

(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
2021 年 3 月 11 日 (11.03.2021)



(10) 国际公布号
WO 2021/043095 A1

- (51) 国际专利分类号:
H04L 9/08 (2006.01) **H04W 12/04** (2009.01)
- (21) 国际申请号: PCT/CN2020/112415
- (22) 国际申请日: 2020 年 8 月 31 日 (31.08.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910842413.7 2019年9月6日 (06.09.2019) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 于小博(YU, Xiaobo); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 肖月振(XIAO, Yuezheng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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,

(54) Title: KEY GENERATION AND TERMINAL PROVISIONING METHOD AND APPARATUS, AND DEVICES

(54) 发明名称: 密钥生成以及终端配网方法、装置、设备

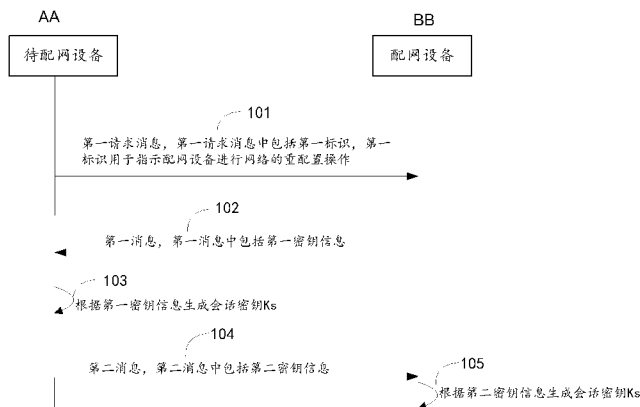


图 1

(57) Abstract: Embodiments of the present application provide a key generation and terminal provisioning method and apparatus, and devices. The key generation method comprises: an enrollee device sends a first request message to a configurator device, the first request message comprising a first identifier, and the first identifier being used for instructing the configurator device to perform a network reconfiguration operation; the enrollee device receives a first message comprising first key information sent by the configurator device; the enrollee device generates a session key according to the first key information; the enrollee device sends a second message comprising second key information to the configurator device, so that the configurator device generates a session key according to the second key information. The enrollee device and the configurator device exchange the key information with each other in the process of performing first-time network configuration to generate the session key required for subsequent network reconfiguration of the enrollee device, so that when network reconfiguration is performed on the enrollee device, an authentication process does not need to be performed again, thereby improving the network configuration efficiency.

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))。

(57) 摘要: 本申请实施例提供一种密钥生成以及终端配网方法、装置、设备, 该密钥生成方法包括: 待配网设备向配网设备发送第一请求消息, 第一请求消息中包括第一标识, 第一标识用于指示配网设备进行网络的重配置操作; 待配网设备接收配网设备发送的包括第一密钥信息的第一消息; 待配网设备根据第一密钥信息生成会话密钥; 待配网设备向配网设备发送第二消息, 第二消息中包括第二密钥信息, 以使配网设备根据第二密钥信息生成所述会话密钥。待配网设备与配网设备在进行第一次配网的过程中, 交换彼此的密钥信息以生成用于后续对待配网设备进行网络重配置所需的会话密钥, 使得对待配网设备进行网络重配置时, 无需再次执行鉴权过程, 提高了网络配置效率。

密钥生成以及终端配网方法、装置、设备

本申请要求 2019 年 09 月 06 日递交的申请号为 201910842413.7、发明名称为“密钥生成以及终端配网方法、装置、设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及通信技术领域，特别是涉及一种密钥生成以及终端配网方法、装置、设备。

10 背景技术

随着通信技术的快速发展，遵循 IEEE802.11 协议标准的无线局域网（Wireless Local Area Networks，简称 WLAN）技术被广泛应用于各种设备中，这些设备中有些设备是具有屏幕（显示屏）的，例如，手机、电脑等智能终端设备；有些设备是不具有屏幕的，例如，智能空调和智能电饭煲等物联网设备。

15 终端配网一直是 Wi-Fi 物联网的一个痛点问题。用户购买一个 Wi-Fi 物联网设备后，需要将此设备配置到家庭 Wi-Fi 网络中。终端配网协议（Device Provisioning Protocol, 简称 DPP）是 Wi-Fi 联盟制定的解决终端配网问题的协议。DPP 由三个子协议组成，分别是 DPP 鉴权协议（DPP authentication protocol），DPP 配置协议（DPP configuration protocol）以及 DPP 介绍协议（DPP Introduction protocol）。DPP 鉴权协议主要用于使配网设备（称为 configurator）和待配网设备（称为 enrollee）之间能够进行双向鉴权并且生成后续 DPP 配置协议所需要的会话密钥。DPP 配置协议主要用于使待配网设备（enrollee）能够从配网设备（configurator）处获得连接接入点（Access Point，简称 AP）所需要的服务集标识（Service Set Identifier，简称 SSID）以及接入密码。DPP 介绍协议主要用于 enrollee 之间利用各自的公私钥来生成相互通信所需要的会话密钥。

25 AP 在重配 SSID 或者接入密码后，往往会重启。enrollee 由于没有获得重配的这些信息，则需要与 configurator 进行二次配置即进行网络的重新配置，重配置只能从 DPP 鉴权协议开始，使协议复杂度和冗余度增加。

发明内容

30 鉴于上述问题，提出了本申请实施例以便提供一种克服上述问题或者至少部分地解

决上述问题的一种密钥生成以及终端配网方法、装置、设备。

第一方面，本申请实施例提供一种密钥生成方法，包括：

待配网设备向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

5 所述待配网设备接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

所述待配网设备根据所述第一密钥信息生成会话密钥；

所述待配网设备向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥。

10 第二方面，本申请实施例提供一种密钥生成装置，位于待配网设备中，包括：

发送模块，用于向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

接收模块，用于接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

15 生成模块，用于根据所述第一密钥信息生成会话密钥；

所述发送模块，还用于向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥。

第三方面，本申请实施例提供一种待配网设备，包括处理器和存储器，其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行第一方面中的密钥生成方法。
20

本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被待配网设备的处理器执行时，使所述处理器执行第一方面中的密钥生成方法。

第四方面，本申请实施例提供一种密钥生成方法，包括：

25 配网设备接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

所述配网设备根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述配网设备接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；
30

所述配网设备根据所述第二密钥信息生成所述会话密钥。

第五方面，本申请实施例提供一种密钥生成装置，位于配网设备中，包括：

接收模块，用于接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

5 发送模块，用于根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述接收模块，还用于接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

生成模块，用于根据所述第二密钥信息生成所述会话密钥。

10 第六方面，本申请实施例提供一种配网设备，包括处理器和存储器，其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行第四方面中的密钥生成方法。

本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被配网设备的处理器执行时，使所述处理器执行第四方面中的密钥生成方法。

15 第七方面，本申请实施例提供一种终端配网方法，该方法包括：

待配网设备向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

20 所述待配网设备接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

所述待配网设备根据所述第一密钥信息生成会话密钥；

所述待配网设备向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥；所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

25 第八方面，本申请实施例提供一种终端配网装置，位于待配网设备，包括：

发送模块，用于向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

接收模块，用于接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

30 生成模块，用于根据所述第一密钥信息生成会话密钥；

所述发送模块，还用于向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥；

所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

第九方面，本申请实施例提供一种待配网设备，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如第七方面所述的终端配网方法。

第十方面，本申请实施例提供一种终端配网方法，该方法包括：

配网设备接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

10 所述配网设备根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述配网设备接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

15 所述配网设备根据所述第二密钥信息生成所述会话密钥，所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

第十一方面，本申请实施例提供一种终端配网装置，位于配网设备，包括：

接收模块，用于接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

20 发送模块，用于根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述接收模块，还用于接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

生成模块，用于根据所述第二密钥信息生成所述会话密钥；所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

25 第十二方面，本申请实施例提供一种配网设备，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如第十方面所述的终端配网方法。

30 在以上各个方面提供的密钥生成方法、终端配网方法中，以网络配置场景来说，待配网设备在当前请求配网设备进行网络配置的过程中，通过与配网设备交互，配网设备将自身产生的第一密钥信息发送给待配网设备，待配网设备将自身产生的第二密钥信息

发送至配网设备，使得配网设备和待配网设备根据自己产生的密钥信息以及从对方接收到的另一密钥信息生成用于后续对待配网设备进行网络重配置所需的会话密钥。从而，当需要对待配网设备进行网络重配置时，无需再执行 DPP 鉴权过程，仅需要基于新生成的会话密钥执行 DPP 配置过程即可，提高了网络配置效率。

5 第十三方面，本申请实施例提供一种密钥生成方法，包括：

待配网设备接收配网设备发送的认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息；

所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

10 所述待配网设备向所述配网设备发送与所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息，以使所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成所述第一会话密钥和所述第二会话密钥。

第十四方面，本申请实施例提供一种密钥生成装置，位于待配网设备中，包括：

15 接收模块，用于接收配网设备发送的认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息；

生成模块，用于根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

20 发送模块，用于向所述配网设备发送与所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息，以使所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成所述第一会话密钥和所述第二会话密钥。

25 第十五方面，本申请实施例提供一种待配网设备，包括处理器和存储器，其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行第十三方面中的密钥生成方法。

第十六方面，本申请实施例提供一种密钥生成方法，包括：

30 配网设备向待配网设备发送认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息，以使所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

所述配网设备接收所述待配网设备发送的所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息；

所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成第一会话密钥和第二会话密钥。

5 第十七方面，本申请实施例提供一种密钥生成装置，位于配网设备中，包括：

发送模块，用于向待配网设备发送认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息，以使所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

10 接收模块，用于接收所述待配网设备发送的所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息；

生成模块，用于根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成第一会话密钥和第二会话密钥。

15 第十八方面，本申请实施例提供一种配网设备，包括处理器和存储器，其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行第十六方面中的密钥生成方法。

以上十三方面提供的密钥生成方法可以适用于 DPP 鉴权过程中，在该鉴权过程中，配网设备和待配网设备各自会生成两个随机数，以用于生成用于两次配网过程的会话密钥。以配网设备触发该鉴权过程为例来说，配网设备将自己产生的两个随机数（假设表示为 I-nonce1, I-nonce2）发送至待配网设备，同样地，待配网设备也将自己产生的两个随机数（假设表示为 R-nonce1, R-nonce2）发送至配网设备，由此，配网设备和待配网设备各自获得四个随机数。配网设备和待配网设备都可以根据 I-nonce1 和 R-nonce1 生成第一会话密钥（假设表示为 ke1），以及根据 I-nonce2 和 R-nonce2 生成第二会话密钥（假设表示为 ke2）。第一会话密钥和第二会话密钥可以被用于后续待配网设备与配网设备之间的两次网络配置过程中。由于一次生成两个会话密钥，在不同的网络配置过程中使用不同的会话密钥，可以使得在重配置过程中不需要再经历一次鉴权协议流程，提高了网络配置效率。

20

25

附图说明

30 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用

的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请一实施例提供的密钥生成方法的原理示意图；

5 图 2 为本申请一实施例提供的密钥生成方法的流程示意图；

图 3 为本申请另一实施例提供的密钥生成方法的流程示意图；

图 4 为本申请一实施例提供的终端配网方法的流程示意图；

图 5 为本申请另一实施例提供的终端配网方法的流程示意图；

图 6 为本申请另一实施例提供的终端配网方法的流程示意图；

10 图 7 为本申请另一实施例提供的终端配网方法的流程示意图；

图 8 为本申请另一实施例提供的密钥生成方法的流程示意图；

图 9 为本申请一实施例提供的使用 ke1 和 ke2 进行网络配置的流程示意图；

图 10 为本申请实施例提供的一种密钥生成装置的结构示意图；

图 11 为与图 10 所示实施例提供的密钥生成装置对应的待配网设备的结构示意图；

15 图 12 为本申请实施例提供的另一种密钥生成装置的结构示意图；

图 13 为与图 12 所示实施例提供的密钥生成装置对应的配网设备的结构示意图；

图 14 为本申请实施例提供的一种终端配网装置的结构示意图；

图 15 为与图 14 所示实施例提供的终端配网装置对应的待配网设备的结构示意图；

图 16 为本申请实施例提供的另一种终端配网装置的结构示意图；

20 图 17 为与图 16 所示实施例提供的终端配网装置对应的配网设备的结构示意图；

图 18 为本申请实施例提供的另一种密钥生成装置的结构示意图；

图 19 为与图 18 所示实施例提供的密钥生成装置对应的待配网设备的结构示意图；

图 20 为本申请实施例提供的另一种密钥生成装置的结构示意图；

图 21 为与图 20 所示实施例提供的密钥生成装置对应的配网设备的结构示意图。

25

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范

30

围。

在本申请实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义，“多种”一般包含至少

5

两种。

取决于语境，如在此所使用的词语“如果”、“若”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测（陈述的条件或事件）”可以被解释成为“当确定时”或“响应于确定”或“当检测（陈述的条件或事件）时”或“响应于检测（陈述的条件或事件）”。

10

还需要说明的是，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商品或者系统不仅包括那些要素，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商品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的商品或者系统中还存在另外的相同要素。

15

另外，下述各方法实施例中的步骤时序仅为一种举例，而非严格限定。

在具体介绍本申请实施例提供的方案前，先对本文中涉及到的几个概念进行说明。

本文中的待配网设备可以是诸如智能冰箱、智能音箱、机器人等物联网设备。特别地，待配网设备也可以是红外传感器，烟雾传感器等具有低功耗需求的物联网设备。该待配网设备是指需要被配网的设备，由于还没有被连接到希望其接入的某个无线网络中，

20

因此称为待配网设备。

本文中的配网设备可以是手机、平板电脑等终端设备，该配网设备可以通过 AP 等网络设备已经接入某个无线网络，比如用户的手机通过家中安装的无线路由器已经接入家庭 Wi-Fi 网络。

值得说明的是，配网设备也可以是已经接入 AP 的智能冰箱、智能音箱等不具有人机交互屏幕的终端设备，此时，该配网设备本地可以存储有其接入的 AP 的网络配置信息，以便对未接入 AP 的待配网设备进行网络配置。其中，网络配置信息包括 AP 的 SSID 和接入密码。

25

另外，配网设备中可以运行有配网应用程序，通过该配网应用程序实现对待配网设备的网络配置。本文中，配网设备和配网应用程序可以做等同替换。

30

下面对本申请实施例提供的方案进行说明。

图 1 为本申请一实施例提供的密钥生成方法的原理示意图，如图 1 所示，该密钥生成方法可以包括如下步骤：

101、待配网设备向配网设备发送第一请求消息，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

5 在配网设备对待配网设备进行网络配置的场景中，本实施例的密钥生成方法可以在 DPP 配置过程中执行。

上述第一请求消息可以是待配网设备请求配网设备为其进行网络配置的请求消息（可以表示为：DPP Configuration request）。而且，该第一请求消息可以是待配网设备首次进行网络配置的时候向配网设备发送的。该第一请求消息中包含的第一标识，用以表明待配网设备具有网络重配置的能力。可选地，第一标识也可以用于指示配网设备在接下来发送的 DPP 配置应答消息中携带第一密钥信息。DPP 配置应答消息可以是第一消息。第一密钥信息可以是配网设备生成的连接器（connector）中所包含的公钥。第一标识可以叫做重配置状态标识（ReconfigStatus）或者叫做发送连接器状态标识（SendConnectorStatus）。第一标识也可以取其他的名称，本发明对此不做具体限定。

