

## (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 9 月 17 日 (17.09.2015) WIPO | PCT

(10) 国际公布号

WO 2015/135292 A1

(51) 国际专利分类号:

H04W 12/04 (2009.01)

(21) 国际申请号:

PCT/CN2014/084808

(22) 国际申请日:

2014 年 8 月 20 日 (20.08.2014)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201410096468.5 2014 年 3 月 14 日 (14.03.2014) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 李阳 (LI, Yang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 林兆骥 (LIN, Zhaoji); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 游世林 (YOU, Shilin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司  
(CHINA PAT INTELLECTUAL PROPERTY OF-

(FICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

## 本国国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: KEY UPDATE METHOD, SUB BASE STATION, TERMINAL, COMMUNICATION SYSTEM AND STORAGE MEDIUM

(54) 发明名称: 密钥更新方法、从基站、终端、通信系统和存储介质



图 1 / FIG. 1

(57) Abstract: The present invention relates to the field of communications. Disclosed are a sub base station key update method, sub base station, terminal and communication system. The sub base station key update method comprises: deriving a new sub base station key according to the current sub base station key and an inside sub base station counter (ISC), the ISC being a count value for deriving the sub base station key (S110). Also disclosed in the present invention is a computer storage medium.

(57) 摘要: 本发明公开了一种从基站密钥更新方法、从基站、终端及通信系统, 涉及通信领域。所述从基站密钥更新方法包括: 依据当前从基站密钥以及内部从基站计数器 (ISC) 推导新的从基站密钥 (S110); 其中, 所述 ISC 为推导从基站密钥的计数值。本发明还同时公开了一种计算机存储介质。

# 密钥更新方法、从基站、终端、通信系统和存储介质

## 技术领域

本发明涉及通信领域的信息安全技术，尤其涉及一种密钥更新方法、从基站、终端、通信系统和存储介质。

## 5    背景技术

长期演进（Long Term Evolution，简称 LTE）网络，由演进全球陆地无线接入网（Evolved Universal Terrestrial Radio Access Network，简称 E-UTRAN）和演进分组交换中心（Evolved Packet Core，简称 EPC）组成，且网络结构呈现扁平化。

10      所述 EUTRAN 通过 S1 接口与 EPC 相连。所述 EUTRAN 由多个相互连接的演进基站（Evolved NodeB，简称 eNB）组成，各个 eNB 之间通过 X2 接口连接。

所述 EPC 由移动性管理实体（Mobility Management Entity，简称 MME）和服务网关实体（Serving Gateway，简称 S-GW）组成。

15      在所述长期演进网络的系统架构中还有一个归属环境（Home Environment，HE）即归属用户服务器（Home Subscriber Server，HSS）或归属位置寄存器（Home Location Register，HLR），作为用户数据库。它包含用户配置文件，执行用户的身份验证和授权，并可提供有关用户物理位置的信息等。

20      为了满足日益增长的大带宽高速移动接入的需求，第三代伙伴组织计划（Third Generation Partnership Projects，简称 3GPP）推出高级长期演进（Long-Term Evolution advance，简称 LTE-Advanced）标准。LTE-Advanced 对于长期演进（Long-Term Evolution，简称 LTE）系统的演进保留了 LTE

的核心，在此基础上采用一系列技术对频域、空域进行扩充，以达到提高频谱利用率、增加系统容量等目的。在某些应用场景下，会使用到小小区（Small Cell，简称 SC）增强技术，用来提高用户的吞吐量。

SC 增强技术的主要实现方式就是双连接（dual connectivity），如图 1  
5 所示。一个用户设备(UE)同时连接两个小区，一个是主小区（Macro Cell），一个是从小区（Small cell）。主小区所在的基站被称为主基站（Macro eNodeB，简称 MeNB），从小区所在的基站被称为从基站（small eNodeB，or secondary eNodeB，简称 SeNB）。UE 与基站之间的信令面功能通过主基站来完成，用户面通过 UE 与主基站和从基站共同完成，即 UE 既与主基站  
10 有用户面连接，也与从基站有用户面连接，简称双连接。

双连接的主要技术就是主基站与从基站之间的用户名协议栈功能的分配问题，目前有几种备选的方案，主要的一种就是图 2 所示的方案。该方案中，主基站的用户名和控制面都保持不变，从基站的用户名协议栈包括从 PDCP 层到 PHY 层所有层。从基站直接与 S-GW 连接，之间的接口 S1-U  
15 与之前的完全相同。UE 被转移的 DRB，在空口上，UE 直接与从基站相连，来传递被转移的 DRB。

UE 与 MeNB 之间的空口安全所使用的密钥由 UE 与 CN 之间的 AKA  
过程产生，即 KeNB。而 SeNB 由 MeNB 选择，此过程并不与 CN 交互，所以 UE 与 SeNB 之间的空口安全所使用的密钥（简称 S-KeNB）不能由 CN  
20 来产生。MeNB 向 SeNB 首次转移 DRB 时，SeNB 所使用的密钥由 MeNB 推导，基于 M-KeNB 和 MeNB 内部计数器 SCC 产生；然后由 MeNB 传递给 SeNB。如果后续 MeNB 向其他的 SeNB 转移该 UE 的 DRB 时，MeNB 仍基于 M-KeNB 和 SCC 产生，然后发给新的 SeNB。MeNB 每推导一次 S-KeNB，SCC 增加 1。而在 MeNB 多次向同一个 SeNB 转移 DRB 时，S-KeNB  
25 如何更新都是待解决的问题。

