

(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 11 月 28 日 (28.11.2024)



(10) 国际公布号
WO 2024/239231 A1

(51) 国际专利分类号:
H04W 12/069 (2021.01)

(21) 国际申请号: PCT/CN2023/095769

(22) 国际申请日: 2023 年 5 月 23 日 (23.05.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **OPPO** 广东移动通信有限公司 (**GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.**) [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: 熊丽晖 (**XIONG, Lihui**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。 甘露 (**GAN, Lu**); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

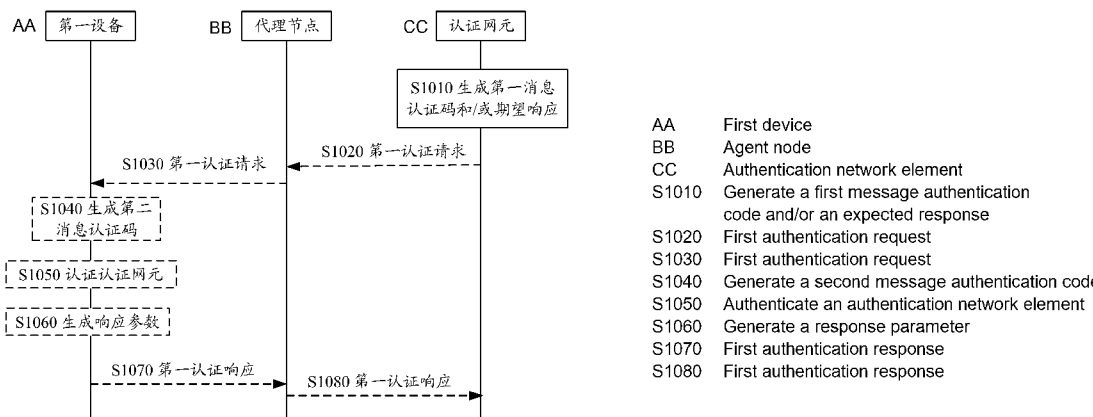
(74) 代理人: 北京布瑞知识产权代理有限公司 (**BEIJING BRIGHT IP AGENCY CO., LTD.**); 中国北京市昌平区七北路 42 号院 3 号楼 12 层 3 单元 1202, Beijing 102200 (CN)。

(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, MG, MK, MN, MU, 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

(54) **Title:** METHOD AND APPARATUS FOR AUTHENTICATION

(54) 发明名称: 认证方法及装置



(57) **Abstract:** The present application provides a method and an apparatus for authentication. The method comprises: a first device receiving a first authentication request from an agent node, wherein the first authentication request comprises a first message authentication code, and the first message authentication code is generated by an authentication network element; the first device generating a second message authentication code on the basis of a first key generation algorithm and a first parameter; the first device authenticating the authentication network element on the basis of the first message authentication code and the second message authentication code; the first device generating a response parameter in the condition that the authentication network element is successfully authenticated; and the first device sending a first authentication response to the agent node, wherein the first authentication response comprises the response parameter, and the response parameter is configured for authenticating the first device.

(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))。

(57) 摘要: 本申请提供了一种认证方法及装置。该方法包括: 第一设备接收来自代理节点的第一认证请求, 所述第一认证请求中包括第一消息认证码, 所述第一消息认证码由认证网元生成; 所述第一设备基于第一密钥生成算法和第一参数生成第二消息认证码; 所述第一设备基于所述第一消息认证码和所述第二消息认证码认证所述认证网元; 在所述认证网元认证成功的情况下, 所述第一设备生成响应参数; 所述第一设备向所述代理节点发送第一认证响应, 所述第一认证响应中包括所述响应参数, 所述响应参数用于认证所述第一设备。

说明书

认证方法及装置

技术领域

本申请涉及通信技术领域，并且更为具体地，涉及一种认证方法及装置。

背景技术

为了提高通信安全性，终端设备在与网络侧进行通信之前，可以先与网络侧进行认证与密钥协商。在引入第一设备（如零功耗终端）后，由于第一设备的计算能力较低，第一设备该如何与网络侧进行认证与密钥协商流程，目前还没有明确的规定。

发明内容

本申请提供一种认证方法及装置。下面对本申请涉及的各个方面进行详细介绍。

第一方面，提供了一种认证方法，包括：第一设备接收来自代理节点的第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成；所述第一设备基于第一密钥生成算法和第一参数生成第二消息认证码；所述第一设备基于所述第一消息认证码和所述第二消息认证码认证所述认证网元；在所述认证网元认证成功的情况下，所述第一设备生成响应参数；所述第一设备向所述代理节点发送第一认证响应，所述第一认证响应中包括所述响应参数，所述响应参数用于认证所述第一设备。

第二方面，提供了一种认证方法，包括：代理节点向第一设备发送第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成，所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成；所述代理节点接收来自所述第一设备的第一认证响应，所述第一认证响应中包括响应参数，所述响应参数用于认证所述第一设备，所述响应参数在所述认证网元认证成功的情况下生成。

第三方面，提供了一种认证方法，包括：认证网元生成第一消息认证码和期望响应，所述期望响应用于认证第一设备，所述第一消息认证码基于第一密钥生成算法和第一参数生成；所述认证网元向所述代理节点发送第一认证请求，所述第一认证请求中包括所述第一消息认证码，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成。

第四方面，提供了一种认证方法，包括：接入网设备向第一设备发送第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成，所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成；所述接入网设备接收来自所述第一设备的第一认证响应，所述第一认证响应中包括响应参数，所述响应参数用于认证所述第一设备，所述响应参数在所述认证网元认证成功的情况下生成。

第五方面，提供一种设备，所述设备为第一设备，所述第一设备包括：接收单元，用于接收来自代理节点的第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成；生成单元，用于基于第一密钥生成算法和第一参数生成第二消息认证码；认证单元，用于基于所述第一消息认证码和所述第二消息认证码认证所述认证网元；所述生成单元，还用于在所述认证网元认证成功的情况下，所述第一设备生成响应参数；发送单元，用于向所述代理节点发送第一认证响应，所述第一认证响应中包括所述响应参数，所述响应参数用于认证所述第一设备。

第六方面，提供一种代理节点，包括：发送单元，用于向第一设备发送第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成，所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成；接收单元，用于接收来自所述第一设备的第一认证响应，所述第一认证响应中包括响应参数，所述响应参数用于认证所述第一设备，所述响应参数在所述认证网元认证成功的情况下生成。

第七方面，提供一种认证网元，包括：生成单元，用于生成第一消息认证码和期望响应，所述期望响应用于认证第一设备，所述第一消息认证码基于第一密钥生成算法和第一参数生成；发送单元，用于向所述代理节点发送第一认证请求，所述第一认证请求中包括所述第一消息认证码，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成。

第八方面，提供一种接入网设备，包括：发送单元，用于向第一设备发送第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成，所述第一消息认证码和第二消息

息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成,所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成;接收单元,用于接收来自所述第一设备的第一认证响应,所述第一认证响应中包括响应参数,所述响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

第九方面,提供一种设备,包括存储器和处理器,所述存储器用于存储程序,所述处理器用于调用所述存储器中的程序,以执行如第一方面所述的方法。

第十方面,提供一种代理节点,包括存储器和处理器,所述存储器用于存储程序,所述处理器用于调用所述存储器中的程序,以执行第二方面所述的方法。

第十一方面,提供一种认证网元,包括存储器和处理器,所述存储器用于存储程序,所述处理器用于调用所述存储器中的程序,以执行如第三方面所述的方法。

第十二方面,提供一种接入网设备,包括存储器和处理器,所述存储器用于存储程序,所述处理器用于调用所述存储器中的程序,以执行第四方面所述的方法。

第十三方面,提供一种装置,包括处理器,用于从存储器中调用程序,以执行如第一方面至第四方面中任一方面所述的方法。

第十四方面,提供一种芯片,包括处理器,用于从存储器调用程序,使得安装有所述芯片的设备执行如第一方面至第四方面中任一方面所述的方法。

第十五方面,提供一种计算机可读存储介质,其上存储有程序,所述程序使得计算机执行如第一方面至第四方面中任一方面所述的方法。

第十六方面,提供一种计算机程序产品,包括程序,所述程序使得计算机执行如第一方面至第四方面中任一方面所述的方法。

第十七方面,提供一种计算机程序,所述计算机程序使得计算机执行如第一方面至第四方面中任一方面所述的方法。

第一设备接收来自代理节点的第一认证请求,所述第一认证请求中包括第一消息认证码,所述第一消息认证码由认证网元生成;所述第一设备基于第一密钥生成算法和第一参数生成第二消息认证码;所述第一设备基于所述第一消息认证码和所述第二消息认证码认证所述认证网元;在所述认证网元认证成功的情况下,所述第一设备生成响应参数;所述第一设备向所述代理节点发送第一认证响应,所述第一认证响应中包括所述响应参数,所述响应参数用于认证所述第一设备。

本申请通过基于第一密钥生成算法和第一参数生成消息认证码(如第二消息认证码),以认证认证网元,从而为第一设备与网络侧间的认证提供了一种明确的方案。

附图说明

图1是本申请实施例应用的无线通信系统100。

图2是一种初始认证的流程示意图。

图3是一种生成AKMA密钥的流程示意图。

图4是一种生成应用密钥的流程示意图。

图5是本申请实施例涉及的各种密钥的衍生过程的示意图。

图6是本申请实施例涉及的各个参数的生成方式的示意图。

图7是本申请实施例提供的一种混合通信系统的示意图。

图8是本申请实施例提供的一种基于3GPP安全凭证的通信系统。

图9是本申请实施例提供的一种基于非3GPP安全凭证的通信系统。

图10是本申请实施例提供的一种认证方法的流程示意图。

图11是本申请实施例提供的一种基于代理节点和3GPP安全凭证的认证方法的流程示意图。

图12是基于图11的生成AKMA密钥的流程示意图。

图13是基于图12的生成应用密钥的流程示意图。

图14是本申请实施例提供的另一种认证方法的流程示意图。

图15是本申请实施例提供的一种基于3GPP安全凭证的认证方法的流程示意图。

图16是基于图15的生成应用密钥的流程示意图。

图17是本申请实施例提供的另一种认证方法的流程示意图。

图18是本申请实施例提供的一种基于代理节点和非3GPP安全凭证的认证方法的流程示意图。

图19是本申请实施例提供的另一种认证方法的流程示意图。

图20是本申请实施例提供的一种基于非3GPP安全凭证的认证方法的流程示意图。

图21是本申请实施例提供的一种第一设备的示意性框图。

图 22 是本申请实施例提供的一种代理节点的示意性框图。

图 23 是本申请实施例提供的一种认证网元的示意性框图。

图 24 是本申请实施例提供的一种接入网设备的示意性框图。

图 25 是本申请实施例提供的一种通信装置的结构示意图。

5

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

图 1 是本申请实施例应用的无线通信系统 100。该无线通信系统 100 可以包括网络设备 110 和终端设备 120。网络设备 110 可以是与终端设备 120 通信的设备。网络设备 110 可以为特定的地理区域提供通信覆盖，并且可以与位于该覆盖区域内的终端设备 120 进行通信。

图 1 示例性地示出了一个网络设备和两个终端设备，可选地，该无线通信系统 100 可以包括多个网络设备并且每个网络设备的覆盖范围内可以包括其它数量的终端设备，本申请实施例对此不做限定。

可选地，该无线通信系统 100 还可以包括网络控制器、移动管理实体等其他网络实体，本申请实施例对此不作限定。

应理解，本申请实施例的技术方案可以应用于各种通信系统，例如：第五代（5th generation, 5G）系统或新无线（new radio, NR）、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）等。本申请提供的技术方案还可以应用于未来的通信系统，如第六代移动通信系统，又如卫星通信系统，等等。

本申请实施例中的终端设备也可以称为用户设备（user equipment, UE）、接入终端、用户单元、用户站、移动站、移动台（mobile station, MS）、移动终端（mobile terminal, MT）、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。本申请实施例中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，可以用于连接人、物和机，例如具有无线连接功能的手持式设备、车载设备等。本申请的实施例中的终端设备可以是手机（mobile phone）、平板电脑（Pad）、笔记本电脑、掌上电脑、移动互联网设备（mobile internet device, MID）、可穿戴设备、虚拟现实（virtual reality, VR）设备、增强现实（augmented reality, AR）设备、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程手术（remote medical surgery）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端等。可选地，UE 可以用于充当基站。例如，UE 可以充当调度实体，其在 V2X 或 D2D 等中的 UE 之间提供侧行链路信号。比如，蜂窝电话和汽车利用侧行链路信号彼此通信。蜂窝电话和智能家居设备之间通信，而无需通过基站中继通信信号。

本申请实施例中的网络设备可以是用于与终端设备通信的设备，该网络设备也可以称为接入网设备或无线接入网设备，如网络设备可以是基站。本申请实施例中的网络设备可以是指将终端设备接入到无线网络的无线接入网（radio access network, RAN）节点（或设备）。基站可以广义的覆盖如下中的各种名称，或与如下名称进行替换，比如：节点 B（NodeB）、演进型基站（evolved NodeB, eNB）、下一代基站（next generation NodeB, gNB）、中继站、传输点（transmitting and receiving point, TRP）、发射点（transmitting point, TP）、主站 MeNB、辅站 SeNB、多制式无线（MSR）节点、家庭基站、网络控制器、接入节点、无线节点、接入点（access point, AP）、传输节点、收发节点、基带单元（base band unit, BBU）、射频拉远单元（Remote Radio Unit, RRU）、有源天线单元（active antenna unit, AAU）、射频头（remote radio head, RRH）、中心单元（central unit, CU）、分布式单元（distributed unit, DU）、定位节点等。基站可以是宏基站、微基站、中继节点、施主节点或类似物，或其组合。基站还可以指用于设置于前述设备或装置内的通信模块、调制解调器或芯片。基站还可以是移动交换中心以及设备到设备 D2D、车辆外联（vehicle-to-everything, V2X）、机器到机器（machine-to-machine, M2M）通信中承担基站功能的设备、6G 网络中的网络侧设备、未来的通信系统中承担基站功能的设备等。基站可以支持相同或不同接入技术的网络。本申请的实施例对网络设备所采用的具体技术和具体设备形态不做限定。

基站可以是固定的，也可以是移动的。例如，直升机或无人机可以被配置成充当移动基站，一个或多个小区可以根据该移动基站的位置移动。在其他示例中，直升机或无人机可以被配置成用作与另一基站通信的设备。

在一些部署中，本申请实施例中的网络设备可以是指 CU 或者 DU，或者，网络设备包括 CU 和 DU。gNB 还可以包括 AAU。

网络设备和终端设备可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上；还可以部署在空中的飞机、气球或卫星上。本申请实施例中对网络设备和终端设备所处的场景不做限定。

应理解,本申请中的通信设备的全部或部分功能也可以通过在硬件上运行的软件功能来实现,或者通过平台(例如云平台)上实例化的虚拟化功能来实现。

应用层的认证与密钥管理(authentication and key management for applications, AKMA)架构

UE与应用功能(application function, AF)之间可以使用应用密钥(K_{AF})进行通信, K_{AF} 可用于对通信进行安全保护。 K_{AF} 的生成过程涉及到多个功能网元,如接入和移动性管理功能(access and mobility management function, AMF)、身份验证服务器功能(authentication server function, AUSF)、统一数据管理(unified data management, UDM)、AKMA锚点功能(AKMA anchor function, AAnF)、AF等,下面对这些功能网元进行介绍。

AMF主要用于移动性管理和接入管理等,可以用于实现移动性管理实体(mobility management entity, MME)功能中除会话管理之外的其他功能,例如,合法监听以及接入授权/鉴权等功能。

AUSF用于鉴权服务、产生密钥、实现对UE的双向鉴权,支持统一的鉴权框架。在本申请实施例中,AUSF主要用于在UE和网络之间进行相互认证,并生成安全密钥以便在后续的流程中使用。

UDM可用于处理UE标识、接入鉴权、注册以及移动性管理等。

AF用于进行应用层的数据路由,接入网络开放功能,与策略框架交互进行策略控制等。

AAnF用于生成AKMA锚定密钥(K_{AKMA}),以及应用密钥(K_{AF})。AAnF和UE可以采用相同的方式生成 K_{AF} 。在生成 K_{AF} 后,AAnF可以将生成的 K_{AF} 发送至AF。由此,AF和UE可以基于相同的密钥 K_{AF} 进行通信,以保证通信的安全性。

为了生成 K_{AF} ,UE可以先与网络侧进行初始认证,在初始认证完成后获得密钥(如 K_{AUSF}),该密钥可用于生成 K_{AF} 。

下面结合图2,对初始认证过程进行介绍。

参见图2,在步骤S202,UDM/认证凭证存储库和处理功能(authentication credential repository and processing function, ARPF)生成认证向量(authentication vector, AV)。

UDM/ARPF可以对每个认证获取请求消息(如Nudm Authenticate Get Request)创建一个5G HE AV。UDM/ARPF可以先生成一个AMF“separation bit”为1的认证向量,然后计算得到 K_{AUSF} 和 $XRES^*$ 。

最后,UDM/ARPF可以创建一个包含RAND、AUTN、 $XRES^*$ 和 K_{AUSF} 的5G HE AV。

在步骤S204,UDM向AUSF发送UE认证获取响应消息(如Nudm_ueauthentication_Get Response)。该UE认证获取响应消息中包括5G HE AV以及指示信息,该指示信息用于指示该5G HE AV用于5G认证与密钥协商(authentication and key agreement, AKA)。如果认证获取请求消息中包含订阅隐藏标识符(subscription concealed identifier, SUCI),则UE认证获取响应消息中可以包含订阅永久标识符(subscription permanent identifier, SUPI)。

在步骤S206,AUSF接收到UE认证获取响应消息后,可以临时保存 $XRES^*$ 以及接收到的SUCI或SUPI。AUSF还可以保存 K_{AUSF} 。

AUSF可以基于从UDM/ARPF接收到的5G HE AV生成一个5G AV。另外,AUSF可以基于 $XRES^*$ 计算 $HXRES^*$,基于 K_{AUSF} 计算 K_{SEAF} ,然后使用 $HXRES^*$ 和 K_{SEAF} 分别替换5G HE AV中的 $XRES^*$ 和 K_{AUSF} 。

在步骤S210,AUSF向安全锚点功能(security anchor function, SEAF)发送UE认证响应(如Nausf_UEAuthentication_Authenticate Response)。该UE认证响应中包括5G SE AV,该5G SE AV可以包括RAND、AUTN和 $HXRES^*$,而不包括 K_{SEAF} 。

在步骤S212,SEAF向UE发送认证请求。该认证请求可以通过非接入层(non-access stratum, NAS)消息(如Auth-Reg)发送。该认证请求中可以包括RAND和认证令牌(auth token, AUTN)。该消息中还可以包括ngKSI,该ngKSI可用于UE和AMF标识 K_{AMF} 和部分原生安全上下文。UE可以包括移动设备(mobile equipment, ME)和全球用户识别模块(universal subscriber identity module, USIM)。UE接收到RAND和AUTN后,ME可以向USIM转发该RAND和AUTN。

在步骤S214,USIM接收到RAND和AUTN后,可以检查AUTN是否被接受,以此来验证认证向量是否为最新,以抵抗重放攻击。如果验证通过,则USIM可以计算响应RES,并向ME返回RES、加密密钥(encrypt key, CK)和完整性密钥(integrity key, IK)。USIM还可以计算Kc(即GPRS Kc),并向ME发送该GPRS Kc。如果GPRS Kc基于CK、IK和第三代合作伙伴计划(the third generation partnership project, 3GPP)TS 33.102中描述的转换函数c3计算得到,则ME可以忽略该GPRS Kc,且该GPRS Kc不应存储在USIM或ME上。

ME可以基于RES计算 RES^* ,以及基于CK||IK计算 K_{AUSF} 。另外,ME还可以基于 K_{AUSF} 计算 K_{SEAF} 。如果ME接入5G,则ME还可以在认证期间检查AUTN的AMF字段“separation bit”是否设为1,其中,“separation bit”是AUTN的AMF字段的第0位。需要说明的是,AUTN的AMF字段中的

“separation bit”不能再用于运营商特定目的。

在步骤 S216, UE 向 SEAF 发送认证响应, 该认证响应中可以包括 RES*。该认证响应可以通过 NAS 消息发送。

5 在步骤 S218, SEAF 基于 RES* 计算 HRES*。SEAF 可以比较 HRES* 和 HXRES*, 确定这两个值是否一致。如果两个值一致, 则 SEAF 从服务网络的角度认为认证成功, 如果两个值不一致, 则 SEAF 可以按照协议 6.1.3.2.1 的规定执行。如果 UE 不可达, 且 SEAF 从未接收到 RES*, SEAF 可以认为认证失败, 并向 AUSF 指示认证失败。

在步骤 S220, SEAF 向 AUSF 发送 UE 认证请求 (如 Nausf_UE Authentication_Authenticate Request) 消息, 该 UE 认证请求消息中可以包括 SUCI 或 SUPI。

10 在步骤 S222, AUSF 接收 UE 认证请求消息, 该 UE 认证请求消息中可以包含 RES*。AUSF 可以验证 AV 是否已经到期, 如果 AV 已经到期, 则 AUSF 可以从归属域网络的角度认为认证不成功。AUSF 可以通过比较接收到的 RES* 与存储的 XRES*, 确定认证是否成功。如果 RES* 和 XRES* 一致, 则 AUSF 从归属域网络的角度认为认证成功; 如果 RES* 和 XRES* 不一致, 则 AUSF 从归属域网络的角度认为认证不成功。

15 在步骤 S224, AUSF 通过 UE 认证响应 (如 Nausf_UE Authentication_Authenticate Response) 消息向 SEAF 指示认证是否成功。如果认证成功, 则 AUSF 可以通过 UE 认证响应消息将 K_{SEAF} 发送至 SEAF。如果认证成功, 且 AUSF 在启动认证时从 SEAF 接收到 SUCI, 则 UE 认证响应消息还可以包括 SUPI。

如果认证成功, SEAF 可以将从 UE 认证响应消息中接收到的密钥 K_{SEAF} 作为锚密钥。另外, SEAF 可以基于 K_{SEAF} 、ABBA 参数以及 SUPI, 计算 K_{AMF} 。SEAF 可以向 AMF 提供 K_{SEAF} 和 ngKSI。

20 如果 SUCI 用于认证, 则 SEAF 可以仅在接收到包含 SUPI 的 UE 认证响应消息后, 才向 AMF 提供 ngKSI 和 K_{AMF} 。在获知 SUPI 之前, 服务网不会向 UE 提供通信服务。

在初始认证完成后, AUSF 和 UE 获得 K_{AUSF} , 该 K_{AUSF} 可用于生成 K_{AF} 。 K_{AF} 的协商流程可以由 UE 向 AF 发送 AKMA 密钥标识 (AKMA key identifier, A-KID) 来触发。下面结合图 3 和图 4, 对 K_{AF} 的生成过程进行介绍。

25 在步骤 S302, 在初始认证完成之后, UE 和 AUSF 可以基于 K_{AUSF} 生成 K_{AKMA} 以及 A-KID。

在步骤 S304, AUSF 可以向 AAnF 发送 AKMA 锚定密钥注册请求 (如 Naanf_AKMA_AnchorKey_Register Request), 该 AKMA 锚定密钥注册请求中可以包括 SUPI、A-KID 以及 K_{AKMA} 。

30 在步骤 S306, AAnF 可以向 AUSF 返回 AKMA 锚定密钥注册响应 (如 Naanf_AKMA_AnchorKey_Register Response)。

参见图 4, 在步骤 S402, 在完成初始认证以及生成 K_{AKMA} 后, UE 可以向 AF 发送应用程序会话建立请求。该应用程序会话建立请求中可以包括 A-KID。

35 在步骤 S404, AF 向 AAnF 发送 AKMA 应用密钥获取请求 (如 Naanf_AKMA_ApplicationKey_Get Request)。该 AKMA 应用密钥获取请求中可以包括 A-KID 以及 AF 的标识 (AF identity, AF-ID)。该 A-KID 为应用程序会话建立请求中的 A-KID。在一些实施例中, AKMA 应用密钥获取请求中还可以包括对 UE 的标识 (UE identity, UE-ID) 的请求。UE-ID 包括 SUPI、SUCI、通用公共订阅标识符 (generic public subscription identifier, GPSI) 中的一种或多种。

在步骤 S406, AAnF 接收到 AKMA 应用密钥获取请求后, 可以基于 A-KID 确定对应的 K_{AKMA} , 并基于 K_{AKMA} 生成密钥 K_{AF} 。

40 在步骤 S408, AAnF 向 AF 发送 AKMA 应用密钥获取响应。该应用密钥获取响应中可以包括 K_{AF} 、 K_{AF} 的有效期 (K_{AF} expTime)、UE-ID 等。

在步骤 S410, AF 向 UE 发送应用程序会话建立响应。

可以理解的是, UE 也可以采用与 AAnF 相同的方式生成 K_{AF} , 即, UE 基于 K_{AKMA} 生成 K_{AF} 的方式与 AAnF 基于 K_{AKMA} 生成 K_{AF} 的方式相同。由此, UE 和 AF 可以使用相同的密钥 K_{AF} 进行通信。

45 本申请实施例对上述密钥 (如 K_{AKMA} 、A-KID、 K_{AF} 等) 的生成方式不做具体限定。例如, 可以使用密钥派生函数 (key derivation function, KDF) 来生成上述密钥。KDF 可以为任意一种能够满足计算安全的密钥派生函数, 例如 KDF 可以为 HMAC-SHA-256 或 HMAC-SM3。下面以 KDF 为例, 对密钥的生成方式进行举例说明。

例如, 从 K_{AUSF} 生成 K_{AKMA} 时, 可以使用以下参数作为 KDF 的输入 S:

- 50
- FC=0xxx (如 0x80);
 - P0="AKMA";
 - L0=AKMA 的长度 (如 0x00 0x04);

- P1=SUPI;

- L1=SUPI 的长度;

输入的密钥 (key) 为 K_{AUSF} 。

又例如, 从 K_{AKMA} 生成 K_{AF} 时, 可以使用以下参数作为 KDF 的输入 S, 下文将该方式称为方式一:

- FC=0xXX (如 0x82);

- P0=AF_ID;

- L0=AF_ID 的长度;

输入的密钥为 K_{AKMA} 。

其中, AF_ID = AF 的 FQDN||Ua*安全协议标识符。

再例如, A-KID 可以包括漫游标识 (routing indicator, RID) 和 AKMA 临时 UE 标识 (AKMA temporary ue identifier, A-TID) 两部分。其中, RID 包含在 SUPI 中, A-TID 可以基于 K_{AUSF} 生成。当从 K_{AUSF} 生成 A-TID 时, 可以使用以下参数作为 KDF 的输入 S:

- FC = 0xXX (如 0x81);

- P0 = "A-TID";

- L0 = "A-TID" 的长度 (如 0x00 0x05);

- P1 = SUPI;

- L1 = SUPI 的长度;

输入的密钥为 K_{AUSF} 。

图 5 是本申请实施例涉及的各种密钥的衍生过程的示意图。

本申请实施例中的 NAS 安全上下文可以包括 K_{AMF} 、下级衍生密钥 K_{NASint} 和 K_{NASenc} , 以及各个密钥对应的密钥标识。

本申请实施例中的接入层 (access stratum, AS) 安全上下文可以包括 K_{gNB} 、下级衍生密钥 K_{RRCint} 、 K_{RRCenc} 、 K_{UPint} 和 K_{UPenc} , 以及各个密钥对应的密钥标识。

本申请实施例涉及的密钥还可以包括机密性保护密钥 (或称为加密密钥) 和完整性保护密钥。从图 5 可以看出, 机密性保护密钥和完整性保护密钥可以由 K_{AMF} 生成, 也可以由 K_{gNB} 生成。其中, K_{AMF} 为 AMF 和 UE 之间的共享密钥, 为 gNB 和 UE 之间的共享密钥。

在生成机密性保护密钥和完整性保护密钥时, 输入的参数可以如下:

-FC = 0xXX (如 00x69);

-P0 = 算法类型标识符 (algorithm type distinguisher);

-L0 = 算法类型标识符的长度 (length of algorithm type distinguisher) (如 0x00 0x01);

-P1 = 算法标识 (algorithm identity);

