(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
2015 年 12 月 30 日 (30.12.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/196890 A1

(51) 国际专利分类号:
G06F 12/14 (2006.01)

(21) 国际申请号: PCT/CN2015/079945

(22) 国际申请日: 2015 年 5 月 27 日 (27.05.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410284498.9 2014 年 6 月 23 日 (23.06.2014) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 李熠斌 (LI, Yibin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, 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))。

(54) Title: SECURITY ACCESS CONTROL METHOD FOR HARD DISK, AND HARD DISK

(54) 发明名称 : 硬盘安全访问控制方法和硬盘

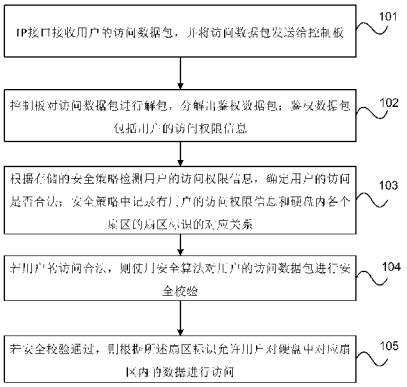


图 1 / Fig. 1

101 Receiving, by an IP interface, an access data packet of a user, and sending the access data packet to a control panel
102 Unpacking, by the control panel, the access data packet, so as to decompose an authentication data packet, the authentication data packet comprising access permission information about the user
103 According to a stored security policy, detecting the access permission information about the user, so as to determine whether the access of the user is valid, the access permission information about the user and the correlation between sector identifiers of various sectors in a hard disk being recorded in the security policy
104 If the access of the user is valid, conducting a security check on the access data packet of the user using a security algorithm
105 If the security check has passed, according to the sector identifiers, permitting the user to access data in the corresponding sectors in the hard disk

(57) Abstract: Provided are a security access control method for a hard disk, and a hard disk. In the security access control method for a hard disk of the present invention, the hard disk comprises an IP interface and a control panel. The method comprises: receiving, by an IP interface, an access data packet of a user, and sending the access data packet to a control panel; unpacking, by the control panel, the access data packet, so as to decompose an authentication data packet, the authentication data packet comprising access permission information about the user; according to a stored security policy, detecting the access permission information about the user, so as to determine whether the access of the user is valid, the access permission information about the user and the correlation between sector identifiers of various sectors in a hard disk being recorded in the security policy; if the access of the user is valid, conducting a security check on the access data packet of the user using a security algorithm; and if the security check has passed, according to the sector identifiers, permitting the user to access data in the corresponding sectors in the hard disk. The embodiments of the present invention improve the security of accessing a hard disk.

(57) 摘要: 本发明实施例提供一种硬盘安全访问控制方法和硬盘。本发明硬盘安全访问控制方法，硬盘包括 IP 接口和控制板，所述方法包括：IP 接口接收用户的访问数据包，并将访问数据包发送给控制板；控制板对访问数据包进行解包，分解出鉴权数据包；鉴权数据包包括用户的访问权限信息；根据存储的安全策略检测所述用户的访问权限信息，确定用户的访问是否合法；安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；若用户的访问合法，则使用安全算法对用户的访问数据包进行安全校验；若安全校验通过，则根据扇区标识允许用户对硬盘中对应扇区内的数据进行访问。本发明实施例提高了对硬盘访问的安全性。

WO 2015/196890 A1

硬盘安全访问控制方法和硬盘

技术领域

本发明实施例涉及计算机技术领域，尤其涉及一种硬盘安全访问控制方法和硬盘。

背景技术

现有的硬盘数据访问控制技术是基于上层应用和上层设备的，例如在存储设备中，普通的块设备存储把磁盘整合为一个独立冗余磁盘阵列（Redundant Array of Independent Disks，简称 RAID）组，在 RAID 上划分出条带，在条带上划分出逻辑单元（Logic Unit，简称 LUN）然后映射给上层主机，主机层通过文件系统或者其他设备系统管理存储数据（例如使用设备的数据库）；或者硬盘直接安装在简单的计算机系统中，操作系统通过文件系统对硬盘上的数据存放和访问方式提供管理。

现有的分布式存储 Key-Value 存储系统是一种基于对象的存储系统，在该存储系统中，把所有的数据划分成小的对象，然后基于散列算法存放到分布式哈希表(Distributed Hash Table，简称 DHT)环的几个位置，这样用户可以通过 Key 来找到对象所对应的数据，对数据实现访问。该存储系统可以实现多个用户对同一套存储系统的同时访问，为了实现多个用户的数据访问隔离，保护数据的安全，该系统会在用户访问的接口上实现一个逻辑层，该逻辑层可以让不同用户能够且只能够访问自己所被分配的数据范围，而不能访问其他用户的数据。

