

(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 3 月 1 日 (01.03.2018)



(10) 国际公布号
WO 2018/035927 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2016/100670

(22) 国际申请日: 2016 年 9 月 28 日 (28.09.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610718846.8 2016年8月24日 (24.08.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

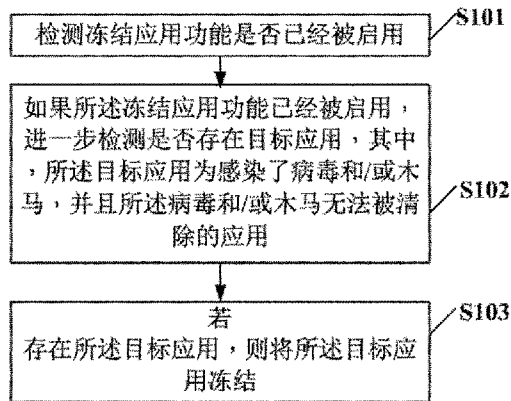
(72) 发明人: 董志伟 (DONG, Zhiwei); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司等 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD. et al.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (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, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) Title: APPLICATION FREEZING METHOD AND APPARATUS, AND TERMINAL

(54) 发明名称: 一种冻结应用的方法、装置以及终端



[Fig. 1]

- S101 Detecting whether an application freezing function has already been started
S102 If the application freezing function has already been started, further detecting whether a target application exists, wherein the target application is an application infected with a virus and/or a trojan, and the virus and/or the trojan cannot be removed
S103 If the target application exists, freezing the target application

(57) Abstract: An application freezing method and apparatus, and a terminal. The method comprises: detecting whether an application freezing function has already been started (S101); if the application freezing function has already been started, further detecting whether a target application exists, wherein the target application is an application infected with a virus and/or a trojan, and the virus and/or the trojan cannot be removed (S102); and if the target application exists, freezing the target application (S103), wherein freezing the target application comprises forbidding read-write permission and communication permission of the application infected with the non-removable virus and/or trojan on a terminal. The method protects the data security of a user, avoids harm to the user, provides the user with a solution to rapidly deal with an application infected with a non-removable virus and/or trojan, and provides the user with a safer use environment at the same time, thereby improving the user experience.

(57) 摘要: 一种冻结应用的方法、装置以及终端。所述方法包括: 检测冻结应用功能是否已经被启用 (S101); 如果所述冻结应用功能已经被启用, 进一步检测是否存在目标应用, 其中, 所述目标应用为感染了病毒和/或木马, 并且所述病毒和/或木马无法被清除的应用 (S102); 若存在所述目标应用, 则将所述目标应用冻结 (S103), 所述将目标应用冻结包括禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限。本方法保护了用户数据安全, 避免了对用户的危害, 给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案, 同时给用户提供了更为安全的使用环境, 提升了用户体验。



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))。

说明书

发明名称：一种冻结应用的方法、装置以及终端

- [1] 本申请要求于2016年8月24日提交中国专利局，申请号为201610718846.8、发明名称为“一种冻结应用的方法、装置以及终端”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

- [2] 本发明涉及电子技术领域，特别涉及一种冻结应用的方法、装置以及终端。

背景技术

- [3] 现阶段，随着技术的不断发展，终端的使用日益普及，基于终端的应用也越来越多。然而，现在的终端的应用非常容易受到病毒和/或木马的攻击，导致用户数据被更改、数据外发或者接收到恶意数据等。如何保证终端在应用受到病毒和/或木马的攻击的情况下仍然能保证终端的安全，是现阶段亟需解决的问题。

对发明的公开

发明内容

- [4] 本发明实施例提供一种冻结应用的方法、装置以及终端，能够保证终端在受到病毒和/或木马的攻击的情况下仍然能保证安全。
- [5] 第一方面，本发明提供了一种冻结应用的方法，包括：
- [6] 检测冻结应用功能是否已经被启用；
- [7] 如果所述冻结应用功能已经被启用，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；
- [8] 若存在所述目标应用，则将所述目标应用冻结。
- [9] 优选地，所述将所述目标应用冻结具体包括：
- [10] 读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；

