(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 7 月 7 日 (07.07.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/106752 A1

(51) 国际专利分类号:
H04L 29/00 (2006.01)

(21) 国际申请号: PCT/CN2014/096064

(22) 国际申请日: 2014 年 12 月 31 日 (31.12.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳大学 (SHENZHEN UNIVERSITY) [CN/CN]; 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。

(72) 发明人: 王博 (WANG, Bo); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。 陈剑勇 (CHEN, Jianyong); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。 喻建平 (YU, Jianping); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。

(74) 代理人: 深圳中一专利商标事务所 (SHENZHEN ZHONGYI PATENT AND TRADEMARK OFFICE); 中国广东省深圳市福田区深南中路 1014 号老特区报社四楼西区（5 号信箱）, Guangdong 518028 (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: SHARED DATA ACCESS CONTROL METHOD, DEVICE AND SYSTEM

(54) 发明名称 : 一种共享数据的访问控制方法、装置及系统

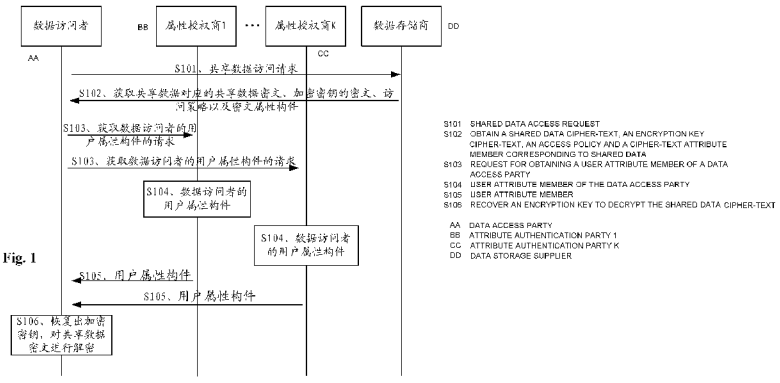

图 1 / Fig. 1

(57) Abstract: The present invention is applied to the field of data security. Provided are a shared data access control method, device and system, the method comprising: a data access party transmits an access request for shared data to a data storage supplier; obtaining a shared data cipher-text, an encryption key cipher-text, an access policy and a cipher-text attribute member from the data storage supplier; transmitting requests for obtaining a user attribute member of the data access party to attribute authentication parties respectively; the attribute authentication party respectively generates the user attribute member of the data access party and transmits the same to the data access party; and the data access party recovers an encryption key, and uses the same to decrypt the shared data cipher-text so as to obtain the shared data of requesting access. The method improves security of the shared data and reduces complexity of data sharing access control.

(57) 摘要:

[见续页]

WO 2016/106752 A1

应用于数据安全领域，提供了一种共享数据的访问控制方法、装置及系统，所述方法包括：数据访问者向数据存储商发送对一共享数据的访问请求，从数据存储商获取共享数据密文、加密密钥的密文、访问策略以及密文属性构件，向属性授权商分别发送获取数据访问者的用户属性构件的请求，所述属性授权商各自生成该数据访问者的用户属性构件，并发送给该数据访问者，数据访问者恢复出加密密钥，使用加密密钥对共享数据密文进行解密，以得到请求访问的共享数据。通过本方法可提高共享数据的安全性，同时，也降低了数据共享访问控制的复杂性。

一种共享数据的访问控制方法、装置及系统

技术领域

本发明属于数据安全领域，尤其涉及一种共享数据的访问控制方法、装置及系统。

背景技术

数据共享的程度反映了一个地区、一个国家的信息发展水平，数据共享程度越高，信息发展水平越高。实现数据共享，可以使更多的人更充分地使用已有数据资源，减少资料收集、数据采集等重复劳动和相应费用，而云存储为数据共享提供了更加安全、有效的平台。云存储是在云计算(cloud computing)概念上延伸和发展出来的一个新的概念，是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统。使用者可以在任何时间、任何地方，透过任何可连网的装置连接到云上方便地存取数据。

因此，如何在保证数据共享的同时，保证共享数据安全性，以保护云存储系统或信息网络中的数据免受各种类型的威胁、干扰和破坏已经成为了云计算研究的一个重要方面。基于属性加密（Attribute-based Encryption，ABE）是近年来新兴的一种公钥加密机制，它是身份加密方法的延伸。在属性加密中，用户的身份通过一系列的属性来描述，只有当用户的身份属性满足系统定义的访问策略时，才能够解密得到明文。这种访问控制机制进一步提高了共享数据的安全性，同时保证了数据共享的灵活性。例如，可以根据用户具有的身份属性以及身份属性值，对用户开放不同的访问权限，这对于一些领域共享的数据的访问控制特别有利。作为示例地，例如在电子医疗记录共享系统中，可以设置只有具有一定职称、设定的医院、具有一定从业年龄、相关领域医生才能查看

一类病人的医疗记录。若简单采用用户名/密码的访问控制策略，则难以实现对共享数据进行有效的访问控制。

然而，现有的基于属性加密的访问控制策略需要中央身份认证授权商作为媒介，对用户身份进行认证，以提供相应参数给不同属性授权商，这样不同属性授权商可以为同一用户提供用户属性构件。可以看出，由于中央身份认证授权商的存在，一旦中央身份认证授权商被攻破，就可以容易地窃取用户属性构件，进而实现数据的解密，从而降低了数据的安全性，同时，也增加了数据共享访问控制的复杂性。

发明内容

本发明实施例的目的在于提供一种共享数据的访问控制方法及系统，旨在解决由于现有技术无法提供一种有效的共享数据的访问控制方法，导致数据的安全性降低，数据共享访问控制的复杂性增加的问题。

一方面，本发明提供了一种共享数据的访问控制方法，所述方法包括下述步骤：

数据访问者向数据存储商发送对一共享数据的访问请求；

数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密；

数据访问者向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性；

所述K个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件，并发送给该数据访问者；

数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥；

数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

另一方面，本发明提供了一种共享数据的访问控制装置，所述装置包括:

访问请求发送单元，用于数据访问者向数据存储商发送对一共享数据的访问请求;

数据获取单元，用于数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密;

数据请求发送单元，用于数据访问者向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性;

数据返回单元，用于所述K个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件，并发送给该数据访问者;

密钥恢复单元，用于数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥;以及

数据解密单元，用于数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

另一方面，本发明提供了一种共享数据的访问控制系统，所述系统包括数据访问者、属性授权商以及数据存储商，其中:

数据访问者，用于向数据存储商发送对一共享数据的访问请求，从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密，向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为