现有技术的 Key-Value 存储设备的实现原理其实也是一种逻辑的隔离。逻辑设计上具有不安全性：通过系统中的用户管理层实现对所有用户访问的管理，必须确保用户的访问接口是唯一并且安全的，用户的访问必须通过该接口鉴权以后才能获得对相关数据的访问；如果系统的访问接口不唯一，一样可以访问到所有用户的数据，或者系统存在相关漏洞后，任何数据都是可以被访问的。

发明内容

本发明实施例提供一种硬盘安全访问控制方法和硬盘，以解决现有技术中对硬盘访问的安全问题。

第一方面，本发明实施例提供一种硬盘安全访问控制方法，所述硬盘包括 IP 接口和控制板，所述方法包括：

所述 IP 接口接收用户的访问数据包，并将所述访问数据包发送给所述控制板；

所述控制板对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；

根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；

若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；

若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

结合第一方面，在第一方面的第一种实现方式中所述根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法，包括：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

结合第一方面、或第一方面的第一种实现方式，在第一方面的第二种实现方式中，所述方法，还包括：

预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

结合第一方面的第二种实现方式，在第一方面的第三种实现方式中，所述使用安全算法对所述用户的访问数据包进行安全校验，包括：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验。

结合第一方面、或第一方面的第一~第三任一种实现方式，在第一方面的第四种实现方式中，当多个所述硬盘提供数据给同一个用户时，各个所述硬

盘通过相同的所述安全算法对所述用户的访问数据包进行安全校验；或，各个所述硬盘通过不同的所述安全算法对所述用户的访问数据包进行安全校验。

第二方面，本发明实施例提供一种硬盘，包括 IP 接口和控制板，

所述 IP 接口，用于接收用户的访问数据包，并将所述访问数据包发送给所述控制板；

所述控制板，包括：

解包模块，用于对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；

检测模块，用于根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；

安全校验模块，用于若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；

访问执行模块，用于若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

结合第二方面，在第二方面的第一种实现方式中，所述检测模块，具体用于：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

结合第二方面、或第二方面的第一种实现方式，在第二方面的第二种实现方式中，所述控制板，还包括：

安全策略建立模块，用于预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

结合第二方面的第二种实现方式，在第二方面的第三种实现方式中，所述安全校验模块，具体用于：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验。

本发明实施例硬盘安全访问控制方法和硬盘，所述硬盘包括 IP 接口和控制板，通过所述 IP 接口接收用户的访问数据包，并将所述访问数据包发送给所述控制板；所述控制板对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问，实现了用户对硬盘访问的安全控制，提高了访问的安全性，解决了现有技术中对硬盘访问的安全问题。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍。

图 1 为本发明硬盘安全访问控制方法实施例一的流程图；

图 2 为本发明硬盘安全访问控制方法实施例一的安全访问控制层的逻辑架构示意图；

图 3 为本发明硬盘实施例一的结构示意图；

图 4 为本发明硬盘实施例二的结构示意图；

图 5 为本发明硬盘设备实施例的结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

图 1 为本发明硬盘安全访问控制方法实施例一的流程图，图 2 为本发明硬盘安全访问控制方法实施例一的安全访问控制层的逻辑架构示意图，本实施例的执行主体为智能硬盘，例如是基于 IP 接口的硬盘。所述硬盘可以通过

软件和硬件实现。如图 1 所示，所述硬盘包括 IP 接口和控制板，本实施例的方法可以包括：

步骤 101、IP 接口接收用户的访问数据包，并将访问数据包发送给控制板。

步骤 102、控制板对访问数据包进行解包，分解出鉴权数据包；鉴权数据包包括用户的访问权限信息。

具体地，例如在基于 IP 接口的硬盘中，硬盘通过 IP 接口实现对外的数据访问，那么该硬盘的 IP 接口具备类似计算机网络节点的链接性，硬盘本身也具备一定的计算能力，本发明在硬盘控制板上设置安全芯片，该安全芯片对硬盘每个扇区（不同的扇区可以对应不同的用户）实现加密和权限验证，基于该控制板上芯片的计算和存储能力实现对本硬盘所有访问的鉴权，所有不合法的访问都不会被执行。

现有的对硬盘中数据的访问控制都在上层的逻辑层次对访问进行控制，若通过鉴权则所有上层下发到硬盘的读写命令都会被执行没有任何制约。而本发明的硬盘安全访问控制是在硬盘上实现的，如图 2 所示，通过安全访问控制层对用户的访问进行鉴权，经过鉴权的访问可以执行，如果不能通过，硬盘会拒绝访问。

