

(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
2017 年 2 月 2 日 (02.02.2017)



(10) 国际公布号
WO 2017/016064 A1

- (51) 国际专利分类号:
G06F 9/46 (2006.01)
- (21) 国际申请号: PCT/CN2015/091236
- (22) 国际申请日: 2015 年 9 月 30 日 (30.09.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510454914.X 2015 年 7 月 29 日 (29.07.2015) 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: 李小辉 (LI, Xiaohui); 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: 北京友联知识产权代理事务所(普通合
伙) (YOU LINK INTELLECTUAL PROPERTY
LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,
CU, CZ, DE, 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,

[见续页]

(54) Title: OPERATION SYSTEM SWITCHING METHOD, OPERATION SYSTEM SWITCHING APPARATUS AND TER-
MINAL

(54) 发明名称: 操作系统切换方法、操作系统切换装置和终端

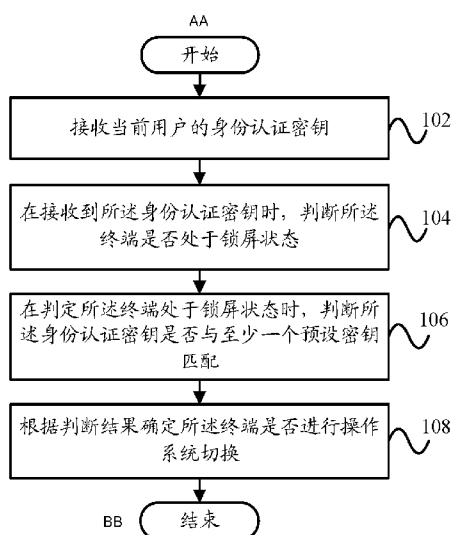


图 1

- 102 Receiving an identity authentication key of a current user
- 104 When the identity authentication key is received, determining whether the terminal is in a screen locking state
- 106 When it is determined that the terminal is in the screen locking state, determining whether the identity authentication key matches at least one pre-set key
- 108 Determining whether the terminal performs operation system switching according to a determination result
- AA Start
- BB End

(57) Abstract: An operation system switching method, an operation system switching apparatus and a terminal. The operation system switching method is used for a terminal to perform operation system switching, a plurality of operation systems are installed in the terminal, and the terminal runs at a current operation system. The switching method comprises: receiving an identity authentication key of a current user (102); when the identity authentication key is received, determining whether the terminal is in a screen locking state (104); when it is determined that the terminal is in the screen locking state, determining whether the identity authentication key matches at least one pre-set key (106); and determining whether the terminal performs operation system switching according to a determination result (108). By means of the method, apparatus and terminal, the problem that the steps of operation system switching performed by a multi-operation system terminal in a screen locking state are complex existing in the prior art can be solved, and the terminal can directly complete a dual function of identity authentication and operation system switching in the screen locking state, so that the convenience and security of operation system switching by a terminal are improved, and the user experience is improved.

(57) 摘要:

[见续页]

WO 2017/016064 A1



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))。

一种操作系统切换方法、一种操作系统切换装置和一种终端。操作系统切换方法用于终端进行操作系统切换，终端上安装有多个操作系统，终端运行在当前操作系统，切换方法包括：接收当前用户的身份认证密钥（102）；在接收到身份认证密钥时，判断终端是否处于锁屏状态（104）；在判定终端处于锁屏状态时，判断身份认证密钥是否与至少一个预设密钥匹配（106）；根据判断结果确定终端是否进行操作系统切换（108）。通过该方法、装置和终端，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

操作系统切换方法、操作系统切换装置和终端

技术领域

5 本发明涉及终端技术领域，具体而言，涉及一种操作系统切换方法、一种操作系统切换装置和一种终端。

背景技术

10 目前，随着用户对终端需求的差异化的深化，以及终端日益突出的安全问题，多操作系统系统终端已经在市场上崭露头角，但是多操作系统之间的切换方式到底该如何设计，切换方式设计的合不合理，直接关系到用户的体验。

15 现有的一种多操作系统切换方法是：通过其中一个系统提供的切换入口（如桌面图标、菜单选项或者下拉托盘）切换到其他的系统中，这种设计方法是最常见的，也是比较符合用户习惯的。

20 但是，这种多操作系统间的切换方式需要解锁进入到一个操作系统中，再通过该操作系统提供的切换入口，切换到其它操作系统中。考虑如下一个场景或用户需求：待机前用户处于系统 A 中，锁屏后用户需要进入到系统 B 中，这时的操作是先解锁进入到系统 A 中，再切换到系统 B 中。很显然，先解锁进入 A 系统显得比较多余，如果在锁屏界面能够直接进入所需目标操作系统中，将会对用户的体验效果带来不小的提升。

因此，如何实现将身份认证和操作系统切换融为一体，在锁屏界面能够直接进入所需的目标操作系统中，从而提高终端操作系统切换的便利性与安全性成为亟待解决的技术问题。

25

发明内容

本发明正是基于上述问题，提出了一种新的技术方案，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高

了终端操作系统切换的便利性与安全性，从而提升了用户体验。

有鉴于此，本发明的一方面提出了一种操作系统切换方法，用于终端进行操作系统切换，所述终端上安装有多个操作系统，所述终端运行在当前操作系统，所述切换方法包括：接收当前用户的身份认证密钥；在接收到
5 所述身份认证密钥时，判断所述终端是否处于锁屏状态；在判定所述终端处于锁屏状态时，判断所述身份认证密钥是否与至少一个预设密钥匹配；根据判断结果确定所述终端是否进行操作系统切换。

