

(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
2024 年 1 月 4 日 (04.01.2024)



(10) 国际公布号
WO 2024/001086 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) **H04L 101/659** (2022.01)
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2022/140617

(22) 国际申请日: 2022 年 12 月 21 日 (21.12.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210745225.4 2022年6月27日 (27.06.2022) CN

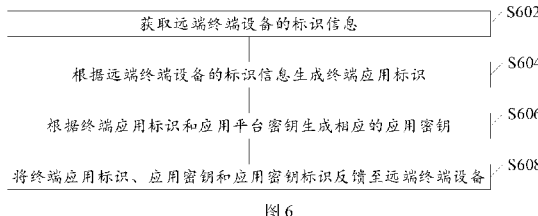
(71) 申请人: 中国电信股份有限公司(CHINA TELECOM CORPORATION LIMITED) [CN/CN]; 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(72) 发明人: 林奕琳(LIN, Yilin); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。刘洁(LIU, Jie); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。朱红梅(ZHU, Hongmei); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。何宇锋(HE, Yufeng); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。陈思柏(CHEN, Sibai); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。毕奇(BI, Qi); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(74) 代理人: 北京律智知识产权代理有限公司(BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路5号B1605、B1606、B1607, Beijing 100101 (CN)。

(54) Title: DATA COMMUNICATION METHOD AND APPARATUS BASED ON SHARED KEY, DEVICE, AND MEDIUM

(54) 发明名称: 一种基于共享密钥进行数据通信的方法、装置、设备和介质



S602 Obtain identification information of a remote user equipment
S604 Generate a terminal application identifier according to the identification information of the remote user equipment
S606 Generate a corresponding application key according to the terminal application identifier and an application platform key
S608 Feed back the terminal application identifier, the application key, and an application key identifier to the remote user equipment

(57) Abstract: The present disclosure provides a data communication method and apparatus based on a shared key, a device, and a medium. The method comprises: obtaining identification information of a remote user equipment (UE); generating a terminal application identifier according to the identification information of the remote UE; generating a corresponding application key according to the terminal application identifier and an application platform key; and feeding back the terminal application identifier, the application key, and an application key identifier to the remote UE, wherein the remote UE is configured to send the application key identifier and the terminal application identifier to a relay application management platform by means of an application session request, so that the relay application management platform is configured to generate the corresponding application key according to the terminal application identifier and the application platform key, and a terminal and the relay application management platform perform data communication on the basis of the application key. By means of the embodiments of the present disclosure, on the premise that a core network does not need to be upgraded and transformed, a secure communication requirement between the remote UE and the application management platform is satisfied, and application scenarios of near-field communication are extended.

(57) 摘要: 本公开提供一种基于共享密钥进行数据通信的方法、装置、设备和介质, 其中, 方法包括: 获取远端终端设备的标识信息; 根据远端终端设备的标识信息生成终端应用标识; 根据终端应用标识和应用平台密钥生成相应的应用密钥; 将终端应用标识、应用密钥和应用密钥标识反馈至远端终端设备, 远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识, 以供中继应用管理平台被配置为能够根据终端应用标识和应用平台密钥生成相应的应用密钥, 终端与中继应用管理平台基于应用密钥进行数据通信。通过本公开实施例, 在不需要对核心网做升级改造的前提下, 满足了远端UE与应用管理平台的安全通信需求, 扩展了在近域通信的应用场景。

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

一种基于共享密钥进行数据通信的方法、装置、设备和介质

本公开要求于 2022 年 06 月 27 日提交的申请号为 202210745225.4、名称为“基于共享密钥进行数据通信的方法、装置、设备和介质”的中国专利申请的优先权，该中国专利
5 申请的全部内容通过引用全部并入本文。

技术领域

公开涉及通信技术领域，具体而言，涉及一种基于共享密钥进行数据通信的方法、装置、设备和介质。

背景技术

目前，3GPP 在 5G 系统中引入了 AKMA (authentication and key management for applications 应用层认证和密钥管理)机制。

在相关技术中，可以基于终端在初次网络认证及密钥协商过程中生成的与网络之间的
15 共享密钥（记作 K_{AUSF} ），并为应用生成 APP 端与应用后台之间的共享密钥 K_{AF} 。

但是，在某些近域通信场景下，当远端 UE（User Equipment，终端设备）通过中继 UE 中转接入移动核心网使用数据业务的情况时，远端 UE 与应用平台之间无法直接利用 AKMA 机制生成应用层的共享密钥。

需要说明的是，在上述背景技术部分公开的信息仅用于加强对本公开的背景的理解，
20 因此可以包括不构成对本领域普通技术人员已知的现有技术的信息。

发明内容

本公开的目的在于提供一种基于共享密钥进行数据通信的方法、装置、设备和介质，
25 用于至少在一定程度上克服由于相关技术的限制和缺陷而导致的远端 UE 与应用平台之间的通信可靠性差的问题。

根据本公开实施例的第一方面，提供一种基于共享密钥进行数据通信的方法，包括：
获取远端终端设备的标识信息；根据所述远端终端设备的标识信息生成终端应用标识；根据
所述终端应用标识和应用平台密钥生成相应的应用密钥；将所述终端应用标识、所述应用
30 密钥和所述应用密钥标识反馈至远端终端设备，所述远端终端设备被配置为通过应用会话
请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供所述中继应用管理平台
被配置为能够根据所述终端应用标识和应用平台密钥生成相应的应用密钥，所述远端终端
设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

在本公开的一种示例性实施例中，在获取远端终端设备的标识信息前，还包括：通过
与应用层进行主认证并生成锚点密钥；基于所述锚点密钥生成应用平台密钥和所述应用密
35 钥标识；请求与所述中继应用管理平台建立应用会话；向所述中继应用管理平台发送所述

应用密钥标识,所述中继应用管理平台被配置为向应用层认证和密钥管理锚点功能发送所述应用密钥标识和应用平台标识,所述应用层认证和密钥管理锚点功能被配置为根据所述锚点密钥确定所述应用平台密钥,并将所述应用平台密钥、所述应用平台密钥的有效期和终端通用公共用户标识反馈至所述中继应用管理平台;通过共享的所述应用平台密钥与所述中继应用管理平台进行数据通信。

在本公开的一种示例性实施例中,根据终端应用标识和应用平台密钥生成相应的应用密钥包括:将所述终端应用标识和所述应用平台密钥代入密钥导出函数进行计算;根据所述密钥导出函数确定相应的应用密钥。

在本公开的一种示例性实施例中,所述密钥导出函数的表达式包括: $K-APP = HMAC-SHA-256(K_{AF}, S)$; $S = FC \parallel P0 \parallel L0$, 其中,所述 $HMAC-SHA-256(K_{AF}, S)$ 表征以所述 K_{AF} 和所述 S 为参数的密钥导出函数,所述 K_{AF} 表征所述应用平台密钥,所述 $K-APP$ 表征所述应用密钥,所述 S 表征中间参数,所述 FC 表征 3GPP 的保留字段,所述 $P0$ 表征所述终端应用标识,所述 $L0$ 表征所述终端应用标识的字符长度。

在本公开的一种示例性实施例中,还包括:获取远端终端设备的通信标识符;根据所述通信标识符生成 IPv6 接口标识,并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息;将所述 IPv6 接口标识分配至对应的远端终端设备。

在本公开的一种示例性实施例中,还包括:获取远端终端设备的通信标识符;根据所述通信标识符生成 IPv6 接口标识,并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息;响应于接收到的所述远端终端设备的数据流,采用生成的 IPv6 接口标识替换所述数据流中的 IPv6 接口标识。

在本公开的一种示例性实施例中,所述通信标识符包括 MSISDN、GPSI、IMSI、SUPI、MAC 地址中的至少一种。

根据本公开实施例的第二方面,提供一种基于共享密钥进行数据通信的装置,包括:获取模块,设置为获取远端终端设备的标识信息;生成模块,设置为根据所述远端终端设备的标识信息生成终端应用标识;所述生成模块,设置为根据所述终端应用标识和应用平台密钥生成相应的应用密钥;交互模块,设置为将所述终端应用标识、所述应用密钥和所述应用密钥标识反馈至远端终端设备,所述远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识,以供所述中继应用管理平台被配置为能够根据所述终端应用标识和应用平台密钥生成相应的应用密钥,所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

根据本公开的第三方面,提供一种电子设备,包括:存储器;以及耦合到所述存储器的处理器,所述处理器被配置为基于存储在所述存储器中的指令,执行如上述任意一项所述的方法。

根据本公开的第四方面,提供一种计算机可读存储介质,其上存储有程序,该程序被处理器执行时实现如上述任意一项所述的基于共享密钥进行数据通信的方法。

本公开实施例，通过获取远端终端设备的标识信息，并根据远端终端设备的标识信息生成终端应用标识，进而根据终端应用标识和应用平台密钥生成相应的应用密钥，最终将终端应用标识、应用密钥和应用密钥标识反馈至远端终端设备，远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供中继应用管理平台被配置为能够根据终端应用标识和应用平台密钥生成相应的应用密钥，远端终端设备与中继应用管理平台基于应用密钥进行数据通信，在不需要对核心网做升级改造的前提下，满足了远端 UE 与应用管理平台的安全通信需求，扩展了在近域通信的应用场景。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

