云计算下可撤销的全外包CP-ABE方案

江泽涛[1,2] 黄 锦[1] 胡 硕[3] 徐 智[1]
(桂林电子科技大学计算机与信息安全学院 广西 桂林 541004)[1]
(桂林电子科技大学广西可信软件重点实验室 广西 桂林 541004)[2]
(南昌航空大学信息学院 南昌 330063)[3]

摘 要 在属性基加密体制(Attribute-Based Encryptionsystem,ABE)中,用户可以通过自身属性进行信息加密和解密,具有灵活性和安全性,因而该机制被广泛应用于云存储的安全数据共享方案。但标准ABE机制具有繁重的计算开销,限制了ABE加密的实际应用,无法满足数据拥有者可以动态、高效地修改用户访问权限的需求。针对以上问题,文中提出一种支持属性撤销的全外包密文策略属性基加密方案。利用计算外包将密钥生成以及加解密过程中的复杂计算交由云服务器完成,减少密钥生成中心(Key Generation Center,KGC)以及用户的计算开销,通过属性密钥密文更新实现对用户属性的细粒度撤销。最后通过理论分析对所提方案的效率和功能进行评估,结果表明其具有良好的安全性及较高的系统效率。

关键词 云计算,属性基加密,计算外包,属性撤销,密钥更新
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.07.018

Fully-outsourcing CP-ABE Scheme with Revocation in Cloud Computing

JIANG Ze-tao[1,2] HUANG Jin[1] HU Shuo[3] XU Zhi[1]
(School of Computer and Information Security,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China)[1]
(Guangxi Key Laboratory of Trusted Software,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China)[2]
(School of Information Engineering,Nanchang Hangkong University,Nanchang 330063,China)[3]

Abstract In the attribute-based encryption system (ABE),users can encrypt and decrypt information through their own attributes,which is flexible and secure. Therefore,the system is widely used in secure data sharing solutions for cloud storage. However,the standard ABE mechanism has a heavy computational overhead,it restricts the practical application of ABE encryption and can't satisfy the requirement that the data owner can dynamically and efficiently modify the user access authority. Aiming at the above problems,this paper proposed a full-outsourcing ciphertext policy attribute-based encryption scheme supporting attribute revocation. By using computational outsourcing,the complex calculations of key generation and encryption and decryption processes are handed over to cloud server to complete,reducing computational overhead of the key generation center (KGC) and the user's,and realizing the fine-grained revocation of user attributes through attribute key ciphertext updating. Finally,the efficiency and function of the proposed scheme were analyzed theoretically. Theoretical analysis was conducted to evaluate efficiency and functions of the proposed scheme. The results show that the proposed scheme has good security and high system efficiency.

Keywords Cloud computing,Attribute base encryption,Computing outsourcing,Attribute revocation,Key update

1 引言

云计算、物联网等新型计算环境提供了便捷的数据共享、融合计算等服务,极大地提高了对数据的处理效率,使计算和存储资源得到了充分的利用。云存储作为一种新兴的服务形式,以其弹性配置、按需购买、易于维护等优点成为人们喜爱的选择,然而在云存储模式下,用户将数据存放在云端,也就失去了对数据的控制,因而为数据安全的担忧。为了消除用户对云存储数据安全的担忧,需要有相对应的安全机制来保证数据的机密性和安全共享。属性基加密(ABE)是云存储模

到稿日期:2018-06-07 返修日期:2018-08-26 本文受国家自然科学基金(61572147),广西科技计划项目(AC16380108),广西图像图形智能处理重点实验项目(GIIP201701),广西研究生教育创新计划资助项目(2018YJCX46),江西省自然科学基金资助项目(20171BAB212015)资助。
江泽涛(1961-),男,博士,教授,主要研究方向为图像处理、计算机视觉、网络信息安全;黄 锦(1994-),男,硕士生,主要研究方向为网络信息安全;胡 硕(1983-),男,硕士,讲师,主要研究方向为智能计算;徐 智(1981-),男,博士,副教授,主要研究方向为计算机视觉,E-mail:645882969@qq.com(通信作者)。

式下提高用户数据机密性和实现细粒度访问控制的重要方法[1]。

Shamir 等[2]提出并实现了身份加密（Identity-BasedEncryption，IBE）机制，首次将用户密钥与用户身份信息相关联。以身份加密为基础，Sahai 等[3]提出了属性基加密（Attribute-Based Encryption，ABE）的概念，将密文和密钥与一系列的属性相关联，通过定义访问结构，指定能够解密数据的属性集合实现细粒度的访问控制。为表示更加灵活的访问策略，Goyal 等[4]提出密钥策略的基于属性的加密方案（Key Policy Attribute Based Encryption，KP-ABE），将关于文件的描述性信息作为属性，采用树形访问控制结构来描述访问控制策略，并将访问树嵌入密钥中。KP-ABE 的缺点是数据拥有者缺乏对访问策略的掌控。Bethencourt 等[5]提出密文策略属性加密方案（Ciphertext Policy Attribute Based Encryption，CP-ABE），以用户身份信息为属性，数据拥有者决定访问策略，完全掌握访问策略的控制权。