## 发明内容

有鉴于此，本发明实施例期望提供一种从基站密钥更新方法、从基站、终端、通信系统和计算机存储介质，简化从基站密钥更新方法，提高从基站与终端之间的信息安全性。

5 为达到上述目的，本发明实施例的技术方案是这样实现的：

本发明实施例第一方面提供一种从基站密钥更新方法，所述方法包括：

依据当前从基站密钥以及 ISC 推导新的从基站密钥；

其中，所述 ISC 为推导从基站密钥的计数值。

基于上述方案，在所述从基站密钥以及 ISC 推导新的从基站密钥之后，

10 所述方法还包括：

向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

其中，所述 ISC 由所述主基站通过 RRC 重配置请求消息发送到终端；

所述 RRC 重配置请求消息用于指示终端依据所述 ISC 及当前从基站密

15 钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基  
站密钥建立与所述从基站的连接。

基于上述方案，在所述从基站依据当前从基站密钥以及 ISC 推导新的  
从基站密钥之前，所述方法还包括：

接收主基站发送的添加修改 DRB 请求消息；

判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

若否，则进入所述从基站依据当前从基站密钥以及 ISC 推导新的从基  
站密钥的步骤。

基于上述方案，

在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，

25 所述方法还包括：

依据密钥推导决策判断是否触发更新从基站密钥；

若是，则进入所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

基于上述方案；所述依据密钥推导决策判断是否触发更新从基站密钥

5 包括：

判断当前从基站密钥是失效；

若失效则触发更新的从基站密钥；或

判断从基站与终端的从基站密钥是否同步；

若不同步则触发更新的从基站密钥。

10 基于上述方案，所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥包括：

依据从基站密钥、ISC 及推导参数推导新的从基站密钥。

基于上述方案，

所述推导参数包括小区物理标识和/或小区载频；

15 所述小区为由所述从基站覆盖所形成的小区。

基于上述方案，在所述依据从基站密钥及 ISC 推导新的从基站密钥之后，所述方法包括：

更新所述 ISC。

本发明实施例第二方面提供一种从基站密钥更新方法，，所述方法包  
20 括：

接收主基站发送的 RRC 重配置请求消息；所述 RRC 重配置请求消息中包括 ISC；

根据所述 ISC 及当前从基站密钥推导新的从基站密钥；

根据所述 RRC 重配置请求消息和所述新的从基站密钥，与从基站建立

25 连接；

其中，所述 ISC 为推导从基站密钥的计数值。

本发明实施例第三方面提供一种从基站密钥更新方法，所述方法包括：

从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥；

从基站向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包

5 括所述 ISC；

主基站接收所述添加修改 DRB 命令消息；

主基站向终端发送 RRC 重配置请求消息；所述 RRC 重配置消息包含所述 ISC；

终端接收所述 RRC 重配置请求消息；

10 终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥；

终端依据所述 RRC 重配置消息及所述新的从基站密钥与从基站建立连接。

其中，所述 ISC 为推导从基站密钥的计数值。

基于上述方案，在所述从基站依据当前从基站密钥以及 ISC 推导新的

15 从基站密钥之前，所述方法还包括：

主基站发送添加修改 DRB 请求消息；

从基站接收所述添加修改 DRB 请求消息；

从基站依据判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

20 若否，则从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

基于上述方案，在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，所述方法还包括

从基站依据密钥推导决策判断是否触发更新从基站密钥；

25 若是，从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的

从基站密钥的步骤。

基于上述方案，所述从基站依据密钥推导决策判断是否触发更新从基站密钥包括：

从基站判断当前从基站密钥是失效；

5 若失效则从基站自行触发更新的从基站密钥；或

从基站判断从基站与终端的从基站密钥是否同步；

若不同步则从基站自行触发更新的从基站密钥。

基于上述方案，在所述从基站向主基站发送添加修改 DRB 命令消息之后，所述方法还包括：

10 从基站更新所述 ISC。

本发明实施例第四方面提供一种从基站，所述从基站包括：

第一推导单元，配置为依据当前从基站密钥以及 ISC 推导新的从基站密钥；

其中，所述 ISC 为推导从基站密钥的计数器的计数值。

15 基于上述方案，所述从基站还包括第一接收单元；

所述第一发送单元，配置为在所述从基站密钥以及 ISC 推导新的从基站密钥之后，向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

其中，所述 ISC 由所述主基站通过 RRC 重配置请求消息发送到终端；

20 所述 RRC 重配置请求消息用于指示终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与从基站的连接。

基于上述方案，所述从基站还包括第一接收单元及判断单元；

所述第一接收单元，配置为在所述从基站依据当前从基站密钥以及 ISC 25 推导新的从基站密钥之前，接收主基站发送的添加修改 DRB 请求消息；

所述判断单元，配置为判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

所述第一推导单元，配置为当添加修改 DRB 请求消息没有携带从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

5 基于上述方案，所述从基站还包括触发单元；

所述触发单元，配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，依据密钥推导决策判断是否触发更新从基站密钥；

所述第一推导单元，还配置为在所述触发单元触发更新的从基站密钥之后，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

10 基于上述方案，所述触发单元，配置为判断当前从基站密钥是失效及当所述从基站密钥失效时触发更新的从基站密钥；或判断从基站与终端的从基站密钥是否同步及当不同步时触发更新的从基站密钥。

基于上述方案，所述第一推导单元，配置为依据从基站密钥、ISC 及推导参数推导新的从基站密钥。

15 基于上述方案，

所述推导参数包括小区物理标识和/或小区载频；

所述小区为由所述从基站覆盖所形成的小区。

基于上述方案，所述从基站还包括计数器；

所述计数器，配置为在所述依据从基站密钥及 ISC 推导新的从基站密钥之后，更新所述 ISC。

本发明实施例第五方面提供一种终端，所述终端包括：

第二接收单元，配置为接收主基站发送的 RRC 重配置请求消息；

第二推导单元，配置为依据当前所述 ISC 及从基站密钥推导新的从基站密钥；

25 连接单元，配置为依据所述 RRC 重配置请求消息及所述新的从基站密

钥建立与从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

本发明实施例第六方面提供一种通信系统，所述通信系统包括：

从基站，配置为依据当前从基站密钥以及 ISC 推导新的从基站密钥；

5 向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

主基站，配置为接收所述添加修改 DRB 命令消息，提取所述 ISC；通

过 RRC 重配置请求消息向终端发送所述 ISC；

终端，配置为接收所述 RRC 重配置请求消息；依据所述 ISC 更新及从

基站密钥从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站

10 密钥建立与所述从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

基于上述方案，

所述主基站，还配置为在所述从基站依据当前从基站密钥以及 ISC 推

导新的从基站密钥之前发送添加修改 DRB 请求消息；

15 所述从基站，还配置为接收所述添加修改 DRB 请求消息；判断所述添

加修改 DRB 请求消息中是否有携带从基站密钥；且所述添加修改 DRB 请

求消息没有携带从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从

基站密钥。

基于上述方案，

20 所述从基站，还配置为在所述从基站依据当前从基站密钥以及 ISC 推

导新的从基站密钥之前依据密钥推导决策判断是否触发更新从基站密钥；

且当触发更新从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基

站密钥的步骤。

基于上述方案，所述从基站，配置为判断当前从基站密钥是否失效或判

25 断从基站与终端的从基站密钥是否同步；且当所述从基站密钥失效时自行

触发更新的从基站密钥或当不同时自行触发更新的从基站密钥。

基于上述方案，所述从基站，还配置为在所述从基站向主基站发送添加修改 DRB 命令消息之后，更新所述 ISC。

本发明实施例第六方面提供一种计算机存储介质，所述计算机存储介质中存储有计算机可执行指令，所述计算机可执行指令用于执行权利本发明实施例第一方面至第三方面所述方法的至少其中之一。

本发明实施例所述的从基站密钥更新方法、从基站、终端及通信系统，通过从基站自行推导从基站密钥，解决了主基站向同一从基站多次转移相关联的 DRB 中从基站密钥更新的方法，同时避免了从基站密钥在基站之间的传输带来的安全隐患，从而提升了通信安全。

### 附图说明

图 1 为本发明实施例一所述的从基站密钥更新方法的流程示意图之一；

图 2 为本发明实施例一所述的从基站密钥更新方法的流程示意图之二；

图 3 为本发明实施例二所述的从基站密钥更新方法的流程示意图；

图 4 为本发明实施例三所述的从基站密钥推导方法的示意图之一；

图 5 为本发明实施例三所述的从基站密钥推导方法的示意图之二；

图 6 为本发明实施例三所述的从基站密钥更新方法的流程示意图之一；

图 7 为本发明实施例三所述的从基站密钥更新方法的流程示意图之二；

图 8 为本发明实施例四所述的从基站的结构示意图之一；

图 9 为本发明实施例四所述的从基站的结构示意图之二；

图 10 为本发明实施例五所述的终端的结构示意图；

图 11 为本发明实施例六所述的通信系统的结构示意图之一；

图 12 为本发明实施例六所述的通信系统的结构示意图之二。

## 具体实施方式

以下结合附图对本发明的优选实施例进行详细说明，应当理解，以下所说明的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

### 实施例一：

5 本实施例提供一种从基站密钥更新方法，所述方法包括：

依据当前从基站密钥以及 ISC 推导新的从基站密钥；

其中，所述 ISC 为推导从基站密钥的计数值。

本实施例所述的从基站密钥更新方法，是由从基站根据其内部当前所存储的从基站密钥及 ISC 推导新的从基站密钥。所述新的从基站密钥与推导之前的所述当前从基站密钥不同；所述从基站密钥无需由主基站向从基站行发送；首先提供了一种全新的从基站密钥获取方法，其次从基站自行推导从基站密钥，从而避免了从基站密钥的传输导致的安全问题，从而提高了信息安全性。具体的密钥推导方法可以参见现有技术进行推导。

作为本实施例的进一步改进，如图 1 所示，所述方法还包括：

15 步骤 S110：依据当前从基站密钥以及 ISC 推导新的从基站密钥；

步骤 S120：向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

其中，所述 RRC 重配置请求消息用于指示终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与所述从基站的连接。