图 1 示出了可以应用本发明实施例的基于共享密钥进行数据通信的方案的示例性系统架构的示意图；

图 2 是本公开示例性实施例中应用于外部应用平台 AF 的 3GPP 应用层认证及密钥管理架构的示意图；

图 3 是本公开示例性实施例中认证及密钥协商过程的示意图；

图 4 是本公开示例性实施例中基于共享密钥进行数据通信的交互示意图；

图 5 是本公开示例性实施例中应用层密钥推导过程的交互示意图；

图 6 是本公开示例性实施例中一种基于共享密钥进行数据通信的方法的流程图；

图 7 是本公开示例性实施例中另一种基于共享密钥进行数据通信的方法的流程图；

图 8 是本公开示例性实施例中另一种基于共享密钥进行数据通信的方法的流程图；

图 9 是本公开示例性实施例中另一种基于共享密钥进行数据通信的方法的流程图；

图 10 是本公开示例性实施例中另一种基于共享密钥进行数据通信的方法的流程图；

图 11 示出了可以应用本发明实施例的一种应用层密钥推导过程的示意图；

图 12 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信方案的系统架构的示意图；

图 13 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信的方案的示意图；

图 14 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信交互过程的示意图；

图 15 是本公开示例性实施例中一种基于共享密钥进行数据通信的装置的方框图；

图 16 是本公开示例性实施例中一种电子设备的方框图。

具体实施方式

现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实

施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本公开将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施方式中。在下面的描述中，提供许多具体细节从而给出对本公开的实施方式的充分理解。然而，本领域技术人员将意识到，
5 可以实践本公开的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知技术方案以避免喧宾夺主而使得本公开的各方面变得模糊。

此外，附图仅为本公开的示意性图解，图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。附图中所示的一些方框图是功能实体，不一定必须与物理
10 或逻辑上独立的实体相对应。可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

图 1 示出了可以应用本发明实施例的基于共享密钥进行数据通信的方案的示例性系统架构的示意图。

15 如图 1 所示，系统架构 100 可以包括终端设备 101、102、103 中的一种或多种，网络 104 和服务器 105。网络 104 用以在终端设备 101、102、103 和服务器 105 之间提供通信链路的介质。网络 104 可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

应该理解，图 1 中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，
20 可以具有任意数目的终端设备、网络和服务器的数目。比如无线网络除了现有功能之外还可以有其它网络功能、服务器 105 可以是多个服务器组成的服务器集群等。

用户可以使用终端设备 101、102、103 通过网络 104 与服务器 105 交互，以接收或发送消息等。终端设备 101、102、103 可以是具有显示屏的各种电子设备，包括但不限于智能手机、平板电脑、便携式计算机和台式计算机等等。此处所述的终端设备，除了终端自
25 身的软硬件功能，也可以包含为实现上述功能的应用 APP 软件。

在一些实施例中，本发明实施例所提供的基于共享密钥进行数据通信的方法一般由通信网络中的网元执行，相应地，基于共享密钥进行数据通信的装置一般设置于网元中。

下面对本公开的实施例涉及的名词和概念进行说明。

UDM: Unified Data Management, 统一数据管理功能, 3GPP AKA 认证、用户识别、
30 访问授权、注册、移动、订阅、短信管理等。

AUSF: Authentication Server Function, 认证服务器功能, 实现 3GPP 和非 3GPP 的接入认证。

AMF: Access and Mobility Management Function, 接入和移动性管理功能, 执行注册、连接、可达性、移动性管理。

35 NEF: Network Exposure Function, 网络开放功能, 开放各 NF 的能力, 转换内外部信

息，也可用于边缘计算场景。

AF: Application Function, 应用功能, 各种应用平台。

UE: User Equipment, 用户设备, 指各种用户终端设备。

RAN: Radio Access Network, 无线接入网。

5 HPLMN: Home Public Land Mobile Network, 本地公用陆地移动网络。

ME: Mobile Equipment, 移动设备。

IPv6: Internet Protocol Version 6, 互联网协议第 6 版的缩写, 是互联网工程任务组设计的用于替代 IPv4 的下一代 IP 协议。

AAnf: 应用层认证和密钥管理锚点功能。

10 图 2 是本公开示例性实施例中应用于外部应用平台 AF 的 3GPP 应用层认证及密钥管理架构的示意图。

参考图 2, 应用于外部应用平台 AF 的 3GPP 应用层认证及密钥管理架构 200 包括 UDM、AUSF、AMF、RAN、NEF、UE、AF 和 AAnf, 并按照如图所示的方式进行应用层认证及密钥管理。

15 图 3 是本公开示例性实施例中认证及密钥协商过程的示意图。

参考图 3, 应用于内部应用平台 AF 的 3GPP 应用层认证及密钥管理架构 300 包括 UDM、AUSF、AMF、RAN、UE、AF 和 AAnf, 并按照如图 3 所示的方式进行应用层认证及密钥管理。

图 4 是本公开示例性实施例中基于共享密钥进行数据通信的交互示意图。

20 参考图 4, 基于共享密钥进行数据通信的交互过程 400 包括 HPLMN 和 Serving Network 两部分, 在 HPLMN 中确定 K_{AUSF} , 在 Serving Network 中根据 K_{SEAF} 确定 K_{AMF} , 并基于 K_{AMF} 确定 K_{N3IWF} 、 $K_{gNB,NH}$ 、 K_{NASint} 和 K_{NASenc} , 进而由 $K_{gNB,NH}$ 确定 K_{RRCint} 、 K_{RRCenc} 、 K_{UPint} 、 K_{UPenc} 。

图 5 是本公开示例性实施例中应用层密钥推导过程的交互示意图。

25 参考图 5, 应用层密钥推导过程 500 包括由 K_{AUSF} 确定 K_{AKMA} , 继而由 K_{AKMA} 确定 K_{AF} 这两个过程。

下面结合附图对本公开示例实施方式进行详细说明。

图 6 是本公开示例性实施例中基于共享密钥进行数据通信的方法的流程图。

参考图 6, 基于共享密钥进行数据通信的方法可以包括:

30 步骤 S602, 获取远端终端设备的标识信息。

步骤 S604, 根据所述远端终端设备的标识信息生成终端应用标识。

步骤 S606, 根据所述终端应用标识和应用平台密钥生成相应的应用密钥。

步骤 S608, 将所述终端应用标识、所述应用密钥和所述应用密钥标识反馈至远端终端设备, 所述远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识, 以供所述中继应用管理平台被配置为能够根据所述终端应用标识和

35

应用平台密钥生成相应的应用密钥,所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

本公开实施例,通过获取远端终端设备的标识信息,并根据远端终端设备的标识信息生成终端应用标识,进而根据终端应用标识和应用平台密钥生成相应的应用密钥,最终将终端应用标识、应用密钥和应用密钥标识反馈至远端终端设备,远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识,以供中继应用管理平台被配置为能够根据终端应用标识和应用平台密钥生成相应的应用密钥,远端终端设备与中继应用管理平台基于应用密钥进行数据通信,在不需要对核心网做升级改造的前提下,满足了远端 UE 与应用管理平台的安全通信需求,扩展了在近域通信的应用场景。

下面,对基于共享密钥进行数据通信的方法的各步骤进行详细说明。

在本公开的一种示例性实施例中,如图 7 所示,在获取远端终端设备的标识信息前,还包括:

步骤 S702,通过与应用层进行主认证并生成锚点密钥。

步骤 S704,基于所述锚点密钥生成应用平台密钥和所述应用密钥标识。

步骤 S706,请求与所述中继应用管理平台建立应用会话。

步骤 S708,向所述中继应用管理平台发送所述应用密钥标识,所述中继应用管理平台被配置为向应用层认证和密钥管理锚点功能发送所述应用密钥标识和应用平台标识,所述应用层认证和密钥管理锚点功能被配置为根据所述锚点密钥确定所述应用平台密钥,并将所述应用平台密钥、所述应用平台密钥的有效期和终端通用公共用户标识反馈至所述中继应用管理平台。

步骤 S710,通过共享的所述应用平台密钥与所述中继应用管理平台进行数据通信。

在本公开的一种示例性实施例中,如图 8 所示,根据终端应用标识和应用平台密钥生成相应的应用密钥包括:

步骤 S802,将所述终端应用标识和所述应用平台密钥代入密钥导出函数进行计算。

步骤 S804,根据所述密钥导出函数确定相应的应用密钥。

在本公开的一种示例性实施例中,所述密钥导出函数的表达式包括: $K-APP = HMAC-SHA-256(K_{AF}, S)$, $S = FC \parallel P0 \parallel L0$, 其中,所述 $HMAC-SHA-256(K_{AF}, S)$ 表征以所述 K_{AF} 和所述 S 为参数的密钥导出函数,所述 K_{AF} 表征所述应用平台密钥,所述 $K-APP$ 表征所述应用密钥,所述 S 表征中间参数,所述 FC 表征 3GPP 的保留字段,所述 $P0$ 表征所述终端应用标识 (UE-APP-ID),所述 $L0$ 表征所述终端应用标识的字符长度。