-L1 = 算法标识的长度 (length of algorithm identity) (如 0x00 0x01)。

根据生成密钥的不同, 输入的算法类型标识符的值也不同, 如表 1 所示。

表 1

算法类型标识符	值
N-NAS-enc-alg	0x01
N-NAS-int-alg	0x02
N-RRC-enc-alg	0x03
N-RRC-int-alg	0x04
N-UP-enc-alg	0x05
N-UP-int-alg	0x06

根据使用的算法的不同, 输入的算法标识的值也可以不同。本申请实施例使用的加密算法可以包括以下中的一种或多种: NIA1, NIA2, NIA3, 完整性保护算法可以包括以下中的一种或多种: EIA1, EIA2, EIA3。

图 6 示出了本申请实施例涉及的各种参数的生成方式。

UE 可以存储一个长期密钥 K 以及归属域网络的公钥, 该公钥可用于加密 SUPI。在 USIM 中计算的 5 个重要参数可以包括消息认证码 (message authentication code, MAC)、响应 (response, RES)、CK、IK 和 AK, 这些参数的计算方式可以如下:

$MAC = f1_K(SQN \parallel RAND \parallel AMF);$

$RES = f2_K(RAND);$

$CK = f3_K(RAND);$

$IK = f4_K(RAND);$

$AK = f5_K(\text{RAND})$ 。

零功耗通信

随着无线通信技术的发展,人们希望将无线通信系统与物流、制造、运输、能源等各个垂直行业进行融合,例如,可以将无线通信系统与工业无线传感器网络(industrial wireless sensor network, IWSN)进行融合。又例如,可以将无线通信系统与智慧物流和智慧仓储进行融合。又例如,可以将无线通信系统与智能家庭网络进行融合。

然而,在这些行业中,终端设备通常需要具备较低的成本、较小的尺寸(如超薄)、免维护、长寿命等特点。因此,为了满足上述条件,网络设备和终端设备之间可以采用零功耗通信技术进行通信,在这种情况下,终端设备又可以称为“零功耗通信终端”、零功耗终端或标签(Tag)。

在引入零功耗终端后,零功耗终端目前有两种通信方式。下面分别对这两种通信方式进行介绍。

通信方式一是零功耗终端与基站直接进行通信。基站可以向零功耗终端提供无线供能信号和触发信号。无线供能信号可用于向零功耗终端提供能量。触发信号可以携带发送给零功耗终端的控制信息。零功耗终端可以通过反向散射的方式将信息传输给基站。

通信方式二是混合通信方式,即该通信方式中包括蜂窝通信和侧行通信。在零功耗系统的实际部署中,基于蜂窝通信和侧行通信的零功耗通信系统可灵活共存或组合使用,从而匹配更多的潜在应用场景。

图7示出的是一种混合通信系统。图7示出的通信方式包括四种,下面分别对这四种通信方式进行介绍。

方式一,零功耗终端由终端设备提供供能信号和触发信号,零功耗终端的反向散射信号由基站接收。

方式二,基站向零功耗终端提供无线供能信号和发送触发信令,零功耗终端的反向散射信号由终端设备接收,从而完成侧行通信。另外,终端设备可以向基站发送空口数据。

方式三,终端设备为零功耗终端提供供能信号,基站向零功耗终端发送触发信息,并接收零功耗终端的反向散射信号。

方式四,终端设备接收网络设备发送的空口信令和/或数据。终端设备为零功耗终端提供供能信号和触发信号,并接收零功耗终端发送的反向散射信号,以完成侧行通信。

针对零功耗终端,如何实现零功耗终端与网络侧之间的安全认证,目前还没有明确的方案。

目前面向物联网的低吞吐量机器类型通信设备设计的电池高效安全(battery efficient security for very low throughput machine type communication devices, BEST)、机器类型通信(machine type communication, MTC)、新无线物联网(new radio- internet of things, NB-IoT)的安全标准基于AKA、通用引导架构(generic bootstrapping architecture, GBA)、AKMA等认证与密钥协商机制,存在密钥架构、交互流程和安全计算复杂度高的问题。如上文描述的认证方式,在生成认证向量的过程中,需要终端设备同时支持f1-f5中的各种函数。MAC使用的是f1函数,RES使用的是f2函数,CK使用的是f3函数,IK使用的是f4函数,AK使用的是f5函数。由于零功耗终端的计算能力较低,因此,这种方式不适合零功耗终端。

针对蜂窝与侧行通信混合的应用场景,目前的用户设备到网络中继(user equipment-to-network relay)安全存在基于近场的服务通信(proximity-based service communication, PC)5安全、U2N中继安全密钥架构、交互流程、安全计算复杂度高的问题,使得这种安全方式也不适用于零功耗终端。

另外,目前的国际标准化组织(international organization for standardization, ISO)射频识别(radio frequency identification, RFID)安全标准和标签与读写器空中接口安全(tag and reader air interface security, TRAFIS)安全标准仅支持Tag和读写器(Reader)之间的认证和密钥协商,不支持Tag与网络侧之间的认证和密钥协商,也就是说,这些安全标准无法实现Tag与网络侧之间的认证与密钥协商。

针对上述问题,本申请实施例提供一种认证方法和装置,能够以一种简化的方式实现认证与密钥协商流程,从而能够适用于第一设备(如零功耗终端)与网络侧之间的安全认证。本申请实施例的认证方法只需要第一设备支持一种或两种密钥生成算法,即可实现第一设备与网络侧之间的认证与密钥协商流程,从而可以降低第一设备的复杂度。

本申请实施例中的第一设备可以为零功耗终端。该第一设备例如可以为Tag或环境使能的物联网设备(ambient power-enabled internet of things, A-IoT)设备。

在介绍本申请提供的认证方法之前,先对第一设备的通信模式和本申请涉及的安全凭证进行介绍。

本申请实施例根据第一设备的协议栈设计不同,可以将第一设备的通信模式分为两类。第一类为非直接模式(indirect mode),第二类为直接模式(direct mode)。

对于非直接模式,第一设备不支持应用层协议,第一设备可以通过代理节点连接到服务域网元和/或AF。

本申请实施例中的服务域网元例如可以包括以下中的一种或多种:AMF、服务管理功能(service

management function, SMF)、SEAF、特定于 A-IoT 服务的核心网功能 (ambient network function, A-NF) 等。代理节点例如可以包括终端设备和/或集成接入和回程 (integrated access and backhaul, IAB) 节点等。终端设备例如可以为 UE。

在一些实现方式中,代理节点可以转发第一设备与网络侧(如认证网元)之间的认证信息。在另一些实现方式中,代理节点也可以对认证信息进行一些处理。例如,代理节点可以通过 NAS 消息(如 NAS 安全上下文)或 AS 消息(如 AS 安全上下文)传输认证信息。又例如,代理节点可以对认证过程中的一些加密信息(如第一设备的隐藏身份标识)进行解密。下文将会结合具体的实施例对代理节点的具体处理方式详细描述。

对于直接模式,第一设备可以支持应用层协议(如超文本传输协议(hyper text transfer protocol, HTTP))。或者,第一设备的媒体接入控制(media access control, MAC)层或物理(physical, PHY)层具有支持上层协议(如应用层)的功能,从而使得第一设备支持应用层协议功能。在一些实现方式中,第一设备可以通过应用层协议连接到 AF。

本申请实施例可以在第一设备与第三方服务器(如 AF)之间建立安全的通信链路。第三方服务器可以依赖核心网对第一设备进行认证与密钥协商。根据安全凭证提供方的不同,本申请实施例中的安全凭证可以分为两类。一类安全凭证为 3GPP 安全凭证,另一类安全凭证为非 3GPP 安全凭证。

3GPP 安全凭证可以理解为第一设备与认证网元之间共享的根密钥(简称 K)。如果安全凭证为 3GPP 安全凭证,则网络侧(如 UDM)可以进行授权管理,如存储认证结果。该管理授权可以为基于订阅凭证的授权管理。该认证结果例如可以包括以下中的一种或多种:第一设备认证的时间戳、第一设备的 ID、第一设备的认证方式和第一设备安全上下文的标识。

图 8 示出的是一种基于 3GPP 安全凭证的通信架构。第一设备可以与核心网执行认证与密钥协商流程。在一些实现方式中,第一设备可以和第三方服务器进行通信,第三方服务器可以和核心网进行通信。

非 3GPP 安全凭证可以为第三方应用服务器提供的安全凭证,如第一设备与 AF 或网络应用功能(network application function, NAF)之间共享的根密钥(简称 K)。第三方应用服务器(如 AF 或 NAF)可以进行授权管理。该授权管理可以为基于应用层的授权管理。在涉及代理节点的场景中,第三方应用服务器可以管理代理节点与第一设备之间的映射,以及向认证网元提供安全凭证 K,或向认证网元提供由安全凭证 K 衍生出的下级密钥。

图 9 示出的是一种基于 3GPP 安全凭证的通信架构。与图 8 不同的是,第三方服务器可以与核心网进行通信,以向核心网提供安全凭证 K 或由安全凭证 K 衍生出的下级密钥。

需要说明的是,本申请实施例中的安全凭证可以理解为根密钥。

下面结合图 10-图 20,对本申请实施例的认证方式进行详细介绍。需要说明的是,以下四个示例和不同附图中的方案在不存在冲突的情况下,都可以相互结合使用。

示例一

示例一的方案中,安全凭证为 3GPP 安全凭证,第一设备通过代理节点与网络侧进行通信。

图 10 是本申请实施例提供的一种认证方法的流程示意图。参见图 10,在步骤 S1010,认证网元生成第一消息认证码和/或期望响应。第一消息认证码可用于认证认证网元。期望响应可用于认证第一设备。在一些实施例中,第一消息认证码可以使用第一 MAC 表示,期望响应可以使用 XRES 表示。

本申请实施例对第一消息认证码的生成方式不做具体限定。例如,该第一消息认证码可以基于第一密钥生成算法和第一参数生成。第一密钥生成算法可以为任意一种函数。该函数可以为以下中的任意一种:f 函数、KDF 或其他轻量级函数。f 函数例如可以为 3GPP 定义的 f1 函数、f2 函数、f3 函数、f4 函数、f5 函数中的任意一个。KDF 例如可以为 HMAC-SHA-256 或 HMAC-SM3。轻量级函数例如可以为 ASCON。

第一参数可以包括以下中的一种或多种:安全凭证、第一随机数、第二随机数和第一密钥。例如,第一参数可以包括安全凭证和第二随机数。又例如,第一参数可以包括安全凭证、第二随机数和第一密钥。又例如,第一参数可以包括安全凭证、第二随机数和第一随机数。又例如,第一参数可以包括安全凭证、第二随机数、第一随机数和第一密钥。

安全凭证可以是上文描述的 3GPP 安全凭证或非 3GPP 安全凭证。第一随机数(记为 N2)可以是认证网元选择的随机数或者也可以是认证网元与第一设备之间的共享密钥。该第一随机数可用于抵御重放攻击。第二随机数(记为 RAND)可以是认证网元选择的随机数。第一密钥(记为 N1)可以为以下中的一种或多种:第一设备与网络侧设备(如认证网元)预先共享的随机数,第一设备与代理节点之间的共享密钥,第一设备与基站之间的共享密钥。该共享密钥可以为物理层密钥。

在一些实施例中,第一消息认证码和期望响应可以基于相同的密钥生成算法和不同的参数生成,或者,第一消息认证码和期望响应可以基于不同的密钥生成算法和相同的参数生成,这样可以降低生成第

一消息认证码和期望响应的复杂度。

作为一个示例，生成期望响应所使用的密钥生成算法与生成第一消息认证码所使用的密钥生成算法相同。例如，第一消息认证码可以基于第一密钥生成算法和第一参数生成，期望响应可以基于第一密钥生成算法和第二参数生成。

第二参数可以包括以下中的一种或多种：安全凭证、第一随机数、第二随机数和第一密钥。第一参数与第二参数不同，以保证生成的期望响应与第一消息认证码不同。例如，第一参数包括安全凭证和第一随机数。第二参数包括安全凭证、第一随机数和第二随机数。又例如，第二参数包括安全凭证、第一随机数和第二随机数，第二参数包括第二参数包括安全凭证、第一随机数、第二随机数和第一密钥。又例如，第一参数包括安全凭证、第一随机数和第二随机数，第二参数包括安全凭证和第一随机数。

作为另一个示例，生成期望响应所使用的参数与生成第一消息认证码所使用的参数相同。例如，第一消息认证码可以基于第一密钥生成算法和第一参数生成，期望响应可以基于第二密钥生成算法和第一参数生成。

第一密钥生成算法与第二密钥生成算法不同，以保证生成的期望响应与第一消息认证码不同。第二密钥生成算法可以为任意一种函数。例如，第二密钥生成算法可以为以下中的任意一种：f 函数、KDF 或其他轻量级函数。f 函数例如可以为 3GPP 定义的 f1 函数、f2 函数、f3 函数、f4 函数、f5 函数中的任意一个。KDF 例如可以为 HMAC-SHA-256 或 HMAC-SM3。轻量级函数例如可以为 ASCON。

类似地，第一设备可以生成第二消息认证码和/或响应参数。第二消息认证码可用于认证认证网元，响应参数可用于认证第一设备。在一些实施例中，第二消息认证码可以使用第二 MAC 表示，响应参数可以使用 RES 表示。

在一些实施例中，第二消息认证码的生成方式与第一消息认证码的生成方式一致。例如，第二消息认证码可以基于第一密钥生成算法和第一参数生成。第一密钥生成算法与第一参数可以参见前文的描述，为了简洁，此处不再赘述。

举例说明，消息认证码可以基于以下公式中的一种或多种确定： $MAC = f_K(RAND, N1, N2)$ 、 $MAC = f_K(RAND)$ 、 $MAC = f_K(RAND, N1)$ 、 $MAC = f_K(RAND, N2)$ 。

期望响应可以基于以下公式中的一种或多种确定： $XRES = f_K(RAND, N1, N2)$ 、 $XRES = f_K(RAND)$ 、 $XRES = f_K(RAND, N1)$ 、 $XRES = f_K(RAND, N2)$ 。

其中，MAC 表示第一消息认证码或第二消息认证码，f 表示第一密钥生成算法或第二密钥生成算法，RAND 表示第二随机数，N1 表示第一密钥，N2 表示第二随机数，K 表示安全凭证。

在一些实施例中，响应参数的生成方式与期望响应的生成方式一致。例如，响应参数可以基于第二密钥生成算法和第一参数生成，或者，响应参数可以基于第一密钥生成算法和第二参数生成。响应参数的具体生成方式可以参见前文期望响应的生成方式，为了简洁，此处不再赘述。

在一些实施例中，第一设备可以接收来自认证网元的第一消息认证码。第一设备可以通过代理节点接收来自认证网元的第一消息认证码。第一设备可以比较第一消息认证码和第二消息认证码，以认证认证网元。如果第一消息认证码和第二消息认证码一致，则表示认证网元认证成功；如果第一消息认证码和第二消息认证码不一致，则表示认证网元认证失败。

在一些实施例中，认证网元可以接收来自第一设备的响应参数。认证网元可以通过代理节点接收来自第一设备的响应参数。认证网元可以比较响应参数与期望响应，以认证第一设备。如果响应参数与期望响应一致，则表示第一设备认证成功；如果响应参数与期望响应不一致，则表示第一设备认证失败。

在一些实现方式中，图 10 所示的方法还可以包括步骤 S1020~步骤 S1070。

在步骤 S1020，认证网元向代理节点发送第一认证请求。该第一认证请求中包括第一消息认证码。认证网元向代理节点发送第一认证请求可以指认证网元直接向代理节点发送第一认证请求，或者，可以指认证网元通过其他设备向代理节点发送第一认证请求。其他设备例如可以包括基站和/或服务域网元。该服务域网元可以包括 AMF 和/或 SMF。

在步骤 S1030，代理节点向第一设备发送第一认证请求。

在步骤 S1040，第一设备基于第一密钥生成算法和第一参数生成第二消息认证码。具体的生成方式可以参见前文的描述。在一些实施例中，第一设备可以在接收到第一认证请求之前，生成第二消息认证码，或者，第一设备也可以在接收到第一认证请求之后，再生成第二消息认证码。

在步骤 S1050，第一设备基于第一消息认证码和第二消息认证码认证认证网元。如果第一消息认证码与第二消息认证码一致，则第一设备可以确定认证网元认证成功；如果第一消息认证码和第二消息认证码不一致，则第一设备可以确定认证网元认证失败。

在步骤 S1060，在认证网元认证成功的情况下，第一设备生成响应参数。如果认证网元认证失败，则第一设备可以不生成响应参数，以降低第一设备的计算量。当然，在一些实施例中，不论认证网元是

否认证成功，第一设备都可以生成响应参数。例如，第一设备可以在接收到第一认证请求之前，生成响应参数。

在步骤 S1070，第一设备向代理节点发送第一认证响应。该第一认证响应中可以包括响应参数。

在步骤 S1080，代理节点向认证网元发送第一认证响应。该第一认证响应中可以包括响应参数。

5 在一些实施例中，代理节点可以向认证网元发送响应参数。认证网元接收到响应参数后，可以比较响应参数和期望响应，以认证第一设备。

为了提高认证的安全性，本申请实施例可以从归属域网络、服务域网络和接入网络的角度对第一设备进行认证。例如，响应参数可以包括以下中的一种或多种：第一响应参数、第二响应参数和第三响应参数。第一响应参数可用于归属域网络（或归属域网元）认证第一设备，第二响应参数可用于服务域网络（或服务域网元）认证第一设备，第三响应参数可用于接入网络（或接入网设备）认证第一设备。第一响应参数可以记为 RES1，第二响应参数可以记为 RES2，第三响应参数可以记为 RES3。

又例如，期望响应可以包括以下中的一种或多种：第一期望响应、第二期望响应和第三期望响应。第一期望响应可用于归属域网络（或归属域网元）认证第一设备，第二期望响应可用于服务域网络（或服务域网元）认证第一设备，第三期望响应可用于接入网络（或接入网设备）认证第一设备。第一期望响应可以记为 XRES1，第二期望响应可以记为 XRES2，第三期望响应可以记为 XRES3。

10 在一些实施例中，期望响应可以包括第一期望响应和第二期望响应，以从归属域网络和服务域网络的角度认证第一设备。在一些实施例中，期望响应可以包括第一期望响应和第三期望响应，以从归属域网络和接入网络的角度认证第一设备。在一些实施例中，期望响应可以包括第二期望响应和第三期望响应，以从服务域网络和接入网络的角度认证第一设备。在一些实施例中，期望响应可以包括第一期望响应、第二期望响应和第三期望响应，以从归属域网络、服务域网络和接入网络的角度认证第一设备。

下面对各个网络认证第一设备的认证方式进行介绍。

归属域网元可以比较第一响应参数和第一期望响应，以认证第一设备。第一期望响应可以由归属域网元生成，第一响应参数可以由第一设备生成。第一设备可以将第一响应参数发送至归属域网元。如果第一响应参数与第一期望响应一致，则归属域网元可以从归属域网络的角度认为认证成功。如果第一响应参数和第一期望响应不一致，则归属域网元可以从归属域网络的角度认为认证失败。归属域网元可以包括 AUSF 和/或 UDM。

25 服务域网元可以比较第二响应参数和第二期望响应，以认证第一设备。第二期望响应可以由归属域网元生成，归属域网元可以将第二期望响应发送至服务域网元。第二响应参数可以由第一设备生成，第一设备可以将第二响应参数发送至服务域网元。如果第二响应参数和第二期望响应一致，则服务域网元可以从服务域网络的角度认为认证成功。如果第二响应参数和第二期望响应不一致，则服务域网元可以从服务域网络的角度认为认证失败。服务域网元可以包括 AMF 和/或 SMF。

接入网设备可以比较第三响应参数和第三期望响应，以认证第一设备。如果第三响应参数和第三期望响应一致，则接入网设备可以从接入网络的角度认为认证成功。如果第三响应参数和第三期望响应不一致，则接入网设备可以从接入网络的角度认为认证失败。接入网设备可以为基站。

35 在一些实施例中，第三期望响应可以由归属域网元生成，归属域网元可以将第三期望响应发送至接入网设备。或者，第三期望响应可以由接入网设备生成。认证网元可以向接入网设备发送第一期望响应，接入网设备基于接收到的第一期望响应，生成第三期望响应。例如，对于第一密钥为第一设备与接入网设备之间的共享密钥的情况，接入网设备可以基于第一期望响应和第一密钥生成第三期望响应。

40 在一些实施例中，第三响应参数可以由第一设备生成，第一设备可以将第三响应参数发送至接入网设备。

下面对各个响应参数和各个期望响应的生成方式进行介绍。

在一些实施例中，第一响应参数和第二消息认证码（或第一消息认证码）所基于的密钥生成算法相同，以降低第一设备的计算复杂度。例如，第一响应参数可以基于第一密钥生成算法和第二参数生成，换句话说，第一设备可以基于第一密钥生成算法和第二参数生成第一响应参数。

45 在一些实施例中，第一响应参数和第二消息认证码（或第一消息认证码）所基于的参数相同，以降低第一设备的计算复杂度。例如，第一响应参数可以基于第二密钥生成算法和第一参数生成，换句话说，第一设备可以基于第二密钥生成算法和第一参数生成第一响应参数。第一响应参数的生成方式可以与上文中的期望响应的生成方式一致。

举例说明，第一响应参数可以基于以下公式确定：

$$RES1 = f_K(RAND, N1, N2)$$

50 其中，RES1 表示第一响应参数，f 表示第一密钥生成算法或第二密钥生成算法，RAND 表示第二随机数，N1 表示第一密钥，N2 表示第二随机数，K 表示安全凭证。

在一些实施例中，第二响应参数可以基于第一响应参数和第三参数生成，换句话说，第一设备可以基于第一响应参数和第三参数生成第二响应参数。第三参数可以包括以下中的一种或多种：安全凭证、服务域网络名称（SN name）（或服务域网络标识）。在一些实现方式中，第二响应参数和第一响应参数可以基于相同的密钥生成算法生成，或者，第二响应参数和第二消息认证码（或第一消息认证码）可以基于相同的密钥生成算法生成。例如，第二响应参数可以基于第一密钥生成算法、第一响应参数和第三参数生成。又例如，第二响应参数可以基于第二密钥生成算法、第一响应参数和第三参数生成。

举例说明，第二响应参数可以基于以下公式确定：

$$RES2=f_K(RES1, SN\ name)$$

其中，RES2表示第二响应参数，f表示第一密钥生成算法或第二密钥生成算法，RES1表示第一响应参数，SN name表示服务域网络名称或标识，K表示安全凭证。

在一些实施例中，第三响应参数可以基于第一响应参数和第四参数生成，换句话说，第一设备可以基于第一响应参数和第四参数生成第三响应参数。第四参数可以包括第一密钥。在一些实现方式中，第三响应参数和第一响应参数可以基于相同的密钥生成算法生成，或者，第三响应参数和第二消息认证码（或第一消息认证码）可以基于相同的密钥生成算法生成。例如，第三响应参数可以基于第一密钥生成算法、第一响应参数和第四参数生成。又例如，第三响应参数可以基于第二密钥生成算法、第一响应参数和第四参数生成。

举例说明，第三响应参数可以基于以下公式确定：

$$RES3=f_{N1}(XRES1)$$

其中，RES3表示第三响应参数，f表示第一密钥生成算法或第二密钥生成算法，RES1表示第一响应参数，N1表示第一密钥。

上述各个响应参数的生成方式仅是一种示例，本申请实施例对此不做具体限定。例如，第二响应参数可以基于第三响应参数生成。又例如，第三响应参数可以基于第二响应参数生成。

第一期望响应与第一响应参数的生成方式类似，第二期望响应与第二响应参数的生成方式类似，第三期望响应与第三响应参数的生成方式类似，为了简洁，此处不再赘述。

在一些实施例中，认证网元可以生成第一匿名密钥。第一匿名密钥可用于第一设备与网络侧之间的安全传输。

在一些实施例中，为了降低生成第一匿名密钥的计算复杂度，第一匿名密钥可以基于第一密钥生成算法或第二密钥生成算法生成。例如，第一匿名密钥可以基于第一密钥生成算法和第九参数生成。又例如，第一匿名密钥可以基于第二密钥生成算法和第九参数生成。第九参数可以包括以下参数中的一种或多种：安全凭证、第一随机数、第二随机数和第一密钥。

以第九参数包括安全凭证和第二随机数为例，第一匿名密钥可以基于如下公式确定：

$$AK=f_K(RAND)$$

其中，AK表示第一匿名密钥，K表示安全凭证，RAND表示第二随机数，f表示第一密钥生成算法或第二密钥生成算法。

公式 $AK=f_K(RAND)$ 适用于第一密钥是第一设备与认证网元之间的共享密钥的情况，也适用于第一密钥是代理节点发送给认证网元的情况。

在一些实施例中，为了降低生成第一匿名密钥的计算复杂度，第一匿名密钥可以通过异或的运算方式生成。例如，第一匿名密钥可以由安全凭证和第一密钥通过异或的方式生成。也就是说，第一匿名密钥可以基于如下公式确定：

$$AK=K\oplus N1$$

其中，AK表示第一匿名密钥，K表示安全凭证，N1表示第一密钥， $\oplus$ 表示异或运算。

上述公式 $AK=K\oplus N1$ 适用于第一密钥是第一设备与认证网元之间的共享密钥的情况。认证网元可以基于共享密钥 N1 生成 AK。

类似地，第一设备也可以生成第二匿名密钥。第二匿名密钥的生成方式与第一匿名密钥的生成方式相同，为了简洁，此处不再赘述。

在接收来自代理节点的第一认证请求之前，第一设备可以向代理节点发送第二认证请求。换句话说，第一设备可以通过发送第二认证请求，以触发第一设备与网络侧之间的认证流程。

在一些实施例中，第二认证请求中可以包括第一设备的隐藏身份标识。为了保证信息的安全性，第一设备可以对第一设备的身份标识进行匿名处理，得到隐藏身份标识。

隐藏身份标识的生成方式有多种。例如，隐藏身份标识可以基于第一设备的身份标识和第一密钥生成。又例如，隐藏身份标识可以基于第一设备的身份标识、第一密钥和安全凭证生成。第一设备的身份标识可以理解第一设备的真实身份标识。

下文以隐藏身份标识基于第一设备的身份标识和第一密钥生成为例，对隐藏身份标识的生成方式进行详细描述。

在一些实施例中，隐藏身份标识可以通过异或的运算方式生成，以降低第一设备的计算复杂度。例如，隐藏身份标识可以由第一设备的身份标识和第一密钥通过异或的运算方式生成。换句话说，第一设备可以对第一设备的身份标识以及第一密钥进行异或运算，生成隐藏身份标识。

举例说明，隐藏身份标识可以基于以下公式确定：

$$DIDi = IDi \oplus N1$$

其中， $DIDi$ 表示隐藏身份标识， IDi 表示第一设备的身份标识， $N1$ 表示第一密钥， $\oplus$ 表示异或运算。

在一些实施例中，隐藏身份标识可以基于第一设备的身份标识、第一密钥以及第三密钥生成算法生成。换句话说，第一设备可以基于第一设备的身份标识、第一密钥以及第三密钥生成算法生成隐藏身份标识。其中，第三密钥生成算法可以为第一密钥生成算法或第二密钥生成算法，以降低第一设备的计算复杂度。

举例说明，隐藏身份标识可以基于以下公式确定：

$$DIDi = f_{N1}(IDi)$$

其中， $DIDi$ 表示隐藏身份标识， IDi 表示第一设备的身份标识， $N1$ 表示第一密钥， f 表示第三密钥生成算法。

第一密钥可以为第一设备与网络侧（如认证网元）之间的共享密钥（或随机数），或者也可以是第一设备与代理节点之间的共享密钥，或者也可以是第一设备与基站之间的共享密钥。该共享密钥可以为物理层密钥。如果第一密钥为物理层密钥，则第一设备可以不用预先存储第一密钥，而是通过提取物理层信道特征得到第一密钥。

如果第一密钥可以为第一设备与网络侧（如认证网元）之间的共享密钥，则认证网元可以向第一设备发送新的第一密钥，以更新隐藏身份标识。

根据第一密钥的不同，第一设备生成隐藏身份标识的方式可以不同。例如，如果第一密钥为第一设备与网络侧之间的共享密钥，则隐藏身份标识可以通过公式 $DIDi = IDi \oplus N1$ 生成。又例如，如果第一密钥为第一设备与代理节点之间的共享密钥，则隐藏身份标识可以通过公式 $DIDi = IDi \oplus N1$ 或公式 $DIDi = f_{N1}(IDi)$ 生成。

