

(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
2020 年 12 月 17 日 (17.12.2020)



(10) 国际公布号
WO 2020/248749 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

静 (HOU, Yunjing); 中国北京市海淀区学院路29号, Beijing 100083 (CN)。

(21) 国际申请号: PCT/CN2020/089289

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(22) 国际申请日: 2020 年 5 月 8 日 (08.05.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910503450.5 2019年6月11日 (11.06.2019) 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(71) 申请人: 大唐移动通信设备有限公司 (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) [CN/CN]; 中国北京市海淀区学院路29号, Beijing 100083 (CN)。

(72) 发明人: 毕晓宇 (BI, Xiaoyu); 中国北京市海淀区学院路29号, Beijing 100083 (CN)。 侯云

(54) Title: KEY UPDATE METHOD AND DEVICE

(54) 发明名称: 密钥更新方法及装置

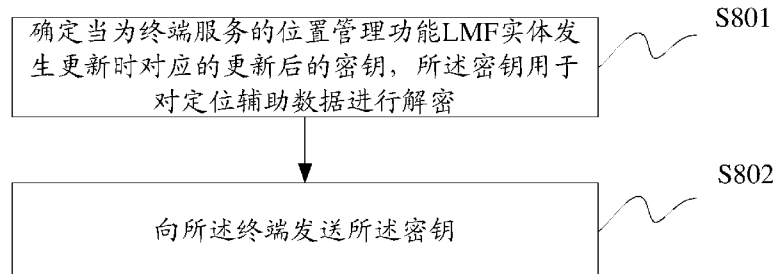


图 8

S801 Determine a corresponding updated key when updating a Location Management Function (LMF) entity serving a terminal, the key being used for decrypting positioning assistance data
S802 Send the key to the terminal

(57) Abstract: Disclosed are a key update method and device, for providing a solution how to update a key for decrypting positioning assistance data when a Location Management Function (LMF) entity serving a terminal changes. The key update method provided in embodiments of the present application comprises: determining a corresponding updated key when updating the LMF entity serving the terminal, the key being used for decrypting the positioning assistance data; sending the key to the terminal.

(57) 摘要: 本申请公开了密钥更新方法及装置, 用以提供当为终端服务的 LMF 实体发生变更时, 用于对定位辅助数据进行解密的密钥如何更新的解决方案。本申请实施例提供的一种密钥更新方法包括: 确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥, 所述密钥用于对定位辅助数据进行解密; 向所述终端发送所述密钥。



WO 2020/248749 A1

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

密钥更新方法及装置

相关申请的交叉引用

本申请要求在2019年06月11日提交中国专利局、申请号为201910503450.5、
申请名称为“密钥更新方法及装置”的中国专利申请的优先权，其全部内容
5 通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及密钥更新方法及装置。

背景技术

支持定位服务的网络架构如图 1 所示，对图中主要的网络功能的介绍如下：

网关移动位置中心(Gateway Mobile Location Center, GMLC)：接收位置
服务 (LoCation Services, LCS) 客户端的定位请求的功能实体，触发定位过
15 程，并向 LCS 客户端返回用户设备 (User Equipment, UE) 位置。

统一数据管理功能 (Unified Data Management, UDM) 实体：存储 UE 的
信息的功能实体，例如签约信息，已建立协议数据单元 (Protocol Data Unit,
PDU) 会话的信息。

移动性管理功能 (Access and Mobility Management Function, AMF) 实体：
20 接入认证和跟踪 UE 的位置。

位置管理功能 (Location Management Function, LMF) 实体：获取 UE 的
位置。

定位辅助数据和加密密钥的下发主要涉及 LMF 实体、UDM 和 AMF 实体
等实体。其中 LMF 实体负责制定加密密钥和定位辅助数据。UDM 实体存储
25 UE 签约的辅助数据类型。AMF 实体接收 LMF 实体下发的辅助数据和密钥，
其中辅助数据将通过无线接入网 (Radio Access Network, RAN) 广播出去，

AMF 实体通过注册过程将密钥发送给 UE。当 UE 接收到密钥之后,可使用密钥对接收到的广播的辅助数据进行解密。

广播网络辅助数据的具体过程如图 2 所示,描述如下:

步骤 201、LMF 实体通过 AMF 通信 N1N2 消息传输消息 (Namf_Communication_N1N2MessageTransfer), 向 AMF 实体发送网络辅助数据 (Network Assistance Data)。

步骤 202、AMF 实体通过 N2 Transport, 向 5G 无线接入网 (NG-RAN) 发送网络辅助数据。

步骤 203、NG-RAN 通过广播消息 (Broadcast Message) 向 UE 发送网络辅助数据。

目前, LMF 实体变更流程支持服务 LMF 实体在 5G 核心网移动终端位置请求 (5th-Generation Core Network Mobile Terminated Location Request, 5GC-MT-LR) 流程中变更。目标 UE 的移动性可能导致原始服务 LMF 实体不适合的服务 AMF 实体的改变。例如, 服务 LMF 实体可以远离新服务 AMF 实体, 导致 AMF 实体到 LMF 实体信令的更高资源利用率, 或者 LMF 实体可以不配置用于 UE 的当前接入网络的信息 (例如, 小区数据库)。在这种情况下, 服务的 LMF 实体可能需要改变。

发明内容

本申请实施例提供了密钥更新方法及装置, 用以提供当为终端服务的 LMF 实体发生变更时, 用于对定位辅助数据进行解密的密钥如何更新的解决方案。

在网络侧, 例如在 LMF 实体侧, 本申请实施例提供的一种密钥更新方法包括:

确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥, 所述密钥用于对定位辅助数据进行解密;

向所述终端发送所述密钥。

通过该方法，确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；向所述终端发送所述密钥，提供了当为终端服务的 LMF 实体发生变更时，用于对定位辅助数据进行解密的密钥如何更新的解决方案，使得更新后的密钥可以发送给终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

在网络侧，例如在 AMF 实体侧，本申请实施例提供的一种密钥更新方法，包括：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

将所述密钥发送给所述终端。

通过该方法，接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；将所述密钥发送给所述终端，因此提供了当为终端服务的 LMF 实体发生变更时，用于对定位辅助数据进行解密的密钥如何更新的解决方案，使得更新后的密钥可以发送给终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

可选地，当通过非接入层 NAS 消息接收所述密钥时，该方法还包括对所述密钥进行管理并保存。

5 在终端侧，本申请实施例提供的一种密钥更新方法，包括：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存所述密钥。

10 通过该方法，接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；保存所述密钥，从而使得终端可以获取 LMF 实体发生更新后的密钥，即由当前为终端服务的最新的 LMF 实体产生的用于对定位辅助数据进行解密的密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

15 可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

在网络侧，例如在 LMF 实体侧，本申请实施例提供的一种密钥更新装置，包括：

20 存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

向所述终端发送所述密钥。

25 可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发

送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

5 可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

在网络侧，例如在 AMF 实体侧，本申请实施例提供的一种密钥更新装置，包括：

10 存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

将所述密钥发送给所述终端。

15 可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

20 可选地，当通过非接入层 NAS 消息接收所述密钥时，所述处理器还用于调用所述存储器中存储的程序指令，按照获得的程序执行：对所述密钥进行管理并保存。

在终端侧，本申请实施例提供的一种密钥更新装置，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

25 接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

5 可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

在网络侧，例如在 LMF 实体侧，本申请实施例提供的另一种密钥更新装置，包括：

确定单元，用于确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

10 发送单元，用于向所述终端发送所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

15 可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

20 可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

在网络侧，例如在 AMF 实体侧，本申请实施例提供的另一种密钥更新装置，包括：

接收单元，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

25 发送单元，用于将所述密钥发送给所述终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

可选地，当通过非接入层 NAS 消息接收所述密钥时，所述处理器还用于调用所述存储器中存储的程序指令，按照获得的程序执行：对所述密钥进行管理并保存。

在终端侧，本申请实施例提供的另一种密钥更新装置，包括：

接收单元，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存单元，用于保存所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

本申请另一实施例提供了一种计算设备，其包括存储器和处理器，其中，所述存储器用于存储程序指令，所述处理器用于调用所述存储器中存储的程序指令，按照获得的程序执行上述任一种方法。

本申请另一实施例提供了一种计算机存储介质，所述计算机存储介质存储有计算机可执行指令，所述计算机可执行指令用于使所述计算机执行上述任一种方法。

附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅是本申请的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为现有技术中支持定位服务的网络架构示意图；

图 2 为现有技术中广播网络辅助数据的具体过程示意图;

图 3 为本申请实施例提供的 LMF 变更流程示意图;

图 4 为本申请实施例提供的 LMF 变更流程示意图;

图 5 为本申请实施例提供的 LMF 变更流程示意图;

