一种属性可撤销的安全云存储模型

张柄虹[1] 张串绒[1] 焦和平[2] 张欣威[1]
(空军工程大学信息与导航学院 西安 710077)[1] (西北工业大学 西安 710072)[2]

摘 要 针对云存储服务中数据用户权限撤销粒度较粗及现有方案密钥分发计算量大等问题,基于双系统加密的思想,在合数阶双线性群上提出了一种新的细粒度权限撤销的安全云存储模型。数据拥有者同时也作为属性分发机构,保证了对自身数据的绝对控制,确保了在云服务商不可信情况下开放环境中的云端存储数据的安全。从模型架构和属性密钥分发两个方面对模型进行了研究,并用严格的数学方法证明了本方案是适应性安全的。云存储模型的数据访问策略根据实际需要可灵活设置,适用于云存储等开放式环境。

关键词 属性加密,双系统加密,云存储,属性撤销,适应性安全
中图法分类号 TN918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.046

Secure Model of Cloud Storage Supporting Attribute Revocation

ZHANG Bing-hong[1] ZHANG Chuan-rong[1] JIAO He-ping[2] ZHANG Xin-wei[1]
(School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China)[1]
(Northwestern Polytechnical University, Xi'an 710072, China)[2]

Abstract To solve the problem of coarse-grained attribute revocation for data users and huge computation for key distribution in the existing cloud storage model, we proposed a new secure model of cloud storage supporting fine-grained attribute revocation over the composite order bilinear groups. Data owner is also the attribute distributing authority, assuring the absolute control of the data in the cloud, which ensures that the data stored in open environment is secure on condition that the cloud service provider is unbelievable. We studied the model in two aspects, the frame of the model and the key distribution. The strict mathematical proofs of the model show that the scheme is adaptively secure. Based on the model, data access strategy is flexible and diverse, therefore it is suitable for open environment like cloud storage.

Keywords Attribute-based encryption, Dual-system encryption, Cloud storage, Attribute revocation, Adaptive security

随着信息技术的发展,全世界每天更新的数据都在以惊人的速度增长。人们对大数据存储的需求日益强烈。云存储技术的飞速发展,给人们提供了新的存储理念和大量廉价的存储空间。越来越多的国内厂商如百度、阿里、小米等都纷纷推出自己的云存储服务,云存储用户可以选择将自己的数据资料放在"云"上,实现对数据高效便捷的访问。云存储给我们工作生活带来巨大便利的同时,也存在一些安全隐患。用户将数据通过终端上传到云端后,便失去了对数据的绝对控制权[1]。安全性是用户首先需要考虑的问题,用户存储在云端的数据并不希望被其他的未经授权的用户访问,甚至云服务提供商也不能访问。制度和法律上的约束并不能够绝对消除数据用户对自身数据安全的忧虑,因而必须从技术上对数据安全性加以保证。与此同时,云存储是在开放式的环境当中,因而需要制定灵活、多变、开放的访问策略,才能满足用户的多样化需求。

在2005年的欧密会上,Sahai和Waters[2]提出了基于属性加密的概念,其以一系列的属性为公钥,将密文和用户私钥与属性关联,灵活地表示访问控制策略,因而十分适合开放分布式的网络进行灵活的数据共享。此后基于属性的加密方案得到了广大研究人员的广泛研究和讨论[3-5],2006年Goyal[4]根据属性及访问策略是依附于密文还是私钥,将属性加密方案分为基于密钥策略的属性加密(KP-ABE)算法和基于密文策略的属性加密(CP-ABE)算法。2010年,Lin等[5]针对Chase[6]等属性加密方案需要一个完全可信的第三方,容易出现单点失效的问题,设计了一种无中心的安全门限属性加密方案。方案中,在初始化阶段,所有的属性机构需要相互通信(交互)而不泄露任何私密信息。属性机构间的交互增加了系统开销,同时也由于交互的存在,当有新的属性机构要加入时,系统参数需要全部更新,大大影响了系统的扩展性。但该方案缺少属性撤销机制。Muller等[7]提出了一种分布式属性加密方案,有效地解决了合谋攻击的问题,能够验证用户的合法身份,用户也可以验证属性私钥的正确性,有效地防止了欺诈问题,但是方案的可拓展性、灵活性较差。2010年,Lewko等[8]基于双系统加密的思想[9]提出了一种一次性使用的无中

到稿日期:2014-07-29 返修日期:2014-10-08 本文受国家自然科学基金项目(61272486,61103231),国家自然基金青年基金(61202489),陕西省自然科学基础研究计划面上计划(2011JM8012)资助。
张柄虹(1989-),男,硕士生,主要研究方向为密码学与信息安全,E-mail:zbh_1989ing@163.com;张串绒(1964-),女,教授,硕士生导师,主要研究方向为密码学与信息安全;焦和平(1964-),男,高级教师,主要研究方向为应用数学;张欣威(1992-),男,硕士生,主要研究方向为密码学与网络安全。

心的属性加密方案，属性机构分发给用户的属性私钥是一次性的，用户使用一次后，所拥有的所有属性全部撤销，从而保证了数据的安全性。同时，该方案基于双系统加密，能够抵抗合谋攻击，对于云存储等实际商业运用具有现实意义。王鹏翩等[10]在 Lewko 等[8]和 Waters 等[9]方案的基础上提出了一种基于合数阶双线性群构造的适应性安全属性加密方案，实现了完全细粒度的属性撤销，但该方案的公钥参数与用户数量线性相关，在实际应用中容易造成公钥参数过长。

本文在已有属性加密方案的基础上，基于双系统加密的思想，提出了一种新的细粒度权限撤销的云存储模型。数据拥有者和数据用户均需要在云处理中心注册为合法用户，并得到相应的身份标识。数据拥有者作为属性分发机构，负责数据用户属性私钥的分发，保证了对自身数据的绝对控制。数据用户的权限可撤销，使得方案能够灵活地根据实际需求配置访问控制策略。

