

(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 6 月 30 日 (30.06.2016)



(10) 国际公布号
WO 2016/101559 A1

- (51) 国际专利分类号:
G06F 21/60 (2013.01)
- (21) 国际申请号: PCT/CN2015/081962
- (22) 国际申请日: 2015 年 6 月 19 日 (19.06.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410834664.8 2014 年 12 月 26 日 (26.12.2014) CN
- (71) 申请人: 深圳市中兴微电子技术有限公司 (ZHONGXING MICROELECTRONICS TECHNOLOGY CO.LTD) [CN/CN]; 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。
- (72) 发明人: 邓宁堃 (DENG, Ningkun); 中国广东省深圳市盐田区大梅沙 1 号厂房, Guangdong 518085 (CN)。
- (74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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 METHOD AND DEVICE, AND COMPUTER STORAGE MEDIUM

(54) 发明名称: 一种数据安全存取方法、装置和计算机存储介质

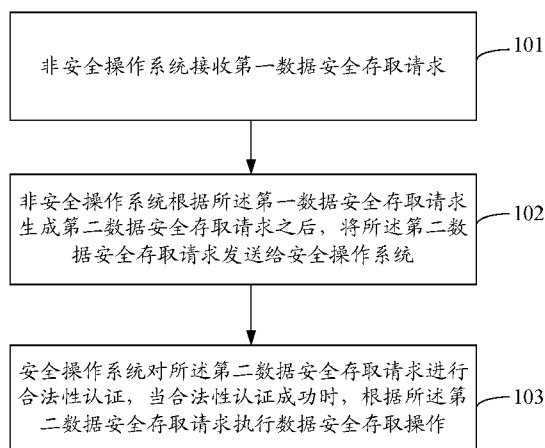


图 1 / Fig. 1

- 101 A NON-SECURE OPERATING SYSTEM RECEIVES A FIRST SECURE DATA ACCESS REQUEST
- 102 THE NON-SECURE OPERATING SYSTEM GENERATES A SECOND SECURE DATA ACCESS REQUEST ACCORDING TO THE FIRST SECURE DATA ACCESS REQUEST, AND THEN TRANSMITS THE SECOND SECURE DATA ACCESS REQUEST TO A SECURE OPERATING SYSTEM
- 103 THE SECURE OPERATING SYSTEM PERFORMS LEGALITY AUTHENTICATION ON THE SECOND SECURE DATA ACCESS REQUEST, AND EXECUTES A SECURE DATA ACCESS OPERATION ACCORDING TO THE SECOND SECURE DATA ACCESS REQUEST WHEN THE LEGALITY AUTHENTICATION IS SUCCESSFUL

(57) Abstract: A secure data access method, a secure data access device and a computer storage medium. The method comprises: a non-secure operating system receives a first secure data access request (101); the non-secure operating system generates a second secure data access request according to the first secure data access request, and then transmits the second secure data access request to a secure operating system (102); and the secure operating system performs legality authentication on the second secure data access request, and executes a secure data access operation according to the second secure data access request when the legality authentication is successful (103).

(57) 摘要: 一种数据安全存取方法、数据安全存取装置和计算机存储介质。其中, 该方法包括: 非安全操作系统接收第一数据安全存取请求 (101); 非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求之后, 将所述第二数据安全存取请求发送给安全操作系统 (102); 安全操作系统对所述第二数据安全存取请求进行合法性认证, 当合法性认证成功时, 根据所述第二数据安全存取请求执行数据安全存取操作 (103)。



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))。

一种数据安全存取方法、装置和计算机存储介质

技术领域

本发明涉及智能终端安全存储领域，更具体的说，是一种数据安全存取方法、装置和计算机存储介质。

5 背景技术

随着现代通信技术的飞速发展，终端，尤其是智能终端，如手机、平板电脑、智能手表等越来越深入到人们的学习、工作和生活中并发挥着至关重要的作用。随着用户对智能终端的依赖，一些重要的数据，例如，个人资料、通讯录、私密照片、机密文件等通常也被存储在智能终端中。确
10 保这些数据的安全十分重要。

市场上主流的智能终端操作系统有三种：安卓（Android）操作系统、苹果操作系统（iOS，iPhone Operating System）、Windows 操作系统。但是，每一种操作系统都不能完全保证终端的安全性，尤其是 Android 操作系统终端，由于 Android 操作系统自身的开放性，使得 Android 操作系统终端很有
15 可能感染病毒或者木马，从而导致重要信息的泄露或者破坏。再者，由于智能终端的便捷性，用户很有可能丢失智能终端，有价值的信息也会随之丢失，比如个人隐私信息或者商业机密信息等。若被他人得到，这些信息可能被泄漏，这样会带来严重的损失。

然而，针对智能终端的本地数据安全存取，特别是用户能够快速、便捷
20 的存储、提取重要的安全数据，同时保证用户安全数据不会被泄露或破坏，目前还没有可靠的方案来实现。

发明内容

为了解决现有存在的技术问题，本发明实施例期望提供一种数据安全

存取方法、装置和计算机存储介质。

本发明实施例提供了一种数据安全存取方法，所述方法包括：

非安全操作系统接收第一数据安全存取请求；

非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；

安全操作系统对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

上述方案中，当所述第一数据安全存取请求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径；

当所述第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径。

上述方案中，当所述第一数据安全存取请求为数据安全存储请求时，所述方法还包括：所述非安全存取任务将待存储的数据从非安全存储器中读到非安全内存中。

上述方案中，所述非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求，包括：

非安全操作系统中的非安全存取任务将以下参数一和参数二携带在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识、数据存取信息，参数二包括验证码 MAGIC_NS。

上述方案中，所述合法性认证包括：第一次合法性认证和第二次合法性认证；

其中，所述第一次合法性认证，包括：安全操作系统中的安全监控任务判断所述第二数据安全存取请求中是否携带验证码 MAGIC_NS，如果是，

则确定所述第二数据安全存取请求第一次合法性认证成功；如果否，则确定所述第二数据安全存取请求第一次合法性失败；

所述第二次合法性认证包括：所述安全操作系统中的主控任务判断所述参数一中的各个参数是否合法，当所述参数一中各个参数均合法时，第二次合法性认证成功，否则，第二次合法性认证失败。

上述方案中，所述安全操作系统根据所述第二数据安全存取请求执行数据安全存取操作，包括：

当所述第二数据安全存取请求为数据安全存储请求时，安全存取任务执行以下操作：将已经存储在非安全内存中的待存储数据复制到安全内存，在安全内存中对待存储数据进行加密操作，将加密后的待存储数据写入安全存储器；

当所述第二数据安全存取请求为数据安全提取请求时，安全存取任务执行以下操作：将待提取数据从安全存储器读到安全内存；在安全内存中对待提取数据进行解密操作；将解密后的待提取数据复制到非安全内存。

