

(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
2016 年 2 月 18 日 (18.02.2016)



(10) 国际公布号
WO 2016/023367 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2015/074876

(22) 国际申请日: 2015 年 3 月 23 日 (23.03.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410403939.2 2014 年 8 月 15 日 (15.08.2014) CN

(71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。

(72) 发明人: 李飞云 (LI, Feiyun); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 高自光 (GAO, Ziguang); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 任桥 (REN, Qiao); 中国北京市海淀区清河中街 68 号华润

五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。

(74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802, 1803, 1805, Beijing 100101 (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, 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, KN, KP, KR, 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, 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,

[见续页]

(54) Title: METHOD, APPARATUS AND SYSTEM FOR ACCESS VERIFICATION

(54) 发明名称: 访问认证方法、装置及系统

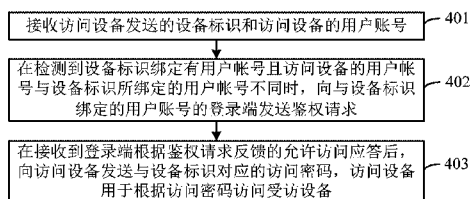


图4 / Fig. 4

401 Receive a device identifier and an accessing device user account sent by an access device
402 Send an authentication request to a login end of a user account bound to the device identifier when it is detected that the device identifier is bound with the user account and the user account of the accessing device is different from the user account bound to the device identifier
403 After an access-allowed response fed back by the login end according to the authentication request is received, send an access password corresponding to the device identifier to the access device, the access device being used for accessing an accessed device according to the access password

(57) Abstract: The disclosure relates to the technical field of computers. Disclosed are a method, apparatus and system for access verification. The method for access verification comprises: acquiring a device identifier of an accessed device; sending the device identifier and a user account of an accessing device to a third-party device, the third-party device being used for sending an authentication request to a login end when the device identifier is bound to a user account and the user account is different from the user account of the accessing device; after an access-allowed response fed back by the login end is received, sending an access password of the accessed device to the accessing device; and accessing the accessed device according to the received access password. Authentication to a login end is performed in a third-party device, an access password is sent to an accessing device after the authentication succeeds, and the accessing device accesses the accessed device according to the access password; the invention solves the poor security problem of manual user input of an access password on a mobile phone application making it easy for illicit users to obtain said access password; the effect of improving the security of the accessed device is achieved.

(57) 摘要:

[见续页]



WO 2016/023367 A1



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))。

本公开揭示了一种访问认证方法、装置及系统,属于计算机技术领域。所述访问认证方法包括:获取受访设备的设备标识;向第三方设备发送设备标识和访问设备的用户帐号,第三方设备用于在设备标识绑定有用户帐号且该用户帐号与访问设备的用户帐号不同时,向登录端发送鉴权请求,在接收到登录端反馈的允许访问应答后,向访问设备发送受访设备的访问密码;根据接收到的访问密码访问受访设备。通过在第三方设备中向登录端进行鉴权,鉴权成功后向访问设备发送访问密码,访问设备根据访问密码访问受访设备;解决了由于需要用户在手机 App 上手动输入访问密码,非法使用者很容易获取到该访问密码,安全性比较差的问题;达到了提高受访设备安全性的效果。

访问认证方法、装置及系统

本申请基于申请号为 CN 201410403939.2、申请日为 2014 年 8 月 15 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开涉及计算机技术领域，特别涉及一种访问认证方法、装置及系统。

10 背景技术

随着 Wi-Fi (Wireless-Fidelity, 无线保真) 的普及，带 Wi-Fi 的智能设备越来越多，一般 Wi-Fi 智能设备连上网络后，需要配合手机 App (Application, 应用程序) 来使用，手机 App 可以查看智能设备的状态和结果，并可以发送指令控制智能设备。而智能设备如何认证手机 App，让手机 App 安全访问控制智能设备的问题，显得尤为重要。

15 在相关技术中提供的一种访问认证方法是：用户通过手机 App 对 Wi-Fi 智能设备进行访问时，需要用户在手机 App 上手动输入访问密码，手机 App 将用户输入的访问密码发送给 Wi-Fi 智能设备，Wi-Fi 智能设备在匹配到该访问密码成功之后，允许该手机 App 进行访问。

20 发明人在实现本公开的过程中，发现相关技术至少存在如下缺陷：由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差。

发明内容

25 为了解决相关技术中由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题，本公开提供一种访问认证方法、装置及系统。所述技术方案如下：

根据本公开实施例的第一方面，提供一种访问认证方法，应用于访问设备中，所述方法包括：

获取受访设备的设备标识；

30 向第三方设备发送所述设备标识和所述访问设备的用户帐号；

接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据
35 所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问

密码,所述鉴权请求用于请求允许所述访问设备访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

可选的,所述获取受访设备的设备标识,包括:

5 接收所述受访设备广播发送的携带有所述受访设备的设备标识的广播消息,从所述广播消息中获取所述受访设备的设备标识;或,

通过扫描所述受访设备上的图形码获取所述受访设备的设备标识。

根据本公开实施例的第二方面,提供一种访问认证方法,应用于受访设备中,所述方法包括:

10 接收访问设备发送的访问密码,所述访问密码是第三方设备在接收到所述访问设备发送的设备标识和所述访问设备的用户帐号,在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送的与所述设备标识对应的访问密码,所述鉴权请求用于请求允许所述访问设备访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述
15 受访设备;

检测所述访问密码是否与所述受访设备生成的所述访问密码相同;

在检测出所述访问密码与所述受访设备生成的所述访问密码相同时,允许所述访问设备访问所述受访设备。

可选的,所述方法还包括:

20 生成所述访问密码;

向所述第三方设备发送所述访问密码和所述受访设备的设备标识,所述第三方设备用于将所述访问密码和所述设备标识进行绑定并保存。

可选的,所述方法还包括:

定期更改所述访问密码,得到更改后的访问密码;

25 将更改后的访问密码以及所述受访设备的设备标识发送给第三方设备,所述第三方设备将预存的所述设备标识所绑定的访问密码更新绑定为所述更改后的访问密码。

根据本公开实施例的第三方面,提供一种访问认证方法,应用于第三方设备中,所述方法包括:

接收访问设备发送的受访设备的设备标识和所述访问设备的用户帐号;

30 在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,所述鉴权请求用于请求允许所述访问设备访问所述受访设备;

在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送与
35 所述设备标识对应的访问密码,所述访问设备用于根据所述访问密码访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

可选的，所述方法还包括：

检测所述设备标识是否绑定有用户帐号；

在检测出所述设备标识未绑定有用户帐号时，将所述设备标识和所述访问设备的用户帐号进行绑定，将所述访问设备确定为所述登录端。

- 5 可选的，所述在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，包括：

在检测到所述设备标识绑定有用户帐号时，检测所述访问设备的用户帐号是否与所述设备标识所绑定的用户帐号相同；

- 10 在检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，执行所述向与所述设备标识绑定的用户帐号的登录端发送鉴权请求的步骤。

可选的，所述向所述访问设备发送与所述设备标识对应的访问密码，包括：

在检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号相同时，执行所述向所述访问设备发送与所述设备标识对应的访问密码的步骤。

- 15 可选的，所述方法还包括：

接收所述受访设备发送的所述访问密码和所述受访设备的设备标识；

当所述受访设备的设备标识不存在绑定的访问密码时，将所述访问密码和所述受访设备的设备标识进行绑定并保存。

可选的，所述方法还包括：

- 20 当所述受访设备的设备标识存在绑定的访问密码，检测接收到的所述访问密码是否与绑定的访问密码相同；

在接收到的所述访问密码与绑定的访问密码不同时，所述设备标识绑定的访问密码更新绑定为接收到的所述访问密码。

- 25 根据本公开实施例的第四方面，提供一种访问认证装置，应用于访问设备中，所述装置包括：

获取模块，被配置为获取受访设备的设备标识；

第一发送模块，被配置为向第三方设备发送所述设备标识和所述访问设备的用户帐号；

- 30 访问模块，被配置为接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，
- 35 所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

可选的，所述获取模块，包括：

第一获取子模块，被配置为接收所述受访设备广播发送的携带有所述受访设备的设备标识的广播消息，从所述广播消息中获取所述受访设备的设备标识；或，

5 第二获取子模块，被配置为通过扫描所述受访设备上的图形码获取所述受访设备的设备标识。

根据本公开实施例的第五方面，提供一种访问认证装置，应用于受访设备中，所述装置包括：

10 第一接收模块，被配置为接收访问设备发送的访问密码，所述访问密码是第三方设备在接收到所述访问设备发送的设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与
所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备；

15 第一检测模块，被配置为检测所述访问密码是否与所述受访设备生成的所述访问密码相同；

允许模块，被配置为在所述第一检测模块检测出所述访问密码与所述受访设备生成的所述访问密码相同时，允许所述访问设备访问所述受访设备。

可选的，所述装置还包括：

20 生成模块，被配置为生成所述访问密码；

第二发送模块，被配置为向所述第三方设备发送所述访问密码和所述受访设备的设备标识，所述第三方设备用于将所述访问密码和所述设备标识进行绑定并保存。

可选的，所述装置还包括：

更改模块，被配置为定期更改所述访问密码，得到更改后的访问密码；

25 第三发送模块，被配置为将更改后的访问密码以及所述受访设备的设备标识发送给第三方设备，所述第三方设备将预存的所述设备标识所绑定的访问密码更新绑定为所述更改后的访问密码。

根据本公开实施例的第六方面，提供一种访问认证装置，应用于第三方设备中，所述装置包括：

30 第二接收模块，被配置为接收访问设备发送的受访设备的设备标识和所述访问设备的用户帐号；

第四发送模块，被配置为在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，所述鉴权请求用于请求允许所述访问设备访问所述受访设备；

35 第五发送模块，被配置为在接收到所述登录端根据所述鉴权请求反馈的允许访问应答

后，向所述访问设备发送与所述设备标识对应的访问密码，所述访问设备用于根据所述访问密码访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

可选的，所述装置还包括：

5 第二检测模块，被配置为检测所述设备标识是否绑定有用户帐号；

第一绑定模块，被配置为在所述第二检测模块检测出所述设备标识未绑定有用户帐号时，将所述设备标识和所述访问设备的用户帐号进行绑定，将所述访问设备确定为所述登录端。

可选的，所述第四发送模块，包括：

10 检测子模块，被配置为在在所述第二检测模块检测到所述设备标识绑定有用户帐号时，检测所述访问设备的用户帐号是否与所述设备标识所绑定的用户帐号相同；

发送子模块，被配置为在所述检测子模块检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求。

15 可选的，所述第五发送模块，还被配置为在所述检测子模块检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号相同时，向所述访问设备发送与所述设备标识对应的访问密码。

可选的，所述装置还包括：

20 第三接收模块，被配置为接收所述受访设备发送的所述访问密码和所述受访设备的设备标识；

第二绑定模块，被配置为当所述受访设备的设备标识不存在绑定的访问密码时，将所述访问密码和所述受访设备的设备标识进行绑定并保存。

可选的，所述装置还包括：

25 第三检测模块，被配置为当所述受访设备的设备标识存在绑定的访问密码时，检测接收到的所述访问密码是否与绑定的访问密码相同；

第三绑定模块，被配置为当接收到的所述访问密码与绑定的访问密码不同时，所述设备标识绑定的访问密码更新绑定为接收到的所述访问密码。

根据本公开实施例的第七方面，提供一种访问认证系统，所述访问认证系统包括访问设备、受访设备和第三方设备；

30 所述访问设备包括如上述第四方面或第四方面各种可选方案中任一所述的访问认证装置；

所述受访设备包括上述第五方面或第五方面各种可选方案中任一所述的访问认证装置；

35 所述第三方设备包括如上述第六方面或第六方面各种可选方案中任一所述的访问认证装置。

根据本公开实施例的第八方面，提供一种访问认证装置，应用于访问设备中，所述装置包括：

处理器；

用于存储所述处理器可执行指令的存储器；

5 其中，所述处理器被配置为：

获取受访设备的设备标识；

向第三方设备发送所述设备标识和所述访问设备的用户帐号；

10 接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

15 根据本公开实施例的第九方面，提供一种访问认证装置，应用于受访设备中，所述装置包括：

处理器；

用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

20 接收访问设备发送的访问密码，所述访问密码是第三方设备在接收到所述访问设备发送的设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许
25 所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备；

检测所述访问密码是否与所述受访设备生成的所述访问密码相同；

在检测出所述访问密码与所述受访设备生成的所述访问密码相同时，允许所述访问设备访问所述受访设备。

30 根据本公开实施例的第十方面，提供一种访问认证装置，应用于第三方设备中，所述装置包括：

处理器；

用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

35 接收访问设备发送的设备标识和所述访问设备的用户帐号；

在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，所述鉴权请求用于请求允许所述访问设备访问所述受访设备；