5 图 6 为本申请实施例提供的 LMF 变更流程示意图;

图 7 为本申请实施例提供的 LMF 变更流程示意图;

图 8 为本申请实施例提供的 LMF 实体侧的密钥更新方法的流程示意图;

图 9 为本申请实施例提供的 AMF 实体侧的密钥更新方法的流程示意图;

图 10 为本申请实施例提供的终端侧的密钥更新方法的流程示意图;

10 图 11 为本申请实施例提供的 LMF 实体侧的密钥更新装置的结构示意图;

图 12 为本申请实施例提供的 AMF 实体侧的密钥更新装置的结构示意图;

图 13 为本申请实施例提供的终端侧的密钥更新装置的结构示意图;

图 14 为本申请实施例提供的 LMF 实体侧的另一密钥更新装置的结构示意图;

15 图 15 为本申请实施例提供的 AMF 实体侧的另一密钥更新装置的结构示意图;

图 16 为本申请实施例提供的终端侧的另一密钥更新装置的结构示意图。

具体实施方式

20 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,并不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

在 5G 系统中当采用延迟 (deferred) 5GC-MT-LR 定位方法,UE 不会立即上报位置信息,当触发定位 (可能是事件触发的定位,或者可能是周期性的触发的定位)时,外部客户端向 GMLC 发起对目标用户的定位请求,GMLC 与 UDM 之间执行隐私验证,如果 UE 允许定位,则 GMLC 向 AMF 实体发送

25

定位请求。AMF 实体选择了一个 LMF 实体，UE 与 LMF 实体之间执行定位流程，其中，UE 可能需要从网络获取到 LMF 实体发送的定位辅助信息。此时由于 UE 的移动，AMF 实体为 UE 选择了一个新的 LMF 实体，参见图 3，具体包括如下步骤：

5 301.UE 触发了服务请求（UE Triggered Service Request）。

302.UE 向服务 AMF 实体发送包含事件报告消息的非接入层（Non-access stratum, NAS）传输消息。NAS 传输消息包括指示 LMF 1（更新前的原 LMF 实体）的标识符（Identity document, ID）和事件报告（Event Report）。

10 303.基于运营商配置和策略，AMF 实体可以评估并确定 LMF 1 不适合或不能支持当前 UE 接入网络或服务小区的位置，并且确定 LMF 2（更新后的目标 LMF 实体）是更合适的 LMF 实体。

15 304. AMF 实体向 LMF 1 调用 AMF 通信 N1 消息告知消息（Namf_Communication_N1MessageNotify）服务操作。服务操作包括在步骤 302 中接收的事件报告。如果 AMF 实体在步骤 303 中确定应该使用新的 LMF 2，则它也向 LMF 1 指示。

305.如果 AMF 实体在步骤 304 中没有指示新的 LMF 实体，则基于运营商配置和策略，LMF 1 可以评估并确定它不适合或不能支持当前 UE 接入网络或服务小区的位置并且确定 LMF 2 为是一个更合适的 LMF 实体。

20 306. LMF 1 向 LMF 2 调用 LMF 位置上下文传输（Nlmf_LocationContextTransfer）请求服务操作以提供 UE 的当前位置上下文，并包括在步骤 304 中接收的事件报告消息。服务操作包括 AMF 实体标识和 LMF 1 最初为周期性接收的信息或者所有信息。根据从 AMF 实体触发位置请求，或者根据此过程从早期服务的 LMF 实体触发位置请求。服务操作还可以包括事件报告的当前状态（例如，到目前为止从 UE 接收的事件报告的数量和/或到目前为止的事件报告的持续时间），并且可以包括 UE 的位置相关信息，
25 例如先前的位置估计。

307. LMF 2 通知 LMF 1 位置上下文传输操作结果

(Nlmf_LocationContextTransfer Response)。然后 LMF 1 释放该过程的所有资源。

308. LMF 2 向 AMF 实体调用 AMF 通信 N1N2 消息传输 (Nlmf_Communication_N1N2MessageTransfer) 服务操作, 以请求向 UE 传送事件报告确认 (Event Report Acknowledgment) 消息。事件报告确认指示 LMF 实体的改变并且包括指示 LMF 2 的标识符。

309. AMF 实体在 NAS 传输消息中将事件报告确认转发给 UE。AMF 实体还向 LMF 2 通知事件报告确认的交付结果。

310. 如果事件报告需要位置估计, 则 LMF 2 可以执行 UE 的定位过程 (UE Positioning Procedure) 确定 UE 位置。

5G 与 4G 不同, 在 5G 系统的 deferred 5GC-MT-LR 流程中, 定位的上下文保存在 LMF 实体中, 如果 LMF 实体负责产生辅助数据广播的密钥, 当 UE 的位置变化, 辅助数据也将发生变化 (辅助数据包含了 UE 的位置信息、小区的 ID 以及时序等信息)。

LMF 实体负责定位方式的选择, LMF 1 根据公共陆地移动网络 (Public Land Mobile Network, PLMN) 以及服务质量 (Quality of Service, QoS) 选择了几种定位方式, 并产生与此对应的密钥用于辅助数据的定位。LMF 1 会将之前的密钥传给 LMF 2, 用于后续向 UE 发送辅助数据时的加密。但存在这样的问题:

当 AMF 实体重选了 LMF 实体时, 由于辅助数据变化, 使用与之前的密钥进行加密将导致安全隐患, 需要 UE 与新的 LMF 实体之前建立新的密钥同步关系。否则, UE 在 LMF 2 的范围内, 将无法获得 LMF 实体发送的信息辅助信息用于 UE 的定位计算。

当选择了 LMF 2 之后, 有其他服务请求 UE 的定位, 且 LMF 1 根据服务的 QoS 以及 PLMN 选择了不同的定位方式, 而这些定位方式与之前 LMF 1 选择的定位方式不同, UE 没有新的密钥将无法获取到辅助数据而执行 UE 的定位。

综上所述，在 5G 系统中，NG-RAN 通过广播方式发送被加密的网络辅助数据，UE 根据从网络接收到的加密密钥对该数据进行解密。在 deferred 5GC-MT-LR 的流程中会涉及到 LMF 变更的问题，目前没有对该场景下密钥以及安全上下文的处理描述，因此，本申请实施例提供了密钥更新方法及装置，用以提供当为终端服务的 LMF 实体发生变更时，用于对定位辅助数据进行解密的密钥更新解决方案。

其中，方法和装置是基于同一申请构思的，由于方法和装置解决问题的原理相似，因此装置和方法的实施可以相互参见，重复之处不再赘述。

本申请实施例提供的技术方案可以适用于多种系统，尤其是 5G 系统。例如适用的系统可以是全球移动通讯（global system of mobile communication, GSM）系统、码分多址（code division multiple access, CDMA）系统、宽带码分多址（Wideband Code Division Multiple Access, WCDMA）、通用分组无线业务（general packet radio service, GPRS）系统、长期演进（long term evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、通用移动系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）系统、5G 系统以及 5G 新空口（New Radio, NR）系统等。这多种系统中均包括终端设备和网络设备。

本申请实施例涉及的终端设备，可以是指向用户提供语音和/或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。在不同的系统中，终端设备的名称可能也不相同，例如在 5G 系统中，终端设备可以称为 UE。无线终端设备可以经 RAN 与一个或多个核心网进行通信，无线终端设备可以是移动终端设备，如移动电话（或称为“蜂窝”电话）和具有移动终端设备的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。例如，个人通信业务（personal communication service, PCS）电话、无绳电话、会话发起协议（session initiated protocol, SIP）话机、无线本地环路

(wireless local loop, WLL)站、个人数字助理(personal digital assistant, PDA)
等设备。无线终端设备也可以称为系统、订户单元(subscriber unit)、订户站
(subscriber station)、移动站(mobile station)、移动台(mobile)、远程站(remote
station)、接入点(access point)、远程终端设备(remote terminal)、接入终端
5 设备(access terminal)、用户终端设备(user terminal)、用户代理(user agent)、
用户装置(user device)，本申请实施例中并不限定。

本申请实施例涉及的网络设备，可以为核心网设备，例如 LMF 实体和
AMF 实体。

下面结合说明书附图对本申请各个实施例进行详细描述。需要说明的是，
10 本申请实施例的展示顺序仅代表实施例的先后顺序，并不代表实施例所提供的
的技术方案的优劣。

需要说明的是，本申请实施例中，更新密钥的过程中可以更新密钥集信
息(即不仅可以下发更新后的密钥，还可以下发与更新后的密钥相关的信息
等)，密钥集信息可以包括密钥类型、密钥、有效期、密钥标识等信息。本申
15 请实施例中密钥及其相关的信息内容可以在非接入层(Non-Access Stratum,
NAS)消息中携带，此时 AMF 实体可见；也可以在长期演进定位协议(Long
Term Evolution Positioning Protocol, LPP)消息中携带，如事件报告(event report)
消息中携带，则 AMF 实体不可见。