在硬盘的控制板上使用计算芯片和存储芯片实现“安全访问控制层”，计算芯片、存储芯片和安全芯片可以通过同一个芯片实现，也可以是几个不同的芯片实现的，如图 2 所示，安全访问控制层在硬盘的 I/O 处理路径上，由四个主要的层次决定：安全访问协议解包层、扇区标识表库层、算法库层和访问执行层，访问执行层之后还包括硬盘读写实现层，该层可以采用现有的硬盘对读写的实现方式，步骤 102 可以在安全访问协议解包层上实现，对用户的访问数据包进行解包，把访问数据包中包含有用户的访问权限信息的鉴权数据包分解出来，给下层使用。

步骤 103、根据存储的安全策略检测用户的访问权限信息，确定用户的访问是否合法；安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系。

具体地，步骤 103 可以在扇区标识表库层上实现，访问权限信息例如包括用户可以访问的扇区的扇区标识、用户使用的安全算法等；安全策略中记

录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系，所述对应关系如用户 1 的访问权限对应扇区标识 1，用户 2 的访问权限对应扇区标识 2 等，则可以根据安全策略中的对应关系检测确定访问权限信息确定用户的访问是否合法，如访问权限信息中的扇区标识与该访问权限信息与扇区标识的对应关系中的扇区标识一致，则认为是合法的，否则不合法。

步骤 104、若用户的访问合法，则使用安全算法对用户的访问数据包进行安全校验。

具体地，步骤 104 可以在算法库层上实现，若检测到用户的访问合法，则使用安全算法对用户的访问数据包进行安全校验，可以使用现有技术中的校验方式进行校验。算法库层存储对用户的访问进行安全校验的安全算法。

步骤 105、若安全校验通过，则根据所述扇区标识允许用户对硬盘中对应扇区内的数据进行访问。

具体地，步骤 105 可以在访问执行层上实现，若安全校验通过，则允许用户对硬盘中对应扇区内的数据进行访问。

本发明实施例实现硬盘内最终数据存放用户的真正安全隔离。

本发明是完全基于最终用户，而非面对使用该硬盘的任何设备和逻辑层次，具有设备无关性和逻辑独立性；该架构结构简单，容易实现。

本实施例的硬盘包括固态硬盘以及其他存储设备，或增加 IP 接口和安全芯片的传统硬盘。

本实施例，所述硬盘包括 IP 接口和控制板，通过所述 IP 接口接收用户的访问数据包，并将所述访问数据包发送给所述控制板；所述控制板对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问，实现了用户对硬盘访问的安全控制，提高了访问的安全性，解决了现有技术中对硬盘访问的安全问题。

在本发明硬盘安全访问控制方法实施例二中，在方法实施例一的基础上，

本实施例的方法，根据存储的安全策略检测用户的访问权限信息，确定用户的访问是否合法，包括：

将用户的访问权限信息与对应关系中的用户的访问权限信息进行匹配；若匹配成功，则用户的访问合法；若匹配不成功，则用户的访问不合法。

具体地，可以在扇区标识表库层上实现对本硬盘中所有的扇区进行标识，设置不同的扇区标识与用户的访问权限的对应关系，如用户 1 的访问权限对应扇区标识 1，用户 2 的访问权限对应扇区标识 2 等，将所述用户的访问权限信息与硬盘内各个扇区的扇区标识对应的用户的访问权限信息进行匹配，通过匹配可以实现不同用户的访问隔离。

可选地，所述方法，还包括：

预先在所述控制板中建立用户对应的计算策略，计算策略为对用户的访问数据包进行安全校验时使用安全算法的策略。

可选地，使用安全算法对用户的访问数据包进行安全校验，包括：

对于用户的每次访问，根据所述计算策略选择不同的安全算法或不同的安全算法的组合对访问数据包进行安全校验。

具体地，在算法库层中，可以建立用户对应的计算策略，可以对存储的多个安全算法实现策略的管理，可以指定不同的算法管理不同的扇区，在基于磁盘的多用户系统中，各个用户可以选择特定的算法来管理自己的数据区域；还可以对一些特定的区域实现多个不同算法的重叠校验，以增加安全性。

对于用户的每次访问，通过计算策略可以选择不同的安全算法或不同的安全算法的组合对访问数据包进行安全校验。即对于用户的每次访问使用的安全算法可以是“一次性”，也可以是“多次性”；其中，“一次性”是指一次有效，即每次访问使用的安全算法不同，多次性是指多次访问使用的安全算法相同，一次性可以实现比较高的安全度。

