(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 11 月 3 日 (03.11.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/173118 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2015/082980

(22) 国际申请日: 2015 年 6 月 30 日 (30.06.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510219696.1 2015 年 4 月 30 日 (30.04.2015) 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: 张学林 (ZHANG, Xuelin); 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: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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,

[见续页]

(54) Title: SECURE DATA ACCESS CONTROL METHOD AND SYSTEM, AND TERMINAL

(54) 发明名称 : 安全数据的访问控制方法及系统、终端

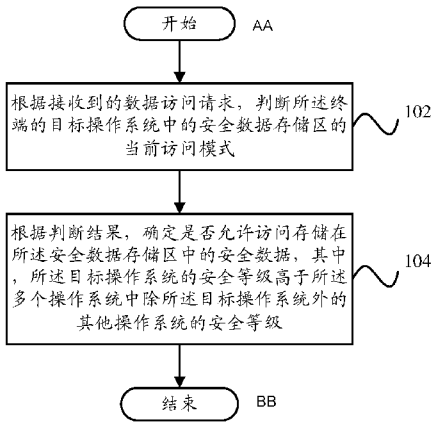

图 1

102 According to a received data access request, judging the current access mode of a secure data storage area in a target operating system of the terminal
104 According to a judgement result, determining whether access is permitted to the secure data stored in the secure data storage area, wherein the security level of the target operating system is higher than the security levels of other operating systems apart from the target operating system in the plurality of operating systems
AA Start
BB End

(57) Abstract: A secure data access control method, a secure data access control system, and a terminal, a plurality of operating systems being installed on the terminal, and the access control method comprising: according to a received data access request, judging the current access mode of a secure data storage area in a target operating system of the terminal (102); and according to a judgement result, determining whether access is permitted to the secure data stored in the secure data storage area, wherein the security level of the target operating system is higher than the security levels of other operating systems apart from the target operating system in the plurality of operating systems (104). The technical solution can be more adapted to the actual requirements of a user. Secure data of a secure operating system is effectively protected from being stolen, and the loss of privacy data is prevented, so that the privacy security of the user is further improved.

(57) 摘要: 一种安全数据的访问控制方法、一种安全数据的访问控制系统和一种终端，所述终端上安装有多个操作系统，所述访问控制方法包括：根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式(102)；根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级（104）。通过该技术方案，可以更加适应用户的实际需求，有效地保护了安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

WO 2016/173118 A1

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))。

安全数据的访问控制方法及系统、终端

本申请要求于 2015 年 4 月 30 日提交中国专利局，申请号为 201510219696.1、发明名称为“安全数据的访问控制方法及系统、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

本发明涉及终端技术领域，具体而言，涉及一种安全数据的访问控制方法、一种安全数据的访问控制系统和一种终端。

背景技术

目前，现有安全操作系统隐私数据的保护方法主要有如下方案：

方案一、备份保护。通过云端数据备份，若安全操作系统出现数据丢失、破坏等情况，可快速通过云端备份恢复安全操作系统中的隐私数据，达到对安全操作系统隐私数据的保护。

方案二、数据伪装保护。其他非安全操作系统访问安全操作系统中隐私数据时，将安全操作系统中的数据通过伪装处理后显示，从而保护了安全操作系统隐私数据不被窃取。

方案三、屏蔽安全操作系统硬件达到隐私数据的保护。已有人提出一种双系统数据的保护方法的申请，具体是通过云端指令快速屏蔽安全操作系统中的部分硬件，让用户无法窃取安全操作系统中的私密数据；另外，可以通过修改指令参数，让安全操作系统的硬件有效，从而保护双系统中安全操作系统的数据安全。

现有技术方案的缺陷描述如下：

方案一、备份保护方案虽然可以通过数据备份防止数据丢失、破坏，但仍存在隐私数据泄露的危险，这种云端数据泄露案例已有很多，如小米账号的泄露、CSDN（Chinese Software Develop Net，中国软件开发联盟）账号的泄露等。一旦发生隐私数据泄漏，将会存在很大的安全隐患。

方案二、数据伪装保护，这种方案是为了防止非安全操作系统访问、窃取安装系统隐私数据。但还是不能彻底的保护隐私数据的丢失，例如手机丢失、被窃，别人如果能进入安全操作系统，那么安全操作系统中的隐私数据仍然存在泄露的风险。

方案三、硬件屏蔽保护，这种方案可以有效的保护隐私数据被窃取，但在安全操作系统出现故障，无法进入安全操作系统，可会出现安全操作系统隐私数据无法获取的窘况，如果急需安全操作系统中的重要隐私数据，将会非常麻烦。

因此，如何进一步提升安全操作系统的隐私数据的安全，成为亟待解决的技术问题。

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，可以更加适应用户的实际需求，有效地保护了安全系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

有鉴于此，本发明的一方面提出了一种安全数据的访问控制方法，用于终端，所述终端上安装有多个操作系统，所述访问控制方法包括：根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式；根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

