(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 11 月 30 日 (30.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/201692 A1

(51) 国际专利分类号:
G06F 21/31 (2013.01)

(21) 国际申请号: PCT/CN2016/083335

(22) 国际申请日: 2016 年 5 月 25 日 (25.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 北京小米移动软件有限公司(BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) [CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 9 层 01 房间, Beijing 100085 (CN)。

(72) 发明人: 伍亮雄(WU, Liangxiong); 中国北京市海淀区清河中街68号华润五彩城购物中心二期9层01房间, Beijing 100085 (CN)。 刘海涛(LIU, Haitao); 中国北京市海淀区清河中街68号华润五彩城购物中心二期9层01房间, Beijing 100085 (CN)。 王广健(WANG, Guangjian); 中国北京市海淀区清河中街68号华润五彩城购物中心二期9层01房间, Beijing 100085 (CN)。

(74) 代理人: 北京三高永信知识产权代理有限责任公司(BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市海淀区学院路蓟门里和景园A座1单元102室, Beijing 100088 (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,

(54) **Title:** APPLICATION ENCRYPTION METHOD AND DEVICE

(54) **发明名称**: 应用加密方法及装置

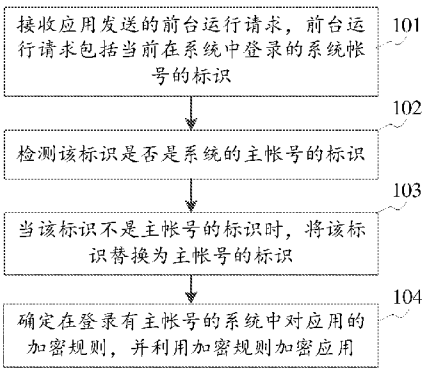

图 1

101 Receive a foreground operation request sent by an application, the foreground operation request comprising an identifier of a system account currently logged in a system
102 Detect whether the identifier is an identifier of a primary account of the system
103 If the identifier is not the identifier of the primary account, replace the identifier with the identifier of the primary account
104 Determine an encryption rule for the application in the system in which the primary account is logged, and encrypt the application by using the encryption rule

(57) **Abstract:** An application encryption method and device, relating to the technical field of computers. The method comprises: receiving a foreground operation request sent by an application, the foreground operation request comprising an identifier of a system account currently logged in a system (101); detecting whether the identifier is an identifier of a primary account of the system (102); if the identifier is not the identifier of the primary account, replacing the identifier with the identifier of the primary account (103); and determining an encryption rule for the application in the system in which the primary account is logged, and encrypting the application by using the encryption rule (104). The invention enables an application lock in a terminal to encrypt an application operating in a system in which a non-primary account is logged, and resolves the problem of a small application range of the application lock due to the fact that the application lock can only encrypt the application operating in the system in which the primary account is logged, thereby enlarging the application range of the application lock.

(57) **摘要**: 一种应用加密方法及装置，属于计算机技术领域。所述方法包括：接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识(101)；检测该标识是否是系统的主帐号的标识(102)；当该标识不是主帐号的标识时，将该标识替换为主帐号的标识(103)；确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用(104)，使得终端中的应用锁可以对运行在登录有非主帐号的系统中的应用进行加密，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

WO 2017/201692 A1

[见续页]

GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

应用加密方法及装置

技术领域

本公开涉及计算机技术领域，特别涉及一种应用加密方法及装置。

背景技术

随着用户对信息安全的重视，具有应用加密的功能的应用锁的使用越来越普遍。

目前，终端中可以设置多个系统帐号，每个系统帐号对应一个资源文件，每个资源文件用于存储在登录对应的系统帐号期间，运行系统中安装的各个应用所需要调用的资源。由于多个系统帐号包括一个主帐号和多个子帐号，且应用锁只能读取主帐号对应的资源文件，因此，应用锁只能对利用主帐号在系统中安装的应用进行加密。

