

(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 12 月 15 日 (15.12.2016)



(10) 国际公布号
WO 2016/197769 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/081386
- (22) 国际申请日: 2016 年 5 月 9 日 (09.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510326052.2 2015 年 6 月 12 日 (12.06.2015) CN
- (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 518000 (CN)。
- (72) 发明人: 张鹏 (ZHANG, Peng); 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)。刘宏伟 (LIU, Hongwei); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。孙志伟 (SUN, Zhiwei); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。

- (74) 代理人: 深圳市恒申知识产权事务所 (普通合伙) (HENSEN INTELLECTUAL PROPERTY FIRM); 中国广东省深圳市福田区南园路 68 号上步大厦 10H, Guangdong 518000 (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)。

[见续页]

(54) Title: CLOUD STORAGE CIPHERTEXT ACCESS CONTROL SYSTEM BASED ON TABLE ATTRIBUTES

(54) 发明名称: 一种基于表格属性的云存储密文访问控制系统

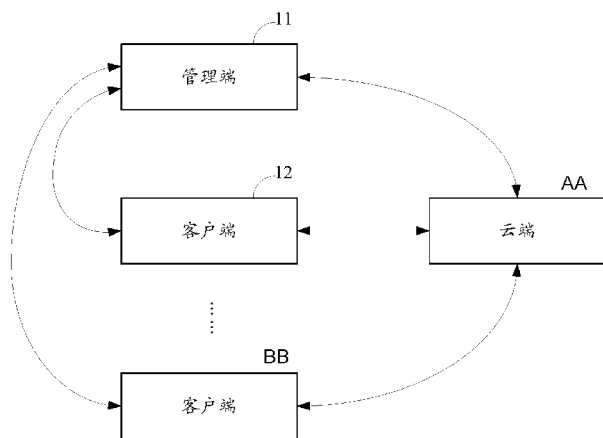


图 1

- 11 Management end
12 Client
AA Cloud
BB Client

(57) Abstract: The present invention pertains to the technical field of cloud storage services, and provides a cloud storage ciphertext access control system based on table attributes and an access control method thereof. According to the system and the method, during the process of encryption, a data owner classifies leaf nodes on an access structure tree according to whether the threshold of a parent node corresponding to each leaf node is 1; the data owner further classifies a set of leaf nodes of which the thresholds of the parent nodes are 1 according to different types of parent nodes; then the data owner encrypts data according to the result of the classification and uploads the data to the cloud. In this way, the length of ciphertext obtained by the data owner, the amount of encryption calculation, and the amount of decryption calculation for subsequent sharing users are only related to an attribute set in which thresholds of parent nodes are not 1. In the access structure tree, if the threshold is 1, the parent node corresponds to an OR gate; otherwise, the parent node corresponds to an AND gate. Therefore, the system overheads are only related to an attribute set in

which parent nodes are AND gates. When the number of OR gates in the access structure tree increases, the computational cost and communication overheads of the system are greatly reduced.

(57) 摘要:

[见续页]



WO 2016/197769 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明属于云存储服务技术领域，提供了一种基于表格属性的云存储密文访问控制系统及其访问控制方法。该系统及方法中，数据属主在加密过程中，根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对数据加密后上传至云端。这样，数据属主得到的密文长度、加密计算量和后续共享用户的解密计算量均只与父节点阈值不为 1 的属性集合有关，而在访问结构树中，阈值为 1 对应或门，否则对应与门，因此可以说，系统开销只与父节点为与门的属性集合有关，当访问结构树中的或门增加时，系统的计算代价和通信开销将大为降低。

一种基于表格属性的云存储密文访问控制系统

技术领域

本发明属于云存储服务技术领域，尤其涉及一种基于表格属性的云存储密文访问控制系统。

背景技术

在云存储服务平台中，由于采用数据远程托管技术，云存储服务提供商是数据的物理拥有者，却与数据属主并不在同一个信任域中。云存储服务提供商管理着多个用户及其资源，当用户跨边界访问其它用户资源时，需要采用一定的访问控制策略来控制对数据和服务的访问。但实际中，由于云存储服务平台是采用虚拟化存储技术，云存储服务同底层硬件环境之间是松耦合的，不同用户的数据间缺乏固定不变的安全边界，由此增加了在云存储服务平台对数据实施访问控制的难度。

现有技术中，基于属性的加密（Attribute-based Encryption, ABE）方案以属性描述用户身份，用户私钥和密文分别与一组属性相关，当用户私钥属性与密文属性相互匹配度达到设定门限值时，用户才能成功解密密文。

但 ABE 方案仅能支持门限访问控制策略，为了表达更灵活的访问控制策略，基于密文策略的属性加密（Cipher Policy Attribute-based Encryption, CP-ABE）方案被提出。在 CP-ABE 方案中，密文与访问策略相关，用户私钥与属性集合相关，当且仅当用户私钥的属性满足密文的访问策略时，用户才能成功解密密文。CP-ABE 方案极大地降低了数据共享细粒度访问控制带来的网络带宽和结点计算的开销，是最适合于云存储平台的密文访问控制技术之一。

对于采用 CP-ABE 方案的云存储平台，考虑企业应用场景，属性与访问策略需要通过表格部署。但由于属性集合较为庞大，访问结构十分复杂，CP-ABE

方案在云存储平台中的执行效率很低。

发明内容

本发明的目的在于提供一种基于表格属性的云存储密文访问控制系统，旨在解决现有采用 CP-ABE 方案的云存储平台通过表格部署属性与访问策略，由于属性集合庞大、访问结构复杂，使得 CP-ABE 方案执行效率低的问题。

