(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
2015 年 8 月 6 日 (06.08.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/113207 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2014/071675

(22) 国际申请日: 2014 年 1 月 28 日 (28.01.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

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

(72) 发明人: **常俊仁 (CHANG, Junren)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **毕皓 (BI, Hao)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **郭轶 (GUO, Yi)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **张冬梅 (ZHANG, Dongmei)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **蔺波 (LIN, Bo)**; 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: **深圳市深佳知识产权代理事务所（普通合伙） (SHENPAT INTELLECTUAL PROPERTY AGENCY)**; 中国广东省深圳市国贸大厦 15 楼西座 1521 室, Guangdong 518014 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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)。

[见续页]

(54) **Title**: SECURITY PASSWORD CHANGING METHOD, BASE STATION, AND USER EQUIPMENT

(54) **发明名称** : 一种安全密钥更改方法和基站及用户设备

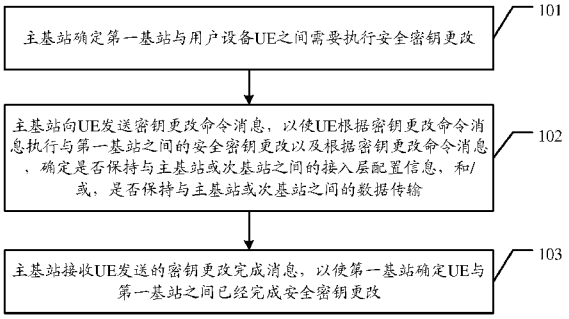

图 1 / FIG. 1

101 THE MENB DETERMINES THAT EXECUTION OF THE SECURITY PASSWORD CHANGE IS REQUIRED BETWEEN THE FIRST BASE STATION AND THE UE

102 THE MENB TRANSMITS TO THE UE THE PASSWORD CHANGE COMMAND MESSAGE, THUS ALLOWING THE UE TO EXECUTE, ON THE BASIS OF THE PASSWORD CHANGE COMMAND MESSAGE, THE SECURITY PASSWORD CHANGE WITH THE FIRST BASE STATION AND TO DETERMINE, ON THE BASIS OF THE PASSWORD CHANGE COMMAND MESSAGE, WHETHER OR NOT TO MAINTAIN THE ACCESS STRATUM CONFIGURATION INFORMATION WITH EITHER THE MENB OR THE SECONDARY BASE STATION AND/OR WHETHER OR NOT TO MAINTAIN DATA TRANSMISSION WITH EITHER THE MENB OR THE SECONDARY BASE STATION

103 THE MENB RECEIVES THE PASSWORD CHANGE COMPLETE MESSAGE TRANSMITTED BY THE UE, THUS ALLOWING THE FIRST BASE STATION TO DETERMINE THAT THE SECURITY PASSWORD CHANGE IS COMPLETED BETWEEN THE UE AND THE FIRST BASE STATION

(57) **Abstract**: A security password changing method, base station, and user equipment (UE). The method may comprise: a main base station (MeNB) determines that execution of a security password change is required between a first base station and a UE, where the first base station comprises at least one base station among the MeNB and a secondary base station; the MeNB transmits to the UE a password change command message, thus allowing the UE to execute, on the basis of the password change command message, the security password change with the first base station and to determine, on the basis of the password change command message, whether or not to maintain access stratum configuration information with either the MeNB or the secondary base station and/or whether or not to maintain data transmission with either the MeNB or the secondary base station; and, the MeNB receives a password change complete message transmitted by the UE, thus allowing the first base station to determine that the security password change is completed between the UE and the first base station.

(57) **摘要**: 一种安全密钥更改方法和基站及用户设备。其中一种方法可包括：主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；所述主基站向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；所述主基站接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

WO 2015/113207 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种安全密钥更改方法和基站及用户设备

技术领域

本发明实施例涉及通信领域，尤其涉及一种安全密钥更改方法和基站及用户设备。

背景技术

目前，为了提高无线网络的传输速率，第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）组织正在讨论成立小小区网络增强的新研究项目。

在现有技术中小小区的部署中通常会采用低频段载波和高频段载波，例如，频率 F1 为低频段载波，其特点是覆盖范围大，但是资源比较稀缺。而 F2 为高频段载波，其特点是覆盖范围小，但是资源比较丰富。在现有的蜂窝网络中，一般使用较低频段的载波，例如使用 F1 为用户提供服务。但是，随时智能手机的普及，用户对无线传输速率提出了更高的要求。为了满足用户的需求，需要逐步使用资源丰富的高频段载波来为用户提供服务。由于高频段载波具有覆盖范围小的特点，通常把这种使用高频段载波进行一定的小覆盖的基站（evolved NodeB，eNB）称为小型基站，该小型基站覆盖的范围一般称之为小小区。一般而言，会将宏基站选择为主基站（Macro evolved NodeB，MeNB），而将小基站选择为次基站（Small evolved NodeB，SeNB）。在 MeNB 下可以有多个小区，从这些多个小区中选出一个小区为主小区 （Primary Cell，PCell）为用户设备（User Equipment，UE）提供服务，而其他小区可以为次小区（Secondary Cell，SCell），并且次基站下的小区一般都选择作为次小区为 UE 提供服务，这种 UE 可以同时使用 MeNB 和 SeNB 分别提供的无线资源进行通信的方式定义为双连接通信，由于双连接通信的数据传输效率高、吞吐量大，越来越多的被用于基站与 UE 之间的数据传输。

在基站和 UE 之间在传输数据时，通常需要使用安全密钥，但是在一些情况下需要对安全密钥进行更改，在长期演进（Long Term Evolution，LTE）系统中，对于安全密钥的更改过程都可以通过小区内切换过程来完成的，其中，小区内切换过程指的是 UE 在执行切换的时候，源小区和目标小区是一个基站

下的同一个小区，即切换前后主小区是相同的一个小区，并没有发生改变。

本发明的发明人在实现本发明的过程中发现: 现有技术中至少存在以下缺陷: 现有的安全密钥更改方法只适用于 UE 与一个基站进行数据传输时的安全密钥更改,但是对于 UE 同时与 MeNB 和 SeNB 执行双连接通信的应用场景下，如何对安全密钥进行更改却并没有给出相关的实现方案。

发明内容

本发明实施例提供了一种安全密钥更改方法和基站及用户设备,用于实现 UE 同时与 MeNB 和 SeNB 执行双连接通信时的安全密钥更改。

第一方面，本发明实施例提供一种安全密钥更改方法，包括:

主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

所述主基站向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息,确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

所述主基站接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

结合第一方面，在第一方面的第一种可能的实现方式中，若所述主基站确定出的所述第一基站包括所述次基站时，所述主基站接收所述 UE 发送的密钥更改完成消息之后，还包括:

所述主基站向所述次基站转发所述密钥更改完成消息,以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

结合第一方面，在第一方面的第二种可能的实现方式中，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

结合第一方面的第二种可能的实现方式,在第一方面的第三种可能的实现方式中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述主基站向所述 UE 发送密钥更改命令消息，包括:

所述主基站向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息,以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

结合第一方面，在第一方面的第四种可能的实现方式中，所述主基站MeNB确定第一基站与用户设备UE之间需要执行安全密钥更改，包括:

所述主基站接收移动管理实体MME发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述UE之间执行密钥再生产Key Re-key，和/或指示所述次基站和所述UE之间执行Key Re-key;

所述主基站根据所述密钥指示命令确定出第一基站与所述UE之间执行Key Re-key。

结合第一方面的第四种可能的实现方式，在第一方面的第五种可能的实现方式中，若所述主基站确定所述第一基站与所述UE之间执行Key Re-key，所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

结合第一方面，在第一方面的第六种可能的实现方式中，若所述主基站确定出的所述第一基站包括所述次基站时，所述主基站MeNB确定第一基站与用户设备UE之间需要执行安全密钥更改之后，还包括:

所述主基站向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括: 所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括: 所述MME为所述次基站生成的次基站侧中间密钥。

结合第一方面，在第一方面的第七种可能的实现方式中，所述主基站MeNB确定第一基站与用户设备UE之间需要执行安全密钥更改，包括:

所述主基站判断所述UE当前在主基站侧的分组数据汇聚协议计数PDCP Count在预置次数内是否发生反转，若所述UE当前在主基站侧的PDCP Count在预置次数发生反转，则所述主基站确定第一基站与所述UE之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新Key Refresh，其中，所述第一基站为所述主基站;

和/或，

当所述主基站接收到所述次基站发送的次基站侧的PDCP Count在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需

要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，所述主基站确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

结合第一方面或第一方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能的实现方式，在第一方面的第八种可能的实现方式中，所述密钥更改命令消息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

结合第一方面的第八种可能的实现方式，在第一方面的第九种可能的实现方式中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第一方面或第一方面的的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能的实现方式，在第一方面的第十种可能的实现方式中，所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

结合第一方面的第十种可能的实现方式，在第一方面的第十一种可能的实现方式中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第一方面，在第一方面的第十二种可能的实现方式中，所述密钥更改命令消息中通过密钥改变指示 Key Change Indicator 字段的取值指示所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第一方面，在第一方面的第十三种可能的实现方式中，所述密钥更改

命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，或指示所述 UE 暂停与所述第一基站之间的数据传输，或指示所述 UE 停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

结合第一方面或第一方面的的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第一方面的第十四种可能的实现方式中，所述密钥更改命令消息具体为小区内切换 HO 命令消息。

第二方面，本发明实施例提供另一种安全密钥更改方法，包括:

用户设备 UE 接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述 UE 与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改;

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

所述 UE 向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

结合第二方面，在第二方面的第一种可能的实现方式中，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息，所述 UE 接收主基站发送的密钥更改命令消息之后，还包括:

所述 UE 根据所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息确定是否在所述第一基站执行随机接入。

结合第二方面或第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述 UE 接收主基站发送的密钥更改命令消息，包括:

所述 UE 接收所述主基站发送的包含随机接入资源的信息的密钥更改命令

消息，并根据所述随机接入资源的信息执行向所述第一基站的随机接入。

结合第二方面，在第二方面的第三种可能的实现方式中，若所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述 UE 根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

结合第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 根据所述第一指示信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 根据所述第二指示信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

结合第二方面，在第二方面的第五种可能的实现方式中，所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述 UE 根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

结合第二方面的第五种可能的实现方式，在第二方面的第六种可能的实现方式中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所

述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述UE根据所述第一安全密钥上下文信息按照Key Re-key或Key Refresh执行与所述主基站之间的安全密钥更改；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh，所述UE根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述UE根据所述第二安全密钥上下文信息按照Key Re-key或Key Refresh执行与所述次基站之间的安全密钥更改。

结合第二方面，在第二方面的第七种可能的实现方式中，若所述密钥更改命令消息中包含的指示信息为密钥改变指示Key Change Indicator字段，所述UE根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述UE通过所述Key Change Indicator字段的取值指示确定按照Key Re-key或Key Refresh执行与所述第一基站之间的安全密钥更改。

结合第二方面，在第二方面的第八种可能的实现方式中，所述UE根据所述密钥更改命令信息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，包括：

所述UE根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述UE之间需要执行安全密钥更改；

或者，

所述UE根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述UE之间需要执行安全密钥更改；

或者，

所述UE根据所述密钥更改命令消息中包含的密钥改变指示Key Change Indicator字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息；

或者，

所述 UE 根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

结合第二方面的第八种可能的实现方式，在第二方面的第九种可能的实现方式中，所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息，包括:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，所述 UE 确定不保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，所述 UE 确定保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时，所述 UE 确定保持与所述主基站或所述次基站之间的接入层配置信息。

结合第二方面，在第二方面的第十种可能的实现方式中，所述 UE 根据所述密钥更改命令信息，确定是否保持与所述主基站或所述次基站之间的数据传输，包括:

所述UE根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

所述UE根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输；

或者，

所述 UE 根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

结合第二方面的第十种可能的实现方式，在第二方面的第十一种可能的实现方式中，所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输，包括：

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，所述 UE 确定不保持与所述主基站以及次基站之间的数据传输；或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，所述 UE 确定保持与所述次基站之间的数据传输；

或者，

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，所述 UE 确定保持与所述次基站之间的数据传输。

结合第二方面，在第二方面的第十二种可能的实现方式中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述主基站之间的接入层配置信息，和/或，需要保持与所述主基站之间的数据传输时，所述保持与所述主基站之间的接入层配置信息，和/或，保持与所述主基站之间的数据传输，包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

所述 UE 保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活

状态;

所述 UE 保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI;

所述 UE 保持或暂停所述 UE 与所述主基站之间的数据传输。

结合第二方面，在第二方面的第十三种可能的实现方式中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，所述保持与所述次基站之间的接入层配置信息，和/或，保持与所述次基站之间的数据传输，包括如下步骤中的至少一个步骤:

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态;

所述 UE 保持所述 UE 与所述次基站之间通信使用的 C-RNTI;

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第十四种可能的实现方式中，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，包括: 当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，所述 UE 按照 Key Refresh 执行与所述主基站之间的安全密钥更改;

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤:

所述 UE 保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置;

所述 UE 保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态;

所述 UE 保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI;

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

结合第二方面的第十四种可能的实现方式,在第二方面的第十五种可能的实现方式中,所述 UE 按照 Key Refresh 执行与所述主基站之间的安全密钥更改,包括:

所述 UE 基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值,使用当前的与所述主基站对应的 UE 侧中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥;

所述 UE 使用更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥,所述新的与所述主基站对应的安全密钥包括: 所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

结合第二方面的第十五种可能的实现方式,在第二方面的第十六种可能的实现方式中,所述 UE 根据所述密钥更改命令消息,确定是否保持与所述主基站或所述次基站之间的接入层配置信息,和/或,是否保持与所述主基站或所述次基站之间的数据传输之前,还包括:

所述 UE 确定所述按照 Key Refresh 执行与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的 UE 侧中间密钥进行的。

结合第二方面的第十四种可能的实现方式,在第二方面的第十七种可能的实现方式中,所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh,具体为:

所述UE根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息,确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第

四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第十八种可能的实现方式中，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，包括：当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，所述 UE 按照 Key Re-key 执行与所述主基站之间的安全密钥更改；

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤：

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 停止所述 UE 与所述主基站之间的数据传输；

所述 UE 停止所述 UE 与所述次基站之间的数据传输。

结合第二方面的第十八种可能的实现方式，在第二方面的第十九种可能的实现方式中，所述 UE 按照 Key Re-key 执行与所述主基站之间的安全密钥更改，包括：

所述UE基于更新后的接入层管理实体ASME中间密钥更新与所述主基站之间的 UE 侧中间密钥；

所述 UE 根据更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

结合第二方面的第十九种可能的实现方式，在第二方面的第二十种可能的实现方式中，所述 UE 基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥之后，还包括：

所述 UE 根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的 UE 侧中间密钥;

所述 UE 根据更新后的与所述次基站对应的 UE 侧中间密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括: 所述 UE 与所述次基站通信时使用的加密密钥。

结合第二方面的第十八种可能的实现方式，在第二方面的第二十一种可能的实现方式中，所述 UE 根据所述密钥更改命令消息包含的指示信息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，具体为:

所述UE根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十二种可能的实现方式中，若所述密钥更改命令消息中包含的指示信息指示所述 UE 保持与所述第二基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤:

所述 UE 保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站;

所述UE保持所述UE与所述第二基站之间所建立的所有RB的RLC配置;

所述 UE 保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态;

所述 UE 保持所述 UE 与所述第二基站之间通信使用的 C-RNTI;

所述 UE 保持所述 UE 与所述第二基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第

四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十三种可能的实现方式中，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态；

所述 UE 保持所述 UE 与所述第一基站之间通信使用的 C-RNTI；

所述 UE 暂停所述 UE 与所述第一基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十四种可能的实现方式中，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤：

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 停止所述 UE 与所述第一基站之间的数据传输。

第三方面，本发明实施例还提供一种基站，所述基站具体为主基站 MeNB，

包括:

密钥更改确定模块，用于确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

消息发送模块，用于向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

消息接收模块，用于接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

结合第三方面，在第三方面的第一种可能的实现方式中，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块，还用于所述消息接收模块接收所述 UE 发送的密钥更改完成消息之后，向所述次基站转发所述密钥更改完成消息，以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

结合第三方面，在第三方面的第二种可能的实现方式中，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

结合第三方面的第二种可能的实现方式，在第三方面的第三种可能的实现方式中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述消息发送模块，具体用于向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

结合第三方面，在第三方面的第四种可能的实现方式中，所述密钥更改确定模块，包括:

命令接收子模块，用于接收移动管理实体 MME 发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述 UE 之间执行 Key Re-key，和/或指示所述次基站和所述 UE 之间执行 Key Re-key;

密钥更改确定子模块，用于根据所述密钥指示命令确定出第一基站与所述 UE 之间执行 Key Re-key。

结合第三方面的第四种可能的实现方式，在第三方面的第五种可能的实现

方式中，若所述主基站确定所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

结合第三方面，在第三方面的第六种可能的实现方式中，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块，还用于所述密钥更改确定子模块根据所述密钥指示命令确定出第一基站与所述UE之间需要执行安全密钥更改之后，向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括：所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括：所述 MME 为所述次基站生成的次基站侧中间密钥。

结合第三方面，在第三方面的第七种可能的实现方式中，所述密钥更改确定模块，具体用于判断所述 UE 当前在主基站侧的分组数据汇聚协议计数 PDCP Count 在预置次数内是否发生反转，若所述 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新 Key Refresh，其中，所述第一基站为所述主基站；和/或，当所述主基站接收到所述次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

结合第三方面或第三方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能的实现方式，在第三方面的第八种可能的实现方式中，所述密钥更改命令消息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述UE之间需要执行安全密钥更改。

结合第三方面的第八种可能的实现方式，在第三方面的第九种可能的实现

方式中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第三方面或第三方面的的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能的实现方式，在第三方面的第十种可能的实现方式中，所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

结合第三方面的第十种可能的实现方式，在第三方面的第十一种可能的实现方式中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第三方面，在第三方面的第十二种可能的实现方式中，所述密钥更改命令消息中通过密钥改变指示 Key Change Indicator 字段的取值指示所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

结合第三方面，在第三方面的第十三种可能的实现方式中，所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，或指示所述 UE 暂停与所述第一基站之间的数据传输，或指示所述 UE 停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

结合第三方面或第三方面的的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第三方面的第十四种可能的实现方式中，所述密钥更改命令消息具体为小区内切换 HO 命令消息。

第四方面，本发明实施例还提供一种用户设备 UE，包括：

消息接收模块，用于接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述UE与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；

密钥更改模块，用于根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改；

决策模块，用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；

消息发送模块，用于向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述UE与所述第一基站之间已经完成安全密钥更改。

结合第二方面，在第二方面的第一种可能的实现方式中，所述密钥更改命令消息携带指示所述UE是否在所述第一基站执行随机接入的指示信息，所述决策模块，还用于所述消息接收模块接收主基站发送的密钥更改命令消息之后，根据所述密钥更改命令消息携带指示所述UE是否在所述第一基站执行随机接入的指示信息确定是否在所述第一基站执行随机接入。

结合第二方面或第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，若所述密钥更改命令消息指示所述UE在所述第一基站执行随机接入时，所述UE，还包括：随机接入模块，其中，

所述消息接收模块，具体用于接收主基站发送的包含随机接入资源的信息的密钥更改命令消息；

所述随机接入模块，用于根据所述随机接入资源的信息执行向所述第一基站的随机接入。

结合第二方面，在第二方面的第三种可能的实现方式中，若所述UE接收到的所述密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述UE之间需要执行安全密钥更改，则所述密钥更改模块，还用于根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和

所述次基站。

结合第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第一指示信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第二指示信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

结合第二方面，在第二方面的第五种可能的实现方式中，所述 UE 接收到的所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述密钥更改模块，还用于根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

结合第二方面的第五种可能的实现方式，在第二方面的第六种可能的实现方式中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第一安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

结合第二方面，在第二方面的第七种可能的实现方式中，若所述密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，所述密钥更改模块，具体用于通过所述 Key Change Indicator 字段的取值指示确定

按照 Key Re-key 或 Key Refresh 执行与所述第一基站之间的安全密钥更改。

结合第二方面，在第二方面的第八种可能的实现方式中，所述决策模块具体用于:

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

根据所述密钥更改命令消息中包含的指示所述UE保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

结合第二方面的第八种可能的实现方式，在第二方面的第九种可能的实现方式中，所述决策模块具体用于:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key

Refresh 时，确定保持与所述主基站或所述次基站之间的接入层配置信息。

结合第二方面，在第二方面的第十种可能的实现方式中，所述决策模块具体用于:

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输;

或者，

根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

结合第二方面的第十种可能的实现方式，在第二方面的第十一种可能的实现方式中，所述决策模块具体用于:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站以及次基站之间的数据传输; 或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与所述次基站之间的数据传输;

或者，

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，确定保持与所述次基站之间的数据传输。

结合第二方面，在第二方面的第十二种可能的实现方式中，当所述 UE 根

据所述密钥更改命令信息，确定需要保持与所述主基站之间的接入层配置信息，和/或，需要保持与所述主基站之间的数据传输时，所述决策模块，具体用于确定如下内容中的至少一项：

所述 UE 保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

所述 UE 保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活状态；

所述 UE 保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述主基站之间的数据传输。

结合第二方面，在第二方面的第十三种可能的实现方式中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，所述保持与所述次基站之间的接入层配置信息，和/或，保持与所述次基站之间的数据传输，所述决策模块，具体用于确定如下内容中的至少一项：

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态；

所述 UE 保持所述 UE 与所述次基站之间通信使用的 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第十四种可能的实现方式中，所述密钥更改模块，具体用于当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述

主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，按照 Key Refresh 执行与所述主基站之间的安全密钥更改;

所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块:

PDCP 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置;

RLC 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置;

MAC 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置;

激活保持模块，用于保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态;

C-RNTI 保持模块，用于保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI;

第一传输控制模块，用于保持或暂停所述 UE 与所述次基站之间的数据传输。

结合第二方面的第十四种可能的实现方式，在第二方面的第十五种可能的实现方式中，所述密钥更改模块，包括:

第一中间密钥更新子模块，用于基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值，使用当前的与所述主基站对应的 UE 侧中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥;

第一密钥更改子模块，用于使用更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括: 所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

结合第二方面的第十五种可能的实现方式，在第二方面的第十六种可能的实现方式中，所述决策模块，还用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之前，确定所述按照 Key Refresh 执行

与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的UE侧中间密钥进行的。

结合第二方面的第十四种可能的实现方式，在第二方面的第十七种可能的实现方式中，所述密钥更改模块，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述UE之间执行安全密钥更改的方式为Key Refresh。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第十八种可能的实现方式中，所述密钥更改模块，具体用于当所述第一基站为所述主基站时，若所述UE根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，按照 Key Re-key 执行与所述主基站之间的安全密钥更改；

所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置；重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置；

RLC 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置；重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置；

MAC 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置；重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置；

第二传输控制模块，用于停止所述 UE 与所述主基站之间的数据传输；停止所述 UE 与所述次基站之间的数据传输。

结合第二方面的第十八种可能的实现方式，在第二方面的第十九种可能的实现方式中，所述密钥更改模块，包括：

第二中间密钥更新子模块，用于基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥；

第一密钥更改子模块，用于根据更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

结合第二方面的第十九种可能的实现方式，在第二方面的第二十种可能的实现方式中，所述密钥更改模块，还包括：

所述第三中间密钥更新子模块，还用于所述第二中间密钥更新子模块基于接入层管理实体 ASME 中间密钥更新与所述主基站对应的 UE 侧中间密钥之后，根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的UE侧中间密钥；

第二密钥更改子模块，用于根据更新后的与所述次基站对应的 UE 侧中间密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括：所述 UE 与所述次基站通信时使用的加密密钥。

结合第二方面的第十八种可能的实现方式，在第二方面的第二十一种可能的实现方式中，所述密钥更改模块，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十二种可能的实现方式中，若所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站；

RLC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 RLC 配置；

MAC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置；

激活保持模块，用于保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态；

C-RNTI 保持模块，用于保持所述 UE 与所述第二基站之间通信使用的 C-RNTI；

传输保持模块，用于保持所述 UE 与所述第二基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十三种可能的实现方式中，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

RLC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

MAC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

激活保持模块，用于保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态；

C-RNTI 保持模块，用于保持所述 UE 与所述第一基站之间通信使用的 C-RNTI；

传输暂停模块，用于暂停所述 UE 与所述第一基站之间的数据传输。

结合第二方面或第二方面的第一种可能或第二种可能或第三种可能或第四种可能或第五种可能或第六种可能或第七种可能或第八种可能或第九种可

能或第十种可能或第十一种可能或第十二种可能或第十三种可能的实现方式，在第二方面的第二十四种可能的实现方式中，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

