基于授权的多服务器可搜索密文策略属性基加密方案

张玉磊[①] 刘文静*[①] 刘祥震[①] 张永洁[②] 王彩芬[①]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](甘肃卫生职业学院 兰州 730070)

摘 要：针对现有属性基可搜索加密方案缺乏对云服务器授权的服务问题，该文提出一种基于授权的可搜索密文策略属性基加密(CP-ABE)方案。方案通过云过滤服务器、云搜索服务器和云存储服务器协同合作实现搜索服务。用户可将生成的授权信息和陷门信息分别发送给云过滤服务器和云搜索服务器，在不解密密文的情况下，云过滤服务器可对所有密文进行检测。该方案利用多个属性授权机构，在保证数据机密性的前提下能进行高效的细粒度访问，解决数据用户密钥泄露问题，提高数据用户对云端数据的检索效率。通过安全性分析，证明方案在提供数据检索服务的同时无法窃取数据用户的敏感信息，且能够有效地防止数据隐私的泄露。

关键词：云存储；授权服务器；可搜索加密；密文策略属性基加密；多属性授权机构

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)08-1808-07

DOI: 10.11999/JEIT180944

Searchable Multi-server CP-ABE Scheme Based on Authorization

ZHANG Yulei[①] LIU Wenjing[①] LIU Xiangzhen[①]

ZHANG Yongjie[②] WANG Caifen[①]

[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*Gansu Health Vocational College*, *Lanzhou* 730070, *China*)

Abstract: Considering that the existing attribute-based searchable encryption scheme lacks the authorization service to the cloud server, a multi-server searchable Ciphertext Polity Attribute Base Encryption (CP-ABE) scheme is proposed based on authorization. The scheme implements search services through a cloud filter server, cloud search server and cloud storage server cooperation mechanism. The users send the authorization information to the cloud filter server at once, then the server creates the authorization information; The cloud search server creates the trapdoor information based on the trapdoor information sent by the users. Without decrypting the cipher text, the cloud filter server can detect all the cipher texts. Multiple attribute authorities can be used to ensure efficient and fine-grained access under the premise of ensuring data confidentiality, solving the problem of leakage of data user keys. It can improve the data retrieval efficiency when people use the cloud server. Through security analysis, it is proved that the scheme can not steal sensitive information of data users while providing data retrieval services, and it can effectively prevent the leakage of data privacy.

Key words: Cloud storage; Authorization server; Searchable encryption; Attribute-based cipher text policy encryption; Multi-attribute authority

1 引言

云服务具有灵活、方便、快捷等特点，许多数据用户将数据上传至云端存储。这些数据可能会包含用户隐私信息，如果云服务器存在安全漏洞，数据将失去安全保障，并可能给用户带来无法挽回的损失。因此，用户希望将数据加密处理后再上传至云服务器以保证数据机密性，但是却给云服务器实现数据检索带来了困难。2004年，Boneh等人[1]提出能够加密数据，还可以对密文进行检索操作[2]的公钥可搜索加密(Public key Encryption with Keyword Search, PEKS) 方案。2006年，Baek等人[3]提出了改进方案，但仅适用于安全信道的传输。

收稿日期：2018-10-10；改回日期：2019-01-19；网络出版：2019-02-18

*通信作者： 刘文静 lwj19940212@qq.com

基金项目：国家自然科学基金(61163038, 61262056, 61262057)，甘肃省高等学校科研项目(2017A-003, 2018A-207)

Foundation Items: The National Natural Science Foundation of China (61163038, 61262056, 61262057), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

2008年，Baek等人[4]又提出不需要安全信道的PEKS方案，解决传输关键词陷门时需要安全信道的不足。2013年，文献[5]构造了一种多关键字搜索方案，但该方案仅适用于用户自己检索自己上传至云服务器的数据，无法支持其他用户对数据检索的功能。随后，一些学者提出能够实现多用户搜索的加密方案[6,7]。这些方案通过共享对称密钥的方式进行数据共享，但是无法真正实现对用户访问权限的细粒度访问。

属性基加密[8](Attribute-Based Encryption, ABE)可以对数据进行“一对多”加密，实现高效的细粒度信息共享，更适用于云存储环境[9]。2014年，李双等人[10]首次提出属性基可搜索加密方案，实现关键词密文细粒度的安全共享，解决数据用户密钥泄露问题，提高数据用户对云端数据的检索效率。但该方案不支持数据用户自主生成搜索凭证，需要在授权机构和用户之间建立安全信道，造成额外开销。2016年，文献[11]和文献[12]分别提出可验证的属性基可搜索加密方案。两个方案均能实现对数据的高效搜索，但都无法抵抗关键词猜测攻击。

基于授权的公钥可搜索加密方案是由Luan等人在文献[13]中首次提出，这种加密方式只需一次授权就能够对所有密文消息进行搜索。文献[14,15]通过指派搜索服务器构造了属性基可搜索加密方案，能够抵抗关键词猜测攻击。但这两个方案在执行加密和搜索操作时，对属性访问策略有限制，算法的复杂度较高。2017年，文献[16]提出了一个多数据拥有者认证的密文检测方案，该方案由数据拥有者向用户授权，若用户发生增减，授权权限也会随之发生变化，造成系统额外开销。同年，文献[17]构造了一个多服务器多关键词的可搜索加密方案，该方案仅仅是将数据消息以密文的形式分别存储到多个云服务器并不能实现对所有密文消息进行搜索。