在上述实施例中,密钥导出函数的定义在 3GPP TS33.220 中有具体描述, 3GPP 引用了 IETF RFC 2104 中的"HMAC: Keyed-Hashing for Message Authentication"和 ISO/IEC 10118-3:2004 中的"Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions"。

在上述实施例中,上述参数表达式还可以采用以下方式:

FC: 可在 3GPP 保留的字段 0xF0-0xFE (0xF0 和 0xFE 均为十六进制) 中选取其一;
P0 = UE-APP-ID;

L0 = length of UE_APP_ID;

其中, UE-APP-ID=UE-ID||AF FQDN||Ua*安全协议 ID。

- 5 在上述实施例中, HMAC 是一种使用单向散列函数来构造消息认证码的方法, 其中 HMAC 中的 H 就是 Hash 的意思。

HMAC 中所使用的单向散列函数并不仅限于一种, 任何高强度的单向散列函数都可以被用于 HMAC, 如果将来设计出的新的单向散列函数, 也同样可以使用。

- 10 使用 SHA-1、SHA-224、SHA-256、SHA-384、SHA-512 所构造的 HMAC, 分别称为 HMAC-SHA1、HMAC-SHA-224、HMAC-SHA-384、HMAC-SHA-512。

HMAC 的计算步骤包括:

- 1、密钥填充: 如果密钥比单向散列函数分组长度要短, 就需要在末尾填充 0, 直到其长度达到单向散列函数的分组长度为止。如果密钥比分组长度要长, 则要用单向散列函数求出密钥的散列值, 然后将这个散列值用作 HMAC 的密钥。
- 15 2、填充后的密钥与 ipad 的 XOR: 将填充后的密钥与被称为 ipad 的比特序列进行 XOR 运算。ipad 是将 00110110 这一比特序列不断循环反复直到达到分组长度所形成的比特序列, 其中 ipad 的 i 是 inner 的意思。XOR 运算所得到的值, 就是一个和单向散列函数的分组长度相同, 且和密钥相关的比特序列。这里将这个比特序列称为 ipadkey。
- 20 3、与消息组合: 将 ipadkey 与消息组合, 也就是将和密钥相关的比特序列 (ipadkey) 附加在消息的开头。
- 4、计算散列值: 将 3 的结果输入单向散列函数, 并计算出散列值。
- 5、填充后的密钥与 opad 的 XOR: 将填充后的密钥与被称为 opad 的比特序列进行 XOR 运算, opad 是将 01011100 这一比特序列不断循环反复直到达到分组长度所形成的比特序列, 其中 opad 的 o 是 outer 的意思。XOR 运算所得到的结果也是一个和单向散列函数的分组长度相同, 且和密钥相关的比特序列。这里将这个比特序列称为 opadkey。
- 25 6、与散列值组合: 将 4 的散列值拼在 opadkey 后面。
- 7、计算散列值: 将 6 的结果输入单向散列函数, 并计算出散列值, 这个散列值就是最终的 MAC 值。通过上述流程可以看出, 最后得到的 MAC 值, 一定是一个和输入的消息以及密钥都相关的长度固定的比特序列。

- 30 在本公开的一种示例性实施例中, 如图 9 所示, 基于共享密钥进行数据通信的方法还包括:

步骤 S902, 获取远端终端设备的通信标识符。

步骤 S904, 根据所述通信标识符生成 IPv6 接口标识, 并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息。

- 35 步骤 S906, 将所述 IPv6 接口标识分配至对应的远端终端设备。

在上述实施例中，远端 UE 与中继 UE 完成认证后，中继 UE 需获取远端 UE 的 ID，此处远端 UE 的 ID 可以是 MSISDN/GPSI、IMSI/SUPI、MAC 地址等，中继 UE 可以在利用远端 UE ID 生成 IPv6 接口 ID 后，向远端 UE 分配该 IPv6 接口 ID。

在本公开的一种示例性实施例中，如图 10 所示，基于共享密钥进行数据通信的方法还包括：

步骤 S1002，获取远端终端设备的通信标识符。

步骤 S1004，根据所述通信标识符生成 IPv6 接口标识，并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息。

步骤 S1006，响应于接收到的所述远端终端设备的数据流，采用生成的 IPv6 接口标识替换所述数据流中的 IPv6 接口标识。

在上述实施例中，如果中继 UE 未向远端 UE 分配接口 ID，则需要在远端 UE 的数据流中，将源 IPv6 接口 ID 替换为利用远端 UE ID 生成的 IPv6 接口 ID。

在上述实施例中，在实现了所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信的同时，核心网需要将不同源 IPv6 接口 ID 的流量分别统计，分别生成流量记录，并发送给 IT 系统进行计费。

在本公开的一种示例性实施例中，所述通信标识符包括 MSISDN、GPSI、IMSI、SUPI、MAC 地址中的至少一种。

其中，IMSI 是国际移动用户识别码（International MobileSubscriber Identification Number）是区别移动用户的标志，储存在 SIM 卡的 EF-IMSI 文件中，可用于区别移动用户的有效信息。IMSI 是 SIM 卡的 id 号码，可以区分每一张 SIM 卡。IMSI 由一串十进制数字组成，最大长度为 15 位，实际使用的 IMSI 的长度绝大部分都是 15 位。

其中，MSISDN（MobileSubscriber International ISDN number）移动台国际用户识别码，即移动用户的 ISDN 号码，是在公共交换电话网交换网络编号计划中，唯一能识别移动用户的号码，俗称为手机号，MSISDN 号码其组成包含如下三个部分：

（1）CC：Country Code，国家码，中国的国家码为 86。

（2）NDC：National Destination Code，国内目的地码，也称网络接入码，由各个国家的通信主管部门分配给各个网络运营商。中国移动网络接入码为 134~139、150~152、188 等，中国联通为 130~132、185~186 等，中国电信为 133、153、180、189 等。

（3）SN：Subscriber Number，客户号码，由网络运营商分配。

SUPI：Subscription Permanent Identifier，用户永久标识，类似于 4G 的 IMSI。手机的真实身份在 5G 里称为 SUPI（SUBscription Permanent Identifier，用户永久标识符），类似 IMSI，通过公钥加密后的密文称为 SUCI（Subscription Concealed Identifier，用户隐藏标识符），SUCI 传送给基站后，基站直接上传至核心网。

GPSI：Generic PublicSubscription Identifier，通用公共用户标识，等同于 4G 的 MSISDN，SUPI 和 GPSI 之间不一定一一对应，用户如果访问不同的数据网络，就会存

在多个 GPSI 标识, 网络需要将外部网络 GPSI 与 SUPI 建立关系。NEF 可以实现 External GPSI 与 Inter GPSI 有映射关系, UDR 上保存有 Internal GPSI 与 SUPI 的映射关系。

MAC: Medium/Media Access Control 地址, 用来表示互联网上每一个站点的标识符, 采用十六进制数表示, 共六个字节(48 位)。其中, 前三个字节是由 IEEE 的注册管理机构 RA 负责给不同厂家分配的代码(高位 24 位), 也称为"编制上唯一的标识符"(Organizationally Unique Identifier), 后三个字节(低位 24 位)由各厂家自行指派给生产的适配器接口, 称为扩展标识符(唯一性)。一个地址块可以生成 2 个不同的地址。MAC 地址实际上就是适配器地址或适配器标识符。

图 11 示出了可以应用本发明实施例的一种应用层密钥推导过程的示意图。

如图 11 所示, 应用层密钥推导过程 1100 包括: 新增由 K_{AF} 推导出 K_{APP} (根据远端 UE 的数量确定所需的个数), 该 K_{APPn} 由中继 ME 自组网生成并发送给远端 UE_n , 用于应用平台 AF 与 ME_n 之间的安全通信。

图 12 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信方案的系统架构的示意图。

如图 12 所示, 系统架构可以包括远端终端设备 1202、中继终端设备 1204、无线网络和互联网 1210。无线网络用以在终端设备和服务器之间提供通信链路的介质。无线网络可以包括基站 1206、用户面功能 1208、接入与移动性管理功能 1212 和会话管理功能 1214。无线网络的连接类型包括有线、无线通信链路或者光纤电缆, 但不限于此。

图 13 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信的方案示意图。

如图 13 所示, 基于共享密钥进行数据通信的方案包括以下流程:

步骤 S1302, 中继 UE 完成主认证, 生成共享密钥 K_{AUSF} , 基于 K_{AUSF} 生成锚点密钥 K_{AKMA} 、应用密钥标识 A-KID, 并与平台 AF 完成 K_{AF} 的协商及生成。