RLC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

MAC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

传输停止模块，用于停止所述 UE 与所述第一基站之间的数据传输。

从以上技术方案可以看出，本发明实施例具有以下优点：

本发明实施例中，主基站首先确定第一基站与 UE 之间需要执行安全密钥更改，其中，第一基站包括主基站和次基站两者之中的至少一个基站，主基站确定第一基站与 UE 之间需要执行安全密钥更改之后，主基站向 UE 发送密钥更改命令消息，则 UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

附图说明

图 1 为本发明实施例提供的一种安全密钥更改方法的流程方框示意图；

图 2 为本发明实施例提供的另一种安全密钥更改方法的流程方法示意图；

图 3-a 所示，为本发明实施例中主基站、次基站、UE 之间的一种交互流

程示意图；

图 3-b 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图；

图 3-c 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图；

图 3-d 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图；

图 3-e 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图；

图 4-a 为本发明实施例提供的一种基站的组成结构示意图；

图 4-b 为本发明实施例提供的一种密钥更改确定模块的组成结构示意图；

图 5-a 为本发明实施例提供的一种 UE 的组成结构示意图；

图 5-b 为本发明实施例提供的另一种 UE 的组成结构示意图；

图 5-c 为本发明实施例提供的另一种 UE 的组成结构示意图；

图 5-d 为本发明实施例提供的一种密钥更改模块的组成结构示意图；

图 5-e 为本发明实施例提供的另一种 UE 的组成结构示意图；

图 6 为本发明实施例提供的另一种基站的组成结构示意图；

图 7 为本发明实施例提供的另一种 UE 的组成结构示意图。

具体实施方式

本发明实施例提供了一种安全密钥更改方法和基站及用户设备，用于实现 UE 同时与 MeNB 和 SeNB 执行双连接通信时的安全密钥更改。

为使得本发明的发明目的、特征、优点能够更加的明显和易懂，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，下面所描述的实施例仅仅是本发明一部分实施例，而非全部实施例。基于本发明中的实施例，本领域的技术人员所获得的所有其他实施例，都属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本发明的实施例中对相同属

性的对象在描述时所采用的区分方式。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，以便包含一系列单元的过程、方法、系统、产品或设备不必限于那些单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它单元。

以下分别进行详细说明。

本发明安全密钥更改方法的一个实施例，可应用于基站中，尤其适用于UE同时与两个以上的基站执行双连接通信时的主基站，该方法可包括如下步骤：主基站确定第一基站与用户设备UE之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；主基站向UE发送密钥更改命令消息，以使UE根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输；主基站接收UE发送的密钥更改完成消息，以使第一基站确定UE与第一基站之间已经完成安全密钥更改。

请参阅图1所示，本发明一个实施例提供的安全密钥更改方法，可以包括如下步骤：

101、主基站确定第一基站与用户设备UE之间需要执行安全密钥更改。

其中，第一基站包括主基站和次基站两者之中的至少一个基站。

在本发明实施例中，在基站和UE之间在传输数据时，通常需要使用安全密钥，但是在一些情况下需要对安全密钥进行更改，同样的，当一个UE至少通过两个网络节点来进行通信时，也常常出现需要对执行双连接通信的UE使用的安全密钥进行更改的应用需要，例如一个UE同时使用MeNB和SeNB分别提供的无线资源进行通信时就需要对安全密钥进行更改，但是在UE执行双连接通信时两个网络节点之间是通过非理想（即存在一定的时延）的传输网进行相连，在UE与基站的数据传输应用场景中，在上述UE与MeNB和SeNB执行双连接通信时，如果不考虑双连接通信的特殊性，则至少存在如下问题：例如SeNB侧建立的RB的PDCP、RLC层需要重新建立，并且MAC也需要重新配置，从而导致UE与SeNB之间的数据传输需要中断；另外SeNB侧的SCell的状态将变更为去激活状态，在安全密钥更改完成后，需要对SeNB侧的SCell重新进行激活，导致不必要的数据传输延迟。另外主小区和次小区也

具有很大的区别，例如主要区别在于，主小区为 UE 初始连接或切换时建立无线资源控制（Radio Resource Control，RRC）连接的小区，主小区为 UE 提供安全和移动性管理相关的参数，也用于传输 UE 的用户面数据，而次小区则主要负责为 UE 传输用户面数据。这些对于双连接通信而言具有的诸多特点，使得UE执行双连接通信时如何对安全密钥进行更改仍需要本领域技术人员进行更深入的研究。

本发明实施例为了解决 UE 执行双连接通信时对安全密钥的更改问题，可以由主基站首先确定主基站与 UE 之间是否需要执行安全密钥更改以及 SeNB 与 UE 之间是否需要执行安全密钥更改，即主基站针对 UE 同时使用主基站和次基站分别提供的无线资源执行双连接通信时分别侦测主基站与UE之间的数据传输过程、次基站与 UE 之间的数据传输过程，从而主基站分别判断主基站与 UE 之间是否需要执行安全密钥更改、次基站与 UE 之间是否需要执行安全密钥更改。并且主基站可以判断主基站与 UE 之间执行安全密钥更改的方式，主基站还可以判断次基站与 UE 之间执行安全密钥更改的方式。

需要说明的是，在本发明实施例中，安全密钥更改的方式包括密钥再生产（英文称之为 Key Re-key）和密钥刷新（英文称之为 Key Refresh），Key Re-key 和 Key Refresh 二者本质上都是为了进行安全密钥的更改。不同之处在于 Key Re-key 的实现过程是由移动管理实体（Mobility Management Entity，MME）发起的，并且 MME 会提供新的中间密钥（可用符号 K_{eNB} 表示）用于进行安全密钥的改变过程。而 Key Refresh 则是由 eNB 发起的，一般是由于分组数据汇聚协议（Packet Data Convergence Protocol，PDCP）计数（Count）的反转会触发进行 Key Refresh，从而进行安全密钥的改变过程，接下来进行详细说明：

在本发明的一些实施例中，步骤 101 主基站确定第一基站与 UE 之间需要执行安全密钥更改，可以包括如下步骤：

A1、主基站接收 MME 发送的密钥指示命令，其中，密钥指示命令用于指示主基站和 UE 之间执行 Key Re-key，和/或指示次基站和 UE 之间执行 Key Re-key；

A2、主基站根据密钥指示命令确定出第一基站与 UE 之间执行 Key Re-key。

也就是说，MME 可以决定主基站和次基站中的哪个基站与 UE 之间需要

执行安全密钥更改，并且MME还可以决定具体采用Key Re-key的方式与UE之间执行安全密钥更改，MME在确定哪个基站与UE执行安全密钥更改以及采用的方式后，MME向主基站发送密钥指示命令，主基站通过对该密钥指示命令的解析，就可以获取到MME对执行安全密钥更改的具体指示，本发明实施例中，将主基站判断出的结果用第一基站与UE执行安全密钥更改来描述，即执行步骤A2主基站确定第一基站与UE执行安全密钥更改并且确定采用的方式是Key Re-key。其中，第一基站表示的是主基站确定出的需要与UE执行安全密钥更改的基站，在本发明实施例中，对于第一基站的具体确定方式有三种：1、第一基站为主基站，2、第一基站为次基站，3、第一基站为主基站和次基站，即主基站可以通过密钥指示命令从这三种第一基站的实现中选择一种，例如，若MME通过密钥指示命令仅指示主基站和UE之间需要执行安全密钥更改并且采用的方式是Key Re-key，在这种情况下主基站就可以确定此时第一基站具体指的是主基站。

在本发明的另一些实施例中，若主基站确定出的第一基站包括次基站时，步骤101主基站确定第一基站与UE之间需要执行安全密钥更改之后，本发明实施例还可以包括如下步骤：

主基站向次基站发送密钥更改指示消息，密钥更改指示消息用于指示次基站执行安全密钥更改，密钥更改指示消息包括：主基站根据更新后的主基站侧中间密钥、次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，密钥更改指示消息包括：MME为次基站生成的次基站侧中间密钥。

其中，对于主基站确定出第一基站包括次基站，具体指的是第一基站为次基站，也可以指的是第一基站为主基站和次基站，即主基站确定出与UE之间需要执行安全密钥更改的基站包括有次基站时，主基站需要向次基站发送密钥更改指示消息，指示次基站执行安全密钥更改，并且主基站在密钥更改指示消息中携带如下信息：主基站根据更新后的主基站侧中间密钥、次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥。或，密钥更改指示消息携带如下信息：MME为次基站生成的次基站侧中间密钥。也就是说，对于次基站与UE之间需要执行安全密钥更改时，次基站需要使用次基站侧中间密钥，该次基站侧中间密钥可以由主基站来

决定，也可以由 MME 来决定，当次基站侧中间密钥由主基站来决定时，主基站根据更新后的主基站侧中间密钥、次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息就可以生成次基站侧中间密钥，当次基站侧中间密钥由 MME 来决定时，MME 向主基站发送的密钥指示命令中就可以携带该次基站侧中间密钥，并且由主基站携带在密钥更改指示消息中发送给次基站。

具体的，在本发明的另一些实施例中，若主基站确定第一基站与 UE 之间执行安全密钥更改的方式为 Key Re-key，则密钥更改命令消息中携带次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。也就是说，若次基站侧中间密钥由主基站侧生成时，主基站向 UE 发送的密钥更改命令消息中还需要携带次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息，则 UE 通过主基站发送的密钥更改命令消息，UE 可以获取到次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息，UE 可以使用该小区信息以及更新后的主基站侧中间密钥生成次基站侧中间密钥。

前述内容中对于执行安全密钥更改的方式为 Key Re-key 进行了说明，接下来对执行安全密钥更改的方式为 Key Refresh 进行说明，请参阅如下描述，在本发明的一些实施例中，步骤 101 主基站确定第一基站与 UE 之间需要执行安全密钥更改，可以包括如下步骤:

B1、主基站判断 UE 当前在主基站侧的 PDCP Count 在预置次数内是否发生反转，若 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则主基站确定第一基站与 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，第一基站为主基站;

和/或，

B2、当主基站接收到次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或主基站接收到次基站发送的次基站需要执行 Key Refresh 的指示信息，或主基站接收到 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，主基站确定第一基站与 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，第一基站为次基站。

也就是说，UE 当前在主基站侧的 PDCP Count 在预置次数内是否发生反

转，其中预置次数的多少可以由主基站自己决定，至于该次数的取值可以由主基站根据具体应用场景来设定，此处不做限定，另外 UE 当前在主基站侧的 PDCP Count 在预置次数内发生反转也可以简单描述为: UE 当前在主基站侧的 PDCP Count 将要反转，UE 当前在主基站侧的 PDCP Count 在预置次数内不发生反转也可以简单描述为：UE 当前在主基站侧的 PDCP Count 将不反转。其中，步骤 B1 中主基站通过确定 PDCP Count 将要反转确定主基站与 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，在这种情况下第一基站就可以指的是主基站。

对于步骤 B2，主基站在如下三种情况中的任一种情况产生时，主基站就可以确定次基站与 UE 之间需要执行安全密钥更改，并且确定更改的方式为 Key Refresh，这三种情况分别是：1、次基站侧的 PDCP Count 在预置次数内发送反转，次基站向主基站发送次基站侧的 PDCP Count 在预置次数发生反转的指示信息，2、次基站需要执行 Key Refresh，次基站向主基站发送次基站需要执行 Key Refresh 的指示信息，3、UE 获知当前次基站侧的 PDCP Count 在预置次数发生反转，UE 向主基站上报当前次基站侧的 PDCP Count 在预置次数发生反转。其中预置次数的多少可以由次基站自己决定，至于该时间段的取值可以由次基站根据具体应用场景来设定，此处不做限定，另外次基站侧的 PDCP Count 在预置次数内发送反转也可以简单描述为：次基站侧的 PDCP Count 将要反转。其中，步骤 B2 中主基站通过确定 PDCP Count 将要反转确定次基站与 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，在这种情况下第一基站就可以指的是次基站。另外，步骤 B1 和步骤 B2 之间是和/或关系，当步骤 B1 和步骤 B2 都实现时，主基站就可以确定出主基站和 UE 之间需要执行安全密钥更改，主基站还可以确定出次基站和 UE 之间需要执行安全密钥更改，并且主基站确定它们执行安全密钥更改的方式是 Key Refresh。

102、主基站向 UE 发送密钥更改命令消息，以使 UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输。

在本发明实施例中，主基站通过步骤 101 就可以判定主基站和次基站中哪

个基站与 UE 之间需要执行安全密钥更改，主基站记判断结果用第一基站与 UE 之间需要执行安全密钥更改，然后主基站向 UE 发送密钥更改命消息，以触发 UE 执行更改安全密钥，其中密钥更改命令消息中携带主基站和次基站中哪个基站的标识信息，并且密钥更改命令消息中还可以携带执行 UE 执行安全密钥更改的方式。

在本发明的一些实施例中，主基站向 UE 发送的密钥更改命令消息，包括：第一指示信息和第二指示信息，其中，

第一指示信息用于指示主基站与 UE 之间需要执行安全密钥更改；

第二指示信息用于指示次基站与 UE 之间需要执行安全密钥更改。

也就是说，主基站生成的密钥更改命令消息中分别携带第一指示信息和第二指示信息，分别通过两个指示信息来向 UE 指示是否执行安全密钥更改，其中，第一指示信息指示的是主基站，第二指示信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一指示信息和第二指示信息的取值。例如，故当第一指示信息指示主基站和 UE 之间需要执行安全密钥更改、且第二指示信息指示次基站和 UE 之间需要执行安全密钥更改时，主基站可以确定第一基站指的是主基站和次基站，故 UE 通过第一指示信息和第二指示信息就可以获取 UE 与主基站和次基站之间都需要执行安全密钥更改。

进一步的，在本发明的另一些实施例中，第一指示信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh；第二指示信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。也就是说，主基站在生成的密钥更改命令消息中分别携带第一指示信息和第二指示信息之后，还可以使用第一指示信息和第二指示信息进一步指示执行安全密钥更改的方式，第一指示信息指示的是主基站，第二指示信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一指示信息和第二指示信息的取值，故当第一指示信息指示主基站和 UE 之间执行安全密钥更改的方式为 Key Re-key、且第二指示信息指示次基站和 UE 之间执行安全密钥更改的方式为 Key Refresh 时，UE 通过第一指示信息就可以获取 UE 与主基站之间执行安全密钥更改的方式为 Key Re-key，UE 通过第二指示信息就可以获取 UE 与次基站之间执行安全密钥更

改的方式为 Key Refresh。

在本发明的另一些实施例中，主基站向 UE 发送的密钥更改命令消息，包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，

第一安全密钥上下文信息用于指示主基站与 UE 之间需要执行安全密钥更改；

第二安全密钥上下文信息用于指示次基站与 UE 之间需要执行安全密钥更改。

也就是说，主基站生成的密钥更改命令消息中分别携带第一安全密钥上下文信息和第二安全密钥上下文信息，分别通过两个安全密钥上下文信息来向 UE 指示是否执行安全密钥更改，其中，第一安全密钥上下文信息指示的是主基站，第二安全密钥上下文信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一安全密钥上下文信息和第二安全密钥上下文信息的取值，故当第一安全密钥上下文信息指示主基站和 UE 之间需要执行安全密钥更改、且第二安全密钥上下文信息指示次基站和 UE 之间需要执行安全密钥更改时，主基站可以确定第一基站指的是主基站和次基站，故 UE 通过第一安全密钥上下文信息和第二安全密钥上下文信息就可以获取 UE 与主基站和次基站之间都需要执行安全密钥更改。

进一步的，在本发明的另一些实施例中，第一安全密钥上下文信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh；第二安全密钥上下文信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。也就是说，主基站在生成的密钥更改命令消息中分别携带第一安全密钥上下文信息和第二安全密钥上下文信息之后，还可以使用第一安全密钥上下文信息和第二安全密钥上下文信息进一步指示执行安全密钥更改的方式，第一安全密钥上下文信息指示的是主基站，第二安全密钥上下文信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一安全密钥上下文信息和第二安全密钥上下文信息的取值，故当第一安全密钥上下文信息指示主基站和 UE 之间执行安全密钥更改的方式为 Key Re-key、且第二安全密钥上下文信息指示次基站和 UE 之间执行安全密钥更改的方式为 Key Refresh 时，UE 通过第一安全密钥上下文信息就可以获取 UE 与主基站之间执行安全密钥更改的方式为 Key

Re-key，UE 通过第二安全密钥上下文信息就可以获取 UE 与次基站之间执行安全密钥更改的方式为 Key Refresh。

在本发明的另一些实施例中，主基站向 UE 发送的密钥更改命令消息，还包括：密钥改变指示（Key Change Indicator），主基站可以通过 Key Change Indicator 字段的取值指示第一基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。例如，主基站可以将 Key Change Indicator 的取值置为真（True）表示需要第一基站与 UE 之间执行 Key Re-key，主基站可以将 Key Change Indicator 的取值置为假（False）表示需要第一基站与 UE 之间执行 Key Refresh。

在本发明的另一些实施例中，主基站向 UE 发送的密钥更改命令消息，还包括：指示 UE 与第一基站或第二基站之间传输数据的指示信息，该指示信息的内容可以为以下三种情况中的任意一种：1、指示 UE 保持与第二基站之间的数据传输，2、指示 UE 暂停与第一基站之间的数据传输，3、指示 UE 停止与第一基站之间的数据传输，当第二基站为主基站时，第一基站为次基站，当第二基站为次基站时，第二基站为主基站。具体的，当上述指示信息的内容为第 1、2 种情况时，UE 根据上述指示信息按照 Key Refresh 执行安全密钥的更改，当上述指示信息的内容为第 3 种情况时，UE 根据上述指示信息按照 Key Re-key 执行安全密钥的更改。

需要说明的是，在本发明的一些实施例中，主基站向 UE 发送的密钥更改命令消息具体为小区内切换（Handover，HO）命令消息。也就是说，在本发明实施例中针对UE执行双连接通信时安全密钥的更改过程也可以通过小区内切换过程来完成的，其中，小区内切换过程指的是 UE 在执行切换的时候，源小区和目标小区是一个基站下的同一个小区，即切换前后主小区是相同的一个小区，并没有发生改变。

103、主基站接收 UE 发送的密钥更改完成消息，以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改。

在本发明实施例中，UE 接收到主基站发送的密钥更改命令消息之后，UE 可以根据该密钥更改命令消息执行与第一基站之间的安全密钥更改，当 UE 完成与第一基站之间的安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，当主基站接收到 UE 发送

的密钥更改完成消息之后，第一基站也可以通过主基站接收到的密钥更改完成消息确定 UE 与第一基站之间的安全密钥更改已经完成，第一基站可以使用新的安全密钥继续与 UE 之间进行数据传输，需要说明的是，根据前述内容的描述可知，第一基站可以指的是主基站，也可以指的是次基站，还可以指的是主基站和次基站，故需要指示与 UE 之间需要执行安全密钥更改的基站在得到 UE 反馈的安全密钥已经更改完成之后可以继续与 UE 之间进行数据传输，故主基站与 UE 执行安全密钥更改并不会影响到次基站与 UE 之间的数据传输，同样的，次基站与 UE 执行安全密钥更改并不会影响到主基站与 UE 之间的数据传输。

需要说明的是，在本发明的一些实施例中，若主基站确定出的第一基站包括次基站时，步骤 103 主基站接收 UE 发送的密钥更改完成消息之后，本发明实施例还可以包括如下步骤:

主基站向次基站转发密钥更改完成消息，以使次基站确定 UE 与次基站之间已经完成安全密钥更改。

也就是说，若 UE 执行的是与次基站之间的安全密钥更改，那么当主基站接收到 UE 反馈的与次基站之间的安全密钥更改完成之后，主基站可以向次基站转发密钥更改完成消息，则次基站通过该密钥更改完成消息确定 UE 与次基站之间已经完成安全密钥更改，从而次基站可以根据该密钥更改完成消息恢复 UE 与次基站的数据传输。

在本发明的一些实施例中，主基站向 UE 发送的密钥更改命令消息还可以携带指示 UE 是否在第一基站执行随机接入的指示信息。即主基站可以明确通知 UE 在哪个基站上执行随机接入，UE 可以按照主基站的指示发起随机接入。进一步的，若密钥更改命令消息指示 UE 在第一基站执行随机接入，且第一基站包括主基站时，步骤 101 主基站向 UE 发送密钥更改命令消息，具体包括:

主基站向 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使 UE 根据随机接入资源的信息与第一基站执行随机接入。

也就是说，若主基站指示 UE 在主基站上执行随机接入时，主基站可以给 UE 分配随机接入资源，并在密钥更改命令消息中携带随机接入资源的信息，当 UE 向主基站发送随机接入请求时，主基站向 UE 发送随机接入响应，以指示 UE 与主基站执行随机接入，从而完成整个随机接入过程。需要说明的是，

若主基站指示 UE 在次基站上执行随机接入时也可以按照上述方法由 UE 和次基站来完成整个随机接入过程，当然主基站也可以指示 UE 分别在主基站、次基站上分别执行随机接入，则 UE 在主基站和次基站上分别执行随机接入时，两个随机接入过程还可以是并行的。另外，在 UE 也执行向次基站的随机接入时，次基站也可以通过判断 UE 执行随机接入过程成功来确定安全密钥改变完成，因此这种情况下，主基站也可以不向次基站发送密钥改变完成消息。

通过以上内容对本发明实施例的描述可知，主基站确定第一基站与 UE 之间需要执行安全密钥更改，其中，第一基站包括主基站和次基站两者之中的至少一个基站，若主基站确定第一基站与 UE 之间需要执行安全密钥更改，主基站向 UE 发送密钥更改命令消息，则 UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

上述实施例从主基站一侧对本发明实施例提供的安全密钥更改方法进行了说明，接下来从用户设备一侧对本发明实施例提供的安全密钥更改方法进行详细说明，本发明安全密钥更改方法的另一个实施例，可应用于用户设备中，尤其适用于同时与两个以上的基站执行双连接通信时的 UE，该方法可包括如下步骤： UE 接收主基站发送的密钥更改命令消息，其中，密钥更改命令消息包括主基站命令 UE 与第一基站之间需要执行安全密钥更改的指示信息，第一基站包括主基站和次基站两者之中的至少一个基站；UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改；UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输；UE 向主基站发送密钥更改完成消息，以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改。

请参阅图 2 所示，本发明另一个实施例提供的安全密钥更改方法，可以包括如下步骤:

201、UE 接收主基站发送的密钥更改命令消息。

其中，密钥更改命令消息包括主基站命令 UE 与第一基站之间需要执行安全密钥更改的指示信息，第一基站包括主基站和次基站两者之中的至少一个基站。

在本发明实施例中，在基站和 UE 之间在传输数据时，通常需要使用安全密钥，但是在一些情况下需要对安全密钥进行更改，同样的，当一个 UE 至少通过两个网络节点来进行通信时，也常常出现需要对执行双连接通信的 UE 使用的安全密钥进行更改的应用需要，本发明实施例为了解决 UE 执行双连接通信时对安全密钥的更改问题，可以由主基站首先判断主基站与 UE 之间需要执行安全密钥更改以及次基站与 UE 之间需要执行安全密钥更改，即主基站针对 UE 同时使用主基站和次基站分别提供的无线资源执行双连接通信时分别侦测主基站与 UE 之间的数据传输过程、次基站与 UE 之间的数据传输过程，从而主基站分别判断主基站与 UE 之间是否需要执行安全密钥更改、次基站与 UE 之间是否需要执行安全密钥更改。并且主基站可以判断主基站与 UE 之间执行安全密钥更改的方式，主基站还可以判断次基站与 UE 之间执行安全密钥更改的方式。

主基站在判定出主基站与 UE 之间需要执行安全密钥更改、和/或次基站与 UE 之间需要执行安全密钥更改之后，主基站可以向 UE 发送密钥更改命令消息，以指示 UE 与第一基站之间需要执行安全密钥更改，其中，第一基站表示的是主基站确定出的需要与 UE 执行安全密钥更改的基站，在本发明实施例中，对于第一基站的具体确定方式有三种：1、第一基站为主基站，2、第一基站为次基站，3、第一基站为主基站和次基站，即主基站可以通过密钥指示命令从这三种第一基站的实现中选择一种，例如，若 MME 通过密钥指示命令仅指示主基站和 UE 之间需要执行安全密钥更改并且采用的方式是 Key Re-key，在这种情况下主基站就可以确定此时第一基站具体指的是主基站，主基站在向 UE 发送的密钥更改命令消息中携带该主基站的标识，UE 就可以根据密钥更改命令消息获知 UE 与主基站之间需要执行安全密钥更改。