- [11] 若所述目标应用的读写权限的标志位的值为第二值，则所述终端将所述目标应用的读写权限的标志位的值从第二值修改为第一值。
- [12] 优选地，所述将所述目标应用冻结具体包括：
- [13] 读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；
- [14] 若所述目标应用的通信权限的标志位的值为第四值，则所述终端将所述目标应用的通信权限的标志位的值从第四值修改为第三值。优选地，所述检测是否存在目标应用具体包括：
- [15] 检测终端中的应用是否存在感染了病毒和/或木马的应用；
- [16] 若存在感染了病毒和/或木马的应用，则对所述病毒和/或木马进行删除；
- [17] 所述终端进一步检测是否存在所述病毒和/或木马无法被清除的应用，从而检测是否存在目标应用。
- [18] 优选地，所述通信权限包括网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。
- [19] 本发明第二方面提供了一种冻结应用的装置，包括：
- [20] 第一检测模块，设置为检测冻结应用功能是否已经被启用；
- [21] 第二检测模块，设置为在所述冻结应用功能已经被启用时，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；
- [22] 处理模块，设置为存在所述目标应用时，将所述目标应用进行冻结。
- [23] 优选地，所述处理模块还包括：
- [24] 读取模块，设置为读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；
- [25] 修改模块，设置为在所述目标应用的读写权限的标志位的值为第二值时，则所

述处理模块将所述目标应用的读写权限的标志位的值从第二值修改为第一值

[26] 优选地，所述处理模块还包括：

[27] 读取模块，还设置为读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；

[28] 修改模块，还设置为在所述目标应用的通信权限的标志位的值为第四值时，所述修改模块将所述目标应用的通信权限的标志位的值从第四值修改为第三值。

[29] 优选地，所述第二检测模块具体设置为：

[30] 检测终端中的应用是否存在感染了病毒和/或木马的应用；

[31] 进一步检测是否存在所述病毒和/或木马无法被清除的应用从而检测是否存在目标应用。

[32] 优选地，所述通信权限包括网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。

[33] 本发明第三方面提供了一种冻结应用的终端，包括上述所述的冻结应用的装置。

[34] 实施本发明实施例，具有如下有益效果：

[35] 本发明通过禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限，保护了用户数据安全，避免了对用户的危害，给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案，同时给用户提供了更为安全的使用环境，提升了用户体验。

附图说明

[36] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[37] 图1是本发明实施例提供的一种冻结应用的方法的第一实施例的流程图。

[38] 图2是本发明实施例提供的一种冻结应用的方法的第二实施例的流程图。

[39] 图3是本发明实施例提供的一种冻结应用的装置的第一实施例的结构示意图。

[40] 图4是本发明实施例提供的一种冻结应用的装置的第一实施例中的处理模块的结构示意图。

[41] 图5是本发明实施例提供的一种冻结应用的终端的第一实施例的结构示意图。

具体实施方式

[42] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[43] 需要说明的是，在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[44] 请参阅图1，图1是本发明实施例提供的一种冻结应用的方法第一实施例的流程图。在本实施方式中，该冻结应用的方法应用于终端，所述终端可以是手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备（MID，mobile internet device）、可穿戴设备（例如智能手表（iwatch等）、智能手环等）或其他可以安装应用客户端的终端。所述终端用于启用冻结应用功能之后，检测所述终端上感染了无法清除的病毒和/或木马的应用，对检测到的所述感染了无法清除的病毒和/或木马的应用做冻结处理。所述冻结应用的方法包括以下步骤S101-S103。

[45] 在步骤S101中，检测冻结应用功能是否已经被启用。

[46] 在本实施方式中，可以通过两种方式实现冻结应用功能：（1）、冻结应用功能集成在终端的系统功能中，作为现有的系统功能中的一个可设置选项，用户可以在系统设置中开启冻结应用功能。（2）、冻结应用也可为一个独立的应用，可安装在运行IOS、Android、Windows等操作系统的终端中，用户可以通过打

开该冻结应用，从而开启冻结应用功能。

[47] 在步骤S102中，如果所述冻结应用功能已经被启用，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用。

[48] 在本实施方式中，所述终端可以对所有的应用进行检测，以确定所有的应用中存在感染了无法清除的病毒和/或木马的应用。在另一种实施方式中，用户还可以通过设置，选择部分应用进行检测，例如，可以是用户通过触摸屏直接选取需检测的部分应用进行检测；还可以是终端上设置有不同类别的应用，例如分别是通讯类应用、视频类应用等，用户可以直接选择需要检测的应用类别进行检测；还可以根据用户的使用频率建立常使用应用类别，以供用户选择所述常使用应用类别进行检测；还可以根据网络安全数据建立容易受到病毒和/或木马的攻击的应用类别供用户选择进行检测。