代理节点接收到第二认证请求后，可以向认证网元发送该第二认证请求。代理节点发送的第二认证请求中可以包括以下信息中的一种或多种：第一密钥、第一设备的身份标识、隐藏身份标识和代理节点的标识。代理节点的标识可以包括以下中的一种或多种：GPSI、SUCI、全球唯一临时标识（globally unique temporary identifier, GUTI）、SUPI。

在一些实施例中，代理节点可以根据第一密钥的不同，采取不同的处理策略。作为一个示例，如果第一密钥为第一设备与网络侧之间的共享密钥，则代理节点发送的第二认证请求中可以包括以下中的一种或多种：隐藏身份标识和代理节点的标识。

作为另一个示例，如果第一密钥为第一设备与代理节点之间的共享密钥，则代理节点可以对隐藏身份标识进行解匿名，得到第一设备的身份标识。例如，代理节点可以基于第一密钥与隐藏身份标识，确定第一设备的身份标识。

如果隐藏身份标识由第一密钥和第一设备的身份标识通过异或的方式生成，则代理节点可以通过如下公式确定第一设备的身份标识：

$$IDi = DIDi \oplus N1$$

其中， $DIDi$ 表示隐藏身份标识， IDi 表示第一设备的身份标识， $N1$ 表示第一密钥， $\oplus$ 表示异或运算。

如果隐藏身份标识基于第一密钥、第一设备的身份标识和第三密钥生成算法生成，则代理节点可以通过如下公式确定第一设备的身份标识：

$$IDi = f_{N1}(DIDi)$$

其中， $DIDi$ 表示隐藏身份标识， IDi 表示第一设备的身份标识， $N1$ 表示第一密钥， f 表示第三密钥生成算法。

在得到第一设备的身份标识后，第一设备发送的第二认证请求中可以包括以下中的一种或多种：第一密钥、第一设备的身份标识和代理节点的标识。

如果第二认证请求中包括第一设备的身份标识，为了保证信息的安全性，代理节点可以通过 NAS 消息或 AS 消息发送第二认证请求消息。例如，代理节点可以通过 NAS 安全上下文或 AS 安全上下文发送第二认证请求消息。

认证网元接收到第二认证请求后,如果第二认证请求中包括隐藏身份标识,则认证网元可以通过对隐藏身份标识进行解匿名,得到第一设备的身份标识。例如,如果第一密钥为第一设备与认证网元之间的共享密钥,则认证网元可以基于第一密钥,对隐藏身份标识进行解匿名。例如,认证网元可以通过公式 $ID_i = DID_i \oplus N1$ 得到第一设备的身份标识。

5 认证网元在得到第一设备的身份标识后,可以利用第一设备的身份标识生成后文中的第四密钥。

在第一设备和认证网元认证成功的情况下,第一设备和认证网元可以生成第二密钥(记为 K_s)。第二密钥也可以理解为第一设备与认证网元之间的共享密钥。第二密钥可以基于第六密钥生成算法和第六参数生成。第六密钥生成算法可以为第一密钥生成算法或第二密钥生成算法,以降低第一设备的计算复杂度。第六参数可以包括以下参数中的一种或多种:第一匿名密钥、第一密钥、第一随机数、代理节点的标识、第一设备的标识、服务域网络的名称和归属域网络标识。

10 举例说明,第二密钥可以基于以下公式确定:

$$K_s = f_{AK}(N1, N2, UE\ ID, ID_i, SN\ name)$$

其中, K_s 表示第二密钥, AK 表示第一匿名密钥, $N1$ 表示第一密钥, $N2$ 表示第一随机数, $UE\ ID$ 表示代理节点的标识, ID_i 表示第一设备的身份标识, $SN\ name$ 表示服务域网络的名称, f 表示第六密钥生成算法。

生成 AKMA 密钥

上述第二密钥可用于 AKMA 密钥的生成。也就是说,第一设备可以基于第二密钥,生成 AKMA 密钥。或者,认证网元可以基于第二密钥,生成 AKMA 密钥。

可以理解的是,第一设备生成 AKMA 密钥的方式与认证网元生成 AKMA 密钥的方式相同。下面以第一设备为例,对 AKMA 密钥的生成方式进行介绍。认证网元生成 AKMA 密钥的方式可以参考第一设备生成 AKMA 密钥的方式,为了简洁,不再重复描述。

第一设备可以基于第二密钥和第四密钥生成算法,生成 AKMA 密钥。第四密钥生成算法可以为第一密钥生成算法或第二密钥生成算法,以降低第一设备的计算复杂度。在一些实施例中,第一设备可以基于第二密钥、第四密钥生成算法以及第五参数生成。第五参数可以包括以下中的一种或多种: AKMA、第一设备的身份标识。

25 举例说明, AKMA 密钥可以基于以下公式确定:

$$K_{AKMA} = f_{K_s}("AKMA", "ID_i")$$

其中, K_{AKMA} 表示 AKMA 密钥, K_s 表示第一匿名密钥, ID_i 表示第一设备的身份标识。

在一些实施例中,第二密钥可用于生成密钥标识。或者说,第一设备可以基于第二密钥生成密钥标识。该密钥标识例如可以包括 A-TID 和/或 A-KID。例如, A-TID 可以基于第一设备的身份标识、第一匿名密钥和第七密钥生成算法生成。该第七密钥生成算法可以为第一密钥生成算法或第二密钥生成算法。

举例说明, A-TID 可以基于以下公式确定:

$$A-TID = f_{K_s}(ID_i)$$

35 其中, f 表示第七密钥生成算法, K_s 表示第一匿名密钥, ID_i 表示第一设备的身份标识。

在一些实施例中, A-KID 可以基于 A-TID 生成。例如, A-KID 可以基于 A-TID 以及第七参数生成。第七参数可以包括以下参数中的一种或多种: RID 和归属域网络标识(home network identifier, HNI)。为了降低第一设备的计算复杂度, A-KID 可以由 A-TID、RID 和第七参数通过级联的方式得到。

例如, A-KID 可以基于以下公式确定:

$$A-KID = A-TID || RID || HNI$$

40 在一些实施例中,认证网元可以向 AAnF 和/或密钥管理服务(key management server, KMS)发送密钥参数,该密钥参数可以包括以下中的一种或多种: AKMA 密钥、A-KID 和第一设备的标识。

在一些实施例中, AAnF 和/或 AMF 接收到 AKMA 密钥后,可以基于 AKMA 密钥生成应用密钥(记为 K_{AF})。应用密钥可以基于第八密钥生成算法和第八参数生成。第八参数可以包括以下参数中的一种或多种: AF ID、 ID_i 、代理节点的标识、A-KID。第八密钥生成算法可以为第一密钥生成算法或第二密钥生成算法,以降低第一设备的计算复杂度。

例如,应用密钥可以基于以下公式确定:

$$K_{AF} = f_{K_s}(AF\ ID, ID_i, UE\ ID, A-KID)$$

50 其中, K_{AF} 表示应用密钥, f 表示第八密钥生成算法, AF ID 表示 AF 的标识, ID_i 表示第一设备的身份标识, UE ID 表示代理节点的标识。

在一些实施例中, AAnF 可以在接收到来自 AF 的应用密钥请求消息后,生成应用密钥。

可以理解的是,第一设备生成应用密钥的方式与 AAnF 生成应用密钥的方式相同,为了简洁,此处不再赘述。在一些实施例中,第一设备可以在向 AF 发送应用会话建立请求消息后,生成应用密钥。

在一些实施例中,应用密钥可用于生成第三密钥,该第三密钥可用于第一设备与代理节点之间的安全通信。也就是说,第一设备与代理节点可以基于第三密钥,进行安全通信。

在一些实现方式中,第三密钥可以包括完整性保护密钥和/或加密密钥。也就是说,以设备和代理节点可以基于应用密钥生成完整性保护密钥和/或加密密钥。基于应用密钥生成完整性保护密钥和/或加密密钥的方式可以为相关技术中的方式,本申请实施例对此不做具体限定。

在一些实现方式中,第三密钥可以基于应用密钥和第一密钥生成。第一密钥为第一设备与代理节点之间的共享密钥。为了降低第一设备的计算复杂度,第三密钥可以由应用密钥和第一密钥通过异或的方式生成。

例如,第三密钥可以基于以下公式确定:

$$K_{ul}=K_{AF} \oplus N1$$

其中, K_{ul} 表示第三密钥, K_{AF} 表示应用密钥, $N1$ 表示第一密钥, $\oplus$ 表示异或运算。

在一些实施例中,第三密钥(如 K_{ul})可用于进一步生成完整性保护密钥和/或加密密钥。本申请实施例通过先生成第三密钥,再生成完整性保护密钥和/或加密密钥,能够为第一设备的移动性管理提供一种简化的方式。例如,如果第一设备由于移动,导致连接的代理节点发生了变化,第一设备可以直接基于与代理节点之间的共享密钥生成第三密钥,并进一步生成完整性保护密钥和/或加密密钥,从而可以不用再进行第一设备与网络侧之间的认证与密钥协商流程。

举例说明,如果与第一设备连接的代理节点从第一代理节点变为第二代理节点,第一设备与第一代理节点之间的共享密钥为 $N1$,第一设备与第二代理节点之间的共享密钥为 $N3$,在第一设备与第一代理节点处于连接状态时,第一设备可以基于应用密钥以及 $N1$,生成第三密钥,并进一步生成与第一代理节点进行安全通信的完整性保护密钥和/或加密密钥。在第一设备与第二代理节点处于连接状态时,第一设备可以基于应用密钥以及 $N3$,生成第三密钥,并进一步生成与第二代理节点进行安全通信的完整性保护密钥和/或加密密钥。由上可知,在连接的代理节点发生变化时,第一设备可以跳过认证与密钥协商流程,来生成不同的完整性保护密钥和/或加密密钥,而是可以基于不同的第一密钥,生成不同的完整性保护密钥和/或加密密钥,以与不同的代理节点进行安全通信。

对于第一消息认证码需要基于第一随机数生成的情况,如果第一随机数由认证网元选择,则认证网元还可以将第一随机数发送至第一设备,以使第一设备可以基于第一随机数生成第二消息认证码。

在一些实施例中,为了保证第一随机数的安全性,认证网元可以使用第一匿名密钥保护第一随机数的传输安全。为了降低计算复杂度,认证网元可以将第一匿名密钥与第一随机数进行异或运算,得到第十参数,即第十参数可以为 $N2 \oplus AK$ 。认证网元可以向第一设备发送第十参数,或者认证网元可以向第一设备发送第十一参数,第十一参数可以为 $N2 \oplus AK \parallel MAC$ 。其中, MAC 为第一消息认证码, $N2$ 为第一随机数, AK 为第一匿名密钥, $\parallel$ 表示级联。

第一设备接收到认证网元发送的第十参数或者第十一参数后,可以基于第一匿名密钥,确定第一随机数。然后基于第一随机数,生成第二消息认证码。进一步地,第一设备可以基于第一消息认证码和第二消息认证码,认证认证网元。

在一些实施例中,对于第一消息认证码基于第二随机数生成的情况,认证网元还可以将第二随机数发送至第一设备,以使第一设备基于第二随机数,生成第二消息认证码。

下面结合图 11-图 13,对有代理节点参与的认证与密钥协商流程进行详细介绍。

图 11 示出的是第一设备与认证网元之间进行认证的流程。第一设备可以与认证网元共享密钥 K ,该密钥 K 即为上文描述的安全凭证。第一设备可以与基站和/或代理节点共享密钥 $N1$,该密钥 $N1$ 即为上文描述的第一密钥。该密钥 $N1$ 可以为物理层密钥。

参见图 11,在步骤 S1102,第一设备向代理节点发送认证请求。该认证请求中可以包括第一设备的隐藏身份标识 $DIDi$ 。隐藏身份标识 $DIDi$ 可以基于第一设备的身份标识 IDi 生成。

隐藏身份标识 $DIDi$ 的生成方式有两种。如果 $N1$ 是第一设备与 AUSE 之间预先共享的密钥(或随机数),则 $DIDi$ 可以基于以下公式确定: $DIDi = IDi \oplus N1$ 。在建立第一设备的安全上下文之后,AUSE 可以向第一设备发送新的第一密钥以更新 $DIDi$ 。

如果 $N1$ 是第一设备与代理节点之间的共享密钥(如物理层密钥),则 $DIDi$ 可以基于公式 $DIDi = IDi \oplus N1$ 或 $DIDi = f_{N1}(IDi)$ 确定。

在步骤 S1104,代理节点向服务域网元发送认证请求。在一些实现方式中,代理节点可以通过基站向服务域网元发送认证请求。服务域网元可以包括 AMF、SEAF、SMF、A-NF 中的一个或多个。

在一些实施例中,该认证请求中可以包括 $DIDi$ 和代理节点的标识。例如,如果 $N1$ 为第一设备与认证网元之间的共享密钥,则认证请求中可以包括 $DIDi$ 和代理节点的标识。

在一些实施例中,如果 $N1$ 是第一设备与代理节点之间的共享密钥,则代理节点可以基于 $N1$ 对

DIDi 解匿名, 得到第一设备的身份标识 IDi。代理节点发送的认证请求中可以包括以下中的一种或多种: IDi、代理节点的标识和 N1。

代理节点的标识可以包括 GPSI、SUCI、GUTI 中的一种或多种。

5 为了保证信息的安全性, 代理节点可以通过 NAS 消息发送认证请求, 例如, 代理节点可以通过 NAS 安全上下文发送认证请求。

在步骤 S1106, 服务域网元向认证网元发送认证请求, 该认证请求中可以包括服务域网络的名称 (SN name)。该认证请求中还可以包括 DIDi 和代理节点的标识。或者, 该认证请求中可以包括 IDi、N1 和代理节点的标识。

10 在一些实施例中, 该认证请求中可以包括可指示认证类型的标识。认证类型的标识可以通过以下中的一种或多种指示: BSF ID、A-NF 的标识类型、IDi 的类型、认证类型标识 (Auth_type_ID)。

在步骤 S1108, 认证网元可以进行认证类型的确认。

认证网元可以通过核心网网元 (如 UDM) 查询第一设备与代理节点的订阅凭证。核心网网元可以基于 IDi 和代理节点的标识检查第一设备与代理节点的订阅凭证, 以确定第一设备是否有权使用 A-IoT 服务。

15 认证网元可以基于可指示认证类型的标识判断认证类型, 如判断认证类型是否为 A-IoT 认证。

如果认证网元接收到的认证请求中包括 DIDi, 则认证网元可以对 DIDi 进行解匿名, 得到 IDi。例如, 如果 N1 是第一设备与认证网元之间的共享密钥, 则认证网元可以基于 N1 对 DIDi 进行解匿名, 得到 IDi。举例说明, IDi 可以基于公式 $IDi = DIDi \oplus N1$ 确定。

20 认证网元可以生成第一匿名密钥 AK。如果 N1 是第一设备与认证网元之间的共享密钥, 则第一匿名密钥 AK 可以基于公式 $AK = K \oplus N1$ 确定。如果 N1 是第一设备与代理节点之间的共享密钥 (代理节点可以向认证网元发送 N1), 或者 N1 是第一设备与认证网元之间的共享密钥, 则第一匿名密钥 AK 可以基于公式 $AK = f_k(RAND)$ 确定。其中, RAND 是认证网元选取的随机数。

25 认证网元可以生成第一消息认证码 (记为 MAC) 和第一期望响应 (记为 XRES1)。MAC 和 XRES1 可以基于公式 $MAC/XRES1 = f_k(RAND, N1, N2)$ 确定。其中, N2 可以是第一设备与认证网元之间共享的密钥, 或者 N2 是认证网元选择的随机数。

上述 MAC 和 XRES1 的生成方式中引入的参数包括 RAND、N1 和 N2, 但这仅是一种示例, 本申请实施例对此不做具体限定。例如, MAC 和 XRES1 中引入的参数可以仅包含 RAND、或 RAND 和 N1、或 RAND 和 N2。

30 MAC 和 XRES1 的生成方式不同, 以使得到的 MAC 和 XRES1 的值不同。例如, 如果 MAC 和 XRES1 计算时使用相同的函数 f, 则引入的参数可以不同。又例如, 如果 MAC 和 XRES1 计算时引入的参数相同, 则可以使用不同的函数 f。

函数 f 可以有多种。例如, 函数 f 可以是 3GPP 定义的 f1-f5 中的任意一种函数。又例如, 函数 f 可以为 KDF (如 HMAC-SHA256)。又例如, 函数 f 可以为其他轻量级函数 (如 ASCON)。

如果 N2 是认证网元选择的随机数, 则 AK 可用于保护 N2, 如可以通过 AK 对 N2 进行加密处理。

35 认证网元可以生成第二期望响应 XRES2, XRES2 为服务域网络认证第一设备的材料。XRES2 可以基于公式 $XRES2 = f_k(XRES1, SN\ name)$ 确定。

认证网元可以生成第三期望响应 XRES3, XRES3 为基站认证第一设备的材料。XRES3 可以基于公式 $XRES3 = f_{N1}(XRES1)$ 确定。

40 认证网元可以生成认证向量。该认证向量可以包括认证网元生成和/或选择的多个参数。如该认证向量中可以包括以下中的一种或多种: RAND、N2、AK、MAC、XRES1、XRES2 和 XRES3。如果 N2 由认证网元选择, 则认证向量中可以包括 N2; 如果 N2 是第一设备与认证网元之间共享的, 则认证向量中可以不包括 N2。

在一些实施例中, 认证向量可以为 $AV = RAND || N2 \oplus AK || MAC || XRES1 || XRES2 || XRES3$ 。在另一些实施例中, 认证向量可以为 $AV = RAND || AK || MAC || XRES1 || XRES2 || XRES3$ 。

45 在一些实施例中, 认证向量中还可以包括以下参数中的一种或多种: IDi, UE ID, SN name。

在步骤 S1110, 认证网元向服务域网元发送认证响应。该认证响应中包括认证向量 AV。在一些实施例中, 该认证响应中还可以包括 IDi。

在步骤 S1112, 服务域网元接收到认证向量后, 可以存储认证向量中的 XRES2。

50 在步骤 S1114, 服务域网元向基站发送认证请求 (或认证响应)。该认证请求中包括认证向量。在一些实施例中, 该认证向量可以不包括 XRES2。在一些实施例中, 该认证响应中还可以包括 IDi。

在步骤 S1116, 如果认证向量中包括 XRES3, 则基站存储 XRES3; 如果认证向量中不包括 XRES3, 则基站可以基于 XRES1 生成 XRES3。

在步骤 S1118, 基站通过代理节点向第一设备发送认证请求。该认证请求中可以包括 RAND 和 MAC。或者, 该认证请求中可以包括 RAND 和 $N2 \oplus AK \parallel MAC$ 。其中, 如果 N2 是认证网元选择的随机数, 该 AK 可用于保护 N2 的安全。

在步骤 S1120, 第一设备接收到认证请求后, 可以检验 MAC。检验成功后, 第一设备可以计算第一响应参数 RES1、第二响应参数 RES2 和第三响应参数 RES3。另外, 第一设备还可以生成密钥 Ks。密钥 Ks 可以基于如下公式 $Ks = f_{AK}(N1, N2, UE\ ID, IDi, SN\ name)$ 确定。

在步骤 S1122, 第一设备通过代理节点向基站发送认证响应。该认证响应中包括 RES1、RES2 和 RES3。

在步骤 S1124, 基站比较 RES3 和 XRES3, 以认证第一设备。如果 RES3 和 XRES3 一致, 则第一设备认证成功。基站从接入网络的角度认为第一设备认证成功。

在步骤 S1126, 在第一设备认证成功后, 基站向服务域网元发送认证响应。该认证响应中包括 RES2 和 RES1。

在步骤 S1128, 服务域网元接收到认证响应后, 可以从认证响应中获取 RES2。服务域网元比较 RES2 和 XRES2, 以认证第一设备。认证成功后, 服务域网元从服务域网络的角度认为第一设备认证成功。

在步骤 S1130, 服务域网元向认证网元发送认证请求 (或者认证响应), 该认证请求中包括 RES1。

在步骤 S1132, 认证网元比较 RES1 和 XRES1, 以认证第一设备。认证成功后, 认证网元从归属域网络的角度认为第一设备认证成功。

认证网元还可以生成密钥 Ks。密钥 Ks 可以基于公式 $Ks = f_{AK}(N1, N2, UE\ ID, IDi, SN\ name)$ 确定。

在步骤 S1134, 认证网元向代理节点发送响应消息或者认证网元向服务域网元发送响应消息。在一些实施例中, 认证网元可以通过服务域网元和基站向代理节点发送响应消息。

在一些实施例中, 该认证响应中可以包括密钥 Ks。该密钥 Ks 可用于代理节点生成完整性保护密钥和/或加密密钥。

图 12 示出的是初始认证 (或轻量级初始认证) 完成后, 生成 AKMA 密钥的流程。

参见图 12, 在步骤 S1202, 认证网元生成密钥 Ks、A-KID 和 AKMA 密钥。第一设备生成密钥 Ks、A-KID 和 AKMA 密钥。

在一些实施例中, 认证网元可以基于密钥 Ks 生成 A-TID。作为一个示例, A-TID 可以基于 Ks 和 IDi 生成。例如, A-TID 可以基于公式 $A-TID = f_{Ks}(IDi)$ 确定。

在一些实施例中, 认证网元可以基于 A-TID 生成 A-KID。作为一个示例, A-KID 可以基于 A-TID、RID 和 HNI 生成。例如, A-KID 可以基于公式 $A-KID = A-TID \parallel RID \parallel HNI$ 确定。

在一些实施例中, 认证网元可以生成 AKMA 密钥 (记为 K_{AKMA})。AKMA 密钥可以基于 Ks 生成, 在该情况下, Ks 的作用与相关技术中的 K_{AUSF} 的作用相同。作为一个示例, AKMA 密钥可以基于 Ks、IDi 和 AKMA 生成。例如, AKMA 密钥可以基于公式 $Kakma = f_{Ks}("AKMA", "IDi")$ 确定。

在步骤 S1204, 认证网元可以向 AAnF 或 KMS 发送注册请求, 该注册请求中可以包括以下信息中的一种或多种: AKMA 密钥、A-KID 和第一设备的标识 IDi。该注册请求例如可以为 AKMA 锚点密钥注册请求 (如 $Naanf_AKMA_AnchorKey_Register\ Request$)。

类似地, 在步骤 S1202, 第一设备可以生成密钥 Ks、A-KID 和 AKMA 密钥。第一设备生成 A-KID 的方式与认证网元生成 A-KID 的方式类似, 第一设备生成 AKMA 密钥的方式与认证网元生成 AKMA 密钥的方式类似, 为了简洁, 此处不再赘述。

图 13 示出的是生成应用密钥的流程。

参见图 13, 在步骤 S1302, 第一设备向 AF 发送应用会话建立请求。该应用会话建立请求中可以包括 A-KID。该应用会话建立请求也可以为其他的通信请求。

在一些实施例中, 该应用会话建立请求中可以包括 UE ID 和 DIDi。UE ID 例如可以为 GPSI。UE ID 为代理节点的标识。

在步骤 S1304, AF 接收到应用会话建立请求后, 向 AAnF 或 KMS 发送应用密钥请求。该应用密钥请求中可以包括 A-KID。在一些实施例中, 该应用密钥请求中还可以包括 UE ID 和 DIDi。

在步骤 S1306, AAnF 或 KMS 接收到应用密钥请求后, 可以基于 A-KID 生成应用密钥。

在一些实施例中, 该应用密钥 K_{AF} 可以基于 Ks、AF ID、IDi、UE ID 以及 A-KID 生成。例如, 应用密钥 K_{AF} 可以基于公式 $KAF = f_{Ks}(AF\ ID, IDi, UE\ ID, A-KID)$ 确定。

在步骤 S1308, AAnF 或 KMS 向 AF 发送应用密钥响应。该应用密钥响应中包括 K_{AF} 和 K_{AF} 的有效期。

AAnF 或 KMS 可以存储 K_{AF} 和 K_{AF} 的有效期, 以便于第一设备的移动性管理。

在步骤 S1310, AF 向代理节点发送应用密钥响应。该应用密钥响应中包括 K_{AF} 和 K_{AF} 的有效期。

在步骤 S1312, 代理节点生成密钥 K_{u1} 。密钥 K_{u1} 可以基于 K_{AF} 生成。作为一个示例, K_{u1} 可以基于 K_{AF} 和 $N1$ 生成。例如, K_{u1} 可以基于公式 $K_{u1}=K_{AF} \oplus N1$ 确定。其中, $N1$ 为第一设备与代理节点之间的共享密钥。

在步骤 S1314, 代理节点向第一设备发送应用会话建立响应。

在步骤 S1316, 第一设备生成应用密钥 K_{AF} 和密钥 K_{u1} 。第一设备生成 K_{AF} 的方式与 AAnF 或 KMS 生成 K_{AF} 的方式类似, 第一设备生成密钥 K_{u1} 和代理节点生成密钥 K_{u1} 的方式类似, 为了简洁, 此处不再赘述。

在步骤 S1318, 第一设备可以向代理节点发送响应消息。

上述密钥 K_{u1} 可用于生成完整性保护密钥和/或加密密钥, 该完整性保护密钥和/或加密密钥可用于保证第一设备与代理节点之间的安全通信。之后, 如果第一设备使用其他的设备 (如 UEx) 作为代理节点时, 可以使用第一设备与 UEx 之间的共享密钥 N_x , 以及 K_{AF} , 生成下级密钥 K_{ux} 。该 K_{ux} 可用于进一步生成完整性保护密钥和/或加密密钥。这样, 在代理节点发生变化时, 第一设备不一定需要进行第一设备的认证与密钥协商流程, 从而可以降低第一设备的复杂度。

示例二

示例二的方案中, 安全凭证为 3GPP 安全凭证, 第一设备不需要通过代理节点与网络侧进行通信, 即第一设备可以直接与网络侧进行通信。

示例二与示例一的区别在于: 1、没有代理节点参与, 2、认证信息中不包括代理节点的信息 (如代理节点的标识或 UE ID)。

示例二的方案与示例一的方案基本类似, 示例二中未详细描述的内容可以参见示例一的描述。

图 14 是本申请实施例提供的一种认证方法的流程示意图。参见图 14, 在步骤 S1410, 认证网元生成第一消息认证码和/或期望响应。第一消息认证码和期望响应的生成方式可以参见示例一的描述。

在步骤 S1420, 认证网元向接入网设备发送第一认证请求。该第一认证请求中可以包括第一消息认证码。

认证网元向接入网设备发送第一认证请求, 可以指认证网元直接向接入网设备发送第一认证请求, 或者, 也可以指认证网元通过其他设备向接入网设备发送第一认证请求。其他设备例如可以包括服务域网元。服务域网元例如可以包括 AMF 和/或 SMF。

在步骤 S1430, 接入网设备向第一设备发送第一认证请求。

在步骤 S1440, 第一设备基于第一密钥生成算法和第二参数生成第二消息认证码。

在步骤 S1450, 第一设备基于第一消息认证码和第二消息认证码认证认证网元。

在步骤 S1460, 在认证网元认证成功的情况下, 第一设备生成响应参数。

在步骤 S1470, 第一设备向接入网设备发送第一认证响应。该第一认证响应中包括响应参数。

在步骤 S1480, 接入网设备向认证网元发送第一认证响应。该第一认证响应中包括响应参数。

在一些实施例中, 接入网设备可以向认证网元发送响应参数。认证网元接收到响应参数后, 可以比较响应参数和期望响应, 以认证第一设备。

在一些实施例中, 在接收来自接入网设备的第一认证请求之前, 第一设备可以向接入网设备发送第二认证请求。换句话说, 第一设备可以通过发送第二认证请求, 以触发第一设备与网络侧之间的认证流程。

在一些实施例中, 第二认证请求中可以包括第一设备的隐藏身份标识。为了保证信息的安全性, 第一设备可以对第一设备的身份标识进行匿名处理, 得到隐藏身份标识。

接入网设备接收到第二认证请求后, 可以向认证网元发送该第二认证请求。接入网设备发送的第二认证请求中可以包括以下信息中的一种或多种: 第一密钥、第一设备的身份标识、隐藏身份标识。

在一些实施例中, 接入网设备可以根据第一密钥的不同, 采取不同的处理策略。作为一个示例, 如果第一密钥为第一设备与网络侧之间的共享密钥, 则接入网设备发送的第二认证请求中可以包括隐藏身份标识。