一个数值，表示数据访问者拥有该数值对应的属性；

属性授权商，用于接收到数据访问者发送的获取所述用户属性构件的请求后，生成该数据访问者的用户属性构件，并发送给该数据访问者；

数据存储商，用于接收所述数据访问者发送的对一共享数据的访问请求，向所述数据访问者返回所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件；

数据访问者还用于根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥，使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

在本发明实施例中，无需设立中央身份认证授权，各个属性授权商对用户的属性进行独立授权鉴定，从而提高了数据的安全性，同时，也降低了数据共享访问控制的复杂性。

附图说明

图 1 是本发明实施例一提供的共享数据的访问控制方法的实现流程图；

图 2 是本发明实施例二提供的共享数据的访问控制方法的实现流程图；

图 3 是本发明实施例三提供的共享数据的访问控制方法的实现流程图；

图 4 是本发明实施例四提供的共享数据的访问控制装置的结构图；以及

图 5 是本发明实施例五提供的共享数据的访问控制系统的结构图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

以下结合具体实施例对本发明的具体实现进行详细描述：

实施例一：

图 1 示出了本发明实施例一提供的共享数据的访问控制方法的实现流程，详述如下：

在步骤 S101 中，数据访问者向数据存储商发送对一共享数据的访问请求。

在本发明实施例中，数据存储商用于存储用户（即数据拥有者）共享的数据，并根据用户（数据拥有者）设置的访问策略对用户的共享数据进行访问控制。优选地，所述数据存储商为云存储服务器，从而向用户提供云存储数据共享服务。

在步骤 S102 中，数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件。

在本发明实施例中，基于属性对共享数据进行访问控制，从而能够根据相关实体/用户的属性动态变化，适时更新访问控制决策，从而提供了一种细粒度，更加灵活的访问控制方法。作为示例地，一个用户可具有多个属性，例如，工作部门、职称、工作年限等。基于用户属性，数据拥有者（即共享数据的拥有者）可在共享数据时对访问策略进行设置。

在本发明实施例中，访问策略是指能够用于解密密文的一系列属性的树状逻辑结构，即访问策略树。数据拥有者可以根据其共享数据的安全强度需求，将一系列的属性用一个树状结构组合起来，从而形成一个访问策略。这个树状结构的叶子节点都是属性的文字描述，非叶子节点就是一些“与或门”以及“阈值门”。例如{（“访问者是内科医生”OR“访问者是护士”）AND（“访问者医疗从业时间大于 3 年”）AND（“访问者在医院 J 工作”）}就是一个树状的访问策略，这样，通过一系列属性的树状逻辑结构将有权解密此加密的共享数据的人限定在一个范围内。其中 AND（与门）是（K，K）的阈值门，OR（或门）是指（1，K）的阈值门。

在本发明实施例中，密文属性构件为一数值，以表征请求访问共享数据的数据访问者的属性，在后续中用于恢复共享数据密文的加密密钥，所述加密密

钥用于对所述共享数据进行加密，在这里加密密钥以密文的形式存储。

在步骤 S103 中，数据访问者向所述访问策略关联的 K 个属性授权商分别发送获取数据访问者的用户属性构件的请求。

在本发明实施例中，用户属性构件为一数值，用于表明数据访问者拥有所述访问策略关联的属性，以与前述密文属性构件一起用于恢复共享数据的加密密钥。所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性。

在本发明实施例中，数据访问者发送的获取数据访问者用户属性构件的请求中包括数据访问者的全局唯一标识符（Globally Unique Identifier, GID），GID 用于全局唯一地标识用户的身份，例如，用户名等。

在本发明实施例中，属性授权商用于定义属性，鉴定数据访问者是否拥有该定义的属性以及为数据访问者生成用户属性构件。由于访问策略关联多个属性，而这些属性可以由一个或多个属性授权商管理，因此，数据访问者需要将用户属性构件请求发送给 K 个属性授权商，K 个属性授权商即为访问策略中关联（涉及）到的属性的属性授权商，其中 K 为正整数。

在本发明实施例中，优选地，在数据访问者向所述访问策略关联的属性授权商发送获取用户属性构件请求之前，对所述获取用户属性构件请求进行数字签名，以防止数据访问者抵赖。另外，属性授权商在接收数据访问者发送的获取用户属性构件请求时也会对所述数据请求者进行身份认证，例如，通过传统用户名/密码、生物特征认证等。

在步骤 S104 中，所述 K 个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件。

在本发明实施例中，属性授权商接收到获取数据访问者解密私钥的请求后，各自生成该数据访问者的解密私钥。具体地，各个属性授权商根据获取用户属性构件的请求中包含的数据访问者的全局唯一标识符生成第一哈希值，并根据数据访问者的属性的标识符生成第二哈希值，根据所述第一哈希值、第二

哈希值以及预先生成的属性主密钥生成所述用户属性构件，其中，属性主密钥包括两个数值，在本发明实施例中，将该两个数值记为第一参数值和第二参数值。

在本发明实施例中，属性授权商管理的一个或多个预设属性对应同一个属性主密钥，由于属性主密钥由属性授权商自身进行管理保存，这样可在不降低安全的情形下，减少属性主密钥的存储要求，同时，简化用户属性构件生成过程。

优选地，作为示例地，可通过下述公式生成数据访问者的用户属性构件:

$$uAc = H(att)^a \cdot H(GID)^b \qquad \text{公式（1）}$$

其中 att 表示所述数据访问者的属性的标识符，H(att)表示所述第二哈希值，H(GID)表示所述第一哈希值，a、b 表示属性主密钥的两个参数值。

在步骤 S105 中，属性授权商将各自生成的用户属性构件发送给数据访问者。

在步骤 S106 中，数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥，数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

在本发明实施例中，由前所述，所述数据访问者可接收到N个所述用户属性构件、M个所述密文属性构件。

作为示例地，所述数据访问者可根据接收到的数据，通过以下方式恢复出所述加密密钥:

（1） 将作为所述访问策略的访问策略树的叶子节点所关联的密文属性构件以及同一属性相关联的用户属性构件作为预设的一双线性映射函数的输入，从而得到叶子节点的节点相关值。

（2）根据所述访问策略树的层次结构，由访问策略树的叶子节点层次开始，自底向上，每一层都需要按照预设的秘密共享函数的逆运算，以该层的节

点相关值作为输入，计算得到该层父节点的节点相关值。自底向上，迭代使用所述秘密共享函数的逆运算，直到最后得到所述访问策略树的根节点的节点相关值，此相关值作为第一中间恢复数据。

（3）将所述第一中间恢复数据与所述加密密钥的所述密文相乘，即可得到加密密钥。之后，数据访问者使用所述加密密钥对所述用户数据密文进行解密，以得到请求访问的共享数据。