发明内容

为解决相关技术中的问题，本公开提供了一种应用加密方法及装置。

根据本公开实施例的第一方面，提供一种应用加密方法，该方法包括：

接收应用发送的前台运行请求，该前台运行请求包括当前在系统中登录的系统帐号的标识；

检测该标识是否是系统的主帐号的标识；

当该标识不是主帐号的标识时，将该标识替换为主帐号的标识；

确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

可选的，该方法还包括：

检测标识是否是系统的双开帐号的标识，应用在登录有双开帐号的系统中运行时的应用帐号与在登录有主帐号的系统中运行时的应用帐号不同；

在标识是双开帐号的标识时，触发执行将标识替换为主帐号的标识的步骤。

可选的，该方法还包括：

检测在登录有主帐号的系统中运行应用时是否对应用加密；

当在登录有主帐号的系统中运行应用时对应用加密，则触发执行确定在登录有主帐号的系统中对应用的加密规则的步骤。

可选的，检测在登录有主帐号的系统中运行应用时是否对应用加密，包括：

读取应用的加密指示，加密指示用于指示是否对应用加密；

在加密指示指示了对应用加密时，确定在登录有主帐号的系统中运行应用时对应用加密。

可选的，该方法还包括：

接收用户输入的验证密码；

根据加密规则验证该验证密码是否正确；

在验证出该验证密码正确时，对应用进行解密；

将加密指示由指示对应用加密修改为不对应用加密。

可选的，该方法还包括：

在修改加密指示之后，检测加密指示是否满足预设的更新条件；

在加密指示满足更新条件时，将加密指示由指示不对应用加密修改为对应用加密。

可选的，更新条件是应用切换到后台运行，或者，应用切换到后台运行的时长达到预设时长，或者，终端的屏幕由非锁屏状态转换为锁屏状态。

根据本公开实施例的第二方面，提供一种应用加密装置，该装置包括：

第一接收模块，被配置为接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识；

第一检测模块，被配置为检测第一接收模块得到的标识是否是系统的主帐号的标识；

替换模块，被配置为当第一检测模块检测出标识不是主帐号的标识时，将标识替换为主帐号的标识；

加密模块，被配置为确定在登录有替换模块得到的主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

可选的，该装置还包括：

第二检测模块，被配置为检测标识是否是系统的双开帐号的标识，应用在登录有双开帐号的系统中运行时的应用帐号与在登录有主帐号的系统中运行时的应用帐号不同；

第一触发模块，被配置为在第二检测模块检测出标识是双开帐号的标识时，触发执行将标识替换为主帐号的标识的步骤。

可选的，该装置还包括：

第三检测模块，被配置为检测在登录有主帐号的系统中运行应用时是否对应用加密；

第二触发模块，被配置为当第三检测模块检测出在登录有主帐号的系统中运行应用时对应用加密，则触发执行确定在登录有主帐号的系统中对应用的加密规则的步骤。

可选的，第三检测模块，包括：

读取子模块，被配置为读取应用的加密指示，加密指示用于指示是否对应用加密；

确定子模块，被配置为在读取子模块得到的加密指示指示了对应用加密时，确定在登录有主帐号的系统中运行应用时对应用加密。

可选的，该装置还包括：

第二接收模块，被配置为接收用户输入的验证密码；

验证模块，被配置为根据加密规则验证第二接收模块接收的验证密码是否正确；

解密模块，被配置为在验证模块验证出验证密码正确时，对应用进行解密；

第一修改模块，被配置为将加密指示由指示对应用加密修改为不对应用加密。

可选的，该装置还包括：

第四检测模块，被配置为在修改加密指示之后，检测加密指示是否满足预设的更新条件；

第二修改模块，被配置为在第四检测模块检测出加密指示满足更新条件时，将加密指示由指示不对应用加密修改为对应用加密。

可选的，更新条件是应用切换到后台运行，或者，应用切换到后台运行的时长达到预设时长，或者，终端的屏幕由非锁屏状态转换为锁屏状态。

根据本公开实施例的第三方面，提供一种应用加密装置，装置包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，处理器被配置为：

接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识；

检测该标识是否是系统的主帐号的标识；

当该标识不是主帐号的标识时，将该标识替换为主帐号的标识；

确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

本公开的实施例提供的技术方案可以包括以下有益效果：

通过在应用发送的前台运行请求包括的标识不是系统的主帐号的标识时，终端将该标识替换为主帐号的标识，使得终端中的应用锁可以根据在登录有主帐号的系统中对应用的加密规则来加密该应用，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，导致应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

通过检测标识是否是系统的双开帐号的标识，在检测出标识是双开帐号的标识时，将该标识替换为主帐号的标识，使得终端只有在前台运行请求包括的系统帐号的标识是双开帐号的标识时，才能控制应用锁读取主帐号对应的资源文件，并利用资源文件中该应用的加密规则对该应用进行加密，提高了主帐号对应的资源文件的安全性。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本公开说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

图 1 是根据一示例性实施例示出的一种应用加密方法的流程图。

图 2 是根据另一示例性实施例示出的一种应用加密方法的流程图。

图 3 是根据一示例性实施例示出的一种应用加密装置的框图。

图 4 是根据一示例性实施例示出的一种应用加密装置的框图。

图 5 是根据一示例性实施例示出的一种用于应用加密的装置的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

图 1 是根据一示例性实施例示出的一种应用加密方法的流程图，该应用加密方法应用于终端中，该终端可以设置多个系统帐号，如图 1 所示，该应用加密方法包括以下步骤。

在步骤 101 中，接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识。

在步骤 102 中，检测该标识是否是系统的主帐号的标识。

在步骤 103 中，当该标识不是主帐号的标识时，将该标识替换为主帐号的标识。

在步骤 104 中，确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

综上所述，本公开提供的应用加密方法，通过在应用发送的前台运行请求包括的标识不是系统的主帐号的标识时，终端将该标识替换为主帐号的标识，使得终端中的应用锁可以根据在登录有主帐号的系统中对应用的加密规则来加密该应用，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

图 2 是根据另一示例性实施例示出的一种应用加密方法的流程图，该应用加密方法应用于终端中，该终端可以设置多个系统帐号，如图 2 所示，该应用加密方法包括如下步骤。

在步骤 201 中，接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识。

当用户开启一个应用时，开启的应用会向终端发送前台运行请求，该前台运行请求用于请求终端在前台运行该应用。其中，前台运行请求包括当前在系统中登录的系统帐号的标识，该当前在系统中登录的系统帐号的标识是指该应用运行时所使用的资源文件对应的系统帐号的标识。其中，终端中的每个系统帐号都对应一个资源文件，且资源文件用于存储在登录对应的系统帐号的期间运行的各个应用所需要使用的数据。

本实施例中，系统帐号包括一个主帐号和多个子帐号，系统帐号的标识可以为系统帐号的身份标识号码（Identity，ID），比如主帐号的 ID 为 user0，子帐号的 ID 为 user8、user10、user11 等。

在步骤 202 中，检测标识是否是系统的主帐号的标识，当标识不是主帐号的标识时，执行步骤 203。

终端检测前台运行请求中的系统帐号的标识和主帐号的标识是否相同，若不相同，则该系统帐号的标识不是主帐号的标识，执行步骤 203；若相同，则该系统帐号的标识是主帐号的标识，终端控制应用锁读取主帐号对应的资源文件，该主帐号对应的资源文件中包括每个应用对应的加密指示以及加密规则，然后，终端控制应用锁在该资源文件中查找生成该前台运行请求的应用对应的加密指示以及加密规则，在查找得到的加密指示指示了对应用进行加密时，利用查找得到的加密规则对该应用进行加密。其中，应用锁用于对终端中安装的应用进行加密，且该应用锁只能读取该主帐号对应的资源文件；加密指示用于指示是否对应用加密，该加密指示可以为字符，如以 0 指示不对应用加密，以 1 指示对应用加密；加密规则至少包括加密形式和加密密码，加密形式可以是手势滑动形式，相应地，加密密码是手势滑动的图案；加密形式也可以是字符输入形式，相应地，加密密码是字符；加密形式还可以是音频输入形式，相应地，加密密码是音频，本实施例不对加密形式和加密密码作限定。