作为另一个示例, 如果第一密钥为第一设备与接入网设备之间的共享密钥, 则接入网设备可以对隐藏身份标识进行解匿名, 得到第一设备的身份标识。例如, 接入网设备可以基于第一密钥与隐藏身份标识, 确定第一设备的身份标识。

如果隐藏身份标识由第一密钥和第一设备的身份标识通过异或的方式生成, 则接入网设备可以通过如下公式确定第一设备的身份标识:

$$ID_i = DID_i \oplus N1$$

其中, DID_i 表示隐藏身份标识, ID_i 表示第一设备的身份标识, $N1$ 表示第一密钥, $\oplus$ 表示异或运算。

如果隐藏身份标识基于第一密钥、第一设备的身份标识和第三密钥生成算法生成，则接入网设备可以通过如下公式确定第一设备的身份标识：

$$IDi = f_{N1}(DIDi)$$

其中，DIDi 表示隐藏身份标识，IDi 表示第一设备的身份标识，N1 表示第一密钥，f 表示第三密钥生成算法。

在得到第一设备的身份标识后，第一设备发送的第二认证请求中可以包括以下中的一种或多种：第一密钥、第一设备的身份标识。

第一设备与认证网元认证完成后，可以生成第二密钥 Ks。第二密钥也可以理解为第一设备与认证网元之间的共享密钥。第二密钥可以基于第六密钥生成算法和第六参数生成。第六密钥生成算法可以为第一密钥生成算法或第二密钥生成算法，以降低第一设备的计算复杂度。第六参数可以包括以下参数中的一种或多种：第一匿名密钥、第一密钥、第一随机数、第一设备的标识和服务域网络的名称。

举例说明，第二密钥可以基于以下公式确定：

$$Ks = f_{AK}(N1, N2, IDi, SN\ name)$$

其中，Ks 表示第二密钥，AK 表示第一匿名密钥，N1 表示第一密钥，N2 表示第一随机数，IDi 表示第一设备的身份标识，SN name 表示服务域网络的名称，f 表示第六密钥生成算法。

下面结合图 15 和 16，对没有代理节点参与的认证与密钥协商流程进行详细介绍。

图 15 示出的是第一设备与认证网元之间进行认证的流程。第一设备可以与认证网元共享密钥 K，该密钥 K 即为上文描述的安全凭证。第一设备可以与基站共享密钥 N1，该密钥 N1 即为上文描述的第一密钥。该密钥 N1 可以为物理层密钥。

图 15 所示的方法与图 11 所示的方案基本类似，图 15 中未详细描述的内容可以参见图 11 中的描述。

参见图 15，在步骤 S1502，第一设备向基站发送认证请求。该认证请求中可以包括第一设备的隐藏身份标识 DIDi。隐藏身份标识 DIDi 可以基于第一设备的身份标识 IDi 生成。

在步骤 S1504，基站向服务域网元发送认证请求。

在一些实施例中，该认证请求中可以包括 DIDi。例如，如果 N1 为第一设备与认证网元之间的共享密钥，则认证请求中可以包括 DIDi。

在一些实施例中，如果 N1 为第一设备与基站之间的共享密钥，则基站可以基于 N1 对 DIDi 解匿名，得到第一设备的身份标识 IDi。基站发送的认证请求中可以包括以下中的一种或多种：IDi 和 N1。

在步骤 S1506，服务域网元向认证网元发送认证请求，该认证请求中可以包括服务域网络的名称 (SN name)。在一些实施例中，该认证请求中还可以包括 DIDi，或者，该认证请求中可以包括 IDi 和 N1。

在步骤 S1508，认证网元可以进行认证类型的确认。

在一些实施例中，如果认证网元接收到的认证请求中包括 DIDi，则认证网元可以对 DIDi 进行解匿名，得到 IDi。

在一些实施例中，认证网元可以生成第一匿名密钥 AK、第一消息认证码、第一期望响应、第二期望响应和第三期望响应。

在一些实施例中，认证网元可以生成认证向量。该认证向量可以包括认证网元生成和/或选择的多个参数。如该认证向量中可以包括以下中的一种或多种：RAND、N2、AK、MAC、XRES1、XRES2 和 XRES3。如果 N2 由认证网元选择，则认证向量中可以包括 N2；如果 N2 是第一设备与认证网元之间共享的，则认证向量中可以不包括 N2。

在一些实施例中，认证向量可以为 $AV = RAND \parallel N2 \oplus AK \parallel MAC \parallel XRES1 \parallel XRES2 \parallel XRES3$ 。在另一些实施例中，认证向量可以为 $AV = RAND \parallel AK \parallel MAC \parallel XRES1 \parallel XRES2 \parallel XRES3$ 。

在一些实施例中，认证向量中还可以包括以下参数中的一种或多种：IDi，UE ID，SN name。

在步骤 S1510，认证网元向服务域网元发送认证响应。该认证响应中包括认证向量 AV。

在步骤 S1512，服务域网元接收到认证向量后，可以存储认证向量中的 XRES2。

在步骤 S1514，服务域网元向基站发送认证请求（或认证响应）。该认证请求中包括认证向量。在一些实施例中，该认证向量可以不包括 XRES2。

在步骤 S1516，如果认证向量中包括 XRES3，则基站存储 XRES3；如果认证向量中不包括 XRES3，则基站可以基于 XRES1 生成 XRES3。

在步骤 S1518，基站向第一设备发送认证请求。该认证请求中可以包括 RAND 和 MAC。或者，该认证请求中可以包括 RAND 和 $N2 \oplus AK \parallel MAC$ 。其中，如果 N2 是认证网元选择的随机数，该 AK 可用于保护 N2 的安全。

在步骤 S1520, 第一设备接收到认证请求后, 可以检验 MAC。检验成功后, 第一设备可以计算第一响应参数 RES1、第二响应参数 RES2 和第三响应参数 RES3。另外, 第一设备还可以生成密钥 Ks。密钥 Ks 可以基于如下公式 $Ks=f_{AK}(N1,N2, IDi, SN\ name)$ 确定。

在步骤 S1522, 第一设备向基站发送认证响应。该认证响应中包括 RES1、RES2 和 RES3。

5 在步骤 S1524, 基站比较 RES3 和 XRES3, 以认证第一设备。如果 RES3 和 XRES3 一致, 则第一设备认证成功。基站从接入网络的角度认为第一设备认证成功。

在步骤 S1526, 在第一设备认证成功后, 基站向服务域网元发送认证响应。该认证响应中包括 RES2 和 RES1。

10 在步骤 S1528, 服务域网元接收到认证响应后, 可以从认证响应中获取 RES2。服务域网元比较 RES2 和 XRES2, 以认证第一设备。认证成功后, 服务域网元从服务域网络的角度认为第一设备认证成功。

在步骤 S1530, 服务域网元向认证网元发送认证请求 (或者认证响应), 该认证请求中包括 RES1。

在步骤 S1532, 认证网元比较 RES1 和 XRES1, 以认证第一设备。认证成功后, 认证网元从归属域网络的角度认为第一设备认证成功。

认证网元还可以生成密钥 Ks。密钥 Ks 可以基于公式 $Ks=f_{AK}(N1,N2, IDi, SN\ name)$ 确定。

15 在步骤 S1534, 认证网元可以向服务域网元发送响应消息。

在得到密钥 Ks 后, 认证网元和第一设备可以按照图 12 所示的方法生成 AKMA 密钥。另外, 认证网元可以向 AAnF 或 KMS 发送注册请求, 该注册请求中可以包括以下信息中的一种或多种: AKMA 密钥、A-KID 和第一设备的标识 IDi。

图 16 示出的是生成应用密钥的流程。

20 参见图 16, 在步骤 S1602, 第一设备向 AF 发送应用会话建立请求。该应用会话建立请求中可以包括 A-KID。该应用会话建立请求也可以为其他的通信请求。在一些实施例中, 该应用会话建立请求中可以包括 DIDI。

在步骤 S1604, AF 接收到应用会话建立请求后, 向 AAnF 或 KMS 发送应用密钥请求。该应用密钥请求中可以包括 A-KID。在一些实施例中, 该应用密钥请求中还可以包括 DIDI。

25 在步骤 S1606, AAnF 或 KMS 接收到应用密钥请求后, 可以基于 A-KID 生成应用密钥。

在一些实施例中, 该应用密钥 K_{AF} 可以基于 Ks、AF ID、IDi 以及 A-KID 生成。例如, 应用密钥 K_{AF} 可以基于公式 $K_{AF}=f_{Ks}(AF\ ID, IDi, A-KID)$ 确定。

在步骤 S1608, AAnF 或 KMS 向 AF 发送应用密钥响应。该应用密钥响应中包括 K_{AF} 和 K_{AF} 的有效期。

30 AAnF 或 KMS 可以存储 K_{AF} 和 K_{AF} 的有效期, 以便于第一设备的移动性管理。

在步骤 S1610, AF 向第一设备发送应用会话建立响应。

之后, 第一设备和 AF 可以基于 K_{AF} 建立安全连接 (如 TLS 连接)。

示例三

35 示例三的方案中, 安全凭证为非 3GPP 安全凭证, 如安全凭证为第一设备与应用功能网元之间的共享密钥, 第一设备通过代理节点与网络侧进行通信。

图 17 是本申请实施例提供的一种认证方法的流程示意图。参见图 17, 在步骤 S1710, 第一设备向应用功能网元发送认证请求。在一些实施例中, 第一设备可以通过代理节点向应用功能网元发送认证请求。

40 该认证请求中可以包括以下信息中的一种或多种: 第一设备的隐藏身份标识、第一设备的身份标识、代理节点的标识和第一密钥。在一些实施例中, 认证请求中可以包括第一设备的隐藏身份标识和代理节点的标识。在另一些实施例中, 认证请求中可以包括第一设备的身份标识、代理节点的标识和第一密钥。

在步骤 S1720, 应用功能网元对第一设备和/或代理节点进行授权检查。例如, 应用功能网元可以检查第一设备是否被授权使用某种服务 (如 A-IoT 服务)。又例如, 应用功能网元可以检查代理节点是否被授权作为代理为第一设备提供服务 (如 A-IoT 服务)。

45 在一些实施例中, 应用功能网元可以管理第一设备的白名单与代理节点之间的映射。

应用功能网元在对第一设备进行授权检查时, 可以基于第一设备的身份标识 IDi 对第一设备进行授权检查。应用功能网元在对代理节点进行授权检查时, 可以基于代理节点的标识 (如 UE ID) 对代理节点进行授权检查。

第一设备的身份标识和代理节点的标识可由代理节点发送至应用功能网元。

50 在一些实施例中, 第一设备可以向代理节点发送认证请求, 该认证请求中可以包括第一设备的隐藏身份标识 DIDI。代理节点可以对隐藏身份标识 DIDI 进行解匿名, 得到第一设备的身份标识。

代理节点可以向应用功能网元发送认证请求, 该认证请求中可以包括第一设备的身份标识 IDi 和代

理节点的标识。为了保证信息的安全性,代理节点可以通过 NAS 安全上下文或 AS 安全上下文发送认证请求。

在步骤 S1730,在第一设备和/或代理节点授权检查成功的情况下,应用功能网元向认证网元发送认证请求。

- 5 如果第一设备和/或代理节点授权检查失败,则应用功能网元可以不向认证网元发送认证请求,即不进行后续的认证与密钥协商流程。

本申请实施例可以由应用功能网元先对第一设备和代理节点进行授权检查,在授权检查成功的情况下,才进行后续的认证与密钥协商流程,有利于降低第一设备的计算复杂度。例如,如果在认证与密钥协商流程完成后,才进行授权检查,会出现授权检查失败的情况,这就会使得第一设备的认证与密钥协商流程无效,从而造成资源的浪费,不利于降低第一设备的计算复杂度。

10 在一些实施例中,隐藏身份标识可以基于第一密钥 N1 生成。第一密钥可以为第一设备与应用功能网元之间的共享密钥,或者,第一密钥可以为第一设备与代理节点之间的共享密钥(如物理层密钥)。

如果第一密钥为第一设备与代理节点之间的共享密钥,则代理节点可以基于第一密钥,对隐藏身份标识进行解匿名,得到第一设备的身份标识。如果第一密钥为第一设备与应用功能网元之间的共享密钥,则应用功能网元可以对隐藏身份标识进行解匿名,得到第一设备的身份标识。

15 举例说明,第一设备的身份标识 IDi 可以通过公式 $IDi = DIDi \oplus N1$ 或公式 $IDi = f_{N1}(DIDi)$ 确定。

如果第一密钥为第一设备与代理节点之间的共享密钥,则代理节点向应用功能网元发送的认证请求中可以包括第一设备的身份标识、代理节点的标识和第一密钥。如果第一密钥为第一设备与应用功能网元之间的共享密钥,则代理节点向应用功能网元发送的认证请求中可以包括第一设备的隐藏身份标识和代理节点的标识。

20 在一些实施例中,应用功能网元可以向认证网元发送安全凭证 K,或者应用功能网元可以向认证网元发送安全凭证 K 的下级密钥(记为 Kb)。该下级密钥为基于安全凭证 K 生成的密钥。认证网元可以基于下级密钥,确定出安全凭证 K。

下级密钥例如可以基于安全凭证 K、第一密钥(记为 N1)和第一随机数(记为 N2)中的一个或多个生成。例如,下级密钥 Kb 可以基于公式 $Kb = K \oplus N1$ 或公式 $Kb = K \oplus N2$ 生成。其中,N2 可以是第一设备与 AF 之间的共享密钥,或者,N2 可以是 AF 选择的随机数。

如果认证网元接收的是安全凭证 K,则认证网元可以基于安全凭证 K 生成认证过程中所需要的参数。该参数例如可以为认证向量中包含的参数。该参数例如可以包括以下中的一种或多种:第一匿名密钥、第一消息认证码、期望响应、密钥 Ks 等。密钥 Ks 为第一设备与认证网元认证成功后,生成的共享密钥。

30 在一些实施例中,第一匿名密钥可以基于安全凭证 K 和目标参数生成。该目标参数可以包括 RAND 和/或 N1。例如,第一匿名密钥 AK 可以基于公式 $AK = f_K(RAND)$ 或公式 $AK = K \oplus N1$ 确定。

35 在一些实施例中,第一消息认证码可以基于安全凭证 K 和目标参数生成。该目标参数可以包括以下中的一种或多种:RAND、N1 和 N2。例如,目标参数包括 RAND。又例如,目标参数包括 RAND 和 N1。又例如,目标参数包括 RAND 和 N2。又例如,目标参数包括 RAND、N1 和 N2。

举例说明,第一消息认证码可以基于以下公式中的一种或多种确定: $MAC = f_K(RAND, N1, N2)$, $MAC = f_K(RAND, N1)$, $MAC = f_K(RAND, N2)$, $MAC = f_K(RAND)$ 。

40 在一些实施例中,期望响应可以基于安全凭证 K 和目标参数生成。该目标参数可以包括以下中的一种或多种:RAND、N1 和 N2。例如,目标参数包括 RAND。又例如,目标参数包括 RAND 和 N1。又例如,目标参数包括 RAND 和 N2。又例如,目标参数包括 RAND、N1 和 N2。

举例说明,期望响应可以基于以下公式中的一种或多种确定: $XRES = f_K(RAND, N1, N2)$, $XRES = f_K(RAND, N1)$, $XRES = f_K(RAND, N2)$, $XRES = f_K(RAND)$ 。

45 密钥 Ks 可以基于安全凭证 K 和目标参数生成。目标参数可以包括以下中的一种或多种:AK、N1、N2、IDi、UE ID、AF ID、HNI、SN name。例如,目标参数可以包括 AK、N1、N2、IDi、UE ID、AF ID、HNI。又例如,目标参数可以包括 AK、N1、N2、IDi、UE ID、AF ID、SN name。

举例说明,密钥 Ks 可以基于公式 $Ks = f_{AK}(N1, N2, IDi, UE ID, AF ID, HNI)$ 或公式 $Ks = f_{AK}(N1, N2, IDi, UE ID, AF ID, SN name)$ 确定。

50 如果认证网元接收的是密钥 Kb,则认证网元可以基于密钥 Kb 生成认证过程中所需要的参数。该参数例如可以为认证向量中包含的参数。该参数例如可以包括以下中的一种或多种:第一消息认证码、期望响应、密钥 Ks 等。

第一消息认证码可以基于密钥 Kb 以及目标参数生成。该目标参数可以包括以下中的一种或多种:RAND、N1 和 N2。例如,目标参数包括 RAND。又例如,目标参数包括 RAND 和 N1。又例如,目标

参数包括 RAND 和 N2。又例如, 目标参数包括 RAND、N1 和 N2。

举例说明, 第一消息认证码可以基于以下公式中的一种或多种确定: $MAC = f_{kb}(RAND, N1, N2)$, $MAC = f_{kb}(RAND, N1)$, $MAC = f_{kb}(RAND, N2)$, $MAC = f_{kb}(RAND)$ 。

在一些实施例中, 期望响应可以基于安全凭证 K 和目标参数生成。该目标参数可以包括以下中的一种或多种: RAND、N1 和 N2。例如, 目标参数包括 RAND。又例如, 目标参数包括 RAND 和 N1。又例如, 目标参数包括 RAND 和 N2。又例如, 目标参数包括 RAND、N1 和 N2。

举例说明, 期望响应可以基于以下公式中的一种或多种确定: $XRES = f_{kb}(RAND, N1, N2)$, $XRES = f_{kb}(RAND, N1)$, $XRES = f_{kb}(RAND, N2)$, $XRES = f_{kb}(RAND)$ 。

密钥 K_s 可以基于安全凭证 K 和目标参数生成。目标参数可以包括以下中的一种或多种: AK、N1、N2、IDi、UE ID、AF ID、HNI、SN name。例如, 目标参数可以包括 AK、N1、N2、IDi、UE ID、AF ID、HNI。又例如, 目标参数可以包括 AK、N1、N2、IDi、UE ID、AF ID、SN name。

举例说明, 密钥 K_s 可以基于公式 $K_s = f_{kb}(N1, N2, IDi, UE ID, AF ID, HNI)$ 或公式 $K_s = f_{kb}(N1, N2, IDi, UE ID, AF ID, SN name)$ 确定。

在一些实施例中, 第一设备可以采用与认证网元相同的方式, 生成以下参数中的一种或多种: 第一匿名密钥、第二消息认证码、响应参数、密钥 K_s 等。例如, 第二消息认证码的生成方式与第一消息认证码的生成方式相同。又例如, 响应参数的生成方式与期望响应的生成方式相同。

在一些实施例中, 上述期望响应可以包括第一期望响应、第二期望响应和第三期望响应。第一期望响应的生成方式可以为上文中的期望响应的生成方式。第二期望响应和第三期望响应可以基于第一期望响应生成, 具体的生成方式可以参见其他示例中的描述。

在一些实施例中, 上述响应参数可以包括第一响应参数、第二响应参数和第三响应参数。第一响应参数的生成方式可以为上文中的响应参数的生成方式。第二响应参数和第三响应参数可以基于第一响应参数生成, 具体的生成方式可以参见其他示例中的描述。

上述公式中的 f 可以为相同的密钥生成算法, 或者上述公式中的 f 可以包括第一密钥生成算法和第二密钥生成算法。例如, 第一密钥生成算法用于生成第一消息认证码或第二消息认证码, 第二密钥生成算法用于生成期望响应或响应参数。

在得到 K_s 后, 第一设备和认证网元可以基于 K_s 生成 A-TID、A-KID 以及 AKMA 密钥中的一种或多种。具体的生成方式可以参见前文中其他示例的描述。

由于应用功能网元参与了认证与密钥协商流程, 则应用功能网元可以直接接收 AAnF 发送的应用密钥。例如, AAnF 可以在生成应用密钥后, 直接向 AF 发送应用密钥, 而不需要 AF 发送应用密钥请求来触发。

AF 接收到应用密钥后, 可以向代理节点发送应用密钥。该应用密钥可用于代理节点生成第三密钥 (如 K_{u1})。

AAnF 生成应用密钥的方式、以及代理节点生成第三密钥的方式可以参见前文的描述, 此处不再赘述。

图 17 所示的方案中涉及的第一设备与网络侧之间的认证与密钥协商流程可以与前文中的方案类似, 未详细描述的内容可以参见前文的描述, 为了简洁, 此处不再赘述。

下面结合图 18, 对有代理节点参与的认证与密钥协商流程进行详细介绍。在图 18 所示的方案中, 第一设备可以与 AF 共享密钥 K。

参见图 18, 在步骤 S1802, 第一设备向代理节点发送认证请求。该认证请求中包括第一设备的隐藏身份标识 DIDi。隐藏身份标识 DIDi 可以基于第一设备的身份标识 IDi 生成。

隐藏身份标识 DIDi 的生成方式有两种。如果 N1 是第一设备与 AF 之间预先共享的密钥 (或随机数), 则 DIDi 可以基于以下公式确定: $DIDi = IDi \oplus N1$ 。在建立第一设备的安全上下文之后, AF 可以向第一设备发送新的第一密钥以更新 DIDi。

如果 N1 是第一设备与代理节点之间的共享密钥 (如物理层密钥), 则 DIDi 可以基于公式 $DIDi = IDi \oplus N1$ 或 $DIDi = f_{N1}(IDi)$ 确定。

在步骤 S1804, 代理节点向 AF 发送认证请求。

在一些实施例中, 该认证请求中可以包括 DIDi 和代理节点的标识。例如, 如果 N1 为第一设备与 AF 之间的共享密钥, 则认证请求中可以包括 DIDi 和代理节点的标识。

在一些实施例中, 如果 N1 是第一设备与代理节点之间的共享密钥, 则代理节点可以基于 N1 对 DIDi 解匿名, 得到第一设备的身份标识 IDi。代理节点发送的认证请求中可以包括以下中的一种或多种: IDi、代理节点的标识和 N1。

代理节点的标识可以包括 GPSI、SUCI、GUTI 中的一种或多种。

为了保证信息的安全性,代理节点可以通过 NAS 消息发送认证请求,例如,代理节点可以通过 NAS 安全上下文发送认证请求。

在步骤 S1806, AF 可以进行授权管理。

5 在一些实施例中,如果 N1 为第一设备与 AF 之间的共享密钥,则 AF 可以根据 N1 解匿名得到第一设备的身份标识 IDi。例如, IDi 可以通过公式 $IDi = D \parallel IDi \oplus N1$ 或公式 $IDi = f_{N1}(D \parallel IDi)$ 确定。

在一些实施例中,AF 可以检查第一设备是否被授权。在一些实施例中,AF 可以检查代理节点是否被授权为第一设备提供服务(如 A-IoT 服务)。在一些实施例中,AF 还可以检查第一设备与代理节点之间的映射关系。AF 可以管理第一设备的白名单与代理节点名单间的映射。

10 在一些实施例中,如果 AF 接收到的认证请求中包括 IDi、代理节点的标识和 N1,则 AF 可以直接进行授权检查,以及管理第一设备与代理节点之间的映射。

在步骤 S1808, AF 向认证网元发送认证请求。该认证请求中可以包括安全凭证 K 或由安全凭证 K 衍生的下级密钥 Kb。在一些实施例中,该认证请求中还可以包括以下信息中的一种或多种: IDi, UE ID, AF ID。

15 在一些实施例中,该认证请求中可以包括以下中的一种或多种: K、K||N1、K||N1||N2 和 K||N2。其中, N1 可以是第一设备与代理节点之间的共享密钥,或者 N1 可以是第一设备与 AF 之间的共享密钥。N2 可以是第一设备与 AF 之间的共享密钥,或者 N2 可以是 AF 选择的随机数。

在一些实施例中,该认证请求中可以包括以下中的一种或多种: Kb、Kb||N2、Kb||N1。

如果 Kb 基于 K 和 N1 生成,则认证请求中可以包括 Kb||N2;如果 Kb 基于 K 和 N2 生成,则认证请求中可以包括 Kb||N1。

20 在一些实施例中,该认证请求中可以包括可指示认证类型的标识。认证类型的标识可以通过以下中的一种或多种指示: AF ID、IDi 的类型、认证类型标识(Auth_type_ID)。

在步骤 S1810,第一设备与认证网元之间进行认证(如 AKA 认证)。该认证方式可以参见前文的描述,如参见前文图 11 的描述。

代理节点可以转发第一设备与认证网元之间的认证消息。

25 认证网元可以通过核心网网元(如 UDM)查询第一设备与代理节点的订阅凭证。核心网网元可以基于 IDi 和代理节点的标识检查第一设备与代理节点的订阅凭证,以确定第一设备是否有权使用 A-IoT 服务。

认证网元可以基于可指示认证类型的标识判断认证类型,如判断认证类型是否为 A-IoT 认证。

认证网元生成认证向量。认证网元可以选择随机数 RAND,该随机数 RAND 可用于生成认证向量。

30 如果认证网元接收到的认证请求中包括 K、K||N1、K||N1||N2、K||N2 中的一个或多个,则认证网元可以基于 K 和 RAND 生成认证参数。该认证参数包括以下中的一种或多种: 第一匿名密钥 AK、第一消息认证码 MAC、期望响应 XRES 和认证向量 AV。

第一匿名密钥 AK 可以通过公式 $AK = f_K(RAND)$ 或公式 $AK = K \oplus N1$ 确定。

第一消息认证码 MAC 可以基于公式 $MAC = f_K(RAND, N1, N2)$ 确定。

35 期望响应 XRES 可以基于公式 $XRES = f_K(RAND, N1, N2)$ 确定。

认证向量可以为 $AV = RAND \parallel AK \parallel MAC \parallel XRES$ 。

MAC 与 XRES 计算时可以使用相同的函数 f 和不同的参数。或者,MAC 和 XRES 计算时可以使用相同的参数和不同的函数 f。

40 如果认证网元接收到的认证请求中包括 Kb、Kb||N1、Kb||N2 中的一个或多个,则认证网元可以基于 Kb 和 RAND 生成认证参数。该认证参数包括以下中的一种或多种: 第一消息认证码 MAC、期望响应 XRES 和认证向量 AV。

第一消息认证码 MAC 可以基于以下公式中一种或多种确定: $MAC = f_{Kb}(RAND, N1, N2)$ 、 $MAC = f_{Kb}(RAND)$ 、 $MAC = f_{Kb}(RAND, N1)$ 、 $MAC = f_{Kb}(RAND, N2)$ 。

45 期望响应 XRES 可以基于以下公式中一种或多种确定: $XRES = f_{Kb}(RAND, N1, N2)$ 、 $XRES = f_{Kb}(RAND)$ 、 $XRES = f_{Kb}(RAND, N1)$ 、 $XRES = f_{Kb}(RAND, N2)$ 。

认证向量可以为 $AV = RAND \parallel MAC \parallel XRES$ 。

MAC 与 XRES 计算时可以使用相同的函数 f 和不同的参数。或者,MAC 和 XRES 计算时可以使用相同的参数和不同的函数 f。

50 在一些实施例中,认证网元可以通过代理节点向第一设备发送认证响应。该认证响应中可以包括 RAND 和第一消息认证码。在一些实施例中,如果 N2 是 AF 选择的随机数,则认证响应中还可以包括 $AK \oplus N2$ 或者 $Kb \oplus N2$,其中, AK 和 Kb 用于保护 N2,以保证 N2 安全地传输。在一些实施例中,认证响应中可以包括 AF ID 和 IDi。

第一设备可以计算第二消息认证码，并比较第一消息认证码和第二消息认证码，以认证认证网元。认证成功后，第一设备可以生成密钥 K_s 。密钥 K_s 可以基于以下公式中的一种或多种确定： $K_s = f_{AK}(N1, N2, ID_i, UE\ ID, AF\ ID, SN\ name)$ ， $K_s = f_{AK}(N1, N2, ID_i, UE\ ID, AF\ ID, HNI)$ ， $K_s = f_{kb}(N1, N2, ID_i, UE\ ID, AF\ ID, SN\ name)$ ， $K_s = f_{kb}(N1, N2, ID_i, UE\ ID, AF\ ID, HNI)$ 。

5 在一些实施例中，第一设备可以生成 A-TID。A-TID 可以基于公式 $A-TID = f_{K_s}(ID_i)$ 确定。在一些实施例中，第一设备可以生成 A-KID，A-KID 可以基于公式 $A-KID = A-TID || RID || HNI$ 确定。在一些实施例中，第一设备可以生成 AKMA 密钥，AKMA 密钥可以基于公式 $K_{AKMA} = f_{K_s}("AKMA", "ID_i")$ 确定。