10 其中，配网设备生成的连接器中包含其生成的公私钥对中的公钥。连接器的作用概括来说就是为两个设备进行通信连接提供安全的通道，这两个设备比如为待配网设备和配网设备。

可以理解的是，在第一请求消息中携带该第一标识，可以促使配网设备执行网络的重配置操作，即下述步骤的执行。

20 102、配网设备根据第一标识向待配网设备发送第一消息，第一消息中包括第一密钥信息。

配网设备接收到第一请求消息时，解析发现该第一请求消息中包含预设的该第一标识，则确定待配网设备具有网络重配置的能力，从而，会触发向待配网设备发送包含第一密钥信息的第一消息。

25 其中，第一密钥信息可以是配网设备在接收到包含第一标识的第一请求消息时生成的公私钥对中的公钥。

可选地，第一请求消息中也可以不包含第一标识。配网设备可以直接在第一消息中携带第一密钥信息。待配网设备在接收到第一消息后，如果检测到不支持重配置能力，可以忽略第一消息中的第一密钥信息。反之，待配网设备可以在向配网设备发送的第二消息中携带第二密钥信息。

30

可选地，第一请求消息中还可以包括生成会话密钥数量的信息。待配网设备在收到生成会话密钥数量的信息后，会根据该信息生成相应数量的连接器（connector）。例如，如果生成会话密钥数量的信息为 3，则配网设备在向待配网设备发送的第一信息中包括 3 个连接器中的公钥，分别是 $\text{Connector}_{\text{confC1}}$ 、 $\text{Connector}_{\text{confC2}}$ 以及 $\text{Connector}_{\text{confC3}}$ 。待配网设备会根据收到的三个连接器中的公钥以及自身生成的公私钥对里的私钥来依次生成 $Ks1$ 、 $Ks2$ 以及 $Ks3$ 。同样的，待配网设备会在发送给配网设备的第二消息中携带 3 个连接器的公钥，分别为 $\text{Connector}_{\text{confE1}}$ 、 $\text{Connector}_{\text{confE2}}$ 以及 $\text{Connector}_{\text{confE3}}$ 。配网设备会根据收到的三个连接器中的公钥以及之前自身生成的公私钥对里的私钥来依次生成 $Ks1$ 、 $Ks2$ 以及 $Ks3$ 。三个会话密钥依次用于第二次配置过程，第三次配置过程以及第四次配置过程。配网设备和待配网设备在接收以及发送配置过程中的连接状态查询结果消息后，会删除当下配网过程中所用到的会话密钥。

为方便描述，本文中仅以生成第二次配置过程中所需的会话密钥 Ks 为例进行说明。

103、待配网设备根据第一密钥信息生成会话密钥 Ks 。

待配网设备可以在发送上述第一请求消息后生成公私钥对，将该公钥作为第二密钥信息。

待配网设备在得到第一密钥信息后，结合自己生成的第二密钥信息（即结合自己所生成的公钥所对应的私钥），生成用于后续对该待配网设备进行网络重配置所需用到的会话密钥 Ks 。

其中，会话密钥 Ks 的计算方式如下：

$N = \text{第一密钥信息} \times \text{第二密钥信息对应的私钥}$ ；

会话密钥 $Ks = \text{HKDF}(\langle \rangle, \text{"DPP second config"}, N.x)$ 。

其中， $\times$ 表示乘法；“DPP second config”表示此处有一串字符串，其取值可以自定义； $\langle \rangle$ 作为盐（salt）传递给 HKDF，表示 HKDF 的无盐（salt）调用；HKDF 表示一种特定的密钥衍生函数（HMAC-based Key Derivation Function）。

其中，在使用 HKDF 的过程中，椭圆曲线上的每个点都有 (x, y) 坐标。可以通过采用其 x 坐标并忽略 y 坐标将复数元素转换为标量。例如： $\text{val} = \text{Pub}.x$ 。

基于此， $N.x$ 表示复数 N 的标量， x 可以是 N 这个复数在椭圆曲线上对应的横坐标。

如前文所述，第一密钥信息为配网设备生成的公私钥对中的公钥，第二密钥信息为待配网设备生成的公私钥对中的公钥。

104、待配网设备向配网设备发送第二消息，第二消息中包括第二密钥信息。

105、配网设备根据第二密钥信息生成会话密钥 K_s 。

配网设备生成会话密钥 K_s 的方式与待配网设备生成会话密钥 K_s 的方式相同。可以理解的是，待配网设备和配网设备最终都会得到相同的会话密钥，以 K_s 表示。

在一可选实施例中，配网设备和待配网设备所生成的会话密钥 K_s 可以被用于对待配网设备进行网络的重配置的过程中。

本文中，网络重配置的意思是指：假设待配网设备通过第一次网络配置过程已经接入 AP，之后，由于 AP 的 SSID 或接入密码被更新，从而会触发 AP 重启。AP 重启后，由于此时待配网设备并未获得 AP 的新的网络配置信息，使得待配网设备与 AP 断开了连接，从而需要对该待配网设备进行网络重配置，使其再次接入该 AP。基于此，上述会话密钥 K_s 即可以被用于对该待配网设备进行网络重配置的过程中。

可以理解的是，当上述会话密钥 K_s 被用于对该待配网设备进行网络重配置的过程中时，若待配网设备重新接入 AP，则该会话密钥 K_s 便会失效，即此后待配网设备与配网设备之间的数据交互将不再使用该会话密钥 K_s 进行加密。当然，可选地，该会话密钥 K_s 的生命周期也是可以被设定的，比如在待配网设备重新接入 AP 后，待配网设备与配网设备之间的数据交互也可以使用该会话密钥 K_s 进行加密。

图 1 所示实施例仅是对密钥生成方法的原理进行了简单介绍，下面结合以下实施例对该密钥生成方法的一些具体的实现过程进行示例性说明。

图 2 为本申请一实施例提供的密钥生成方法的流程示意图，如图 2 所示，该密钥生成方法可以包括如下步骤：

201、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

本实施例中，可选地，在配网设备首次对待配网设备进行网络配置时，可以触发该 DPP 鉴权过程的执行。该 DPP 鉴权过程可以由待配网设备发起，也可以由配网设备发起。

在 DPP 鉴权过程中可以生成会话密钥 K_e (K_e 的生成属于现有技术，不展开赘述)，在后续第一次对待配网设备进行网络配置的过程中，可以使用该会话密钥 K_e 对待配网设备与配网设备之间的交互消息进行加密传输。

202、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

203、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密，第一应答消息中包括第一密钥信息。

204、待配网设备根据第一密钥信息生成会话密钥 K_s 。

205、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密，第一确认消息中包括第二密钥信息。

206、配网设备根据第二密钥信息生成会话密钥 K_s 。

5 上述步骤 201 至步骤 206 可以是在配网设备在首次对待配网设备进行网络配置的过程中执行。

其中，第一请求消息也可以称为 DPP 配置请求，可以表示为 DPP Configuration Request，其中携带有前文中所述的第一标识，可以表示为 SecondConfigStatus。

10 响应于该第一请求消息，配网设备向待配网设备发送第一应答消息，第一应答消息中包括第一密钥信息，该第一密钥信息可以是配网设备当前生成的公钥，该第一密钥信息可以表示为：Connector_{confc}。待配网设备根据 Connector_{confc} 生成会话密钥 K_s 的过程可以参见前述实施例中的说明。Connector 即为连接器。第一应答消息可以表示为 DPP configuration Response，从而，第一应答消息也可以称为第一 DPP 配置确认消息。

15 待配网设备若成功接收到第一应答消息，则可以向配网设备发送包含第二密钥信息的第一确认消息，第一确认消息可以表示为 DPP configuration confirm。其中，第二密钥信息可以是待配网设备当前生成的公私钥对中的公钥。该第一密钥信息可以表示为：Connector_{confe}。配网设备根据 Connector_{confe} 生成会话密钥 K_s 的过程可以参见前述实施例中的说明。

至此，在对待配网设备的第一次网络配置过程中，生成了用于对待配网设备进行网络重配置所需的会话密钥 K_s 。

20 207、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

208、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密。

209、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

25 其中，第二确认消息可以表示为 DPP configuration confirm，从而，第二应答消息也可以称为第二 DPP 配置确认消息。

上述步骤 207 至步骤 208 可以是在配网设备对待配网设备进行网络重配置的过程中执行。

30 实际应用中，AP 的 SSID 或接入密码往往是由于用户的手动更新而发生变化的，因此，用户在改变 AP 的 SSID 或接入密码后，可选地，可以对待配网设备施加触发操作，以触发待配网设备执行步骤 207。比如，待配网设备上可以设置有启动配网的按键，用

户按下这个按键，触发待配网设备执行步骤 207。

图 3 为本申请另一实施例提供的密钥生成方法的流程示意图，如图 3 所示，该密钥生成方法可以包括如下步骤：

301、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

5 302、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

303、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密。

10 304、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密，第一确认消息中包括第二密钥信息。

305、配网设备根据第二密钥信息生成会话密钥 K_s 。

可选地，第一应答消息中可以包括 AP 当前的第一网络配置信息，以使得待配网设备可以根据该第一网络配置信息接入 AP。

15 在一可选实施例中，待配网设备在接收到第一确认消息后，可以在预设时间间隔后向配网设备发送连接状态查询结果消息（可以表示为：Status Query Result），以告知配网设备该待配网设备与 AP 是否处于连接状态。基于此，可选地，待配网设备也可以将第二密钥信息携带在该连接状态报告信息中以发送至配网设备。

306、配网设备向待配网设备发送通知消息，通知消息用于使得待配网设备启动网络的重配置过程，通知消息中包括第一密钥信息，通知消息由 K_e 加密。

20 在步骤 306 中，当待配网设备不能接入 AP 时，会触发配网设备向该待配网设备发送该通知消息。可选地，当 AP 的网络配置信息发生改变时，用户可以通过操作配网设备扫描待配网设备上设置的二维码来触发配网设备向该待配网设备发送该通知消息。

值得说明的是，待配网设备往往是低功耗设备，为降低耗能，配置待配网设备工作于被动的监听模式，当发现连接不上 AP 后，以周期性监听配网设备发送的该通知消息。
25 如果待配网设备不是低功耗设备，则待配网设备可以在检测到不能接入 AP 时，直接退回到配置信道（configuration channel），并且在配置信道上周期性的发送 DPP 配置请求消息（即对应于下文中的第二请求消息），发送的 DPP 配置请求消息用 K_s 进行加密。

可选地，可以在通知消息中携带预设的第二标识，第二标识用于指示待配网设备启动网络的重配置过程。也就是说，当待配网设备接收到包含该第二标识的通知消息时，
30 启动网络重配置过程的执行，即下面步骤的执行。

307、待配网设备根据第一密钥信息生成会话密钥 K_s 。

308、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

309、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密。

5 310、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

由图 2 和图 3 所示实施例可知，上文中的第一密钥信息和第二密钥信息的发送时机并不严格限定，只要在重配置过程启动之前完成会话密钥 K_s 的生成即可。

图 2 和图 3 所示实施例中着重说明了在对待配网设备进行网络配置的过程中密钥生成方法如何执行，相对应地，当采用这种密钥生成方法时，终端配网方案可以参照如下

10 实施例实施。

图 4 为本申请一实施例提供的终端配网方法的流程示意图，如图 4 所示，该终端配网方法可以包括如下步骤：

401、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

402、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

403、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密，第一应答消息中包括第一密钥信息以及 AP 的第一网络配置信息。

404、待配网设备根据第一密钥信息生成会话密钥 K_s 。

20 405、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密，第一确认消息中包括第二密钥信息。

406、待配网设备根据第一网络配置信息接入 AP。

配网设备可以将当前 AP 的网络配置信息（称为第一网络配置信息）也携带在第一应答消息中传输给待配网设备。

25 待配网设备使用 K_e 解密得到该第一网络配置信息，进而接入 AP。

407、配网设备根据第二密钥信息生成会话密钥 K_s 。

408、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

409、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密，第二应答消息中包括 AP 的第二网络配置信息。

30 AP 的网络配置信息发生改变后，将此时 AP 的网络配置信息称为第二网络配置信息。

410、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

411、待配网设备根据会话密钥 K_s 解密出第二网络配置信息以接入 AP。

图 5 为本申请另一实施例提供的终端配网方法的流程示意图，如图 5 所示，该终端配网方法可以包括如下步骤：

5 501、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

502、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

503、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密，第一应答消息中包括第一密钥信息以及 AP 的第一网络配置信息。
10

504、待配网设备根据第一密钥信息生成会话密钥 K_s 。

505、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密。

506、待配网设备根据第一网络配置信息接入 AP。

15 507、待配网设备向配网设备发送连接状态查询结果消息，连接状态查询结果消息中包括第二密钥信息。

可以理解的是，连接状态查询结果消息中还可以包括指示待配网设备与 AP 是否处于连接状态的字段。

508、配网设备根据第二密钥信息生成会话密钥 K_s 。

20 509、配网设备向待配网设备发送通知消息，通知消息中包括第二标识，以用于使得待配网设备启动网络的重配置过程，通知消息由会话密钥 K_s 加密。

510、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

511、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密，第二应答消息中包括 AP 的第二网络配置信息。

25 第二网络配置信息中包括 SSID 以及 SSID 对应的接入密码。其中，第二网络配置信息中的 SSID 和/或接入密码与第一网络配置信息中包括的 SSID 以及接入密码不同。

512、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

513、待配网设备根据会话密钥 K_s 解密出第二网络配置信息以接入 AP。

30 图 6 为本申请另一实施例提供的终端配网方法的流程示意图，如图 6 所示，该终端配网方法可以包括如下步骤：

601、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

602、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

5 603、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密，第一应答消息中包括 AP 的第一网络配置信息。

604、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密。

605、待配网设备根据第一网络配置信息接入 AP。

10 606、待配网设备向配网设备发送连接状态查询结果消息，连接状态查询结果消息中包括第二密钥信息，连接状态查询结果消息由 K_e 加密。

607、配网设备根据第二密钥信息生成会话密钥 K_s 。

608、配网设备向待配网设备发送通知消息，通知消息中包括第二标识和第一密钥信息，以用于使得待配网设备启动网络的重配置过程，通知消息由 K_e 加密。

609、待配网设备根据第一密钥信息生成会话密钥 K_s 。

15 610、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

611、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密，第二应答消息中包括 AP 的第二网络配置信息。

612、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

613、待配网设备根据会话密钥 K_s 解密出第二网络配置信息以接入 AP。

20 图 7 为本申请另一实施例提供的终端配网方法的流程示意图，如图 7 所示，该终端配网方法可以包括如下步骤：

701、待配网设备与配网设备通过 DPP 鉴权过程生成初始的会话密钥 K_e 。

702、待配网设备向配网设备发送第一请求消息，第一请求消息由 K_e 加密，第一请求消息中包括第一标识，第一标识用于指示配网设备进行网络的重配置操作。

25 703、配网设备根据第一标识向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消息由 K_e 加密，第一应答消息中包括 AP 的第一网络配置信息。