可选地，当多个所述硬盘提供数据给同一个用户时，各个所述硬盘通过相同的所述安全算法对所述用户的访问数据包进行安全校验；或，各个所述硬盘通过不同的所述安全算法对所述用户的访问数据包进行安全校验。

具体地，当多个硬盘提供数据给同一个用户时，多个硬盘可以只提供硬盘存储能力中的部分扇区去组成该用户的私有存储空间，那么对每块硬盘的数据访问控制可以通过同样的安全算法实现，也可以通过不同的安全算法实

现，这可以由算法库层中的安全策略来实现。

本实施例，可以实现以硬盘的磁头的访问扇区为最小粒度的隔离和安全，也是说，支持的用户数量在逻辑上是可以达到一个硬盘内所有正常访问的扇区数目为极限（一个用户对应一个扇区）。多个硬盘可以对等加密，实现对同一用户使用相同的安全算法；或不对等的加密，实现对同一用户使用不同的算法，最终实现了用户对硬盘访问的安全控制，提高了访问的安全性，解决了现有技术中对硬盘访问的安全问题。

图 3 为本发明硬盘实施例一的结构示意图，如图 3 所示，本实施例的硬盘 30，包括 IP 接口 31 和控制板 32，所述 IP 接口 31，用于接收用户的访问数据包，并将所述访问数据包发送给所述控制板；

所述控制板 32，包括：解包模块 301、检测模块 302、安全校验模块 303 和访问执行模块 304，其中，解包模块 301，用于对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；检测模块 302，用于根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；安全校验模块 303，用于若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；访问执行模块 304，用于若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

本实施例的硬盘，可以用于执行图 1 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 4 为本发明硬盘实施例二的结构示意图，如图 4 所示，本实施例的硬盘在图 3 所示硬盘结构的基础上，进一步地，检测模块 302，具体用于：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

可选地，所述控制板 32，还包括：

安全策略建立模块 305，用于预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

可选地，安全校验模块 303，具体用于：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验。

本实施例的硬盘，可以用于执行方法实施例二的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 5 为本发明硬盘设备实施例的结构示意图。如图 5 所示，本实施例提供的硬盘设备 50 包括 IP 接口 501 和控制板 502，其中控制板 502 包括处理器 5020 和存储器 5021；其中，IP 接口 501 用于接收用户的访问数据包，并将所述访问数据包发送给所述控制板；存储器 5021 存储数据和执行指令，当硬盘设备 50 运行时，处理器 5020 与存储器 5021 之间通信，处理器 5020 调用存储器 5021 中的执行指令，用于执行以下操作：

对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；

根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；

若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；

若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

可选地，所述处理器 5020，还用于：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

可选地，所述处理器 5020，还用于：

预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

可选地，所述处理器 5020，还用于：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验。

可选地，所述处理器 5020，还用于：

当多个所述硬盘提供数据给同一个用户时，各个所述硬盘通过相同的所述安全算法对所述用户的访问数据包进行安全校验；或，各个所述硬盘通过不同的所述安全算法对所述用户的访问数据包进行安全校验。

本实施例的硬盘设备，用于执行任一方法实施例所述的技术方案，其实现原理和技术效果类似，此处不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述单元或模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或模块可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，设备或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权 利 要 求 书

1、一种硬盘安全访问控制方法，所述硬盘包括 IP 接口和控制板，其特征在于，所述方法包括：

所述 IP 接口接收用户的访问数据包，并将所述访问数据包发送给所述控制板；

所述控制板对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；

根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；

若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；

若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

2、根据权利要求 1 所述的方法，其特征在于，所述根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法，包括：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

3、根据权利要求 1-2 任一项所述的方法，其特征在于，所述方法，还包括：

预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

4、根据权利要求 3 所述的方法，其特征在于，所述使用安全算法对所述用户的访问数据包进行安全校验，包括：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，当多个所述硬盘提供数据给同一个用户时，各个所述硬盘通过相同的所述安全算法对所述用

户的访问数据包进行安全校验；或，各个所述硬盘通过不同的所述安全算法对所述用户的访问数据包进行安全校验。

6、一种硬盘，所述硬盘包括 IP 接口和控制板，其特征在于，

所述 IP 接口，用于接收用户的访问数据包，并将所述访问数据包发送给所述控制板；

所述控制板，包括：

解包模块，用于对所述访问数据包进行解包，分解出鉴权数据包；所述鉴权数据包包括用户的访问权限信息；

检测模块，用于根据存储的安全策略检测所述用户的访问权限信息，确定所述用户的访问是否合法；所述安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系；

