

(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
2018年5月31日 (31.05.2018)



(10) 国际公布号
WO 2018/094938 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2017/078852
- (22) 国际申请日: 2017年3月30日 (30.03.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201611057266.5 2016年11月26日 (26.11.2016) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 许剑峰 (XU, Jianfeng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区宝盛南路1号院20号楼8层101-01, Beijing 100192 (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, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM,

(54) Title: METHOD FOR SECURELY CONTROLLING SMART HOME APPLIANCE AND TERMINAL DEVICE

(54) 发明名称: 一种安全控制智能家居的方法及终端设备

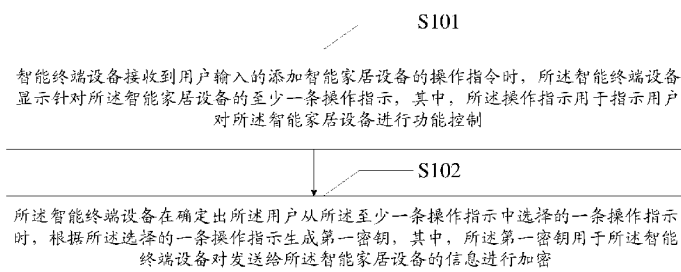


图 1

- S101 UPON RECEIVING AN OPERATION COMMAND INPUTTED BY A USER TO ADD A SMART HOME APPLIANCE, AN INTELLIGENT TERMINAL DEVICE DISPLAYS ONE OR MORE OPERATION INSTRUCTIONS WITH RESPECT TO THE SMART HOME APPLIANCE, WHEREIN THE OPERATION INSTRUCTIONS INDICATE CONTROL OF FUNCTIONS OF THE SMART HOME APPLIANCE PERFORMED BY THE USER
- S102 AFTER DETERMINING ONE OPERATION INSTRUCTION SELECTED BY THE USER FROM THE ONE OR MORE OPERATION INSTRUCTIONS, THE INTELLIGENT TERMINAL DEVICE GENERATES A FIRST CIPHER KEY ACCORDING TO THE SELECTED OPERATION INSTRUCTION, WHEREIN THE FIRST CIPHER KEY IS USED TO ENCRYPT INFORMATION TRANSMITTED TO THE SMART HOME APPLIANCE BY THE INTELLIGENT TERMINAL DEVICE

(57) Abstract: Provided are a method for securely controlling a smart home appliance and a terminal device capable of solving a problem in the prior art in which an intelligent terminal device is impersonated. The method comprises: upon receiving an operation command inputted by a user to add a smart home appliance, an intelligent terminal device displaying one or more operation instructions with respect to the smart home appliance, wherein the operation instructions indicate control of functions of the smart home appliance performed by the user; and after determining one operation instruction selected by the user from the one or more operation instructions, the intelligent terminal device generating a first cipher key according to the selected operation instruction, wherein the first cipher key

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, 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))。

is used to encrypt information transmitted to the smart home appliance by the intelligent terminal device.

(57) 摘要: 一种安全控制智能家居的方法及终端设备, 用以解决现有技术中存在的智能终端设备被仿冒的问题。该方法包括: 智能终端设备接收到用户输入的添加智能家居设备的操作指令时, 所述智能终端设备显示针对所述智能家居设备的至少一条操作指示, 其中, 所述操作指示用于指示用户对所述智能家居设备进行功能控制; 所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时, 根据所述选择的一条操作指示生成第一密钥, 其中, 所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

一种安全控制智能家居的方法及终端设备

本申请要求在2016年11月26日提交中国专利局、申请号为201611057266.5、发明名称为“一种Wi-Fi网络配置过程的安全性增强的方法和设备”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。

技术领域

本申请涉及通信技术领域，尤指一种安全控制智能家居的方法及终端设备。

背景技术

随着无线保真（Wireless-Fidelity，Wi-Fi）网络的广泛应用，基于Wi-Fi网络进行通信的智能设备越来越多。在智能家居领域，有大量的智能家居设备需要接入到路由器生成的Wi-Fi网络，但受限于智能家居设备的形态，例如智能台灯、智能插座等，通常没有显示屏以及键盘，无法选择Wi-Fi网络的服务集标识（Service Set Identifier，SSID），且无法输入Wi-Fi网络的密码；当智能家居设备通过一些智能手机APP配网的方法连接到Wi-Fi网络时，也无法在设备上查看所连接的路由器的情况。

现有技术中，采用以下两种方式实现智能家居设备与Wi-Fi网络的配网。

方式一，Soft-AP配网技术，待入网智能家居设备处于Soft-AP模式，发布所述待入网智能家居设备的名称，用户在智能设备的应用程序（Application，APP）界面选择需配置的待入网智能家居设备，在APP界面中输入路由器生成的Wi-Fi的名称、密码，点击配置按钮，完成配置；当智能设备的APP扫描到所述智能家居设备名称时，断开与当前路由器的连接，连接到待入网智能家居设备的Soft-AP上，然后发送预先设置的配网信息给所述智能家居设备，其中，所述配网信息包括路由器生成的Wi-Fi的名称以及密码；待入网智能家居设备从APP获取路由器生成的Wi-Fi的名称以及密码后，退出Soft-AP模式，连接到所述路由器，APP返回到与主路由器的连接，收到待入网智能家居设备的上线通知。

方式二，广播配网技术，智能设备通过发送Wi-Fi组播、广播、单播或者上述三者任意组合的方式，携带配网信息，发送到智能家居设备上，智能家居设备接收配网信息后，自动连接到配网信息指定的Wi-Fi网络，其中，所述智能设备包括，智能手机、机顶盒（Set Top Box，STB）、智能电视盒子（Over The Top，OTT）等智能家具设备。