更新后的新的从基站密钥将用于从基站与终端的通信过程中，而此时从基站和终端之间还未建立连接，故需要由主基站转发到终端。同时为了保证从基站密钥安全；所述从基站密钥不能在基站与终端之间发送，但是终端的从基站功能模块需要和从基站内的从基站密钥保持同步，故还需将推导从基站密钥的 ISC 发送到终端，由终端根据所述 ISC 自行推导从基站

密钥。终端推导从基站密钥的方法与从基站推导从基站密钥的方法一致。

所述主基站通常为宏基站；所述从基站通常为小基站或家庭基站，同样也可以是普通宏基站。所述终端通常为双连接终端或多连接终端。

作为本实施例的进一步改进，如图 2 所示，所述方法还可包括以下步

骤：

步骤 S101：接收主基站发送的添加修改 DRB 请求消息；

步骤 S102：判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

若否，则执行步骤 S110 或执行步骤 S110 和步骤 S120。

此处，提供了一种由主基站通过添加修改 DRB 请求消息的方式触发从基站用于自行更新从基站密钥的方法。具体的应用场景包括在主基站多次向同一个从基站转移相关联的 DRB，且本次转移 DRB 为非首次转移 DRB 的情景。所述 DRB 为 date radio bearing 的缩写，可译为用户面无线承载数据。

此外，在某些场景下所述从基站还可以自发进行从基站密钥更新，在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，本实施例所述的方法还包括：

依据密钥推导决策判断是否触发更新从基站密钥；

若是，则进入所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

具体的所述依据密钥推导决策判断是否触发更新从基站密钥包括：

判断当前从基站密钥是失效或者判断从基站与终端的从基站密钥是否同步；若失效则触发更新的从基站密钥或若不同步则触发更新的从基站密钥。

在具体的执行过程中还包括从基站在数据解密出现故障时，需重新确

定从基站与终端所用的从基站密钥是否正确，同样的可由从基站自行触发更新从基站密钥，以顺利实现通信和数据解密。

上述改进，使得本实施例所述的方法还提供了从基站自发更新从基站密钥的步骤，进一步完善了从基站密钥更新方法。

5 以下提供步骤 S110 的具体操作，所述步骤 S110 包括：依据从基站密钥、ISC 及推导参数推导新的从基站密钥；其中，所述推导参数包括小区物理标识和/或小区载频；所述小区为由所述从基站覆盖所形成的小区。

作为本实施例的进一步改进，为了方便下次进行从基站密钥更新，在所述从基站将 ISC 通过添加修改 DRB 命令消息发送给主基站以后，所述从 10 基站还需要更新 ISC；通常 ISC 加 1；且通常所述 ISC 的取值从 0 开始。

综合上述，本实施例提供了一种从基站密钥更新方法，由从基站自行推导从基站密钥，避免了密钥的传输，同时解决了现有技术中从基站密钥出现的错误、基站与终端之间从基站密钥不同步以及主基站多次向同一从基站转移 DRB 时带来的问题。

## 15 实施例二

如图 3 所示，一种终端侧从基站密钥更新方法，所述方法包括：

步骤 S210：接收主基站发送的 RRC 重配置请求消息；所述 RRC 重配 20 置请求消息中包括 ISC

步骤 S220：依据所述 ISC 及从基站密钥推导新的从基站密钥；

步骤 S230：依据所述 RRC 重配置请求消息及所述新的从基站密钥，建 25 立与从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

所述 RRC 重配置请求消息中除了所述 ISC 以外，还包括用于建立连接的配置参数。所述步骤 S230 中，终端依据所述配置消息及所述新的从基站密钥，建立与从基站的连接。

本实施例所述的终端根据

主基站所发送的 RRC 重配置请求消息中所携带的 ISC 参数及当前从基站密钥推导新的从基站密钥，并根据所述 RRC 重配置请求消息及所述新的从基站密钥建立与从基站之间的连接，改变了终端获取从基站密钥的方法，  
5 此方法同样的有利于用来解决现有技术中从基站密钥出现的错误、基站与终端之间从基站密钥不同步以及主基站多次向同一从基站转移 DRB 时带来的问题。

实施例三：

本实施例提供一种从基站密钥更新方法，所述方法包括：

10 从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥；

从基站向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

主基站接收所述添加修改 DRB 命令消息，提取所述 ISC；

主基站通过 RRC 重配置请求消息向终端发送所述 ISC，

15 终端接收所述 RRC 重配置请求消息；

终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥；

终端依据所述 RRC 重配置请求消息及所述新的从基站密钥，建立与所述从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

如图 4 所示，所述从基站推导从基站新的从基站密钥的方法；当主基站首次向从基站 SeNB 转移 DRB 时，则由主基站生成密钥 KeNB，并发送给从基站 SeNB 作为第一个从基站密钥 S-KeNB，且此时推导从基站密钥推导的计数值 ISC 为 0。本实施例中的所述主基站可为宏基站 MeNB。宏基站继续向从基站 SeNB 转移 DRB，且此时所述 DRB 与上次转移的 DRB 之间  
25 存在上下文等关系时，后续从基站将自行推导根据当前从基站密钥 S-KeNB

与 ISC 推导新的从基站密钥。所述密钥 KeNB 为主基站根据主基站内部存储的主基站密钥 M-KeNB 及推导计数值 SCC 推导的。主基站每推导一次密钥 KeNB 则所述 SCC 计数值加 1，且通常所述 SCC 的取值从 0 开始。在具体的实现过程中所述从基站内设有内部计数器 Intra Smallcell Counter，用于 5 计数形成所述 ISC；所述主基站内部设有计数器，用于计数形成所述 SCC。

为了实现从基站和终端内从基站密钥的同步，在本实施例中所述从基站将通过添加修改 DRB 命令消息将所述 ISC 发送到主基站，主基站在进行提取和存储备份后，通过 RRC 重配置请求消息将所述 ISC 发送到终端；终端将根据当前从基站密钥及接收到的所述 RRC 重配置请求消息中的 ISC 推 10 导新的从基站密钥，推导过程与从基站推导从基站密钥相似。

图 5 所示的为从基站 SeNB 及终端 UE 用于根据从基站密钥及 ISC 推导新的从基站密钥的方法。其中，所述 KDF 为 Key Deviation Function 的缩写；在具体的实现过程中推导新的从基站密钥的依据，除原先存储的从基站密钥及 ISC 以外还可包括其他推导参数，如小区物理标识或小区载频等信息； 15 所述小区为所述从基站所覆盖形成的小区。

作为本实施例的进一步改进，本实施例所述方法在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前还包括：

主基站发送添加修改 DRB 请求消息；

20 从基站接收所述添加修改 DRB 请求消息；

从基站判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

若否，则从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

故本实施例所述的方法，具体的实现可如图 6 所示，包括以下步骤：

25 步骤 S1.1：终端 UE 与主基站 MeNB 之间完成了 RRC 连接建立； RRC 为： Radio Resource Control 无线资源控制；

步骤 S1.2: 主基站 MeNB 向从基站 SeNB 发送添加修改 DRB 请求消息; 从基站接收所述添加修改 DRB 请求消息;

步骤 S1.3: 从基站依据所述添加修改 DRB 请求消息, 判断所述添加修改 DRB 请求消息中是否有携带从基站密钥; 若否则从基站执行所述从基站  
5 依据当前从基站密钥以及 ISC 推导新的从基站密钥;

步骤 S1.4: 从基站向主基站发送添加修改 DRB 命令消息; 所述 DRB 命令消息中包括由 ISC; 在具体的实现过程中还会包括其他的参数, 具体的可参见现有技术;

步骤 S1.5: 主基站接收所述添加修改 DRB 命令消息, 并向从基站发送  
10 RRC 重配置请求消息; 所述 RRC 重配置请求消息中包括所述 ISC;

步骤 S1.6: 终端 UE 接收所述 RRC 重配置请求消息, 依据所述 ISC 及当前从基站密钥推导新的从基站密钥; 并依据所述 RRC 重配置请求消息及新的从基站密钥建立与从基站的连接;