1 理论基础

1.1 线性秘密共享[11]

设参与者的集合 $P=(P_1,P_2,\cdots,P_n)$，(A,π)表示访问结构 Γ，A 为 $l\times k$ 的矩阵，π 是一个从$\{1,2,\cdots,l\}$到 P 的映射，即将 A 的每一行映射一个参与者。一个线性秘密共享方案包括以下两种算法。

(1)秘密分享算法：令 s 是要分享的秘密值，随机选择 $y_2,y_3,\cdots,y_k\in Z_p$ 组成一个 k 维向量 $\bar{v}=(s,y_2,y_3,\cdots,y_k)$。若 $\bar{A}_i$ 代表矩阵 A 第 i 行的向量，则 $\lambda_i=\bar{A}_i\cdot\bar{v}$ 代表参与者 $\pi(i)$ 所得到的秘密份额。

(2)秘密恢复算法：设参与者的集合 $\omega\in A$，令授权子集 $L=\{i\mid\pi(i)\in\omega\}$，则可以根据 A 计算出一组恢复系数 $\{\mu_i\}_{i\in L}$，使得 $\sum_{i\in L}\mu_i\cdot\lambda_i=s$。

1.2 合数阶上的双线性映射[12]

令 $N=p_1p_2p_3$（p_1,p_2,p_3 是两两不同的素数），G_1,G_2 是阶为 N 的群，g 是 G_1 的一个生成元。若 $e:G_1\times G_1\to G_2$ 满足下列 3 个性质，则称 e 为一个从 G_1 到 G_2 的双线性映射。

(1)双线性：$\forall a,b\in Z_N,e(g^a,g^b)=e(g,g)^{ab}$；

(2)非退化性：$\exists g\in G_1$，使得 $e(g,g)$的阶为 N；

(3)可计算性：对于所有 $P,Q\in G_1$，总存在有效的方法计算 $e(P,Q)$。

合数阶上的双线性映射还具有以下特性：设 G_{p_1},G_{p_2},G_{p_3} 分别是 G_1 中阶为 p_1,p_2,p_3 的子群，设 $h_i\in G_i,h_j\in G_j$ $(i,j\in\{p_1,p_2,p_3\})$，若 $i\neq j$，则有 $e(h_i,h_j)=1$。

1.3 困难性假设[8]

假设 1　令 $N=p_1p_2p_3$（p_1,p_2,p_3 是两两不同的素数），G_1,G_2 是阶为 N 的群，G_{p_1},G_{p_2},G_{p_3} 分别是 G_1 中阶为 p_1,p_2,p_3 的子群，其生成元分别为 g,X,Y。取双线性映射 $e:G_1\times G_1\to G_2$。给定(N,G_1,G_2,e,g,Y)，则不存在一种算法能够在多项式时间内区分 $G_{p_1},G_{p_1p_3}$ 上的元素。

假设 2　令 $N=p_1p_2p_3$（p_1,p_2,p_3 是两两不同的素数），G_1,G_2 是阶为 N 的群，G_{p_1},G_{p_2},G_{p_3} 分别是 G_1 中阶为 p_1,p_2,p_3 的子群，其生成元分别为 g,X,Y。取双线性映射 $e:G_1\times G_1\to G_2$。从 Z_N 中随机选择 4 个元素(s,c_1,c_2,d)。给定$(N,G_1,G_2,e,g,g^sX^{c_1},Y,X^{c_2}Y^d)$，则不存在一种算法能够在多项式时间内区分 $G_1,G_{p_1p_3}$ 上的元素。

假设 3　令 $N=p_1p_2p_3$（p_1,p_2,p_3 是两两不同的素数），G_1,G_2 是阶为 N 的群，G_{p_1},G_{p_2},G_{p_3} 分别是 G_1 中阶为 p_1,p_2,p_3 的子群，其生成元分别为 g,X,Y。取双线性映射 $e:G_1\times G_1\to G_2$。从 Z_N 中随机选择 6 个元素(α,s,c_1,c_2,c_3,d)。给定$(N,G_1,G_2,e,g,g^\alpha X^{c_1},g^sX^{c_2},Y)$，则不存在一种算法能够在多项式时间内区分 $e(g,g)^{\alpha s}$ 与 G_2 上的随机元素。

1.4 双系统加密[9]

2009 年，Waters 等人提出了双系统加密的思想，其核心是：引入一些攻击游戏，通过构造适当的半功能密钥和半功能密文，使得真实的攻击游戏与这些游戏无法区分。接着在最终的游戏中通过加密一条随机消息，使得攻击者不具备任何攻击优势。双系统加密并没有严格的形式化定义，这里只介绍双系统加密具有的一些基本性质：

(1)半功能密钥可以解密正常的密文；

(2)正常的密钥可以解密半功能密文；

(3)半功能密钥不可以解密半功能密文。

1.5 安全模型

对于基于身份的加密体制，存在两种基本的安全定义：静态安全和适应性安全[13]，对应地有两类攻击模型：静态攻击和适应性攻击。在静态攻击模型中，攻击者在取得系统的公共参数之前就必须确定要攻击目标的身份集合；而在适应性攻击模型中，攻击者并不首先确定要攻击目标的身份集合，而是在对用户进行询问后根据询问的结果确定要攻击目标的身份集合。因此，适应性安全是更为标准的安全概念。