在该技术方案中，终端上安装有多个操作系统，在当前用户需要切换操作系统时，在终端上输入身份认证密钥，通过终端在接收到当前用户的身份认证密钥时，判断终端是否处于锁屏状态，在判定终端处于锁屏状态时，
10 判断身份认证密钥是否与至少一个预设密钥匹配，以根据判断结果确定终端是否进行操作系统切换，如此，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利
15 性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述根据判断结果确定所述终端是否进行操作系统切换，具体包括：在判定所述身份认证密钥与所述至少一个预设密钥匹配时，解锁屏幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至
20 少一个预设密钥不匹配时，保持所述锁屏状态，并控制所述终端运行在所述当前操作系统。

在该技术方案中，在终端处于锁屏状态时，需要进行身份认证过程，在判定当前用户的身份认证密钥与至少一个预设密钥匹配时，说明身份认证成功，则解锁屏幕，并控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，如此，实现在终端锁屏状态下，直接完成身份认证和操
25 作系统切换的双重功能，解决了现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，而在判定当前用户的身份认证密钥与至少一个预设密钥不匹配时，说明身份认证失败，有可能是恶意操作，则保持锁屏状态，并控制终端运行在当前操作系统，从而避免了用户信息的泄漏，提

高了终端操作系统切换的便利性与安全性，从而提升了用户体验；当然也可以设置允许错误输入身份认证密钥的次数，进一步提高了终端系统的安全性和可靠性。

在上述技术方案中，优选地，还包括：在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至少一个预设密钥匹配；以及在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制所述终端运行在所述当前操作系统。

在该技术方案中，在判定终端处于解锁状态时，即无需身份认证过程，仅仅需要进行操作系统切换，则在判定身份认证密钥与至少一个预设密钥匹配时，控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，在判定身份认证密钥与至少一个预设密钥不匹配时，控制终端运行在当前操作系统，如此，通过本方案，不仅可以实现终端处于锁屏状态下的操作系统切换，同时兼顾了终端处于解锁状态下的操作系统切换功能，进一步提高了终端操作系统切换的便利性与适用性，从而提升了用户体验。

在上述技术方案中，优选地，在所述接收当前用户的身份认证密钥之前，还包括：建立所述至少一个预设密钥与所述终端中的所述多个操作系统的匹配关系。

在该技术方案中，首先进行预设密钥的设置，具体地，根据实际需要终端上的每一个操作系统进行预设密钥的设置，即每一个操作系统都关联一个特定的预设密钥，以供在切换操作系统时与当前用户的身份认证密钥进行匹配，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述身份认证密钥和所述至少一个预设密钥包括：指纹密钥、图案密钥和数字密钥。

在该技术方案中，身份认证密钥和至少一个预设密钥包含但不限于：指纹密钥、图案密钥和数字密钥，即用户可以根据实际需要选择一种密钥形式，选定之后，此被选定的密钥形式可以被应用到终端上所有的操作系统

中，如此，多样化的密钥形式选择，提高了操作系统切换方法的适用性，从而提升了用户体验。

本发明的另一方面提出了一种操作系统切换装置，用于终端进行操作系统切换，所述终端上安装有多个操作系统，所述终端运行在当前操作系统，所述切换装置包括：接收模块，用于接收当前用户的身份认证密钥；判断模块，用于在接收到所述身份认证密钥时，判断所述终端是否处于锁屏状态，以及在判定所述终端处于锁屏状态时，判断所述身份认证密钥是否与至少一个预设密钥匹配；控制模块，用于根据判断结果确定所述终端是否进行操作系统切换。

在该技术方案中，终端上安装有多个操作系统，在当前用户需要切换操作系统时，在终端上输入身份认证密钥，通过终端在接收到当前用户的身份认证密钥时，判断终端是否处于锁屏状态，在判定终端处于锁屏状态时，判断身份认证密钥是否与至少一个预设密钥匹配，以根据判断结果确定终端是否进行操作系统切换，如此，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述控制模块具体用于：在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制解锁屏幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制保持锁屏状态，并控制所述终端运行在所述当前操作系统。

在该技术方案中，在终端处于锁屏状态时，需要进行身份认证过程，在判定当前用户的身份认证密钥与至少一个预设密钥匹配时，说明身份认证成功，则解锁屏幕，并控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，如此，实现在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，解决了现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，而在判定当前用户的身份认证密钥与至少一个预设密钥不匹配时，说明身份认证失败，有可能是恶意操作，则保持锁

屏状态，并控制终端运行在当前操作系统，从而避免了用户信息的泄漏，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验；当然也可以设置允许错误输入身份认证密钥的次数，进一步提高了终端系统的安全性和可靠性。

5 在上述技术方案中，优选地，所述判断模块还用于：在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至少一个预设密钥匹配；以及所述控制模块还用于在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至少一个预设密
10 钥不匹配时，控制所述终端运行在所述当前操作系统。

