终端设备，其特征在于，所述收发模块还用于，当所述第二网络设备不支持所述第一加密算法时，向所述第二网络设备发送无线资源控制 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识;

所述收发模块还用于，接收所述第二网络设备发送的 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息;

所述处理模块用于确定第二加密算法，包括:

所述处理模块用于，根据所述收发模块接收的所述第二指示信息，获取所述第二加密算法。

6、根据权利要求 3 所述的终端设备，其特征在于，所述系统广播消息中包括用于指示所述第二网络设备支持的加密算法的所述第一指示信息;

所述处理模块用于确定第二加密算法，包括:

所述处理模块用于，当所述第二网络设备不支持所述第一加密算法时，基于所述第一指示信息指示的所述第二网络设备支持的加密算法，获取所述第二加密算法。

7、根据权利要求 4 所述的终端设备，其特征在于，所述收发模块还用于，当所述第二网络设备的小区不在所述管理区域内时，向所述第二网络设备发送 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识；接收所述第二网络设备发送的 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息；

所述处理模块用于确定第二加密算法，包括：

所述处理模块用于，根据所述第二指示信息，获取所述第二加密算法。

8、根据权利要求 1 所述的终端设备，其特征在于，所述收发模块还用于，向所述第二网络设备发送第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法；接收所述第二网络设备发送的加密算法更新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法；

所述处理模块用于确定第二加密算法，包括：

所述处理模块用于，根据所述加密算法更新命令，获取所述第二加密算法。

9、根据权利要求 8 所述的终端设备，其特征在于，所述终端设备向所述第二网络设备发送的使用所述第二加密算法加密的数据为所述第一数据。

10、根据权利要求 9 所述的终端设备，其特征在于，所述收发模块还用于，在向所述第二网络设备发送使用所述第二加密算法加密后的所述第一数据之前，接收所述第二网络设备发送的第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

11、一种网络设备，其特征在于，包括：

收发模块，用于接收终端设备发送的使用第二加密算法加密后的数据，所述第二加密算法为所述网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述网络设备；

处理模块，用于基于所述第二加密算法，解密所述终端设备发送的数据。

12、根据权利要求 11 所述的网络设备，其特征在于，所述收发模块还用于，在接收所述终端设备发送的使用第二加密算法加密后的数据之前，向所述终端设备发送系统广播消息，所述系统广播消息中包括用于指示所述网络设备支持或不支持的加密算法的第一指示信息。

13、根据权利要求 11 所述的网络设备，其特征在于，所述收发模块还用于，在接收所述终端设备发送的使用第二加密算法加密后的数据之前，接收所述终端设备发送的无线资源控制 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识；

所述收发模块还用于，向所述终端设备发送 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述网络设备支持的加密算法的第二指示信息。

14、根据权利要求 11 所述的网络设备，其特征在于，所述收发模块还用于，在接收所述终端设备发送的使用第二加密算法加密后的数据之前，接收所述终端设备发送的第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法；

所述处理模块还用于，基于所述收发模块接收的所述终端设备的标识，向所述第一网络设备请求所述终端设备的上下文信息；

所述处理模块还用于，根据所述上下文信息，获取所述第一加密算法；

所述收发模块还用于，当所述网络设备不支持所述第一加密算法时，所述终端设备发送加密算法更新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法。

15、根据权利要求 14 所述的网络设备，其特征在于，所述网络设备接收的所述终端设备发送的使用所述第二加密算法加密后的数据为所述第一数据。

16、根据权利要求 15 所述的网络设备，其特征在于，所述收发模块还用于，在接收终端设备发送的使用第二加密算法加密后的数据之前，向所述终端设备发送第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

17、一种通信方法，其特征在于，包括:

终端设备移动到第二网络设备的小区后，所述终端设备确定第二加密算法，所述第二加密算法为所述第二网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述第二网络设备;

所述终端设备向所述第二网络设备发送使用所述第二加密算法加密后的数据。

18、根据权利要求 17 所述的通信方法，其特征在于，所述终端设备确定第二加密算法，包括:

所述终端设备判断所述第二网络设备是否支持第一加密算法，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法;

当所述第二网络设备支持所述第一加密算法时，所述终端设备将所述第一加密算法确定为所述第二加密算法。

19、根据权利要求 18 所述的通信方法，其特征在于，所述终端设备判断所述第二网络设备是否支持所述第一加密算法，包括:

所述终端设备接收所述第二网络设备发送的系统广播消息，所述系统广播消息中包括用于指示所述第二网络设备支持或不支持的加密算法的第一指示信息;

所述终端设备根据所述第一指示信息，判断所述第二网络设备是否支持所述第一加密算法。

20、根据权利要求 18 所述的通信方法，其特征在于，所述通信方法还包括:

所述终端设备接收所述第一网络设备发送的小区加密算法信息，所述小区加密算法信息用于指示所述第一网络设备的管理区域内的各个小区的加密算法相关信息;

所述终端设备判断所述第二网络设备是否支持所述第一加密算法，包括:

当所述第二网络设备的小区在所述管理区域内时，所述终端设备根据所述小区加密算法信息，判断所述第二网络设备是否支持所述第一加密算法。

21、根据权利要求 18 至 20 中任一项所述的通信方法，其特征在于，所述终端设备确定第二加密算法，包括:

