(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 10 月 6 日 (06.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/155283 A1

(51) 国际专利分类号:
G06F 21/35 (2013.01) *H04L 29/06* (2006.01)
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2015/092018

(22) 国际申请日: 2015 年 10 月 15 日 (15.10.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510153178.4 2015 年 4 月 1 日 (01.04.2015) CN

(71) 申请人: 惠州 TCL 移动通信有限公司 (HUIZHOU TCL MOBILE COMMUNICATION CO.,LTD) [CN/CN]; 中国广东省惠州市仲恺高新区和畅七路西 86 号, Guangdong 516006 (CN)。

(72) 发明人: 黄严良 (HUANG, Yanliang); 中国广东省惠州市仲恺高新区和畅七路西 86 号, Guangdong 516006 (CN)。

(74) 代理人: 深圳市威世博知识产权代理事务所（普通合伙） (CHINA WISPRO INTELLECTUAL PROPERTY LLP.); 中国广东省深圳市南山区高新区粤兴三道 8 号中国地质大学产学研基地中地大楼 A806, Guangdong 518057 (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, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD AND SYSTEM FOR ELECTRONIC DEVICE PRIVACY PROTECTION BASED ON WIFI HOTSPOT

(54) 发明名称 : 基于 WIFI 热点实现电子设备私密保护的方法及系统

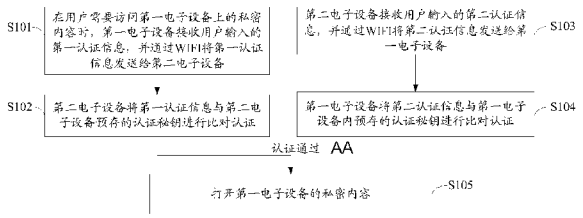

图 1

S101 When an access to private contents of a first electronic device is required by a user, the first electronic device receives first authentication information inputted by the user and transmits the first authentication information to a second electronic device via WIFI

S102 A second electronic device compares and authenticates the first authentication information with a prestored authentication key of the second electronic device

S103 The second electronic device receives second information inputted by the user, and transmits the second authentication information to the first electronic device via WIFI

S104 The first electronic device compares and authenticates the second authentication information with a prestored authentication key in the first electronic device

S105 Open private contents of the first electronic device

AA Authentication passed

(57) Abstract: Disclosed in the present invention are a method and system for electronic device privacy protection based on a WIFI hotspot. The method comprises: when an access to private contents of a first electronic device is required, receiving, by the first electronic device, first authentication information and transmitting the same to a second electronic device via WIFI; comparing and authenticating, by the second electronic device, the first authentication information with a prestored authentication key; receiving, by the second electronic device, the second authentication information, and transmitting the same to the first electronic device via WIFI; comparing and authenticating, by the first electronic device, the second authentication information with a prestored authentication key; if both the first authentication information and the second authentication information pass authentication, opening the private contents. The present invention can ensure security of private contents.

(57) 摘要: 本发明公开一种基于 WIFI 热点实现电子设备私密保护的方法及系统包括：在需要访问第一电子设备上的私密内容时，第一电子设备接收第一认证信息，通过 WIFI 发送给第二电子设备；第二电子设备将第一认证信息与预存的认证秘钥进行比对认证；第二电子设备接收第二认证信息，通过 WIFI 发送给第一电子设备；第一电子设备将第二认证信息与预存的认证秘钥进行比对认证；在第一认证信息与第二认证信息都通过认证时，打开私密内容。本发明能够保障私密内容的安全。

WO 2016/155283 A1

说明书

发明名称: 基于WIFI热点实现电子设备私密保护的方法及系统

[1] 【技术领域】

[2] 本发明涉及一种基于WIFI热点实现电子设备私密保护的方法及系统。

[3] 【背景技术】

[4] 随着现在生活的发展，人们对电子设备应用越来越广，拍照，录像，录音等等。常规的电子设备如手机、平板电脑、笔记本电脑等也变成一个容易外泄私密内容的一个重要的载体。人们也越来越注重手机内容的保密，但是依旧经常有人丢失电子设备，经常有电子设备私密内容外泄，给用户带来极大的困扰。

[5] 传统的私密内容保护，就是在自己的电子设备里面，设置某一个文件或者照片等为保护的对象，为其设置一个保护的密码，如想查看上锁的内容，需要输入相应的密码。这方能打开查看。但是这种方式的保护力度也不尽如人意。

[6] 【发明内容】

[7] 本发明主要解决的技术问题是解决现有技术中电子设备私密内容保护力度不够强而导致私密内容外泄的技术问题，提供一种基于WIFI热点实现电子设备私密保护的方法及系统，能够更有效的确保电子设备内的私密内容的安全，给用户更好的个人体验。