本文方案的安全性通过下列攻击游戏来定义。

初始化：攻击者运行方案初始化算法，并将系统公钥 PK 返回给攻击者。

阶段 1　攻击者询问用户 ID 关于属性集合 ω 的私钥，但要求攻击者询问的私钥不能直接解密最终的密文，最后，将 $SK_{ID,\omega}$返回给攻击者。

挑战阶段：攻击者将两条长度相等的明文 M_0,M_1 传给挑战者，后者从中随机选择一条明文 M_θ 加密，并将最后的询问结果返回给攻击者。

阶段 2　与阶段 1 相同，攻击者继续向挑战者发起对用户私钥的询问。

猜想：攻击者输出对 θ 的猜测 θ'，若 $\theta'=\theta$，则攻击者获胜。

定义攻击者在上述游戏中的优势 Adv 为 $\Pr[\theta'=\theta]-1/2$。

安全性定义：一个支持细粒度用户权限撤销的属性加密方案是安全的，当且仅当在上述游戏中，所有多项式时间的攻击者攻击优势是可以忽略的。

2 框架设计

本文方案设计的安全云存储模型如图 1 所示。

云存储模型包含 4 个实体：数据拥有者(Data Owner，DO)、用户(User)、云服务器(Cloud Server，CS)、云处理中心(Cloud Processing Center，CPC)。

数据拥有者同时也是属性机构，用户需要向数据拥有者请求相应的权限(属性)，才能访问数据。数据(或者加密密钥)由数据拥有者的私钥以及属性加密密钥共同加密，从而使得只有数据拥有者自己才能独立地解密数据，而云处理中心不能。在该模型中，数据拥有者对自己的数据具有最高权限，

云处理中心只是处理用户注册，执行系统指令等任务。

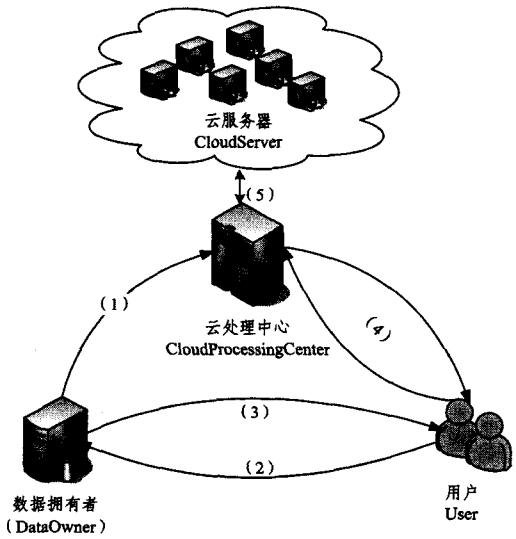

图1 方案模型

文献[14]对大数据的安全分布式存储做了详细的研究综述，分析对比了几种常见的数据存储方式。非对称密码因其高安全性得到了广泛的应用，而在云中实现大数据的存储，若使用非对称加密体制加密数据，则计算量大、效率低。因此，本文借鉴文献[14]的研究，使用对称密码(如 AES)加密数据信息，用非对称密码加密对称密钥，并利用秘密共享技术确保密钥的安全存储，防止单点失效、合谋攻击等破坏。

下面简单介绍模型各实体之间的交互过程。

数据拥有者及用户在使用该存储模型时，均需要向云处理中心(云处理中心是云服务商提供的信息处理机构)注册，分别获得自己的身份标识(ID_i，id_i)及对应的公私钥(DO_i，do_i)(为了简化系统，这里取身份标识为公钥)。数据拥有者也是属性服务器，负责产生属性集 AA_i(i 为数据拥有者属性集数目，不固定，由数据拥有者自己动态确定)；用属性密钥加密自己存储的数据，同时根据用户权限，响应用户请求，分发相应的属性集给使用自己数据的用户。未经云处理中心注册的用户无法在云存储系统中存储或使用数据。

(1)数据拥有者对数据进行预处理，将数据信息分组为 $M=(m_1,m_2,\cdots,m_N)$，并随机选取对称密码 E_k 加密数据得到 $E=(e_1,e_2,\cdots,e_N)$。数据拥有者将加密数据发送给云处理中心，再由云处理中心按照一定的数据存储算法将数据存储在云服务器中(云处理中心对数据的存储不是本文的重点，因而不对其详细介绍)。

(2)用户要使用数据，需要向数据拥有者 DO 提出申请。数据拥有者 DO 首先根据用户的标识确定用户是否是该云存储系统中的用户，若是，则数据拥有者根据用户的职位、信用记录、缴费情况等信息确定用户拥有的权限；若不是，则返回“不合法用户，请注册”。

(3)数据拥有者根据用户的标识信息 ID 分发与用户权限相对应的属性集(值)。属性值与用户的标识信息紧密相关，从而能够防止合谋攻击。其他用户即使从该用户得到标识过的属性，也不能将其与自己的属性合并，进而解密数据。

(4)用户向云处理中心请求数据。云处理中心首先确定用户的身份是否合法，若不合法，则拒绝数据请求，并返回“不合法用户，请注册”；若合法，则根据用户拥有的权限返回相应的加密数据。用户得到密文 E，根据数据拥有者分发的属性私钥计算得到对称加密密钥 E_k，利用加密密钥求解出数据 M。

(5)云处理中心根据数据拥有者和数据用户的请求，将加密数据通过秘密共享的方法分布式存储在云存储服务器上，并根据用户需要及其访问策略将加密数据恢复，返回给数据用户。

3 具体方案

本方案着重研究属性密钥的产生、分发和秘密恢复过程，对云处理中心对数据的分布式存储过程不加描述。需要注意的是，下述方案中运用到云存储模型中的明文信息 M 实际上指的是加密密钥 E_k。

令 $N=p_1p_2p_3$(p_1,p_2,p_3 是两两不同的素数)，G_1,G_2 是阶为 N 的群，G_{p_1},G_{p_2},G_{p_3} 分别是 G_1 中阶为 p_1,p_2,p_3 的子群，其生成元分别为 g,X,Y。取双线性映射 $e:G_1\times G_1\to G_2$。