当所述第二网络设备不支持所述第一加密算法时，所述终端设备向所述第二网络设备发送无线资源控制 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标

识;

所述终端设备接收所述第二网络设备发送的RRC连接恢复响应，所述RRC连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息;

所述终端设备根据所述第二指示信息，获取所述第二加密算法。

22、根据权利要求19所述的通信方法，其特征在于，所述系统广播消息中包括用于指示所述第二网络设备支持的加密算法的所述第一指示信息;

所述终端设备确定第二加密算法，包括:

当所述第二网络设备不支持所述第一加密算法时，所述终端设备基于所述第一指示信息指示的所述第二网络设备支持的加密算法，获取所述第二加密算法。

23、根据权利要求20所述的通信方法，其特征在于，所述终端设备确定第二加密算法，包括:

当所述第二网络设备的小区不在所述管理区域内时，所述终端设备向所述第二网络设备发送RRC连接恢复请求，所述RRC连接恢复请求中包括所述终端设备的标识;

所述终端设备接收所述第二网络设备发送的RRC连接恢复响应，所述RRC连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息;

所述终端设备根据所述第二指示信息，获取所述第二加密算法。

24、根据权利要求17所述的通信方法，其特征在于，所述终端设备确定第二加密算法，包括:

所述终端设备向所述第二网络设备发送第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法;

所述终端设备接收所述第二网络设备发送的加密算法更新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法;

所述终端设备根据所述加密算法更新命令，获取所述第二加密算法。

25、根据权利要求24所述的通信方法，其特征在于，所述终端设备向所述第二网络设备发送的使用所述第二加密算法加密的数据为所述第一数据。

26、根据权利要求25所述的通信方法，其特征在于，在所述终端设备向所述第二网络设备发送使用所述第二加密算法加密后的所述第一数据之前，所述通信方法还包括:

所述终端设备接收所述第二网络设备发送的第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

27、一种通信方法，其特征在于，包括:

第二网络设备接收终端设备发送的使用第二加密算法加密后的数据，所述第二加密算法为所述第二网络设备所支持的加密算法，所述终端设备处于保存所述终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态，所述第一网络设备不同于所述第二网络设备;

所述第二网络设备基于所述第二加密算法，解密所述终端设备发送的数据。

28、根据权利要求27所述的通信方法，其特征在于，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括:

所述第二网络设备向所述终端设备发送系统广播消息，所述系统广播消息中包括用于

指示所述第二网络设备支持或不支持的加密算法的第一指示信息。

29、根据权利要求 27 所述的通信方法，其特征在于，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括:

所述第二网络设备接收所述终端设备发送的无线资源控制 RRC 连接恢复请求，所述 RRC 连接恢复请求中包括所述终端设备的标识;

所述第二网络设备向所述终端设备发送 RRC 连接恢复响应，所述 RRC 连接恢复响应中包括用于指示所述第二网络设备支持的加密算法的第二指示信息。

30、根据权利要求 27 所述的通信方法，其特征在于，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括:

所述第二网络设备接收所述终端设备发送的第一消息，所述第一消息包括所述终端设备的标识，以及使用第一加密算法加密后的第一数据，所述第一加密算法为所述第一网络设备为所述终端设备配置的加密算法;

所述第二网络设备基于所述终端设备的标识，向所述第一网络设备请求所述终端设备的上下文信息;

所述第二网络设备根据所述上下文信息，获取所述第一加密算法;

当所述第二网络设备不支持所述第一加密算法时，所述第二网络设备向所述终端设备发送加密算法更新命令，所述加密算法更新命令用于指示将所述第一加密算法更新为所述第二加密算法。

31、根据权利要求 30 所述的通信方法，其特征在于，所述第二网络设备接收的所述终端设备发送的使用所述第二加密算法加密后的数据为所述第一数据。

32、根据权利要求 31 所述的通信方法，其特征在于，在所述第二网络设备接收终端设备发送的使用第二加密算法加密后的数据之前，所述通信方法还包括:

所述第二网络设备向所述终端设备发送第三指示信息，所述第三指示信息用于指示将使用所述第一加密算法发送的数据进行重传。

33、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求 17 至 26 中任一项所述的通信方法。

34、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求 27 至 32 中任一项所述的通信方法。

35、一种通信装置，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的程序，其特征在于，所述处理器执行所述程序时实现权利要求 17 至 26 中任一项所述的通信方法。

36、一种通信装置，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的程序，其特征在于，所述处理器执行所述程序时实现权利要求 27 至 32 中任一项所述的通信方法。

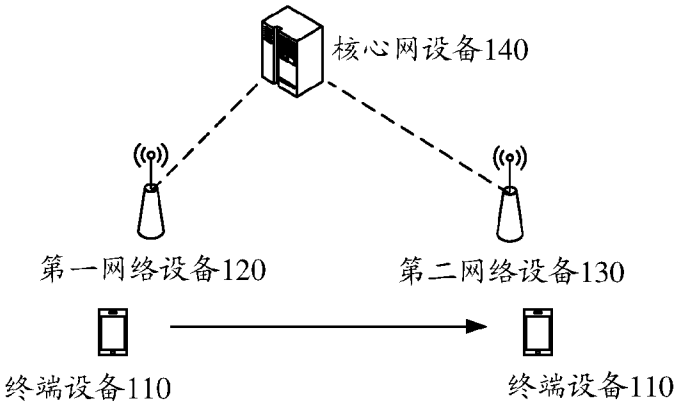
核心网设备140
第一网络设备120
第二网络设备130
终端设备110
终端设备110