本发明是这样实现的，一种基于表格属性的云存储密文访问控制系统，所述系统包括：

由认证中心运行的管理端，用于生成并向每一合法用户分发用户私钥，所述用户私钥与对应用户的属性相关联；

由用户运行的客户端，用于在上传数据到云端时，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对所述会话密钥加密以得到会话密钥密文，之后将所述会话密钥密文和加密后的数据上传到云端，还用于在从云端下载数据时，从云端下载会话密钥密文和对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会话密钥，之后利用解密得到的所述会话密钥解密所述对应的共享数据。

本发明的另一目的在于提供一种如上所述的基于表格属性的云存储密文访问控制系统的访问控制方法，所述方法包括：

认证中心运行管理端，生成系统公钥与主私钥，将所述系统公钥上传至云端；

认证中心运行管理端，根据用户发出的系统加入请求，认证用户是否为合法用户，并当用户为合法用户时，计算用户的用户私钥，并分发给用户；

数据属主运行客户端，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点

进行分类, 并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类, 之后根据分类结果对所述会话密钥加密以得到会话密钥密文, 之后将所述会话密钥密文和加密后的数据上传到云端;

共享用户运行客户端, 从云端下载会话密钥密文和对应的共享数据, 并当与自身用户私钥相关联的属性满足访问结构树时, 由会话密钥密文解密得到会话密钥, 之后利用解密得到的所述会话密钥解密所述对应的共享数据。

本发明提供的基于表格属性的云存储密文访问控制系统及其访问控制方法中, 数据属主在加密过程中, 根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类, 并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类, 之后根据分类结果对数据加密后上传至云端。这样, 数据属主得到的密文长度、加密计算量和后续共享用户的解密计算量均只与父节点阈值不为 1 的属性集合有关, 而在访问结构树中, 阈值为 1 对应或门, 否则对应与门, 因此可以说, 系统开销只与父节点为与门的属性集合有关, 当访问结构树中的或门增加时, 相对于现有的 CP-ABE 方案, 系统的计算代价和通信开销将大为降低, 从而能够更高效的为用户提供隐私保护、数据共享与访问控制服务。

附图说明

图 1 是本发明提供的基于表格属性的云存储密文访问控制系统的结构图;

图 2 是本发明提供的基于表格属性的云存储密文访问控制系统的访问控制方法的流程图;

图 3 是本发明的一种访问结构树实例图。

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。

针对现有技术存在的问题，考虑到表格属性具有如下两个特点：一、属性是分类的，如下表 1 所示为一企业的花名册：

表 1

序号	姓名	性别	职位	部门
001	Alan	女	首席执行官	总部
002	John	男	总经理	总部
003	Alex	男	经理	人力资源部
004	Steven	男	经理	财务部
...	...	...	...	...

上表中，所有属性被分为 5 种类型；二、访问结构树中同种属性类型或门（OR 门）多于与门（AND 门），如上表所示，序号 001 OR 002 OR 003 发生概率较大，序号 001 AND 002 AND 003 发生概率极低。从而，本发明中，数据属主在加密过程中，根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对数据加密后上传至云端。

图 1 示出了本发明提供的基于表格属性的云存储密文访问控制系统的结构，为了便于说明，仅示出了与本发明相关的部分。

具体而言，本发明的系统包括：由认证中心运行的管理端 11，用于生成并向每一合法用户分发用户私钥，用户私钥与对应用户的属性相关联；由用户运行的客户端 12，用于在上传数据到云端时，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对会话密钥加密以得到会话密钥密文，之后将会话密钥密文和加密后的数据上传到云端，还用于在从云

端下载数据时，从云端下载会话密钥密文和对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会话密钥，之后利用解密得到的会话密钥解密对应的共享数据。

本发明中，系统的合法用户可被区分为数据属主和共享用户，数据属主、共享用户分别是客户端 12 的运行主体，认证中心是管理端 11 的运行主体。其中，数据属主是指云端上共享数据的提供方，数据属主制定访问策略，并基于访问策略对需上传的数据进行加密，之后将加密后的数据托管至云端；共享用户（即访问者）是指从云端下载共享数据方，共享用户访问云端存储的密文数据，只有当共享用户的用户私钥中的属性满足密文中定义的访问策略，共享用户才能成功解密密文；认证中心是指除数据属主和共享用户之外、与云端交互的可信第三方，认证中心建立系统并接受用户注册，负责为每个用户生成关联其各自属性的用户私钥。应当理解，定义数据属主与共享用户的目的是为了区别运行客户端 12 的主体在系统某次运行过程中的功能是上传数据或下载数据，因而在系统某次运行过程中的数据属主可以是另一次运行过程中的共享用户，同样地，在系统某次运行过程中的共享用户可以是另一次运行过程中的数据属主。

本发明的基于表格属性的云存储密文访问控制系统的工作原理是：系统建立后，认证中心运行管理端 11，生成系统公钥与主私钥，将系统公钥上传至云端。

用户若希望加入系统，则运行客户端 12，向认证中心发出系统加入请求，认证中心运行管理端 11，根据该系统加入请求，认证该用户是否为合法用户，是则计算该用户的用户私钥，并分发给该用户。

当数据属主上传数据时，数据属主运行客户端 12，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对会话密钥加

密以得到会话密钥密文，之后将会话密钥密文和加密后的数据上传到云端。

当共享用户从云端下载数据时，共享用户运行客户端 12，从云端下载会话密钥密文和对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会话密钥，之后利用解密得到的会话密钥解密对应的共享数据。

