(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103220291 A
(43)申请公布日 2013.07.24

(21)申请号 201310132586.2

(22)申请日 2013.04.09

(71)申请人 电子科技大学
地址 611731 四川省成都市高新西区西源大道2006号电子科技大学清水河校区计算机学院

(72)发明人 邢建川 韩帅

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)

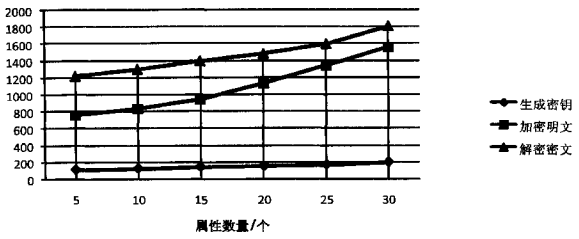
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种基于属性加密算法的访问控制方法

(57)摘要

本发明公开了一种基于属性加密算法的访问控制方法，包括初始化；数据文件的访问；访问权限的变更。利用基于属性加密算法在分布式环境下所具有的优势，有效解决了云计算环境下解密方不固定等数据文件共享方面所存在的问题。不仅支持了云计算环境下对于数据文件的安全访问，同时还充分考虑到用户权限的撤销及用户误读脏数据等方面的问题。



CN 103220291 A

1. 一种基于属性加密算法的访问控制方法，其特征在于，包括以下步骤：

A 初始化

A1)USER 向 CDC 发出存储数据文件请求，CDC 为数据文件生成 AES 加密密钥 Key，并对文件进行加密；

A2)CDC 对文件进行分块操作，进行 Merkle Hash Tree 的构造和文件根节点值的计；

A3)CDC 调用 PKeyGen() 函数为文件生成公开参数 P_k；

A4)CDC 调用 MKeyGen() 函数为文件生成主密钥 M_k；

A5)CDC 根据数据文件的实际权限划分需求，生成用于加密数据文件的属性集合 U，同时生成数据文件的属性列表 FAL；

A6)CDC 为拥有数据文件不同访问权限的所有 USER 生成相应的属性集合，所有 USER 的属性集合中必须包含文件关键属性 KA 和文件标识属性 RA，其中文件标识属性 RA 由步骤 A2) 计算得到的文件 Merkle Hash Tree 根节点值定义；

A7)CDC 根据数据文件的共享要求确定数据文件的访问控制树结构，访问控制树根节点的门限函数设置为与门，左子树由 KA 作为唯一叶子节点，右子树根节点的门限函数设置为与门，右子树的左子树由 RA 作为唯一叶子节点；

A8) 调用 Encrypt(P_k, M, T) 函数对密钥 Key 进行加密；

A9) 使用得到的密文生成解密信息列表 DIL；

A10) 调用 SKeyGen(M_k, A) 生成不同权限 USER 的私钥 S_k；

A11) 生成用户私钥列表 UKL；

A12) 将 FAL、DIL 和 UKL 通过通信信道传送给 TPA，TPA 对其进行副本的保存以备查验；

B 数据文件的访问

B1)USER 提出数据文件的访问请求，并使用 USER 的私钥对所请求的数据文件的相应访问控制密文进行解密；如果解密成功，则执行步骤 B2)；反之，则执行步骤 B7)；

B2)CDC 根据 USER 拥有的访问权限，限定 USER 对数据文件的操，如果 USER 拥有读权限，则执行步骤 B3)；反之，则执行步骤 B4)；

B3)USER 对数据文件进行读操作，操作结束之后，USER 向 CDC 交还数据文件的访问控制权，数据文件的访问操作结束；

B4)USER 对数据文件进行写操作，操作结束之后，CDC 将重新计算数据文件的文件 Merkle Hash Tree 根节点值，然后，CDC 根据 USER 的权限再分配请求为仍然拥有数据文件访问权限的 USER 更新私钥，最后，USER 向 CDC 交还数据文件的访问控制权，如果 USER 没有对任何数据文件的访问控制权限进行更改，则执行步骤 B5)；反之，则执行步骤 B6；

B5)CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL 和 UKL，同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL 和 UKL，数据文件的访问操作结束；

B6)CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL、UKL 和 DIL，同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL、UKL 和 DIL，数据文件的访问操作结束；

B7)USER 向 TPA 提出数据文件的访问请求，TPA 将 USER 的私钥信息与保存的 DIL 进行比对查验，如果 USER 仍拥有数据文件的访问权限，则 TPA 为 USER 分发新的私钥，然后执行步骤 B2；反之，则拒绝 USER 的数据文件访问请求，数据文件的访问操作结束；

C 访问权限的变更

C1) 撤销所有 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有 USER 失去对于数据文件的访问权限；

C2) 撤销所有拥有写操作权限 USER 的数据文件访问权限；

C3) 撤销所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限；

C4) 更改所有拥有写操作权限 USER 的数据文件访问权限，CDC 根据 USER 的请求为仍然拥有写操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有写操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止；

C5) 更改所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限，CDC 根据 USER 的请求为仍然拥有读操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有读操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止；

C6) 更改部分拥有写操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，CDC 根据 USER 的请求为相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除；

C7) 更改部分拥有读操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，CDC 根据 USER 的请求为相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除；

C8) 以上所有步骤操作完成之后，CDC 都将与 TPA 进行 FAL、UKL 和 DIL 的更新操作通信，更新 TPA 存储的数据文件 FAL、UKL 和 DIL。

2. 根据权利要求 1 所述的基于属性加密算法的访问控制方法，其特征在于，所述步骤 C2) 中对数据文件的关键属性 KA 进行更改，或者对数据文件的文件标识属性 RA 进行更改，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。

3. 根据权利要求 1 所述的基于属性加密算法的访问控制方法，其特征在于，所述 C4) 对数据文件的关键属性 KA 进行更改，或者对数据文件的文件标识属性 RA 进行更改，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。

一种基于属性加密算法的访问控制方法

技术领域

[0001] 本发明属于云计算技术领域，涉及一种基于属性加密算法的访问控制方法。

背景技术

[0002] 基于属性的加密算法通过加入对用户身份属性的描述，使用与门、或门和包含门等门限函数作为约束条件，显著提高了数据文件的共享能力，使系统在分布式环境下的访问控制效率明显优于传统的使用唯一身份标签的基于身份的加密算法，非常适用于云计算这种数据文件共享率很高的计算环境。将基于属性的加密算法应用到访问控制方案中的研究在很早之前便已受到业界的普遍关注，学者们提出的解决方案在权限撤销、门限函数的支持和代理重加密等方面也都取得了一定的成绩。但遗憾的是，大多数学者的研究内容仅局限于使用基于属性的加密算法解决传统计算模式中所存在的访问控制问题，而其中绝大多数的研究成果都不能够满足云计算环境下的应用需求。下面首先对学者们之前的相关研究成果进行一下总结。