目前，已经有许多 CP-ABE 方案被提出，实现了细粒度的访问控制。然而在现有的大多数 CP-ABE 方案中，主要的问题之一是加密和解密的复杂性计算数量（双线性映射和指数运算）随着访问结构的复杂度的增加而变大，这也制约了 ABE 在现实中的广泛应用，尤其是针对移动设备和计算受限设备；此外，密钥生成中心还必须处理海量用户的私钥申请，进行大量指数运算生成用户私钥，而且私钥的计算量随着访问结构复杂度的增加而增加。为了解决这一问题，Green 等[6]提出利用解密算法进行外包计算的方案。Zhou 等[7]提出具有隐私保护的 CP-ABE 方案，在没有信息泄露的前提下，将加密和解密的繁重计算交予第三方服务器执行。Asim 等[8]提出将部分加密和解密算法分别委托给两个代理云服务器进行计算的方案。Chow 等[9]提出了一种从单授权中心到多授权中心且支持属性撤销和外包加密的通用构建方案，Mao 等[10]提出支持数据验证和加解密外包计算的基属性加密的通用构造方案。Wang 等[11]提出了一种可验证的外包 CP-ABE 方案，该方案可以通过第三方服务器验证外包计算的正确性。另一个问题是关于 ABE 系统中的属性撤销，云存储环境下存在大量的用户，而 ABE 中不同的用户可能共享相同的属性。若某个用户的某个属性被撤销，对于如何保证在不影响其他正常用户访问的前提下对该用户实现相应访问权限的撤销的问题，Yu 等[12]引入了半可信的代理服务器，基于代理重加密实现了对属性的及时撤销。Yang 等[13]提出支持属性撤销的 CP-ABE 方案，由属性权威对密文和未被撤销的用户密钥进行更新。Hur 等[14]提出一个支持完全细粒度属性撤销的 CP-ABE 方案，基于二叉树向合法用户分发一个对称密钥，实现属性的及时撤销。李勇等[15]提出支持属性撤销的外包 CP-ABE 方案，通过使用属性版本号进行属性撤销。马华等[16]提出了具有属性撤销和解密外包功能的属性基加密方案，通过密钥加密树实现密钥更新。方雪峰等[17]提出一个可撤销用户的外包加解密 CP-ABE 方案，利用中国剩余定理实现了用户撤销和密文更新。Zhang 等[18]提出了支持用户撤销和属性更新的 CP-ABE 方案。已有的支持外包的 CP-ABE 方案通过将部分加解密权限外包给第三方服务器来减少终端用户的计算开销。但大多数方案只针对加解密算法进行了优化，忽略了海量用户申请私钥的系统计算开销以及数据拥有者可以动态、高效地修改用户访问权限的需求。

针对上述问题，文中提出一种支持属性撤销的全外包 CP-ABE 方案，将密钥生成以及加解密中的复杂幂指数以及双线性映射计算外包给第三方服务器以降低系统和用户的计算开销；本文方案通过对未撤销用户及云服务器广播撤销属性的对应属性更新密钥进行升级，实现属性撤销并降低属性撤销的系统开销。

2　预备知识

2.1　访问结构

定义 1　令$\{P_1,P_2,P_3,\cdots,P_n\}$为一个集合，一个访问结构 A 是 2^P 的一个非空子集。若访问结构 A 是单调的，则有：$\forall B,C$，若 $B\in A$ 且 $B\subseteq C$，则 $C\subseteq A$。访问结构 A 的集合被称作授权集合，反之不在访问结构 A 的集合被称作非授权集合。

定义 2　令访问树 Γ 是一个表示访问结构的树，每一个非叶子节点表示一个阀门，由其子节点和门限值表示。令 num_x 表示节点的子节点数量，且对每个节点的子节点以从 1 到 num_x 的顺序进行编号。K_x 表示节点的门限值，则有 $0\leqslant K_x\leqslant num_x$。当 $K_x=1$ 时表示阀门是或门；当 $K_x=num_x$ 时表示阀门是与门。每一个叶子节点由一个属性表示且其门限值 $K_x=1$。