步骤 S1304, 远程 UE 与中继 UE 建立连接, 中继 UE 获得远端 UE ID。

步骤 S1306, 中继 UE 为远端 UE 生成 UE-APP-ID, 利用 UE-APP-ID 和 K_{AF} 生成 K-app。

步骤 S1308, 中继 UE 将 UE-APP-ID、应用密钥 K-app 和 A-KID 发送给远端 UE。

步骤 S1310, 应用平台 AF 利用 UE-APP-ID 和应用平台密钥 K_{AF} 生成应用密钥 K-app。

步骤 S1312, 远端 UE 和平台 AF 之间利用 K-app 进行安全通信。

图 14 示出了可以应用本发明实施例的一种基于共享密钥进行数据通信交互过程的示意图。

如图 14 所示, 基于共享密钥进行数据通信交互过程主要涉及远端 UE1402、中继 UE1404、认证服务器功能 1406、应用层认证和密钥管理锚点功能 (AAmf) 1408、网络开放功能 (NEF) 1410 和中继应用管理平台 (AF) 1412, 中继 UE1404 与应用层认证和密钥管理锚点功能 (AAmf) 1408 之间进行主认证及 K_{AKMA} 密钥建立, 中继 UE1404 生成

A-KID 和 K_{AF} ，中继 UE1404 与中继应用管理平台（AF）1412 之间进行，中继应用管理平台 AF1412 发送 A-KID 和 AF_ID，并经由 NEF 从 AAnF 获取 K_{AF} 、 K_{AF} 有效期、手机号 GPSI 等，中继 UE1404 与中继应用管理平台（AF）1412 之间的应用会话建立响应，中继 UE1404 利用共享密钥 K_{AF} 进行安全通信，接下来远端 UE 与中继应用管理平台（AF）

5 1412 之间的安全通信主要通过以下步骤实现：

1. 远端 UE1402 与中继 UE1404 建立安全连接，中继 UE1404 获取远端 UE1402 的 ID。

2. 中继 UE1404 利用远端 UE1402 的 ID 生成 UE_APP_ID。

3. 中继 UE1404 利用 UE_APP_ID 和 K_{AF} 生成 K_{app} 。

4. 中继 UE1404 将 UE_APP_ID、 K_{app} 、A-KID 发送至远端 UE1402。

10 5. 远端 UE1402 与中继应用管理平台（AF）1412 之间的应用会话建立请求（A-KID、UE_APP_ID）。

6. 中继应用管理平台（AF）1412 利用 UE_APP_ID 和 K_{AF} 生成 K_{app} 。

7. 远端 UE1402 与中继应用管理平台（AF）1412 之间的应用会话建立响应。

15 8. 远端 UE1402 与中继应用管理平台（AF）1412 之间利用共享密钥 K_{app} 进行安全通信。

对应于上述方法实施例，本公开还提供一种基于共享密钥进行数据通信的装置，可以用于执行上述方法实施例。

图 15 是本公开示例性实施例中一种基于共享密钥进行数据通信的装置的方框图。

参考图 15，基于共享密钥进行数据通信的装置 1500 可以包括：

20 获取模块 1502，设置为获取远端终端设备的标识信息。

生成模块 1504，设置为根据所述远端终端设备的标识信息生成终端应用标识。

所述生成模块 1504，设置为根据所述终端应用标识和应用平台密钥生成相应的应用密钥。

25 交互模块 1506，设置为将所述终端应用标识、所述应用密钥和所述应用密钥标识反馈至远端终端设备，所述远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供所述中继应用管理平台被配置为能够根据所述终端应用标识和应用平台密钥生成相应的应用密钥，所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

30 在本公开的一种示例性实施例中，交互模块 1506 还设置为：通过与应用层进行主认证并生成锚点密钥；基于所述锚点密钥生成应用平台密钥和所述应用密钥标识；请求与所述中继应用管理平台建立应用会话；向所述中继应用管理平台发送所述应用密钥标识，所述中继应用管理平台被配置为向应用层认证和密钥管理锚点功能发送所述应用密钥标识和应用平台标识，所述应用层认证和密钥管理锚点功能被配置为根据所述锚点密钥确定所述应用平台密钥，并将所述应用平台密钥、所述应用平台密钥的有效期和终端通用公共用户标识反馈至所述中继应用管理平台；通过共享的所述应用平台密钥与所述中继应用管理

35

平台进行数据通信。

在本公开的一种示例性实施例中，生成模块 1504 还设置为：将所述终端应用标识和所述应用平台密钥代入密钥导出函数进行计算；根据所述密钥导出函数确定相应的应用密钥。

5 在本公开的一种示例性实施例中，所述密钥导出函数的表达式包括： $K\text{-APP} = \text{HMAC-SHA-256}(K_{\text{AF}}, S)$ ； $S = FC \parallel P0 \parallel L0$ ，其中，所述 HMAC-SHA-256(K_{AF}, S) 表征以所述 K_{AF} 和所述 S 为参数的密钥导出函数，所述 K_{AF} 表征所述应用平台密钥，所述 K-APP 表征所述应用密钥，所述 S 表征中间参数，所述 FC 表征 3GPP 的保留字段，所述 P0 表征所述终端应用标识，所述 L0 表征所述终端应用标识的字符长度。

10 在本公开的一种示例性实施例中，交互模块 1506 还设置为：获取远端终端设备的通信标识符；根据所述通信标识符生成 IPv6 接口标识，并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息；将所述 IPv6 接口标识分配至对应的远端终端设备。

 在本公开的一种示例性实施例中，交互模块 1506 还设置为：获取远端终端设备的通信标识符；根据所述通信标识符生成 IPv6 接口标识，并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息；响应于接收到的所述远端终端设备的数据流，采用生成的 IPv6 接口标识替换所述数据流中的 IPv6 接口标识。

15 在本公开的一种示例性实施例中，所述通信标识符包括 MSISDN、GPSI、IMSI、SUPI、MAC 地址中的至少一种。

 由于基于共享密钥进行数据通信的装置 1500 的各功能已在其对应的方法实施例中予以详细说明，本公开于此不再赘述。

20 应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本公开的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

25 在本公开的示例性实施例中，还提供了一种能够实现上述方法的电子设备。

 所属技术领域的技术人员能够理解，本发明的各个方面可以实现为系统、方法或程序产品。因此，本发明的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式（包括固件、微代码等），或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

30 下面参照图 16 来描述根据本发明的这种实施方式的电子设备 1600。图 16 显示的电子设备 1600 仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

 如图 16 所示，电子设备 1600 以通用计算设备的形式表现。电子设备 1600 的组件可以包括但不限于：上述至少一个处理单元 1610、上述至少一个存储单元 1620、连接不同系统组件（包括存储单元 1620 和处理单元 1610）的总线 1630。

35 其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元 1610 执行，

使得所述处理单元 1610 执行本说明书上述“示例性方法”部分中描述的根据本发明各种示例性实施方式的步骤。例如，所述处理单元 1610 可以执行如本公开实施例所示的方法。

存储单元 1620 可以包括易失性存储单元形式的可读介质，例如随机存取存储单元（RAM）16201 和/或高速缓存存储单元 16202，还可以进一步包括只读存储单元（ROM）16203。

存储单元 1620 还可以包括具有一组（至少一个）程序模块 16205 的程序/实用工具 16204，这样的程序模块 16205 包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

总线 1630 可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

电子设备 1600 也可以与一个或多个外部设备 1640（例如键盘、指向设备、蓝牙设备等）通信，还可与一个或者多个使得用户能与该电子设备 1600 交互的设备通信，和/或与使得该电子设备 1600 能与一个或多个其它计算设备进行通信的任何设备（例如路由器、调制解调器等等）通信。这种通信可以通过输入/输出（I/O）接口 1650 进行。并且，电子设备 1600 还可以通过网络适配器 1660 与一个或者多个网络（例如局域网（LAN），广域网（WAN）和/或公共网络，例如因特网）通信。如图所示，网络适配器 1660 通过总线 1630 与电子设备 1600 的其它模块通信。应当明白，尽管图中未示出，可以结合电子设备 1600 使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID 系统、磁带驱动器以及数据备份存储系统等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、终端装置、或者网络设备等）执行根据本公开实施方式的方法。

在本公开的示例性实施例中，还提供了一种计算机可读存储介质，其上存储有能够实现本说明书上述方法的程序产品。在一些可能的实施方式中，本发明的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在终端设备上运行时，所述程序代码用于使所述终端设备执行本说明书上述“示例性方法”部分中描述的根据本发明各种示例性实施方式的步骤。

根据本发明的实施方式的用于实现上述方法的程序产品可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备，例如个人电脑上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器（CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。

计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。

可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++ 等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网（LAN）或广域网（WAN），连接到用户计算设备，或者，可以连接到外部计算设备（例如利用因特网服务提供商来通过因特网连接）。