上述方案中，所述安全操作系统根据所述第二数据安全存取请求执行数据安全存取操作之后，所述方法还包括：

安全操作系统中的安全存取任务生成数据安全存取结果并发送给安全操作系统中的安全监控任务，所述数据安全存取结果包括：参数三和参数四；其中参数三包括数据安全存取是否成功的指示消息，参数四为验证码MAGIC_SECURE；

所述安全监控任务判断数据安全存取结果中的参数四的值是否是MAGIC_SECURE，如果是，则安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证成功，数据安全存取流程结束；如果否，安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证不成功，安全监控任务向非安全操作系统返回处理失败的结果，数据安全存取流程结束。

本发明实施例提供了一种数据安全存取装置，所述装置包括：非安全操作系统和安全操作系统；其中，

所述非安全操作系统，配置为接收第一数据安全存取请求；并根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；

所述安全操作系统，配置为对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

上述方案中，当所述第一数据安全存取请求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径；

当所述第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径。

上述方案中，所述非安全操作系统包括非安全存取任务模块，配置为将待存储的数据从非安全存储器中读到非安全内存中。

上述方案中，所述非安全存取任务模块，还配置为将以下参数一和参数二携带在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识、数据存取信息，参数二包括验证码 MAGIC_NS。

上述方案中，所述合法性认证包括：第一次合法性认证和第二次合法性认证；

所述安全操作系统，包括安全监控任务模块和主控任务模块；其中，

所述安全监控任务模块，配置为接收非安全操作系统发送的第二数据安全存取请求，并通过以下方式对所述数据安全存取请求进行第一次合法性认证：安全监控任务模块判断所述第二数据安全存取请求中是否携带验

证码 MAGIC_NS，如果是，则确定所述第二数据安全存取请求第一次合法性认证成功；如果否，则确定所述第二数据安全存取请求第一次合法性失败；

所述主控任务模块，配置为通过以下方式对所述第二数据安全存取请求进行第二次合法性认证：主控任务模块判断第二数据安全存取请求中参数一中的各个参数是否合法，当所述参数一中各个参数均合法时，第二次合法性认证成功，否则，第二次合法性认证失败。

上述方案中，安全操作系统还包括安全存取任务模块，配置为通过以下方式执行数据安全存取操作：

10 当所述第二数据安全存取请求为数据安全存储请求时，安全存取任务模块执行以下操作：将已经存储在非安全内存中的待存储数据复制到安全内存，在安全内存中对待存储数据进行加密操作，将加密后的待存储数据写入安全存储器；

15 当所述第二数据安全存取请求为数据安全提取请求时，安全存取任务模块执行以下操作：将待提取数据从安全存储器读到安全内存；在安全内存中对待提取数据进行解密操作；将解密后的待提取数据复制到非安全内存。

20 上述方案中，所述安全存取任务模块，还配置为生成数据安全存取结果并发送给安全监控任务模块，所述数据安全存取结果包括：参数三和参数四；其中参数三包括数据安全存取是否成功的指示消息，参数四为验证码 MAGIC_SECURE；

所述安全监控任务模块，还配置为通过以下方式对数据安全存取结果的合法性进行验证：

25 安全监控任务模块判断数据安全存取结果中的参数四的值是否是 MAGIC_SECURE，如果是，则安全监控任务模块对安全存取任务模块所发送的数据安全存取结果的合法性验证成功；如果否，安全监控任务模块对

安全存取任务模块所发送的数据安全存取结果的合法性验证不成功。

本发明实施例还提供了一种计算机存储介质，所述存储介质包括一组计算机可执行指令，所述指令用于执行本发明实施例所述的数据安全存取方法。

- 5 本发明实施例所提供的一种数据安全存取方法、装置和计算机存储介质，非安全操作系统接收第一数据安全存取请求；非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；安全操作系统对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。如此，用户能够快速、便捷的存储活提
- 10 取重要的安全数据，同时保证用户安全数据不会被泄露或破坏。

附图说明

图 1 为本发明实施例提供的数据安全存取方法流程图；

图 2 为本发明实施例提供的数据安全存取装置的基本结构图；

- 15 图 3 为本发明实施例提供的数据安全存储方法流程图；

图 4 为本发明实施例提供的数据安全提取方法流程图。

具体实施方式

- 本发明实施例中，非安全操作系统接收第一数据安全存取请求；非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；安全操作系统对
- 20 所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

下面通过附图及具体实施例对本发明做进一步的详细说明。

实施例一

本发明实施例一提供了一种数据安全存取方法，如图 1 所示，该方法包括以下步骤：

步骤 101：非安全操作系统接收第一数据安全存取请求。

非安全操作系统通常运行在处理器的非安全状态（例如，支持信任区域（Trust Zone）安全方法的进阶精简指令集（ARM，Advanced RISC Machine）处理器包括两种状态：安全状态和非安全状态），非安全操作系统只能访问非安全硬件（即，非安全存储器、非安全内存）。非安全存储器是指，只在处理器的非安全状态下才能访问的存储器，由存储器控制器控制实现；非安全内存是指，在处理器的安全状态或非安全状态下都能访问的内存，由内存控制器控制实现。

在该步骤中，由非安全操作系统的非安全存取任务接收用户发送的第一数据安全存取请求。

用户发送的第一数据安全存取请求通常可以包括：数据安全存储请求或数据安全提取请求。

当所述第一数据安全存取请求为数据安全存储请求时，所述非安全存取任务需要将待存储的数据从非安全存储器中读到非安全内存中，用于后续安全操作系统使用。

当第一数据安全存取请求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径；

当第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径（也即，待提取数据的存储路径）。

步骤 102：非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统。

在这一步骤中，是由非安全操作系统中的非安全存取任务根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全

全存取请求发送给安全操作系统的安全监控任务。

非安全操作系统中的非安全存取任务根据所述第一数据安全存取请求生成第二数据安全存取请求，包括：

非安全存取任务将以下参数一和参数二携带在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识及数据存取信息，用于后续操作中安全操作系统执行数据安全存取操作时使用；

这里的参数一是根据第一数据安全存取请求生成的，所述任务标识的取值为 SECURE_SOURCE 或 UNSECURE_SOURCE，用于指示资源类型，即安全类型资源（SECURE_SOURCE）、或非安全类型资源（UNSECURE_SOURCE）；由于本发明实施例涉及的是一种数据安全存取方法，因此，所生成的参数一中任务标识的取值均为 SECURE_SOURCE；所述操作标识的取值为安全存储（SECURE_SAVE）、或安全提取（SECURE_LOAD），用于指示对任务标识所标识的资源类型的数据所进行的操作；所述参数一中的数据存取信息即为第一数据安全存取请求中的数据存取信息；

参数二包括验证码 MAGIC_NS，用于后续步骤中安全操作系统对第二数据安全存取请求的合法性进行认证；所述验证码 MAGIC_NS 是由非安全操作系统与安全操作系统事先约定的验证码。