[8] 为解决上述技术问题，本发明采用的一个技术方案是：提供一种基于WIFI热点实现电子设备私密保护的方法，所述方法包括：第一电子设备与第二电子设备进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥；在用户需要访问所述第一电子设备上的私密内容时，所述第一电子设备接收用户输入的第一认证信息，并通过WIFI将所述第一认证信息发送给第二电子设备；所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果；所述第二电子设备接收用户输入的第二认证信息，并通过WIFI将所述第二认证信息发送给所述第一电子设备；所述第一电子设备将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；在所述第一认证信息与所述第二认证信息

都通过认证时，打开所述第一电子设备的私密内容。

[9] 其中，所述第一电子设备与第二电子设备进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥包括：所述第一电子设备与所述第二电子设备开启WIFI；所述第一电子设备接收用户输入的第一认证秘钥，通过WIFI将所述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；所述第二电子设备接收并保存所述第一认证秘钥；所述第二电子设备接收用户输入的第二认证秘钥，通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；所述第一电子设备接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[10] 其中，所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果包括：在所述第一认证信息通过认证时，通过WIFI向所述第一电子设备返回认证通过通知；在所述第一认证信息未通过认证时，通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[11] 为解决上述技术问题，本发明采用的另一个技术方案是：提供一种基于WIFI热点实现电子设备私密保护的方法，所述方法包括：在用户需要访问所述第一电子设备上的私密内容时，所述第一电子设备接收用户输入的第一认证信息，并通过WIFI将所述第一认证信息发送给第二电子设备；所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；所述第二电子设备接收用户输入的第二认证信息，并通过WIFI将所述第二认证信息发送给所述第一电子设备；所述第一电子设备将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；在所述第一认证信息与所述第二认证信息都通过认证时，打开所述第一电子设备的私密内容。

[12] 其中，所述方法还包括：所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥。

[13] 其中，所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥包括：所述第一电子设备与所述第二电子设备开启WIFI；所述第一电子设备接收用户输入的第一认证秘钥，通过WIFI将所

述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；所述第二电子设备接收并保存所述第一认证秘钥；所述第二电子设备接收用户输入的第二认证秘钥，通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；所述第一电子设备接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[14] 其中，所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证之后，还包括：所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果。

[15] 其中，所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果包括：在所述第一认证信息通过认证时，通过WIFI向所述第一电子设备返回认证通过通知；在所述第一认证信息未通过认证时，通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[16] 为解决上述技术问题，本发明采用的还有一个技术方案是：提供一种基于WIFI热点实现私密保护的系统，所述系统包括第一电子设备以及第二电子设备，其中，所述第一电子设备包括第一接收模块、第一通信模块、第一认证模块以及第一控制模块，所述第二电子设备包括第二接收模块、第二通信模块以及第二认证模块，其中：在用户需要访问所述第一电子设备上的私密内容时，所述第一接收模块接收用户输入的第一认证信息；所述第一通信模块通过WIFI将所述第一认证信息发送给第二电子设备；所述第二认证模块将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；所述第二接收模块接收用户输入的第二认证信息；所述第二通信模块通过WIFI将所述第二认证信息发送给所述第一电子设备；所述第一认证模块将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；所述第一控制模快在所述第一认证信息与所述第二认证信息都通过认证时，控制打开所述私密内容。

[17] 其中，所述第一通信模块和所述第二通信模块还用于使所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥。

[18] 其中，所述第一接收模块用于接收用户输入的第一认证秘钥；所述第一通信模块通过WIFI将所述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；所述第二接收模块用于接收并保存所述第一认证秘钥，并接收用户输入的第二认证秘钥；所述第二通信模块通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；所述第一接收模块接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[19] 其中，所述第二电子设备还包括第二控制模块：所述第二控制模块控制所述第二通信模块通过WIFI向所述第一电子设备反馈认证结果。

[20] 其中，所述第二控制模块在所述第一认证信息通过认证时，控制第二通信模块通过WIFI向所述第一电子设备返回认证通过通知；在所述第一认证信息未通过认证时，控制所述第二通信模块通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[21] 本发明的有益效果是：区别于现有技术的情况，本发明提供的基于WIFI热点实现电子设备私密保护的方法及系统，当用户需要查看电子设备内的私密内容时，需要当前电子设备与另一电子设备相互配合通过认证才能查看，通过两个不同的电子设备并配合认证秘钥双层保护机制，即使是电子设备丢失，也不会导致私密内容外泄，有效保障电子设备内私密内容的安全，给用户更好的个人体验。

[22] 【附图说明】

[23] 图1是本发明实施例提供的基于WIFI热点实现电子设备私密保护的方法的流程图；

[24] 图2是本发明实施例提供的第一电子设备与第二电子设备进行WIFI初始化配对的流程图；

[25] 本发明实施例提供的一种基于WIFI热点实现私密保护的系统的结构示意图。

[26] 【具体实施方式】

[27] 参阅图1，图1是本发明实施例提供的基于WIFI热点实现电子设备私密保护的方法的流程图，如图所示，本实施例提供的基于WIFI热点实现电子设备私密保护

的方法包括：

[28] S101：在用户需要访问第一电子设备上的私密内容时，第一电子设备接收用户输入的第一认证信息，并通过WIFI将第一认证信息发送给第二电子设备；

[29] 当用户需要访问第一电子设备上的私密内容时，通过特定按键或软键盘触发，弹出私密模式登录界面。本发明实施例所提到的私密内容，可以是电子设备内的图片、录音、录像、短信或来电记录等等。具体私密内容所包括的内容可以根据用户需要自行设置。

