

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局

(43) 国际公布日  
2018 年 5 月 11 日 (11.05.2018)



(10) 国际公布号  
**WO 2018/082237 A1**

(51) 国际专利分类号:  
**G06F 21/30** (2013.01)

国广东省广州市经济技术开发区科珠路  
192号, Guangdong 510663 (CN)。

(21) 国际申请号: PCT/CN2017/077050

(22) 国际申请日: 2017 年 3 月 17 日 (17.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
201610978867.3 2016年11月7日 (07.11.2016) CN

(71) 申请人: 广州视源电子科技股份有限公司 (GUANGZHOU SHIYUAN ELECTRONICS CO., LTD.) [CN/CN]; 中国广东省广州市黄埔区云埔四路6号, Guangdong 510530 (CN)。广州视臻信息科技有限公司 (GUANGZHOU SHIZHEN ELECTRONICS CO., LTD.) [CN/CN]; 中

(72) 发明人: 李逸然 (LI, Yiran); 中国广东省广州市经济技术开发区科珠路192号, Guangdong 510663 (CN)。陈双龙 (CHEN, Shuanglong); 中国广东省广州市经济技术开发区科珠路192号, Guangdong 510663 (CN)。

(74) 代理人: 广州华进联合专利商标代理有限公司 (ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区花城大道85号3901房, Guangdong 510623 (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,

(54) Title: PASSWORD INPUT METHOD AND APPARATUS

(54) 发明名称: 密码输入方法和装置

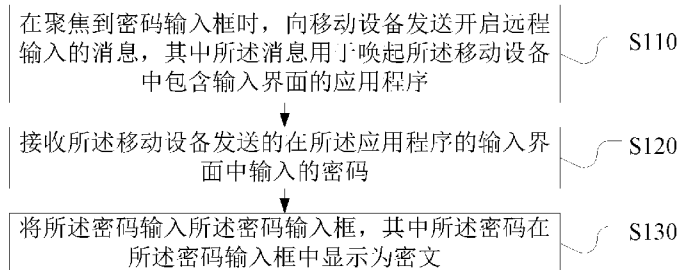


图 1

- S110 Send a message for starting remote input to a mobile device when a password input box is focused, wherein the message is used for arousing an application which contains an input interface in the mobile device
- S120 Receive a password which is input in the input interface of the application and is sent by the mobile device
- S130 Input the password into the password input box, wherein the password is displayed as a ciphertext in the password input box

(57) Abstract: The invention relates to a password input method and apparatus. The method comprises the steps of: sending a message for starting remote input to a mobile device when a password input box is focused, wherein the message is used for arousing an application which contains an input interface in the mobile device; receiving a password which is input in the input interface of the application and is sent by the mobile device; and inputting the password into the password input box, wherein the password is displayed as a ciphertext in the password input box. The present invention utilizes the characteristics of universality and privacy of the mobile device, provides a more safe and reliable password input environment for a user of a device to be subjected to password input, so that the user does not need to input the password one by one in the password input box of the device to be subjected to password input in public, thereby effectively improving the input safety and privacy of sensitive information including passwords and the like in the

JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, 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)。

根据细则4.17的声明:

- 关于申请人有权要求在先申请的优先权 (细则4.17(iii))

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

---

device to be subjected to password input, and improving the practicability of the device to be subjected to password input.

(57) 摘要: 本发明涉及一种密码输入方法和装置。所述方法包括步骤: 在聚焦到密码输入框时, 向移动设备发送开启远程输入的消息, 其中所述消息用于唤起所述移动设备中包含输入界面的应用程序; 接收所述移动设备发送的在所述应用程序的输入界面中输入的密码; 将所述密码输入所述密码输入框, 其中所述密码在所述密码输入框中显示为密文。本发明利用移动设备普遍性和私密性的特点, 为待输入密码的设备的用户提供了一个更加安全可靠的密码输入环境, 用户不需要在众目睽睽下在待输入密码的设备的密码输入框中一一输入密码, 有效提高了待输入密码的设备中密码等敏感信息输入的安全性和私密性, 提升了待输入密码的设备的实用性。

## 密码输入方法和装置

### 技术领域

本发明涉及电子设备技术领域，特别是涉及一种密码输入方法和装置。

5

### 背景技术

随着科技的发展，大屏设备，例如智能平板和教学触摸一体机等，已经广泛应用于教育教学、企业会议、商业展示等各个领域。人们利用大屏设备的触摸技术可以实现对主机的操作，从而使人机交互更为直截了当。

10 大屏设备的密码输入是人机交互中一个重要的环节。目前在大屏设备输入密码时，一般通过虚拟键盘输入和手写输入两种方式实现。但是由于大屏设备的屏幕较大，无论是虚拟键盘输入还是手写输入均需要用户在众目睽睽下输入密码等敏感信息，安全性与私密性都得不到良好的保障。

### 15 发明内容

基于此，有必要针对上述问题，提供一种密码输入方法和装置，能够有效保证大屏设备密码输入的安全性和私密性。

为了达到上述目的，本发明采取的技术方案如下：

一种密码输入方法，包括步骤：

20 在聚焦到密码输入框时，向移动设备发送开启远程输入的消息，其中所述消息用于唤起所述移动设备中包含输入界面的应用程序；

接收所述移动设备发送的在所述应用程序的输入界面中输入的密码；

将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

25 上述密码输入方法，在待输入密码的设备弹出密码输入框时，向移动设备发送开启远程输入的消息，移动设备根据该消息代替待输入密码的设备进行密码的输入，然后将输入的密码发送给待输入密码的设备，待输入密码的设备将接收的密码以密文形式显示在密码输入框。利用移动设备普遍性和私密性的特点，为待输入密码的设备的用户提供了一个更加安全可靠的密码输入环境，用

户不需要在众目睽睽下在待输入密码的设备的密码输入框中一一输入密码，有效提高了待输入密码的设备中密码等敏感信息输入的安全性和私密性，提升了待输入密码的设备的实用性。