步骤 103：安全操作系统对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

安全操作系统运行在处理器的安全状态，可以访问安全硬件（即，安全存储器、安全内存），也可以访问非安全硬件中的非安全内存，安全操作系统专门用来处理安全级别高的任务，如存储与提取安全数据、安全数据的加解密、数字版权管理、虚拟专用网络（VPN，Virtual Private Network）

管理等。它是精简、稳定的操作系统，安全操作系统中运行的安全任务是串行执行的，调度策略是非抢占式的，提高了系统内部的安全性和稳定性。安全存储器是指，只在处理器的安全状态下才能访问的存储器，由存储器控制器控制实现；安全内存是指，只在处理器的安全状态下才能访问的内存，由内存控制器控制实现。

这一步骤中，所述合法性认证包括：第一次合法性认证和第二次合法性认证；其中，第一次合法性认证在安全操作系统中的安全监控任务中执行，第二次合法性认证在安全操作系统中的主控任务中执行；其中，安全操作系统中主控任务处于就绪或执行状态，该任务通过安全监控任务传递的参数，创建相应的安全任务，完成用户需要的安全操作。安全监控任务还负责安全操作系统和非安全操作系统之间的通信和切换，非安全操作系统和安全操作系统都可以通过执行一条特殊的指令，如 ARM 的安全监控调用（SMC，Secure Monitor Call）指令跳转到安全监控任务，所述 SMC 指令的参数一和参数二用来保存非安全操作系统向安全操作系统传递的参数。

接收到所述携带了参数一和参数二的第二数据安全存取请求的安全监控任务对所述第二数据安全存取请求进行第一次合法性认证，所述第一次合法性认证，包括：

安全监控任务判断所述第二数据安全存取请求中是否携带验证码 MAGIC_NS（即参数二），如果是，则确定所述第二数据安全存取请求第一次合法性认证成功；如果否，则确定所述第二数据安全存取请求第一次合法性失败。

当第一次合法性认证失败，向非安全操作系统返回错误信息，不再执行后续操作；

当第一次合法性认证成功时，所述安全操作系统中的安全监控任务将所述第二数据安全存取请求中的参数一发送给安全操作系统中的主控任务；之后，进行第二次合法性认证，所述第二次合法性认证，包括：所述

主控任务对所述参数一中的各个参数的合法性进行认证（也即，判断参数一中各个参数包括任务标识、操作标识的取值是否为合法取值，判断数据存取信息中的文件名及存储或提取路径是否正确），当所述参数一中各个参数均合法时，第二次合法性认证成功，否则，第二次合法性认证失败。

- 5 当第二次合法性认证失败时，主控任务向非安全操作系统返回错误信息，不再进行后续操作；

当第二次合法性认证成功时，主控任务指示安全操作系统中的安全存取任务根据所述第二数据安全存取请求执行数据安全存取操作。

- 安全存取任务根据所述第二数据安全存取请求执行数据安全存取操作，包括：
- 10

当所述第二数据安全存取请求为数据安全存储请求时，安全存取任务执行以下操作：将已经存储在非安全内存中的待存储数据复制到安全内存，在安全内存中对待存储数据进行加密操作，将加密后的待存储数据写入安全存储器；

- 15 当所述第二数据安全存取请求为数据安全提取请求时，安全存取任务执行以下操作：将待提取数据从安全存储器读到安全内存；在安全内存中对待提取数据进行解密操作；将解密后的待提取数据复制到非安全内存。

对待存储数据进行加密的算法以及对待提取数据进行解密的算法可以根据实际需要进行选择，这里不作限制。

- 20 当数据安全存储或数据安全提取操作执行完毕后，还需要进行以下操作，确保数据安全存取流程的安全性：

- 安全存取任务生成数据安全存取结果并发送给安全监控任务，所述数据安全存取结果包括：参数三和参数四；其中参数三包括数据安全存取是否成功的指示消息，参数四为验证码 MAGIC_SECURE，该验证码是安全存取任务与安全监控任务事先约定的用于安全存取任务向安全监控任务进行合法性认证的验证码。
- 25

接收到数据安全存取结果之后，安全监控任务判断数据安全存取结果中的参数四的值是否是 MAGIC_SECURE，如果是，则安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证成功，此时，保存安全操作系统上下文，恢复非安全系统上下文，数据安全存取流程结束；如果否，安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证不成功，此时，安全监控任务本地保存错误信息，并向非安全操作系统返回处理失败的结果，数据安全存取流程结束。

实施例二

本发明实施例二提供了一种数据安全存取装置，位于终端上，如图 2 所示，所述装置包括：非安全操作系统 21 和安全操作系统 22；其中，

所述非安全操作系统 21，配置为接收第一数据安全存取请求；并根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统 22；

所述安全操作系统 22，配置为对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

其中，非安全操作系统 21 运行在处理器的非安全状态（例如，支持 Trust Zone 安全方法的 ARM 处理器包括两种状态：安全状态和非安全状态），只能访问非安全硬件（即，非安全存储器、非安全内存）。例如：运行在当前智能终端上的主流操作系统 Android，它用来满足用户在智能终端上多样的应用需求，由于该系统是开源、免费的，用户可以浏览网页、安装各种应用程序，所以系统的安全性不高，可能受到病毒或木马的攻击，导致安全数据的泄露或破坏。

安全操作系统 22 运行在处理器的安全状态，可以访问安全硬件（即，安全存储器 26、安全内存 25），也可以访问非安全硬件中的非安全内存 23，

专门用来处理安全级别高的任务，如存储与提取安全数据、安全数据的加解密、数字版权管理、VPN 管理等。它是精简、稳定的操作系统，安全操作系统中运行的安全任务是串行执行的，调度策略是非抢占式的，提高了系统内部的安全性和稳定性。

5 安全操作系统 22 包括安全存取任务模块 2201、安全监控任务模块 2202 和主控任务模块 2203；其中，

主控任务模块 2203 中运行的主控任务处于就绪或执行状态，该任务通过安全监控任务模块 2202 中安全监控任务传递的参数，创建相应的安全任务，完成用户需要的安全操作。安全应用需经过安全认证才能安装到该系
10 统中，保证了安全操作系统的外部安全性。安全存取任务模块 2201 中运行着安全侧存取任务。安全监控任务模块 2202，还负责安全操作系统 22 和非安全操作系统 21 之间的通信和切换，非安全操作系统 21 和安全操作系统 22 都可以通过执行一条特殊的指令，如 ARM 的 SMC 指令跳转到安全监控任务，SMC 指令的参数一和参数二用来保存非安全操作系统向安全操作系
15 统传递的参数。

当第一数据安全存取请求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径；

当第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径。

20 所述装置还可包括：非安全内存 23、非安全存储器 24、安全内存 25 及安全存储器 26，分别用于存储数据，包括安全数据和非安全数据；其中，安全存储器 26 和非安全存储器 24 均由存储器控制器控制实现；安全内存 25 和非安全内存 23 均由内存控制器控制实现。