[49] 其中，所述终端对应用进行检测以确定目标应用，包括确认感染了病毒和/或木马，并且该病毒不能够被终端的杀毒软件所删除，或者删除后还会再出现病毒和/或木马不能清除等情况的应用为目标应用。

[50] 在步骤S103中，若存在所述目标应用，则将所述目标应用冻结。

[51] 具体的，在检测到了感染了无法清除的病毒和/或木马的目标应用之后，对所述感染了无法清除的病毒和/或木马的应用做冻结处理。在本实施方式中，对所述感染了无法清除的病毒和/或木马的应用做冻结处理至少包括禁止所述应用对终端的读取、篡改或者外发用户个人数据的权限。

[52] 在其他实施方式中，当有应用被冻结处理后，若用户需要再次使用所述感染了病毒和/或木马的应用，则输出提示，提示用户该应用已被冻结，该应用的部分功能不能如常使用。可以理解的是，终端可以通过语音、文字或者图像来提示用户被冻结应用的信息，其中，被冻结应用的信息包括所感染的病毒和/或木马的数量、等级、被限制的功能等，终端还可以使用其他类型的提示信息来提醒用户，本实施例并不以此为限。

[53] 上述可知，本发明实施例中的冻结应用的方法，通过禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限，保护了用户数据安全，避免

了对用户的危害，给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案，同时给用户提供了更为安全的使用环境，提升了用户体验。

[54] 图2是本发明实施例提供的一种冻结应用的方法第二实施例的流程图。在本实施方式中，该冻结应用方法包括步骤S201-S206。

[55] 在步骤S201中，检测冻结应用功能是否已经被启用。

[56] 在本实施方式中，可以通过两种方式实现冻结应用功能：（1）、冻结应用功能集成在终端的系统功能中，作为现有的系统功能中的一个可设置选项，用户可以在系统设置中开启冻结应用功能。（2）、冻结应用也可为一个独立的应用，可安装在运行IOS、Android、Windows等操作系统的终端中，用户可以通过打开该冻结应用，从而开启冻结应用功能。

[57] 在步骤S202中，如果所述冻结应用功能已经被启用，检测所述终端中的应用是否存在感染了病毒和/或木马的应用。

[58] 在本实施方式中，所述终端可以对所有的应用进行检测，以确定所有的应用中存在感染了无法清除的病毒和/或木马的应用。在另一种实施方式中，用户还可以通过设置，选择部分应用进行检测，例如，可以是用户通过触摸屏直接选取需检测的部分应用进行检测；还可以是终端上设置有不同类别的应用，例如分别是通讯类应用、视频类应用等，用户可以直接选择需要检测的应用类别进行检测；还可以根据用户的使用频率建立常使用应用类别，以供用户选择所述常使用应用类别进行检测；还可以根据网络安全数据建立容易受到病毒和/或木马的攻击的应用类别供用户选择进行检测。

[59] 在步骤S203中，若存在感染了病毒和/或木马的应用，则对所述病毒和/或木马进行删除。

[60] 具体的，如果检测到存在感染了病毒和/或木马的应用，则首先利用终端上的杀毒软件对所述病毒和/或木马进行删除。

[61] 在步骤S204中，确认感染了病毒和/或木马并且所述病毒和/或木马无法被终端的杀毒软件清除的应用。

[62] 其中，所述终端对应用进行检测以确定目标应用，包括确认感染了病毒和/或木马，并且该病毒不能够被终端的杀毒软件所删除，或者删除后还会再出现病

毒和/或木马不能清除等情况的应用为目标应用。

[63] 在步骤S205中，禁止所述感染了无法清除的病毒和/或木马的应用对终端的读写权限。

[64] 具体的，所述终端读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对所述终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；如果所述目标应用的读写权限的标志位的值为第二值，则所述终端将所述目标应用的读写权限的标志位的值从第二值修改为第一值。

[65] 具体的，禁止所述感染了无法清除的病毒和/或木马的应用对终端的读写权限，包括禁止所述感染了无法清除的病毒和/或木马的应用对终端的数据进行读取、写入、篡改等操作。

[66] 在步骤S206中，禁止所述感染了无法清除的病毒和/或木马的应用的通信权限。

[67] 具体的，所述终端读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过所述终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；如果所述目标应用的通信权限的标志位的值为第四值，则所述终端将所述目标应用的通信权限的标志位的值从第四值修改为第三值。

