

(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
2009 年 10 月 22 日 (22.10.2009)

PCT

(10) 国际公布号
WO 2009/127114 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2008/073868

(22) 国际申请日: 2008 年 12 月 30 日 (30.12.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810066591.7 2008 年 4 月 16 日 (16.04.2008) CN

(71) 申请人 (对除美国外的所有指定国): **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: 及

(75) 发明人/申请人 (仅对美国): **甘露 (GAN, Lu)** [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)。 **杜忠达 (DU, Zhongda)** [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)。 **程翔 (CHENG, Xiang)** [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)。 **柯雅珠 (KE, Yazhu)** [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)。

(74) 代理人: **北京康信知识产权代理有限公司 (KANGXIN PARTNERS, P.C.)**; 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: A CRYPTOGRAPHIC KEY GENERATING METHOD, DEVICE AND SYSTEM

(54) 发明名称: 密钥生成方法、装置及系统

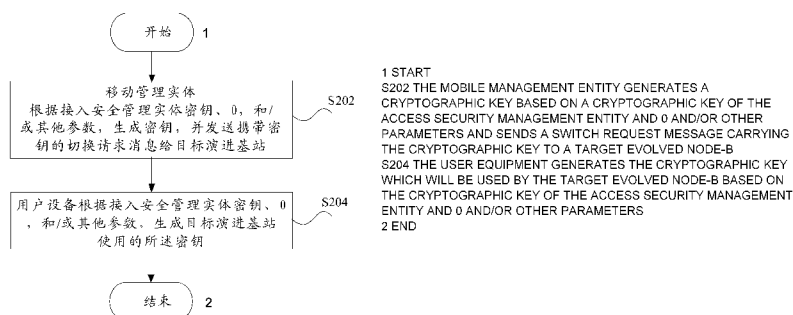


图 2 / Fig. 2

(57) Abstract: A cryptographic key generating method, device and system are provided, wherein, the method is used for generating a cryptographic key in the process of the user equipment switching to an EUTRAN (Evolved UTMS (Universal Mobile Telecommunication System) Terrestrial Radio Access Network) network from the other network, the method includes: a MME (Mobile Management Entity) of the EUTRAN network and a special value and/or other parameters and sends a switch request message carrying the cryptographic key to a target evolved Node-B, i.e. eNB (evolved Node-B); a UE (user equipment) generates the cryptographic key which will be used by the target eNB based on the root cryptographic key K_{ASME} of the EUTRAN network and the special value and/or other parameters. The application of the present invention adopts a special value and K_{ASME} and/or other parameters to output a cryptographic key, which can solve the problem existed in the related technology, the problem is that the middle cryptographic key used by access layer while switching between different access system couldn't be generated, and then it could not realize the safety protection of the access layer. So the application of the present invention makes the signaling and/or data of the access layer be efficiently protected, thereby improving the safety of the access layer.

[见续页]



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种密钥生成方法、装置及系统,其中,该方法用于在用户设备从其他网络切换到 EUTRAN 网络的过程中生成密钥,该方法包括: MME 根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数,生成密钥,并发送携带密钥的切换请求消息给目标演进的基站即目标 eNB; UE 根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数,生成目标 eNB 使用的密钥。通过本发明,采用特定值、 K_{ASME} 和/或其他参数,来输出密钥,能够解决相关技术中存在的不同接入系统间切换时无法生成由接入层使用的中间密钥、从而无法实现接入层安全性保护的问题,从而使接入层的信令和/或数据能得到有效保护,能够加强接入层的安全性。

密钥生成方法、装置及系统

技术领域

本发明涉及通信领域中密钥生成技术，具体地，涉及在不同系统间切换时的密钥生成方法、装置及系统。

5 背景技术

第三代合作伙伴计划（3rd Generation Partnership Project，简称为 3GPP）演进的分组系统（Evolved Packet System，简称为 EPS）由演进的陆地无线接入网（Evolved UMTS Terrestrial Radio Access Network，简称为 EUTRAN）和 EPS 演进的分组核心网（Evolved Packet Core，简称为 EPC）组成。其中，
10 EPC 能够支持用户从全球移动通讯系统增强型数据速率 GSM 演进实体无线接入网（Global System for Mobile Communication Enhanced Data Rate for GSM Evolution radio access network，简称为 GERAN）和通用陆地无线接入网（Universal Terrestrial Radio Access Network，简称为 UTRAN）的接入。

EPC 分组核心网包含移动管理实体（Mobility Management Entity，简称为 MME），MME 负责移动性的管理、非接入层信令的处理、以及用户安全模式的管理等控制面相关的工作。其中，MME 保存 EUTRAN 的根密钥——
15 接入安全管理实体密钥（Key Access Security Management Entity，简称为 K_{ASME} ）。在 EUTRAN 中，基站设备为演进的基站（evolved Node-B，简称为 eNB），主要负责无线通信、无线通信管理、和移动性上下文的管理。供 eNB
20 使用的接入层的根密钥是演进的基站密钥（Key eNB，简称为 K_{eNB} ）。

3GPP 通用移动通信系统（Universal Mobile Telecommunication System，简称为 UMTS）系统中负责移动性上下文的管理、和/或用户安全模式的管理的设备是服务通用分组无线业务支持节点（Serving General Packet Radio Service Support Node，简称为 SGSN）。此外，SGSN 还负责认证用户设备（User
25 Equipment，简称为 UE）。