所述非安全操作系统 21 包括非安全存取任务模块 2101，配置为将待存
25 储的数据从非安全存储器 24 中读到非安全内存 23 中。

所述非安全存取任务模块 2101，还配置为将以下参数一和参数二携带

在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识、数据存取信息，参数二包括验证码 MAGIC_NS。

所述合法性认证包括：第一次合法性认证和第二次合法性认证。

5 所述安全操作系统 22 中的安全监控任务模块 2202，配置为接收非安全操作系统 21 发送的第二数据安全存取请求，并通过以下方式对所述第二数据安全存取请求进行第一次合法性认证：安全监控任务模块 2202 判断所述第二数据安全存取请求中是否携带验证码 MAGIC_NS，如果是，则确定所述
10 第二数据安全存取请求第一次合法性认证成功；如果否，则确定所述第二数据安全存取请求第一次合法性失败；

 所述安全操作系统 22 中的主控任务模块 2203，配置为通过以下方式对所述第二数据安全存取请求进行第二次合法性认证：主控任务模块 2203 判断第二数据安全存取请求中参数一的各个参数是否合法，当所述参数一中各个参数均合法时，第二次合法性认证成功，否则，第二次合法性认证失
15 败。

 安全操作系统 22 中的安全存取任务模块 2201，配置为通过以下方式执行数据安全存取操作：

 当所述第二数据安全存取请求为数据安全存储请求时，安全存取任务模块 2201 执行以下操作：将已经存储在非安全内存 23 中的待存储数据复制
20 到安全内存 25，在安全内存 25 中对待存储数据进行加密操作，将加密后的待存储数据写入安全存储器 26；

 当所述第二数据安全存取请求为数据安全提取请求时，安全存取任务模块 2201 执行以下操作：将待提取数据从安全存储器 26 读到安全内存 25；在安全内存 25 中对待提取数据进行解密操作；将解密后的待提取数据复制
25 到非安全内存 23。

 所述非安全操作系统 21 还包括非安全侧文件系统 2102 和非安全侧底

层驱动 2103，配置为实现非安全操作系统 21 中的数据存取操作；

所述安全操作系统 22 还包括安全侧文件系统 2204 及安全侧底层驱动 2205，配置为实现安全操作系统 22 中的数据存取操作。

所述安全存取任务模块 2201 还配置为生成数据安全存取结果并发送给
5 安全监控任务模块 2202，所述数据安全存取结果包括：参数三和参数四；
其中，参数三包括数据安全存取是否成功的指示消息，参数四为验证码
MAGIC_SECURE；

所述安全监控任务模块 2202，还配置为通过以下方式对数据安全存取
结果的合法性进行验证：

10 安全监控任务模块 2202 判断数据安全存取结果中的参数四的值是否是
MAGIC_SECURE，如果是，则安全监控任务模块 2202 对安全存取任务模
块 2201 所发送的数据安全存取结果的合法性验证成功；如果否，安全监控
任务模块 2202 对安全存取任务模块 2201 所发送的数据安全存取结果的合
法性验证不成功。

15

下面通过具体示例，对本发明实施例所述方法作以下详细介绍。

本发明实施例提供的数据安全存储方法，在实际实现中，从整体上看，
如图 3 所示，主要包括以下几个步骤：

步骤 301：非安全侧数据存储任务启动；

20 步骤 302：选择需存储的数据；

步骤 303：将需存储的数据从非安全存储器读到非安全内存；

步骤 304：准备好存储任务相关参数并切换到安全操作系统；

步骤 305：安全侧判断存储任务相关参数是否合法；合法时，转至步骤
307 继续执行；当不合法时，转至步骤 306 继续执行；

25 步骤 306：向非安全侧返回错误信息，并跳出当前流程；

步骤 307：安全侧存储任务启动；

步骤 308: 指示用户输入密码, 并接收用户发送的密码;

步骤 309: 判断密码是否合法; 当不合法时, 转至步骤 310; 当合法时, 转至步骤 311;

步骤 310: 向非安全侧返回错误信息, 并跳出当前流程;

5 步骤 311: 执行数据安全存储流程。

该流程是包括: 将非安全内存中的文件复制到安全内存、将安全内存中的文件加密、将文件写到安全存储器、存储成功并返回非安全系统。

本发明实施例提供的数据安全提取方法, 在实际实现中, 从整体上看, 如图 4 所示, 主要包括以下几个步骤:

10 步骤 401: 非安全侧数据提取任务启动;

步骤 402: 准备好数据提取任务相关参数并切换到安全操作系统;

步骤 403: 判断所述数据提取任务相关参数是否合法; 当不合法时, 转至步骤 404 继续执行; 合法时, 转至步骤 405 继续执行;

步骤 404: 向非安全侧返回错误信息, 并跳出当前流程;

15 步骤 405: 安全侧安全数据提取任务启动;

步骤 406: 指示用户输入密码; 并接收用户发送的密码;

步骤 407: 判断密码是否合法; 当不合法时, 转至步骤 408; 当合法时, 转至步骤 409;

步骤 408: 向非安全侧返回错误信息, 并跳出当前流程;

20 步骤 409: 执行数据安全提取流程。

所述数据安全提取流程是包括: 将文件从安全存储器读到安全内存、将安全内存中的文件解密、将安全内存中的文件复制到非安全内存、准备参数并返回非安全操作系统、非安全侧存储任务启动、选择存储路径、将文件从非安全内存写入非安全存储器;

25 执行完以上流程后, 数据安全提取流程成功。

下面以数据安全存储流程为例, 对本发明实施例提供的数据安全存取

方法作以下详细介绍;

该示例包括以下步骤:

步骤 501: 处理器启动安全操作系统和非安全操作系统;

5 终端上电时, 处理器处于安全状态, 首先启动安全操作系统; 安全操作系统初始化, 创建主控任务并执行; 初始化非安全操作系统上下文, 并切换到安全监控任务; 安全监控保存安全操作系统上下文, 恢复非安全操作系统上下文, 启动非安全操作系统; 非安全操作系统初始化之后, 系统正常运行;

步骤 502: 用户发起安全存储请求;

10 用户打开终端中的安全存储应用程序, 选择待存储的文件, 并选择存储路径, 点击相应用于发起存储请求按钮;

步骤 503: 非安全存储器中的非安全存取任务响应用户的存储请求;

非安全存取任务从用户发起的存储请求中获取存储信息: 待存储的文件的文件名及存储路径;

15 步骤 504: 非安全存取任务如果是存储请求, 将非安全存储器中待存储的文件读到非安全内存中, 然后, 非安全存取任务准备好 SMC 指令参数, 切换到安全监控; 将安全存储命令 (包含任务标识: SECURE_SOURCE、操作标识: SECURE_SAVE、文件参数) 的地址存放到 SMC 指令的参数 1 中, 用于后续步骤中, 安全操作系统中安全存取任务执行数据存取操作时
20 使用; 将验证码 MAGIC_NS 存放到 SMC 指令的参数 2 中, 用于安全监控验证 SMC 指令的合法性; 之后, 切换到安全监控任务;