综上所述，现有技术中用户采用非接触式和非近距离的配网方式，存在将其它智能家居设备误添加到用户家的路由器的Wi-Fi网络上，也存在用户家的智能家居设备被配置到其它用户家的路由器的其它Wi-Fi网络上，其它用户的智能终端仿冒用户家的智能终端设备，配置信息被周围的恶意无线监听设备偷听到等问题，如何提供一个安全可靠的智能家居设备与Wi-Fi网络配网的方案，防止配网信息泄露是目前需要解决的问题。

发明内容

本申请实施例提供了一种安全控制智能家居设备的方法及终端设备，用以解决现有技术中存在的智能终端设备被仿冒的问题。

第一方面，本申请提供了一种安全控制智能家居设备的方法，该方法包括：智能终端设备接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制，其中，所述操作指示是根据所述智能家居设备的类型确定的；所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密，所述信息可以为发送给所述智能家居设备的配网认证信息，也可以为发送给所述智能家居的控制命令信息。所述操作指示可以由所述智能终端设备自动生成的，也可以是所述智能终端设备接收到的用户预先设置的组合。

本发明实施例中，提供了一种安全控制智能家居设备的方法，智能终端设备根据智能家居设备的类型选择相应的操作指示，根据所述操作指示生成用于给发送给智能家居设备的信息进行加密的第一密钥，由用户近距离的对配网密码进行管控，提供一个安全可靠的智能家居设备与 Wi-Fi 网络配网的方案，防止配网信息泄露。

在一种可能的设计中，所述智能终端设备接收用户选择的所述至少一条操作指示中的一条操作指示。

在一种可能的设计中，所述智能终端设备在确定出所述操作指示时，采用设定算法对所述操作指示对应的功能控制执行运算得到第一密钥之后，所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

本发明实施例中，采用第二密钥对所述智能终端设备对发送给所述智能家居设备的信息进行加密，进一步的提高了配网信息的安全性。

在一种可能的设计中，所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥之后，所述智能终端设备使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

第二方面，本申请提供了一种安全控制智能家居设备的方法，该方法包括：智能家居设备接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；所述智能家居设备根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，所述智能家居设备根据所述功能控制指令生成第一密钥之后，所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，所述智能家居设备根据所述功能控制指令生成第一密钥之后，该方法还包括：

所述智能家居设备接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；所述智能家居设备使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

第三方面，本申请提供了一种智能终端设备，该智能终端设备包括：显示模块，用于接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制；处理模块，用于在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

在一种可能的设计中，所述处理模块还用于：接收用户选择的所述至少一条操作指示中的任一条操作指示。

在一种可能的设计中，所述处理模块还用于：根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

在一种可能的设计中，该智能终端设备还包括：发送模块，用于使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

第四方面，本申请提供了一种智能家居设备，该智能家居设备包括：接收模块，用于接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；生成模块，用于根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，所述处理模块还用于：根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，处理模块，用于接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；所述处理模块还用于，使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

第五方面，本申请实施例还提供了一种智能终端设备，存储器，用于存储器程序指令；处理器，用于调用所述存储器中存储的程序指令，接收用户输入的添加智能家居设备的操作指令时，控制显示器显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制；在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。该智能终端设备可以是移动终端、计算机等等。

在一种可能的设计中，所述处理器还用于：接收用户选择的所述至少一条操作指示中的一条操作指示。

在一种可能的设计中，所述处理器还用于：根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

在一种可能的设计中，所述处理器还用于：所述智能终端设备使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密

码、或者证书中的至少一项。

第六方面，本申请提供了一种智能家居设备，该智能家居设备包括：存储器，用于存储器程序指令；处理器，用于调用所述存储器中存储的程序指令，接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，所述处理器还用于：

根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的设计中，所述处理器还用于：

接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；

所述第二处理器使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

第七方面，本申请实施例中还提供一种计算机存储介质，该存储介质中存储软件程序，该软件程序在被一个或多个处理器读取并执行时可实现第一方面或上述第一方面的任意一种设计提供的方法。

附图说明

- 图 1 为本申请实施例提供的一种安全控制智能家居设备的方法流程图；
- 图 2 为本申请实施例提供的另一种安全控制智能家居设备的方法流程图；
- 图 3 为本申请实施例提供的再一种安全控制智能家居设备的方法流程图；
- 图 4 为本申请实施例提供的又一种安全控制智能家居设备的方法流程图；
- 图 5 为本申请实施例提供的一种智能终端设备示意图；
- 图 6 为本申请实施例提供的一种智能家居设备示意图；
- 图 7 为本申请实施例提供的一种智能终端设备硬件结构图；
- 图 8 为本申请实施例提供的一种智能家居设备硬件结构图。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。

本申请实施例提供一种安全控制智能家居设备的方法及终端设备，用以解决现有技术中存在的智能家居设备与 Wi-Fi 网络的配置信息被周围的恶意无线监听设备偷听、智能家居设备被仿冒、或者智能终端被仿冒的问题。其中，方法和装置是基于同一发明构思的，由于方法及装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。

另外，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

下面结合附图对本申请提供的一种安全控制智能家居设备的方法进行具体说明。

参见图 1，为本申请提供的一种安全控制智能家居设备的方法流程图，当需要为智能家居设备配置网络时，用户在智能设备的 APP 界面上添加需配置的待入网智能家居设备，该方法包括：