[0003] 现有技术提出了一种以密文策略为基础的代理重加密访问控制方案，方案通过使用代理的方式，很好的解决了密文策略中用户权限撤销繁琐复杂的难题。但是，文章中描述的方案只是简单的以属性集合为单位进行访问权限的撤销，没有能够达到较为精细的权限撤销。中科院软件所的冯登国等人在现有技术中，提出了一套将基于密文策略的属性加密算法与公钥密码算法相结合的访问控制方案。不过遗憾的是，他们提出的方案使数据的拥有者承担了大量额外的重加密任务。现有技术通过扩展用户属性并加入终止时间标签的方式，设计了一套新颖的访问控制方案。但是，由于需要进行周期性的申请私钥工作，使用户背上了较为沉重的负担，同时也出现了许多诸如用户权限无法撤销的问题。现有技术假定服务提供商在一定程度上可信的情况下，设计了一套由服务提供商完成部分工作的基于密文策略的访问控制方案。该方案很好地利用了服务提供商庞大的计算资源，是研究领域的一大突破。不过遗憾的是，该方案的门限支持不足，访问控制策略不够灵活，很难在实际应用环境下发挥作用。此外，现有技术提出的基于属性加密的访问控制方案，创造性地将密钥分割和代理重加密技术结合了起来。但是方案没有对用户数据文件的完整性和一致性进行考虑，存在误读脏数据的安全风险。

发明内容

[0004] 本发明的目的是克服现有技术的缺陷，提供一种基于属性加密算法的访问控制方法，利用基于属性加密算法在分布式环境下所具有的优势，有效解决了云计算环境下解密方不固定等数据文件共享方面所存在的问题。不仅支持了云计算环境下对于数据文件的安全访问，同时还充分考虑到用户权限的撤销及用户误读脏数据等方面的问题。

[0005] 其技术方案为：

[0006] 一种基于属性加密算法的访问控制方法，包括以下步骤：

[0007] A 初始化

[0008] A1)USER 向 CDC 发出存储数据文件请求，CDC 为数据文件生成 AES 加密密钥 Key，并对文件进行加密；

[0009] A2)CDC 对文件进行分块操作，进行 Merkle Hash Tree 的构造和文件根节点值的计；

[0010] A3)CDC 调用 PKeyGen() 函数为文件生成公开参数 P_k；

[0011] A4)CDC 调用 MKeyGen() 函数为文件生成主密钥 M_k；

[0012] A5)CDC 根据数据文件的实际权限划分需求，生成用于加密数据文件的属性集合 U，同时生成数据文件的属性列表 FAL；

[0013] A6)CDC 为拥有数据文件不同访问权限的所有 USER 生成相应的属性集合，所有 USER 的属性集合中必须包含文件关键属性 KA 和文件标识属性 RA，其中文件标识属性 RA 由步骤 A2) 计算得到的文件 Merkle Hash Tree 根节点值定义；

[0014] A7)CDC 根据数据文件的共享要求确定数据文件的访问控制树结构，访问控制树根节点的门限函数设置为与门，左子树由 KA 作为唯一叶子节点，右子树根节点的门限函数设置为与门，右子树的左子树由 RA 作为唯一叶子节点；

[0015] A8) 调用 Encrypt(P_k, M, T) 函数对密钥 Key 进行加密；

[0016] A9) 使用得到的密文生成解密信息列表 DIL；

[0017] A10) 调用 SKeyGen(M_k, A) 生成不同权限 USER 的私钥 S_k；

[0018] A11) 生成用户私钥列表 UKL；

[0019] A12) 将 FAL、DIL 和 UKL 通过通信信道传送给 TPA，TPA 对其进行副本的保存以备查验；

[0020] B 数据文件的访问

[0021] B1)USER 提出数据文件的访问请求，并使用 USER 的私钥对所请求的数据文件的相应访问控制密文进行解密；如果解密成功，则执行步骤 B2)；反之，则执行步骤 B7)；

[0022] B2)CDC 根据 USER 拥有的访问权限，限定 USER 对数据文件的操，如果 USER 拥有读权限，则执行步骤 B3)；反之，则执行步骤 B4)；

[0023] B3)USER 对数据文件进行读操作，操作结束之后，USER 向 CDC 交还数据文件的访问控制权，数据文件的访问操作结束；

[0024] B4)USER 对数据文件进行写操作，操作结束之后，CDC 将重新计算数据文件的文件 Merkle Hash Tree 根节点值，然后，CDC 根据 USER 的权限再分配请求为仍然拥有数据文件访问权限的 USER 更新私钥，最后，USER 向 CDC 交还数据文件的访问控制权，如果 USER 没有对任何数据文件的访问控制权限进行更改，则执行步骤 B5)；反之，则执行步骤 B6；

[0025] B5)CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL 和 UKL，同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL 和 UKL，数据文件的访问操作结束；

[0026] B6)CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL、UKL 和 DIL，同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL、UKL 和 DIL，数据文件的访问操作结束；

[0027] B7)USER 向 TPA 提出数据文件的访问请求，TPA 将 USER 的私钥信息与保存的 DIL 进行比对查验，如果 USER 仍拥有数据文件的访问权限，则 TPA 为 USER 分发新的私钥，然后执行步骤 B2；反之，则拒绝 USER 的数据文件访问请求，数据文件的访问操作结束；

[0028] C 访问权限的变更

[0029] C1) 撤销所有 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有 USER 失去对于数据文件的访问权限；

[0030] C2) 撤销所有拥有写操作权限 USER 的数据文件访问权限；

[0031] C3) 撤销所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限；

[0032] C4) 更改所有拥有写操作权限 USER 的数据文件访问权限，CDC 根据 USER 的请求为仍然拥有写操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有写操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止；

[0033] C5) 更改所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限，CDC 根据 USER 的请求为仍然拥有读操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有读操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止；

[0034] C6) 更改部分拥有写操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，CDC 根据 USER 的请求为相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除；

[0035] C7) 更改部分拥有读操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，CDC 根据 USER 的请求为相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除；

[0036] C8) 以上所有步骤操作完成之后，CDC 都将与 TPA 进行 FAL、UKL 和 DIL 的更新操作通信，更新 TPA 存储的数据文件 FAL、UKL 和 DIL。

[0037] 进一步优选，所述步骤 C2) 中对数据文件的关键属性 KA 进行更改，或者对数据文件的文件标识属性 RA 进行更改，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。

[0038] 进一步优选，所述 C4) 对数据文件的关键属性 KA 进行更改，或者对数据文件的文件标识属性 RA 进行更改，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。

[0039] 本发明的有益效果：

[0040] 本发明通过将文件关键属性 KA 和文件标识属性 RA 引入进来，不仅使方案所述的基于属性的加密算法仍然能够支持与门、或门和包含门等门限函数。同时，也使得 CDC 在撤销特定 USER 的访问权限时，无需更新其他所有 USER 的私钥组件，从而使方案成功地避免了大量的密钥生成和访问权限的重新加密工作。因此，本发明所述方案能够有效地提高云计算环境下共享数据文件的海量用户的权限变更速率。