704、待配网设备向配网设备发送与第一应答消息对应的第一确认消息，第一确认消息由 K_e 加密，第一确认消息中包括第二密钥信息。

705、待配网设备根据第一网络配置信息接入 AP。

30 706、配网设备根据第二密钥信息生成会话密钥 K_s 。

707、待配网设备向配网设备发送连接状态查询结果消息。

708、配网设备向待配网设备发送通知消息，通知消息中包括第二标识和第一密钥信息，第二标识用于使得待配网设备启动网络的重配置过程，通知消息由 K_e 加密。

709、待配网设备根据第一密钥信息生成会话密钥 K_s 。

5 710、待配网设备向配网设备发送第二请求消息，第二请求消息由会话密钥 K_s 加密。

711、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由会话密钥 K_s 加密，第二应答消息中包括 AP 的第二网络配置信息。

712、待配网设备向配网设备发送第二确认消息，第二确认消息由会话密钥 K_s 加密。

713、待配网设备根据会话密钥 K_s 解密出第二网络配置信息以接入 AP。

10 综上，以上各个实施例提供了一种新的 DPP 配置过程的实现方案。在该方案下，待配网设备和配网设备在第一次网络配置过程中互相交换在后续第二次重新配网过程中所需的密钥信息：上述第一密钥信息和第二密钥信息，以使得配网设备和待配网设备都生成在下一次网络重配过程中所需使用的会话密钥 K_s ，如此，在网络重配过程中，直接基于会话密钥 K_s 执行 DPP 配置过程即可，无需再次执行 DPP 鉴权过程，提高了配网效率。

15 以上各实施例中提供的方案主要涉及的是 DPP 配置过程。下面，本申请实施例还提供一种在 DPP 鉴权过程中实施的密钥生成方法。

图 8 为本申请另一实施例提供的密钥生成方法的流程示意图，如图 8 所示，该密钥生成方法包括如下步骤：

801、配网设备向待配网设备发送认证请求消息，认证请求消息中包括第一随机数信息
20 和第二随机数信息。

802、待配网设备根据第一随机数信息、第二随机数信息以及待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥。

803、待配网设备向配网设备发送与认证请求消息对应的认证应答消息，认证应答消息中包括第三随机数信息和第四随机数信息。

25 804、配网设备根据第一随机数信息、第二随机数信息以及第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥。

下面为描述方便，将第一随机数信息和第二随机数信息分别表示为： $I\text{-nonce1}$ 和 $I\text{-nonce2}$ ，将第三随机数信息和第四随机数信息分别表示为： $R\text{-nonce1}$ 和 $R\text{-nonce2}$ ，将第一会话密钥和第二会话密钥分别表示为： $ke1$ 和 $ke2$ 。

30 本实施例提供的密钥生成方法可以适用于配网设备对待配网设备进行网络配置的场

景中。

可选地，可以在待配网设备上设置一个二维码，当需要对待配网设备进行网络配置时，通过扫描该二维码可以触发配网设备向待配网设备发送上述认证请求消息。

值得说明的是，本实施例中，是以配网设备主动触发了 DPP 鉴权过程为例进行的说明，实际上，DPP 鉴权过程也可以由待配网设备触发。此时，待配网设备向配网设备发送包含自己的第三随机数信息和第四随机数信息的认证请求消息（可以表示为 DPP authentication request），配网设备向待配网设备发送包括自己的第一随机数信息和第二随机数信息的认证应答消息（可以表示为 DPP authentication response）。此时，可选地，在待配网设备上可以设置触发配网的按键，当用户按下该按键时，可以触发待配网设备向配网设备发送认证请求消息。

可以理解的是，对于配网设备和待配网设备来说，都会得到上述四个随机数：I-nonce1、I-nonce2、R-nonce1 和 R-nonce2。

概括来说，对配网设备来说，其可以根据 I-nonce1 和 R-nonce1 生成 ke1，以及根据 I-nonce2 和 R-nonce2 生成 ke2。同样地，对于待配网设备来说，也可以根据 I-nonce1 和 R-nonce1 生成 ke1，以及根据 I-nonce2 和 R-nonce2 生成 ke2。

值得说明的是，待配网设备可以被配置为：当接收到包括 I-nonce1 和 I-nonce2 两个随机数的认证请求消息时，即得知需要生成两个会话密钥，其中，一个被用在配网设备对待配网设备的首次网络配置过程中，另一个被用在配网设备对待配网设备的网络重配置过程中。假设 ke1 被用在配网设备对待配网设备的首次网络配置过程中，ke2 被用在配网设备对待配网设备的网络重配置过程中。

当然，可选地，上述认证请求消息中可以包括预设的第一标识，第一标识指示待配网设备生成用于进行网络重配置的会话密钥。也就是说，可以在认证请求消息中携带该第一标识，以使待配网设备接收到包含该第一标识的认证请求消息时，直接得知需要生成两个会话密钥：ke1 和 ke2。也即是说，待配网设备基于该第一标识得知，除了需要生成被用在配网设备对待配网设备的首次网络配置过程中的会话密钥 ke1 外，还需要生成被用在配网设备对待配网设备的网络重配置过程中的会话密钥 ke2。

下面对 ke1 和 ke2 的详细生成过程进行说明。

对于待配网设备来说：

$$Ke1 = HKDF(I-nonce1 \parallel R-nonce1, \text{“DPP Re-configuration Key”}, M.x \parallel N.x \parallel L.x);$$
$$Ke2 = HKDF(I-nonce2 \parallel R-nonce2, \text{“DPP Re-configuration Key”}, M.x \parallel N.x \parallel L.x)。$$

其中, $M.x$ 表示 M 的标量, x 可以是 M 这个复数在椭圆曲线上对应的横坐标, M 是由配网设备的协议密钥 (protocol key) 对中的公钥 P_1 以及待配网设备中的引导密钥 (bootstrapping key) 对中的私钥 b_R 生成的, 生成公式为:

$$M = b_R \times P_1。$$

5 其中, $N.x$ 表示 N 的标量, x 可以是 N 这个复数在椭圆曲线上对应的横坐标, N 是由配网设备的协议密钥 (protocol key) 对中的公钥 P_1 以及待配网设备中的协议密钥 (protocol key) 对中的私钥 p_R 生成的, 生成公式为:

$$N = p_R \times P_1。$$

10 其中, $L.x$ 表示 L 的标量, x 可以是 L 这个复数在椭圆曲线上对应的横坐标, L 是由待配网设备中的引导密钥 (bootstrapping key) 对中的私钥 b_R 以及待配网设备中的协议密钥 (protocol key) 对中的私钥 p_R 以及配网设备中的引导密钥 (bootstrapping key) 对中的公钥 B_1 生成的, 生成公式为:

$$L = ((b_R + p_R) \text{ modulo } q) \times B_1$$

15 其中, $|$ 表示拼接 (串联) 操作, “DPP Re-configuration Key” 表示此处是一串字符串, 该字符串的取值可以自定义。 $[]$ 表示该中括号中的变量或字段 $L.x$ 是可选的或者只有在特定条件下才使用。modulo q 表示模运算。

对于配网设备来说:

$$Ke1 = HKDF(I\text{-}nonce1|R\text{-}nonce1, \text{“DPP Re-configuration Key”}, M.x|N.x[|L.x]);$$

$$Ke2 = HKDF(I\text{-}nonce2|R\text{-}nonce2, \text{“DPP Re-configuration Key”}, M.x|N.x[|L.x])。$$

20 其中, M 是由配网设备的协议密钥 (protocol key) 对中的私钥 p_1 以及待配网设备中的引导密钥 (bootstrapping key) 对中的公钥 B_R 生成的, 生成公式为:

$$M = p_1 \times B_R。$$

其中, N 是由配网设备的协议密钥 (protocol key) 对中的私钥 p_1 以及待配网设备中的协议密钥 (protocol key) 对中的公钥 P_R 生成的, 生成公式为:

$$25 \quad N = p_1 \times P_R。$$

其中, L 是由配网设备中的引导密钥 (bootstrapping key) 对中的私钥 b_1 以及待配网设备中的协议密钥 (protocol key) 对中的公钥 P_R 以及待配网设备中的引导密钥 (bootstrapping key) 对中的公钥 B_R 生成的, 生成公式为:

$$L = b_1 \times (B_R + P_R)。$$

30 值得说明的是, 对于配网设备和待配网设备来说, 上述公式中涉及到的 M 、 N 、 L 的

计算方式是不相同的。

可选地，DPP 认证请求消息中还可以包括生成会话密钥数量的信息。重配网可能需要进行多于 2 次。因此，配网设备以及待配网设备可以在 DPP 鉴权过程中生成 2 个以上的会话密钥。例如，如果生成会话密钥数量的信息为 3，则配网设备在向待配网设备中
5 发送的 DPP 鉴权请求信息中携带 3 个随机数，依次是 I-nonce1, I-nonce2 以及 I-nonce3。待配网设备收到配网设备发送的 DPP 鉴权请求消息后，会根据收到的 3 个随机数以及自身生成的 3 个随机数 R-nonce1, R-nonce2 以及 R-nonce3 依次生成 3 个会话密钥 Ke1, Ke2 以及 Ke3。之后，待配网设备向配网设备发送 DPP 鉴权答复消息，DPP 鉴权答复消息中包括 R-nonce1, R-nonce2 以及 R-nonce3。配网设备收到待配网设备发送的 DPP 鉴权
10 应答消息后，会根据收到的 3 个随机数以及之前生成的 3 个随机数 I-nonce1, I-nonce2 以及 I-nonce3 依次生成 3 个会话密钥 Ke1, Ke2 以及 Ke3。三个会话密钥依次用于第一次配置过程，第二次配置过程以及第三次配置过程。配网设备和待配网设备在接收以及发送配置过程中的连接状态查询结果消息后，会删除当下配网过程中所用到的会话密钥。

在配网设备对待配网设备进行网络配置的场景中，上述生成的 ke1 和 ke2 可以被用于后续两个 DPP 配置过程中。下面结合图 9 所示实施例对 ke1 和 ke2 的使用过程进行说明。

图 9 为本申请一实施例提供的使用 ke1 和 ke2 进行网络配置的流程示意图，如图 9 所示，包括如下步骤：

901、待配网设备与配网设备在 DPP 鉴权过程中生成第一会话密钥 ke1 和第二会话密
20 钥 ke2。

其中，ke1 和 ke2 的生成过程参见图 8 所示实施例中的说明，在此不赘述。

902、待配网设备向配网设备发送第一请求消息，第一请求消息由第一会话密钥 ke1 加密。

903、配网设备向待配网设备发送与第一请求消息对应的第一应答消息，第一应答消
25 息由第一会话密钥 ke1 加密，第一应答消息中包括 AP 的第一网络配置信息。

904、待配网设备向配网设备发送第一确认消息，第一确认消息由第一会话密钥 ke1 加密。

905、待配网设备使用第一会话密钥 ke1 解密出第一网络配置信息以接入 AP。

906、待配网设备向配网设备发送连接状态查询结果消息，连接状态查询结果消息由
30 第一会话密钥 ke1 加密。

可选地，待配网设备在接收到第一确认消息后，可以在预设时间间隔后向配网设备发送连接状态查询结果消息（可以表示为：Status Query Result），以告知配网设备该待配网设备与 AP 是否处于连接状态。

5 907、配网设备向待配网设备发送通知消息，通知消息用于使得待配网设备启动网络的重配置过程，通知消息由第二会话密钥 ke2 加密。

如前文所述，当 AP 的网络配置信息由第一网络配置信息变为第二网络配置信息时，且当待配网设备为低功耗设备时，可以触发配网设备向待配网设备发送该通知消息。

可选地，AP 的网络配置信息发生改变时，用户可以操作配网设备扫描待配网设备上的二维码，以触发配网设备向待配网设备发送该通知消息。

10 值得说明的是，待配网设备往往是低功耗设备，为降低耗能，配置待配网设备工作于被动的监听模式，当发现连接不上 AP 后，以周期性监听配网设备发送的该通知消息。如果待配网设备不是低功耗设备，则待配网设备可以在检测到不能接入 AP 时，直接退回到配置信道（configuration channel），并且在配置信道上周期性的发送 DPP 配置请求消息（即对应于下文中的第二请求消息），发送的 DPP 配置请求消息用 Ks 进行加
15 密。

可选地，上述通知消息中可以包括第二标识，第二标识用于指示待配网设备启动网络的重配置过程。

908、待配网设备向配网设备发送第二请求消息，第二请求消息由第二会话密钥 ke2 加密。

20 909、配网设备向待配网设备发送与第二请求消息对应的第二应答消息，第二应答消息由第二会话密钥 ke2 加密，第二应答消息中包括 AP 的第二网络配置信息。

910、待配网设备向配网设备发送第二确认消息，第二确认消息由第二会话密钥 ke2 加密。

911、待配网设备使用第二会话密钥 ke2 解密出第二网络配置信息以接入 AP。

25 以下将详细描述本申请的一个或多个实施例的密钥生成装置、终端配网装置。本领域技术人员可以理解，这些装置均可使用市售的硬件组件通过本方案所教导的步骤进行配置来构成。

图 10 为本申请实施例提供的一种密钥生成装置的结构示意图，如图 10 所示，该装置包括：发送模块 11、接收模块 12、生成模块 13。

发送模块 11，用于向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作。

接收模块 12，用于接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息。

5 生成模块 13，用于根据所述第一密钥信息生成会话密钥。

所述发送模块 11，还用于向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥。

可选地，所述第一消息是与所述第一请求消息对应的第一应答消息。

可选地，所述第二消息是与所述第一应答消息对应的第一确认消息。

10 可选地，所述第一消息是通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程。

可选地，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

可选地，在向所述配网设备发送第二消息之后，所述发送模块 11 还用于：向所述配网设备发送第二请求消息，所述第二请求消息由所述会话密钥加密。所述接收模块 12 还用于：接收所述配网设备发送的与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述会话密钥加密。

可选地，接收所述配网设备发送的与所述第二请求消息对应的第二应答消息之后，所述发送模块 11 还用于：向所述配网设备发送第二确认消息，所述第二确认消息由所述会话密钥加密。

图 10 所示装置可以执行前述图 1 至图 3 所示各实施例中待配网设备所执行的步骤，本实施例未详细描述的部分，可参考前述实施例的相关说明，在此不再赘述。

在一个可能的设计中，上述图 10 所示的密钥生成装置的结构可实现为待配网设备。如图 11 所示，该待配网设备可以包括：第一处理器 21、第一存储器 22。其中，所述第
25 一存储器 22 上存储有可执行代码，当所述可执行代码被所述第一处理器 21 执行时，至少使所述第一处理器 21 实现前述图 1 至图 3 所示实施例中待配网设备所执行的各步骤。

其中，该待配网设备的结构中还可以包括第一通信接口 23，用于与其他设备或通信网络通信。

另外，本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被待配网设备的处理器执行时，使
30

所述处理器执行前述图 1 至图 3 所示实施例中的待配网设备所执行的各步骤。

图 12 为本申请实施例提供的另一种密钥生成装置的结构示意图，如图 12 所示，该装置包括：接收模块 31、发送模块 32、生成模块 33。

接收模块 31，用于接收待配网设备发送的第一请求消息，所述第一请求消息中包括
5 第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作。