[30] 其中，本发明的方案依赖于WIFI实现，因此，第一电子设备与第二电子设备都需要具有无线接入功能。WIFI热点是指电子设备将其接收GPRS或3G信号转化为wifi信号再发出去，这样，该电子设备即成了一个WIFI热点。

[31] 第一电子设备与第二电子设备预先进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥。这里第一电子设备与第二电子设备可以是同属于一个用户的两个不同的电子设备，比如用户A的手机与平板电脑，或者平板电脑与笔记本电脑等，也可以是分别属于不同用户的电子设备。比如用户A的平板电脑，用户B的手机。本发明对此不做限定。

[32] 在私密模式界面，用户输入第一认证信息，第一电子设备将第一认证信息通过WIFI发送给第二电子设备以进行身份认证。

[33] 其中，请进一步参阅图2，图2是本发明实施例提供的第一电子设备与第二电子设备进行WIFI初始化配对的流程图，如图所示，第一电子设备与第二电子设备进行WIFI初始化配对包括以下步骤：

[34] S201：第一电子设备与第二电子设备开启WIFI；

[35] 第一电子设备与第二电子设备都开启WIFI，并处于能够进行WIFI通信的范围内。

[36] S202：第一电子设备接收用户输入的第一认证秘钥，通过WIFI将第一认证秘钥发送给第二电子设备，第一认证秘钥用于对第一电子设备进行认证；

[37] 用户在第一电子设备的WIFI设备中找到第二电子设备的WIFI标识，并输入用于对第一电子设备进行认证的第一认证秘钥。第一电子设备将第一认证秘钥通过WIFI发送给第二电子设备，以使第二电子设备存储第一认证秘钥便于后续对

所述第一电子设备进行认证。

[38] S203：第二电子设备接收并保存第一认证秘钥；

[39] 第二电子设备通过WIFI接收第一认证秘钥，并将第一认证秘钥进行保存。比如可以将第一认证秘钥保存在处理器中或者内存中。

[40] S204：第二电子设备接收用户输入的第二认证秘钥，通过WIFI将第二认证秘钥发送给第一电子设备，第二认证秘钥用于对第二电子设备进行认证；

[41] 同理，用户在第二电子设备界面找到第一电子设备的WIFI标识，并输入用于对第二电子设备进行身份认证的第二认证秘钥。第二电子设备接收用户输入的第二认证秘钥，通过WIFI将第二认证秘钥发送给第一电子设备，以使第一电子设备存储第二认证秘钥便于后续对所述第二电子设备进行认证。

[42] S205：第一电子设备接收并保存第二认证秘钥；

[43] 第一电子设备通过WIFI接收第二认证秘钥，并将第二认证秘钥进行保存。比如可以将第二认证秘钥保存在处理器中或者内存中。

[44] S206：完成WIFI初始化配对，绑定用于访问私密内容的认证秘钥。

[45] 经过以上步骤，完成了第一电子设备与第二电子设备的WIFI初始化配对，并且第一电子设备与第二电子设备相互绑定了用于访问私密内容的认证秘钥。也就是说，在需要访问任何一个电子设备的私密内容时，都需要与之配对的另一个电子设备与该电子设备配合都通过身份认证才能查看私密内容。

[46] 需要注意的是，上述步骤S202-S203与步骤S204-S205并不严格区分先后顺序，本实施例只是为了区分两个不同的步骤而进行这样的编号，事实上，第一电子设备发送第一认证秘钥与第二电子设备发送第二认证秘钥可以是同时进行，也可以是第二电子设备先发送第二认证秘钥，第一电子设备接收到第二认证秘钥后再发送第一认证秘钥。只要两个电子设备能够相互配对并绑定认证秘钥，本发明该步骤的实现先后顺序不做限定。

[47] S102：第二电子设备将第一认证信息与第二电子设备预存的认证秘钥进行比对认证；

[48] 第二电子设备通过WIFI接收第一认证信息，并将第一认证信息与第二电子设备预存的认证秘钥进行比对认证。当第一认证信息与第二电子设备预存的认证秘

钥相同时，第一认证信息通过认证，否则，第一认证信息没有通过认证。

[49] 在一些优选的实施例中，第二电子设备进行第一认证信息认证后，还包括通过WIFI向第一电子设备反馈认证结果。

[50] 具体可以是以下实施方案：当第一认证信息通过认证时，第二电子设备通过WIFI向第一电子设备返回认证通过通知，当第一认证信息没有通过认证时，第二电子设备通过WIFI向第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[51] 当然，这只是本发明实施例的一种实现方式举例，在实际应用过程中，可以通过预先设置来实现认证结果反馈。比如设置当第一认证信息通过时，再向第一电子设备发送第二认证信息，否则不发送第二认证信息。

