

(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
2023 年 2 月 16 日 (16.02.2023)



(10) 国际公布号
WO 2023/016451 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2022/111148

(22) 国际申请日: 2022 年 8 月 9 日 (09.08.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110909519.1 2021年8月9日 (09.08.2021) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION CO., LTD RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 黄晓婷 (HUANG, Xiaoting); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。黄震宁 (HUANG, Zhenning); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW

FIRM); 中国北京市海淀区西直门北大街32号院枫蓝国际中心2号楼10层, Beijing 100082 (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, 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, 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。

(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))。

(54) Title: UPDATE METHOD, NETWORK SIDE DEVICE, TERMINAL, AND COMPUTER READABLE STORAGE MEDIUM

(54) 发明名称: 更新方法、网络侧设备、终端和计算机可读存储介质

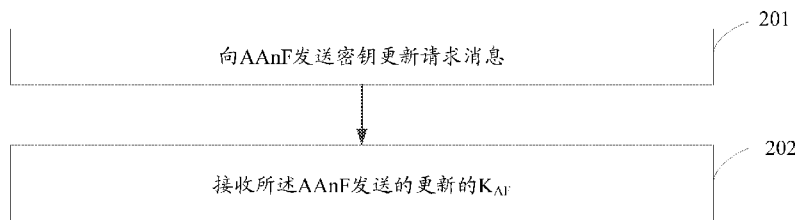


图 2

201 Send a key update request message to an AAnF

202 Receive an updated K_{AF} sent by the AAnF

(57) Abstract: The present disclosure provides an update method, a network side device, a terminal, and a computer readable storage medium. The update method applied to an AF comprises: sending a key update request message to an authentication and key management for applications (AKMA) anchor function (AAnF); and receiving an updated key K_{AF} sent by the AAnF.

(57) 摘要: 本公开提供一种更新方法、网络侧设备、终端和计算机可读存储介质, 其中, 应用于 AF 的更新方法, 包括: 向会话密钥管理锚点功能实体 AAnF 发送密钥更新请求消息; 接收所述 AAnF 发送的更新的会话密钥 K_{AF}。



WO 2023/016451 A1

更新方法、网络侧设备、终端和计算机可读存储介质

相关申请的交叉引用

本公开主张在 2021 年 8 月 9 日在中国提交的中国专利申请号 No. 202110909519.1 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及通信技术领域，尤其涉及一种更新方法、网络侧设备、终端和计算机可读存储介质。

背景技术

相关的应用层认证和会话密钥管理（Authentication and Key Management for Applications, AKMA）流程中，只有在用户设备（User Equipment, UE）和网络之间进行了新的初始认证，以产生了新的 AKMA 中间密钥（AKMA Anchor Key, K_{AKMA} ）的时候，才会通过 UE 和应用功能实体（Application Function, AF）之间的 Ua* 协议更新 AKMA 会话密钥（AKMA Application Key, K_{AF} ）。这样，就存在 K_{AF} 过期后，如果 UE 和网络之间没有进行新的初始认证，则 UE 和网络之间的 AKMA 业务就会由于 K_{AF} 失效而中断的缺陷。

发明内容

本公开提供一种更新方法、网络侧设备、终端和计算机可读存储介质，能够主动发起 K_{AF} 的更新流程，以避免 UE 和网络之间的 AKMA 业务，因 UE 和网络之间未进行新的初始认证而中断的问题。

为解决上述技术问题，本公开是这样实现的：

第一方面，本公开提供了一种更新方法，应用于 AF，所述更新方法包括：

向会话密钥管理锚点功能实体（AKMA anchor Function, AAnF）发送密钥更新请求消息；

接收所述 AAnF 发送的更新的 K_{AF} 。

第二方面，本公开提供了一种更新方法，应用于 AAnF，所述更新方法

包括:

接收 AF 发送的密钥更新请求消息;

向所述 AF 发送更新的 K_{AF} 。

第三方面,本公开提供了一种更新方法,应用于统一数据管理功能实体 (Unified Data Management, UDM),所述更新方法包括:

接收 AAnF 发送的参数更新请求消息;

发送更新参数到 UE,所述更新参数用于所述 UE 结合所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成 K_{AF} 。

第四方面,本公开提供了一种更新方法,应用于 UE,所述更新方法包括:

接收 AF 发送的密钥更新指示消息,所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

第五方面,本公开提供了一种 AF,包括:

第一发送模块,用于向 AAnF 发送密钥更新请求消息;

第一接收模块,用于接收所述 AAnF 发送的更新的 K_{AF} 。

第六方面,本公开提供了一种 AAnF,包括:

第二接收模块,用于接收 AF 发送的密钥更新请求消息;

第三发送模块,用于向所述 AF 发送更新的 K_{AF} 。

第七方面,本公开提供了一种 UDM,包括:

第四接收模块,用于接收 AAnF 发送的参数更新请求消息;

第五发送模块,用于发送更新参数到 UE,所述更新参数用于所述 UE 结合所述 UE 当前存储的 K_{AKMA} 生成 K_{AF} 。

第八方面,本公开提供了一种 UE,包括:

第五接收模块,用于接收 AF 发送的密钥更新指示消息,所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

第九方面,本公开提供了一种网络侧设备,包括:处理器和收发机;

所述收发机,用于向 AAnF 发送密钥更新请求消息;

所述收发机,还用于接收所述 AAnF 发送的更新的 K_A ;

和/或

所述收发机,用于接收 AF 发送的密钥更新请求消息;

所述收发机，还用于向所述 AF 发送更新的 K_{AF} ；

和/或

所述收发机，用于接收 AAnF 发送的参数更新请求消息；

所述收发机，还用于发送更新参数到 UE，所述更新参数用于所述 UE 结合所述 UE 当前存储的 K_{AKMA} 生成 K_{AF} 。

第十方面，本公开提供了一种用户设备 UE，包括：处理器和收发机；

所述收发机，用于接收 AF 发送的密钥更新指示消息，所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

第十一方面，本公开提供了一种网络侧设备，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如第一方面所述的更新方法中的步骤，或者实现如第二方面所述的更新方法中的步骤，或者实现如第三方面所述的更新方法中的步骤。

第十二方面，本公开提供了一种终端设备，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如第四方面所述的更新方法中的步骤。

第十三方面，本公开提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时，实现如第一方面所述的更新方法中的步骤，或者实现如第二方面所述的更新方法中的步骤，或者实现如第三方面所述的更新方法中的步骤，或者实现如第四方面所述的更新方法中的步骤。

本公开实施例中，提供了一种 AF 主动发起的密钥更新流程，能够主动更新 K_{AF} ，以避免相关技术中由于 UE 和网络之间没有进行新的初始认证而导致的 K_{AF} 过期的问题，进而能够保证 AKMA 业务的顺利进行。

附图说明

图 1 是相关技术中 K_{AF} 的更新流程示意图；

图 2 是本公开实施例提供的一种应用于 AF 的更新方法的流程图；

图 3 是本公开实施例提供的一种应用于 AAnF 的更新方法的流程图；

图 4 是本公开实施例提供的一种应用于 UDM 的更新方法的流程图；

图 5 是本公开实施例提供的一种应用于 UE 的更新方法的流程图；

图 6 是本公开实施例中 UE 与网络侧设备之间的数据交互示意图；

图 7 是本公开实施例提供的一种 AF 的结构示意图；

图 8 是本公开实施例提供的一种 AAnF 的结构示意图；

图 9 是本公开实施例提供的一种 UDM 的结构示意图；

图 10 是本公开实施例提供的一种网络侧设备的结构示意图；

图 11 是本公开实施例提供的一种 UE 的结构示意图；

图 12 是本公开实施例提供的一种终端设备的结构示意图。

具体实施方式

为使本公开要解决的技术问题、技术方案和优点更加清楚，下面将结合附图及具体实施例进行详细描述。在下面的描述中，提供诸如具体的配置和组件的特定细节仅仅是为了帮助全面理解本公开的实施例。因此，本领域技术人员应该清楚，可以对这里描述的实施例进行各种改变和修改而不脱离本公开的范围和精神。另外，为了清楚和简洁，省略了对已知功能和构造的描述。