在该技术方案中，可以为目标操作系统（即安全操作系统）的安全数据存储区设置访问模式，其中，不同的访问模式可以对应不同的访问权限，例如，可以为安全操作系统的安全数据存储区设定访问安全标识锁，然后通过安全标识锁在不同场景控制对安全数据存储区的访问保护，其中，安全标识锁的不同锁状态对应于安全数据存储区的不同访问模式。通过这种方法可以彻底防止因数据备份而导致的数据泄露，同时，如果手机被窃，同样可以通过远程发送指令触发访问模式的转变，防止别人进入安全操作系统获取隐私数据，另外，若安全操作系统出现故障，也可以根据事先设定的触发机制，触发访问模式的转变。因此，当安全数据存储区接收到数据访问请求时，终端就可以根据当前的访问模式确定是否运行其被访问，从而可以更加适应用户的实际需求，有效地保护了终端的安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐

私安全。

在上述技术方案中，优选地，当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统，并在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

在该技术方案中，可以为安全数据存储区设置安全访问模式，在安全访问模式下，只有目标操作系统可以正常访问安全数据存储区的数据，禁止终端中的其他系统访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

在该技术方案中，还可以为安全数据存储区设置共享访问模式和屏蔽访问模式，在共享访问模式下，每个系统都可以正常访问安全数据存储区的数据，在屏蔽访问模式下，禁止所有系统正常访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式；以及在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

在该技术方案中，当访问安全数据的请求被禁止时，可以提示用户是否重置访问模式，并可以根据用户的设置重置访问模式，从而使访问模式的设置和转变更具灵活性，提升了用户体验。

在上述技术方案中，优选地，根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，还包括：预设所述安全数据存储区的所述当前访问模式。

在该技术方案中，可以根据实际需求或用户指令预设访问模式，其中，访问模式的设置不能简单地通过手机中的设置进行转变，而是需要通过专

有指令来转变的。具体地，变更访问模式的指令可以是如下形式:

command : =op state state

op : =change | other

state : =safe | share | unsafe

其中，op state state 中，op 是变更操作，前一个 state 代表原访问模式，后一个 state 代表新访问模式，op 和 state 分别可以由 2、3bit（字节）二进制表示，比如 000 表示 unsafe，unsafe 代表屏蔽访问模式。目前的 op 和 state 还不多，后边如有扩展，可以增加二进制 bit 位数进行实现。

本发明的另一方面提出了一种安全数据的访问控制系统，用于终端，所述终端上安装有多个操作系统，所述访问控制系统包括：判断模块，用于根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式；控制模块，用于根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

在该技术方案中，可以为目标操作系统（即安全操作系统）的安全数据存储区设置访问模式，其中，不同的访问模式可以对应不同的访问权限，例如，可以为安全操作系统的安全数据存储区设定访问安全标识锁，然后通过安全标识锁在不同场景控制对安全数据存储区的访问保护，其中，安全标识锁的不同锁状态对应于安全数据存储区的不同访问模式。通过这种方法可以彻底防止因数据备份而导致的数据泄露，同时，如果手机被窃，同样可以通过远程发送指令触发访问模式的转变，防止别人进入安全操作系统获取隐私数据，另外，若安全操作系统出现故障，也可以根据事先设定的触发机制，触发访问模式的转变。因此，当安全数据存储区接收到数据访问请求时，终端就可以根据当前的访问模式确定是否运行其被访问，从而可以更加适应用户的实际需求，有效地保护了终端的安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

在上述技术方案中，优选地，所述判断模块还用于：当判定所述安全

数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统；以及所述控制模块具体用于：在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

在该技术方案中，可以为安全数据存储区设置安全访问模式，在安全访问模式下，只有目标操作系统可以正常访问安全数据存储区的数据，禁止终端中的其他系统访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，所述控制模块具体还用于：当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

在该技术方案中，还可以为安全数据存储区设置共享访问模式和屏蔽访问模式，在共享访问模式下，每个系统都可以正常访问安全数据存储区的数据，在屏蔽访问模式下，禁止所有系统正常访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，所述判断模块还用于：当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式；以及还包括：重置模块，用于在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

在该技术方案中，当访问安全数据的请求被禁止时，可以提示用户是否重置访问模式，并可以根据用户的设置重置访问模式，从而使访问模式的设置和转变更具灵活性，提升了用户体验。

在上述技术方案中，优选地，还包括：设置模块，用于根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，预设所述安全数据存储区的所述当前访问模式。

在该技术方案中，可以根据实际需求或用户指令预设访问模式，其中，

访问模式的设置不能简单地通过手机中的设置进行转变，而是需要通过专有指令来转变的。具体地，变更访问模式的指令可以是如下形式:

command : =op state state

op : =change | other

state : =safe | share | unsafe

其中，op state state 中，op 是变更操作，前一个 state 代表原访问模式，后一个 state 代表新访问模式，op 和 state 分别可以由 2、3bit（字节）二进制表示，比如 000 表示 unsafe，unsafe 代表屏蔽访问模式。目前的 op 和 state 还不多，后边如有扩展，可以增加二进制 bit 位数进行实现。

本发明的再一方面提出了一种终端，所述终端上安装有多个操作系统，所述终端包括处理器和存储器，其中，所述存储器中存储一组程序代码，且所述处理器用于调用所述存储器中存储的程序代码，用于执行以下操作:

根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式;

根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

在该技术方案中，可选地，所述处理器执行:

当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统，并在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

在该技术方案中，可选地，所述处理器执行:

当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者

当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

在该技术方案中，可选地，所述处理器执行:

当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式；以及

在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

在该技术方案中，可选地，所述处理器根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，还执行：

预设所述安全数据存储区的所述当前访问模式。

通过以上技术方案，可以更加适应用户的实际需求，有效地保护了安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

附图说明

图 1 示出了根据本发明的一个实施例的安全数据的访问控制方法的流程示意图；

图 2 示出了根据本发明的一个实施例的安全数据的访问控制系统的结构示意图；

图 3 示出了根据本发明的一个实施例的终端的结构示意图；

图 4 示出了根据本发明的一个实施例的安全数据存储区的访问模式转换示意图；

图 5 示出了根据本发明的另一个实施例的安全数据的访问控制方法的流程示意图；

图 6 示出了根据本发明的另一个实施例的终端的结构示意图。

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安全数据的访问控制方法的流程

示意图。

如图 1 所示，根据本发明的一个实施例的安全数据的访问控制方法，用于终端，终端上安装有多个操作系统，包括:

步骤 102，根据接收到的数据访问请求，判断终端的目标操作系统中的安全数据存储区的当前访问模式。

步骤 104，根据判断结果，确定是否允许访问存储在安全数据存储区中的安全数据，其中，目标操作系统的安全等级高于多个操作系统中除目标操作系统外的其他操作系统的安全等级。

在该技术方案中，可以为目标操作系统（即安全操作系统）的安全数据存储区设置访问模式，其中，不同的访问模式可以对应不同的访问权限，例如，可以为安全操作系统的安全数据存储区设定访问安全标识锁，然后通过安全标识锁在不同场景控制对安全数据存储区的访问保护，其中，安全标识锁的不同锁状态对应于安全数据存储区的不同访问模式。通过这种方法可以彻底防止因数据备份而导致的数据泄露，同时，如果手机被窃，同样可以通过远程发送指令触发访问模式的转变，防止别人进入安全操作系统获取隐私数据，另外，若安全操作系统出现故障，也可以根据事先设定的触发机制，触发访问模式的转变。因此，当安全数据存储区接收到数据访问请求时，终端就可以根据当前的访问模式确定是否运行其被访问，从而可以更加适应用户的实际需求，有效地保护了终端的安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

在上述技术方案中，优选地，当判定安全数据存储区的当前访问模式为安全访问模式时，判断数据访问请求是否来自目标操作系统，并在判定当前访问模式为安全访问模式时，允许访问安全数据，否则禁止访问安全数据。

在该技术方案中，可以为安全数据存储区设置安全访问模式，在安全访问模式下，只有目标操作系统可以正常访问安全数据存储区的数据，禁止终端中的其他系统访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，当判定安全数据存储区的当前访问模式为共享访问模式时，允许访问安全数据；或者当判定安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问安全数据。

在该技术方案中，还可以为安全数据存储区设置共享访问模式和屏蔽访问模式，在共享访问模式下，每个系统都可以正常访问安全数据存储区的数据，在屏蔽访问模式下，禁止所有系统正常访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，当禁止访问安全数据时，判断是否重新设定目标操作系统中的安全数据存储区的访问模式；以及在判定重新设定安全数据存储区的访问模式时，根据接收到的重置指令，重新设定目标操作系统中的安全数据存储区的访问模式。

在该技术方案中，当访问安全数据的请求被禁止时，可以提示用户是否重置访问模式，并可以根据用户的设置重置访问模式，从而使访问模式的设置和转变更具灵活性，提升了用户体验。

在上述技术方案中，优选地，在步骤 102 之前，还包括：预设安全数据存储区的当前访问模式。

在该技术方案中，可以根据实际需求或用户指令预设访问模式，其中，访问模式的设置不能简单地通过手机中的设置进行转变，而是需要通过专有指令来转变的。具体地，变更访问模式的指令可以是如下形式：

command : =op state state

op : =change | other

state : =safe | share | unsafe

其中，op state state 中，op 是变更操作，前一个 state 代表原访问模式，后一个 state 代表新访问模式，op 和 state 分别可以由 2、3bit（字节）二进制表示，比如 000 表示 unsafe，unsafe 代表屏蔽访问模式。目前的 op 和 state 还不多，后边如有扩展，可以增加二进制 bit 位数进行实现。

图 2 示出了根据本发明的一个实施例的安全数据的访问控制系统的结构示意图。

如图 2 所示，根据本发明的一个实施例的安全数据的访问控制系统 200，用于终端，终端上安装有多个操作系统，包括：判断模块 202，用于根据接收到的数据访问请求，判断终端的目标操作系统中的安全数据存储区的当前访问模式；控制模块 204，用于根据判断结果，确定是否允许访问存储在安全数据