图 1

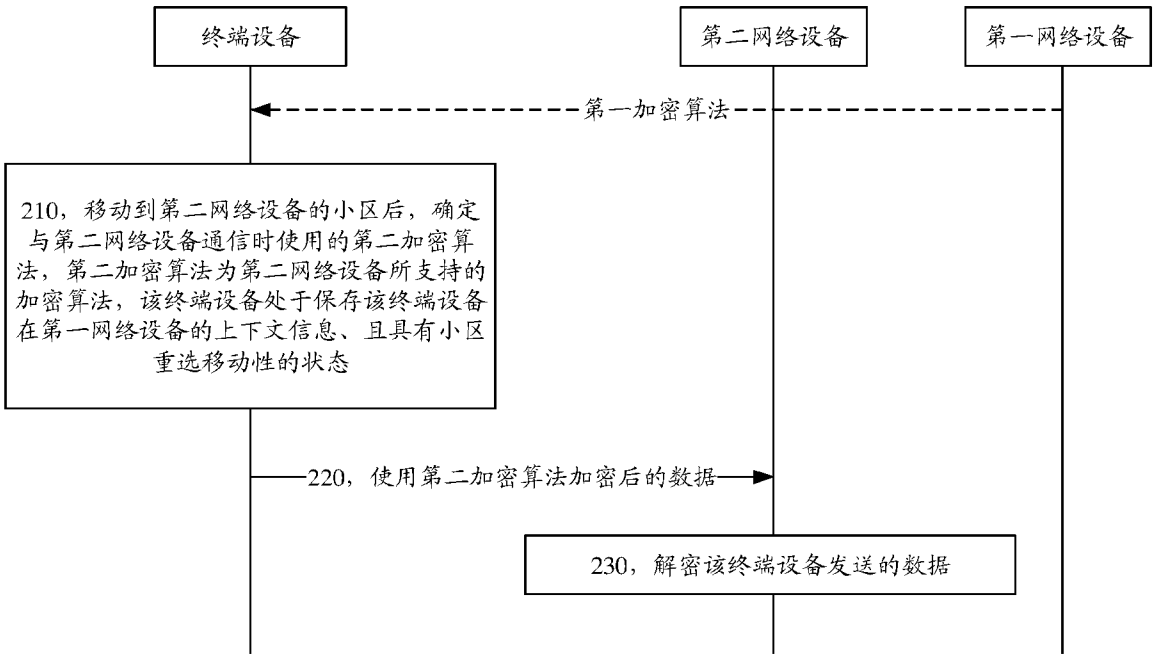
终端设备
第二网络设备
第一网络设备
第一加密算法
210，移动到第二网络设备的小区后，确定与第二网络设备通信时使用的第二加密算法，第二加密算法为第二网络设备所支持的加密算法，该终端设备处于保存该终端设备在第一网络设备的上下文信息、且具有小区重选移动性的状态
220，使用第二加密算法加密后的数据
230，解密该终端设备发送的数据