其中，终端控制应用锁在主帐号对应的资源文件中查找生成该前台运行请求的应用对应的加密指示以及加密规则，包括：终端从前台运行请求中获取该应用的标识，根据预设的加密指示以及加密规则与应用标识的对应关系，得到该应用的标识对应的加密指示以及加密规则，其中，应用的标识可以为应用的包名。

在步骤 203 中，当标识不是主帐号的标识时，将标识替换为主帐号的标识，执行步骤 206。

在一种实现方式中，终端将标识替换为主帐号的标识，包括：终端获取前台运行请求包括的标识，将该标识修改成主帐号的标识。在另一种实现方式中，终端将标识替换为主帐号的标识，包括：终端删除前台运行请求包括的标识，并将主帐号的标识添加到前台运行请求中。本实施不对终端将标识替换为主帐号的标识的替换方式作限定。

假设主帐号的标识为 user0，前台运行请求包括的标识为 user8，终端检测出 user8 与 user0 不同，将 user8 修改成 user0。

可选的，为了提高主帐号对应的资源文件的安全性，终端只有在前台运行请求包括的标识是双开帐号的标识时，再将标识替换为主帐号的标识，也即，在步骤 201 之后，不执行步骤 202 和步骤 203，直接执行步骤 204。其中，双开帐号是系统的子帐号中的一个。每个在登录有双开帐号的系统中运行的双开应用都对应一个运行在登录有主帐号的系统中的应用，且每个双开应用的标识与对应的应用的标识相同，在每个双开应用中登录的应用帐号与在运行在登录有主帐号的系统中的应用中登录的应用帐号不同。

在步骤 204 中，检测标识是否是系统的双开帐号的标识。

终端检测标识是否是系统的双开帐号的标识的方式，与步骤 202 中终端检测标识是否是系统的主帐号的标识的方式相同，在此不作赘述。

假设双开应用 qx 发送了前台运行请求，终端获取到该前台运行请求包括的系统帐号的标识为 user8，再检测 user8 是否是系统的双开帐号的标识。

在步骤 205 中，在标识是双开帐号的标识时，将标识替换为主帐号的标识。

由于在前台运行请求包括的系统帐号的标识是主帐号的标识时，终端才会控制应用锁读取主帐号对应的资源文件，因此，当前台运行请求包括的系统帐号的标识是双开帐号的标识时，终端需要将该标识替换为主帐号的标识，这样，终端才会控制应用锁读取主帐号对应的资源文件；而在登录有除双开帐号之外的其他子帐号的系统中运行的应用发送前台运行请求时，终端不会将前台运行请求包括的系统帐号的标识替换为主帐号的标识，从而不会控制应用锁读取主帐号对应的资源文件，提高了主帐号对应的资源文件的安全性。

在步骤 206 中，检测在登录有主帐号的系统中运行应用时是否对应用加密。

检测在登录有主帐号的系统中运行应用时是否对应用加密，包括：读取应用的加密指示；在加密指示指示了对应用加密时，确定在登录有主帐号的系统中运行应用时对应用加密。

在主帐号对应的资源文件中预存有每个应用的标识对应的加密指示，终端控制应用锁读取该应用的标识对应的加密指示，即可获知是否需要对该应用进行加密。

在步骤207中，当在登录有主帐号的系统中运行应用时对应用加密，确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

在步骤208中，接收用户输入的验证密码。

可选的，终端控制应用锁利用加密规则加密应用后，会显示加密界面，接收用户在该加密界面中输入的验证密码，控制应用锁对该应用进行解密，并允许用户使用该应用。

在步骤209中，根据加密规则验证验证密码是否正确，在验证出验证密码正确时，执行步骤210。

终端验证用户输入的验证密码与加密规则中加密的密码是否匹配，若验证密码与加密的密码匹配，则验证出该验证密码正确；若验证密码与加密的密码不匹配，则验证出该验证密码错误。

在验证出验证密码错误时，终端不控制应用锁对应用进行解密。可选的，在验证出验证密码错误时，终端可以显示提示信息以提示用户输入的验证密码不正确，需要重新输入验证密码。

在步骤210中，在验证出验证密码正确时，对应用进行解密。

在验证出验证密码正确时，终端控制应用锁对应用进行解密，此时，用户能够使用该应用。

在步骤211中，将加密指示由指示对应用加密修改为不对应用加密。

比如终端将加密指示由1修改为0，表示终端将对应用加密修改为不对应用加密。

步骤211可以在步骤210之后执行，也可以在步骤210之前执行，还可以和步骤210同时执行，本实施例不作限定。

在步骤212中，在修改加密指示之后，检测加密指示是否满足预设的更新条件，在加密指示满足更新条件时，执行步骤213。

更新条件是应用切换到后台运行，或者，应用切换到后台运行的时长达到预设时长，或者，终端的屏幕由非锁屏状态转换为锁屏状态。该更新条件可以由用户设置，也可以由开发者设置，本实施例不作限定。其中锁屏状态是指终端未点亮屏幕的状态，非锁屏状态是指终端点亮屏幕的状态。

当更新条件是应用切换到后台运行时，若该应用从前台切换到后台运行，则触发终端修改加密指示；当更新条件是应用切换到后台运行的时长达到预设时长时，若该应用从前台切换到后台运行，则触发终端启动计时器，在计时器达到该预设时长时，终端修改加密指示；当更新条件是终端的屏幕由非锁屏状态转换为锁屏状态时，若终端的屏幕由非锁屏状态转换为锁屏状态，则触发终端修改加密指示。

在步骤213中，在加密指示满足更新条件时，将加密指示由指示不对应用加密修改为对应用加密。

终端将加密指示由指示不对应用加密修改为对应用加密，使得该应用在下一次发送前台运行请求时，终端还能够控制应用锁对该应用加密，要求用户输入验证密码，在终端验证该验证密码通过后，允许用户才能使用该应用，提高了该应用的安全性。