需要说明的是，主基站在密钥更改命令消息中还可以进一步的携带指示 UE 执行安全密钥更改的方式，具体的，主基站指示 UE 执行安全密钥更改的方式包括 Key Re-key 和 Key Refresh，Key Re-key 和 Key Refresh 二者本质上

都是为了进行安全密钥的更改。UE 通过主基站发送的密钥更改命令消息可以获知执行安全密钥更改的方式，接下来进行详细说明：

在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，第一指示信息用于指示主基站与 UE 之间需要执行安全密钥更改，第二指示信息用于指示次基站与 UE 之间需要执行安全密钥更改，则 UE 根据第一指示信息和/或第二指示信息确定出第一基站为以下三种情况中的一种：第一基站为主基站、第一基站为次基站、第一基站为主基站和次基站。

也就是说，主基站生成的密钥更改命令消息中分别携带第一指示信息和第二指示信息，分别通过两个指示信息来向 UE 指示是否执行安全密钥更改，其中，第一指示信息指示的是主基站，第二指示信息指示的是次基站，例如，当第一指示信息指示主基站和 UE 之间需要执行安全密钥更改、且第二指示信息指示次基站和 UE 之间需要执行安全密钥更改时，UE 可以确定第一基站指的是主基站和次基站，故 UE 通过第一指示信息和第二指示信息就可以获取 UE 与主基站和次基站之间都需要执行安全密钥更改。

进一步的，在本发明的另一些实施例中，第一指示信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh；第二指示信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，也就是说，主基站在生成的密钥更改命令消息中分别携带第一指示信息和第二指示信息之后，还可以使用第一指示信息和第二指示信息进一步指示执行安全密钥更改的方式，第一指示信息指示的是主基站，第二指示信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一指示信息和第二指示信息的取值，故当第一指示信息指示主基站和 UE 之间执行安全密钥更改的方式为 Key Re-key、且第二指示信息指示次基站和 UE 之间执行安全密钥更改的方式为 Key Refresh 时，UE 通过第一指示信息就可以获取 UE 与主基站之间执行安全密钥更改的方式为 Key Re-key，UE 通过第二指示信息就可以获取 UE 与次基站之间执行安全密钥更改的方式为 Key Refresh。

在本发明的另一些实施例中，若 UE 接收到的密钥更改命令消息中包含的指示信息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，

第一安全密钥上下文信息用于指示主基站与 UE 之间需要执行安全密钥更改，第二安全密钥上下文信息用于指示次基站与 UE 之间需要执行安全密钥更改，则 UE 根据第一安全密钥上下文信息和/或第二安全密钥上下文信息确定出第一基站为以下三种情况中的一种：第一基站为主基站、第一基站为次基站、第一基站为主基站和次基站。

也就是说，主基站生成的密钥更改命令消息中分别携带第一安全密钥上下文信息和第二安全密钥上下文信息，分别通过两个安全密钥上下文信息来向 UE 指示是否执行安全密钥更改，其中，第一安全密钥上下文信息指示的是主基站，第二安全密钥上下文信息指示的是次基站，例如，当第一安全密钥上下文信息指示主基站和 UE 之间需要执行安全密钥更改、且第二安全密钥上下文信息指示次基站和 UE 之间需要执行安全密钥更改时，UE 可以确定第一基站指的是主基站和次基站，故 UE 通过第一安全密钥上下文信息和第二安全密钥上下文信息就可以获取 UE 与主基站和次基站之间都需要执行安全密钥更改。

进一步的，在本发明的另一些实施例中，第一安全密钥上下文信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh；第二安全密钥上下文信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，也就是说，主基站在生成的密钥更改命令消息中分别携带第一安全密钥上下文信息和第二安全密钥上下文信息之后，还可以使用第一安全密钥上下文信息和第二安全密钥上下文信息进一步指示执行安全密钥更改的方式，第一安全密钥上下文信息指示的是主基站，第二安全密钥上下文信息指示的是次基站，主基站具体可以在密钥更改命令消息中设置两个字段分别用来表示第一安全密钥上下文信息和第二安全密钥上下文信息的取值，故当第一安全密钥上下文信息指示主基站和 UE 之间执行安全密钥更改的方式为 Key Re-key、且第二安全密钥上下文信息指示次基站和 UE 之间执行安全密钥更改的方式为 Key Refresh 时，UE 通过第一安全密钥上下文信息就可以获取 UE 与主基站之间执行安全密钥更改的方式为 Key Re-key，UE 通过第二安全密钥上下文信息就可以获取 UE 与次基站之间执行安全密钥更改的方式为 Key Refresh。

在本发明的另一些实施例中，若密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，UE 根据密钥更改命令消息包含的指示

信息为 Key Change Indicator 字段的取值获知 UE 与第一基站之间执行安全密钥更改的方式，例如，主基站可以将 Key Change Indicator 的取值置为 True 表示需要第一基站与 UE 之间执行 Key Re-key，则 UE 通过 Key Change Indicator 的取值置为 True 获知执行的是 Key Re-key。主基站可以将 Key Change Indicator 的取值置为 False 表示需要第一基站与 UE 之间执行 Key Refresh，则 UE 通过 Key Change Indicator 的取值置为 False 获知执行的是 Key Refresh。

在本发明的一些实施例中，主基站向 UE 发送的密钥更改命令消息还可以携带指示 UE 是否在第一基站执行随机接入的指示信息，步骤 201 UE 接收主基站发送的密钥更改命令消息之后，本发明实施例还可以包括如下步骤:

UE 根据密钥更改命令消息携带指示 UE 是否在第一基站执行随机接入的指示信息确定是否在第一基站执行随机接入。

也就是说，主基站可以明确通知 UE 在哪个基站上执行随机接入，UE 可以按照主基站的指示确定是否要发起随机接入以及在哪个基站上发起随机接入。若密钥更改命令消息指示 UE 在第一基站执行随机接入时，步骤 201UE 接收主基站发送的密钥更改命令消息，包括:

UE 接收主基站发送的包含随机接入资源的信息的密钥更改命令消息，并根据随机接入资源的信息执行向第一基站的随机接入。

也就是说，若主基站指示 UE 在主基站上执行随机接入时，主基站可以给 UE 分配随机接入资源，并在密钥更改命令消息中携带随机接入资源的信息，当 UE 向主基站发送随机接入请求时，主基站向 UE 发送随机接入响应，以指示 UE 与主基站执行随机接入，从而完成整个随机接入过程。需要说明的是，若主基站指示 UE 在次基站上执行随机接入时也可以按照上述方法由 UE 和次基站来完成整个随机接入过程，当然主基站也可以指示 UE 分别在主基站、次基站上分别执行随机接入，则 UE 在主基站和次基站上分别执行随机接入时，两个随机接入过程还可以是并行的。

202、UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改。

在本发明实施例中，UE 接收到主基站发送的密钥更改命令消息之后，UE 根据主基站的指示执行与第一基站之间的安全密钥更改，具体的，若第一基站为主基站，则 UE 需要执行与主基站之间的安全密钥更改，若第一基站为次基站，则 UE 需要执行与次基站之间的安全密钥更改，若第一基站为主基站和次

基站，则 UE 需要分别执行与主基站之间的安全密钥更改、与次基站之间的安全密钥更改。

在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包括有第一指示信息和第二指示信息，并且主基站通过第一指示信息向 UE 指示主基站与 UE 之间需要执行安全密钥更改，若主基站在第一指示信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh 时，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，具体为：UE 根据第一指示信息按照 Key Re-key 或 Key Refresh 执行与主基站之间的安全密钥更改。也就是说，若主基站在第一指示信息中向 UE 指示采用 Key Re-key，则 UE 需要根据第一指示信息按照 Key Re-key 执行与主基站之间的安全密钥更改，若主基站在第一指示信息中向 UE 指示采用 Key Refresh，则 UE 需要根据第一指示信息按照 Key Refresh 执行与主基站之间的安全密钥更改。

另外，在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包括有第一指示信息和第二指示信息，并且主基站通过第二指示信息向 UE 指示次基站与 UE 之间需要执行安全密钥更改，若主基站在第二指示信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh 时，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，具体为：UE 根据第一指示信息按照 Key Re-key 或 Key Refresh 执行与次基站之间的安全密钥更改。也就是说，若主基站在第一指示信息中向 UE 指示采用 Key Re-key，则 UE 需要根据第一指示信息按照 Key Re-key 执行与次基站之间的安全密钥更改，若主基站在第一指示信息中向 UE 指示采用 Key Refresh，则 UE 需要根据第一指示信息按照 Key Refresh 执行与次基站之间的安全密钥更改。

在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包括有第一安全密钥上下文信息和第二安全密钥上下文信息，并且主基站通过第一安全密钥上下文信息向 UE 指示主基站与 UE 之间需要执行安全密钥更改，若主基站在第一安全密钥上下文信息中还包括：指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh 时，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，具体为：UE 根据第一安全密钥上

下文信息按照 Key Re-key 或 Key Refresh 执行与主基站之间的安全密钥更改。也就是说，若主基站在第一安全密钥上下文信息中向 UE 指示采用 Key Re-key，则 UE 需要根据第一安全密钥上下文信息按照 Key Re-key 执行与主基站之间的安全密钥更改，若主基站在第一安全密钥上下文信息中向 UE 指示采用 Key Refresh，则 UE 需要根据第一安全密钥上下文信息按照 Key Refresh 执行与主基站之间的安全密钥更改。

另外，在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包括有第一安全密钥上下文信息和第二安全密钥上下文信息，并且主基站通过第二安全密钥上下文信息向 UE 指示次基站与 UE 之间需要执行安全密钥更改，若主基站在第二安全密钥上下文信息中还包括：指示次基站与 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh 时，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，具体为：UE 根据第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与次基站之间的安全密钥更改。也就是说，若主基站在第二安全密钥上下文信息中向 UE 指示采用 Key Re-key，则 UE 需要根据第二安全密钥上下文信息按照 Key Re-key 执行与次基站之间的安全密钥更改，若主基站在第二安全密钥上下文信息中向 UE 指示采用 Key Refresh，则 UE 需要根据第二安全密钥上下文信息按照 Key Refresh 执行与次基站之间的安全密钥更改。

在本发明的一些实施例中，若 UE 接收到的密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，具体为：UE 通过 Key Change Indicator 字段的取值指示确定按照 Key Re-key 或 Key Refresh 执行与第一基站之间的安全密钥更改。例如，若主基站在密钥更改命令消息中 Key Change Indicator 字段的取值为 True，则 UE 按照 Key Re-key 执行与第一基站之间的安全密钥更改，若主基站在密钥更改命令消息中 Key Change Indicator 字段的取值为 False，则 UE 按照 Key Refresh 执行与第一基站之间的安全密钥更改。

203、UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输。

在本发明实施例中，UE 通过密钥更改命令消息可以获知哪个基站与 UE 之间需要执行安全密钥更改，进一步的可以获取执行安全密钥更改的方式是

Key Re-key 或者 Key Refresh。故 UE 可以确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输。具体的，步骤 203 可以包括如下三种实现方式：1、UE 确定是否保持与主基站或次基站之间的接入层配置信息；2、UE 确定是否保持与主基站或次基站之间的数据传输；3、UE 确定是否保持与主基站或次基站之间的接入层配置信息以及是否保持与主基站或次基站之间的数据传输。对于上述的第 1 种情况，包括两种实现方式：第一种是 UE 确定保持与主基站或次基站之间的接入层配置信息，第二种是 UE 确定重置与主基站或次基站之间的接入层配置信息。并且对于 UE 保持与主基站或次基站之间的接入层配置信息具体可以有两种实现方式：第一种是 UE 保持与主基站之间的接入层配置信息，第二种是 UE 保持与次基站之间的接入层配置信息。对于上述的第 2 种情况，包括两种实现方式：第一种是 UE 确定保持与主基站或次基站之间的数据传输，第二种是 UE 确定暂停或停止与主基站或次基站之间的数据传输。并且对于 UE 保持与主基站或次基站之间的数据传输具体可以有两种实现方式：第一种是 UE 保持与主基站之间的数据传输，第二种是 UE 保持与次基站之间的数据传输。对于 UE 暂停或停止与主基站或次基站之间的数据传输可以有四种实现方式：第一种是 UE 暂停与主基站之间的数据传输，第二种是 UE 暂停与次基站之间的数据传输，第三种是 UE 停止与主基站之间的数据传输，第四种是 UE 停止与次基站之间的数据传输。

需要说明的是，在本发明的一些实施例中，步骤 203 的第 1 种实现方式：UE 根据密钥更改命令信息，确定是否保持与主基站或次基站之间的接入层配置信息，包括如下步骤：

UE 根据密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与主基站或次基站之间的接入层配置信息，其中，第一指示信息用于指示主基站与 UE 之间需要执行安全密钥更改，第二指示信息用于指示次基站与 UE 之间需要执行安全密钥更改；

或者，

UE 根据密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与主基站或次基站之间的接入层配置信息，其中，第一安全密钥上下文信息用于指示主基站与 UE 之间需要执行安全密钥更

改，第二安全密钥上下文信息用于指示次基站与 UE 之间需要执行安全密钥更改；

或者，

UE 根据密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与主基站或次基站之间的接入层配置信息；

或者；

UE 根据密钥更改命令消息中包含的指示 UE 保持与主基站或次基站之间的数据传输的指示信息确定是否保持与主基站或次基站之间的接入层配置信息。

其中，如上实施例给出了 UE 确定是否保持与主基站或次基站之间的接入层配置信息的几种实现方式，基于本发明实施例提供的实现方式的启示还可以有其它的实现方式，此处只是举例说明。

具体的，UE 根据密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与主基站或次基站之间的接入层配置信息，包括：

当根据 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与主基站或次基站之间的接入层配置信息；

或者，

当根据 Key Change Indicator 字段确定需要基于与主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与主基站或次基站之间的接入层配置信息；

或者，

当根据 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时，确定保持与主基站或次基站之间的接入层配置信息。

需要说明的是，在本发明的一些实施例中，步骤 203 的第 2 种实现方式：UE 根据密钥更改命令信息，确定是否保持与主基站或次基站之间的数据传输，包括：

UE 根据密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与主基站或次基站之间的数据传输，其中，第一指示信息用于指示主基站与 UE 之间需要执行安全密钥更改，第二指示信息用于指示次基站与 UE 之间需要执行安全密钥更改；

或者，

UE 根据密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与主基站或次基站之间的数据传输，其中，第一安全密钥上下文信息用于指示主基站与 UE 之间需要执行安全密钥更改，第二安全密钥上下文信息用于指示次基站与 UE 之间需要执行安全密钥更改；

或者，

UE根据密钥更改命令消息中包含的Key Change Indicator字段确定是否保持与主基站或次基站之间的数据传输；

或者，

UE 根据密钥更改命令消息中包含的指示 UE 保持与主基站或次基站之间的数据传输的指示信息确定是否保持与主基站或次基站之间的数据传输。

其中，如上实施例给出了 UE 确定是否保持与主基站或次基站之间的数据传输的几种实现方式，基于本发明实施例提供的实现方式的启示还可以有其它的实现方式，此处只是举例说明。

具体的，UE 根据密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与主基站或次基站之间的数据传输，包括：

当根据 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与主基站以及次基站之间的数据传输；或者，

当根据 Key Change Indicator 字段确定需要基于与主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与次基站之间的数据传输；

或者，

当根据 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，确定保持与次基站之间的数据传输。

在本发明的一些实施例中，当 UE 根据密钥更改命令信息，确定需要保持与主基站之间的接入层配置信息，和/或，需要保持与主基站之间的数据传输时，保持与主基站之间的接入层配置信息，和/或，保持与主基站之间的数据传输，具体可以包括如下步骤中的至少一个步骤：

UE 保持 UE 与主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

UE 保持 UE 与主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

UE 保持 UE 与主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置;

UE 保持 UE 与主基站之间的已激活的次小区 SCell 的激活状态;

UE 保持 UE 与主基站之间通信使用的小区无线网络临时标识符 C-RNTI;

UE 保持或暂停 UE 与主基站之间的数据传输。

在本发明的一些实施例中，当 UE 根据密钥更改命令信息，确定需要保持与次基站之间的接入层配置信息，和/或，需要保持与次基站之间的数据传输时，保持与次基站之间的接入层配置信息，和/或，保持与次基站之间的数据传输，具体可以包括如下步骤中的至少一个步骤:

UE 保持 UE 与次基站之间所建立的所有 RB 的 PDCP 配置;

UE 保持 UE 与次基站之间所建立的所有 RB 的 RLC 配置;

UE 保持 UE 与次基站之间所建立的所有 RB 的 MAC 配置;

UE 保持 UE 与次基站之间的已激活的 SCell 的激活状态;

UE 保持 UE 与次基站之间通信使用的 C-RNTI;

UE 保持或暂停 UE 与次基站之间的数据传输。

在本发明实施例的一些实施例中，若密钥更改命令消息指示主基站与 UE 之间需要执行安全密钥更改，则 UE 可以确定重置主基站与 UE 之间的接入层配置信息，且 UE 可以确定暂停或停止主基站与 UE 之间的数据传输，若密钥更改命令消息指示次基站与 UE 之间需要执行安全密钥更改，则 UE 可以确定重置次基站与 UE 之间的接入层配置信息，且 UE 可以确定暂停或停止次基站与 UE 之间的数据传输。需要说明的是，在本发明实施例中当 UE 确定了是否保持与主基站或次基站之间的接入层配置信息，和/或是否保持与主基站或次基站之间的数据传输之后，UE 可以按照确定出来的结果来对 UE 与主基站或次基站之间的接入层配置信息进行处理，也可以按照确定出来的结果对 UE 与主基站或次之间的数据传输进行控制，接下来分别进行举例说明。

在本发明的一些实施例中，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，包括如下步骤:

C1、当第一基站为主基站时，若 UE 根据密钥更改命令消息确定主基站与 UE 之间执行安全密钥更改的方式为 Key Refresh，UE 按照 Key Refresh 执行与主基站之间的安全密钥更改。

也就是说，若 UE 根据密钥更改命令消息确定主基站指示 UE 与主基站之

间需要执行安全密钥更改，并且安全密钥更改的方式为 Key Refresh，则 UE 可以按照 Key Refresh 执行与主基站之间的安全密钥更改。

具体的，步骤 C1 中 UE 根据所述密钥更改命令消息确定主基站与 UE 之间执行安全密钥更改的方式为 Key Refresh，具体为：

UE 根据密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定主基站与 UE 之间执行安全密钥更改的方式为 Key Refresh。

也就是说，主基站可以使用密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息来指示主基站与 UE 之间执行安全密钥更改的方式为 Key Refresh，故 UE 接收到密钥更改命令消息之后，通过第一指示信息或第一安全密钥上下文信息就可以获知主基站与UE之间执行安全密钥更改的方式为 Key Refresh，另外，在本发明的一些实施例中，密钥更改命令消息具体可以为小区内切换命令消息，在这种情况下也使用小区内切换命令消息中携带的安全上下文来指示主基站与 UE 之间执行安全密钥更改的方式为 Key Refresh。

需要说明的是，在本发明的另一些实施例中，在步骤 203UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之后，本发明实施例提供的安全密钥更改方法还包括如下步骤中的至少一个步骤：

C2、UE 保持 UE 与次基站之间所建立的所有（Radio Bearer，RB）的 PDCP 配置；

C3、UE 保持 UE 与次基站之间所建立的所有 RB 的无线链路控制（Radio Link Control，RLC）配置；

C4、UE 保持 UE 与次基站之间所建立的所有 RB 的媒体接入控制（Medium Access Control，MAC）配置；

C5、UE 保持 UE 与次基站之间的已激活的 SCell 的激活状态；

C6、UE 保持 UE 与次基站之间通信使用的小区无线网络临时标识符（Cell-Radio Network Temporary Identity，C-RNTI）；

C7、UE 保持或暂停 UE 与次基站之间的数据传输。

其中，步骤 C1 中 UE 按照 Key Refresh 执行与主基站之间的安全密钥更改，说明 UE 与主基站之间需要执行安全密钥更改，在这种情况下，步骤 C2 至步

骤C7中的至少一个步骤在执行时可以根据具体需要来决定执行其中的一个步骤或者多个步骤，通过保持UE与次基站之间的接入层配置信息，并且在UE保持UE与次基站之间的数据传输时，可以避免UE与主基站之间的安全密钥更改导致RB的接入层配置信息都需要重置，可以保证UE与次基站之间的RB的正常数据传输，以避免UE与主基站之间执行安全密钥更改导致UE与次基站之间不必要的数据传输中断，从而减少不必要的数据传输延迟。需要说明的是，上述步骤中描述的UE保持UE与次基站之间所建立的所有RB的PDCP配置指的是UE对该PDCP配置的配置信息维持当前的配置，另外保持RLC配置、MAC配置的含义相类似，保持UE与次基站之间的已激活的SCell的激活状态指的是已经激活的SCell的激活状态仍然维持激活状态，保持UE与次基站之间通信使用的C-RNTI指的是UE仍然使用当前的C-RNTI值。

进一步的，步骤C1UE按照Key Refresh执行与主基站之间的安全密钥更改，具体可以包括如下步骤:

C11、UE 基于密钥更改命令消息中指示的下一跳链接计数（英文称之为Next Hop Chaining Count）的值，使用当前的与主基站对应的UE侧中间密钥或者下一跳（Next Hop，NH）更新与主基站对应的UE侧中间密钥;

C12、UE使用更新后的与主基站对应的UE侧中间密钥和主基站的安全算法生成新的与主基站对应的安全密钥，新的与主基站对应的安全密钥包括:UE与主基站通信时使用的加密密钥和完整性保护密钥。

其中，UE在生成与主基站对应的安全密钥时，先对主基站对应的UE侧中间密钥进行更新，然后使用更新的与主基站对应的UE侧中间密钥、主基站的安全算法生成新的与主基站对应的安全密钥。

具体的，在步骤203 UE根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之前，本发明实施例还可以包括如下步骤括:

UE 确定按照 Key Refresh 执行与主基站之间的安全密钥更改是基于当前的与主基站对应的UE侧中间密钥进行的。

也就是说，UE在执行与主基站之间的安全密钥更改时若确定基于当前的与主基站对应的UE侧中间密钥，则步骤C11中就可以使用当前的与主基站对应的UE侧中间密钥更新与主基站对应的UE侧中间密钥，从而得到更新后的

与主基站对应的 UE 侧中间密钥。

在本发明的一些实施例中，步骤 202UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改，包括如下步骤:

D1、当第一基站为主基站时，若 UE 根据密钥更改命令消息确定主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key，UE 按照 Key Re-key 执行与主基站之间的安全密钥更改。

也就是说，若 UE 根据密钥更改命令消息确定主基站指示 UE 与主基站之间需要执行安全密钥更改，并且安全密钥更改的方式为 Key Re-key，则 UE 可以按照 Key Re-key 执行与主基站之间的安全密钥更改。

需要说明的是，在本发明的另一些实施例中，在步骤 203UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之后，本发明实施例提供的安全密钥更改方法还包括如下步骤中的至少一个步骤:

D2、UE 重置 UE 与主基站之间所建立的所有 RB 的 PDCP 配置;

D3、UE 重置 UE 与次基站之间所建立的所有 RB 的 PDCP 配置;

D4、UE 重置 UE 与主基站之间所建立的所有 RB 的 RLC 配置;

D5、UE 重置 UE 与次基站之间所建立的所有 RB 的 RLC 配置;

D6、UE 重置 UE 与主基站之间所建立的所有 RB 的 MAC 配置;

D7、UE 重置 UE 与次基站之间所建立的所有 RB 的 MAC 配置;

D8、UE 停止 UE 与主基站之间的数据传输;

D9、UE 停止 UE 与次基站之间的数据传输。

其中，步骤 D1 中 UE 按照 Key Re-key 执行与主基站之间的安全密钥更改，说明 UE 与主基站之间需要执行安全密钥更改，在这种情况下，步骤 D2 至步骤 D9 中的至少一个步骤在执行时可以根据具体需要来决定执行其中的一个步骤或者多个步骤，通过重置 UE 与主基站、次基站之间的接入层配置信息，并且在 UE 停止 UE 与主基站、次基站之间的数据传输时，可以避免 UE 与主基站、次基站之间的数据传输失败。需要说明的是，上述步骤中描述的 UE 重置 PDCP 配置指的是 UE 对该 PDCP 配置的配置信息进行重新配置，另外重置 RLC 配置、MAC 配置的含义相类似。