存储区中的安全数据，其中，目标操作系统的安全等级高于多个操作系统中除目标操作系统外的其他操作系统的安全等级。

在该技术方案中，可以为目标操作系统（即安全操作系统）的安全数据存储区设置访问模式，其中，不同的访问模式可以对应不同的访问权限，例如，可以为安全操作系统的安全数据存储区设定访问安全标识锁，然后通过安全标识锁在不同场景控制对安全数据存储区的访问保护，其中，安全标识锁的不同锁状态对应于安全数据存储区的不同访问模式。通过这种方法可以彻底防止因数据备份而导致的数据泄露，同时，如果手机被窃，同样可以通过远程发送指令触发访问模式的转变，防止别人进入安全操作系统获取隐私数据，另外，若安全操作系统出现故障，也可以根据事先设定的触发机制，触发访问模式的转变。因此，当安全数据存储区接收到数据访问请求时，终端就可以根据当前的访问模式确定是否运行其被访问，从而可以更加适应用户的实际需求，有效地保护了终端的安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

在上述技术方案中，优选地，判断模块 202 还用于：当判定安全数据存储区的当前访问模式为安全访问模式时，判断数据访问请求是否来自目标操作系统；以及控制模块 204 具体用于：在判定当前访问模式为安全访问模式时，允许访问安全数据，否则禁止访问安全数据。

在该技术方案中，可以为安全数据存储区设置安全访问模式，在安全访问模式下，只有目标操作系统可以正常访问安全数据存储区的数据，禁止终端中的其他系统访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，控制模块 204 具体还用于：当判定安全数据存储区的当前访问模式为共享访问模式时，允许访问安全数据；或者当判定安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问安全数据。

在该技术方案中，还可以为安全数据存储区设置共享访问模式和屏蔽访问模式，在共享访问模式下，每个系统都可以正常访问安全数据存储区的数据，在屏蔽访问模式下，禁止所有系统正常访问安全数据存储区的数据，从而有效地保护了终端的安全操作系统的安全数据不被窃取，进一步提升了用户的隐私安全。

在上述技术方案中，优选地，判断模块 202 还用于：当禁止访问安全数据时，判断是否重新设定目标操作系统中的安全数据存储区的访问模式；以及还包括：重置模块 206，用于在判定重新设定安全数据存储区的访问模式时，根据接收到的重置指令，重新设定目标操作系统中的安全数据存储区的访问模式。

在该技术方案中，当访问安全数据的请求被禁止时，可以提示用户是否重置访问模式，并可以根据用户的设置重置访问模式，从而使访问模式的设置和转变更具灵活性，提升了用户体验。

在上述技术方案中，优选地，还包括：设置模块 208，用于根据接收到的数据访问请求，判断安全数据存储区的当前访问模式之前，预设安全数据存储区的当前访问模式。

在该技术方案中，可以根据实际需求或用户指令预设访问模式，其中，访问模式的设置不能简单地通过手机中的设置进行转变，而是需要通过专有指令来转变的。具体地，变更访问模式的指令可以是如下形式：

command : =op state state

op : =change | other

state : =safe | share | unsafe

其中，op state state 中，op 是变更操作，前一个 state 代表原访问模式，后一个 state 代表新访问模式，op 和 state 分别可以由 2、3bit（字节）二进制表示，比如 000 表示 unsafe，unsafe 代表屏蔽访问模式。目前的 op 和 state 还不多，后边如有扩展，可以增加二进制 bit 位数进行实现。

图 3 示出了根据本发明的一个实施例的终端的结构示意图。

如图 3 所示，根据本发明的一个实施例的终端 300，包括安全数据的访问控制系统 200，因此，终端 300 具有和上述技术方案中任一项所述的安全数据的访问控制系统 200 相同的技术效果，在此不再赘述。

图 4 示出了根据本发明的一个实施例的安全数据存储区的访问模式转换示意图。

如图 4 所示，可以为安全系统（目标操作系统）的安全数据存储区设定访问安全标识锁，然后通过安全标识锁在不同场景控制对安全数据存储区的访问保护，其中，安全标识锁的不同锁状态对应于安全数据存储区的不同访问模式。

安全标识锁可以有 Safe、Unsafe、Share 三种锁状态。其中，处于 Safe 锁状态时，只有安全系统可以正常访问数据存储区的数据，处于 Unsafe 锁状态时，无论是安全系统还是非安全系统都不可以访问数据存储区的数据，而处于 Share 锁状态时，安全系统和非安全系统都可以访问数据存储区的数据。

通过设置不同的触发事件，还可以控制安全锁状态间的互相转变。通过这种方法可以彻底防止因数据备份而导致的数据泄露，同时，如果手机被窃，同样可以通过远程发送指令触发安全锁状态向 Unsafe 转变，防止别人进入安全系统获取隐私数据，另外，若安全系统出现故障，根据事先设定的触发机制，触发安全锁状态向 Share 转变。并且，用户不能简单地通过手机中的设置转变安全锁状态，而是需要通过专有指令来转变安全锁状态，具体地，变更访问模式的指令可以是如下形式:

command : =op state state

op : =change | other

state : =safe | share | unsafe

其中，op state state 中，op 是变更操作，前一个 state 代表原访问模式，后一个 state 代表新访问模式，op 和 state 分别可以由 2、3bit（字节）二进制表示，比如 000 表示 unsafe，unsafe 代表屏蔽访问模式。目前的 op 和 state 还不多，后边如有扩展，可以增加二进制 bit 位数进行实现。