发送模块 32，用于根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥。

所述接收模块 31，还用于接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息。

10 生成模块 33，用于根据所述第二密钥信息生成所述会话密钥。

可选地，所述第一消息是与所述第一请求消息对应的第一应答消息。

可选地，所述第二消息是与所述第一应答消息对应的第一确认消息。

可选地，所述第一消息是通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程。

15 可选地，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

可选地，根据所述第二密钥信息生成所述会话密钥之后，所述接收模块 31 还用于：接收所述待配网设备发送的第二请求消息，所述第二请求消息由所述会话密钥加密。所述发送模块 32 还用于：向所述待配网设备发送与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述会话密钥加密。所述接收模块 31 还用于：接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述会话密钥加密。
20

图 12 所示装置可以执行前述图 1 至图 3 所示实施例中配网设备所执行的步骤，本实施例未详细描述的部分，可参考前述实施例的相关说明，在此不再赘述。

在一个可能的设计中，上述图 12 所示的密钥生成装置的结构可实现为配网设备。如图 13 所示，该配网设备可以包括：第二处理器 41、第二存储器 42。其中，所述第二存储器 42 上存储有可执行代码，当所述可执行代码被所述第二处理器 41 执行时，至少使所述第二处理器 41 实现前述图 1 至图 3 所示实施例中配网设备所执行的各步骤。其中，该配网设备的结构中还可以包括第二通信接口 43，用于与其他设备或通信网络通信。
25

另外，本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被配网设备的处理器执行时，使所
30

述处理器执行前述图 1 至图 3 所示实施例中的配网设备所执行的各步骤。

图 14 为本申请实施例提供的一种终端配网装置的结构示意图,该终端配网配置装置位于待配网设备中。如图 14 所示,该装置包括:发送模块 51、接收模块 52、生成模块 53。

5 发送模块 51,用于向配网设备发送第一请求消息,所述第一请求消息中包括第一标识,所述第一标识用于指示所述配网设备进行网络的重配置操作。

接收模块 52,用于接收所述配网设备发送的第一消息,所述第一消息中包括第一密钥信息。

生成模块 53,用于根据所述第一密钥信息生成会话密钥。

10 所述发送模块 51,还用于向所述配网设备发送第二消息,所述第二消息中包括第二密钥信息,以使所述配网设备根据所述第二密钥信息生成所述会话密钥;所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

可选地,所述第一消息是与所述第一请求消息对应的第一应答消息。

可选地,所述第二消息是与所述第一应答消息对应的第一确认消息。

15 可选地,向配网设备发送第一请求消息之后,所述接收模块 52 还用于:接收所述配网设备发送的与所述第一请求消息对应的第一应答消息,第一应答消息中包括接入点的第一网络配置信息。

可选地,所述发送模块 51 还用于:向所述配网设备发送连接状态查询结果消息,所述第二消息是所述连接状态查询结果消息。

20 可选地,向所述配网设备发送连接状态查询结果消息之后,所述接收模块 52 还用于:接收所述配网设备发送的通知消息,所述通知消息用于使得所述待配网设备启动网络的重配置过程,所述第一消息是所述通知消息。

可选地,所述发送模块 51 还用于:向所述配网设备发送第二请求消息,所述第二请求消息由所述会话密钥加密。所述接收模块 52 还用于:接收所述配网设备发送的与所述
25 第二请求消息对应的第二应答消息,所述第二应答消息中包括接入点的第二网络配置信息,所述第二应答消息由所述会话密钥加密。所述发送模块 51 还用于:向所述配网设备发送第二确认消息,所述第二确认消息由所述会话密钥加密。

图 14 所示装置可以执行前述图 4 至图 7 所示实施例中待配网设备所执行的步骤,本实施例未详细描述的部分,可参考前述实施例的相关说明,在此不再赘述。

30 在一个可能的设计中,上述图 14 所示的终端配网装置的结构可实现为待配网设备。

如图 15 所示, 该待配网设备可以包括: 第三处理器 61、第三存储器 62。其中, 所述第三存储器 62 上存储有可执行代码, 当所述可执行代码被所述第三处理器 61 执行时, 至少使所述第三处理器 61 实现前述图 4 至图 7 所示实施例中待配网设备所执行的各步骤。

其中, 该待配网设备的结构中还可以包括第三通信接口 63, 用于与其他设备或通信网络通信。

另外, 本申请实施例提供了一种非暂时性机器可读存储介质, 所述非暂时性机器可读存储介质上存储有可执行代码, 当所述可执行代码被待配网设备的处理器执行时, 使所述处理器执行前述图 4 至图 7 所示实施例中的待配网设备所执行的各步骤。

图 16 为本申请实施例提供的另一种终端配网装置的结构示意图, 位于待入网设备中, 如图 16 所示, 该装置包括: 接收模块 71、发送模块 72、生成模块 73。

接收模块 71, 用于接收待配网设备发送的第一请求消息, 所述第一请求消息中包括第一标识, 所述第一标识用于指示所述配网设备进行网络的重配置操作。

发送模块 72, 用于根据所述第一标识向所述待配网设备发送第一消息, 所述第一消息中包括第一密钥信息, 以使所述待配网设备根据所述第一密钥信息生成会话密钥。

所述接收模块 71, 还用于接收所述待配网设备发送的第二消息, 所述第二消息中包括第二密钥信息。

生成模块 73, 用于根据所述第二密钥信息生成所述会话密钥; 所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

可选地, 所述第一消息是与所述第一请求消息对应的第一应答消息。

可选地, 所述第二消息是与所述第一应答消息对应的第一确认消息。

可选地, 所述发送模块 72 还用于: 向所述待配网设备发送与所述第一请求消息对应的第一应答消息, 第一应答消息中包括接入点的第一网络配置信息。

可选地, 向所述待配网设备发送与所述第一请求消息对应的第一应答消息之后, 所述接收模块 71 还用于: 接收所述待配网设备发送的连接状态查询结果消息, 所述第二消息是所述连接状态查询结果消息。所述发送模块 72 还用于: 向所述待配网设备发送通知消息, 所述通知消息用于使得所述待配网设备启动网络的重配置过程, 所述第一消息是所述通知消息。

可选地, 所述接收模块 71 还用于: 接收所述待配网设备发送的第二请求消息, 所述第二请求消息由所述会话密钥加密。所述发送模块 72 还用于: 向所述待配网设备发送与所述第二请求消息对应的第二应答消息, 所述第二应答消息由所述会话密钥加密, 所述

第二应答消息中包括接入点的第二网络配置信息。所述接收模块 71 还用于：接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述会话密钥加密。

图 16 所示装置可以执行前述图 4 至图 7 所示实施例中配网设备所执行的步骤，本实施例未详细描述的部分，可参考前述实施例的相关说明，在此不再赘述。

5 在一个可能的设计中，上述图 16 所示的终端配网装置的结构可实现为配网设备。如图 17 所示，该配网设备可以包括：第四处理器 81、第四存储器 82。其中，所述第四存储器 82 上存储有可执行代码，当所述可执行代码被所述第四处理器 81 执行时，至少使所述第四处理器 81 实现前述图 4 至图 7 所示实施例中配网设备所执行的各步骤。

10 其中，该配网设备的结构中还可以包括第四通信接口 83，用于与其他设备或通信网络通信。

另外，本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被配网设备的处理器执行时，使所述处理器执行前述图 4 至图 7 所示实施例中的配网设备所执行的各步骤。

15 图 18 为本申请实施例提供的另一种密钥生成装置的结构示意图，如图 18 所示，该装置包括：接收模块 91、生成模块 92、发送模块 93。

接收模块 91，用于接收配网设备发送的认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息。

生成模块 92，用于根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥。

20 发送模块 93，用于向所述配网设备发送与所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息，以使所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成所述第一会话密钥和所述第二会话密钥。

25 可选地，所述认证请求消息中包括第一标识，所述第一标识指示所述待配网设备生成用于进行网络重配置的会话密钥。

30 可选地，所述发送模块 93 还用于：向所述配网设备发送第一请求消息，所述第一请求消息由所述第一会话密钥加密。所述接收模块 91 还用于：接收所述配网设备发送的与所述第一请求消息对应的第一应答消息，所述第一应答消息由所述第一会话密钥加密，所述第一应答消息中包括接入点的第一网络配置信息。所述发送模块 93 还用于：向所述配网设备发送第一确认消息，所述第一确认消息由所述第一会话密钥加密。

可选地，所述发送模块 93 还用于：向所述配网设备发送连接状态查询结果消息，所述连接状态查询结果消息由所述第一会话密钥加密。

可选地，所述接收模块 91 还用于：接收所述配网设备发送的通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述通知消息由所述第二会话密钥加密。

其中，可选地，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

可选地，接收所述配网设备发送的通知消息之后，所述发送模块 93 还用于：向所述配网设备发送第二请求消息，所述第二请求消息由所述第二会话密钥加密。所述接收模块 91 还用于：接收所述配网设备发送的与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述第二会话密钥加密，所述第二应答消息中包括接入点的第二网络配置信息。所述发送模块 93 还用于：向所述配网设备发送第二确认消息，所述第二确认消息由所述第二会话密钥加密。

图 18 所示装置可以执行前述图 8 至图 9 所示各实施例中待配网设备所执行的步骤，本实施例未详细描述的部分，可参考前述实施例的相关说明，在此不再赘述。

在一个可能的设计中，上述图 18 所示的密钥生成装置的结构可实现为待配网设备。如图 19 所示，该待配网设备可以包括：第五处理器 191、第五存储器 192。其中，所述第五存储器 192 上存储有可执行代码，当所述可执行代码被所述第五处理器 191 执行时，至少使所述第五处理器 191 实现前述图 8 至图 9 所示实施例中待配网设备所执行的各步骤。

其中，该待配网设备的结构中还可以包括第五通信接口 193，用于与其他设备或通信网络通信。

另外，本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被待配网设备的处理器执行时，使所述处理器执行前述图 8 至图 9 所示实施例中的待配网设备所执行的各步骤。

图 20 为本申请实施例提供的另一种密钥生成装置的结构示意图，如图 20 所示，该装置包括：发送模块 2001、接收模块 2002、生成模块 2003。

发送模块 2001，用于向待配网设备发送认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息，以使所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一

会话密钥和第二会话密钥。

接收模块 2002，用于接收所述待配网设备发送的所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息。

生成模块 2003，用于根据所述第一随机数信息、所述第二随机数信息以及所述第三
5 随机数信息和所述第四随机数信息生成第一会话密钥和第二会话密钥。

可选地，所述认证请求消息中包括第一标识，所述第一标识指示所述待配网设备生成用于进行网络重配置的会话密钥。

可选地，所述接收模块 2002 还用于：接收所述待配网设备发送的第一请求消息，所述
10 第一请求消息由所述第一会话密钥加密。所述发送模块 2001 还用于：向所述待配网设备发送与所述第一请求消息对应的第一应答消息，所述第一应答消息由所述第一会话密钥加密，所述第一应答消息中包括接入点的第一网络配置信息。所述接收模块 2002 还用于：接收所述待配网设备发送的第一确认消息，所述第一确认消息由所述第一会话密钥加密。

可选地，向所述待配网设备发送与所述第一请求消息对应的第一应答消息之后，所
15 述接收模块 2002 还用于：所述配网设备接收所述待配网设备发送的连接状态查询结果消息，所述连接状态查询结果消息由所述第一会话密钥加密。

可选地，所述发送模块 2001 还用于：向所述待配网设备发送通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述通知消息由所述第二会话密钥加密。

20 其中，可选地，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

可选地，发送通知消息之后，所述接收模块 2002 还用于：所述配网设备接收所述待配网设备发送的第二请求消息，所述第二请求消息由所述第二会话密钥加密。所述发送模块 2001 还用于：向所述待配网设备发送与所述第二请求消息对应的第二应答消息，所
25 述第二应答消息由所述第二会话密钥加密，所述第二应答消息中包括接入点的第二网络配置信息。所述接收模块 2002 还用于：接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述第二会话密钥加密。

图 20 所示装置可以执行前述图 8 至图 9 所示实施例中配网设备所执行的步骤，本实施例未详细描述的部分，可参考前述实施例的相关说明，在此不再赘述。

30 在一个可能的设计中，上述图 20 所示的密钥生成装置的结构可实现为配网设备。如

图 21 所示，该配网设备可以包括：第六处理器 2101、第六存储器 2102。其中，所述第六存储器 2102 上存储有可执行代码，当所述可执行代码被所述第六处理器 2101 执行时，至少使所述第六处理器 2101 实现前述图 8 至图 9 所示实施例中配网设备所执行的各步骤。

5 其中，该配网设备的结构中还可以包括第六通信接口 2103，用于与其他设备或通信网络通信。

另外，本申请实施例提供了一种非暂时性机器可读存储介质，所述非暂时性机器可读存储介质上存储有可执行代码，当所述可执行代码被配网设备的处理器执行时，使所述处理器执行前述图 8 至图 9 所示实施例中的配网设备所执行的各步骤。

10 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

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各实施方式可借助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和软件结合的方式来实现。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以计算机产品的形式体现出来，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

20 本申请实施例提供的网络配置方法可以由某一种或多种程序/软件来执行，该程序/软件可以由网络侧提供，前述实施例中提及的配网设备、待配网设备可以将所需的相应程序/软件下载到本地的非易失性存储介质中，并在其需要执行前述密钥生成方法、终端配网方法时，通过 CPU 将该程序/软件读取到内存中，进而由 CPU 执行该程序/软件以实现前述实施例中所提供的密钥生成方法、终端配网方法，执行过程可以参见前述图 1 至
25 图 9 中的示意。

最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

30

权 利 要 求 书

1、一种密钥生成方法，其特征在于，包括：

待配网设备向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

5 所述待配网设备接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

所述待配网设备根据所述第一密钥信息生成会话密钥；

所述待配网设备向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥。

10 2、根据权利要求 1 所述的方法，其特征在于，所述第一消息是与所述第一请求消息对应的第一应答消息。

3、根据权利要求 2 所述的方法，其特征在于，所述第二消息是与所述第一应答消息对应的第一确认消息。

15 4、根据权利要求 1 所述的方法，其特征在于，所述第一消息是通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程。

5、根据权利要求 4 所述的方法，其特征在于，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

6、根据权利要求 1 所述的方法，其特征在于，所述待配网设备向所述配网设备发送第二消息之后，还包括：

20 所述待配网设备向所述配网设备发送第二请求消息，所述第二请求消息由所述会话密钥加密；

所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述会话密钥加密。

25 7、根据权利要求 6 所述的方法，其特征在于，所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息之后，还包括：

所述待配网设备向所述配网设备发送第二确认消息，所述第二确认消息由所述会话密钥加密。

8、一种密钥生成方法，其特征在于，包括：

30 配网设备接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

所述配网设备根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述配网设备接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

5 所述配网设备根据所述第二密钥信息生成所述会话密钥。

9、根据权利要求 8 所述的方法，其特征在于，所述第一消息是与所述第一请求消息对应的第一应答消息。

10、根据权利要求 9 所述的方法，其特征在于，所述第二消息是与所述第一应答消息对应的第一确认消息。

10 11、根据权利要求 8 所述的方法，其特征在于，所述第一消息是通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程。