实施例一、

20 参见图 4，需要在 LMF 实体变更时，网络直接通过 LMF 实体变更流程下
发更新的密钥给 UE，并指示 UE 变化，具体包括：

步骤 401 至步骤 406，同图 3 所示的 LMF 实体变更流程中步骤 301 至步
骤 306 的相关描述，在此不再赘述。

25 步骤 4X. LMF 2 收到 NLMF_LocationContextTransfer 请求服务操作后，
产生新的密钥(Key generation)。

步骤 407. 同图 3 所示的 LMF 实体变更流程中步骤 307。

步骤 408. LMF 2 将更新的密钥通过 NAS 消息发给 AMF 实体，该 NAS 消

息中携带密钥更新指示和/或新的密钥集 (key update indication and/or new key set)。

步骤 409.AMF 实体通过 NAS 消息,将 key update indication and/or new key set 发给 UE; 或者步骤 410.LMF 2 通过事件报告消息,将 key update indication and/or new key set 透传给 AMF 实体,AMF 实体通过 NAS 消息,将 key update indication and/or new key set 转发给 UE。

实施例二、

参见图 5,需要在 LMF 变更时,AMF 实体选择了新的 LMF 实体,AMF 实体作为密钥的申请方通过 LMF 1 向 LMF 2 请求密钥。具体流程如下:

步骤 501 至步骤 503,同图 3 所示 LMF 实体变更流程中的步骤 301 至步骤 303,在此不再赘述。

步骤 504、AMF 实体选择了新的 LMF 实体后,向源 LMF 实体转发密钥请求 (该请求中还可以包含密钥的类型)。

步骤 505、同图 3 所示的 LMF 实体变更流程中的步骤 305。

步骤 506、源 LMF 实体向目标 LMF 实体转发密钥请求 (该请求中还可以包含密钥的类型)。

步骤 5x. 目标 LMF 实体产生新的密钥。

步骤 507 至步骤 510,同实施例一中步骤 407 至步骤 410,在此不再赘述。

实施例三、

UE 在事件报告中携带密钥请求,具体流程参见图 6,包括:

步骤 601、同图 3 所示的 LMF 实体变更流程的步骤 301。

步骤 602、UE 在事件报告中携带密钥请求,还可以携带请求的密钥类型;

步骤 603 至步骤 610,同实施例二步骤 503 至步骤 510,在此不再赘述。

实施例四、

AMF 实体透传 (类似于 2G/3G 的方法),当 AMF 实体刚选择了新的 LMF 实体,又有新的服务发起定位,则需要基于 LPP 协议传输密钥。具体流程参见图 7,包括:

步骤 701 至步骤 705、同图 3 所示的 LMF 实体变更流程中所述的步骤 301 至步骤 305。

步骤 706、包括步骤 706a 和步骤 706b，即 LMF 2 通过下行定位消息下发密钥，该下行定位消息中携带 key update indication and/or new key set。

5 步骤 707 至步骤 710，同图 3 所示的 LMF 实体变更流程所述的步骤 306 至步骤 309。

需要说明的是，步骤 707 中，源 LMF 可以向目标 LMF 请求密钥，如果目标 LMF 已经通过下行的定位消息发送了更新的密钥，会在响应消息步骤 708-710 中携带密钥信息，如果请求的密钥类型与步骤 706 相同的密钥，则返回相同的密钥标识。

综上所述，在网络侧，例如在 LMF 实体侧，参见图 8，本申请实施例提供一种密钥更新方法包括：

S801、确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

15 S802、向所述终端发送所述密钥。

通过该方法，提供了当为终端服务的 LMF 实体发生变更时，用于对定位辅助数据进行解密的密钥如何更新的解决方案，使得更新后的密钥可以发送给终端。

20 可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

25 可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所

述终端发送所述密钥。

在网络侧，例如在 AMF 实体侧，参见图 9，本申请实施例提供的一种密钥更新方法，包括：

5 S901、接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

S902、将所述密钥发送给所述终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

10 可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

可选地，当通过非接入层 NAS 消息接收所述密钥时，该方法还包括对所述密钥进行管理并保存。

在终端侧，参见图 10，本申请实施例提供的一种密钥更新方法，包括：

15 S101、接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

S102、保存所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

20 可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

在网络侧，例如在核心网设备 LMF 实体侧，参见图 11，本申请实施例提供一种密钥更新装置，包括：

存储器 141，用于存储程序指令；

25 处理器 140，用于调用所述存储器 141 中存储的程序指令，按照获得的程序执行：

确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的

密钥，所述密钥用于对定位辅助数据进行解密；

向所述终端发送所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

5 可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

10 可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

收发机 142，用于在处理器 140 的控制下接收和发送数据。

其中，在图 11 中，总线架构可以包括任意数量的互联的总线和桥，具体
15 由处理器 140 代表的一个或多个处理器和存储器 141 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 142 可以是多个元件，即包括发送机和收发机，提供用于在传输介质上与各种其他装置通信的单元。
20 处理器 140 负责管理总线架构和通常的处理，存储器 141 可以存储处理器 140 在执行操作时所使用的数据。

处理器 140 可以是中央处理器（central processing unit，CPU）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field - Programmable Gate Array，FPGA）或复杂可编程逻辑器件（Complex
25 Programmable Logic Device，CPLD）。

在网络侧，例如在核心网设备 AMF 实体侧，参见图 12，本申请实施例提供的一种密钥更新装置，包括：

存储器 155，用于存储程序指令；

处理器 154，用于调用所述存储器 155 中存储的程序指令，按照获得的程序执行：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的
5 密钥，所述密钥用于对定位辅助数据进行解密；

将所述密钥发送给所述终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标
10 LMF 实体发送的所述密钥。

可选地，当通过非接入层 NAS 消息接收所述密钥时，所述处理器 154 还用于调用所述存储器 155 中存储的程序指令，按照获得的程序执行：对所述密钥进行管理并保存。

收发机 151，用于在处理器 154 的控制下接收和发送数据。

15 在图 12 中，总线架构（用总线 156 来代表），总线 156 可以包括任意数量的互联的总线和桥，总线 156 将包括由处理器 154 代表的一个或多个处理器和存储器 155 代表的存储器的各种电路链接在一起。总线 156 还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口 153
20 在总线 156 和收发机 151 之间提供接口。收发机 151 可以是一个元件，也可以是多个元件，比如多个接收器和发送器，提供用于在传输介质上与各种其他装置通信的单元。经处理器 154 处理的数据通过天线 152 在无线介质上进行传输，进一步，天线 152 还接收数据并将数据传送给处理器 154。

处理器 154 负责管理总线 156 和通常的处理，还可以提供各种功能，包
25 括定时，外围接口，电压调节、电源管理以及其他控制功能。而存储器 155 可以被用于存储处理器 154 在执行操作时所使用的数据。

可选的，处理器 154 可以是 CPU、ASIC、FPGA 或 CPLD。

在终端侧，参见图 13，本申请实施例提供的一种密钥更新装置，包括：

存储器 160，用于存储程序指令；

处理器 161，用于调用所述存储器 160 中存储的程序指令，按照获得的程序执行：

5 接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

10 可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

收发机 162，用于在处理器 161 的控制下接收和发送数据。

其中，在图 13 中，总线架构可以包括任意数量的互联的总线和桥，具体
15 由处理器 161 代表的一个或多个处理器和存储器 160 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机 162 可以是多个元件，即包括发送机和接收机，提供用于在传输介质上与各种其他装置通信的单元。
20 针对不同的用户设备，用户接口 163 还可以是能够外接内接需要设备的接口，连接的设备包括但不限于小键盘、显示器、扬声器、麦克风、操纵杆等。