在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送与
5 所述设备标识对应的访问密码，所述访问设备用于根据所述访问密码访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

本公开的实施例提供的技术方案可以包括以下有益效果：

通过利用访问设备获取受访设备的设备标识，向第三方设备发送设备标识和访问设备的用户帐号，在第三方设备向登录端询问确定允许访问设备访问受访设备后，接收第三
10 方设备发送的访问密码，并根据访问密码访问受访设备；由于访问设备访问受访设备时需要通过登录端允许，因此解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

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

15

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并于说明书一起用于解释本公开的原理。

- 图 1 是根据部分示例性实施例示出的一种访问认证方法所涉及的实施环境的示意图；
20 图 2 是根据一示例性实施例示出的一种访问认证方法的流程图；
图 3 是根据另一示例性实施例示出的一种访问认证方法的流程图；
图 4 是根据再一示例性实施例示出的一种访问认证方法的流程图；
图 5A 是根据还一示例性实施例示出的一种访问认证方法的流程图；
图 5B 是根据一示例性实施例示出的一种第三方设备向访问设备发送绑定请求的示意
25 图；
图 6A 是根据还一示例性实施例示出的一种访问认证方法的流程图；
图 6B 是根据一示例性实施例示出的一种通过局域网广播获取受访设备的设备标识的示意图；
图 6C 是根据一示例性实施例示出的一种通过扫描受访设备上图形码获取受访设备的
30 设备标识的示意图；
图 6D 是根据一示例性实施例示出的一种第三方设备向登录端发送鉴权请求的示意图；
图 7 是根据一示例性实施例示出的一种访问认证装置的框图；
图 8 是根据另一示例性实施例示出的一种访问认证装置的框图；
35 图 9 是根据再一示例性实施例示出的一种访问认证装置的框图；

图 10 是根据再一示例性实施例示出的一种访问认证装置的框图；

图 11 是根据再一示例性实施例示出的一种访问认证装置的框图；

图 12 是根据再一示例性实施例示出的一种访问认证装置的框图；

图 13 是根据一示例性实施例示出的一种访问认证系统的框图；

5 图 14 是根据一示例性实施例示出的一种用于访问受访设备的装置的框图；

图 15 是根据一示例性实施例示出的一种用于验证访问设备的装置的框图。

具体实施方式

10 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

15 图 1 是根据部分示例性实施例示出的一种访问认证方法所涉及的实施环境的示意图，如图 1 所示，该实施环境可以包括受访设备 120、访问设备 140、第三方设备 160 和登录端 180。

受访设备 120 可以是带 Wi-Fi 的智能设备，该智能设备可以是摄像头、路由器、智能电视等等。该受访设备 120 带有恢复出厂设置功能，能够解除与受访设备 120 绑定的用户帐号。该受访设备 120 可以通过路由器与互联网相连。

20 访问设备 140 可以是能够安装 App 的电子设备，该电子设备可以是智能手机、平板电脑、智能电视、电子书阅读器、MP4（Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面 4）播放器、膝上型便携计算机和台式计算机等等。

25 第三方设备 160 可以是具有绑定、鉴权等功能的服务器、路由器等。当第三方设备 160 为服务器时，可以是一台服务器，或者由若干台服务器组成的服务器集群，或者是一个云计算服务中心。

登录端 180 可以是能够安装 App 的电子设备，该电子设备可以是智能手机、平板电脑、智能电视、电子书阅读器、MP4（Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面 4）播放器、膝上型便携计算机和台式计算机等等。该登录端 180 上登录的用户帐号对受访设备 120 具有拥有者权限。

30 受访设备 120、访问设备 140、第三方设备 160 和登录端 180 之间可以通过无线网络连接，该无线网络可以是 Wi-Fi、蓝牙、红外线等等。

图 2 是根据一示例性实施例示出的一种访问认证方法的流程图，如图 2 所示，该访问认证方法应用于图 1 所示的实施环境中的访问设备 140 中，包括以下步骤。

35 在步骤 201 中，获取受访设备的设备标识。

在步骤 202 中，向第三方设备发送设备标识和访问设备的用户帐号。

在步骤 203 中，接收访问密码，根据访问密码访问受访设备，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码。

这里的鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

综上所述，本公开实施例中提供的访问认证方法，通过利用访问设备获取受访设备的设备标识，向第三方设备发送设备标识和访问设备的用户帐号，在第三方设备向登录端询问确定允许访问设备访问受访设备后，接收第三方设备发送的访问密码，并根据访问密码访问受访设备；由于访问设备访问受访设备时需要通过登录端允许，因此解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

图 3 是根据另一示例性实施例示出的一种访问认证方法的流程图，如图 3 所示，该访问认证方法应用于图 1 所示的实施环境中的受访设备 120 中，包括以下步骤。

在步骤 301 中，接收访问设备发送的访问密码，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码。

这里的鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

在步骤 302 中，检测访问密码是否与受访设备生成的访问密码相同。

在步骤 303 中，在检测出访问密码与受访设备生成的访问密码相同时，允许访问设备访问受访设备。

综上所述，本公开实施例中提供的访问认证方法，通过接收访问设备发送的访问密码，在检测到访问密码与受访设备生成的访问密码相同后，允许该访问设备访问受访设备；由于受访设备接收访问密码后需要在验证与生成的访问密码相同后才允许访问设备访问，因此解决了若不对访问密码进行验证，受访设备在更改访问密码后，访问设备仍能够访问受访设备，安全性低的问题；达到了提高受访设备安全性的效果。

图 4 是根据再一示例性实施例示出的一种访问认证方法的流程图，如图 4 所示，该访

问认证方法应用于图 1 所示的实施环境中的第三方设备 160 中, 包括以下步骤。

在步骤 401 中, 接收访问设备发送的设备标识和访问设备的用户帐号。

在步骤 402 中, 在检测到设备标识绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求。

5 这里的鉴权请求用于请求允许访问设备访问受访设备。

在步骤 403 中, 在接收到登录端根据鉴权请求反馈的允许访问应答后, 向访问设备发送与设备标识对应的访问密码, 访问设备用于根据访问密码访问受访设备。

这里的允许访问应答用于指示允许访问设备访问受访设备。

10 综上所述, 本公开实施例中提供的访问认证方法, 通过接收访问设备发送的设备标识和访问设备的用户帐号, 在检测到设备标识被绑定后向登录端发送鉴权请求, 在接收到登录端反馈的允许访问应答后向访问设备发送与设备标识对应的访问密码; 由于需要登录端允许后, 第三方设备才能将访问密码发送给访问设备, 因此解决了非法使用者获取到访问密码后, 就能利用该访问密码对该 Wi-Fi 智能设备进行访问, 安全性比较差的问题; 达到了提高受访设备安全性的效果。

15

在访问设备访问受访设备之前, 受访设备需要先生成访问密码, 将生成的访问密码与受访设备的设备标识发送给第三方设备进行绑定。当第一个访问设备访问受访设备时, 第三方设备将该访问设备的用户帐号与受访设备的设备标识绑定, 使得该用户帐号获得该受访设备的拥有者权限。具体实现步骤请参见图 5A。

20

图 5A 是根据还一示例性实施例示出的一种访问认证方法的流程图, 如图 5A 所示, 该访问认证方法应用于图 1 所示的实施环境中, 包括以下步骤。

在步骤 501 中, 受访设备生成访问密码。

可选的, 受访设备可以随机生成访问密码。

25 可选的, 受访设备可以定期更改访问密码; 或者在接收到与该受访设备对应的登录端发送的更改访问密码指令后, 更改受访设备的访问密码。

在步骤 502 中, 受访设备向第三方设备发送该访问密码和受访设备的设备标识。

这里的设备标识可以是受访设备在被生产的时候赋予的, 该设备标识唯一标识受访设备。实际应用中, 该设备标识可以是字符串, 该字符串可以由数字、字母或其他类型字符中的至少一类组合而成。

30

可选的, 为了保证访问密码的安全性, 受访设备可以通过加密通道将生成的访问密码和设备标识发送给第三方设备, 其中的加密通道可以降低访问密码泄露的可能性。

在步骤 503 中, 第三方设备接收受访设备发送的访问密码和受访设备的设备标识。

在步骤 504 中, 当受访设备的设备标识不存在绑定的访问密码, 第三方设备则将该访问密码和受访设备的设备标识进行绑定并保存。

35

第三方设备在接收受访设备发送的访问密码和受访设备的设备标识之后, 首先检测该

设备标识是否被绑定有访问密码，如果检测到接收到的设备标识没有绑定访问密码时，则将接收到的访问密码与设备标识进行绑定并保存。

在一种情况下，受访设备为了保证安全性，可以随时更改绑定的访问密码，即首先定期更改访问密码，得到更改后的访问密码，并将更改后的访问密码以及该受访设备的设备标识发送给第三方设备；第三方设备在检测到接收到的设备标识存在绑定的访问密码时，则检测接收到的访问密码是否与该绑定的访问密码相同，若接收到的访问密码与该绑定的访问密码相同，第三方设备不作操作，若接收到的访问密码与该绑定的访问密码不同，第三方设备将该绑定的访问密码与设备标识解除绑定，将接收到的访问密码与设备标识进行绑定并保存。也即，当第三方设备接收到受访设备发送的访问密码和设备标识之后，如果检测到该访问密码和与该设备标识已经绑定的访问密码不同时，则将预存的该设备标识所绑定的访问密码更新绑定为更改后的访问密码。

根据上述步骤 501 至步骤 504 可知，第三方设备绑定了受访设备的设备标识和受访设备生成的访问密码。

在步骤 505 中，访问设备获取受访设备的设备标识。

访问设备在获取受访设备的设备标识时，可以接收受访设备广播发送的携带有受访设备的设备标识的广播消息，从广播消息中获取受访设备的设备标识；或者可以通过扫描受访设备上的图形码获取受访设备的设备标识。

需要说明的是，本实施例对访问设备获取受访设备的设备标识的具体方式不作限定。

在步骤 506 中，访问设备向第三方设备发送该设备标识和访问设备的用户帐号。

这里的用户帐号是用户在第三方设备上注册的，用户可以在不同的访问设备上登录该用户帐号。

访问设备在获取受访设备的设备标识后，将该设备标识和访问设备登录的用户帐号发送给第三方设备。

在步骤 507 中，第三方设备接收访问设备发送的设备标识和访问设备的用户帐号。

在步骤 508 中，第三方设备在检测到接收的设备标识未绑定有用户帐号时，将接收到的访问设备的用户帐号与该设备标识进行绑定。

第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号之后，会检测该设备标识是否绑定有用户帐号。

在第三方设备检测到设备标识未绑定有用户帐号时，将接收到的访问设备的用户帐号与该设备标识进行绑定。可选的，可以向访问设备发送绑定请求，绑定请求用于向访问设备询问是否将受访设备的设备标识和访问设备的用户帐号进行绑定。

举例来讲，请参见图 5B，其是根据一示例性实施例示出的一种第三方设备向访问设备发送绑定请求的示意图。如图 5B 所示，访问设备在接收到第三方设备发送的绑定请求后，在屏幕上显示“是否与设备：9527 进行绑定？”的请求，此时用户可以通过点击：“是”选项，同意与设备：9527 进行绑定，也可以点击“否”选项，放弃与设备：9527 进行绑

定。

若访问设备同意和受访设备进行绑定，第三方设备则将该访问设备的用户帐号和受访设备的设备标识绑定，同时该访问设备的用户帐号获得该受访设备的拥有者权限。

5 为了区分与其他普通访问设备(即不具有该受访设备的拥有者权限的访问设备)，将该具有受访设备的拥有者权限的访问设备确定为登录端。但需要说明的是，登录端是一种具有该受访设备的拥有者权限的访问设备，该登录端的命名并不用于限制本发明的保护范围，在实际应用中，该登录端还可以有其他命名。

在步骤 509 中，第三方设备向访问设备发送与设备标识对应的访问密码。

10 也即，第三方设备在将该访问设备（也即登录端）的用户帐号与受访设备的设备标识绑定之后，则可以直接向该访问设备发送与该设备标识对应的访问密码，以便该访问设备根据该访问密码直接访问该受访设备。

在步骤 510 中，访问设备接收访问密码。

可选的，访问设备（也即登录端）在接收访问密码时，可以通过无线网络或者短信等方式进行接收。

15 需要说明的是，本实施例对访问设备接收访问密码的具体方式不作限定。

在步骤 511 中，访问设备向受访设备发送访问密码。

访问设备在接收到访问密码之后，则根据该访问密码访问受访设备。

20 在一种使用场景中，访问设备（也即登录端）根据该访问密码访问受访设备，可以向受访设备发送访问密码，此时可以由该访问设备将通过无线网络获取的访问密码直接发送给受访设备，在这种场景中，该访问设备可以不显示接收到的访问密码，以此加强受访设备的访问密码的安全性。