在一些实施例中，第一设备可以生成响应参数 RES，RES 的计算方式与 XRES 的计算方式相同。

10 第一设备可以通过代理节点向认证网元发送认证响应，该认证响应可以包括响应参数 RES。认证网元可以比较 RES 和 XRES，以认证第一设备。如果 RES 和 XRES 一致，则第一设备认证成功；如果 RES 和 XRES 不一致，则第一设备认证失败。在第一设备认证成功后，认证网元可以生成以下参数中的一种或多种： K_s 、A-TID、A-KID 以及 AKMA 密钥。认证网元生成这些参数的方式与第一设备生成对应参数的方式相同。

在步骤 S1812，认证网元向 AAnF 提供密钥材料，该密钥材料可以包括 AKMA 密钥和 A-KID。

15 在步骤 S1814，AAnF 基于 AKMA 密钥生成应用密钥 K_{AF} 。应用密钥 K_{AF} 可以基于公式 $K_{AF} = f_{KAKMA}(AF\ ID, ID_i, UE\ ID)$ 确定。

在步骤 S1816，AAnF 向 AF 和/或代理节点发送响应消息。该消息可以为成功响应消息。该响应消息中可以包括应用密钥和/或应用密钥的有效期。在一些实施例中，响应消息中还可以包括新选取的第一密钥（或随机数），新的第一密钥可用于更新隐藏身份标识。

20 在步骤 S1818，代理节点生成密钥 K_{ul} 。

在步骤 S1820，第一设备生成密钥 K_{ul} 。

密钥 K_{ul} 可以基于应用密钥生成。具体的生成方式可以参见前文的描述。

25 在一些实施例中，代理节点可以向第一设备发送响应消息。该响应消息中包括以下信息中的一种或多种：A-KID、应用密钥的有效期、新选取的第一密钥、消息完整性校验码（message integrity check, MIC）。该响应消息可以通过密钥进行保护，如完整性保护和/或加密保护。该密钥可以包括以下中的一种或多种： K_{AF} 、 K_{ul} 、由 K_{AF} 衍生出的下级密钥、由 K_{ul} 衍生出的下级密钥。

30 第一设备与代理节点之间的共享密钥 $N1$ 可用于移动性管理。例如，第一设备和代理节点可以基于 $N1$ 和 K_{AF} 生成密钥 K_{ul} ，然后基于 K_{ul} 生成完整性保护密钥和/或加密密钥。之后，如果第一设备使用其他的设备（如 UEx）作为代理节点时，可以使用第一设备与 UEx 之间的共享密钥 N_x ，以及 K_{AF} ，生成下级密钥 K_{ux} 。该 K_{ux} 可用于进一步生成完整性保护密钥和/或加密密钥。这样，在代理节点发生变化时，第一设备不一定需要进行第一设备的认证与密钥协商流程，从而可以降低第一设备的复杂度。

当然，在一些实施例中，认证网元也可以按照前文描述的方式生成 XRES1、XRES2 和 XRES3，第一设备可以按照前文描述的方式生成 RES1、RES2 和 RES3。

示例四

35 示例四的方案中，安全凭证为非 3GPP 安全凭证，如安全凭证为第一设备与应用功能网元之间的共享密钥，第一设备直接与网络侧进行通信。

图 19 是本申请实施例提供的一种认证方法的流程示意图。参见图 19，在步骤 S1910，第一设备向应用功能网元发送认证请求。

40 该认证请求中可以包括以下信息中的一种或多种：第一设备的隐藏身份标识、第一设备的身份标识和第一密钥。在一些实施例中，认证请求中可以包括第一设备的隐藏身份标识。在另一些实施例中，认证请求中可以包括第一设备的身份标识和第一密钥。

在一些实施例中，隐藏身份标识可以基于第一密钥 $N1$ 生成。第一密钥可以为第一设备与应用功能网元之间的共享密钥。

45 在步骤 S1920，应用功能网元对第一设备进行授权检查。例如，应用功能网元可以检查第一设备是否被授权使用某种服务（如 A-IoT 服务）。

在一些实施例中，应用功能网元可以管理第一设备的白名单。

50 应用功能网元在对第一设备进行授权检查时，可以基于第一设备的身份标识 ID_i 对第一设备进行授权检查。在一些实施例中，认证请求中可以包括第一设备的隐藏身份标识 DID_i 。应用功能网元可以对隐藏身份标识 DID_i 进行解匿名，得到第一设备的身份标识。例如，应用功能网元可以利用第一密钥 $N1$ 对隐藏身份标识 DID_i 进行解匿名，得到第一设备的身份标识。举例说明，第一设备的身份标识 ID_i 可以通过公式 $ID_i = DID_i \oplus N1$ 或公式 $ID_i = f_{N1}(DID_i)$ 确定。

在步骤 S1930，在第一设备授权检查成功的情况下，应用功能网元向认证网元发送认证请求。

如果第一设备授权检查失败,则应用功能网元可以不向认证网元发送认证请求,即不进行后续的认证与密钥协商流程。

本申请实施例可以由应用功能网元先对第一设备进行授权检查,在授权检查成功的情况下,才进行后续的认证与密钥协商流程,有利于降低第一设备的计算复杂度。例如,如果在认证与密钥协商流程完成后,才进行授权检查,会出现授权检查失败的情况,这就会使得第一设备的认证与密钥协商流程无效,从而造成资源的浪费,不利于降低第一设备的计算复杂度。

在一些实施例中,应用功能网元可以向认证网元发送安全凭证 K,或者应用功能网元可以向认证网元发送安全凭证 K 的下级密钥(记为 Kb)。该下级密钥为基于安全凭证 K 生成的密钥。认证网元可以基于下级密钥,确定出安全凭证 K。

下级密钥例如可以基于安全凭证 K、第一密钥(记为 N1)和第一随机数(记为 N2)中的一个或多个生成。例如,下级密钥 Kb 可以基于公式 $Kb=K \oplus N1$ 或公式 $Kb=K \oplus N2$ 生成。其中, N2 可以是第一设备与 AF 之间的共享密钥,或者, N2 可以是 AF 选择的随机数。

如果认证网元接收的是安全凭证 K,则认证网元可以基于安全凭证 K 生成认证过程中所需要的参数。该参数例如可以为认证向量中包含的参数。该参数例如可以包括以下中的一种或多种:第一匿名密钥、第一消息认证码、期望响应、密钥 Ks 等。密钥 Ks 为第一设备与认证网元认证成功后,生成的共享密钥。这些参数的具体生成方式可以参见示例三的描述,为了简洁,此处不再赘述。

如果认证网元接收的是密钥 Kb,则认证网元可以基于密钥 Kb 生成认证过程中所需要的参数。该参数例如可以为认证向量中包含的参数。该参数例如可以包括以下中的一种或多种:第一消息认证码、期望响应、密钥 Ks 等。这些参数的具体生成方式可以参见示例三的描述,为了简洁,此处不再赘述。

在一些实施例中,第一设备可以采用与认证网元相同的方式,生成以下参数中的一种或多种:第一匿名密钥、第二消息认证码、响应参数、密钥 Ks 等。例如,第二消息认证码的生成方式与第一消息认证码的生成方式相同。又例如,响应参数的生成方式与期望响应的生成方式相同。

在一些实施例中,上述期望响应可以包括第一期望响应、第二期望响应和第三期望响应。第一期望响应的生成方式可以为上文中的期望响应的生成方式。第二期望响应和第三期望响应可以基于第一期望响应生成,具体的生成方式可以参见其他示例中的描述。

在一些实施例中,上述响应参数可以包括第一响应参数、第二响应参数和第三响应参数。第一响应参数的生成方式可以为上文中的响应参数的生成方式。第二响应参数和第三响应参数可以基于第一响应参数生成,具体的生成方式可以参见其他示例中的描述。

上述公式中的 f 可以为相同的密钥生成算法,或者上述公式中的 f 可以包括第一密钥生成算法和第二密钥生成算法。例如,第一密钥生成算法用于生成第一消息认证码或第二消息认证码,第二密钥生成算法用于生成期望响应或响应参数。

在得到 Ks 后,第一设备和认证网元可以基于 Ks 生成 A-TID、A-KID 以及 AKMA 密钥中的一种或多种。具体的生成方式可以参见前文中其他示例的描述。

由于应用功能网元参与了认证与密钥协商流程,则应用功能网元可以直接接收 AAnF 发送的应用密钥。例如, AAnF 可以在生成应用密钥后,直接向 AF 发送应用密钥,而不需要 AF 发送应用密钥请求来触发。

AF 接收到应用密钥后,可以向代理节点发送应用密钥。该应用密钥可用于代理节点生成第三密钥(如 Kul)。

AAnF 生成应用密钥的方式、以及代理节点生成第三密钥的方式可以参见前文的描述,此处不再赘述。

图 19 所示的方案中涉及的第一设备与网络侧之间的认证与密钥协商流程可以与前文中的方案类似,未详细描述的内容可以参见前文的描述,为了简洁,此处不再赘述。

下面结合图 20,对没有代理节点参与的认证与密钥协商流程进行详细介绍。在图 20 所示的方案中,第一设备可以与 AF 共享密钥 K。

参见图 20,在步骤 S2002,第一设备向 AF 发送认证请求。该认证请求中包括第一设备的隐藏身份标识 DIDi。隐藏身份标识 DIDi 可以基于第一设备的身份标识 IDi 生成。

如果 N1 是第一设备与 AF 之间预先共享的密钥(或随机数),则 DIDi 可以基于以下公式确定: $DIDi=IDi \oplus N1$ 。在建立第一设备的安全上下文之后,AF 可以向第一设备发送新的第一密钥以更新 DIDi。

在步骤 S2004,AF 可以进行授权管理。

在一些实施例中,如果 N1 为第一设备与 AF 之间的共享密钥,则 AF 可以根据 N1 解匿名得到第一设备的身份标识 IDi。例如, IDi 可以通过公式 $IDi=DIDi \oplus N1$ 或公式 $IDi=f_{N1}(DIDi)$ 确定。

在一些实施例中,AF 可以检查第一设备是否被授权。在一些实施例中,AF 还可以管理第一设备的

白名单。

在步骤 S2006, AF 向认证网元发送认证请求。该认证请求中可以包括安全凭证 K 或由安全凭证 K 衍生的下级密钥 Kb。在一些实施例中, 该认证请求中还可以包括 AF ID 和 IDi。

在一些实施例中, 该认证请求中可以包括以下中的一种或多种: K、K||N1、K||N1||N2 和 K||N2。其中, N1 可以是第一设备与代理节点之间的共享密钥, 或者 N1 可以是第一设备与 AF 之间的共享密钥。N2 可以是第一设备与 AF 之间的共享密钥, 或者 N2 可以是 AF 选择的随机数。

在一些实施例中, 该认证请求中可以包括以下中的一种或多种: Kb、Kb||N2、Kb||N1。

如果 Kb 基于 K 和 N1 生成, 则认证请求中可以包括 Kb||N2; 如果 Kb 基于 K 和 N2 生成, 则认证请求中可以包括 Kb||N1。

在一些实施例中, 该认证请求中可以包括可指示认证类型的标识。认证类型的标识可以通过以下中的一种或多种指示: AF ID、IDi 的类型、认证类型标识 (Auth_type_ID)。

在步骤 S2008, 第一设备与认证网元之间进行认证 (如 AKA 认证)。该认证方式可以参见前文的描述, 如参见前文图 11 的描述。

认证网元可以通过核心网网元 (如 UDM) 查询第一设备与代理节点的订阅凭证。核心网网元可以基于 IDi 和代理节点的标识检查第一设备与代理节点的订阅凭证, 以确定第一设备是否有权使用 A-IoT 服务。

认证网元可以基于可指示认证类型的标识判断认证类型, 如判断认证类型是否为 A-IoT 认证。

认证网元生成认证向量。认证网元可以选择随机数 RAND, 该随机数 RAND 可用于生成认证向量。

如果认证网元接收到的认证请求中包括 K、K||N1、K||N1||N2、K||N2 中的一个或多个, 则认证网元可以基于 K 和 RAND 生成认证参数。该认证参数包括以下中的一种或多种: 第一匿名密钥 AK、第一消息认证码 MAC、期望响应 XRES 和认证向量 AV。

第一匿名密钥 AK 可以通过公式 $AK=f_K(RAND)$ 或公式 $AK=K \oplus N1$ 确定。

第一消息认证码 MAC 可以基于公式 $MAC=f_K(RAND, N1, N2)$ 确定。

期望响应 XRES 可以基于公式 $XRES=f_K(RAND, N1, N2)$ 确定。

认证向量可以为 $AV=RAND||AK||MAC||XRES$ 。

MAC 与 XRES 计算时可以使用相同的函数 f 和不同的参数。或者, MAC 和 XRES 计算时可以使用相同的参数和不同的函数 f。

如果认证网元接收到的认证请求中包括 Kb、Kb||N1、Kb||N2 中的一个或多个, 则认证网元可以基于 Kb 和 RAND 生成认证参数。该认证参数包括以下中的一种或多种: 第一消息认证码 MAC、期望响应 XRES 和认证向量 AV。

第一消息认证码 MAC 可以基于以下公式中一种或多种确定: $MAC=f_{Kb}(RAND, N1, N2)$ 、 $MAC=f_{Kb}(RAND)$ 、 $MAC=f_{Kb}(RAND, N1)$ 、 $MAC=f_{Kb}(RAND, N2)$ 。

期望响应 XRES 可以基于以下公式中一种或多种确定: $XRES=f_{Kb}(RAND, N1, N2)$ 、 $XRES=f_{Kb}(RAND)$ 、 $XRES=f_{Kb}(RAND, N1)$ 、 $XRES=f_{Kb}(RAND, N2)$ 。

认证向量可以为 $AV=RAND||MAC||XRES$ 。

MAC 与 XRES 计算时可以使用相同的函数 f 和不同的参数。或者, MAC 和 XRES 计算时可以使用相同的参数和不同的函数 f。

在一些实施例中, 认证网元可以通过代理节点向第一设备发送认证响应。该认证响应中可以包括 RAND 和第一消息认证码。在一些实施例中, 如果 N2 是 AF 选择的随机数, 则认证响应中还可以包括 $AK \oplus N2$ 或者 $Kb \oplus N2$, 其中, AK 和 Kb 用于保护 N2, 以保证 N2 安全地传输。在一些实施例中, 认证响应中可以包括 AF ID 和 IDi。

第一设备可以计算第二消息认证码, 并比较第一消息认证码和第二消息认证码, 以认证认证网元。认证成功后, 第一设备可以生成密钥 Ks。密钥 Ks 可以基于以下公式中的一种或多种确定: $Ks=f_{AK}(N1, N2, IDi, UE\ ID, AF\ ID, SN\ name)$ 、 $Ks=f_{AK}(N1, N2, IDi, UE\ ID, AF\ ID, HNI)$ 、 $Ks=f_{Kb}(N1, N2, IDi, UE\ ID, AF\ ID, SN\ name)$ 、 $Ks=f_{Kb}(N1, N2, IDi, UE\ ID, AF\ ID, HNI)$ 。

在一些实施例中, 第一设备可以生成 A-TID。A-TID 可以基于公式 $A-TID=f_{Ks}(IDi)$ 确定。在一些实施例中, 第一设备可以生成 A-KID, A-KID 可以基于公式 $A-KID=A-TID||RID||HNI$ 确定。在一些实施例中, 第一设备可以生成 AKMA 密钥, AKMA 密钥可以基于公式 $K_{AKMA}=f_{Ks}("AKMA", "IDi")$ 确定。

在一些实施例中, 第一设备可以生成响应参数 RES, RES 的计算方式与 XRES 的计算方式相同。

第一设备可以通过代理节点向认证网元发送认证响应, 该认证响应可以包括响应参数 RES。认证网元可以比较 RES 和 XRES, 以认证第一设备。如果 RES 和 XRES 一致, 则第一设备认证成功; 如果 RES 和 XRES 不一致, 则第一设备认证失败。在第一设备认证成功后, 认证网元可以生成以下参数中的一种

或多种: K_s 、A-TID、A-KID 以及 AKMA 密钥。认证网元生成这些参数的方式与第一设备生成对应参数的方式相同。

在步骤 S2010, 认证网元向 AAnF 提供密钥材料, 该密钥材料可以包括 AKMA 密钥和 A-KID。

在步骤 S2012, AAnF 基于 AKMA 密钥生成应用密钥 K_{AF} 。应用密钥 K_{AF} 可以基于公式 $K_{AF}=f_{KAKMA}(AF\ ID, ID_i, UE\ ID)$ 确定。类似地, 第一设备基于 AKMA 密钥生成应用密钥 K_{AF} 。

在步骤 S2014, AAnF 向 AF 发送响应消息。该响应消息可以为成功响应消息。该响应消息中包括应用密钥和/或应用密钥的有效期。在一些实施例中, 响应消息中还可以包括新选取的第一密钥 (或随机数), 新的第一密钥可用于更新隐藏身份标识。

在步骤 S2016, AF 向第一设备发送响应消息。该响应消息中包括以下信息中的一种或多种: A-KID、应用密钥的有效期、新选取的第一密钥、消息完整性校验码 (message integrity check, MIC)。该响应消息可以通过密钥进行保护, 如完整性保护和/或加密保护。该密钥可以包括以下中的一种或多种: K_{AF} 、 K_{ul} 、由 K_{AF} 衍生出的下级密钥、由 K_{ul} 衍生出的下级密钥。

下文描述的方案对以上四个示例均适用。

在一些实施例中, 为了减少密钥的衍生次数, 认证网元可以将 K_s 发送至代理节点, 以使代理节点基于 K_s 保护传输在空中的信息。例如, 代理节点可以基于 K_s 生成完整性保护密钥和/或加密密钥, 该完整性保护密钥和/或加密密钥用于第一设备与代理节点之间的安全通信。

在一些实施例中, 为了减少密钥的衍生次数, 认证网元可以将 K_s 发送至 AF, AF 与第一设备可以基于 K_s 建立安全连接 (如安全传输层 (transport layer security, TLS) 连接), 以保护传输在空中的信息。

在一些实施例中, 对于有代理节点参与的方案, 在触发第一设备与网络侧之间的认证与密钥协商之前, 第一设备可以与代理节点之间进行相互认证, 以避免恶意的第一设备利用代理节点对网络发起分布式拒绝服务 (distributed denial of service, DDOS) 攻击, 影响网络质量, 或恶意的代理节点发起中间人攻击, 窃取第一设备与网络、第三方应用间的通信数据, 或者第一设备的认证信令搭载在恶意的代理节点上, 导致无法成功认证与密钥协商。

第一设备与代理节点之间的认证方式可以包括以下中的一种或多种: 配对、代理节点激活第一设备、物理不可克隆函数 (physical unclonable function, PUF) 和物理层认证。

在认证成功后, 代理节点可以使用自身的安全上下文, 保护第一设备的认证消息。例如, 代理节点在接收到第一设备的认证请求或响应消息后, 可以将第一设备的认证容器 (如 Tag_authentication_container) 使用第一设备的 NAS 安全上下文或 AS 安全上下文进行传输, 以与网络侧进行交互。

上文中的 AF 与认证网元之间的信息传输可以通过网络开放功能 (network exposure function, NEF) 来实现。例如, NEF 可以转发 AF 与认证网元之间的传输消息。

上文中的安全凭证也可以称为密钥或根密钥等。

上文描述的方案是基于应用密钥保护第一设备与代理节点之间的安全传输。在一些实施例中, 为了减少密钥的衍生次数, 可以直接使用密钥 K_s 保护第一设备与代理节点之间的安全传输。也就是说, 密钥 K_s 相当于密钥 K_{AF} 的功能。例如, 认证网元可以将密钥 K_s 发送至代理节点, 代理节点可以基于密钥 K_s 生成完整性保护密钥和/或加密密钥。类似地, 第一设备也可以基于密钥 K_s 生成完整性保护密钥和/或加密密钥。

在一些实施例中, 密钥 K_s 可用于生成 NAS 安全上下文和/或 AS 安全上下文。例如, 认证网元可以基于 K_s 生成 K_{AMF} , 并向 AMF 提供 K_{AMF} 。在该情况下, K_s 相当于 K_{AUSF} 的功能。AMF 可以基于 K_{AMF} 生成 NAS 安全上下文。又例如, 认证网元可以向 AMF 提供 K_s , 在该情况下, K_s 相当于 K_{AMF} 的功能。AMF 可以基于 K_s 生成 NAS 安全上下文。NAS 安全上下文例如可以包括 $K_{nas-int}$ 和 $K_{nas-enc}$ 。

又例如, 认证网元可以基于 K_s 生成 K_{gnb} , 并向基站提供 K_{gnb} 。在该情况下, K_s 相当于 K_{AUSF} 的功能。基站可以基于 K_{gnb} 生成 AS 安全上下文。又例如, 认证网元可以向基站提供 K_s , 在该情况下, K_s 相当于 K_{gnb} 的功能。基站可以基于 K_s 生成 AS 安全上下文。

在一些实施例中, 代理节点的中继方式可以包括 L2 中继和 L3 中继。即代理节点在用于中继通信时, 中继使用的协议栈可以属于 L2 层, 也可以属于 L3 层。对于 L2 中继, 第一设备与核心网之间有单独的上下文。第一设备与网络间存在逐跳 (hop by hop) 和端到端 (end-to-end) 的安全连接。对于 L3 中继, 第一设备只需要实现与代理节点之间的安全连接即可。

对于 L3 中继, 安全上下文可以包括第一设备与代理节点之间的安全上下文。对于 L2 中继, 安全上下文包括第一设备与代理节点之间的安全上下文、NAS 安全上下文和 AS 安全上下文。

上述公式中的函数 f 可以是 3GPP 定义的 fl-f5 中的任意一种函数。或者, 函数 f 可以为 KDF (如

HMAC-SHA256)。或者,函数f可以为其他轻量级函数(如ASCON)。

上文中的归属域网元或认证网元可以包括以下网元中的一种或多种:UDM、AUSF、KMS、ARPF。上文中的服务域网元可以包括以下中的一种或多种:AMF、SMF、SEAF、特定于A-IoT服务的核心网网元A-NF。

5 上文中的代理节点如果为终端设备,则代理节点的标识可以使用UE ID来表示。

上文中的第一密钥N1有三种用途:一是可用于保护第一设备的身份标识;二是可用于计算认证向量和哦共享密钥Ks;三是可用于移动性管理,即生成Kul。

需要说明的是,本申请实施例对产生的密钥的产生不做限定,可以为任意长度。密钥生成过程中可能引入编号FC、参数长度等值,本申请实施例对这些值的大小也不做具体限定。

10 上文结合图1至图20,详细描述了本申请的方法实施例,下面结合图21至图25,详细描述本申请的装置实施例。应理解,方法实施例的描述与装置实施例的描述相互对应,因此,未详细描述的部分可以参见前面方法实施例。

15 图21是本申请实施例提供的一种第一设备的示意性框图。图21所示的第一设备2100可以为上文描述的任意一种第一设备。该第一设备2100可以包括接收单元2110、生成单元2120、认证单元2130和发送单元2140。下面对这些单元进行详细介绍。

接收单元2110,用于接收来自代理节点的第一认证请求,所述第一认证请求中包括第一消息认证码,所述第一消息认证码由认证网元生成。

生成单元2120,用于基于第一密钥生成算法和第一参数生成第二消息认证码。

认证单元2130,用于基于所述第一消息认证码和所述第二消息认证码认证所述认证网元。

20 生成单元2120,还用于在所述认证网元认证成功的情况下,所述第一设备生成响应参数。

发送单元2140,用于向所述代理节点发送第一认证响应,所述第一认证响应中包括所述响应参数,所述响应参数用于认证所述第一设备。

25 在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述生成单元用于:基于所述第一密钥生成算法和第二参数生成所述第一响应参数。

在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述生成单元用于:基于第二密钥生成算法和所述第一参数生成所述第一响应参数。

在一些实现方式中,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述生成单元用于:基于所述第一响应参数和第三参数,生成所述第二响应参数。

30 在一些实现方式中,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述生成单元用于:基于所述第一响应参数和第四参数,生成所述第三响应参数。

在一些实现方式中,所述生成单元还用于:在接收来自代理节点的第一认证请求之前,对所述第一设备的身份标识以及第一密钥进行异或运算,生成所述第一设备的隐藏身份标识;所述发送单元还用于:向所述代理节点发送第二认证请求,所述第二认证请求中包括所述隐藏身份标识。

35 在一些实现方式中,所述生成单元还用于:在接收来自代理节点的第一认证请求之前,基于所述第一设备的身份标识、第一密钥以及第三密钥生成算法,生成所述第一设备的隐藏身份标识,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法;所述发送单元还用于:向所述代理节点发送第二认证请求,所述第二认证请求中包括所述隐藏身份标识。

40 在一些实现方式中,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

在一些实现方式中,所述生成单元还用于:在所述认证网元认证成功的情况下,生成第二密钥;基于所述第二密钥和第四密钥生成算法,生成应用层的认证和密钥管理密钥。

45 在一些实现方式中,所述发送单元还用于:向所述代理节点发送应用会话建立请求消息;所述接收单元还用于:接收来自所述代理节点的应用会话建立响应消息;所述生成单元还用于:响应于接收到所述应用会话建立响应消息,基于所述应用层的认证和密钥管理密钥,生成应用密钥;以及基于所述应用密钥、第一密钥以及第五密钥生成算法,生成第三密钥,所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥,所述第五密钥生成算法为所述第一密钥生成算法或第二密钥生成算法;所述设备还包括通信单元,用于基于所述第三密钥,与所述代理节点进行安全通信。

50 图22是本申请实施例提供的一种代理节点的示意性框图。图22所示的代理节点2200可以为上文描述的任意一种代理节点。该代理节点2200可以包括发送单元2210和接收单元2220。下面对这些单元进行详细介绍。

发送单元2210,用于向第一设备发送第一认证请求,所述第一认证请求中包括第一消息认证码,

所述第一消息认证码由认证网元生成,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成,所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成。

接收单元 2220,用于接收来自所述第一设备的第一认证响应,所述第一认证响应中包括响应参数,所述响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

在一些实现方式中,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述第二响应参数基于所述第一响应参数和第三参数生成。

在一些实现方式中,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述第三响应参数基于所述第一响应参数和第四参数生成。

在一些实现方式中,所述接收单元还用于:在向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

在一些实现方式中,所述接收单元还用于:在向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

在一些实现方式中,所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥,所述代理节点还包括确定单元,用于基于所述第一密钥和所述隐藏身份标识,确定所述第一设备的身份标识;所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述第一密钥、所述第一设备的身份标识和所述代理节点的标识。

在一些实现方式中,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述隐藏身份标识和所述代理节点的标识。

在一些实现方式中,所述接收单元还用于:接收来自应用功能网元的应用密钥;所述代理节点还包括:生成单元,用于基于所述应用密钥、第一密钥以及第五密钥生成算法,生成第三密钥,所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥,所述第五密钥生成算法为所述第一密钥生成算法或第二密钥生成算法;通信单元,用于基于所述第三密钥,与所述第一设备进行安全通信。

图 23 是本申请实施例提供的一种认证网元的示意性框图。图 23 所示的认证网元 2300 可以为上文描述的任意一种认证网元。该认证网元 2300 可以包括生成单元 2310 和发送单元 2320。下面对这些单元进行详细介绍。

生成单元 2310,用于生成第一消息认证码和期望响应,所述期望响应用于认证第一设备,所述第一消息认证码基于第一密钥生成算法和第一参数生成。

发送单元 2320,用于向所述代理节点发送第一认证请求,所述第一认证请求中包括所述第一消息认证码,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成。

在一些实现方式中,所述期望响应包括第一期望响应,所述第一期望响应用于归属域网元认证所述第一设备,所述生成单元用于:基于所述第一密钥生成算法和第二参数生成所述第一期望响应。

在一些实现方式中,所述期望响应包括第一期望响应,所述第一期望响应用于归属域网元认证所述第一设备,所述生成单元用于:基于第二密钥生成算法和所述第一参数生成所述第一期望响应。

在一些实现方式中,所述期望响应包括第二期望响应,所述第二期望响应用于服务域网元认证所述第一设备,所述生成单元用于:基于所述第一期望响应和第三参数,生成所述第二期望响应。