综上所述，本公开提供的应用加密方法，通过在应用发送的前台运行请求包括的标识不是系统的主帐号的标识时，将该标识替换为主帐号的标识，使得终端中的应用锁可以根据在登录有主帐号的系统中对应用的加密规则来加密该应用，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

另外，通过检测标识是否是系统的双开帐号的标识，在检测出标识是双开帐号的标识时，将该标识替换为主帐号的标识，使得终端只有在系统帐号的标识是双开帐号的标识时，才能控制应用锁读取主帐号对应的资源文件，并利用资源文件中该应用的加密规则对该应用进行加密，提高了主帐号对应的资源文件的安全性。

图3是根据一示例性实施例示出的一种应用加密装置的框图，该应用加密装置应用于终端中，该终端可以设置多个系统帐号，如图3所示，该应用加密装置包括：第一接收模块310、第一检测模块320、替换模块330、加密模块340。

该第一接收模块310，被配置为接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识；

该第一检测模块320，被配置为检测第一接收模块310得到的标识是否是系统的主帐号的标识；

该替换模块 330，被配置为当第一检测模块 320 检测出标识不是主帐号的标识时，将标识替换为主帐号的标识；

该加密模块 340，被配置为确定在登录有替换模块得到的主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

综上所述，本公开提供的应用加密装置，通过在应用发送的前台运行请求包括的标识不是系统的主帐号的标识时，将该标识替换为主帐号的标识，使得终端中的应用锁可以根据在登录有主帐号的系统中对应用的加密规则来加密该应用，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

图 4 是根据一示例性实施例示出的一种应用加密装置的框图，该应用加密装置应用于终端中，该终端可以设置多个系统帐号，如图 4 所示，该应用加密装置包括：第一接收模块 410、第一检测模块 420、替换模块 430、加密模块 440。

该第一接收模块 410，被配置为接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识；

该第一检测模块 420，被配置为检测第一接收模块 410 得到的标识是否是系统的主帐号的标识；

该替换模块 430，被配置为当第一检测模块 420 检测出标识不是主帐号的标识时，将标识替换为主帐号的标识；

该加密模块 440，被配置为确定在登录有替换模块得到的主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

可选的，该装置还包括：第二检测模块 450、第一触发模块 460。

该第二检测模块 450，被配置为检测标识是否是系统的双开帐号的标识，应用在登录有双开帐号的系统中运行时的应用帐号与在登录有主帐号的系统中运行时的应用帐号不同；

该第一触发模块 460，被配置为在第二检测模块 450 检测出标识是双开帐号的标识时，触发执行将标识替换为主帐号的标识的步骤。

可选的，该装置还包括：第三检测模块 470、第二触发模块 480。

该第三检测模块 470，被配置为检测在登录有主帐号的系统中运行应用时是否对应用加密；

该第二触发模块 480，被配置为当第三检测模块 470 检测出在登录有主帐号的系统中运行应用时对应用加密，则触发执行确定在登录有主帐号的系统中对应用的加密规则的步骤。

可选的，第三检测模块 470，包括：读取子模块 471、确定子模块 472。

该读取子模块 471，被配置为读取应用的加密指示，加密指示用于指示是否对应用加密；

该确定子模块 472，被配置为在读取子模块 471 得到的加密指示指示了对应用加密时，确定在登录有主帐号的系统中运行应用时对应用加密。

可选的，该装置还包括：第二接收模块 490、验证模块 491、解密模块 492、第一修改模块 493。

该第二接收模块 490，被配置为接收用户输入的验证密码；

该验证模块 491，被配置为根据加密规则验证第二接收模块 490 接收的验证密码是否正确；

该解密模块 492，被配置为在验证模块 491 验证出验证密码正确时，对应用进行解密；

该第一修改模块 493，被配置为将加密指示由指示对应用加密修改为不对应用加密。

可选的，该装置还包括：第四检测模块 494、第二修改模块 495。

该第四检测模块 494，被配置为在修改加密指示之后，检测加密指示是否满足预设的更新条件；

该第二修改模块 495，被配置为在第四检测模块 494 检测出加密指示满足更新条件时，将加密指示由指示不对应用加密修改为对应用加密。

可选的，更新条件是应用切换到后台运行，或者，应用切换到后台运行的时长达到预设时长，或者，终端的屏幕由非锁屏状态转换为锁屏状态。

综上所述，本公开提供的应用加密装置，通过在应用发送的前台运行请求包括的标识不是系统的主帐号的标识时，将该标识替换为主帐号的标识，使得终端中的应用锁可以根据在登录有主帐号的系统中对应用的加密规则来加密该应用，解决了应用锁只能对运行在登录有主帐号的系统中的应用进行加密，应用锁应用范围小的问题，达到了扩大应用锁的应用范围的效果。

另外，通过检测标识是否是系统的双开帐号的标识，在检测出标识是双开帐号的标识时，将该标识替换为主帐号的标识，使得终端只有在系统帐号的标

识是双开帐号的标识时，才能控制应用锁读取主帐号对应的资源文件，并利用资源文件中该应用的加密规则对该应用进行加密，提高了主帐号对应的资源文件的安全性。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

本公开一示例性实施例提供了一种应用加密装置，能够实现本公开提供的应用加密方法，该应用加密装置包括：处理器、用于存储处理器可执行指令的存储器；

其中，处理器被配置为：

接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识；

检测该标识是否是系统的主帐号的标识；

当该标识不是主帐号的标识时，将该标识替换为主帐号的标识；

确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用。

图 5 是根据一示例性实施例示出的一种用于应用加密的装置 500 的框图。例如，装置 500 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

参照图 5，装置 500 可以包括以下一个或多个组件：处理组件 502，存储器 504，电源组件 506，多媒体组件 508，音频组件 510，输入/输出（I/O）的接口 512，传感器组件 514，以及通信组件 516。