图 2

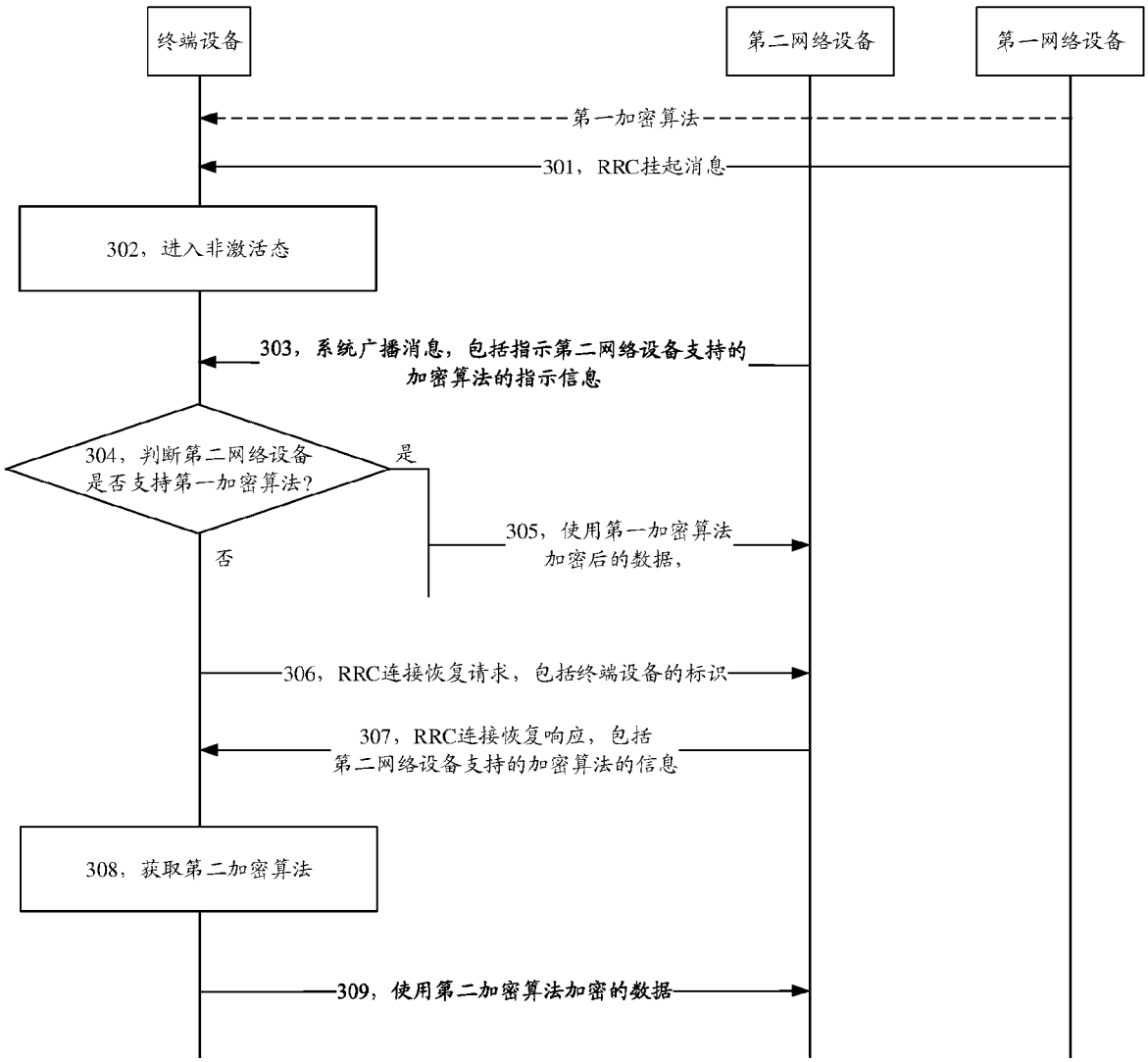
终端设备
第二网络设备
第一网络设备
第一加密算法
301，RRC挂起消息
302，进入非激活态
303，系统广播消息，包括指示第二网络设备支持的加密算法的指示信息
304，判断第二网络设备是否支持第一加密算法？
是
否
305，使用第一加密算法加密后的数据，
306，RRC连接恢复请求，包括终端设备的标识
307，RRC连接恢复响应，包括第二网络设备支持的加密算法的信息
308，获取第二加密算法
309，使用第二加密算法加密的数据

图 3

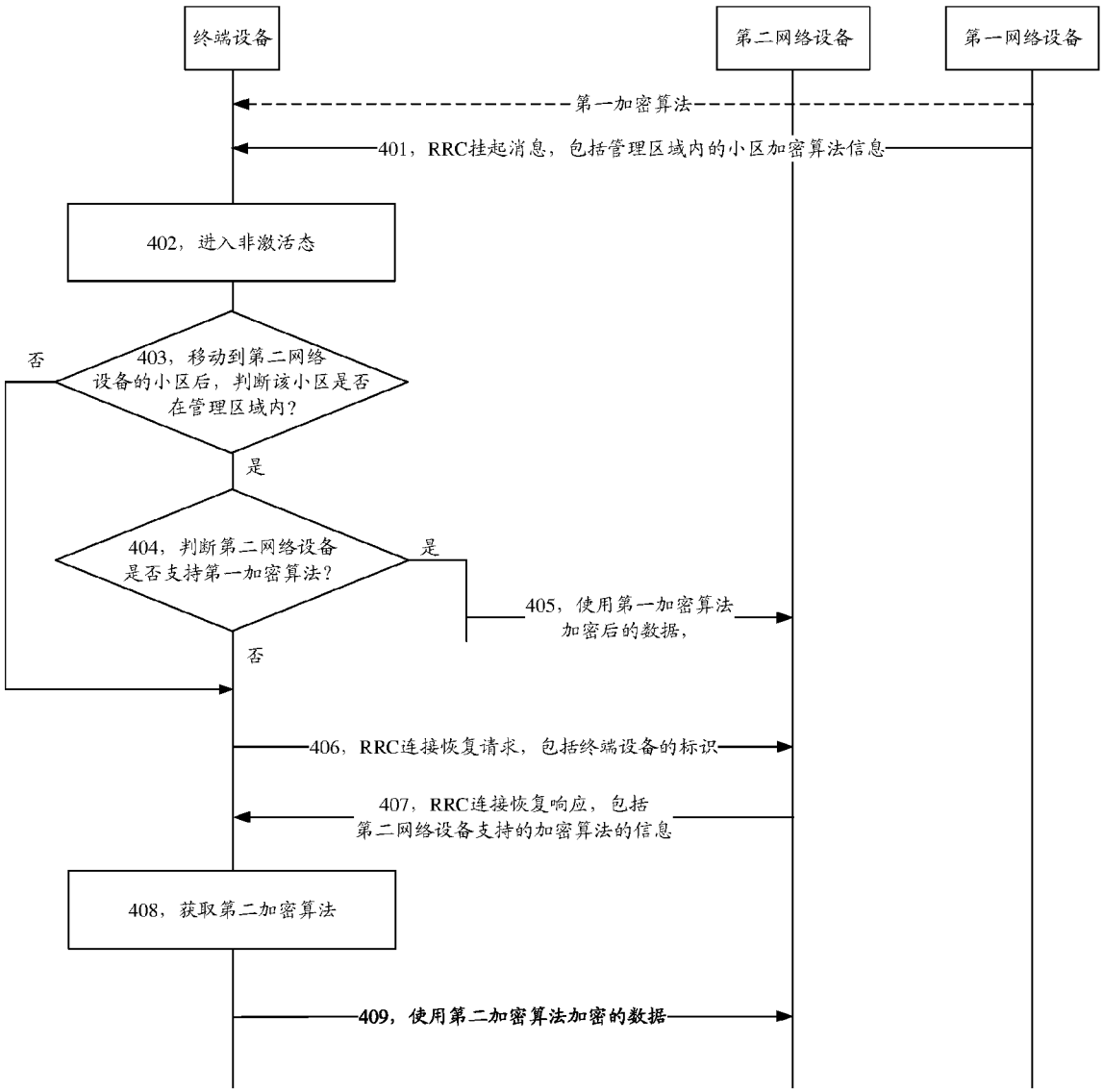
终端设备
第二网络设备
第一网络设备
第一加密算法
401，RRC挂起消息，包括管理区域内的小区加密算法信息
402，进入非激活态
403，移动到第二网络设备的小区后，判断该小区是否在管理区域内？
否
是
404，判断第二网络设备是否支持第一加密算法？
是
405，使用第一加密算法加密后的数据，
否
406，RRC连接恢复请求，包括终端设备的标识
407，RRC连接恢复响应，包括第二网络设备支持的加密算法的信息
408，获取第二加密算法
409，使用第二加密算法加密的数据