在一些实现方式中,所述期望响应包括第三期望响应,所述第三期望响应用于接入网设备认证所述第一设备,所述生成单元用于:基于所述第一期望响应和第四参数,生成所述第三期望响应。

在一些实现方式中,所述认证网元还包括:接收单元,用于:在所述认证网元生成第一消息认证码和期望响应之前,接收来自所述代理节点的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,确定单元,用于基于所述隐藏身份标识与第一密钥,确定所述第一设备的身份标识。

在一些实现方式中,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

在一些实现方式中,所述生成单元用于:在所述第一设备认证成功的情况下,生成第二密钥;基于所述第二密钥和第四密钥生成算法,生成应用层的认证和密钥管理密钥。

在一些实现方式中,所述第一参数包括第一随机数,所述第一随机数由所述认证网元选择,或所述第一随机数由所述认证网元与所述第一设备预共享。

图 24 是本申请实施例提供的一种接入网设备的示意性框图。图 24 所示的接入网设备 2400 可以为上文描述的任意一种接入网设备。该接入网设备 2400 可以包括发送单元 2410 和接收单元 2420。下面对这些单元进行详细介绍。

发送单元 2410,用于向第一设备发送第一认证请求,所述第一认证请求中包括第一消息认证码,所述第一消息认证码由认证网元生成,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成,所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成。

接收单元 2420,用于接收来自所述第一设备的第一认证响应,所述第一认证响应中包括响应参数,所述响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

在一些实现方式中,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

在一些实现方式中,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述第二响应参数基于所述第一响应参数和第三参数生成。

在一些实现方式中,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述第三响应参数基于所述第一响应参数和第四参数生成。

在一些实现方式中,所述接收单元还用于:在所述接入网设备向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

在一些实现方式中,所述接收单元还用于:在所述接入网设备向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

在一些实现方式中,所述第一密钥为所述第一设备与所述接入网设备之间的物理层密钥,所述接入网设备还包括确定单元,用于基于所述第一密钥和所述隐藏身份标识,确定所述第一设备的身份标识;所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述第一密钥和所述第一设备的身份标识。

在一些实现方式中,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括所述隐藏身份标识。

在一些实现方式中,所述第一认证响应中包括第三响应参数,所述接收单元还用于:接收来自所述认证网元的第二认证响应,所述第二认证响应中包括第三期望响应;所述接入网设备还包括:比较单元,用于比较所述第三响应参数和所述第三认证响应,以认证所述第一设备。

图 25 是本申请实施例的通信装置的示意性结构图。图 25 中的虚线表示该单元或模块为可选的。该装置 2500 可用于实现上述方法实施例中描述的方法。装置 2500 可以是芯片、第一设备、代理节点、认证网元、接入网设备或应用功能网元。

装置 2500 可以包括一个或多个处理器 2510。该处理器 2510 可支持装置 2500 实现前文方法实施例所描述的方法。该处理器 2510 可以是通用处理器或者专用处理器。例如,该处理器可以为中央处理单元 (central processing unit, CPU)。或者,该处理器还可以是其他通用处理器、数字信号处理器 (digital signal processor, DSP)、专用集成电路 (application specific integrated circuit, ASIC)、现成可编程门阵列 (field programmable gate array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

装置 2500 还可以包括一个或多个存储器 2520。存储器 2520 上存储有程序,该程序可以被处理器 2510 执行,使得处理器 2510 执行前文方法实施例所描述的方法。存储器 2520 可以独立于处理器 2510 也可以集成在处理器 2510 中。

装置 2500 还可以包括收发器 2530。处理器 2510 可以通过收发器 2530 与其他设备或芯片进行通信。例如,处理器 2510 可以通过收发器 2530 与其他设备或芯片进行数据收发。

本申请实施例还提供一种计算机可读存储介质,用于存储程序。该计算机可读存储介质可应用于本

申请实施例提供的第一设备、代理节点、认证网元、接入网设备或应用功能网元中，并且该程序使得计算机执行本申请各个实施例中的由第一设备、代理节点、认证网元、接入网设备或应用功能网元执行的方法。

5 本申请实施例还提供一种计算机程序产品。该计算机程序产品包括程序。该计算机程序产品可应用于本申请实施例提供的第一设备、代理节点、认证网元、接入网设备或应用功能网元中，并且该程序使得计算机执行本申请各个实施例中的由第一设备、代理节点、认证网元、接入网设备或应用功能网元执行的方法。

10 本申请实施例还提供一种计算机程序。该计算机程序可应用于本申请实施例提供的第一设备、代理节点、认证网元、接入网设备或应用功能网元中，并且该计算机程序使得计算机执行本申请各个实施例中的由第一设备、代理节点、认证网元、接入网设备或应用功能网元执行的方法。

应理解，本申请使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。

15 在本申请的实施例中，提到的“包括”可以指直接包括，也可以指间接包括。可选地，可以将本申请实施例中提到的“包括”替换为“指示”或“用于确定”。例如，A 包括 B，可以替换为 A 指示 B，或 A 用于确定 B。

在本申请实施例中，术语“对应”可表示两者之间具有直接对应或间接对应的关系，也可以表示两者之间具有关联关系，也可以是指示与被指示、配置与被配置等关系。

20 本申请实施例中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

在本申请的各种实施例中，上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，而不对本申请实施例的实施过程构成任何限定。

25 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种认证方法，其特征在于，包括：

第一设备接收来自代理节点的第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成；

5 所述第一设备基于第一密钥生成算法和第一参数生成第二消息认证码；

所述第一设备基于所述第一消息认证码和所述第二消息认证码认证所述认证网元；

在所述认证网元认证成功的情况下，所述第一设备生成响应参数；

所述第一设备向所述代理节点发送第一认证响应，所述第一认证响应中包括所述响应参数，所述响应参数用于认证所述第一设备。

10 2、根据权利要求1所述的方法，其特征在于，所述响应参数包括第一响应参数，所述第一响应参数用于归属域网元认证所述第一设备，所述第一设备生成响应参数，包括：

所述第一设备基于所述第一密钥生成算法和第二参数生成所述第一响应参数。

3、根据权利要求1所述的方法，其特征在于，所述响应参数包括第一响应参数，所述第一响应参数用于归属域网元认证所述第一设备，所述第一设备生成响应参数，包括：

15 所述第一设备基于第二密钥生成算法和所述第一参数生成所述第一响应参数。

4、根据权利要求2或3所述的方法，其特征在于，所述响应参数包括第二响应参数，所述第二响应参数用于服务域网元认证所述第一设备，所述第一设备生成响应参数，包括：

所述第一设备基于所述第一响应参数和第三参数，生成所述第二响应参数。

20 5、根据权利要求2-4中任一项所述的方法，其特征在于，所述响应参数包括第三响应参数，所述第三响应参数用于接入网设备认证所述第一设备，所述第一设备生成响应参数，包括：

所述第一设备基于所述第一响应参数和第四参数，生成所述第三响应参数。

6、根据权利要求1-5中任一项所述的方法，其特征在于，在所述第一设备接收来自代理节点的第一认证请求之前，所述方法还包括：

25 所述第一设备对所述第一设备的身份标识以及第一密钥进行异或运算，生成所述第一设备的隐藏身份标识；

所述第一设备向所述代理节点发送第二认证请求，所述第二认证请求中包括所述隐藏身份标识。

7、根据权利要求1所述的方法，其特征在于，在所述第一设备接收来自代理节点的第一认证请求之前，所述方法还包括：

30 所述第一设备基于所述第一设备的身份标识、第一密钥以及第三密钥生成算法，生成所述第一设备的隐藏身份标识，所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法；

所述第一设备向所述代理节点发送第二认证请求，所述第二认证请求中包括所述隐藏身份标识。

8、根据权利要求6或7所述的方法，其特征在于，所述第一密钥为所述第一设备与所述认证网元之间的共享密钥，或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

9、根据权利要求1-8中任一项所述的方法，其特征在于，所述方法还包括：

35 在所述认证网元认证成功的情况下，所述第一设备生成第二密钥；

所述第一设备基于所述第二密钥和第四密钥生成算法，生成应用层的认证和密钥管理密钥。

10、根据权利要求9所述的方法，其特征在于，所述方法还包括：

所述第一设备向所述代理节点发送应用会话建立请求消息；

所述第一设备接收来自所述代理节点的应用会话建立响应消息；

40 响应于接收到所述应用会话建立响应消息，所述第一设备基于所述应用层的认证和密钥管理密钥，生成应用密钥；

所述第一设备基于所述应用密钥、第一密钥以及第五密钥生成算法，生成第三密钥，所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥，所述第五密钥生成算法为所述第一密钥生成算法或第二密钥生成算法；

45 所述第一设备基于所述第三密钥，与所述代理节点进行安全通信。

11、一种认证方法，其特征在于，包括：

代理节点向第一设备发送第一认证请求，所述第一认证请求中包括第一消息认证码，所述第一消息认证码由认证网元生成，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成，所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成；

50 所述代理节点接收来自所述第一设备的第一认证响应，所述第一认证响应中包括响应参数，所述响应参数用于认证所述第一设备，所述响应参数在所述认证网元认证成功的情况下生成。

12、根据权利要求 11 所述的方法，其特征在于，所述响应参数包括第一响应参数，所述第一响应参数用于归属域网元认证所述第一设备，所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

5 13、根据权利要求 11 所述的方法，其特征在于，所述响应参数包括第一响应参数，所述第一响应参数用于归属域网元认证所述第一设备，所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

14、根据权利要求 12 或 13 所述的方法，其特征在于，所述响应参数包括第二响应参数，所述第二响应参数用于服务域网元认证所述第一设备，所述第二响应参数基于所述第一响应参数和第三参数生成。

10 15、根据权利要求 12-14 中任一项所述的方法，其特征在于，所述响应参数包括第三响应参数，所述第三响应参数用于接入网设备认证所述第一设备，所述第三响应参数基于所述第一响应参数和第四参数生成。

16、根据权利要求 11-15 中任一项所述的方法，其特征在于，在所述代理节点向第一设备发送第一认证请求之前，所述方法还包括：

15 所述代理节点接收来自所述第一设备的第二认证请求，所述第二认证请求中包括所述第一设备的隐藏身份标识，所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

17、根据权利要求 11-15 中任一项所述的方法，其特征在于，在所述代理节点向第一设备发送第一认证请求之前，所述方法还包括：

20 所述代理节点接收来自所述第一设备的第二认证请求，所述第二认证请求中包括所述第一设备的隐藏身份标识，所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成，所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

18、根据权利要求 16 或 17 所述的方法，其特征在于，所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥，所述方法还包括：

所述代理节点基于所述第一密钥和所述隐藏身份标识，确定所述第一设备的身份标识；

25 所述代理节点向所述认证网元发送所述第二认证请求，所述第二认证请求中包括以下信息中的一种或多种：所述第一密钥、所述第一设备的身份标识和所述代理节点的标识。

19、根据权利要求 16 或 17 所述的方法，其特征在于，所述第一密钥为所述第一设备与所述认证网元之间的共享密钥，所述方法还包括：

30 所述代理节点向所述认证网元发送所述第二认证请求，所述第二认证请求中包括以下信息中的一种或多种：所述隐藏身份标识和所述代理节点的标识。

20、根据权利要求 11-19 中任一项所述的方法，其特征在于，所述方法还包括：

所述代理节点接收来自应用功能网元的应用密钥；

35 所述代理节点基于所述应用密钥、第一密钥以及第五密钥生成算法，生成第三密钥，所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥，所述第五密钥生成算法为所述第一密钥生成算法或第二密钥生成算法；

所述代理节点基于所述第三密钥，与所述第一设备进行安全通信。

21、一种认证方法，其特征在于，包括：

认证网元生成第一消息认证码和期望响应，所述期望响应用于认证第一设备，所述第一消息认证码基于第一密钥生成算法和第一参数生成；

40 所述认证网元向所述代理节点发送第一认证请求，所述第一认证请求中包括所述第一消息认证码，所述第一消息认证码和第二消息认证码用于认证所述认证网元，所述第二消息认证码由所述第一设备生成。

22、根据权利要求 21 所述的方法，其特征在于，所述期望响应包括第一期望响应，所述第一期望响应用于归属域网元认证所述第一设备，所述认证网元生成期望响应，包括：

45 所述认证网元基于所述第一密钥生成算法和第二参数生成所述第一期望响应。

23、根据权利要求 21 所述的方法，其特征在于，所述期望响应包括第一期望响应，所述第一期望响应用于归属域网元认证所述第一设备，所述认证网元生成期望响应，包括：

所述认证网元基于第二密钥生成算法和所述第一参数生成所述第一期望响应。

50 24、根据权利要求 22 或 23 所述的方法，其特征在于，所述期望响应包括第二期望响应，所述第二期望响应用于服务域网元认证所述第一设备，所述方法还包括：

所述认证网元基于所述第一期望响应和第三参数，生成所述第二期望响应。

25、根据权利要求 22-24 中任一项所述的方法，其特征在于，所述期望响应包括第三期望响应，所

述第三期望响应用于接入网设备认证所述第一设备,所述方法还包括:

所述认证网元基于所述第一期望响应和第四参数,生成所述第三期望响应。

26、根据权利要求 21-25 中任一项所述的方法,其特征在于,在所述认证网元生成第一消息认证码和期望响应之前,所述方法还包括:

5 所述认证网元接收来自所述代理节点的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,

所述认证网元基于所述隐藏身份标识与第一密钥,确定所述第一设备的身份标识。

27、根据权利要求 26 所述的方法,其特征在于,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

10 28、根据权利要求 21-27 中任一项所述的方法,其特征在于,所述方法还包括:

在所述第一设备认证成功的情况下,所述认证网元生成第二密钥;

所述认证网元基于所述第二密钥和第四密钥生成算法,生成应用层的认证和密钥管理密钥。

29、根据权利要求 21-28 中任一项所述的方法,其特征在于,所述第一参数包括第一随机数,所述第一随机数由所述认证网元选择,或所述第一随机数由所述认证网元与所述第一设备预共享。

15 30、一种认证方法,其特征在于,包括:

接入网设备向第一设备发送第一认证请求,所述第一认证请求中包括第一消息认证码,所述第一消息认证码由认证网元生成,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成,所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成;

20 所述接入网设备接收来自所述第一设备的第一认证响应,所述第一认证响应中包括响应参数,所述响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

31、根据权利要求 30 所述的方法,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

25 32、根据权利要求 30 所述的方法,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

33、根据权利要求 31 或 32 所述的方法,其特征在于,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述第二响应参数基于所述第一响应参数和第三参数生成。

30 34、根据权利要求 31-33 中任一项所述的方法,其特征在于,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述第三响应参数基于所述第一响应参数和第四参数生成。

35、根据权利要求 30-34 中任一项所述的方法,其特征在于,在所述接入网设备向第一设备发送第一认证请求之前,所述方法还包括:

所述接入网设备接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

36、根据权利要求 30-34 中任一项所述的方法,其特征在于,在所述接入网设备向第一设备发送第一认证请求之前,所述方法还包括:

40 所述接入网设备接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

37、根据权利要求 35 或 36 所述的方法,其特征在于,所述第一密钥为所述第一设备与所述接入网设备之间的物理层密钥,所述方法还包括:

45 所述接入网设备基于所述第一密钥和所述隐藏身份标识,确定所述第一设备的身份标识;

所述接入网设备向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述第一密钥和所述第一设备的身份标识。

38、根据权利要求 35 或 36 所述的方法,其特征在于,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,所述方法还包括:

50 所述接入网设备向所述认证网元发送所述第二认证请求,所述第二认证请求中包括所述隐藏身份标识。

39、根据权利要求 30-38 中任一项所述的方法,其特征在于,所述第一认证响应中包括第三响应参

数, 所述方法还包括:

所述接入网设备接收来自所述认证网元的第二认证响应, 所述第二认证响应中包括第三期望响应;
所述接入网设备比较所述第三响应参数和所述第三认证响应, 以认证所述第一设备。

40、一种设备, 其特征在于, 所述设备为第一设备, 所述第一设备包括:

5 接收单元, 用于接收来自代理节点的第一认证请求, 所述第一认证请求中包括第一消息认证码, 所述
第一消息认证码由认证网元生成;

生成单元, 用于基于第一密钥生成算法和第一参数生成第二消息认证码;

认证单元, 用于基于所述第一消息认证码和所述第二消息认证码认证所述认证网元;

所述生成单元, 还用于在所述认证网元认证成功的情况下, 所述第一设备生成响应参数;

10 发送单元, 用于向所述代理节点发送第一认证响应, 所述第一认证响应中包括所述响应参数, 所述
响应参数用于认证所述第一设备。

41、根据权利要求 40 所述的设备, 其特征在于, 所述响应参数包括第一响应参数, 所述第一响应
参数用于归属域网元认证所述第一设备, 所述生成单元用于:

基于所述第一密钥生成算法和第二参数生成所述第一响应参数。

15 42、根据权利要求 40 所述的设备, 其特征在于, 所述响应参数包括第一响应参数, 所述第一响应
参数用于归属域网元认证所述第一设备, 所述生成单元用于:

基于第二密钥生成算法和所述第一参数生成所述第一响应参数。

43、根据权利要求 41 或 42 所述的设备, 其特征在于, 所述响应参数包括第二响应参数, 所述第二
响应参数用于服务域网元认证所述第一设备, 所述生成单元用于:

20 基于所述第一响应参数和第三参数, 生成所述第二响应参数。

44、根据权利要求 41-43 中任一项所述的设备, 其特征在于, 所述响应参数包括第三响应参数, 所
述第三响应参数用于接入网设备认证所述第一设备, 所述生成单元用于:

基于所述第一响应参数和第四参数, 生成所述第三响应参数。

45、根据权利要求 40-44 中任一项所述的设备, 其特征在于, 所述生成单元还用于: 在接收来自代
25 理节点的第一认证请求之前, 对所述第一设备的身份标识以及第一密钥进行异或运算, 生成所述第一设
备的隐藏身份标识;

所述发送单元还用于: 向所述代理节点发送第二认证请求, 所述第二认证请求中包括所述隐藏身份
标识。

46、根据权利要求 40 所述的设备, 其特征在于, 所述生成单元还用于: 在接收来自代理节点的第
30 一认证请求之前, 基于所述第一设备的身份标识、第一密钥以及第三密钥生成算法, 生成所述第一设备
的隐藏身份标识, 所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法;

所述发送单元还用于: 向所述代理节点发送第二认证请求, 所述第二认证请求中包括所述隐藏身份
标识。

47、根据权利要求 45 或 46 所述的设备, 其特征在于, 所述第一密钥为所述第一设备与所述认证网
35 元之间的共享密钥, 或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

48、根据权利要求 40-47 中任一项所述的设备, 其特征在于, 所述生成单元还用于:

在所述认证网元认证成功的情况下, 生成第二密钥;

基于所述第二密钥和第四密钥生成算法, 生成应用层的认证和密钥管理密钥。

49、根据权利要求 48 所述的设备, 其特征在于,

40 所述发送单元还用于: 向所述代理节点发送应用会话建立请求消息;

所述接收单元还用于: 接收来自所述代理节点的应用会话建立响应消息;

所述生成单元还用于: 响应于接收到所述应用会话建立响应消息, 基于所述应用层的认证和密钥管
理密钥, 生成应用密钥; 以及基于所述应用密钥、第一密钥以及第五密钥生成算法, 生成第三密钥, 所
述第一密钥为所述第一设备与所述代理节点之间的物理层密钥, 所述第五密钥生成算法为所述第一密
45 钥生成算法或第二密钥生成算法;

所述设备还包括通信单元, 用于基于所述第三密钥, 与所述代理节点进行安全通信。

50、一种代理节点, 其特征在于, 包括:

发送单元, 用于向第一设备发送第一认证请求, 所述第一认证请求中包括第一消息认证码, 所述第
一消息认证码由认证网元生成, 所述第一消息认证码和第二消息认证码用于认证所述认证网元, 所述第
50 二消息认证码由所述第一设备生成, 所述第一消息认证码和所述第二消息认证码基于第一密钥生成算
法和第一参数生成;

接收单元, 用于接收来自所述第一设备的第一认证响应, 所述第一认证响应中包括响应参数, 所述

响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

51、根据权利要求 50 所述的代理节点,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

5 52、根据权利要求 50 所述的代理节点,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

10 53、根据权利要求 51 或 52 所述的代理节点,其特征在于,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述第二响应参数基于所述第一响应参数和第三参数生成。

54、根据权利要求 51-53 中任一项所述的代理节点,其特征在于,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述第三响应参数基于所述第一响应参数和第四参数生成。

15 55、根据权利要求 50-54 中任一项所述的代理节点,其特征在于,
所述接收单元还用于:在向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

20 56、根据权利要求 50-54 中任一项所述的代理节点,其特征在于,
所述接收单元还用于:在向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

25 57、根据权利要求 55 或 56 所述的代理节点,其特征在于,所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥,所述代理节点还包括确定单元,用于基于所述第一密钥和所述隐藏身份标识,确定所述第一设备的身份标识;

所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述第一密钥、所述第一设备的身份标识和所述代理节点的标识。

30 58、根据权利要求 55 或 56 所述的代理节点,其特征在于,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,

所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述隐藏身份标识和所述代理节点的标识。

59、根据权利要求 50-58 中任一项所述的代理节点,其特征在于,所述接收单元还用于:接收来自应用功能网元的应用密钥;

所述代理节点还包括:

35 生成单元,用于基于所述应用密钥、第一密钥以及第五密钥生成算法,生成第三密钥,所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥,所述第五密钥生成算法为所述第一密钥生成算法或第二密钥生成算法;

通信单元,用于基于所述第三密钥,与所述第一设备进行安全通信。

60、一种认证网元,其特征在于,包括:

40 生成单元,用于生成第一消息认证码和期望响应,所述期望响应用于认证第一设备,所述第一消息认证码基于第一密钥生成算法和第一参数生成;

发送单元,用于向所述代理节点发送第一认证请求,所述第一认证请求中包括所述第一消息认证码,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成。

45 61、根据权利要求 60 所述的认证网元,其特征在于,所述期望响应包括第一期望响应,所述第一期望响应用于归属域网元认证所述第一设备,所述生成单元用于:

基于所述第一密钥生成算法和第二参数生成所述第一期望响应。

62、根据权利要求 60 所述的认证网元,其特征在于,所述期望响应包括第一期望响应,所述第一期望响应用于归属域网元认证所述第一设备,所述生成单元用于:

50 基于第二密钥生成算法和所述第一参数生成所述第一期望响应。

63、根据权利要求 61 或 62 所述的认证网元,其特征在于,所述期望响应包括第二期望响应,所述第二期望响应用于服务域网元认证所述第一设备,所述生成单元用于:

基于所述第一期望响应和第三参数,生成所述第二期望响应。

64、根据权利要求 61-63 中任一项所述的认证网元,其特征在于,所述期望响应包括第三期望响应,所述第三期望响应用于接入网设备认证所述第一设备,所述生成单元用于:

基于所述第一期望响应和第四参数,生成所述第三期望响应。

5 65、根据权利要求 60-64 中任一项所述的认证网元,其特征在于,所述认证网元还包括:

接收单元,用于:在所述认证网元生成第一消息认证码和期望响应之前,接收来自所述代理节点的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,

确定单元,用于基于所述隐藏身份标识与第一密钥,确定所述第一设备的身份标识。

10 66、根据权利要求 65 所述的认证网元,其特征在于,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,或所述第一密钥为所述第一设备与所述代理节点之间的物理层密钥。

67、根据权利要求 60-66 中任一项所述的认证网元,其特征在于,所述生成单元用于:

在所述第一设备认证成功的情况下,生成第二密钥;

基于所述第二密钥和第四密钥生成算法,生成应用层的认证和密钥管理密钥。

15 68、根据权利要求 60-67 中任一项所述的认证网元,其特征在于,所述第一参数包括第一随机数,所述第一随机数由所述认证网元选择,或所述第一随机数由所述认证网元与所述第一设备预共享。

69、一种接入网设备,其特征在于,包括:

20 发送单元,用于向第一设备发送第一认证请求,所述第一认证请求中包括第一消息认证码,所述第一消息认证码由认证网元生成,所述第一消息认证码和第二消息认证码用于认证所述认证网元,所述第二消息认证码由所述第一设备生成,所述第一消息认证码和所述第二消息认证码基于第一密钥生成算法和第一参数生成;

接收单元,用于接收来自所述第一设备的第一认证响应,所述第一认证响应中包括响应参数,所述响应参数用于认证所述第一设备,所述响应参数在所述认证网元认证成功的情况下生成。

25 70、根据权利要求 69 所述的接入网设备,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于所述第一密钥生成算法和第二参数生成。

71、根据权利要求 69 所述的接入网设备,其特征在于,所述响应参数包括第一响应参数,所述第一响应参数用于归属域网元认证所述第一设备,所述第一响应参数基于第二密钥生成算法和所述第一参数生成。

30 72、根据权利要求 70 或 71 所述的接入网设备,其特征在于,所述响应参数包括第二响应参数,所述第二响应参数用于服务域网元认证所述第一设备,所述第二响应参数基于所述第一响应参数和第三参数生成。

73、根据权利要求 70-72 中任一项所述的接入网设备,其特征在于,所述响应参数包括第三响应参数,所述第三响应参数用于接入网设备认证所述第一设备,所述第三响应参数基于所述第一响应参数和第四参数生成。

35 74、根据权利要求 69-73 中任一项所述的接入网设备,其特征在于,所述接收单元还用于:

在所述接入网设备向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的身份标识与第一密钥通过异或运算生成。

75、根据权利要求 69-73 中任一项所述的接入网设备,其特征在于,所述接收单元还用于:

40 在所述接入网设备向第一设备发送第一认证请求之前,接收来自所述第一设备的第二认证请求,所述第二认证请求中包括所述第一设备的隐藏身份标识,所述隐藏身份标识由所述第一设备的隐藏身份标识、第一密钥以及第三密钥生成算法生成,所述第三密钥生成算法为所述第一密钥生成算法或第二密钥生成算法。

45 76、根据权利要求 74 或 75 所述的接入网设备,其特征在于,所述第一密钥为所述第一设备与所述接入网设备之间的物理层密钥,所述接入网设备还包括确定单元,用于基于所述第一密钥和所述隐藏身份标识,确定所述第一设备的身份标识;

所述发送单元还用于:向所述认证网元发送所述第二认证请求,所述第二认证请求中包括以下信息中的一种或多种:所述第一密钥和所述第一设备的身份标识。

50 77、根据权利要求 74 或 75 所述的接入网设备,其特征在于,所述第一密钥为所述第一设备与所述认证网元之间的共享密钥,所述发送单元还用于:

向所述认证网元发送所述第二认证请求,所述第二认证请求中包括所述隐藏身份标识。

78、根据权利要求 69-77 中任一项所述的接入网设备,其特征在于,所述第一认证响应中包括第三

响应参数，所述接收单元还用于：接收来自所述认证网元的第二认证响应，所述第二认证响应中包括第三期望响应；

所述接入网设备还包括：比较单元，用于比较所述第三响应参数和所述第三认证响应，以认证所述第一设备。

5 79、一种设备，其特征在于，所述设备为第一设备，所述第一设备包括存储器和处理器，所述存储器用于存储程序，所述处理器用于调用所述存储器中的程序，以使所述第一设备执行如权利要求 1-10 中任一项所述的方法。

80、一种代理节点，其特征在于，包括存储器和处理器，所述存储器用于存储程序，所述处理器用于调用所述存储器中的程序，以使所述代理节点执行如权利要求 11-20 中任一项所述的方法。

10 81、一种认证网元，其特征在于，包括存储器和处理器，所述存储器用于存储程序，所述处理器用于调用所述存储器中的程序，以使所述认证网元执行如权利要求 21-29 中任一项所述的方法。

82、一种接入网设备，其特征在于，包括存储器和处理器，所述存储器用于存储程序，所述处理器用于调用所述存储器中的程序，以使所述接入网设备执行如权利要求 30-39 中任一项所述的方法。