处理组件 502 通常控制装置 500 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 502 可以包括一个或多个处理器 518 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 502 可以包括一个或多个模块，便于处理组件 502 和其他组件之间的交互。例如，处理组件 502 可以包括多媒体模块，以方便多媒体组件 508 和处理组件 502 之间的交互。

存储器 504 被配置为存储各种类型的数据以支持在装置 500 的操作。这些数据的示例包括用于在装置 500 上操作的任何应用程序或方法的指令，联系人

数据，电话簿数据，消息，图片，视频等。存储器 504 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

电源组件 506 为装置 500 的各种组件提供电力。电源组件 506 可以包括电源管理系统，一个或多个电源，及其他与为装置 500 生成、管理和分配电力相关联的组件。

多媒体组件 508 包括在所述装置 500 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器（LCD）和触摸面板（TP）。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 508 包括一个前置摄像头和/或后置摄像头。当装置 500 处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

音频组件 510 被配置为输出和/或输入音频信号。例如，音频组件 510 包括一个麦克风（MIC），当装置 500 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 504 或经由通信组件 516 发送。在一些实施例中，音频组件 510 还包括一个扬声器，用于输出音频信号。

I/O 接口 512 为处理组件 502 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 514 包括一个或多个传感器，用于为装置 500 提供各个方面的状态评估。例如，传感器组件 514 可以检测到装置 500 的打开/关闭状态，组件的相对定位，例如所述组件为装置 500 的显示器和小键盘，传感器组件 514 还可以检测装置 500 或装置 500 一个组件的位置改变，用户与装置 500 接触的存在或不存在，装置 500 方位或加速/减速和装置 500 的温度变化。传感器组件

514 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 514 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 514 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

通信组件 516 被配置为便于装置 500 和其他设备之间有线或无线方式的通信。装置 500 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 516 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 516 还包括近场通信（NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

在示例性实施例中，装置 500 可以被一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 504，上述指令可由装置 500 的处理器 518 执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器（RAM）、CD-ROM、磁带、软盘和光数据存储设备等。

本领域技术人员在考虑说明书及实践这里的公开后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

1、一种应用加密方法，其特征在于，所述方法包括：

接收应用发送的前台运行请求，所述前台运行请求包括当前在系统中登录的系统帐号的标识；

检测所述标识是否是所述系统的主帐号的标识；

当所述标识不是所述主帐号的标识时，将所述标识替换为所述主帐号的标识；

确定在登录有所述主帐号的系统中对所述应用的加密规则，并利用所述加密规则加密所述应用。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

检测所述标识是否是所述系统的双开帐号的标识，所述应用在登录有所述双开帐号的系统中运行时的应用帐号与在登录有所述主帐号的系统中运行时的应用帐号不同；

在所述标识是所述双开帐号的标识时，触发执行所述将所述标识替换为所述主帐号的标识的步骤。

3、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

检测在登录有所述主帐号的系统中运行所述应用时是否对所述应用加密；

当在登录有所述主帐号的系统中运行所述应用时对所述应用加密，则触发执行所述确定在登录有所述主帐号的系统中对所述应用的加密规则的步骤。

4、根据权利要求 3 所述的方法，其特征在于，所述检测在登录有所述主帐号的系统中运行所述应用时是否对所述应用加密，包括：

读取所述应用的加密指示，所述加密指示用于指示是否对所述应用加密；

在所述加密指示指示了对所述应用加密时，确定在登录有所述主帐号的系统中运行所述应用时对所述应用加密。

5、根据权利要求 1 至 4 任一所述的方法，其特征在于，所述方法还包括：

接收用户输入的验证密码；

根据所述加密规则验证所述验证密码是否正确；

在验证出所述验证密码正确时，对所述应用进行解密；

将所述加密指示由指示对所述应用加密修改为不对所述应用加密。

6、根据权利要求 5 所述的方法，其特征在于，所述方法还包括：

在修改所述加密指示之后，检测所述加密指示是否满足预设的更新条件；

在所述加密指示满足所述更新条件时，将所述加密指示由指示不对所述应用加密修改为对所述应用加密。

7、根据权利要求 6 所述的方法，其特征在于，所述更新条件是所述应用切换到后台运行，或者，所述应用切换到后台运行的时长达到预设时长，或者，终端的屏幕由非锁屏状态转换为锁屏状态。

8、一种应用加密装置，其特征在于，所述装置包括：

第一接收模块，被配置为接收应用发送的前台运行请求，所述前台运行请求包括当前在系统中登录的系统帐号的标识；

第一检测模块，被配置为检测所述第一接收模块得到的所述标识是否是所述系统的主帐号的标识；

替换模块，被配置为当所述第一检测模块检测出所述标识不是所述主帐号的标识时，将所述标识替换为所述主帐号的标识；

加密模块，被配置为确定在登录有所述替换模块得到的所述主帐号的系统中对所述应用的加密规则，并利用所述加密规则加密所述应用。

9、根据权利要求 8 所述的装置，其特征在于，所述装置还包括：

第二检测模块，被配置为检测所述标识是否是所述系统的双开帐号的标识，所述应用在登录有所述双开帐号的系统中运行时的应用帐号与在登录有所述主帐号的系统中运行时的应用帐号不同；

第一触发模块，被配置为在所述第二检测模块检测出所述标识是所述双开帐号的标识时，触发执行所述将所述标识替换为所述主帐号的标识的步骤。

10、根据权利要求 8 所述的装置，其特征在于，所述装置还包括：

第三检测模块，被配置为检测在登录有所述主帐号的系统中运行所述应用时是否对所述应用加密；

第二触发模块，被配置为当所述第三检测模块检测出在登录有所述主帐号的系统中运行所述应用时对所述应用加密，则触发执行所述确定在登录有所述主帐号的系统中对所述应用的加密规则的步骤。