图 4

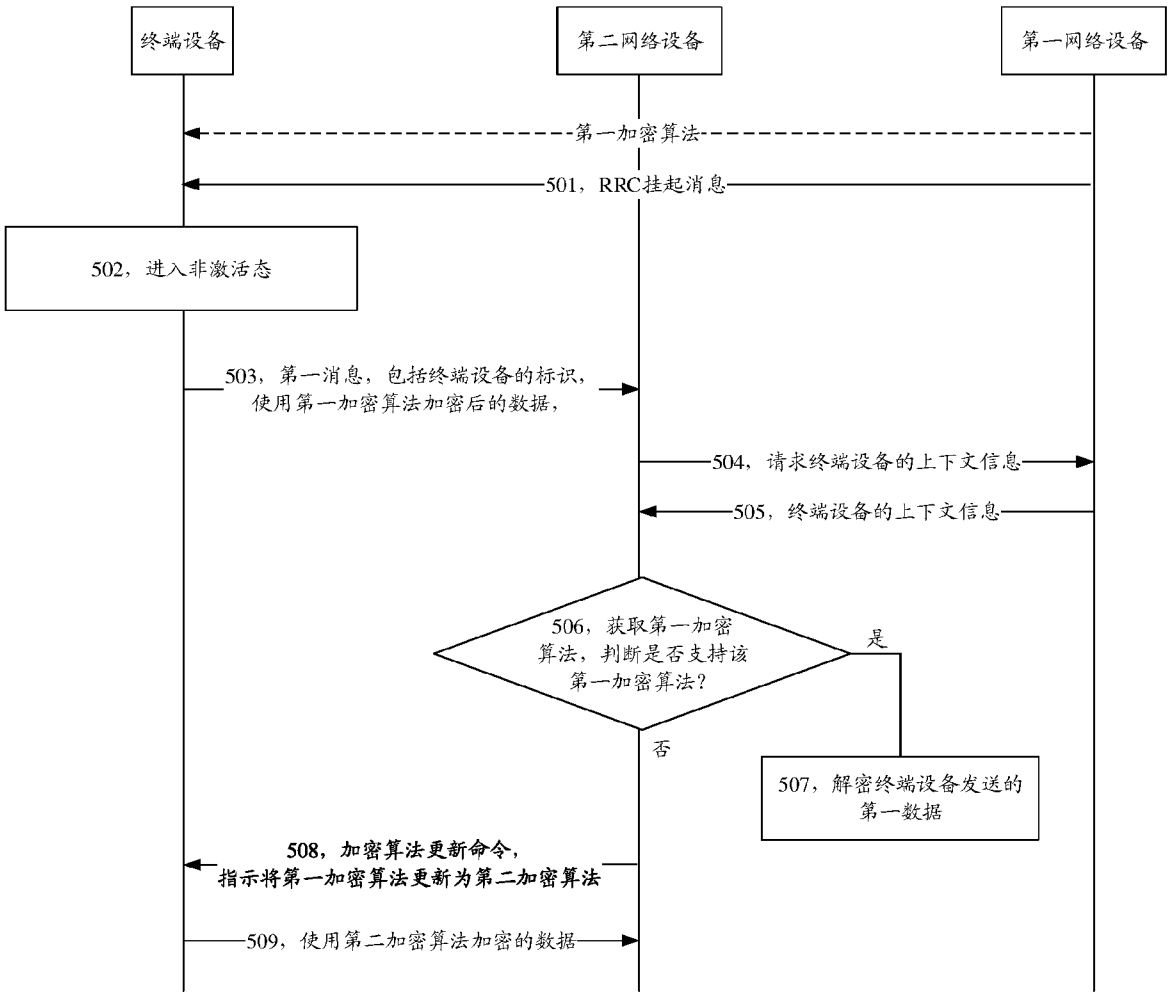
终端设备
第二网络设备
第一网络设备
第一加密算法
501，RRC挂起消息
502，进入非激活态
503，第一消息，包括终端设备的标识，使用第一加密算法加密后的数据，
504，请求终端设备的上下文信息
505，终端设备的上下文信息
506，获取第一加密算法，判断是否支持该第一加密算法？
是
否
507，解密终端设备发送的第一数据
508，加密算法更新命令，指示将第一加密算法更新为第二加密算法
509，使用第二加密算法加密的数据