应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本公开的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。

在本公开的各种实施例中，应理解，下述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本公开实施例的实施过程构成任何限定。

在相关技术中，第三代合作伙伴计划 (3rd Generation Partnership Project, 3GPP) 相关协议定义了如下应用层认证和密钥管理的架构和流程：

如图 1 所示，在调用 AKMA 服务之前，UE 应已成功注册到第五代 (the 5th Generation, 5G) 核心网，这样，在通过 5G 接入认证后，认证服务器功能

(Authentication Server Function, AUSF) 密钥 (AUSF Key, K_{AUSF}) 将存储在 AUSF 和 UE 中。

其中, AUSF、AAnF 以及 UE 同属于一个用户归属的公共陆地移动网络 (Home Public Land Mobile Network, HPLMN)。

如图 1 所示, 在用户设备 (即 UE, 其也可以称之为终端) 接入运营商网络并执行完主认证 (其也称之为初始认证) 规定的 5G 个人身份验证成功之后, 终端和网络侧的认证服务器功能实体 (Authentication Server Function, AUSF) 就生成密钥 K_{AUSF} 。如果终端注册并签约了 AKMA 服务, 那么在初始认证完成之后, 终端和 AUSF 就会相应地生成 AKMA 中间密钥 K_{AKMA} 及对应的密钥标识符 (AKMA Key Identifier, A-KID), 并基于该 K_{AKMA} 及 A-KID 向应用服务器提供后续的会话密钥 K_{AF} , 进而使 UE 和应用服务器能够基于该 K_{AF} 进行对应用层认证或数据加密等。

具体的, 终端向应用服务器发起业务请求时, 在请求消息中会携带 A-KID, 当应用服务器收到该请求时, 会带着该 A-KID 向 AAnF 请求会话密钥。此时, AAnF 根据从 AUSF 处获取的 AKMA 中间密钥 K_{AKMA} 推衍会话密钥 K_{AF} , 并将该会话密钥 K_{AF} 返回给应用服务器。相应的, 终端在收到应用服务器返回给自己的应用层响应消息后, 也根据自身存储的 K_{AKMA} 推衍出会话密钥 K_{AF} 。这样, 应用服务器和终端即可使用该会话密钥进行后续的应用层认证或数据加密等。

需要说明的是, 在执行下一次成功的初始认证 (隐式生存期) 之前, 当前的 K_{AKMA} 和 A-KID 是有效的。而在执行下一次成功的初始认证之后, K_{AKMA} 和 A-KID 会被更新。而 AKMA 的会话密钥 K_{AF} 根据运营商的政策具有明确的寿命。当 K_{AF} 的生存期到期时, 将需要基于当前 AKMA 中间密钥 K_{AKMA} 建立新的 AKMA 应用程序密钥。而相关技术中, 并不是所有的 Ua* 协议都支持密钥刷新, 比如传输层安全 (Transport Layer Security, TLS) 协议并不支持对应的更新流程。所以当 Ua* 不支持密钥更新机制时, 就存在以下问题: 如果此时 UE 和网络侧之间没有进行新的初始认证, 即 K_{AKMA} 没有更新, 即则无法触发 K_{AF} 的更新流程。

换言之, 在初始认证周期内即使 K_{AF} 过期, 由于此时 K_{AKMA} 没有发生

更新,则无法触发 K_{AF} 的更新,造成 AF 可能会断开与 UE 的应用层连接,进而出现 AKMA 业务中断。

而本公开实施例中,提供了一种 AF 主动发起的密钥更新流程,即使在 UE 和网络之间没有进行新的初始认证时,也能够主动更新 K_{AF} ,以避免相关技术中由于 UE 和网络之间没有进行新的初始认证而导致的 K_{AF} 过期的问题,进而能够保证 AKMA 业务的顺利进行。

为了更清楚的说明本公开提供的更新方法,以下实施例中,结合附图,对本公开实施例提供的更新方法进行说明:

请参阅图 2,本公开实施例提供的第一种更新方法,其执行主体可以是 AF,如图 2 所示,该更新方法可以包括以下步骤:

步骤 201、向 AAnF 发送密钥更新请求消息。

在具体实施中,执行本公开实施例提供的更新方法的 AF,具体可以是使用 AKMA 服务的 AF,其具有以下附加功能:

支持使用 A-KID 从 AAnF 请求 K_{AF} 。

在向 AF 提供 AKMA 应用密钥之前,AF 应由运营商网络进行认证和授权。

本步骤中,AF 通过向 AAnF 发送密钥更新请求消息,以使 AAnF 根据该密钥更新请求消息生成新的 K_{AF} ,并将该新生成的 K_{AF} 返回给 AF。

步骤 202、接收所述 AAnF 发送的更新的 K_{AF} 。

在一种可选的实施方式中,AAnF 在接收到所述密钥更新请求消息时,可以触发 UE 和网络执行的新的初始认证,以生成新的 K_{AKMA} ,然后再根据新生成的 K_{AKMA} 来实现 K_{AF} 的更新,即 $K_{AF}=KDF(K_{AKMA}, AF_ID)$ 。

本实施方式中,即使 UE 和网络之间不需要进行新的初始认证的情况下,但由于 K_{AF} 的更新需求,需要触发新的初始认证。这种方式下,应用层的密钥更新会影响 5G 网络基础主认证。而 K_{AF} 的更新需求相对于初始认证更加频繁,因此上述的方式会导致对 5G 网络频繁发起主认证,进而造成对 5G 网络的 DDos 攻击隐患,影响 5G 网络基础业务运行。

当然,上述 UE 和网络之间的新的初始认证也可以由 AAnF 指示终端,以由终端发起。而这种方式,需要对终端进行改动,且影响终端的基础安全

机制，例如：需要终端释放非接入层（Non-Access Stratum, NAS）链接，并修改 NAS 密钥集标识（NAS key set identifier, ngKSI）参数，故而触发主认证。

因此，为了解决上述的问题，本公开实施例还提供如下另一种可选的实施方式，以使 K_{AF} 的更新不再依赖于 K_{AKMA} 的更新：

所述 K_{AF} 可以是至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

本实施方式中，当 AAnF 接收到 AF 发送的密钥更新请求消息之后，可以基于接收到该密钥更新请求消息，而直接根据更新参数和 AAnF 当前存储的 K_{AKMA} 生成新的 K_{AF} 。

在相关技术中， K_{AF} 的推衍公式如下：

$$K_{AF} = \text{KDF} (K_{AKMA}, AF_ID)$$

其中，KDF 表示密钥推衍函数（Key Derivation Function）。AF_ID 表示 AF 的标识符。

而本实施方式中，可以将 K_{AF} 的推衍公式修改为：

$$K_{AF} = \text{KDF} (K_{AKMA}, AF_ID, \text{freshness parameter}) \text{ 或 } K_{AF} = \text{KDF} (K_{AKMA}, \text{freshness parameter})$$

其中，freshness parameter 即表示上述更新参数。

可选的，上述更新参数，可以理解为：密钥新鲜参数（freshness parameter），用于表示 K_{AF} 的新鲜度，且该更新参数的取值可以是计数器（COUNTER）的计数值或随机数等等，这样，每一次推衍 K_{AF} 时可以采用不同取值的更新参数，以使根据上述推衍公式推衍出的 K_{AF} 不同。

当然，上述更新参数还可以是其他 UE 参数更新（UE Parameter Update, UPU）参数。

本实施方式相较于上一可选的实施方式来说，新增了更新参数，使得 K_{AF} 的更新不再依赖于 K_{AKMA} 的更新，而是可以通过对更新参数进行更新来实现基于相同的 K_{AKMA} 实现对 K_{AF} 的更新。上述的方式中，即使在 UE 和网络之间没有进行新的初始认证时，也不再需要发起 UE 和网络之间的新的初始认证来更新 K_{AKMA} ，而是通过引入的 K_{AKMA} 之外的更新参数来实现 K_{AF} 的更新。