本发明提供的基于表格属性的云存储密文访问控制系统中，数据属主在加密过程中，根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对数据加密后上传至云端。这样，数据属主得到的密文长度、加密计算量和后续共享用户的解密计算量均只与父节点阈值不为 1 的属性集合有关，而在访问结构树中，阈值为 1 对应或门，否则对应与门，因此可以说，系统开销只与父节点为与门的属性集合有关，当访问结构树中的或门增加时，相对于现有的 CP-ABE 方案，系统的计算代价和通信开销将大为降低，从而能够更高效的为用户提供隐私保护、数据共享与访问控制服务。

图 2 示出了本发明提供的基于表格属性的云存储密文访问控制系统的访问控制方法的流程，包括以下步骤：

S1：认证中心运行管理端 11，生成系统公钥与主私钥，将系统公钥上传至云端。

进一步地，生成系统公钥与主私钥的步骤又可包括以下步骤：

S11：定义 $\mathbb{G}_0$ 是阶为素数 P 的双线性群， g 为 $\mathbb{G}_0$ 的生成元。定义双线性映射 $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ ， $H: \{0,1\}^* \rightarrow \mathbb{G}_0$ 是一个哈希函数。定义系统的属性空间 $U = \{U_1, \dots, U_m\}$ ，对于 $i \in \mathbb{Z}_p$ 与属性集合 S ，属性集合 $S \subseteq U$ ，定义拉格朗日系数

$$\Delta_{i,S} = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}。$$

S12：输入安全参数 λ ，选择随机数 $\alpha, \beta \in \mathbb{Z}_p$ ，并计算 $h = g^\beta, u = g^\alpha$ 和

$v = e(g, g)^\alpha$ ，进而根据公式 $PK = (\mathbb{G}_0, g, h, v)$ 得到系统公钥 PK ，并根据公式 $MK = (\beta, u)$ 得到主私钥 MK 。

S2: 认证中心运行管理端 11，根据用户发出的系统加入请求，认证用户是否为合法用户，并当用户为合法用户时，计算用户的用户私钥，并分发给用户。

进一步地，计算用户的用户私钥的步骤又包括以下步骤：

S21: 认证中心利用属性空间 U ，根据用户的角色或身份，为用户分配相应的属性集合 S ，属性集合 $S \subseteq U$ 。

S22: 输入主私钥 MK 和用户的属性集合 S ，为用户选取随机数 $r \in \mathbb{Z}_p$ ，并为属性集合 S 中的每一属性 $j \in S$ 选取随机数 $r_j \in \mathbb{Z}_p$ ，依照下式计算用户私钥 SK ：

$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in S: D_j = g^{r_j} \cdot H(j)^{r_j}, \tilde{D}_j = g^{r_j} \cdot H(type(j))^{r_j}, D'_j = g^{r_j})$$

其中， $type(j)$ 为属性 j 所在的表格门类， D 为双线性群 $\mathbb{G}_0$ 上的元素， D_j 为双线性群 $\mathbb{G}_0$ 上的元素， $\tilde{D}_j$ 为双线性群 $\mathbb{G}_0$ 上的元素， D'_j 为双线性群 $\mathbb{G}_0$ 上的元素。

S3: 数据属主运行客户端 12，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对会话密钥加密以得到会话密钥密文，之后将会话密钥密文和加密后的数据上传到云端。

进一步地，步骤 S3 又包括以下步骤：

S31: 数据属主运行客户端 12，选取会话密钥 ck ，并采用对称加密算法加密需上传的数据 M ，得到加密后的数据 $E_{ck}(M)$ 。

S32: 输入系统公钥 PK 、会话密钥 ck 、以及访问结构树 T ，对于访问结构树 T 中的每个节点 x ，设置其孩子节点数为 num_x ，设置其阈值为 t_x ，且有 $0 < t_x \leq num_x$ ，定义多项式 q_x 的度为 d_x ，且 $d_x = t_x - 1$ ，节点 x 的孩子节点依次标记序号为 $1, \dots, num_x$ ， $index(x)$ 为返回节点 x 的序号， $att(x)$ 为返回与节点 x 相关联的

属性, $type(att(x))$ 为返回属性 $att(x)$ 所在的表格门类, 之后对于访问结构树 T 的根节点, 选取随机数 $s \in \mathbb{Z}_p$ 并设定 $q_R(0) = s$, 进一步随机选择 d_R 个子节点来完整定义多项式 q_R , 对于访问结构树 T 的除根节点以外的其它节点 x , 设定 $q_x(0) = q_{parent}(index(x))$, 进一步随机选择 d_x 个子节点来完整定义多项式 q_x 。其中系统的公钥 PK 是由数据属主从云端下载而得到的。

S33: 对于访问结构树 T 的叶子节点 x , 若叶子节点 x 的父节点 $parent(x)$ 的阈值 $t_{parent(x)} = 1$, 则 $q_x(0) = q_{parent(x)}(0)$, 令 Y_1 为访问结构树 T 中该类叶子节点的集合、 Y_2 是访问结构树 T 中余下的叶子节点的集合, 并进一步根据 Y_1 中各叶子节点的父节点类型的不同, 将 Y_1 划分为 $Y_{11}, Y_{12}, \dots$ 。

S34: 根据如下公式对会话密钥加密, 计算得到会话密钥密文 CT :

$$\begin{aligned} CT &= (T, \tilde{C} = ck \cdot e(g, g)^{\alpha s}, C = h^s, \\ &\forall y \in Y_{1i} (i = 1, 2, \dots): C_y = g^{q_{parent(y)}(0)}, C'_y = H(type(att(y)))^{q_{parent(y)}(0)}, \\ &\forall y \in Y_2: C_y = g^{q_y(0)}, C'_y = H(att(y))^{q_y(0)}) \end{aligned}$$

其中, $\tilde{C}$ 为对会话密钥的计算, C 为对根节点的计算, C_y 为对属性 y 对应的属性值的计算, C'_y 为对属性 y 所在表格门类的计算。特别地, Y_{1i} 中的所有叶子节点具有相同的 C_y , 若不同叶子节点的属性属于相同的类型, 则它们具有相同的 C'_y 。