为了方便计算，定义一些关于树的操作函数，$parent(x)$ 表示为访问树 Γ 中 x 节点的父节点。$attr(x)$ 表示当且仅当 x 节点为访问树 Γ 的叶子节点时与其相关的属性。$index(x)$ 表示节点 x 的子节点索引。

策略树解密：令 Γ 表示一个访问结构树，Γ_x 表示 Γ 中以 x 为根的子树，记根节点为 r，则 Γ 可以表示为 Γ_r。如果属性集合 ω 符合访问树 Γ_x 所表达的访问控制策略，则有 $\Gamma_x(\omega)=1$。$\Gamma_x(\omega)$可以通过以下递归计算。如果 x 为非叶子节点，计算所有关于 x 的子节点 x' 的 $\Gamma_{x'}(\omega)$ 值，当且仅当至少有个 K_x 个子节点返回 1 时，$T_x(\omega)$返回 1；如果 x 为叶子节点，当且仅当 $attr(x)\in\omega$ 时，$\Gamma_x(\omega)$返回 1。

2.2　拉格朗日插值法

设对于某个次数为 n 的多项式，如果给定多项式的 $n+1$ 个不同的点 x_i，y_i，则可以唯一确定一个 x 对应的拉格朗日插值多项式 $F(x)=\sum_{i=0}^{n}y_i\Delta_i s(x)$，每一个 $\Delta_i s(x)$ 为插值基函数，其表达式为：

$$\Delta_i s(x)=\prod_{i=0,i\neq j}^{n}\frac{x-x_i}{x_j-x_i}$$

$$=\frac{x-x_0}{x_j-x_0}\cdots\frac{(x-x_{j-1})(x-x_{j+1})}{(x_j-x_{j-1})(x_j-x_{j+1})}\cdots\frac{x-x_n}{x_j-x_n}$$

其中，$0\leqslant i\leqslant n$。

2.3　双线性映射

令 G_1，G_2 为阶是素数 p 的乘法循环群，g 为 G_1 的生成元，存在双线性映射 $e:G_1\times G_1\rightarrow G_2$ 满足以下性质：

1）双线性。$\forall g,h\in G_1$，$\forall a,b\in Z_p$，均有 $e(g^a,h^b)=e(g,h)^{ab}$。

2)非退化性。$\forall a,b\in G_1$,使 $e(a,b)\neq 1$ 成立。

3)可计算性。存在有效的算法使得 $\forall g,h\in G_1$ 在一个多项式时间内计算 $e(g,h)$。

3 算法定义

支持属性撤销的全外包 CP-ABE 方案有 8 个实体对象,包括密钥生成中心(KGC)、云服务提供商、数据加密方、数据解密方、2 个外包密钥生成服务器、外包加密服务器、外包解密服务器。系统框图如图 1 所示。

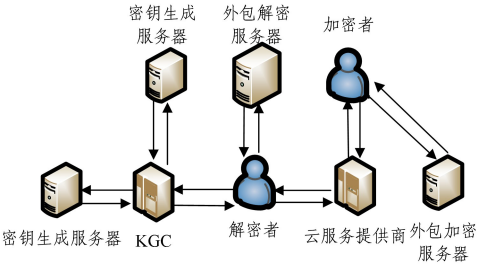

图 1 系统框图

Fig. 1 System chart

初始化算法 $Setup(\lambda,\omega)$:以一个安全参数 λ 及属性集合 ω 作为输入,算法输出系统公钥 PK 和主密钥 MSK,主密钥 MSK 由 KGC 保管。

外包密钥生成预处理 $KeyGen.pre(MSK)$:以主私钥 MSK 作为输入,算法输出外包主密钥 MSK_o 及本地主密钥 MSK_l。

外包密钥生成算法 $KeyGen.out(MSK_o,PK,S)$:以外包主密钥 MSK_o、主公钥 PK,以及用户属性集合 S 作为输入,算法输出中间私钥 ISK。

密钥生成算法 $KeyGen.kgc(PK,MSK_l,ISK_1,ISK_2)$:以本地主密钥 MSK_l 以及两个中间密钥 ISK_1,ISK_2 作为输入,算法输出用户私钥 SK。