通过该技术方案，可以更加适应用户的实际需求，有效地保护了安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

图 5 示出了根据本发明的另一个实施例的安全数据的访问控制方法的流程示意图。

如图 5 所示，根据本发明的另一个实施例的安全数据的访问控制方法，包括:

步骤 502，设置安全系统（目标操作系统）数据存储区的访问锁状态（即预设安全数据存储区的当前访问模式）；

步骤 504，根据接收到的对安全系统数据的访问请求，判断安全系统数据存储区的当前访问锁状态（当前访问模式），若为 Safe 状态（安全访问模式），则执行步骤 506，若为 Share 状态（共享访问模式），则执行步骤 508，若为

Unsafe 状态（屏蔽访问模式），则执行步骤 510;

步骤 506，判断当前所处系统是否为安全系统（即判断发出访问请求的系统是否为安全系统），若是安全系统，则执行步骤 508，否则执行步骤 510;

步骤 508，正常访问安全系统数据;

步骤 510，当无法访问安全系统数据时，判断是否重新设置安全系统数据存储区的访问锁状态，若是，则执行步骤 512，否则，结束进程;

步骤 512，发送指令设置安全系统数据存储区的访问锁状态，在设置完成后，返回步骤 504，继续根据判断安全系统数据存储区的当前访问锁状态。

图 6 示出了根据本发明的另一个实施例的终端的结构示意图，如图 6 所示，该终端 6 可以包括：至少一个处理器 61，例如 CPU，至少一个通信总线 62 以及存储器 63；通信总线 62 用于实现这些组件之间的连接通信；存储器 63 可以是高速 RAM 存储器，也可以是非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。存储器 63 中存储一组程序代码，且处理器 61 用于调用存储器 63 中存储的程序代码，用于执行以下操作：

根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式;

根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

可选地，所述处理器 61 执行:

当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统，并在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

可选地，所述处理器 61 执行:

当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者

当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

可选地，所述处理器 61 执行:

当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所

述安全数据存储区的访问模式；以及

在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

可选地，所述处理器 61 根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，还执行：

预设所述安全数据存储区的所述当前访问模式。

通过该技术方案，可以更加适应用户的实际需求，有效地保护了安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

以上结合附图详细说明了本发明的技术方案，通过以上技术方案，可以更加适应用户的实际需求，有效地保护了安全操作系统的安全数据不被窃取，防止了隐私数据的丢失，从而进一步提升了用户的隐私安全。

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

1. 一种安全数据的访问控制方法，用于终端，其特征在于，所述终端上安装有多个操作系统，目标操作系统所述访问控制方法包括:

根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式;

根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

2. 根据权利要求 1 所述的安全数据的访问控制方法，其特征在于，

当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统，并在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

3. 根据权利要求 1 所述的安全数据的访问控制方法，其特征在于，

当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者

当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

4. 根据权利要求 2 或 3 所述的安全数据的访问控制方法，其特征在于，当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式；以及

在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

5. 根据权利要求 1 至 3 中任一项所述的安全数据的访问控制方法，其特征在于，根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，还包括:

预设所述安全数据存储区的所述当前访问模式。

6. 一种安全数据的访问控制系统，用于终端，其特征在于，所述终端上安装有多个操作系统，所述访问控制系统包括:

判断模块，用于根据接收到的数据访问请求，判断所述终端的目标操作系

统中的安全数据存储区的当前访问模式;

控制模块，用于根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

7. 根据权利要求 6 所述的安全数据的访问控制系统，其特征在于，所述判断模块还用于: 当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统; 以及

所述控制模块具体用于: 在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

8. 根据权利要求 6 所述的安全数据的访问控制系统，其特征在于，所述控制模块具体还用于:

当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据; 或者

当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

9. 根据权利要求 7 或 8 所述的安全数据的访问控制系统，其特征在于，所述判断模块还用于: 当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式; 以及还包括:

重置模块，用于在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

10. 根据权利要求 6 至 8 中任一项所述的安全数据的访问控制系统，其特征在于，还包括:

设置模块，用于根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，预设所述安全数据存储区的所述当前访问模式。

11. 一种终端，其特征在于，所述终端上安装有多个操作系统，所述终端包括处理器和存储器，其中，所述存储器中存储一组程序代码，且所述处理器用于调用所述存储器中存储的程序代码，用于执行以下操作:

根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式;

根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级。

12、根据权利要求 11 所述的终端，其特征在于，所述处理器执行:

当判定所述安全数据存储区的当前访问模式为安全访问模式时，判断所述数据访问请求是否来自所述目标操作系统，并在判定所述当前访问模式为所述安全访问模式时，允许访问所述安全数据，否则禁止访问所述安全数据。

13、根据权利要求 11 所述的终端，其特征在于，所述处理器执行:

当判定所述安全数据存储区的当前访问模式为共享访问模式时，允许访问所述安全数据；或者

当判定所述安全数据存储区的当前访问模式为屏蔽访问模式时，禁止访问所述安全数据。

14、根据权利要求 12 或 13 所述的终端，其特征在于，所述处理器执行:

当禁止访问所述安全数据时，判断是否重新设定所述目标操作系统中的所述安全数据存储区的访问模式；以及

在判定重新设定所述安全数据存储区的访问模式时，根据接收到的重置指令，重新设定所述目标操作系统中的所述安全数据存储区的访问模式。

15、根据权利要求 11 至 13 中任一项所述的终端，其特征在于，所述处理器根据接收到的所述数据访问请求，判断所述安全数据存储区的所述当前访问模式之前，还执行:

预设所述安全数据存储区的所述当前访问模式。

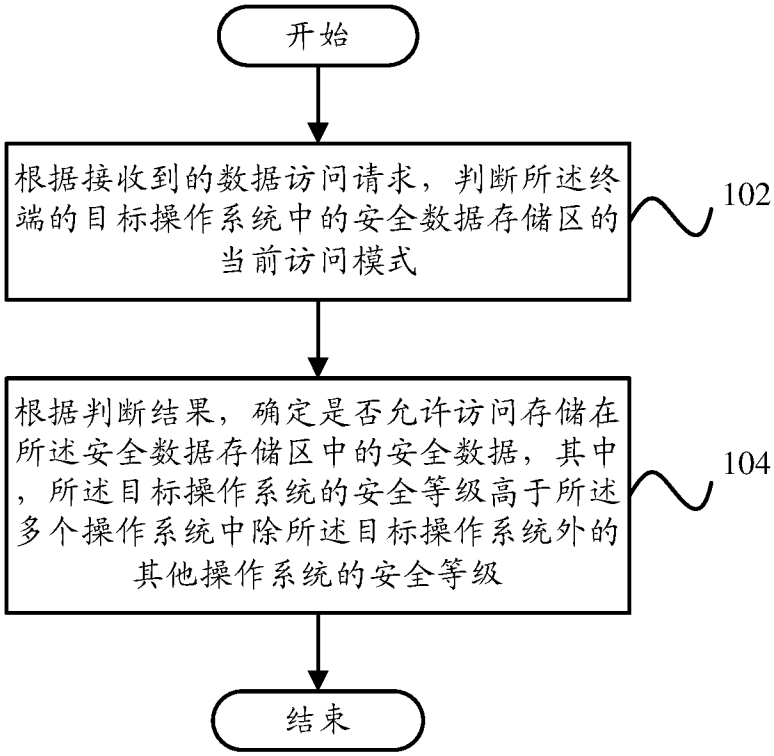
开始
根据接收到的数据访问请求，判断所述终端的目标操作系统中的安全数据存储区的当前访问模式
102
根据判断结果，确定是否允许访问存储在所述安全数据存储区中的安全数据，其中，所述目标操作系统的安全等级高于所述多个操作系统中除所述目标操作系统外的其他操作系统的安全等级
104
结束