此外，上述附图仅是根据本发明示例性实施例的方法所包括的处理的示意性说明，而不是限制目的。易于理解，上述附图所示的处理并不表明或限制这些处理的时间顺序。另外，也易于理解，这些处理可以是例如在多个模块中同步或异步执行的。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和构思由权利要求指出。

工业实用性

实施例，通过获取远端终端设备的标识信息，并根据远端终端设备的标识信息生成终端应用标识，进而根据终端应用标识和应用平台密钥生成相应的应用密钥，最终将终端应用标识、应用密钥和应用密钥标识反馈至远端终端设备，远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供中继应用管理平台

被配置为能够根据终端应用标识和应用平台密钥生成相应的应用密钥,远端终端设备与中继应用管理平台基于应用密钥进行数据通信,在不需要对核心网做升级改造的前提下,满足了远端 UE 与应用管理平台的安全通信需求,扩展了在近域通信的应用场景。

权利要求

1. 一种基于共享密钥进行数据通信的方法，其特征在于，适用于中继终端设备，所述基于共享密钥进行数据通信的方法包括：

获取远端终端设备的标识信息；

5 根据所述远端终端设备的标识信息生成终端应用标识；

根据所述终端应用标识和应用平台密钥生成相应的应用密钥；

将所述终端应用标识、所述应用密钥和所述应用密钥标识反馈至远端终端设备，所述远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供所述中继应用管理平台被配置为能够根据所述终端应用标识和应用平台密钥生成相应的应用密钥，所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

2. 如权利要求 1 所述的基于共享密钥进行数据通信的方法，其特征在于，在获取远端终端设备的标识信息前，还包括：

通过与应用层进行主认证并生成锚点密钥；

15 基于所述锚点密钥生成应用平台密钥和所述应用密钥标识；

请求与所述中继应用管理平台建立应用会话；

向所述中继应用管理平台发送所述应用密钥标识，所述中继应用管理平台被配置为向应用层认证和密钥管理锚点功能发送所述应用密钥标识和应用平台标识，所述应用层认证和密钥管理锚点功能被配置为根据所述锚点密钥确定所述应用平台密钥，并将所述应用平台密钥、所述应用平台密钥的有效期和终端通用公共用户标识反馈至所述中继应用管理平台；通过共享的所述应用平台密钥与所述中继应用管理平台进行数据通信。

3. 如权利要求 1 所述的基于共享密钥进行数据通信的方法，其特征在于，根据终端应用标识和应用平台密钥生成相应的应用密钥包括：

将所述终端应用标识和所述应用平台密钥代入密钥导出函数进行计算；

25 根据所述密钥导出函数确定相应的应用密钥。

4. 如权利要求 3 所述的基于共享密钥进行数据通信的方法，其特征在于，所述密钥导出函数的表达式包括：

$$K\text{-APP} = \text{HMAC-SHA-256} (K_{\text{AF}}, S);$$

$$S = \text{FC} \parallel \text{P0} \parallel \text{L0},$$

30 其中，所述 HMAC-SHA-256 (K_{AF} , S) 表征以所述 K_{AF} 和所述 S 为参数的密钥导出函数，所述 K_{AF} 表征所述应用平台密钥，所述 K-APP 表征所述应用密钥，所述 S 表征中间参数，所述 FC 表征 3GPP 的保留字段，所述 P0 表征所述终端应用标识，所述 L0 表征所述终端应用标识的字符长度。

5. 如权利要求 1-4 中任一项所述的基于共享密钥进行数据通信的方法，其特征在于，
35 还包括：

获取远端终端设备的通信标识符；

根据所述通信标识符生成 IPv6 接口标识，并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息；

将所述 IPv6 接口标识分配至对应的远端终端设备。

- 5 6. 如权利要求 1-4 中任一项所述的基于共享密钥进行数据通信的方法，其特征在于，还包括：

获取远端终端设备的通信标识符；

根据所述通信标识符生成 IPv6 接口标识，并根据所述 IPv6 接口标识确定对应的远端终端设备的标识信息；

- 10 响应于接收到的所述远端终端设备的数据流，采用生成的 IPv6 接口标识替换所述数据流中的 IPv6 接口标识。

7. 如权利要求 6 所述的基于共享密钥进行数据通信的方法，其特征在于，

所述通信标识符包括 MSISDN、GPSI、IMSI、SUPI、MAC 地址中的至少一种。

8. 一种基于共享密钥进行数据通信的装置，其特征在于，包括：

- 15 获取模块，设置为获取远端终端设备的标识信息；

生成模块，设置为根据所述远端终端设备的标识信息生成终端应用标识；

所述生成模块，设置为根据所述终端应用标识和应用平台密钥生成相应的应用密钥；

- 20 交互模块，设置为将所述终端应用标识、所述应用密钥和所述应用密钥标识反馈至远端终端设备，所述远端终端设备被配置为通过应用会话请求向中继应用管理平台发送应用密钥标识和终端应用标识，以供所述中继应用管理平台被配置为能够根据所述终端应用标识和应用平台密钥生成相应的应用密钥，所述远端终端设备与所述中继应用管理平台基于所述应用密钥进行数据通信。

9. 一种电子设备，其特征在于，包括：

存储器；以及

- 25 耦合到所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指令，执行如权利要求 1-7 任一项所述的基于共享密钥进行数据通信的方法。