步骤 505: 安全监控任务验证 SMC 指令中参数的合法性;

安全监控任务首先检查 SMC 指令中参数 2 的值是否是 MAGIC_NS, 若不是, SMC 参数验证失败, 将错误信息保存到 CMD 中, 返回到非安全
25 操作系统处理失败的结果, 此步骤结束; 若是, SMC 参数验证成功, 保存 SMC 指令的参数 1 的值到指定的全局变量 para_cmd 中, 发送给安全操作系

统的主控任务，并保存非安全上下文，恢复安全上下文，此步骤结束；

步骤 506: 主控任务获取安全监控任务传递的 para_cmd 参数，验证参数的合法性；

主控任务验证 para_cmd 参数的合法性，具体为验证任务标识、操作标识和文件参数的取值是否符合要求，即，确定 para_cmd 参数是否为合法的取值，若各参数均合法，根据 CMD 中的任务标识 SECURE_SOURCE 创建安全存取任务，此步骤结束；否则，para_cmd 参数验证失败，将错误信息保存到 CMD 中，切换到安全监控，返回非安全操作系统处理失败的结果，此步骤结束；

10 步骤 507: 安全存取任务运行；

步骤 508: 对用户进行身份认证；

指示用户需输入密码（初次使用数据安全存取功能时，需设置初始密码），验证密码合法性；用于安全文件的存储或提取；

15 即，确定用户输入的密码是否为本地保存的密码；如果是，则用户身份认证成功，如果否，则用户身份认证失败；

首次使用时，用户设置初始密码后，直接登录系统执行数据安全存取操作；安全存取任务加密用户设置的初始密码并保存于本地，用于用户下次发起数据存储或提取请求时，验证用户身份。

步骤 509: 用户选择待存储文件的存储路径，并点击确认；

20 步骤 510: 安全存取任务从非安全内存中将待存储文件的加密存储到安全存储器中；

安全存取任务将非安全内存中的待存储文件的复制到安全内存，在安全内存中对待存储文件的进行加密操作，并将加密后的文件写入安全存储器；

25 步骤 511: 安全存取任务将数据安全存储结果保存到 SMC 指令中，设置 SMC 参数，并切换到安全监控；

所述数据安全存储结果包括参数 3 和参数 4:

其中, 参数 3 包括指示数据安全存储任务是否成功的信息, 参数 4 包括验证码 MAGIC_SECURE;

步骤 512: 安全监控验证 SMC 指令中参数的合法性;

5 检查 SMC 指令的参数 2 的值是否是 MAGIC_SECURE, 若不是, SMC 参数验证失败, 将错误信息保存到 CMD 中, 回到安全操作系统处理失败的结果, 此步骤结束; 若是, SMC 参数验证成功, 保存安全操作系统上下文, 恢复非安全系统上下文, 此步骤结束;

10 步骤 513: 非安全存取任务处理传回的参数, 针对待存储文件的安全存储流程完成;

存储任务完成后, 非安全存取任务还可以切换到其他应用执行其它处理。

在具体实施过程中, 上述非安全操作系统 21 和安全操作系统 22、非安全存取任务模块 2101、安全监控任务模块 2202、主控任务模块 2203、安全存取任务模块 2201、非安全侧文件系统 2102、非安全侧底层驱动 2103、安全侧文件系统 2204 及安全侧底层驱动 2205 可以由终端内的中央处理器 (CPU, Central Processing Unit)、微处理器 (MPU, Micro Processing Unit)、数字信号处理器 (DSP, Digital Signal Processor) 或可编程逻辑阵列 (FPGA, Field - Programmable Gate Array) 来实现。

本发明实施例还提供了一种计算机存储介质, 所述存储介质包括一组计算机可执行指令, 所述指令用于执行本发明实施例所述的数据安全存取方法。

本领域内的技术人员应明白, 本发明的实施例可提供为方法、系统、25 或计算机程序产品。因此, 本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且, 本发明可采用在一个或多个其

中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

5 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功
10 能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

15 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

20 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

权利要求书

1、一种数据安全存取方法，所述方法包括：

非安全操作系统接收第一数据安全存取请求；

非安全操作系统根据所述第一数据安全存取请求生成第二数据安全
5 存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；

安全操作系统对所述第二数据安全存取请求进行合法性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

2、根据权利要求1所述的方法，其中，当所述第一数据安全存取请
10 求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径，

当所述第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径。

15 3、根据权利要求2所述的方法，其中，当所述第一数据安全存取请求为数据安全存储请求时，所述方法还包括：所述非安全操作系统中的非安全存取任务将待存储的数据从非安全存储器中读到非安全内存中。

4、根据权利要求3所述的方法，其中，所述非安全操作系统根据所述第一数据安全存取请求生成第二数据安全存取请求，包括：

20 非安全操作系统中的非安全存取任务将以下参数一和参数二携带在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识、数据存取信息，参数二包括验证码MAGIC_NS。

5、根据权利要求4所述的方法，其中，所述合法性认证包括：第一次
25 合法性认证和第二次合法性认证；

其中，所述第一次合法性认证，包括：安全操作系统中的安全监控任务判断所述第二数据安全存取请求中是否携带验证码 MAGIC_NS，如果是，则确定所述第二数据安全存取请求第一次合法性认证成功；如果否，则确定所述第二数据安全存取请求第一次合法性失败；

- 5 所述第二次合法性认证包括：所述安全操作系统中的主控任务判断所述参数一中的各个参数是否合法，当所述参数一中各个参数均合法时，第二次合法性认证成功，否则，第二次合法性认证失败。

6、根据权利要求 1 至 5 中任一项所述的方法，其中，所述安全操作系统根据所述第二数据安全存取请求执行数据安全存取操作，包括：

- 10 当所述第二数据安全存取请求为数据安全存储请求时，安全存取任务执行以下操作：将已经存储在非安全内存中的待存储数据复制到安全内存，在安全内存中对待存储数据进行加密操作，将加密后的待存储数据写入安全存储器；

- 15 当所述第二数据安全存取请求为数据安全提取请求时，安全存取任务执行以下操作：将待提取数据从安全存储器读到安全内存；在安全内存中对待提取数据进行解密操作；将解密后的待提取数据复制到非安全内存。

7、根据权利要求 6 所述的方法，其中，所述安全操作系统根据所述第二数据安全存取请求执行数据安全存取操作之后，所述方法还包括：

- 20 安全操作系统中的安全存取任务生成数据安全存取结果并发送给安全操作系统中的安全监控任务，所述数据安全存取结果包括：参数三和参数四；其中参数三包括数据安全存取是否成功的指示消息，参数四为验证码 MAGIC_SECURE；

- 25 所述安全监控任务判断数据安全存取结果中的参数四的值是否是 MAGIC_SECURE，如果是，则安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证成功，数据安全存取流程结束；如果否，