在本发明实施例中，无需设立中央身份认证授权，各个属性授权商对用户的属性进行独立授权鉴定，从而提高了数据的安全性，同时，也降低了数据共享访问控制的复杂性。

在本发明实施例中，在数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件之前，共享数据的拥有者（即数据拥有者）应根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，以对共享数据进行访问控制，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商。

在具体实施过程中，优选地，可通过以下公式生成加密密钥的密文：

$$K = key \cdot \hat{e}(g^{a}, H(att))^{s} \qquad \text{公式（2）}$$

其中，key 表示加密密钥，g^{a} 表示所述属性公钥，$H(att)$ 表示所述第二哈希值，$\hat{e}(\cdot,\cdot)$ 表示一预设双线性映射函数，s 表示一随机值，g 为系统预设一个群的生成元。

密文属性构件包括三个数值，优选地，通过以下公式计算：

$$\boldsymbol{pAc1} = \hat{\boldsymbol{e}}(\boldsymbol{g},\boldsymbol{g})^{s_x}\,\hat{\boldsymbol{e}}(\boldsymbol{g}^{a},\boldsymbol{H}(\boldsymbol{att}))^{r_x} \qquad \text{公式（3）}$$

$$\boldsymbol{pAc2} = \boldsymbol{g}^{b\cdot r_x + w_x}, \qquad \text{公式（4）}$$

$$\boldsymbol{pAc3} = \boldsymbol{g}^{r_x} \qquad \text{公式（5）}$$

其中 s_x 为访问策略第 x 个节点所述随机值 s 经过所述秘密共享函数计算得

到的值，r_x表示另一随机值，w_x表示对固定值 0 经过所述秘密共享函数计算得到的值，其余符号与前述公式中意义相同。

在本发明实施例中，数据拥有者在共享数据前，根据加密密钥、属性公钥、第二哈希值、访问策略生成加密密钥的密文以及密文属性构件，以对共享数据进行访问控制，在提高共享数据的安全性的同时，也降低了数据共享访问控制的复杂性。

在本发明实施例中，数据访问者、属性授权商、数据存储商以及数据拥有者可以是提供对应功能的个人计算机、服务器等，通过其上对应的硬件模块执行上述步骤。

实施例二:

图 2 示出了本发明实施例二提供的共享数据的访问控制方法的实现流程，详述如下:

在步骤 S201 中， 属性授权商根据接收到的属性更新指令，生成一新的属性主密钥以及一新的属性版本号，根据所述新的属性主密钥与保存的原属性主密钥生成密文属性构件更新参数。

在本发明实施例中，保存的原属性主密钥为未更新的、旧的属性主密钥。如前所述，属性主密钥包括两个参数值，即第一参数值和第二参数值，在这里可通过对两个参数的改变以实现密文属性构件的更新。作为示例地，可将新的属性主密钥的第二参数值与保存的属性主密钥的第二参数值之差作为密文属性构件更新参数。具体可通过下述公式（6）生成所述密文属性构件更新参数:

$$RK_{att}=b'-b \qquad \text{公式（6）}$$

其中，b’为新的属性主密钥的第二参数值，b 为保存的原属性主密钥第二参数值。

在步骤 S202 中，属性授权商将新的属性版本号以及密文属性构件更新参数发送给数据存储商。

在步骤 S203 中， 数据存储商将接收到的所述新的属性版本号以及所述

密文属性构件更新参数保存到预先建立的更新参数列表。

在本发明实施例中，当用户（例如，所述数据访问者）的属性随着管理需求、时间等发生改变时，属性授权商可以及时地对其管理的属性对应的密文属性构件进行更新，从而及时地调整用户的属性授权，实现属性的快速召回。在本发明实施例中，数据存储商预先建立一更新参数列表，用于记录管理的属性的各个版本以及对应的密文属性构件更新参数。

在步骤 S204 中，数据访问者向数据存储商发送对一共享数据的访问请求。

在步骤 S205 中，数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件。

在本发明实施例中，当数据存储商接收到数据访问者发送的获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件时，数据存储商根据存储的更新参数列表判断该数据访问者对应的密文属性构件随附的属性版本号是否为属性的最新版本号，若是，则向数据访问者返回所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，若不是，则根据存储的更新参数将该数据访问者对应的密文属性构件更新至最新版本的密文属性构件，之后再将共享数据对应的共享数据密文、加密密钥的密文、访问策略以及更新后的密文属性构件返回给数据访问者。这样，只有当用户请求访问共享数据时，才对其密文属性构件进行更新，大大降低了数据存储商的负载。

在步骤 S206 中，数据访问者根据所述数据存储商返回的所述共享数据密文、加密密钥的密文、访问策略以及密文属性构件，在预设的用户属性构件数据库中查询是否存储有对应的用户属性构件。

在本发明实施例中，当数据访问者未存储有对应的用户属性构件时，数据访问者从访问策略关联的 K 个属性授权商分别获取数据访问者的用户属性构件，具体实施步骤如前所述，在此不再赘述。

当数据访问者存储有对应的用户属性构件时，数据访问者判定所述已存储用户属性构件相关联的版本号与所述密文属性构件相关联的版本号是否一致。若不一致，则执行步骤 S207，若一致则数据访问者根据接收到的访问策略、加密密钥的密文、密文属性构件、存储的用户属性构件恢复出加密密钥，数据访问者使用加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

在步骤 S207 中，数据访问者向所述版本号不一致的用户属性构件所对应的属性授权商发送获取用户属性构件更新参数的请求。

在本发明实施例中，当数据访问者的属性更新后，则不能再使用以前的用户属性构件，需要从版本号不一致的用户属性构件所对应的属性授权商获取用户属性构件更新参数对其自身的用户属性构件进行更新。

在步骤 S208 中，属性授权商接收到获取用户属性构件更新参数请求后，各自生成该数据访问者的用户属性构件更新参数。

在本发明实施例中，属性授权商根据数据访问者的所述全局唯一标识符（GID）生成第一哈希值，根据所述第一哈希值、所述新的属性主密钥的第二参数值与保存的属性主密钥的第二参数值生成用户属性构件更新参数。具体可通过下述公式（7）生成所述用户属性构件更新参数:

$$RK_{GID,at} = H(GID)^{b'-b} \qquad \text{公式（7）}$$

其中，各参数的意义可参考前述描述，在此不再赘述。

在本发明实施例中，每一个数据访问者的用户属性构件更新参数都不一致，因此，数据访问者无法共享更新参数，从而提高共享数据的安全性。

在步骤 S209 中，属性授权商将各自生成的用户属性构件更新参数发送给数据访问者。

在步骤 S210 中，数据访问者根据接收到的访问策略、加密密钥的密文、密文属性构件、用户属性构件更新参数、存储的原用户属性构件恢复出加密密钥，数据访问者使用加密密钥对共享数据密文进行解密，以得到请求访问的共