处理器 161 负责管理总线架构和通常的处理，存储器 160 可以存储处理器 161 在执行操作时所使用的数据。

可选的，处理器 161 可以是 CPU、ASIC、FPGA 或 CPLD。

25 在网络侧，例如在 LMF 实体侧，参见图 14，本申请实施例提供的另一种密钥更新装置，包括：

确定单元 11，用于确定当为终端服务的位置管理功能 LMF 实体发生更新

时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

发送单元 12，用于向所述终端发送所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

5 可选地，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

可选地，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

10 可选地，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

可选地，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

在网络侧，例如在 AMF 实体侧，参见图 15，本申请实施例提供的另一种密钥更新装置，包括：

15 接收单元 21，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

发送单元 22，用于将所述密钥发送给所述终端。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

20 可选地，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

可选地，当通过非接入层 NAS 消息接收所述密钥时，所述发送单元 22 还用于：对所述密钥进行管理并保存。

在终端侧，参见图 16，本申请实施例提供的另一种密钥更新装置，包括：

25 接收单元 31，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存单元 32，用于保存所述密钥。

可选地，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

可选地，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

5 可选地，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

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

20 本申请实施例提供了一种计算设备，该计算设备具体可以为桌面计算机、便携式计算机、智能手机、平板电脑、个人数字助理（Personal Digital Assistant, PDA）等。该计算设备可以包括 CPU、存储器、输入/输出设备等，输入设备可以包括键盘、鼠标、触摸屏等，输出设备可以包括显示设备，如液晶显示器（Liquid Crystal Display, LCD）、阴极射线管（Cathode Ray Tube, CRT）等。

25 存储器可以包括只读存储器（ROM）和随机存取存储器（RAM），并向处理器提供存储器中存储的程序指令和数据。在本申请实施例中，存储器可

以用于存储本申请实施例提供的任一所述方法的程序。

处理器通过调用存储器存储的程序指令，处理器用于按照获得的程序指令执行本申请实施例提供的任一所述方法。

5 本申请实施例提供了一种计算机存储介质，用于储存为上述本申请实施例提供的装置所用的计算机程序指令，其包含用于执行上述本申请实施例提供的任一方法的程序。

所述计算机存储介质可以是计算机能够存取的任何可用介质或数据存储设备，包括但不限于磁性存储器（例如软盘、硬盘、磁带、磁光盘（magneto-optical, MO）等）、光学存储器（例如 CD、DVD、BD、HVD 等）、
10 以及半导体存储器（例如 ROM、EPROM、EEPROM、非易失性存储器（NAND FLASH）、固态硬盘（SSD））等。

本申请实施例提供的方法可以应用于终端设备，也可以应用于网络设备。

其中，终端设备也可称之为 UE、移动台（Mobile Station，简称为“MS”）、移动终端（Mobile Terminal）等，可选的，该终端可以具备经 RAN 与一个或多个核心网进行通信的能力，例如，终端可以是移动电话（或称为“蜂窝”电话）、
15 或具有移动性质的计算机等，例如，终端还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置。

所述网络设备可以为核心网设备。

上述方法处理流程可以用软件程序实现，该软件程序可以存储在存储介质中，当存储的软件程序被调用时，执行上述方法步骤。
20

综上所述，本申请实施例提供的技术方案中，更新后的密钥可以通过扩展 NAS 消息下发，也可以通过扩展 LPP 消息下发。具体地，

1、当 LMF 实体变更时，目标 LMF 实体向 AMF 实体发送密钥，AMF 实体通过 NAS/LPP 消息向 UE 发送新的密钥。通过 NAS 消息下发时，AMF 实体管理并保存密钥；通过 LPP 消息下发时，LPP 管理并保存密钥。
25

2、当 LMF 实体变更时，AMF 实体发送密钥申请，向更新后的目标 LMF 实体请求新的密钥，目标 LMF 实体通过 NAS 消息经 AMF 实体发给 UE。

3、UE 在事件上报的时候，携带密钥请求。当 LMF 实体变更时，UE 向网络发起服务请求，携带密钥请求及密钥类型，目标 LMF 实体收到对目标 UE 的定位请求，直接通过 NAS 或者 LPP 消息下发更新的密钥。如果 UE 通过 NAS 消息中携带密钥请求，则 AMF 实体可见，密钥返回时，通过 NAS 消息返回密钥；如果 UE 通过事件报告消息中携带密钥请求，则 AMF 实体不可见，只是透传，密钥返回时通过 LPP 消息返回。

4、在 LMF 实体发生变更时，目标 LMF 实体同时收到新的服务的即时定位请求，将通过下行定位消息将更新的密钥发给 UE。通过 NAS 消息下发时，AMF 实体对密钥可见；通过 LPP 消息下发时，AMF 实体对密钥不可见。

因此，本申请实施例提供的技术方案解决了 LMF 实体变更时密钥更新的相关问题。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、闪存存储器、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或

多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权利要求

1、一种密钥更新方法，其特征在于，该方法包括：

确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

5 向所述终端发送所述密钥。

2、根据权利要求 1 所述的方法，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

3、根据权利要求 1 或 2 所述的方法，其特征在于，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

4、根据权利要求 1 或 2 所述的方法，其特征在于，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

5、根据权利要求 1 或 2 所述的方法，其特征在于，当接收到所述终端的定位请求时，向所述终端发送所述密钥。

6、根据权利要求 1 或 2 所述的方法，其特征在于，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

7、一种密钥更新方法，其特征在于，该方法包括：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

将所述密钥发送给所述终端。

8、根据权利要求 7 所述的方法，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

9、根据权利要求 7 或 8 所述的方法，其特征在于，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

10、根据权利要求 7 所述的方法，其特征在于，当通过非接入层 NAS 消

息接收所述密钥时，该方法还包括对所述密钥进行管理并保存。

11、一种密钥更新方法，其特征在于，该方法包括：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

5 保存所述密钥。

12、根据权利要求 11 所述的方法，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

13、根据权利要求 11 或 12 所述的方法，其特征在于，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

14、根据权利要求 13 所述的方法，其特征在于，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

15、一种密钥更新装置，其特征在于，该装置包括：

存储器，用于存储程序指令；

15 处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

确定当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

向所述终端发送所述密钥。

16、根据权利要求 15 所述的装置，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

17、根据权利要求 15 或 16 所述的装置，其特征在于，通过更新后的目标 LMF 实体，向移动性管理功能 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

18、根据权利要求 15 或 16 所述的装置，其特征在于，当接收到移动性管理功能 AMF 实体发送的新的密钥请求时，向所述 AMF 实体发送所述密钥，通过所述 AMF 实体将所述密钥发送给所述终端。

19、根据权利要求 15 或 16 所述的装置，其特征在于，当接收到所述终

端的定位请求时，向所述终端发送所述密钥。

20、根据权利要求 15 或 16 所述的装置，其特征在于，当接收到新的服务的即时定位请求时，通过下行定位消息向所述终端发送所述密钥。

21、一种密钥更新装置，其特征在于，该装置包括：

5 存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

将所述密钥发送给所述终端。

10 22、根据权利要求 21 所述的装置，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，向所述终端发送所述密钥。

23、根据权利要求 21 或 22 所述的装置，其特征在于，向更新后的目标 LMF 实体发送新的密钥请求后，接收所述目标 LMF 实体发送的所述密钥。

15 24、根据权利要求 21 所述的装置，其特征在于，当通过非接入层 NAS 消息接收所述密钥时，所述处理器还用于调用所述存储器中存储的程序指令，按照获得的程序执行：对所述密钥进行管理并保存。

25、一种密钥更新装置，其特征在于，该装置包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行：

20 接收当为终端服务的位置管理功能 LMF 实体发生更新时对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；

保存所述密钥。

26、根据权利要求 25 所述的装置，其特征在于，通过非接入层 NAS 消息或者长期演进定位协议 LPP 消息，接收所述密钥。

25 27、根据权利要求 25 或 26 所述的装置，其特征在于，向网络侧发送服务请求消息后，接收所述密钥，所述服务请求消息中包括密钥请求和密钥类型信息。

28、根据权利要求 27 所述的装置，其特征在于，所述服务请求消息为非接入层 NAS 消息，或者为事件报告消息。

29、一种密钥更新装置，其特征在于，该装置包括：

确定单元，用于确定当为终端服务的位置管理功能 LMF 实体发生更新时
5 对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；
发送单元，用于向所述终端发送所述密钥。

30、一种密钥更新装置，其特征在于，该装置包括：

接收单元，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时
对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；
10 发送单元，用于将所述密钥发送给所述终端。

31、一种密钥更新装置，其特征在于，该装置包括：

接收单元，用于接收当为终端服务的位置管理功能 LMF 实体发生更新时
对应的更新后的密钥，所述密钥用于对定位辅助数据进行解密；
保存单元，用于保存所述密钥。

15 32、一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机可执行指令，所述计算机可执行指令用于使所述计算机执行权利要求 1 至 14 任一项所述的方法。