15 83、一种装置，其特征在于，包括处理器，用于从存储器中调用程序，以执行如权利要求 1-10 中任一项所述的方法。

84、一种装置，其特征在于，包括处理器，用于从存储器中调用程序，以执行如权利要求 11-20 中任一项所述的方法。

85、一种装置，其特征在于，包括处理器，用于从存储器中调用程序，以执行如权利要求 21-29 中任一项所述的方法。

20 86、一种装置，其特征在于，包括处理器，用于从存储器中调用程序，以执行如权利要求 30-39 中任一项所述的方法。

87、一种芯片，其特征在于，包括处理器，用于从存储器调用程序，使得安装有所述芯片的设备执行如权利要求 1-10 中任一项所述的方法。

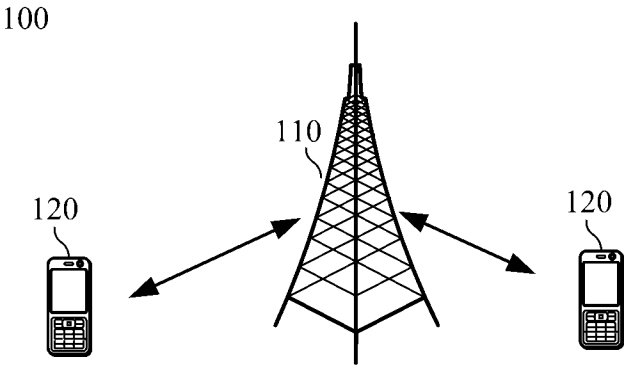


图 1

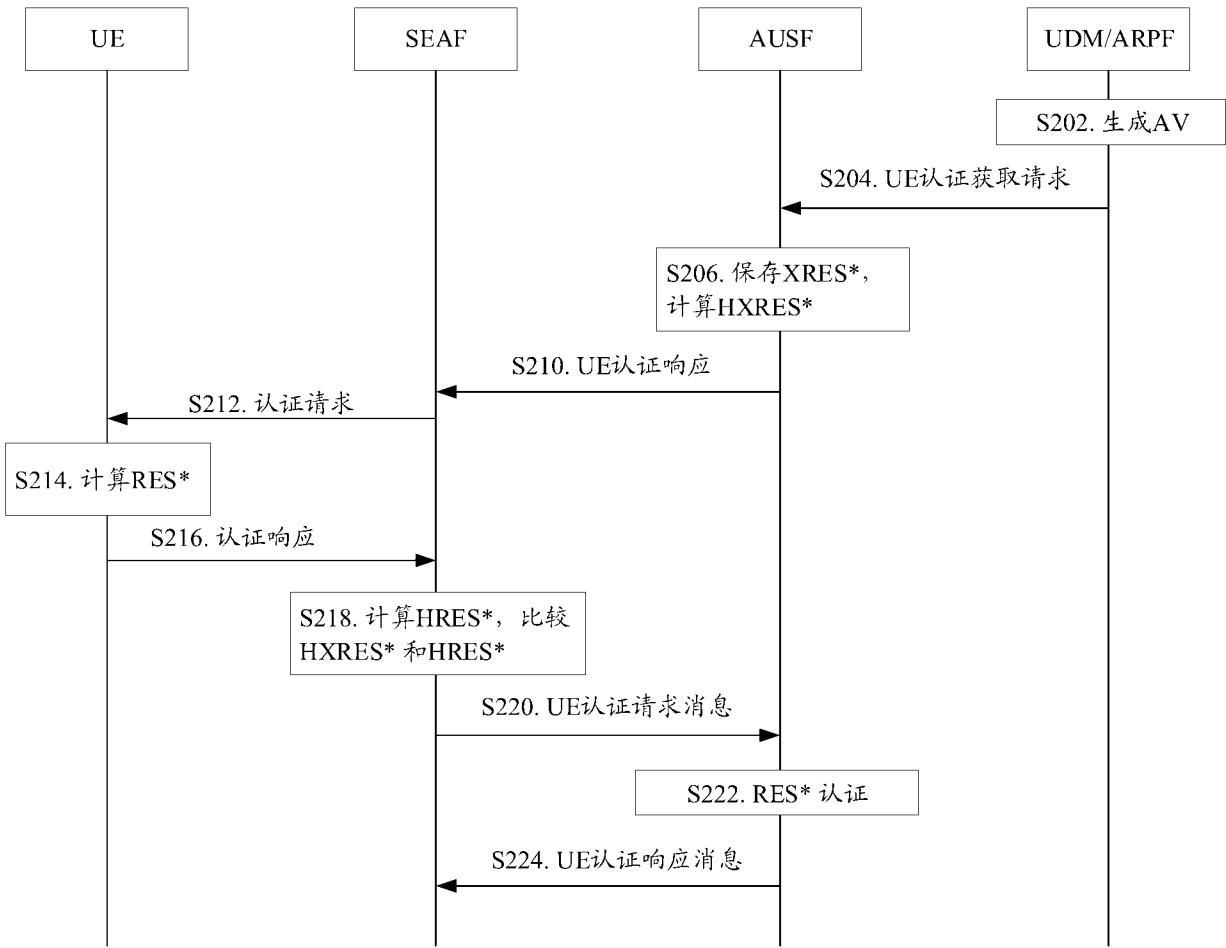


图 2

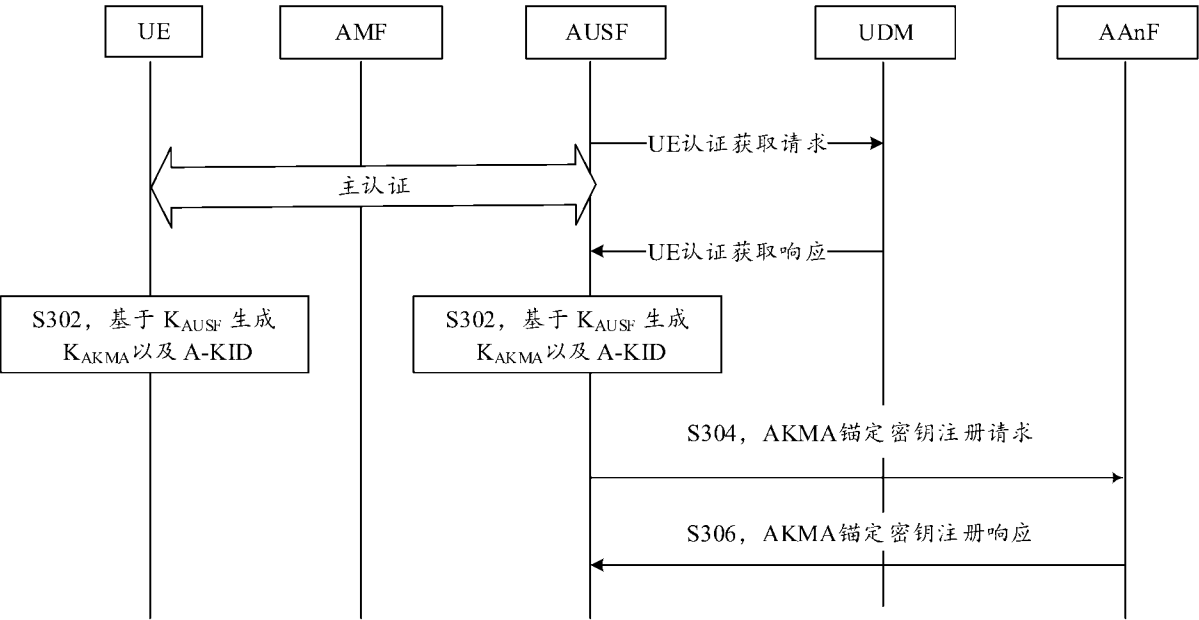


图 3

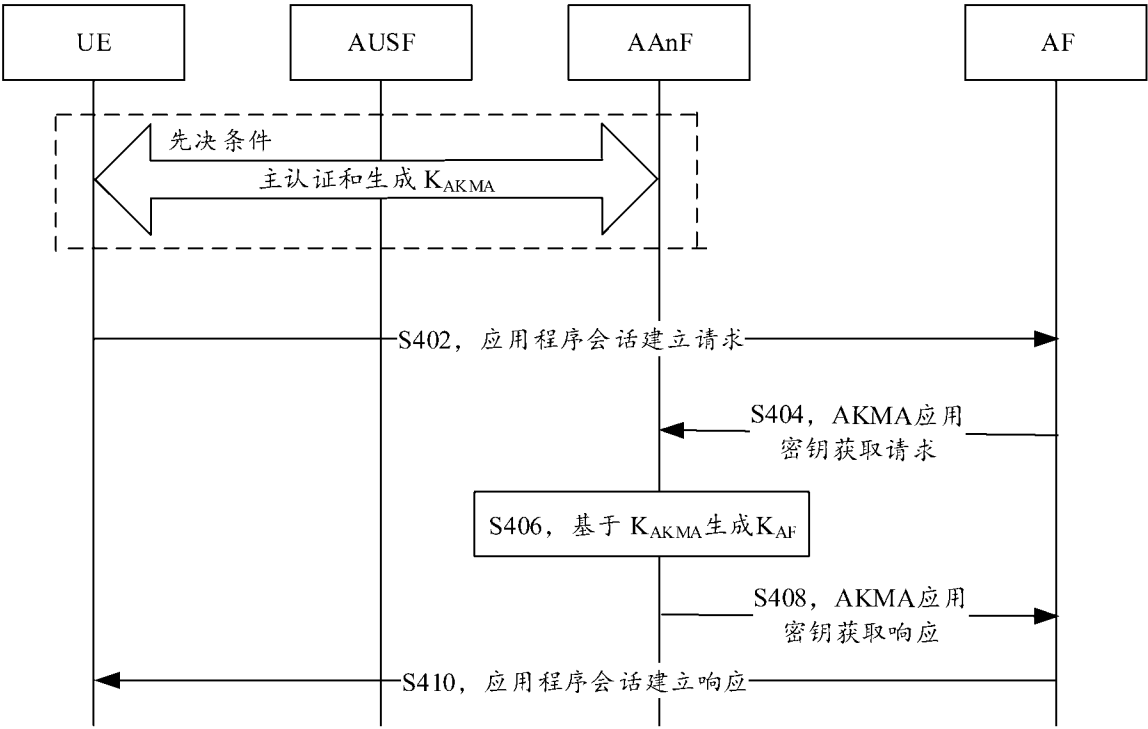


图 4

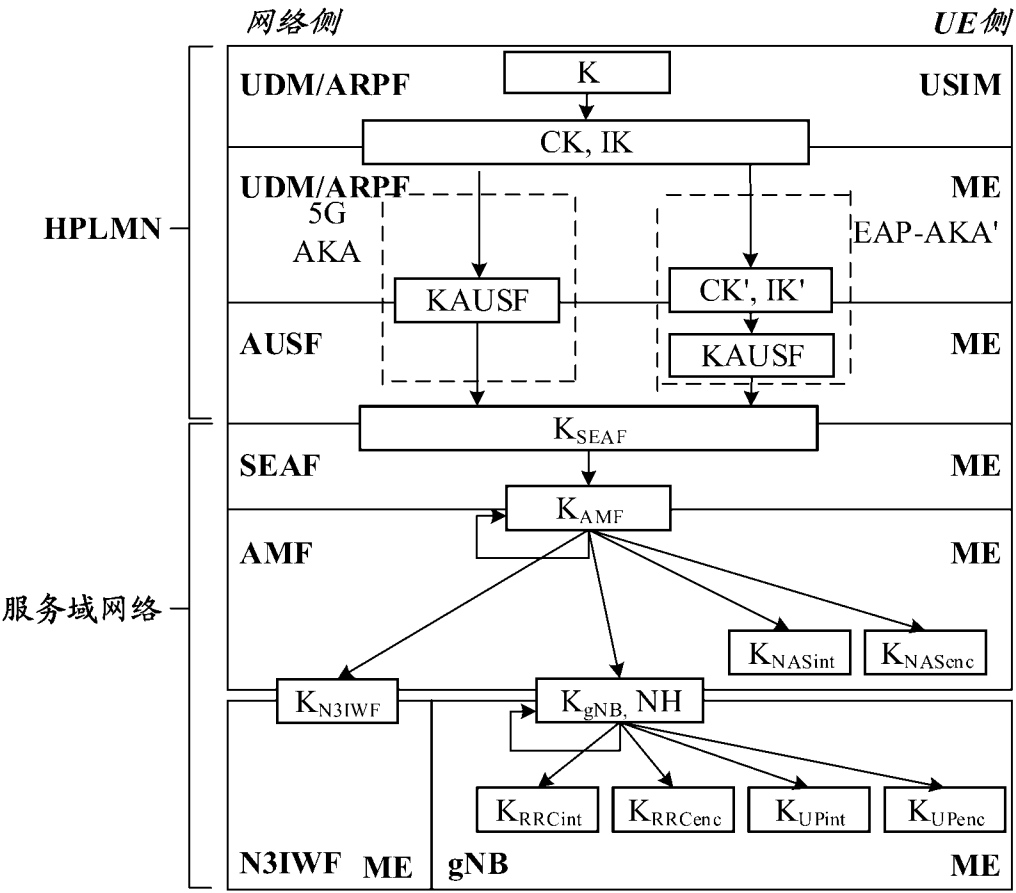


图 5

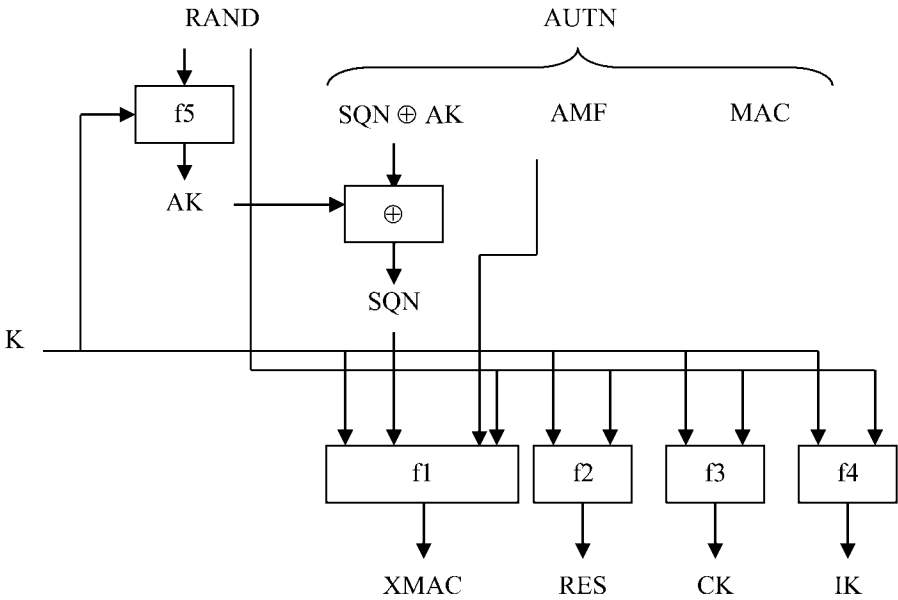


图 6

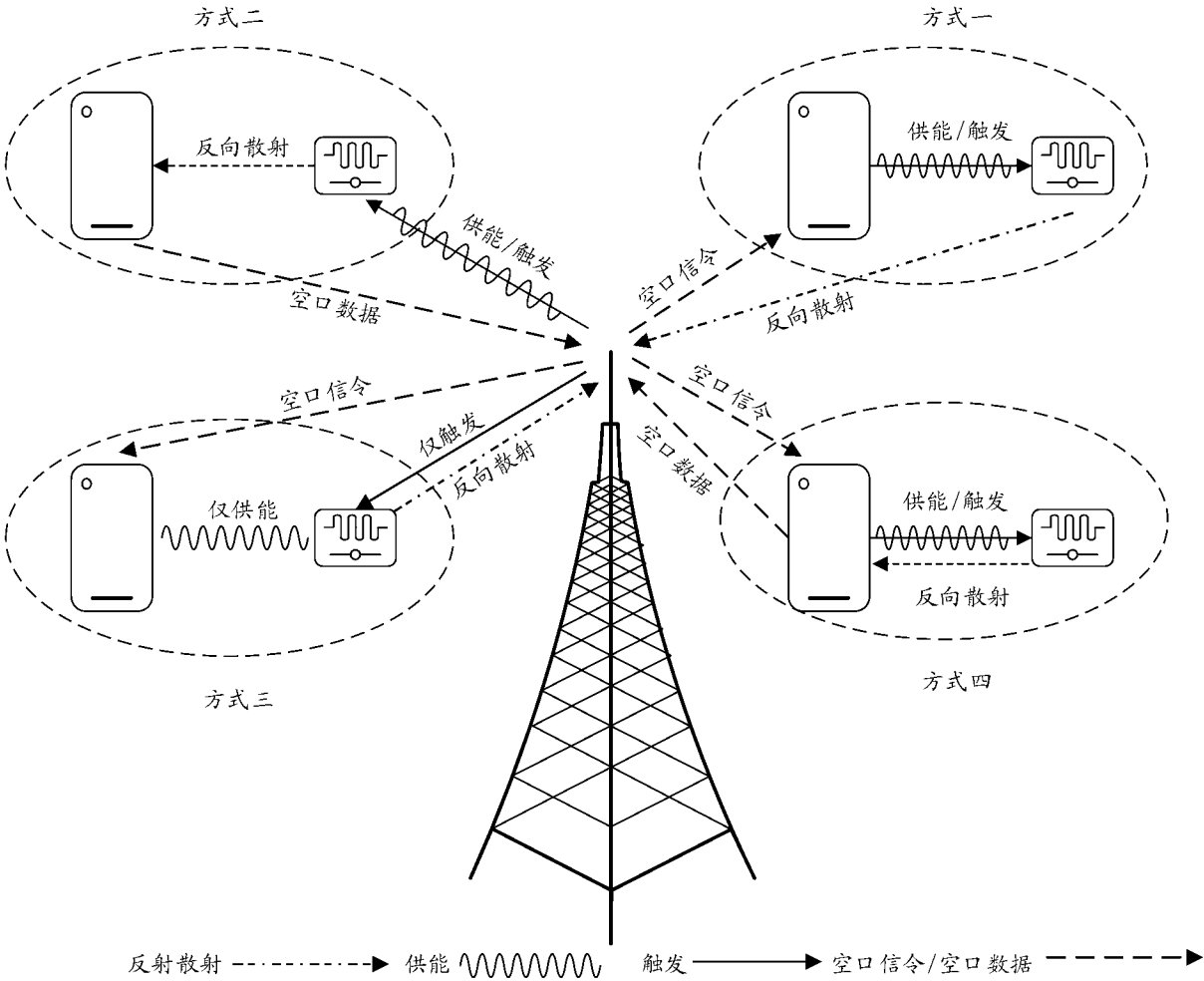


图 7

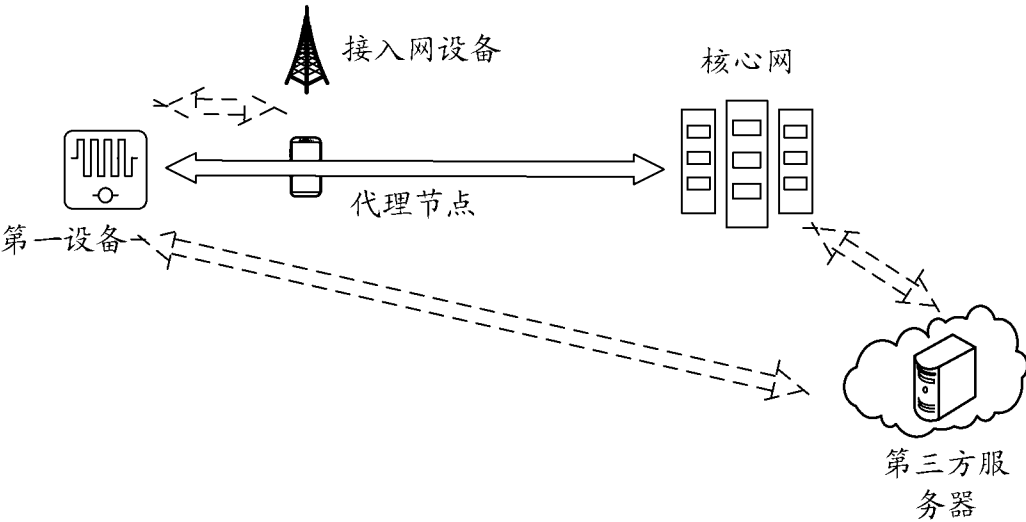


图 8

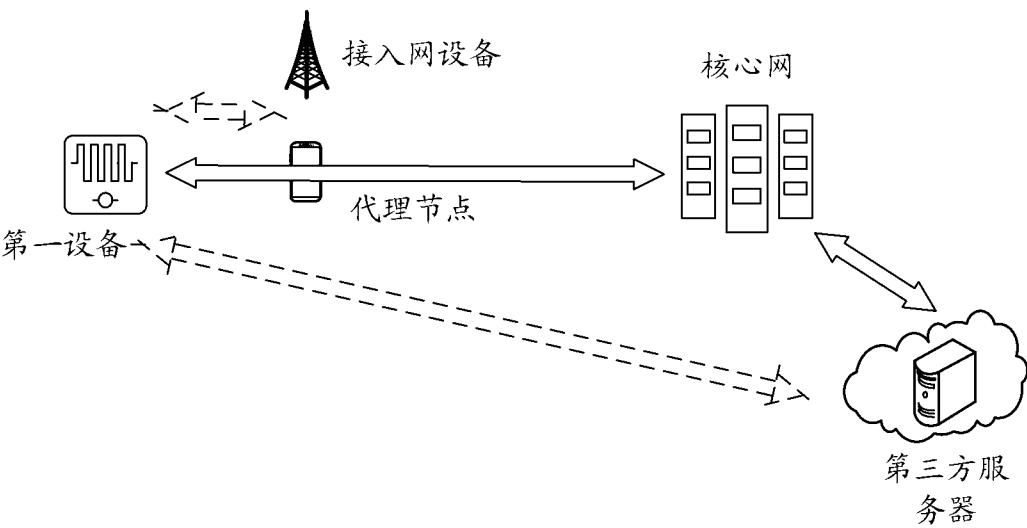


图 9

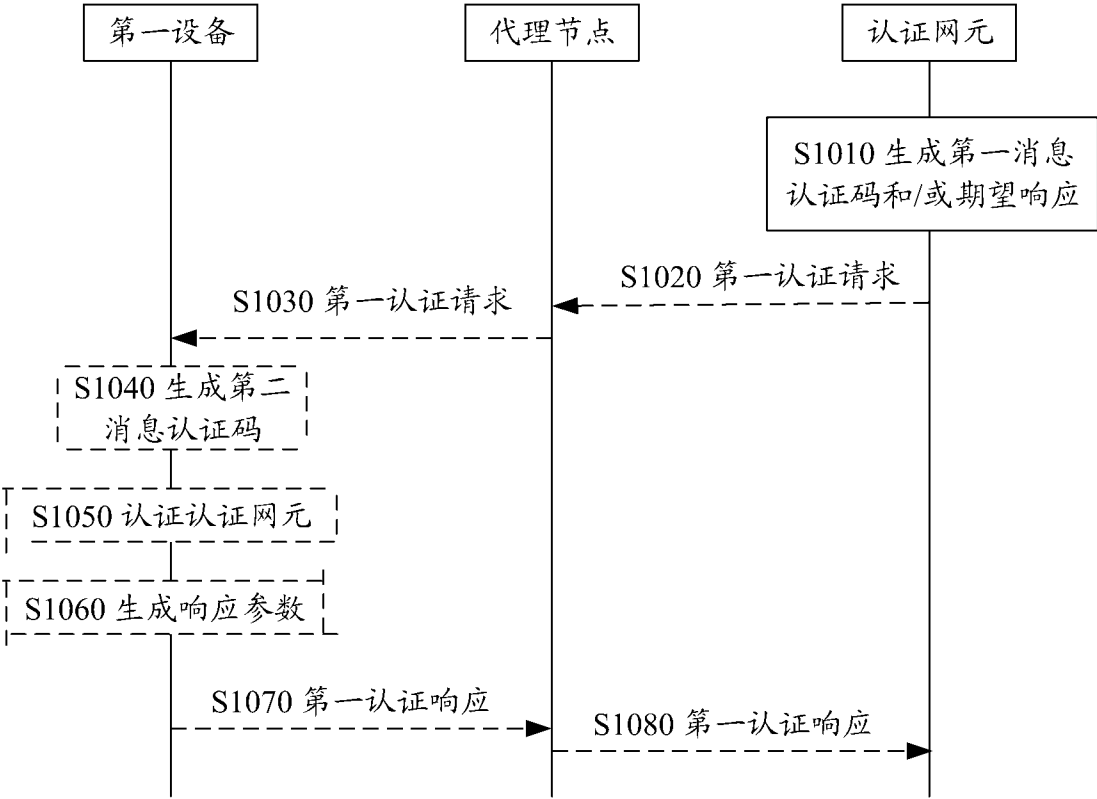


图 10

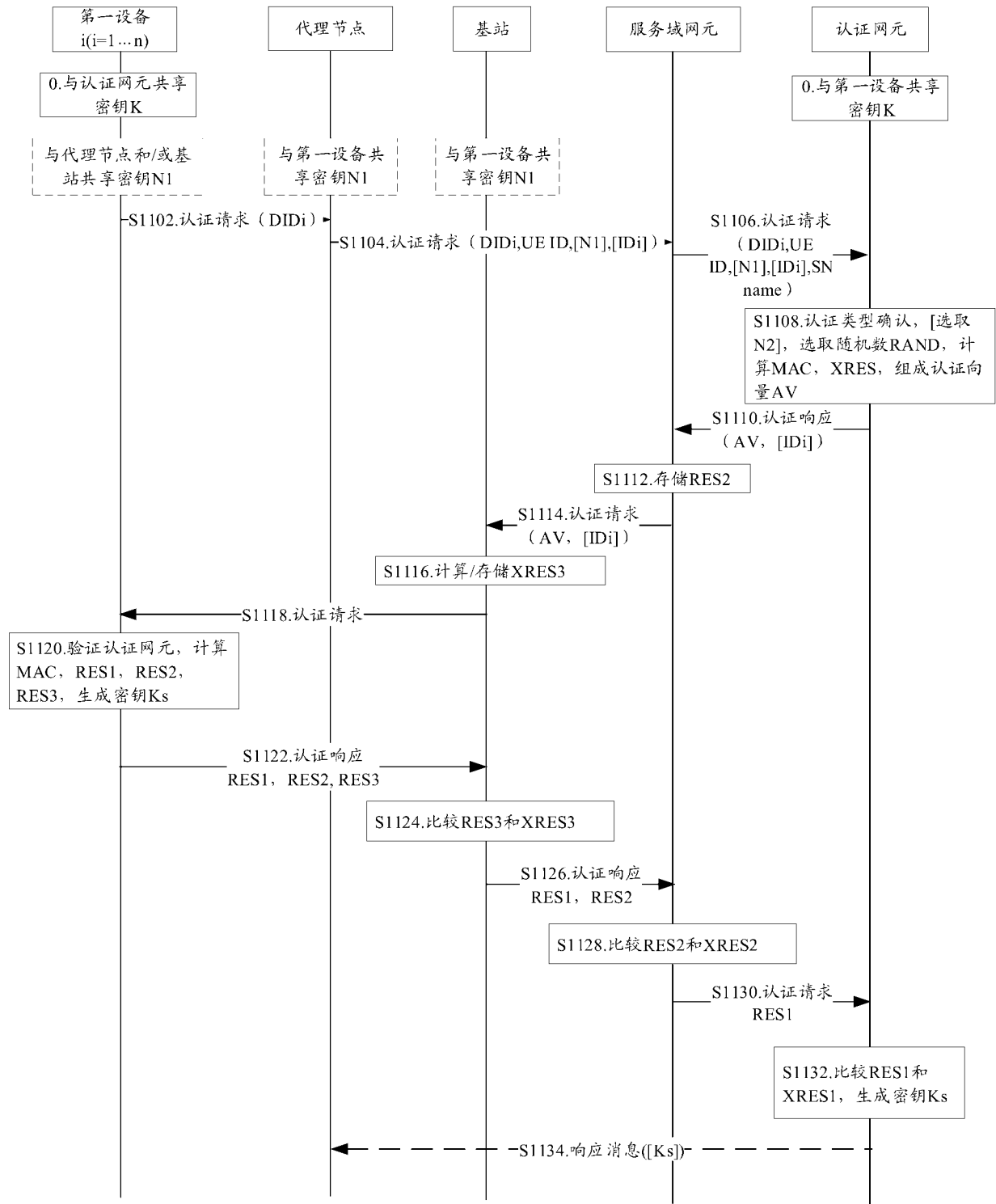


图 11

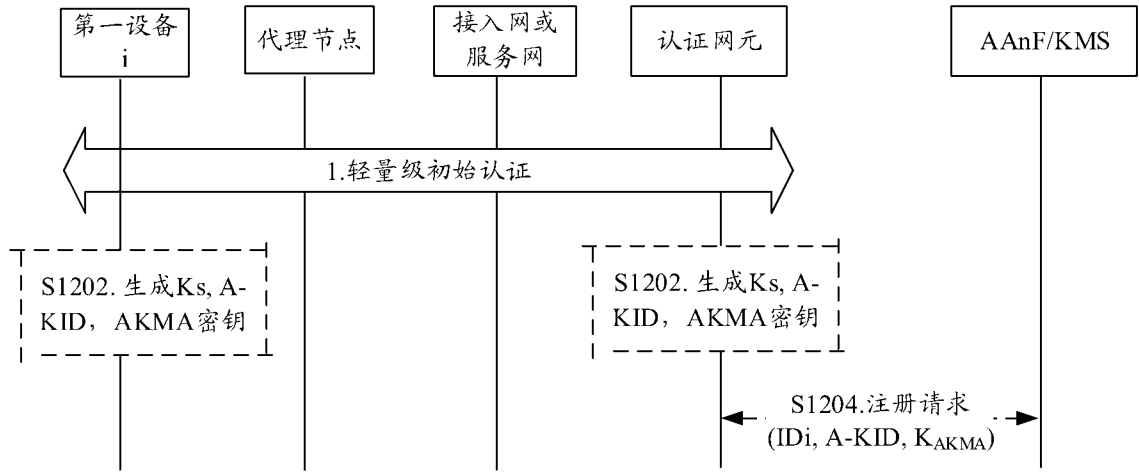


图 12

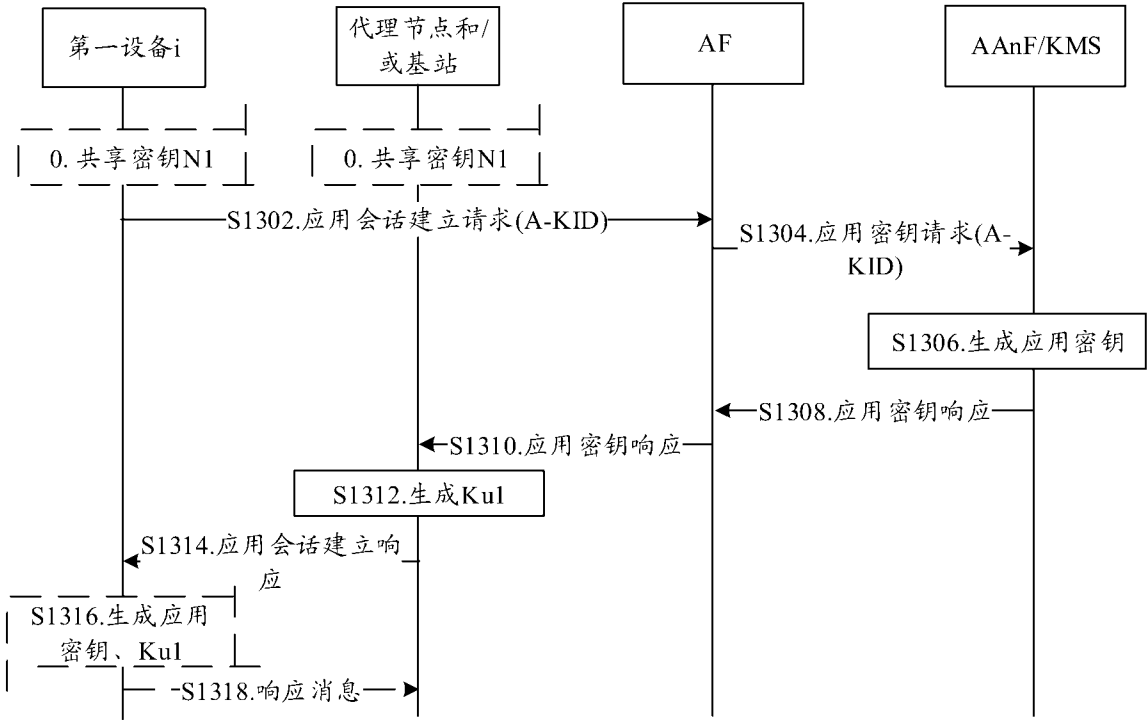


图 13

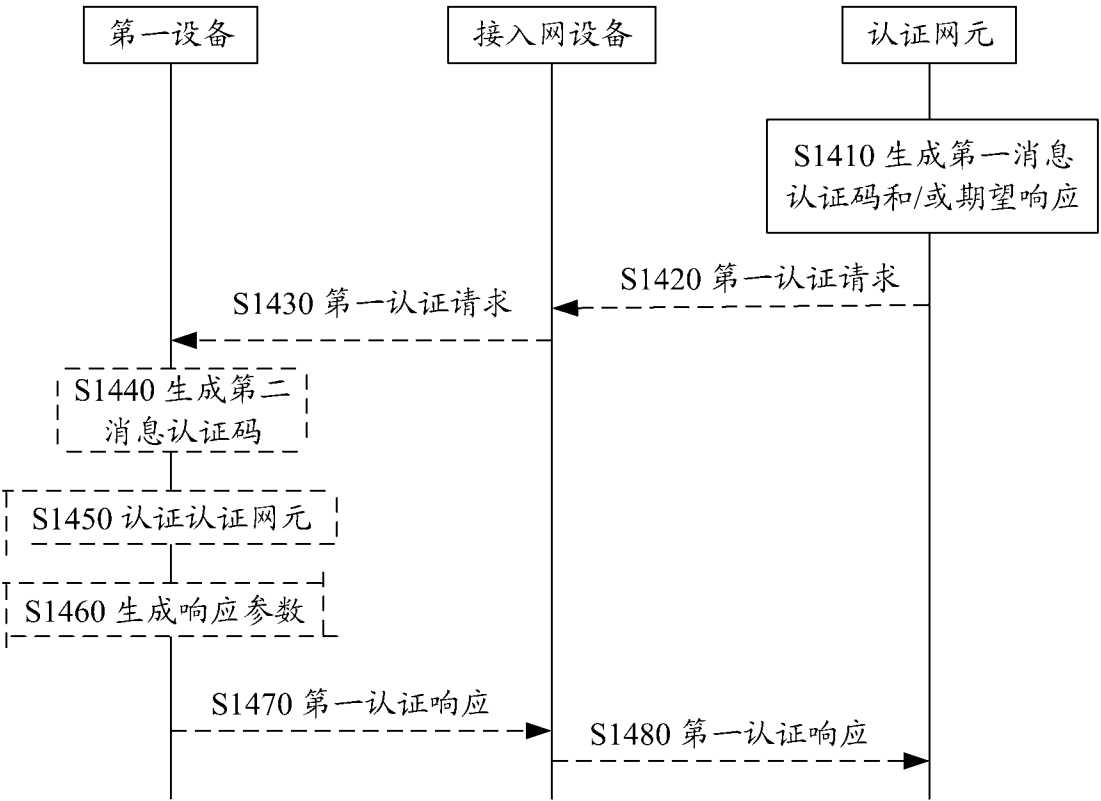


图 14

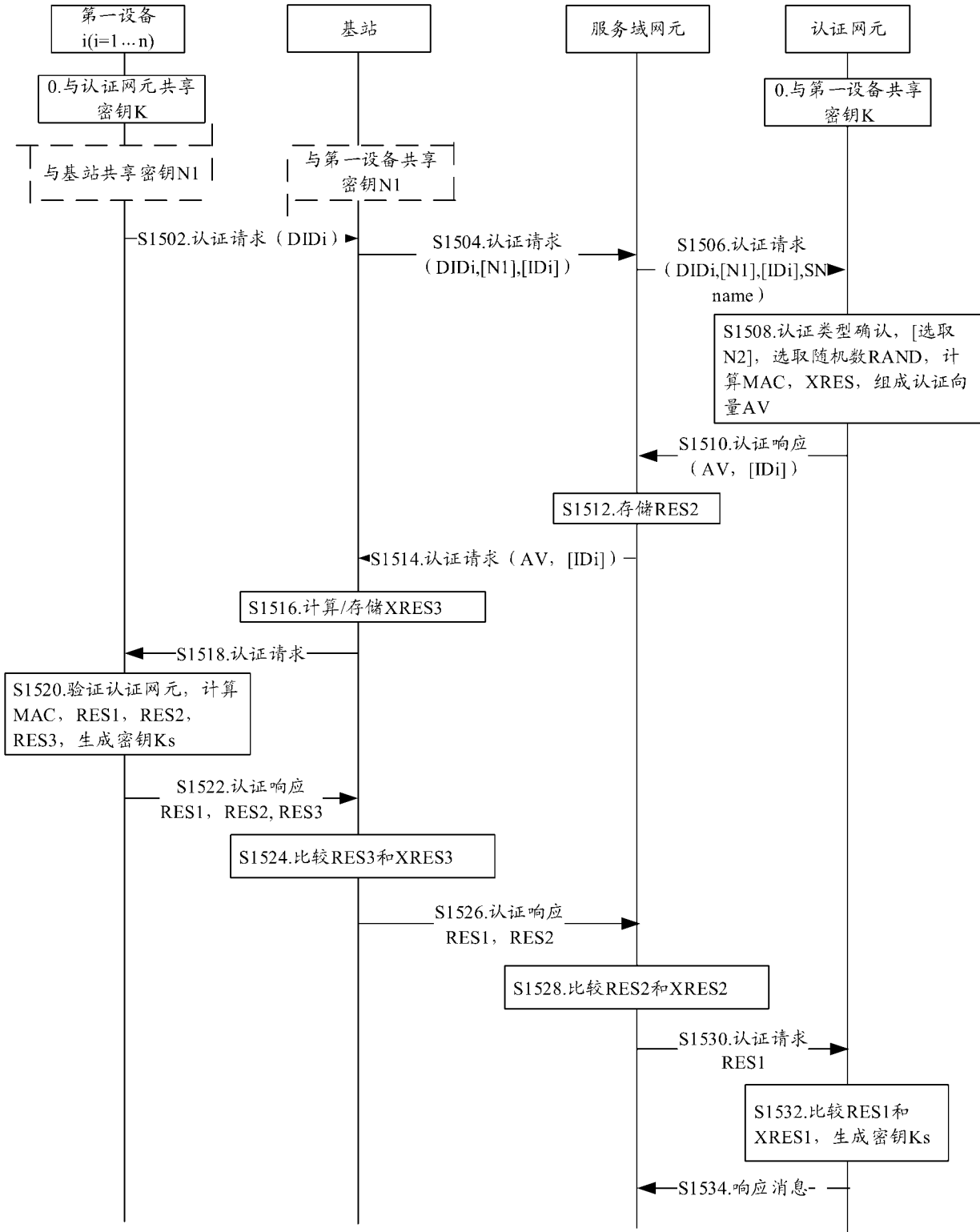


图 15

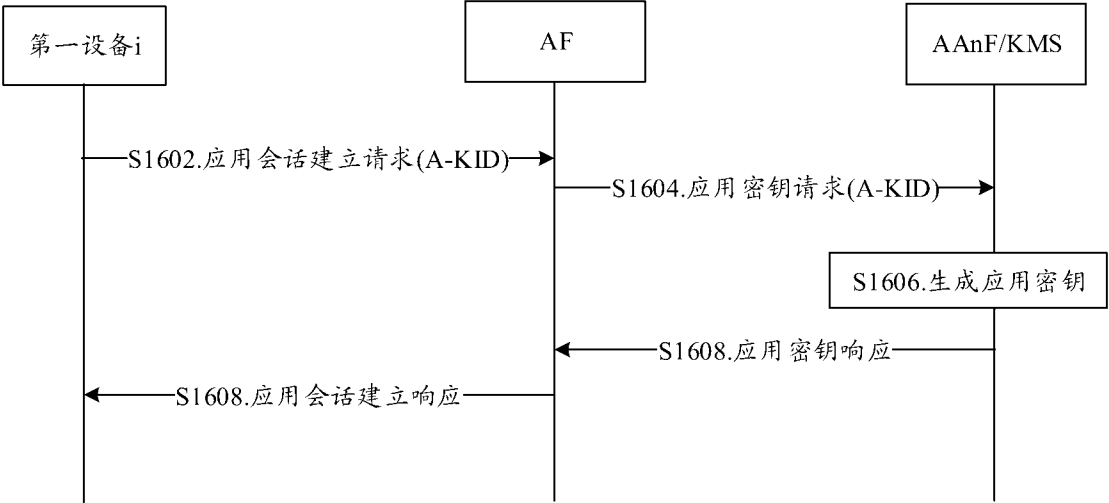


图 16

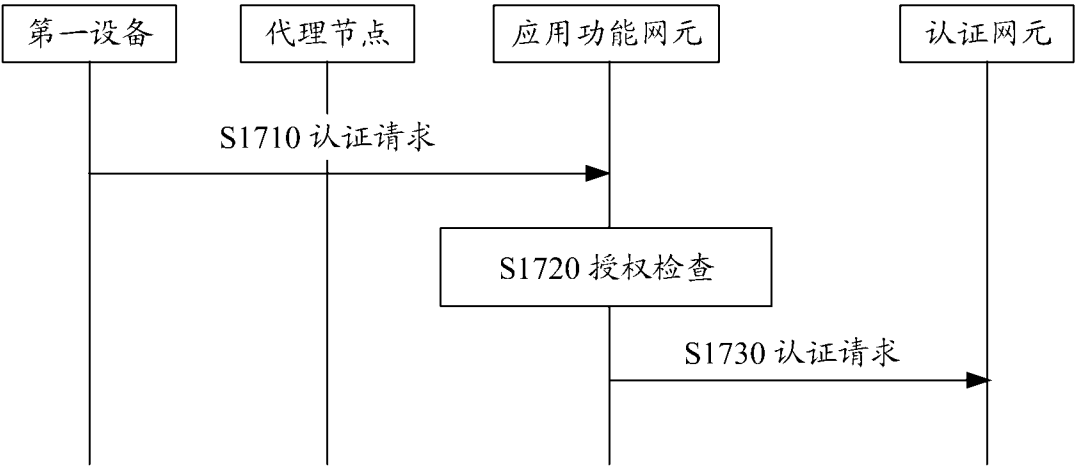


图 17

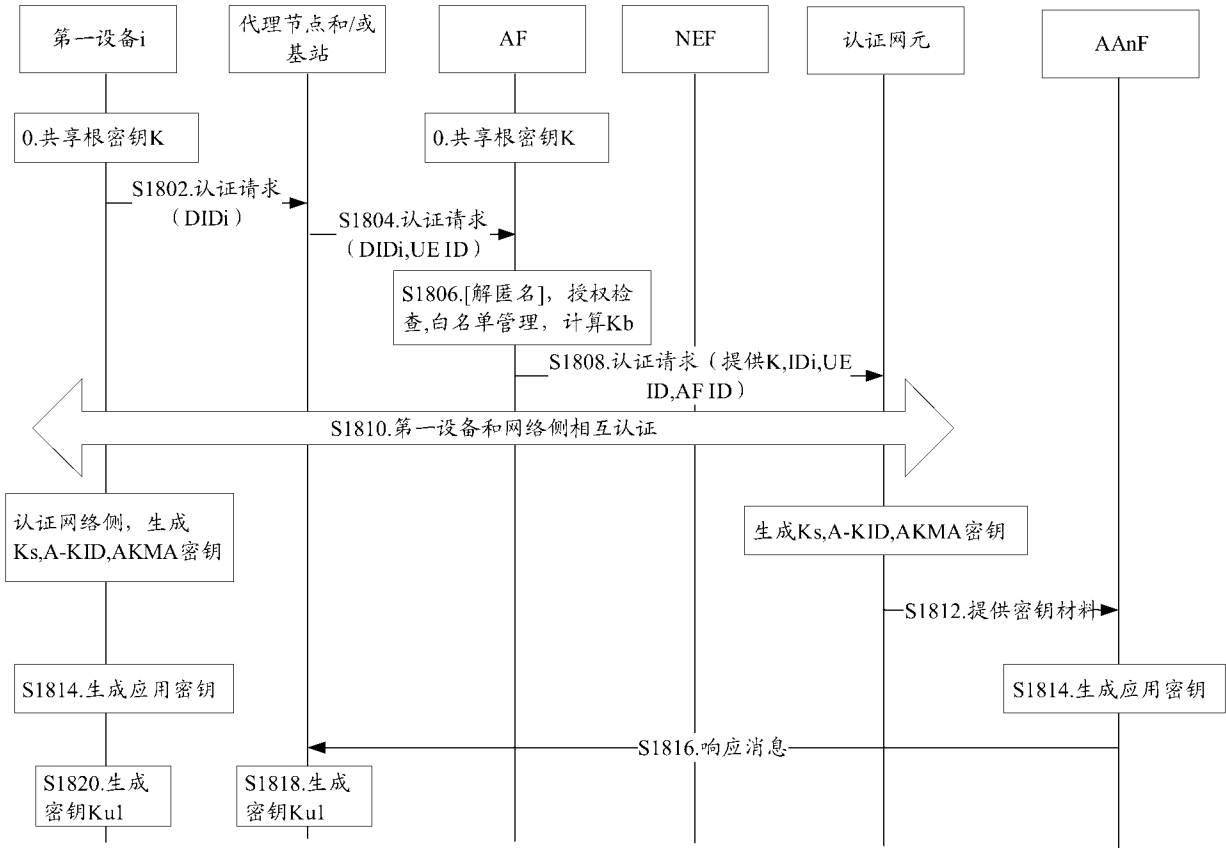


图 18

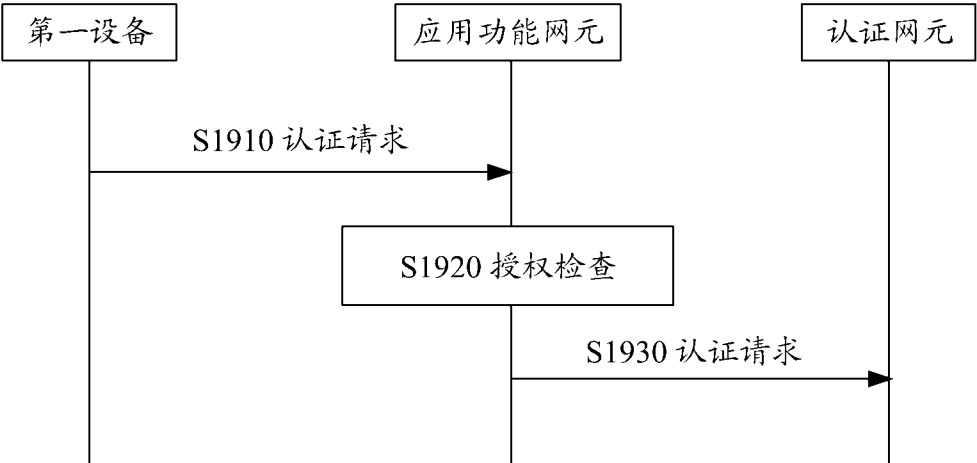


图 19

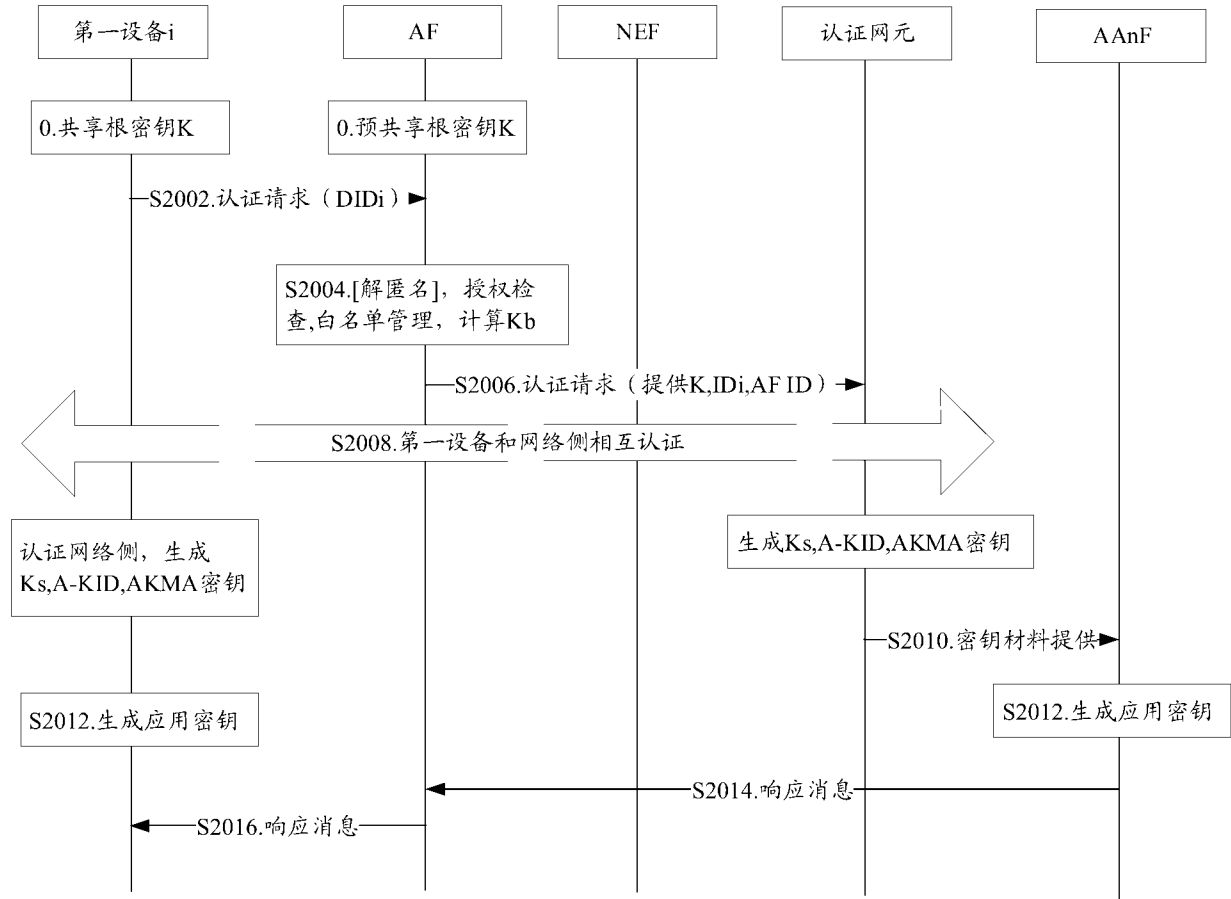


图 20

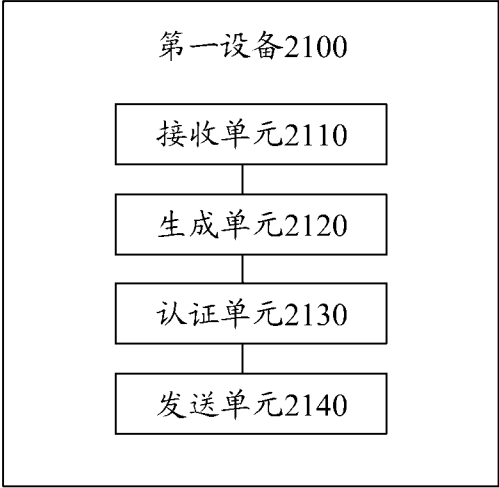


图 21



图 22

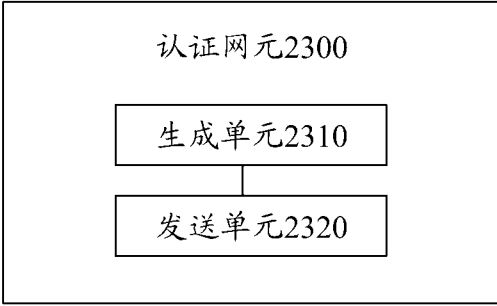


图 23

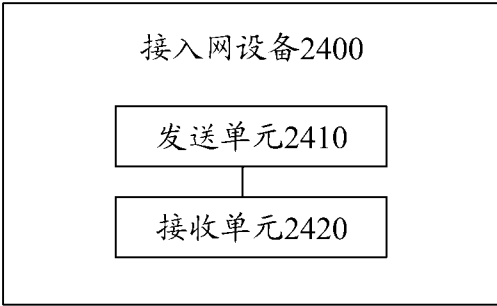


图 24

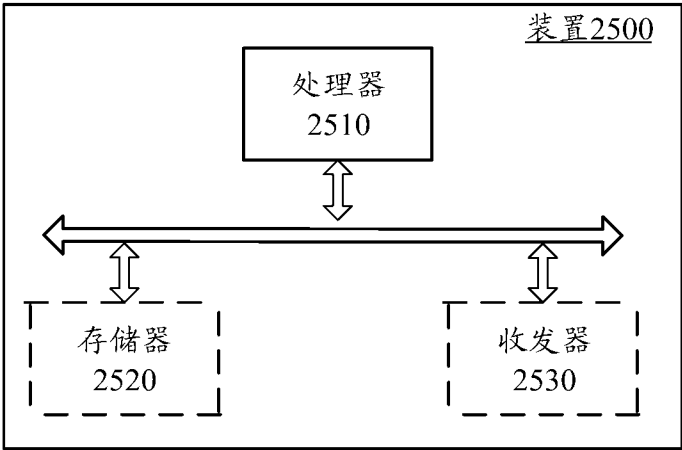


图 25

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/095769

A. CLASSIFICATION OF SUBJECT MATTER H04W 12/069(2021.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC:H04W Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) CNABS; CNTXT; VEN; WOTXT; USTXT; EPTXT; CNKI; 3GPP: 终端, 零功耗, 物联网设备, 代理, 认证, 请求, 消息认证码, 密钥, 算法, 成功, 响应, 基站, 接入网, terminal, UE, IoT, proxy, authenticate, request, MAC, key, success, response, XRES		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110012467 A (BEELINKER TECHNOLOGY (SUZHOU) CO., LTD.) 12 July 2019 (2019-07-12) description, paragraphs [0015]-[0030]	1-87