进一步的，步骤 D1UE 按照 Key Re-key 执行与主基站之间的安全密钥更

改，具体可以包括如下步骤:

D11、UE 基于更新后的接入层管理实体（Access Stratum Management Entity，ASME）中间密钥更新与主基站之间的 UE 侧中间密钥;

D12、UE 根据更新后的与主基站对应的 UE 侧中间密钥和主基站的安全算法生成新的与主基站对应的安全密钥，新的与主基站对应的安全密钥包括: UE 与主基站通信时使用的加密密钥和完整性保护密钥。

其中，UE 在生成与主基站对应的安全密钥时，先对主基站对应的 UE 侧中间密钥进行更新，然后使用更新的与主基站对应的 UE 侧中间密钥、主基站的安全算法生成新的与主基站对应的安全密钥。

进一步的，在本发明的一些实施例中，步骤 D11UE 基于更新后的接入层管理实体 ASME 中间密钥更新与主基站之间的 UE 侧中间密钥之后，本发明实施例提供的安全密钥更改方法还可以包括如下步骤:

E1、UE 根据更新后的主基站侧中间密钥、次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与次基站对应的 UE 侧中间密钥;

E2、UE 根据更新后的与次基站对应的 UE 侧中间密钥和次基站的安全算法生成新的与次基站对应的安全密钥，新的与次基站对应的安全密钥包括: UE 与次基站通信时使用的加密密钥。

其中，UE 在生成与次基站对应的安全密钥时，UE 需要使用到更新后的主基站侧中间密钥，故通过步骤 D11 可以获取到，然后对次基站对应的 UE 侧中间密钥进行更新，然后使用更新的与次基站对应的 UE 侧中间密钥、次基站的安全算法生成新的与次基站对应的安全密钥。需要说明的是，在步骤 E2 中 UE 使用的次基站的安全算法可以与步骤 D11 中 UE 使用的主基站的安全算法相同，当然步骤 E2 中 UE 使用的次基站的安全算法可以与步骤 D11 中 UE 使用的主基站的安全算法不相同，具体可以根据应用场景来决定，此处仅作说明，不做限定。

具体的，步骤 D1 中 UE 根据所述密钥更改命令消息确定主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key，具体为:

UE 根据密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定主基站与 UE 之间执行安全密钥更改的方式为

Key Re-key。

也就是说，主基站可以使用密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息来指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key，故 UE 接收到密钥更改命令消息之后，通过第一指示信息或第一安全密钥上下文信息就可以获知主基站与UE之间执行安全密钥更改的方式为 Key Re-key，另外，在本发明的一些实施例中，密钥更改命令消息具体可以为小区内切换命令消息，在这种情况下也使用小区内切换命令消息中携带的安全上下文来指示主基站与 UE 之间执行安全密钥更改的方式为 Key Re-key。

在本发明的一些实施例中，若密钥更改命令消息中包含的指示信息指示 UE 保持与第二基站之间的数据传输，步骤 203UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之后，本发明实施例提供的安全密钥更改方法还包括如下步骤中的至少一个步骤:

F1、UE 保持 UE 与第二基站之间所建立的所有 RB 的 PDCP 配置;

F2、UE 保持 UE 与第二基站之间所建立的所有 RB 的 RLC 配置;

F3、UE 保持 UE 与第二基站之间所建立的所有 RB 的 MAC 配置;

F4、UE 保持 UE 与第二基站之间的已激活的 SCell 的激活状态;

F5、UE 保持 UE 与第二基站之间通信使用的 C-RNTI;

F6、UE 保持 UE 与第二基站之间的数据传输。

其中，密钥更改命令消息中包含的指示信息指示 UE 保持与第二基站之间的数据传输，当第二基站为主基站时，第一基站为次基站，当第二基站为次基站时，第二基站为主基站，故当密钥更改命令消息中包含的指示信息指示 UE 保持与第二基站之间的数据传输时，说明 UE 与第一基站之间需要执行安全密钥更改，在这种情况下，步骤 F1 至步骤 F6 中的至少一个步骤在执行时可以根据具体需要来决定执行其中的一个步骤或者多个步骤，通过保持 UE 与第二基站之间的接入层配置信息，并且在 UE 保持 UE 与第二基站之间的数据传输时，可以避免 UE 与第一基站之间的安全密钥更改导致 RB 的接入层配置信息都需要重置，可以保证 UE 与第二基站之间的 RB 的正常数据传输，以避免 UE 与第一基站之间执行安全密钥更改导致 UE 与第二基站之间不必要的数据传输中断，从而减少不必要的数据传输延迟。

在本发明的一些实施例中，若密钥更改命令消息携带指示 UE 暂停与第一基站之间的数据传输，步骤 203UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之后，本发明实施例提供的安全密钥更改方法还包括如下步骤中的至少一个步骤：

G1、UE 保持 UE 与第一基站之间所建立的所有 RB 的 PDCP 配置；

G2、UE 保持 UE 与第一基站之间所建立的所有 RB 的 RLC 配置；

G3、UE 保持 UE 与第一基站之间所建立的所有 RB 的 MAC 配置；

G4、UE 保持 UE 与第一基站之间的已激活的 SCell 的激活状态；

G5、UE 保持 UE 与第一基站之间通信使用的 C-RNTI；

G6、UE 暂停 UE 与第一基站之间的数据传输。

其中，密钥更改命令消息中包含的指示信息指示 UE 暂停与第一基站之间的数据传输，在这种情况下，步骤 G1 至步骤 G6 中的至少一个步骤在执行时可以根据具体需要来决定执行其中的一个步骤或者多个步骤，通过保持 UE 与第一基站之间的接入层配置信息，并且在 UE 暂停 UE 与第一基站之间的数据传输时，可以避免 UE 与第一基站之间的接入层配置信息的重新配置。

在本发明的一些实施例中，若密钥更改命令消息携带指示 UE 停止与第一基站之间的数据传输，步骤 203UE 根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输之后，本发明实施例提供的安全密钥更改方法还包括如下步骤中的至少一个步骤：

H1、UE 重置 UE 与第一基站之间所建立的所有 RB 的 PDCP 配置；

H2、UE 重置 UE 与第一基站之间所建立的所有 RB 的 RLC 配置；

H3、UE 重置 UE 与第一基站之间所建立的所有 RB 的 MAC 配置；

H4、UE 停止 UE 与第一基站之间的数据传输。

其中，密钥更改命令消息中包含的指示信息指示 UE 停止与第一基站之间的数据传输，在这种情况下，说明 UE 与第一基站之间需要执行安全密钥更改，在这种情况下，步骤 H1 至步骤 H4 中的至少一个步骤在执行时可以根据具体需要来决定执行其中的一个步骤或者多个步骤，通过重置 UE 与第一基站之间的接入层配置信息，并且在 UE 停止 UE 与第一基站之间的数据传输时，可以

避免 UE 与第一基站之间的数据传输失败。

204、UE 向主基站发送密钥更改完成消息，以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改。

在本发明实施例中，当 UE 完成与第一基站之间的安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，当主基站接收到 UE 发送的密钥更改完成消息之后，第一基站也可以通过主基站接收到的密钥更改完成消息确定 UE 与第一基站之间的安全密钥更改已经完成，第一基站可以使用新的安全密钥继续与 UE 之间进行数据传输，需要说明的是，根据前述内容的描述可知，第一基站可以指的是主基站，也可以指的是次基站，还可以指的是主基站和次基站，故需要指示与 UE 之间需要执行安全密钥更改的基站在得到UE反馈的安全密钥已经更改完成之后可以继续与 UE 之间进行数据传输，故主基站与 UE 执行安全密钥更改并不会影响到次基站与 UE 之间的数据传输，同样的，次基站与 UE 执行安全密钥更改并不会影响到主基站与 UE 之间的数据传输。

通过以上内容对本发明实施例的描述可知，主基站向 UE 发送密钥更改命令消息，UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

为便于更好的理解和实施本发明实施例的上述方案，下面举例相应的应用场景来进行具体说明。

在本发明的一个应用场景中，请参阅如图 3-a 所示，为本发明实施例中主基站、次基站、UE 之间的一种交互流程示意图，具体可以包括如下步骤:

S01、MeNB 确定需要执行安全密钥更改，可以执行 Key Refresh，或者也可以执行 Key Re-key。

具体地，当 MeNB 接收到 MME 的密钥指示命令要求执行 Key Re-key 时，则 MeNB 确定需要进行 Key Re-key。当 MeNB 确定需要进行 Key Refresh 时，例如 MeNB 确定 UE 当前的 PDCP Count 值将要反转时，则确定需要执行 Key Refresh。

S02、当 MeNB 确定需要执行 Key Re-key 时，则 MeNB 可以向 SeNB 发送密钥更改指示消息，指示 SeNB 执行安全密钥更改。具体地，MeNB 可以在该密钥更改指示消息中携带基于 MeNB 的新的主基站侧中间密钥以及 SeNB 的一个或多个小区的频率和 PCI 信息或者 SeNB 特定的安全参数，例如 PDCP COUNT 值，生成的一个或多个次基站侧中间密钥，所述 SeNB 的一个或多个小区是与 SeNB 的安全密钥产生相关联的小区，所述一个或多个次基站侧中间密钥用于产生 SeNB 端的用户面加密密钥。

S03、MeNB 向 UE 发送小区内 HO 命令消息，以使得 UE 根据小区内 HO 命令消息执行安全密钥更改过程。具体地，当需要执行 Key Re-key 时，则所述小区内 HO 命令消息中的 Key Change Indicator 置为 True，否则，需要执行 Key Refresh 时，则将小区内 HO 命令消息中的 Key Change Indicator 置为 False。对于 Key Re-key 的情况，所述小区内 HO 命令消息中可以进一步包含 SeNB 侧的更新的与安全密钥相关联的小区信息或者与安全密钥相关联的基站的安全参数。

S04、UE 接收到 MeNB 发送的小区内切换命令消息之后，UE 执行安全密钥更改，根据小区内 HO 命令消息中的 Key Change Indicator 指示确定是否保持 UE 与 SeNB 之间的接入层配置信息，和/或，是否保持 UE 与 SeNB 之间的数据传输。

具体地，当根据所述小区内 HO 命令的指示确定需要执行 Key Refresh 或者 Key Change Indicator 为 False 时，则 UE 应该执行如下操作中的一项或多项：

1）、保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

2）、保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

3）、保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置；

4）、保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态；

5）、保持 UE 与 SeNB 之间通信使用的 C-RNTI；

6）、保持/暂停与 SeNB 之间的数据传输；

7)、执行与 MeNB 之间的 Key Refresh 过程，具体地，执行与 MeNB 之间的 Key Refresh 为使用小区内 HO 命令消息中指示的 Next Hop Chaining Count 的值基于当前的与 MeNB 对应的 UE 侧中间密钥或者 NH 更新与 MeNB 对应的 UE 侧中间密钥，然后进一步地，使用更新后的与 MeNB 对应的 UE 侧中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

如果根据小区内 HO 命令消息确定需要执行 Key Re-key， 则 UE 应该执行如下操作中的一项或多项:

1)、重置 MeNB 侧的 MAC;

2)、重置 SeNB 侧的 MAC;

3)、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 PDCP;

4)、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 RLC;

5)、停止与 MeNB 及 SeNB 之间的数据传输;

6)、根据小区内 HO 命令消息中的安全上下文信息，更新针对 MeNB 和 SeNB 的安全密钥。具体地，对于 MeNB，UE 基于更新的 ASME 中间密钥产生新的与 MeNB 之间的 UE 侧中间密钥，然后根据新产生的与 MeNB 之间的 UE 侧中间密钥和 MeNB 的安全算法产生新的与 MeNB 通信使用的加密密钥和完整性保护密钥。进一步地，UE 根据新的与 MeNB 之间的 UE 侧中间密钥以及 SeNB 侧与安全密钥更改相关联的小区的信息或者 SeNB 侧与安全相关联的基站特定的参数，例如 PDCP COUNT 产生一个与 SeNB 之间的 UE 侧中间密钥，然后 UE 基于新的与 SeNB 之间的 UE 侧中间密钥和 SeNB 的安全算法或者 MeNB 的安全算法产生新的与 SeNB 通信使用的加密密钥。所述 SeNB 的与安全相关联的小区为 UE 在安全密钥改变前与 SeNB 之间的安全相关联的小区的信息或者是从小区内 HO 命令消息中获得的 SeNB 的更新的安全相关联的小区的信息，具体地，小区信息包含物理小区标识（Physical Cell Identity，PCI）和频率（Freqency）。

S05、UE 向 MeNB 发送切换完成消息。具体地，可以是 UE 在成功执行向 MeNB 的随机接入后，向 MeNB 发送切换完成消息。也可以是 UE 成功向 MeNB 和 SeNB 都成功执行随机接入后，向 MeNB 发送切换完成消息。

具体地，在 UE 确定执行 Key Refresh 时，UE 不需要执行向 SeNB 的随机

接入。在 UE 确定执行 Key Re-key 时，则 UE 可以向 MeNB 和 SeNB 都执行随机接入，所述向 MeNB 和 SeNB 的随机接入可以并行进行。

S06、MeNB 向 SeNB 发送密钥改变完成消息。具体地，在 Key Re-key 的情况下，当 UE 不执行与 SeNB 之间的随机接入时，MeNB 需要向 SeNB 发送密钥改变完成消息，以通知 SeNB 所述 UE 的安全密钥改变过程已经成功完成，UE 与 SeNB 之间的数据传输可以开始使用新的安全密钥进行通信。在 Key Refresh 的情况下，如果 UE 暂停与 SeNB 的数据传输，则上述 MeNB 向 SeNB 发送的密钥改变完成消息用于指示 UE 与 SeNB 之间暂停的数据传输可以恢复。

需要说明的是，在如上图 3-a 介绍的应用场景中，SeNB 依附于 MeNB 产生 SeNB 侧的中间密钥，在这种情况下，当 MeNB 执行 Key Re-key 时，SeNB 需要同时执行安全密钥更改。在本发明的另一个应用场景中，请参阅如图 3-b 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图，具体可以包括如下步骤:

步骤 S11、MeNB 确定需要执行安全密钥更改，要么执行 Key-fresh，要么执行 Key Re-key。

具体地，当 MeNB 接收到 MME 的密钥指示命令要求执行 MeNB 和/或 SeNB 侧的 Key Re-key 时，则 MeNB 确定需要进行 Key Re-key。当 MeNB 确定 UE 当前在 MeNB 侧的 PDCP Count 值将要反转时，MeNB 可以确定需要 UE 针对 MeNB 进行 key Refresh。需要说明的是，在步骤 S11 之前，本发明实施例还可以包括步骤 S10，SeNB 向 MeNB 发送密钥刷新指示信息，当 MeNB 接收到 SeNB 发送的 SeNB 侧的 PDCP Count 值将要发生反转的指示信息，或者 SeNB 发送的 SeNB 需要执行 Key Refresh 的指示信息后，或者在 MeNB 接收到 SeNB 或者 UE 上报的当前 SeNB 侧的 PDCP Count 值将要发生反转时，MeNB 可以确定需要 UE 针对 MeNB 和/或 SeNB 进行安全密钥的 key Refresh。

步骤 S12、当 MeNB 接收到 MME 发送的要求执行 SeNB 侧的安全密钥的 Key Re-key 的指示时，MeNB 需要向 SeNB 发送密钥更改指示消息，以指示 SeNB 执行 Key Re-key 过程。

步骤 S13a、MeNB 在确定 UE 与 MeNB 之间需要执行安全密钥更改时，则向 UE 发送小区内 HO 命令消息，所述小区内 HO 命令消息中包含 UE 执行

针对 MeNB 的安全密钥进行 Key Re-key 还是 Key Refresh 的指示信息，例如通过小区内 HO 命令消息中的 Key Change Indicator 指示。

步骤 S13b、MeNB 在确定 UE 与 SeNB 之间的安全密钥需要更改时，向 UE 发送密钥更改命令消息，所述密钥更改命令消息中包含指示 UE 执行针对 SeNB 侧的安全密钥的 Key Re-key 还是 Key Refresh 的指示信息。

步骤 S14、 UE 接收到 MeNB 发送的小区内 HO 命令消息之后，如果根据所述小区内 HO 命令消息的指示确定需要执行 MeNB 侧的安全密钥更改，则 UE 应该执行下列操作中的一项或多项：

1）、仅仅执行与 MeNB 之间的安全密钥改变过程；

2）、保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

3）、保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

4）、保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置；

5）、保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态；

6）、保持 UE 与 SeNB 之间通信使用的 C-RNTI；

7）、保持/暂停与 SeNB 之间的数据传输；

如果 UE 在接收到小区内 HO 命令消息的时候，也接收到密钥更改命令消息，则 UE 应该执行下列操作中的一项或多项：

1）、重置 SeNB 侧的 MAC；

2）、针对在 SeNB 建立的 RB，重建立 PDCP；

3）、针对在 SeNB 建立的 RB，重建立 RLC；

4）、停止与 SeNB 之间的数据传输；

5）、根据密钥更改命令消息中携带的安全上下文信息以及密钥改变的指示信息，更改与 SeNB 通信的安全密钥；具体地，当根据密钥改变指示信息确定需要执行 Key Re-key 时，则 UE 基于与 SeNB 之间的更新的 ASME 中间密钥更新与 SeNB 之间的 UE 侧中间密钥，然后基于更新后的与 SeNB 之间的 UE 侧中间密钥以及 SeNB 的安全算法产生新的与 SeNB 通信使用的加密密钥；当根据密钥指示信息确定需要执行 key Refresh 时，则 UE 基于当前与 SeNB 对应的 UE 侧中间密钥或者 NH 的值更新与 SeNB 对应的 UE 侧中间密钥，然后基于更新后的与 SeNB 对应的 UE 侧中间密钥以及 SeNB 的安全算法产生新的加密密钥。

S15a、UE 向 MeNB 发送切换完成消息，该步骤为与步骤 S13a 相应的响应。具体地，可以是 UE 在成功执行向 MeNB 的随机接入后，向 MeNB 发送切换完成消息。也可以是 UE 成功向 MeNB 和 SeNB 都成功执行随机接入后，向 MeNB 发送切换完成消息。

具体地，在 UE 确定执行 Key Refresh 时，UE 不需要执行向 SeNB 的随机接入。在 UE 确定执行 Key Re-key 时，则 UE 可以向 MeNB 和 SeNB 都执行随机接入，所述向 MeNB 和 SeNB 的随机接入可以并行进行。

S15b、UE 向 MeNB 发送密钥更改完成消息，该步骤为与步骤 S13b 相应的响应。

S16、MeNB 向 SeNB 发送密钥改变完成消息。具体地，在 Key Re-key 的情况下，当 UE 不执行与 SeNB 之间的随机接入时，MeNB 需要向 SeNB 发送密钥改变完成消息，以通知 SeNB 所述 UE 的安全密钥改变过程已经成功完成，UE 与 SeNB 之间的数据传输可以开始使用新的安全密钥进行通信。在 Key Refresh 的情况下，如果 UE 暂停与 SeNB 的数据传输，则上述 MeNB 向 SeNB 发送的密钥改变完成消息用于指示 UE 与 SeNB 之间暂停的数据传输可以恢复。

在本发明的另一个应用场景中，请参阅如图 3-c 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图，具体可以包括如下步骤：

步骤 S21、MeNB 确定需要执行安全密钥更改，要么执行 Key-fresh，要么执行 Key Re-key。

具体地，当 MeNB 接收到 MME 的密钥指示命令要求执行 MeNB 或 SeNB 侧的 Key Re-key 时，则 MeNB 确定需要进行 Key Re-key。当 MeNB 确定 UE 当前在 MeNB 侧的 PDCP Count 值将要反转时，MeNB 可以确定需要 UE 针对 MeNB 进行 key Refresh。需要说明的是，在步骤 S21 之前，本发明实施例还可以包括步骤 S20，SeNB 向 MeNB 发送密钥刷新指示信息，当 MeNB 接收到 SeNB 发送的 SeNB 侧的 PDCP Count 值将要发生反转的指示信息，或者 SeNB 发送的 SeNB 需要执行 Key Refresh 的指示信息后，或者在 MeNB 接收到 SeNB 或者 UE 上报的当前 SeNB 侧的 PDCP Count 值将要发生反转时，MeNB 可以确定需要 UE 针对 SeNB 进行安全密钥的 key Refresh。

S22、当 MeNB 确定需要执行 Key Re-key 时，则 MeNB 可以向 SeNB 发

送密钥更改指示消息，指示 SeNB 需要执行安全密钥更改。

具体地，在与SeNB对应的中间密钥基于MeNB的中间密钥产生的情况下，可以在该密钥更改指示消息中携带基于MeNB的新的中间密钥以及SeNB的一个或多个小区的频率和 PCI 信息或者 SeNB 特定的安全参数，例如 PDCP COUNT 值生成的一个或多个与 SeNB 对应的中间密钥，所述 SeNB 的一个或多个小区是与 SeNB 的安全密钥产生相关联的小区，所述一个或多个与 SeNB 对应的中间密钥用于产生 SeNB 端的用户面加密密钥。

在与 SeNB 对应的中间密钥由 ASME 中间密钥产生的情况下，则密钥更改指示消息中携带 MME 为 SeNB 新产生的与 SeNB 对应的中间密钥。

S23、MeNB 向 UE 发送密钥更改命令消息，以使得 UE 根据密钥更改命令消息执行安全密钥更改过程。

具体地，所述密钥更改命令消息中包含第一指示信息和第二指示信息。所述第一指示信息用于指示所述 UE 更改与 MeNB 之间的安全密钥，所述第二指示信息用于指示 UE 更改与 SeNB 之间的安全密钥。

进一步地，第一指示信息中还可以包括执行 Key Re-key 还是 key Refresh 的指示信息，所述第二指示信息中还可以包括执行 Key Re-key 还是 Key Refresh 的指示信息。

特殊地，上述密钥更改命令消息可以是小区内 HO 命令消息。

S24、UE 接收到 MeNB 发送的密钥更改命令消息之后，根据密钥更改命令消息中的第一指示信息和第二指示信息确定如何执行安全密钥更改过程。

具体地，当根据所述密钥更改命令消息的指示确定需要仅需要执行与 MeNB 的安全密钥改变时，例如第一指示信息为 True，而第二指示信息为 False 时，则 UE 应该执行如下操作中的一项或多项：

1）、保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

2）、保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

3）、保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置；

4、保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态；

5）、保持 UE 与 SeNB 之间通信使用的 C-RNTI；

6）、保持/暂停与 SeNB 之间的数据传输；

7）、执行与 MeNB 之间的安全密钥改变过程，具体地，当根据第一指示

信息（例如第一指示信息中包括执行 key Refresh 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令消息中包含 Next Hop Chaining Count 的值）确定需要执行与 MeNB 之间的 key Refresh 时，则 UE 基于当前在 MeNB 侧的中间密钥或者 NH 更新产生新的在 MeNB 侧的中间密钥，然后进一步地，使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。当根据第一指示信息（例如第一指示信息中包括执行 key Re-rekey 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令消息中不包含 Next Hop Chaining Count 的值，或者为空），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 MeNB 之间的新的 ASME 中间密钥产生新的在 MeNB 侧的中间密钥，然后使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

如果根据所述密钥更改命令消息的指示确定需要仅需要执行与 SeNB 的安全密钥改变时，例如第一指示信息为 False，而第二指示信息为 True 时，则 UE 应该执行如下操作中的一项或多项：

1）、保持 UE 与 MeNB 之间所建立的所有 RB 的 PDCP，RLC，MAC 配置；

2）、保持 UE 与 MeNB 之间的已激活的 SCell 的激活状态；

3）、保持 UE 与 MeNB 之间的通信；

4）、重置 SeNB 侧的 MAC；

5）、针对 SeNB 侧建立的所有的 RB，重建立这些 RB 的 PDCP；

6）、针对 SeNB 侧建立的所有的 RB，重建立这些 RB 的 RLC；

7）、停止与 SeNB 之间的数据传输；

8）、执行与 SeNB 之间的安全密钥改变过程，具体地，当根据第二指示信息（例如第二指示信息中包括执行 key Refresh 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令中包含 Next Hop Chaining Count 的值）确定需要执行与 SeNB 之间的 key Refresh 时，则 UE 基于当前在 SeNB 侧的中间密钥或者 NH 更新产生新的在 SeNB 侧的中间密钥，然后进一步地，使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。当根据第二指示信息（例如第二指示信息中包括执行 key Re-rekey 的指示），或者密钥更改命令消息中携带的安全上下文信息