S101，智能终端设备接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制。

举例说明，所述智能终端设备可以为智能手机、STB、OTT 等，所述智能家居设备可以为智能台灯、智能空调、智能音箱等。当所述智能终端设备为智能手机，所述智能家居设备为智能台灯时，当智能手机需要对智能台灯进行设置时，智能手机上的应用程序（Application，APP）上显示的操作指示表示的是对所述智能家居能够执行的功能控制的组合，所述组合可以为任意重复次数的任意功能控制，例如，智能台灯的功能控制为：{开灯，关灯，调亮，调暗}，则操作指示可以为进行连续的两次开灯、三次开灯、四次开灯，或者，调亮后调暗智能台灯的亮度。当所述智能家居设备为智能空调时，所述 APP 显示的操作指示可以为按顺序按下智能空调遥控器的一个或多个按键，或组合键。智能手机上的 APP 随机显示一种或多种操作指示，所述操作指示是根据所述智能家居设备的类型确定的。

S102，所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

可选的，所述第一密钥还用于对所述智能终端设备对发送给所述智能家居设备的信息进行鉴权。

具体的，采用设定算法对所述选择的一条操作指示进行处理，生成第一密钥，所述设定算法可以将确定出的操作指示映射为随机数组合，对所述随机数进行加密，还可以采用四方密码、替换加密法、换位加密法、回转轮加密法、多码加密法以及换位加密法，本发明对其不做限定。

本发明实施例中，提供了一种安全控制智能家居设备的方法，智能终端设备根据智能家居设备的类型选择相应的操作指示，根据所述操作指示生成用于给发送给智能家居设备的信息进行加密的第一密钥，由用户近距离的对配网进行管控，提供一个安全可靠的智能家居设备与 Wi-Fi 网络配网的方案，防止配网信息泄露。

在一种可能的实现方式中，在步骤 S101 之后，还包括：所述智能终端设备接收用户选择的所述至少一条操作指示中的一条操作指示。

在一种可能的实现方式中，在步骤 S102 之后，还包括：所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

具体的，所述智能终端设备将所述第一密钥与其它加密方式进行组合，生成第二密钥，所述其它加密方式包括 AES 加密算法。

可选的，所述第二密钥还可以用于所述智能终端设备对发送给所述智能家居设备的信息进行鉴权。

本发明实施例中，使用所述第二密钥将所述智能终端设备发送给所述智能家居设备的信息进行加密，进一步的提高了配网信息的安全性。

在一种可能的实现方式中，步骤 S102 之后，该方法还包括：所述智能终端设备使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

在一种可能的实现方式中，所述智能终端设备保存所述第二密钥之后，该方法还包括：所述智能终端设备使用所述第二密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

参见图 2，为本申请提供的另一种安全控制智能家居设备的方法流程图。该方法包括：

S201，智能终端设备接收用户输入的对智能家居设备执行配网操作的指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制。

S202，所述智能终端设备在确定出所述用户选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

参见图 3，为本申请提供的再一种安全控制智能家居设备的方法流程图。该方法包括：

S301、智能家居设备接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制。

可选的，所述智能家居设备接收到的功能控制指令是用户接触式触发的、或者超近距离的操作。

S302、所述智能家居设备根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

可选的，所述第一密钥还用于鉴权所述智能终端设备发送给所述智能家居设备的信息。

在一种可能的实现方式中，步骤 S302 之后，还包括：所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息，或者鉴权所述智能终端设备发送给所述智能家居设备的信息。

具体的，所述智能终端设备将所述第一密钥与其它解密方式进行组合，生成第二密钥。

在一种可能的实现方式中，步骤 S302 之后，该方法还包括：所述智能家居设备接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；所述智能家居设备使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

在一种可能的实现方式中，所述智能家居设备保存所述第二密钥之后，该方法还包括：所述智能家居设备接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第二密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；所述智能家居设备使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

参见图 4 所示，为本申请实施例提供的又一种安全控制智能家居设备的方法流程图，

假设智能终端设备为智能手机，智能家居设备为智能台灯，该方法包括：

S401，未入网的智能台灯上电启动时，对外创建一个 soft 访问节点 (Access Point, AP) 或者采用广播/组播的方式向周围设备告知所述智能台灯的特殊的 Wi-Fi 服务集标识 (Service Set Identifier, SSID)，其中，所述 SSID 中包含所述智能台灯的型号等。

S402，智能手机通过 Wi-Fi 设备扫描功能，发现位于周围的智能台灯，所述智能手机主动发出发现所述智能台灯的提示信息，或由用户主动进入到所述智能台灯的配置过程中，然后，由用户在手机上触发添加智能台灯的过程。

S403，智能手机上的 APP 根据扫描到的智能台灯的类型，在界面上显示预先定义好的一系列操作指示中随机抽选出的一条操作指示，例如，操作指示为开关智能台灯 3 次。

S404，智能手机上的 APP 将所述抽选出的一条操作指示采用设定的算法进行编码，形成加密密钥，将所述加密密钥与其他加密方式相结合，对认证信息进行加密。

S405，智能台灯接收到用户输入的功能控制指令，其中，所述功能控制指令根据智能手机 APP 在界面上显示的所述抽选出的一条操作指示输入的，例如，开关智能台灯 3 次。

S406，智能台灯记录所述功能控制指令，并根据所述功能控制指令生成解密密钥并保存。

S407，智能手机的 APP 通过已有的组播/广播配网，或者 SoftAP 配网技术将加密后的认证信息发送给智能台灯。

S408，智能台灯接收到认证信息后，使用之前保存的解密密钥，结合其它解密或鉴权方式，例如 AES 加密算法，解密出明文的认证信息。

S409，智能台灯使用解密出的明文认证信息连接到路由器上，并通过路由器网络通知智能手机，完成与智能手机的配网。

基于与方法实施例同样的发明构思，本申请还提供了一种智能终端设备示意图，如图 5 所示，该智能终端设备包括：

显示模块 501，用于接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制。

处理模块 502，用于在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

本发明实施例中，提供了一种智能终端设备，智能终端设备根据智能家居设备的类型选择相应的操作指示，根据所述操作指示生成用于给发送给智能家居设备的信息进行加密的第一密钥，由用户近距离的对配网进行管控，提供一个安全可靠的智能家居设备与 Wi-Fi 网络配网的方案，防止配网信息泄露。