[52] S103：第二电子设备接收用户输入的第二认证信息，并通过WIFI将第二认证信息发送给第一电子设备；

[53] 用户在第二电子设备界面输入用于对第二电子设备进行身份认证的第二认证信息，第二电子设备接收第二认证信息，并通过WIFI将第二认证信息发送给第一电子设备。

[54] S104：第一电子设备将第二认证信息与第一电子设备内预存的认证秘钥进行比对认证；

[55] 第一电子设备通过WIFI接收第二认证信息，并将第二认证信息与第一电子设备预存的认证秘钥进行比对认证。当第二认证信息与第一电子设备预存的认证秘钥相同时，第二认证信息通过认证，否则，第二认证信息没有通过认证。

[56] 作为一种优选的实现方案，在第二认证信息没有通过认证时，第一电子设备通过WIFI向第二电子设备返回认证失败通知，并提示用户重新输入认证信息。

[57] 在第一认证信息与第二认证信息的任何一个没有通过认证时，第一电子设备界面弹出私密模式登录失败提示，或者是直接返回主界面。

[58] S105：打开第一电子设备的私密内容；

[59] 在第一认证信息与第二认证信息都通过认证时，打开第一电子设备的私密内容。

[60] 需要注意的是，本发明实施例的上述步骤S101-S102与步骤S103-S104并不严格

区分先后顺序，甚至有可能是同时进行的。比如可以是当用户触发访问私密内容后，同时向第一电子设备与第二电子设备发送触发指令，第一电子设备与第二电子设备都接收用户输入的认证信息，并将认证信息通过WIFI发送给另一电子设备，两个电子设备的比对认证同时进行。

[61] 在另一种实现方式中，可以是当第一认证信息通过认证后，第二电子设备才向第一电子设备发送第二认证信息。如果第一认证信息没有通过认证，第二电子设备向第一电子设备返回认证失败通知，直到第一认证信息通过认证后才向第一电子设备发送第二认证信息。

[62] 以上实施例只是以用户需要访问第一电子设备的私密内容为例进行详细说明，当用户需要访问第二电子设备的私密内容时，其实现过程跟上述实现过程基本一致，在此本发明实施例对此不再赘述。

[63] 本发明电子设备私密保护的方法，由于是两个电子设备配对，并且需要两个电子设备特定的认证信息都通过认证才能查看私密内容，因此，就算丢失电子设备，别人也不能解锁查看该丢失的电子设备内的私密内容，即使是电子设备的主人想要查看该电子设备内的私密内容，也要另一个电子设备配合进行认证，在两个电子设备认证都通过方能查看私密内容，确保私密内容的安全。

[64] 通过上述本发明实施例的阐述，可以理解，本发明实施例提供的基于WIFI热点实现电子设备私密保护的方法，当用户需要查看电子设备内的私密内容时，需要当前电子设备与另一电子设备相互配合通过认证才能查看，通过两个不同的电子设备并配合认证秘钥双层保护机制，即使是电子设备丢失，也不会导致私密内容外泄，有效保障电子设备内私密内容的安全，给用户更好的个人体验。

[65] 请参阅图3，图3是本发明实施例提供的一种基于WIFI热点实现私密保护的系统100，该系统包括第一电子设备200以及第二电子设备300，其中，第一电子设备200包括第一接收模块20、第一通信模块21、第一认证模块22以及第一控制模块23，第二电子设备300包括第二接收模块30、第二通信模块31以及第二认证模块32，其中：

[66] 在用户需要访问第一电子设备上的私密内容时，第一接收模块20接收用户输入的第一认证信息；

[67] 当用户需要访问第一电子设备上的私密内容时，通过特定按键或软键盘触发，弹出私密模式登录界面。本发明实施例所提到的私密内容，可以是电子设备内的图片、录音、录像、短信或来电记录等等。具体私密内容所包括的内容可以根据用户需要自行设置。

[68] 其中，第一通信模块21与第二通信模块31用于使第一电子设备与第二电子设备预先进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥。这里第一电子设备与第二电子设备可以是同属于一个用户的两个不同的电子设备，比如用户A的手机与平板电脑，或者平板电脑与笔记本电脑等，也可以是分别属于不同用户的电子设备。比如用户A的平板电脑，用户B的手机。本发明对此不做限定。

[69] 在私密模式界面，用户输入第一认证信息，第一接收模块20接收第一认证信息。

[70] 其中，第一电子设备与第二电子设备进行WIFI初始化配对时：

[71] 第一接收模块20用于接收用户输入的第一认证秘钥，第一通信模块21通过WIFI将第一认证秘钥发送给第二电子设备，第一认证秘钥用于对第一电子设备进行认证。第二接收模块30用于接收并保存第一认证秘钥，并接收用户输入的第二认证秘钥，第二通信模块31通过WIFI将第二认证秘钥发送给第一电子设备，第二认证秘钥用于对第二电子设备进行认证，第一接收模块20接收并保存第二认证秘钥，完成WIFI初始化配对，绑定用于访问私密内容的认证秘钥。