（例如密钥更改命令消息中不包含 Next Hop Chaining Count 的值，或者为空），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 SeNB 之间的新的 ASME 中间密钥产生新的在 SeNB 侧的中间密钥，然后使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。

如果根据所述密钥更改命令消息的指示确定需要需要执行与 MeNB 以及和 SeNB 的安全密钥更改过程时，例如第一指示信息和第二指示信息均为 True 时，则 UE 应该执行如下操作中的一项或多项：

1）、重置 MeNB 侧的 MAC；

2）、重置 SeNB 侧的 MAC；

3）、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 PDCP；

4）、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 RLC；

5）、停止与 MeNB 及 SeNB 之间的数据传输；

6）、执行与 MeNB、SeNB 之间的密钥改变过程如下：具体地，

当根据第一指示信息（例如第一指示信息中包括执行 key Refresh 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令消息中包含 Next Hop Chaining Count 的值）确定需要执行与 MeNB 之间的 key Refresh 时，则 UE 基于当前在 MeNB 侧的中间密钥或者 NH 更新产生新的在 MeNB 侧的中间密钥，然后进一步地，使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。当根据第一指示信息（例如第一指示信息中包括执行 key Re-rekey 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令消息中不包含 Next Hop Chaining Count 的值，或者为空），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 MeNB 之间的新的 ASME 中间密钥产生新的在 MeNB 侧的中间密钥，然后使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

具体地，当根据第二指示信息（例如第二指示信息中包括执行 key Refresh 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令中包含 Next Hop Chaining Count 的值）确定需要执行与 SeNB 之间的 key Refresh 时，则 UE 基于当前在 SeNB 侧的中间密钥或者 NH 更新产生新的在

SeNB 侧的中间密钥，然后进一步地，使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。当根据第二指示信息（例如第二指示信息中包括执行 key Re-rekey 的指示），或者密钥更改命令消息中携带的安全上下文信息（例如密钥更改命令消息中不包含 Next Hop Chaining Count 的值，或者为空），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 SeNB 之间的新的 ASME 中间密钥产生新的在 SeNB 侧的中间密钥，然后使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。

S25、UE 向 MeNB 发送密钥改变完成消息。

具体地，根据是否 MeNB 和 SeNB 都进行安全密钥更改，可以是 UE 在成功执行向 MeNB 或者 SeNB 的随机接入后（仅更改 MeNB 或 SeNB 密钥的情况），向 MeNB 发送密钥改变完成消息。也可以是 UE 成功向 MeNB 和 SeNB 都成功执行随机接入后（MeNB 和 SeNB 的密钥都进行更改），向 MeNB 发送密钥改变完成消息。UE 在 MeNB 和 SeNB 都执行随机接入时，两个随机接入过程可以并行进行。

具体地，UE 是否在 MeNB 和/或 SeNB 上执行随机接入，可以在上述密钥改变命令消息中明确通知 UE。即上述密钥改变命令消息中，包含是否在 MeNB 和/或 SeNB 执行随机接入的指示信息。

S26、MeNB 向 SeNB 发送密钥改变完成消息。特殊地，在 UE 也执行向 SeNB 的随机接入时，SeNB 也可以通过判断 UE 执行随机接入过程成功来确定安全密钥改变完成，因此这种情况下，MeNB 也可以不向 SeNB 发送密钥改变完成消息。

在本发明的另一个应用场景中，请参阅如图 3-d 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图，具体可以包括如下步骤：

步骤 S31、MeNB 确定需要执行安全密钥更改，要么执行 Key-fresh，要么执行 Key Re-key。

具体地，当 MeNB 接收到 MME 的密钥指示命令要求执行 MeNB 或 SeNB 侧的 Key Re-key 时，则 MeNB 确定需要进行 Key Re-key。当 MeNB 确定 UE 当前在 MeNB 侧的 PDCP Count 值将要反转时，MeNB 可以确定需要 UE 针对 MeNB 进行 key Refresh。需要说明的是，在步骤 S21 之前，本发明实施例还可

以包括步骤 S30，SeNB 向 MeNB 发送密钥刷新指示信息，当 MeNB 接收到 SeNB 发送的 SeNB 侧的 PDCP Count 值将要发生反转的指示信息，或者 SeNB 发送的 SeNB 需要执行 Key Refresh 的指示信息后，或者在 MeNB 接收到 SeNB 或者 UE 上报的当前 SeNB 侧的 PDCP Count 值将要发生反转时，MeNB 可以确定需要 UE 针对 SeNB 进行安全密钥的 key Refresh。

S32、当 MeNB 确定需要执行 Key Re-key 时，则 MeNB 可以向 SeNB 发送密钥更改指示消息，指示 SeNB 需要执行安全密钥更改。

具体地，在与 SeNB 对应的中间密钥基于 MeNB 的中间密钥产生的情况下，可以在该密钥更改指示消息中携带基于 MeNB 的新的中间密钥以及 SeNB 的一个或多个小区的频率和 PCI 信息或者 SeNB 特定的安全参数，例如 PDCP COUNT 值生成的一个或多个与 SeNB 对应的中间密钥，所述 SeNB 的一个或多个小区是与 SeNB 的安全密钥产生相关联的小区，所述一个或多个与 SeNB 对应的中间密钥用于产生 SeNB 端的用户面加密密钥。

在与 SeNB 对应的中间密钥由 ASME 中间密钥产生的情况下，则密钥更改指示消息中携带 MME 为 SeNB 新产生的与 SeNB 对应的中间密钥。

S33、MeNB 向 UE 发送密钥更改命令消息，以使得 UE 根据密钥更改命令消息执行安全密钥更改过程。

具体地，所述密钥更改命令消息中包含第一安全密钥上下文信息和第二安全密钥上下文信息。所述第一安全密钥上下文信息用于指示所述 UE 更改与 MeNB 之间的安全密钥，所述第二安全密钥上下文信息用于指示 UE 更改与 SeNB 之间的安全密钥。

特殊地，上述密钥更改命令消息可以是小区内 HO 命令消息。

S34、UE 接收到 MeNB 发送的密钥更改命令消息之后，根据密钥更改命令消息中的第一安全密钥上下文信息和第二安全密钥上下文信息确定如何执行安全密钥更改过程。

具体地，如果密钥更改命令消息中仅仅包含第一安全密钥上下文信息，则 UE 根据所述密钥更改命令消息确定仅需要执行与 MeNB 的安全密钥改变，则 UE 应该执行如下操作中的一项或多项：

1）、保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

2）、保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

3)、保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置;

4)、保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态;

5)、保持 UE 与 SeNB 之间通信使用的 C-RNTI;

6)、保持/暂停与 SeNB 之间的数据传输;

7)、执行与 MeNB 之间的安全密钥改变过程，具体地，当根据第一安全密钥上下文信息（例如第一安全密钥上下文信息中包含 Next Hop Chaining Count 的值）确定需要执行与 MeNB 之间的 key Refresh 时，则 UE 基于当前在 MeNB 侧的中间密钥或者 NH 更新产生新的在 MeNB 侧的中间密钥，然后进一步地，使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。当根据第一安全密钥上下文信息（例如第一安全密钥上下文信息中包含 Key Re-key 指示）确定需要执行与 MeNB 之间的 Key Re-key 过程时，则 UE 基于与 MeNB 之间的新的 ASME 中间密钥产生新的在 MeNB 侧的中间密钥，然后使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

如果根据所述密钥更改命令消息中仅仅包含第二安全密钥上下文信息，则 UE 根据所述密钥更改命令消息确定仅需要执行与 SeNB 的安全密钥改变，则 UE 应该执行如下操作中的一项或多项:

1)、保持 UE 与 MeNB 之间所建立的所有 RB 的 PDCP, RLC, MAC 配置;

2)、保持 UE 与 MeNB 之间的已激活的 SCell 的激活状态;

3)、保持 UE 与 MeNB 之间的数据传输;

4)、重置 SeNB 侧的 MAC;

5)、针对 SeNB 侧建立的所有的 RB，重建立这些 RB 的 PDCP;

6)、针对 SeNB 侧建立的所有的 RB，重建立这些 RB 的 RLC;

7)、停止与 SeNB 之间的数据传输;

8)、执行与 SeNB 之间的密钥改变过程，具体地，当根据第二安全密钥上下文信息（例如第二安全密钥上下文信息中包含 Next Hop Chaining Count 的值）确定需要执行与 SeNB 之间的 key Refresh 时，则 UE 基于当前在 SeNB 侧的中间密钥或者 NH 更新产生新的在 SeNB 侧的中间密钥，然后进一步地，使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信

使用的加密密钥。当根据第二安全密钥上下文信息（例如第二安全密钥上下文信息中包括执行 key Re-rekey 的指示），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 SeNB 之间的新的 ASME 中间密钥产生新的在 SeNB 侧的中间密钥，然后使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。

如果根据所述第一安全密钥上下文信息和第二安全密钥上下文信息确定需要执行与 MeNB 以及和 SeNB 的密钥改变时，例如密钥更改命令消息中包含第一安全密钥上下文信息和第二安全密钥上下文信息时，则 UE 应该执行如下操作中的一项或多项：

1）、重置 MeNB 侧的 MAC；

2）、重置 SeNB 侧的 MAC；

3）、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 PDCP；

4）、针对 MeNB 和 SeNB 侧建立的所有的 RB，重建立这些 RB 的 RLC；

5）、停止与 MeNB 及 SeNB 之间的数据传输；

6）、执行与 MeNB、SeNB 之间的密钥改变过程如下：具体地，

当根据第一安全密钥上下文信息（例如第一安全密钥上下文信息中包含 Next Hop Chaining Count 的值）确定需要执行与 MeNB 之间的 key Refresh 时，则 UE 基于当前在 MeNB 侧的中间密钥或者 NH 更新产生新的在 MeNB 侧的中间密钥，然后进一步地，使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。当根据第一安全密钥上下文信息（例如第一安全密钥上下文信息中包含 Key Re-key 指示）确定需要执行与 MeNB 之间的 Key Re-key 过程时，则 UE 基于与 MeNB 之间的新的 ASME 中间密钥产生新的在 MeNB 侧的中间密钥，然后使用更新后的在 MeNB 侧的中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

当根据第二安全密钥上下文信息（例如第二安全密钥上下文信息中包含 Next Hop Chaining Count 的值）确定需要执行与 SeNB 之间的 key Refresh 时，则 UE 基于当前在 SeNB 侧的中间密钥或者 NH 更新产生新的在 SeNB 侧的中间密钥，然后进一步地，使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。当根据第二安全密钥上下文信息

（例如第二安全密钥上下文信息中包括执行 key Re-rekey 的指示），确定需要执行与 MeNB 之间的 Key Re-key 过程，则 UE 基于与 SeNB 之间的新的 ASME 中间密钥产生新的在 SeNB 侧的中间密钥，然后使用更新后的在 SeNB 侧的中间密钥和 SeNB 的安全算法生成新的与 SeNB 通信使用的加密密钥。

S35、UE 向 MeNB 发送密钥改变完成消息。

具体地，根据是否 MeNB 和 SeNB 都进行安全密钥改变，可以是 UE 在成功执行向 MeNB 或者 SeNB 的随机接入后（仅更改 MeNB 或 SeNB 密钥的情况），向 MeNB 发送密钥改变完成消息。也可以是 UE 成功向 MeNB 和 SeNB 都成功执行随机接入后（MeNB 和 SeNB 的密钥都进行更改），向 MeNB 发送密钥改变完成消息。UE 在 MeNB 和 SeNB 都执行随机接入时，两个随机接入过程可以并行进行。

具体地，UE 是否在 MeNB 和/或 SeNB 上执行随机接入，可以在上述密钥更改命令消息中明确通知 UE。即上述密钥更改命令消息中，包含是否在 MeNB 和/或 SeNB 执行随机接入的指示信息。

S36、MeNB 向 SeNB 发送密钥改变完成消息。特殊地，在 UE 也执行向 SeNB 的随机接入时，SeNB 也可以通过判断 UE 执行随机接入过程成功来确定安全密钥改变完成，因此这种情况下，MeNB 也可以不向 SeNB 发送密钥改变完成消息。

在本发明的另一个应用场景中，请参阅如图 3-e 所示，为本发明实施例中主基站、次基站、UE 之间的另一种交互流程示意图，具体可以包括如下步骤：

S41、MeNB 确定需要执行安全密钥更改，可以执行 Key Refresh，或者也可以执行 Key Re-key。

具体地，当 MeNB 接收到 MME 的密钥指示命令要求执行 Key Re-key 时，则 MeNB 确定需要进行 Key Re-key。当 MeNB 确定需要进行 Key Refresh 时，例如 MeNB 确定 UE 当前的 PDCP Count 值将要反转时，则确定需要执行 Key Refresh。

S42、当 MeNB 确定需要执行 Key Re-key 时，则 MeNB 可以向 SeNB 发送密钥更改指示消息，指示 SeNB 执行安全密钥更改。具体地，MeNB 可以在该密钥更改指示消息中携带基于 MeNB 的新的主基站侧中间密钥以及 SeNB 的一个或多个小区的频率和 PCI 信息或者 SeNB 特定的安全参数，例如 PDCP

COUNT 值生成的一个或多个次基站侧中间密钥，所述 SeNB 的一个或多个小区是与 SeNB 的安全密钥产生相关联的小区，所述一个或多个次基站侧中间密钥用于产生 SeNB 端的用户面加密密钥。

S43、MeNB 向 UE 发送小区内 HO 命令消息，以使得 UE 根据小区内 HO 命令消息执行安全密钥更改过程。所述小区内 HO 命令消息中包含 SeNB 侧数据传输的指示信息，所述指示信息可以包含继续保持与 SeNB 传输的指示信息，或者停止与 SeNB 之间的数据传输的指示信息，或者暂停与 SeNB 之间的数据传输的指示信息，以使得 UE 根据该指示信息确定如何执行 SeNB 侧的数据传输。

S44、UE 接收到 MeNB 发送的小区内 HO 切换命令消息后，根据小区内 HO 命令中的指示信息确定如何处理与 SeNB 之间的数据传输。

如果 MeNB 指示 UE 保持与 SeNB 的数据传输，则 UE 应该执行如下操作中的一项或多项：

1）、保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

2）、保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

3）、保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置；

4）、保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态；

5）、保持 UE 与 SeNB 之间通信使用的 C-RNTI；

6）、保持与 SeNB 之间的数据传输；

7）、执行与 MeNB 之间的 Key Refresh 过程，具体地，执行与 MeNB 之间的 key Refresh 为使用小区内 HO 命令消息中指示的 Next Hop Chaining Count 的值基于当前的与 MeNB 对应的 UE 侧中间密钥或者 NH 更新与 MeNB 对应的 UE 侧中间密钥，然后进一步地，使用更新后的与 MeNB 对应的 UE 侧中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

如果 MeNB 指示暂停与 SeNB 之间的数据传输，则 UE 应该执行如下操作中的一项或多项：

1）保持 UE 与 SeNB 之间所建立的所有 RB 的 PDCP 配置；

2）保持 UE 与 SeNB 之间所建立的所有 RB 的 RLC 配置；

3）保持 UE 与 SeNB 之间所建立的所有 RB 的 MAC 配置；

4）保持 UE 与 SeNB 之间的已激活的 SCell 的激活状态;

5）保持 UE 与 SeNB 之间通信使用的 C-RNTI;

6）暂停与 SeNB 之间的数据传输;

7）执行与 MeNB 之间的 Key Refresh 过程，具体地，执行与 MeNB 之间的 key Refresh 为使用小区内 HO 命令消息中指示的 Next Hop Chaining Count 的值基于当前的与 MeNB 对应的 UE 侧中间密钥或者 NH 更新与 MeNB 对应的 UE 侧中间密钥，然后进一步地，使用更新后的与 MeNB 对应的 UE 侧中间密钥和 MeNB 的安全算法生成新的与 MeNB 通信使用的加密密钥和完整性保护密钥。

如果 MeNB 指示 UE 停止与 SeNB 的数据传输，则 UE 应该执行如下操作中的一项或多项:

1）、重置 MeNB 侧的 MAC 和 SeNB 侧的 MAC;

2）、针对 MeNB 和 SeNB 的 RB，重建立 PDCP 和 RLC;

3）、停止与 MeNB 及 SeNB 之间的数据传输;

4）、根据小区 HO 命令消息中的安全上下文信息，更新针对 MeNB 和 SeNB 的安全密钥，具体过程可参阅前述实施例的说明。

通过以上实施例对本发明的描述可知，本发明实施例中可以降低 MeNB 的安全密钥改变过程对 UE 与 SeNB 之间的数据传输的影响，避免 MeNB 的安全密钥更改过程中导致不必要的的 RB 的 PDCP, RLC 的重建立和 MAC 重置，保证了 UE 与 SeNB 之间的 RB 的正常数据传输。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

为便于更好的实施本发明实施例的上述方案，下面还提供用于实施上述方案的相关装置。

请参阅图 4-a 所示，本发明实施例提供的一种基站 400，基站 400 具体为主基站 MeNB，可以包括：密钥更改确定模块 401、消息发送模块 402、消息接收模块 403，其中，

密钥更改确定模块 401，用于确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；

消息发送模块 402，用于向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；

消息接收模块 403，用于接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

在本发明的一些实施例中，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块 402，还用于所述消息接收模块接收所述 UE 发送的密钥更改完成消息之后，向所述次基站转发所述密钥更改完成消息，以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

在本发明的一些实施例中，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

在本发明的一些实施例中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述消息发送模块 402，具体用于向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

具体的，在本发明的一些实施例中，请参阅如图 4-b 所示，所述密钥更改确定模块 401，包括：

命令接收子模块 4011，用于接收移动管理实体 MME 发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述 UE 之间执行 Key Re-key，和/或指示所述次基站和所述 UE 之间执行 Key Re-key；

密钥更改确定子模块 4012，用于根据所述密钥指示命令确定出第一基站与所述 UE 之间执行 Key Re-key。

进一步的，在本发明的一些实施例中，若所述主基站确定所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

在本发明的一些实施例中，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块 402，还用于所述密钥更改确定子模块根据所述密钥指示命令确定出第一基站与所述 UE 之间需要执行安全密钥更改之后，向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括：所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括：所述 MME 为所述次基站生成的次基站侧中间密钥。

在本发明的一些实施例中，所述密钥更改确定模块 401，具体用于判断所述 UE 当前在主基站侧的分组数据汇聚协议计数 PDCP Count 在预置次数内是否发生反转，若所述 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新 Key Refresh，其中，所述第一基站为所述主基站；和/或，当所述主基站接收到所述次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

在本发明的一些实施例中，所述密钥更改命令消息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

在本发明的一些实施例中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥

上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

在本发明的一些实施例中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，所述密钥更改命令消息中通过密钥改变指示 Key Change Indicator 字段的取值指示所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，或指示所述 UE 暂停与所述第一基站之间的数据传输，或指示所述 UE 停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

在本发明的一些实施例中，所述密钥更改命令消息具体为小区内切换 HO 命令消息。

通过以上内容对本发明实施例的描述可知，密钥更改确定模块确定第一基站与 UE 之间需要执行安全密钥更改，其中，第一基站包括主基站和次基站两者之中的至少一个基站，若主基站确定第一基站与 UE 之间需要执行安全密钥更改，消息发送模块向 UE 发送密钥更改命令消息，则 UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

请参阅图 5-a 所示，本发明实施例提供的一种 UE500，可以包括：消息接收模块 501、密钥更改模块 502、决策模块 503、消息发送模块 504，其中，

消息接收模块 501，用于接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述UE与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；

密钥更改模块 502，用于根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改；

决策模块 503，用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；

消息发送模块 504，用于向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

在本发明的一些实施例中，密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息，所述决策模块 503，还用于所述消息接收模块接收主基站发送的密钥更改命令消息之后，根据所述密钥更改命令消息携带指示所述UE是否在所述第一基站执行随机接入的指示信息确定是否在所述第一基站执行随机接入。

在本发明的另一些实施例中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述 UE500，请参阅如图 5-b 所示，还包括：随机接入模块 505，其中，

所述消息接收模块 501，具体用于接收主基站发送的包含随机接入资源的信息的密钥更改命令消息；

所述随机接入模块 505，用于根据所述随机接入资源的信息执行向所述第一基站的随机接入。

在本发明的一些实施例中，若所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述密钥更改模块 502，还用于根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

在本发明的一些实施例中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块 502，具体用于根据所述第一指示信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块 502，具体用于根据所述第二指示信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

在本发明的一些实施例中，所述 UE 接收到的所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述密钥更改模块 502，还用于根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

在本发明的一些实施例中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块 502，具体用于根据所述第一安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

在本发明的一些实施例中，若所述密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，所述密钥更改模块 502，具体用于通过所述 Key Change Indicator 字段的取值指示确定按照 Key Re-key 或 Key Refresh 执行与所述第一基站之间的安全密钥更改。

在本发明的一些实施例中，所述决策模块 503 具体用于：

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定

是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

根据所述密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

根据所述密钥更改命令消息中包含的指示所述UE保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

在本发明的一些实施例中，所述决策模块 503 具体用于:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与所述主基站或所述次基站之间的接入层配置信息;

或者，

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时，确定保持与所述主基站或所述次基站之间的接入层配置信息。

在本发明的一些实施例中，所述决策模块 503 具体用于:

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示

信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输,其中,所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改,所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输;

或者,

根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

在本发明的一些实施例中,所述决策模块 503 具体用于:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时,确定不保持与所述主基站以及次基站之间的数据传输;或者,

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时,确定保持与所述次基站之间的数据传输;

或者,

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时,确定保持与所述次基站之间的数据传输。

在本发明的一些实施例中,当所述 UE 根据所述密钥更改命令信息,确定需要保持与所述主基站之间的接入层配置信息,和/或,需要保持与所述主基站之间的数据传输时,所述决策模块 503,具体用于确定如下内容中的至少一项:

所述 UE 保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置;

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置;

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置;

所述 UE 保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活状态;

所述 UE 保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI;

所述 UE 保持或暂停所述 UE 与所述主基站之间的数据传输。

在本发明的一些实施例中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，所述保持与所述次基站之间的接入层配置信息，和/或，保持与所述次基站之间的数据传输，所述决策模块 503，具体用于确定如下内容中的至少一项:

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态;

所述 UE 保持所述 UE 与所述次基站之间通信使用的 C-RNTI;

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，所述密钥更改模块 502，具体用于所述密钥更改模块，具体用于当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，按照 Key Refresh 执行与所述主基站之间的安全密钥更改;

所述决策模块 503 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE500，请参阅如图 5-c 所示，相对于如图 5-a 所示的 UE500，还包括如下模块中的至少一个模块:

PDCP 保持模块 506，用于保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置;

RLC 保持模块 507，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置;

MAC 保持模块 508，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

激活保持模块 509，用于保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态；

C-RNTI 保持模块 510，用于保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI；

第一传输控制模块 511，用于保持或暂停所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，所述密钥更改模块 502，参阅如图 5-d 所示，包括：

第一中间密钥更新子模块 5021，用于基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值，使用当前的与所述主基站对应的 UE 侧中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥；

第一密钥更改子模块 5022，用于使用更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

在本发明的一些实施例中，所述决策模块 503，还用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，确定所述按照 Key Refresh 执行与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的 UE 侧中间密钥进行的。

在本发明的一些实施例中，所述密钥更改模块 502，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh。

在本发明的一些实施例中，所述密钥更改模块 502，具体用于当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，按照 Key Re-key 执行与所述主基站之间的安全密钥更改；

在本发明的一些实施例中，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE500，请参阅如图 5-e 所示，相对于如图 5-a 所示的 UE500，还包括如下模块中的至少一个模块:

PDCP 重置模块 512，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

RLC 重置模块 513，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

MAC 重置模块 514，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

第二传输控制模块 515，用于停止所述 UE 与所述主基站之间的数据传输; 停止所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，所述密钥更改模块 502，包括:

第二中间密钥更新子模块，用于基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥;

第一密钥更改子模块，用于根据更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括: 所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

在本发明的一些实施例中，所述密钥更改模块，还包括:

所述第三中间密钥更新子模块，还用于所述第二中间密钥更新子模块基于接入层管理实体 ASME 中间密钥更新与所述主基站对应的 UE 侧中间密钥之后，根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的 UE 侧中间密钥;