在一种可能的实现方式中，所述处理模块 502 还用于：接收用户选择的所述至少一条操作指示中的一条操作指示。

在一种可能的实现方式中，所述处理模块 502 还用于：根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

在一种可能的实现方式中，该智能终端设备还包括：发送模块，用于使用所述加密密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi

网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

在一种可能的实现方式中，所述操作指示是根据所述智能家居设备的类型确定的。

基于与方法实施例同样的发明构思，本申请还提供了一种智能家居设备示意图，如图 6 所示，该智能家居设备包括：

接收模块 601，用于接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制。

生成模块 602，用于根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的实现方式中，所述处理模块还用于：根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

在一种可能的实现方式中，所述智能家居设备还包括：处理模块，用于接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述解密密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；所述处理模块还用于，使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，另外，在本申请各个实施例中的各功能模块可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

其中，集成的模块既可以采用硬件的形式实现时，如图 7 所示，智能终端设备可以包括处理器 701。上述模块对应的实体的硬件可以为处理器 701。处理器 701，可以是一个中央处理模块（英文：central processing unit，简称 CPU），或者为数字处理模块等等。处理器 701 接收用户发出的添加智能家居设备的操作指令。该装置还包括：存储器 702，用于存储处理器 701 执行的程序。存储器 702 可以是非易失性存储器，比如硬盘（英文：hard disk drive，缩写：HDD）或固态硬盘（英文：solid-state drive，缩写：SSD）等，还可以是易失性存储器（英文：volatile memory），例如随机存取存储器（英文：random-access memory，缩写：RAM）。存储器 702 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。

处理器 701 用于执行存储器 702 存储的程序代码，具体调用所述第一存储器中存储的程序指令，接收到用户输入的添加智能家居设备的操作指令时，控制显示器 703 显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制；在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

本申请实施例中不限定上述处理器 701、存储器 702 以及显示器 703 之间的具体连接介质。本申请实施例在图 7 中以存储器 702、处理器 701 以及显示器 703 之间通过总线 704 连接，总线在图 7 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 7 中仅

用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本发明实施例还提供了一种智能家居设备，该智能家居设备包括：存储器 802，用于存储器程序指令；处理器 801，用于调用所述存储器 802 中存储的程序指令，接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；根据所述功能控制指令生成第一密钥其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。本申请实施例中不限定上述处理器 801 以及存储器 802 之间的具体连接介质。本申请实施例在图 8 中以存储器 802 与处理器 801 之间通过总线 803 连接，总线在图 8 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

本发明实施例还提供了一种计算机可读存储介质，用于存储为执行上述处理器所需执行的计算机软件指令，其包含用于执行上述处理器所需执行的程序。

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

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

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

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

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

权利要求

1、一种安全控制智能家居设备的方法，其特征在于，该方法包括：

智能终端设备接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制；

所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

2、根据权利要求 1 所述的方法，其特征在于，智能终端设备接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示之后，还包括：

所述智能终端设备接收用户选择的所述至少一条操作指示中的一条操作指示。

3、根据权利要求 1 所述的方法，其特征在于，所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥之后，还包括：

所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

4、根据权利要求 1 所述的方法，其特征在于，所述智能终端设备在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥之后，该方法还包括：

所述智能终端设备使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

5、根据权利要求 1 所述的方法，其特征在于，所述操作指示是根据所述智能家居设备的类型确定的。

6、一种安全控制智能家居设备的方法，其特征在于，该方法包括：

智能家居设备接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；

所述智能家居设备根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

7、根据权利要求 6 所述的方法，其特征在于，所述智能家居设备根据所述功能控制指令生成第一密钥之后，还包括：

所述智能终端设备根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

8、根据权利要求 6 所述的方法，其特征在于，所述智能家居设备根据所述功能控制指令生成第一密钥之后，该方法还包括：

所述智能家居设备接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi

网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；

所述智能家居设备使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

9、一种智能终端设备，其特征在于，该智能终端设备包括：

显示模块，用于接收到用户输入的添加智能家居设备的操作指令时，所述智能终端设备显示针对所述智能家居设备的至少一条操作指示，其中，所述操作指示用于指示用户对所述智能家居设备进行功能控制；

处理模块，用于在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

10、根据权利要求 9 所述的智能终端设备，其特征在于，所述处理模块还用于：

接收用户选择的所述至少一条操作指示中的一条操作指示。

11、根据权利要求 9 所述的智能终端设备，其特征在于，所述处理模块还用于：

根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

12、根据权利要求 9 所述的智能终端设备，其特征在于，该智能终端设备还包括：

发送模块，用于使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

13、根据权利要求 9 所述的智能终端设备，其特征在于，所述操作指示是根据所述智能家居设备的类型确定的。

14、一种智能家居设备，其特征在于，该智能家居设备包括：

接收模块，用于接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；

生成模块，用于根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

15、根据权利要求 12 所述的智能家居设备，其特征在于，所述处理模块还用于：

根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

16、根据权利要求 12 所述的智能家居设备，其特征在于，所述智能家居设备还包括：

处理模块，用于接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；

所述处理模块还用于，使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

17、一种智能终端设备，其特征在于，该智能终端设备包括：

存储器，用于存储器程序指令；

处理器，用于调用所述存储器中存储的程序指令，接收用户输入的添加智能家居设备的操作指令时，控制显示器显示针对所述智能家居设备的至少一条操作指示，其中，所述

操作指示用于指示用户对所述智能家居设备进行功能控制；在确定出所述用户从所述至少一条操作指示中选择的一条操作指示时，根据所述选择的一条操作指示生成第一密钥，其中，所述第一密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