[72] 其中，第一电子设备和第二电子设备可以分别将第二认证秘钥与第一认证秘钥保存在处理器或内存中，以用于后续对第二电子设备与第一电子设备进行身份认证。

[73] 第一通信模块21通过WIFI将第一认证信息发送给第二电子设备；

[74] 第一通信模块21将第一认证信息通过WIFI发送给第二电子设备以进行身份认证。

[75] 第二认证模块32将第一认证信息与第二电子设备预存的认证秘钥进行比对认证；

[76] 第二认证模块32将第一认证信息与第二电子设备预存的认证秘钥进行比对认证

。当第一认证信息与第二电子设备预存的认证秘钥相同时，第一认证信息通过认证，否则，第一认证信息没有通过认证。

[77] 在一些优选的实施例中，本发明的第二电子设备还进一步包括第二控制模块33，第二控制模块33控制第二通信模块31通过WIFI向第一电子设备反馈认证结果。

[78] 具体地，第二控制模块33在第一认证信息通过认证时，控制第二通信模块31通过WIFI向第一电子设备返回认证通过通知；在第一认证信息未通过认证时，控制第二通信模块31通过WIFI向第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[79] 当然，这只是本发明实施例的一种实现方式举例，在实际应用过程中，第二控制模块33可以根据预先设置来实现认证结果反馈。比如预先设置当第一认证信息通过时，第二控制模块33控制再向第一电子设备发送第二认证信息，否则不发送第二认证信息。

[80] 第二接收模块30接收用户输入的第二认证信息；

[81] 用户在第二电子设备界面输入用于对第二电子设备进行身份认证的第二认证信息，第二接收模块30接收第二认证信息。

[82] 第二通信模块31通过WIFI将第二认证信息发送给第一电子设备；

[83] 第二通信模块31通过WIFI将第二认证信息发送给第一电子设备以使第一电子设备进行比对认证。

[84] 第一认证模块22将第二认证信息与第一电子设备内预存的认证秘钥进行比对认证；

[85] 第一电子设备通过WIFI接收第二认证信息，并将第二认证信息与第一电子设备预存的认证秘钥进行比对认证。当第二认证信息与第一电子设备预存的认证秘钥相同时，第二认证信息通过认证，否则，第二认证信息没有通过认证。

[86] 作为一种优选的实现方案，在第二认证信息没有通过认证时，第一通信模块21通过WIFI向第二电子设备返回认证失败通知，并提示用户重新输入认证信息。

[87] 在第一认证信息与第二认证信息的任何一个没有通过认证时，第一电子设备界面弹出私密模式登录失败提示，或者是直接返回主界面。

[88] 第一控制模快23在第一认证信息与第二认证信息都通过认证时，控制打开私密内容。

[89] 在第一认证信息与第二认证信息都通过认证时，第一控制模块23控制打开第一电子设备的私密内容。

[90] 以上系统的实施例只是以用户需要访问第一电子设备的私密内容为例进行详细说明，当用户需要访问第二电子设备的私密内容时，其实现过程跟上述实现过程基本一致，在此本发明实施例对此不再赘述。

[91] 通过上述本发明实施例基于WIFI热点实现电子设备私密保护的方法及系统，可以理解，本发明的私密保护方法当用户需要查看电子设备内的私密内容时，需要当前电子设备与另一电子设备相互配合通过认证才能查看，通过两个不同的电子设备并配合认证秘钥双层保护机制，即使是电子设备丢失，也不会导致私密内容外泄，有效保障电子设备内私密内容的安全，给用户更好的个人体验。

[92] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[93] 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，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[94] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[95] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用

时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

[96] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

[权利要求 1] 一种基于WIFI热点实现电子设备私密保护的方法，其中，所述方法包括：

第一电子设备与第二电子设备进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥；

在用户需要访问所述第一电子设备上的私密内容时，所述第一电子设备接收用户输入的第一认证信息，并通过WIFI将所述第一认证信息发送给第二电子设备；

所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；

所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果；

所述第二电子设备接收用户输入的第二认证信息，并通过WIFI将所述第二认证信息发送给所述第一电子设备；

所述第一电子设备将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；

在所述第一认证信息与所述第二认证信息都通过认证时，打开所述第一电子设备的私密内容。

[权利要求 2] 根据权利要求1所述的方法，其中，所述第一电子设备与第二电子设备进行WIFI初始化配对，相互绑定用于访问私密内容的认证秘钥包括：

所述第一电子设备与所述第二电子设备开启WIFI；

所述第一电子设备接收用户输入的第一认证秘钥，通过WIFI将所述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；