11、根据权利要求 10 所述的装置，其特征在于，所述第三检测模块，包括：

读取子模块，被配置为读取所述应用的加密指示，所述加密指示用于指示是否对所述应用加密；

确定子模块，被配置为在所述读取子模块得到的所述加密指示指示了对所述应用加密时，确定在登录有所述主帐号的系统中运行所述应用时对所述应用加密。

12、根据权利要求 8 至 11 任一所述的装置，其特征在于，所述装置还包括：

第二接收模块，被配置为接收用户输入的验证密码；

验证模块，被配置为根据所述加密规则验证所述第二接收模块接收的所述验证密码是否正确；

解密模块，被配置为在所述验证模块验证出所述验证密码正确时，对所述应用进行解密；

第一修改模块，被配置为将所述加密指示由指示对所述应用加密修改为不对所述应用加密。

13、根据权利要求 12 所述的装置，其特征在于，所述装置还包括：

第四检测模块，被配置为在修改所述加密指示之后，检测所述加密指示是否满足预设的更新条件；

第二修改模块，被配置为在所述第四检测模块检测出所述加密指示满足所述更新条件时，将所述加密指示由指示不对所述应用加密修改为对所述应用加密。

14、根据权利要求 13 所述的装置，其特征在于，所述更新条件是所述应用切换到后台运行，或者，所述应用切换到后台运行的时长达到预设时长，或者，

终端的屏幕由非锁屏状态转换为锁屏状态。

15、一种应用加密装置，其特征在于，所述装置包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收应用发送的前台运行请求，所述前台运行请求包括当前在系统中登录的系统帐号的标识；

检测所述标识是否是所述系统的主帐号的标识；

当所述标识不是所述主帐号的标识时，将所述标识替换为所述主帐号的标识；

确定在登录有所述主帐号的系统中对所述应用的加密规则，并利用所述加密规则加密所述应用。

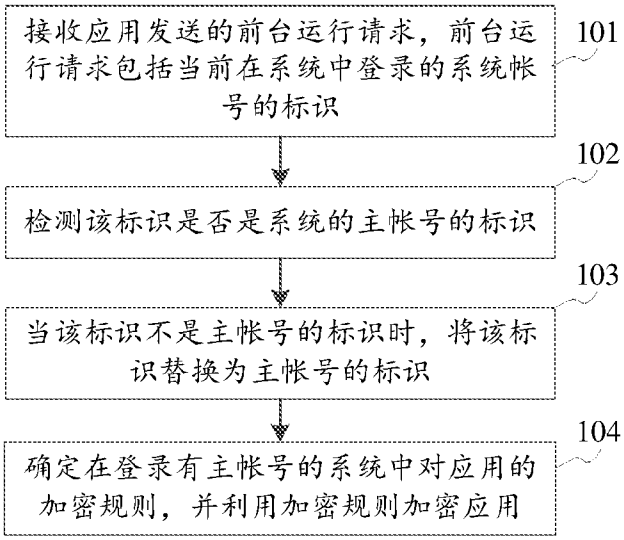
接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识
101
检测该标识是否是系统的主帐号的标识
102
当该标识不是主帐号的标识时，将该标识替换为主帐号的标识
103
确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用
104

图 1

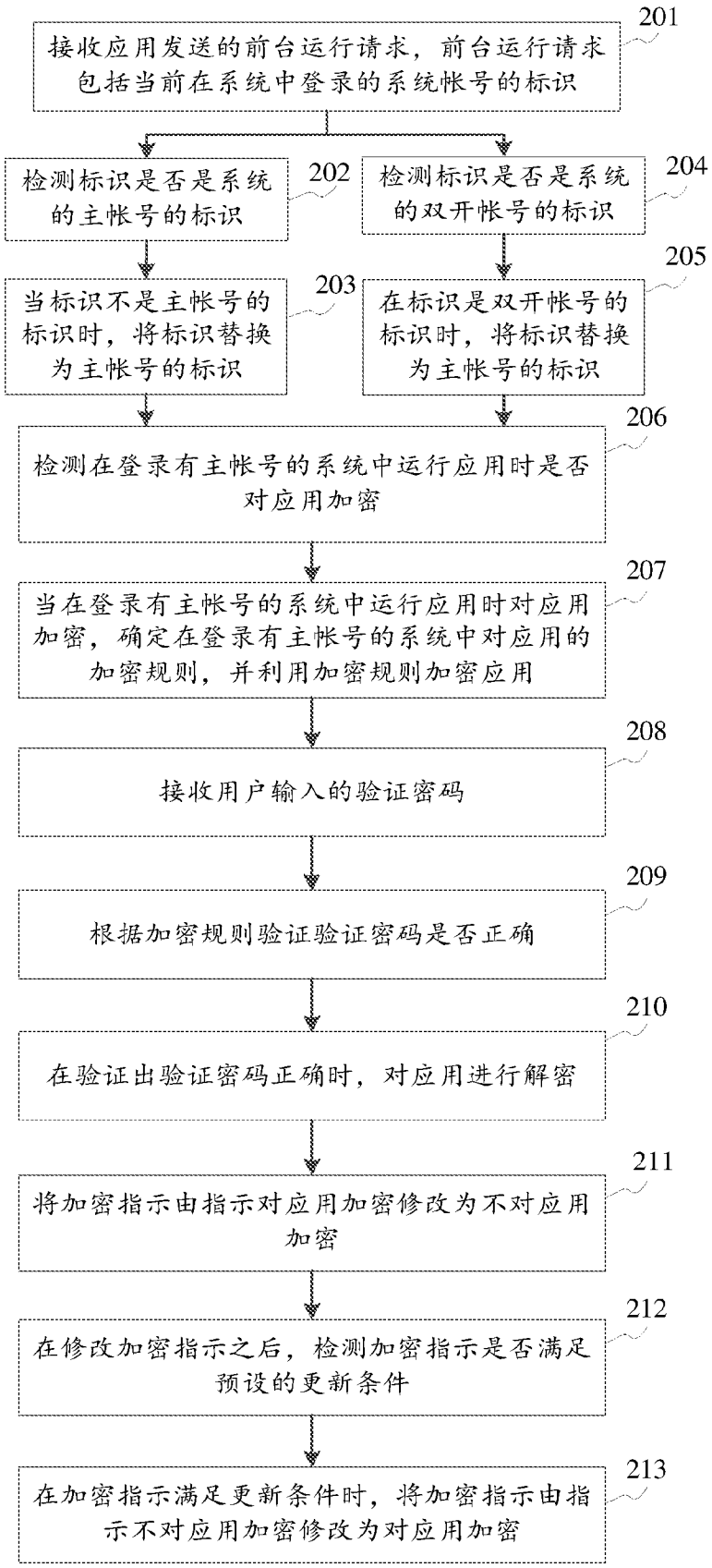
201
接收应用发送的前台运行请求，前台运行请求包括当前在系统中登录的系统帐号的标识
202
检测标识是否是系统的主帐号的标识
204
检测标识是否是系统的双开帐号的标识
203
当标识不是主帐号的标识时，将标识替换为主帐号的标识
205
在标识是双开帐号的标识时，将标识替换为主帐号的标识
206
检测在登录有主帐号的系统中运行应用时是否对应用加密
207
当在登录有主帐号的系统中运行应用时对应用加密，确定在登录有主帐号的系统中对应用的加密规则，并利用加密规则加密应用
208
接收用户输入的验证密码
209
根据加密规则验证验证密码是否正确
210
在验证出验证密码正确时，对应用进行解密
211
将加密指示由指示对应用加密修改为不对应用加密
212
在修改加密指示之后，检测加密指示是否满足预设的更新条件
213
在加密指示满足更新条件时，将加密指示由指示不对应用加密修改为对应用加密