18、根据权利要求 17 所述的智能终端设备，其特征在于，所述处理器还用于：
接收用户选择的所述至少一条操作指示中的一条操作指示。

19、根据权利要求 17 所述的智能终端设备，其特征在于，所述处理器还用于：
根据所述第一密钥生成第二密钥，其中，所述第二密钥用于所述智能终端设备对发送给所述智能家居设备的信息进行加密。

20、根据权利要求 17 所述的智能终端设备，其特征在于，所述处理器还用于：
所述智能终端设备使用所述第一密钥对控制所述智能终端设备接入的 Wi-Fi 网络的认证信息加密，并将加密后的所述 Wi-Fi 网络的认证信息发送给所述智能家居设备，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项。

21、一种智能家居设备，其特征在于，该智能家居设备包括：
存储器，用于存储器程序指令；
处理器，用于调用所述存储器中存储的程序指令，接收用户触发的功能控制指令，其中，所述功能控制指令为用户根据智能终端设备上显示的至少一条操作指示输入的，所述操作指示用于指示用户对所述智能家居设备进行功能控制；根据所述功能控制指令生成第一密钥，其中，所述第一密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

22、根据权利要求 21 所述的智能家居设备，其特征在于，所述处理器还用于：
根据所述第一密钥生成第二密钥，其中，所述第二密钥用于解密所述智能终端设备发送给所述智能家居设备的加密信息。

23、根据权利要求 21 所述的智能家居设备，其特征在于，所述处理器还用于：
接收所述智能终端设备发来的加密后的 Wi-Fi 网络的认证信息，并使用保存的所述第一密钥对所述加密后的 Wi-Fi 网络的认证信息解密，得到解密后的 Wi-Fi 网络的认证信息，其中，所述认证信息包括所述 Wi-Fi 网络的名称和密码、或者证书中的至少一项；
所述第二处理器使用解密后的 Wi-Fi 网络的认证信息接入对应的 Wi-Fi 网络。

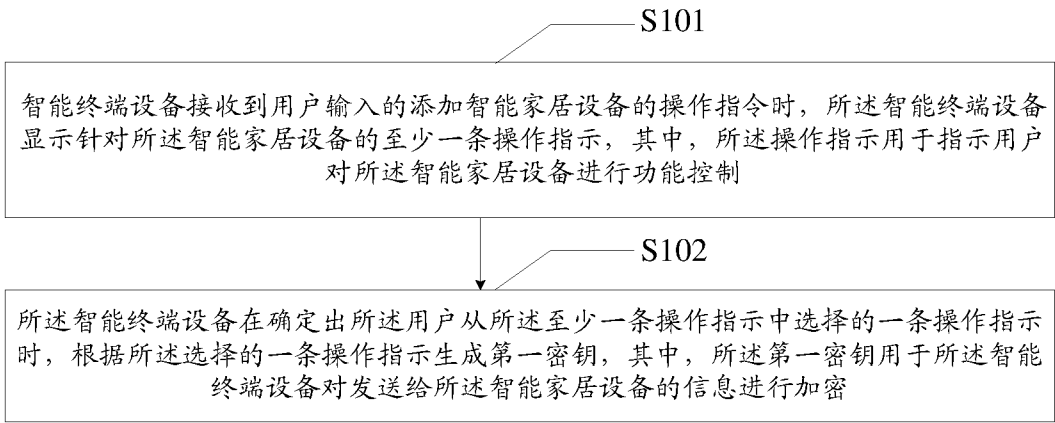


图 1

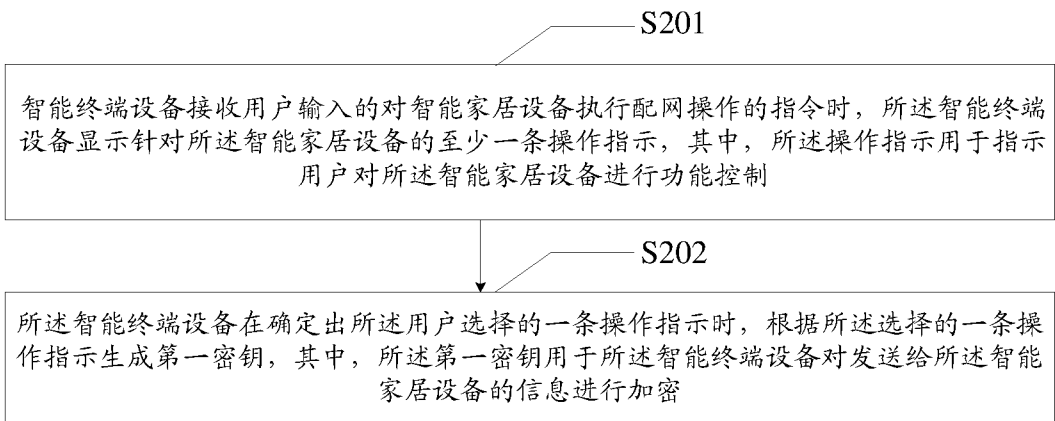
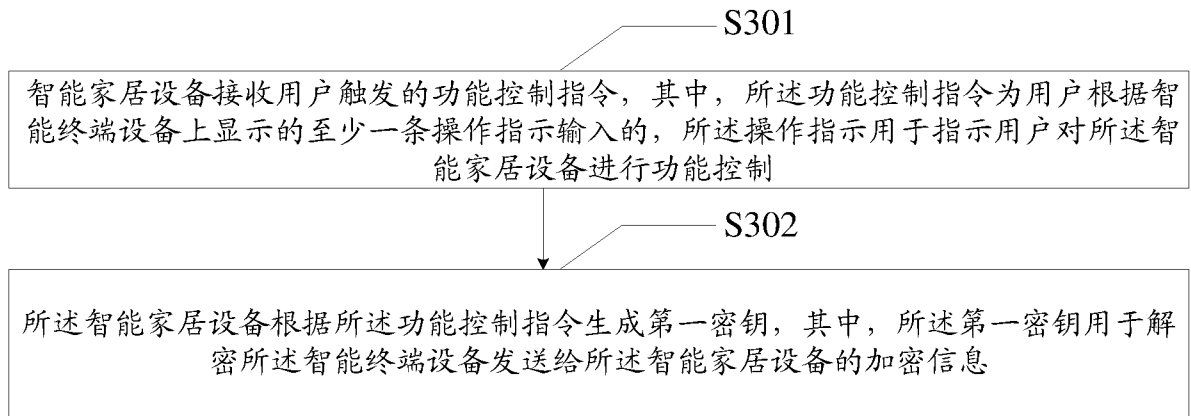