在一个实施例中，接收所述移动设备发送的在所述应用程序的输入界面中  
5 输入的密码的步骤包括：接收所述移动设备对输入完成的密码进行加密后发送的加密密码，所述密码为在所述应用程序的输入界面中输入的密码。移动设备对输入的密码进行加密，可以有效保证密码传输的安全性，从而进一步保证密码输入的安全性。另外，移动设备所输入的密码只在最终完成阶段才通过密文一次性发送，有效提高了密码传输的效率，节省了网络资源。

10 在一个实施例中，接收所述移动设备发送的在所述应用程序的输入界面中输入的密码之前，还包括步骤：接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框。在移动设备的密码输入过程中，将不涉及密码敏感信息的伪密码发送给待输入密码的设备，从而使用户及时了解密码输入的当前状态，提高了用户体验。

15 在一个实施例中，将所述密码输入所述密码输入框的步骤包括：对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。当接收到移动设备发送的加密密码时，需要先进行解密，然后将密码输入框当前输入的伪密码替换为真正的密码。

在一个实施例中，当未与移动设备建立连接时，所述消息包括连接请求，  
20 或者，包括连接请求和密钥，所述密钥用于对移动设备发送的密码进行加密；当与移动设备建立连接后，所述消息包括密钥。当未与移动设备建立连接时，在聚焦到密码输入框时，可以向移动设备发送连接请求，移动设备接收到连接请求后建立与待输入密码的设备的通信连接并且启动包含输入界面的应用程序，另外，考虑到密码传输的安全性，在建立通信连接过程中还可以交换密钥。  
25 当与移动设备建立连接后，当聚焦到密码输入框时，可以向移动设备发送密钥，移动设备接收到密钥后启动包含输入界面的应用程序并将该密钥应用于后续的密码加密。通过该消息的设置，可以减少数据传输的次数，有效降低网络资源损耗。

一种密码输入装置，包括：

消息发送模块,用于在聚焦到密码输入框时,向移动设备发送开启远程输入的消息,其中所述消息用于唤起所述移动设备中包含输入界面的应用程序;

密码接收模块,用于接收所述移动设备发送的在所述应用程序的输入界面中输入的密码;

5 密码输入模块,用于将所述密码输入所述密码输入框,其中所述密码在所述密码输入框中显示为密文。

上述密码输入装置,在待输入密码的设备弹出密码输入框时,向移动设备发送开启远程输入的消息,移动设备根据该消息代替待输入密码的设备进行密码的输入,然后将输入的密码发送给待输入密码的设备,待输入密码的设备将  
10 接收的密码以密文形式显示在密码输入框。利用移动设备普遍性和私密性的特点,为待输入密码的设备的用户提供了一个更加安全可靠的密码输入环境,用户不需要在众目睽睽下在待输入密码的设备的密码输入框中一一输入密码,有效提高了待输入密码的设备中密码等敏感信息输入的安全性和私密性,提升了待输入密码的设备的实用性。

15 在一个实施例中,当未与移动设备建立连接时,所述消息包括连接请求,或者,包括连接请求和密钥,所述密钥用于对移动终端发送的密码进行加密;当与移动设备建立连接后,所述消息包括密钥。当未与移动设备建立连接时,在聚焦到密码输入框时,可以向移动设备发送连接请求,移动设备接收到连接请求后建立与待输入密码的设备的通信连接并且启动包含输入界面的应用程序,另外,考虑到密码传输的安全性,在建立通信连接过程中还可以交换密钥。  
20 当与移动设备建立连接后,当聚焦到密码输入框时,可以向移动设备发送密钥,移动设备接收到密钥后启动包含输入界面的应用程序并将该密钥应用于后续的密码加密。通过该消息的设置,可以减少数据传输的次数,有效降低网络资源损耗。

25 在一个实施例中,所述密码接收模块用于接收所述移动设备对输入完成的密码进行加密后发送的加密密码,所述密码为在所述应用程序的输入界面中输入的密码。移动设备对输入的密码进行加密,可以有效保证密码传输的安全性,从而进一步保证密码输入的安全性。另外,移动设备所输入的密码只在最终完成阶段才通过密文一次性发送,有效提高了密码传输的效率,节省了网络资源。

在一个实施例中，所述密码输入装置还包括伪密码输入模块，所述伪密码输入模块用于接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框。在移动设备的密码输入过程中，将不涉及密码敏感信息的伪密码发送给待输入密码的设备，从而使用户及时了解密码输入的当前状态，提高了用户体验。

在一个实施例中，所述密码输入模块用于对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。当接收到移动设备发送的加密密码时，需要先进行解密，然后将密码输入框当前输入的伪密码替换为真正的密码。

另一种密码输入方法，包括步骤：

接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

根据所述消息启动包含输入界面的应用程序；

获取在所述应用程序的输入界面中输入密码；

将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

上述密码输入方法，接收待输入密码的设备在弹出密码输入框时发送的开启远程输入的消息，根据该消息开启移动设备的应用程序，用户在该应用程序的输入界面中输入密码并发送给待输入密码的设备，实现待输入密码的设备密码的输入。利用移动设备普遍性和私密性的特点，为待输入密码的设备的用户提供了一个更加安全可靠的密码输入环境，用户不需要在众目睽睽下在待输入密码的设备的密码输入框中一一输入密码，有效提高了待输入密码的设备中密码等敏感信息输入的安全性和私密性，提升了待输入密码的设备的实用性。

在一个实施例中，将所述密码发送给所述待输入密码的设备的步骤包括：对输入完成的密码进行加密，将加密后的密码发送给所述待输入密码的设备。对输入的密码进行加密，可以有效保证密码传输的安全性，从而进一步保证待输入密码的设备密码输入的安全性。另外，所输入的密码只在最终完成阶段才

通过密文一次性发送，有效提高了密码传输的效率，节省了网络资源。

在一个实施例中，将所述密码发送给所述待输入密码的设备之前，还包括步骤：在密码输入过程中将伪密码发送给所述待输入密码的设备。在移动设备的密码输入过程中，将不涉及密码敏感信息的伪密码发送给待输入密码的设备，从而使用户及时了解密码输入的当前状态，提高了用户体验。