享数据。

在本发明实施例中，无需设立中央身份认证授权，各个属性授权商对用户的属性进行独立授权鉴定，从而提高了数据的安全性，同时，也降低了数据共享访问控制的复杂性。

实施例三：

图 3 示出了本发明实施例三提供的共享数据的访问控制方法的实现流程，详述如下：

在步骤 S301 中， 属性授权商根据接收到的属性更新指令，生成一新的属性主密钥，并生成一新的属性版本号，根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第二哈希值、所述新的属性主密钥与保存的原属性主密钥生成密文属性构件更新参数。

在本发明实施例中，当接收到属性更新指令时，可生成一新的属性主密钥的第一参数值，并生成一新的属性版本号，根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第二哈希值、所述新的属性主密钥的第一参数值与保存的原属性主密钥第一参数值生成密文属性构件更新参数。具体可通过下述公式（8）生成所述密文属性构件更新参数：

$$RK_{att} = H(att)^{a'-a}$$

公式（8）

其中，a'为新的属性主密钥的第一参数值，a 为保存的原属性主密钥第一参数值。

在步骤 S302 中，属性授权商将新的属性版本号以及密文属性构件更新参数发送给数据存储商。

在步骤 S303 中， 数据存储商将接收的所述新的属性版本号以及所述密文属性构件更新参数保存到预先建立的更新参数列表。

在本发明实施例中，当用户（例如，所述数据访问者）的属性随着管理需求、时间等发生改变时，属性授权商可以及时地对其管理的属性进行更新操

作，从而及时地调整用户的属性授权，实现属性的快速召回。在本发明实施例中，数据存储商预先建立一更新参数列表，用于记录管理的属性的各个版本以及对应的更新参数。

在步骤 S304 中，数据访问者向数据存储商发送对一共享数据的访问请求。

在步骤 S305 中，数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件。

在本发明实施例中，当数据存储商接收到数据访问者发送的获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件时，数据存储商根据存储的更新参数列表判断该数据访问者对应的密文属性构件随附的属性版本号是否为属性的最新版本号，若是，则向数据访问者返回所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，若不是，则根据存储的更新参数将该数据访问者对应的密文属性构件更新至最新版本的密文属性构件，之后再将共享数据对应的共享数据密文、加密密钥的密文、访问策略以及更新后的密文属性构件返回给数据访问者。这样，只有当用户请求访问共享数据时，才对其密文属性构件进行更新，大大降低了数据存储商的负载。

在步骤 S306 中，数据访问者根据所述数据存储商返回的所述共享数据密文、加密密钥的密文、访问策略以及密文属性构件，在预设的用户属性构件数据库中查询是否存储有对应的用户属性构件。

在本发明实施例中，当数据访问者未存储有对应的用户属性构件时，数据访问者从访问策略关联的 K 个属性授权商分别获取数据访问者的用户属性构件，具体实施步骤如前所述，在此不再赘述。

当数据访问者存储有对应的用户属性构件时，数据访问者判定所述已存储用户属性构件相关联的版本号与所述密文属性构件相关联的版本号是否一致。若不一致，则执行步骤 S307，若一致则数据访问者根据接收到的访问策略、

加密密钥的密文、密文属性构件、存储的用户属性构件恢复出加密密钥，数据访问者使用加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

在步骤 S307 中，数据访问者向所述版本号不一致的用户属性构件所对应的属性授权商发送获取用户属性构件更新参数的请求。

在本发明实施例中，当数据访问者的属性更新后，则不能再使用以前的用户属性构件，需要从版本号不一致的用户属性构件所对应的属性授权商获取用户属性构件更新参数对其自身的用户属性构件进行更新。

在步骤 S308 中，属性授权商接收到获取用户属性构件更新参数请求后，各自生成该数据访问者的用户属性构件更新参数。

在本发明实施例中，可生成一新的属性主密钥的第一参数值，并生成一新的属性版本号，根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第二哈希值、所述新的属性主密钥的第一参数值与保存的原属性主密钥第一参数值生成用户属性构件更新参数，具体可通过下述公式（9）生成所述用户属性构件更新参数:

$$RK_{GID,att} = H(att)^{a'-a} \qquad \text{公式（9）}$$

其中，各参数的意义可参考前述描述，在此不再赘述。

在本发明实施例中，每一个数据访问者的用户属性构件更新参数是一致的，从而可减少属性授权商产生用户属性构件更新参数的计算量，提高计算效率。

在步骤 S309 中，属性授权商将各自生成的用户属性构件更新参数发送给数据访问者。

在步骤 S310 中，数据访问者根据接收到的访问策略、加密密钥的密文、密文属性构件、用户属性构件更新参数、存储的原用户属性构件恢复出加密密钥，数据访问者使用加密密钥对共享数据密文进行解密，以得到请求访问的共享数据。

在本发明实施例中，无需设立中央身份认证授权，各个属性授权商对用户的属性进行独立授权鉴定，从而提高了数据的安全性，同时，也降低了数据共享访问控制的复杂性。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如 ROM/RAM、磁盘、光盘等。

实施例四：

图 4 示出了本发明实施例四提供的共享数据的访问控制装置 4 的结构，为了便于说明，仅示出了与本发明实施例相关的部分，所述访问装置 4 包括：

访问请求发送单元 401，用于数据访问者向数据存储商发送对一共享数据的访问请求；

数据获取单元 402，用于数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密；

数据请求发送单元 403，用于数据访问者向所述访问策略关联的 K 个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性；

数据返回单元 411，用于所述 K 个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件，并发送给该数据访问者；

密钥恢复单元 404，用于数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥；以及

数据解密单元 405，用于数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

作为示例地，访问请求发送单元 401、数据获取单元 402、数据请求发送单元 403、密钥恢复单元 404 以及数据解密单元 405 位于一数据访问者 40 中，数据返回单元 411 位于属性授权商 41 中。

在本发明一实施例中，作为示例地，所述数据返回单元 411 可以包括构件生成单元 4111，用于各个属性授权商根据所述获取所述用户属性构件的请求中包含的数据访问者的全局唯一标识符生成第一哈希值，并根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第一哈希值、第二哈希值以及预先生成的属性主密钥生成所述用户属性构件，其中，属性授权商管理的一个或多个预设属性对应同一个属性主密钥。