安全校验模块，用于若所述用户的访问合法，则使用安全算法对所述访问数据包进行安全校验；

访问执行模块，用于若所述安全校验通过，则根据所述扇区标识允许所述用户对硬盘中对应扇区内的数据进行访问。

7、根据权利要求 6 所述的硬盘，其特征在于，所述检测模块，具体用于：

将所述用户的访问权限信息与所述对应关系中的用户的访问权限信息进行匹配；若匹配成功，则所述用户的访问合法；若匹配不成功，则所述用户的访问不合法。

8、根据权利要求 6-7 任一项所述的硬盘，其特征在于，所述控制板，还包括：

安全策略建立模块，用于预先在所述控制板中建立所述用户对应的计算策略，所述计算策略为对所述用户的访问数据包进行安全校验时使用安全算法的策略。

9、根据权利要求 8 所述的硬盘，其特征在于，所述安全校验模块，具体用于：

对于所述用户的每次访问，根据所述计算策略选择不同的所述安全算法或不同的所述安全算法的组合对所述访问数据包进行安全校验

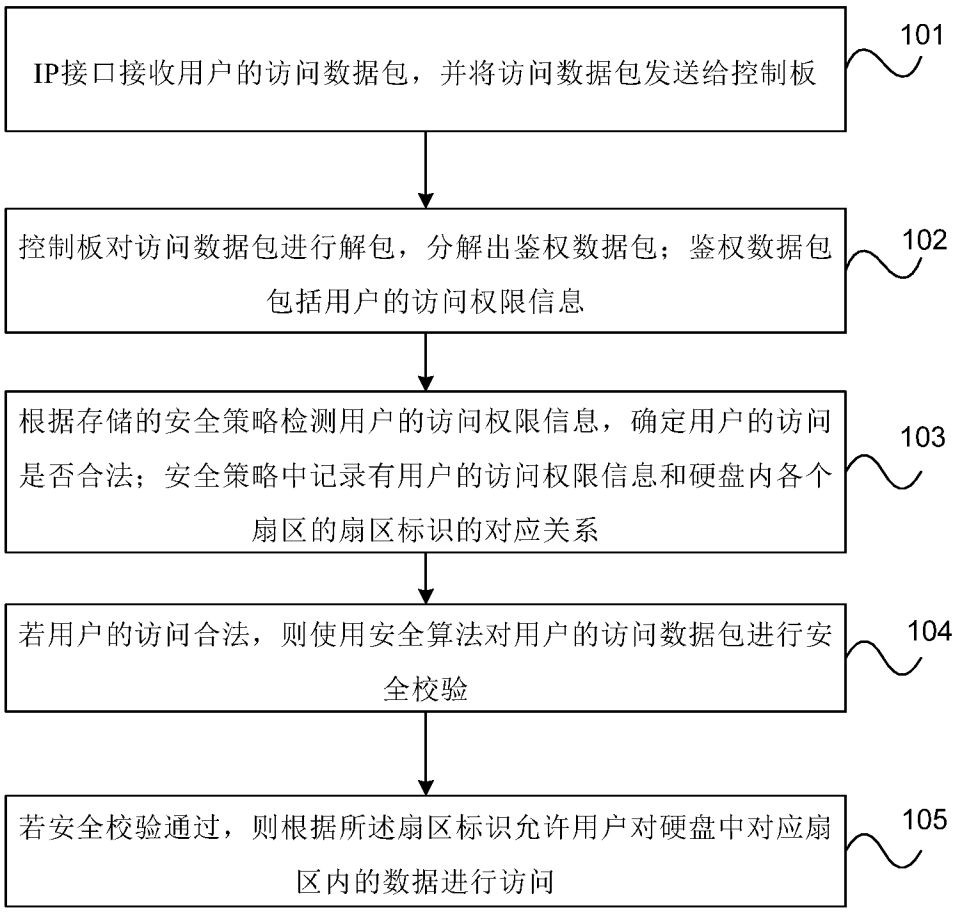

IP接口接收用户的访问数据包，并将访问数据包发送给控制板
101
控制板对访问数据包进行解包，分解出鉴权数据包；鉴权数据包包括用户的访问权限信息
102
根据存储的安全策略检测用户的访问权限信息，确定用户的访问是否合法；安全策略中记录有用户的访问权限信息和硬盘内各个扇区的扇区标识的对应关系
103
若用户的访问合法，则使用安全算法对用户的访问数据包进行安全校验
104
若安全校验通过，则根据所述扇区标识允许用户对硬盘中对应扇区内的数据进行访问
105