所述第二电子设备接收并保存所述第一认证秘钥；

所述第二电子设备接收用户输入的第二认证秘钥，通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；

所述第一电子设备接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[权利要求 3] 根据权利要求1所述的方法，其中，所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果包括：

在所述第一认证信息通过认证时，通过WIFI向所述第一电子设备返回认证通过通知；

在所述第一认证信息未通过认证时，通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[权利要求 4] 一种基于WIFI热点实现电子设备私密保护的方法，其中，所述方法包括：

在用户需要访问第一电子设备上的私密内容时，所述第一电子设备接收用户输入的第一认证信息，并通过WIFI将所述第一认证信息发送给第二电子设备；

所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；

所述第二电子设备接收用户输入的第二认证信息，并通过WIFI将所述第二认证信息发送给所述第一电子设备；

所述第一电子设备将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；

在所述第一认证信息与所述第二认证信息都通过认证时，打开所述第一电子设备的私密内容。

[权利要求 5] 根据权利要求4所述的方法，其中，所述方法还包括：

所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥。

[权利要求 6] 根据权利要求5所述的方法，其中，所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥包括：

所述第一电子设备与所述第二电子设备开启WIFI；

所述第一电子设备接收用户输入的第一认证秘钥，通过WIFI将所述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；

所述第二电子设备接收并保存所述第一认证秘钥；

所述第二电子设备接收用户输入的第二认证秘钥，通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；

所述第一电子设备接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[权利要求 7] 根据权利要求4所述的方法，其中，所述第二电子设备将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证之后，还包括：

所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果。

[权利要求 8] 根据权利要求7所述的方法，其中，所述第二电子设备通过WIFI向所述第一电子设备反馈认证结果包括：

在所述第一认证信息通过认证时，通过WIFI向所述第一电子设备返回认证通过通知；

在所述第一认证信息未通过认证时，通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

[权利要求 9] 一种基于WIFI热点实现私密保护的系统，其中，所述系统包括第一电子设备以及第二电子设备，其中，所述第一电子设备包括第一接收模块、第一通信模块、第一认证模块以及第一控制模块，所述第二电子设备包括第二接收模块、第二通信模块以及第二认证模块，其中：

在用户需要访问所述第一电子设备上的私密内容时，所述第一接收模块接收用户输入的第一认证信息；

所述第一通信模块通过WIFI将所述第一认证信息发送给第二电子设备；

所述第二认证模块将所述第一认证信息与所述第二电子设备预存的认证秘钥进行比对认证；

所述第二接收模块接收用户输入的第二认证信息；

所述第二通信模块通过WIFI将所述第二认证信息发送给所述第一电子设备；

所述第一认证模块将所述第二认证信息与所述第一电子设备内预存的认证秘钥进行比对认证；

所述第一控制模快在所述第一认证信息与所述第二认证信息都通过认证时，控制打开所述私密内容。

[权利要求 10] 根据权利要求9所述的系统，其中，所述第一通信模块和所述第二通信模块还用于使所述第一电子设备与所述第二电子设备进行WIFI初始化配对，相互绑定用于访问所述私密内容的认证秘钥。

[权利要求 11] 根据权利要求10所述的系统，其中，

所述第一接收模块用于接收用户输入的第一认证秘钥；

所述第一通信模块通过WIFI将所述第一认证秘钥发送给所述第二电子设备，所述第一认证秘钥用于对所述第一电子设备进行认证；

所述第二接收模块用于接收并保存所述第一认证秘钥，并接收用户输入的第二认证秘钥；

所述第二通信模块通过WIFI将所述第二认证秘钥发送给所述第一电子设备，所述第二认证秘钥用于对所述第二电子设备进行认证；

所述第一接收模块接收并保存所述第二认证秘钥，完成WIFI初始化配对，绑定用于访问所述私密内容的认证秘钥。

[权利要求 12] 根据权利要求9所述的系统，其中，所述第二电子设备还包括第二控制模块：

所述第二控制模块控制所述第二通信模块通过WIFI向所述第一电子设备反馈认证结果。

[权利要求 13] 根据权利要求12所述的系统，其中，所述第二控制模块在所述第一认证信息通过认证时，控制第二通信模块通过WIFI向所述第一电子设备返回认证通过通知；在所述第一认证信息未通过认证时，控制所述第二通信模块通过WIFI向所述第一电子设备返回认证失败通知，提示用户重新输入认证信息。