初始化：令用户的集合为 $U=(ID_1,ID_2,\cdots,ID_n)$，属性机构管理的属性集合为 $\Omega=(a_1,a_2,\cdots,a_m)$。对于任意属性 $a_i\in\Omega$，随机选取两个元素 $t_i,\gamma_i\in Z_N$，计算 $T_i=g^{t_i}$，$h_i=g^{\gamma_i}$。随机选择 $\alpha,b\in Z_N$。最后可以得到系统的公钥 PK 为 $PK=(N,g,g^b,g^{b^2},e(g,g)^\alpha,\{T_i,h_i\}_{i\in U},Y)$；系统私钥为 $SK=(\alpha,b)$。其中(t_i,T_i)、(γ_i,h_i)分别用于与属性本身和属性撤销相关的计算，Y 用于对用户私钥的随机化。

密钥分发(ID,Ω,SK,PK)：输入用户的 $ID\in U$，以及相应的属性集 $\omega\in\Omega$。首先，随机选取元素 $t\in Z_N$，$Y_0\in G_{p_3}$，计算 $D_0=g^tY_0$；对任意属性 $a_i\in\omega$，随机选择元素 $r_i\in Z_N$，并选择 $Y_{i,1},Y_{i,2},Y_{i,3}\in G_{p_3}$，计算 $D_{i,1}=g^{\alpha+b^2t+t_ir_i}Y_{i,1}$，$D_{i,2}=g^{bID}h_iY_{i,2}$，$D_{i,3}=g^{r_i}Y_{i,3}$。则最终生成的用户私钥为 $SK_{ID,\omega}=(D_0,\{D_{i,1},D_{i,2},D_{i,3}\}_{i\in\omega})$，$Y_{i,1},Y_{i,2},Y_{i,3}$用于用户私钥的随机化。

加密$(S,M,(A,\rho),PK)$：令 $S\subseteq U$ 为属性合法的用户列表，(A,ρ)为线性访问结构，其中 A 为 $l\times k$ 的矩阵。令 $R=U\backslash S$，定义 $R=\{ID_1,ID_2,\cdots,ID_r\}$。随机选择 $s,y_2,\cdots,y_k\in Z_N$，取 $\vec{v}=(s,y_2,\cdots,y_k)$，并计算 $\lambda_x=\vec{A}_x\cdot\vec{v}$。随机选择 $s_1,s_2,\cdots,s_r\in Z_N$，使得 $s=s_1+s_2+\cdots+s_r$。最后得到如下密文：

$$C=(C_0,\{C_{x,0},C_{x,1}\}_{x\in[1,l]},\{C_{x,2}C_{x,3}\}_{x\in[1,r]})$$

其中

$$C_0=M\cdot e(g,g)^{\alpha s},C_{x,0}=g^{\lambda_x},C_{x,1}=g^{b^2ID_x}h^b_{\pi(x)}$$

$$C_{x,2}=g^{bs_x},C_{x,3}=T^{\lambda_x}_{\pi(x)}=g^{t_{\pi(x)}\lambda_x}$$

解密$(SK_{ID,\omega},C,(S,(A,\rho)),(ID,\omega),PK)$：假设属性集合 ω 满足线性访问结构(A,ρ)，且用户 $ID\in S$。设 $L=\{x|\pi(x)\in\omega\}$，则可计算得到恢复系数$\{\mu_x\}_{x\in L}$，使得 $\sum_{x\in L}\mu_x\cdot\lambda_x=s$。

最后计算可得：

$$K=\prod_{x=1}^{l}\left(\frac{e(D_{\pi(x),1},C_{x,0})}{e(D_{\pi(x),3},C_{x,3})}\right)^{\mu_x}\prod_{x=1}^{r}\left(\frac{e(C^x_{x,1},D_0)}{e(D^t_{\pi(x),2},C_{x,2})}\right)^{1/(ID-ID_x)}$$

从而可得，$M=C_0/K$。

正确性：用户想要解密数据，则自己的访问权限即数据拥有者分发给用户的属性私钥，需要在属性的合法访问列表中。

(1)式正确性证明如下：

$$K=\prod_{x=1}^{l}\left(\frac{e(D_{\pi(x),1},C_1)}{e(D_{\pi(x),3},C_{x,3})}\right)^{\mu_x}\cdot \prod_{x=1}^{r}\left(\frac{e(C_{x,1}^{s_x},D_0)}{e(D_{\pi(x),2}^{\lambda_x},C_{x,2})}\right)^{1/(ID-ID_x)}$$

$$=\prod_{x=1}^{l}\left(\frac{e(g^{a+b^2t+t_{\pi(x)}r_{\pi(x)}},g^{\lambda_x})}{e(g^{r_{\pi(x)}},g^{t\pi(x)\lambda_x})}\right)^{\mu_x}\cdot \prod_{x=1}^{r}\left(\frac{e((g^{b^2ID_x}g^{br_{\pi(x)}})^{s_x},g^t)}{e((g^{bID}g^{r_{\pi(x)}})^t,g^{bs_x})}\right)^{1/(ID-ID_x)}$$

$$=e(g,g)^{(a+b^2t)s}\cdot e(g,g)^{-b^2ts}=e(g,g)^{as}$$

从而可得 $M=C_0/K=C_0=M\cdot e(g,g)^{as}/K$。

任何非法用户，即在属性撤销列表中的用户，无法完成上述解密过程。

4 安全性证明

基于 1.3 节双系统加密的困难性假设，可以证明本文的方案是适应性安全的。

首先构造半功能密文和半功能密钥，然后根据构造的一系列攻击游戏，利用困难性假设证明攻击者无法将真实的攻击游戏与构造的游戏区分开来，从而得出结论：攻击者在真实的攻击游戏中没有攻击优势，进而证明方案的安全性。