图 5

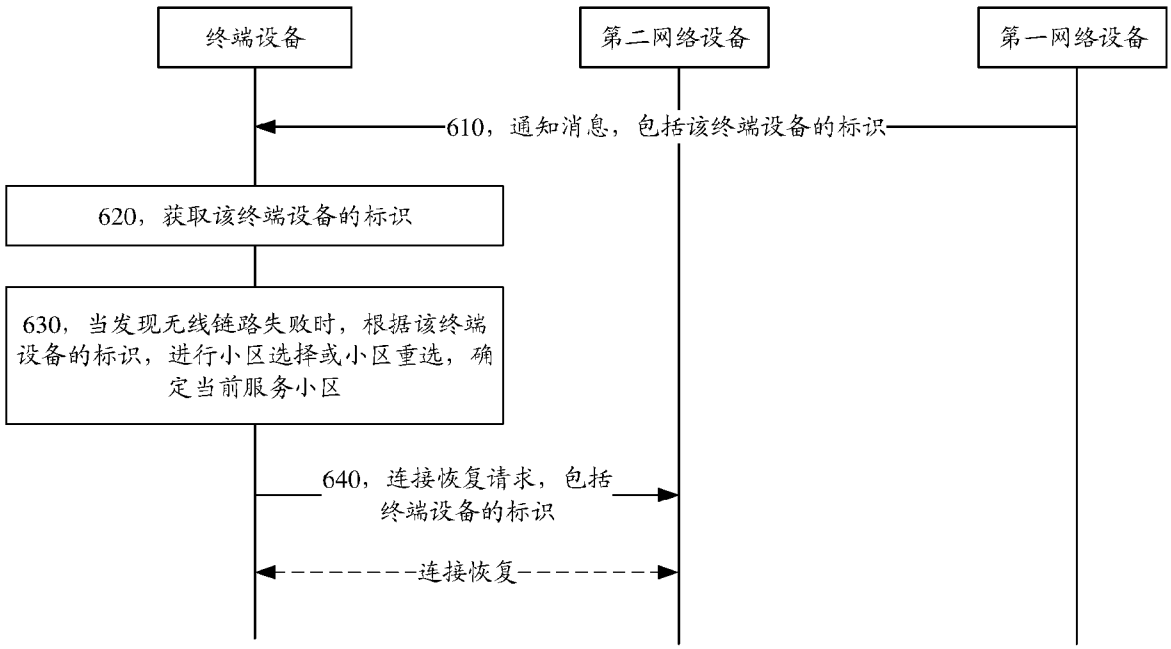
终端设备
第二网络设备
第一网络设备
610，通知消息，包括该终端设备的标识
620，获取该终端设备的标识
630，当发现无线链路失败时，根据该终端设备的标识，进行小区选择或小区重选，确定当前服务小区
640，连接恢复请求，包括终端设备的标识
连接恢复