安全监控任务对安全存取任务所发送的数据安全存取结果的合法性验证不成功，安全监控任务向非安全操作系统返回处理失败的结果，数据安全存取流程结束。

8、一种数据安全存取装置，所述装置包括：非安全操作系统和安全
5 操作系统；其中，

所述非安全操作系统，配置为接收第一数据安全存取请求；并根据所述第一数据安全存取请求生成第二数据安全存取请求之后，将所述第二数据安全存取请求发送给安全操作系统；

所述安全操作系统，配置为对所述第二数据安全存取请求进行合法性
10 性认证，当合法性认证成功时，根据所述第二数据安全存取请求执行数据安全存取操作。

9、根据权利要求 8 所述的装置，其中，当所述第一数据安全存取请求为数据安全存储请求时，所述第一数据安全存取请求中包括以下数据存取信息：待存储数据的文件名、及其存储路径，

15 当所述第一数据安全存取请求为数据安全提取请求时，所述第一数据安全存取请求中包括以下数据存取信息：待提取数据的文件名及其提取路径。

10、根据权利要求 9 所述的装置，其中，所述非安全操作系统包括非安全存取任务模块，配置为将待存储的数据从非安全存储器中读到非
20 安全内存中。

11、根据权利要求 10 所述的装置，其中，所述非安全存取任务模块，还配置为将以下参数一和参数二携带在所述第一数据安全存取请求中，生成第二数据安全存取请求：

其中，参数一包括任务标识、操作标识、数据存取信息，参数二包
25 括验证码 MAGIC_NS。

12、根据权利要求 11 所述的装置，其中，所述合法性认证包括：第

一次合法性认证和第二次合法性认证;

所述安全操作系统包括安全监控任务模块和主控任务模块; 其中,

所述安全监控任务模块, 配置为接收非安全操作系统发送的第二数据安全存取请求, 并通过以下方式对所述数据安全存取请求进行第一次
5 合法性认证: 安全监控任务模块判断所述第二数据安全存取请求中是否携带验证码 MAGIC_NS, 如果是, 则确定所述第二数据安全存取请求第一次合法性认证成功; 如果否, 则确定所述第二数据安全存取请求第一次合法性失败;

所述主控任务模块, 配置为通过以下方式对所述第二数据安全存取
10 请求进行第二次合法性认证: 主控任务模块判断第二数据安全存取请求中参数一中的各个参数是否合法, 当所述参数一中各个参数均合法时, 第二次合法性认证成功, 否则, 第二次合法性认证失败。

13、根据权利要求 12 所述的方法, 其中, 安全操作系统还包括安全存取任务模块, 配置为通过以下方式执行数据安全存取操作:

15 当所述第二数据安全存取请求为数据安全存储请求时, 安全存取任务模块执行以下操作: 将已经存储在非安全内存中的待存储数据复制到安全内存, 在安全内存中对待存储数据进行加密操作, 将加密后的待存储数据写入安全存储器;

20 当所述第二数据安全存取请求为数据安全提取请求时, 安全存取任务模块执行以下操作: 将待提取数据从安全存储器读到安全内存; 在安全内存中对待提取数据进行解密操作; 将解密后的待提取数据复制到非安全内存。

14、根据权利要求 13 所述的装置, 其中, 所述安全存取任务模块, 还配置为生成数据安全存取结果并发送给安全监控任务模块, 所述数据安全存取结果包括: 参数三和参数四; 其中参数三包括数据安全存取是否成功的指示消息, 参数四为验证码 MAGIC_SECURE;

所述安全监控任务模块，还配置为通过以下方式对数据安全存取结果的合法性进行验证：

安全监控任务模块判断数据安全存取结果中的参数四的值是否是MAGIC_SECURE，如果是，则安全监控任务模块对安全存取任务模块所发送的数据安全存取结果的合法性验证成功；如果否，安全监控任务模块对安全存取任务模块所发送的数据安全存取结果的合法性验证不成功。