 在该技术方案中，在判定终端处于解锁状态时，即无需身份认证过程，仅仅需要进行操作系统切换，则在判定身份认证密钥与至少一个预设密钥匹配时，控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，在判定身份认证密钥与至少一个预设密钥不匹配时，控制终端运行在当
15 前操作系统，如此，通过本方案，不仅可以实现终端处于锁屏状态下的操作系统切换，同时兼顾了终端处于解锁状态下的操作系统切换功能，进一步提高了终端操作系统切换的便利性与适用性，从而提升了用户体验。

 在上述技术方案中，优选地，还包括：关联模块，用于在所述接收当前用户的身份认证密钥之前，建立所述至少一个预设密钥与所述终端中的所
20 述多个操作系统的匹配关系。

 在该技术方案中，首先进行预设密钥的设置，具体地，根据实际需要终端上的每一个操作系统进行预设密钥的设置，即每一个操作系统都关联一个特定的预设密钥，以供在切换操作系统时与当前用户的身份认证密钥进行匹配，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。
25 验。

 在上述技术方案中，优选地，所述身份认证密钥和所述至少一个预设密钥包括：指纹密钥、图案密钥和数字密钥。

 在该技术方案中，身份认证密钥和至少一个预设密钥包含但不限于：指纹密钥、图案密钥和数字密钥，即用户可以根据实际需要选择一种密钥形式，选定之后，此被选定的密钥形式可以被应用到终端上所有的操作系统
30 。

中，如此，多样化的密钥形式选择，提高了操作系统切换方法的适用性，从而提升了用户体验。

本发明的又一方面提出了一种终端，包括如上任一项技术方案所述的操作系统切换装置，因此，该终端具有上任一项技术方案所述的操作系统切换装置的所有有益效果，在此不再赘述。

通过本发明的技术方案，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，同时兼顾了终端处于解锁状态下的操作系统切换功能，从而提升了用户体验。

附图说明

图 1 示出了根据本发明的一个实施例的操作系统切换方法的流程示意图；

图 2 示出了根据本发明的一个实施例的操作系统切换装置的框图；

图 3 示出了根据本发明的一个实施例的终端的框图；

图 4 示出了根据本发明的一个实施例的多操作系统终端框架结构图；

图 5 示出了根据本发明的一个实施例的锁屏状态下操作系统与预设密钥的对应关系的方案图；

图 6 示出了根据本发明的一个实施例的解锁状态下操作系统与预设密钥的对应关系的方案图；

图 7 示出了根据本发明的另一个实施例的多操作系统终端框架结构图。

具体实施方式

为了可以更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，

本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的操作系统切换方法的流程示意图。

- 5 如图 1 所示，本发明的一个实施例的操作系统切换方法，用于终端进行操作系统切换，所述终端上安装有多个操作系统，所述终端运行在当前操作系统，所述切换方法包括：步骤 102，接收当前用户的身份认证密钥；步骤 104，在接收到所述身份认证密钥时，判断所述终端是否处于锁屏状态；步骤 106，在判定所述终端处于锁屏状态时，判断所述身份认证密钥是否与至少一个预设密钥匹配；步骤 108，根据判断结果确定所述终端是否进行操作系统切换。

- 15 在该技术方案中，终端上安装有多个操作系统，在当前用户需要切换操作系统时，在终端上输入身份认证密钥，通过终端在接收到当前用户的身份认证密钥时，判断终端是否处于锁屏状态，在判定终端处于锁屏状态时，判断身份认证密钥是否与至少一个预设密钥匹配，以根据判断结果确定终端是否进行操作系统切换，如此，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

- 20 在上述技术方案中，优选地，所述步骤 108 具体包括：在判定所述身份认证密钥与所述至少一个预设密钥匹配时，解锁屏幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，保持所述锁屏状态，并控制所述终端运行在所述当前操作系统。

- 25 在该技术方案中，在终端处于锁屏状态时，需要进行身份认证过程，在判定当前用户的身份认证密钥与至少一个预设密钥匹配时，说明身份认证成功，则解锁屏幕，并控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，如此，实现在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，解决了现有技术中多操作系统终端在锁屏时进行

操作系统切换步骤繁琐的问题，而在判定当前用户的身份认证密钥与至少一个预设密钥不匹配时，说明身份认证失败，有可能是恶意操作，则保持锁屏状态，并控制终端运行在当前操作系统，从而避免了用户信息的泄漏，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验；当然也可以设置允许错误输入身份认证密钥的次数，进一步提高了终端系统的安全性和可靠性。

在上述技术方案中，优选地，还包括：在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至少一个预设密钥匹配；以及在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制所述终端运行在所述当前操作系统。

在该技术方案中，在判定终端处于解锁状态时，即无需身份认证过程，仅仅需要进行操作系统切换，则在判定身份认证密钥与至少一个预设密钥匹配时，控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，在判定身份认证密钥与至少一个预设密钥不匹配时，控制终端运行在当前操作系统，如此，通过本方案，不仅可以实现终端处于锁屏状态下的操作系统切换，同时兼顾了终端处于解锁状态下的操作系统切换功能，进一步提高了终端操作系统切换的便利性与适用性，从而提升了用户体验。