A	CN 111669276 A (HUAWEI TECHNOLOGIES CO., LTD.) 15 September 2020 (2020-09-15) entire document	1-87
A	CN 115380570 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 November 2022 (2022-11-22) entire document	1-87
A	CN 115776398 A (CHINA RESOURCES DIGITAL TECHNOLOGY CO., LTD.) 10 March 2023 (2023-03-10) entire document	1-87
A	US 2017353859 A1 (SEARS BRANDS, L.L.C.) 07 December 2017 (2017-12-07) entire document	1-87
☐ 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 23 January 2024		Date of mailing of the international search report 04 February 2024
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		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/095769

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110012467	A	12 July 2019	None			
CN	111669276	A	15 September 2020	None			
CN	115380570	A	22 November 2022	None			
CN	115776398	A	10 March 2023	None			
US	2017353859	A1	07 December 2017	US	10064062	B2	28 August 2018

A. 主题的分类

H04W 12/069(2021.01)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)

IPC:H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS;CNTXT;VEN;WO TXT;USTXT;EPTXT;CNKI;3GPP: 终端, 零功耗, 物联网设备, 代理, 认证, 请求, 消息认证码, 密钥, 算法, 成功, 响应, 基站, 接入网, terminal, UE, IoT, proxy, authenticate, request, MAC, key, success, response, XRES

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 110012467 A (苏州博联科技有限公司) 2019年7月12日 (2019 - 07 - 12) 说明书第[0015]–[0030]段	1–87
A	CN 111669276 A (华为技术有限公司) 2020年9月15日 (2020 - 09 - 15) 全文	1–87
A	CN 115380570 A (华为技术有限公司) 2022年11月22日 (2022 - 11 - 22) 全文	1–87
A	CN 115776398 A (华润数字科技有限公司) 2023年3月10日 (2023 - 03 - 10) 全文	1–87
A	US 2017353859 A1 (SEARS BRANDS LLC) 2017年12月7日 (2017 - 12 - 07) 全文	1–87

☐ 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

2024年1月23日

国际检索报告邮寄日期

2024年2月4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

授权官员

邱德洁

电话号码 (+86) 0512-88996146

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/095769

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	110012467	A	2019年7月12日	无	
CN	111669276	A	2020年9月15日	无	
CN	115380570	A	2022年11月22日	无	
CN	115776398	A	2023年3月10日	无	
US	2017353859	A1	2017年12月7日	US 10064062 B2	2018年8月28日