附图说明

[0041] 图 1 为访问控制结构；

[0042] 图 2 为本发明采用的访问控制树结构；

[0043] 图 3 为本发明的初始化过程；

[0044] 图 4 为本发明文件的访问流程图；

[0045] 图 5 为更改文件标识属性 RA；

[0046] 图 6 为更改文件关键属性 KA；

[0047] 图 7 为更改访问控制结构特定属性 A_1；

[0048] 图 8 为属性加密算法中属性数量与时间的关系。

具体实施方式

[0049] 下面结合附图和具体实施例来详细描述本发明的技术方案。

[0050] 安全假定

[0051] 方案假定所有的通信信道不存在恶意丢包的情况发生（通信信道包括USER与CDC之间、CDC 与 TPA 之间和 TPA 与 USER 之间三部分）。同时，方案中的 TPA 是无偏见的、完全可信的第三方审计机构，能够忠实的完成 USER 委托的所有任务。本发明的 CDC 与以往方案中的 CDC 略有不同，方案中的 CDC 尽管拥有好奇心，但能够忠实的完成任务，不再完全不可信。CDC 承担的所有参数计算、加密任务和密钥生成及分发工作，都可以保证结果的绝对正确性、无欺骗性和不可抵赖性。CDC 能够无条件响应任意 USER 在任意时间发出的文件访问请求，并严格遵守方案制定的协议规定进行密钥的生成、变更和分发工作。此外，TPA 能够实时更新 CDC 传送的访问控制和文件信息，对 CDC 进行监督。

[0052] 基于属性加密算法的访问控制方案描述

[0053] 方案参与者

[0054] 方案的主要参与者由三部分组成：用户 (USER)、云计算数据中心 (CDC) 和可信第三方审计机构 (TPA)。三部分通过网络连接进行通信。

[0055] USER 由数据文件的拥有者和使用者两大群体组成。数据文件的拥有者定义为拥有权限对存储在 CDC 中的数据文件进行读和写操作（包括插入、删除和修改等动态操作）的用户群体，而数据的使用者仅拥有对数据文件进行读操作的权限。本方案允许数据文件拥有不止一个的拥有者和使用者，充分支持云计算环境下对于数据文件的共享需求。此外，USER 还能够与 TPA 进行通信，并发出身份验证的请求，更新自己的私钥。

[0056] CDC 作为云计算数据存储服务的提供者，不仅提供了海量的数据存储空间供 USER 使用，还负责 USER 的访问控制认证工作。本方案中，CDC 响应所有通过访问控制认证用户的数据文件操作请求，并按照预先设定的用户权限划分策略对 USER 的数据文件操作请求进行限制。CDC 为所有数据文件保留操作日志，以供日后的查验之用。此外，CDC 还负责对数据文件进行加密以及用户密钥的生成和分发工作，并与 TPA 进行信息的实时更新，保证 TPA 存储的数据文件访问控制信息的实效性。

[0057] TPA 作为可信的第三方审计机构，负责维护所有用户数据文件的访问控制信息，并响应 USER 的身份验证和密钥更新请求。此外，TPA 具有对存储在 CDC 中的用户数据文件进行审查的能力，能够代替 USER 对存储在 CDC 中的数据文件进行监管。

[0058] 方案相关定义

[0059] 定义 1 访问控制结构：基于属性加密算法的访问控制结构是一个树状结构，能够

描述加密算法的访问控制策略。树中的每个叶子节点均对应属性集合中的一个属性，非叶子节点则与门限函数（与门、或门或包含门）相对应。访问控制树中的每个内部节点都控制着一个权限，自底向上，越靠近根节点，则权限越大。如图 1 所示的访问控制结构中，X、Y 和 Z 均为相应属性集合中的一个属性，内部节点由门限函数 OR 和 AND 控制，由于 AND 节点是根节点，因此其代表的权限要大于 OR 节点所代表的权限。

[0060] 定义 2 属性集合：在进行密钥生成工作之前，CDC 会为每一个数据文件专门生成一个具备足够权限划分能力的属性集合 $U = \{U_1, U_2, U_3, U_4, \ldots, U_n\}$。同时，每个对数据文件拥有访问权限的用户也都会拥有一个与自己私钥相关联的属性集合 $P = \{P_1, P_2, P_3, P_4 \ldots, P_m\}(m \leqslant n)$。所有用户的属性集合 P 均为集合 U 的一个非空子集。

[0061] 定义 3 文件关键属性 KA(Key-Attribute)：方案规定，方案中的访问控制树由 KA 作为其根节点的唯一左孩子节点，根节点的门限函数设置为与门。同时，赋予根节点对数据文件进行修改的权限，即写操作。方案的访问控制树如图 2 所示。

[0062] 方案通过关键属性 KA 的引入，使数据文件在进行权限撤销的过程中可以不必更改其他私钥组件，简化了权限的撤销和再分配。

[0063] 定义 4 文件标识属性 RA(Root-Attribute)：方案使用的文件 Merkle Hash Tree 根节点值作为文件标识属性 RA。方案中的访问控制树由 RA 作为其右子树的唯一左孩子节点，右子树根节点的门限函数设置为与门，如图 2 所示。文件标识属性 RA 的引入，使得 USER 每次对数据文件进行访问之前，都可以通过自身的私钥对数据文件进行是否与上次访问版本一致的验证。该策略使所有拥有文件访问权限的 USER 能够在第一时间知晓文件的变更情况，加强了避免用户误读脏数据的能力。

[0064] 定义 5 用户私钥列表 UKL(User Key List)：该列表一式两份，分别由 CDC 和 TPA 保管，列表记录了拥有数据文件访问权限的所有 USER 的私钥及其变更情况。CDC 负责为每个数据文件创建 UKL，并根据 USER 私钥的变更情况对 UKL 进行更新。同时，CDC 在与 TPA 进行通信过程中将对 UKL 能够进行实时更新，以保证 UKL 为最新版本。

[0065] 定义 6 文件属性列表 FAL(File Attribute List)：该列表一式两份，分别由 CDC 和 TPA 保管，列表记录了数据文件的属性集合信息。CDC 负责为每个数据文件创建 FAL，并根据数据文件属性集合的变更情况对 FAL 进行更新。同时，CDC 在与 TPA 进行通信过程中将对 UKL 能够进行实时更新，以保证 UKL 是当前最新的版本。

[0066] 定义 7 解密信息列表 DIL(Decryption Information List)：该列表一式两份，分别由 CDC 和 TPA 保管，列表记录了加密后的数据文件对称密钥和 USER 的权限信息。CDC 负责为数据文件创建 DIL，并根据数据文件的加密密钥和访问控制权限信息的变更情况对 DIL 进行更新。同时，CDC 在与 TPA 进行通信过程中将对 DIL 能够进行实时更新，以保证 DIL 为最新版本。