15、一种计算机存储介质，所述存储介质包括一组计算机可执行指令，所述指令用于执行权利要求 1 至 7 任一项所述的数据安全存取方法。

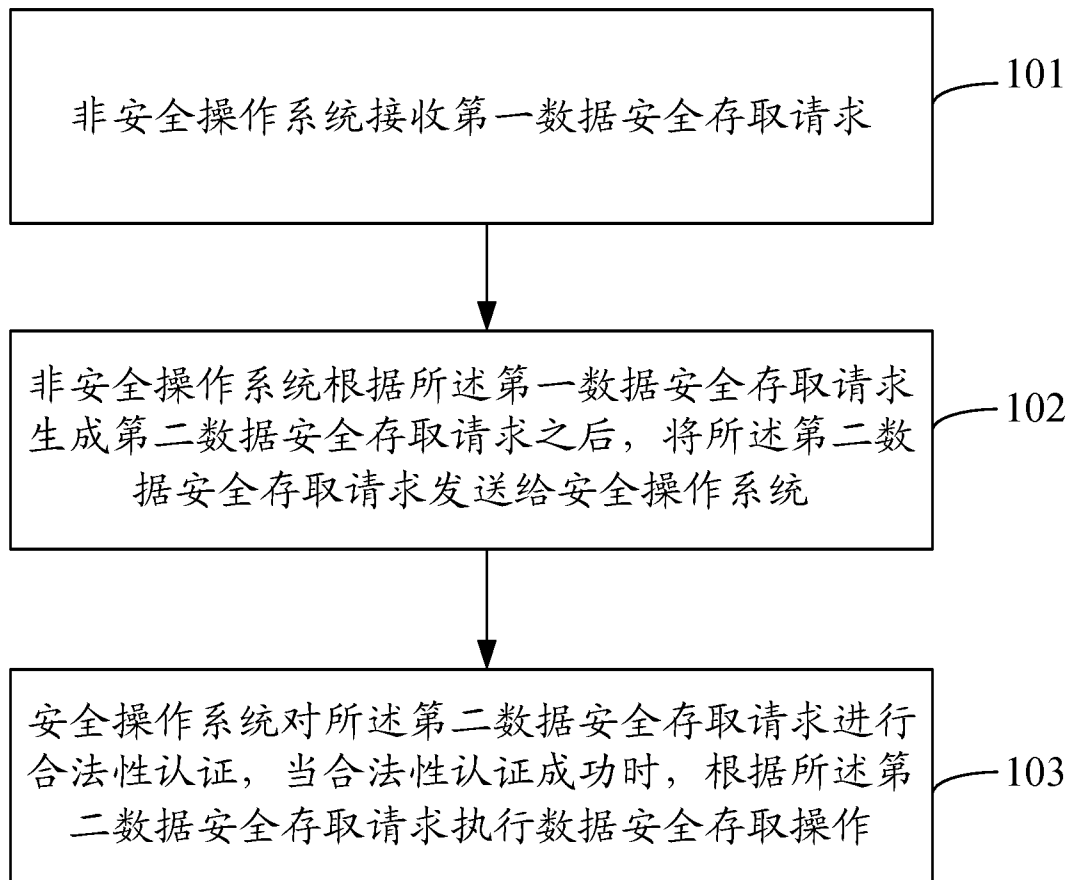


图 1

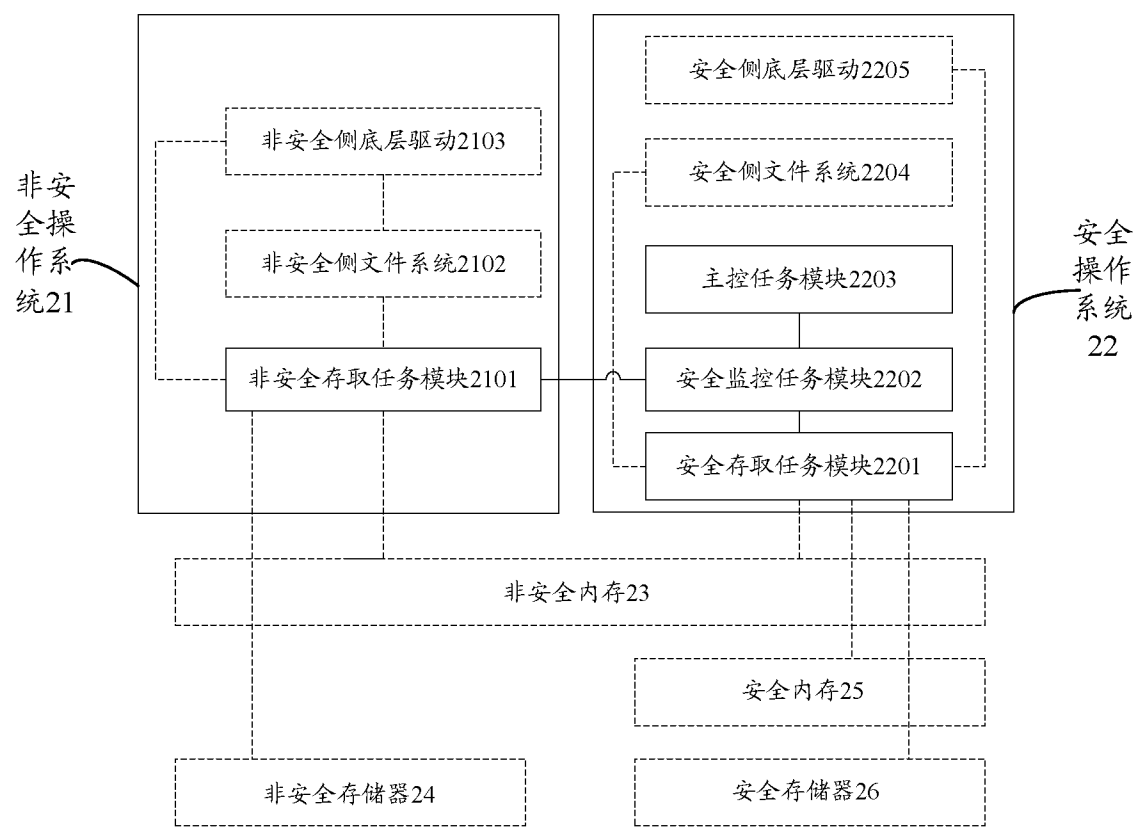


图 2

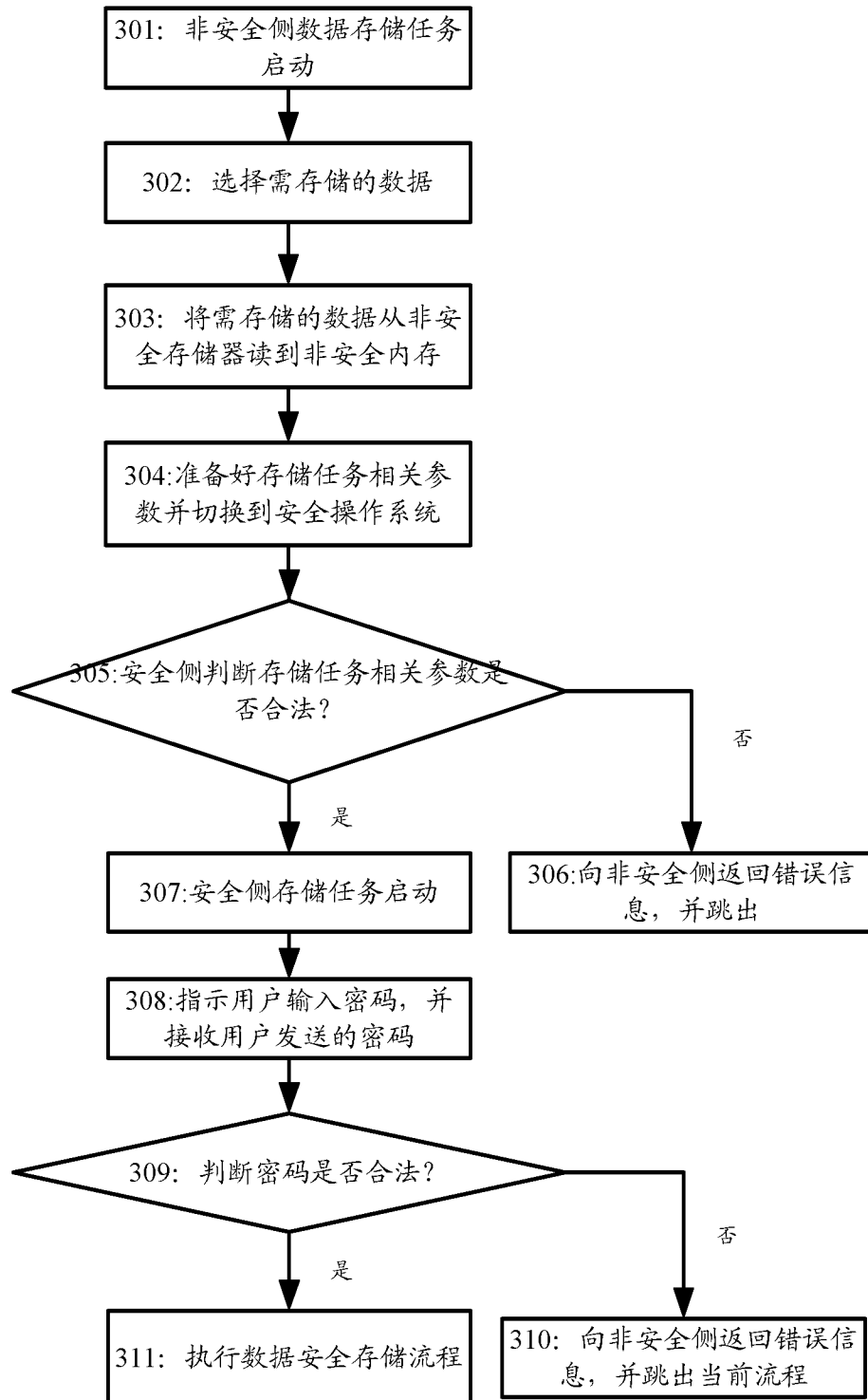


图 3

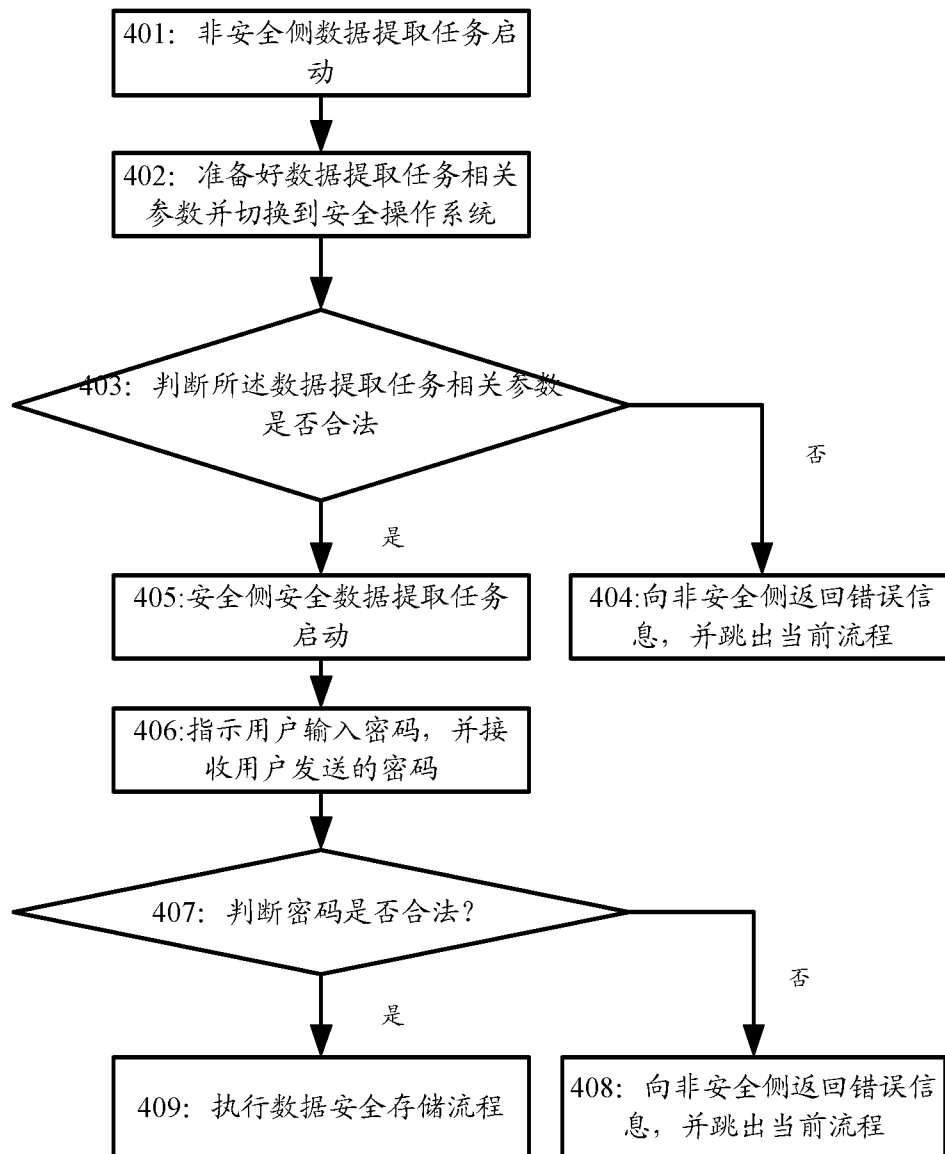


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/081962

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

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, IEEE: OS, operating system, identification, safe, authenticat? security, user request, security region, name, path, access, non-safe

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104102876 A (WATCHDATA SYSTEM CO., LTD.) 15 October 2014 (15.10.2014) description, paragraphs [0045]-[0089], [0094]	1-3, 8-10, 15
X	CN 101281506 A (ARM CO., LTD.) 08 October 2008 (08.10.2008) description, page 11, the third paragraph to page 13, the second paragraph	1-3, 8-10, 15
X	CN 103714459 A (UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA) 09 April 2014 (09.04.2014) description, paragraphs [0087]-[0101]	1-3, 8-10, 15
A	CN 103621009 A (SK PLANET CO., LTD.) 05 March 2014 (05.03.2014) description, paragraphs [0059]-[0117]	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
14 August 2015

Date of mailing of the international search report
26 August 2015

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
LIU, Xu
Telephone No. (86-10) 82245207

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/081962

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104102876 A	15 October 2014	None	
CN 101281506 A	08 October 2008	US 2008250217 A1	09 October 2008
		GB 2448151 A	08 October 2008
		JP 2008257734 A	23 October 2008
CN 103714459 A	09 April 2014	None	