3GPP UMTS 系统中，负责无线通信管理的设备是 UTRAN 中的无线网络控制器（Radio Network Controller，简称为 RNC）。图 1 示出了根据相关技术的 UE 从 UTRAN 切换到 EUTRAN 的密钥生成方法流程，如图 1 所示，

UE 从 UTRAN 切换到 EUTRAN 时 (即, 执行步骤 S101), 如果 UE 和 MME 中没有保存 EPS 安全相关参数, 如 K_{ASME} , 则 RNC 需要通过发送重定向请求 (即, 执行步骤 S102 至步骤 S104), 使 MME 生成 EUTRAN 中的密钥 K_{ASME} ; MME 在 eNB 确认切换请求之后, 向 RNC 转发重定向回复 (即, 执行步骤 S106 至步骤 S112), RNC 执行 UTRAN 切换命令 (即, 执行步骤 S114), UE 侧生成 EUTRAN 中的密钥 K_{ASME} , 完成切换到 EUTRAN (即, 执行步骤 S116)。

目前, 在相关技术中, 在不同接入系统之间进行切换时, 例如, 从其他网络切换到 EUTRAN 时, 虽然可以生成 EUTRAN 的根密钥 K_{ASME} , 但无法生成由接入层使用的密钥, 例如, 供 eNB 使用的接入层的根密钥 K_{eNB} , 因此, 接入层的信令和/或数据无法得到有效保护, 存在安全隐患。

发明内容

考虑到相关技术中存在的不同接入系统间切换时无法生成由接入层使用的中间密钥、从而无法实现接入层安全性保护的问题, 本发明的主要目的在于提供一种改进的密钥生成方案, 以解决相关技术中的上述问题至少之一。

为实现上述目的, 根据本发明的一个方面, 提供了一种密钥生成方法。

根据本发明的密钥生成方法, 用于在用户设备从其他网络切换到 EUTRAN 网络的过程中生成密钥, 包括: MME 根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数, 生成密钥, 并发送携带密钥的切换请求消息给目标演进的基站即目标 eNB; 用户设备根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数, 生成目标 eNB 使用的密钥。

优选地, 上述特定值为移动管理实体和用户设备共同拥有, 从而不需要转发给移动管理实体, 这样就不会产生额外的信令负担。

优选地, 上述特定值为移动管理实体和用户设备共同拥有的值 0。

优选地, 根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数, 生成密钥的操作具体可以包括: 将特定值和/或其他参数和根密钥 K_{ASME} 输入预设的单向密钥生成函数; 将单向密钥生成函数的输出作为密钥。

优选地, MME 可以根据接收到的重定向请求消息生成 EUTRAN 网络的根密钥 K_{ASME} 。

优选地，目标 eNB 收到密钥之后，该方法还可以包括：MME 接收与切换请求消息对应的切换请求确认消息，并向当前网络的 SGSN 发送与重定向请求消息对应的重定向回复消息；当前网络的 SGSN 接收重定向回复消息，并发送重定向命令消息；当前网络的无线网络控制器向用户设备发送切换命令消息；用户设备根据接收到的切换命令消息生成 EUTRAN 网络的根密钥 K_{ASME} 。

为实现上述目的，根据本发明的另一个方面，提供了一种密钥生成装置。

根据本发明实施例的密钥生成装置，包括：第一单元，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0 和/或其他参数，生成密钥。

10 优选地，第一单元可以设置于 MME，第一单元包括：第一密钥产生模块，用于根据接收到的重定向请求消息生成根密钥 K_{ASME} ，并根据根密钥 K_{ASME} 、特定值和/或其他参数，生成密钥；第一发送模块，用于发送携带密钥的切换请求消息给目标 eNB。

优选地，第一单元还可以设置于用户设备上。

15 为实现上述目的，根据本发明的另一个方面，提供了一种密钥生成系统。

根据本发明实施例的密钥生成系统，包括：移动管理实体，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0 和/或其他参数，生成密钥，并发送携带密钥的切换请求消息；用户设备，用于接收切换命令消息，并根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值和/或其他参数，生成密钥。

20 借助于上述技术方案，通过采用特定值、 K_{ASME} 和/或其他参数，来生成接入层使用的中间密钥，并输出该密钥，能够解决相关技术中存在的不同接入系统间切换时无法生成由接入层使用的中间密钥、从而无法实现接入层安全性保护的问题，从而使接入层的信令和/或数据能得到有效保护，能够实现接入层的安全性保护。

25 进一步地，本发明各实施例的密钥生成方法、装置和系统，因为使用特定值 0 生成密钥，从而不需要转发给移动管理实体，因此不需要额外的信令负担。

本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优

点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 为根据相关技术的 UE 从 UTRAN 切换到 EUTRAN 的密钥生成方法流程图；

图 2 为根据本发明方法实施例的密钥生成方法的流程图；

图 3 为根据本发明方法实施例一的密钥生成方法的具体实施的流程图；

10 图 4 为根据本发明方法实施例二的密钥生成方法的信令流程图；

图 5 为根据本发明装置实施例的密钥生成装置示意图；

图 6 为根据本发明装置实施例的密钥生成装置的详细结构的示意图；

图 7 为根据本发明系统实施例的密钥生成系统示意图。

具体实施方式

15 功能概述

考虑到相关技术中存在的不同接入系统间切换时无法生成由接入层使用的中间密钥、从而无法实现接入层安全性保护的问题，本发明的实施例提供了一种改进的密钥生成方案，在本发明的实施例中，用特定值、 K_{ASME} 和/或其他参数生成接入层使用的中间密钥，并输出该密钥，使接入层的信令和/或数据能得到有效保护，能够实现接入层的安全性保护。