外包加密算法 $Encrypt.out(\Gamma,PK)$:以访问树 Γ 以及主公钥 PK 作为输入,输出中间密文 CT'。

用户加密算法 $Encrypt.user(PK,CT',m)$:以系统公钥 PK、中间密文 CT'、明文 m 作为输入,算法输出最终密文 CT。

解密预处理算法 $Decryption.pre(SK)$:以用户私钥作为输入,算法输出外包解密密钥 SK_o 和本地解密密钥 SK_l。

外包解密算法 $Decryption.out(SK_o,CT)$:以外包解密密钥 SK_o 以及密文 CT 作为输入,算法输出中间解密密文 CT''。

用户解密算法 $Decryption.user(SK_l,CT'')$:以本地解密密钥 SK_l 以及中间解密密文 CT'' 作为输入,算法输出明文 m。

4 全外包 CP-ABE 方案

4.1 基本思想

本文将私钥生成工作交由两个密钥生成服务器完成,最后由密钥生成中心(KGC)进行整合,以确保私钥的安全性。将基于访问策略树的属性加密工作交由外包加密服务器完成,数据拥有者负责明文加密和密文整合。在解密部分,用户对私钥进行局部加密并交由外包解密服务器进行数据解密,最终用户只需要进行轻量级的解密。在属性撤销方面,针对撤销属性给未被撤销用户和云服务商分发对应的属性更新密钥,实现即时撤销。

4.2 系统初始化

$setup(\lambda,\omega)$:初始化算法选取一个阶为素数 p、生成元为 g 的双线性群 G_0,然后随机选取 $a,b,\alpha\in Z_p$,对于系统属性集合的每一个元素 a_i,随机选取 $h_i\in Z_p$ 与其一一对应,并计算 $H_i=g^{h_i}$。最后生成系统公钥 PK 和系统主密钥 MSK。

$$PK=\{G_0,g,g^a,g^b,e(g,g)^\alpha,\{H_i=g^{h_i}\mid a_i\in\omega\}\}$$

$$MSK=\{\alpha,a,\{h_i\mid a_i\in\omega\}\}$$

4.3 密钥生成

$KeyGen.pre(MSK)$ 算法由 KGC 运行,随机选取 $\alpha'\in Z_p$,并计算 $MSK_o=g^{\alpha'}$,$MSK_l=g^{\alpha-\alpha'}MSK_o$ 作为外包主公钥,交由密钥生成服务器,进行中间私钥的生成。MSK_l 作为本地主公钥,用于中间私钥的整合。

$KeyGen.out(MSK_o,PK,S)$算法由两个外包密钥生成服务器分别运行,假设用户属性集合 S 包含 n 个属性,外包密钥生成服务器分别随机选取 $n+1$ 个随机数 $t,k_1,k_2,\cdots,k_n\in Z_p$,$t$ 作为用户的随机隐化因子。计算 $d_0=g^{\alpha'}g^t$,$d_1=g^t$;对于用户属性集合的每一个属性 a_i,计算 $d_{i,1}=g^tH_i^{k_i}=g^tg^{h_ik_i}$,$d_{i,2}=g^{k_i}$,然后输出中间密钥 $ISK=\{d_0,d_1,\{d_{i,1},d_{i,2}\}_{i\in[1,n]}\}$,并将中间密密钥 ISK 交由密钥生成中心进行整合。

$KeyGen.kgc(PK,MSK_l,ISK_1,ISK_2)$算法由 KGC 运行,输入本地主密钥和两个中间密钥 ISK_1,ISK_2:

$$ISK_1=\{d'_0,d'_1,\{d'_{i,1},d'_{i,2}\}_{i\in[1,n]}\}$$

$$ISK_2=\{d''_0,d''_1,\{d''_{i,1},d''_{i,2}\}_{i\in[1,n]}\}$$

随机选取 $\lambda,\rho\in Z_p$,并计算:

$$t=t_1+t_2$$

$$d_0=\frac{d'_0\cdot d''_0\cdot g^{a\lambda}\cdot MSK_l}{MSK_o}=g^\alpha g^t g^{a\lambda}$$

$$d_1=g^{t_1}\cdot g^{t_2}\cdot g^{bp}=g^t g^{bp}$$

$$d_2=g^\rho,d_3=g^\lambda$$

对于用户属性集合的每个属性,计算:

$$\{d_{i,1}=d'_{i,1}\cdot d''_{i,1}=g^tg^{h_ik_i},d_{i,2}=d'_{i,2}\cdot d''_{i,2}=g^{k_i}\}_{i\in[1,n]}$$

$$k_i=k'_i+k''_i$$

最后得出用户密钥:

$$SK=\{d_0,d_1,d_2,d_3,\{d_{i,1},d_{i,2}\}_{i\in[1,n]}\}$$

4.4 密文生成

$Encrypt.out(\Gamma,PK)$算法由外包加密服务器运行,输入访问结构树 Γ 和系统主公钥 PK,从访问结构树 Γ 的根节点开始,自上而下对访问结构树的每个非叶子节点 x 随机选取一个(K_x-1)次的多项式 f_x。随机选取 $s'\in Z_p$ 作为访问结构树 Γ 根节点 r 的节点值,设置 $f_r(0)=s'$。对于其他非叶节点 x,设置 $f_x(0)=f_{parent(x)}(index(x))$,令 S 是访问结构树 Γ 中叶子节点的属性集合,计算:

$$\{c_{j,1}=H_j^{f_x(0)}=g^{h_jf_x(0)},c_{j,2}=g^{f_x(0)}\}_{attr(x)\in S}$$

并输出中间密文：

$CT'=\{c'_0=g^{s'},c'_1=g^{bs'},\{c_{j,1},c_{j,2}\}_{attr(x)\in S}\}$

Encrypt.user(PK,CT',m)算法由数据拥有者运行，输入系统公钥 PK，中间密文 CT'，明文信息 m，用户随机选取 $s\in Z_p$，计算：$c=me(g,g)^{as}$，$c_0=g^s$，$c_1=g^{s'}\cdot g^s$，$c_2=g^{bs'}\cdot g^{bs}$，$c_3=g^{as}$，整合得到最终密文 $CT=\{c,c_0,c_1,c_2,c_3\{c_{j,1},c_{j,2}\}_{attr(x)\in S}\}$。

4.5　解密密文

Decryption.pre(SK)算法由数据解密者执行，以私钥 SK 作为输入，随机选取 $a_u\in Z_p$，并计算 $d'_0=d_0\cdot g^{a_u}$，最后得到外包解密密钥：

$SK_o=\{d_0',d_1,d_2,d_3,\{d_{i,1},d_{i,2}\}_{i\in[1,n]}\}$

Decryption.out(SK_o,CT)算法由外包解密服务器运行，以外包解密密钥 SK_o 和密文 CT 作为输入。使用嵌套方式计算访问结构树根节点的值，定义递归算法使用叶子节点的值自底向上进行解密。

1）如果节点 x 是叶子节点，令 $a_j=attr(x)$。如果 $a_j\notin S$，设置 $T_x=$null。如果 $a_j\in S$，则计算：

$$T_x=\frac{e(d_{j,1},c_{j,2})}{e(d_{j,2},c_{j,1})}=e(g,g)^{t\cdot f_x(0)}$$

2）如果节点 x 是非叶子节点，对其自底向上依次进行解密操作。如果 x 的子节点集合 N_x 不满足$|(z\in N_x)\wedge(T_z\neq\text{null})|\geqslant K_x$，设置 $T_x=$null。若满足上述条件，则计算：

$$\begin{aligned}T_x&=\prod_{z\in N_x}T_z^{\Delta_j,s'_x(0)}\\&=\prod_{z\in N}(e(g,g)^{t\cdot f_z(0)})^{\Delta_j,s'_x(0)}\\&=\prod_{z\in N}(e(g,g)^{t\cdot f_{parent(z)}(index(z))})^{\Delta_j,s'_x(0)}\\&=\prod_{z\in N}(e(g,g)^{t\cdot f_x(j)})^{\Delta_j,s'_x(0)}\\&=e(g,g)^{tf_x(0)}\end{aligned}$$

3）如果用户私钥满足访问结构树，最后可以获得根节点的值 $T_r=e(g,g)^{ts'}$，否则计算得到根节点的节点值为 null。

4）根据解密获得的根节点值计算：

$$B=\frac{T_r\cdot e(c_0,d_0')\cdot e(c_3,d_3)^{-1}}{e(c_1,d_2)/e(c_2,d_2)}=e(g,g)^{s(\alpha+a_u)}$$

并将 $CT''=\{c,B\}$ 发送到数据解密者。

Decryption.user(SK_l,CT'')算法由数据解密者执行，输入本地解密密钥 SK_l 和中间解密密文 CT''，计算 $\dfrac{C}{e(g,g)^{s(\alpha+a_u)}/e(g^s,g^{a_u})}=m$。

4.6　属性撤销

在云存储环境中，用户属性的变更较频繁，为了使共享数据不被属性撤销用户获取，提出了属性撤销算法，以保证数据的后向安全性。

当发生属性撤销时，*KGC* 运行密钥更新算法，以系统主密钥 MSK 和撤销属性 a'_i 作为输入，生成新的属性密钥 H'_i，随机选取 $h'_i\in Z_p$，$h'_i\neq h_i$，生成公钥更新密钥和密文更新密钥 $UK'=h'_i/h_i$，用户更新密钥 $USK=g^{(h'_i-h_i)k_i}$。更新公钥 $H^*_{x'}=(H_{x'})^{UK'}=g^{h'_i}$，并将更新密钥分发到云服务提供商和未被属性撤销用户。