可选的，在该访问设备向受访设备发送访问密码时，该访问设备将接收到的访问密码显示给用户，并弹出密码输入框，由用户将接收到的访问密码输入密码输入框，该访问设备在接收到用户输入的密码之后，将该密码发送给受访设备。

25 在步骤 512 中，受访设备接收该访问密码。

在步骤 513 中，受访设备检测该访问密码是否与受访设备生成的访问密码相同。

由于受访设备会更改访问密码，因此需要检测接收到的访问密码是否与受访设备生成的访问密码相同。

30 在步骤 514 中，若检测出访问密码与受访设备生成的访问密码相同，受访设备则允许该访问设备访问受访设备。

需要说明的是，在该访问设备（也即登录端）再次访问该受访设备时，第三方设备检测到该访问设备的用户帐号与受访设备的设备标识是绑定关系后，将直接向该访问设备发送该受访设备的访问密码，该访问设备接收并根据该访问密码对受访设备进行访问。

35 综上所述，本公开实施例中提供的访问认证方法，通过第三方设备在检测到设备标识未被绑定时，将接收到的用户帐号与该设备标识绑定，并确定该用户帐号对该受访设备具

有拥有者权限；由于通过将用户帐号与受访设备的设备标识进行绑定确定了拥有者权限，访问设备需要得到登录端允许才能访问受访设备，解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

5

在第一个访问受访设备的访问设备的用户帐号获得该受访设备的拥有者权限后，普通的访问设备在访问该受访设备时，需要获得与该具有拥有者权限的用户帐号对应的访问设备的允许才能对该受访设备进行访问。具体实现步骤请参见图 6A。

图 6A 是根据还一示例性实施例示出的一种访问认证方法的流程图，如图 6A 所示，该访问认证方法应用于图 1 所示的实施环境中，包括以下步骤。

10

在步骤 601 中，访问设备获取受访设备的设备标识。

访问设备在获取受访设备的设备标识时，可以接收受访设备广播发送的携带有受访设备的设备标识的广播消息，从广播消息中获取受访设备的设备标识；或者可以通过扫描受访设备上的图形码获取受访设备的设备标识。

15

举例来讲，请参见图 6B，其是根据一示例性实施例示出的一种通过局域网广播获取受访设备的设备标识的示意图。如图 6B 所示，访问设备通过局域网广播搜索到附近的受访设备后，将搜索结果显示在屏幕上，此时用户可以点击想要连接的受访设备的设备标识进行连接，在用户点击设备标识：9527 后，访问设备弹出“是否与设备：9527 建立连接？”的询问。

20

举例来讲，请参见图 6C，其是根据一示例性实施例示出的一种通过扫描受访设备上图形码获取受访设备的设备标识的示意图。如图 6C 所示，访问设备在扫描受访设备上的二维码后，直接弹出“是否与设备：9527 建立连接？”的询问。

需要说明的是，本实施例对获取受访设备的设备标识的具体方法不作限定。

在步骤 602 中，访问设备向第三方设备发送设备标识和访问设备的用户帐号。

25

这里的用户帐号是用户在第三方设备上注册的，用户可以在不同的访问设备上登录该用户帐号。

访问设备在获取受访设备的设备标识后，将该设备标识和访问设备登录的用户帐号发送给第三方设备。

30

举例来讲，仍请参见图 6B 或图 6C，在访问设备弹出“是否与设备：9527 建立连接？”的询问后，用户可以通过点击“否”选项放弃与设备：9527 建立连接，或者可以点击“是”选项确定与设备：9527 建立连接，此时访问设备将该受访设备的设备标识：9527 和访问设备登录的用户帐号发送给第三方设备。

在步骤 603 中，第三方设备接收访问设备发送的设备标识和访问设备的用户帐号。

35

在步骤 604 中，第三方设备在检测到设备标识绑定有用户帐号且接收到的用户帐号与绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求。

第三方设备接收访问设备发送的设备标识和访问设备的用户帐号之后，检测该设备标识是否绑定有用户帐号，在检测到该设备标识绑定有用户帐号时，检测该访问设备的用户帐号是否与该设备标识所绑定的用户帐号相同，在检测出该访问设备的用户帐号与该设备标识所绑定的用户帐号不同时，向与该设备标识绑定的用户帐号的登录端发送鉴权请求。

5 也即，第三方设备在检测到设备标识绑定有用户帐号且接收到的用户帐号与绑定的用户帐号不同时，则表明发送该用户帐号的访问设备不具有该受访设备的拥有者权限，也即该访问设备为普通访问设备，此时需要向该受访设备的拥有者进行鉴权，即向该受访设备的登录端进行鉴权。

10 这里的登录端是指在该登录端上登录的用户帐号与该设备标识存在绑定关系，即该登录端拥有该受访设备的拥有者权限。

这里的鉴权请求用于请求允许该访问设备访问受访设备。比如，该鉴权请求中可以携带有该访问设备上发送的用户帐号。

而第三方设备在检测到设备标识绑定有用户帐号且接收到的用户帐号与绑定的用户帐号相同时，则表明该访问设备为具有该受访设备的拥有者权限，此时可以直接向该访问设备发送与该设备标识对应的访问密码。

15 在步骤 605 中，登录端接收该鉴权请求。

登录端接收第三方设备发送的鉴权请求后，可以根据该鉴权请求向该登录端的用户进行提示，比如可以将该鉴权请求显示在登录端的屏幕上。

20 举例来讲，请参见图 6D，其是根据一示例性实施例示出的一种第三方设备向登录端发送鉴权请求的示意图。如图 6D 所示，登录端接收第三方设备发送的鉴权请求后，在屏幕上显示“是否同意设备：visitor 对设备：9527 进行访问？”的询问。

在步骤 606 中，登录端向第三方设备发送允许访问应答。

这里的允许访问应答用于指示允许访问设备访问受访设备。

25 在一种使用场景中，登录端的用户如果允许访问设备对受访设备进行访问，则向第三方设备发送允许访问应答。

30 举例来讲，仍请参见图 6D，当登录端的用户允许访问设备：visitor 对受访设备：9527 进行访问时，用户可以点击“是”选项，此时登录端向第三方设备发送允许访问应答。相反的，当登录端的用户禁止访问设备：visitor 对受访设备：9527 进行访问时，用户可以点击“否”选项，此时登录端向第三方设备发送禁止访问应答，可选的，第三方设备在接收到禁止访问应答后，可以向访问设备：visitor 发送错误码，以此说明该访问设备：visitor 不能访问受访设备。

在步骤 607 中，第三方设备接收该允许访问应答。

在步骤 608 中，第三方设备向访问设备发送与设备标识对应的访问密码。

在步骤 609 中，访问设备接收该访问密码。

35 可选的，访问设备在接收该访问密码时，可以通过无线网络或者短信等方式进行接收。

需要说明的是，本实施例对访问设备接收访问密码的具体方式不作限定。

在步骤 610 中，访问设备向受访设备发送该访问密码。

访问设备在接收到访问密码之后，则根据该访问密码访问受访设备。

5 在一种使用场景中，访问设备（也即登录端）根据该访问密码访问受访设备，可以向受访设备发送访问密码，此时可以由访问设备将通过无线网络获取的访问密码直接发送给受访设备，在这种场景中，访问设备可以不显示接收到的访问密码，以此加强受访设备的访问密码的安全性。

10 可选的，在访问设备向受访设备发送访问密码时，访问设备将接收到的访问密码显示给用户，并弹出密码输入框，由用户将接收到的访问密码输入密码输入框，访问设备在接收到用户输入的密码之后，将该密码发送给受访设备。

在步骤 611 中，受访设备接收该访问密码。

在步骤 612 中，受访设备检测该访问密码是否与受访设备生成的访问密码相同。

15 由于受访设备会更改访问密码，因此需要检测接收到的访问密码是否与受访设备生成的访问密码相同。举例来讲，如果受访设备不再继续让已经访问过的访问设备进行访问，除了在登录端禁止其访问外，受访设备还可以将原有访问密码修改为了现有访问密码，此时访问设备如果利用原来得知的原有访问密码再次访问受访设备时，由于受访设备可以对接收到的原有访问密码与更新后的现有访问密码进行匹配，在匹配不成功时，禁止该访问设备进行访问，从而可以保证受访设备被访问时所需的最新权限。

20 在步骤 613 中，若检测出访问密码与受访设备生成的访问密码相同，受访设备则允许访问设备访问受访设备。

可选的，若检测出接收到的访问密码与受访设备生成的访问密码不同，受访设备则禁止访问设备访问受访设备，此时受访设备可以向访问设备发送错误码，以此说明该访问设备不能访问受访设备。

25 需要说明的是，访问设备访问受访设备的访问权限只保留一段时间，受访设备可以通过更改访问密码来取消访问设备的访问权限。

30 综上所述，本公开实施例中提供的访问认证方法，通过利用访问设备获取受访设备的设备标识，向第三方设备发送设备标识和访问设备的用户帐号，在第三方设备向登录端询问确定允许访问设备访问受访设备后，接收第三方设备向访问设备发送的访问密码，并根据访问密码访问受访设备；由于访问设备访问受访设备时需要通过登录端允许，因此解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

35 本公开实施例中提供的访问认证方法，通过接收访问设备发送的访问密码，在检测到访问密码与受访设备生成的访问密码相同后，允许该访问设备访问受访设备；由于受访设备接收访问密码后需要在验证与生成的访问密码相同后才允许访问设备访问，因此解决了

若不对访问密码进行验证，受访设备在更改访问密码后，访问设备仍能够访问受访设备，安全性低的问题；达到了提高受访设备安全性的效果。

本公开实施例中提供的访问认证方法，通过接收访问设备发送的设备标识和访问设备的用户帐号，在检测到设备标识被绑定后向登录端发送鉴权请求，在接收到登录端反馈的允许访问应答后向访问设备发送与设备标识对应的访问密码；由于需要登录端允许后，第三方设备才能将访问密码发送给访问设备，因此解决了非法使用者获取到访问密码后，就能利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

下述为本公开装置实施例，可以用于执行本公开方法实施例。对于本公开装置实施例中未披露的细节，请参照本公开方法实施例。

图 7 是根据一示例性实施例示出的一种访问认证装置的框图，如图 7 所示，该访问认证装置应用于图 1 所示实施环境中的访问设备 140 中。该访问认证装置包括但不限于：获取模块 702、第一发送模块 704 和访问模块 706。

该获取模块 702，被配置为获取受访设备的设备标识。

该第一发送模块 704，被配置为向第三方设备发送设备标识和访问设备的用户帐号。

该访问模块 706，被配置为接收访问密码，根据访问密码访问受访设备，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码，鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

综上所述，本公开实施例中提供的访问认证装置，通过访问设备获取受访设备的设备标识，向第三方设备发送设备标识和访问设备的用户帐号，在第三方设备向登录端询问确定允许访问设备访问受访设备后，第三方设备向访问设备发送访问密码，访问设备根据访问密码访问受访设备；由于访问设备访问受访设备时需要通过登录端允许，因此解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

图 8 是根据另一示例性实施例示出的一种访问认证装置的框图，如图 8 所示，该访问认证装置应用于图 1 所示实施环境中的访问设备 140 中。该访问认证装置包括但不限于：获取模块 802、第一发送模块 804 和访问模块 806。

该获取模块 802，被配置为获取受访设备的设备标识。

该第一发送模块 804，被配置为向第三方设备发送设备标识和访问设备的用户帐号。

该访问模块 806, 被配置为接收访问密码, 根据访问密码访问受访设备, 访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号, 在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求, 在接收到登录端根据鉴权请求反馈的允许访问应答后, 向访问设备发送的与设备标识对应的访问密码, 鉴权请求用于请求允许访问设备访问受访设备, 允许访问应答用于指示允许访问设备访问受访设备。

在一种可能的实施例中, 该获取模块 802 可以包括: 第一获取子模块 802a 或第二获取子模块 802b。

该第一获取子模块 802a, 被配置为接收受访设备广播发送的携带有受访设备的设备标识的广播消息, 从广播消息中获取受访设备的设备标识。或,

该第二获取子模块 802b, 被配置为通过扫描受访设备上的图形码获取受访设备的设备标识。

综上所述, 本公开实施例中提供的访问认证装置, 通过访问设备获取受访设备的设备标识, 向第三方设备发送设备标识和访问设备的用户帐号, 在第三方设备向登录端询问确定允许访问设备访问受访设备后, 第三方设备向访问设备发送访问密码, 访问设备根据访问密码访问受访设备; 由于访问设备访问受访设备时需要通过登录端允许, 因此解决了由于需要用户在手机 App 上手动输入访问密码, 非法使用者很容易获取到该访问密码, 并利用该访问密码对该 Wi-Fi 智能设备进行访问, 安全性比较差的问题; 达到了提高受访设备安全性的效果。