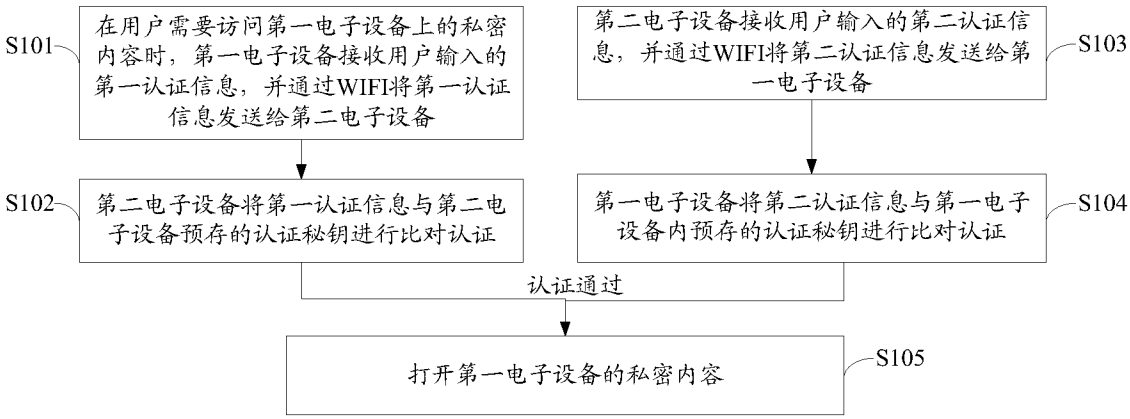
S101
在用户需要访问第一电子设备上的私密内容时，第一电子设备接收用户输入的第一认证信息，并通过WIFI将第一认证信息发送给第二电子设备
S102
第二电子设备将第一认证信息与第二电子设备预存的认证秘钥进行比对认证
第二电子设备接收用户输入的第二认证信息，并通过WIFI将第二认证信息发送给第一电子设备
S103
第一电子设备将第二认证信息与第一电子设备内预存的认证秘钥进行比对认证
S104
认证通过
打开第一电子设备的私密内容
S105

图 1

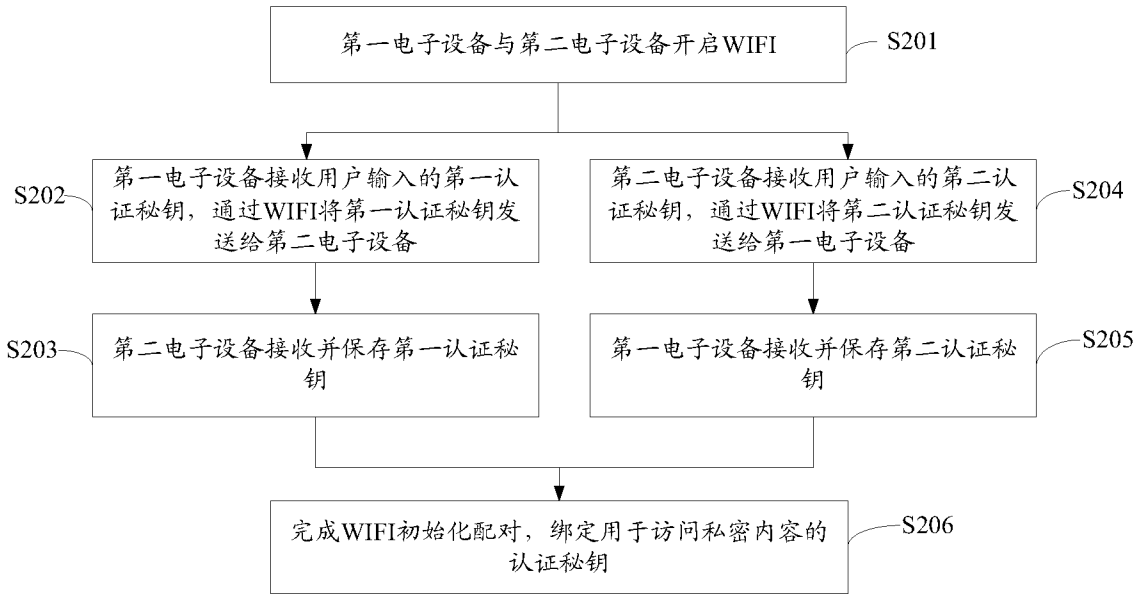
第一电子设备与第二电子设备开启WIFI
S201
S202
第一电子设备接收用户输入的第一认证秘钥，通过WIFI将第一认证秘钥发送给第二电子设备
第二电子设备接收用户输入的第二认证秘钥，通过WIFI将第二认证秘钥发送给第一电子设备
S204
S203
第二电子设备接收并保存第一认证秘钥
第一电子设备接收并保存第二认证秘钥
S205
完成WIFI初始化配对，绑定用于访问私密内容的认证秘钥
S206