用户私钥更新。当用户收到用户更新密钥，运行密钥更新算法更新其密钥：

$SK^*=\{d'_0,d_1,d_2,d_3,d_{i,2},\forall x\in S\backslash\{x'\}:d_{x,1}=g^tg^{h_xk_x},$
$d^*_{x',1}=d_{x',1}\cdot USK=g^tg^{h'_{x'}k_{x'}}\}$

密文更新。当云服务提供商收到密文更新密钥后，运行密钥更新算法更新其密文：

$CT=\{c,c_0,c_1,c_2,c_3,c_{j,2},\forall x\in S\backslash\{x'\}:c^*_{x,1}=c_{x,1},$
$c^*_{x',1}=(c_{x',1})^{UK'}=g^{h'_iq_{x'}(0)}\}$

5　全外包 CP-ABE 方案分析

5.1　安全性分析

本节通过证明 3 个定理来验证全外包 CP-ABE 方案可以抵抗选择性明文攻击、用户合谋攻击，且具有前后向安全性能，保障数据在网络通信中的安全性。

定义 1（DBDH 问题，判定双线性问题）　设 G_1,G_2 为阶是素数 p 的乘法循环群，g 为 G_1 的生成元。存在双线性映射 $e:G_1\times G_1\rightarrow G_2$，判定双线性问题为：给定 $a,b,c,\theta\in Z_p^*$，$\mathbb{Z}\in G_1,g,g^a,g^b,g^c,\mathbb{Z}=e(g,g)^\theta$，判定 $\mathbb{Z}=e(g,g)^{abc}$ 是否成立。若等式成立，则 $g,g^a,g^b,g^c,\mathbb{Z}$ 是一个 DBDH 元组。如果有一个概率多项式的算法解决上述问题的概率为 ε，则称该算法解决 DBDH 问题的优势为 ε。

定理 1　在 DBDH 游戏中，如果任意概率多项式时间的敌手的优势可以忽略，则本文方案是选择明文安全的。

证明：假设存在一个多项式敌手 A 可以攻破全外包 CP-ABE 方案，则存在一个算法 B 能以 ε 的优势攻破 DBDH 问题。

初始化阶段：攻击者 A 选择访问结构树 Γ^*，并将其发送给挑战者 B。

系统设置：挑战者 B 运行 *setup*(λ,ω)算法，具体过程如下。

1）选择随机数 $x'\in Z_p^*$，使得 $e(g,g)^{ab}e(g,g)^{x'}=e(g,g)^{\alpha}$；

2）对于所有的 $a_i\in S$，随机选取 $q_i\in Z_p^*$，当 $a_i\notin\Gamma^*$，设 $H_i=B^{1/q_i}$，得 $h_i=b/q_i$，如果 $a_i\in\Gamma^*$，设 $H_i=g^{q_i}$，此时 $h_i=q_i$；

3）计算 $Y=e(g,g)^\alpha$，生成公钥 $PK=\{G_0,g,g^x,g^y,Y,H_i(1\leqslant i\leqslant n)\}$ 和主密钥 $MSK=\{\alpha,x,q_i(1\leqslant i\leqslant n)\}$。

挑战者 B 将公钥交给攻击者 A，自己保留主密钥。

阶段 1：攻击者 A 选择属性集 $w=\{a_i|a_i\notin\Gamma^*\}$，并向挑战者 B 发出私钥申请。

1）挑战者 B 选择 $t'\in Z_p^*$，计算 $d_0=g^{x'-t'b}g^{a\lambda}$，得出 $t=-(ab+t'b)$；

2）由得出的 t 计算对应的属性私钥 $d_1,d_2,d_3,\{d_{i,1},d_{i,2}\}$。

挑战者 B 将属性私钥返回给攻击者 A。

挑战：攻击者 A 递交两个长度相等的信息 m_0,m_1，挑战者 B 抛硬币选取 $v\in\{0,1\}$，返回密文 C_v。

1）第一层加密 $c_0=g^c$。

$c=m_ve(g,g)^{\alpha c}=m_ve(g,g)^{abc+x'c}=m_v\mathbb{Z}e(g^c,g^{x'})$

2）第二层加密，随机选取一个 $c'\in Z_p^*$，c' 为访问结构树根

节点的值。自上而下对访问结构树进行赋值，生成对应的 $c_{j,1}$，$c_{j,2}$。

3）计算对应的 c_1，c_2，c_3，输出密文 $C_v=\{c,c_0,c_1,c_2,c_3,\forall a_j\in\Gamma^*:\{c_{j,1},c_{j,2}\}\}$。挑战者 B 将密文 C_v 返回给攻击者 A。