为了通知主基站及从基站已经完成了从基站密钥的更新, 作为本实施  
15 例的进一步改进, 所述方法还包括:

步骤 S1.7: 终端向主基站发送 RRC 重配置响应消息; 所述从 RRC 重配置响应消息包括了终端更新从基站密钥的相关信息;

步骤 S1.8: 主基站在接收到所述 RRC 重配置响应消息之后, 将根据所述 RRC 重配置响应消息向从基站发送 SeNB 状态传输信息。

本实施例上述改进是从基站基于主基站的请求消息触发更新从基站密钥, 适用于解决现有问题中主基站向同一基站多次转达相关联的 DRB 时从基站密钥生成的问题。以下提供一种从基站根据自身需要, 自发更新从基站密钥的方法操作如下:

在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前,  
25 所述方法还包括

从基站依据密钥推导决策判断是否触发更新从基站密钥；

若是，从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

优选地，所述从基站依据密钥推导决策判断是否触发更新从基站密钥

5 包括：

从基站判断当前从基站密钥是失效；

若失效则从基站自行触发更新的从基站密钥；或

从基站判断从基站与终端的从基站密钥是否同步；

若不同步则从基站自行触发更新的从基站密钥。

10 在具体的执行过程中，从基站依据密钥推导决策判断是否触发更新从基站密钥的情况不限于上述情况，具体还可包括从基站密钥在解密过程中出现解密故障，需要重新生成新的从基站密钥以实现数据的顺利传输等。

所述从基站自行触发从基站密钥更新的方法，具体实现可如图 7 所示，  
包括：

15 步骤 S2.1：从基站 SeNB 若想更新从基站密钥 S-KeNB，直接依据现有的当前从基站密钥和 ISC 产生新的从基站密钥；

步骤 S2.2：从基站向主基站发送添加修改 DRB 命令消息，所述添加修改 DRB 命令消息中包括 ISC；

20 步骤 S2.3：主基站接收到所述添加修改 DRB 命令消息后，向终端发送 RRC 重配置请求消息；所述 RRC 重配置请求消息中包括有所述 ISC；

步骤 S2.4：终端接收到所述 RRC 重配置请求消息后，依据所述 RRC 重配置请求消息中的 ISC 参数及当前从基站密钥推导新的从基站密钥；并依据所述 RRC 重配置请求消息及新的从基站密钥建立与从基站的连接；

25 为了进一步告知主基站和从基站当前连接状况和/或从基站密钥的更新状况；所述方法还包括：

步骤 S2.5：终端向所述主基站发送 RRC 重配置响应；

步骤 S2.6：主基站接收到所述 RRC 重配置响应后，依据所述 RRC 重配置响应向所述从基站发送 SeNB 状态传输信息，以向从基站反馈当前连接状况等消息。

5 为了方便下一次从基站密钥的更新，在本实施例中任一个技术方案的基础上，在所述从基站向主基站发送添加修改 DRB 命令消息之后，所述方法还包括：从基站更新所述 ISC。具体的更新所述 ISC 可为 ISC 的计数值加 1。

综合上述本实施例是实施例一与实施例二的结合，可视为实现实施例  
10 一与实施例二的各种技术方案的组合，同样的具有解决了现有技术中从基  
站密钥更新中的不足，还实现了终端与从基站之间的安全高保障。

#### 实施例四：

本实施例提供一种从基站，所述从基站包括：

第一推导单元，配置为依据当前从基站密钥以及 ISC 推导新的从基站  
15 密钥；

其中，所述 ISC 为推导从基站密钥计数值。

所述第一推导单元的具体结构可为处理器；所述处理器包括多核或单  
核的中央处理器、单片机、数字信号处理及可编程阵列等具有处理功能的  
电子元器件。在具体的实现过程中所述从基站还可包括计数器；所述计数  
20 器可配置为形成所述 ISC；在具体的实现过程中，所述 ISC 的取值可从 0  
或 1 开始；在本实施例中从 0 开始计数。

本实施例提供了一种从基站，可自行更新从基站密钥，为实施例一中  
所述的从基站密钥更新方法提供了实现的硬件支撑，从而同样的具有解决  
了现有技术中主基站向同一从基站多次推送相关联 DRB 中导致的从基站密  
25 钥更新的问题。

优选地，如图 8 所示，所述从基站包括第一推导单元 110 及第一接收单元 120；

所述第一发送单元 120，配置为在所述从基站密钥以及 ISC 推导新的从基站密钥之后，向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；  
5

其中，所述 ISC 由所述主基站通过 RRC 重配置请求消息发送到终端；

所述 RRC 重配置请求消息用于指示终端连接所述从基站及终端，并依据所述 ISC 更新的从基站密钥。

所述第一发送单元 120 的具体结构可为有线或无线的发送接口，具体的如发送天线或双绞线、同轴电缆或光纤所对应的有线通信接口。所述发送接口与所述第一推导单元 110 相连。  
10

优选地，如图 9 所示，所述从基站还包括第一接收单元 130 及判断单元 140；

所述第一接收单元 130，配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，接收主基站发送的添加修改 DRB 请求消息；  
15

所述判断单元 140，配置为判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

所述第一推导单元 110，配置为当所述添加修改 DRB 请求消息没有携带从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基站密钥。  
20

所述第一接收单元 130 的具体结构可包括接收接口，如接收天线或其他有线网络通信接口等结构；所述判断单元 140 的具体结构可为处理器；所述处理器可为中央处理器、单片机、数字信号处理或可编程逻辑编程阵列等具有处理功能的电子元器件；在具体的实现过程中所述判断单元 140 和所述第一推导单元 110 可以各自分别对应一个处理器；处理器之间通过从基站内部的连接接口或总线进行连接；还可以是集成在同一处理器上，  
25

由处理器通过时分复用或以不同线程的方式分别完成所述第一推导单元即所述判断单元 140 的相应功能。

优选地，所述从基站还包括触发单元；

所述触发单元，配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，依据密钥推导决策判断是否触发更新从基站密钥；  
5

所述第一推导单元 110，还配置为在所述触发单元触发更新的从基站密钥之后，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

具体地所述触发单元，具体配置为判断当前从基站密钥是失效及当所述从基站密钥失效时触发更新的从基站密钥；或判断从基站与终端的从基站密钥是否同步及当不同步时触发更新的从基站密钥。  
10

所述触发单元同样的可以对应为处理器；或其他有线网络通信接口等结构；所述触发单元的具体结构可为处理器；所述处理器可为中央处理器、单片机、数字信号处理或可编程逻辑编程阵列等具有处理功能的电子元器件；且所述触发单元可以单独包括一个处理器，还可与其他功能单元集成  
15 对应于同一处理器。在具体的实现过程中，所述处理器还将与存储介质相连；通过运行存储在存储介质中的程序或软件可以分别实现第一推导单元 110、判断单元 140 以及触发单元的功能。

优选地，所述第一推导单元 110，具体配置为依据从基站密钥、ISC 及推导参数推导新的从基站密钥。所述推导参数包括小区物理标识及小区载频的至少其中之一；所述小区为由所述从基站覆盖所形成的小区。在具体的实施过程中所述推导参数还包括其他的参数，不局限于所述小区物理标识和小区载频。  
20

优选地，所述从基站还包括计数器；所述计数器，配置为在所述依据从基站密钥及 ISC 推导新的从基站密钥之后，更新所述 ISC。

25 实施例五：

如图 10 所示，本实施例提供一种终端，所述终端包括：

第二接收单元 210，配置为接收主基站发送的 RRC 重配置请求消息；

第二推导单元 220，配置为依据所述 ISC 及从基站密钥推导新的从基站密钥；

5 连接单元 230，配置为依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

其中所述终端可为双模终端或多模终端，至少可以实现与两个基站之间的连接。

10 所述第二接收单元 210 的具体结构可包括接收天线等通信接口。所述第二推导单元 220 可包括处理器，配置为从第二接收单元 210 中所接收的消息中提取所需的信息，具体依据所述 RRC 重配置请求消息中的 ISC 及终端中当前所存储的当前从基站密钥推导新的从基站密钥。所述处理器可为中央处理器、单片机、数字信号处理或可编程逻辑编程阵列等具有处理功能的电子元器件。在具体的实现过程中，所述处理器还将与存储介质相连；  
15 通过运行存储在存储介质中的程序或软件可以分别实现第二推导单元 220 的功能。