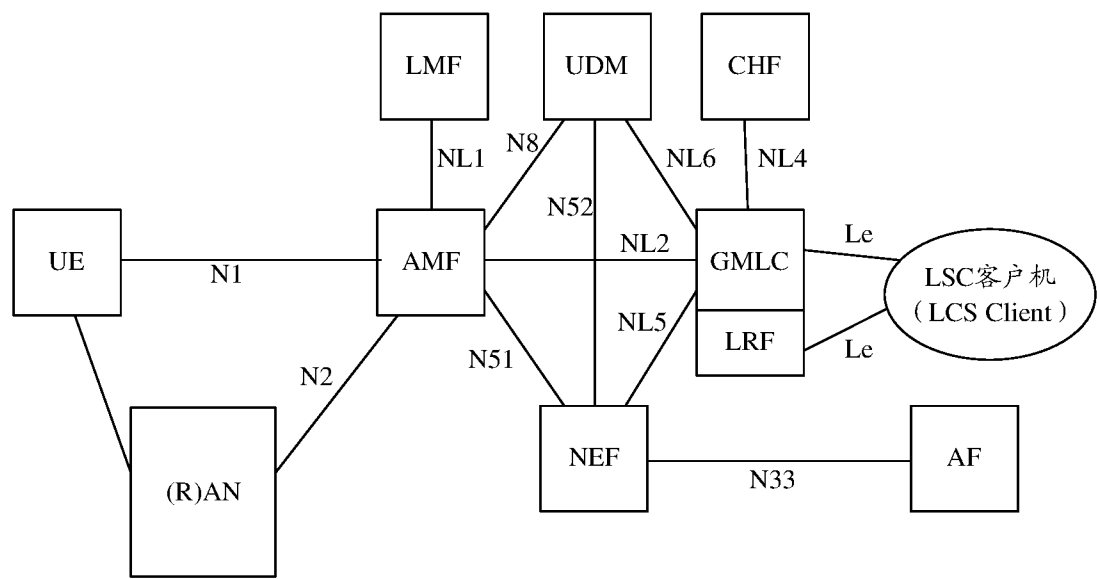


图 1

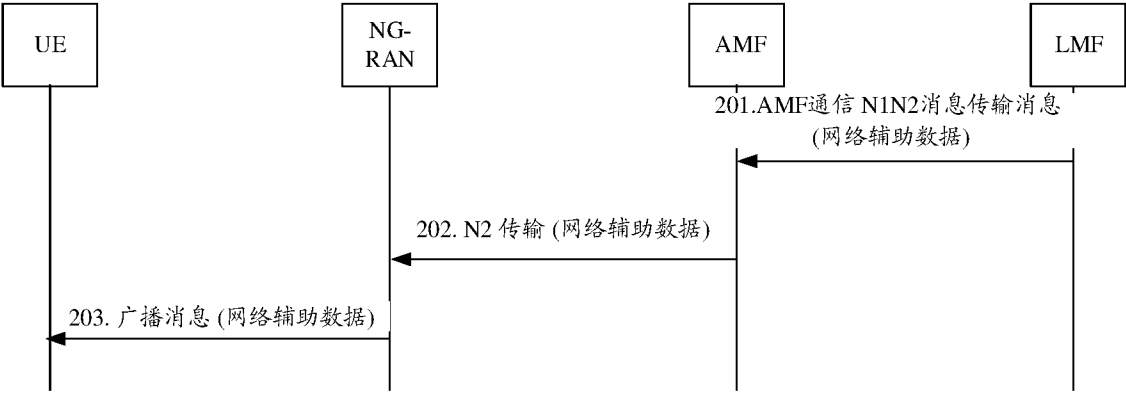


图 2

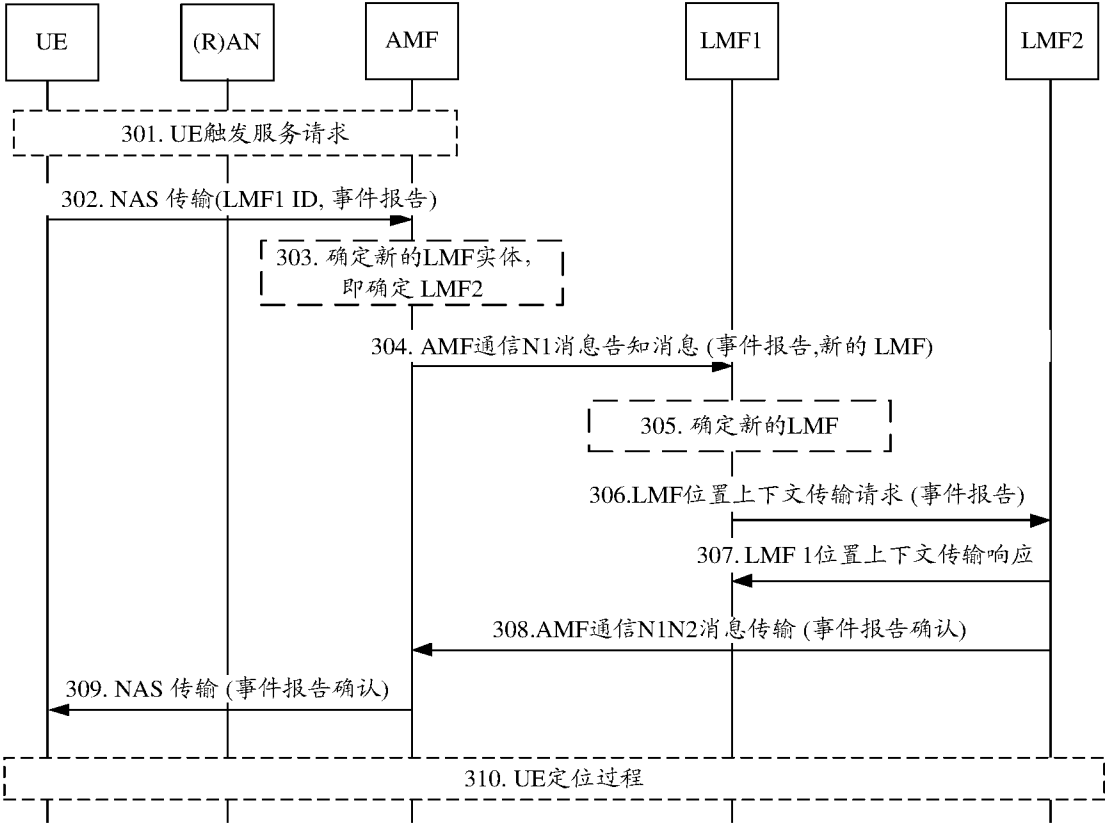


图 3

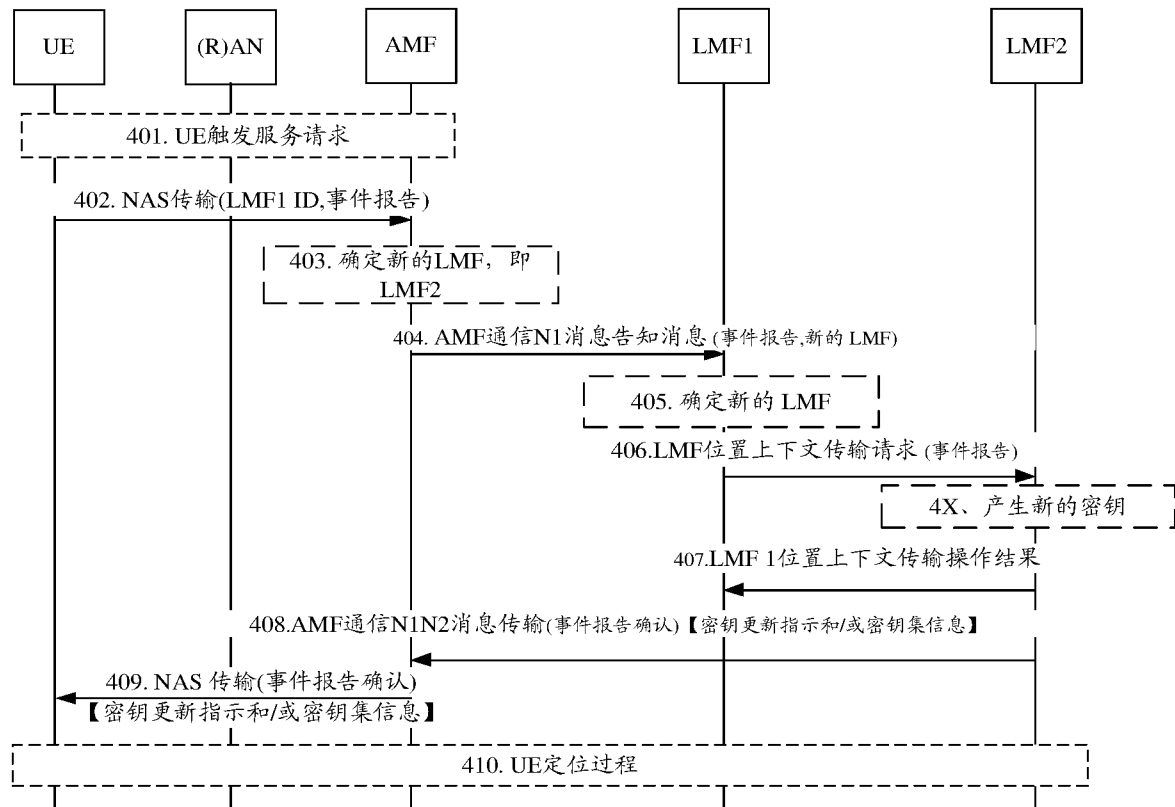


图 4

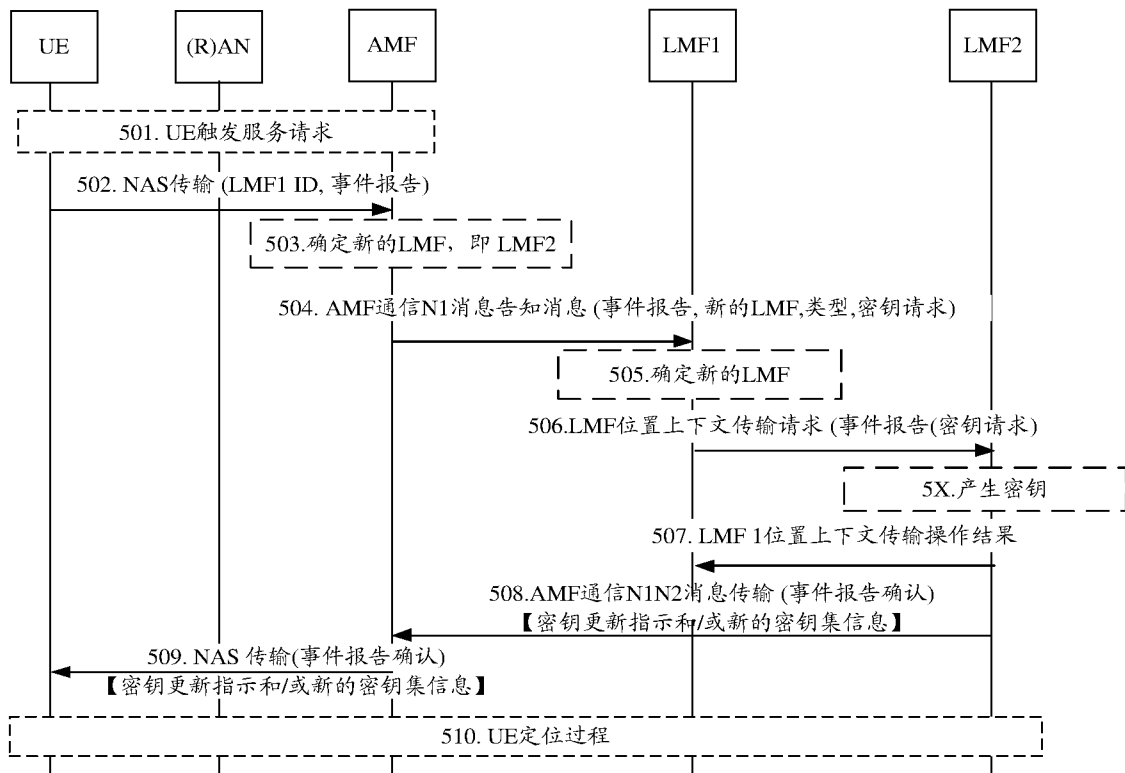


图 5

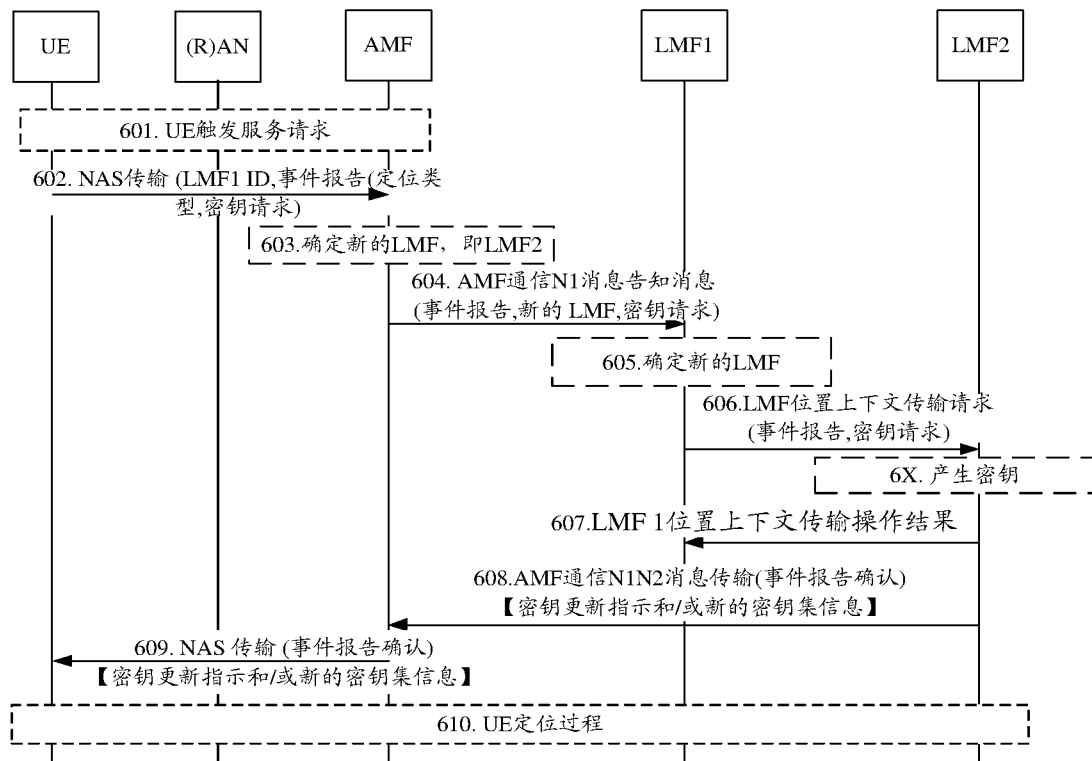


图 6

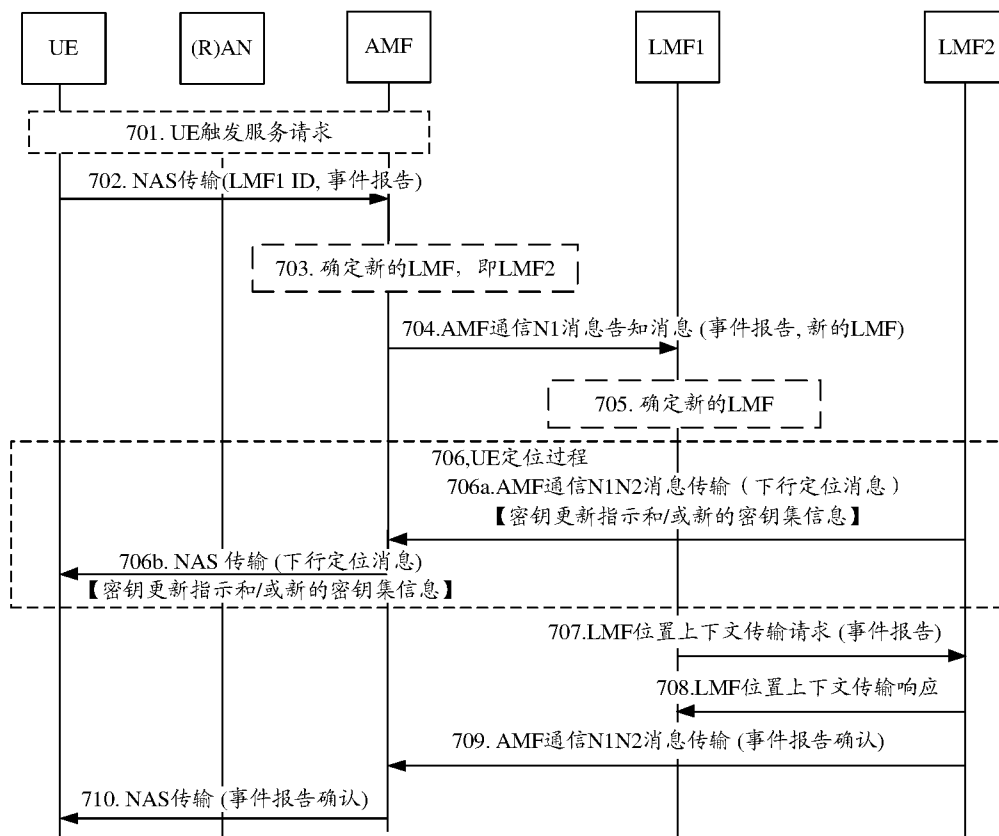


图 7

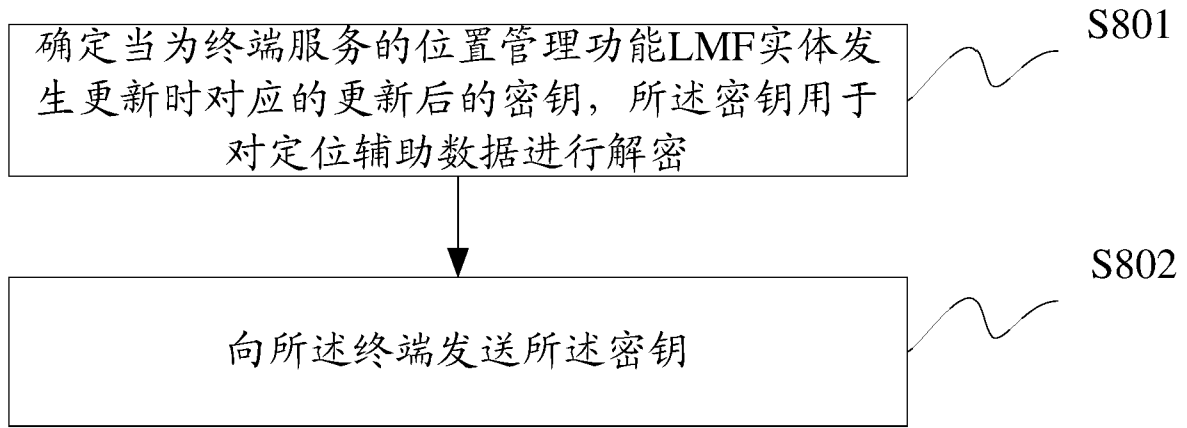


图 8

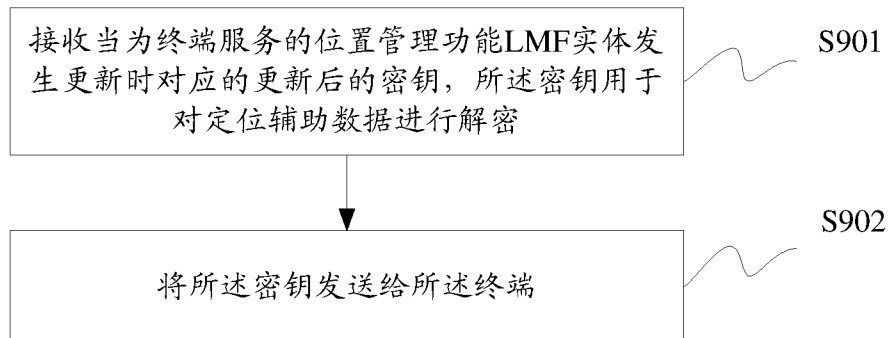


图 9

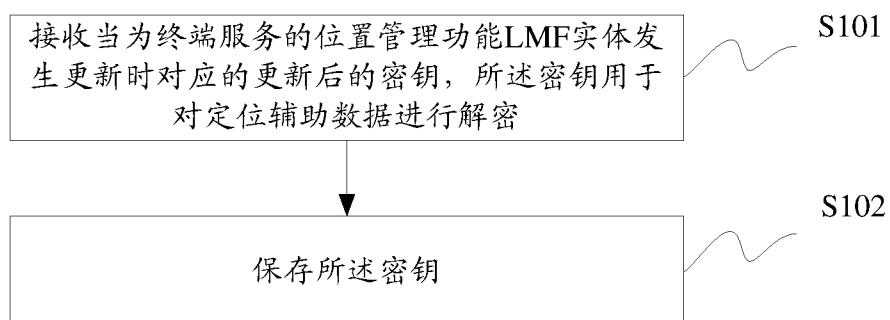


图 10

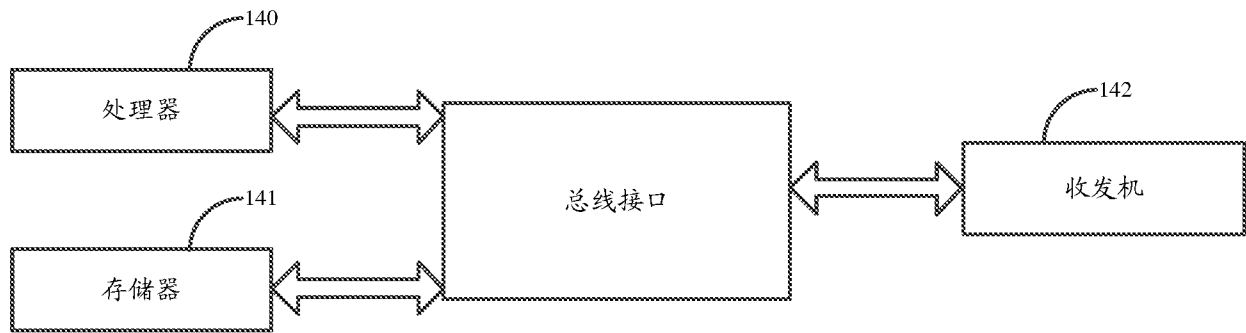


图 11

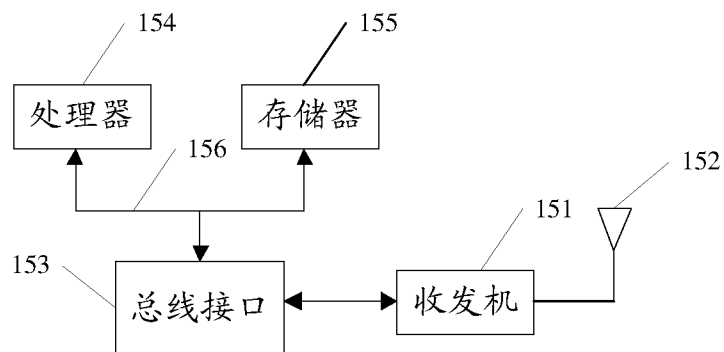


图 12

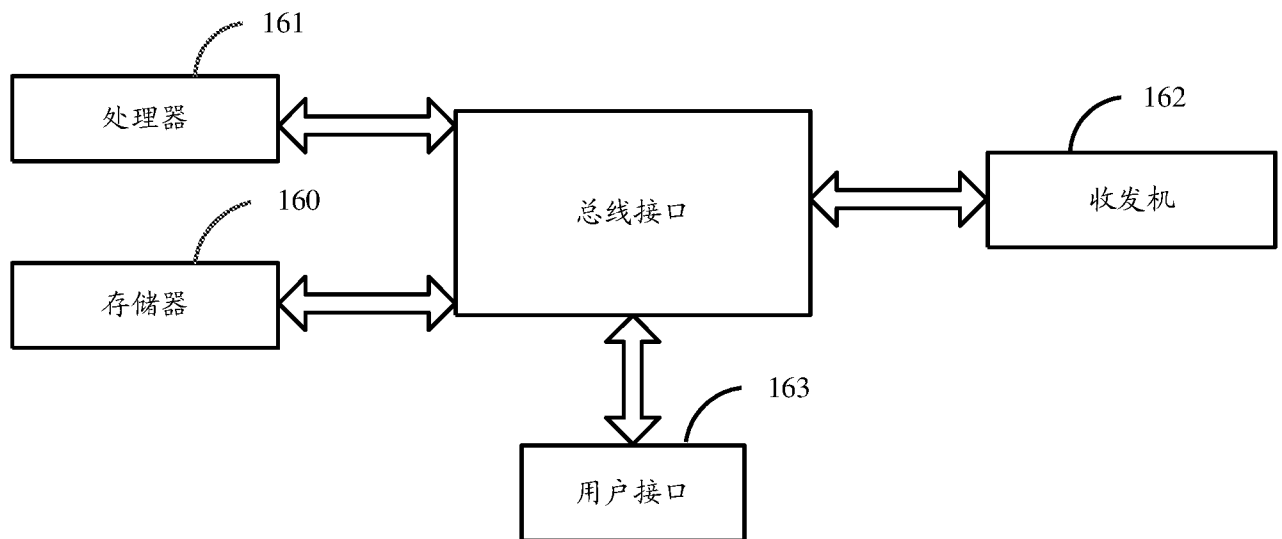


图 13

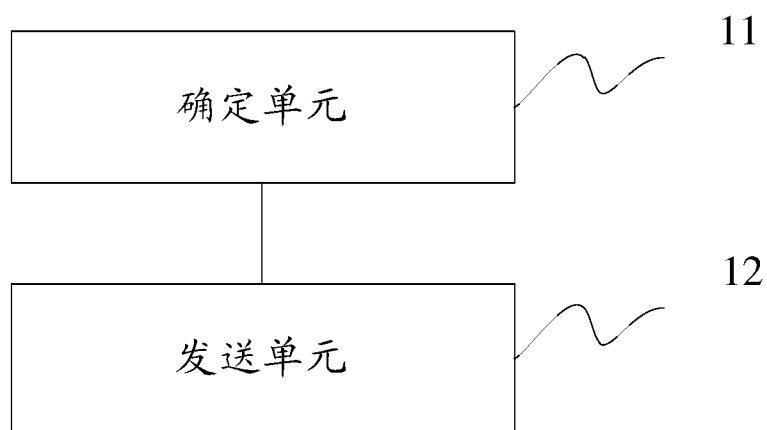


图 14

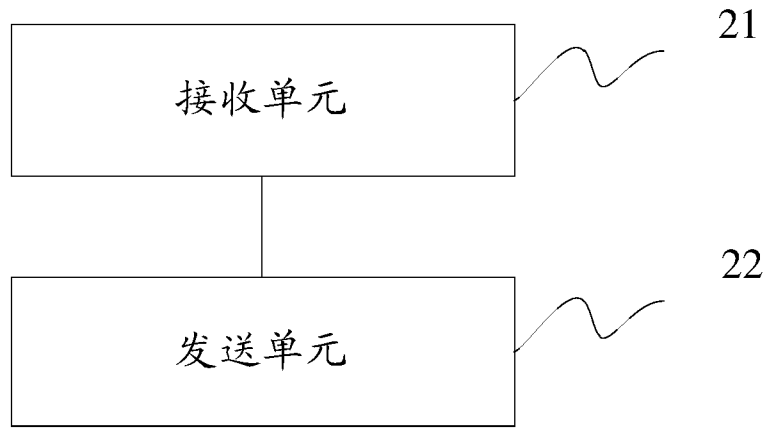


图 15

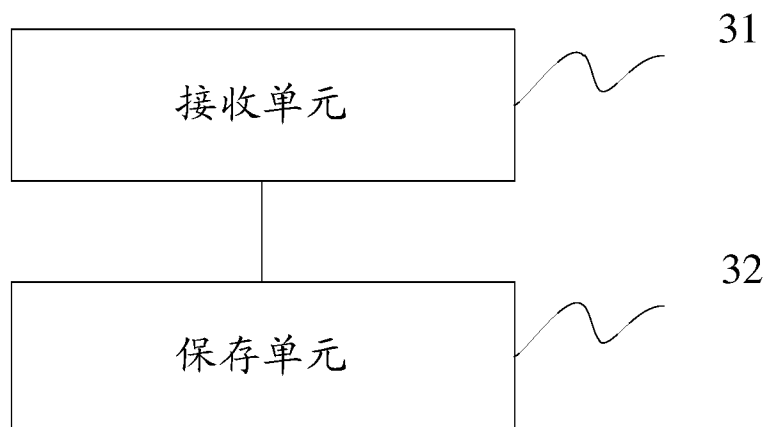


图 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/089289

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(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

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)

3GPP; VEN; CNABS; CNTXT; USTXT; EPTXT; WOTXT; CNKI: 位置管理功能, 移动性管理功能, 更新, 改变, 变更, 新, 密钥, LMF, AMF, update, change, new, ciphering key?, key?, generat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CATT. "Ciphering Keys Update During LMF Change" <i>3GPP TSG-SA WG2 Meeting #134 S2-1907555</i> , 18 June 2019 (2019-06-18), pp. 1-3	1-32
PX	CATT. "PCR to TR33.814 - The Solution for the Ciphering Key Management of Broadcast Assistance Data" <i>3GPP TSG SA WG3 (Security) Meeting #95-Bis S3-191965</i> , 17 June 2019 (2019-06-17), p. 1	1-32