图 2

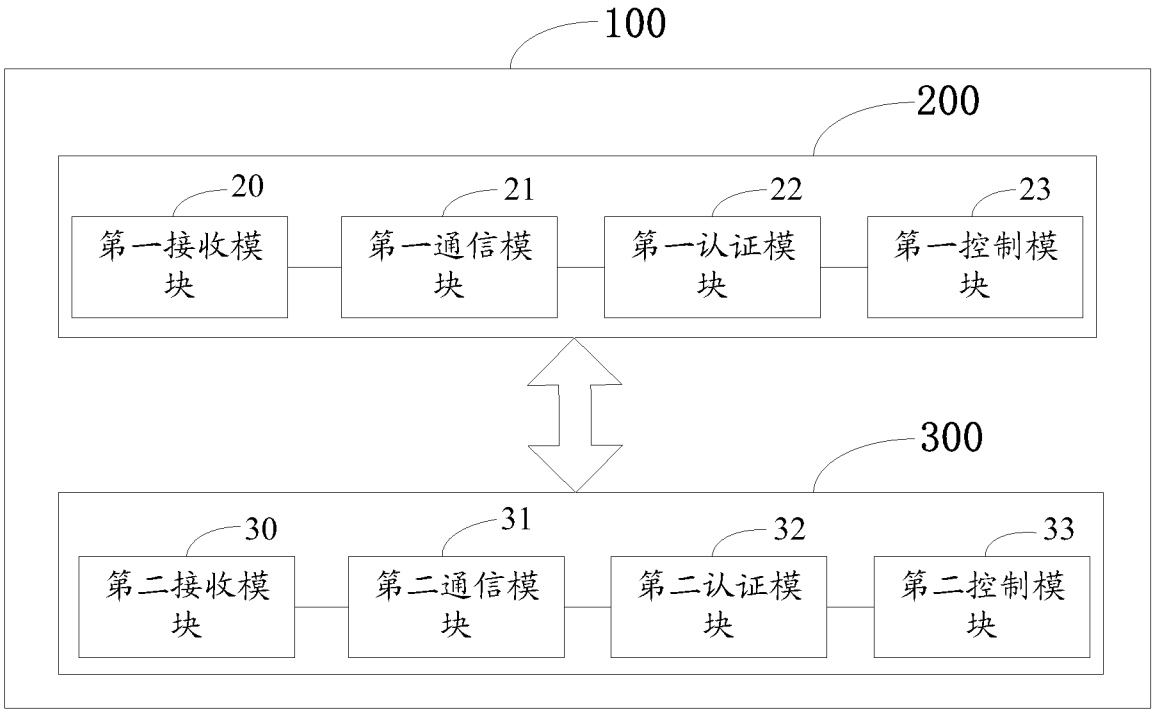
100
200
20
第一接收模块
21
第一通信模块
22
第一认证模块
23
第一控制模块
300
30
第二接收模块
31
第二通信模块
32
第二认证模块
33
第二控制模块

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/092018

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/35 (2013.01) i; G06F 21/62 (2013.01) i; 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)

G06F; 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)

CPRSABS; CNTXT; VEN; CNKI: wifi, NFC, Bluetooth, close, near, range, distance, binding, match, cell, phone, mobile, terminal, device, station, apparatus, authenticate, validate, twice, cross, bidirection, two, way, key, security, safe, safety, access, protect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103888265 A (SHANGHAI BOLU INFORMATION TECHNOLOGY CO., LTD.) 2014 June 25 (2014.06.25) description, paragraphs [0036], [0084]-[0087]	1-13
PX	CN 104836794 A (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD.) 2015 August 12 (2015.08.12) claims 1-10	1-13
A	KR 20070079955 A (JUNG YUN SUK) 2007 August 08 (2007.08.08) the abstract	1-13

☐ 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	Date of mailing of the international search report
05 January 2016	21 January 2016

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	BAI, Tan Telephone No. (86-10) 62411245

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/092018

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103888265 A	25 June 2014	None	
CN 104836794 A	12 August 2015	None	
KR 20070079955 A	08 August 2007	None	

国际检索报告

国际申请号
PCT/CN2015/092018

A. 主题的分类

G06F 21/35(2013.01)i; G06F 21/62(2013.01)i; 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)

G06F; H04L; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CPRSABS; CNTXT; VEN; CNKI: 近距离，蓝牙，近场，绑定，配合，手机，移动，终端，设备，站，装置，蜂窝，验证，认证，双层，两层，二次，交差，双向，密钥，密码，安全，访问，保护，wifi，NFC，bluetooth，close，near，range，distance，binding，match，cell，phone，mobile，terminal，device，station，apparatus，authenticate，validate，twice，cross，bidirection，two，way，key，security，safe，safety，access，protect

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103888265 A (上海博路信息技术有限公司) 2014年 6月 25日 (2014-06-25) 说明书第[0036]、[0084]-[0087]段	1-13
PX	CN 104836794 A (惠州TCL移动通信有限公司) 2015年 8月 12日 (2015-08-12) 权利要求1-10	1-13
A	KR 20070079955 A (JUNG YUN SUK) 2007年 8月 8日 (2007-08-08) 摘要	1-13

☐ 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	国际检索报告邮寄日期
2016年 1月 5日	2016年 1月 21日

ISA/CN的名称和邮寄地址	受权官员
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	白坦
传真号 (86-10)62019451	电话号码 (86-10)62411245

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/092018

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	103888265	A	2014年 6月 25日	无	
CN	104836794	A	2015年 8月 12日	无	
KR	20070079955	A	2007年 8月 8日	无	