进一步地，在本发明一实施例中，该共享数据的访问控制装置还包括数据生成单元 421，以用于数据拥有者根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商。作为示例地，数据生成单元 421 可位于一数据拥有者 42 中

在本发明实施例中，共享数据的访问控制装置 4 各单元的实施方式具体可参考实施例一中的对应步骤的实施，在此不再赘述。

在本发明实施例中，数据访问者、属性授权商、数据存储商以及数据拥有者可以是提供对应功能的个人计算机、服务器等，而上述单元可以为个人计算机或服务器中通过对应硬件执行其功能的功能单元或硬件单元。

实施例五：

图 5 示出了本发明实施例五提供的共享数据的访问控制系统 5 的结构，为了便于说明，仅示出了与本发明实施例相关的部分，其中包括：

所述系统 5 包括数据访问者 51、属性授权商 52 以及数据存储商 53，其中：

数据访问者 51，用于向数据存储商 53 发送对一共享数据的访问请求，从数据存储商 53 获取所述共享数据对应的共享数据密文、加密密钥的密文、访

问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密，向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性；

属性授权商 52，用于接收到数据访问者 51 发送的获取所述用户属性构件的请求后，生成该数据访问者的用户属性构件，并发送给该数据访问者；

数据存储商 53，用于接收所述数据访问者 51 发送的对一共享数据的访问请求，向所述数据访问者 51 返回所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件。

数据访问者 51 还用于根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥，使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

在本发明一实施例中，该系统还包括数据拥有者 50，所述数据拥有者 50 根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商 53。

在本发明实施例中，无需设立中央身份认证授权，各个属性授权商对用户的属性进行独立授权鉴定，从而提高了数据的安全性，同时，也降低了数据共享访问控制的复杂性。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种共享数据的访问控制方法，其特征在于，所述方法包括下述步骤:

数据访问者向数据存储商发送对一共享数据的访问请求;

数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密;

数据访问者向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性;

所述K个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件，并发送给该数据访问者;

数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥;

数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

2、如权利要求 1 所述的方法，其特征在于，生成该数据访问者的用户属性构件的步骤包括:

各个属性授权商根据所述获取所述用户属性构件的请求中包含的数据访问者的全局唯一标识符生成第一哈希值，并根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第一哈希值、第二哈希值以及预先生成的属性主密钥生成所述用户属性构件。

3、如权利要求 2 所述的方法，其特征在于，属性授权商管理的一个或多个预设属性对应同一个属性主密钥。

4、如权利要求 1 所述的方法，其特征在于，数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属

性构件的步骤之前，还包括:

数据拥有者根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商。

5、一种共享数据的访问控制装置，其特征在于，所述装置包括:

访问请求发送单元，用于数据访问者向数据存储商发送对一共享数据的访问请求;

数据获取单元，用于数据访问者从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密;

数据请求发送单元，用于数据访问者向所述访问策略关联的K个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性;

数据返回单元，用于所述K个属性授权商接收到获取所述用户属性构件的请求后，各自生成该数据访问者的用户属性构件，并发送给该数据访问者;

密钥恢复单元，用于数据访问者根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥;以及

数据解密单元，用于数据访问者使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

6、如权利要求5所述的装置，其特征在于，所述数据返回单元包括:

构件生成单元，用于各个属性授权商根据所述获取所述用户属性构件的请求中包含的数据访问者的全局唯一标识符生成第一哈希值，并根据所述数据访问者的属性的标识符生成第二哈希值，根据所述第一哈希值、第二哈希值以及预先生成的属性主密钥生成所述用户属性构件。

7、如权利要求 6 所述的装置，其特征在于，属性授权商管理的一个或多个预设属性对应同一个属性主密钥。

8、如权利要求 5 所述的装置，其特征在于，所述装置还包括:

数据生成单元，用于数据拥有者根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商。

9、一种共享数据的访问控制系统，其特征在于，所述系统包括数据访问者、属性授权商以及数据存储商，其中:

数据访问者，用于向数据存储商发送对一共享数据的访问请求，从数据存储商获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件，所述密文属性构件为一个数值，用于表征数据访问者的属性，所述加密密钥用于对所述共享数据进行加密，向所述访问策略关联的 K 个属性授权商分别发送获取数据访问者的用户属性构件的请求，所述用户属性构件为一个数值，表示数据访问者拥有该数值对应的属性;

属性授权商，用于接收到数据访问者发送的获取所述用户属性构件的请求后，生成该数据访问者的用户属性构件，并发送给该数据访问者;

数据存储商，用于接收所述数据访问者发送的对一共享数据的访问请求，向所述数据访问者返回所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件;

数据访问者还用于根据接收到的所述访问策略、所述加密密钥的所述密文、所述密文属性构件、所述用户属性构件恢复出所述加密密钥，使用所述加密密钥对所述共享数据密文进行解密，以得到请求访问的共享数据。

10、如权利要求 9 所述的访问控制系统，其特征在于，所述系统还包括数据拥有者，所述数据拥有者根据所述加密密钥、属性公钥、所述第二哈希值、所述访问策略生成所述加密密钥的所述密文以及所述密文属性构件，并将所述加密密钥的所述密文以及所述密文属性构件发送给所述数据存储商。