在上述技术方案中，优选地，在所述接收当前用户的身份认证密钥之前，还包括：建立所述至少一个预设密钥与所述终端中的所述多个操作系统的匹配关系。

在该技术方案中，首先进行预设密钥的设置，具体地，根据实际需要终端上的每一个操作系统进行预设密钥的设置，即每一个操作系统都关联一个特定的预设密钥，以供在切换操作系统时与当前用户的身份认证密钥进行匹配，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述身份认证密钥和所述至少一个预设密钥包括：指纹密钥、图案密钥和数字密钥。

在该技术方案中，身份认证密钥和至少一个预设密钥包含但不限于：指纹密钥、图案密钥和数字密钥，即用户可以根据实际需要选择一种密钥形式，选定之后，此被选定的密钥形式可以被应用到终端上所有的操作系统中，如此，多样化的密钥形式选择，提高了操作系统切换方法的适用性，从而提升了用户体验。

图 2 示出了根据本发明的一个实施例的操作系统切换装置的框图。

如图 2 所示，本发明的一个实施例的操作系统切换装置 200，用于终端进行操作系统切换，所述终端上安装有多个操作系统，所述终端运行在当前操作系统，所述切换装置包括：接收模块 202，用于接收当前用户的身份认证密钥；判断模块 204，用于在接收到所述身份认证密钥时，判断所述终端是否处于锁屏状态，以及在判定所述终端处于锁屏状态时，判断所述身份认证密钥是否与至少一个预设密钥匹配；控制模块 206，用于根据判断结果确定所述终端是否进行操作系统切换。

在该技术方案中，终端上安装有多个操作系统，在当前用户需要切换操作系统时，在终端上输入身份认证密钥，通过终端在接收到当前用户的身份认证密钥时，判断终端是否处于锁屏状态，在判定终端处于锁屏状态时，判断身份认证密钥是否与至少一个预设密钥匹配，以根据判断结果确定终端是否进行操作系统切换，如此，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述控制模块 206 具体用于：在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制解锁屏幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制保持锁屏状态，并控制所述终端运行在所述当前操作系统。

在该技术方案中，在终端处于锁屏状态时，需要进行身份认证过程，在判定当前用户的身份认证密钥与至少一个预设密钥匹配时，说明身份认证成功，则解锁屏幕，并控制终端从当前操作系统切换至与身份认证密钥对应

的目标操作系统，如此，实现在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，解决了现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，而在判定当前用户的身份认证密钥与至少一个预设密钥不匹配时，说明身份认证失败，有可能是恶意操作，则保持锁屏状态，并控制终端运行在当前操作系统，从而避免了用户信息的泄漏，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验；当然也可以设置允许错误输入身份认证密钥的次数，进一步提高了终端系统的安全性和可靠性。

在上述技术方案中，优选地，所述判断模块 204 还用于：在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至少一个预设密钥匹配；以及所述控制模块 206 还用于在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制所述终端运行在所述当前操作系统。

在该技术方案中，在判定终端处于解锁状态时，即无需身份认证过程，仅仅需要进行操作系统切换，则在判定身份认证密钥与至少一个预设密钥匹配时，控制终端从当前操作系统切换至与身份认证密钥对应的目标操作系统，在判定身份认证密钥与至少一个预设密钥不匹配时，控制终端运行在当前操作系统，如此，通过本方案，不仅可以实现终端处于锁屏状态下的操作系统切换，同时兼顾了终端处于解锁状态下的操作系统切换功能，进一步提高了终端操作系统切换的便利性与适用性，从而提升了用户体验。

在上述技术方案中，优选地，还包括：关联模块 208，用于在所述接收当前用户的身份认证密钥之前，建立所述至少一个预设密钥与所述终端中的所述多个操作系统的匹配关系。

在该技术方案中，首先进行预设密钥的设置，具体地，根据实际需要终端上的每一个操作系统进行预设密钥的设置，即每一个操作系统都关联一个特定的预设密钥，以供在切换操作系统时与当前用户的身份认证密钥进行匹配，提高了终端操作系统切换的便利性与安全性，从而提升了用户体验。

在上述技术方案中，优选地，所述身份认证密钥和所述至少一个预设密钥包括：指纹密钥、图案密钥和数字密钥。

在该技术方案中，身份认证密钥和至少一个预设密钥包含但不限于：指纹密钥、图案密钥和数字密钥，即用户可以根据实际需要选择一种密钥形式，选定之后，此被选定的密钥形式可以被应用到终端上所有的操作系统中，如此，多样化的密钥形式选择，提高了操作系统切换方法的适用性，从而提升了用户体验。

图 3 示出了根据本发明的一个实施例的终端的框图。

如图 3 所示，本发明的一个实施例的终端 300，包括如上任一项技术方案所述的操作系统切换装置 200，因此，该终端 300 具有上任一项技术方案所述的操作系统切换装置 200 的所有有益效果，在此不再赘述。