图 1


判断模块202
控制模块204
重置模块206
设置模块208
安全数据的访问控制系统200

图 2


安全数据的访问控制系统200
终端300

图 3

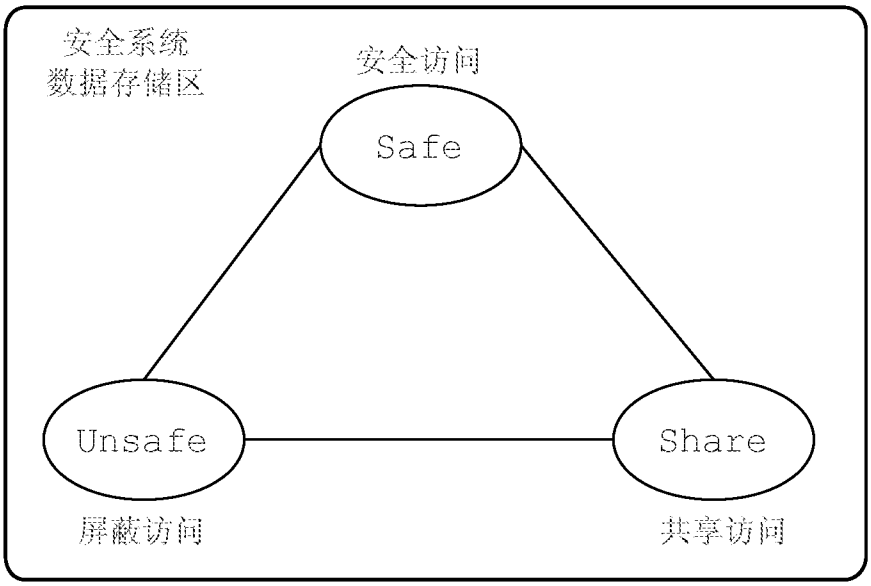

图 4

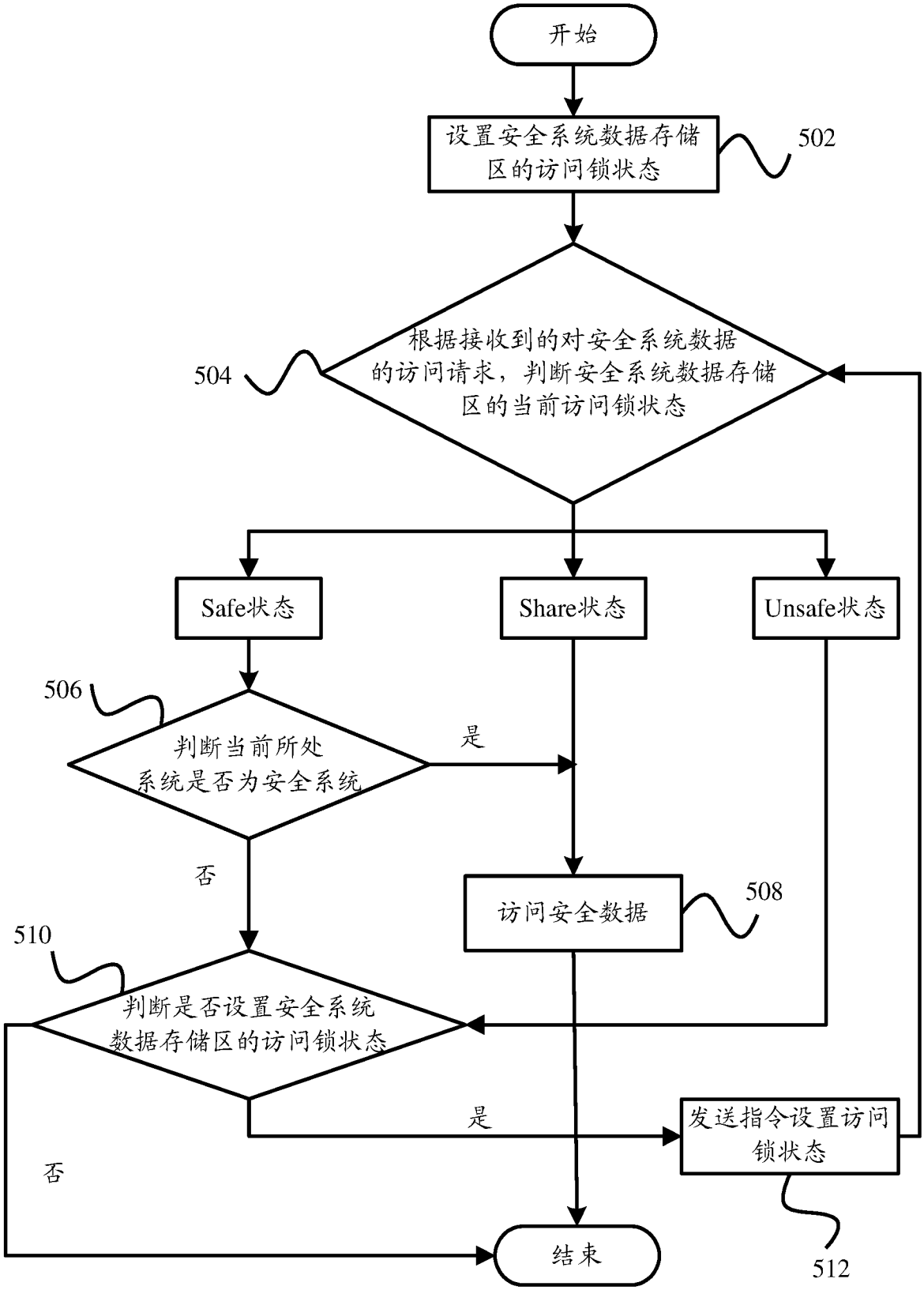
开始
设置安全系统数据存储区的访问锁状态
502
根据接收到的对安全系统数据的访问请求，判断安全系统数据存储区的当前访问锁状态
504
Safe状态
Share状态
Unsafe状态
506
判断当前所处系统是否为安全系统
是
否
访问安全数据
508
510
判断是否设置安全系统数据存储区的访问锁状态
是
否
发送指令设置访问锁状态
512
结束