这种方式避免了对 5G 网络的频发的主认证以及对网络和终端的改动。

上述的两种方式中，根据不同的场景或者处理方式，可以根据已有的推导公式来生成 K_{AF} ，也可以根据新增密钥新鲜参数的推导公式来生成 K_{AF} ，也就是本公开具体实施例中，上述的 freshness parameter 为可选的参数，根据不同的处理方式而确定。例如：在 K_{AF} 的更新依赖于 K_{AKMA} 的更新的实施方式下，可以在推导公式中不采用 freshness parameter；而在 K_{AF} 的更新不再依赖于 K_{AKMA} 的更新的实施方式下，可以在推导公式中采用 freshness parameter。

进一步的，上述密钥更新请求消息还可以携带 A-KID。

作为一种可选的实施方式，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

在具体实施中，上述密钥更新指示符用于指示 AF 需要更新 K_{AF} 。

在具体实施中，上述密钥获取请求消息为相关技术中的密钥获取请求消息，且上述密钥更新指示符通过密钥获取请求消息中的保留字段来实现。这样，能够利用已有密钥获取请求消息来实现 K_{AF} 更新流程，并通过密钥获取请求消息中的保留字段来实现更新指示。

在实际应用中，密钥获取请求消息中也可以不携带密钥更新指示符，此时，AAnF 在接收到 AF 发送的密钥获取请求消息之后，可以不对 K_{AF} 进行更新，而是在密钥获取响应消息中携带 AAnF 当前存储的 K_{AF} 。

例如：在 K_{AF} 未过期，且 AF 丢失或未成功接收到 K_{AF} 的情况下，AAnF 可以重新向 AF 发送当前存储的 K_{AF} 。

相应的，在 K_{AF} 未更新的情况下，不需要将 K_{AF} 和 UE 同步，这样，可以避免因密钥更新流程与密钥获取流程未区分而造成，的不论是更新 K_{AF} 还是获取 K_{AF} ，都需要与 UE 进行密钥同步，而是仅在密钥更新流程中才与 UE 进行密钥同步，可以简化密钥获取流程。

本实施方式中，利用现有的密钥获取请求消息中是否携带密钥更新指示符，使密钥更新流程区别于现有的密钥获取流程，使得更新 K_{AF} 和获取 K_{AF} 可以通过不同的流程来实现，简化了流程。

当然，在实际应用中，上述密钥更新请求消息也可以是新增的消息，在此不作具体限定。

可选地，在步骤 202 之后，为了实现 AF 与 UE 之间的密钥同步，AF 还可以执行以下步骤：

向 UE 发送指示消息，指示所述 UE 更新 K_{AF} 。

本步骤中，AF 可以在从 AAnF 获取到的新的 K_{AF} 之后，通知/指示 UE 更新 K_{AF} ，以使 UE 和 AF 使用相同的 K_{AF} 。

当然，在实际应用中，还可以通过其他方式实现 AF 与 UE 之间的密钥同步，例如：通过 UPU 流程来实现，或者由 AAnF 指示 UE 更新 K_{AF} ，在此对 AF 与 UE 之间的密钥同步的具体实现方式，不作具体限定。

可选地，所述 K_{AF} 携带于密钥更新响应消息中。

也就是说，步骤 202 具体可以是：接收所述 AAnF 发送的密钥更新响应消息，且所述密钥更新响应消息中携带更新的 K_{AF} 。

当然，除了上述密钥更新响应消息之外，AAnF 还可以通过其他任意消息或指示信息将更新的 K_{AF} 发送至 AF，在此不作具体限定。

作为一种可选的实施方式，所述密钥更新响应消息还携带密钥生命周期，所述向 AAnF 发送密钥更新请求消息，具体包括：

根据所述密钥生命周期，向 AAnF 发送所述密钥更新请求消息。

在具体实施中，AF 能够根据该密钥生命周期确定 K_{AF} 在什么时间过期，例如：上述密钥生命周期可以是一个时间点，在达到该时间点时 K_{AF} 过期，或者上述密钥生命周期可以是预设时间长度， K_{AF} 在使用预设时间长度后过期。在此对密钥生命周期的具体形式不作限定。

在一种可选的实施方式中，上述根据所述密钥生命周期，向 AAnF 发送所述密钥更新请求消息，可以理解为：根据所述密钥生命周期，在确定当前的 K_{AF} 即将过期时，向 AAnF 发送所述密钥更新请求消息。例如：在当前的 K_{AF} 到期之前的预设时间（例如：1s、2s 等），向 AAnF 发送所述密钥更新请求消息。

本实施方式可以在当前的 K_{AF} 到期之前，提前发起 K_{AF} 的更新流程。

在另一种可选的实施方式中，上述根据所述密钥生命周期，向 AAnF 发送所述密钥更新请求消息，可以理解为：根据所述密钥生命周期，在确定当前的 K_{AF} 过期时，向 AAnF 发送所述密钥更新请求消息。例如：在确定当前

的 K_{AF} 到期后的预设时间（例如：0s、1s、2s 等），向 AAnF 发送所述密钥更新请求消息。

本实施方式可以在当前的 K_{AF} 到期之后，发起 K_{AF} 的更新流程。

本公开实施例中，提供了一种 AF 主动发起的密钥更新流程，能够主动更新 K_{AF} ，以避免相关技术中由于 UE 和网络之间没有进行新的初始认证而导致的 K_{AF} 过期的问题，进而能够保证 AKMA 业务的顺利进行。

请参阅图 3，本公开实施例提供的第二种更新方法，其执行主体可以是 AAnF，如图 3 所示，该更新方法可以包括以下步骤：

步骤 301、接收 AF 发送的密钥更新请求消息。

步骤 302、向所述 AF 发送更新的 K_{AF} 。

本公开实施例中的上述密钥更新请求消息、更新的 K_{AF} 分别与如图 2 所示方法实施例中的密钥更新请求消息、更新的 K_{AF} 具有相同的含义和作用，在此不再赘述。

本公开实施例同样能够在 AF 的触发下，主动更新 K_{AF} ，以避免相关技术中由于 UE 和网络之间没有进行新的初始认证而导致的 K_{AF} 过期的问题，进而能够保证 AKMA 业务的顺利进行。

可选地，所述 K_{AF} 携带于密钥更新响应消息中。

在一种可选的实施方式中，AAnF 在接收到 AF 发送的密钥更新请求消息之后，可以按照如图 2 所示方法实施例中 K_{AF} 的更新流程对 K_{AF} 进行更新，并在密钥更新响应消息中携带更新后的 K_{AF} 。

例如：在 K_{AF} 即将过期，或者 K_{AF} 已经过期的情况下，可以按照如图 2 所示方法实施例中 K_{AF} 的更新流程对 K_{AF} 进行更新，并在密钥更新响应消息中携带更新后的 K_{AF} 。

在实际应用中，可以在密钥更新请求消息中携带 A-KID、AF_ID 以及更新指示（refresh indicator）信息。

这样，AAnF 可以根据更新这些信息区分是初次请求获取 K_{AF} 还是用于请求更新 K_{AF} 。

可选的，所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

本实施方式中，通过新增更新参数，使得 K_{AF} 的更新不再依赖于 K_{AKMA} 的更新，而是可以通过更新参数的更新来实现 K_{AF} 的更新，从而不再需要通过 UE 和网络之间的新的初始认证来更新 K_{AKMA} ，便可以实现 K_{AF} 的更新。这种方式避免了对 5G 网络的主认证以及终端的改动。

可选的，在上述步骤 301 和步骤 302 之间，本公开实施例提供的更新方法还包括：

向 UDM 发送参数更新请求消息，指示所述 UDM 发送所述更新参数到用户设备 UE；

接收所述 UDM 发送的参数更新响应消息。

在具体实施中，UDM 可以存储 AKMA 服务订阅用户的 AKMA 订阅数据。在实施中，UDM 基于接收到的参数更新请求消息，可以发起 UPU 流程，以更新 UE 参数，该 UE 参数包括更新参数。这样，可以利用现有的 UPU 流程向 UE 下发更新参数，以使 UE 能够根据该更新参数推衍得到更新后的 K_{AF} ，即实现了利用现有的 UE 参数更新流程将更新后的更新参数同步至 UE。