图 1

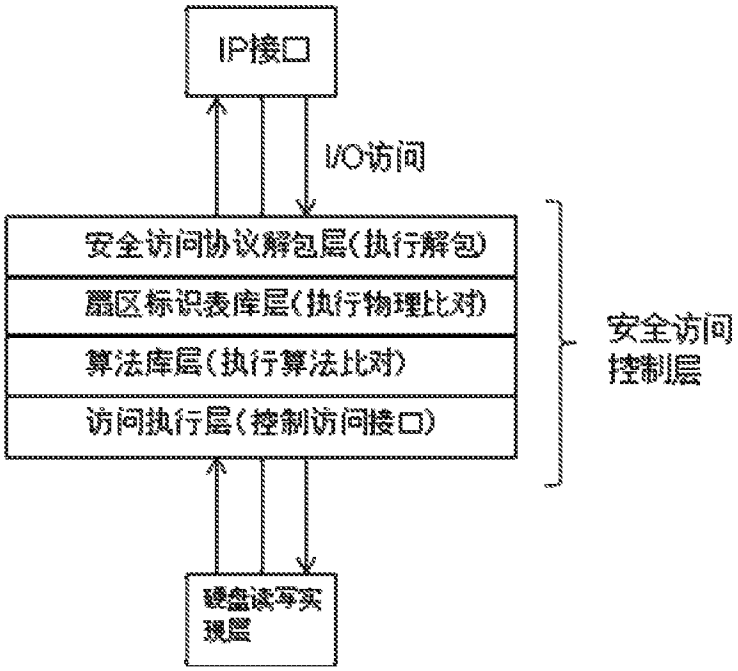

IP接口
I/O访问
安全访问协议解包层(执行解包)
扇区标识表库层(执行物理比对)
算法库层(执行算法比对)
访问执行层(控制访问接口)
安全访问控制层
硬盘读写实现层