[68] 具体的，所述通信权限包括但不限于网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。

[69] 在其他实施方式中，在步骤S205和S206之后，若用户需要再次使用所述感染了病毒和/或木马的应用，则输出提示，提示用户该应用已被冻结，该应用的部分功能不能如常使用。可以理解的是，终端可以通过语音、文字或者图像来提示用户的被冻结应用的信息，其中，被冻结应用的信息包括所感染的病毒和/或木马的数量、等级、被限制的功能等，终端还可以使用其他类型的提示信息来提醒用户，本实施例并不以此为限。

- [70] 上述可知，本发明实施例中的冻结应用的方法，通过禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限，有效防止感染了无法清除的病毒和/或木马的应用读取、写入、篡改或是外发用户个人数据以及接收恶意数据，保护了用户数据安全，避免了对用户的危害，给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案，同时给用户提供了更为安全的使用环境，提升了用户体验。
- [71] 图3是本发明实施例提供的一种冻结应用装置的结构示意图。在本实施方式中，该冻结应用装置包括：
- [72] 第一检测模块301，设置为检测冻结应用功能是否已经被启用；
- [73] 第二检测模块302，设置为在所述冻结应用功能已经被启用时，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；
- [74] 处理模块303，设置为存在所述目标应用时，将所述目标应用冻结。
- [75] 其中，参阅图4，如图4所示，所述处理模块303包括：
- [76] 读取模块401，设置为读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；
- [77] 修改模块402，设置为在所述目标应用的读写权限的标志位的值为第二值时，则所述处理模块将所述目标应用的读写权限的标志位的值从第二值修改为第一值。
- [78] 在其他实施例中，所述处理模块303还包括：
- [79] 读取模块401，还设置为读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过所述终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；
- [80] 修改模块402，还设置为在所述目标应用的通信权限的标志位的值为第四值时

，所述修改模块将所述目标应用的通信权限的标志位的值从第四值修改为第三值。

[81] 其中，所述通信权限包括但不限于网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。

[82] 在本实施方式中，所述第二检测模块302具体设置为：所述第二检测模块302可以对所有的应用进行检测，以确定所有的应用中存在感染了无法清除的病毒和/或木马的应用。在另一种实施方式中，用户还可以通过设置，选择部分应用进行检测，例如，可以是用户通过触摸屏直接选取需检测的部分应用进行检测；还可以是终端上设置有不同类别的应用，例如分别是通讯类应用、视频类应用等，用户可以直接选择需要检测的应用类别进行检测；还可以根据用户的使用频率建立常使用应用类别，以供用户选择所述常使用应用类别进行检测；还可以根据网络安全数据建立容易受到病毒和/或木马的攻击的应用类别供用户选择进行检测。

[83] 其中，所述第二检测模块302对应用进行检测以确定目标应用，包括确认感染了病毒和/或木马，并且该病毒不能够被终端的杀毒软件所删除，或者删除后还会再出现病毒和/或木马不能清除等情况的应用为目标应用。其中，在其他实施方式中，所述冻结应用装置还包括：

[84] 存储模块304，设置为存储相关程序代码以及所述感染了无法清除的病毒和/或木马的应用的相关信息，所述感染了无法清除的病毒和/或木马的应用的相关信息包括所感染的病毒和/或木马的数量、等级、该应用被限制的功能等所有和所述感染了无法清除的病毒和/或木马的应用相关的信息。

[85] 可以理解的是，本实施例的装置的各功能模块可根据上述图1-图2所示方法实施例中的方法具体实现，其具体过程可以参照上述方法实施例的相关描述。

[86] 上述可知，本实施例中的冻结应用装置，通过禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限，有效防止感染了无法清除的病毒和/或木马的应用读取、写入、篡改或是外发用户个人数据以及接收恶意数据，保护了用户数据安全，避免了对用户的危害，给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案，同时给用户提供了更为安全的使用环境

，提升了用户体验。

[87] 请参阅图5，其示出了本发明实施例所涉及的冻结应用的终端，该终端可以用于实施上述实施例中提供的冻结应用的方法，其过程可根据上述图1-图2所示方法实施例中的方法具体实现，所述终端包括上述实施例中提供的冻结应用的装置。具体来讲：