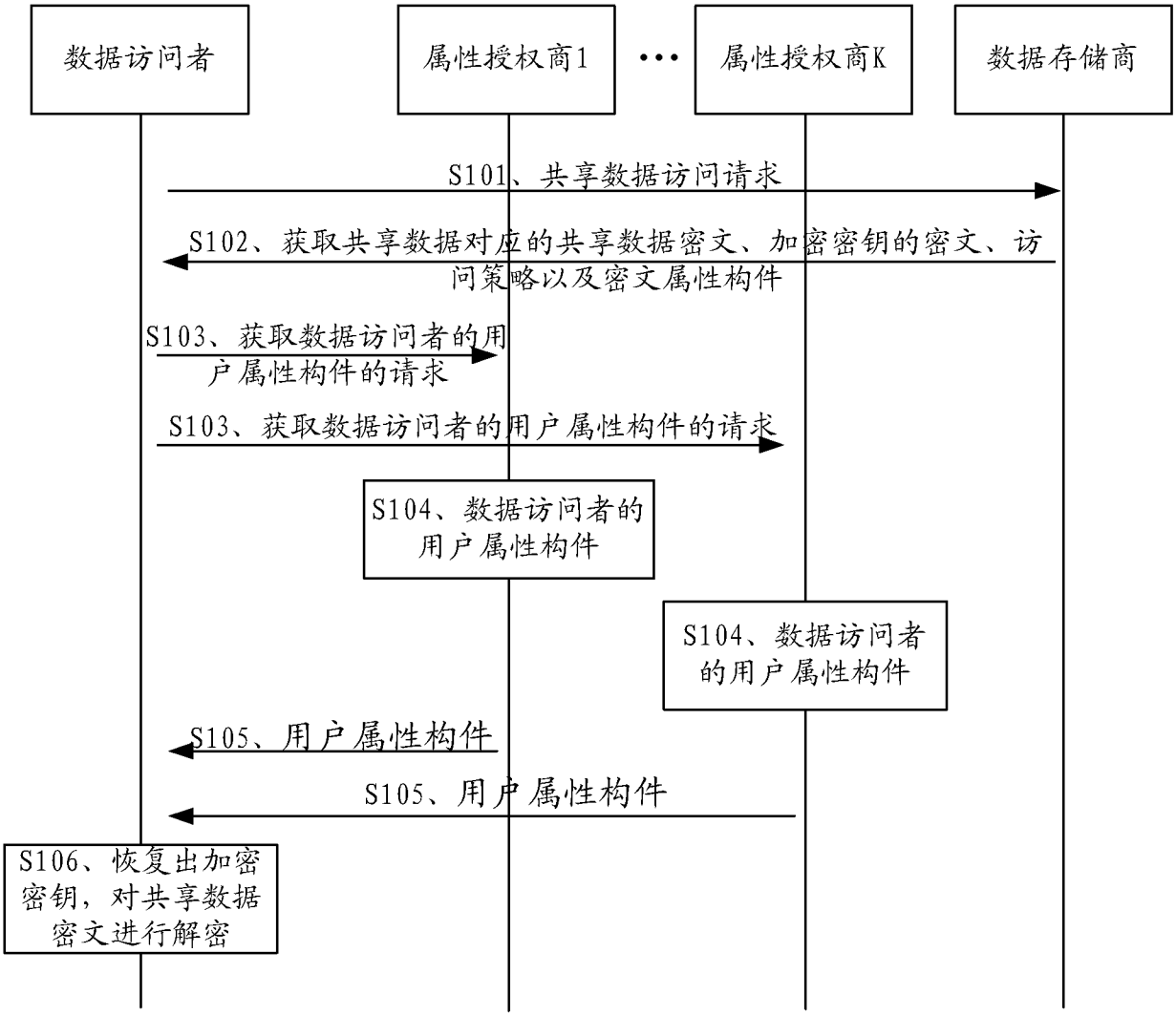
数据访问者
属性授权商1
•••
属性授权商K
数据存储商
S101、共享数据访问请求
S102、获取共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件
S103、获取数据访问者的用户属性构件的请求
S103、获取数据访问者的用户属性构件的请求
S104、数据访问者的用户属性构件
S104、数据访问者的用户属性构件
S105、用户属性构件
S105、用户属性构件
S106、恢复出加密密钥，对共享数据密文进行解密

图 1

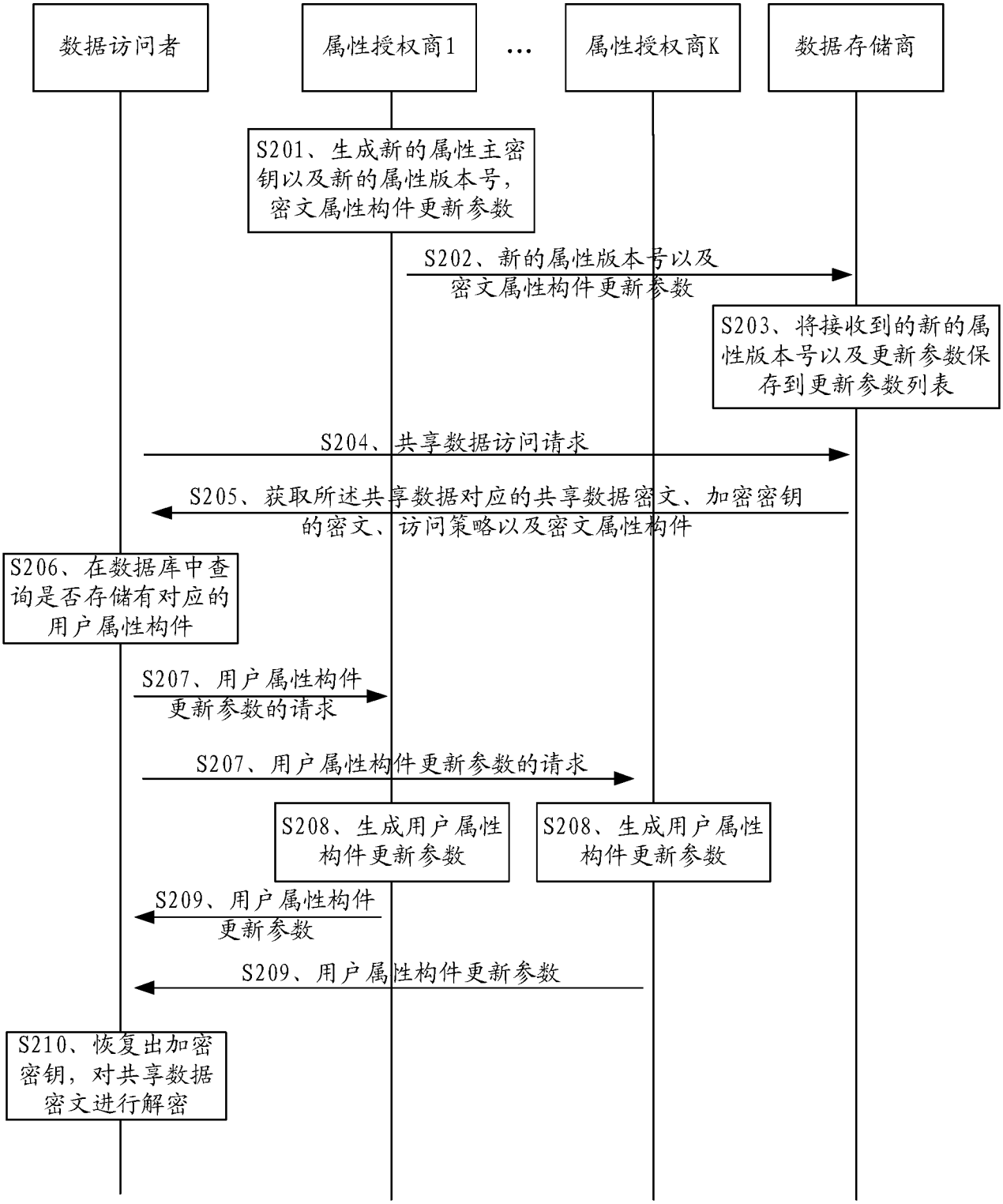
数据访问者
属性授权商1
...
属性授权商K
数据存储商
S201、生成新的属性主密钥以及新的属性版本号，密文属性构件更新参数
S202、新的属性版本号以及密文属性构件更新参数
S203、将接收到的新的属性版本号以及更新参数保存到更新参数列表
S204、共享数据访问请求
S205、获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件
S206、在数据库中查询是否存储有对应的用户属性构件
S207、用户属性构件更新参数的请求
S207、用户属性构件更新参数的请求
S208、生成用户属性构件更新参数
S208、生成用户属性构件更新参数
S209、用户属性构件更新参数
S209、用户属性构件更新参数
S210、恢复出加密密钥，对共享数据密文进行解密