下面结合图 4 至图 7 详细说明本发明的技术方案：

图 4 示出了根据本发明的一个实施例的多操作系统终端框架结构图。

图 5 示出了根据本发明的一个实施例的锁屏状态下操作系统与预设密钥的对应关系的方案图。

图 6 示出了根据本发明的一个实施例的解锁状态下操作系统与预设密钥的对应关系的方案图。

图 7 示出了根据本发明的另一个实施例的多操作系统终端框架结构图。

为了更好的说明本发明的技术方案，下面给出一种多操作系统终端的框架结构，如图 4 所示，以此多操作系统终端来阐述本发明。应当清楚，本多操作系统终端只是为了说明发明的技术方案，本发明的技术方案不仅适用于该种架构的多操作系统终端，对其它架构类型的多操作系统终端也是适用的。

如图 4 所示，本发明的一个实施例的多操作系统终端框架结构，这里多操作系统终端，是指有多个操作系统运行在终端上，假设操作系统的个数为 n ，将这些操作系统分别称之为系统 1，系统 2，...，系统 n 。为了能够实现统一管理各个操作系统，增加了一个管理的模块，暂且称之为管理系统（即控制模块），管理系统能够对所有的操作系统进行统一的管理调

度。在多操作系统终端中，各操作系统共享终端的某些硬件资源，比如指纹识别传感器、视频、音频等。

其中，终端中每个操作系统均是独立运行的，但是操作系统与操作系统之间存在数据交互，数据交互的方式也可以多种多样的，比如共享内存、发送消息、管道等等。

为了实现本发明的功能，终端上需要包含一些必要的功能模块，主要有身份认证模块（相当于关联模块和判断模块）、系统切换模块（即控制模块），还包括一个存放用户身份的身份认证档案库（即关联模块）。

身份认证模块主要完成以下的功能：一是设置用户的身份认证方式（即预设密钥和身份认证密钥的形式）并与操作系统绑定；二是屏幕解锁时完成用户的身份认证。详细说明如下：

（1）用户设置的身份认证方式可以是多种多样的，比如指纹识别（即指纹密钥）、图案解锁（即图案密钥）以及数字密码（即数字密钥）等等。当用户选定一种认证方式之后，就可以设置每个操作系统的解锁密钥（即预设密钥）。以指纹认证方式为例：系统 1 的解锁指纹（即预设密钥）设为右手拇指，系统 2 的解锁指纹设为右手食指等等。为了后面的说明方便，将这些能够解锁的指纹（图案或者密码）统称为身份认证密钥 K。

在锁屏状态时，每一个操作系统都对应一个预设密钥 K，并且每个系统的 K 都不一样，即系统 i 与 K_i 一一绑定，如图 5 所示。

在解锁状态时，如果要进行系统切换，此时的任何一个预设密钥 $K(K_1, K_2, \dots, K_n)$ 均可以身份认证成功（相当于不需要解锁过程，不需要身份认证过程，仅仅需要操作系统切换过程），即此时对系统 i 进行切换时，其身份认证对应多个密钥 $K(K_1, K_2, \dots, K_n)$ ，如图 6 所示。

（2）进行身份认证时，如果此时屏幕处于锁定状态，用户提供 K_i 进行身份认证成功，那么启用系统切换模块，解锁屏幕，并将当前系统切换到系统 i 中；如果认证失败，屏幕解锁失败，终端保持当前操作系统。

（3）进行身份认证时，如果此时屏幕已经处于解锁状态，用户任意提供存储的合法的 K_i 均可以身份认证成功，并完成系统的切换。

系统切换模块完成操作系统切换的功能，包括屏幕解锁态的切换和屏幕锁屏态的切换。所谓屏幕解锁态的操作系统切换，是指用户已完成了屏幕解锁，正常处于系统 i 中，这时要切换到系统 j 中；所谓屏幕锁屏态的系统切换，是指当前屏幕处于锁定状态，根据用户提供的身份认证密钥，
5 完成身份认证而屏幕解锁，并且直接进入系统 i 中。

身份认证档案库是存储用户身份认证的资料的，在本发明方案中，不仅要存储用于屏幕解锁的预设密钥 K ，同时要存储预设密钥 K_i 所对应的系统 i 。身份认证档案库的实现方式可以多种多样，可以是一个数据库，也可以是一个文件。数据的组织方式也可以多种多样，只要能保证系统 i
10 与 K_i 相关联即可。

本发明的技术方案主要解决多操作系统终端在锁屏状态下快速完成身份认证并切换到指定系统的问题，同时也兼顾了屏幕解锁状态下的系统切换功能。为了实现本发明技术方案，已对终端的核心模块做了说明，包括身份认证模块、系统切换模块以及一个身份认证档案库。

需要说明的是，实现本发明的技术方案，多操作系统终端不仅仅包含上述的几个核心模块，一般终端的基本模块都会包含的。下面结合上述的多操作系统终端，给出本发明的一种实施实例。本实例中，我们将系统切换模块和身份认证档案库放到管理系统中，身份认证模块放到各个系统中，添加核心模块后的多操作系统终端结构如图 7 所示，在图 7 中，双向
15 箭头表示相关模块之间可以相互访问或者调用，单向箭头表示控制关系，即管理系统的系统切换模块可以控制系统 i 和系统 j 的切换。