第二密钥更改子模块，用于根据更新后的与所述次基站对应的 UE 侧中间

密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括：所述 UE 与所述次基站通信时使用的加密密钥。

在本发明的一些实施例中，所述密钥更改模块 502，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

在本发明的一些实施例中，若所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置；

RLC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 RLC 配置；

MAC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置；

激活保持模块，用于保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态；

C-RNTI 保持模块，用于保持所述 UE 与所述第二基站之间通信使用的 C-RNTI；

传输保持模块，用于保持所述 UE 与所述第二基站之间的数据传输。

在本发明的一些实施例中，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

RLC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

MAC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

激活保持模块，用于保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态；

C-RNTI 保持模块，用于保持所述 UE 与所述第一基站之间通信使用的 C-RNTI；

传输暂停模块，用于暂停所述 UE 与所述第一基站之间的数据传输。

在本发明的一些实施例中，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

RLC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

MAC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

传输停止模块，用于停止所述 UE 与所述第一基站之间的数据传输。

通过以上内容对本发明实施例的描述可知，主基站向 UE 发送密钥更改命令消息，密钥更改模块根据密钥更改命令消息执行与第一基站之间的安全密钥更改，决策模块根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，消息发送模块向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

本发明实施例还提供一种计算机存储介质，其中，该计算机存储介质存储有程序，该程序执行包括上述方法实施例中记载的部分或全部步骤。

接下来介绍本发明实施例提供的另一种基站，该基站具体指的是主基站，请参阅图 6 所示，基站 600 包括:

输入装置 601、输出装置 602、处理器 603 和存储器 604 (其中基站 600 中的处理器 603 的数量可以一个或多个，图 6 中以一个处理器为例)。在本发明的一些实施例中，输入装置 601、输出装置 602、处理器 603 和存储器 604 可通过总线或其它方式连接，其中，图 6 中以通过总线连接为例。

其中，处理器 603，用于执行如下步骤:

确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

在本发明的一些实施例中，处理器 603 还用于执行以下步骤: 若所述主基站确定出的所述第一基站包括所述次基站时，接收所述 UE 发送的密钥更改完成消息之后，向所述次基站转发所述密钥更改完成消息，以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

在本发明的一些实施例中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，处理器 603 还用于执行以下步骤向所述 UE 发送随机接入资源的信息，包括: 向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

在本发明的一些实施例中，处理器 603 用于执行以下步骤: 所述主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，可以包括:

所述主基站接收移动管理实体 MME 发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述 UE 之间执行密钥再生产 Key Re-key，和/或指示所述次基站和所述 UE 之间执行 Key Re-key;

所述主基站根据所述密钥指示命令确定出第一基站与所述 UE 之间执行 Key Re-key。

在本发明的一些实施例中，若所述主基站确定所述第一基站与所述 UE 之间执行 Key Re-key，存储器 604 中存储的所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

在本发明的一些实施例中，处理器 603 具体用于执行以下步骤：若所述主基站确定出的所述第一基站包括所述次基站时，确定第一基站与用户设备 UE 之间需要执行安全密钥更改之后，向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括：所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括：所述 MME 为所述次基站生成的次基站侧中间密钥。

在本发明的一些实施例中，处理器 603 用于执行以下步骤：确定第一基站与用户设备 UE 之间需要执行安全密钥更改，具体包括：

判断所述 UE 当前在主基站侧的分组数据汇聚协议计数 PDCP Count 在预置次数内是否发生反转，若所述 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新 Key Refresh，其中，所述第一基站为所述主基站;

和/或，

当所述主基站接收到所述次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

在本发明的一些实施例中，存储器 604 中存储的所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

在本发明的一些实施例中，存储器 604 中存储的所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh；所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息中通过密钥改变指示 Key Change Indicator 字段的取值指示所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，或指示所述 UE 暂停与所述第一基站之间的数据传输，或指示所述 UE 停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

在本发明的一些实施例中，存储器 604 中存储的所述密钥更改命令消息具体为小区内切换 HO 命令消息。

通过以上内容对本发明实施例的描述可知，主基站确定第一基站与 UE 之

间需要执行安全密钥更改，其中，第一基站包括主基站和次基站两者之中的至少一个基站，若主基站确定第一基站与 UE 之间需要执行安全密钥更改，主基站向 UE 发送密钥更改命令消息，则 UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

接下来介绍本发明实施例提供的另一种 UE，请参阅图 7 所示，UE700 包括:

输入装置 701、输出装置 702、处理器 703 和存储器 704 (其中 UE700 中的处理器 703 的数量可以一个或多个，图 7 中以一个处理器为例)。在本发明的一些实施例中，输入装置 701、输出装置 702、处理器 703 和存储器 704 可通过总线或其它方式连接，其中，图 7 中以通过总线连接为例。

其中，处理器 703，用于执行如下步骤:

接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述 UE 与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改;

根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

在本发明的一些实施例中，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息，处理器 703 还用于执行以下步骤:

接收主基站发送的密钥更改命令消息之后，根据所述密钥更改命令消息携带指示所述UE是否在所述第一基站执行随机接入的指示信息确定是否在所述第一

基站执行随机接入。

在本发明的一些实施例中，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，处理器 703 用于执行以下步骤接收主基站发送的密钥更改命令消息，包括：接收所述主基站发送的包含随机接入资源的信息的密钥更改命令消息，并根据所述随机接入资源的信息执行向所述第一基站的随机接入。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：若所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

在本发明的一些实施例中，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：根据所述第一指示信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

在本发明的一些实施例中，所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：根据所述第二指示信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所

述次基站、所述第一基站为所述主基站和所述次基站。

在本发明的一些实施例中，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：根据所述第一安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改。

在本发明的一些实施例中，所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：根据所述第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

在本发明的一些实施例中，若所述密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：通过所述 Key Change Indicator 字段的取值指示确定按照 Key Re-key 或 Key Refresh 执行与所述第一基站之间的安全密钥更改。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令信息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，具体包括：

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改；

或者，

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基

站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

在本发明的一些实施例中,处理器 703 用于执行以下步骤:所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息,具体包括:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时,确定不保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时,确定保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时,确定保持与所述主基站或所述次基站之间的接入层配置信息。

在本发明的一些实施例中,处理器 703 用于执行以下步骤:所述 UE 根据所述密钥更改命令信息,确定是否保持与所述主基站或所述次基站之间的数据传输,具体包括:

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输,其中,所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改,所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输,

其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改；

或者，

根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输；

或者，

根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输，具体包括：

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站以及次基站之间的数据传输；或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与所述次基站之间的数据传输；

或者，

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，确定保持与所述次基站之间的数据传输。

在本发明的一些实施例中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述主基站之间的接入层配置信息，和/或，需要保持与所述主基站之间的数据传输时，处理器 703 用于执行以下步骤：所述保持与所述主基站之间的接入层配置信息，和/或，保持与所述主基站之间的数据传输，包括如下步骤中的至少一个步骤：

保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC

配置;

保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活状态;

保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI;

保持或暂停所述 UE 与所述主基站之间的数据传输。

在本发明的一些实施例中，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，处理器 703 用于执行以下步骤：所述保持与所述次基站之间的接入层配置信息，和/或，保持与所述次基站之间的数据传输，包括如下步骤中的至少一个步骤：

保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态;

保持所述 UE 与所述次基站之间通信使用的 C-RNTI;

保持或暂停所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体包括：

当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，按照 Key Refresh 执行与所述主基站之间的安全密钥更改;

根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，处理器 703 用于执行以下步骤中的至少一个步骤：

保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置;

保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置;

保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置;

保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态;

保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI;

保持或暂停所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 按照 Key Refresh 执行与所述主基站之间的安全密钥更改，具体包括:

基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值，使用当前的与所述主基站对应的 UE 侧中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥;

使用更新后的与所述主基站对应的UE侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之前，确定所述按照 Key Refresh 执行与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的 UE 侧中间密钥进行的。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息确定所述主基站与所述UE之间执行安全密钥更改的方式为 Key Refresh，具体为:

根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh。

在本发明的一些实施例中，处理器 703 用于执行以下步骤：所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体包括:

当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，按照 Key Re-key 执行与所述主基站之间的安全密钥更改;

根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数

据传输之后，处理器 703 还用于执行以下步骤中的至少一个步骤:

重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置;

重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置;

重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置;

重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

停止所述 UE 与所述主基站之间的数据传输;

停止所述 UE 与所述次基站之间的数据传输。

在本发明的一些实施例中，处理器 703 用于执行以下步骤: 所述 UE 按照 Key Re-key 执行与所述主基站之间的安全密钥更改，具体包括:

基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥;

根据更新后的与所述主基站对应的UE侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括: 所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

在本发明的一些实施例中，处理器 703 还用于执行以下步骤: 所述 UE 基于更新后的接入层管理实体ASME中间密钥更新与所述主基站之间的UE侧中间密钥之后，根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的 UE 侧中间密钥;

根据更新后的与所述次基站对应的UE侧中间密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括: 所述 UE 与所述次基站通信时使用的加密密钥。

在本发明的一些实施例中，处理器 703 用于执行以下步骤: 所述 UE 根据所述密钥更改命令消息包含的指示信息确定所述主基站与所述UE之间执行安全密钥更改的方式为 Key Re-key，具体为:

根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

在本发明的一些实施例中，若所述密钥更改命令消息中包含的指示信息指示所述 UE 保持与所述第二基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，处理器 703 还用于执行以下步骤中的至少一个步骤：

保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站；

保持所述 UE 与所述第二基站之间所建立的所有 RB 的 RLC 配置；

保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置；

保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态；

保持所述 UE 与所述第二基站之间通信使用的 C-RNTI；

保持所述 UE 与所述第二基站之间的数据传输。

在本发明的一些实施例中，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，处理器 703 还用于执行以下步骤中的至少一个步骤：

保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态；

保持所述 UE 与所述第一基站之间通信使用的 C-RNTI；

暂停所述 UE 与所述第一基站之间的数据传输。

在本发明的一些实施例中，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，处理器 703 用于执行以下步骤中的至少一个步骤：

重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置;

重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置;

停止所述 UE 与所述第一基站之间的数据传输。

通过以上内容对本发明实施例的描述可知，主基站向 UE 发送密钥更改命令消息，UE 根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输，当 UE 完成安全密钥更改之后，UE 向主基站发送密钥更改完成消息，则主基站可以接收到 UE 发送的密钥更改完成消息，并通过主基站可以使第一基站确定 UE 与第一基站之间已经完成安全密钥更改，进而第一基站和 UE 就可以使用新的安全密钥进行数据传输，故按照本发明实施例中可以在 UE 同时与 MeNB 和 SeNB 执行双连接通信时实现对安全密钥的更改。

另外需说明的是，以上所描述的装置实施例仅仅是示意性的，其中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模块来实现本实施例方案的目的。另外，本发明提供的装置实施例附图中，模块之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过专用硬件包括专用集成电路、专用 CPU、专用存储器、专用元器件等来实现。一般情况下，凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现，而且，用来实现同一功能的具体硬件结构也可以是多种多样的，例如模拟电路、数字电路或专用电路等。但是，对本发明而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献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可读取的存储介质中，如计算机的软盘，U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等，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）执行本发明各个实施例所述的方法。

综上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照上述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对上述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

权 利 要 求

1、一种安全密钥更改方法，其特征在于，包括:

主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

所述主基站向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

所述主基站接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

2、根据权利要求 1 所述的方法，其特征在于，若所述主基站确定出的所述第一基站包括所述次基站时，所述主基站接收所述 UE 发送的密钥更改完成消息之后，还包括:

所述主基站向所述次基站转发所述密钥更改完成消息，以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

3、根据权利要求 1 所述的方法，其特征在于，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

4、根据权利要求 3 所述的方法，其特征在于，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述主基站向所述 UE 发送密钥更改命令消息，包括:

所述主基站向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

5、根据权利要求 1 所述的方法，其特征在于，所述主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，包括:

所述主基站接收移动管理实体 MME 发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述 UE 之间执行密钥再生产 Key Re-key，和/或指示所述次基站和所述 UE 之间执行 Key Re-key;

所述主基站根据所述密钥指示命令确定出第一基站与所述 UE 之间执行 Key Re-key。

6、根据权利要求 5 所述的方法，其特征在于，若所述主基站确定所述第

一基站与所述 UE 之间执行 Key Re-key，所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

7、根据权利要求 1 所述的方法，其特征在于，若所述主基站确定出的所述第一基站包括所述次基站时，所述主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改之后，还包括:

所述主基站向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括: 所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括: 所述 MME 为所述次基站生成的次基站侧中间密钥。

8、根据权利要求 1 所述的方法，其特征在于，所述主基站 MeNB 确定第一基站与用户设备 UE 之间需要执行安全密钥更改，包括:

所述主基站判断所述 UE 当前在主基站侧的分组数据汇聚协议计数 PDCP Count 在预置次数内是否发生反转，若所述 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则所述主基站确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新 Key Refresh，其中，所述第一基站为所述主基站;

和/或，

当所述主基站接收到所述次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，所述主基站确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

9、根据权利要求 1 至 8 中任一项所述的方法，其特征在于，所述密钥更改命令消息包括: 第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

10、根据权利要求 9 所述的方法，其特征在于，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

11、根据权利要求 1 至 8 中任一项所述的方法，其特征在于，所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

12、根据权利要求 11 所述的方法，其特征在于，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

13、根据权利要求 1 所述的方法，其特征在于，所述密钥更改命令消息中通过密钥改变指示 Key Change Indicator 字段的取值指示所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

14、根据权利要求 1 所述的方法，其特征在于，所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，或指示所述 UE 暂停与所述第一基站之间的数据传输，或指示所述 UE 停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

15、根据权利要求 1 至 14 中任一项所述的方法，其特征在于，所述密钥更改命令消息具体为小区内切换 HO 命令消息。

16、一种安全密钥更改方法，其特征在于，包括：

用户设备 UE 接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述 UE 与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；

所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥

更改;

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输;

所述 UE 向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

17、根据权利要求 16 所述的方法，其特征在于，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息，所述 UE 接收主基站发送的密钥更改命令消息之后，还包括:

所述 UE 根据所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息确定是否在所述第一基站执行随机接入。

18、根据权利要求 16 或 17 所述的方法，其特征在于，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述 UE 接收主基站发送的密钥更改命令消息，包括:

所述UE接收所述主基站发送的包含随机接入资源的信息的密钥更改命令消息，并根据所述随机接入资源的信息执行向所述第一基站的随机接入。

19、根据权利要求 16 所述的方法，其特征在于，若所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括: 第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述 UE 根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种: 所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

20、根据权利要求 19 所述的方法，其特征在于，所述第一指示信息中还包括: 指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为: 所述 UE 根据所述第一指示信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改;

所述第二指示信息中还包括: 指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令

消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 根据所述第二指示信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

21、根据权利要求 16 所述的方法，其特征在于，所述 UE 接收到的所述密钥更改命令消息中包含的指示信息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改，则所述 UE 根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

22、根据权利要求 21 所述的方法，其特征在于，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 根据所述第一安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 根据所述第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

23、根据权利要求 16 所述的方法，其特征在于，若所述密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，具体为：所述 UE 通过所述 Key Change Indicator 字段的取值指示确定按照 Key Re-key 或 Key Refresh 执行与所述第一基站之间的安全密钥更改。

24、根据权利要求 16 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令信息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，包括：

所述UE根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述UE之间需要执行安全密钥更改；

或者，

所述UE根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述UE之间需要执行安全密钥更改；

或者，

所述 UE 根据所述密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息；

或者，

所述UE根据所述密钥更改命令消息中包含的指示所述UE保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

25、根据权利要求 24 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息，包括：

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，所述 UE 确定不保持与所述主基站或所述次基站之间的接入层配置信息；

或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，所述 UE 确定保持与所述主基站或所述次基站之间的接入层配置信息；

或者，

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时，所述 UE 确定保持与所述主基站或所述次基站之间的接入层配置

信息。

26、根据权利要求 16 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令信息，确定是否保持与所述主基站或所述次基站之间的数据传输，包括:

所述UE根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

所述UE根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者，

所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输;

或者，

所述 UE 根据所述密钥更改命令消息中包含的指示所述 UE 保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

27、根据权利要求 26 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输，包括:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，所述 UE 确定不保持与所述主基站以及次基站之间的数据传输；或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，所述 UE 确定保持与所述次基站之间的数据传输;

或者，

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，所述 UE 确定保持与所述次基站之间的数据传输。

28、根据权利要求 16 所述的方法，其特征在于，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述主基站之间的接入层配置信息，和/或，需要保持与所述主基站之间的数据传输时，所述保持与所述主基站之间的接入层配置信息，和/或，保持与所述主基站之间的数据传输，包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

所述 UE 保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活状态；

所述 UE 保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述主基站之间的数据传输。

29、根据权利要求 16 所述的方法，其特征在于，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，所述保持与所述次基站之间的接入层配置信息，和/或，保持与所述次基站之间的数据传输，包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态；

所述 UE 保持所述 UE 与所述次基站之间通信使用的 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

30、根据权利要求 16 至 29 中任一项所述的方法，其特征在于，所述 UE

根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，包括：当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，所述 UE 按照 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

所述 UE 保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态；

所述 UE 保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

31、根据权利要求 30 所述的方法，其特征在于，所述 UE 按照 Key Refresh 执行与所述主基站之间的安全密钥更改，包括：

所述 UE 基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值，使用当前的与所述主基站对应的 UE 侧中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥；

所述 UE 使用更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

32、根据权利要 31 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之前，还包

括:

所述 UE 确定所述按照 Key Refresh 执行与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的 UE 侧中间密钥进行的。

33、根据权利要求 30 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，具体为:

所述UE根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh。

34、根据权利要求 16 至 29 种任一项所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改，包括:

当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，所述 UE 按照 Key Re-key 执行与所述主基站之间的安全密钥更改;

所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤:

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 停止所述 UE 与所述主基站之间的数据传输;

所述 UE 停止所述 UE 与所述次基站之间的数据传输。

35、根据权利要求 34 所述的方法，其特征在于，所述 UE 按照 Key Re-key 执行与所述主基站之间的安全密钥更改，包括:

所述UE基于更新后的接入层管理实体ASME中间密钥更新与所述主基站之间的 UE 侧中间密钥;

所述 UE 根据更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站

的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

36、根据权利要求 35 所述的方法，其特征在于，所述 UE 基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥之后，还包括：

所述 UE 根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的 UE 侧中间密钥；

所述 UE 根据更新后的与所述次基站对应的 UE 侧中间密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括：所述 UE 与所述次基站通信时使用的加密密钥。

37、根据权利要求 34 所述的方法，其特征在于，所述 UE 根据所述密钥更改命令消息包含的指示信息确定所述主基站与所述UE之间执行安全密钥更改的方式为 Key Re-key，具体为：

所述UE根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

38、根据权利要求 16 至 29 中任一项所述的方法，其特征在于，若所述密钥更改命令消息中包含的指示信息指示所述UE保持与所述第二基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤：

所述 UE 保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站；

所述UE保持所述UE与所述第二基站之间所建立的所有RB的RLC配置；

所述 UE 保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态；

所述 UE 保持所述 UE 与所述第二基站之间通信使用的 C-RNTI;

所述 UE 保持所述 UE 与所述第二基站之间的数据传输。

39、根据权利要求 16 至 29 中任一项所述的方法，其特征在于，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤:

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态;

所述 UE 保持所述 UE 与所述第一基站之间通信使用的 C-RNTI;

所述 UE 暂停所述 UE 与所述第一基站之间的数据传输。

40、根据权利要求 16 至 29 中任一项所述的方法，其特征在于，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述 UE 根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述方法还包括如下步骤中的至少一个步骤:

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置;

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置;

所述 UE 重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置;

所述 UE 停止所述 UE 与所述第一基站之间的数据传输。

41、一种基站，其特征在于，所述基站具体为主基站 MeNB，包括:

密钥更改确定模块，用于确定第一基站与用户设备 UE 之间需要执行安全密钥更改，其中，所述第一基站包括所述主基站和次基站两者之中的至少一个基站;

消息发送模块，用于向所述 UE 发送密钥更改命令消息，以使所述 UE 根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改以及根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；

消息接收模块，用于接收所述 UE 发送的密钥更改完成消息，以使所述第一基站确定所述 UE 与所述第一基站之间已经完成安全密钥更改。

42、根据权利要求 41 所述的基站，其特征在于，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块，还用于所述消息接收模块接收所述 UE 发送的密钥更改完成消息之后，向所述次基站转发所述密钥更改完成消息，以使所述次基站确定所述 UE 与所述次基站之间已经完成安全密钥更改。

43、根据权利要求 41 所述的基站，其特征在于，所述密钥更改命令消息携带指示所述 UE 是否在所述第一基站执行随机接入的指示信息。

44、根据权利要求 43 所述的基站，其特征在于，若所述密钥更改命令消息指示所述 UE 在所述第一基站执行随机接入时，所述消息发送模块，具体用于向所述 UE 发送包含随机接入资源的信息的密钥更改命令消息，以使所述 UE 根据所述随机接入资源的信息与所述第一基站执行随机接入。

45、根据权利要求 41 所述的基站，其特征在于，所述密钥更改确定模块，包括：

命令接收子模块，用于接收移动管理实体 MME 发送的密钥指示命令，所述密钥指示命令用于指示所述主基站和所述 UE 之间执行 Key Re-key，和/或指示所述次基站和所述 UE 之间执行 Key Re-key；

密钥更改确定子模块，用于根据所述密钥指示命令确定出第一基站与所述 UE 之间执行 Key Re-key。

46、根据权利要求 45 所述的基站，其特征在于，若所述主基站确定所述第一基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，所述密钥更改命令消息中携带所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息。

47、根据权利要求 41 所述的基站，其特征在于，若所述主基站确定出的所述第一基站包括所述次基站时，所述消息发送模块，还用于所述密钥更改确

定子模块根据所述密钥指示命令确定出第一基站与所述UE之间需要执行安全密钥更改之后，向所述次基站发送密钥更改指示消息，所述密钥更改指示消息用于指示所述次基站执行安全密钥更改，所述密钥更改指示消息包括：所述主基站根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息生成的次基站侧中间密钥，或，所述密钥更改指示消息包括：所述 MME 为所述次基站生成的次基站侧中间密钥。

48、根据权利要求 41 所述的基站，其特征在于，所述密钥更改确定模块，具体用于判断所述 UE 当前在主基站侧的分组数据汇聚协议计数 PDCP Count 在预置次数内是否发生反转，若所述 UE 当前在主基站侧的 PDCP Count 在预置次数发生反转，则确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为密钥刷新 Key Refresh，其中，所述第一基站为所述主基站；和/或，当所述主基站接收到所述次基站发送的次基站侧的 PDCP Count 在预置次数发生反转的指示信息，或所述主基站接收到所述次基站发送的所述次基站需要执行 Key Refresh 的指示信息，或所述主基站接收到所述 UE 上报的当前次基站侧的 PDCP Count 在预置次数发生反转时，确定第一基站与所述 UE 之间需要执行安全密钥更改，并且确定采用的方式为 Key Refresh，其中，所述第一基站为所述次基站。

49、根据权利要求 41 至 48 中任一项所述的基站，其特征在于，所述密钥更改命令消息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改。

50、根据权利要求 49 所述的基站，其特征在于，所述第一指示信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh;

所述第二指示信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh。

51、根据权利要求 41 至 48 中任一项所述的基站，其特征在于，所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执

行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述UE之间需要执行安全密钥更改。

52、根据权利要求51所述的基站，其特征在于，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh。

53、根据权利要求41所述的基站，其特征在于，所述密钥更改命令消息中通过密钥改变指示Key Change Indicator字段的取值指示所述第一基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh。

54、根据权利要求41所述的基站，其特征在于，所述密钥更改命令消息携带指示所述UE保持与所述第二基站之间的数据传输，或指示所述UE暂停与所述第一基站之间的数据传输，或指示所述UE停止与所述第一基站之间的数据传输的指示信息，当所述第二基站为所述主基站时，所述第一基站为所述次基站，当所述第二基站为所述次基站时，所述第二基站为所述主基站。

55、根据权利要求41至54中任一项所述的基站，其特征在于，所述密钥更改命令消息具体为小区内切换HO命令消息。

56、一种用户设备UE，其特征在于，包括：

消息接收模块，用于接收主基站发送的密钥更改命令消息，所述密钥更改命令消息包括所述主基站命令所述UE与第一基站之间需要执行安全密钥更改的指示信息，所述第一基站包括所述主基站和次基站两者之中的至少一个基站；