图 9 是根据再一示例性实施例示出的一种访问认证装置的框图, 如图 9 所示, 该访问认证装置应用于图 1 所示实施环境中的受访设备 120 中。该访问认证装置包括但不限于: 第一接收模块 902、第一检测模块 904 和允许模块 906。

该第一接收模块 902, 被配置为接收访问设备发送的访问密码, 访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号, 在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求, 在接收到登录端根据鉴权请求反馈的允许访问应答后, 向访问设备发送的与设备标识对应的访问密码, 鉴权请求用于请求允许访问设备访问受访设备, 允许访问应答用于指示允许访问设备访问受访设备。

该第一检测模块 904, 被配置为检测访问密码是否与受访设备生成的访问密码相同。

该允许模块 906, 被配置为在第一检测模块 904 检测出访问密码与受访设备生成的访问密码相同时, 允许访问设备访问受访设备。

综上所述, 本公开实施例中提供的访问认证装置, 通过接收访问设备发送的访问密码, 检测到访问密码与受访设备生成的访问密码相同后, 允许该访问设备访问受访设备; 由于受访设备接收访问密码后需要进行验证与生成的访问密码相同后才能允许访问设备访问,

因此解决了若不对访问密码进行验证，受访设备在更改访问密码后，访问设备仍能够访问受访设备，安全性低的问题；达到了提高受访设备安全性的效果。

图 10 是根据再一示例性实施例示出的一种访问认证装置的框图，如图 10 所示，该访问认证装置应用于图 1 所示实施环境中的受访设备 120 中。该访问认证装置包括但不限于：第一接收模块 1002、第一检测模块 1004 和允许模块 1006。

该第一接收模块 1002，被配置为接收访问设备发送的访问密码，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码，鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

该第一检测模块 1004，被配置为检测访问密码是否与受访设备生成的访问密码相同。

该允许模块 1006，被配置为在第一检测模块 1004 检测出访问密码与受访设备生成的访问密码相同时，允许访问设备访问受访设备。

在一种可能的实施例中，该装置还包括：生成模块 1008 和第二发送模块 1010。

该生成模块 1008，被配置为生成访问密码。

该第二发送模块 1010，被配置为向第三方设备发送访问密码和受访设备的设备标识，第三方设备用于将访问密码和设备标识进行绑定并保存。

在一种可能的实施例中，该装置还包括：更改模块 1012 和第三发送模块 1014。

该更改模块 1012，被配置为定期更改访问密码，得到更改后的访问密码。

该第三发送模块 1014，被配置为将更改后的访问密码以及受访设备的设备标识发送给第三方设备，第三方设备将预存的设备标识所绑定的访问密码更新绑定为更改后的访问密码。

综上所述，本公开实施例中提供的访问认证装置，通过接收访问设备发送的访问密码，检测到访问密码与受访设备生成的访问密码相同后，允许该访问设备访问受访设备；由于受访设备接收访问密码后需要进行验证与生成的访问密码相同后才能允许访问设备访问，因此解决了若不对访问密码进行验证，受访设备在更改访问密码后，访问设备仍能够访问受访设备，安全性低的问题；达到了提高受访设备安全性的效果。

图 11 是根据再一示例性实施例示出的一种访问认证装置的框图，如图 11 所示，该访问认证装置应用于图 1 所示实施环境中的第三方设备 160 中。该访问认证装置包括但不限于：第二接收模块 1102、第四发送模块 1104 和第五发送模块 1106。

该第二接收模块 1102，被配置为接收访问设备发送的受访设备的设备标识和访问设备的用户帐号。

该第四发送模块 1104, 被配置为在检测到设备标识绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求, 鉴权请求用于请求允许访问设备访问受访设备。

5 该第五发送模块 1106, 被配置为在接收到登录端根据鉴权请求反馈的允许访问应答后, 向访问设备发送与设备标识对应的访问密码, 访问设备用于根据访问密码访问受访设备, 允许访问应答用于指示允许访问设备访问受访设备。

综上所述, 本公开实施例中提供的访问认证装置, 通过接收访问设备发送的设备标识和访问设备的用户帐号, 在检测到设备标识被绑定后向登录端发送鉴权请求, 在接收到登录端反馈的允许访问应答后向访问设备发送与设备标识对应的访问密码; 由于需要登录端
10 允许后, 第三方设备才能将访问密码发送给访问设备, 因此解决了非法使用者获取到访问密码后, 就能利用该访问密码对该 Wi-Fi 智能设备进行访问, 安全性比较差的问题; 达到了提高受访设备安全性的效果。

图 12 是根据再一示例性实施例示出的一种访问认证装置的框图, 如图 12 所示, 该访问认证装置应用于图 1 所示实施环境中的第三方设备 160 中。该访问认证装置包括但不限于: 第二接收模块 1202、第四发送模块 1204 和第五发送模块 1206。
15

该第二接收模块 1202, 被配置为接收访问设备发送的设备标识和访问设备的用户帐号。

该第四发送模块 1204, 被配置为在检测到设备标识绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求, 鉴权请求用于请求允许访问设备访问受访设备。
20

该第五发送模块 1206, 被配置为在接收到登录端根据鉴权请求反馈的允许访问应答后, 向访问设备发送与设备标识对应的访问密码, 访问设备用于根据访问密码访问受访设备, 允许访问应答用于指示允许访问设备访问受访设备。

25 在一种可能的实施例中, 该装置还包括: 第二检测模块 1208 和第一绑定模块 1210。

该第二检测模块 1208, 被配置为检测设备标识是否绑定有用户帐号。

该第一绑定模块 1210, 被配置为在第二检测模块 1208 检测出设备标识未绑定有用户帐号时, 将设备标识和访问设备的用户帐号进行绑定, 将访问设备确定为登录端。

30 在一种可能的实施例中, 该第四发送模块 1204 可以包括: 检测子模块 1204a 和发送子模块 1204b。

该检测子模块 1204a, 被配置为在第二检测模块 1208 检测到设备标识绑定有用户帐号时, 检测访问设备的用户帐号是否与设备标识所绑定的用户帐号相同。

该发送子模块 1204b, 被配置为在检测子模块 1204a 检测出访问设备的用户帐号与设备标识所绑定的用户帐号不同时, 向与设备标识绑定的用户帐号的登录端发送鉴权请求。

35 在一种可能的实施例中, 该第五发送模块 1206 还被配置为在检测子模块 1204a 检测

出访问设备的用户帐号与设备标识所绑定的用户帐号相同时，向访问设备发送与设备标识对应的访问密码。

在一种可能的实施例中，该装置还包括：第三接收模块 1212 和第二绑定模块 1214。

该第三接收模块 1212，被配置为接收受访设备发送的访问密码和受访设备的设备标识。

该第二绑定模块 1214，被配置为当受访设备的设备标识不存在绑定的访问密码时，将访问密码和受访设备的设备标识进行绑定并保存。

在一种可能的实施例中，该装置还包括：第三检测模块 1216 和第三绑定模块 1218。

该第三检测模块 1216，被配置为当受访设备的设备标识存在绑定的访问密码时，检测接收到的访问密码是否与绑定的访问密码相同。

该第三绑定模块 1218，被配置为当接收到的访问密码与绑定的访问密码不同时，设备标识绑定的访问密码更新绑定为接收到的访问密码。

综上所述，本公开实施例中提供的访问认证装置，通过接收访问设备发送的设备标识和访问设备的用户帐号，在检测到设备标识被绑定后向登录端发送鉴权请求，在接收到登录端反馈的允许访问应答后向访问设备发送与设备标识对应的访问密码；由于需要登录端允许后，第三方设备才能将访问密码发送给访问设备，因此解决了非法使用者获取到访问密码后，就能利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图 13 是根据一示例性实施例示出的一种访问认证系统的框图，如图 13 所示，该访问认证系统应用于图 1 所示实施环境中。该访问认证系统包括但不限于：受访设备 1302、访问设备 1304 和第三方设备 1306。

该受访设备 1302 包括图 9 或图 10 中所描述的访问认证装置。

该访问设备 1304 包括图 7 或图 8 中所描述的访问认证装置。

该第三方设备 1306 包括图 11 或图 12 中所描述的访问认证装置。

综上所述，本公开实施例中提供的访问认证系统，通过利用访问设备获取受访设备的设备标识，向第三方设备发送设备标识和访问设备的用户帐号，在第三方设备向登录端询问确定允许访问设备访问受访设备后，接收第三方设备向访问设备发送的访问密码，并根据访问密码访问受访设备；由于访问设备访问受访设备时需要通过登录端允许，因此解决了由于需要用户在手机 App 上手动输入访问密码，非法使用者很容易获取到该访问密码，并利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

本公开实施例中提供的访问认证系统，通过接收访问设备发送的访问密码，在检测到访问密码与受访设备生成的访问密码相同后，允许该访问设备访问受访设备；由于受访设备接收访问密码后需要在验证与生成的访问密码相同后才允许访问设备访问，因此解决了若不对访问密码进行验证，受访设备在更改访问密码后，访问设备仍能够访问受访设备，安全性低的问题；达到了提高受访设备安全性的效果。

本公开实施例中提供的访问认证系统，通过接收访问设备发送的设备标识和访问设备的用户帐号，在检测到设备标识被绑定后向登录端发送鉴权请求，在接收到登录端反馈的允许访问应答后向访问设备发送与设备标识对应的访问密码；由于需要登录端允许后，第三方设备才能将访问密码发送给访问设备，因此解决了非法使用者获取到访问密码后，就能利用该访问密码对该 Wi-Fi 智能设备进行访问，安全性比较差的问题；达到了提高受访设备安全性的效果。

关于上述实施例中的系统，其执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

本公开一示例性实施例提供了一种访问认证装置，应用于访问设备中，能够实现本公开提供的访问认证方法，该访问认证装置包括：处理器、用于存储处理器可执行指令的存储器；

其中，处理器被配置为：

获取受访设备的设备标识；

向第三方设备发送设备标识和访问设备的用户帐号；

接收访问密码，根据访问密码访问受访设备，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码，鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

本公开一示例性实施例提供了一种访问认证装置，应用于受访设备中，能够实现本公开提供的访问认证方法，该访问认证装置包括：处理器、用于存储处理器可执行指令的存储器；

其中，处理器被配置为：

接收访问设备发送的访问密码，访问密码是第三方设备在接收到访问设备发送的设备标识和访问设备的用户帐号，在设备标识已绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，在

接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送的与设备标识对应的访问密码，鉴权请求用于请求允许访问设备访问受访设备，允许访问应答用于指示允许访问设备访问受访设备；

检测访问密码是否与受访设备生成的访问密码相同；

5 在检测出访问密码与受访设备生成的访问密码相同时，允许访问设备访问受访设备。

本公开一示例性实施例提供了一种访问认证装置，应用于第三方设备中，能够实现本公开提供的访问认证方法，该访问认证装置包括：处理器、用于存储处理器可执行指令的存储器；

10 其中，处理器被配置为：

接收访问设备发送的设备标识和访问设备的用户帐号；

在检测到设备标识绑定有用户帐号且访问设备的用户帐号与设备标识所绑定的用户帐号不同时，向与设备标识绑定的用户帐号的登录端发送鉴权请求，鉴权请求用于请求允许访问设备访问受访设备；

15 在接收到登录端根据鉴权请求反馈的允许访问应答后，向访问设备发送与设备标识对应的访问密码，访问设备用于根据访问密码访问受访设备，允许访问应答用于指示允许访问设备访问受访设备。

20 图 14 是根据一示例性实施例示出的一种用于访问受访设备的装置的框图。例如，装置 1400 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

参照图 14，装置 1400 可以包括以下一个或多个组件：处理组件 1402，存储器 1404，电源组件 1406，多媒体组件 1408，音频组件 1410，输入/输出（I/O）接口 1412，传感器组件 1414，以及通信组件 1416。

25 处理组件 1402 通常控制装置 1400 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 1402 可以包括一个或多个处理器 1418 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 1402 可以包括一个或多个模块，便于处理组件 1402 和其他组件之间的交互。例如，处理组件 1402 可以包括多媒体模块，以方便多媒体组件 1408 和处理组件 1402 之间的交互。

30 存储器 1404 被配置为存储各种类型的数据以支持在装置 1400 的操作。这些数据的示例包括用于在装置 1400 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 1404 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），
35 磁存储器，快闪存储器，磁盘或光盘。

电源组件 1406 为装置 1400 的各种组件提供电力。电源组件 1406 可以包括电源管理系统，一个或多个电源，及其他与为装置 1400 生成、管理和分配电力相关联的组件。

多媒体组件 1408 包括在装置 1400 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器（LCD）和触摸面板（TP）。如果屏幕包括触摸面板，
5 屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 1408 包括一个前置摄像头和/或后置摄像头。当装置 1400 处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头
10 和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

音频组件 1410 被配置为输出和/或输入音频信号。例如，音频组件 1410 包括一个麦克风（MIC），当装置 1400 处于操作模式，如呼叫模式、记录模式和语音识别模式时，
麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 1404
或经由通信组件 1416 发送。在一些实施例中，音频组件 1410 还包括一个扬声器，用于输出
15 音频信号。