S35: 将会话密钥密文 CT 和加密后的数据 $E_{ck}(M)$ 上传到云端。

S4: 共享用户运行客户端 12, 从云端下载会话密钥密文和对应的共享数据, 并当与自身用户私钥相关联的属性满足访问结构树时, 由会话密钥密文解密得到会话密钥, 之后利用解密得到的会话密钥解密对应的共享数据。

进一步地, 步骤 S4 又可包括以下步骤:

S41: 共享用户运行客户端 12, 从云端下载会话密钥密文 CT 和对应的共享数据 $E_{ck}(M)$, 并输入系统公钥 PK 、用户拥有的属性集合 S 所对应的私钥 SK_s 、以及密钥密文 CT 。

S42: 共享用户调用预先定义的递归函数 $DecryptNode(CT, SK, x) = e(g, g)^{rq_x(0)}$, 若共享用户的属性集合 S 满足访问结构树 T , 则计算解密信息 A 为:

$$A = DecryptNode(CT, SK, R) = e(g, g)^{rq_R(0)} = e(g, g)^{rs}$$

本发明中, 递归函数 $DecryptNode(CT, SK, x)$ 的定义如下:

a、如果节点 x 是叶子节点, 且其父节点的阈值 $k_x > 1$, 则定义:

$$\begin{aligned} DecryptNode(CT, SK, x) &= \frac{e(D_{att(x)}, C_x)}{e(D'_{att(x)}, C'_x)} \\ &= \frac{e(g^r \cdot H(att(x))^{r_{att(x)}}, g^{q_x(0)})}{e(g^{r_{att(x)}}, H(att(x))^{q_x(0)})} \\ &= e(g, g)^{rq_x(0)} \end{aligned}$$

b、如果节点 x 是叶子节点, 且其父节点的阈值 $k_x = 1$, 则定义:

$$\begin{aligned} DecryptNode(CT, SK, x) &= \frac{e(\tilde{D}_{att(x)}, C_x)}{e(D'_{att(x)}, C'_x)} \\ &= \frac{e(g^r \cdot H(type(att(y)))^{r_{att(x)}}, g^{q_{parent(x)}(0)})}{e(g^{r_{att(x)}}, H(type(att(y)))^{q_{parent(x)}(0)})} \\ &= e(g, g)^{rq_{parent(x)}(0)} = e(g, g)^{rq_x(0)} \end{aligned}$$

c、如果节点 x 是非叶子节点, 对节点 x 的所有子节点 z , 递归调用 $DecryptNode(CT, SK, z)$ 并输出 F_z 。定义 S_x 是任意 t_x 个节点 z 的集合, 且 $F_z \neq \perp$, 依照下式计算 F_x , 若找不到满足条件的 S_x 集合, 则 $F_x = \perp$:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{i, S'_x}(0)} \quad \text{where } i = index(z), S'_x = \{index(z)\} \\ &= \prod_{z \in S_x} (e(g, g)^{rq_z(0)})^{\Delta_{i, S'_x}(0)} \\ &= \prod_{z \in S_x} (e(g, g)^{rq_z(0)})^{\Delta_{i, S'_x}(0)} \\ &= e(g, g)^{r \sum_{z \in S_x} q_z(0) \Delta_{i, S'_x}(0)} \\ &= e(g, g)^{rq_x(0)} \end{aligned}$$

S43: 根据下式对会话密钥密文 CT 解密, 得到会话密钥 ck :

$$\frac{\tilde{C}}{e(C, D) / A} = \frac{ck \cdot e(g, g)^{\alpha s}}{e(h^s, g^{(\alpha+r)/\beta}) / e(g, g)^{rs}} = \frac{ck \cdot e(g, g)^{\alpha s}}{e(h^s, g^{(\alpha+r)/\beta}) / e(g, g)^{rs}} = ck$$

S44: 根据解密得到的会话密钥 ck 和共享数据 $E_{ck}(M)$, 解密得到数据 M 。

以下对上述基于表格属性的云存储密文访问控制系统的访问控制方法的效率进行分析:

定义 $\mathbb{G}_0$ 和 $\mathbb{G}_1$ 表示群上的点乘运算, C_e 表示双线性对运算。令 $\mathbb{G}_0$ 与 $\mathbb{G}_1$ 中元素长度分别为 $L_{\mathbb{G}_0}$ 与 $L_{\mathbb{G}_1}$, $L_{\mathbb{Z}_p}$ 是有限域 $\mathbb{Z}_p$ 上元素的长度。定义 A_c 是密文 c 所包含的属性集, A_{c1} 是父节点阈值为 1 的属性集且 N 为满足条件的父节点个数, A_{c2} 是父节点阈值大于 1 的属性集, 于是有 $|A_c| = |A_{c1}| + |A_{c2}|$ 。定义 A_u 是用户属性集, S 表示满足访问结构的最小属性集合。本发明与经典 BSW07 方案的效率对比分析如下表 2 所示:

表 2

方法	公钥长度	主密钥长度	私钥长度	密文长度	加密	解密
BSW07	$3L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_0}$	$(2 A_u + 1)L_{\mathbb{G}_0}$	$(2 A_c + 1)L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$	$(2 A_c + 1)\mathbb{G}_0 + 2\mathbb{G}_1$	$2 A_u C_e + 2(S + 2)\mathbb{G}_1$
本发明	$3L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$	$L_{\mathbb{Z}_p} + L_{\mathbb{G}_0}$	$(3 A_u + 1)L_{\mathbb{G}_0}$	$(2 A_{c2} + 2N + 1)L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$	$(2 A_{c2} + 2N + 1)\mathbb{G}_0 + 2\mathbb{G}_1$	$2 A_u C_e + 2(S + 2)\mathbb{G}_1$