所述连接单元 230 配置为建立终端与从基站之间建立连接通道，具体所对应的结构可包括通信接口，如空口。

20 本实施例所述的终端为实施例二中所述的从基站密钥更新方法，提供了硬件支持，能够用于实现实施例二中任一所述的技术方案，同样的具有从基站密钥更新的功能以及无需从主基站或从基站获取密钥，进而具有安全性高的优点。

实施例六：

25 如图 11 所示，本实施例提供一种通信系统，所述通信系统包括：

从基站 330，配置为依据当前从基站密钥以及 ISC 推导新的从基站密钥；向主基站 310 发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

主基站 310，配置为接收所述添加修改 DRB 命令消息，提取所述 ISC；

5 通过 RRC 重配置请求消息向终端发送所述 ISC；

终端 320，配置为接收所述 RRC 重配置请求消息；依据所述 ISC 及当前从基站密钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与所述从基站 330 的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

10 优选地，所述主基站 310，还配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前发送添加修改 DRB 请求消息；所述从基站 330，还配置为接收所述添加修改 DRB 请求消息；判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；且当所述添加修改 DRB 请求消息没有携带从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

15 所述从基站 330，还配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前依据密钥推导决策判断是否触发更新从基站密钥；且当触发更新从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。所述从基站 330，配置为判断当前从基站密钥是失效或判断从基站与终端的从基站密钥是否同步；且当所述从基站密钥失效时自行触发更新的从基站密钥或当不同时自行触发更新的从基站密钥。

所述从基站 330，还配置为在所述从基站向主基站发送添加修改 DRB 命令消息之后，更新所述 ISC。

主基站 310、终端 320 及从基站 330 都是通过无线网络相连。

图 12 所示的为一个通信系统的示例，其中包括宏基站、小基站及终端；  
25 所述宏基站作为主基站形成大椭圆所围成的宏小区 Macro cell；所述小基站

作为从基站形成小椭圆所围成的小小区 Small cell。终端分别于宏基站及小基站都有连接；其中终端与宏基站之间通过载波 Carrier (F1) 相互传输数据，如 U-plane data；终端与小基站之间通过载波 Carrier (F2) 相互传输数据如 U-plane data；所述 U-plane data 为用户面数据。

5 本实施例所述的通信系统为实施例三中所述的从基站密钥更新方法提供了硬件支持，能够用于实现实施例三中任一所述的技术方案，具有解决了现有技术从基站密钥更新的问题，同时提升了从基站和终端之间的信息传输的安全性。

本发明实施例还提供一种计算机存储介质，所述计算机存储介质中存  
10 储有计算机可执行指令，所述计算机可执行指令用于执行权利实施例一至  
实施例三中所述方法的至少其中之一，具体如图 1、图 2、图 3 和/或图 6  
中所示的方法。

所述计算机存储介质包括：移动存储设备、只读存储器 (ROM,  
Read-Only Memory)、随机存取存储器 (RAM, Random Access Memory)、  
15 磁碟或者光盘等各种可以存储程序代码的介质；优先为非瞬间存储介质。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保  
护范围。凡按照本发明原理所作的修改，都应当理解为落入本发明的保护  
范围。

## 权利要求书

1、一种从基站密钥更新方法，所述方法包括：

依据当前从基站密钥以及 ISC 推导新的从基站密钥；

其中，所述 ISC 为推导从基站密钥的计数值。

5 2、根据权利要求 1 所述的方法，其中，在所述从基站密钥以及 ISC 推导新的从基站密钥之后，所述方法还包括：

向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

其中，所述 ISC 由所述主基站通过 RRC 重配置请求消息发送到终端；

10 所述 RRC 重配置请求消息用于指示终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与所述从基站的连接。

3、根据权利要求 1 或 2 所述的方法，其中，在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，所述方法还包括：

15 接收主基站发送的添加修改 DRB 请求消息；

判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

若否，则进入所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

4、根据权利要求 1 或 2 所述的方法，其中，

20 在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，所述方法还包括：

依据密钥推导决策判断是否触发更新从基站密钥；

若是，则进入所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

5、根据权利要求 4 所述的方法，其中，所述依据密钥推导决策判断是否触发更新从基站密钥包括：

判断当前从基站密钥是失效；

若失效则触发更新的从基站密钥；或

5 判断从基站与终端的从基站密钥是否同步；

若不同步则触发更新的从基站密钥。

6、根据权利要求 1 或 2 所述的方法，其中，所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥包括：

依据从基站密钥、ISC 及推导参数推导新的从基站密钥。

10 7、根据权利要求 6 所述的方法，其中，

所述推导参数包括小区物理标识和/或小区载频；

所述小区为由所述从基站覆盖所形成的小区。

8、根据权利要求 1 或 2 所述的方法，其中，在所述依据从基站密钥及 ISC 推导新的从基站密钥之后，所述方法包括：

15 更新所述 ISC。

9、一种从基站密钥更新方法，所述方法包括：

接收主基站发送的 RRC 重配置请求消息；所述 RRC 重配置请求消息中包括 ISC；

根据所述 ISC 及当前从基站密钥推导新的从基站密钥；

20 根据所述 RRC 重配置请求消息和所述新的从基站密钥，与从基站建立连接；

其中，所述 ISC 为推导从基站密钥的计数值。

10、一种从基站密钥更新方法，其中，所述方法包括：

从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥；

25 从基站向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包

括所述 ISC;

主基站接收所述添加修改 DRB 命令消息；

主基站向终端发送 RRC 重配置请求消息；所述 RRC 重配置消息包含所述 ISC；

5 终端接收所述 RRC 重配置请求消息；

终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥；

终端依据所述 RRC 重配置消息及所述新的从基站密钥与从基站建立连接；

其中，所述 ISC 为推导从基站密钥的计数值。

10 11、根据权利要求 10 所述的方法，其中，在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，所述方法还包括：

主基站发送添加修改 DRB 请求消息；

从基站接收所述添加修改 DRB 请求消息；

从基站判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

15 若否，则从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

12、根据权利要求 10 所述的方法，其中，在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，所述方法还包括

从基站依据密钥推导决策判断是否触发更新从基站密钥；

20 若是，从基站执行所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥的步骤。

13、根据权利要求 12 所述的方法，其中，所述从基站依据密钥推导决策判断是否触发更新从基站密钥包括：

从基站判断当前从基站密钥是失效；

25 若失效则从基站自行触发更新的从基站密钥；或

从基站判断从基站与终端的从基站密钥是否同步；

若不同步则从基站自行触发更新的从基站密钥。

14、根据权利要求 10 至 13 中任一项所述的方法，其中，在所述从基站向主基站发送添加修改 DRB 命令消息之后，所述方法还包括：

5 从基站更新所述 ISC。

15、一种从基站，所述从基站包括：

第一推导单元，配置为依据当前从基站密钥以及 ISC 推导新的从基站密钥；

其中，所述 ISC 为推导从基站密钥的计数器的计数值。

10 16、根据权利要求 15 所述的从基站，其中，所述从基站还包括第一接收单元；

所述第一发送单元，配置为在所述从基站密钥以及 ISC 推导新的从基站密钥之后，向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；

15 其中，所述 ISC 由所述主基站通过 RRC 重配置请求消息发送到终端；

所述 RRC 重配置请求消息用于指示终端依据所述 ISC 及当前从基站密钥推导新的从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站密钥建立与从基站的连接。