图 6

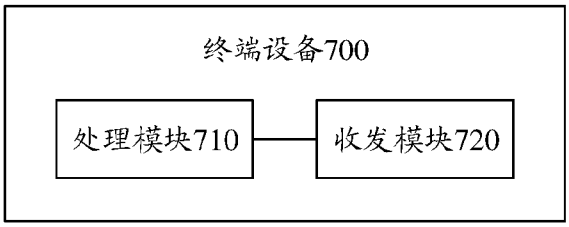
终端设备700
处理模块710
收发模块720

图 7

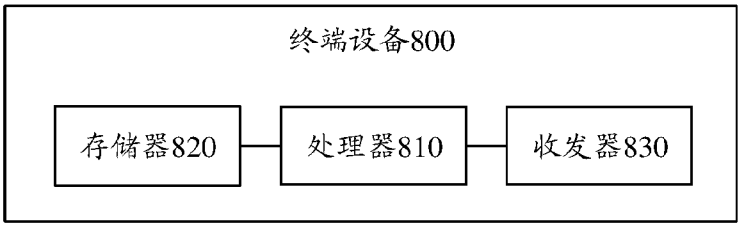
终端设备800
存储器820
处理器810
收发器830

图 8

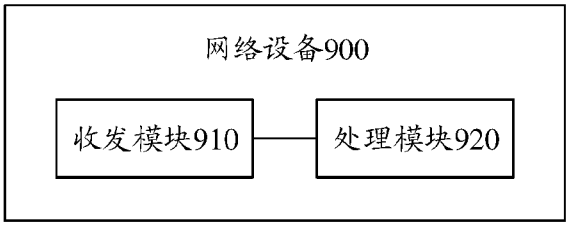
网络设备900
收发模块910
处理模块920

图 9

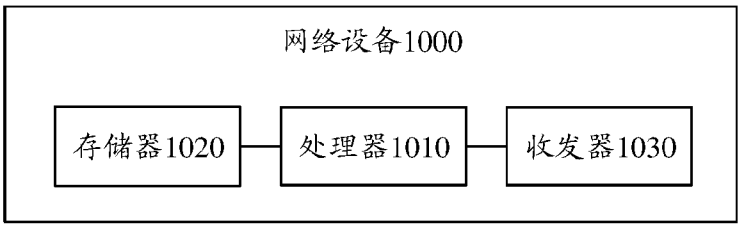
网络设备1000
存储器1020
处理器1010
收发器1030

图 10

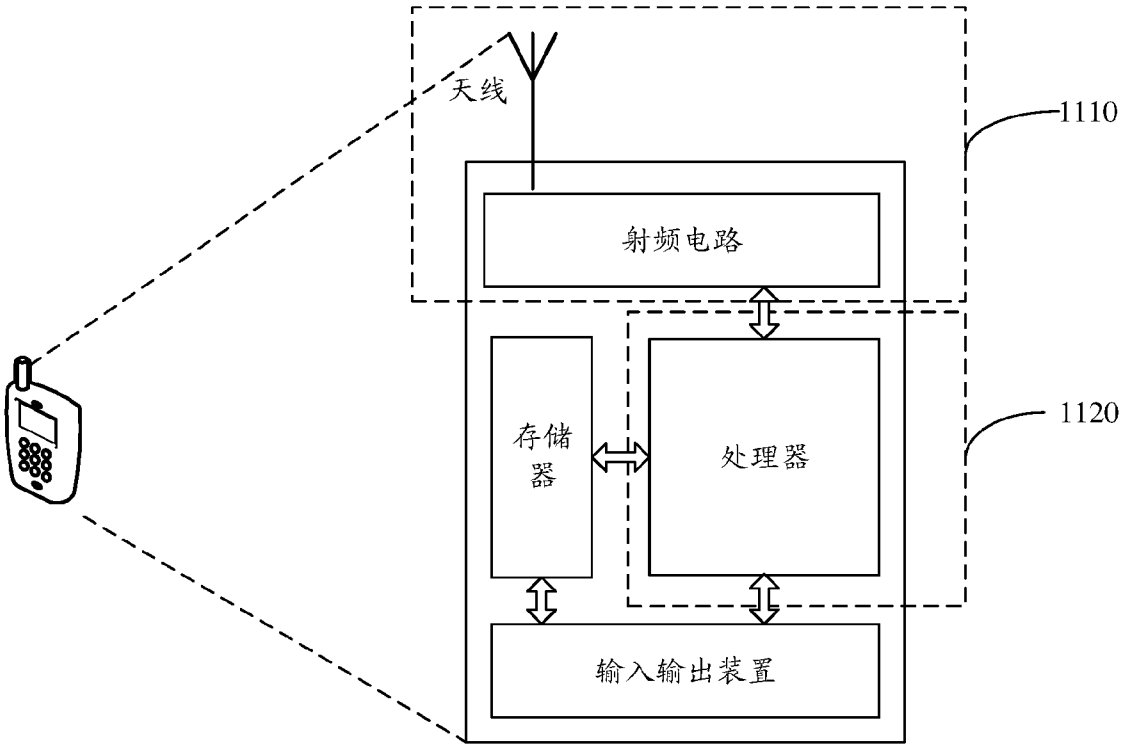
天线
1110
射频电路
存储器
处理器
1120
输入输出装置

图 11

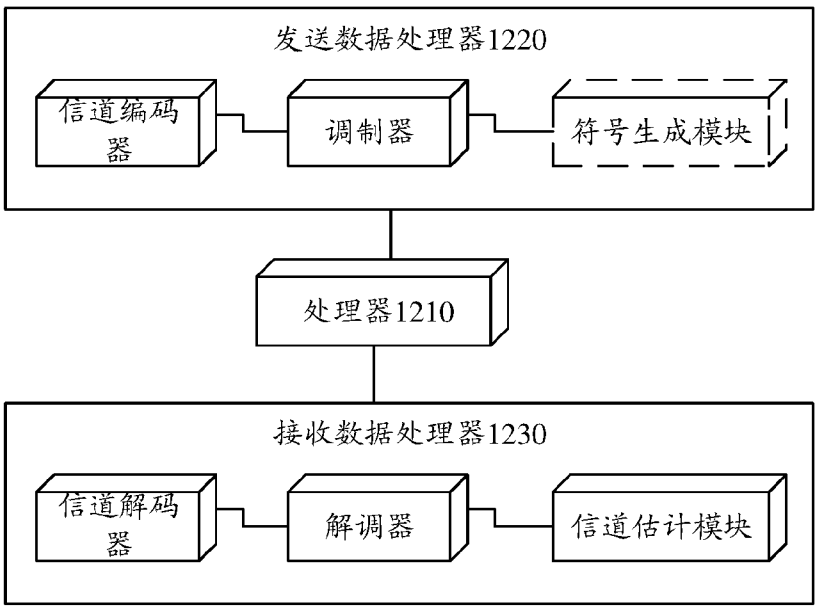
发送数据处理器1220
信道编码器
调制器
符号生成模块
处理器1210
接收数据处理器1230
信道解码器
解调器
信道估计模块