为简化表述过程，下文中所有与 X 相关的元素都是在 G_{p_2} 中随机选取的，与 Y 相关的元素都是在 G_{p_3} 中随机选取的。

半功能密文：

随机选取 $s,u_1,u_2,\cdots,u_k,y_1,y_2,\cdots,y_{k'},c_1,z_x\in Z_N$，令 $\bar{v}=(s,y_1,y_2,\cdots,y_{k'})$，$\bar{u}=(s,u_1,u_2,\cdots,u_k)$，则可以得出半功能密文为

$C_0'=Me(g,g)^{as}$，$C'_{x,0}=g^{\lambda_x}X^{\bar{A}_x\cdot\bar{u}}$，$C'_{x,1}=g^{b^2ID_x}h^b_{\pi(x)}$，

$C'_{x,2}=g^{bs_x}X^{c_1z_x}$，$C'_{x,3}=T^{\lambda_x}_{\pi(x)}=(g^{\lambda_x}X^{\bar{A}_x\cdot\bar{u}})^{t_{\pi(x)}}$

半功能密钥：

(1)第一种形式的半功能密钥：

$D_0=g^tX_0Y_0$，$D_{i,1}=g^{a+b^2t+t_ir_i}X_{i,1}Y_{i,1}$

$D_{i,2}=g^{bID}h_iX_{i,2}Y_{i,2}$，$D_{i,3}=g^{r_i}X_{i,3}Y_{i,3}$

(2)第二种形式的半功能密钥：

$D_0=g^tY_0$，$D_{i,1}=g^{a+b^2t+t_ir_i}X_{i,1}Y_{i,1}$

$D_{i,2}=g^{bID}h_iX_{i,2}Y_{i,2}$，$D_{i,3}=g^{r_i}Y_{i,3}$

假设攻击者进行了 m 次私钥查询，对 $\forall 1\leqslant k\leqslant m$，可以定义下面两个攻击游戏。

$Game_{k,1}$：在该游戏中，对于攻击者前 $k-1$ 次查询请求，挑战者将返回第二种形式的半功能密钥；对第 k 次私钥查询请求，将返回第一种形式的半功能密钥；而对于 k 次以后的私钥查询请求，将返回正常的密钥。在挑战阶段，挑战者将返回攻击者一条半功能密文。

$Game_{k,2}$：在该游戏中，对于攻击者前 k 次查询请求，挑战者将返回第二种形式的半功能密钥；而对于 k 次以后的私钥查询请求，将返回正常的密钥。在挑战阶段，挑战者将返回攻击者一条半功能密文。

另外，定义如下 3 个攻击游戏。

$Game_{real}$：该游戏即是 1.5 节定义的真实游戏；

$Game_0$：与 $Game_{real}$ 基本一致，唯一的区别是，在 $Game_0$ 的挑战阶段，挑战者将返回攻击者一条半功能密文；

$Game_{final}$：与 $Game_{k,1}$、$Game_{k,2}$ 基本一致，唯一的区别是，在 $Game_{final}$ 的挑战阶段，挑战者将对一条随机信息进行加密，并将半功能密文返回给攻击者。因此，$Game_{final}$ 中，攻击者的攻击优势是可以忽略的。

基于 1.3 的困难性假设，通过以下 4 个引理可以证明上述定义的攻击游戏是无法区分的，从而将在 $Game_{real}$ 中的攻击优势规约到最终的攻击游戏 $Game_{final}$ 中。

引理 1 若存在一个多项式时间的攻击者 A，使得 $Game_{real}Adv_A-Game_0Adv_A=\varepsilon$，则可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 1。

证明：挑战者将 $\{g,Y,T\}$ 发送给 B。

首先 B 运行攻击者 A，输出一个访问结构 $(A^*_{l\times k},\pi)$。

B 运行初始化，令用户的集合为 $U=(ID_1,ID_2,\cdots,ID_n)$，属性集合为 $\Omega=(a_1,a_2,\cdots,a_m)$，对于任意属性 $a_i\in\Omega$，随机选取元素 $t_i\in Z_N$，可计算 $T_i=g^{t_i}$；令 $\omega^*=\{\pi(x)|_{x\in\{1,2,\cdots,l\}}\}$，若 $a_i\neq\omega^*$，则随机选择一个元素 $\gamma_i\in Z_N$，并计算 $h_i=g^{\gamma_i}$。随机选择 $\alpha,b\in Z_N$。最后将系统的公钥 PK 传给 A：$PK=(N,g,g^b,g^{b^2},e(g,g)^a,\{T_i,h_i\}_{i\in U})$。系统私钥为 $SK=(\alpha,b,\{t_i,\gamma_i\}_{i\in U},Y)$。

阶段 1 由于 B 拥有系统的公钥 PK，因此对于 A 的任何私钥询问请求，B 都可以进行模拟并生成。

挑战：攻击者 A 提交两条长度相等的明文信息 M_0 和 M_1，B 首先随机选择 $v_2',v_3',\cdots,v_k'\in Z_N$，令 $v'=(1,v_2',v_3',\cdots,v_k')$，然后随机选择一条明文 $M_\theta(\theta\in\{0,1\})$加密，并将最后的询问密文 C^* 返回给攻击者：

$$\{C_0^*=M_\theta\cdot e(g^a,T),C^*_{x,0}=T^{\bar{A}^*_x\cdot\bar{u}},C^*_{x,1}=g^{b^2ID_x}h^b_{\pi(x)},$$

$$C^*_{x,2}=g^{bs_x},C^*_{x,3}=T^{\bar{A}^*_x\cdot\bar{u}\cdot t_{\pi(x)}}\}_{x\in\{1,2,\cdots,l\}}$$

阶段 2 与阶段 1 相同，攻击者继续向挑战者发起对用户私钥的询问。

猜想：攻击者输出对 θ 的猜测。

(1)若 $T\in G_{p_1}$，设 $T=g^s$，则此时的询问密文 C^* 是一条正常密文，这时进行的游戏为 $Game_{real}$。

(2)若 $T\in G_{p_1p_2}$，设 $T=g^sX^c$，则此时的询问密文 C^* 是一条半功能密文，这时进行的游戏为 $Game_0$。

可见，此时 $Game_{real}Adv_A-Game_0Adv_A=\varepsilon$，即可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 1。