X	HUAWEI et al. "Solution on Key Updating for Broadcast Assistant Data Protection" <i>3GPP TSG-SA WG3 (Security) Meeting #94 ad-hoc S3-190718</i> , 04 March 2019 (2019-03-04), pp. 1-3	1-32
A	QUALCOMM INC. "Addition of LMF Change Procedure for TS 23.273" <i>3GPP TSG-SA WG2 Meeting #131 S2-1902227</i> , 28 February 2019 (2019-02-28), entire document	1-32
A	WO 2019083596 A1 (QUALCOMM INCORPORATED) 02 May 2019 (2019-05-02) entire document	1-32

☐ 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

29 June 2020

Date of mailing of the international search report

30 July 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2020/089289

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2019083596	A1	02 May 2019	US	10080098	B1	18 September 2018
				CN	111213412	A	29 May 2020

国际检索报告

国际申请号

PCT/CN2020/089289

A. 主题的分类 H04L 9/08 (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 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)) 3GPP; VEN; CNABS; CNTXT; USTXT; EPTXT; WOTXT; CNKI: 位置管理功能, 移动性管理功能, 更新, 改变, 变更, 新, 密钥, LMF, AMF, update, change, new, ciphering key?, key?, generat+																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CATT. "Ciphering Keys Update During LMF Change" 3GPP TSG-SA WG2 Meeting #134 S2-1907555, 2019年 6月 18日 (2019 - 06 - 18), 第1-3页</td> <td>1-32</td> </tr> <tr> <td>PX</td> <td>CATT. "PCR to TR33.814 - The Solution for the Ciphering Key Management of Broadcast Assistance Data" 3GPP TSG SA WG3 (Security) Meeting #95-Bis S3-191965, 2019年 6月 17日 (2019 - 06 - 17), 第1页</td> <td>1-32</td> </tr> <tr> <td>X</td> <td>HUAWEI 等. "Solution on Key Updating for Broadcast Assistant Data Protection" 3GPP TSG-SA WG3 (Security) Meeting #94 ad-hoc S3-190718, 2019年 3月 4日 (2019 - 03 - 04), 第1-3页</td> <td>1-32</td> </tr> <tr> <td>A</td> <td>QUALCOMM INCORPORATED. "Addition of LMF Change Procedure for TS 23.273" 3GPP TSG-SA WG2 Meeting #131 S2-1902227, 2019年 2月 28日 (2019 - 02 - 28), 全文</td> <td>1-32</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CATT. "Ciphering Keys Update During LMF Change" 3GPP TSG-SA WG2 Meeting #134 S2-1907555, 2019年 6月 18日 (2019 - 06 - 18), 第1-3页	1-32	PX	CATT. "PCR to TR33.814 - The Solution for the Ciphering Key Management of Broadcast Assistance Data" 3GPP TSG SA WG3 (Security) Meeting #95-Bis S3-191965, 2019年 6月 17日 (2019 - 06 - 17), 第1页	1-32	X	HUAWEI 等. "Solution on Key Updating for Broadcast Assistant Data Protection" 3GPP TSG-SA WG3 (Security) Meeting #94 ad-hoc S3-190718, 2019年 3月 4日 (2019 - 03 - 04), 第1-3页	1-32	A	QUALCOMM INCORPORATED. "Addition of LMF Change Procedure for TS 23.273" 3GPP TSG-SA WG2 Meeting #131 S2-1902227, 2019年 2月 28日 (2019 - 02 - 28), 全文	1-32
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	CATT. "Ciphering Keys Update During LMF Change" 3GPP TSG-SA WG2 Meeting #134 S2-1907555, 2019年 6月 18日 (2019 - 06 - 18), 第1-3页	1-32															