图 2

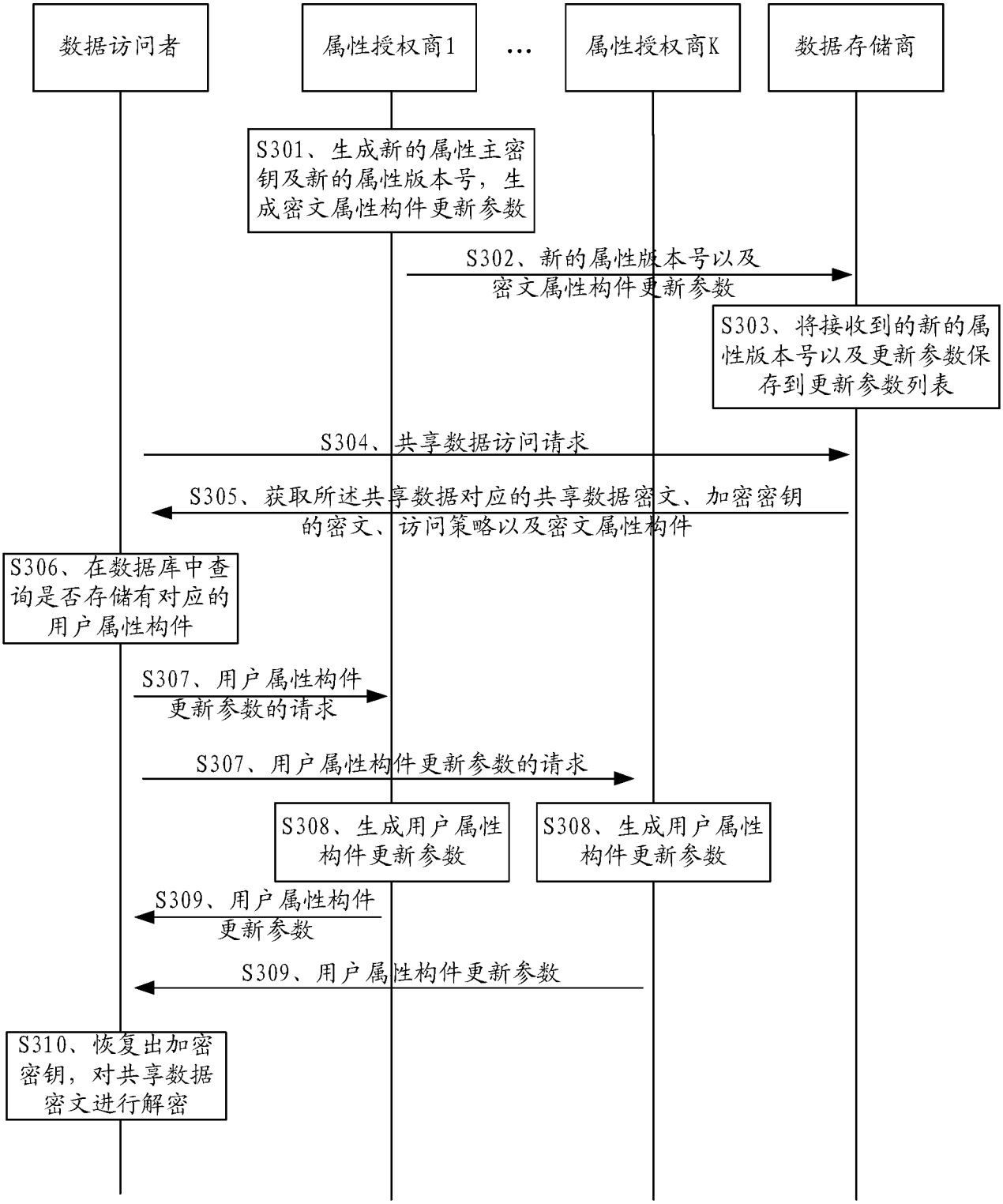
数据访问者
属性授权商1
...
属性授权商K
数据存储商
S301、生成新的属性主密钥及新的属性版本号，生成密文属性构件更新参数
S302、新的属性版本号以及密文属性构件更新参数
S303、将接收到的新的属性版本号以及更新参数保存到更新参数列表
S304、共享数据访问请求
S305、获取所述共享数据对应的共享数据密文、加密密钥的密文、访问策略以及密文属性构件
S306、在数据库中查询是否存储有对应的用户属性构件
S307、用户属性构件更新参数的请求
S307、用户属性构件更新参数的请求
S308、生成用户属性构件更新参数
S308、生成用户属性构件更新参数
S309、用户属性构件更新参数
S309、用户属性构件更新参数
S310、恢复出加密密钥，对共享数据密文进行解密