12、根据权利要求 11 所述的方法，其特征在于，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

15 13、根据权利要求 8 所述的方法，其特征在于，所述配网设备根据所述第二密钥信息生成所述会话密钥之后，还包括：

所述配网设备接收所述待配网设备发送的第二请求消息，所述第二请求消息由所述会话密钥加密；

所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述会话密钥加密。

20 14、根据权利要求 13 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息之后，还包括：

所述配网设备接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述会话密钥加密。

15、一种终端配网方法，其特征在于，包括：

25 待配网设备向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

所述待配网设备接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

所述待配网设备根据所述第一密钥信息生成会话密钥；

30 所述待配网设备向所述配网设备发送第二消息，所述第二消息中包括第二密钥信

息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥；所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

16、根据权利要求 15 所述的方法，其特征在于，所述第一消息是与所述第一请求消息对应的第一应答消息。

5 17、根据权利要求 16 所述的方法，其特征在于，所述第二消息是与所述第一应答消息对应的第一确认消息。

18、根据权利要求 15 所述的方法，其特征在于，所述待配网设备向配网设备发送第一请求消息之后，还包括：

10 所述待配网设备接收所述配网设备发送的与所述第一请求消息对应的第一应答消息，第一应答消息中包括接入点的第一网络配置信息。

19、根据权利要求 18 所述的方法，其特征在于，所述方法还包括：

所述待配网设备向所述配网设备发送连接状态查询结果消息，所述第二消息是所述连接状态查询结果消息。

15 20、根据权利要求 19 所述的方法，其特征在于，所述待配网设备向所述配网设备发送连接状态查询结果消息之后，还包括：

所述待配网设备接收所述配网设备发送的通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述第一消息是所述通知消息。

21、根据权利要求 15 至 20 中任一项所述的方法，其特征在于，所述方法还包括：

20 所述待配网设备向所述配网设备发送第二请求消息，所述第二请求消息由所述会话密钥加密；

所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息，所述第二应答消息中包括接入点的第二网络配置信息，所述第二应答消息由所述会话密钥加密。

25 22、根据权利要求 21 所述的方法，其特征在于，所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息之后，还包括：

所述待配网设备向所述配网设备发送第二确认消息，所述第二确认消息由所述会话密钥加密。

23、一种终端配网方法，其特征在于，包括：

30 配网设备接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

所述配网设备根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述配网设备接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

5 所述配网设备根据所述第二密钥信息生成所述会话密钥，所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

24、根据权利要求 23 所述的方法，其特征在于，所述第一消息是与所述第一请求消息对应的第一应答消息。

25、根据权利要求 24 所述的方法，其特征在于，所述第二消息是与所述第一应答
10 消息对应的第一确认消息。

26、根据权利要求 23 所述的方法，其特征在于，所述配网设备接收待配网设备发送的第一请求消息之后，还包括：

所述配网设备向所述待配网设备发送与所述第一请求消息对应的第一应答消息，第一应答消息中包括接入点的第一网络配置信息。

15 27、根据权利要求 26 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第一请求消息对应的第一应答消息之后，还包括：

所述配网设备接收所述待配网设备发送的连接状态查询结果消息，所述第二消息是所述连接状态查询结果消息。

28、根据权利要求 27 所述的方法，其特征在于，所述配网设备接收所述待配网设备
20 发送的连接状态查询结果消息之后，还包括：

所述配网设备向所述待配网设备发送通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述第一消息是所述通知消息。

29、根据权利要求 23 至 28 中任一项所述的方法，其特征在于，所述方法还包括：

所述配网设备接收所述待配网设备发送的第二请求消息，所述第二请求消息由所述
25 会话密钥加密；

所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述会话密钥加密，所述第二应答消息中包括接入点的第二网络配置信息。

30 30、根据权利要求 29 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息之后，还包括：

所述配网设备接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述会话密钥加密。

31、一种密钥生成装置，其特征在于，位于待配网设备中，包括：

发送模块，用于向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，

5 所述第一标识用于指示所述配网设备进行网络的重配置操作；

接收模块，用于接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

生成模块，用于根据所述第一密钥信息生成会话密钥；

所述发送模块，还用于向所述配网设备发送第二消息，所述第二消息中包括第二密
10 钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥。

32、一种密钥生成装置，其特征在于，位于配网设备中，包括：

接收模块，用于接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

发送模块，用于根据所述第一标识向所述待配网设备发送第一消息，所述第一消息
15 中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

所述接收模块，还用于接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

生成模块，用于根据所述第二密钥信息生成所述会话密钥。

33、一种待配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上
20 存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利要求 1 至 7 中任一项所述的密钥生成方法。

34、一种配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利要求 8 至 14 中任一项所述的密钥生成方法。

25 35、一种终端配网装置，其特征在于，位于待配网设备中，包括：

发送模块，用于向配网设备发送第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

接收模块，用于接收所述配网设备发送的第一消息，所述第一消息中包括第一密钥信息；

30 生成模块，用于根据所述第一密钥信息生成会话密钥；

所述发送模块，还用于向所述配网设备发送第二消息，所述第二消息中包括第二密钥信息，以使所述配网设备根据所述第二密钥信息生成所述会话密钥；

所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

36、一种终端配网装置，其特征在于，位于配网设备中，包括：

5 接收模块，用于接收待配网设备发送的第一请求消息，所述第一请求消息中包括第一标识，所述第一标识用于指示所述配网设备进行网络的重配置操作；

发送模块，用于根据所述第一标识向所述待配网设备发送第一消息，所述第一消息中包括第一密钥信息，以使所述待配网设备根据所述第一密钥信息生成会话密钥；

10 所述接收模块，还用于接收所述待配网设备发送的第二消息，所述第二消息中包括第二密钥信息；

生成模块，用于根据所述第二密钥信息生成所述会话密钥；所述会话密钥被用于对所述待配网设备进行网络的重配置的过程中。

37、一种待配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利要求 15 至 22 中任一项所述的终端配网方法。

38、一种配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利要求 23 至 30 中任一项所述的终端配网方法。

39、一种密钥生成方法，其特征在于，包括：

20 待配网设备接收配网设备发送的认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息；

所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

25 所述待配网设备向所述配网设备发送与所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息，以使所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成所述第一会话密钥和所述第二会话密钥。

40、根据权利要求 39 所述的方法，其特征在于，所述认证请求消息中包括第一标识，所述第一标识指示所述待配网设备生成用于进行网络重配置的会话密钥。

30 41、根据权利要求 39 所述的方法，其特征在于，所述待配网设备向所述配网设备

发送与所述认证请求消息对应的认证应答消息之后，还包括：

所述待配网设备向所述配网设备发送第一请求消息，所述第一请求消息由所述第一会话密钥加密；

5 所述待配网设备接收所述配网设备发送的与所述第一请求消息对应的第一应答消息，所述第一应答消息由所述第一会话密钥加密，所述第一应答消息中包括接入点的第一网络配置信息。

42、根据权利要求 41 所述的方法，其特征在于，所述待配网设备接收所述配网设备发送的与所述第一请求消息对应的第一应答消息之后，还包括：

10 所述待配网设备向所述配网设备发送第一确认消息，所述第一确认消息由所述第一会话密钥加密。

43、根据权利要求 41 所述的方法，其特征在于，所述方法还包括：

所述待配网设备向所述配网设备发送连接状态查询结果消息，所述连接状态查询结果消息由所述第一会话密钥加密。

44、根据权利要求 39 至 43 中任一项所述的方法，其特征在于，所述方法还包括：

15 所述待配网设备接收所述配网设备发送的通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述通知消息由所述第二会话密钥加密。

45、根据权利要求 44 所述的方法，其特征在于，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

20 46、根据权利要求 44 所述的方法，其特征在于，所述待配网设备接收所述配网设备发送的通知消息之后，还包括：

所述待配网设备向所述配网设备发送第二请求消息，所述第二请求消息由所述第二会话密钥加密；

25 所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述第二会话密钥加密，所述第二应答消息中包括接入点的第二网络配置信息。

47、根据权利要求 46 所述的方法，其特征在于，所述待配网设备接收所述配网设备发送的与所述第二请求消息对应的第二应答消息之后，还包括：

所述待配网设备向所述配网设备发送第二确认消息，所述第二确认消息由所述第二会话密钥加密。

30 48、一种密钥生成方法，其特征在于，包括：

配网设备向待配网设备发送认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息，以使所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

- 5 所述配网设备接收所述待配网设备发送的所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息；

所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成第一会话密钥和第二会话密钥。

- 49、根据权利要求 48 所述的方法，其特征在于，所述认证请求消息中包括第一标识，所述第一标识指示所述待配网设备生成用于进行网络重配置的会话密钥。

50、根据权利要求 48 所述的方法，其特征在于，所述方法还包括：

所述配网设备接收所述待配网设备发送的第一请求消息，所述第一请求消息由所述第一会话密钥加密；

- 15 所述配网设备向所述待配网设备发送与所述第一请求消息对应的第一应答消息，所述第一应答消息由所述第一会话密钥加密，所述第一应答消息中包括接入点的第一网络配置信息。

51、根据权利要求 50 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第一请求消息对应的第一应答消息之后，还包括：

- 20 所述配网设备接收所述待配网设备发送的第一确认消息，所述第一确认消息由所述第一会话密钥加密。

52、根据权利要求 50 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第一请求消息对应的第一应答消息之后，还包括：

所述配网设备接收所述待配网设备发送的连接状态查询结果消息，所述连接状态查询结果消息由所述第一会话密钥加密。

- 25 53、根据权利要求 48 至 52 中任一项所述的方法，其特征在于，所述方法还包括：

所述配网设备向所述待配网设备发送通知消息，所述通知消息用于使得所述待配网设备启动网络的重配置过程，所述通知消息由所述第二会话密钥加密。

54、根据权利要求 53 所述的方法，其特征在于，所述通知消息中包括第二标识，所述第二标识用于指示所述待配网设备启动网络的重配置过程。

- 30 55、根据权利要求 53 所述的方法，其特征在于，所述配网设备向所述待配网设备

发送通知消息之后，还包括：

所述配网设备接收所述待配网设备发送的第二请求消息，所述第二请求消息由所述第二会话密钥加密；

5 所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息，所述第二应答消息由所述第二会话密钥加密，所述第二应答消息中包括接入点的第二网络配置信息。

56、根据权利要求 55 所述的方法，其特征在于，所述配网设备向所述待配网设备发送与所述第二请求消息对应的第二应答消息之后，还包括：

10 所述配网设备接收所述待配网设备发送的第二确认消息，所述第二确认消息由所述第二会话密钥加密。

57、一种密钥生成装置，其特征在于，位于待配网设备，包括：

接收模块，用于接收配网设备发送的认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息；

15 生成模块，用于根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

发送模块，用于向所述配网设备发送与所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息，以使所述配网设备根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成所述第一会话密钥和所述第二会话密钥。

20 58、一种密钥生成装置，其特征在于，位于配网设备，包括：

发送模块，用于向待配网设备发送认证请求消息，所述认证请求消息中包括第一随机数信息和第二随机数信息，以使所述待配网设备根据所述第一随机数信息、所述第二随机数信息以及所述待配网设备对应的第三随机数信息和第四随机数信息生成第一会话密钥和第二会话密钥；

25 接收模块，用于接收所述待配网设备发送的所述认证请求消息对应的认证应答消息，所述认证应答消息中包括所述第三随机数信息和所述第四随机数信息；

生成模块，用于根据所述第一随机数信息、所述第二随机数信息以及所述第三随机数信息和所述第四随机数信息生成第一会话密钥和第二会话密钥。

30 59、一种待配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利

要求 39 至 47 中任一项所述的密钥生成方法。

60、一种配网设备，其特征在于，包括：存储器、处理器；其中，所述存储器上存储有可执行代码，当所述可执行代码被所述处理器执行时，使所述处理器执行如权利要求 48 至 56 中任一项所述的密钥生成方法。