I/O 接口 1412 为处理组件 1402 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 1414 包括一个或多个传感器，用于为装置 1400 提供各个方面的状态评估。
20 例如，传感器组件 1414 可以检测到装置 1400 的打开/关闭状态，组件的相对定位，例如组件为装置 1400 的显示器和小键盘，传感器组件 1414 还可以检测装置 1400 或装置 1400 一个组件的位置改变，用户与装置 1400 接触的存在或不存在，装置 1400 方位或加速/减速和装置 1400 的温度变化。传感器组件 1414 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 1414 还可以包括光传感器，如 CMOS
25 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 1414 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

通信组件 1416 被配置为便于装置 1400 和其他设备之间有线或无线方式的通信。装置 1400 可以接入基于通信标准的无线网络，如 Wi-Fi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 1416 经由广播信道接收来自外部广播管理系统的广播信号或广播
30 相关信息。在一个示例性实施例中，通信组件 1416 还包括近场通信（NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

在示例性实施例中，装置 1400 可以被一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行以
35

访问设备或受访设备为执行主体的访问认证方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 1404，上述指令可由装置 1400 的处理器 1418 执行以完成以访问设备或受访设备为执行主体的访问认证方法。例如，非临时性计算机可读存储介质可以是 ROM、

5 随机存取存储器（RAM）、CD-ROM、磁带、软盘和光数据存储设备等。

图 15 是根据一示例性实施例示出的一种用于验证访问设备的装置的框图。例如，装置 1500 可以被提供为一服务器。参照图 15，装置 1500 包括处理组件 1502，其进一步包括一个或多个处理器，以及由存储器 1504 所代表的存储器资源，用于存储可由处理组件 10 1502 的执行的指令，例如应用程序。存储器 1504 中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件 1502 被配置为执行指令，以执行以第三方设备为执行主体的访问认证方法。

装置 1500 还可以包括一个电源组件 1506 被配置为执行装置 1500 的电源管理，一个有线或无线网络接口 1508 被配置为将装置 1500 连接到网络，和一个输入输出（I/O）接口 1510。装置 1500 可以操作基于存储在存储器 1504 的操作系统，例如 Windows Server™，15 Mac OS X™，Unix™，Linux™，FreeBSD™ 或类似。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者 20 适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

权利要求

1、一种访问认证方法，其特征在于，应用于访问设备中，所述方法包括：

获取受访设备的设备标识；

向第三方设备发送所述设备标识和所述访问设备的用户帐号；

5 接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问
10 密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

2、根据权利要求1所述的方法，其特征在于，所述获取受访设备的设备标识，包括：

接收所述受访设备广播发送的携带有所述受访设备的设备标识的广播消息，从所述广

15 播消息中获取所述受访设备的设备标识；或，

通过扫描所述受访设备上的图形码获取所述受访设备的设备标识。

3、一种访问认证方法，其特征在于，应用于受访设备中，所述方法包括：

接收访问设备发送的访问密码，所述访问密码是第三方设备在接收到所述访问设备发
20 送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述
25 受访设备；

检测所述访问密码是否与所述受访设备生成的所述访问密码相同；

在检测出所述访问密码与所述受访设备生成的所述访问密码相同时，允许所述访问设备访问所述受访设备。

30 4、根据权利要求3所述的方法，其特征在于，所述方法还包括：

生成所述访问密码；

向所述第三方设备发送所述访问密码和所述受访设备的设备标识，所述第三方设备用于将所述访问密码和所述设备标识进行绑定并保存。

35 5、根据权利要求4所述的方法，其特征在于，所述方法还包括：

定期更改所述访问密码，得到更改后的访问密码；

将更改后的访问密码以及所述受访设备的设备标识发送给第三方设备，所述第三方设备将预存的所述设备标识所绑定的访问密码更新绑定为所述更改后的访问密码。

5 6、一种访问认证方法，其特征在于，应用于第三方设备中，所述方法包括：

接收访问设备发送的受访设备的设备标识和所述访问设备的用户帐号；

在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，所述鉴权请求用于请求允许所述访问设备访问所述受访设备；

10 在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送与所述设备标识对应的访问密码，所述访问设备用于根据所述访问密码访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

7、根据权利要求6所述的方法，其特征在于，所述方法还包括：

15 检测所述设备标识是否绑定有用户帐号；

在检测出所述设备标识未绑定有用户帐号时，将所述设备标识和所述访问设备的用户帐号进行绑定，将所述访问设备确定为所述登录端。

8、根据权利要求6所述的方法，其特征在于，所述在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，包括：

在检测到所述设备标识绑定有用户帐号时，检测所述访问设备的用户帐号是否与所述设备标识所绑定的用户帐号相同；

25 在检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，执行所述向与所述设备标识绑定的用户帐号的登录端发送鉴权请求的步骤。

9、根据权利要求8所述的方法，其特征在于，所述向所述访问设备发送与所述设备标识对应的访问密码，包括：

30 在检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号相同时，执行所述向所述访问设备发送与所述设备标识对应的访问密码的步骤。

10、根据权利要求6至9中任一所述的方法，其特征在于，所述方法还包括：

接收所述受访设备发送的所述访问密码和所述受访设备的设备标识；

35 当所述受访设备的设备标识不存在绑定的访问密码时，将所述访问密码和所述受访设备的设备标识进行绑定并保存。

11、根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

当所述受访设备的设备标识存在绑定的访问密码，检测接收到的所述访问密码是否与绑定的访问密码相同；

5 当接收到的所述访问密码与绑定的访问密码不同时，所述设备标识绑定的访问密码更新绑定为接收到的所述访问密码。

12、一种访问认证装置，其特征在于，应用于访问设备中，所述装置包括：

获取模块，被配置为获取受访设备的设备标识；

10 第一发送模块，被配置为向第三方设备发送所述设备标识和所述访问设备的用户帐号；

访问模块，被配置为接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

20 13、根据权利要求 12 所述的装置，其特征在于，所述获取模块，包括：

第一获取子模块，被配置为接收所述受访设备广播发送的携带有所述受访设备的设备标识的广播消息，从所述广播消息中获取所述受访设备的设备标识；或，

第二获取子模块，被配置为通过扫描所述受访设备上的图形码获取所述受访设备的设备标识。

25

14、一种访问认证装置，其特征在于，应用于受访设备中，所述装置包括：

第一接收模块，被配置为接收访问设备发送的访问密码，所述访问密码是第三方设备在接收到所述访问设备发送的设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时，向与
30 所述设备标识绑定的用户帐号的登录端发送鉴权请求，在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后，向所述访问设备发送的与所述设备标识对应的访问密码，所述鉴权请求用于请求允许所述访问设备访问所述受访设备，所述允许访问应答用于指示允许所述访问设备访问所述受访设备；

第一检测模块，被配置为检测所述访问密码是否与所述受访设备生成的所述访问密码
35 相同；

允许模块,被配置为在所述第一检测模块检测出所述访问密码与所述受访设备生成的所述访问密码相同时,允许所述访问设备访问所述受访设备。

15、根据权利要求 14 所述的装置,其特征在于,所述装置还包括:

5 生成模块,被配置为生成所述访问密码;

第二发送模块,被配置为向所述第三方设备发送所述访问密码和所述受访设备的设备标识,所述第三方设备用于将所述访问密码和所述设备标识进行绑定并保存。

16、根据权利要求 15 所述的装置,其特征在于,所述装置还包括:

10 更改模块,被配置为定期更改所述访问密码,得到更改后的访问密码;

第三发送模块,被配置为将更改后的访问密码以及所述受访设备的设备标识发送给第三方设备,所述第三方设备将预存的所述设备标识所绑定的访问密码更新绑定为所述更改后的访问密码。

15 17、一种访问认证装置,其特征在于,应用于第三方设备中,所述装置包括:

第二接收模块,被配置为接收访问设备发送的受访设备的设备标识和所述访问设备的用户帐号;

20 第四发送模块,被配置为在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,所述鉴权请求用于请求允许所述访问设备访问所述受访设备;

第五发送模块,被配置为在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送与所述设备标识对应的访问密码,所述访问设备用于根据所述访问密码访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

25

18、根据权利要求 17 所述的装置,其特征在于,所述装置还包括:

第二检测模块,被配置为检测所述设备标识是否绑定有用户帐号;

30 第一绑定模块,被配置为在所述第二检测模块检测出所述设备标识未绑定有用户帐号时,将所述设备标识和所述访问设备的用户帐号进行绑定,将所述访问设备确定为所述登录端。

19、根据权利要求 17 所述的装置,其特征在于,所述第四发送模块,包括:

检测子模块,被配置为在所述第二检测模块检测到所述设备标识绑定有用户帐号时,检测所述访问设备的用户帐号是否与所述设备标识所绑定的用户帐号相同;

35 发送子模块,被配置为在所述检测子模块检测出所述访问设备的用户帐号与所述设备

标识所绑定的用户帐号不同时，向与所述设备标识绑定的用户帐号的登录端发送鉴权请求。

20、根据权利要求 19 所述的装置，其特征在于，

5 所述第五发送模块，还被配置为在所述检测子模块检测出所述访问设备的用户帐号与所述设备标识所绑定的用户帐号相同时，向所述访问设备发送与所述设备标识对应的访问密码。

21、根据权利要求 17 至 20 中任一所述的装置，其特征在于，所述装置还包括：

10 第三接收模块，被配置为接收所述受访设备发送的所述访问密码和所述受访设备的设备标识；

第二绑定模块，被配置为当所述受访设备的设备标识不存在绑定的访问密码时，将所述访问密码和所述受访设备的设备标识进行绑定并保存。

15 22、根据权利要求 21 所述的装置，其特征在于，所述装置还包括：

第三检测模块，被配置为当所述受访设备的设备标识存在绑定的访问密码时，检测接收到的所述访问密码是否与绑定的访问密码相同；

第三绑定模块，被配置为当接收到的所述访问密码与绑定的访问密码不同时，所述设备标识绑定的访问密码更新绑定为接收到的所述访问密码。

20

23、一种访问认证系统，其特征在于，所述访问认证系统包括访问设备、受访设备和第三方设备；

所述访问设备包括如权利要求 12 或 13 所述的访问认证装置；

所述受访设备包括如权利要求 14 至 16 中任一所述的访问认证装置；

25 所述第三方设备包括如权利要求 17 至 22 中任一所述的访问认证装置。

24、一种访问认证装置，其特征在于，应用于访问设备中，所述装置包括：
处理器；

用于存储所述处理器可执行指令的存储器；

30 其中，所述处理器被配置为：

获取受访设备的设备标识；

向第三方设备发送所述设备标识和所述访问设备的用户帐号；

35 接收所述访问密码，根据所述访问密码访问所述受访设备，所述访问密码是第三方设备在接收到所述访问设备发送的所述设备标识和所述访问设备的用户帐号，在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同

时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送的与所述设备标识对应的访问密码,所述鉴权请求用于请求允许所述访问设备访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

5

25、一种访问认证装置,其特征在于,应用于受访设备中,所述装置包括:
处理器;

用于存储所述处理器可执行指令的存储器;

其中,所述处理器被配置为:

10 接收访问设备发送的访问密码,所述访问密码是第三方设备在接收到所述访问设备发送的设备标识和所述访问设备的用户帐号,在所述设备标识已绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送的与所述设备标识对应的访问密码,所述鉴权请求用于请求允许
15 所述访问设备访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备;

检测所述访问密码是否与所述受访设备生成的所述访问密码相同;

在检测出所述访问密码与所述受访设备生成的所述访问密码相同时,允许所述访问设备访问所述受访设备。

20

26、一种访问认证装置,其特征在于,应用于第三方设备中,所述装置包括:
处理器;

用于存储所述处理器可执行指令的存储器;

其中,所述处理器被配置为:

25 接收访问设备发送的设备标识和所述访问设备的用户帐号;

在检测到所述设备标识绑定有用户帐号且所述访问设备的用户帐号与所述设备标识所绑定的用户帐号不同时,向与所述设备标识绑定的用户帐号的登录端发送鉴权请求,所述鉴权请求用于请求允许所述访问设备访问所述受访设备;

在接收到所述登录端根据所述鉴权请求反馈的允许访问应答后,向所述访问设备发送
30 与所述设备标识对应的访问密码,所述访问设备用于根据所述访问密码访问所述受访设备,所述允许访问应答用于指示允许所述访问设备访问所述受访设备。