图 2

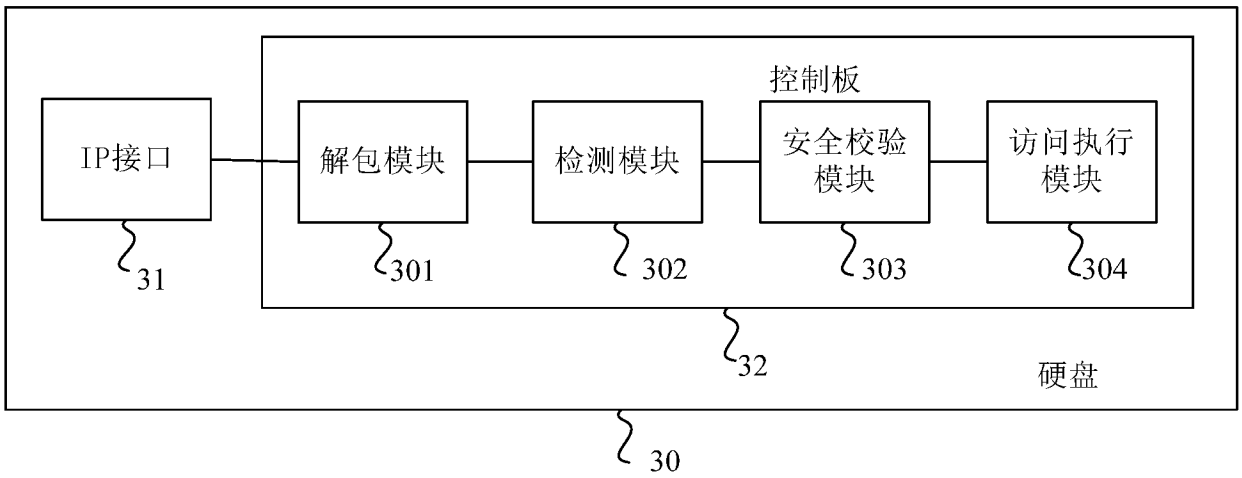

控制板
IP接口
解包模块
检测模块
安全校验模块
访问执行模块
31
301
302
303
304
32
硬盘
30

图 3

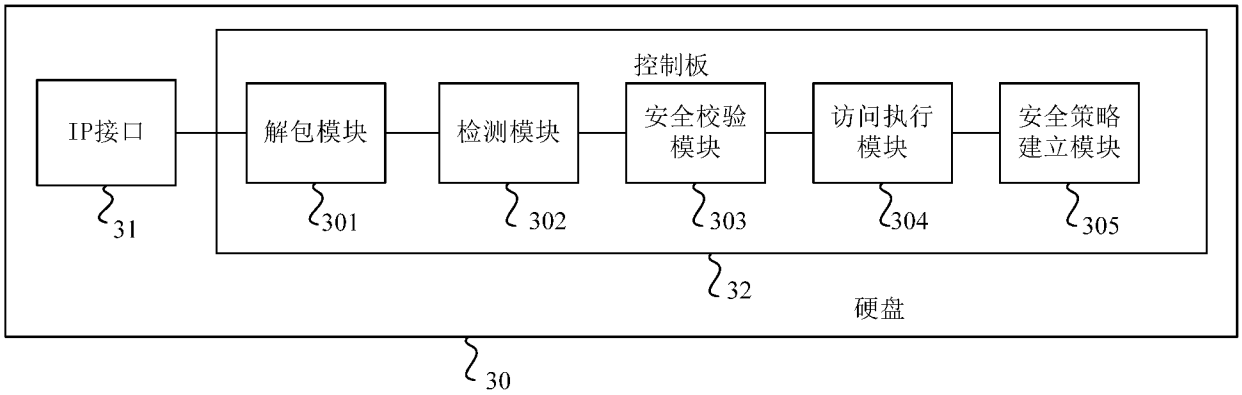

控制板
IP接口
解包模块
检测模块
安全校验模块
访问执行模块
安全策略建立模块
31
301
302
303
304
305
32
硬盘
30

图 4

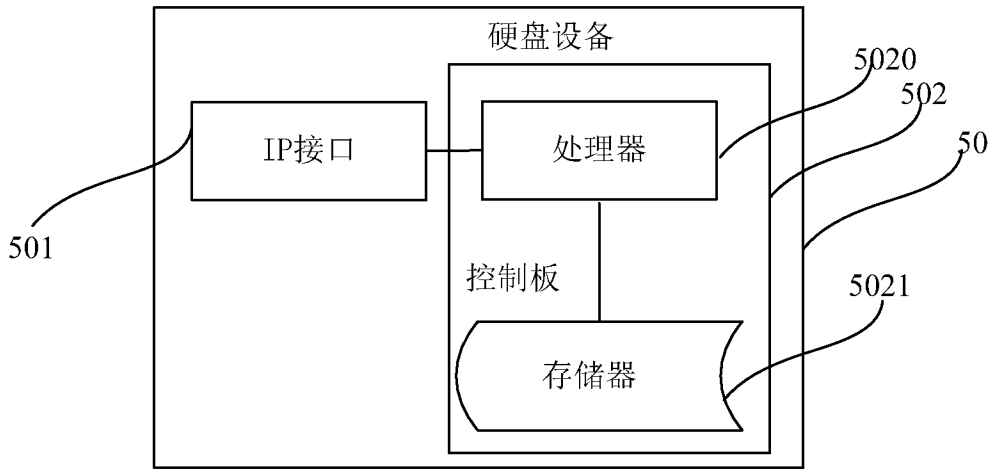

硬盘设备
5020
502
50
IP接口
处理器
501
控制板
5021
存储器

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/079945

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/14 (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)

WPI, EPODOC, CNPAT, CNKI, CNTXT: authentication, hard disc, communication, CONTROL, SAFETY, AUTHORITY, ACCESS, HARD, DISC, CHECK, DATA, PACKAGE, ALLOW, USER, CORRESPOND, SECTOR, PASS, IDENTIFY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104063641 A (HUAWEI TECHNOLOGIES CO., LTD.), 24 September 2014 (24.09.2014), claims 1-9	1-9
A	CN 101030175 A (INTERNATIONAL BUSINESS MACHINES CORP.), 05 September 2007 (05.09.2007), the whole document	1-9
A	CN 101441604 A (HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.), 27 May 2009 (27.05.2009), the whole document	1-9
A	CN 1795439 A (SECURE SYSTEMS LTD.), 28 June 2006 (28.06.2006), the whole document	1-9
A	GB 201102541 D0 (FUJITSU LTD.), 30 March 2011 (30.03.2011), the whole document	1-9
A	US 2010017575 A1 (KIM, S.H.), 21 January 2010 (21.01.2010), the whole document	1-9

☐ 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
08 July 2015 (08.07.2015)	**03 August 2015 (03.08.2015)**
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 **LIU, Huan** Telephone No.: (86-10) **62411853**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/079945