根据如上表 2 所示, 对比 BSW07 方案和本发明, 本发明的私钥长度稍长。然而, BSW07 方案中的密文长度、加密计算量均与 $|A_c|$ 相关, 而本发明所提方法的密文长度、加密计算量、解密计算量均与 $|A_{c2}|$ 相关, 由于 $|A_c| > |A_{c2}|$, 故本发明显著改善了密文访问控制方法的通信与计算效率。

若数据属主采用如图 3 所示的访问结构树执行加密过程, BSW07 方案的密文长度为 $11L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$ 、加密计算量为 $11\mathbb{G}_0 + 2\mathbb{G}_1$; 本发明方法的密文长度为 $7L_{\mathbb{G}_0} + L_{\mathbb{G}_1}$ 、加密计算量为 $7\mathbb{G}_0 + 2\mathbb{G}_1$ 。同时, 访问结构树中或门越多效率改进越显著。

综上所述, 本发明提供的基于表格属性的云存储密文访问控制系统及其访问控制方法中, 数据属主在加密过程中, 根据访问结构树上每一叶子节点对应

的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对数据加密后上传至云端。这样，数据属主得到的密文长度、加密计算量和后续共享用户的解密计算量均只与父节点阈值不为 1 的属性集合有关，而在访问结构树中，阈值为 1 对应或门，否则对应与门，因此可以说，系统开销只与父节点为与门的属性集合有关，当访问结构树中的或门增加时，相对于现有的 CP-ABE 方案，系统的计算代价和通信开销将大为降低，从而能够更高效的为用户提供隐私保护、数据共享与访问控制服务。

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程序来控制相关的硬件完成，所述的程序可以在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。

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、一种基于表格属性的云存储密文访问控制系统，其特征在于，所述系统包括：

由认证中心运行的管理端，用于生成并向每一合法用户分发用户私钥，所述用户私钥与对应用户的属性相关联；

由用户运行的客户端，用于在上传数据到云端时，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对所述会话密钥加密以得到会话密钥密文，之后将所述会话密钥密文和加密后的数据上传到云端，还用于在从云端下载数据时，从云端下载会话密钥密文和对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会话密钥，之后利用解密得到的所述会话密钥解密所述对应的共享数据。

2、一种如权利要求 1 所述的基于表格属性的云存储密文访问控制系统的访问控制方法，其特征在于，所述方法包括：

认证中心运行管理端，生成系统公钥与主私钥，将所述系统公钥上传至云端；

认证中心运行管理端，根据用户发出的系统加入请求，认证用户是否为合法用户，并当用户为合法用户时，计算用户的用户私钥，并分发给用户；

数据属主运行客户端，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为 1、来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为 1 的叶子节点的集合进行分类，之后根据分类结果对所述会话密钥加密以得到会话密钥密文，之后将所述会话密钥密文和加密后的数据上传到云端；

共享用户运行客户端，从云端下载会话密钥密文和对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会

话密钥，之后利用解密得到的所述会话密钥解密所述对应的共享数据。

3、如权利要求2所述的基于表格属性的云存储密文访问控制系统的访问控制方法，其特征在于，所述生成系统公钥与主私钥的步骤包括以下步骤：

定义 $\mathbb{G}_0$ 是阶为素数 p 的双线性群， g 为 $\mathbb{G}_0$ 的生成元，定义双线性映射 $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ ， $H: \{0,1\}^* \rightarrow \mathbb{G}_0$ 是一个哈希函数，定义系统的属性空间 $U = \{U_1, \dots, U_m\}$ ，对于 $i \in \mathbb{Z}_p$ 与属性集合 S ，所述属性集合 $S \subseteq U$ ，定义拉格朗日系数 $\Delta_{i,S} = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$ ；

输入安全参数 λ ，选择随机数 $\alpha, \beta \in \mathbb{Z}_p$ ，并计算 $h = g^\beta, u = g^\alpha$ 和 $v = e(g, g)^\alpha$ ，进而根据公式 $PK = (\mathbb{G}_0, g, h, v)$ 得到系统公钥 PK ，并根据公式 $MK = (\beta, u)$ 得到主私钥 MK 。

4、如权利要求3所述的基于表格属性的云存储密文访问控制系统的访问控制方法，其特征在于，所述计算用户的用户私钥的步骤包括以下步骤：

认证中心利用所述属性空间 U ，根据用户的角色或身份，为用户分配相应的属性集合 S ，所述属性集合 $S \subseteq U$ ；

输入主私钥 MK 和用户的属性集合 S ，为用户选取随机数 $r \in \mathbb{Z}_p$ ，并为属性集合 S 中的每一属性 $j \in S'$ 选取随机数 $r_j \in \mathbb{Z}_p$ ，依照下式计算用户私钥 SK ：

$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in S: D_j = g^{r_j} \cdot H(j)^{r_j}, \tilde{D}_j = g^{r_j} \cdot H(type(j))^{r_j}, D'_j = g^{r_j})$$

其中， $type(j)$ 为属性 j 所在的表格门类， D 为双线性群 $\mathbb{G}_0$ 上的元素， D_j 为双线性群 $\mathbb{G}_0$ 上的元素， $\tilde{D}_j$ 为双线性群 $\mathbb{G}_0$ 上的元素， D'_j 为双线性群 $\mathbb{G}_0$ 上的元素。