[0067] 定义 8 主要函数定义：

[0068] $1P_k = PKeyGen()$：该函数用来生成公开参数 P_k。函数在初始阶段将选择一个阶为素数 p，生成元为 g 的双线性群 G，并作双线性配对运算 $e: G \times G \rightarrow G_t$。属性空间 $U = \{U_1, U_2, U_3, \ldots, U_n\}$，$U_i \in U(1 \leqslant i \leqslant n)$，随机选取 x_i、a、$b \in Z_p$。函数 PKeyGen() 如公式 4-1 所示。

[0069] $$\{G_t, g, g_b, e(g,g)^a, \{T_i = g_{x_i}\}_{i=1}^n\} \qquad (4\text{-}1)$$

[0070] $2M_k$ = MKeyGen()：该函数用来生成主密钥 M_k。其中 g、a、b 的定义如上，函数 MkeyGen() 如公式 4-2 所示。

[0071] $$\{g^a, b, \{x_i\}_{i=1}^n\} \quad (4\text{-}2)$$

[0072] 3、C = Encrypt(P_k, M, T)：该函数使用公开参数 P_k 和访问控制结构 T 对明文 M 进行加密，并得到密文 C。令构造的访问控制结构 T 的任意节点 y 的值为 k_y，为节点随机生成 (k_y-1) 次的多项式 q_y，则 $q_y(0)$ 为节点保存的秘密信息。令 $q_R(0) = s, s \in Z_p$，且为随机选取，其中 R 代表根节点。相应的，其他节点 y 的 $q_y(0) = q_{father(y)}(tag(y))$，其中 father(y) 代表 y 的父亲节点，tag(y) 代表节点 y 的编号。再令 X 为所有叶子节点的集合，Γ 为满足相应访问控制结构的授权集集合要求。函数 Encrypt(P_k, M, T) 如公式 4-3 所示。其中，att(x) 返回节点 x 的属性信息。

[0073] $$(\Gamma, \tilde{C} = Me(g, g)^{as}, C = g^{bs}, \forall x \in X: C_x = g^{q_y(0)}, C_x' = T_{att(x)}^{q_y(0)}) \quad (4\text{-}3)$$

[0074] 4、S_k = SKeyGen(M_k, A)：该函数使用主密钥 M_k 和用户属性集合 A 生成用户私钥 S_k。A 作为用户私钥所关联的属性集合，是数据文件属性集合 U 的一个非空子集。选择随机数 $\gamma \in Z_p$，单独属性 $s \in A$，随机数 $\gamma_s \in Z_p$。函数 SKeyGen(M_k, A) 如公式 4-4 所示。

[0075] $$(D = g^{(a+\gamma)/b}, \forall s \in A: D_s = g^{\gamma} T_s^{\gamma_s}, D_s' = g^{\gamma_s}) \quad (4\text{-}4)$$

[0076] 5、M = Decrypt(C, S_k)：该函数使用用户私钥 S_k 解密密文 CT 得到明文 M。定义该函数之前，首先定义递归运算 Decrypt(C, S_k, y)，令 i = att(x)，每个叶子节点 y 都可计算递归函数 DecryptN(C, S_k, y) 如公式 4-5 所示。

[0077] $$\begin{cases} \dfrac{e(D_i, C_y)}{e(D_i', C_y')} = e(g,g)^{\gamma q_y(0)}, i \in A \\ \perp, i \notin A \end{cases} \quad (4\text{-}5)$$

[0078] 每一个非叶子节点 y，最少可利用 k_y 个 $e(g,g)^{\gamma q_y(0)}$ 作为拉格朗日多项式插值节点，经过计算得到 $e(g,g)^{\gamma q_{z_s}(0)}$，$e(g,g)^{\gamma q_y(0)}$ 可以通过节点 y 的孩子节点 $\{Z_s\}$ 计算得来。假设 $V = e(g,g)^{\gamma q_R(0)} = e(g,g)^{\gamma s}$，则 Decrypt(C, S_k) 如公式 4-6 所示。

[0079] $$\tilde{C} / e(C, D) / V \quad (4\text{-}6)$$

[0080] 方案具体实现

[0081] 本发明提出的基于属性加密算法的访问控制方案是由 USER、CDC 和 TPA 三部分组成。因此，方案的初始化也需要三部分的共同协作。初始化的实现如图 3 所示，具体步骤描述如下：

[0082] (1)、USER 向 CDC 发出存储数据文件请求。CDC 为数据文件生成 AES 加密密钥 Key，并对文件进行加密。

[0083] (2)、CDC 对文件进行分块操作，进行 Merkle Hash Tree 的构造和文件根节点值的计算。

[0084] (3)、CDC 调用 PKeyGen() 函数为文件生成公开参数 P_k。

[0085] (4)、CDC 调用 MKeyGen() 函数为文件生成主密钥 M_k。

[0086] (5)、CDC 根据数据文件的实际权限划分需求，生成用于加密数据文件的属性集合

U，同时生成数据文件的属性列表 FAL。

[0087] (6)、CDC 为拥有数据文件不同访问权限的所有 USER 生成相应的属性集合。需要说明的是，所有 USER 的属性集合中必须包含文件关键属性 KA 和文件标识属性 RA，其中文件标识属性 RA 由步骤 (2) 计算得到的文件 Merkle Hash Tree 根节点值定义。

[0088] (7)、CDC 根据数据文件的共享要求确定数据文件的访问控制树结构。访问控制树顶端的基本结构必须遵循图 4-2 所示的结构要求，即访问控制树根节点的门限函数设置为与门，左子树由 KA 作为唯一叶子节点，右子树根节点的门限函数设置为与门，右子树的左子树由 RA 作为唯一叶子节点。

[0089] (8)、调用 Encrypt(P_k, M, T) 函数对密钥 Key 进行加密。

[0090] (9)、使用得到的密文生成解密信息列表 DIL。

[0091] (10)、调用 SKeyGen(M_k, A) 生成不同权限 USER 的私钥 S_k。

[0092] (11)、生成用户私钥列表 UKL。

[0093] (12)、将 FAL、DIL 和 UKL 通过通信信道传送给 TPA，TPA 对其进行副本的保存以备查验。

[0094] 数据文件的访问

[0095] 方案规定，拥有写操作权限的 USER 只要对数据文件进行了修改，则所有拥有该数据文件访问权限的 USER 的私钥都将随着文件 Merkle Hash Tree 根节点值的改变而失效，所有 USER 的访问控制权限都将被重新授予。当 USER 使用失效的密钥提出数据文件的访问请求时，CDC 将会将请求转交给 TPA 进行处理，TPA 在确认 USER 的身份之后，会根据数据文件新的访问控制权限进行私钥的重新发放等操作。如果 USER 仍然拥有数据文件的访问权限，则 TPA 将为 USER 发放新的私钥，以使 USER 能够对数据文件进行相应的操作；反之，则 TPA 拒绝 USER 的文件访问请求。算法的具体执行步骤如图 4 所示，详细描述如下：