在一个实施例中，当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥。通过该消息的设置，可以减少数据传输的次数，有效降低网络资源损耗。

另一种密码输入装置，包括：

消息接收模块，用于接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

应用程序启动模块，用于根据所述消息启动包含输入界面的应用程序；

密码获取模块，用于获取在所述应用程序的输入界面中输入密码；

密码发送模块，用于将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

上述密码输入装置，接收待输入密码的设备在弹出密码输入框时发送的开启远程输入的消息，根据该消息开启移动设备的应用程序，用户在该应用程序的输入界面中输入密码并发送给待输入密码的设备，实现待输入密码的设备密码的输入。利用移动设备普遍性和私密性的特点，为待输入密码的设备的用户提供了一个更加安全可靠的密码输入环境，用户不需要在众目睽睽下在待输入密码的设备的密码输入框中一一输入密码，有效提高了待输入密码的设备中密码等敏感信息输入的安全性和私密性，提升了待输入密码的设备的实用性。

在一个实施例中，当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥。通过该消息的设置，可以减少数据传输的次数，有效降低网络资源损耗。

在一个实施例中，所述密码发送模块用于对输入完成的密码进行加密，将

加密后的密码发送给所述待输入密码的设备。对输入的密码进行加密，可以有效保证密码传输的安全性，从而进一步保证待输入密码的设备密码输入的安全性。另外，所输入的密码只在最终完成阶段才通过密文一次性发送，有效提高了密码传输的效率，节省了网络资源。

5        在一个实施例中，所述密码输入装置还包括伪密码发送模块，所述伪密码发送模块用于在密码输入过程中将伪密码发送给所述待输入密码的设备。在移动设备的密码输入过程中，将不涉及密码敏感信息的伪密码发送给待输入密码的设备，从而使用户及时了解密码输入的当前状态，提高了用户体验。

## 10    附图说明

图 1 为一实施例的密码输入方法的流程示意图；

图 2 为一实施例的密码输入装置的结构示意图；

图 3 为另一实施例的密码输入方法的流程示意图；

图 4 为另一实施例的密码输入装置的结构示意图；

15       图 5 为一具体实施例的智能平板和智能手机的交互示意图。

## 具体实施方式

为更进一步阐述本发明所采取的技术手段及取得的效果，下面结合附图及较佳实施例，分别从待输入密码的设备角度和移动设备角度出发，对本发明的技术方案，进行清楚和完整的描述。

首先从待输入密码的设备角度出发，对本发明密码输入方法和装置进行详细介绍。

如图 1 所示，一种密码输入方法，包括步骤：

25       S110、在聚焦到密码输入框时，向移动设备发送开启远程输入的消息，其中所述消息用于唤起所述移动设备中包含输入界面的应用程序；

S120、接收所述移动设备发送的在所述应用程序的输入界面中输入的密码；

S130、将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

本实施例方法可以通过相应的程序实现，程序运行在待输入密码的设备中。待输入密码的设备可以为屏幕较大的大屏设备，例如应用于会议或教学领域的智能平板等，也可以为屏幕较小的设备，例如穿戴式设备等。为了更好地理解本发明，下面对各个步骤的具体实施方式进行详细介绍。

- 5       在步骤 S110 中，待输入密码的设备开启后，可以启动一个常驻后台的服务，用于监听输入框的聚焦事件。输入框的聚焦事件的监听可以通过现有技术中已有的方式实现，例如可以通过监听虚拟键盘弹起事件获取当前聚焦的输入框。当检测到输入框聚焦事件时，判断该输入框是否为密码输入框，可以通过读取焦点所在的控件类型或者属性判断是否为密码输入框。若聚焦到密码输入
- 10   框，意味着用户需要在待输入密码的设备中输入密码，则向移动设备发送开启远程输入的消息。

移动设备也被称为行动装置、流动装置、手持装置等，是一种口袋大小的计算设备，通常有一个小的显示屏幕，触控输入，或是小型的键盘。移动设备包括智能手机和平板电脑等。为了保证密码输入的安全性，待输入密码的设备

15   发送消息的移动设备需要为授权的设备。待输入密码的设备中存储有授权的移动设备的信息，当需要进行远程密码输入时，根据存储的移动设备的信息向对应的移动设备发送开启远程输入的消息。

开启远程输入的消息包含的具体内容可以根据用户实际需要进行设置。开启远程输入的消息用于开启移动设备中包含输入界面的应用程序，以使移动设备

20   在输入界面中输入字符，起到替代待输入密码的设备本身输入方式的作用。包含输入界面的应用程序可以为移动设备中能够输入字符的任意现有的应用程序，也可以为用户自行编辑的输入界面。

考虑到数据传输的次数以及网络资源损耗，在一个实施例中，当未与移动设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述

25   密钥用于对移动设备发送的密码进行加密；当与移动设备建立连接后，所述消息包括密钥。连接请求用于建立移动设备与待输入密码的设备之间的通信连接。为了进一步保证数据传输的安全，所述密钥为随机密钥，即每一次开启远程输入时所述消息包含的密钥随机生成，每次发送的密钥基本上都不相同。

在待输入密码的设备与移动设备未建立连接时，待输入密码的设备监听密

码输入框，当聚焦到密码输入框时，向授权的移动设备发送开启远程输入的消息，所述消息包含连接请求。移动设备接收到待输入密码的设备发送的连接请求后，根据该连接请求与待输入密码的设备建立连接，并启动包含输入界面的应用程序。不需要单独将开启远程输入的消息设置为一个预设的消息格式，然后  
5 在未连接时先发送连接请求，再发送该预设的消息，所以本发明消息的设置减少了数据传输的次数，有效降低网络资源损耗。

在待输入密码的设备与移动设备未建立连接时，待输入密码的设备监听密码输入框，当聚焦到密码输入框时，向授权的移动设备发送开启远程输入的消息，所述消息包含连接请求和密钥。移动设备接收到待输入密码的设备发送的  
10 连接请求和密钥后，根据该连接请求与待输入密码的设备建立连接，存储密钥，并启动包含输入界面的应用程序。不需要单独将开启远程输入的消息设置为一个预设的消息形式，然后在未连接时先发送连接请求，再分别发送该预设的消息和密钥，所以本发明消息的设置减少了数据传输的次数，有效降低网络资源损耗。