图 2

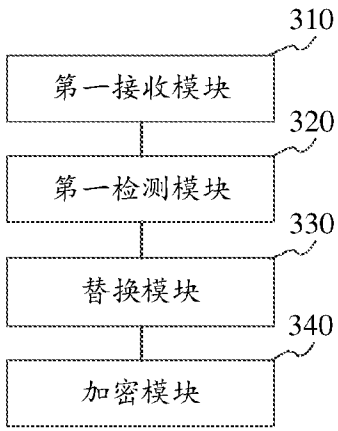

图 3

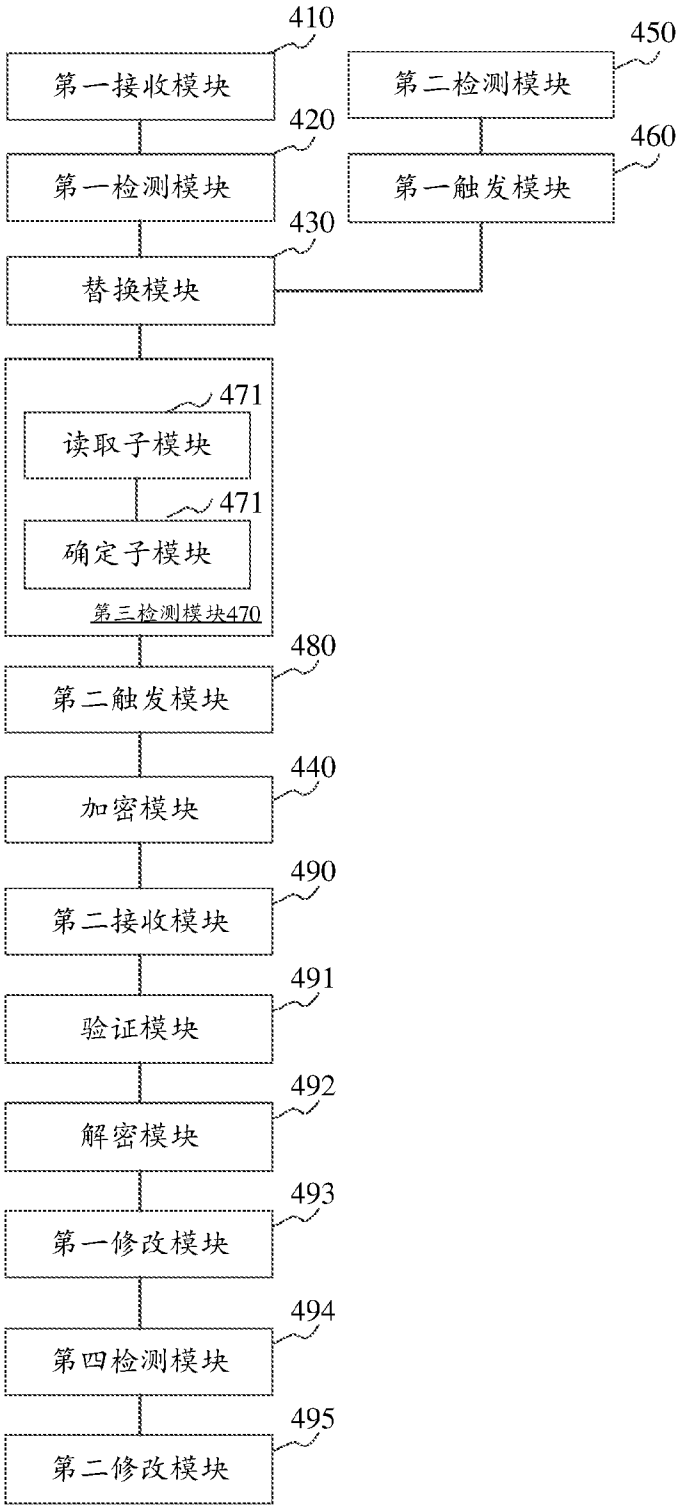
410
第一接收模块
450
第二检测模块
420
第一检测模块
460
第一触发模块
430
替换模块
471
读取子模块
471
确定子模块
第三检测模块470
480
第二触发模块
440
加密模块
490
第二接收模块
491
验证模块
492
解密模块
493
第一修改模块
494
第四检测模块
495
第二修改模块