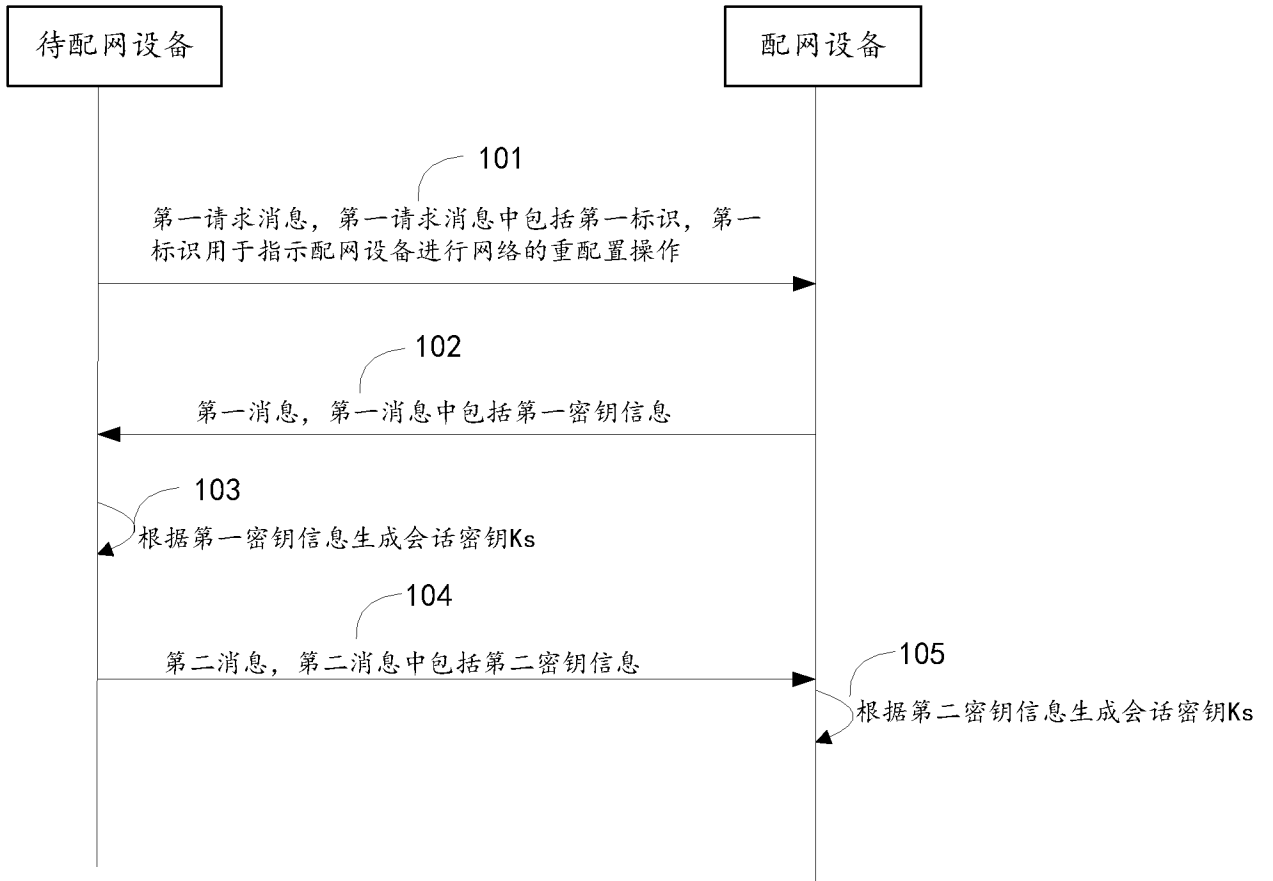


图 1

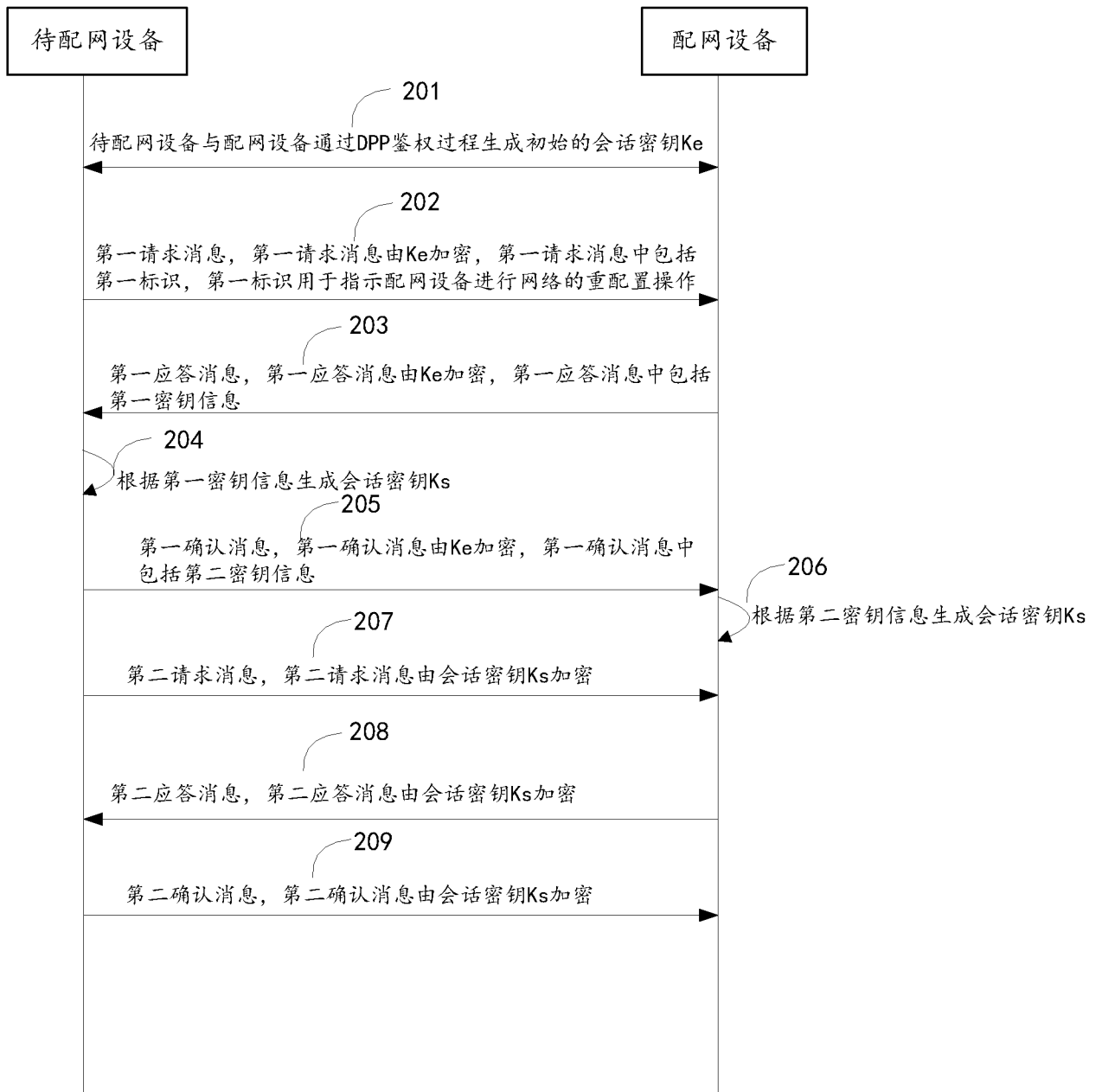


图 2

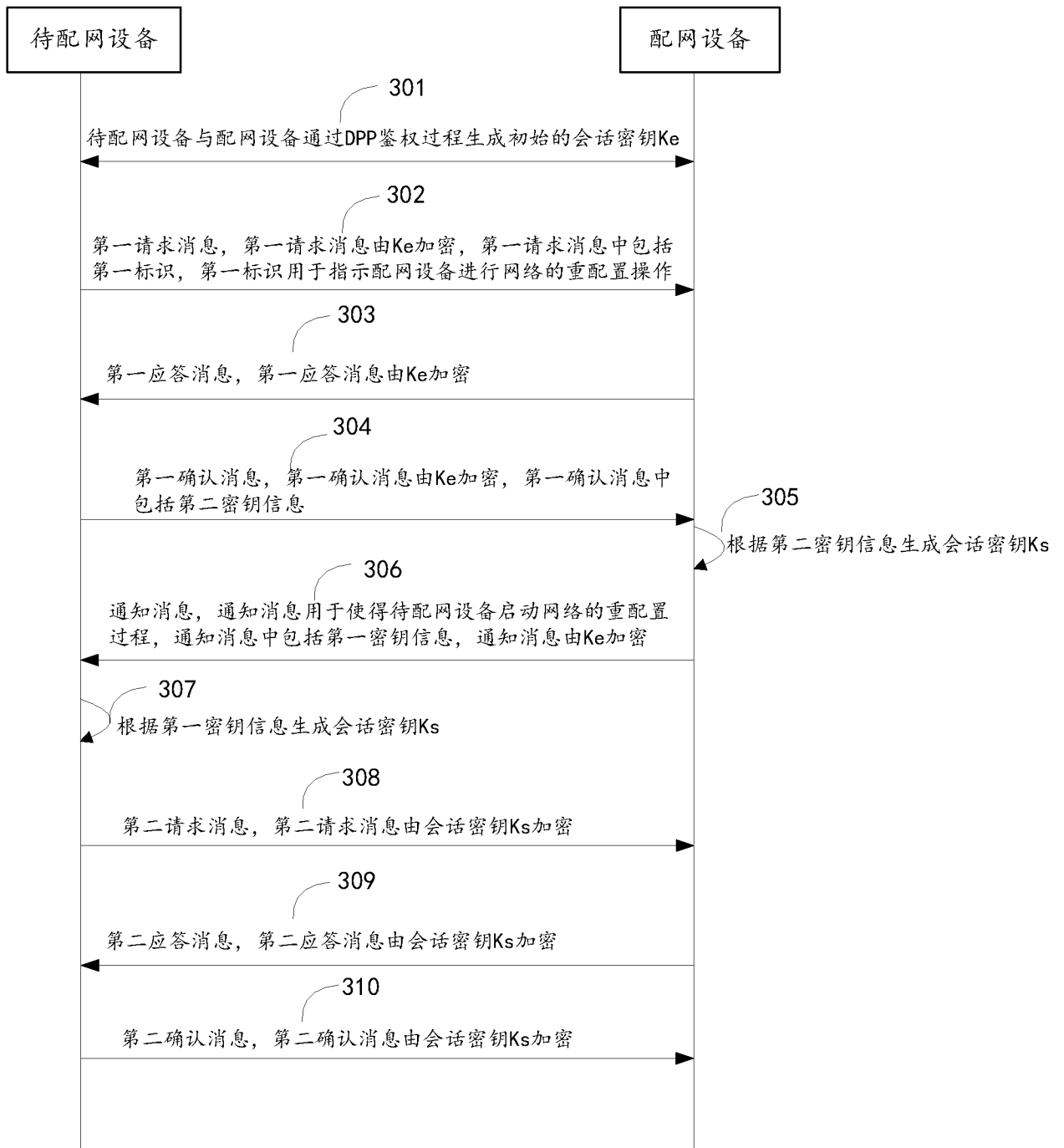


图 3

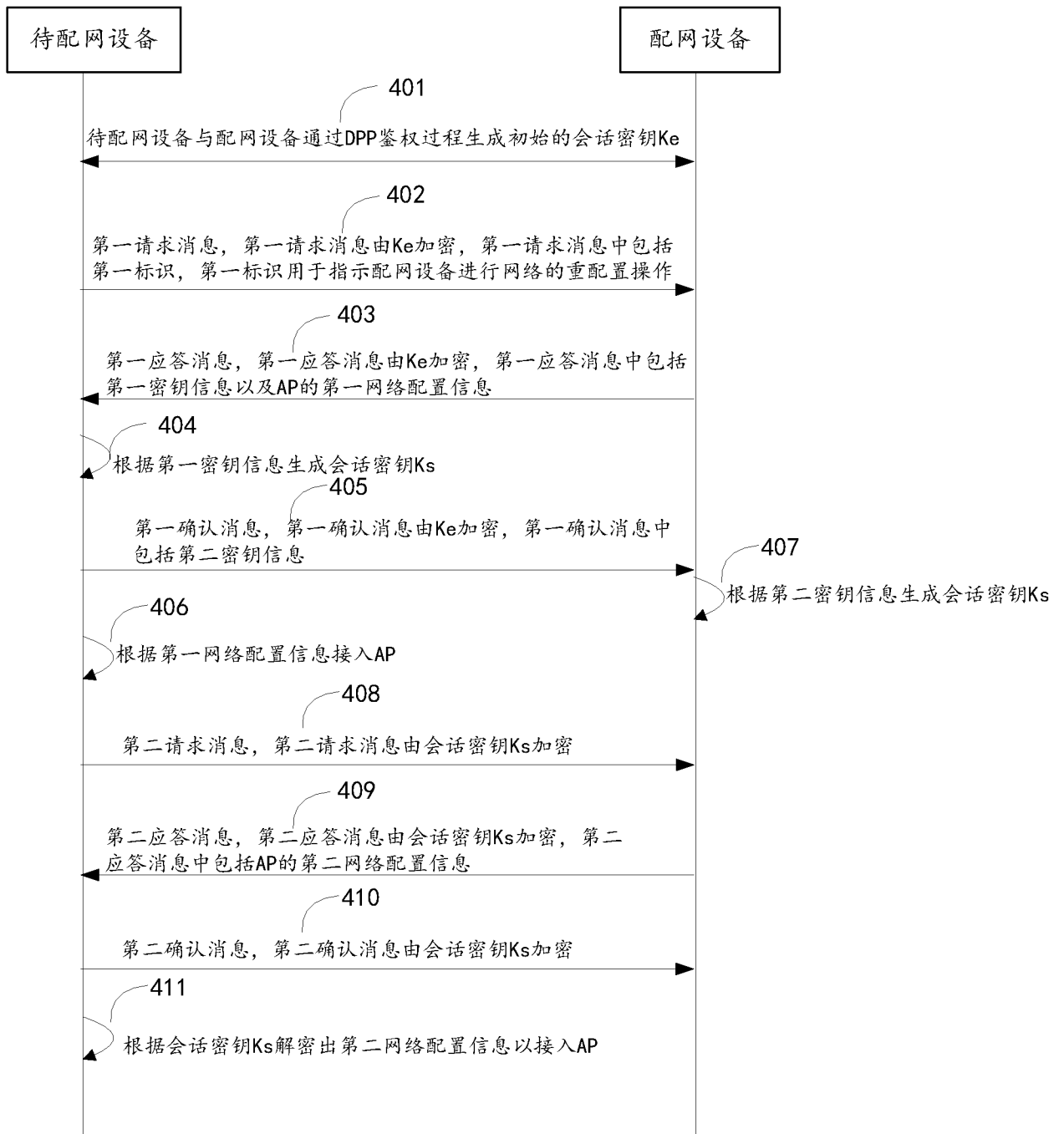


图 4

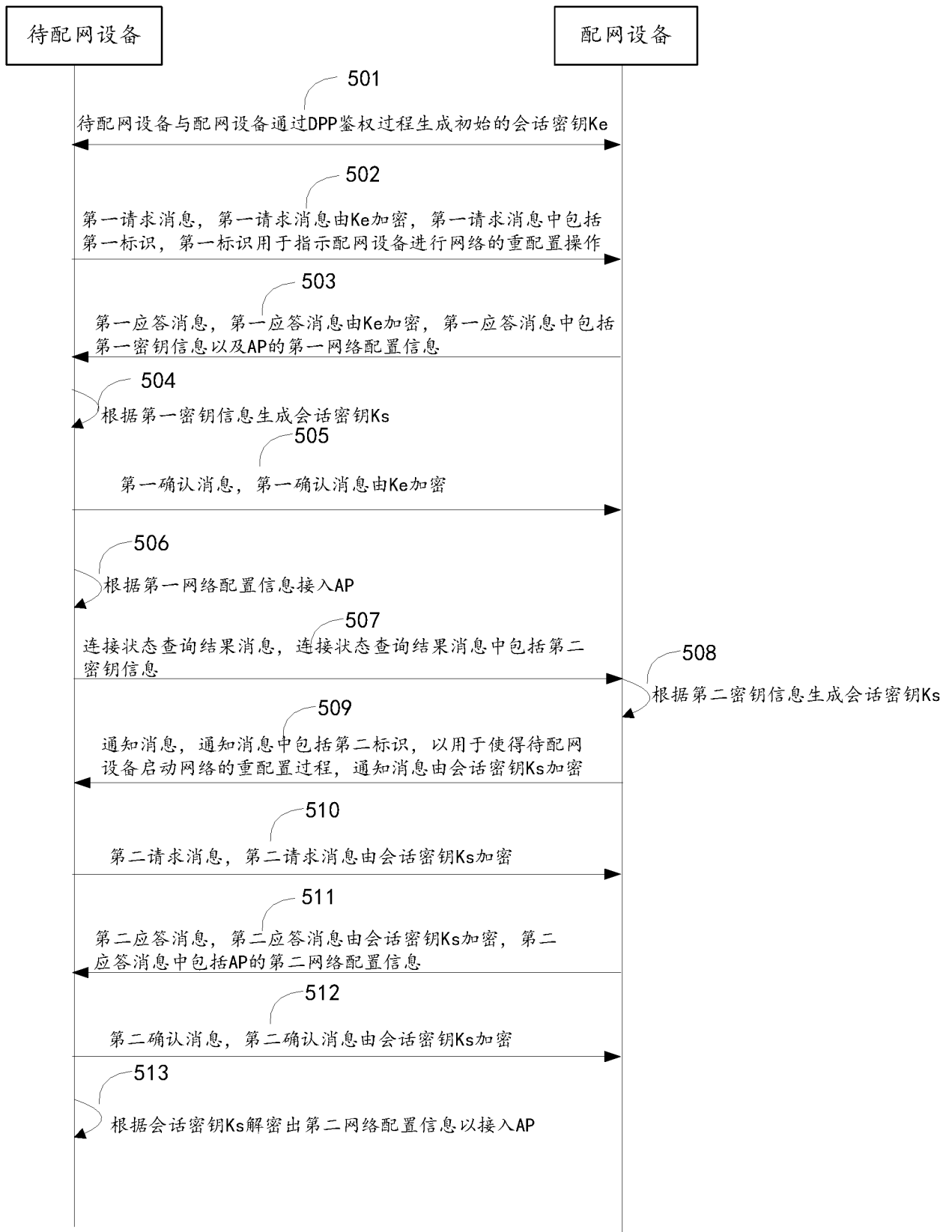


图 5

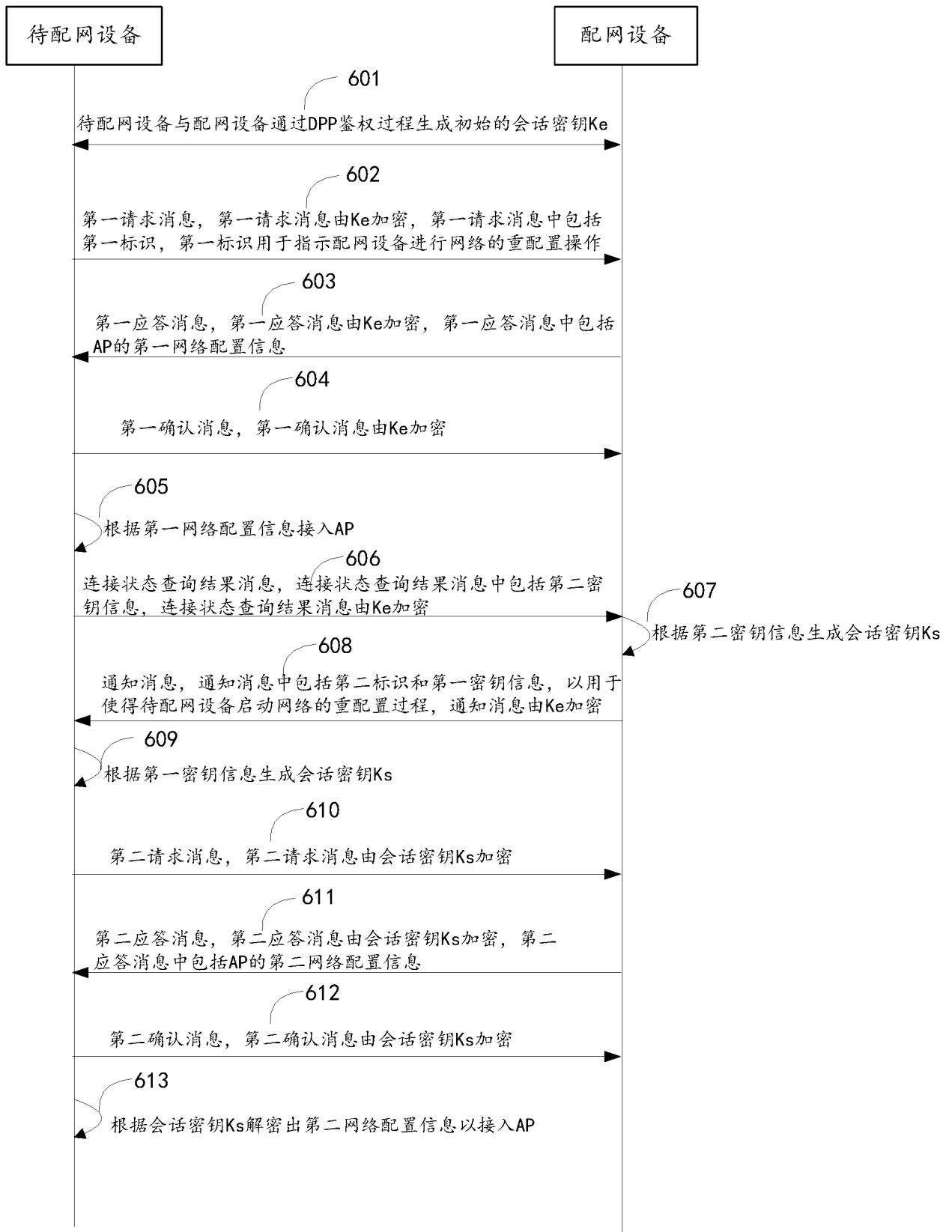


图 6

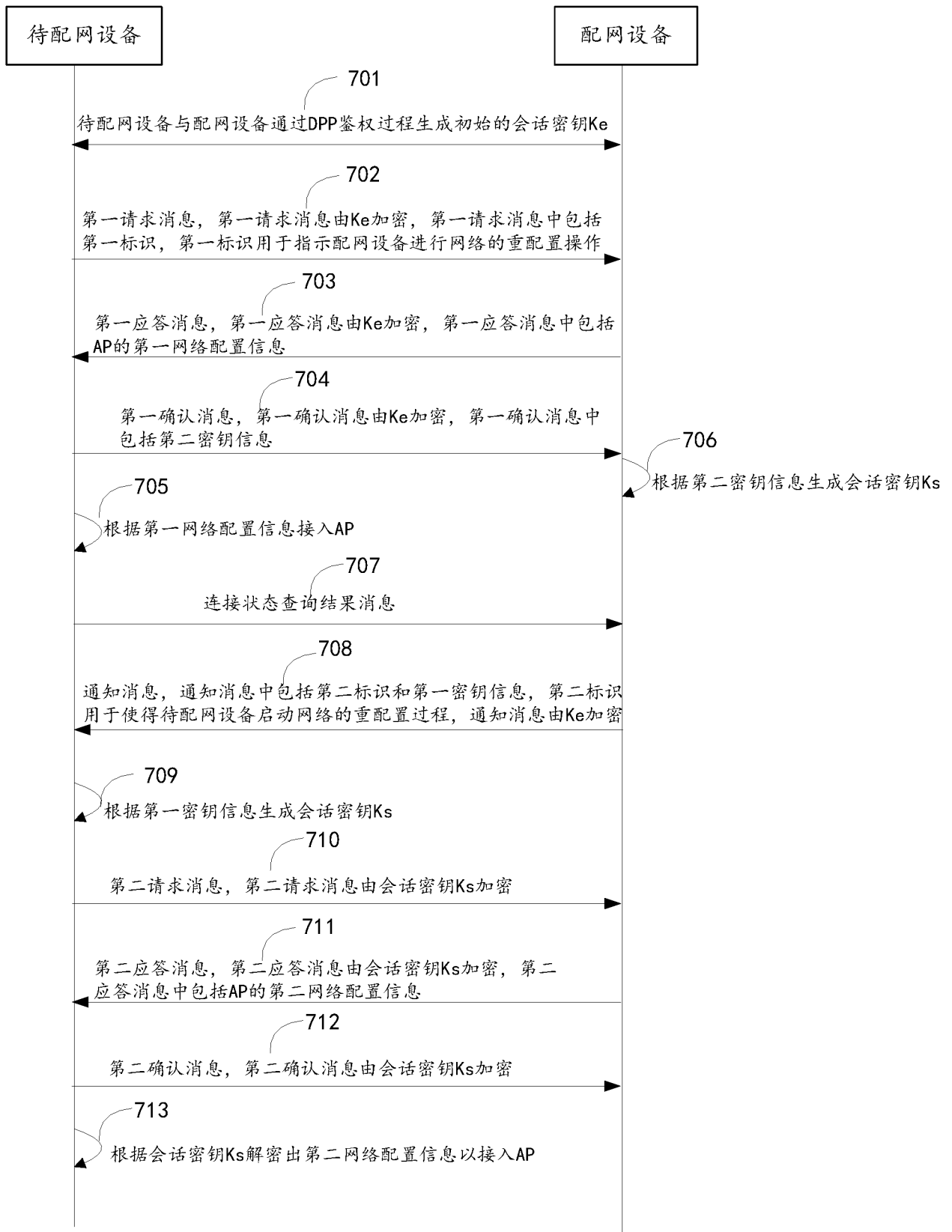


图 7

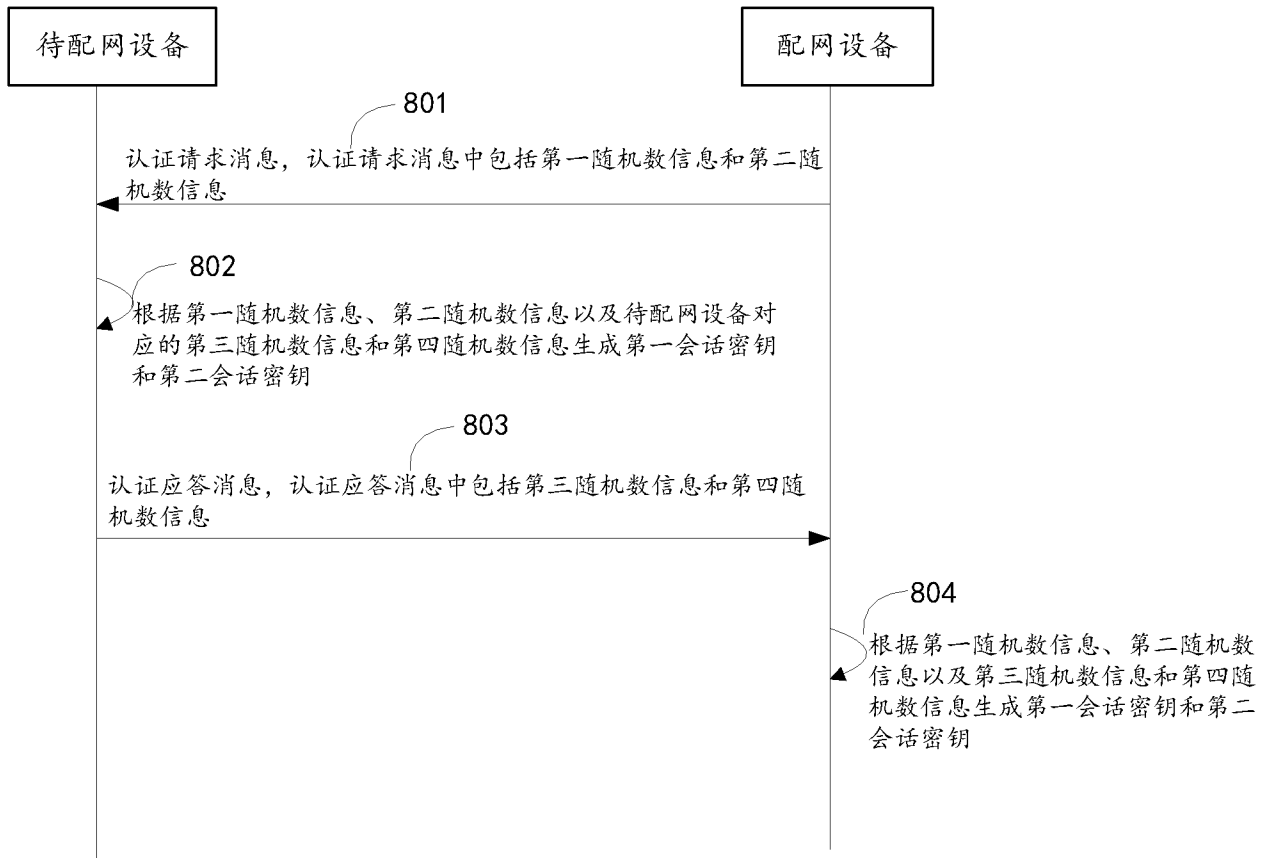


图 8

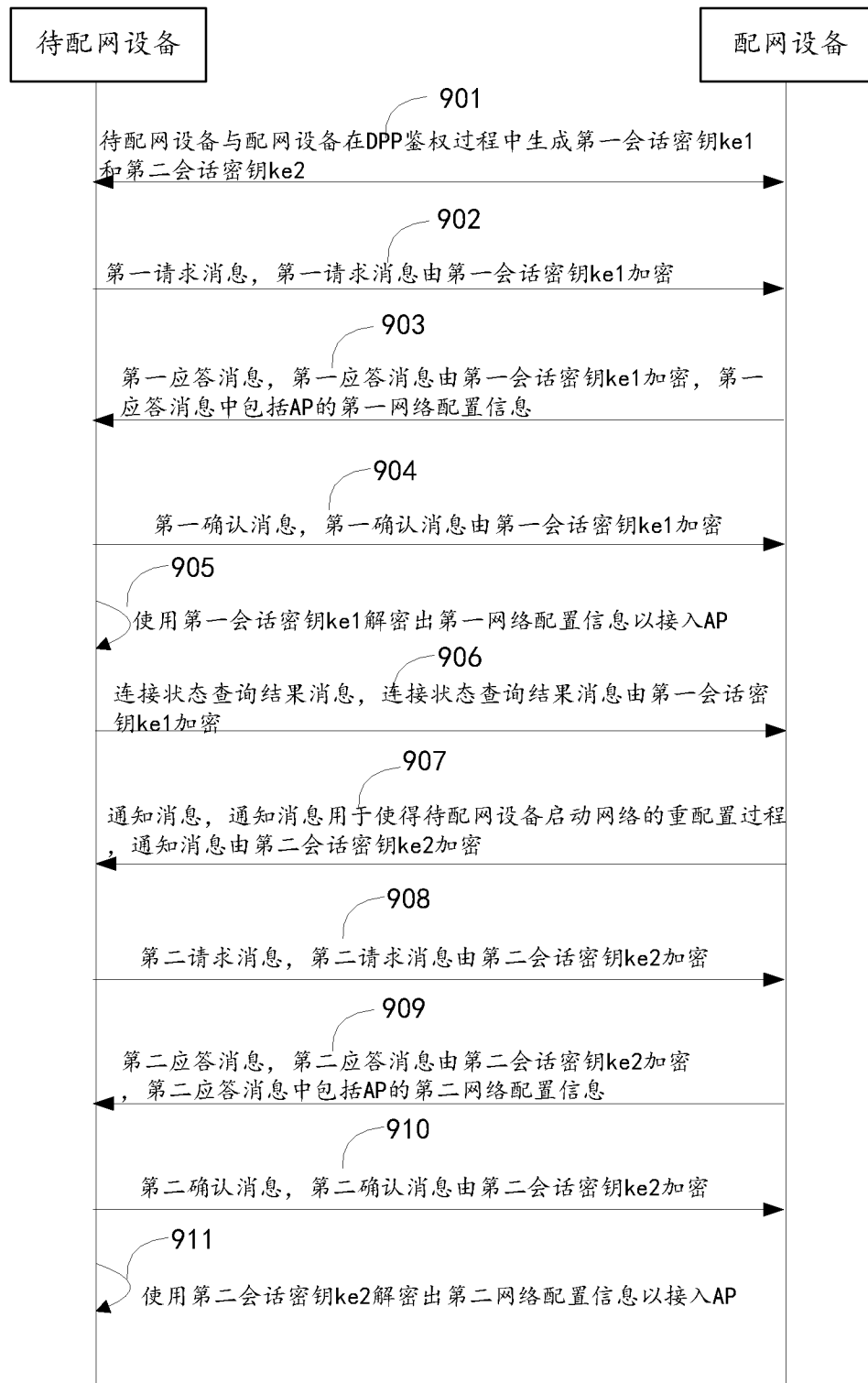


图 9

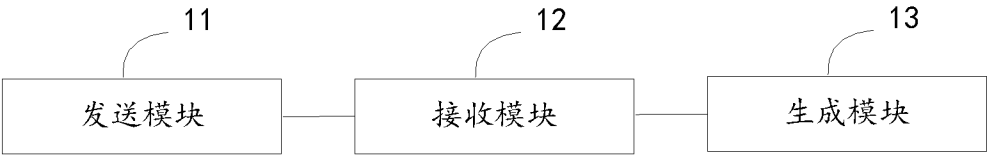


图 10

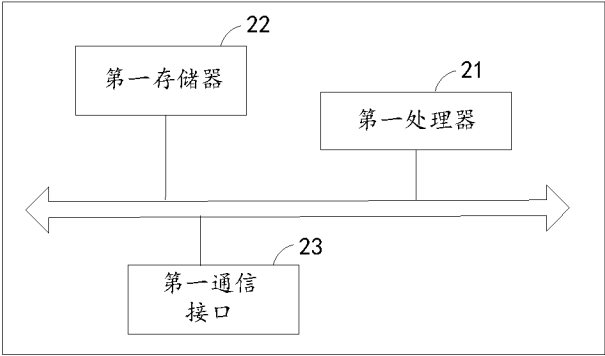


图 11

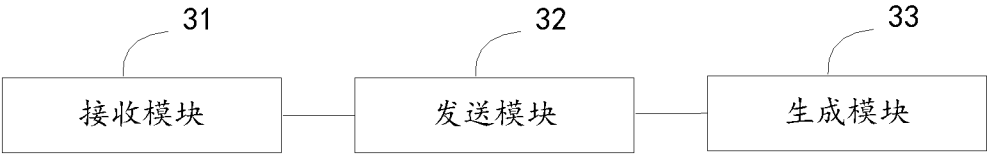


图 12

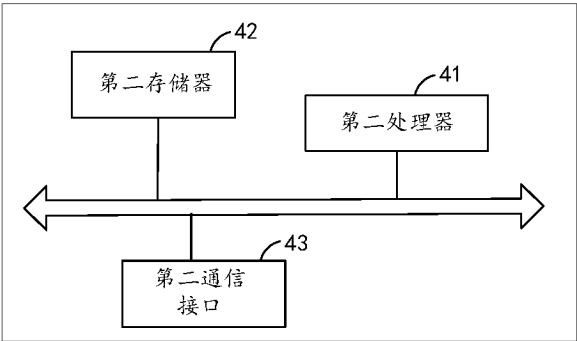


图 13

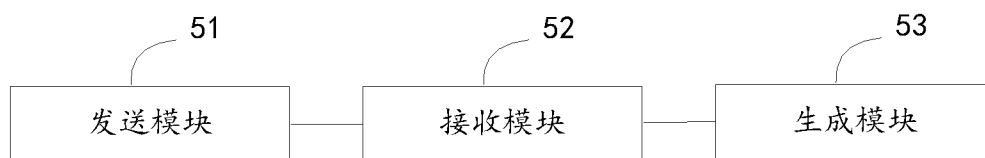


图 14

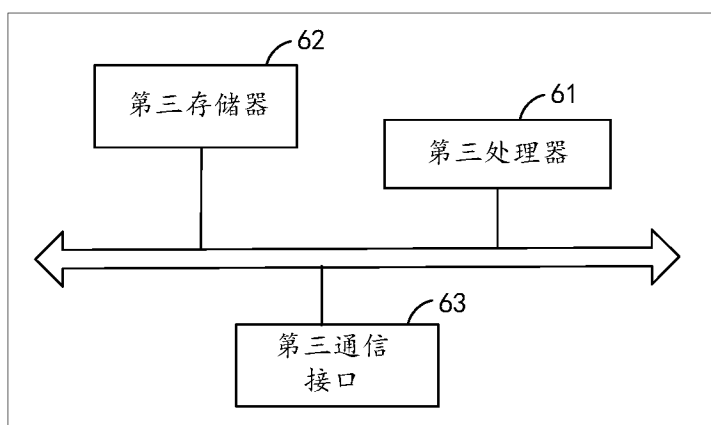


图 15

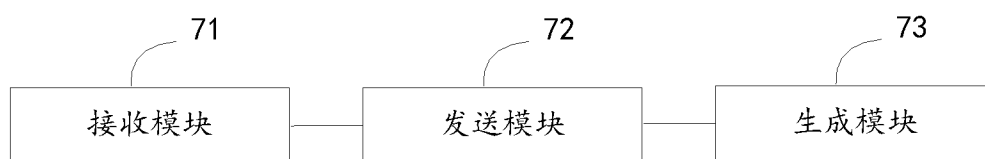


图 16

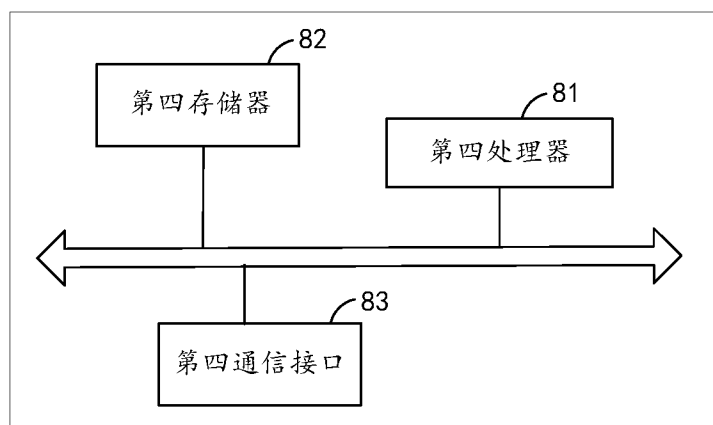


图 17

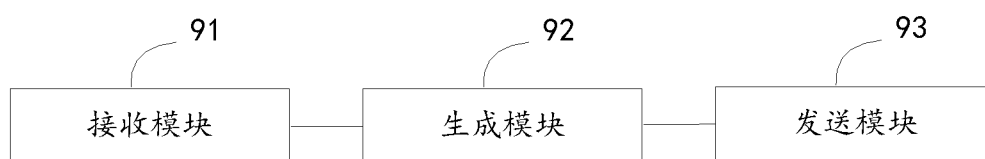


图 18

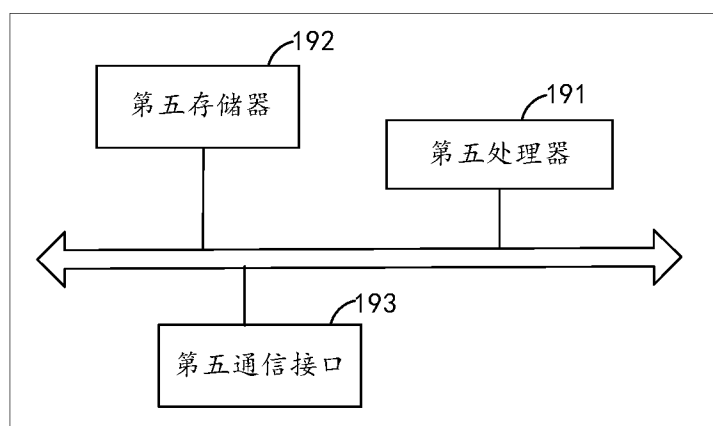


图 19



图 20

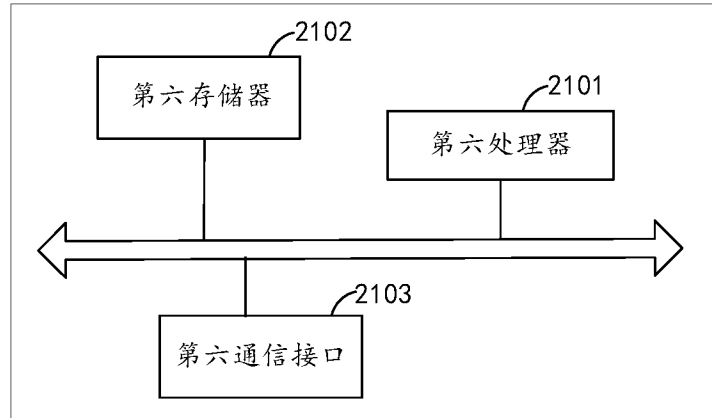


图 21

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/112415

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04W 12/04(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)

CNPAT, CNKI, WPI, EPODOC, IEEE: 装置配置协议, DPP配置请求, 设备配置协议, 终端配网协议, DPP, 密钥, 公钥, 重配置, 待配网设备, 配网设备, 配置者, 随机数, device, provisioning, protocol, request, reconfig+, enrollee, connector, wi?fi, configurator, random, nonce, public, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	WI-FI ALLIANCE. "DRAFT Device Provisioning Protocol Specification Version 1.2" https://www.wi-fi.org/download.php?file=/sites/default/files/private/DRAFT%20Device_Provisioning_Protocol_Specification_v1.2_0.pdf , 03 March 2020 (2020-03-03), chapters 2-8	1-60
Y	WI-FI ALLIANCE. "Device Provisioning Protocol Specification Version 1.1" https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf/35330 , 03 December 2018 (2018-12-03), chapters 2-8	1-60
Y	FISH_OU. "(non-official translation: Diffie Hellman (DH) Key Exchange and ECDH (quote))" https://www.cnblogs.com/fishou/p/4206451.html , 06 January 2015 (2015-01-06), entire document	1-60
A	CN 110115099 A (CANON KK) 09 August 2019 (2019-08-09) entire document	1-60
A	WO 2018075135 A1 (QUALCOMM INC.) 26 April 2018 (2018-04-26) entire document	1-60



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

19 November 2020

Date of mailing of the international search report

26 November 2020