假设当前用户处于系统 i （当前操作系统）中，需要切换到系统 j （目标操作系统）中，此时屏幕处于锁定状态，用户切换到系统 j 的实施步骤如下：

25 步骤（1-1），用户提供身份识别密钥 K_x （指纹/图案/密码等等），启动用户身份认证模块。

步骤（1-2），从管理系统的身份认证档案库中检索预设密钥库 $K(K_1, K_2, \dots, K_n)$ 。

步骤（1-3），如果 K_x 与预设密钥库 K 中的 K_j 匹配，身份认证成功

功，并启动管理系统的系统切换模块，执行步骤（1-4）；如果 K_x 与预设密钥库 $K(K_1, K_2, \dots, K_n)$ 中的任何一个密钥都不匹配，则执行步骤（1-5）。

5 步骤（1-4），系统切换模块控制系统 i 切换到系统 j ，屏幕解锁，完成操作系统切换。

步骤（1-5），身份认证失败，用户仍处于系统 i 中，屏幕未解锁。

如果用户处于系统 i （当前操作系统）中，并且屏幕已经解锁了，那么要切换到系统 j （目标操作系统）中，需要实施如下步骤：

10 步骤（2-1），用户通过系统 i 提供的系统切换入口，启用身份认证模块。

步骤（2-2），从管理系统的身份认证档案库中检索预设密钥库 $K(K_1, K_2, \dots, K_n)$

15 步骤（2-3），如果用户提供的身份认证密钥 K_x 与预设密钥库 $K(K_1, K_2, \dots, K_n)$ 中的任何一个密钥相匹配，则身份认证成功，并启用管理系统的系统切换模块，执行步骤（2-4）；如果 K_x 与预设密钥库 $K(K_1, K_2, \dots, K_n)$ 中的任何一个密钥都不匹配，则执行步骤（2-5）。

步骤（2-4），系统切换模块控制系统 i 切换到系统 j ，完成操作系统切换。

20 步骤（2-5），身份认证失败，操作系统切换失败，用户仍处于系统 i 中。

25 以上结合附图详细说明了本发明的技术方案，可以解决现有技术中多操作系统终端在锁屏时进行操作系统切换步骤繁琐的问题，可以在终端锁屏状态下，直接完成身份认证和操作系统切换的双重功能，提高了终端操作系统切换的便利性与安全性，同时兼顾了终端处于解锁状态下的操作系统切换功能，从而提升了用户体验。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1. 一种操作系统切换方法，用于终端进行操作系统切换，所述终端上安装有多个操作系统，所述终端运行在当前操作系统，其特征在于，所述
5 切换方法包括：

接收当前用户的身份认证密钥；

在接收到所述身份认证密钥时，判断所述终端是否处于锁屏状态；

在判定所述终端处于锁屏状态时，判断所述身份认证密钥是否与至少一个预设密钥匹配；

10 根据判断结果确定所述终端是否进行操作系统切换。

2. 根据权利要求 1 所述的操作系统切换方法，其特征在于，所述根据判断结果确定所述终端是否进行操作系统切换，具体包括：

在判定所述身份认证密钥与所述至少一个预设密钥匹配时，解锁屏幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标
15 操作系统；以及

在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，保持所述锁屏状态，并控制所述终端运行在所述当前操作系统。

3. 根据权利要求 1 所述的操作系统切换方法，其特征在于，还包括：

在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至
20 少一个预设密钥匹配；以及

在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；

在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制所述终端运行在所述当前操作系统。

25 4. 根据权利要求 1 所述的操作系统切换方法，其特征在于，在所述接收当前用户的身份认证密钥之前，还包括：

建立所述至少一个预设密钥与所述终端中的所述多个操作系统的匹配关系。

5. 根据权利要求 1 至 4 中任一项所述的操作系统切换方法，其特征在于，所述身份认证密钥和所述至少一个预设密钥包括：

指纹密钥、图案密钥和数字密钥。

6. 一种操作系统切换装置，用于终端进行操作系统切换，所述终端上
5 安装有多个操作系统，所述终端运行在当前操作系统，其特征在于，所述切换装置包括：

接收模块，用于接收当前用户的身份认证密钥；

判断模块，用于在接收到所述身份认证密钥时，判断所述终端是否处于
锁屏状态，以及在判定所述终端处于锁屏状态时，判断所述身份认证密钥是
10 否与至少一个预设密钥匹配；

控制模块，用于根据判断结果确定所述终端是否进行操作系统切换。

7. 根据权利要求 6 所述的操作系统切换装置，其特征在于，所述控制模块具体用于：

在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制解锁屏
15 幕，并控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的目标操作系统；以及

在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制保持锁屏状态，并控制所述终端运行在所述当前操作系统。