密钥更改模块，用于根据所述密钥更改命令消息执行与所述第一基站之间的安全密钥更改；

决策模块，用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输；

消息发送模块，用于向所述主基站发送密钥更改完成消息，以使所述第一基站确定所述UE与所述第一基站之间已经完成安全密钥更改。

57、根据权利要求56所述的UE，其特征在于，所述密钥更改命令消息携

带指示所述UE是否在所述第一基站执行随机接入的指示信息，所述决策模块，还用于所述消息接收模块接收主基站发送的密钥更改命令消息之后，根据所述密钥更改命令消息携带指示所述UE是否在所述第一基站执行随机接入的指示信息确定是否在所述第一基站执行随机接入。

58、根据权利要求56或57所述的UE，其特征在于，若所述密钥更改命令消息指示所述UE在所述第一基站执行随机接入时，所述UE，还包括：随机接入模块，其中，

所述消息接收模块，具体用于接收主基站发送的包含随机接入资源的信息的密钥更改命令消息；

所述随机接入模块，用于根据所述随机接入资源的信息执行向所述第一基站的随机接入。

59、根据权利要求56所述的UE，其特征在于，若所述UE接收到的所述密钥更改命令消息中包含的指示信息包括：第一指示信息和第二指示信息，其中，所述第一指示信息用于指示所述主基站与所述UE之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述UE之间需要执行安全密钥更改，则所述密钥更改模块，还用于根据所述第一指示信息和/或所述第二指示信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

60、根据权利要求59所述的UE，其特征在于，所述第一指示信息中还包括：指示所述主基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh，所述密钥更改模块，具体用于根据所述第一指示信息按照Key Re-key或Key Refresh执行与所述主基站之间的安全密钥更改；

所述第二指示信息中还包括：指示所述次基站与所述UE之间执行安全密钥更改的方式为Key Re-key或Key Refresh，所述密钥更改模块，具体用于根据所述第二指示信息按照Key Re-key或Key Refresh执行与所述次基站之间的安全密钥更改。

61、根据权利要求56所述的UE，其特征在于，所述UE接收到的所述密钥更改命令消息包括：第一安全密钥上下文信息和第二安全密钥上下文信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述UE之间需要

执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述UE之间需要执行安全密钥更改，则所述密钥更改模块，还用于根据所述第一安全密钥上下文信息和/或所述第二安全密钥上下文信息确定出所述第一基站为以下三种情况中的一种：所述第一基站为所述主基站、所述第一基站为所述次基站、所述第一基站为所述主基站和所述次基站。

62、根据权利要求61所述的UE，其特征在于，所述第一安全密钥上下文信息中还包括：指示所述主基站与所述 UE 之间执行安全密钥更改的方式为Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第一安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述第二安全密钥上下文信息中还包括：指示所述次基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key 或 Key Refresh，所述密钥更改模块，具体用于根据所述第二安全密钥上下文信息按照 Key Re-key 或 Key Refresh 执行与所述次基站之间的安全密钥更改。

63、根据权利要求56所述的UE，其特征在于，若所述密钥更改命令消息中包含的指示信息为密钥改变指示 Key Change Indicator 字段，所述密钥更改模块，具体用于通过所述 Key Change Indicator 字段的取值指示确定按照 Key Re-key 或 Key Refresh 执行与所述第一基站之间的安全密钥更改。

64、根据权利要求56所述的UE，其特征在于，所述决策模块具体用于：

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或次基站之间的接入层配置信息，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改；

或者，

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改；

或者，

根据所述密钥更改命令消息中包含的密钥改变指示 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

根据所述密钥更改命令消息中包含的指示所述UE保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的接入层配置信息。

65、根据权利要求 64 所述的 UE，其特征在于，所述决策模块具体用于:

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时,确定保持与所述主基站或所述次基站之间的接入层配置信息;

或者,

当根据所述 Key Change Indicator 字段确定需要基于下一跳 NH 执行 Key Refresh 时，确定保持与所述主基站或所述次基站之间的接入层配置信息。

66、根据权利要求 56 所述的 UE，其特征在于，所述决策模块具体用于:

根据所述密钥更改命令消息中包含的第一指示信息和第二指示信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一指示信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改，所述第二指示信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的第一安全密钥上下文信息和第二安全密钥上下文信息确定是否保持与所述主基站或所述次基站之间的数据传输，其中，所述第一安全密钥上下文信息用于指示所述主基站与所述 UE 之间需要执行安全密钥更改,所述第二安全密钥上下文信息用于指示所述次基站与所述 UE 之间需要执行安全密钥更改;

或者,

根据所述密钥更改命令消息中包含的 Key Change Indicator 字段确定是否保持与所述主基站或所述次基站之间的数据传输;

或者，

根据所述密钥更改命令消息中包含的指示所述UE保持与所述主基站或次基站之间的数据传输的指示信息确定是否保持与所述主基站或所述次基站之间的数据传输。

67、根据权利要求 66 所述的 UE，其特征在于，所述决策模块具体用于：

当根据所述 Key Change Indicator 字段确定需要执行 Key Re-key 时，确定不保持与所述主基站以及次基站之间的数据传输；或者，

当根据所述 Key Change Indicator 字段确定需要基于与所述主基站对应的 UE 侧中间密钥执行 Key Refresh 时，确定保持与所述次基站之间的数据传输；

或者，

当根据所述 Key Change Indicator 字段确定需要基于 NH 执行 Key Refresh 时，确定保持与所述次基站之间的数据传输。

68、根据权利要求 56 所述的 UE，其特征在于，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述主基站之间的接入层配置信息，和/或，需要保持与所述主基站之间的数据传输时，所述决策模块，具体用于确定如下内容中的至少一项：

所述 UE 保持所述 UE 与所述主基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

所述 UE 保持所述 UE 与所述主基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

所述 UE 保持所述 UE 与所述主基站之间的已激活的次小区 SCell 的激活状态；

所述 UE 保持所述 UE 与所述主基站之间通信使用的小区无线网络临时标识符 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述主基站之间的数据传输。

69、根据权利要求 56 所述的 UE，其特征在于，当所述 UE 根据所述密钥更改命令信息，确定需要保持与所述次基站之间的接入层配置信息，和/或，需要保持与所述次基站之间的数据传输时，所述保持与所述次基站之间的接入

层配置信息，和/或，保持与所述次基站之间的数据传输，所述决策模块，具体用于确定如下内容中的至少一项：

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置；

所述 UE 保持所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置；

所述 UE 保持所述 UE 与所述次基站之间的已激活的 SCell 的激活状态；

所述 UE 保持所述 UE 与所述次基站之间通信使用的 C-RNTI；

所述 UE 保持或暂停所述 UE 与所述次基站之间的数据传输。

70、根据权利要求 56 至 69 中任一项所述的 UE，其特征在于，所述密钥更改模块，具体用于当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh，按照 Key Refresh 执行与所述主基站之间的安全密钥更改；

所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有无线承载 RB 的分组数据汇聚协议 PDCP 配置；

RLC 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的无线链路控制 RLC 配置；

MAC 保持模块，用于保持所述 UE 与所述次基站之间所建立的所有 RB 的媒体接入控制 MAC 配置；

激活保持模块，用于保持所述 UE 与所述次基站之间的已激活的次小区 SCell 的激活状态；

C-RNTI 保持模块，用于保持所述 UE 与所述次基站之间通信使用的小区无线网络临时标识符 C-RNTI；

第一传输控制模块，用于保持或暂停所述 UE 与所述次基站之间的数据传输。

71、根据权利要求 70 所述的 UE，其特征在于，所述密钥更改模块，包括：

第一中间密钥更新子模块，用于基于密钥更改命令消息中指示的下一跳链接计数 Next Hop Chaining Count 的值，使用当前的与所述主基站对应的 UE 侧

中间密钥或者下一跳 NH 更新与所述主基站对应的 UE 侧中间密钥;

第一密钥更改子模块，用于使用更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括: 所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

72、根据权利要求 71 所述的 UE，其特征在于，所述决策模块，还用于根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之前，确定所述按照 Key Refresh 执行与所述主基站之间的安全密钥更改是基于当前的与所述主基站对应的 UE 侧中间密钥进行的。

73、根据权利要求 71 所述的 UE，其特征在于，所述密钥更改模块，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Refresh。

74、根据权利要求 56 至 69 种任一项所述的 UE，其特征在于，所述密钥更改模块，具体用于当所述第一基站为所述主基站时，若所述 UE 根据所述密钥更改命令消息确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key，按照 Key Re-key 执行与所述主基站之间的安全密钥更改;

所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块:

PDCP 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 PDCP 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 PDCP 配置;

RLC 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 RLC 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 RLC 配置;

MAC 重置模块，用于重置所述 UE 与所述主基站之间所建立的所有 RB 的 MAC 配置; 重置所述 UE 与所述次基站之间所建立的所有 RB 的 MAC 配置;

第二传输控制模块，用于停止所述 UE 与所述主基站之间的数据传输; 停

止所述 UE 与所述次基站之间的数据传输。

75、根据权利要求 74 所述的 UE，其特征在于，所述密钥更改模块，包括：

第二中间密钥更新子模块，用于基于更新后的接入层管理实体 ASME 中间密钥更新与所述主基站之间的 UE 侧中间密钥；

第一密钥更改子模块，用于根据更新后的与所述主基站对应的 UE 侧中间密钥和所述主基站的安全算法生成新的与所述主基站对应的安全密钥，所述新的与所述主基站对应的安全密钥包括：所述 UE 与所述主基站通信时使用的加密密钥和完整性保护密钥。

76、根据权利要求 75 所述的 UE，其特征在于，所述密钥更改模块，还包括：

所述第三中间密钥更新子模块，还用于所述第二中间密钥更新子模块基于接入层管理实体 ASME 中间密钥更新与所述主基站对应的 UE 侧中间密钥之后，根据更新后的主基站侧中间密钥、所述次基站的与安全密钥更改相关联的小区信息或与安全密钥更改相关联的基站信息更新与所述次基站对应的 UE 侧中间密钥；

第二密钥更改子模块，用于根据更新后的与所述次基站对应的 UE 侧中间密钥和所述次基站的安全算法生成新的与所述次基站对应的安全密钥，所述新的与所述次基站对应的安全密钥包括：所述 UE 与所述次基站通信时使用的加密密钥。

77、根据权利要求 74 所述的 UE，其特征在于，所述密钥更改模块，具体用于根据所述密钥更改命令消息中携带的第一指示信息或第一安全密钥上下文信息或安全上下文信息，确定所述主基站与所述 UE 之间执行安全密钥更改的方式为 Key Re-key。

78、根据权利要求 56 至 69 中任一项所述的 UE，其特征在于，若所述密钥更改命令消息携带指示所述 UE 保持与所述第二基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 PDCP 配置，当所述第二基站为所述主基站时，所述第一基站为所述次基站，

当所述第二基站为所述次基站时，所述第二基站为所述主基站;

RLC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 RLC 配置;

MAC 保持模块，用于保持所述 UE 与所述第二基站之间所建立的所有 RB 的 MAC 配置;

激活保持模块，用于保持所述 UE 与所述第二基站之间的已激活的 SCell 的激活状态;

C-RNTI 保持模块，用于保持所述 UE 与所述第二基站之间通信使用的 C-RNTI;

传输保持模块，用于保持所述 UE 与所述第二基站之间的数据传输。

79、根据权利要求 56 至 69 中任一项所述的 UE，其特征在于，若所述密钥更改命令消息携带指示所述 UE 暂停与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间的数据传输之后，所述 UE，还包括如下模块中的至少一个模块:

PDCP 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置;

RLC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置;

MAC 保持模块，用于保持所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置;

激活保持模块，用于保持所述 UE 与所述第一基站之间的已激活的 SCell 的激活状态;

C-RNTI 保持模块，用于保持所述 UE 与所述第一基站之间通信使用的 C-RNTI;

传输暂停模块，用于暂停所述 UE 与所述第一基站之间的数据传输。

80、根据权利要求 56 至 69 中任一项所述的 UE，其特征在于，若所述密钥更改命令消息携带指示所述 UE 停止与所述第一基站之间的数据传输，所述决策模块根据所述密钥更改命令消息，确定是否保持与所述主基站或所述次基站之间的接入层配置信息，和/或，是否保持与所述主基站或所述次基站之间

的数据传输之后，所述 UE，还包括如下模块中的至少一个模块：

PDCP 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 PDCP 配置；

RLC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 RLC 配置；

MAC 重置模块，用于重置所述 UE 与所述第一基站之间所建立的所有 RB 的 MAC 配置；

传输停止模块，用于停止所述 UE 与所述第一基站之间的数据传输。

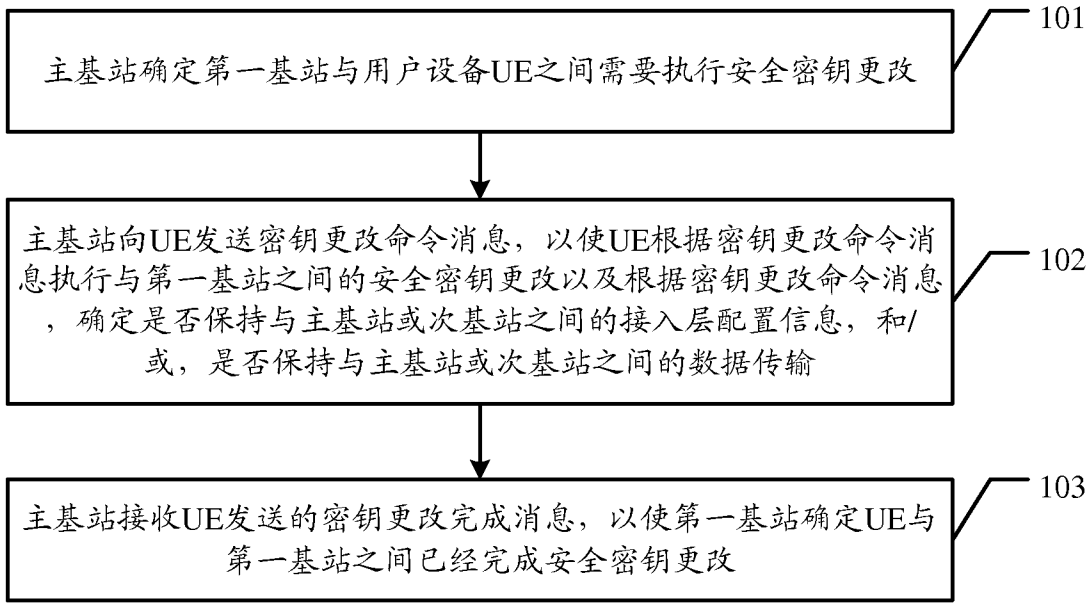
主基站确定第一基站与用户设备UE之间需要执行安全密钥更改
101
主基站向UE发送密钥更改命令消息，以使UE根据密钥更改命令消息执行与第一基站之间的安全密钥更改以及根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输
102
主基站接收UE发送的密钥更改完成消息，以使第一基站确定UE与第一基站之间已经完成安全密钥更改
103

图 1

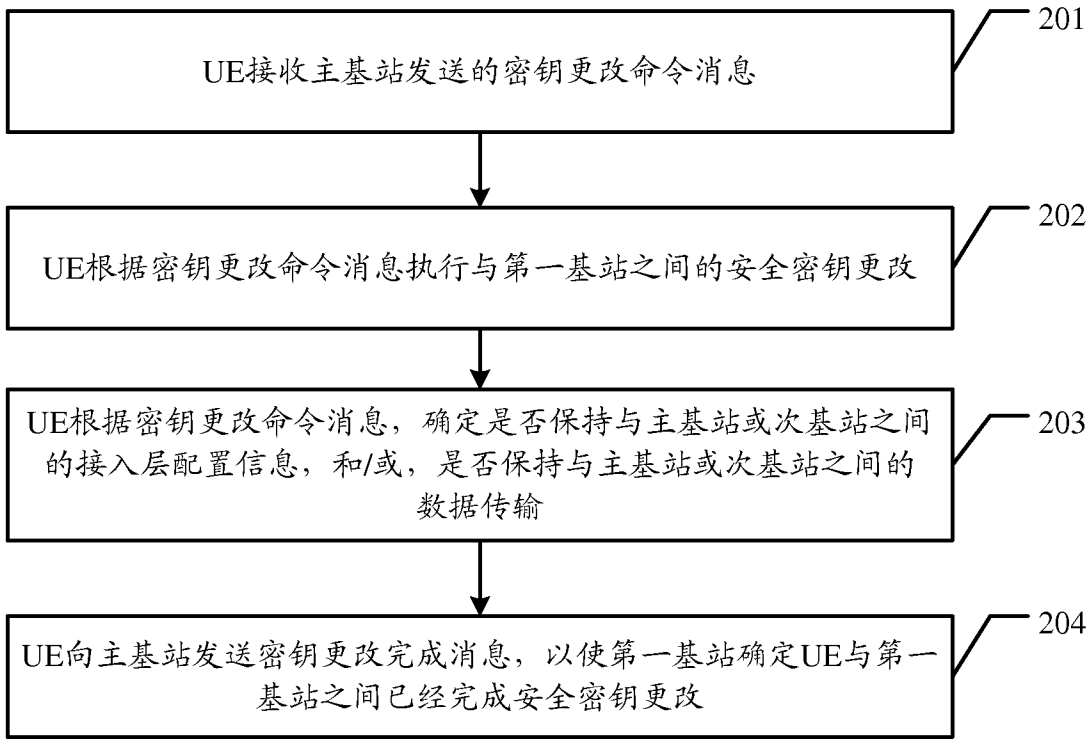
UE接收主基站发送的密钥更改命令消息
201
UE根据密钥更改命令消息执行与第一基站之间的安全密钥更改
202
UE根据密钥更改命令消息，确定是否保持与主基站或次基站之间的接入层配置信息，和/或，是否保持与主基站或次基站之间的数据传输
203
UE向主基站发送密钥更改完成消息，以使第一基站确定UE与第一基站之间已经完成安全密钥更改
204

图 2

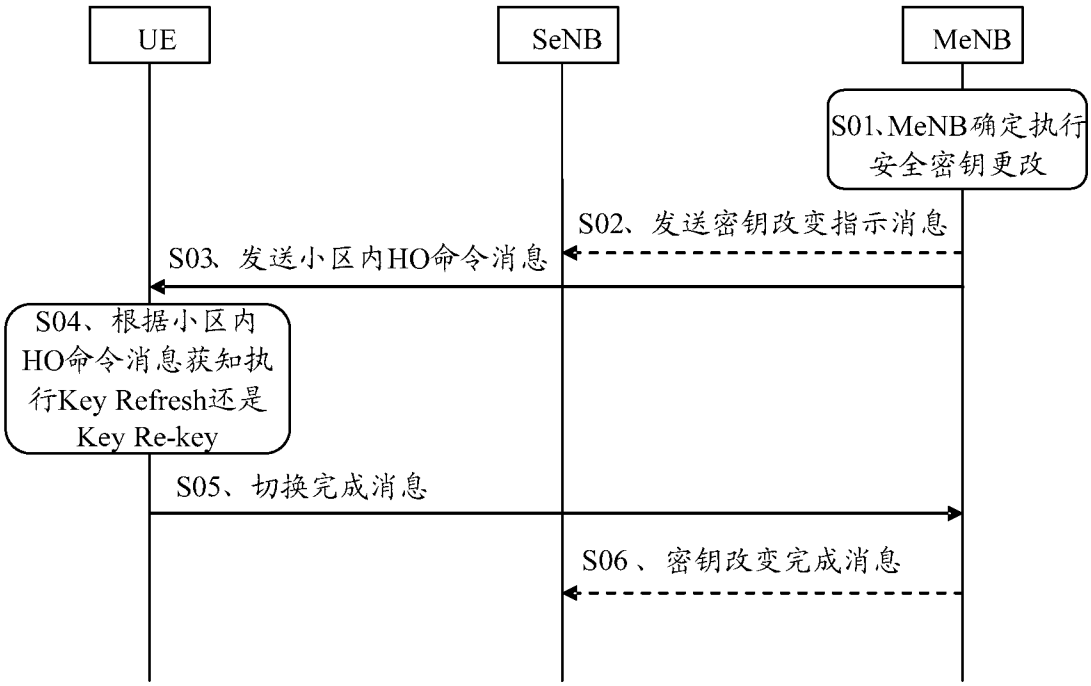
UE
SeNB
MeNB
S01、MeNB确定执行安全密钥更改
S02、发送密钥改变指示消息
S03、发送小区内HO命令消息
S04、根据小区内HO命令消息获知执行Key Refresh还是Key Re-key
S05、切换完成消息
S06、密钥改变完成消息

图 3-a

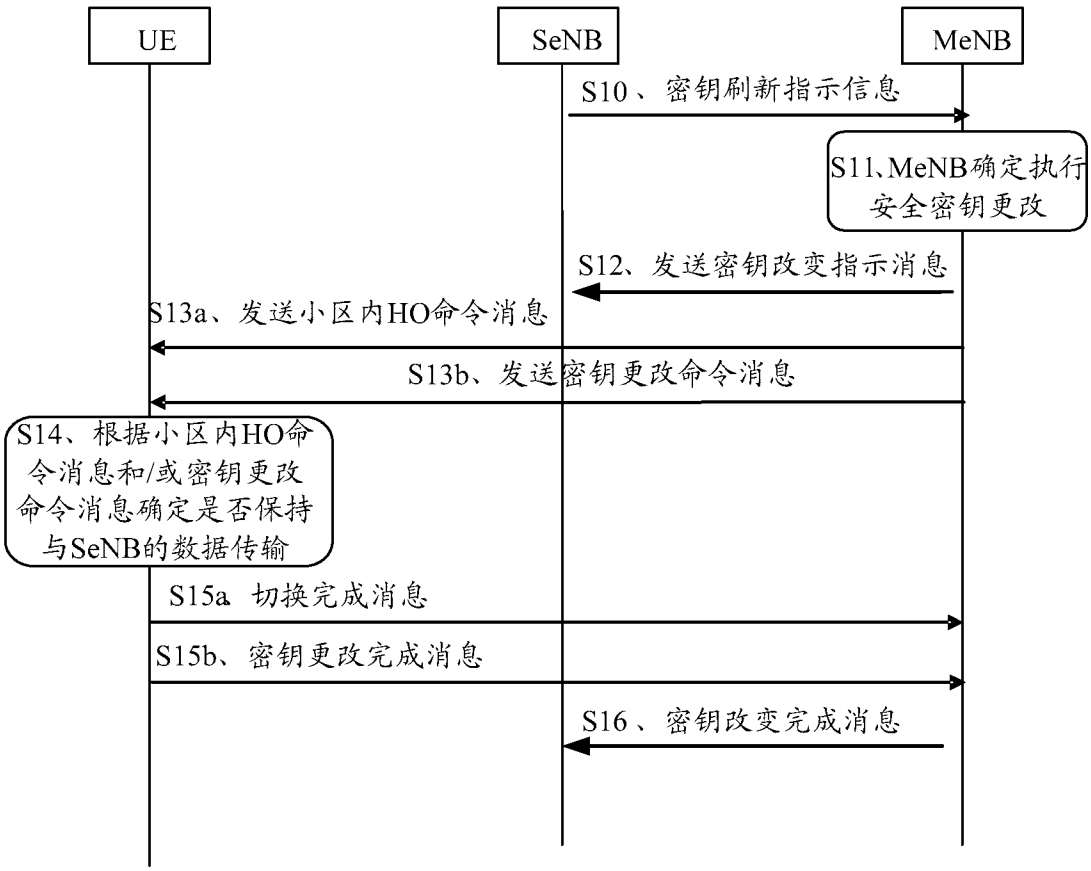
UE
SeNB
MeNB
S10、密钥刷新指示信息
S11、MeNB确定执行安全密钥更改
S12、发送密钥改变指示消息
S13a、发送小区内HO命令消息
S13b、发送密钥更改命令消息
S14、根据小区内HO命令消息和/或密钥更改命令消息确定是否保持与SeNB的数据传输
S15a 切换完成消息
S15b、密钥更改完成消息
S16、密钥改变完成消息