CN 103621009 A	05 March 2014	JP 2014519674 A	14 August 2014
		EP 2874345 A1	20 May 2015
		WO 2013191325 A1	27 December 2013
		US 2014090041 A1	27 March 2014
		KR 20130143263 A	31 December 2013
		SG 195656 A1	29 January 2014

国际检索报告

国际申请号

PCT/CN2015/081962

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

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, IEEE: 安全, 存取, 操作系统, 非安全, 认证, 文件名, 路径, OS, operating system, identification, safe, authenticat? security, user request, security region, name, path

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 104102876 A (北京握奇智能科技有限公司) 2014年 10月 15日 (2014 - 10 - 15) 说明书第45-89、94段	1-3, 8-10, 15
X	CN 101281506 A (ARM有限公司) 2008年 10月 8日 (2008 - 10 - 08) 说明书第11页第3段-第13页第2段	1-3, 8-10, 15
X	CN 103714459 A (电子科技大学) 2014年 4月 9日 (2014 - 04 - 09) 说明书第87-101段	1-3, 8-10, 15
A	CN 103621009 A (SK 普兰尼特有限公司) 2014年 3月 5日 (2014 - 03 - 05) 说明书第59-117段	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

2015年 8月 14日

国际检索报告邮寄日期

2015年 8月 26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)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

授权官员

刘栩

电话号码 (86-10)82245207

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/081962

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	104102876	A	2014年 10月 15日	无			
CN	101281506	A	2008年 10月 8日	US	2008250217	A1	2008年 10月 9日
				GB	2448151	A	2008年 10月 8日
				JP	2008257734	A	2008年 10月 23日
CN	103714459	A	2014年 4月 9日	无			
CN	103621009	A	2014年 3月 5日	JP	2014519674	A	2014年 8月 14日
				EP	2874345	A1	2015年 5月 20日
				WO	2013191325	A1	2013年 12月 27日
				US	2014090041	A1	2014年 3月 27日
				KR	20130143263	A	2013年 12月 31日
				SG	195656	A1	2014年 1月 29日

表 PCT/ISA/210 (同族专利附件) (2009年7月)