图 12

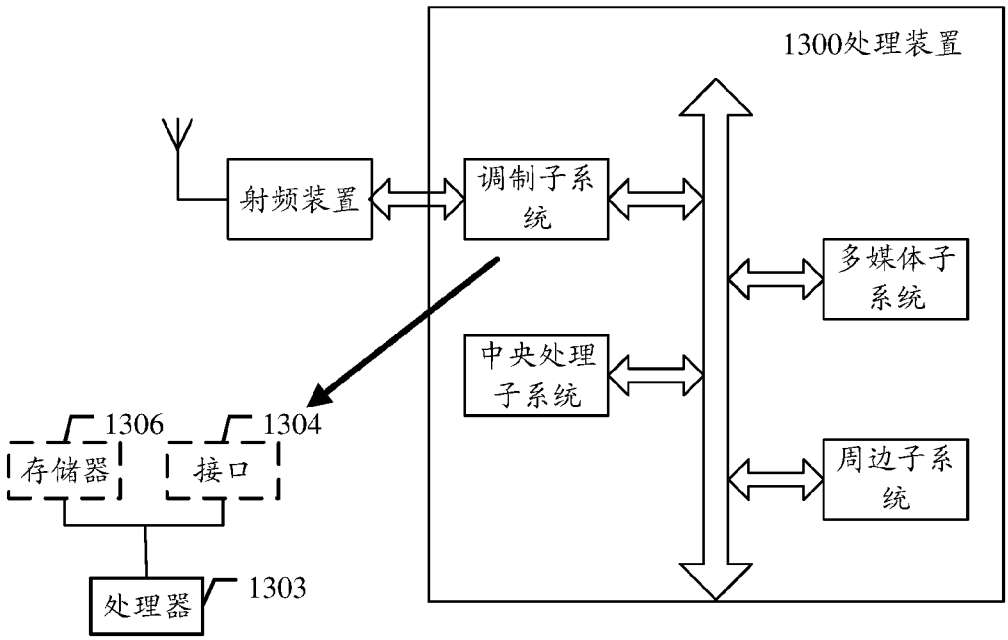
1300处理装置
射频装置
调制子系统
多媒体子系统
中央处理子系统
周边子系统
1306
1304
存储器
接口
处理器
1303

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/083474

A. CLASSIFICATION OF SUBJECT MATTER

H04W 36/00 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 轻连接, 加密算法, 密钥, 非激活, 去激活, 挂起, 支持, 锚点, RAN, RRC, 小区, 重选, 上下文, 恢复, connect??, suspend, resume, anchor, cell, context, encryption, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2017/048170 A1 (TELEFONAKTIEBOLAGET LM ERICSSONPUBL), 23 March 2017 (23.03.2017), description, page 14, paragraph 2 to page 15, paragraph 3, and figure 6	1-36
A	CN 101094096 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 December 2007 (26.12.2007), entire document	1-36
A	CN 101888684 A (ZTE CORP.), 17 November 2010 (17.11.2010), entire document	1-36
A	CN 104219787 A (CHINA ACADEMY OF TELECOMMUNICATIONS TECHNOLOGY), 17 December 2014 (17.12.2014), entire document	1-36
A	CN 101442714 A (ZTE CORP.), 27 May 2009 (27.05.2009), entire document	1-36

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 June 2018	06 July 2018

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
FANG, Ting
Telephone No. 86-010-53961654

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/083474

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2017/048170 A1	23 March 2017	CN 108029015 A	11 May 2018
CN 101094096 A	26 December 2007	None	
CN 101888684 A	17 November 2010	None	
CN 104219787 A	17 December 2014	None	
CN 101442714 A	27 May 2009	None	

国际检索报告

国际申请号
PCT/CN2018/083474

A. 主题的分类

H04W 36/00(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI,WPI,EPODOC,3GPP:轻连接，加密算法，密钥，非激活，去激活，挂起，支持，锚点，RAN，RRC，小区，重选，上下文，恢复，connect??，suspend，resume，anchor，cell，context，encryption，key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	WO 2017/048170 A1 (TELEFONAKTIEBOLAGET LM ERICSSONPUBL) 2017年 3月 23日 (2017-03-23) 说明书第14页第2段-第15页第3段，图6	1-36
A	CN 101094096 A (华为技术有限公司) 2007年 12月 26日 (2007-12-26) 全文	1-36
A	CN 101888684 A (中兴通讯股份有限公司) 2010年 11月 17日 (2010-11-17) 全文	1-36
A	CN 104219787 A (电信科学技术研究院) 2014年 12月 17日 (2014-12-17) 全文	1-36
A	CN 101442714 A (中兴通讯股份有限公司) 2009年 5月 27日 (2009-05-27) 全文	1-36

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 6月 21日	2018年 7月 6日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	方婷
传真号 (86-10)62019451	电话号码 86-010-53961654

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/083474

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
WO 2017/048170 A1	2017年 3月 23日	CN 108029015 A	2018年 5月 11日
CN 101094096 A	2007年 12月 26日	无	
CN 101888684 A	2010年 11月 17日	无	
CN 104219787 A	2014年 12月 17日	无	
CN 101442714 A	2009年 5月 27日	无	