[88] 终端500可以包括RF（Radio Frequency，射频）电路110、包括有一个或一个以上计算机可读存储介质的存储器120、输入单元130、显示单元140、传感器150、音频电路160、WiFi(wireless fidelity，无线保真)模块170、包括有一个或者一个以上处理核心的处理器180、以及电源190等部件。本领域技术人员可以理解，图5中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[89] RF电路110可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，交由一个或者一个以上处理器180处理；另外，将涉及上行的数据发送给基站。通常，RF电路110包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块（SIM）卡、收发信机、耦合器、LNA（Low Noise Amplifier，低噪声放大器）、双工器等。此外，RF电路110还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于GSM(Global System of Mobile communication，全球移动通讯系统)、GPRS(General Packet Radio Service，通用分组无线服务)、CDMA(Code Division Multiple Access，码分多址)、WCDMA(Wideband Code Division Multiple Access，宽带码分多址)、LTE(Long Term Evolution,长期演进)、电子邮件、SMS(Short Messaging Service，短消息服务)等。

[90] 存储器120可用于存储软件程序以及模块，处理器180通过运行存储在存储器120的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器120可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据终端500的使用所创建的数据（比如音频数据、电话本等）等。此

外，存储器120可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器120还可以包括存储器控制器，以提供处理器180和输入单元130对存储器120的访问。

- [91] 输入单元130可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地，输入单元130可包括触敏表面131以及其他输入设备132。触敏表面131，也称为触摸显示屏或者触控板，可收集用户在其上或附近的触摸操作（比如用户使用手指、触笔等任何适合的物体或附件在触敏表面131上或在触敏表面131附近的操作），并根据预先设定的程式驱动相应的连接装置。可选的，触敏表面131可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器180，并能接收处理器180发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面131。除了触敏表面131，输入单元130还可以包括其他输入设备132。具体地，其他输入设备132可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。

- [92] 显示单元140可用于显示由用户输入的信息或提供给用户的信息以及终端500的各种图形用户接口，这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元140可包括显示面板141，可选的，可以采用LCD(Liquid Crystal Display, 液晶显示器)、OLED(Organic Light-Emitting Diode, 有机发光二极管)等形式来配置显示面板141。进一步的，触敏表面131可覆盖显示面板141，当触敏表面131检测到在其上或附近的触摸操作后，传送给处理器180以确定触摸事件的类型，随后处理器180根据触摸事件的类型在显示面板141上提供相应的视觉输出。虽然在图5中，触敏表面131与显示面板141是作为两个独立的部件来实现输入和输出功能，但是在某些实施例中，可以将触敏表面131与显示面板141集成而实现输入和输出功能。

- [93] 终端500还可包括至少一种传感器150，比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示面板141的亮度，接近传感器可在终端500移动到耳边时，关闭显示面板141和/或背光。作为运动传感器的一种，重力加速度传感器可检测各个方向上（一般为三轴）加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用（比如横竖屏切换、相关游戏、磁力计姿态校准）、振动识别相关功能（比如计步器、敲击）等；至于终端500还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。
- [94] 音频电路160、扬声器161，传声器162可提供用户与终端500之间的音频接口。音频电路160可将接收到的音频数据转换后的电信号，传输到扬声器161，由扬声器161转换为声音信号输出；另一方面，传声器162将收集的声音信号转换为电信号，由音频电路160接收后转换为音频数据，再将音频数据输出处理器180处理后，经RF电路110以发送给比如另一终端，或者将音频数据输出至存储器120以便进一步处理。音频电路160还可能包括耳塞插孔，以提供外设耳机与终端500的通信。
- [95] WiFi属于短距离无线传输技术，终端500通过WiFi模块170可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图5示出了WiFi模块170，但是可以理解的是，其并不属于终端500的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。
- [96] 处理器180是终端500的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器120内的软件程序和/或模块，以及调用存储在存储器120内的数据，执行终端500的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器180可包括一个或多个处理核心；优选的，处理器180可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器180中。
- [97] 终端500还包括给各个部件供电的电源190（比如电池），优选的，电源可以通

过电源管理系统与处理器180逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源190还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[98] 尽管未示出，终端500还可以包括摄像头、蓝牙模块等，在此不再赘述。具体在本实施例中，终端的显示单元是触摸屏显示器，终端还包括有存储器，以及一个或者一个以上的程序，其中一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于进行以下操作的指令：

[99] 终端检测冻结应用功能是否已经被启用；

[100] 如果所述冻结应用功能已经被启用，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；

[101] 如果存在所述目标应用，则将所述目标应用冻结。

[102] 具体的，将所述目标应用冻结具体包括：

[103] 所述终端读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对所述终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；

[104] 如果所述目标应用的读写权限的标志位的值为第二值，则所述终端将所述目标应用的读写权限的标志位的值从第二值修改为第一值。

[105] 具体的，将所述目标应用进行冻结具体包括：

[106] 所述终端读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过所述终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；