8. 根据权利要求 6 所述的操作系统切换装置，其特征在于，所述判断模
20 块还用于：

在判定所述终端处于解锁状态时，判断所述身份认证密钥是否与所述至少一个预设密钥匹配；以及

所述控制模块还用于在判定所述身份认证密钥与所述至少一个预设密钥匹配时，控制所述终端从所述当前操作系统切换至与所述身份认证密钥对应的
25 的目标操作系统；以及

在判定所述身份认证密钥与所述至少一个预设密钥不匹配时，控制所述终端运行在所述当前操作系统。

9. 根据权利要求 6 所述的操作系统切换装置，其特征在于，还包括：

关联模块，用于在所述接收当前用户的身份认证密钥之前，建立所述至少一个预设密钥与所述终端中的所述多个操作系统的匹配关系。

10. 根据权利要求 6 至 9 中任一项所述的操作系统切换装置，其特征在于，所述身份认证密钥和所述至少一个预设密钥包括：

5 指纹密钥、图案密钥和数字密钥。

11. 一种终端，其特征在于，包括如权利要求 6 至 10 任一项所述的操作系统切换的装置。

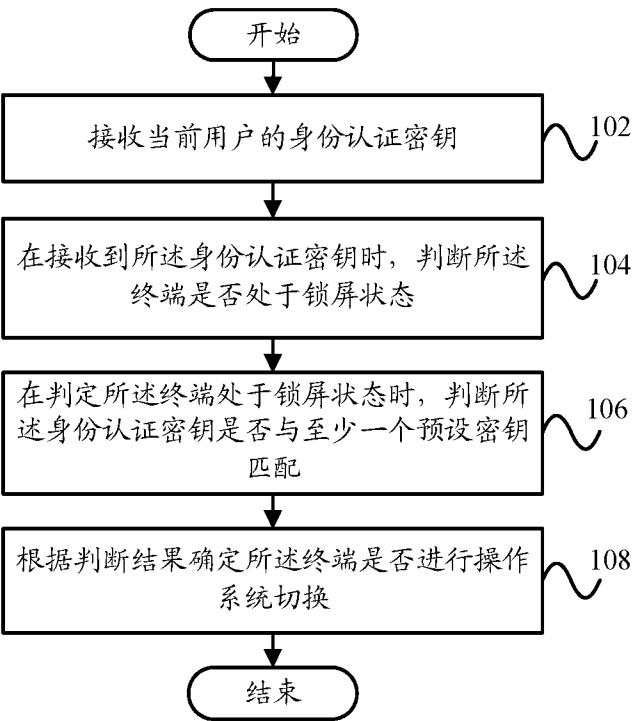


图 1

5



图 2



图 3

10

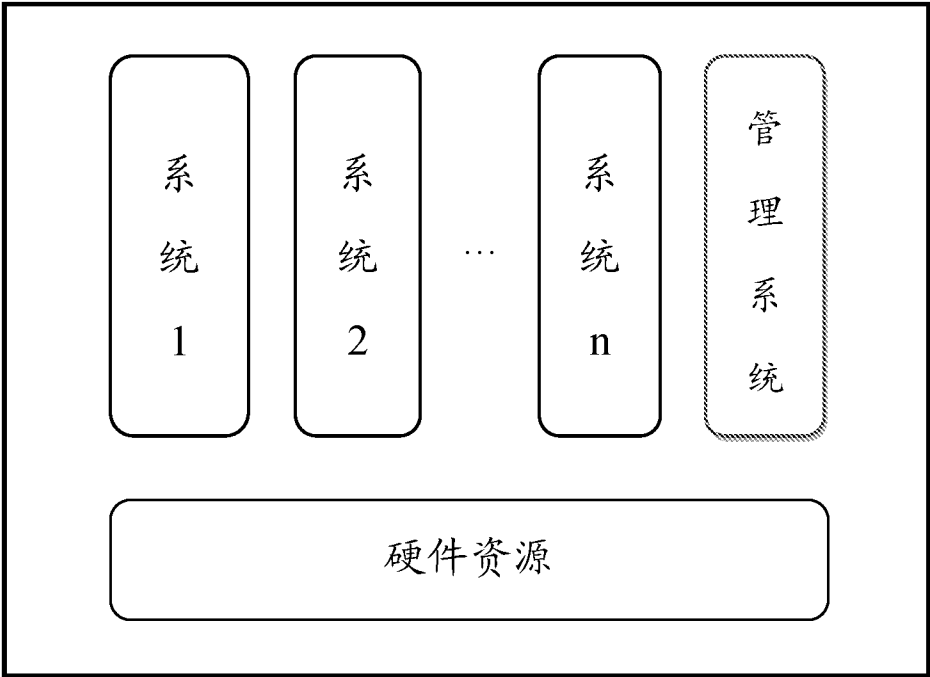


图 4

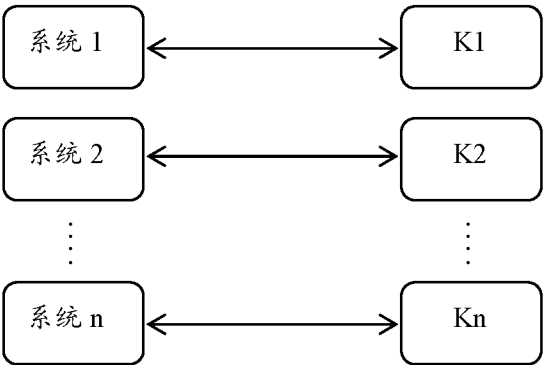


图 5

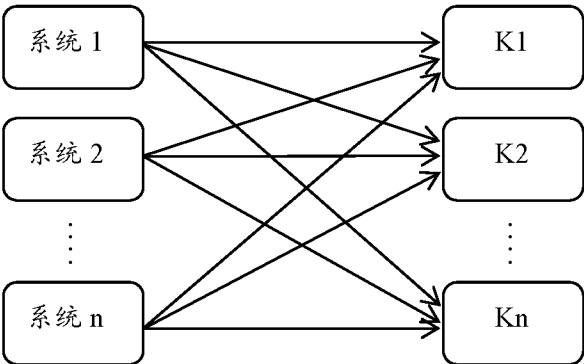


图 6

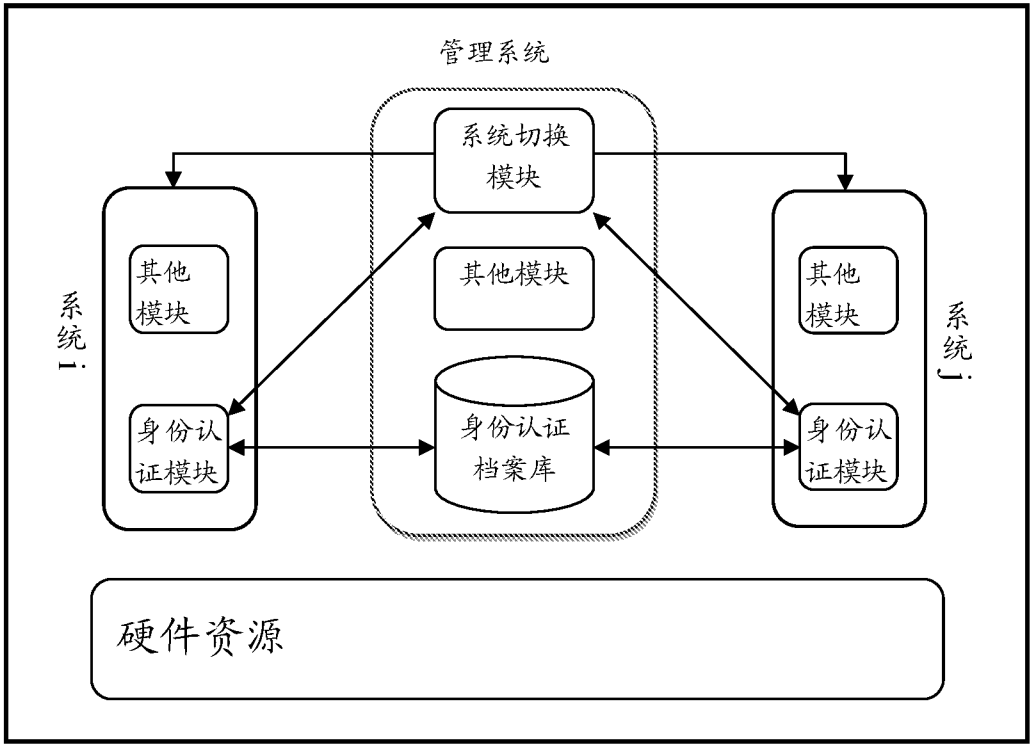


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/091236

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/46 (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

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)

CNPAT, WPI, EPODOC, CNKI, IEEE, GOOGLE: Operating systems, OS, lock, login, interface, switch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104360900 A (SHANGHAI MICROVIRT SOFTWARE TECHNOLOGY CO., LTD.), 18 February 2015 (18.02.2015), description, paragraphs [0094]-[0098]	1-11
A	CN 101615123 A (BYD COMPANY LIMITED), 30 December 2009 (30.12.2009), the whole document	1-11
A	JP 2003345615 A (FUJITSU LIMITED), 05 December 2003 (05.12.2003), the whole document	1-11