在待输入密码的设备与移动设备建立连接后，待输入密码的设备监听密码输入框，当聚焦到密码输入框时，向连接的移动设备发送开启远程输入的消息，所述消息包含密钥。移动设备接收到待输入密码的设备发送的密钥后，根据该  
15 密钥启动包含输入界面的应用程序，并将该密钥应用于后续的密码加密。不需要单独将开启远程输入的消息设置为一个预设的消息形式，然后在连接时分别发送该预设的消息以及密钥，所以本发明消息的设置减少了数据传输的次数，有效降低网络资源损耗。

在步骤 S120 中，移动设备接收待输入密码的设备发送的开启远程输入的消息，根据该消息开启包含输入界面的应用程序。然后用户在该输入界面中输入  
20 对应的密码，并将输入的密码发送给待输入密码的设备。

为了保证密码传输的安全性，以及提高数据传输的效率，在一个实施例中，接收所述移动设备发送的在所述应用程序的输入界面中输入的密码的步骤包括：接收所述移动设备对输入完成的密码进行加密后发送的加密密码，所述密  
25 码为在所述应用程序的输入界面中输入的密码。移动设备根据接收的密钥对待传输的密码进行加密，然后将加密的密码传输给待输入密码的设备，从而提高

了数据传输的安全性。移动设备在密码输入完成后再对密码进行一次性加密传输，避免了密码边输入边加密边发送所导致的网络资源的浪费，提高了数据传输的效率。

考虑到当移动设备与待输入密码的设备距离较远，操作移动设备和待输入密码的设备的为不同的用户的情况，为了使操作待输入密码的设备用户及时了解当前密码输入框的密码输入状态，在一个实施例中，接收所述移动设备发送的在所述应用程序的输入界面中输入的密码之前，还可以包括步骤：接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框。伪密码为不同于真实密码的字符，伪密码可以设置为固定形式的字符，例如“\*”等，也可以根据真实密码输入的内容，选取不同于真实密码的任意字符作为伪密码。当用户在移动设备的输入界面中输入密码时，同步发送不同于密码的伪密码，待输入密码的设备接收到伪密码后，将伪密码输入到聚焦的密码输入框内，以使用户及时了解密码输入框的密码输入进展，伪密码发送过程中不涉及真实密码敏感信息的传输，所以在密码输入过程中发送的伪密码不需要进行加密传输。

在步骤 S130 中，待输入密码的设备接收移动设备发送的密码，并输入密码输入框，即实现待输入密码的设备的密码输入。为了保证密码的安全性和私密性，在密码输入框中显示的密码为密文。将密码显示为密文可以通过密码输入框本身所具有的属性实现，也可以在接收到密码后，生成不同于密码的一串字符，然后将生成的一串字符显示在密码输入框，真实的密码隐藏，在发送登录验证请求时将真实的密码发送给对应的服务器。

在一个实施例中，将所述密码输入所述密码输入框的步骤可以包括：对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。若接收到的为加密密码，则需要根据对应的密钥对加密密码进行解密，然后将解密后的密码替换密码输入框中的伪密码，完成密码输入框的密码输入。

基于同一发明构思，本发明还提供一种密码输入装置，下面结合附图对本发明装置的具体实施方式做详细描述。

如图 2 所示，一种密码输入装置，包括：

消息发送模块 110，用于在聚焦到密码输入框时，向移动设备发送开启远

程输入的消息，其中所述消息用于唤起所述移动设备中包含输入界面的应用程序；

密码接收模块 120，用于接收所述移动设备发送的在所述应用程序的输入界面中输入的密码；

5 密码输入模块 130，用于将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

本实施例装置运行在待输入密码的设备中。待输入密码的设备可以为屏幕较大的大屏设备，例如应用于会议或教学领域的智能平板等，也可以为屏幕较小的设备，例如穿戴式设备等。为了更好地理解本发明，下面对各个模块的功能进行详细介绍。

待输入密码的设备开启后，消息发送模块 110 监听输入框的聚焦事件，当检测到输入框聚焦事件时，可以通过读取焦点所在的控件类型或者属性判断是否为密码输入框，若聚焦到密码输入框，意味着用户需要在待输入密码的设备中输入密码，则向移动设备发送开启远程输入的消息。

15 开启远程输入的消息包含的具体内容可以根据用户实际需要进行设置。考虑到数据传输的次数以及网络资源损耗，在一个实施例中，当未与移动设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对移动设备发送的密码进行加密；当与移动设备建立连接后，所述消息包括密钥。连接请求用于建立移动设备与待输入密码的设备之间的通信连接。为了  
20 进一步保证数据传输的安全，所述密钥为随机密钥，即每一次开启远程输入时所述消息包含的密钥随机生成，每次发送的密钥基本上都不相同。

为了保证密码传输的安全性，以及提高数据传输的效率，在一个实施例中，所述密码接收模块 120 用于接收所述移动设备对输入完成的密码进行加密后发送的加密密码，所述密码为在所述应用程序的输入界面中输入的密码。移动设备根据接收的密钥对待传输的密码进行加密，然后将加密的密码传输给待输入密码的设备，从而提高了数据传输的安全性。移动设备在密码输入完成后再对密码进行一次性加密传输，避免了密码边输入边加密边发送所导致的网络资源的浪费，提高了数据传输的效率。

考虑到当移动设备与待输入密码的设备距离较远，操作移动设备和待输入

密码的设备的为不同的用户的情况，为了使操作待输入密码的设备用户及时了解当前密码输入框的密码输入状态，在一个实施例中，所述密码输入装置还可以包括伪密码输入模块 140，所述伪密码输入模块 140 用于接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框。伪密码为不同于真实密码的字符，伪密码可以设置为固定形式的字符，例如“\*”等，也可以根据真实密码输入的内容，选取不同于真实密码的任意字符作为伪密码。当用户在移动设备的输入界面中输入密码时，同步发送不同于密码的伪密码，待输入密码的设备接收到伪密码后，将伪密码输入到聚焦的密码输入框内，以使用户及时了解密码输入框的密码输入进展，伪密码发送过程中不涉及真实密码敏感信息的传输，所以在密码输入过程中发送的伪密码不需要进行加密传输。