20 以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述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。如果不冲突，本发明实施例以及实施例中的特征可以相互组合。

方法实施例

25 根据本发明实施例，首先提供了一种密钥生成方法。

图 2 为根据本发明实施例的密钥生成方法的流程图。需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

5 如图 2 所示，根据本发明实施例的密钥生成方法包括以下处理过程（步骤 S202 至步骤 S204）：

 优选地，在执行步骤 S202 之前，MME 根据接收到的重定向请求消息生成 EUTRAN 网络的根密钥 K_{ASME} ；

 步骤 S202，MME 根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0，和/或其他参数，生成密钥，并发送携带密钥的切换请求消息给目标 eNB；该特定值为 MME 和用户设备共同拥有的特定值，例如，MME 和用户设备默认该特定值为 0；

 具体地，生成密钥的操作具体可以包括：将特定值和/或其他参数和根密钥 K_{ASME} 输入预设的单向密钥生成函数；将该单向密钥生成函数的输出

15 作为密钥；

 优选地，在目标 eNB 收到所述的密钥之后，MME 接收与切换请求消息对应的切换请求确认消息，并向当前网络的 SGSN 发送与重定向请求消息对应的重定向回复消息；当前网络的 SGSN 接收重定向回复消息，并发送重定向命令消息；当前网络的 RNC 向用户设备发送切换命令消息；用户设备根据接收到的切换命令消息生成 EUTRAN 网络的根密钥 K_{ASME} ；

20

 步骤 S204，用户设备根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0，和/或其他参数，生成目标 eNB 使用的所述密钥。

 本发明实施例的密钥生成方法，可以生成 EUTRAN 网络接入层使用的密钥，使得接入层的信令和/或数据能得到有效保护，加强接入层的安全性。

25 此外，由于本实施例使用 EUTRAN 网络的特定值 0 生成密钥，从而不需要转发给移动管理实体，因此不需要额外的信令负担。

实施例一

 图 3 为根据本发明实施例一的密钥生成方法的具体实施的流程图，如图 3 所示，本实施例示出了 UE 从 UTRAN 切换到 EUTRAN 的密钥生成方法的

流程图, 该处理过程包括以下步骤 (步骤 S310 至步骤 S350):

步骤 S310, MME 收到由 SGSN 转发的来自 RNC 的重定向请求消息后, 根据重定向请求消息生成 K_{ASME} ; 优选地, MME 可以使用重定向请求消息中的参数来生成 K_{ASME} , 参数包括完整性密钥 (Integrity Key, 简称为 IK), 加密密钥 (Ciphering Key, 简称为 CK), 此外, 还可以进一步使用重定向请求消息中的公共陆地移动通信网标识 (Public Land Mobile Network Identity, 简称为 PLMN-ID) 信息生成 K_{ASME} ;

步骤 S320, MME 使用特定值 0 和 K_{ASME} 生成密钥;

10 步骤 S330, MME 生成密钥后, 在切换请求消息携带该密钥并发送给目标 eNB;

步骤 S340, UE 收到切换命令后生成 K_{ASME} ;

步骤 S350, UE 使用特定值 0 和 K_{ASME} 生成该目标 eNB 的密钥。

15 优选地, 生成 eNB 使用的接入层的密钥之后, 还可以包括以下步骤: eNB 和 UE 还可以进一步根据生成的密钥, 生成 EUTRAN 网络的加密密钥、完整性保护密钥、和/或用户面加密密钥以启动相应的安全保护。

本实施例的密钥生成方法因为采用特定值 0 和 K_{ASME} 来输出, 所以克服了现有技术中在 UE 从 UTRAN 切换到 EUTRAN 时无法生成 K_{eNB} 的问题, 从而能加强安全保护。

实施例二

20 图 4 为根据本发明实施例二的密钥生成方法的信令流程图, 其中, 图 4 中源 RNC 以及源 SGSN 表示 UE 当前连接到的 UMTS 中的设备; 目标 eNB 以及目标 MME 标识 UE 将要切换到的 EPS 中的设备。如图 4 所示, 根据本发明实施例二的密钥生成方法的信令流程包括以下处理过程 (步骤 S401 至步骤 S415):

25 步骤 S401, UTRAN 中的源 RNC 决定发起切换, 具体可以是根据 UE 发给该 RNC 的测量报告触发, 也可以是根据其他原因由 RNC 发起切换决定;

步骤 S402, 源 RNC 向源 SGSN 发送重定向请求消息;

步骤 S403, 源 SGSN 向目标 MME 转发该重定向请求消息, 并且同时发送 IK, CK 给目标 MME;

步骤 S404, 目标 MME 收到重定向请求消息后, 使用完整性密钥 IK、加密密钥 CK 及其他的参数, 如 PLMN-ID, 生成 K_{ASME} ;

5 步骤 S405, 目标 MME 使用特定值 0 和 K_{ASME} , 生成密钥 K_{eNB} ;

步骤 S406, 目标 MME 在切换请求消息中将密钥 K_{eNB} 发送给目标 eNB;

步骤 S407, 目标 eNB 还可以进一步使用密钥 K_{eNB} 生成 EUTRAN 网络的其他密钥, 如: 无线资源控制加密密钥、完整性保护密钥, 以及用户面加密密钥; 目标 eNB 成功启动安全保护;