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/112415

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018316562 A1 (BLACKBERRY LIMITED) 01 November 2018 (2018-11-01) entire document	1-60

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/112415

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110115099	A	09 August 2019	KR	20190097190	A	20 August 2019
				WO	2018123357	A1	05 July 2018
				US	2019306698	A1	03 October 2019
				JP	2018107619	A	05 July 2018
				EP	3562256	A1	30 October 2019
WO	2018075135	A1	26 April 2018	US	2018109381	A1	19 April 2018
				EP	3530020	A1	28 August 2019
				KR	20190068549	A	18 June 2019
				CN	109863770	A	07 June 2019
				JP	2019537871	A	26 December 2019
				BR	112019007571	A2	02 July 2019
				CA	3036803	A1	26 April 2018
US	2018316562	A1	01 November 2018	EP	3616426	A1	04 March 2020
				US	2019123964	A1	25 April 2019
				WO	2018197194	A1	01 November 2018

国际检索报告

国际申请号

PCT/CN2020/112415

A. 主题的分类 H04L 9/08(2006.01)i; H04W 12/04(2009.01)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)) CNPAT, CNKI, WPI, EPDOC, IEEE: 装置配置协议, DPP配置请求, 设备配置协议, 终端配网协议, DPP, 密钥, 公钥, 重配置, 待配网设备, 配网设备, 配置者, 随机数, device, provisioning, protocol, request, reconfig+, enrollee, connector, wi?fi, configurator, random, nonce, public, key																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>WI-FI ALLIANCE. "DRAFT Device Provisioning Protocol Specification Version 1.2" https://www.wi-fi.org/download.php?file=/sites/default/files/private/DRAFT%20Device_Provisioning_Protocol_Specification_v_1.2_0.pdf, 2020年 3月 3日 (2020 - 03 - 03), 第2-8章</td> <td>1-60</td> </tr> <tr> <td>Y</td> <td>WI-FI ALLIANCE. "Device Provisioning Protocol Specification Version 1.1" https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf/35330, 2018年 12月 3日 (2018 - 12 - 03), 第2-8章</td> <td>1-60</td> </tr> <tr> <td>Y</td> <td>FISH OU. "DH密钥交换和ECDH原理(转)" https://www.cnblogs.com/fishou/p/4206451.html, 2015年 1月 6日 (2015 - 01 - 06), 全文</td> <td>1-60</td> </tr> <tr> <td>A</td> <td>CN 110115099 A (佳能株式会社) 2019年 8月 9日 (2019 - 08 - 09) 全文</td> <td>1-60</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	WI-FI ALLIANCE. "DRAFT Device Provisioning Protocol Specification Version 1.2" https://www.wi-fi.org/download.php?file=/sites/default/files/private/DRAFT%20Device_Provisioning_Protocol_Specification_v_1.2_0.pdf , 2020年 3月 3日 (2020 - 03 - 03), 第2-8章	1-60	Y	WI-FI ALLIANCE. "Device Provisioning Protocol Specification Version 1.1" https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf /35330, 2018年 12月 3日 (2018 - 12 - 03), 第2-8章	1-60	Y	FISH OU. "DH密钥交换和ECDH原理(转)" https://www.cnblogs.com/fishou/p/4206451.html , 2015年 1月 6日 (2015 - 01 - 06), 全文	1-60	A	CN 110115099 A (佳能株式会社) 2019年 8月 9日 (2019 - 08 - 09) 全文	1-60