密码输入模块 130 接收移动设备发送的密码，并输入密码输入框，即实现待输入密码的设备的密码输入，在一个实施例中，所述密码输入模块 130 用于对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。另外，为了保证密码的安全性和私密性，在密码输入框中显示的密码为密文。将密码显示为密文可以通过密码输入框本身所具有的属性实现，也可以在接收到密码后，生成不同于密码的一串字符，然后将生成的一串字符显示在密码输入框，真实的密码隐藏，在发送登录验证请求时将真实的密码发送给对应的服务器。

下面从移动设备的角度出发，本发明另一种密码输入方法和装置进行详细介绍。

如图 3 所示，一种密码输入方法，包括步骤：

S210、接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

S220、根据所述消息启动包含输入界面的应用程序；

S230、获取在所述应用程序的输入界面中输入密码；

S240、将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示

为密文。

本实施例方法可以通过相应的程序实现，程序运行在移动设备中。移动设备也被称为行动装置、流动装置、手持装置等，是一种口袋大小的计算设备，通常有一个小的显示屏幕，触控输入，或是小型的键盘。移动设备包括智能手机和平板电脑等。为了更好地理解本发明，下面对各个步骤的具体实施方式进行详细介绍。

在步骤 S210 中，待输入密码的设备可以为屏幕较大的智能设备，例如应用于会议或教学领域的智能平板等，也可以为屏幕较小的设备，例如穿戴式设备等。待输入密码的设备开启后，可以启动一个常驻后台的服务，用于监听输入框的聚焦事件。输入框的聚焦事件的监听可以通过现有技术中已有的方式实现，例如可以通过监听虚拟键盘弹起事件获取当前聚焦的输入框。当检测到输入框聚焦事件时，判断该输入框是否为密码输入框，可以通过读取焦点所在的控件类型或者属性判断是否为密码输入框。若聚焦到密码输入框，意味着用户需要在待输入密码的设备中输入密码，则向移动设备发送开启远程输入的消息。

移动设备可以设置一个常驻移动设备后台的服务或应用，用于接收待输入密码的设备发来的开启远程输入的消息。开启远程输入的消息包含的具体内容可以根据用户实际需要进行设置。考虑到数据传输的次数以及网络资源损耗，在一个实施例中，当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥。为了进一步保证数据传输的安全，所述密钥为随机密钥，即每一次开启远程输入时所述消息包含的密钥随机生成，每次发送的密钥基本上都不相同。

在步骤 S220 中，开启远程输入的消息用于开启移动设备中包含输入界面的应用程序，以使移动设备在输入界面中输入字符，起到替代待输入密码的设备本身输入方式的作用。包含输入界面的应用程序可以为移动设备中能够输入字符的任意现有的应用程序，也可以为用户自行编辑的输入界面。

在步骤 S230 和步骤 S240 中，用户在该输入界面中输入对应的密码，将输入的密码发送给待输入密码的设备，待输入密码的设备将密码输入所述密码输

入框，从而完成待输入密码的设备的密码输入过程。

为了保证密码传输的安全性，以及提高数据传输的效率，在一个实施例中，将所述密码发送给所述待输入密码的设备的步骤可以包括：对输入完成的密码进行加密，将加密后的密码发送给所述待输入密码的设备。移动设备根据接收的密钥对待传输的密码进行加密，然后将加密的密码传输给待输入密码的设备，从而提高了数据传输的安全性。移动设备在密码输入完成后再对密码进行一次性加密传输，避免了密码边输入边加密边发送所导致的网络资源的浪费，提高了数据传输的效率。

考虑到当移动设备与待输入密码的设备距离较远，操作移动设备和待输入密码的设备的为不同的用户的情况，为了使操作待输入密码的设备的用户及时了解当前密码输入框的密码输入状态，在一个实施例中，将所述密码发送给所述待输入密码的设备之前，还可以包括步骤：在密码输入过程中将伪密码发送给所述待输入密码的设备。伪密码为不同于真实密码的字符，伪密码可以设置为固定形式的字符，例如“\*”等，也可以根据真实密码输入的内容，选取不同于真实密码的任意字符作为伪密码。当用户在移动设备的输入界面中输入密码时，同步发送不同于密码的伪密码，待输入密码的设备接收到伪密码后，将伪密码输入到聚焦的密码输入框内，以使用户及时了解密码输入框的密码输入进展，伪密码发送过程中不涉及真实密码敏感信息的传输，所以在密码输入过程中发送的伪密码不需要进行加密传输。

基于同一发明构思，本发明还提供另一种密码输入装置，下面结合附图对本发明装置的具体实施方式做详细描述。

如图4所示，一种密码输入装置，包括：

消息接收模块210，用于接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

应用程序启动模块220，用于根据所述消息启动包含输入界面的应用程序；

密码获取模块230，用于获取在所述应用程序的输入界面中输入密码；

密码发送模块240，用于将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

本实施例装置可以通过相应的程序实现，程序运行在移动设备中，移动设备包括智能手机和平板电脑等。为了更好地理解本发明，下面对各个模块的功能进行详细介绍。

消息接收模块 210 为一个常驻移动设备后台的服务或应用，用于接收待输入密码的设备在聚焦到密码输入框时发来的开启远程输入的消息。开启远程输入的消息包含的具体内容可以根据用户实际需要进行设置。考虑到数据传输的次数以及网络资源损耗，在一个实施例中，当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥。为了进一步保证数据传输的安全，所述密钥为随机密钥，即每一次开启远程输入时所述消息包含的密钥随机生成，每次发送的密钥基本上都不相同。