另外，AAnF 在接收到 UDM 发送的参数更新响应消息时，可以基于更新参数和当前的 K_{AKMA} 推衍 K_{AF} 。这样，便可以通过步骤 302 将推衍得到的新的 K_{AF} 发送给 AF。

本实施方式中，可以利用现有的 UE 参数更新流程将更新后的更新参数同步至 UE，进而使 UE 和 AAnF 可以基于同步的更新参数推衍得到相同的 K_{AF} 。

换个方向来说，在实际应用中还可能存在 UPU 失败的情况，此时，因 UPU 失败，UE 没能够获取到更新参数，此时若 AAnF 直接执行步骤 302，则存在因 UPU 不成功，而导致 UE 和 AF 密钥不一致的问题。

而本实施方式中，AAnF 在收到 UDM 发送的参数更新响应消息之后，才执行步骤 302，能够避免因 UPU 不成功，则导致的 UE 和 AF 密钥不一致的问题。

可选的，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

本实施方式中，利用已有密钥获取请求消息来实现 K_{AF} 更新流程，并通

过密钥获取请求消息中的保留字段来实现更新指示。

本公开实施例中用于 AAnF 的更新方法与如图 2 所示用于 AF 的更新方法相对应，且能够取得与如图 2 所示用于 AF 的更新方法相同的有益效果，在此不再赘述。

请参阅图 4，本公开实施例提供的第三种更新方法，其执行主体可以是 UDM，如图 4 所示，该更新方法可以包括以下步骤：

步骤 401、接收 AAnF 发送的参数更新请求消息。

步骤 402、发送更新参数到 UE，所述更新参数用于所述 UE 结合所述 UE 当前存储的 K_{AKMA} 生成会话密钥 K_{AF} 。

可选的，在上述步骤 402 之后，所述更新方法还包括：

向所述 AAnF 发送参数更新响应消息。

本公开实施例中的上述参数更新请求消息、更新参数和参数更新响应消息分别与如图 3 所示方法实施例中的参数更新请求消息、更新参数和参数更新响应消息具有相同的含义，在此不再赘述。

本公开实施例能够取得与如图 3 所示更新方法实施例相同的有益效果，且可以利用现有的 UE 参数更新流程将更新后的更新参数同步至 UE，进而使 UE 和 AAnF 可以基于同步的更新参数推衍得到相同的 K_{AF} 。

请参阅图 5，本公开实施例提供的第四种更新方法，其执行主体可以是 UE，如图 5 所示，该更新方法可以包括以下步骤：

步骤 501、接收应用功能实体 AF 发送的密钥更新指示消息，所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

本公开实施例中的上述密钥更新指示消息与如图 2 所示方法实施例中的密钥更新指示消息具有相同的含义。

可选的，本公开实施例提供的更新方法还包括：

接收 UDM 发送的更新参数；所述 K_{AF} 为至少根据所述更新参数和所述 UE 当前存储的 K_{AKMA} 生成的密钥。

本步骤与如图 4 所示方法实施例中的步骤 402 相对应，在此不再赘述。

本公开实施例能够取得与如图 2 至图 4 中任一项所示更新方法实施例相同的有益效果，且能够主动更新 K_{AF} ，以避免相关技术中由于 UE 和网络之间

没有进行新的初始认证而导致的 K_{AF} 过期的问题, 进而能够保证 AKMA 业务的顺利进行。

为了便于理解本公开实施例通过的更新方法, 以如图 6 所示 UE 与网络侧设备之间的交互过程为例, 对本公开实施例提供的更新方法进行举例说明, 在更新 K_{AF} 的过程中, UE 与网络侧设备之间可以进行以下交互:

步骤 1, 在 K_{AF} 即将过期时, 由 AF 向 AAnF 发送密钥更新请求消息 (Naanf_AKMA_ApplicationKey_Get_Request)。

本步骤中, 上述密钥更新请求消息携带更新指示 (refresh indicator) 信息, 以指示 AAnF 进行 K_{AF} 的更新。上述密钥更新请求消息还可以携带 A-KID 和 AF_ID。

步骤 2, AAnF 向 UDM 发送参数更新请求消息。

本步骤中, 参数更新请求消息可以携带更新参数, 要求 UDM 向 UE 下发该更新参数。

步骤 3, UDM 执行 UPU 流程。

本步骤中, UDM 在执行 UPU 流程的过程中, 在有更新参数的情况下, 将该更新参数发送给 UE。

步骤 4, UPU 流程执行结束, UDM 向 AAnF 返回参数更新响应消息。

步骤 5, AAnF 基于更新参数和 K_{AKMA} 推衍 K_{AF} 。

本步骤中, AAnF 在收到 UDM 发送的参数更新响应消息后, 可以采用以下推衍公式, 实现基于 K_{AKMA} 推衍 K_{AF} :

$$K_{AF} = \text{KDF} (K_{AKMA}, \text{AF_ID}, \text{freshness parameter})。$$

步骤 6, AAnF 向 AF 发送密钥更新响应消息。

本步骤中, 上述密钥更新响应消息可以携带 AAnF 推演出的新的 K_{AF} 及其密钥生命周期。

步骤 7. AF 向 UE 发送指示消息。

本步骤中, 收到更新后的 K_{AF} 后, 通过上述指示消息通知 UE 密钥更新成功, 并指示 UE 根据收到的更新参数在终端侧进行密钥推衍。且 UE 可以采用与步骤 5 中相同的推衍公式, 来根据收到的更新参数在终端侧进行密钥推衍。

如图 6 所示实施方式下, 在 K_{AF} 密钥推衍过程中, 新增了更新参数, 通过新增更新参数使得 K_{AF} 的更新不再依赖于 K_{AKMA} 的更新, 而是通过更新参数的更新来实现 K_{AF} 的更新, 且该更新参数的传递可以利用现有的 UPU 流程。

请参阅图 7, 是本公开实施例提供的一种 AF 的结构示意图, 如图 7 所示, 该 AF 700 包括:

第一发送模块 701, 用于向 AAnF 发送密钥更新请求消息;

第一接收模块 702, 用于接收所述 AAnF 发送的更新的 K_{AF} 。

可选的, 所述 K_{AF} 携带于密钥更新响应消息中。

可选的, AF 700 还包括:

第二发送模块, 用于向 UE 发送指示消息, 指示所述 UE 更新 K_{AF} 。

可选的, 所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

可选的, 所述密钥更新请求消息为密钥获取请求消息, 所述密钥获取请求消息中携带密钥更新指示符。

可选的, 所述密钥更新响应消息还携带密钥生命周期, 第一发送模块 701, 具体用于:

根据所述密钥生命周期, 向 AAnF 发送所述密钥更新请求消息。

本公开实施例提供的 AF 700 具体可以是应用如图 2 所示更新方法的 AF, 且该 AF 700 能够取得与如图 2 所示方法实施例相同的有益效果, 在此不作具体阐述。

请参阅图 8, 是本公开实施例提供的 AAnF 的结构示意图, 如图 8 所示, 该 AAnF 800 包括:

第二接收模块 801, 用于接收 AF 发送的密钥更新请求消息;

第三发送模块 802, 用于向所述 AF 发送更新的 K_{AF} 。

可选的, 所述 K_{AF} 携带于密钥更新响应消息中。

可选的, 所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

可选的, AAnF 800 还包括:

第四发送模块, 用于向 UDM 发送参数更新请求消息, 指示所述 UDM 发

送所述更新参数到 UE;

第三接收模块, 用于接收所述 UDM 发送的参数更新响应消息。

可选的, 所述密钥更新请求消息为密钥获取请求消息, 所述密钥获取请求消息中携带密钥更新指示符。

本公开实施例提供的 AAnF 800 具体可以是应用如图 3 所示更新方法的 AAnF, 且该 AAnF 800 能够取得与如图 3 所示方法实施例相同的有益效果, 在此不作具体阐述。

请参阅图 9, 是本公开实施例提供的 UDM 的结构示意图, 如图 9 所示, 该 UDM 900 包括:

第四接收模块 901, 用于接收 AAnF 发送的参数更新请求消息;