[0096] A：USER 提出数据文件的访问请求，并使用 USER 的私钥对所请求的数据文件的相应访问控制密文进行解密；如果解密成功，则执行步骤 B；反之，则执行步骤 G。

[0097] B：CDC 根据 USER 拥有的访问权限，限定 USER 对数据文件的操作。如果 USER 拥有读权限，则执行步骤 C；反之，则执行步骤 D。

[0098] C：USER 对数据文件进行读操作。操作结束之后，USER 向 CDC 交还数据文件的访问控制权。数据文件的访问操作结束。

[0099] D：USER 对数据文件进行写操作（插入、删除或修改等）。操作结束之后，CDC 将重新计算数据文件的文件 Merkle Hash Tree 根节点值。然后，CDC 根据 USER 的权限再分配请求为仍然拥有数据文件访问权限的 USER 更新私钥（包括当前访问 USER）。最后，USER 向 CDC 交还数据文件的访问控制权。如果 USER 没有对任何数据文件的访问控制权限进行更改，则执行步骤 E；反之，则执行步骤 F。

[0100] E：CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL 和 UKL。同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL 和 UKL。数据文件的访问操作结束。

[0101] F：CDC 根据 USER 对于数据文件的访问权限的修改，更新数据文件的 FAL、UKL 和 DIL。同时，CDC 与 TPA 进行实时通信，更新 TPA 存储的 FAL、UKL 和 DIL。数据文件的访问操作结束。

[0102] G：USER 向 TPA 提出数据文件的访问请求，TPA 将 USER 的私钥信息与保存的 DIL 进

行比对查验。如果 USER 仍拥有数据文件的访问权限，则 TPA 为 USER 分发新的私钥，然后执行步骤 B ；反之，则拒绝 USER 的数据文件访问请求。数据文件的访问操作结束。

[0103] 访问权限的变更

[0104] 基于属性的加密算法使得方案中数据文件的访问控制由 USER 拥有的属性集合和数据文件的访问控制树结构共同决定。方案规定，拥有写操作权限 USER 的属性集合必须包含文件关键属性 KA 和文件标识属性 RA，拥有读操作权限 USER 的属性集合必须包含文件标识属性 RA，这使得方案在很大程度上简化了数据文件访问控制权限的撤销过程。此外，作为 RA 的文件 Merkle Hash Tree 根节点值的引入，使得所有 USER 在访问数据文件之前便可获知数据文件是否与最近一次访问时一致。不仅使数据文件的拥有者能够更为方便快捷地更改或撤销数据文件的访问权限，同时也避免了 USER 读到脏数据的情况发生。文件访问权限的变更操作具体描述如下 ：

[0105] (1)、撤销所有 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改。由于方案访问控制结构的特殊性，RA 的更改将使得所有 USER 失去对于数据文件的访问权限，如图 5 所示。

[0106] (2)、撤销所有拥有写操作权限 USER 的数据文件访问权限，可以采用两种方法。一是，对数据文件的关键属性 KA 进行更改，如图 6 所示。二是，对数据文件的文件标识属性 RA 进行更改，如图 4-5 所示。由于方案访问控制结构的特殊性，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。

[0107] (3)、撤销所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改。由于方案访问控制结构的特殊性，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限，如图 5 所示。

[0108] (4)、更改所有拥有写操作权限 USER 的数据文件访问权限，可以采用两种方法。一是，对数据文件的关键属性 KA 进行更改，如图 6 所示。二是，对数据文件的文件标识属性 RA 进行更改，如图 5 所示。由于方案访问控制结构的特殊性，KA 和 RA 的更改都将使得所有拥有写操作权限的 USER 失去对于数据文件的写操作权限。随后，CDC 根据 USER 的请求为仍然拥有写操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有写操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止。

[0109] (5)、更改所有拥有读操作权限 USER 的数据文件访问权限，只需对数据文件的文件标识属性 RA 进行更改。由于方案访问控制结构的特殊性，RA 的更改将使得所有拥有读操作权限的 USER 失去对于数据文件的读操作访问权限，如图 5 所示。随后，CDC 根据 USER 的请求为仍然拥有读操作权限的 USER 重新生成新的私钥，并保留其旧私钥用来帮助 TPA 进行之后私钥的重新分配工作，旧私钥将一直保留到仍然拥有读操作权限的 USER 获取了最新的私钥或是其不再拥有访问权限为止。

[0110] (6)、更改部分拥有写操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，如图 7 所示。随后，CDC 根据 USER 的请求为相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除。

[0111] (7)、更改部分拥有读操作权限 USER 的数据文件访问权限，只需对相关 USER 属性集合中非 KA 和 RA 的特定属性参数进行更改，如图 7 所示。随后，CDC 根据 USER 的请求为

相关 USER 重新生成新的私钥或将相关 USER 的访问权限信息删除。

[0112] (8)、以上所有步骤操作完成之后，CDC 都将与 TPA 进行 FAL、UKL 和 DIL 的更新操作通信，更新 TPA 存储的数据文件 FAL、UKL 和 DIL。

[0113] 方案首先使用 AES 对称加密算法对数据文件进行了加密，AES 对称加密算法已经被证明拥有较高的安全性，因此存储在 CDC 中的数据文件能够有效避免忠实但好奇假设的 CDC 的窥探。此外，方案使用基于密文策略的属性加密算法对对称密钥进行了加密。基于密文策略的属性加密算法是通过属性集合和访问控制树结构共同保障算法的机密性与安全性，方案中定义使用的基于密文策略的属性加密算法与现有技术提出的基于密文策略的属性加密算法拥有相同的密文形式、访问控制结构和解密过程，所以方案中基于密文策略的属性加密算法的安全性可以参考现有技术中算法的安全性。由于现有技术已经证明了其算法具有极高的安全性，因此方案使用的基于密文策略的属性加密算法也可证明是安全的，进而方案中密钥和访问控制权限信息的安全性也就得到了保障。由于方案使用了本发明所述的云计算数据存储安全体系架构，并基于一定的安全假设（通信信道可靠、TPA 可信和 CDC 忠实等）。因此，数据文件访问控制权限的验证工作在引入了 TPA 之后，比传统的访问控制方案在访问权限变更后的认证和私钥再分配方面拥有了更好的安全保障。此外，文件关键属性 KA 和文件标识属性 RA 的引入，有效地避免了数据文件变更之后 USER 在不知情的情况下误读脏数据情况的发生。非常适用于在云计算环境下对于敏感数据文件的存储。