开启远程输入的消息用于开启移动设备中包含输入界面的应用程序，以使移动设备在输入界面中输入字符，起到替代待输入密码的设备本身输入方式的作用。包含输入界面的应用程序可以为移动设备中能够输入字符的任意现有的应用程序，也可以为用户自行编辑的输入界面。

用户在该输入界面中输入对应的密码，密码获取模块 230 获取输入的密码，密码发送模块 240 将输入的密码发送给待输入密码的设备，待输入密码的设备将密码输入所述密码输入框，从而完成待输入密码的设备的密码输入过程。

为了保证密码传输的安全性，以及提高数据传输的效率，在一个实施例中，所述密码发送模块 240 用于对输入完成的密码进行加密，将加密后的密码发送给所述待输入密码的设备。移动设备根据接收的密钥对待传输的密码进行加密，然后将加密的密码传输给待输入密码的设备，从而提高了数据传输的安全性。移动设备在密码输入完成后再对密码进行一次性加密传输，避免了密码边输入边加密边发送所导致的网络资源的浪费，提高了数据传输的效率。

考虑到当移动设备与待输入密码的设备距离较远，操作移动设备和待输入密码的设备的为不同的用户的情况，为了使操作待输入密码的设备的用户及时了解当前密码输入框的密码输入状态，在一个实施例中，所述密码输入装置还可以包括伪密码发送模块 250，所述伪密码发送模块 250 用于在密码输入过程中将伪密码发送给所述待输入密码的设备。伪密码为不同于真实密码的字符，

伪密码可以设置为固定形式的字符，也可以根据真实密码输入的内容，选取不同于真实密码的任意字符作为伪密码。当用户在移动设备的输入界面中输入密码时，同步发送不同于密码的伪密码，待输入密码的设备接收到伪密码后，将伪密码输入到聚焦的密码输入框内，以使用户及时了解密码输入框的密码输入  
5 进展，伪密码发送过程中不涉及真实密码敏感信息的传输，所以在密码输入过程中发送的伪密码不需要进行加密传输。

为了更好地理解本发明，下面结合一个具体应用场景对本发明的实施方式进行详细介绍。

10 例如，当用户采用智能平板进行会议的过程中，需要登录一个应用，因此需要输入该应用的登录信息，例如密码等。按照传统的方法，用户需要在智能平板弹出的密码输入框中直接输入密码，由于智能平板的屏幕较大，在密码输入过程中就会被进行会议的其它用户看到，安全性和私密性不高。而本发明通过小屏幕设备代替大屏幕设备输入的方式很好地解决了该问题。下面结合图 5  
15 对智能平板和智能手机交互的过程进行说明。

如图 5 所示，智能平板和智能手机的交互过程包括：

S1、智能平板聚焦到密码输入框时，向授权的智能手机发送开启远程输入的消息，该消息包括连接请求和密钥；

20 S2、智能手机接收到该消息后，根据连接请求与智能平板建立连接，存储密钥，并开启包含输入界面的应用程序；用户在输入界面中输入密码时，智能手机同步将“\*”号的伪密码发送给智能平板，智能平板将“\*”号输入密码输入框；

25 S3、用户在智能手机的输入界面完成密码输入后，智能手机根据存储的密钥对密码进行加密，然后将加密的密码发送给智能平板；智能平板根据对应的密钥对接收的加密的密码进行解密，然后将解密的密码替换密码输入框中的伪密码，则可以根据该密码进行应用的登录。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明的保护范围应以所

5 附权利要求为准。

## 权利要求书

1、一种密码输入方法，其特征在于，包括步骤：

在聚焦到密码输入框时，向移动设备发送开启远程输入的消息，其中所述消息用于唤起所述移动设备中包含输入界面的应用程序；

5 接收所述移动设备发送的在所述应用程序的输入界面中输入的密码；

将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

2、根据权利要求 1 所述的密码输入方法，其特征在于，

接收所述移动设备发送的在所述应用程序的输入界面中输入的密码的步骤包括：接收所述移动设备对输入完成的密码进行加密后发送的加密密码，所述密码为在所述应用程序的输入界面中输入的密码；

接收所述移动设备发送的在所述应用程序的输入界面中输入的密码之前，还包括步骤：接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框；

15 将所述密码输入所述密码输入框的步骤包括：对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。

3、根据权利要求 1 或 2 所述的密码输入方法，其特征在于，当未与移动设备建立连接时，所述消息包括连接请求，或者包括连接请求和密钥，所述密钥用于对移动设备发送的密码进行加密；当与移动设备建立连接后，所述消息包括密钥。

4、一种密码输入方法，其特征在于，包括步骤：

接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

根据所述消息启动包含输入界面的应用程序；

25 获取在所述应用程序的输入界面中输入密码；

将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

5、根据权利要求 4 所述的密码输入方法，其特征在于，

将所述密码发送给所述待输入密码的设备的步骤包括：对输入完成的密码进行加密，将加密后的密码发送给所述待输入密码的设备；

将所述密码发送给所述待输入密码的设备之前，还包括步骤：在密码输入过程中将伪密码发送给所述待输入密码的设备。

- 5        6、根据权利要求 4 或 5 所述的密码输入方法，其特征在于，当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥。

7、一种密码输入装置，其特征在于，包括：

- 10        消息发送模块，用于在聚焦到密码输入框时，向移动设备发送开启远程输入的消息，其中所述消息用于唤起所述移动设备中包含输入界面的应用程序；

密码接收模块，用于接收所述移动设备发送的在所述应用程序的输入界面中输入的密码；

- 15        密码输入模块，用于将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

8、根据权利要求 7 所述的密码输入装置，其特征在于，

当未与移动设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对移动设备发送的密码进行加密；当与移动设备建立连接后，所述消息包括密钥；