10. 一种计算机可读存储介质，其上存储有程序，该程序被处理器执行时实现如权利要求 1-7 任一项所述的基于共享密钥进行数据通信的方法。

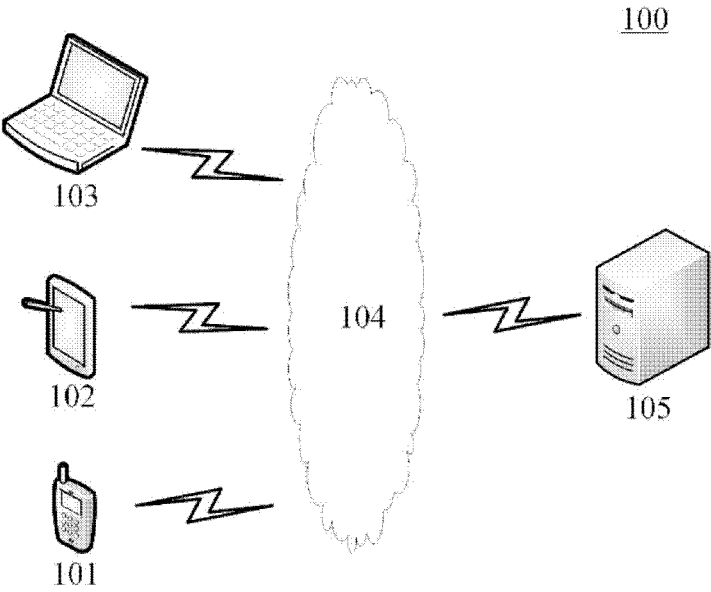


图 1

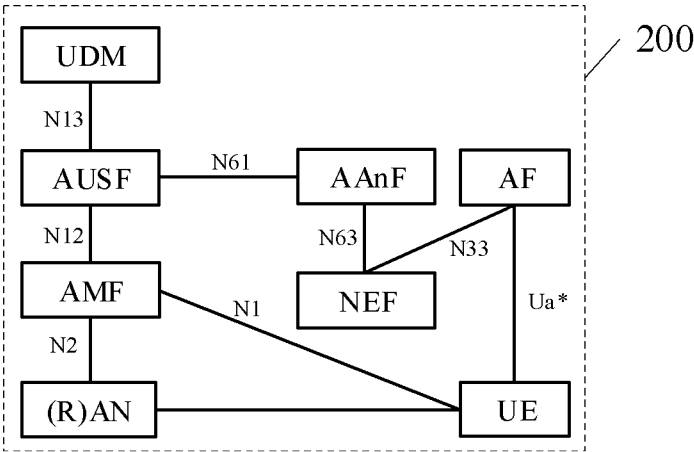


图 2

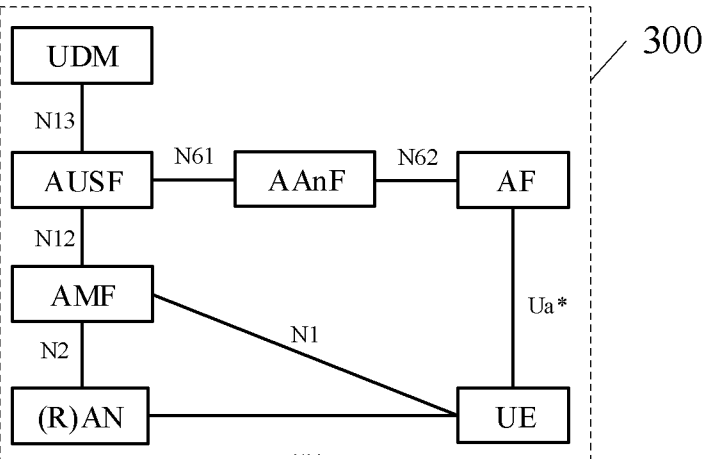


图 3

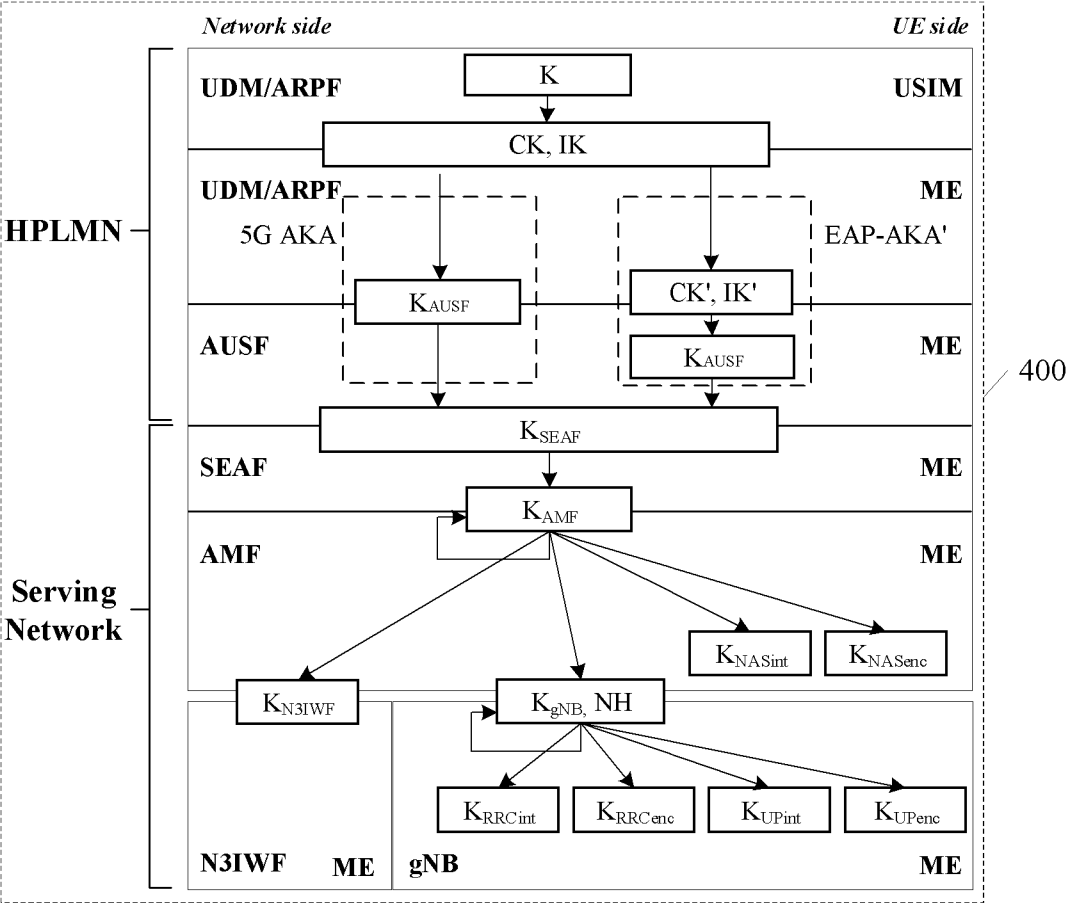


图 4

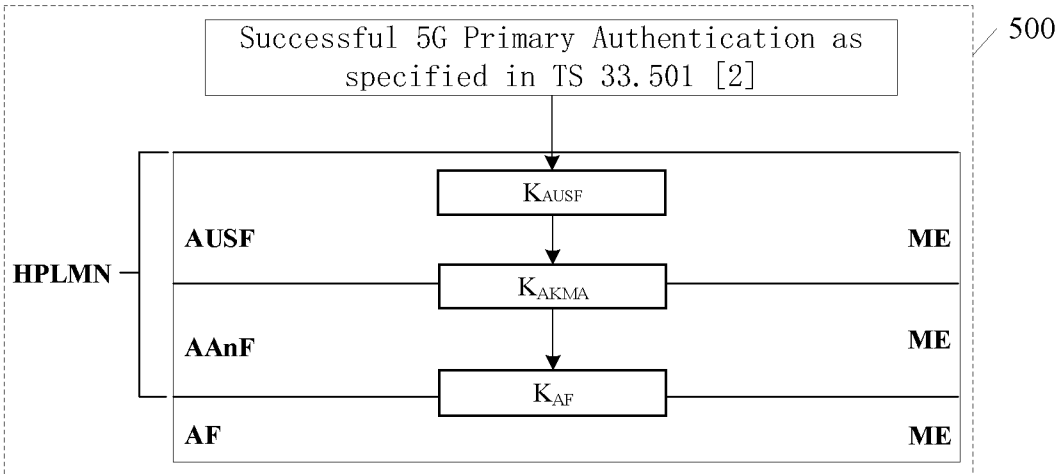


图 5

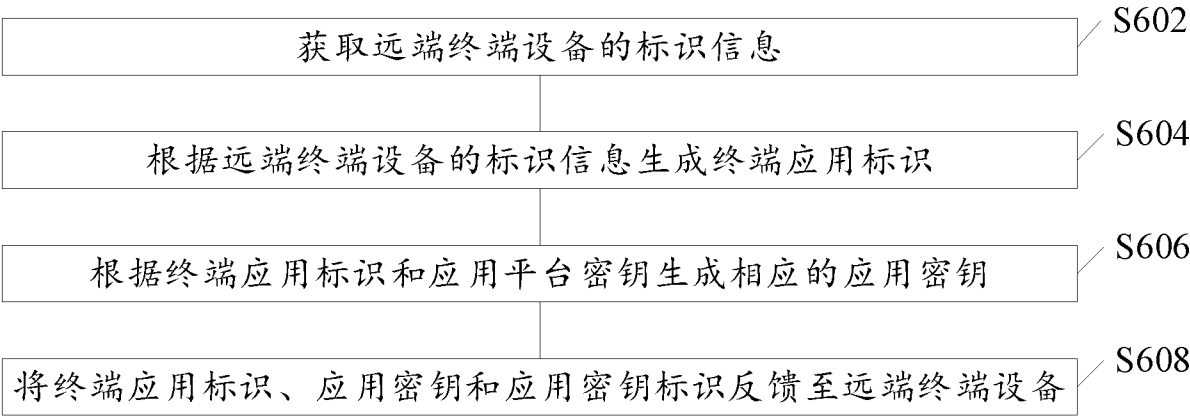


图 6

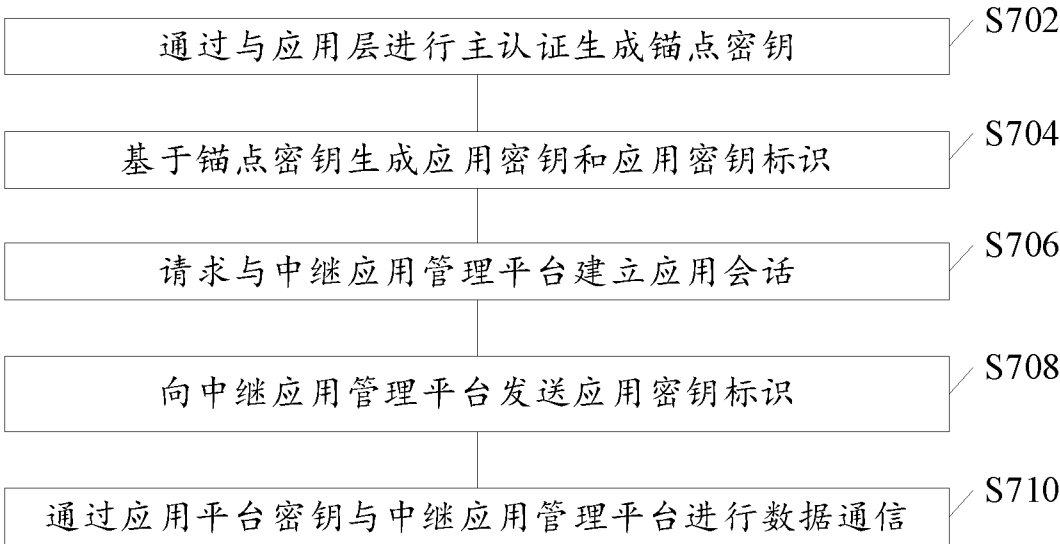


图 7

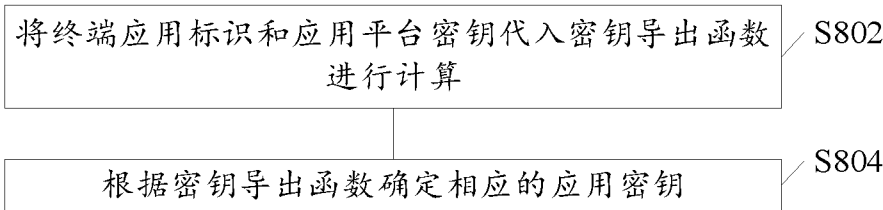


图 8

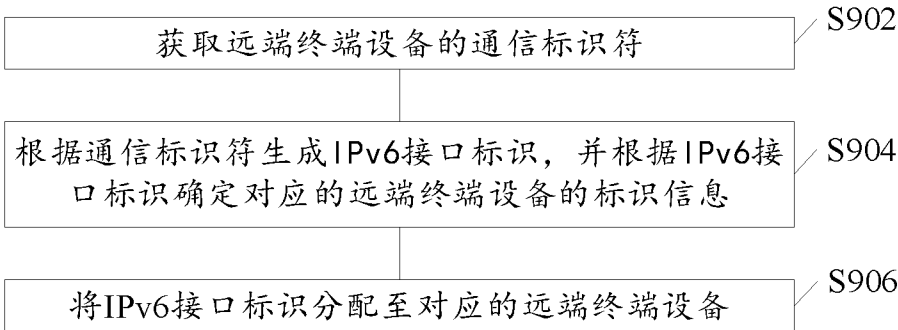


图 9

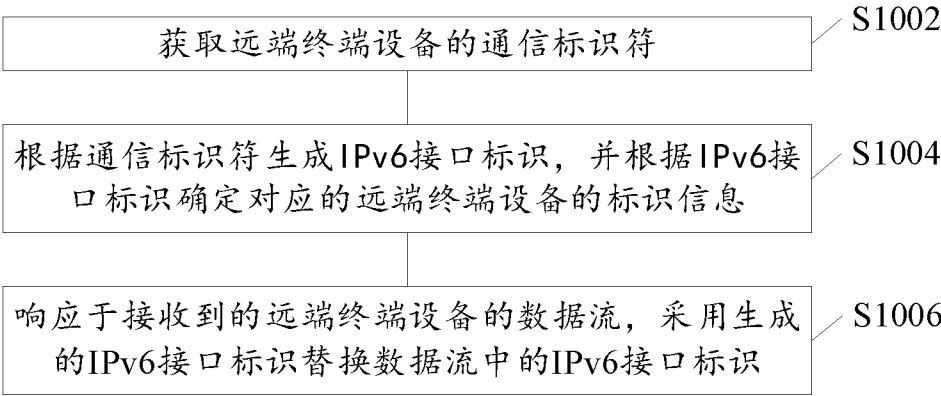


图 10

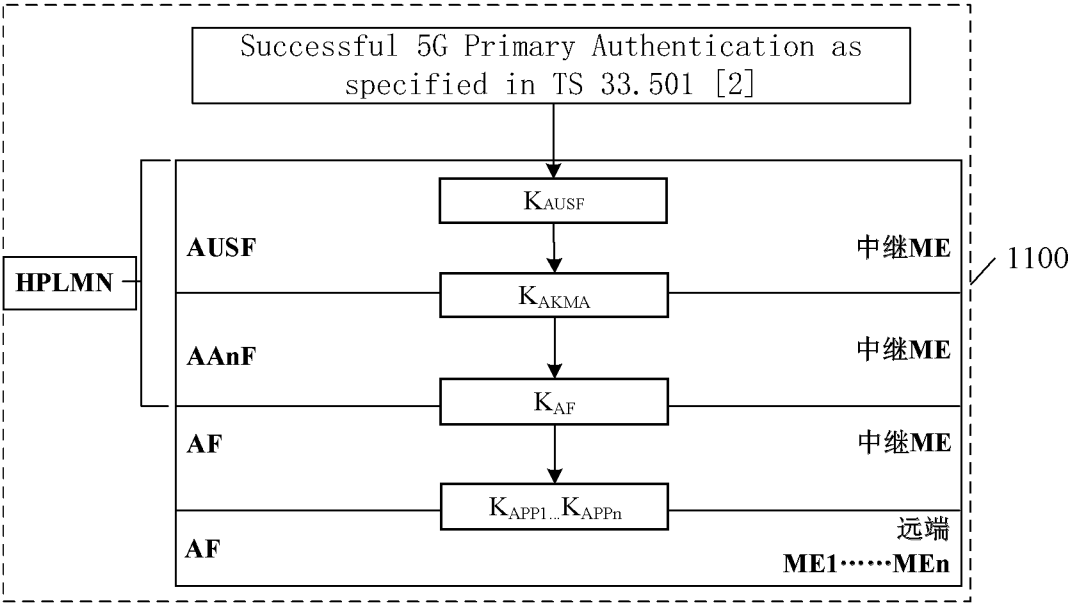


图 11

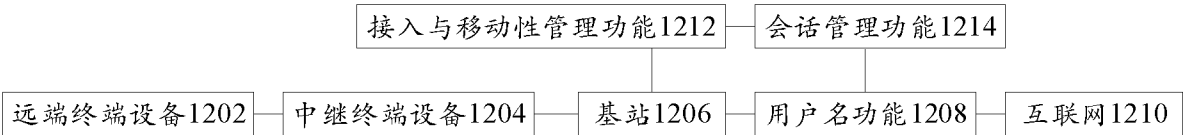


图 12

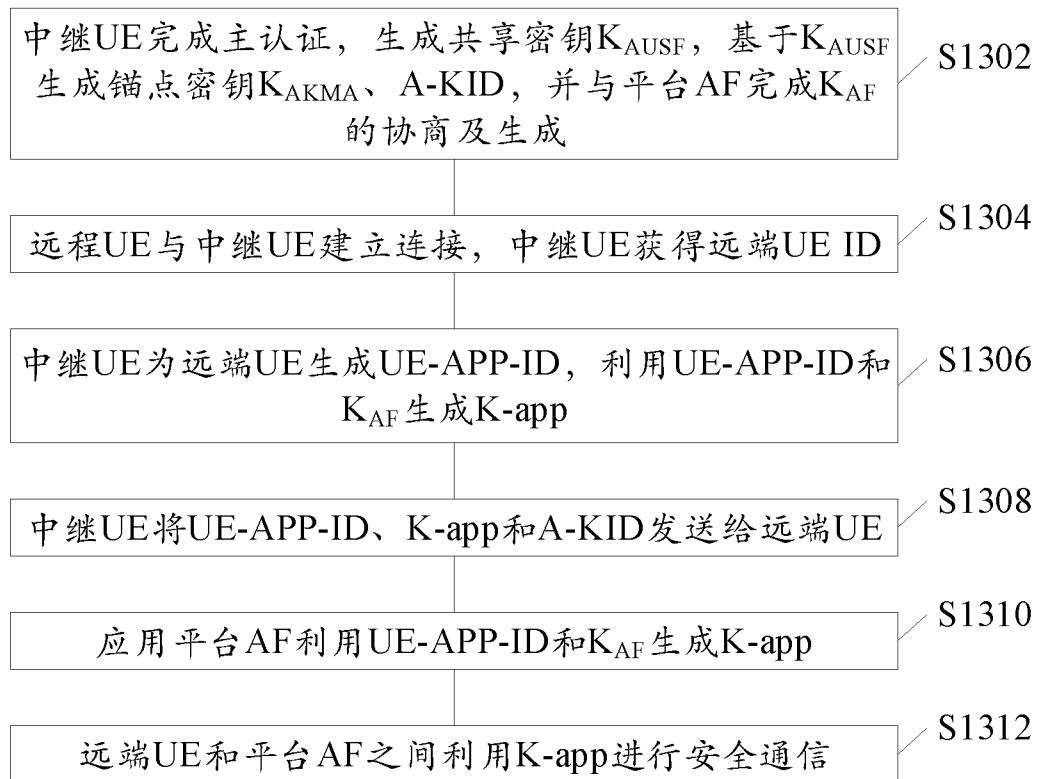


图 13

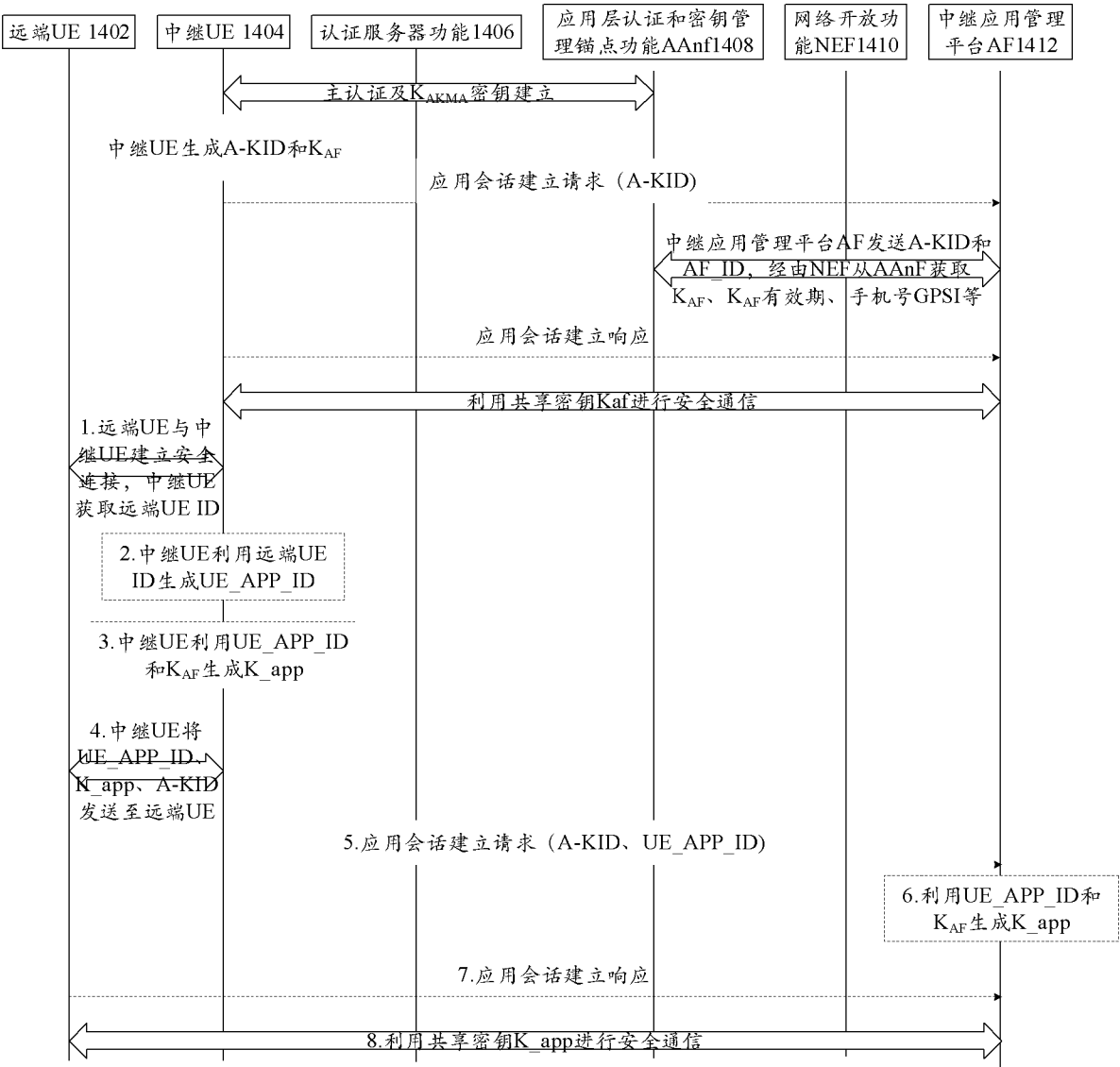


图 14

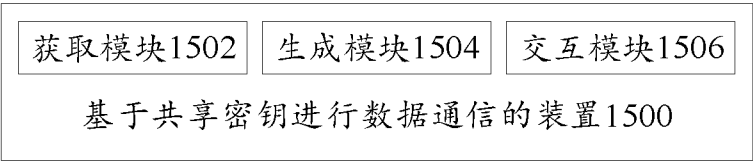


图 15

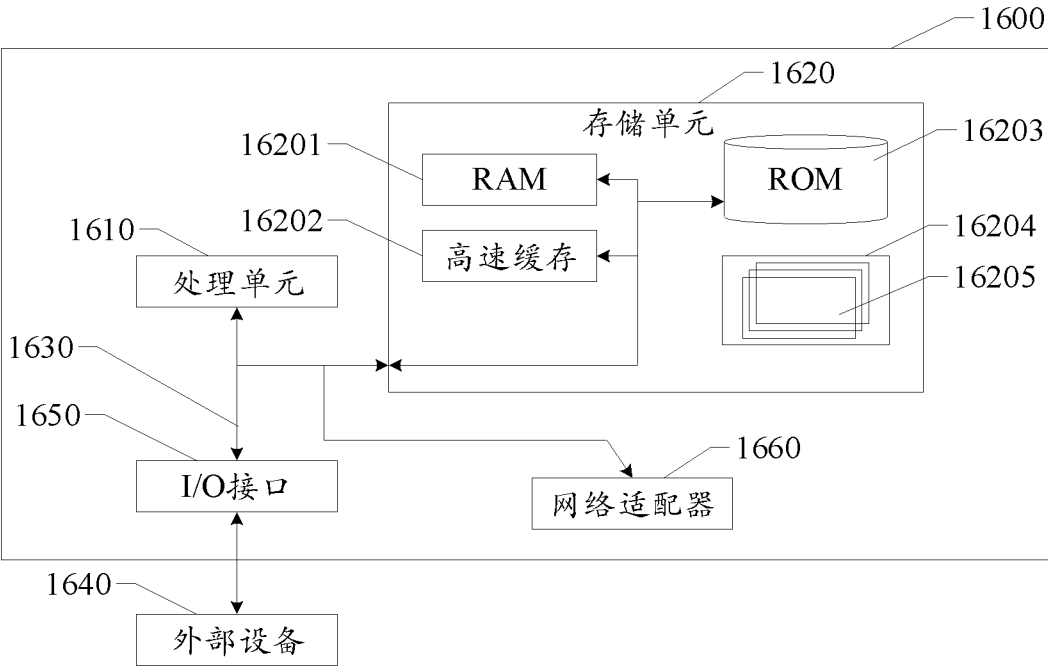


图 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/140617

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01);H04L9/06(2006.01);H04L101/659(2022.01)n

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:H04

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, CJFD, CNTXT, ENTXT, ENTXTC: 密钥, 标识, 协商, 应用功能, 应用密钥, 应用平台, 远程, 远程ue, 远程设备, 远程终端, 远端, 远端ue, 中继, 中继ue, 中继终端, AF, akma, id, key, remote ue, relay ue, application key, identifier?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115150075 A (CHINA TELECOM CORP., LTD.) 04 October 2022 (2022-10-04) claims 1-10	1-10