17、根据权利要求 15 或 16 所述的从基站，其中，所述从基站还包括  
20 第一接收单元及判断单元；

所述第一接收单元，配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，接收主基站发送的添加修改 DRB 请求消息；

所述判断单元，用于判断所述添加修改 DRB 请求消息中是否有携带从基站密钥；

25 所述第一推导单元，配置为当所述添加修改 DRB 请求消息没有携带从

基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

18、根据 15 或 16 所述的从基站，其中，所述从基站还包括触发单元；

所述触发单元，配置为在所述从基站依据当前从基站密钥以及 ISC 推导新的从基站密钥之前，依据密钥推导决策判断是否触发更新从基站密钥；

5 所述第一推导单元，还配置为在所述触发单元触发更新的从基站密钥之后，依据当前从基站密钥以及 ISC 推导新的从基站密钥。

19、根据权利要求 18 所述的从基站，其中，所述触发单元，配置为判断当前从基站密钥是失效及当所述从基站密钥失效时触发更新的从基站密钥；或判断从基站与终端的从基站密钥是否同步及当不同步时触发更新的  
10 从基站密钥。

20、根据权利要求 15 或 16 所述的从基站，其中，所述第一推导单元，配置为依据从基站密钥、ISC 及推导参数推导新的从基站密钥。

21、根据权利要求 20 所述的从基站，其中，

所述推导参数包括小区物理标识和/或小区载频；

15 所述小区为由所述从基站覆盖所形成的小区。

22、根据权利要 15 或 16 所述的从基站，其中，所述从基站还包括计数器；

所述计数器，配置为在所述依据从基站密钥及 ISC 推导新的从基站密钥之后，更新所述 ISC。

20 23、一种终端，所述终端包括：

第二接收单元，配置为接收主基站发送的 RRC 重配置请求消息；

第二推导单元，配置为依据当前所述 ISC 及从基站密钥推导新的从基  
站密钥；

连接单元，配置为依据所述 RRC 重配置请求消息及所述新的从基站密

25 钥建立与从基站的连接；

其中，所述 ISC 为推导从基站密钥的计数值。

24、一种通信系统，所述通信系统包括：

从基站，配置为依据当前从基站密钥以及 ISC 推导新的从基站密钥；  
向主基站发送添加修改 DRB 命令消息；所述 DRB 命令消息包括所述 ISC；  
5 主基站，配置为接收所述添加修改 DRB 命令消息，提取所述 ISC；通  
过 RRC 重配置请求消息向终端发送所述 ISC；

终端，配置为接收所述 RRC 重配置请求消息；依据所述 ISC 更新及从  
基站密钥从基站密钥，并依据所述 RRC 重配置请求消息及所述新的从基站  
密钥建立与所述从基站的连接；

10 其中，所述 ISC 为推导从基站密钥的计数值。

25、根据权利要求 24 所述的系统，其中，

所述主基站，还配置为在所述从基站依据当前从基站密钥以及 ISC 推  
导新的从基站密钥之前发送添加修改 DRB 请求消息；

所述从基站，还配置为接收所述添加修改 DRB 请求消息；判断所述添  
15 加修改 DRB 请求消息中是否有携带从基站密钥；且当所述添加修改 DRB  
请求消息没有携带从基站密钥时，依据当前从基站密钥以及 ISC 推导新的  
从基站密钥。

26、根据权利要求 24 所述的系统，其中，

所述从基站，还配置为在所述从基站依据当前从基站密钥以及 ISC 推  
20 导新的从基站密钥之前依据密钥推导决策判断是否触发更新从基站密钥；  
且当触发更新从基站密钥时，依据当前从基站密钥以及 ISC 推导新的从基  
站密钥的步骤。

27、根据权利要求 26 所述的方法，其中，所述从基站，配置为判断当  
前从基站密钥是失效或判断从基站与终端的从基站密钥是否同步；且当所  
25 述从基站密钥失效时自行触发更新的从基站密钥或当不同时自行触发更新