10 步骤 S408, 目标 eNB 向目标 MME 回复切换请求确认消息, 表示接受切换请求;

步骤 S409, 目标 MME 收到目标 eNB 的切换请求确认消息后向源 SGSN 发送转发重定向回复消息;

步骤 S410, 源 SGSN 向源 RNC 发送重定向命令;

15 步骤 S411, 源 RNC 向 UE 发送 UTRAN 切换命令;

步骤 S412, UE 根据当前 UTRAN 的切换命令, 生成 K_{ASME} ;

步骤 S413, UE 使用特定值 0 和 K_{ASME} 生成 UE 侧的密钥 K_{eNB} ;

20 步骤 S414, UE 进一步使用密钥 K_{eNB} 生成 EUTRAN 网络的其他密钥: 无线资源控制加密密钥、完整性保护密钥, 以及用户面加密密钥; UE 成功启动安全保护;

步骤 S415, UE 向目标 eNB 发送切换完成命令消息, 该切换完成命令消息可以使用 EUTRAN 网络的无线资源控制加密密钥进行加密以及使用完整性密钥进行完整性保护, 由于目标 eNB 生成的无线资源控制加密密钥及完整性密钥与 UE 侧一致, 这样, 可以成功解密用户侧 UE 发送的切换完成命令消息。

25

在本实施例的密钥生成过程中, 可以使用 0 和 K_{ASME} 和/或其他参数,

作为输入参数，采用单向密钥生成函数生成，其他参数可以根据实际情况选取，本实施例为简单起见，不选用其他参数，本领域技术人员应当了解，其他参数，不限定为无，这不影响本发明实施例的实质。

装置实施例

5 根据本发明的实施例，还提供了一种密钥生成装置。

图 5 为根据本发明装置实施例的密钥生成装置示意图，如图 5 所示，根据本发明装置实施例的密钥生成装置包括：

10 第一单元 62，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0 和/或其他参数，生成密钥 K。优选地，第一单元 62 可以设置于 MME 上，也可以设置于用户设备上，以实现用户设备侧 EUTRAN 网络接入层密钥的生成；此外，第一单元 62 的相关功能具体可参见方法实施例的相关说明，不再进行重复说明。

本实施例密钥生成装置与方法实施例的密钥生成过程类似，需要根据 K_{ASME} 和特定值 0，生成 EUTRAN 网络接入层密钥。

15 基于以上的描述，图 6 进一步示出了根据本发明实施例的密钥生成装置的详细结构示意图。如图 6 所示，本实施例中第一单元 72 设置于 MME，其中，第一单元 72 包括：第一密钥产生模块 722，用于根据接收到的重定向请求消息生成根密钥 K_{ASME} ，并根据根密钥 K_{ASME} 及特定值 0，生成密钥 K；第一发送模块 724，用于发送携带密钥 K 的切换请求消息给目标 eNB。

20 本实施例为图 5 实施例的具体化，如上所述，第一单元 72 可以设置于 MME 上，也可以设置于用户设备上，此处不再进行重复说明。

系统实施例

根据本发明实施例，还提供了一种密钥生成系统。

25 图 7 为根据本发明系统实施例的密钥生成系统示意图，如图 7 所示，根据本发明系统实施例的密钥生成系统包括：移动管理实体 82 和用户设备 84，下面对上述结构进行描述。

移动管理实体 82，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值信

息和/或其他参数，生成密钥 K，并发送携带密钥 K 的切换请求消息；

用户设备 84，用于接收切换命令消息，并根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值信息和/或其他参数，生成密钥 K。

5 本实施例具体可参见图 2 至图 4 方法实施例的具体处理流程说明，图 2 至图 4 也可以理解为根据本发明实施例的密钥生成系统的实施例解析示意图，实现目标 eNB 及用户设备生成 EUTRAN 网络接入层使用的密钥。

需要说明的是，在上述多个实施例中特定值取值为 0，也可以取其他值。

综上所述，采用本发明实施例提供的密钥生成方法、装置和系统，采用特定值和 K_{ASME} 来生成接入层使用的密钥，并输出该密钥，使得接入层的信
10 令和/或数据能得到有效保护，加强接入层的安全性。同时，使用的参数某特定值不需要转发给移动管理实体，因此不需要额外的信令负担。

显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。
15

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。
20

权 利 要 求 书

1. 一种密钥生成方法,用于在用户设备从其他网络切换到 EUTRAN 网络的过程中生成密钥,其特征在于,包括:

移动管理实体根据 EUTRAN 网络的根密钥 K_{ASME} 、及特定值和/或其他参数,生成密钥,并发送携带所述密钥的切换请求消息给目标 eNB;

用户设备根据 EUTRAN 网络的根密钥 K_{ASME} 、及特定值和/或其他参数,生成所述目标 eNB 使用的所述密钥。

2. 根据权利要求 1 所述的密钥生成方法,其特征在于,特定值为移动管理实体和用户设备共同拥有。
3. 根据权利要求 1 所述的密钥生成方法,其特征在于,所述特定值为 0。
4. 根据权利要求 1 所述的密钥生成方法,其特征在于,所述根据所述 EUTRAN 网络的根密钥 K_{ASME} 、及特定值和/或其他参数,生成密钥的操作具体包括:

将特定值和/或其他参数和所述根密钥 K_{ASME} 输入预设的单向密钥生成函数;