第五发送模块 902, 用于发送更新参数到 UE, 所述更新参数用于所述 UE 结合所述 UE 当前存储的 K_{AKMA} 生成 K_{AF} 。

可选的, UDM 900 还包括:

第六发送模块, 用于向所述 AAnF 发送参数更新响应消息。

本公开实施例提供的 UDM 900 具体可以是应用如图 4 所示更新方法的 UDM, 且该 UDM 900 能够取得与如图 4 所示方法实施例相同的有益效果, 在此不作具体阐述。

请参阅图 10, 是本公开实施例提供的一种网络侧设备的结构示意图, 如图 10 所示, 该网络侧设备包括: 总线 1001、收发机 1002、天线 1003、总线接口 1004、处理器 1005 和存储器 1006。

在第一种实施方式中, 上述网络侧设备可以是 AF:

收发机 1002, 用于向 AAnF 发送密钥更新请求消息;

收发机 1002, 还用于接收所述 AAnF 发送的更新的 K_{AF} 。

可选地, 所述 K_{AF} 携带于密钥更新响应消息中。

可选地, 收发机 1002, 还用于向 UE 发送指示消息, 指示所述 UE 更新 K_{AF} 。

可选地, 所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

可选地, 所述密钥更新请求消息为密钥获取请求消息, 所述密钥获取请

求消息中携带密钥更新指示符。

可选地，所述密钥更新响应消息还携带密钥生命周期，收发机 1002 执行的所述向 AAnF 发送密钥更新请求消息，具体包括：

根据所述密钥生命周期，向 AAnF 发送所述密钥更新请求消息。

本实施方式中，网络侧设备能够实现图 2 所示方法实施例中 AF 实现的各个过程，且具有相同的有益效果，为避免重复，这里不再赘述。

在第二种实施方式中，上述网络侧设备可以是 AAnF：

收发机 1002，用于接收 AF 发送的密钥更新请求消息；

收发机 1002，还用于向所述 AF 发送更新的 K_{AF} 。

可选地，所述 K_{AF} 携带于密钥更新响应消息中。

可选地，所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的 K_{AKMA} 生成的密钥。

可选地，收发机 1002 在执行所述接收 AF 发送的密钥更新请求消息和向所述 AF 发送更新的 K_{AF} 之间，还用于：

向 UDM 发送参数更新请求消息，指示所述 UDM 发送所述更新参数到 UE；

接收所述 UDM 发送的参数更新响应消息。

可选地，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

本实施方式中，网络侧设备能够实现图 3 所示方法实施例中 AAnF 实现的各个过程，且具有相同的有益效果，为避免重复，这里不再赘述。

在第三种实施方式中，上述网络侧设备可以是 UDM：

收发机 1002，用于接收 AAnF 发送的参数更新请求消息；

收发机 1002，还用于发送更新参数到 UE，所述更新参数用于所述 UE 结合所述 UE 当前存储的 K_{AKMA} 生成会话密钥 K_{AF} 。

可选地，收发机 1002 在执行所述发送更新参数到 UE 之后，还用于：

向所述 AAnF 发送参数更新响应消息。

本实施方式中，网络侧设备能够实现图 4 所示方法实施例中 UDM 实现的各个过程，且具有相同的有益效果，为避免重复，这里不再赘述。

在图 10 中, 总线架构 (用总线 1001 来代表), 总线 1001 可以包括任意数量的互联的总线和桥, 总线 1001 将包括由处理器 1005 代表的一个或多个处理器和存储器 1006 代表的存储器的各种电路链接在一起。总线 1001 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 1004 在总线 1001 和收发机 1002 之间提供接口。收发机 1002 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 1005 处理的数据通过天线 1003 在无线介质上进行传输, 进一步, 天线 1003 还接收数据并将数据传送给处理器 1005。

处理器 1005 负责管理总线 1001 和通常的处理, 还可以提供各种功能, 包括定时, 外围接口, 电压调节、电源管理以及其他控制功能。而存储器 1006 可以被用于存储处理器 1005 在执行操作时所使用的数据。

可选的, 处理器 1005 可以是中央处理器 (Central Processing Unit, CPU)、专用集成电路 (Application Specific Integrated Circuit, ASIC)、现场可编程逻辑门阵列 (Field Programmable Gate Array, FPGA) 或复杂可编程逻辑器件 (Complex Programmable logic device, CPLD)。

优选的, 本公开实施例还提供一种网络侧设备, 包括处理器 1005, 存储器 1006, 存储在存储器 1006 上并可在所述处理器 1005 上运行的计算机程序, 该计算机程序被处理器 1005 执行时实现上述图 2 至图 4 中任一项所示更新方法实施例的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

请参阅图 11, 是本公开实施例提供的 UE 的结构示意图, 如图 11 所示, 该 UE 1100 包括:

第五接收模块 1101, 用于接收 AF 发送的密钥更新指示消息, 所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

可选的, UE 1100 还包括:

第六接收模块, 用于接收 UDM 发送的更新参数; 所述 K_{AF} 为至少根据所述更新参数和所述 UE 当前存储的 K_{AKMA} 生成的密钥。

本公开实施例提供的 UE 1100 具体可以是应用如图 5 所示更新方法的 UE，且该 UE 1100 能够取得与如图 5 所示方法实施例相同的有益效果，在此不作具体阐述。

请参阅图 12，是示意本公开实施例提供的一种终端设备的结构图，如图 12 所示，该第一用户设备包括：总线 1201、收发机 1202、天线 1203、总线接口 1204、处理器 1205 和存储器 1206。

收发机 1202，用于接收 AF 发送的密钥更新指示消息，所述密钥更新指示消息用于指示所述 UE 更新 K_{AF} 。

可选地，收发机 1202，还用于：

接收 UDM 发送的更新参数；所述 K_{AF} 为至少根据所述更新参数和所述 UE 当前存储的 K_{AKMA} 生成的密钥。

本实施方式中，终端设备能够实现图 5 所示方法实施例中 UE 实现的各个过程，且具有相同的有益效果，为避免重复，这里不再赘述。

在图 12 中，总线架构（用总线 1201 来代表），总线 1201 可以包括任意数量的互联的总线和桥，总线 1201 将包括由处理器 1205 代表的一个或多个处理器和存储器 1206 代表的存储器的各种电路链接在一起。总线 1201 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 1204 在总线 1201 和收发机 1202 之间提供接口。收发机 1202 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 1205 处理的数据通过天线 1203 在无线介质上进行传输，进一步，天线 1203 还接收数据并将数据传送给处理器 1205。

处理器 1205 负责管理总线 1201 和通常的处理，还可以提供各种功能，包括定时，外围接口，电压调节、电源管理以及其他控制功能。而存储器 1206 可以被用于存储处理器 1205 在执行操作时所使用的数据。

可选的，处理器 1205 可以是 CPU、ASIC、FPGA 或 CPLD。

优选的，本公开实施例还提供一种终端设备，包括处理器 1205，存储器 1206，存储在存储器 1206 上并可在所述处理器 1205 上运行的计算机程序，

该计算机程序被处理器 1205 执行时实现上述图 5 所示更新方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

本公开实施例还提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述图 2 至图 5 中任一项所示更新方法实施的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

其中，所述的计算机可读存储介质，如只读存储器 (Read-Only Memory, ROM)、随机存取存储器 (Random Access Memory, RAM)、磁碟或者光盘等。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本公开的技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端（可以是手机，计算机，服务器，空调器，或者网络设备等等）执行本公开各个实施例所述的方法。

上面结合附图对本公开的实施例进行了描述，但是本公开并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本公开的启示下，在不脱离本公开宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本公开的保护之内。