图 2

**图 3**

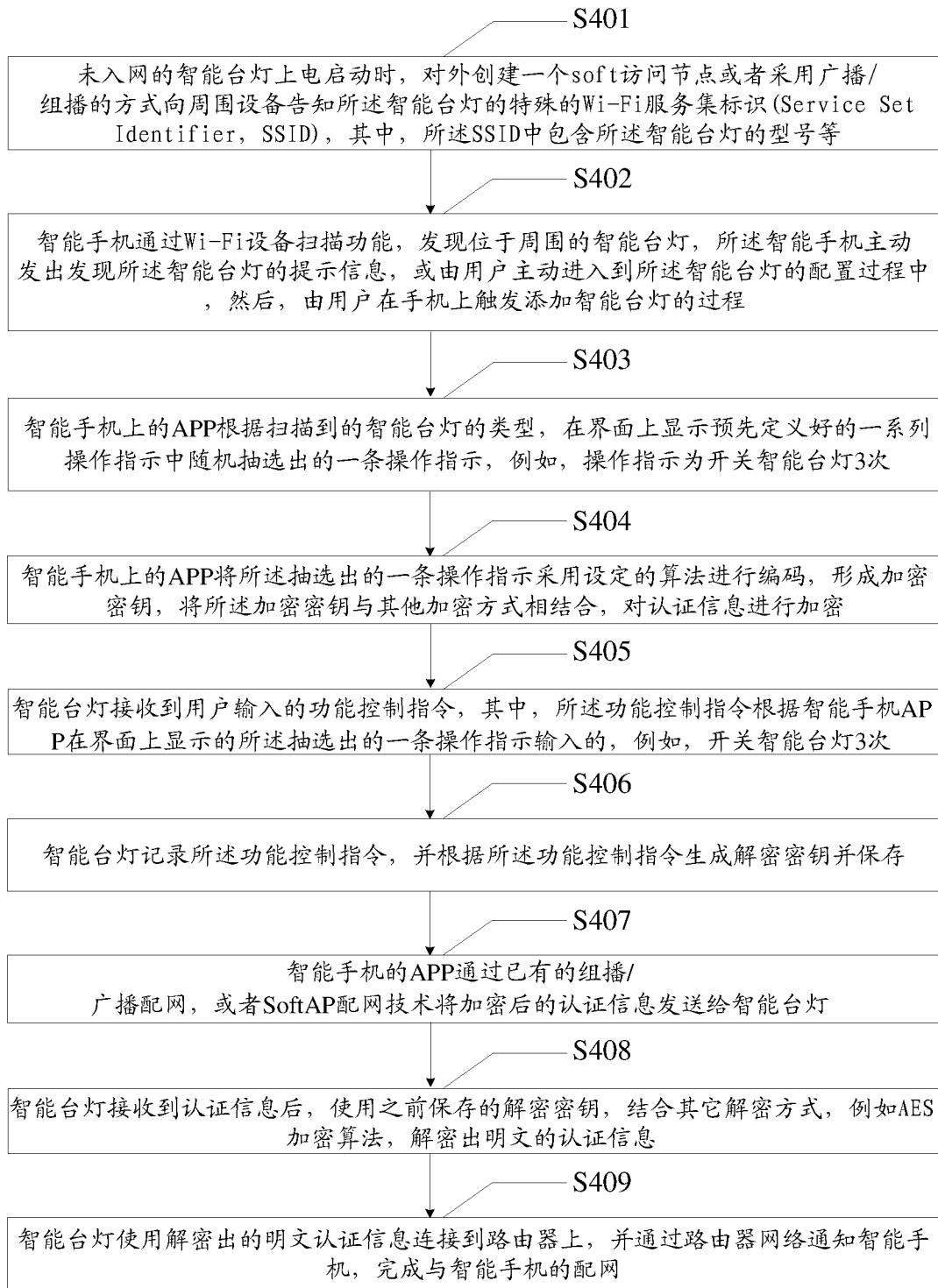


图 4

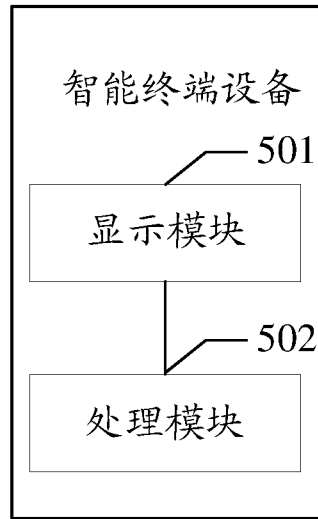


图 5

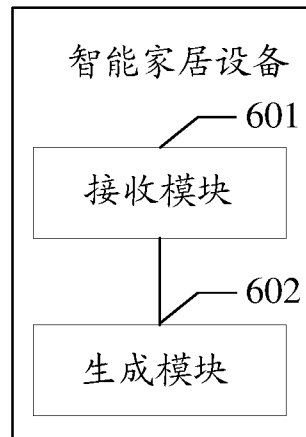


图 6

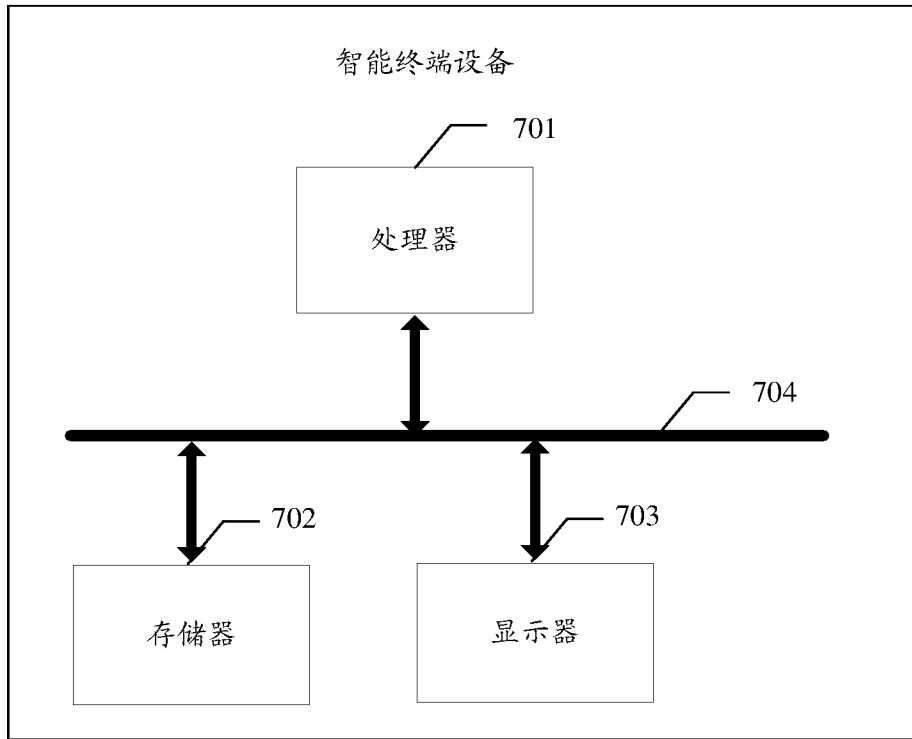


图 7

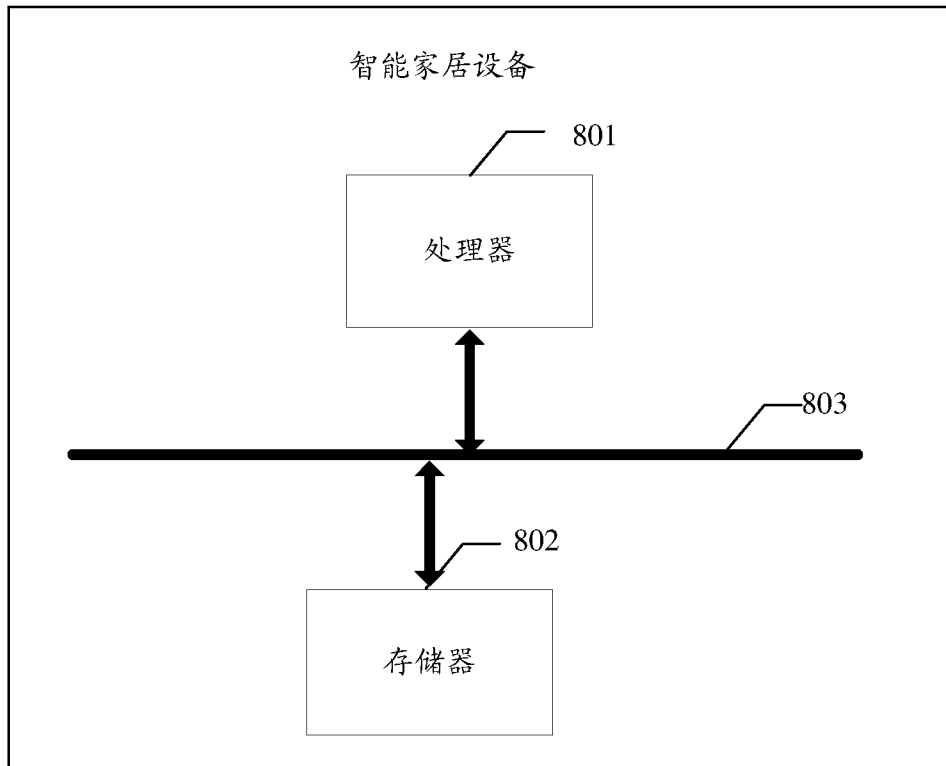


图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/078852

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

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)

CNXTX; CPRSABS; CNKI; VEN: 操作, 指示, 智能, 添加, 加入, 加密, 设备, 生成, 动作, 密码, 密钥, wi-fi, wifi, key, operat+, indicat+, smart, add, join+, encrypt, equipment, generat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103929307 A (TENDYRON CORPORATION), 16 July 2014 (16.07.2014), description, paragraphs 0042-0169, and figures 1-2	1-23
A	CN 104641590 A (NOKIA CORPORATION), 20 May 2015 (20.05.2015), entire document	1-23
A	CN 105243312 A (OYMOTION TECHNOLOGIES, INC.), 13 January 2016 (13.01.2016), entire document	1-23
A	US 2015373538 A1 (MIVALIFE MOBILE TECHNOLOGY INC.), 24 December 2015 (24.12.2015), entire document	1-23