图 4

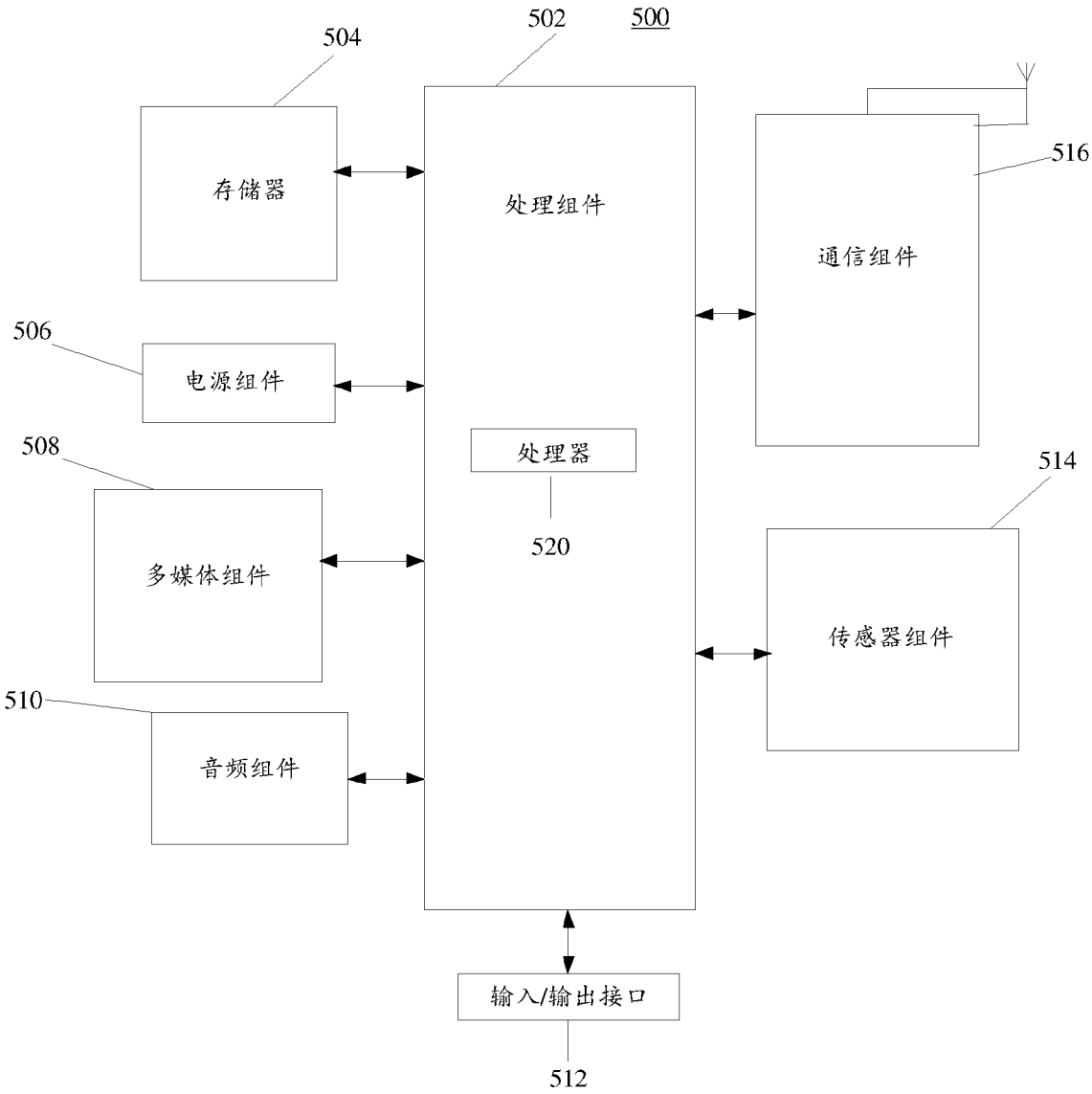
500
502
504
存储器
处理组件
通信组件
516
506
电源组件
处理器
520
508
多媒体组件
514
传感器组件
510
音频组件
输入/输出接口
512

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/083335

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31 (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; CNKI; CNPAT: account, app, application, foreground, start, lock, unlock, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103778381 A (CHINA STANDARD SOFTWARE CO., LTD.) 07 May 2014 (07.05.2014) description, paragraphs [0034]-[0038]	1-15
A	CN 105574437 A (BEIJING KINGSOFT SECURITY SOFTWARE CO., LTD.) 11 May 2016 (11.05.2016) the whole document	1-15
A	US 2014298190 A1 (MICROSOFT CORPORATION) 02 October 2014 (02.10.2014) 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
14 February 2017	10 March 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 ZHUANG, Yong Telephone No. (86-10) 62414020

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/083335

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103778381 A	07 May 2014	None	
CN 105574437 A	11 May 2016	None	
US 2014298190 A1	02 October 2014	WO 2014158223 A1	02 October 2014
		CN 105144183 A	09 December 2015
		EP 2979216 A1	03 February 2016
		KR 20150140302 A	15 December 2015

国际检索报告

国际申请号
PCT/CN2016/083335

A. 主题的分类

G06F 21/31(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;EPODOC;CNKI;CNPAT: 账号,账户,应用,启动,前台,锁定,解锁,加密, account, app, application, foreground, start, lock, unlock, encrypt

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
A	CN 103778381 A (中标软件有限公司) 2014年 5月 7日 (2014-05-07) 说明书第[0034]-[0038]段	1-15
A	CN 105574437 A (北京金山安全软件有限公司) 2016年 5月 11日 (2016-05-11) 全文	1-15
A	US 2014298190 A1 (MICROSOFT CORPORATION) 2014年 10月 2日 (2014-10-02) 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
2017年 2月 14日	2017年 3月 1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 庄湧 电话号码 (86-10)62414020

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/083335

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	103778381	A	2014年 5月 7日	无			
CN	105574437	A	2016年 5月 11日	无			
US	2014298190	A1	2014年 10月 2日	WO	2014158223	A1	2014年 10月 2日
				CN	105144183	A	2015年 12月 9日
				EP	2979216	A1	2016年 2月 3日
				KR	20150140302	A	2015年 12月 15日