图 5

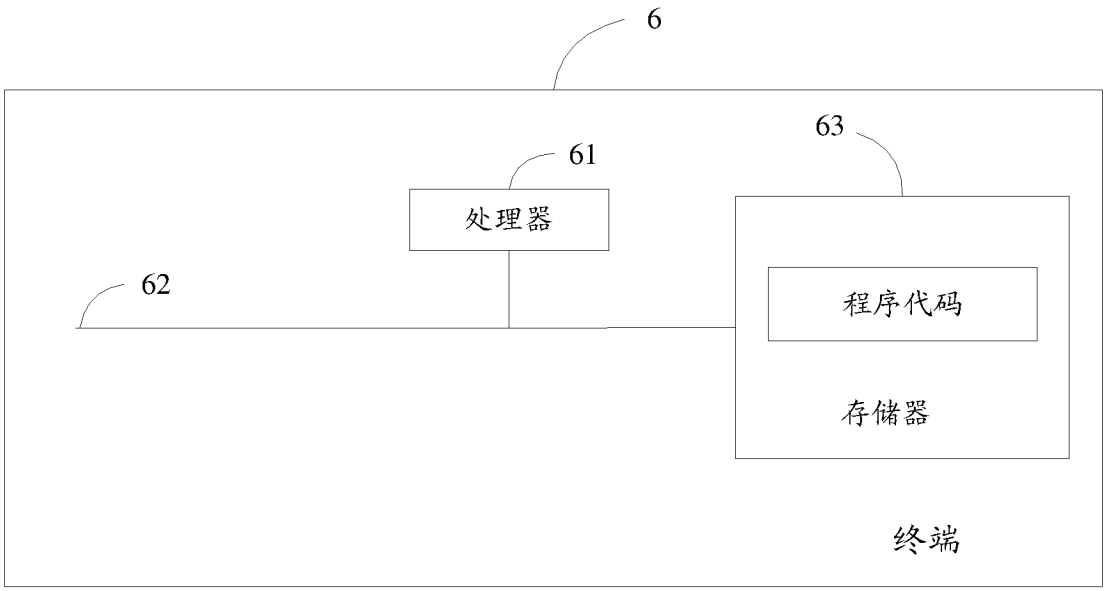

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/082980

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60 (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, H04W, H04L

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: authority, degree, security, secure, data, OS, operating system, multi-, grade, level, mode, call, access, read, storage, store, share, shield, block, forbid, prevent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104184738 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 03 December 2014 (03.12.2014), description, paragraphs 33-49	1-2, 5-7, 10-12, 15
Y	CN 104115152 A (SAMSUNG ELECTRONICS CO., LTD.), 22 October 2014 (22.10.2014), description, paragraphs 34-54	1-2, 5-7, 10-12, 15
A	CN 103369524 A (DONGGUAN YULONG COMMUNICATION TECHNOLOGY CO., LTD. et al.), 23 October 2013 (23.10.2013), the whole document	1-15
A	CN 104202343 A (KUPAI SOFTWARE TECHNOLOGY (SHENZHEN) CO., LTD.), 10 December 2014 (10.12.2014), the whole document	1-15
A	US 2009172411 A1 (ARM LIMITED), 02 July 2009 (02.07.2009), the whole document	1-15

☐ 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
25 December 2015 (25.12.2015)	**27 January 2016 (27.01.2016)**
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 **YANG, Qingli** Telephone No.: (86-10) **61648127**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/082980

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104184738 A	03 December 2014	None	
CN 104115152 A	22 October 2014	US 2013219507 A1	22 August 2013
		TW 201349008 A	01 December 2013
		WO 2013122443 A1	22 August 2013
		KR 20130101628 A	16 September 2013
		EP 2815347 A1	24 December 2014
CN 103369524 A	23 October 2013	WO 2015014017 A1	05 February 2015
CN 104202343 A	10 December 2014	None	
US 2009172411 A1	02 July 2009	CN 101477612 A	08 July 2009
		GB 2458182 A	09 September 2009
		JP 2009163741 A	23 July 2009

国际检索报告

国际申请号 PCT/CN2015/082980

A. 主题的分类

G06F 21/60(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,H04W,H04L

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,EPODOC,CNPAT,CNKI：安全，数据，操作系统，多，等级，级别，权限，模式，访问，度，存储，共享，屏蔽，禁止，阻止，security, secure, data, OS, operating system, multi-, grade, level, mode, call, access, read, storage, store, share, shield, block, forbid, prevent

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
Y	CN 104184738 A (宇龙计算机通信科技深圳有限公司) 2014年 12月 3日 (2014-12-03) 说明书第33-49段	1-2、5-7、10-12、15
Y	CN 104115152 A (三星电子株式会社) 2014年 10月 22日 (2014-10-22) 说明书第34-54段	1-2、5-7、10-12、15
A	CN 103369524 A (东莞宇龙通信科技有限公司等) 2013年 10月 23日 (2013-10-23) 全文	1-15
A	CN 104202343 A (酷派软件技术深圳有限公司) 2014年 12月 10日 (2014-12-10) 全文	1-15
A	US 2009172411 A1 (ARM LIMITED) 2009年 7月 2日 (2009-07-02) 全文	1-15

☐ 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
2015年 12月 25日	2016年 1月 27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	杨庆丽
传真号 (86-10)62019451	电话号码 (86-10)61648127

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/082980

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	104184738	A	2014年 12月 3日		无		
CN	104115152	A	2014年 10月 22日	US	2013219507	A1	2013年 8月 22日
				TW	201349008	A	2013年 12月 1日
				WO	2013122443	A1	2013年 8月 22日
				KR	20130101628	A	2013年 9月 16日
				EP	2815347	A1	2014年 12月 24日
CN	103369524	A	2013年 10月 23日	WO	2015014017	A1	2015年 2月 5日
CN	104202343	A	2014年 12月 10日		无		
US	2009172411	A1	2009年 7月 2日	CN	101477612	A	2009年 7月 8日
				GB	2458182	A	2009年 9月 9日
				JP	2009163741	A	2009年 7月 23日