图 3

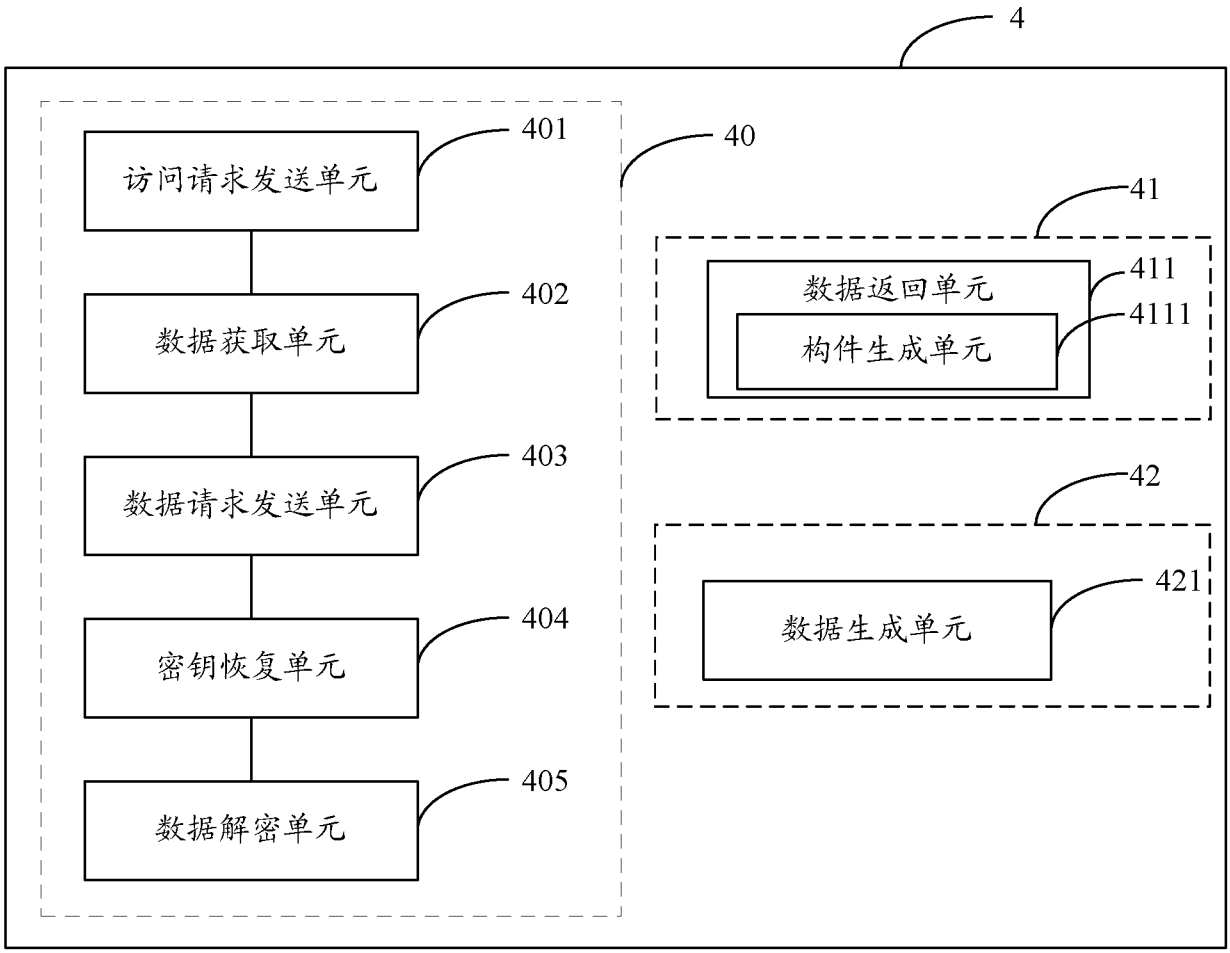
4
401
访问请求发送单元
40
41
402
数据获取单元
数据返回单元
411
4111
构件生成单元
403
数据请求发送单元
42
404
密钥恢复单元
421
数据生成单元
405
数据解密单元

图 4

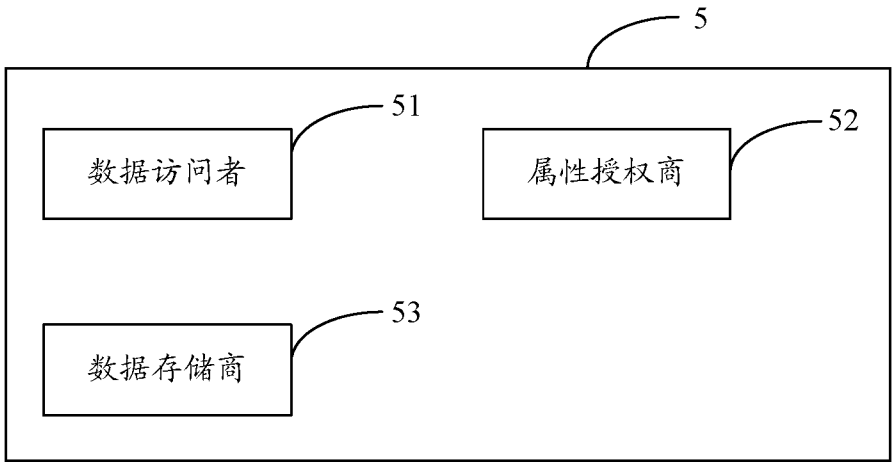
5
51
数据访问者
52
属性授权商
53
数据存储商

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/096064

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/00 (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)

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)

CNPAT, CNKI, WPI, EPODOC: encryption and decryption, encrypt, attribute, share, cloud, data, decrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103763319 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 30 April 2014 (30.04.2014), description, paragraphs [0006]-[0055]	1-10
A	CN 102624522 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 01 August 2012 (01.08.2012), the whole document	1-10
A	CN 102546764 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 04 July 2012 (04.07.2012), the whole document	1-10
A	US 2013080765 A1 (MOHANTY, S. et al.), 28 March 2013 (28.03.2013), the whole document	1-10

☐ 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
09 September 2015 (09.09.2015)	**25 September 2015 (25.09.2015)**
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 **LIN, Songling** Telephone No.: (86-10) **61648099**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/096064

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103763319 A	30 April 2014	None	
CN 102624522 A	01 August 2012	None	
CN 102546764 A	04 July 2012	None	
US 2013080765 A1	28 March 2013	US 2014344572 A1	20 November 2014

国际检索报告

国际申请号
PCT/CN2014/096064

A. 主题的分类

H04L 29/00(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)

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））

CNPAT，CNKI，WPI，EPODOC:解密，加解密，加密，属性，共享，云，数据，encrypt,attribute,share,cloud,data,decrypt

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 103763319 A (华中科技大学) 2014年 4月 30日 (2014-04-30) 说明书第[0006]-[0055]段	1-10
A	CN 102624522 A (华中科技大学) 2012年 8月 1日 (2012-08-01) 全文	1-10
A	CN 102546764 A (华中科技大学) 2012年 7月 4日 (2012-07-04) 全文	1-10
A	US 2013080765 A1 (MOHANTY, SUBHASHIS 等) 2013年 3月 28日 (2013-03-28) 全文	1-10

☐ 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 9月 9日	2015年 9月 25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	林松岭
传真号 (86-10)62019451	电话号码 (86-10)61648099

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/096064

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 103763319 A	2014年 4月 30日	无	
CN 102624522 A	2012年 8月 1日	无	
CN 102546764 A	2012年 7月 4日	无	
US 2013080765 A1	2013年 3月 28日	US 2014344572 A1	2014年 11月 20日