权利要求书

1、一种更新方法，应用于应用功能实体 AF，所述更新方法包括：

向会话密钥管理锚点功能实体 AAnF 发送密钥更新请求消息；

接收所述 AAnF 发送的更新的会话密钥 K_{AF} 。

2、根据权利要求 1 所述的更新方法，其中，所述 K_{AF} 携带于密钥更新响应消息中。

3、根据权利要求 1 所述的更新方法，其中，在所述接收所述 AAnF 发送的更新的 K_{AF} 之后，还包括：

向用户设备 UE 发送指示消息，指示所述 UE 更新 K_{AF} 。

4、根据权利要求 1 所述的更新方法，其中，所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

5、根据权利要求 1 所述的更新方法，其中，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

6、根据权利要求 2 所述的更新方法，其中，所述密钥更新响应消息还携带密钥生命周期，所述向 AAnF 发送密钥更新请求消息，具体包括：

根据所述密钥生命周期，向 AAnF 发送所述密钥更新请求消息。

7、一种更新方法，应用于会话密钥管理锚点功能实体 AAnF，所述更新方法包括：

接收应用功能实体 AF 发送的密钥更新请求消息；

向所述 AF 发送更新的会话密钥 K_{AF} 。

8、根据权利要求 7 所述的更新方法，其中，所述 K_{AF} 携带于密钥更新响应消息中。

9、根据权利要求 8 所述的更新方法，其中，所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

10、根据权利要求 9 所述的更新方法，其中，所述接收 AF 发送的密钥更新请求消息和所述向所述 AF 发送更新的 K_{AF} 之间，还包括：

向统一数据管理功能实体 UDM 发送参数更新请求消息,指示所述 UDM 发送所述更新参数到用户设备 UE;

接收所述 UDM 发送的参数更新响应消息。

11、根据权利要求 7 所述的更新方法,其中,所述密钥更新请求消息为密钥获取请求消息,所述密钥获取请求消息中携带密钥更新指示符。

12、一种更新方法,应用于统一数据管理功能实体 UDM,所述更新方法包括:

接收会话密钥管理锚点功能实体 AAnF 发送的参数更新请求消息;

发送更新参数到用户设备 UE,所述更新参数用于所述 UE 结合所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成会话密钥 K_{AF} 。

13、根据权利要求 12 所述的更新方法,其中,所述发送更新参数到 UE 之后,所述更新方法还包括:

向所述 AAnF 发送参数更新响应消息。

14、一种更新方法,应用于用户设备 UE,所述更新方法包括:

接收应用功能实体 AF 发送的密钥更新指示消息,所述密钥更新指示消息用于指示所述 UE 更新会话密钥 K_{AF} 。

15、根据权利要求 14 所述的更新方法,还包括:

接收统一数据管理功能实体 UDM 发送的更新参数;所述 K_{AF} 为至少根据所述更新参数和所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

16、一种应用功能实体 AF,包括:

第一发送模块,用于向会话密钥管理锚点功能实体 AAnF 发送密钥更新请求消息;

第一接收模块,用于接收所述 AAnF 发送的更新的会话密钥 K_{AF} 。

17、根据权利要求 16 所述的 AF,还包括:

第二发送模块,用于向用户设备 UE 发送指示消息,指示所述 UE 更新 K_{AF} 。

18、根据权利要求 17 所述的 AF,其中,所述 K_{AF} 为至少根据更新参数

和所述 AAnF 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

19、根据权利要求 16 所述的 AF，其中，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

20、一种会话密钥管理锚点功能实体 AAnF，包括：

第二接收模块，用于接收应用功能实体 AF 发送的密钥更新请求消息；

第三发送模块，用于向所述 AF 发送更新的会话密钥 K_{AF} 。

21、根据权利要求 20 所述的 AAnF，其中，所述 K_{AF} 为至少根据更新参数和所述 AAnF 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

22、根据权利要求 20 所述的 AAnF，其中，所述密钥更新请求消息为密钥获取请求消息，所述密钥获取请求消息中携带密钥更新指示符。

23、一种统一数据管理功能实体 UDM，包括：

第四接收模块，用于接收会话密钥管理锚点功能实体 AAnF 发送的参数更新请求消息；

第五发送模块，用于发送更新参数到用户设备 UE，所述更新参数用于所述 UE 结合所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成会话密钥 K_{AF} 。

24、根据权利要求 23 所述的 UDM，还包括：

第六发送模块，用于向所述 AAnF 发送参数更新响应消息。

25、一种用户设备 UE，包括：

第五接收模块，用于接收应用功能实体 AF 发送的密钥更新指示消息，所述密钥更新指示消息用于指示所述 UE 更新会话密钥 K_{AF} 。

26、根据权利要求 25 所述的 UE，还包括：

第六接收模块，用于接收统一数据管理功能实体 UDM 发送的更新参数；所述 K_{AF} 为至少根据所述更新参数和所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成的密钥。

27、一种网络侧设备，包括：处理器和收发机；

所述收发机，用于向会话密钥管理锚点功能实体 AAnF 发送密钥更新请

求消息；

所述收发机，还用于接收所述 AAnF 发送的更新的会话密钥 K_{AF} ；

和/或

所述收发机，用于接收应用功能实体 AF 发送的密钥更新请求消息；

所述收发机，还用于向所述 AF 发送更新的会话密钥 K_{AF} ；

和/或

所述收发机，用于接收会话密钥管理锚点功能实体 AAnF 发送的参数更新请求消息；

所述收发机，还用于发送更新参数到用户设备 UE，所述更新参数用于所述 UE 结合所述 UE 当前存储的应用层认证和会话密钥管理 AKMA 中间密钥 K_{AKMA} 生成会话密钥 K_{AF} 。

28、一种用户设备 UE，包括：处理器和收发机；

所述收发机，用于接收应用功能实体 AF 发送的密钥更新指示消息，所述密钥更新指示消息用于指示所述 UE 更新会话密钥 K_{AF} 。

29、一种网络侧设备，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述计算机程序被所述处理器执行时实现如权利要求 1 至 6 中任一项所述的更新方法中的步骤，或者实现如权利要求 7 至 11 中任一项所述的更新方法中的步骤，或者实现如权利要求 12 或 13 所述的更新方法中的步骤。

30、一种终端设备，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述计算机程序被所述处理器执行时实现如权利要求 14 或 15 所述的更新方法中的步骤。

31、一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，其中，所述计算机程序被处理器执行时，实现如权利要求 1 至 6 中任一项所述的更新方法中的步骤，或者实现如权利要求 7 至 11 中任一项所述的更新方法中的步骤，或者实现如权利要求 12 或 13 所述的更新方法中的步骤，或者实现如权利要求 14 或 15 所述的更新方法中的步骤。