阶段 2：同阶段 1，攻击者 A 可以继续向挑战者 B 询问信息。

猜测：攻击者 A 输出猜测 $v'=\{0,1\}$。如果 $v'=v$，表示 DBDH 成立，$\mathbb{Z}=e(g,g)^{abc}$，反之当 $v'\neq v$，表明 $\mathbb{Z}=e(g,g)^{\theta}$。当 $v'=v$，攻击者获得有效密文时，攻击者的优势等于 $p_r[v'=v|\mathbb{Z}=e(g,g)^{abc}]=1/2+\varepsilon$。反之当 $v'\neq v$，攻击者获得的密文是随机的，攻击者的优势等于 $p_r[v'\neq v|\mathbb{Z}=e(g,g)^{\theta}]=1/2$。

如上所述，攻击者可以以 $\varepsilon/2$ 的优势攻破本文方案，因此，在 DBDH 安全的条件下，本方案是选择性明文安全的。

定理 2 提出的方案可以抵抗用户合谋攻击。

证明：在 CP-ABE 方案中，秘密分享应该被嵌入加密密文中而不是用户密钥中。为了解密密文，合谋攻击者们必须恢复 $e(g,g)^{\alpha s}$，在本方案中若用户需要还原 $e(g,g)^{\alpha s}$，必须先使用用户私钥中的 $d_{i,1}$，$d_{i,2}$ 和加密密文中的 $c_{j,1}$，$c_{j,2}$ 进行双线性配对。假设攻击者没有关于属性 a 的私钥，则其需要从其他合谋用户处获取关于属性 x 对应的 $d_{i,1}$，$d_{i,2}$。但是针对每个用户的 $d_{i,1}$，其中都包含用户唯一的隐化因子 t，因此每个用户的 $d_{i,1}$ 都具有唯一性。合谋攻击者即使拥有 2 个或 2 个以上的用户私钥信息，也无法获得 t 的任何信息。因此，在利用合谋密钥进行叶子节点解密时所获得的叶子节点值的集合可能为：

$$\{e(g,g)^{t_1 f_x(1)},e(g,g)^{t_1 f_x(2)},e(g,g)^{t_2 f_x(3)},\cdots,e(g,g)^{t_n f_x(K_x)}\}$$

由于叶子节点值的标示分别对应多个用户，因此无法自底向上地还原非叶子节点的值。

综上所述，非授权用户无法通过属性串谋的方式解密密文，因此本文能够抵抗合谋攻击。

定理 3 所提方案具有前向安全性和后向安全性。

证明：当发生属性撤销时，系统会针对撤销属性生成对应的用户更新密钥和密文更新密钥。

一方面，当一个属性 x 被撤销，系统中的每一个未被撤销用户都会获得对应的属性更新密钥 USK，进而更新自己的属性私钥。云服务提供商会获得一个密文更新密钥 UK' 来更新新对应的属性密文。被撤销属性的用户无法用原有的私钥解密更新后的密文。因此本文方案具有后向安全性。

另一方面，如果用户的属性满足访问策略，那么其仍能解密未加入系统之前的密文。因为，当用户加入系统时，关于用户属性的私钥已经被更新，用户获得的私钥是更新过的私钥，他可以使用更新后的私钥来解密之前的已更新的密文。因此本文方案具有前向安全性。

5.2 效率分析

为了评估本文 CP-ABE 方案的效率，选取一些高效的 ABE 方案进行性能比较，性能主要以理论计算开销来评价。由于乘法计算开销远小于幂指数运算和双线性对计算，因此本文以幂指数运算和双线性对计算作为标准。对比的第一个方案是 Li 等[19]提出的一种高效、可靠的外包加密方案，将用户的加密计算开销控制在常量级别。第二个方案是李勇等[15]提出的支持属性撤销的外包解密方案，该方案将部分解密交由代理者执行，减小了用户的解密计算量，提高了系统效率。第三个对比方案是 Mao 等[10]提出的可验证的外包解密方案，系统可以验证外包计算结果的正确性，提高系统的整体稳定性。

表 1 和表 2 分别列出了本地计算开销以及网络传输数据开销的对比结果。其中，E 代表幂指数运算，P 代表双线性对计算，N 代表系统属性集合的数量，L 代表加密属性集合的数量，K 表示解密属性集合的数量。由表 1 可知，本文方案的密钥生成、加密、解密、属性撤销的计算开销均是线性的，计算开销明显优于对比方案，虽然使用全外包方案导致传输量线性增加，但其与对比方案的传输开销还是同一个量级。

表 1 计算开销

Table 1 Computational overhead

方案	密钥生成	加密	解密	密钥更新	密文更新
Li[19]	$(1+3N)E$	$4E$	$KE+2KP$	—	—
李勇[15]	$(3+N)E$	$(3L+2)E$	E	E	E
Mao[10]	$(3+N)E$	$(3L+4)E$	E	—	—
本文	$4E$	$4E$	$E+P$	E	E