的从基站密钥。

28、根据权利要求 24 至 26 中任一项所述的方法，其中，所述从基站，还配置为在所述从基站向主基站发送添加修改 DRB 命令消息之后，更新所述 ISC。

5 29、一种计算机存储介质，所述计算机存储介质中存储有计算机可执行指令，所述计算机可执行指令用于执行权利要求 1 至 14 所述方法的至少其中之一。

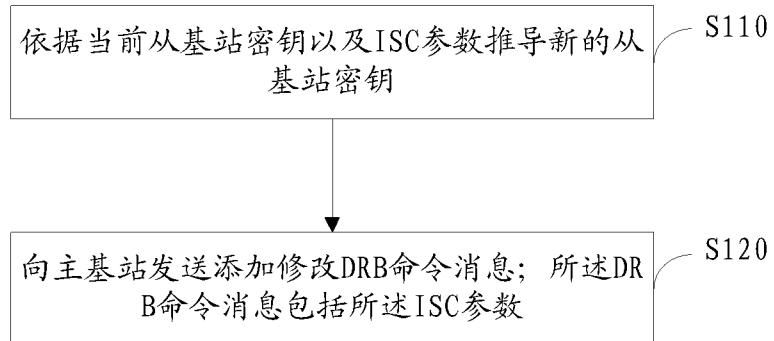


图 1

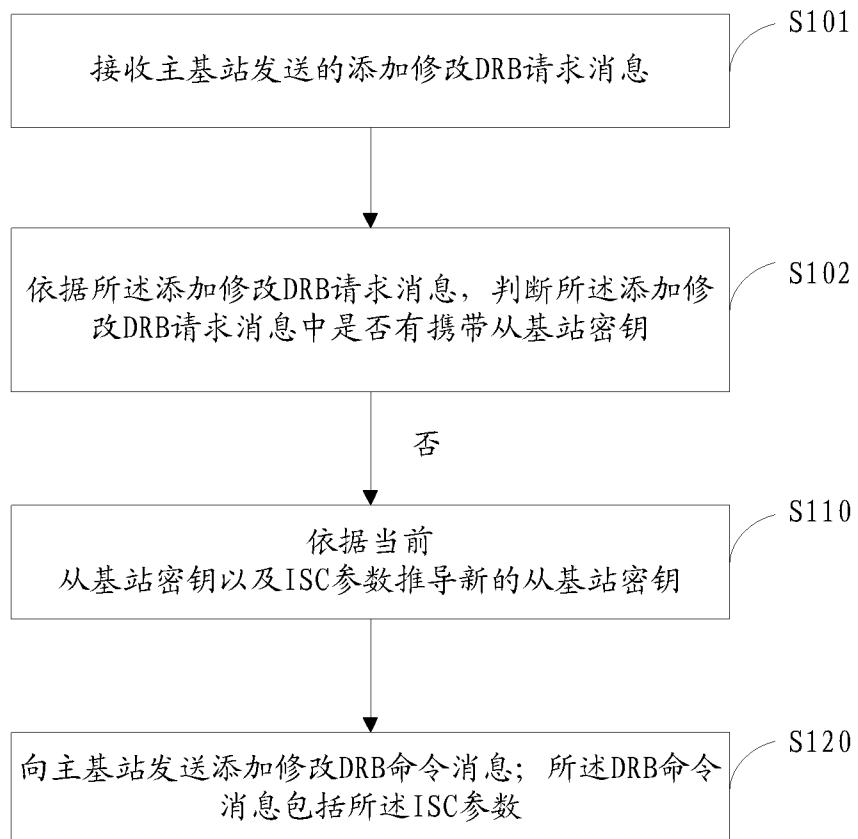


图 2

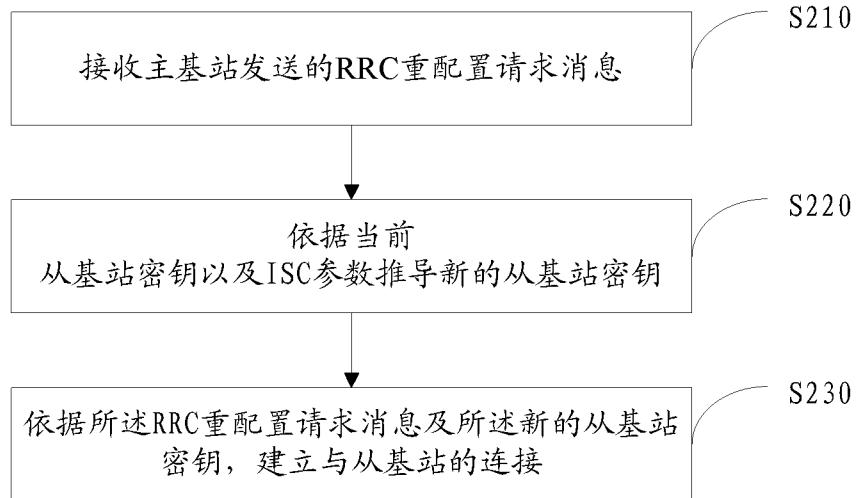


图 3

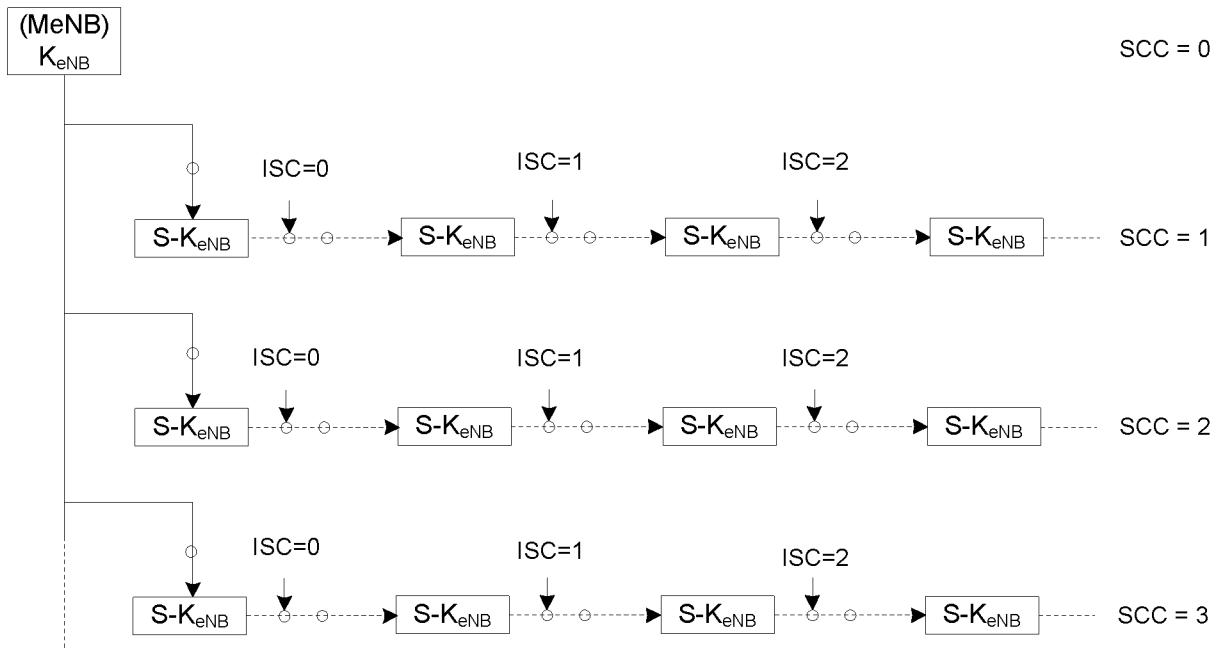


图 4

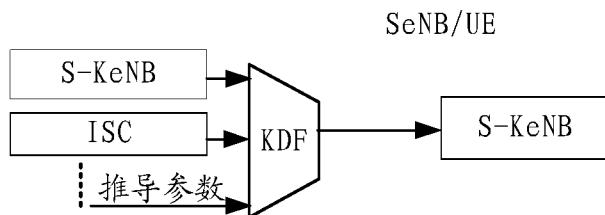


图 5

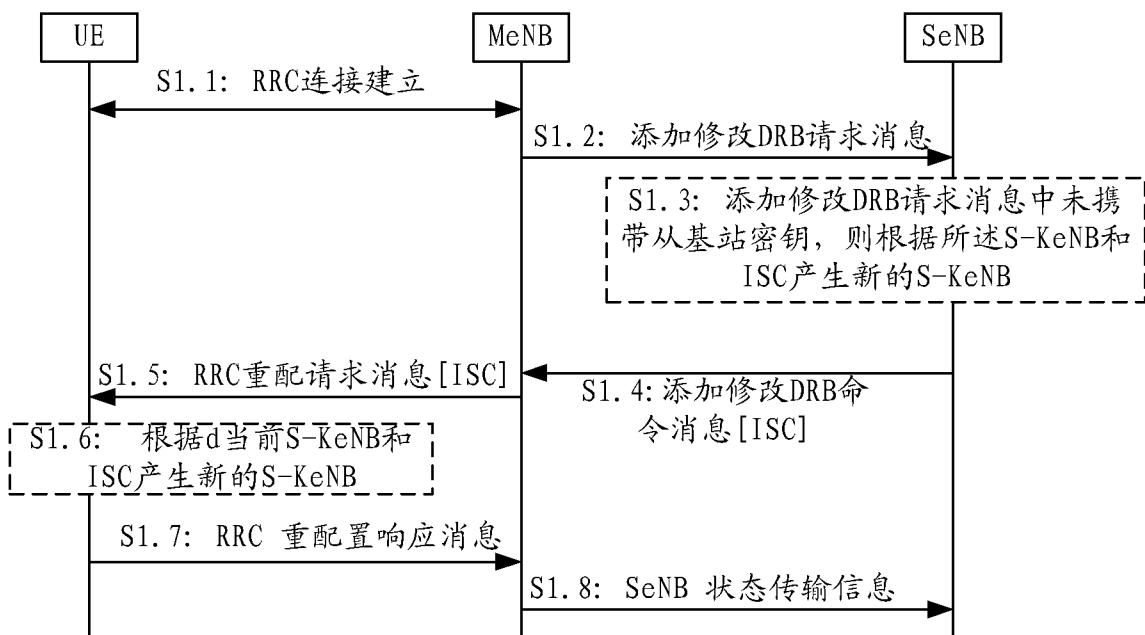


图 6

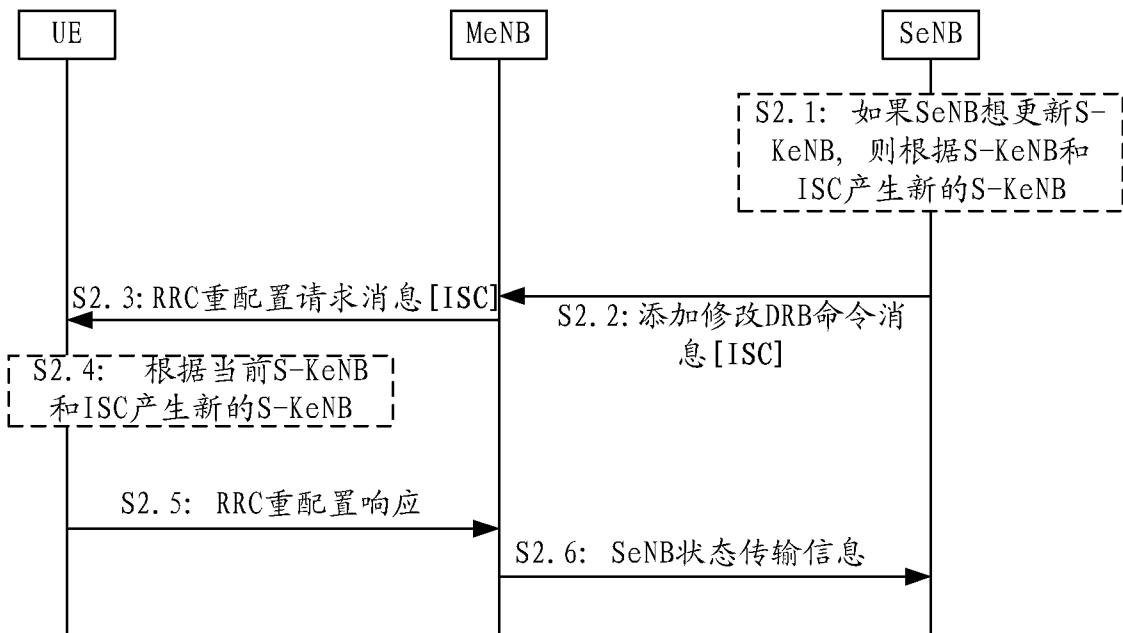


图 7

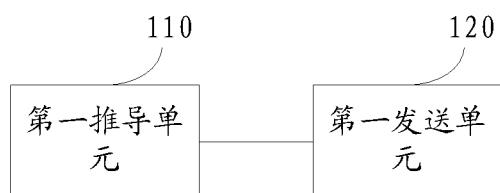


图 8

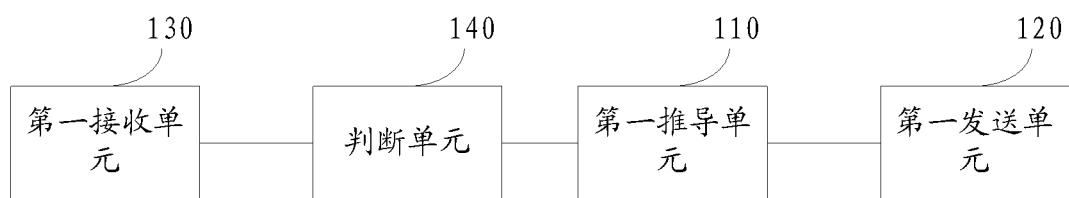


图 9



图 10

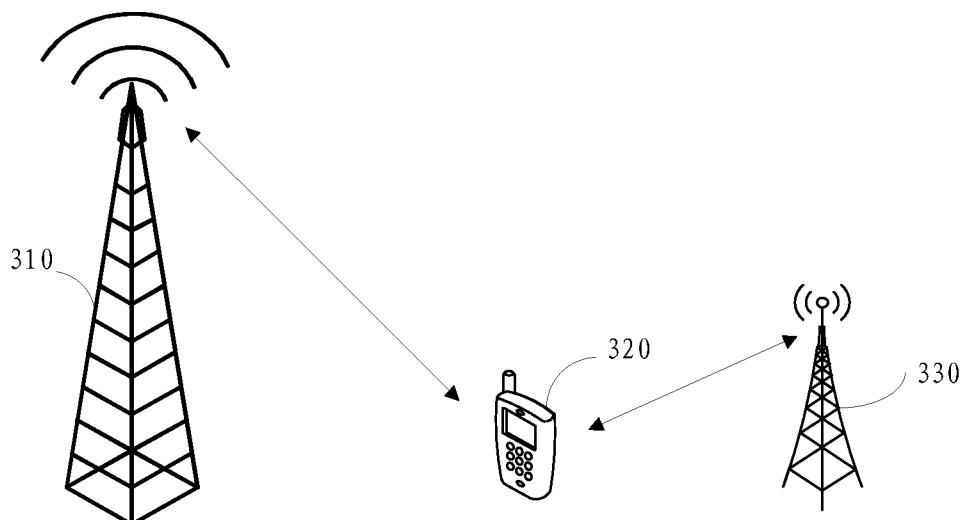


图 11

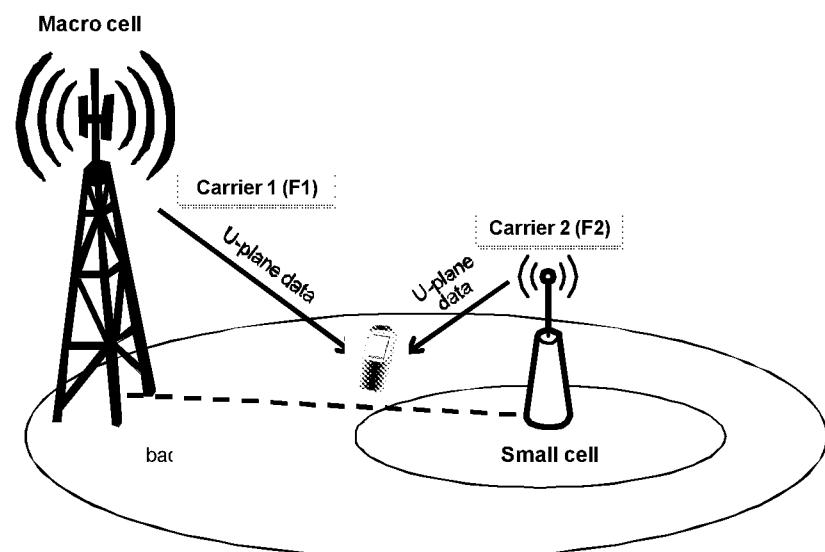


图 12

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/084808

## A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i

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

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04Q

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)

CPRS, CNABS, CNTXT, VEN: main base station, master node, primary cell, macro base station, slave base station, slave cell, slave node, refresh; master, eNB, macro, small, cell, secondary, security key, update, new security key

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2013116976 A1 (NOKIA CORPORATION), 15 August 2013 (15.08.2013), description, page 17, lines 3-18, and figure 5	1-29
A	CN 103096308 A (HUAWEI TECHNOLOGIES CO., LTD.), 08 May 2013 (08.05.2013), the whole document	1-29

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search  
11 December 2014 (11.12.2014)

Date of mailing of the international search report  
**19 December 2014 (19.12.2014)**

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  