[0114] 在时间开销方面，USER 将大量的加密任务和密钥生成及分配工作交由 CDC 完成，节省了 USER 大量的计算资源和时间，更好的发挥了云计算环境下 CDC 所拥有的庞大计算能力。同时，方案通过使用 2.3.3 节描述的云计算数据存储安全体系架构，将可信第三方审计机构引入进来，支持了公开审计。USER 可以不必再亲自完成对存储在 CDC 中的数据文件的验证工作，节省了 USER 的宝贵时间，也使还使得数据文件的审计能力得到了加强。

[0115] 本发明使用基于 Linux 系统的 cpabe-0.7 属性加密算法库函数进行了相关仿真实验代码的编写。实验环境为在 Windows XP 操作系统搭建的 VMware Workstation6.0 虚拟机上运行 Ubuntu10.04，处理器为奔腾双核 E5300 处理器，内存容量为 0.5GB，加密明文大小为 0.5M。

[0116] 仿真实验通过模拟真实加解密运行环境，分别记录了在不同属性数量的情况下，基于属性加密算法的密钥生成、加密明文以及解密密文所耗费的时间，如图 8 所示。

[0117] 由仿真实验的结果可知，基于属性的加密算法在加密明文和解密密文过程中的时间耗费会随着属性数量的增加而大幅度地增多，密钥生成的时间耗费也会随着属性数量的增加而略微增多。因此，在基于属性的加密算法中尽量减少密钥的生成以及加密明文和解密密文的次数，能够有效地提高将基于属性的加密算法应用到访问控制方案的工作效率。

[0118] 本发明所述方案，通过将文件关键属性 KA 和文件标识属性 RA 引入进来，不仅使方案所述的基于属性的加密算法仍然能够支持与门、或门和包含门等门限函数。同时，也使得 CDC 在撤销特定 USER 的访问权限时，无需更新其他所有 USER 的私钥组件，从而使方案成功地避免了大量的密钥生成和访问权限的重新加密工作。因此，本发明所述方案能够有效地提高云计算环境下共享数据文件的海量用户的权限变更速率。

[0119] 在存储空间的开销方面，方案为每个数据文件额外添加了用户私钥列表 UKL、文件属性列表 FAL 和解密信息列表 DIL，所有列表均一式两份，分别由 CDC 和 TPA 保管。UKL 占

用空间的大小由共享数据文件的 USER 数量决定，FAL 占用空间的大小由文件的属性集合大小决定，DIL 占用空间的大小则由共享文件的 USER 数量和当前时刻待更新的私钥数量所共同决定。

[0120] 以上所述，仅为本发明较佳的具体实施方式，本发明的保护范围不限于此，任何熟悉本技术领域的技术人员在本发明披露的技术范围内，可显而易见地得到的技术方案的简单变化或等效替换均落入本发明的保护范围内。