将所述单向密钥生成函数的输出作为所述密钥。

5. 根据权利要求 1 所述的密钥生成方法,其特征在于,所述移动管理实体根据接收到的重定向请求消息生成所述 EUTRAN 网络的根密钥 K_{ASME} 。
6. 根据权利要求 5 所述的密钥生成方法,其特征在于,所述目标 eNB 收到所述的密钥之后,所述方法还包括:

所述移动管理实体接收与所述切换请求消息对应的切换请求确认消息,并向当前网络的 SGSN 发送与所述重定向请求消息对应的重定向回复消息;

所述当前网络的 SGSN 接收所述重定向回复消息,并发送重定向命令消息;

当前网络的无线网络控制器向所述用户设备发送切换命令消息;

所述用户设备根据接收到的切换命令消息生成所述 EUTRAN 网络的根密钥 K_{ASME} 。

7. 一种密钥生成装置，其特征在于，包括：

第一单元，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、特定值 0 和/或其他参数，生成密钥。

8. 根据权利要求 7 所述的密钥生成装置，其特征在于，所述第一单元设置于移动管理实体，所述第一单元包括：

第一密钥产生模块，用于根据接收到的重定向请求消息生成根密钥 K_{ASME} ，并根据所述根密钥 K_{ASME} 及某特定值和/或其他参数，生成密钥；

第一发送模块，用于发送携带所述密钥的切换请求消息给目标 eNB。

9. 根据权利要求 7 所述的密钥生成装置，其特征在于，所述第一单元设置于用户设备上。

10. 一种密钥生成系统，其特征在于，包括：

移动管理实体，用于根据 EUTRAN 网络的根密钥 K_{ASME} 、及特定值 0 和/或其他参数，生成密钥，并发送携带所述密钥的切换请求消息；

用户设备，用于接收切换命令消息，并根据 EUTRAN 网络的根密钥 K_{ASME} 、某特定值和/或其他参数，生成密钥。

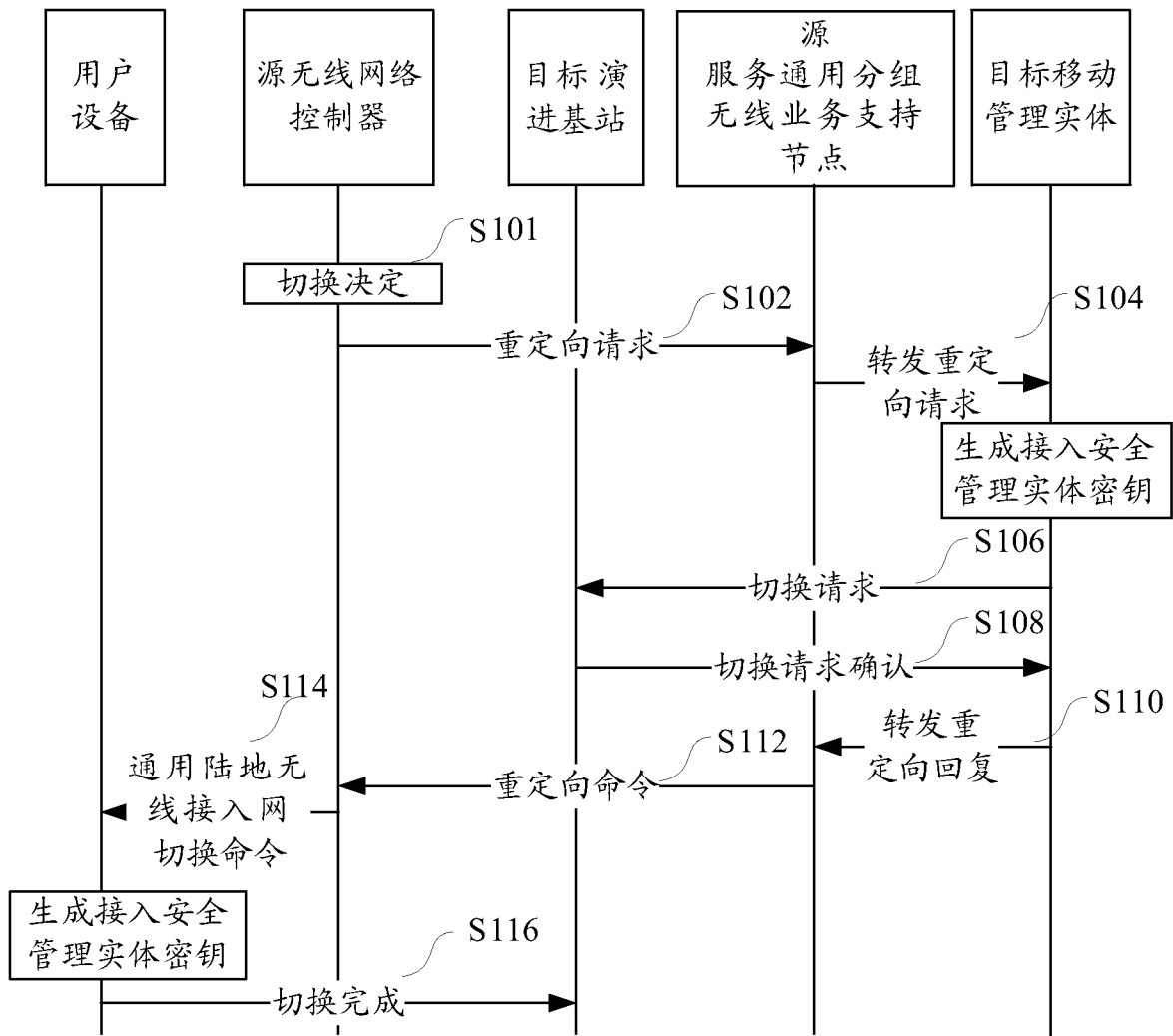


图 1

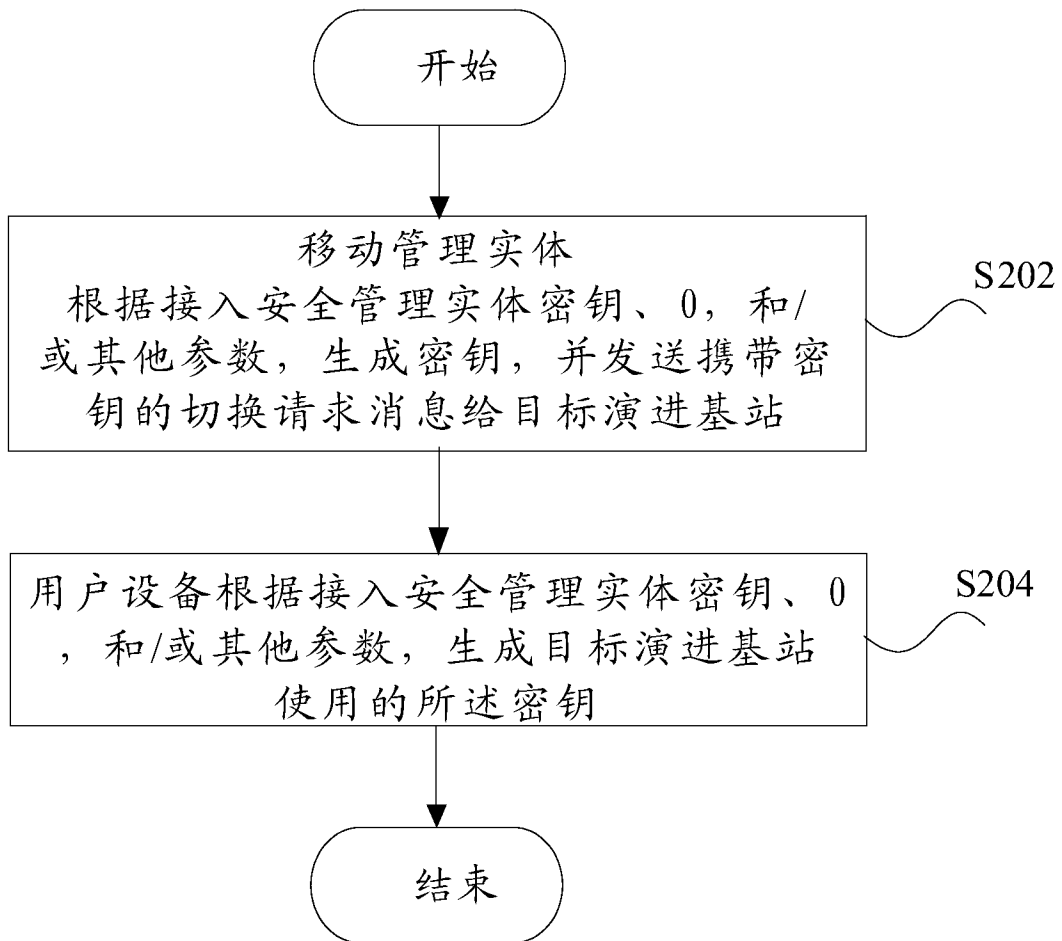


图 2

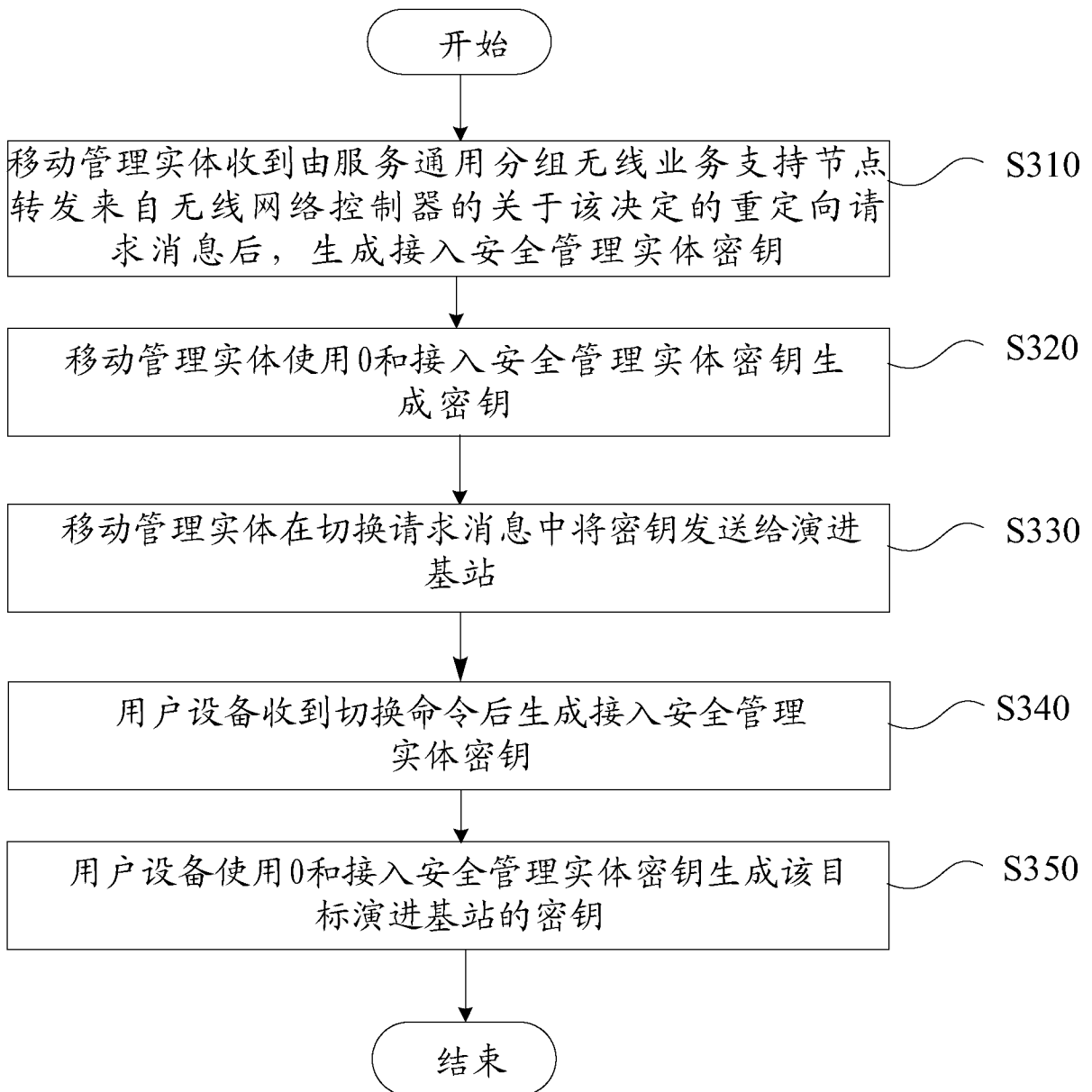


图 3

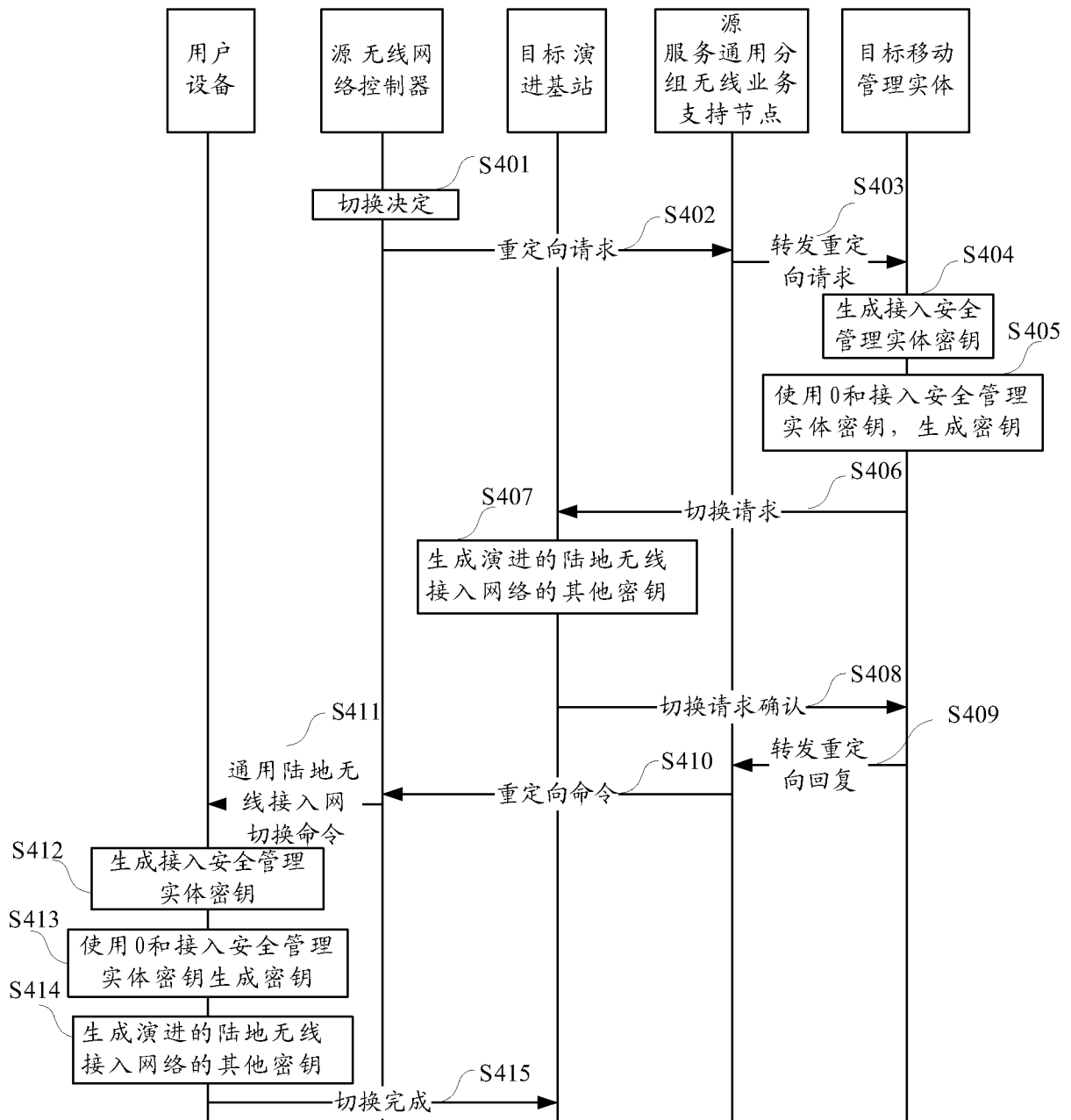


图 4

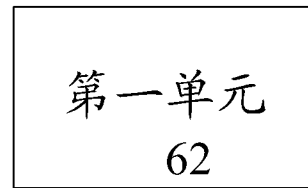