- 20        所述密码接收模块用于接收所述移动设备对输入完成的密码进行加密后发送的加密密码，所述密码为在所述应用程序的输入界面中输入的密码；

所述密码输入装置还包括伪密码输入模块，所述伪密码输入模块用于接收所述移动设备在密码输入过程中发送的伪密码，将所述伪密码输入所述密码输入框；

- 25        所述密码输入模块用于对接收的所述加密密码进行解密，将所述密码输入框中的伪密码替换为解密后的密码。

9、一种密码输入装置，其特征在于，包括：

消息接收模块，用于接收待输入密码的设备在聚焦到密码输入框时发送的开启远程输入的消息；

应用程序启动模块，用于根据所述消息启动包含输入界面的应用程序；

密码获取模块，用于获取在所述应用程序的输入界面中输入密码；

密码发送模块，用于将所述密码发送给所述待输入密码的设备，以使所述待输入密码的设备将所述密码输入所述密码输入框，其中所述密码在所述密码输入框中显示为密文。

10、根据权利要求 9 所述的密码输入装置，其特征在于，

当未与待输入密码的设备建立连接时，所述消息包括连接请求，或者，包括连接请求和密钥，所述密钥用于对密码进行加密；当与待输入密码的设备建立连接后，所述消息包括密钥；

所述密码发送模块用于对输入完成的密码进行加密，将加密后的密码发送给所述待输入密码的设备；

所述密码输入装置还包括伪密码发送模块，所述伪密码发送模块用于在密码输入过程中将伪密码发送给所述待输入密码的设备。

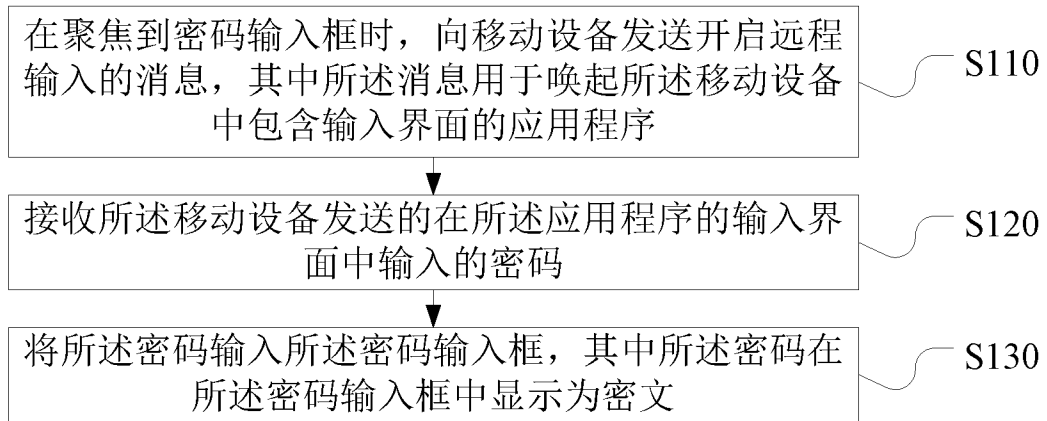


图 1

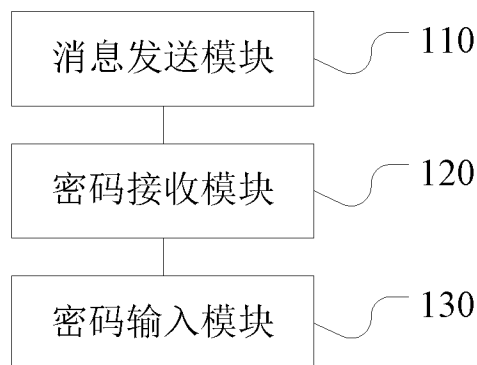


图 2

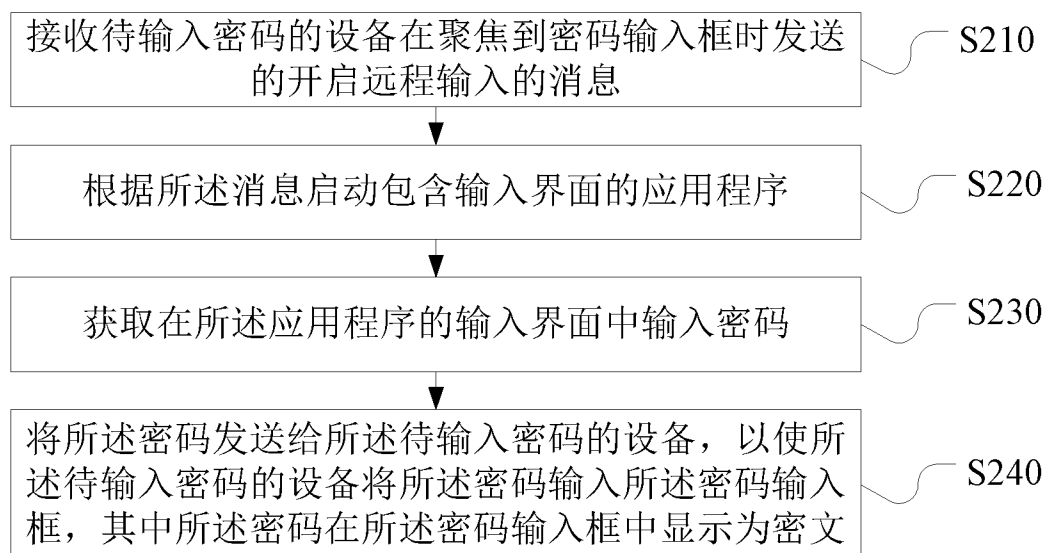


图 3

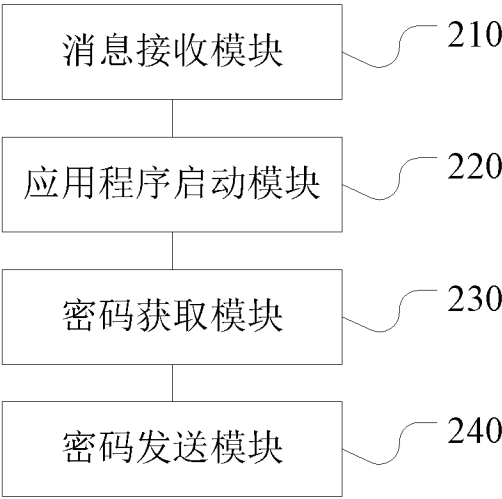


图 4

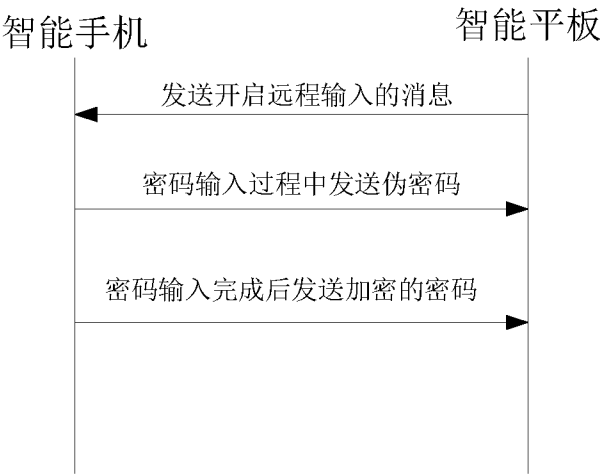


图 5

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/CN2017/077050

## A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30 (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)

DWPI, SIPOABS, CNABS, CNTXT, CNKI: Password, cipher, input, safety, security, fake, encipher, encrypt, decipher, decrypt, replace, remote, send, receive, 密码, 输入, 安全, 私密, 伪密码, 加密, 解密, 替换, 远程, 遥控, 发送, 接收

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                    | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| E         | CN 106599632 A (GUANGZHOU CVT ELECTRONICS TECHNOLOGY CO., LTD. et al.), 26 April 2017 (26.04.2017), claims 1-10                                                       | 1-10                  |
| X         | CN 103425944 A (EXCELSECU DATA TECHNOLOGY INC.), 04 December 2013 (04.12.2013), description, paragraphs 0002-0003 and 0054-0103, and figures 1-4                      | 1, 4, 7, 9            |
| Y         | CN 103425944 A (EXCELSECU DATA TECHNOLOGY INC.), 04 December 2013 (04.12.2013), description, paragraphs 0002-0003 and 0054-0103, and figures 1-4                      | 2-3, 5-6, 8, 10       |
| Y         | CN 105205386 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 30 December 2015 (30.12.2015), description, paragraphs 0013, 0019, 0030-0043 and 0059-0067, and figures 1-9 | 2-3, 5-6, 8, 10       |

☐ 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<br>12 July 2017 | Date of mailing of the international search report<br>09 August 2017 |
|---------------------------------------------------------------------------|----------------------------------------------------------------------|

|                                                                                                                                                                                                               |                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Name and mailing address of the ISA<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No. (86-10) 62019451 | Authorized officer<br><br>ZHANG, Yan<br><br>Telephone No. (86-10) 62411679 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2017/077050

| Patent Documents referred<br>in the Report | Publication Date | Patent Family    | Publication Date |