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104063641 A	24 September 2014	None	
CN 101030175 A	05 September 2007	US 2009300710 A1	03 December 2009
		EP 1989653 A1	12 November 2008
		CN 100580642 C	13 January 2010
		EP 1989653 B1	31 July 2013
		WO 2007099012 A1	07 September 2007
		TW 200830167 A	16 July 2008
CN 101441604 A	27 May 2009	None	
CN 1795439 A	28 June 2006	EP 1609070 A1	28 December 2005
		CA 2520707 C	18 November 2014
		KR 20050112118 A	29 November 2005
		US 8250648 B2	21 August 2012
		KR 101146153 B1	16 May 2012
		JP 2006521602 A	21 September 2006
		AU 2004223343 B2	25 February 2010
		EP 1609070 A4	12 January 2011
		CA 2520707 A1	07 October 2004
		WO 2004086228 A1	07 October 2004
		JP 4690310 B2	01 June 2011
		AU 2003901454 D0	10 April 2003
		US 2008104348 A1	01 May 2008
		CN 1795439 B	04 July 2012
		AU 2004223343 A1	07 October 2004
GB 201102541 D0	30 March 2011	GB 2479227 A	05 October 2011
		JP 2011210129 A	20 October 2011
		US 8713250 B2	29 April 2014
		JP 5565040 B2	06 August 2014
		US 2011246738 A1	06 October 2011
		US 2014258665 A1	11 September 2014
US 2010017575 A1	21 January 2010	JP 2010506327 A	25 February 2010
		US 2012260054 A1	11 October 2012
		EP 2074545 A4	07 December 2011
		KR 100834205 B1	30 May 2008
		KR 20080033064 A	16 April 2008
		US 8185709 B2	22 May 2012
		EP 2074545 A1	01 July 2009

国际检索报告

国际申请号
PCT/CN2015/079945

A. 主题的分类

G06F 12/14(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））

WPI,EPODOC,CNPAT,CNKI,CNTXT:控制，安全，权限，鉴权，访问，硬盘，检测，数据，包，允许，用户，通信，扇区，通过，识别，CONTROL，SAFETY，AUTHORITY，ACCESS，HARD，DISC，CHECK，DATA，PACKAGE，ALLOW，USER，CORRESPOND，SECTOR，PASS，IDENTIFY

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
PX	CN 104063641 A (华为技术有限公司) 2014年 9月 24日 (2014-09-24) 权利要求1-9	1-9
A	CN 101030175 A (国际商业机器公司) 2007年 9月 5日 (2007-09-05) 全文	1-9
A	CN 101441604 A (成都市华为赛门铁克科技有限公司) 2009年 5月 27日 (2009-05-27) 全文	1-9
A	CN 1795439 A (安全系统有限公司) 2006年 6月 28日 (2006-06-28) 全文	1-9
A	GB 201102541 D0 (FUJITSU LTD) 2011年 3月 30日 (2011-03-30) 全文	1-9
A	US 2010017575 A1 (KIM SANGHOON) 2010年 1月 21日 (2010-01-21) 全文	1-9

☐ 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 7月 8日	2015年 8月 3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) 北京市海淀区蓟门桥西土城路6号 100088 中国	刘欢
传真号 (86-10)62019451	电话号码 (86-10)62411853

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/079945

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	104063641	A	2014年 9月 24日	无			
CN	101030175	A	2007年 9月 5日	US	2009300710	A1	2009年 12月 3日
				EP	1989653	A1	2008年 11月 12日
				CN	100580642	C	2010年 1月 13日
				EP	1989653	B1	2013年 7月 31日
				WO	2007099012	A1	2007年 9月 7日
				TW	200830167	A	2008年 7月 16日
CN	101441604	A	2009年 5月 27日	无			
CN	1795439	A	2006年 6月 28日	EP	1609070	A1	2005年 12月 28日
				CA	2520707	C	2014年 11月 18日
				KR	20050112118	A	2005年 11月 29日
				US	8250648	B2	2012年 8月 21日
				KR	101146153	B1	2012年 5月 16日
				JP	2006521602	A	2006年 9月 21日
				AU	2004223343	B2	2010年 2月 25日
				EP	1609070	A4	2011年 1月 12日
				CA	2520707	A1	2004年 10月 7日
				WO	2004086228	A1	2004年 10月 7日
				JP	4690310	B2	2011年 6月 1日
				AU	2003901454	D0	2003年 4月 10日
				US	2008104348	A1	2008年 5月 1日
				CN	1795439	B	2012年 7月 4日
				AU	2004223343	A1	2004年 10月 7日
GB	201102541	D0	2011年 3月 30日	GB	2479227	A	2011年 10月 5日
				JP	2011210129	A	2011年 10月 20日
				US	8713250	B2	2014年 4月 29日
				JP	5565040	B2	2014年 8月 6日
				US	2011246738	A1	2011年 10月 6日
				US	2014258665	A1	2014年 9月 11日
US	2010017575	A1	2010年 1月 21日	JP	2010506327	A	2010年 2月 25日
				US	2012260054	A1	2012年 10月 11日
				EP	2074545	A4	2011年 12月 7日
				KR	100834205	B1	2008年 5月 30日
				KR	20080033064	A	2008年 4月 16日
				US	8185709	B2	2012年 5月 22日
				EP	2074545	A1	2009年 7月 1日