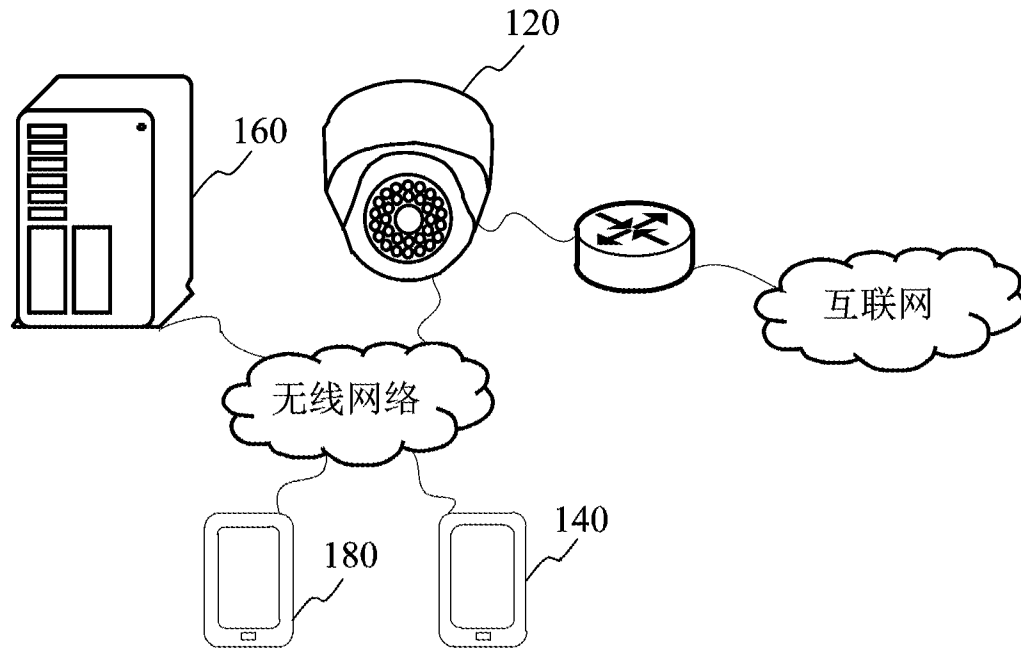


图1

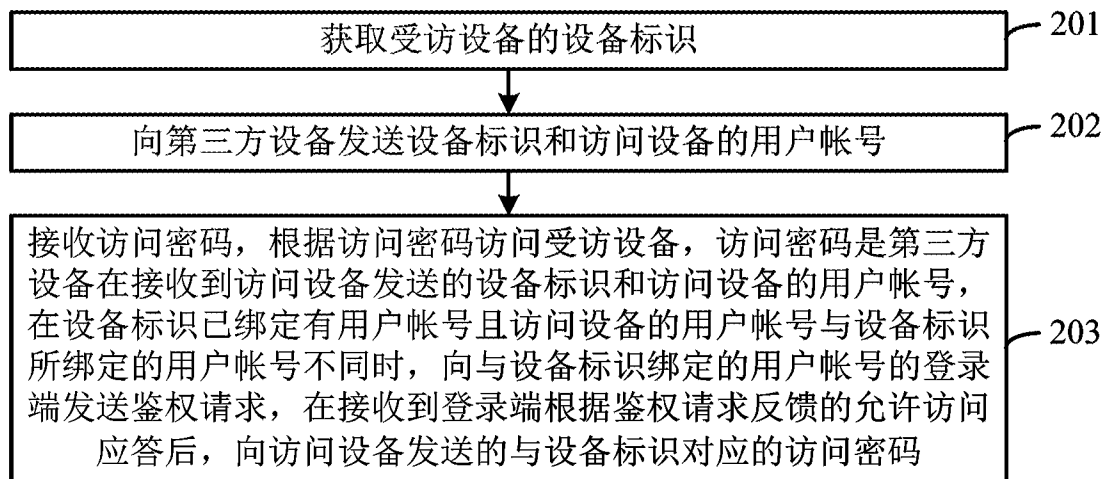


图2

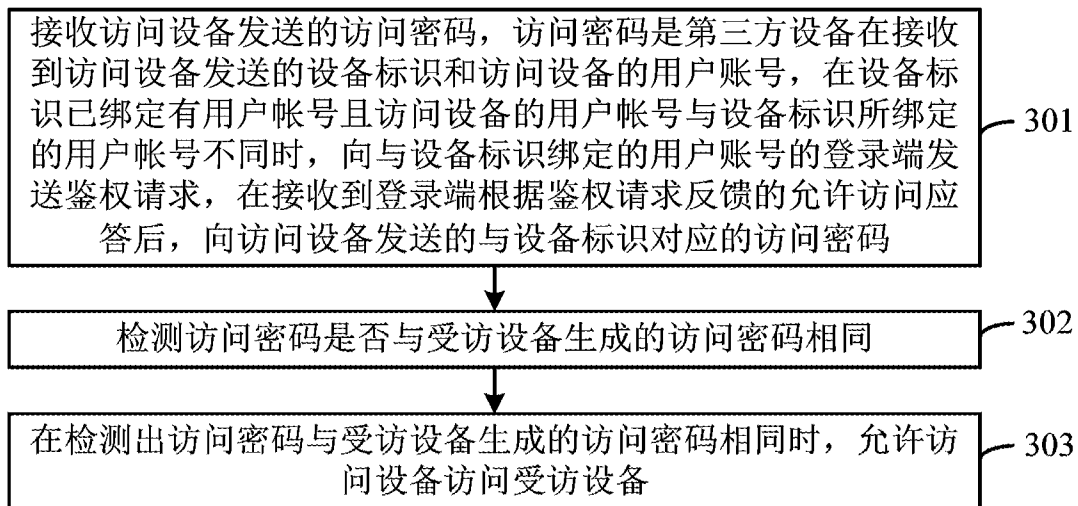


图3

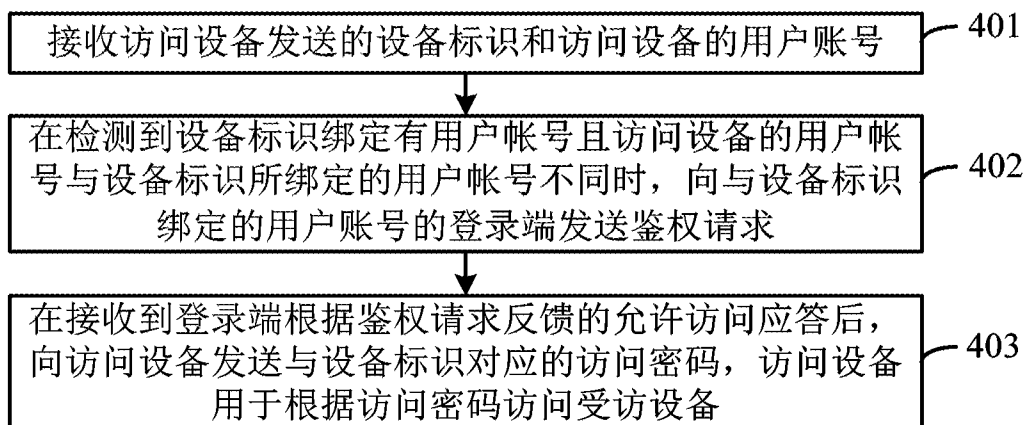


图4

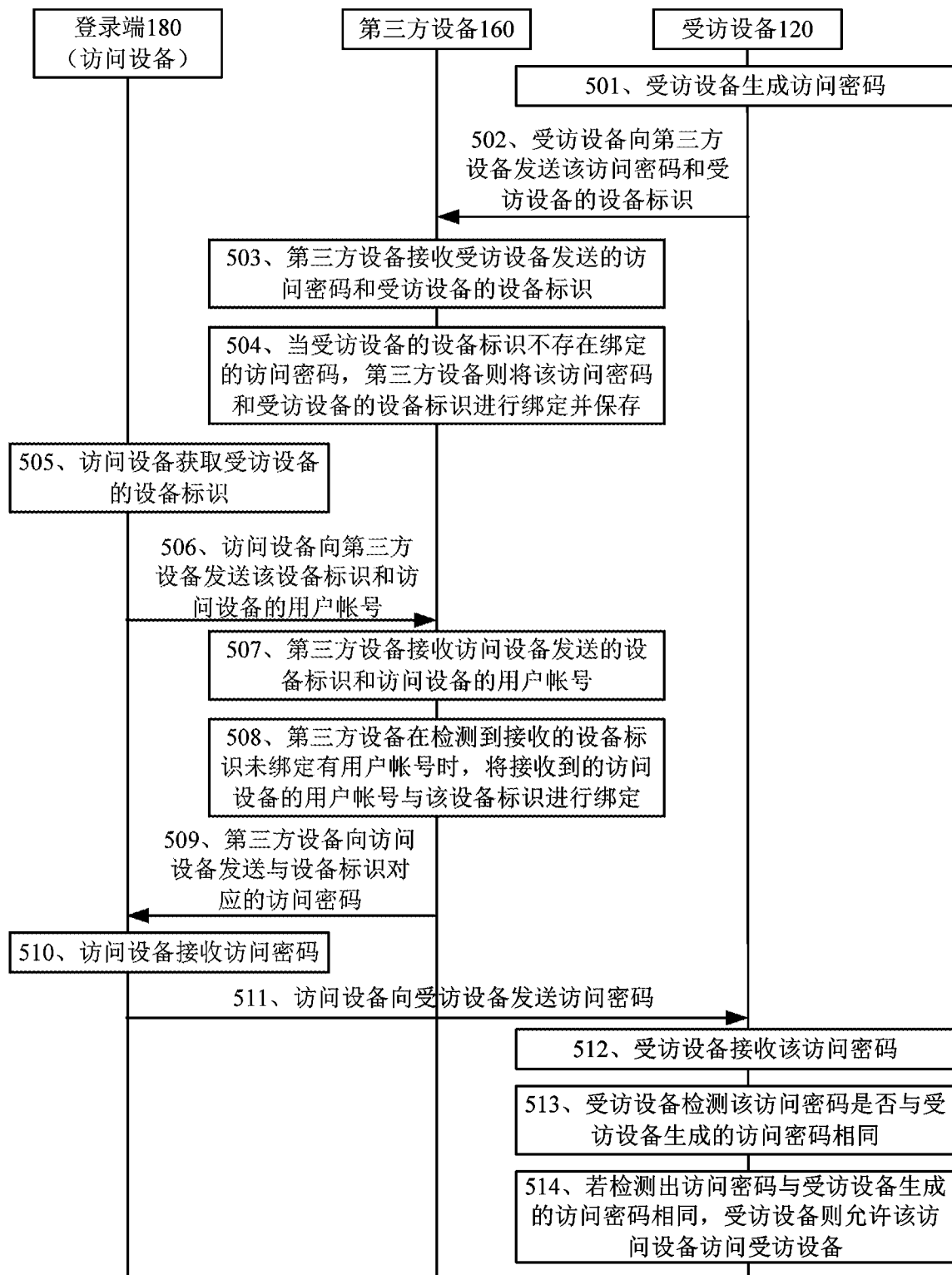


图5A

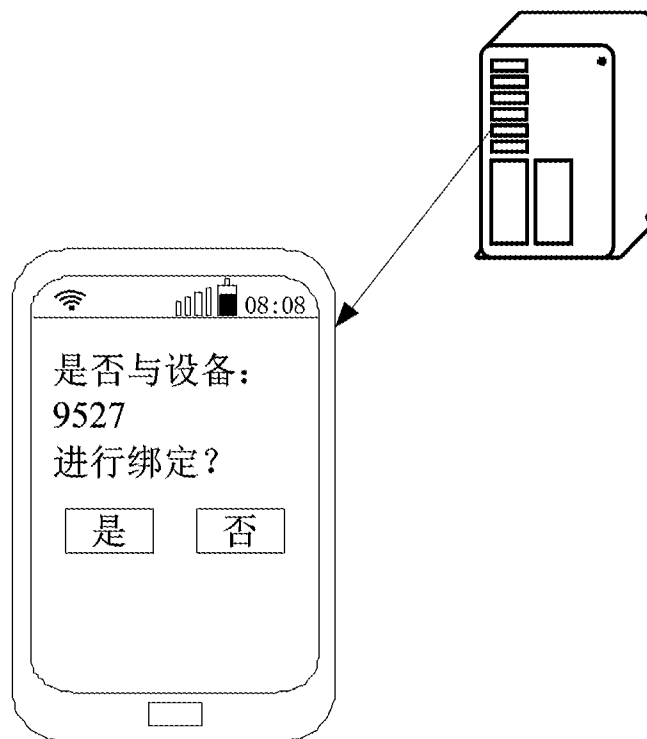


图5B

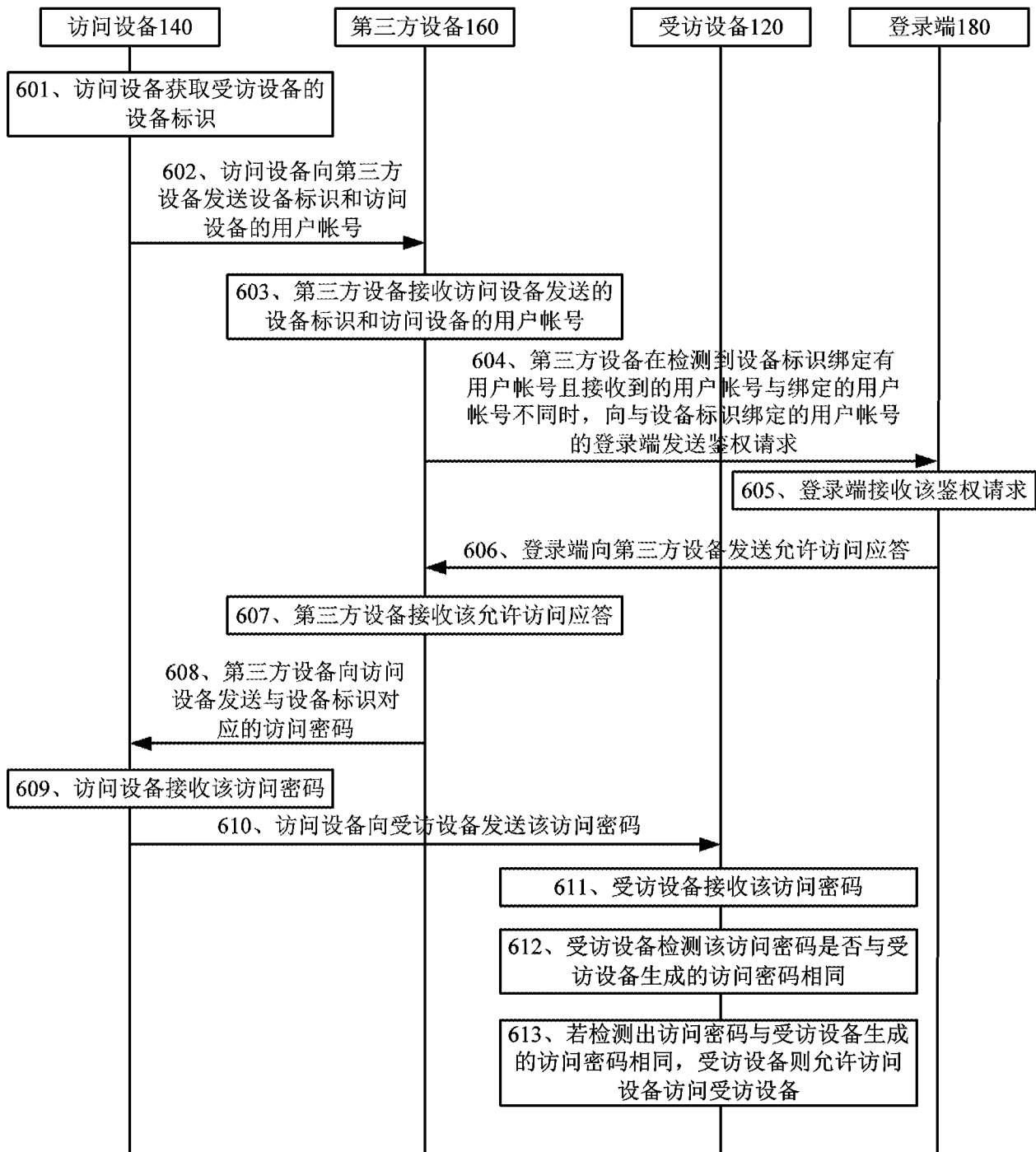


图6A

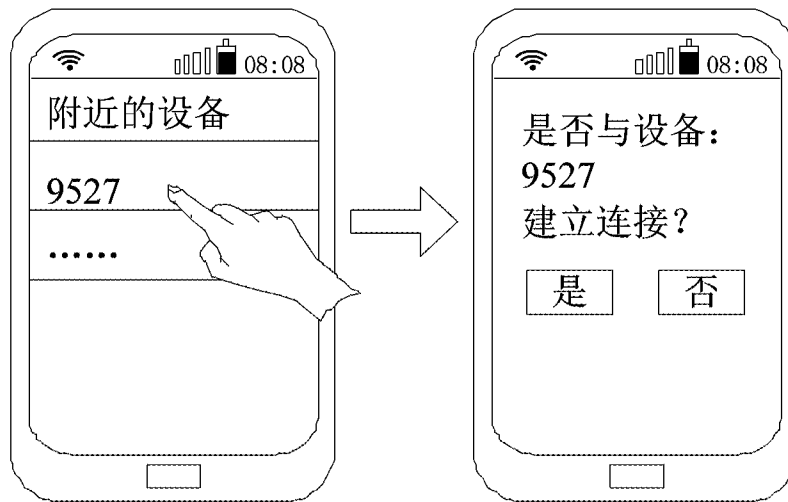


图6B

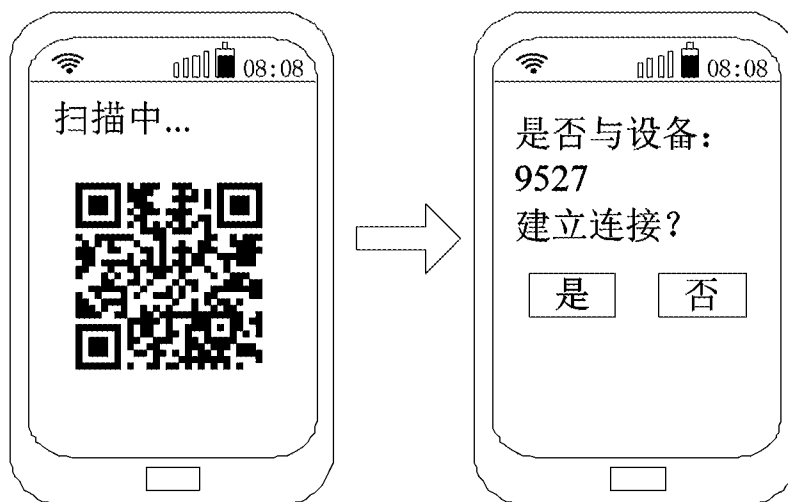


图6C

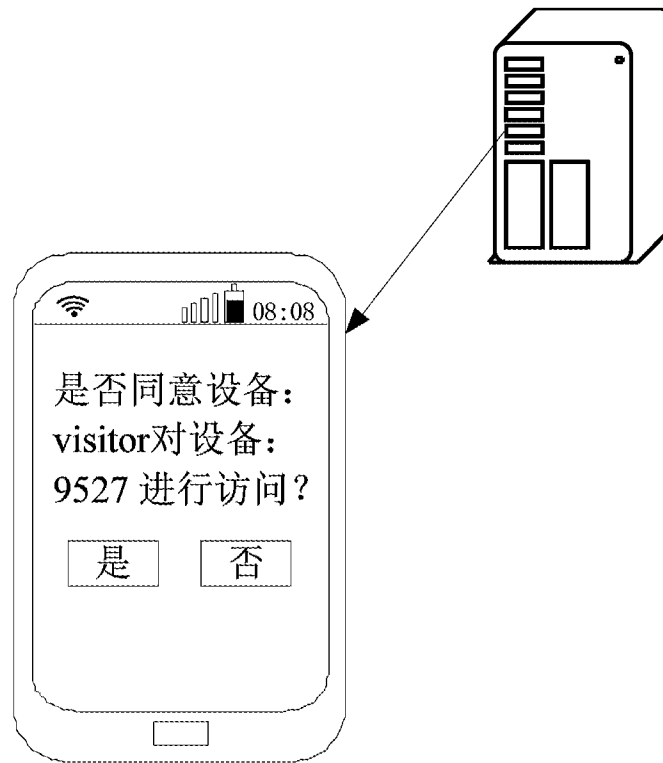


图6D

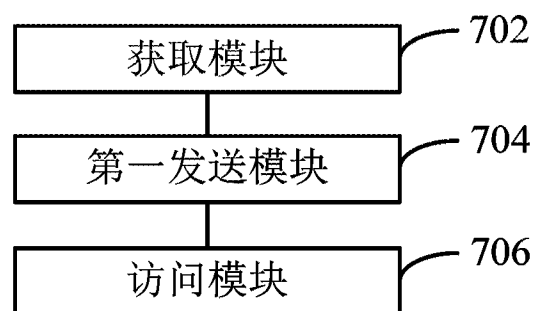


图7

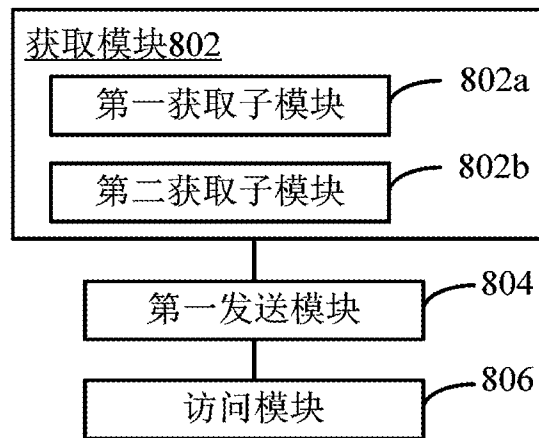


图8

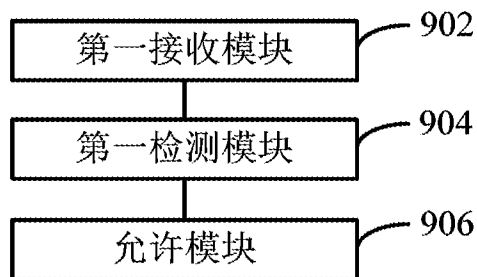


图9

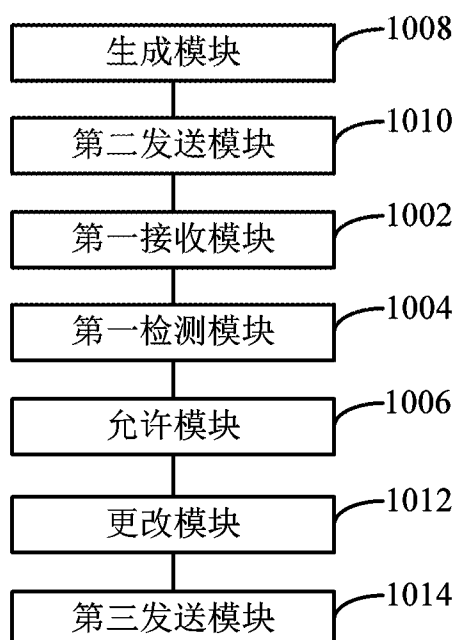


图10

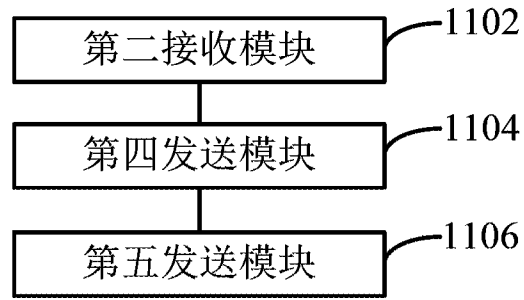


图11

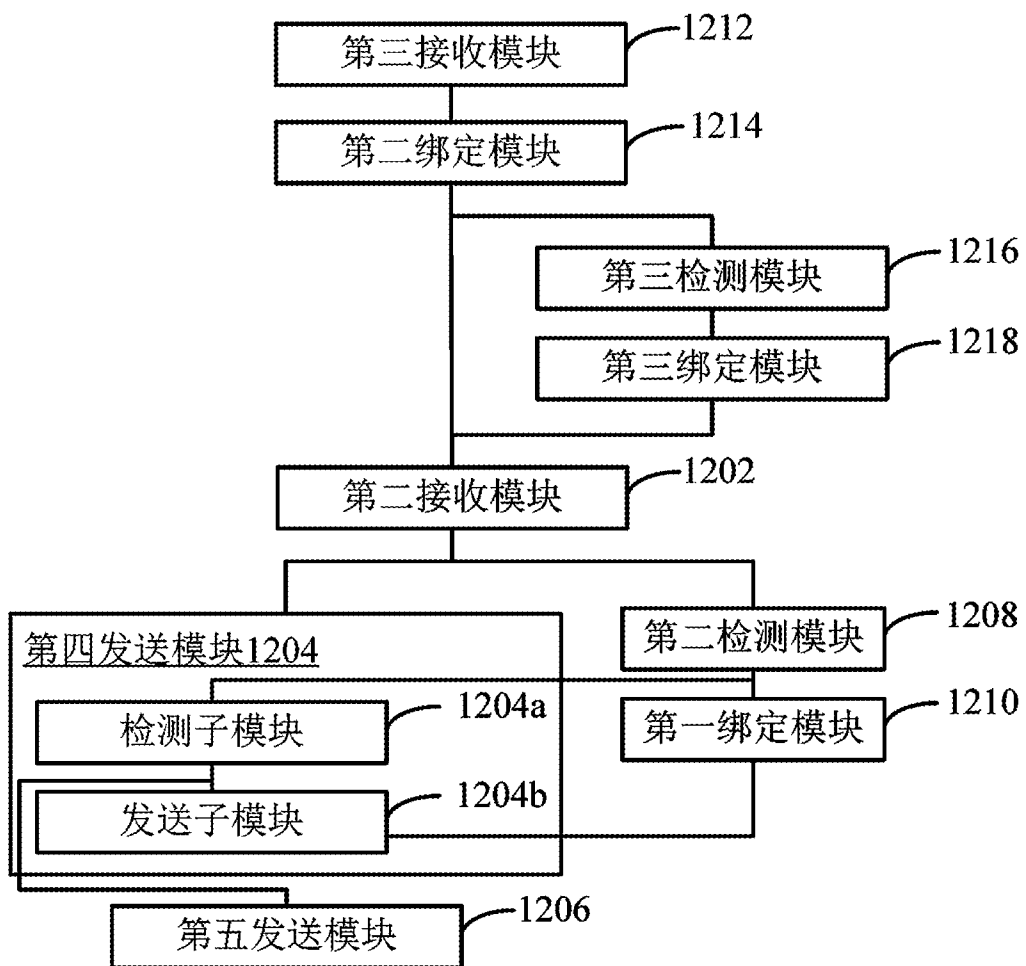


图12

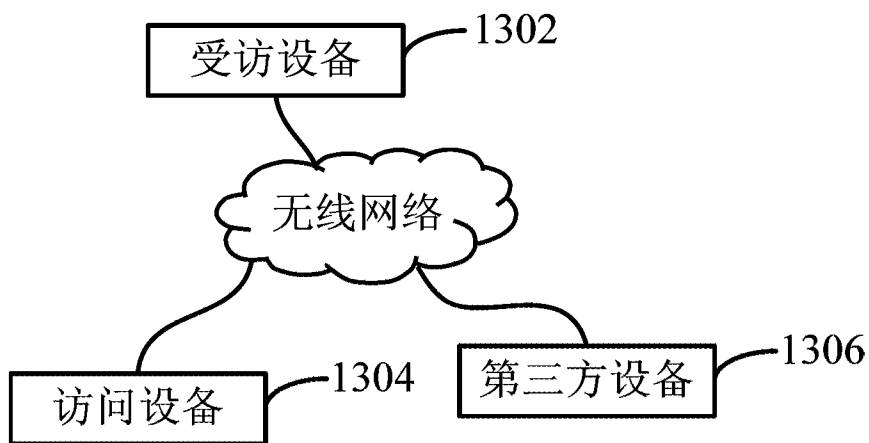


图13

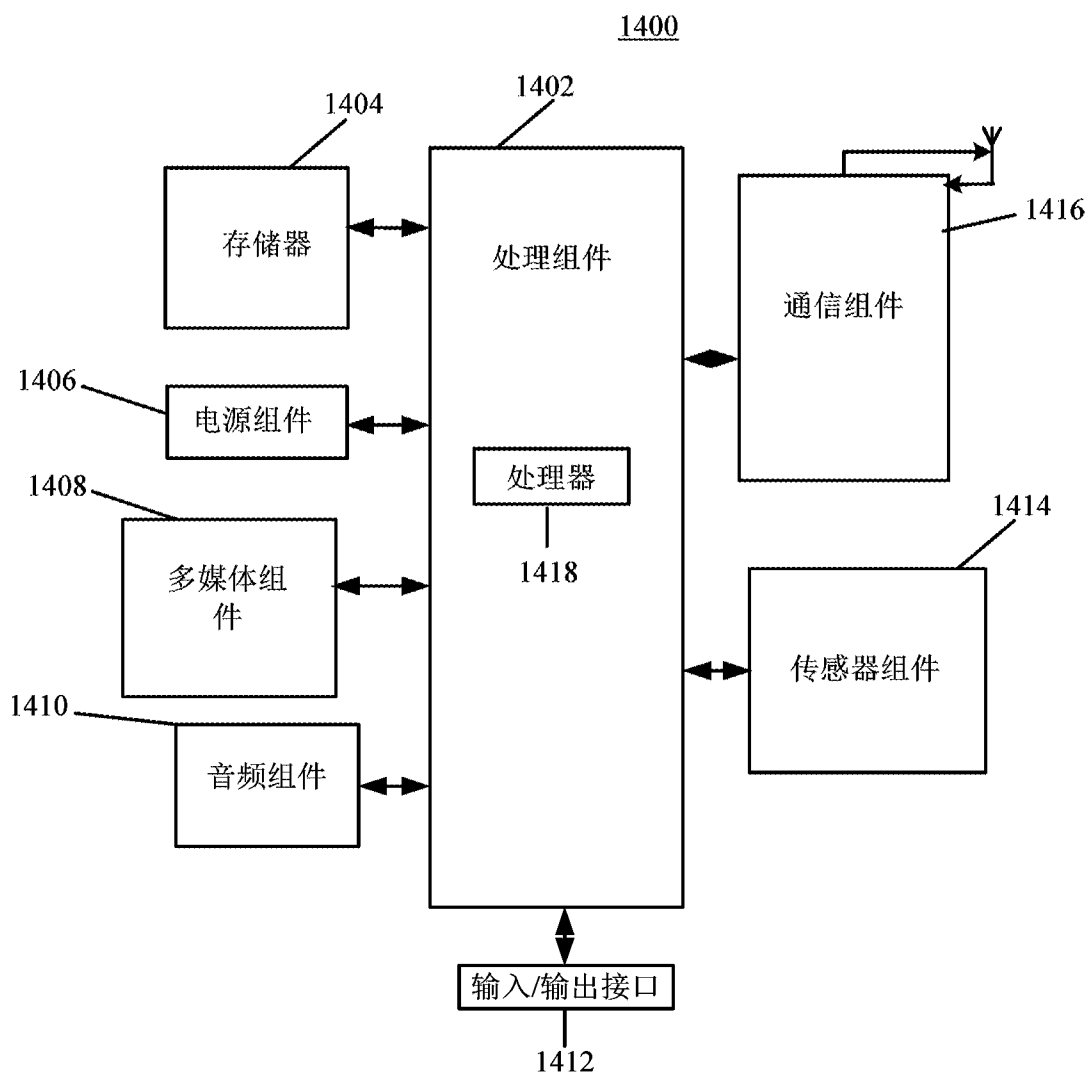


图14

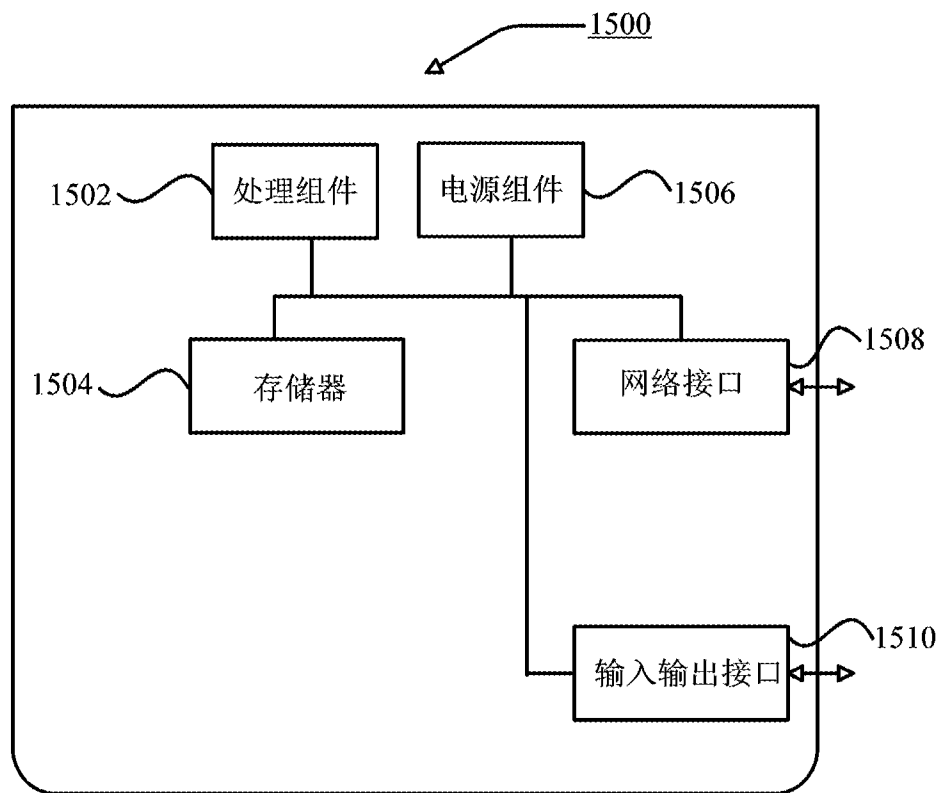


图15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/074876

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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; H04Q; H04W; G06F

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, CNKI, VEN: third party, binding, APP, server, account, access, control+, wifi, intelligent, device, password, authenticate, home

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104202306 A (XIAOMI TECHNOLOGY CO., LTD.), 10 December 2014 (10.12.2014), description, paragraphs [0124]-[0323], and figures 1-15	1-26
A	CN 103078875 A (COMPUTER NETWORK INFORMATION CENTER, CHINESE ACADEMY OF SCIENCES), 01 May 2013 (01.05.2013), the whole document	1-26