|--------------------------------------------|------------------|------------------|------------------|
| CN 106599632 A                             | 26 April 2017    | None             |                  |
| CN 103425944 A                             | 04 December 2013 | None             |                  |
| CN 105205386 A                             | 30 December 2015 | EP 3061024 A1    | 31 August 2016   |
|                                            |                  | KR 20170023113 A | 02 March 2017    |
|                                            |                  | WO 2015196970 A1 | 30 December 2015 |
|                                            |                  | JP 2017510869 A  | 13 April 2017    |
|                                            |                  | EP 3061024 A4    | 05 April 2017    |
|                                            |                  | US 2017061139 A1 | 02 March 2017    |

## 国际检索报告

国际申请号

PCT/CN2017/077050

## A. 主题的分类

G06F 21/30(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))

DWPI, SIPOABS, CNABS, CNTXT, CNKI: Password, cipher, input, safety, security, fake, encipher, encrypt, decipher, decrypt, replace, remote, send, receive, 密码, 输入, 安全, 私密, 伪密码, 加密, 解密, 替换, 远程, 遥控, 发送, 接收

## 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      |
|------|-------------------------------------------------------------------------------------------------------|--------------|
| E    | CN 106599632 A (广州视源电子科技股份有限公司等) 2017年 4月 26日 (2017 - 04 - 26)<br>权利要求1-10                            | 1-10         |
| X    | CN 103425944 A (深圳市文鼎创数据科技有限公司) 2013年 12月 4日 (2013 - 12 - 04)<br>说明书0002-0003、0054-0103段, 图1-4        | 1、4、7、9      |
| Y    | CN 103425944 A (深圳市文鼎创数据科技有限公司) 2013年 12月 4日 (2013 - 12 - 04)<br>说明书0002-0003、0054-0103段, 图1-4        | 2-3、5-6、8、10 |
| Y    | CN 105205386 A (腾讯科技深圳有限公司) 2015年 12月 30日 (2015 - 12 - 30)<br>说明书0013、0019、0030-0043、0059-0067段, 图1-9 | 2-3、5-6、8、10 |

☐ 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

“&amp;” 同族专利的文件

国际检索实际完成的日期

2017年 7月 12日

国际检索报告邮寄日期

2017年 8月 9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

张焰

电话号码 (86-10)62411679

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2017/077050

| 检索报告引用的专利文件 |           |   | 公布日<br>(年/月/日) | 同族专利 |             |    | 公布日<br>(年/月/日) |
|-------------|-----------|---|----------------|------|-------------|----|----------------|
| CN          | 106599632 | A | 2017年 4月 26日   | 无    |             |    |                |
| CN          | 103425944 | A | 2013年 12月 4日   | 无    |             |    |                |
| CN          | 105205386 | A | 2015年 12月 30日  | EP   | 3061024     | A1 | 2016年 8月 31日   |
|             |           |   |                | KR   | 20170023113 | A  | 2017年 3月 2日    |
|             |           |   |                | WO   | 2015196970  | A1 | 2015年 12月 30日  |
|             |           |   |                | JP   | 2017510869  | A  | 2017年 4月 13日   |
|             |           |   |                | EP   | 3061024     | A4 | 2017年 4月 5日    |
|             |           |   |                | US   | 2017061139  | A1 | 2017年 3月 2日    |