图 3-b

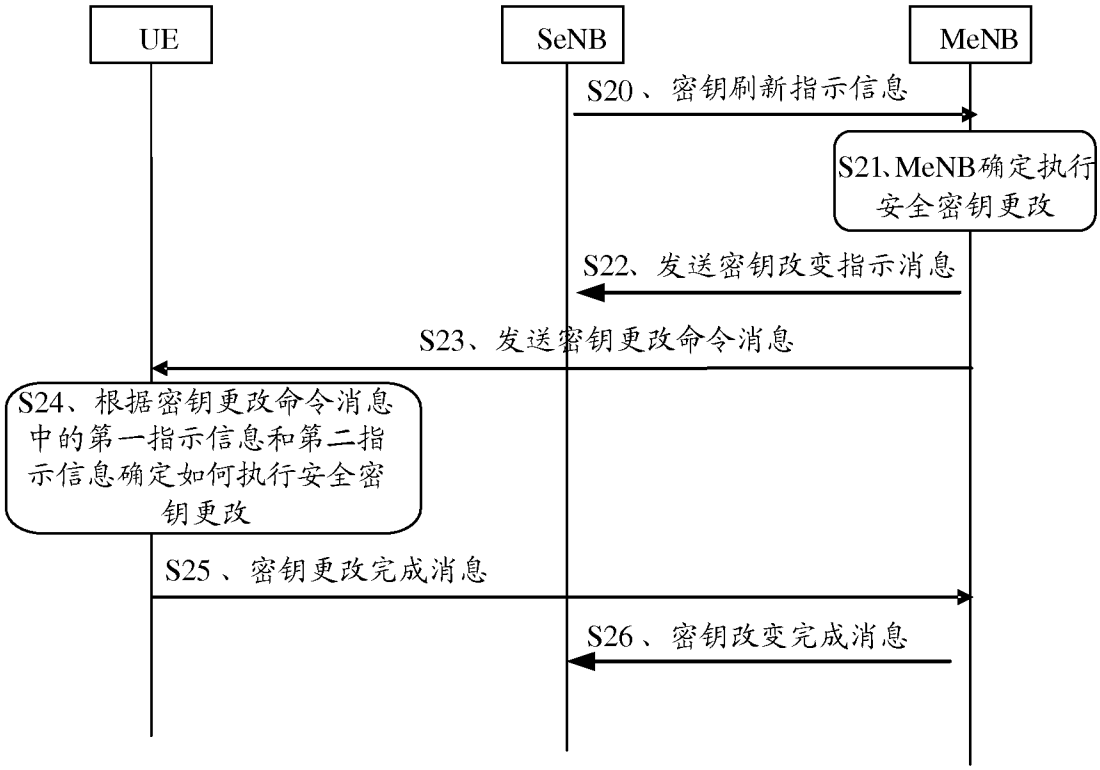
UE
SeNB
MeNB
S20、密钥刷新指示信息
S21、MeNB确定执行安全密钥更改
S22、发送密钥改变指示消息
S23、发送密钥更改命令消息
S24、根据密钥更改命令消息中的第一指示信息和第二指示信息确定如何执行安全密钥更改
S25、密钥更改完成消息
S26、密钥改变完成消息

图 3-c

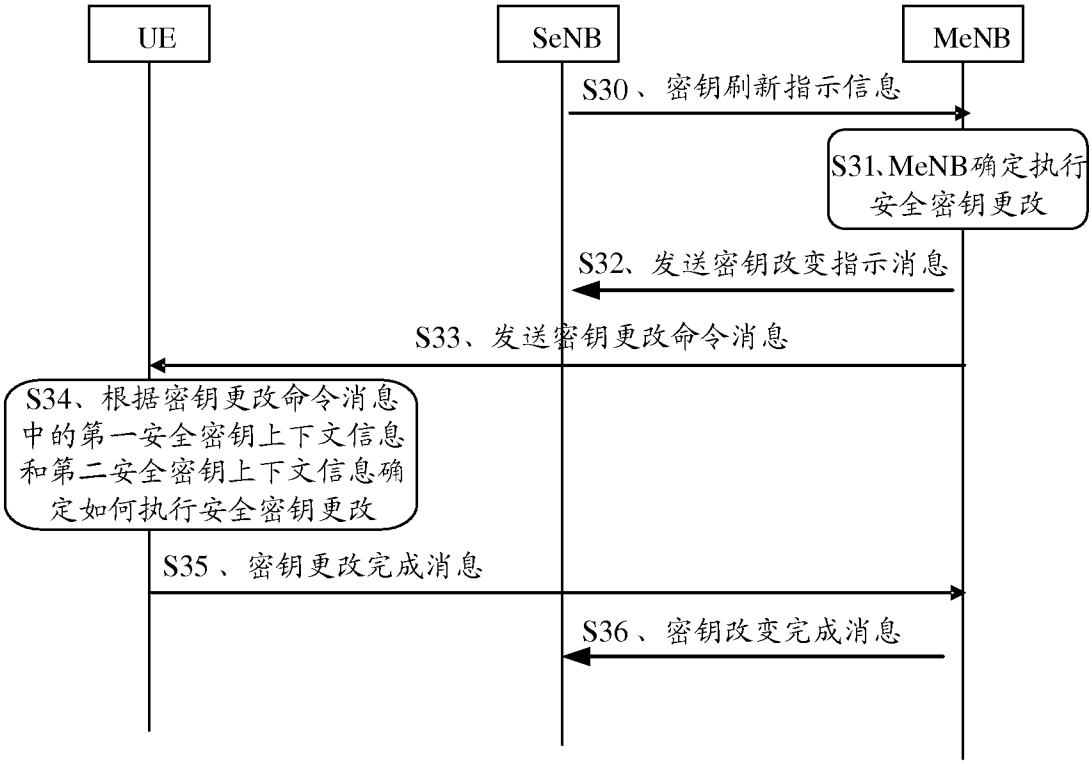
UE
SeNB
MeNB
S30、密钥刷新指示信息
S31、MeNB确定执行安全密钥更改
S32、发送密钥改变指示消息
S33、发送密钥更改命令消息
S34、根据密钥更改命令消息中的第一安全密钥上下文信息和第二安全密钥上下文信息确定如何执行安全密钥更改
S35、密钥更改完成消息
S36、密钥改变完成消息

图 3-d

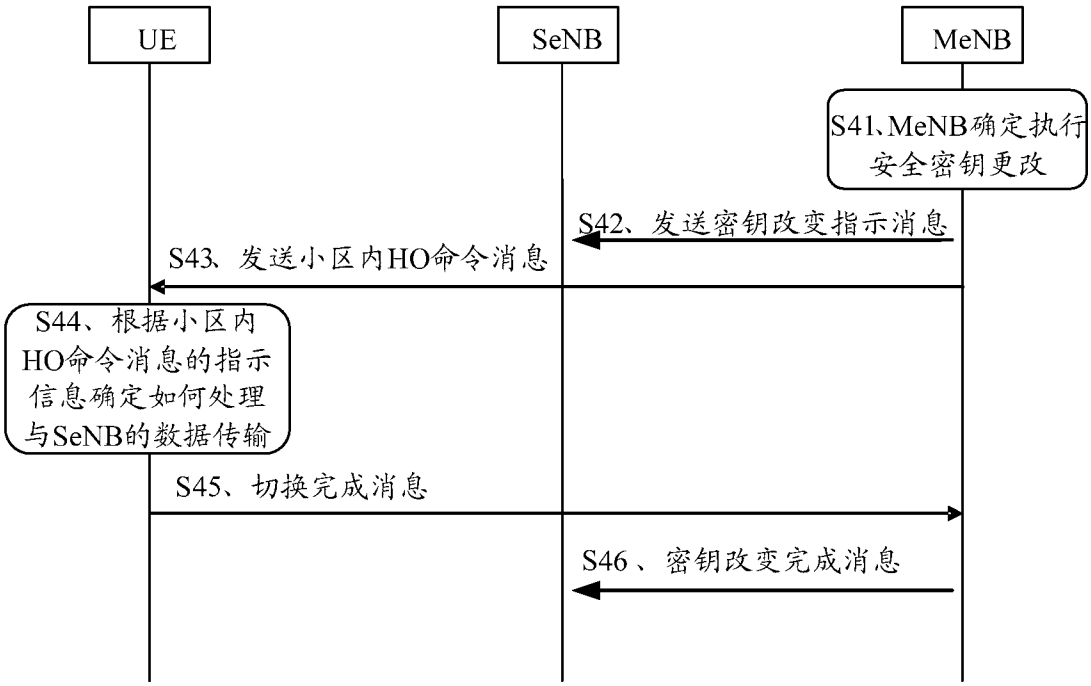
UE
SeNB
MeNB
S41、MeNB确定执行安全密钥更改
S42、发送密钥改变指示消息
S43、发送小区内HO命令消息
S44、根据小区内HO命令消息的指示信息确定如何处理与SeNB的数据传输
S45、切换完成消息
S46、密钥改变完成消息

图 3-e

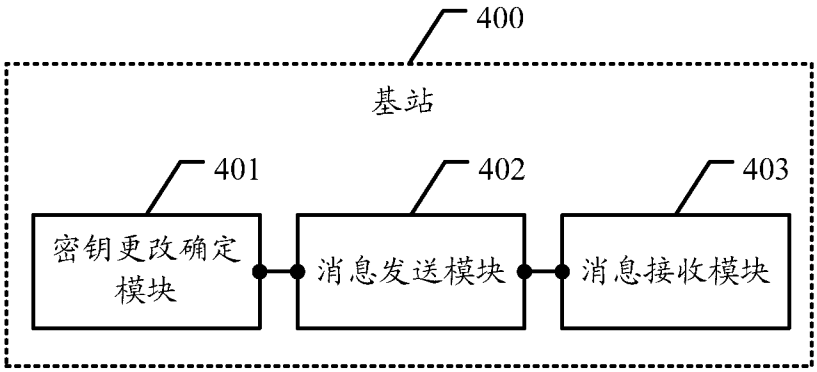
400
基站
401
密钥更改确定模块
402
消息发送模块
403
消息接收模块

图 4-a

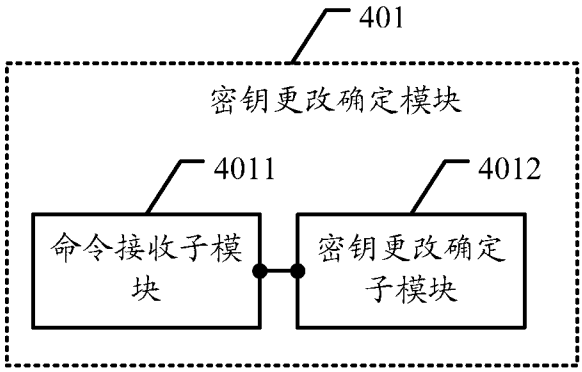
401
密钥更改确定模块
4011
命令接收子模块
4012
密钥更改确定子模块

图 4-b

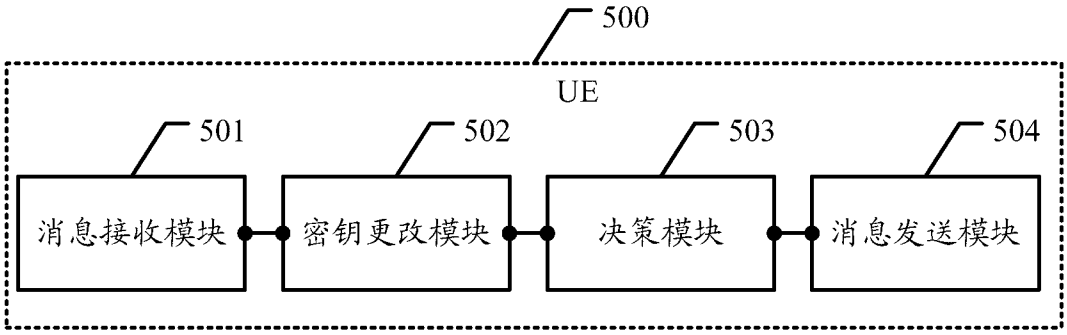
500
UE
501
502
503
504
消息接收模块
密钥更改模块
决策模块
消息发送模块

图 5-a

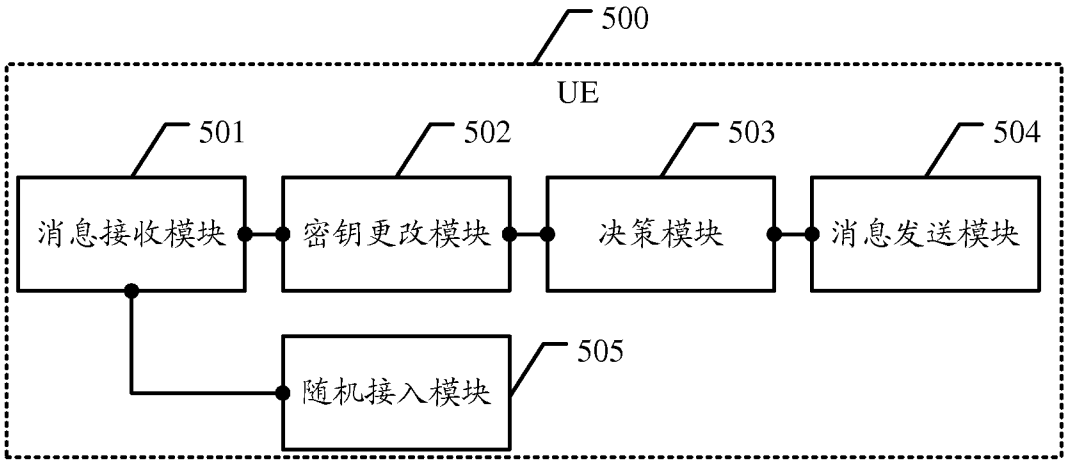
500
UE
501
502
503
504
消息接收模块
密钥更改模块
决策模块
消息发送模块
505
随机接入模块

图 5-b

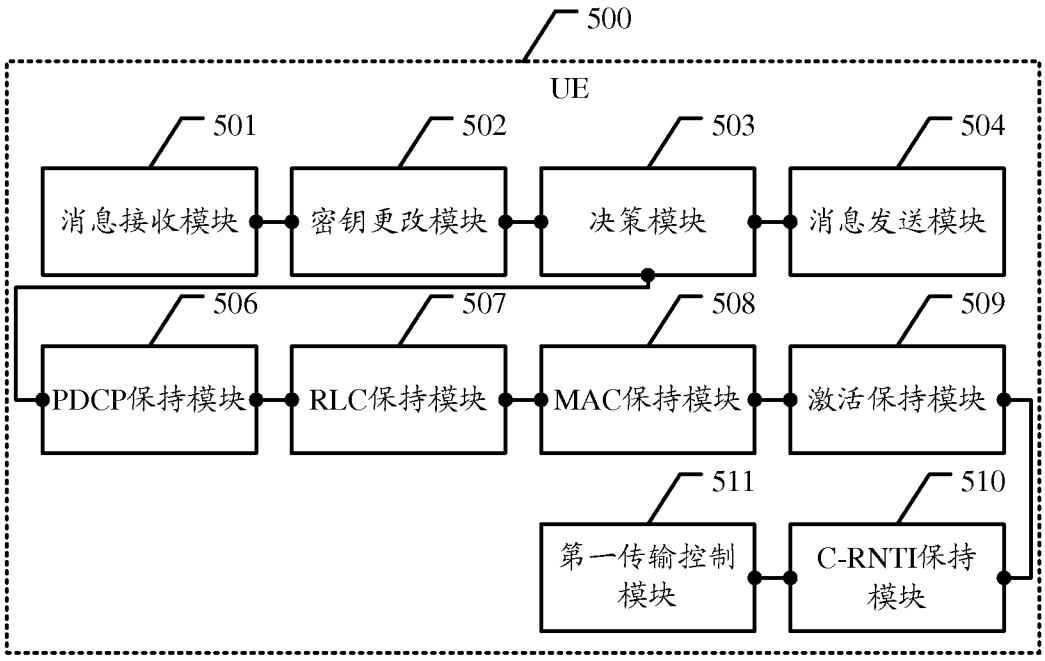
500
UE
501
502
503
504
消息接收模块
密钥更改模块
决策模块
消息发送模块
506
507
508
509
PDCP保持模块
RLC保持模块
MAC保持模块
激活保持模块
511
510
第一传输控制模块
C-RNTI保持模块

图 5-c

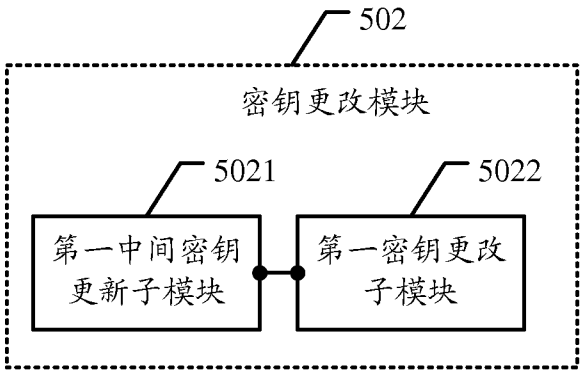
502
密钥更改模块
5021
5022
第一中间密钥更新子模块
第一密钥更改子模块

图 5-d

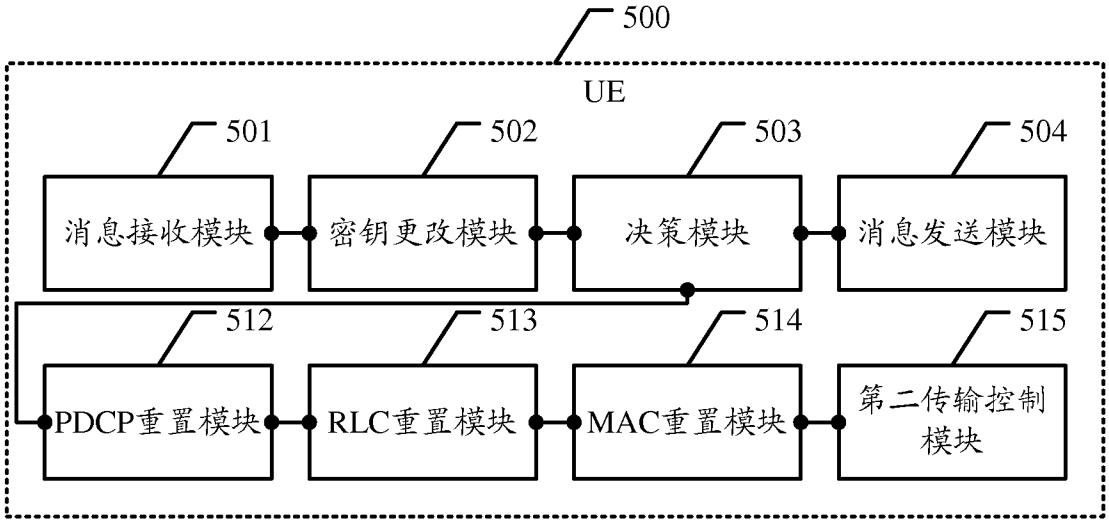
500
UE
501
502
503
504
消息接收模块
密钥更改模块
决策模块
消息发送模块
512
513
514
515
PDCP重置模块
RLC重置模块
MAC重置模块
第二传输控制模块

图 5-e

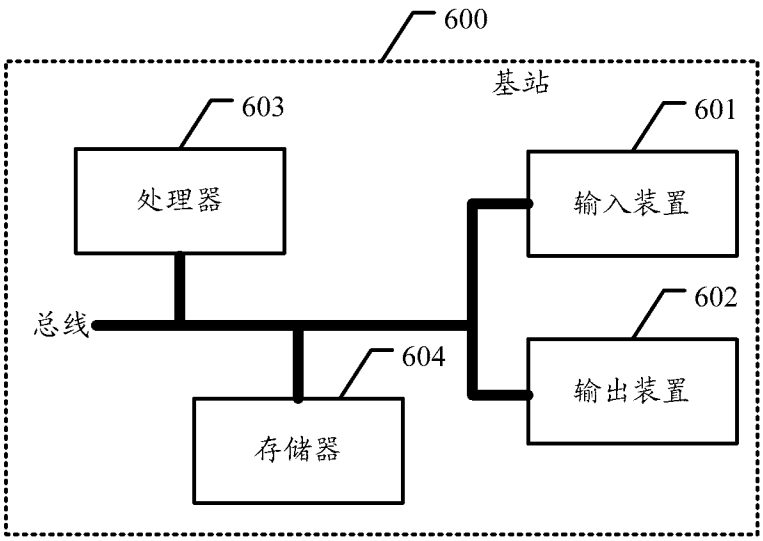
600
基站
603
601
处理器
输入装置
602
总线
604
输出装置
存储器

图 6

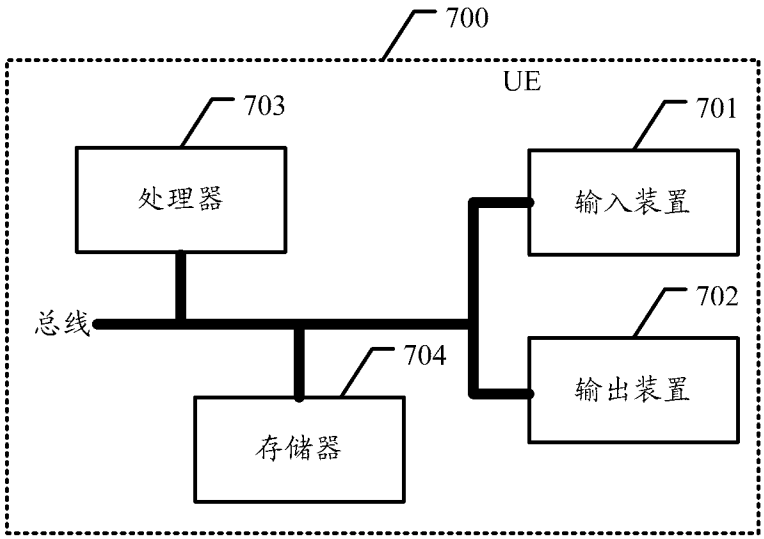

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/071675

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L; H04W; G06F

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)

CPRSABS; DWPI: nodeB, base station, Menb, key, NB, chang+, modify, main base station, macro base station, update

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101047978 A (HUAWEI TECHNOLOGIES CO., LTD.), 03 October 2007 (03.10.2007), the whole document	1-80
A	CN 102440019 A (ALCATEL-LUCENT USA, INC.), 02 May 2012 (02.05.2012), the whole document	1-80
A	CN 1937837 A (HUAWEI TECHNOLOGIES CO., LTD.), 28 March 2007 (28.03.2007), the whole document	1-80
A	CN 102740289 A (ACADEMY OF TELECOMMUNICATION TECHNOLOGY), 17 October 2012 (17.10.2012), the whole document	1-80

☐ 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 September 2014 (21.09.2014)	**29 September 2014 (29.09.2014)**
Name and mailing address of the ISA/CN: 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 **LI, Qi** Telephone No.: (86-10) **62412015**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/071675

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101047978 A	03 October 2007	None	
CN 102440019 A	02 May 2012	KR 101277101 B1	20 June 2013
		US 2009280774 A1	12 November 2009
		EP 2286611 A1	23 February 2011
		US 8666077 B2	04 March 2014
		WO 2009136981 A1	12 November 2009
		JP 2011523264 A	04 August 2011
		KR 20110002076 A	06 January 2011
		IN 20100702 P4	22 July 2011
CN 1937837 A	28 March 2007	None	
CN 102740289 A	17 October 2012	WO 2013185579 A1	19 December 2013

国际检索报告

PCT/CN2014/071675

A. 主题的分类

H04L 29/06(2006.01) 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)

H04L; H04W; G06F

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））

CPRSABS;DWPI:nodeB，basestation，Menb，basestation，key，NB，chang+，更改，修改，主基站，变更，基站，密钥，宏基站，更新，变化，改变

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
A	CN 101047978 A（华为技术有限公司）2007年 10月 03日（2007 - 10 - 03） 全文	1-80
A	CN 102440019 A（阿尔卡特朗讯美国公司）2012年 5月 02日（2012 - 05 - 02） 全文	1-80
A	CN 1937837 A（华为技术有限公司）2007年 3月 28日（2007 - 03 - 28） 全文	1-80
A	CN 102740289 A（电信科学技术研究院）2012年 10月 17日（2012 - 10 - 17） 全文	1-80

☐ 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
2014年 9月 21日	2014年 9月 29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) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	李祁 电话号码 (86-10)62412015

表 PCT/ISA/210（第2页）（2009年7月）

国际检索报告

关于同族专利的信息

PCT/CN2014/071675

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	101047978	A	2007年 10月 03日	无			
CN	102440019	A	2012年 5月 02日	KR	101277101	B1	2013年 6月 20日
				US	2009280774	A1	2009年 11月 12日
				EP	2286611	A1	2011年 2月 23日
				US	8666077	B2	2014年 3月 04日
				WO	2009136981	A1	2009年 11月 12日
				JP	2011523264	A	2011年 8月 04日
				KR	20110002076	A	2011年 1月 06日
				IN	20100702	P4	2011年 7月 22日
CN	1937837	A	2007年 3月 28日	无			
CN	102740289	A	2012年 10月 17日	WO	2013185579	A1	2013年 12月 19日