引理 2 若存在一个多项式时间的敌手 A，使得 $Game_{k-1,2}Adv_A-Game_{k,1}Adv_A=\varepsilon$，则可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 2。

证明：挑战者将 $(g,g^sX^{c_1},Y,X^{c_2}Y^d,T)$ 发送给 B，其中的初始化过程与引理 1 的证明相同。

阶段 1 对于 A 的前 $k-1$ 次私钥询问，B 返回第二种类型的半功能密钥，密钥生成如下：B 随机选择 $Y_0,Y_{i,2},Y_{i,3}\in G_{p_3}$，$t\in Z_N$，对于任意 $a_i\in\omega$，随机选择 $r_i\in Z_N$，计算：$D_0=g^tY_0$，$D_{i,1}=g^{a+b^2t+t_ir_i}(X^{c_2}Y^d)^{r_i}$，$D_{i,2}=g^{bID}h_iY_{i,2}$，$D_{i,3}=g^{r_i}Y_{i,3}$。

对于 A 的第 k 次私钥询问，B 返回以下密钥，密钥生成方式如下：B 随机选择 $Y_0',Y'_{i,1},Y'_{i,2},Y'_{i,3}\in G_{p_3}$，$t'\in Z_N$，对于任意 $a_i\in\omega$，随机选择 $r_i'\in Z_N$，计算：

$D_0=g^{t'}\cdot T\cdot Y_0$，$D_{i,1}=g^{a+b^2t'}\cdot T^{a+b^2}\cdot T^{t_ir_i'}\cdot Y'_{i,1}$

$D_{i,2}=g^{bID}\cdot h_i\cdot Y'_{i,2}$，$D_{i,3}=T^{r_i'}\cdot Y'_{i,3}$

由于 B 拥有系统的私钥 SK，因此对于 A 的第 k 次以后的私钥询问，B 都可以进行模拟并生成。

挑战：攻击者 A 提交两条长度相等的明文信息 M_0 和

M_1，B 首先随机选择 $v_2', v_3', \cdots, v_k' \in Z_N$，令 $v'=(1, v_2', v_3', \cdots, v_k')$，然后随机选择一条明文 $M_\theta(\theta \in \{0,1\})$ 加密，并将最后的询问密文 C^* 返回给攻击者：

$\{C_0^* = M_\theta \cdot e(g^a, g^s X^{c_1}), C_{x,0}^* = (g^s X^{c_1})^{\overline{A}_x^* \cdot \vec{u}}, C_{x,1}^* = g^{b^2 ID_x} h_{\pi(x)}^b, C_{x,2}^* = g^{bs_x}, C_{x,3}^* = (g^s X^{c_1})^{\overline{A}_x^* \cdot \vec{u} \cdot t_{\pi(x)}}\}_{x \in \{1,2,\cdots,l\}}$

阶段 2　与阶段 1 相同，攻击者继续向挑战者发起对用户私钥的询问。

猜想：攻击者输出对 θ 的猜测。

(1)若 $T \in G_1$，设 $T=g^s X^{c'} Y^{d'}$，则攻击者 A 第 k 次私钥询问返回的是第一种类型的半功能密钥，这时进行的游戏为 $Game_{k,1}$。

(2)若 $T \in G_{p_1 p_3}$，设 $T=g^b Y^{d'}$，则攻击者 A 第 k 次私钥询问返回的是正常的密钥，这时进行的游戏为 $Game_{k-1,2}$。

可见，此时 $Game_{k-1,2} Adv_A - Game_{k,1} Adv_A = \varepsilon$，即可以构造一个多项式时间算法 B 以 ε 的优势区别 $G, G_{fr}(r=1,2,3)$ 上的元素。

引理 3　若存在一个多项式时间的敌手 A，使得 $Game_{k,1} Adv_A - Game_{k,2} Adv_A = \varepsilon$，则可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 2。

证明：挑战者将 $(g, g^s X^{c_1}, Y, X^{c_2} Y^d, T)$ 发送给 B，其中的初始化及挑战过程与引理 2 的证明相同。

阶段 1　对于 A 的前 $k-1$ 次私钥询问，B 返回第二种类型的半功能密钥，密钥生成与引理 2 一致。

对于 A 的第 k 次私钥询问，B 返回以下密钥，密钥生成方式如下：B 随机选择 $Y_0', Y'_{i,1}, Y'_{i,2}, Y'_{i,3} \in G_{p_3}, t' \in Z_N$，对于任意 $a_i \in \omega$，随机选择 $r_i', k_i \in Z_N$，计算：$D_0 = g^{t'} \cdot T \cdot Y_0'$，$D_{i,1} = g^{a+b^2 t'} \cdot T^{t_i r_i'} \cdot Y'_{i,1} \cdot (X^{c_2} Y^d)^{k_i}$，$D_{i,2} = g^{bID} \cdot h_i \cdot Y'_{i,2}$，$D_{i,3} = T^{r_i'} \cdot Y'_{i,3}$。

由于 B 拥有系统的私钥 SK，因此对于 A 的第 k 次以后的私钥询问，B 都可以进行模拟并生成。

挑战：攻击者 A 提交两条长度相等的明文信息 M_0 和 M_1，B 首先随机选择 $v_2', v_3', \cdots, v_k' \in Z_N$，令 $v'=(1, v_2', v_3', \cdots, v_k')$，然后随机选择一条明文 $M_\theta(\theta \in \{0,1\})$ 加密，并将最后的询问密文 C^* 返回给攻击者：$\{C_0^* = M_\theta \cdot e(g^a, g^s X^{c_1}), C_{x,0}^* = (g^s X^{c_1})^{\overline{A}_x^* \cdot \vec{u}}, C_{x,1}^* = g^{b^2 ID_x} h_{\pi(x)}^b, C_{x,2}^* = g^{bs_x}, C_{x,3}^* = (g^s X^{c_1})^{\overline{A}_x^* \cdot \vec{u} \cdot t_{\pi(x)}}\}_{x \in \{1,2,\cdots,l\}}$。