A	US 2012297180 A1 (TENG, C.Y. et al.), 22 November 2012 (22.11.2012), the whole 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 23 March 2016 (23.03.2016)	Date of mailing of the international search report 22 April 2016 (22.04.2016)
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 KONG, Xin Telephone No.: (86-10) 62413668

International application No.
PCT/CN2015/091236

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

A. 主题的分类		
G06F 9/46 (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		
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))		
CNPAT, WPI, EPODOC, CNKI, IEEE, GOOGLE: 操作系统, 切换, 锁, 界面, 登陆, Operating systems, OS, lock, login, interface, switch		
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 104360900 A (上海迈微软件科技有限公司) 2015年 2月 18日 (2015 - 02 - 18) 说明书第[0094]-[0098]段	1-11
A	CN 101615123 A (比亚迪股份有限公司) 2009年 12月 30日 (2009 - 12 - 30) 全文	1-11
A	JP 2003345615 A (富士通株式会社) 2003年 12月 5日 (2003 - 12 - 05) 全文	1-11
A	US 2012297180 A1 (TENG, CHIN-YUAN 等) 2012年 11月 22日 (2012 - 11 - 22) 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		国际检索报告邮寄日期
2016年 3月 23日		2016年 4月 22日
ISA/CN的名称和邮寄地址		授权官员
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 传真号 (86-10) 62019451		孔昕
		电话号码 (86-10) 62413668

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/091236

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	104360900	A	2015年 2月 18日	无	
CN	101615123	A	2009年 12月 30日	无	
JP	2003345615	A	2003年 12月 5日	无	
US	2012297180	A1	2012年 11月 22日	TW 201248499 A	2012年 12月 1日