PX	CATT. "PCR to TR33.814 - The Solution for the Ciphering Key Management of Broadcast Assistance Data" 3GPP TSG SA WG3 (Security) Meeting #95-Bis S3-191965, 2019年 6月 17日 (2019 - 06 - 17), 第1页	1-32															
X	HUAWEI 等. "Solution on Key Updating for Broadcast Assistant Data Protection" 3GPP TSG-SA WG3 (Security) Meeting #94 ad-hoc S3-190718, 2019年 3月 4日 (2019 - 03 - 04), 第1-3页	1-32															
A	QUALCOMM INCORPORATED. "Addition of LMF Change Procedure for TS 23.273" 3GPP TSG-SA WG2 Meeting #131 S2-1902227, 2019年 2月 28日 (2019 - 02 - 28), 全文	1-32															
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 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 </td> <td> "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 </td> </tr> </table>			* 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													
* 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 2020年 6月 29日		国际检索报告邮寄日期 2020年 7月 30日															
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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		受权官员 郝玉香 电话号码 (86-512)88996092															

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	W0 2019083596 A1 (QUALCOMM INC) 2019年 5月 2日 (2019 - 05 - 02) 全文	1-32

国际申请号
PCT/CN2020/089289

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)
W0	2019083596	A1	2019年 5月 2日	US	10080098	B1	2018年 9月 18日
				CN	111213412	A	2020年 5月 29日