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	WI-FI ALLIANCE. "DRAFT Device Provisioning Protocol Specification Version 1.2" https://www.wi-fi.org/download.php?file=/sites/default/files/private/DRAFT%20Device_Provisioning_Protocol_Specification_v_1.2_0.pdf , 2020年 3月 3日 (2020 - 03 - 03), 第2-8章	1-60															
Y	WI-FI ALLIANCE. "Device Provisioning Protocol Specification Version 1.1" https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf /35330, 2018年 12月 3日 (2018 - 12 - 03), 第2-8章	1-60															
Y	FISH OU. "DH密钥交换和ECDH原理(转)" https://www.cnblogs.com/fishou/p/4206451.html , 2015年 1月 6日 (2015 - 01 - 06), 全文	1-60															
A	CN 110115099 A (佳能株式会社) 2019年 8月 9日 (2019 - 08 - 09) 全文	1-60															
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件	"T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件													
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件	"T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件																
国际检索实际完成的日期 2020年 11月 19日		国际检索报告邮寄日期 2020年 11月 26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 毕雅超 电话号码 86-(10)-53961777															

C. 相关文件		
类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WO 2018075135 A1 (QUALCOMM INCORPORATED) 2018年 4月 26日 (2018 - 04 - 26) 全文	1-60
A	US 2018316562 A1 (BLACKBERRY LIMITED) 2018年 11月 1日 (2018 - 11 - 01) 全文	1-60

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/112415

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	110115099	A	2019年 8月 9日	KR	20190097190	A	2019年 8月 20日		
				WO	2018123357	A1	2018年 7月 5日		
				US	2019306698	A1	2019年 10月 3日		
				JP	2018107619	A	2018年 7月 5日		
				EP	3562256	A1	2019年 10月 30日		
WO	2018075135	A1	2018年 4月 26日	US	2018109381	A1	2018年 4月 19日		
				EP	3530020	A1	2019年 8月 28日		
				KR	20190068549	A	2019年 6月 18日		
				CN	109863770	A	2019年 6月 7日		
				JP	2019537871	A	2019年 12月 26日		
				BR	112019007571	A2	2019年 7月 2日		
				CA	3036803	A1	2018年 4月 26日		
US	2018316562	A1	2018年 11月 1日	EP	3616426	A1	2020年 3月 4日		
				US	2019123964	A1	2019年 4月 25日		
				WO	2018197194	A1	2018年 11月 1日		