阶段 2　操作与阶段 1 相同。

猜想：攻击者输出对 θ 的猜测。

(1)若 $T \in G_1$，设 $T=g^s X^{c'} Y^{d'}$，则攻击者 A 第 k 次私钥询问返回的是第一种类型的半功能密钥，这时进行的游戏为 $Game_{k,1}$。

(2)若 $T \in G_{p_1 p_3}$，设 $T=g^b Y^{d'}$，则攻击者 A 第 k 次私钥询问返回的是第二种类型的半功能密钥，这时进行的游戏为 $Game_{k,2}$。

可见，此时 $Game_{k,2} Adv_A - Game_{k,1} Adv_A = \varepsilon$，即可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 2。

引理 4　若存在一个多项式时间的敌手 A，使得 $Game_{k,2} Adv_A - Game_{final} Adv_A = \varepsilon$，则可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 3。

证明：挑战者将 $(g, g^a X^{c_1}, g^s X^{c_2}, T)$ 发送给 B，其中的初始化及挑战过程与引理 1 的证明相同。

阶段 1　对于 A 的私钥询问，B 将按照下列密钥生成方式产生半功能密钥：B 随机选择 $Y_0, Y_{i,1}, Y_{i,2}, Y_{i,3}, X_{i,1} \in G_{p_3}$，$t \in Z_N$，对于任意 $a_i \in \omega$，计算：$D_0 = g^t \cdot Y_0$，$D_{i,1} = g^a X^{c_1} \cdot g^{b^2 t + t_i r_i} X_{i,1} Y_{i,1}$，$D_{i,2} = g^{bID} h_i X_{i,2} Y_{i,2}$，$D_{i,3} = g^{r_i} Y_{i,3}$。

挑战：攻击者 A 提交两条长度相等的明文信息 M_0 和 M_1，B 首先随机选择 $v_2', v_3', \cdots, v_k' \in Z_N$，令 $v'=(1, v_2', v_3', \cdots, v_k')$，然后随机选择一条明文 $M_\theta(\theta \in \{0,1\})$ 加密，并将最后的询问密文 C^* 返回给攻击者：

$\{C_0^* = M_\theta \cdot T, C_{x,0}^* = (g^s X^{c_2})^{\overline{A}_x^* \cdot \vec{u}}, C_{x,1}^* = g^{b^2 ID_x} h_{\pi(x)}^b, C_{x,2}^* = g^{bs_x}, C_{x,3}^* = (g^s X^{c_2})^{\overline{A}_x^* \cdot \vec{u} \cdot t_{\pi(x)}}\}_{x \in \{1,2,\cdots,l\}}$

阶段 2　操作与阶段 1 相同。

猜想：攻击者输出对 θ 的猜测。

(1)若 $T=e(g,g)^{as}$，则挑战密文是一条半功能密文，这时进行的游戏为 $Game_{k,2}$。

(2)若 $T \in G_2$，则挑战密文是对随机信息进行加密，这时进行的游戏为 $Game_{final}$。

可见，此时 $Game_{final} Adv_A - Game_{k,2} Adv_A = \varepsilon$，即可以构造一个多项式时间算法 B 以 ε 的优势攻破假设 3。

通过以上一系列攻击游戏的证明归约可以得出：游戏 $Game_{real}$ 与 $Game_{final}$ 具有不可区别性，因而攻击者在 $Game_{real}$ 中的优势是可以忽略的，本文方案是安全的。

5　分析讨论

(1)灵活性

属性机构即数据拥有者可灵活地增加或减少，因此本方案应用范围广泛。任何想进行数据共享的用户仅需要在云处理中心进行注册就可以实现数据的共享，数据拥有者可以借助此平台提供各类数据，因此本方案实用性很强，适用于云存储等开放式网络。同一属性机构可以有多个不同的属性，可以实现对访问策略的灵活设置。而属性密钥都是由数据拥有者分发，从而实现了对数据的绝对控制，任何人没有相应的解密密钥是无法解密存储在云端的数据的。这在实现灵活性的同时保证了方案的安全。

(2)抗攻击特性

属性加密方案的最大威胁就是合谋攻击，即不同的用户合作使得用户获得自己权限所不能取得的数据信息。与使用秘密共享[15]抵抗合谋攻击的方案相比，本方案使用的方法更加安全。本方案使用双系统加密，密钥分发过程中添加了随机化参数，使得不同用户合作无法合谋窃取非法权限。而攻击者可以逐个攻击文献[15]方案的用户，获取身份信息及属性私钥，并在一定时间内取得相应的属性信息。

(3)属性细粒度可撤销

本文基于线性秘密共享矩阵实现对信息的访问控制，用户在属性机构注册时根据自身的地位权限等获得了相对应的属性，其中(γ_i, h_i)是与属性撤销相关的参数。若用户的属性被撤销，则其属性值不会在合法属性集合中，无法恢复数据信息。属性机构根据用户的实际权限调整情况，可以定期对合法属性集合进行更新。若用户的权限发生了调整，相应的属性集也将发生相对应的调整。

(4)性能比较分析

将本文的方案与文献[10]方案从密钥密文长度和算法效率两个方面进行比较，结果如表 1 和表 2 所列。算法的运算

时间主要集中在幂指数运算和双线性对运算，所以下面以这两种运算的运算次数分析算法的效率。

表1 密钥密文长度

密钥/密文	文献[10]方案	本文方案
公钥	$(m+n+4)L_{G_1}$	$(2m+4)L_{G_1}$
私钥	$(2l+n+1)L_{G_1}$	$(3l+1)L_{G_1}$
密文	$(\|\omega\|+3)L_{G_1}$	$(2l+1)L_{G_1}$