5、如权利要求4所述的基于表格属性的云存储密文访问控制系统的访问控制方法，其特征在于，所述数据属主运行客户端，对需上传的数据选取会话密钥并进行加密，之后根据访问结构树上每一叶子节点对应的父节点的阈值是否为1，来对各叶子节点进行分类，并进一步根据父节点类型的不同、对父节点的阈值为1的叶子节点的集合进行分类，之后根据分类结果对所述会话密钥加

密以得到会话密钥密文，之后将所述会话密钥密文和加密后的数据上传到云端的步骤包括以下步骤：

数据属主运行客户端，选取会话密钥 ck ，并采用对称加密算法加密需上传的数据 M ，得到加密后的数据 $E_{ck}(M)$ ；

输入系统公钥 PK 、会话密钥 ck 、以及访问结构树 T ，对于访问结构树 T 中的每个节点 x ，设置其孩子节点数为 num_x ，设置其阈值为 t_x ，且有 $0 < t_x \leq num_x$ ，定义多项式 q_x 的度为 d_x ，且 $d_x = t_x - 1$ ，节点 x 的孩子节点依次标记序号为 $1, \dots, num_x$ ， $index(x)$ 为返回节点 x 的序号， $att(x)$ 为返回与节点 x 相关联的属性， $type(att(x))$ 为返回属性 $att(x)$ 所在的表格门类，之后对于访问结构树 T 的根节点，选取随机数 $s \in \mathbb{Z}_p$ 并设定 $q_R(0) = s$ ，进一步随机选择 d_R 个子节点来完整定义多项式 q_R ，对于访问结构树 T 的除根节点以外的其它节点 x ，设定 $q_x(0) = q_{parent}(index(x))$ ，进一步随机选择 d_x 个子节点来完整定义多项式 q_x ；

对于访问结构树 T 的叶子节点 x ，若叶子节点 x 的父节点 $parent(x)$ 的阈值 $t_{parent(x)} = 1$ ，则 $q_x(0) = q_{parent(x)}(0)$ ，令 Y_1 为访问结构树 T 中该类叶子节点的集合、 Y_2 是访问结构树 T 中余下的叶子节点的集合，并进一步根据 Y_1 中各叶子节点的父节点类型的不同，将 Y_1 划分为 $Y_{11}, Y_{12}, \dots$ ；

根据如下公式对会话密钥加密，计算得到会话密钥密文 CT ：

$$\begin{aligned} CT &= (T, \tilde{C} = ck \cdot e(g, g)^{\alpha s}, C = h^s, \\ &\forall y \in Y_{1i} (i = 1, 2, \dots) : C_y = g^{q_{parent(y)}(0)}, C'_y = H(type(att(y)))^{q_{parent(y)}(0)}, \\ &\forall y \in Y_2 : C_y = g^{q_y(0)}, C'_y = H(att(y))^{q_y(0)}) \end{aligned}$$

其中， $\tilde{C}$ 为对会话密钥的计算， C 为对根节点的计算， C_y 为对属性 y 对应的属性值的计算， C'_y 为对属性 y 所在表格门类的计算；

将会话密钥密文 CT 和加密后的数据 $E_{ck}(M)$ 上传到云端。

6、如权利要求 5 所述的基于表格属性的云存储密文访问控制系统的访问控制方法，其特征在于，所述共享用户运行客户端，从云端下载会话密钥密文和

对应的共享数据，并当与自身用户私钥相关联的属性满足访问结构树时，由会话密钥密文解密得到会话密钥，之后利用解密得到的所述会话密钥解密所述对应的共享数据的步骤包括以下步骤：

共享用户运行客户端，从云端下载会话密钥密文 CT 和对应的共享数据 $E_{ck}(M)$ ，并输入系统公钥 PK 、用户拥有的属性集合 S 所对应的私钥 SK_S 、以及密钥密文 CT ；

共享用户调用预先定义的递归函数 $DecryptNode(CT, SK, x) = e(g, g)^{r_{q_x}(0)}$ ，若共享用户的属性集合 S 满足访问结构树 T ，则计算解密信息 A 为：

$$A = DecryptNode(CT, SK, R) = e(g, g)^{r_{q_R}(0)} = e(g, g)^{rs} ;$$

根据下式对会话密钥密文 CT 解密，得到会话密钥 ck ：

$$\frac{\tilde{C}}{e(C, D) / A} = \frac{ck \cdot e(g, g)^{\alpha s}}{e(h^s, g^{(\alpha+r)/\beta}) / e(g, g)^{rs}} = \frac{ck \cdot e(g, g)^{\alpha s}}{e(h^s, g^{(\alpha+r)/\beta}) / e(g, g)^{rs}} = ck ;$$