表 2 传输开销

Table 2 Transmission overhead

	密钥生成	加密	解密
Li[19]	$(1+2N)E$	$(3+2L)E+P$	$(3+2L)E+P$
李勇[15]	$(2+N)E$	$(1+2L)E+P$	$(2+K)E+P$
Mao[10]	$(2+N)E$	$(1+2L)E+P$	$(2+K)E+P$
本文	$(12+6N)E$	$(3+2L)E+P$	$(4+2K)E+P$

结束语 本文提出了一个支持属性撤销的全外包 CP-ABE 方案，将密钥生成、加密和解密的复杂计算任务外包给相关的外包服务器，将系统和用户的计算开销控制在常量级，减少了用户和系统的总体计算量，提高了系统整体效率。本文给出了一种高效的属性撤销方法，达到了属性撤销的高效性和细粒度的目的。但本方案对访问策略的选取有一定的局限性并且采用全外包方案增加了数据传输开销，因此今后应对访问策略进行优化并对离线状态的外包方案深入研究，使得访问策略更具有灵活性、安全性，同时减少网络传输开销，使其更好地运用到实际环境中。

参 考 文 献

[1] WANG Y D, YANG J H, XU C, et al. Survey on access control technologies for cloud computing[J]. Journal of Software, 2015, 26(5): 1129-1150. (in Chinese)
王于丁，杨家海，徐聪，等. 云计算访问控制技术研究综述[J]. 软件学报，2015，26(5)：1129-1150.

[2] SHAMIR A. Identity-Based Cryptosystems and Signature Schemes[M]// Advances in Cryptology. Springer Berlin Heidelberg, 1984: 47-53.

[3] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005: 457-473.

[4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption[C]// IEEE Symposium on Security & Privacy. 2007.

[6] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]// Usenix Conference on Security. USENIX Association, 2011: 34.

[7] ZHOU Z, HUANG D. Efficient and secure data storage operations for mobile cloud computing[C]// International Conference on Network and Service Management. International Federation for Information Processing, 2012: 37-45.

[8] ASIM M M, PETKOVIC M M, IGNATENKO T T. Attribute-based encryption with encryption and decryption outsourcing [C]// Conference on Innovations in Clouds, Internet and Networks. 2014.

[9] CHOW S S M. A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation[C]// ACM on Symposium on Access Control Models and Technologies. ACM, 2016: 215-226.

[10] MAO X, LAI J, MEI Q, et al. Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption[J]. IEEE Transactions on Dependable & Secure Computing, 2016, 13(5): 533-546.

[11] WANG H, HE D, SHEN J, et al. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing[J]. Soft Computing, 2016, 21(24): 1-11.

[12] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]// INFOCOM, 2010 Proceedings IEEE. IEEE, 2010: 1-9.

[13] YANG K, JIA X, REN K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]// ACM Sigsac Symposium on Information, Computer and Communications Security. ACM, 2013: 523-528.

[14] HUR J, NOH D K. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 22(7): 1214-1221.

[15] LI Y, ZENG Z Y, ZHANG X F. Outsourced decryption scheme supporting attribute revocation[J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12): 1664-1669. (in Chinese)
李勇,曾振宇,张晓菲. 支持属性撤销的外包解密方案[J]. 清华大学学报(自然科学版),2013,53(12):1664-1669.

[16] MA H, BAI C C, LI B, et al. Attribute-based encryption scheme supporting attribute revocation and decryption outsourcing[J]. Journal of Xidian University, 2015, 42(6): 6-10. (in Chinese)
马华,白翠翠,李宾,等. 支持属性撤销和解密外包的属性基加密方案[J]. 西安电子科技大学学报,2015,42(6):6-10.

[17] FANG X F, WANG X M. Outsourced Encryption and Decryption CP-ABE Scheme with User Revocation [J]. Computer Engineering, 2016, 42(12): 124-128, 132. (in Chinese)
方雪锋,王晓明. 可撤销用户的外包加解密 CP-ABE 方案[J]. 计算机工程,2016,42(12):124-128,132.

[18] ZHANG P, CHEN Z, LIANG K, et al. A Cloud-Based Access Control Scheme with User Revocation and Attribute Update[C]// Australasian Conference on Information Security and Privacy. Springer International Publishing, 2016: 525-540.

[19] LI J, JIA C, LI J, et al. Outsourcing encryption of attribute-based encryption with mapreduce[C]// International Conference on Information and Communications Security. Springer-Verlag, 2012: 191-201.