A	CN 103761597 A (STAR SOFTCOMM (CHINA) LTD.), 30 April 2014 (30.04.2014), the whole document	1-26
A	CN 103716161 A (KYUNG DONG ONE CO., LTD.), 09 April 2014 (09.04.2014), the whole document	1-26
A	US 2014098247 A1 (IP HOLDINGS, INC.), 10 April 2014 (10.04.2014), the whole document	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 04 June 2015 (04.06.2015)	Date of mailing of the international search report 30 June 2015 (30.06.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Junjie Telephone No.: (86-10) 62089562

International application No.
PCT/CN2015/074876

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																				
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; H04Q; H04W; G06F 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, CNKI, VEN: 智能, 设备, 家居, 访问, 接入, 控制, 第三方, 服务器, 账号, 密码, 鉴权, 绑定, APP, server, account, access, control+, wifi, intelligent, device, password, authenticate, home																				
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>CN 104202306 A (小米科技有限责任公司) 2014年 12月 10日 (2014 - 12 - 10) 说明书第[0124]-[0323]段, 附图1-15</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>CN 103078875 A (中国科学院计算机网络信息中心) 2013年 5月 1日 (2013 - 05 - 01) 全文</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>CN 103761597 A (北京软通科技有限责任公司) 2014年 4月 30日 (2014 - 04 - 30) 全文</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>CN 103716161 A (株庆东ONE) 2014年 4月 9日 (2014 - 04 - 09) 全文</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>US 