根据解密得到的会话密钥 ck 和共享数据 $E_{ck}(M)$ ，解密得到数据 M 。

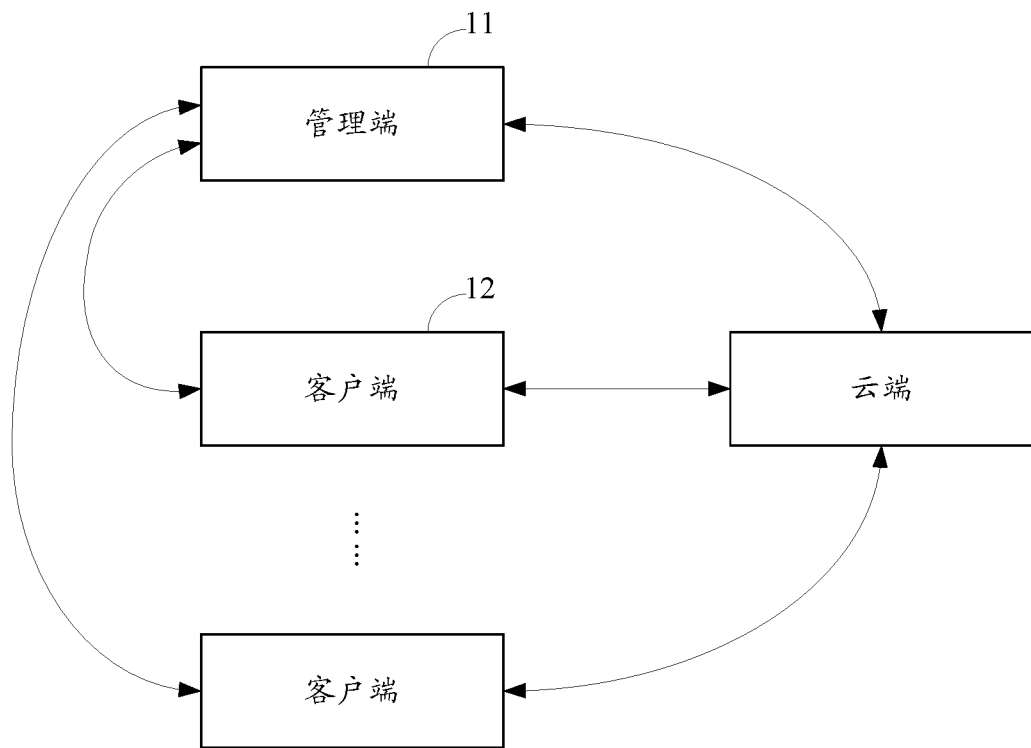


图 1

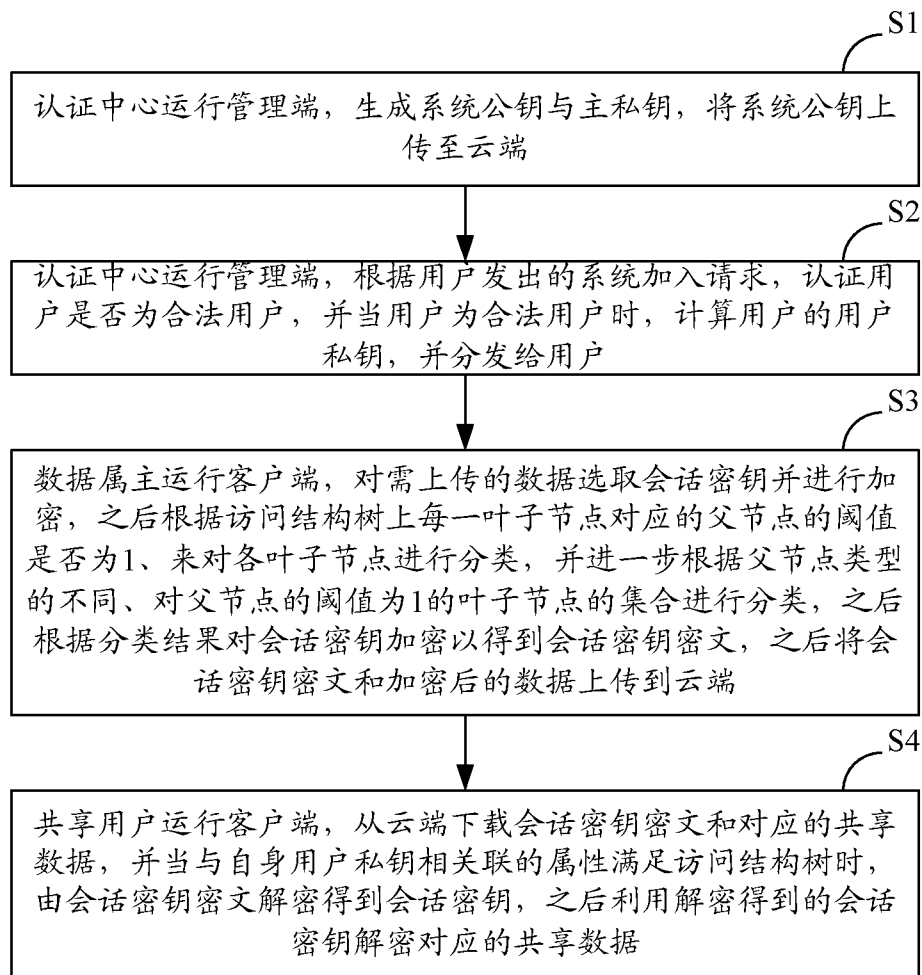


图 2

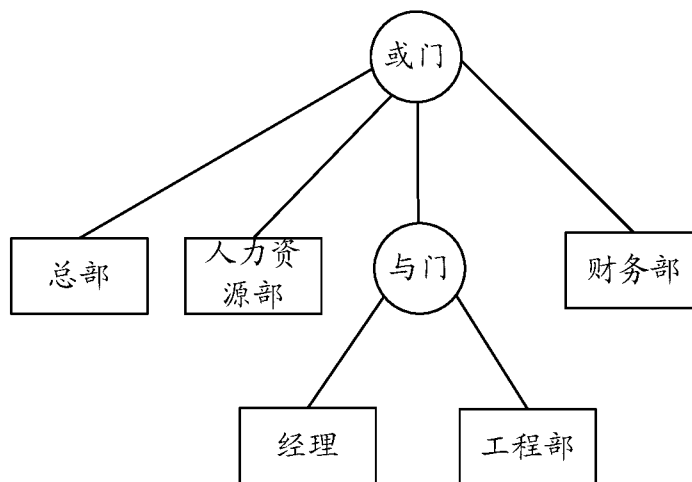


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/081386

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

DWPI; EPODOC; CNPAT; CNKI; 3GPP: cloud storage, structure tree, child, cloud, storage, structure, tree, download+, node, encrypt+, key, decrypt+, cipher, father, classif+, sub, threshold, leaf