A	US 2021360742 A1 (APPLE INC.) 18 November 2021 (2021-11-18) description, paragraphs 66-191, and figure 6	1-10
A	WO 2022019627 A1 (SAMSUNG ELECTRONICS CO., LTD.) 27 January 2022 (2022-01-27) entire document	1-10
A	WO 2022088029 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 05 May 2022 (2022-05-05) entire document	1-10
A	HUAWEI et al. "S3-203432 "Solution on Key Management for UE-to-network Relay" 3GPP tsg_sa\wg3_security, No. tsgs3_101e, 16 November 2020 (2020-11-16), pp. 1-3	1-10
A	QUALCOMM INCORPORATED. "S3-203191 "Sending UE Identifier to the AKMA AF" 3GPP tsg_sa\wg3_security, No. tsgs3_101e, 30 October 2020 (2020-10-30), pp. 1-7	1-10



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

"D" document cited by the applicant in the international application

"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

09 March 2023

Date of mailing of the international search report

10 March 2023

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/140617

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115150075	A	04 October 2022	None			
US	2021360742	A1	18 November 2021	WO	2020072652	A1	09 April 2020
WO	2022019627	A1	27 January 2022	None			
WO	2022088029	A1	05 May 2022	None			

国际检索报告

国际申请号

PCT/CN2022/140617

A. 主题的分类

H04L9/08(2006.01)i;H04L9/06(2006.01)i;H04L101/659(2022.01)n

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)

IPC:H04