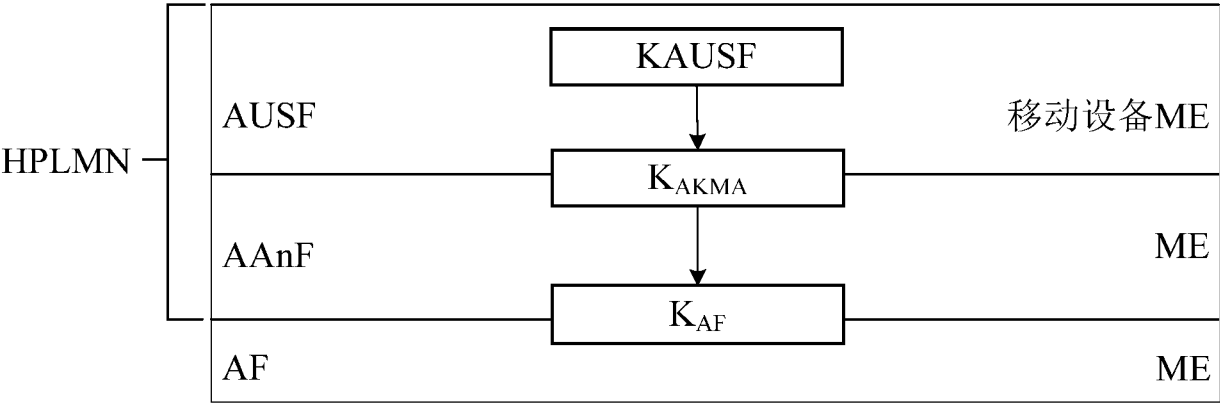


图 1

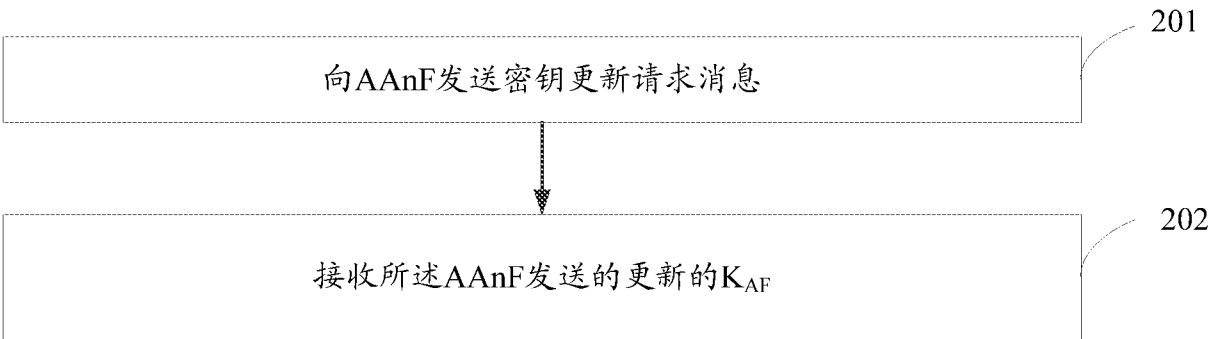


图 2

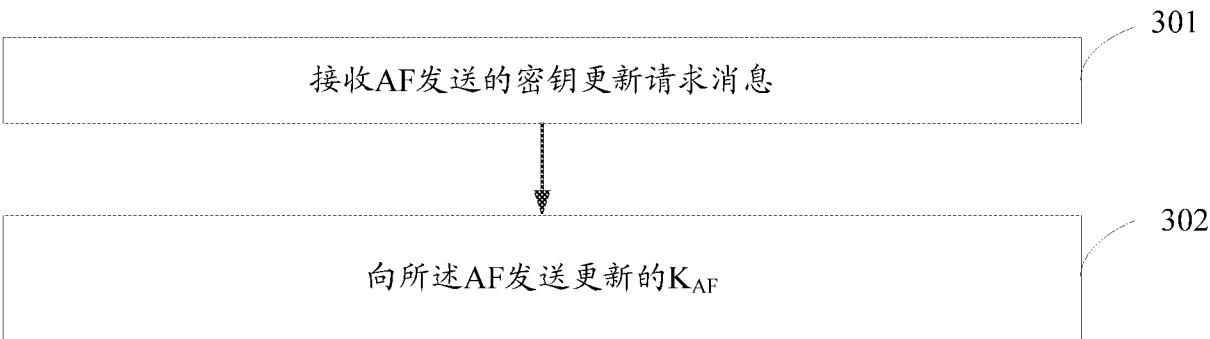


图 3

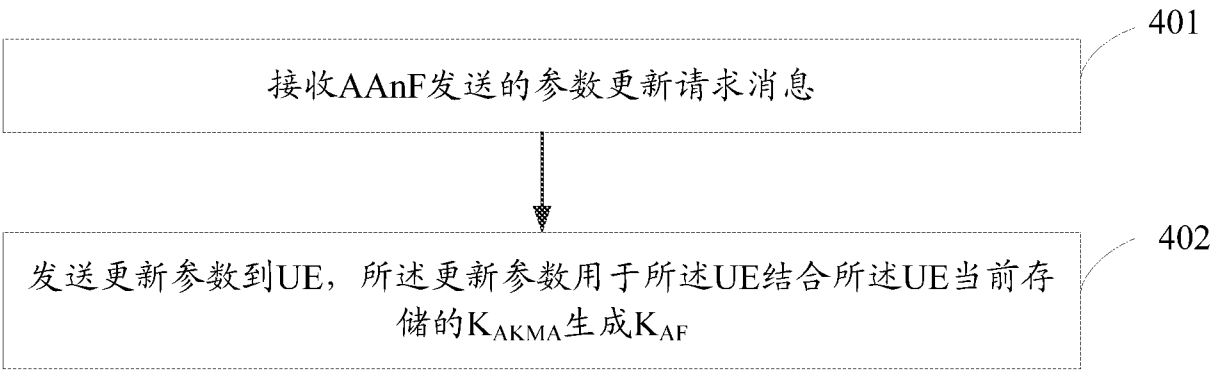


图 4

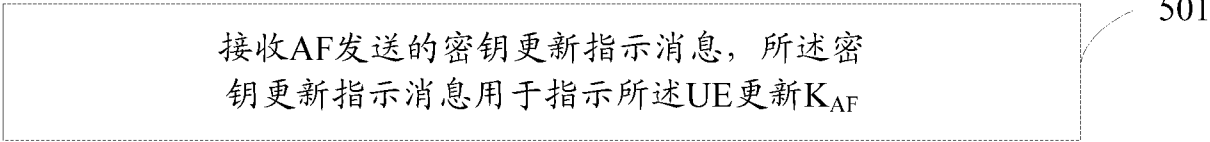


图 5

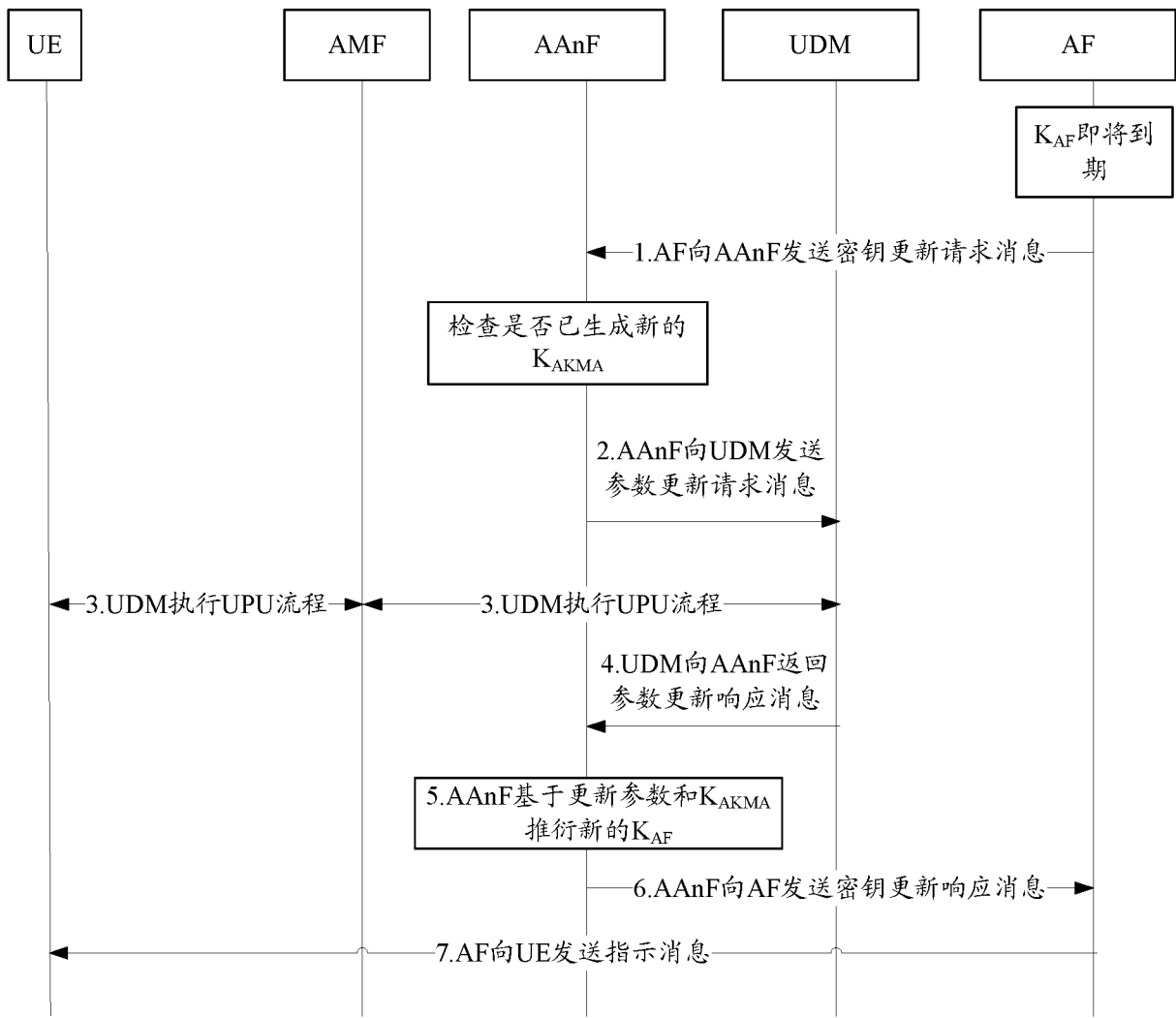


图 6

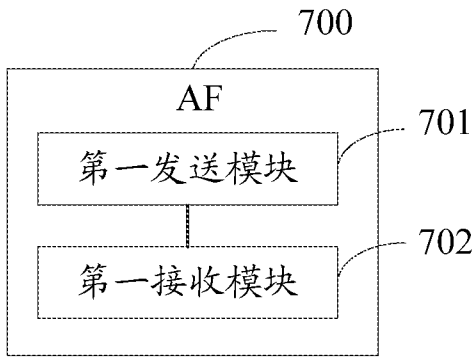


图 7

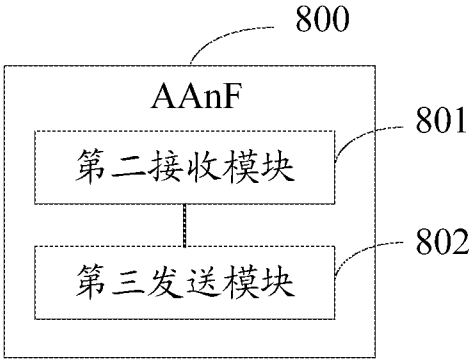


图 8

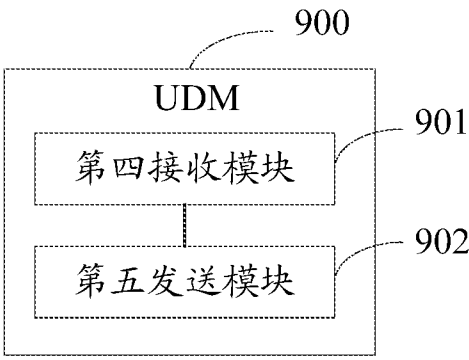


图 9

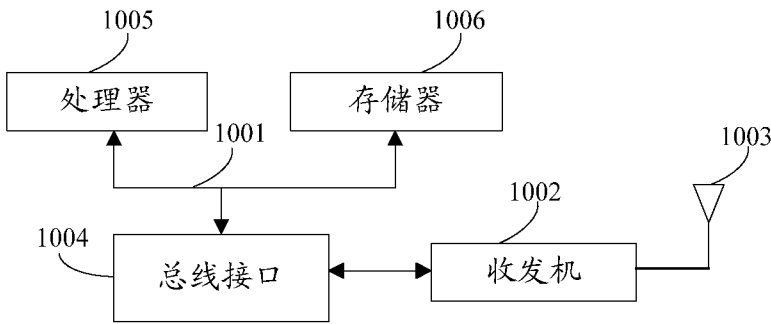


图 10

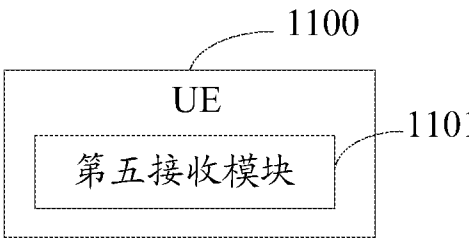


图 11

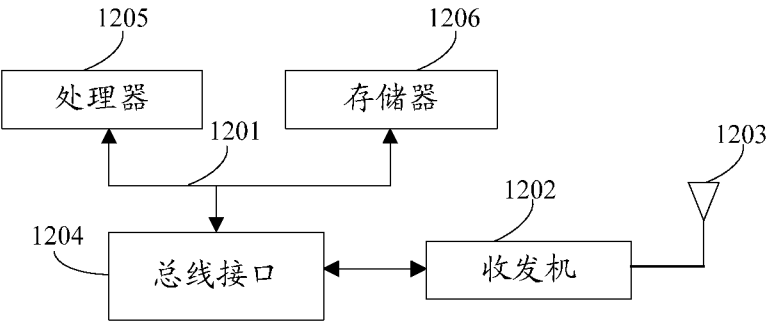


图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/111148

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; 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)

EPODOC, WPI, CNKI, CNPAT, 3GPP, IEEE: 应用, 密钥, 更新, 会话, AF, AAnF, UE, 终端, AKMA, 指示, 锚点, 功能实体, UDM, 参数, 中间, parameter, ID, indicat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 113163402 A (HUAWEI TECHNOLOGIES CO., LTD.) 23 July 2021 (2021-07-23) description, paragraphs [0080]-[0131]	1-11, 14-22, 25-31
X	WO 2021093162 A1 (ZTE CORP.) 20 May 2021 (2021-05-20) description, pages 20-33	12-13, 23-24, 29, 31
X	ERICSSON. "Several clarifications and editorials" <i>3GPP TSG-SA3 Meeting #100e, S3-202039-r1</i> , 28 August 2020 (2020-08-28), sections 4 and 6	1-11, 14-22, 25-31
X	ERICSSON. "pCR to TS 33.535: Update of the AKMA procedures" <i>3GPP TSG-SA3 Meeting #98bis-e, S3-200741</i> , 17 April 2020 (2020-04-17), section 6	12-13, 23-24, 29, 31
A	CN 113225176 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 August 2021 (2021-08-06) entire document	1-31
A	WO 2021098115 A1 (ZTE CORP.) 27 May 2021 (2021-05-27) entire document	1-31



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

23 September 2022

Date of mailing of the international search report

27 October 2022