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103297428 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 11 September 2013 (11.09.2013), see description, paragraphs [0034]-[0056] and [0084]-[0093], and figures 1 and 2	1-2
Y	CN 103297428 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 11 September 2013 (11.09.2013), see description, paragraphs [0034]-[0056] and [0084]-[0093], and figures 1 and 2	3-6
Y	CN 103618729 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 05 March 2014 (05.03.2014), see description, paragraphs [0022]-[0049]	3-6
PX	CN 105141574 A (SHENZHEN UNIVERSITY), 09 December 2015 (09.12.2015), claims 1-6	1-6
A	CN 102624522 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 01 August 2012 (01.08.2012), the whole document	1-6
A	US 2014325363 A1 (SPLUNK INC.), 30 October 2014 (30.10.2014), the whole document	1-6

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 16 June 2016 (16.06.2016)	Date of mailing of the international search report 20 July 2016 (20.07.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer SONG, Limei Telephone No.: (86-10) 62413431

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/081386

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103297428 A	11 September 2013	None	
CN 103618729 A	05 March 2014	None	
CN 105141574 A	09 December 2015	None	
CN 102624522 A	01 August 2012	None	
US 2014325363 A1	30 October 2014	US 2015149914 A1	28 May 2015
		US 2015325017 A1	12 November 2015
		US 2015138208 A1	21 May 2015
		US 2015143173 A1	21 May 2015
		US 2014320500 A1	30 October 2014
		US 2014320502 A1	30 October 2014
		US 2014324862 A1	30 October 2014
		US 2014325058 A1	30 October 2014
		US 2013247042 A1	19 September 2013
		US 2013247044 A1	19 September 2013
		US 2015333987 A1	19 November 2015
		US 2013247043 A1	19 September 2013
		US 2013239111 A1	12 September 2013
		US 2015089503 A1	26 March 2015

A. 主题的分类 H04L 29/06 (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)) DWPI; EPODOC; CNPAT; CNKI; 3GPP; 云存储, 云端, 结构树, 下载, 节点, 加密, 密钥, 解密, 父, 子, 分类, 阈值, 叶子, cloud, storage, structure, tree, download+, node, encrypt+, key, decrypt+, cipher, father, classif+, sub, threshold, leaf																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2</td> <td>1-2</td> </tr> <tr> <td>Y</td> <td>CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2</td> <td>3-6</td> </tr> <tr> <td>Y</td> <td>CN 103618729 A (南京邮电大学) 2014年 3月 5日 (2014 - 03 - 05) 参见说明书第22-49段</td> <td>3-6</td> </tr> <tr> <td>PX</td> <td>CN 105141574 A (深圳大学) 2015年 12月 9日 (2015 - 12 - 09) 权利要求1-6</td> <td>1-6</td> </tr> <tr> <td>A</td> <td>CN 102624522 A (华中科技大学) 2012年 8月 1日 (2012 - 08 - 01) 全文</td> <td>1-6</td> </tr> <tr> <td>A</td> <td>US 2014325363 A1 (SPLUNK INC.) 2014年 10月 30日 (2014 - 10 - 30) 全文</td> <td>1-6</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2	1-2	Y	CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2	3-6	Y	CN 103618729 A (南京邮电大学) 2014年 3月 5日 (2014 - 03 - 05) 参见说明书第22-49段	3-6	PX	CN 105141574 A (深圳大学) 2015年 12月 9日 (2015 - 12 - 09) 权利要求1-6	1-6	A	CN 102624522 A (华中科技大学) 2012年 8月 1日 (2012 - 08 - 01) 全文	1-6	A	US 2014325363 A1 (SPLUNK INC.) 2014年 10月 30日 (2014 - 10 - 30) 全文	1-6
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
X	CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2	1-2																					
Y	CN 103297428 A (南京邮电大学) 2013年 9月 11日 (2013 - 09 - 11) 参见说明书第34段-56段, 84段-93段, 附图1, 2	3-6																					
Y	CN 103618729 A (南京邮电大学) 2014年 3月 5日 (2014 - 03 - 05) 参见说明书第22-49段	3-6																					
PX	CN 105141574 A (深圳大学) 2015年 12月 9日 (2015 - 12 - 09) 权利要求1-6	1-6																					
A	CN 102624522 A (华中科技大学) 2012年 8月 1日 (2012 - 08 - 01) 全文	1-6																					
A	US 2014325363 A1 (SPLUNK INC.) 2014年 10月 30日 (2014 - 10 - 30) 全文	1-6																					
☐ 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 2016年 6月 16日		国际检索报告邮寄日期 2016年 7月 20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		授权官员 宋丽梅 电话号码 (86-10) 62413431																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/081386

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	103297428	A	2013年 9月 11日	无	
CN	103618729	A	2014年 3月 5日	无	
CN	105141574	A	2015年 12月 9日	无	
CN	102624522	A	2012年 8月 1日	无	
US	2014325363	A1	2014年 10月 30日	US 2015149914 A1	2015年 5月 28日
				US 2015325017 A1	2015年 11月 12日
				US 2015138208 A1	2015年 5月 21日
				US 2015143173 A1	2015年 5月 21日
				US 2014320500 A1	2014年 10月 30日
				US 2014320502 A1	2014年 10月 30日
				US 2014324862 A1	2014年 10月 30日
				US 2014325058 A1	2014年 10月 30日
				US 2013247042 A1	2013年 9月 19日
				US 2013247044 A1	2013年 9月 19日
				US 2015333987 A1	2015年 11月 19日
				US 2013247043 A1	2013年 9月 19日
				US 2013239111 A1	2013年 9月 12日
				US 2015089503 A1	2015年 3月 26日