2014098247 A1 (IP HOLDINGS, INC.) 2014年 4月 10日 (2014 - 04 - 10) 全文</td> <td>1-26</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	CN 104202306 A (小米科技有限责任公司) 2014年 12月 10日 (2014 - 12 - 10) 说明书第[0124]-[0323]段, 附图1-15	1-26	A	CN 103078875 A (中国科学院计算机网络信息中心) 2013年 5月 1日 (2013 - 05 - 01) 全文	1-26	A	CN 103761597 A (北京软通科技有限责任公司) 2014年 4月 30日 (2014 - 04 - 30) 全文	1-26	A	CN 103716161 A (株庆东ONE) 2014年 4月 9日 (2014 - 04 - 09) 全文	1-26	A	US 2014098247 A1 (IP HOLDINGS, INC.) 2014年 4月 10日 (2014 - 04 - 10) 全文	1-26
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 104202306 A (小米科技有限责任公司) 2014年 12月 10日 (2014 - 12 - 10) 说明书第[0124]-[0323]段, 附图1-15	1-26																		
A	CN 103078875 A (中国科学院计算机网络信息中心) 2013年 5月 1日 (2013 - 05 - 01) 全文	1-26																		
A	CN 103761597 A (北京软通科技有限责任公司) 2014年 4月 30日 (2014 - 04 - 30) 全文	1-26																		
A	CN 103716161 A (株庆东ONE) 2014年 4月 9日 (2014 - 04 - 09) 全文	1-26																		
A	US 2014098247 A1 (IP HOLDINGS, INC.) 2014年 4月 10日 (2014 - 04 - 10) 全文	1-26																		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																				
国际检索实际完成的日期 2015年 6月 4日		国际检索报告邮寄日期 2015年 6月 30日																		
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451		授权官员 李俊洁 电话号码 (86-10)62089562																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/074876

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	104202306	A	2014年 12月 10日	无	
CN	103078875	A	2013年 5月 1日	无	
CN	103761597	A	2014年 4月 30日	无	
CN	103716161	A	2014年 4月 9日	无	
US	2014098247	A1	2014年 4月 10日	无	