表2 算法效率比较

阶段	运算	文献[10]方案	本文方案
初始化	exp	$1+2m+2n$	$2m+2$
	pairing	0	1
密钥分发	exp	$1+2\|\omega\|$	$2+2\|\omega\|$
	pairing	0	0
加密	exp	$1+3l$ 或 $1+5l$	$2l+2r$
	pairing	1	1
解密	exp	0	0
	pairing	$6\|\omega\|$	$4\|\omega\|$

表1和表2中exp表示指数运算，pairing表示双线性对运算，n 表示方案定义的用户总数，m 表示属性机构定义的属性个数，l 表示线性矩阵的行数，$|\omega|$ 表示与密文相关的属性个数，r 为属性非法用户数，L_{G_1} 表示群元素的长度。

分析表1和表2可以知道，本方案的密钥密文不受用户个数的影响，公私钥长度仅与属性个数相关，系统的用户和属性数目越多，本文方案的优势越明显。在算法效率方面，本文与文献[10]的方案在密钥分发和加密阶段的运算量基本一致；但在初始化阶段和解密阶段，本文方案计算量明显小于文献[10]，尤其是在初始化阶段，文献[10]的运算量与用户数目呈线性相关。

随着信息社会的高速发展，在云存储服务中，进行数据分享的用户数目将是巨大的。本方案的用户密钥及运算量仅与属性相关，大大降低了方案运行过程中的存储量和计算量，效率较高。

结束语 云存储是解决当前大数据存储的重要方法，其数据安全是人们一直以来的担忧，利用属性加密机制共享数据是解决该问题的重要途径。本文基于双系统加密提出了细粒度属性可撤销的密钥策略属性加密安全云存储模型，数据拥有者分发属性私钥，确保了对数据的绝对控制，并从数学上严格地证明了方案是适应性安全的。但方案存在的一个问题是加密数据需要提前知道用户集合，这对于数据访问用户变化快的情况并不适用，因为对本方案而言，要支持用户的快速变换就必须重新加密数据，这将极大地增加方案的运算开销。因此有必要指出本文方案的局限性，即其只适合于数据访问用户集变化很少的情况，比如公司内部员工或特定人员集合访问数据，数据拥有者只希望特定的人员访问且人员变动不大。这将是文章的下一步研究方向。

参考文献

[1] 傅颖勋，罗圣美，舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展，2013，50(1)：136-145
Fu Ying-xun，Luo Sheng-mei，Shu Ji-wu. Survey of Secure Cloud Storage System and Key Technologies[J]. Journal of Computer Research and Development，2013，50(1)：136-145

[2] Sahai A，Waters B. Fuzzy identity-based encryption[C]// Cramer R，ed. Advances in Cryptology-EUROCRYTP 2005：24th Annual International Conference on the Tehroy and Applications of Cryptographic Techniques. Springer Berlin Heidelberg，2005：457-473

[3] 苏金树，曹丹，王小峰，等. 属性基加密机制[J]. 软件学报，2011，22(6)：1299-1315
Su Jin-shu，Cao Dan，Wang Xiao-feng，et al. Attribute-Based Encryption Schemes[J]. Journal of Software，2011，22(6)：1299-1315

[4] Goyal V，Pandey O，Sahai A，et al. Attribute based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria，Virginia，USA，2006：89-98

[5] Lin Huang，Cao Zhen-fu，Liang Xiao-hui，et al. Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority[J]. Information Sciences，2010，180(13)：2618-2632

[6] Chase M. Multi-authority attribute based encryption[C]// Theory of Cryptography：Proceedings of 4th Theory of Cryptography Conference. Springer Berlin Heidelberg，2007：515-534

[7] Müller S，Katzenbeisser S，Eckert C. Distributed attributed-based encryption[M]// Information Security and Cryptology (ICISC 2008). Springer Berlin Heidelberg，2009：20-36

[8] Lewko A，Okamoto T，Sahai A，et al. Fully Secure Functional Encryption：Attribute-Based Encryption and (Hierarchical) Inner Product Encryption[C]// Advances in Cryptology—EUROCRYPT 2010：Proceedings of 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer，2010：62-91

[9] Waters B. Dual System Encryption：Realizing Fully Secure IBE and HIBE under Simple Assumptions[C]// Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag，2009：619-636

[10] 王鹏翩，冯登国，张立武. 一种支持完全细粒度属性撤销的CP-ABE方案[J]. 软件学报，2012，23(10)：2805-2816
Wang Peng-pian，Feng Deng-guo，Zhang Li-wu. CP-ABE Scheme Supporting Fully Fine-Grained Attribute Revocation[J]. Journal of Software，2012，23(10)：2805-2816

[11] Beimel A. Secure schemes for secret sharing and key distribution [D]. Haifa：Israel Institute of Technology，1996

[12] Boneh D，Goh E J，Nissim K. Evaluating 2-DNF formulas on ciphertexts[C]// Proceedings of the Second International Conference on Theory of Cryptography. Springer-Verlag，2005：325-341

[13] Gentry C，Waters B. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts)[C]// Advances in Cryptology-EUROCRYPT 2009：Proceedings of 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer，2009：171—188

[14] Minowa T，Takahashi T. Secure distributed storage for bulk data [C]// Neural Information Processing：Proceedings of 19th International Conference (ICONIP 2012). Springer Berlin Heidelberg，2012：566-575

[15] 吴胜艳，许力，林昌露. 基于门限属性加密的安全分布式云存储模型[J]. 计算机应用，2013，33(7)：1880-1884
Wu Sheng-yan，Xu Li，Lin Chang-lu. Secure and distributed cloud storage model from threshold attribute-based encryption [J]. Journal of Computer Applications，2013，33(7)：1880-1884