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/CN2022/111148

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113163402	A	23 July 2021	WO	2021148027	A1	29 July 2021
WO	2021093162	A1	20 May 2021	CA	3159134	A1	20 May 2021
				CN	115004742	A	02 September 2022
CN	113225176	A	06 August 2021	WO	2021155758	A1	12 August 2021
WO	2021098115	A1	27 May 2021	KR	20220113978	A	17 August 2022

国际检索报告

国际申请号

PCT/CN2022/111148

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; 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))

EPDOC, WPI, CNKI, CNPAT, 3GPP, IEEE: 应用, 密钥, 更新, 会话, AF, AAnF, UE, 终端, AKMA, 指示, 锚点, 功能实体, UDM, 参数, 中间, parameter, ID, indicat+

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
X	CN 113163402 A (华为技术有限公司) 2021年7月23日 (2021 - 07 - 23) 说明书第[0080]-[0131]段	1-11, 14-22, 25-31
X	W0 2021093162 A1 (ZTE CORPORATION) 2021年5月20日 (2021 - 05 - 20) 说明书第20-33页	12-13, 23-24, 29, 31
X	ERICSSON. "Several clarifications and editorials" 3GPP TSG-SA3 Meeting #100e S3-202039-r1, 2020年8月28日 (2020 - 08 - 28), 第4, 6部分	1-11, 14-22, 25-31
X	ERICSSON. "pCR to TS 33.535: Update of the AKMA procedures" 3GPP TSG-SA3 Meeting #98bis-e S3-200741, 2020年4月17日 (2020 - 04 - 17), 第6部分	12-13, 23-24, 29, 31
A	CN 113225176 A (华为技术有限公司) 2021年8月6日 (2021 - 08 - 06) 全文	1-31
A	W0 2021098115 A1 (ZTE CORPORATION) 2021年5月27日 (2021 - 05 - 27) 全文	1-31

☐ 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

2022年9月23日

国际检索报告邮寄日期

2022年10月27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

授权官员

侯艳兰

电话号码 86-(10)-53961644

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/111148

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	113163402	A	2021年7月23日	WO	2021148027	A1	2021年7月29日
WO	2021093162	A1	2021年5月20日	CA	3159134	A1	2021年5月20日
				CN	115004742	A	2022年9月2日
CN	113225176	A	2021年8月6日	WO	2021155758	A1	2021年8月12日
WO	2021098115	A1	2021年5月27日	KR	20220113978	A	2022年8月17日