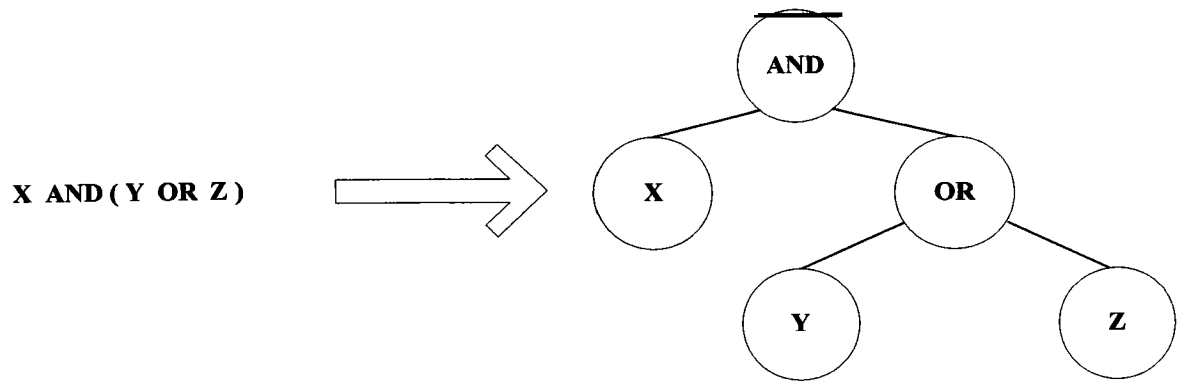


图 1

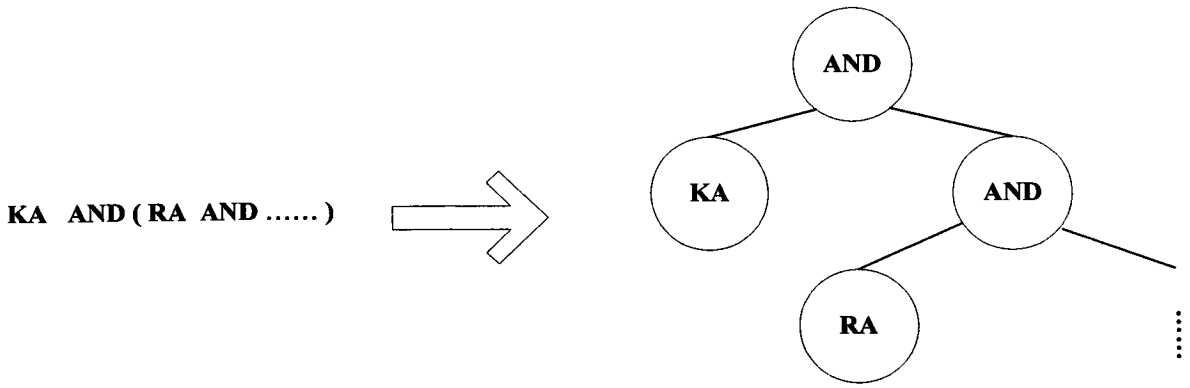


图 2

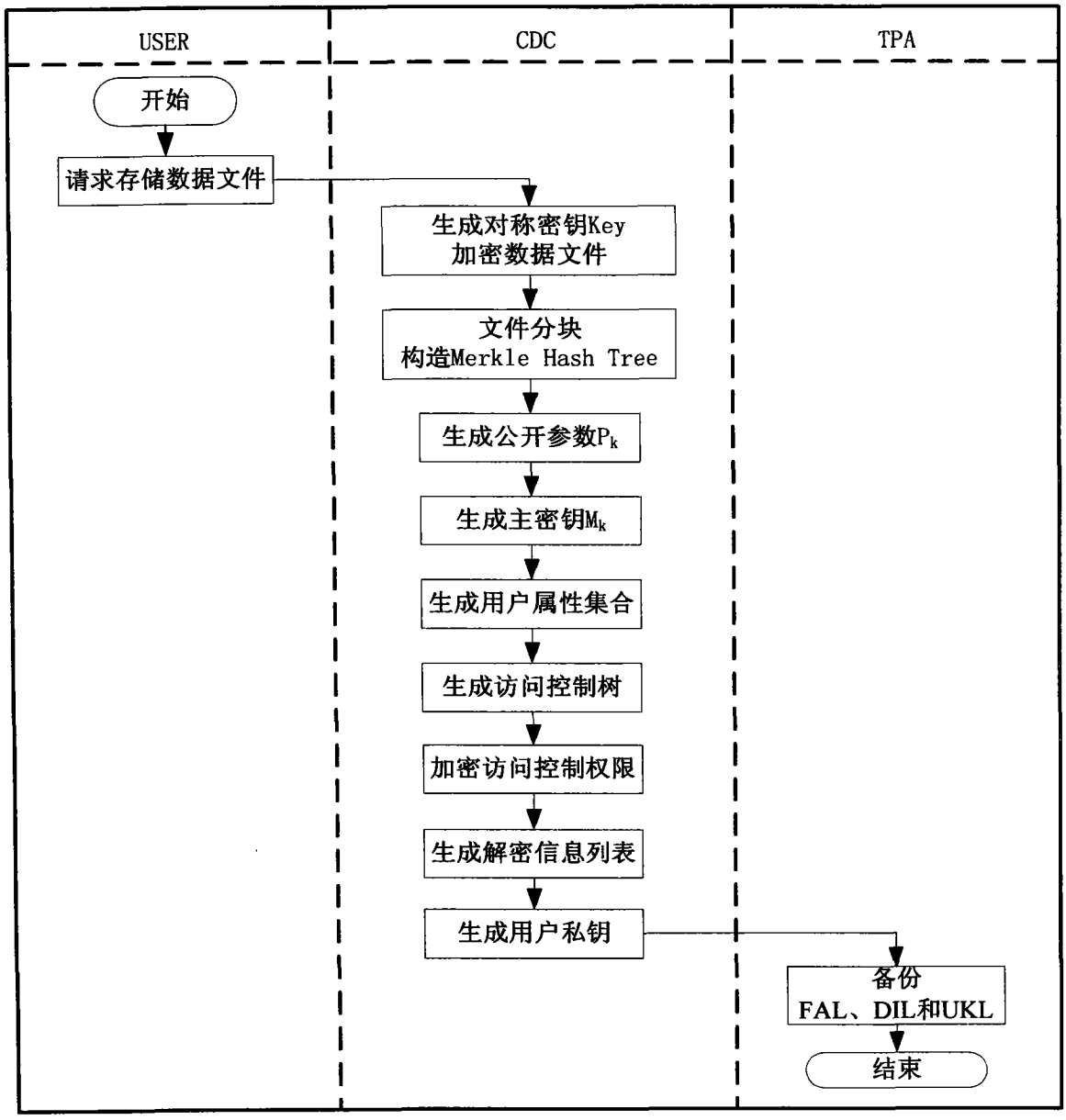

USER
CDC
TPA
开始
请求存储数据文件
生成对称密钥Key
加密数据文件
文件分块
构造Merkle Hash Tree
生成公开参数P_k
生成主密钥M_k
生成用户属性集合
生成访问控制树
加密访问控制权限
生成解密信息列表
生成用户私钥
备份
FAL、DIL和UKL
结束

图 3

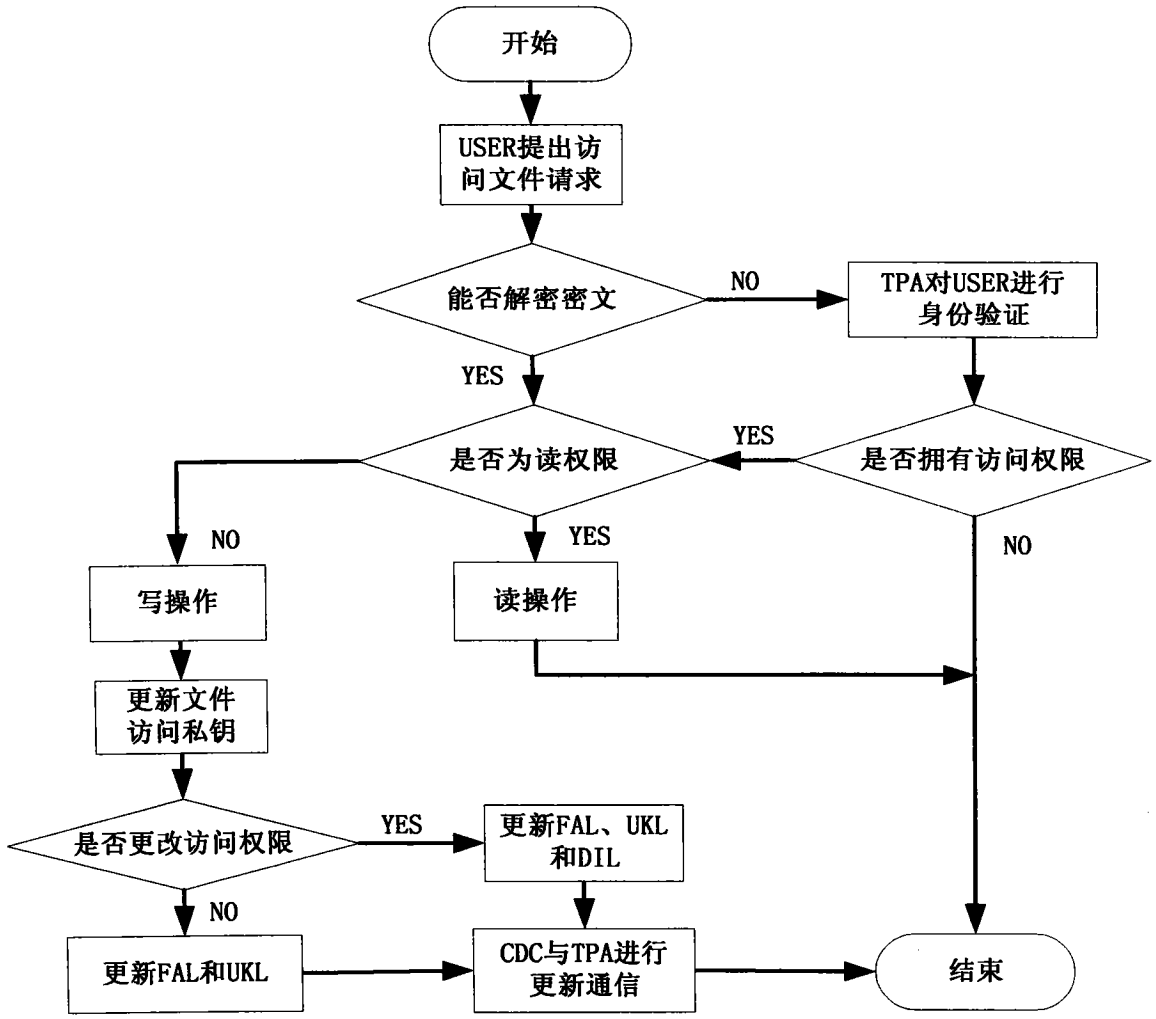

开始
USER提出访问文件请求
能否解密密文
NO
TPA对USER进行身份验证
YES
是否为读权限
YES
是否拥有访问权限
NO
YES
NO
写操作
读操作
更新文件访问私钥
是否更改访问权限
YES
更新FAL、UKL和DIL
NO
更新FAL和UKL
CDC与TPA进行更新通信
结束