**LIU, Xiaohua**  
Telephone No.: (86-10) 62089142

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/CN2014/084808**

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2013116976 A1	15 August 2013	US 2014337935 A1 CN 104160730 A	13 November 2014 19 November 2014
CN 103096308 A	08 May 2013	US 2014237559 A1 WO 2013064041 A1 EP 2765795 A1 EP 2765795 A4	21 August 2014 10 May 2013 13 August 2014 08 October 2014

## 国际检索报告

国际申请号

PCT/CN2014/084808

## A. 主题的分类

H04W 12/04 (2009. 01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

## B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04Q

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))

CPRS, CNABS, CNTXT, VEN: 主基站, 主节点, 主小区, 宏基站, 从基站, 从小区, 从节点, 密钥, 更新, 刷新, 新密钥; master, eNB, macro, small, cell, secondary, security key, update, new security key

## C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	WO 2013116976 A1 (诺基亚公司) 2013年 8月 15日 (2013 - 08 - 15) 说明书第17页第3-18行, 图5	1-29
A	CN 103096308 A (华为技术有限公司) 2013年 5月 08日 (2013 - 05 - 08) 全文	1-29

 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

2014年 12月 11日

国际检索报告邮寄日期

2014年 12月 19日

ISA/CN的名称和邮寄地址

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

受权官员

刘晓华

传真号 (86-10) 62019451

电话号码 (86-10) 62089142

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2014/084808

检索报告引用的专利文件		公布日 (年/月/日)		同族专利		公布日 (年/月/日)	
WO	2013116976	A1	2013年 8月 15日	US	2014337935	A1	2014年 11月 13日
				CN	104160730	A	2014年 11月 19日
CN	103096308	A	2013年 5月 08日	US	2014237559	A1	2014年 8月 21日
				WO	2013064041	A1	2013年 5月 10日
				EP	2765795	A1	2014年 8月 13日
				EP	2765795	A4	2014年 10月 08日

表 PCT/ISA/210 (同族专利附件) (2009年7月)