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, CJFD, CNTXT, ENTXT, ENTXT:密钥,标识,协商,应用功能,应用密钥,应用平台,远程,远程ue,远程设备,远程终端,远端,远端ue,中继,中继ue,中继终端,AF, akma, id, key, remote ue, relay ue, application key, identifier?

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
PX	CN 115150075 A (中国电信股份有限公司) 2022年10月4日 (2022 - 10 - 04) 权利要求1-10	1-10
A	US 2021360742 A1 (APPLE INC.) 2021年11月18日 (2021 - 11 - 18) 说明书第66-191段,图6	1-10
A	WO 2022019627 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2022年1月27日 (2022 - 01 - 27) 全文	1-10
A	WO 2022088029 A1 (华为技术有限公司) 2022年5月5日 (2022 - 05 - 05) 全文	1-10
A	Huawei 等. "S3-203432 "Solution on Key Management for UE-to-network Relay"" 3GPP tsg_sa\wg3_security, 第tsgs3_101e期, 2020年11月16日 (2020 - 11 - 16), 第1-3页	1-10
A	Qualcomm Incorporated. "S3-203191 "Sending UE Identifier to the AKMA AF"" 3GPP tsg_sa\wg3_security, 第tsgs3_101e期, 2020年10月30日 (2020 - 10 - 30), 第1-7页	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

“D” 申请人在国际申请中引证的文件

“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

2023年3月9日

国际检索报告邮寄日期

2023年3月10日

ISA/CN的名称和邮寄地址

中国国家知识产权局

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

郑晓双

电话号码 (+86) 010-62411271

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/140617

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	115150075	A	2022年10月4日	无	
US	2021360742	A1	2021年11月18日	WO 2020072652	A1 2020年4月9日
WO	2022019627	A1	2022年1月27日	无	
WO	2022088029	A1	2022年5月5日	无	