图 4

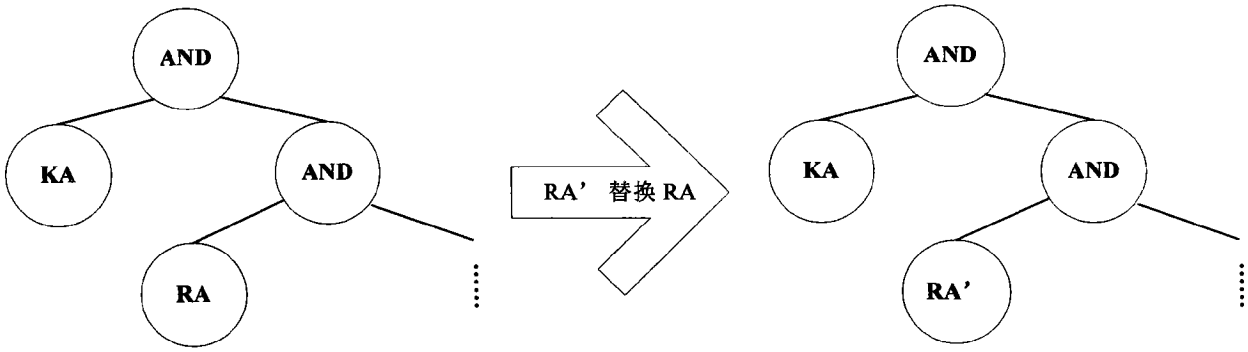

AND
KA
AND
RA
RA' 替换 RA
AND
KA
AND
RA'

图 5

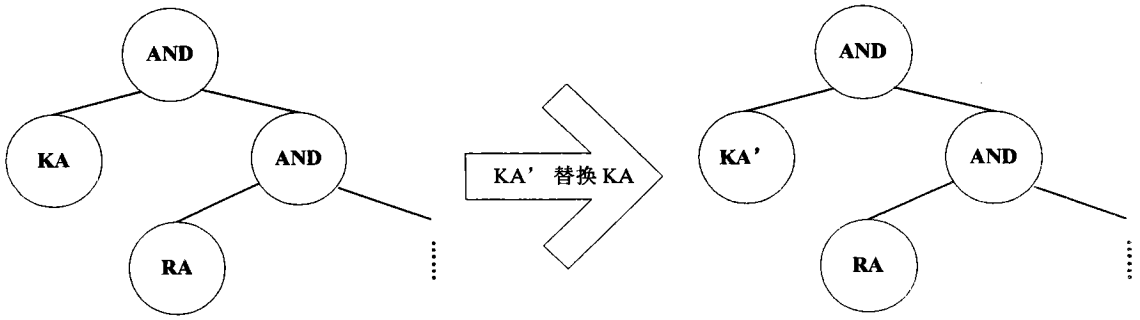

AND
KA
AND
RA
KA' 替换 KA
AND
KA'
AND
RA

图 6

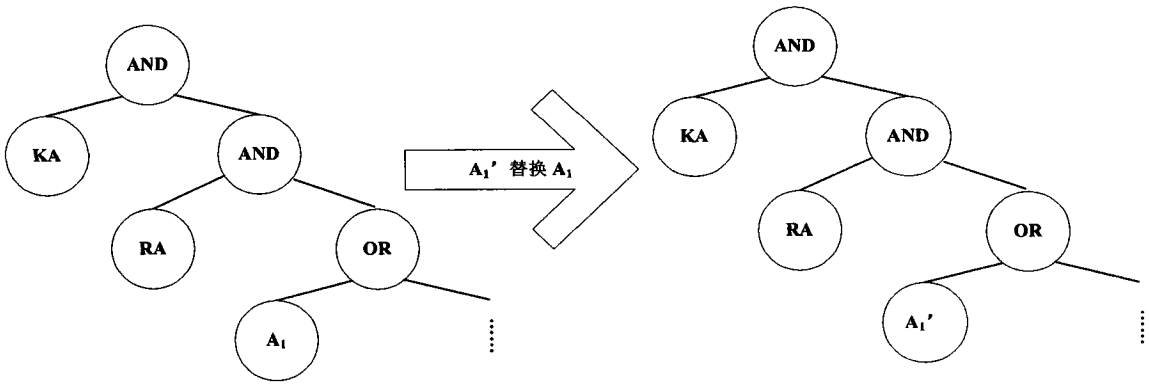

AND
KA
AND
RA
OR
A1
A1' 替换 A1
AND
KA
AND
RA
OR
A1'

图 7

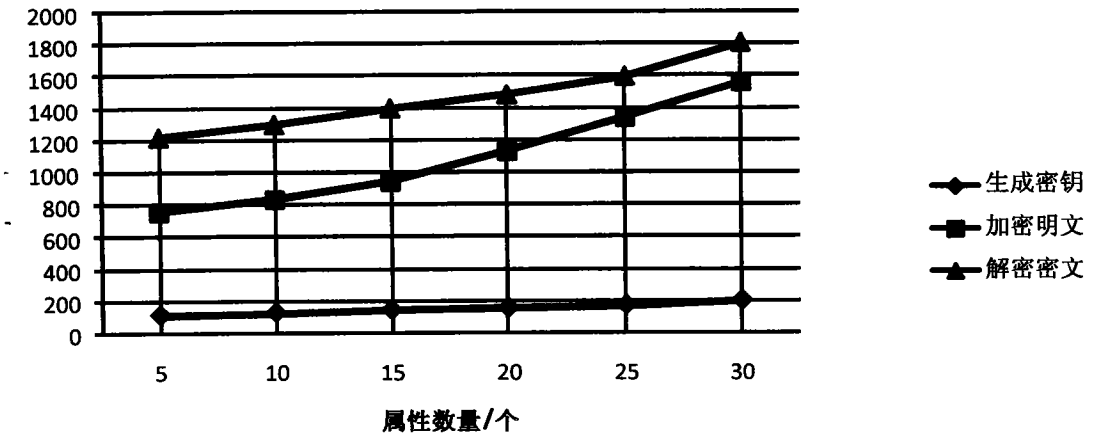

2000
1800
1600
1400
1200
1000
800
600
400
200
0
5
10
15
20
25
30
属性数量/个
生成密钥
加密明文
解密密文

图 8