[107] 如果所述目标应用的通信权限的标志位的值为第四值，则所述终端将所述目标应用的通信权限的标志位的值从第四值修改为第三值。

- [108] 具体的，检测是否存在目标应用具体包括：
- [109] 所述终端检测所述终端中的应用是否存在感染了病毒和/或木马的应用；
- [110] 如果存在感染了病毒和/或木马的应用，则对所述病毒和/或木马进行删除；
- [111] 所述终端进一步检测是否存在所述病毒和/或木马无法被清除的应用从而检测是否存在目标应用。
- [112] 具体的，所述通信权限包括网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。
- [113] 上述可知，本实施例中的冻结应用终端，通过禁止感染了无法清除的病毒和/或木马的应用对终端的读写权限和通信权限，有效防止感染了无法清除的病毒和/或木马的应用读取、写入、篡改或是外发用户个人数据以及接收恶意数据，保护了用户数据安全，避免了对用户的危害，给用户提供了快速处理感染了无法清除的病毒和/或木马的应用的方案，同时给用户提供了更为安全的使用环境，提升了用户体验。
- [114] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。
- [115] 以上所揭露的仅为本发明一种较佳实施例而已，当然不能以此来限定本发明之权利范围，本领域普通技术人员可以理解实现上述实施例的全部或部分流程，并依本发明权利要求所作的等同变化，仍属于发明所涵盖的范围。

权利要求书

- [权利要求 1] 一种冻结应用的方法，其特征在于，包括：
- 检测冻结应用功能是否已经被启用；
- 如果所述冻结应用功能已经被启用，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；
- 若存在所述目标应用，则将所述目标应用冻结。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，所述将所述目标应用冻结具体包括：
- 读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；
- 若所述目标应用的读写权限的标志位的值为第二值，则所述终端将所述目标应用的读写权限的标志位的值从第二值修改为第一值。
- [权利要求 3] 根据权利要求1所述的方法，其特征在于，所述将所述目标应用冻结具体包括：
- 读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过终端进行通信的权限，当所述通信的权限的标志位的值为第四值时，所述目标应用具有通过所述终端进行通信的权限；
- 若所述目标应用的通信权限的标志位的值为第四值，则所述终端将所述目标应用的通信权限的标志位的值从第四值修改为第三值。
- [权利要求 4] 根据权利要求1所述的方法，其特征在于，所述检测是否存在目标

应用具体包括：

检测终端中的应用是否存在感染了病毒和/或木马的应用；

若存在感染了病毒和/或木马的应用，则对所述病毒和/或木马进行删除；

所述终端进一步检测是否存在所述病毒和/或木马无法被清除的应用，从而检测是否存在目标应用。

[权利要求 5] 根据权利要求3所述的方法，其特征在于，所述通信权限包括网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。

[权利要求 6] 一种冻结应用的装置，其特征在于，包括：

第一检测模块，设置为检测冻结应用功能是否已经被启用；

第二检测模块，设置为在所述冻结应用功能已经被启用时，进一步检测是否存在目标应用，其中，所述目标应用为感染了病毒和/或木马，并且所述病毒和/或木马无法被清除的应用；

处理模块，设置为存在所述目标应用时，将所述目标应用冻结。

[权利要求 7] 根据权利要求6所述的装置，其特征在于，所述处理模块包括：
读取模块，设置为读取所述目标应用的读写权限的标志位的值，其中，所述读写权限的标志位的值包括第一值以及第二值，当所述读写权限的标志位的值为第一值时，所述目标应用不具有对终端进行读写的权限，当所述读写权限的标志位的值为第二值时，所述目标应用具有对所述终端进行读写的权限；
修改模块，设置为在所述目标应用的读写权限的标志位的值为第二值时，则所述处理模块将所述目标应用的读写权限的标志位的值从第二值修改为第一值。

[权利要求 8] 根据权利要求6所述的装置，其特征在于，所述处理模块包括：
读取模块，还设置为读取所述目标应用的通信权限的标志位的值，其中，所述通信权限的标志位的值包括第三值以及第四值，当所述通信权限的标志位的值为第三值时，所述目标应用不具有通过终端进行通信的权限，当所述通信的权限的标志位的值为第四

值时，所述目标应用具有通过所述终端进行通信的权限；
修改模块，还设置为在所述目标应用的通信权限的标志位的值为第四值时，所述修改模块将所述目标应用的通信权限的标志位的值从第四值修改为第三值。