Further documents are listed in the continuation of Box C. See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>
---	---

<p>Date of the actual completion of the international search</p> <p style="text-align: center;">16 May 2017</p>	<p>Date of mailing of the international search report</p> <p style="text-align: center;">31 May 2017</p>
<p>Name and mailing address of the ISA</p> <p>State Intellectual Property Office of the P. R. China</p> <p>No. 6, Xitucheng Road, Jimenqiao</p> <p>Haidian District, Beijing 100088, China</p> <p>Facsimile No. (86-10) 62019451</p>	<p>Authorized officer</p> <p style="text-align: center;">MAO, Yunnan</p> <p>Telephone No. (86-10) 62089144</p>

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/078852

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103929307 A	16 July 2014	WO 2015149582 A1	08 October 2015
CN 104641590 A	20 May 2015	US 2015341169 A1	26 November 2015
		WO 2014041397 A1	20 March 2014
		EP 2896154 A1	22 July 2015
		EP 2896154 A4	13 April 2016
CN 105243312 A	13 January 2016	None	
US 2015373538 A1	24 December 2015	None	

国际检索报告

国际申请号

PCT/CN2017/078852

<p>A. 主题的分类</p> <p>H04L 9/32(2006.01)i</p> <p>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</p>																	
<p>B. 检索领域</p> <p>检索的最低限度文献(标明分类系统和分类号)</p> <p>H04L; H04W</p> <p>包含在检索领域中的除最低限度文献以外的检索文献</p> <p>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))</p> <p>CNXT; CPRSABS; CNKI; VEN:操作, 指示, 智能, 添加, 加入, 加密, 设备, 生成, 动作, 密码, 密钥, wi-fi, wifi, key, operat+, indicat+, smart, add, join+, encrypt, equipment, generat+</p>																	
<p>C. 相关文件</p> <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>A</td> <td>CN 103929307 A (天地融科技股份有限公司) 2014年 7月 16日 (2014 - 07 - 16) 说明书0042-0169段, 附图1-2</td> <td>1-23</td> </tr> <tr> <td>A</td> <td>CN 104641590 A (诺基亚公司) 2015年 5月 20日 (2015 - 05 - 20) 全文</td> <td>1-23</td> </tr> <tr> <td>A</td> <td>CN 105243312 A (上海傲意信息科技有限公司) 2016年 1月 13日 (2016 - 01 - 13) 全文</td> <td>1-23</td> </tr> <tr> <td>A</td> <td>US 2015373538 A1 (MIVALIFE MOBILE TECHNOLOGY INC.) 2015年 12月 24日 (2015 - 12 - 24) 全文</td> <td>1-23</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	A	CN 103929307 A (天地融科技股份有限公司) 2014年 7月 16日 (2014 - 07 - 16) 说明书0042-0169段, 附图1-2	1-23	A	CN 104641590 A (诺基亚公司) 2015年 5月 20日 (2015 - 05 - 20) 全文	1-23	A	CN 105243312 A (上海傲意信息科技有限公司) 2016年 1月 13日 (2016 - 01 - 13) 全文	1-23	A	US 2015373538 A1 (MIVALIFE MOBILE TECHNOLOGY INC.) 2015年 12月 24日 (2015 - 12 - 24) 全文	1-23
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
A	CN 103929307 A (天地融科技股份有限公司) 2014年 7月 16日 (2014 - 07 - 16) 说明书0042-0169段, 附图1-2	1-23															
A	CN 104641590 A (诺基亚公司) 2015年 5月 20日 (2015 - 05 - 20) 全文	1-23															
A	CN 105243312 A (上海傲意信息科技有限公司) 2016年 1月 13日 (2016 - 01 - 13) 全文	1-23															
A	US 2015373538 A1 (MIVALIFE MOBILE TECHNOLOGY INC.) 2015年 12月 24日 (2015 - 12 - 24) 全文	1-23															
<p><input type="checkbox"/> 其余文件在C栏的续页中列出。</p> <p><input checked="" type="checkbox"/> 见同族专利附件。</p>																	
<p>* 引用文件的具体类型:</p> <p>“A” 认为不特别相关的表示了现有技术一般状态的文件</p> <p>“E” 在国际申请日的当天或之后公布的在先申请或专利</p> <p>“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)</p> <p>“O” 涉及口头公开、使用、展览或其他方式公开的文件</p> <p>“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</p> <p>“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</p> <p>“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</p> <p>“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</p> <p>“&” 同族专利的文件</p>																	
<p>国际检索实际完成的日期</p> <p>2017年 5月 16日</p>	<p>国际检索报告邮寄日期</p> <p>2017年 5月 31日</p>																
<p>ISA/CN的名称和邮寄地址</p> <p>中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088</p> <p>传真号 (86-10)62019451</p>	<p>受权官员</p> <p>毛韵楠</p> <p>电话号码 (86-10)62089144</p>																

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/078852

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	103929307	A	2014年 7月 16日	WO	2015149582	A1	2015年 10月 8日
CN	104641590	A	2015年 5月 20日	US	2015341169	A1	2015年 11月 26日
				WO	2014041397	A1	2014年 3月 20日
				EP	2896154	A1	2015年 7月 22日
				EP	2896154	A4	2016年 4月 13日
CN	105243312	A	2016年 1月 13日	无			
US	2015373538	A1	2015年 12月 24日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)