图 5

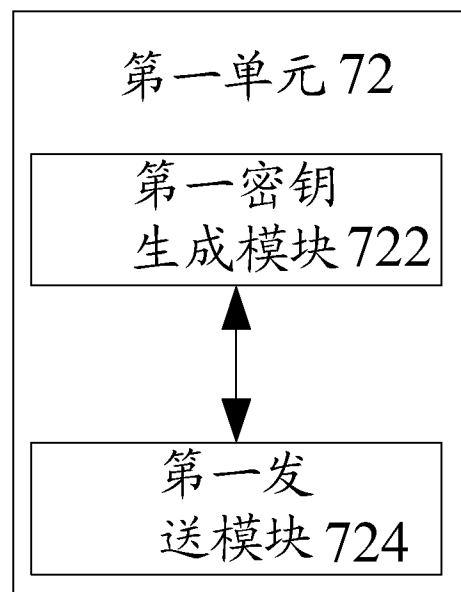


图 6

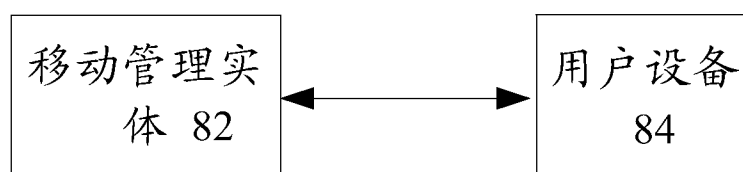


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2008/073868

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32 (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)

IPC: H04L H04W

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

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

CNPAT, CNKI, WPI, EPODOC, PAJ: key, generat+, creat+, root, mobile, manag+, entity, switch+, handover, access, network, target, node, transmit+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	CN101267668A (ZTE CORP) 17 Sep. 2008(17.09.2008) see description page 2 line 20-page 11 line 2, figs. 1-7, claims 1-10	1-10
P, X	CN101257723A (ZTE CORP) 03 Sep. 2008(03.09.2008) see description page 2 line 20-page 14 line 4, figs. 1-8, claims 1-10	1-10
A	CN1905734A (HUAWEI TECHNOLOGIES CO LTD)31 Jan. 2007(31.01.2007) see the whole document	1-10
A	CN101102600A(ZTE CORP) 09 Jan. 2008(09.01.2008) see the whole document	1-10