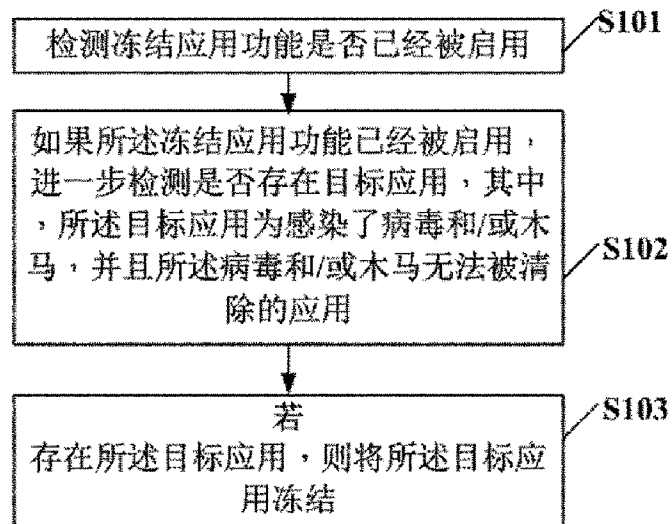
[权利要求 9] 根据权利要求6所述的装置，其特征在于，所述第二检测模块具体设置为：

检测终端中的应用是否存在感染了病毒和/或木马的应用；
进一步检测是否存在所述病毒和/或木马无法被清除的应用，从而检测是否存在目标应用。

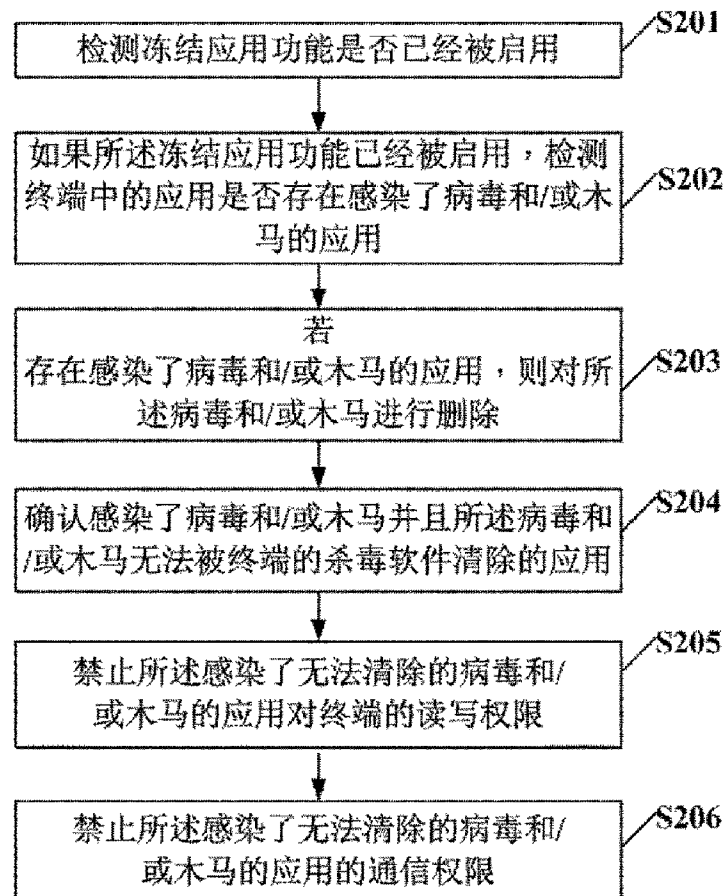
[权利要求 10] 根据权利要求8所述的装置，其特征在于，所述通信权限包括网络连接权限、蓝牙连接权限、zigbee连接权限、gps连接权限。

[权利要求 11] 一种终端，其特征在于，包括如权利要求6-10任一项所述的冻结应用的装置。

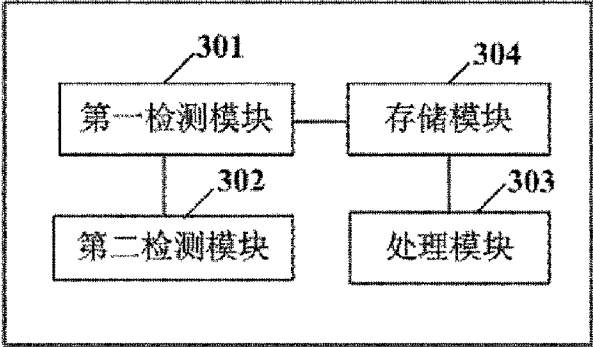
[Fig. 1]