A	WO2007125486A2 (KONINK PHILIPS ELECTRONICS NV) 08 Nov. 2007(08.11.2007) see the whole document	1-10

☐ 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
25 Mar. 2009 (25.03.2009)Date of mailing of the international search report
09 Apr. 2009 (09.04.2009)Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451Authorized officer
LI Zhenhua
Telephone No. (86-10)62411495

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2008/073868

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101267668A	17.09.2008	NONE	
CN101257723A	03.09.2008	NONE	
CN1905734A	31.01.2007	NONE	
CN101102600A	09.01.2008	NONE	
WO2007125486A2	08.11.2007	WO2007125486A3	06.03.2008
		EP2016522A	21.01.2009

国际检索报告

国际申请号

PCT/CN2008/073868

A. 主题的分类

H04L9/32 (2009.01) i

按照国际专利分类表(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)

IPC: H04L H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI: 密钥 生成 根 移动管理 实体 切换 基站 节点 参数 演进 网络 接入 目标

WPI, EPODOC, PAJ: key, generat+, creat+, root, mobile, manag+, entity, switch+, handover, access, network, target, node, transmit+

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
P, X	CN101267668A (中兴通讯股份有限公司) 17.9 月 2008 (17.09.2008) 见说明书第 2 页 20 行-11 页 2 行, 图 1-7, 权利要求 1-10	1-10
P, X	CN101257723A (中兴通讯股份有限公司) 03.9 月 2008 (03.09.2008) 见说明书第 2 页 20 行-14 页 4 行, 图 1-8, 权利要求 1-10	1-10
A	CN1905734A (华为技术有限公司) 31.1 月 2007 (31.01.2007) 见全文	1-10
A	CN101102600A (中兴通讯股份有限公司) 09.1 月 2008 (09.01.2008) 见全文	1-10
A	WO2007125486A2 (KONINK PHILIPS ELECTRONICS NV) 08.11 月 2007 (08.11.2007) 见全文	1-10



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

“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

25.3 月 2009 (25.03.2009)

国际检索报告邮寄日期

09.4 月 2009 (09.04.2009)

中华人民共和国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

授权官员

李振华

电话号码: (86-10) **62411495**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2008/073868

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101267668A	17. 09. 2008	无	
CN101257723A	03. 09. 2008	无	
CN1905734A	31. 01. 2007	无	
CN101102600A	09. 01. 2008	无	
W02007125486A2	08. 11. 2007	W02007125486A3	06. 03. 2008
		EP2016522A	21. 01. 2009