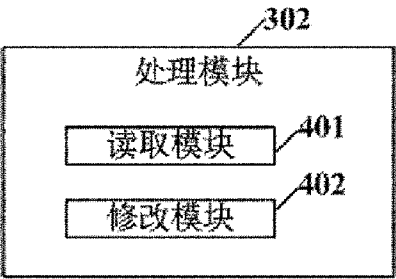
[Fig. 2]



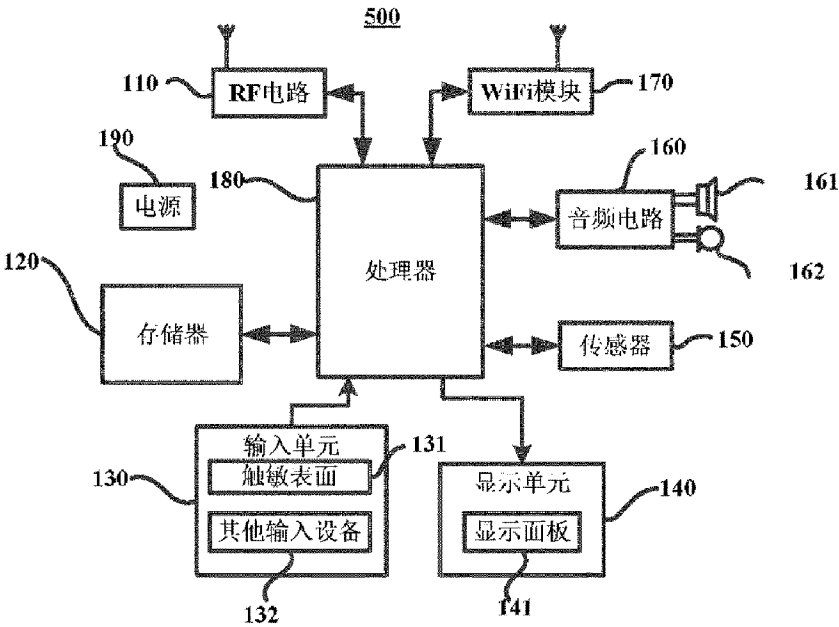
[Fig. 3]



[Fig. 4]



[Fig. 5]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/100670

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) 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

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)

WPI, EPODOC, CNPAT, CNKI: 病毒, 木马, 感染, 应用, 程序, 冻结, 修改, 更改, 变更, 读写, 通信, 权限, virus, trojan, infect, App, program, freeze, modification, modify, vary, read, write, communicate, authority

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105873028 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 17 August 2016 (17.08.2016), description, paragraphs [0042]-[0064], and figure 3	1-11
A	CN 102012982 A (XU, Litao et al.), 13 April 2011 (13.04.2011), entire document	1-11
A	CN 102306254 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 04 January 2012 (04.01.2012), entire document	1-11
A	CN 101377805 A (HUANG, Changsheng), 04 March 2009 (04.03.2009), entire document	1-11

☐ 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 18 April 2017	Date of mailing of the international search report 03 May 2017
Name and mailing address of the ISA 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 SU, Fei Telephone No. (86-10) 62413632

International application No.
PCT/CN2016/100670

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

A. 主题的分类 G06F 21/56 (2013.01) 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 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)) WPI, EPDOC, CNPAT, CNKI: 病毒, 木马, 感染, 应用, 程序, 冻结, 修改, 更改, 变更, 读写, 通信, 权限, virus, trojan, infect, App, program, freeze, modification, modify, vary, read, write, communicate, authority		
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 105873028 A (宇龙计算机通信科技深圳有限公司) 2016年 8月 17日 (2016 - 08 - 17) 说明书第[0042]-[0064]段、附图3	1-11
A	CN 102012982 A (许丽涛 等) 2011年 4月 13日 (2011 - 04 - 13) 全文	1-11
A	CN 102306254 A (奇智软件北京有限公司) 2012年 1月 4日 (2012 - 01 - 04) 全文	1-11
A	CN 101377805 A (黄长生) 2009年 3月 4日 (2009 - 03 - 04) 全文	1-11
☐ 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 2017年 4月 18日		国际检索报告邮寄日期 2017年 5月 3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) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 苏菲 电话号码 (86-10) 62413632

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/100670

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	105873028	A	2016年 8月 17日	无	
CN	102012982	A	2011年 4月 13日	无	
CN	102306254	A	2012年 1月 4日	WO 2013029504 A1	2013年 3月 7日
CN	101377805	A	2009年 3月 4日	无	