为了解决以上不足，本文将基于授权的公钥可搜索加密和属性基加密相结合，提出了一种基于授权的多服务器可搜索密文策略属性基加密(CP-ABE)方案。利用多个属性授权机构，解决用户密钥泄露问题，数据拥有者可选择可信的云过滤服务器和云搜索服务器分别保存授权信息和陷门信息，将密文保存至云存储服务器；当用户需要搜索服务时，云过滤服务器利用授权信息检测用户属性的访问结构与授权信息中的访问结构是否匹配，只有用户属性满足访问结构时才能进行搜索服务。若检测通过，则云搜索服务器利用陷门信息再检测密文信息中是否包含用户选取的明文消息的密文，最后云存储服务器返回密文，用户完成解密。

限于篇幅，本文省略方案涉及的数学困难问题的描述。

2　基于授权的多服务器可搜索CP-ABE方案模型

2.1　方案的系统架构

基于授权的可搜索CP-ABE系统架构主要包括6个主体：数据拥有者(Data Owner, DO)、N个属性授权中心(Attribute Authority, AA_i)、云搜索服务器(Cloud Search Server, CSS′)、云过滤服务器(Cloud Filter Server, CFS)、云存储服务器(Cloud Storage Server, CSS)和数据用户(Data User, DU)。其中，系统模型中的AA_i要求可信；3个云服务器是诚实但好奇的，既能够诚实地根据用户的需求返回相对应的服务，也会在通信过程中尝试窃取用户的隐私，如图1所示。

(1) 数据拥有者DO：数据拥有者为数据定制访问结构W并生成随机数用于数据用户的解密，同时，加密数据生成密文CT并将其上传至CSS。

(2) 数据用户DU：利用自己的私钥$\mathrm{SK_L}$和服务器的公钥$\mathrm{PK_s}$为CSS′和CFS分别产生授权信息$t_{\omega,s}$和陷门信息$t_{m,s}$。只有当属性满足密文对应的访问结构时，才能对密文进行解密。

(3) 多属性授权中心AA_i：系统中有N个AA，主要负责生成系统参数和主密钥，管理DO的不同属性集，为用户生成和分发私钥。这里要求每个AA可信。

(4) 云过滤服务器CFS：收到DU的授权信息$t_{\omega,s}$后，CFS利用$t_{\omega,s}$检测用户自身属性的访问结构与授权信息中所用的访问结构是否匹配，只有自身属性满足访问结构时才能进行搜索服务。

(5) 云搜索服务器CSS′: CSS′保存数据拥有者关键词的密文信息，当且仅当数据用户产生的陷门

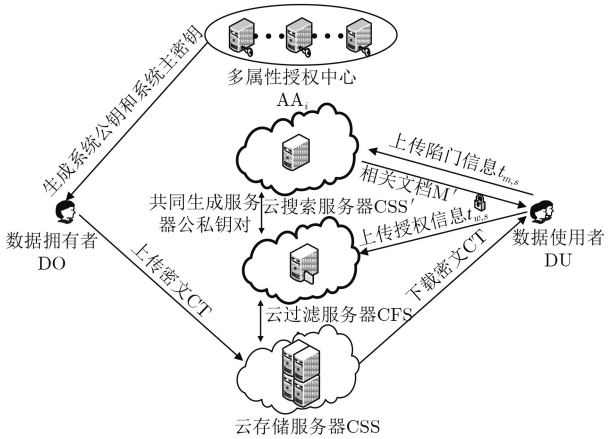

图 1 基于授权的可搜索CP-ABE模型

信息$t_{m,s}$满足关键词的加密信息时返回正确信息，完成密文搜索操作。

(6) 云存储服务器CSS：存储数据用户上传的密文CT，只有CFS和CSS′通过授权信息$t_{\omega,s}$和陷门信息$t_{m,s}$的检测时，才返回给DU密文。

2.2 方案的形式化定义

基于授权的多服务器可搜索CP-ABE方案包括以下9个算法：

(1) Setup：该算法由多个属性授权中心运行，首先生成属性集合U，每个AA_i管理不同的属性集合U_i，生成系统参数pa和系统主密钥msk。

(2) SkeyGen：该算法由云过滤服务器CFS和云搜索服务器CSS′共同运行，输入pa生成公私钥对 ($\mathrm{SK_s}$,$\mathrm{PK_s}$)。

(3) UkeyGen：该算法由DU和AA_i共同运行，输入属性列表L、系统主密钥msk，生成与用户属性相对应的用户私钥$\mathrm{SK_L}$。

(4) Encrypt：该算法由DO执行。输入消息m，指定访问结构W，输出密文CT。

(5) Delegate：该算法由DU执行。输入$\mathrm{PK_s}$和$\mathrm{SK_L}$，为云过滤服务器生成授权信息$t_{\omega,s}$。

(6) TrapGen：该算法由DU执行，为云搜索服务器生成陷门信息$t_{m,s}$。

(7) Test1：该算法由CFS执行，利用云过滤服务器的私钥$\mathrm{SK_s}$和CT检测授权信息$t_{\omega,s}$是否满足CT中定义的访问结构，若满足，则返回1，否则返回0。

(8) Test2：该算法由CSS′执行，当返回值为1时，CSS′将产生搜索数据，并将生成结果返回给DU。

(9) Decrypt：该算法由DU执行，当DU得到从CSS′返回的搜索数据M'时，利用$\mathrm{SK_L}$和CT进行解密得到明文m。

3 基于授权的多服务器可搜索CP-ABE方案

3.1 方案构造

(1) Setup：由多个属性授权机构AA_i运行，首先设全局属性集合为$U=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_i,\cdots,\mathrm{att}_n\}$，$G_0$是阶为$p$，生成元为$g$的双线性群，选取$e: G_0\times G_0\to G_1$为双线性映射。假设有$N$个$\mathrm{AA}_i$，所有授权机构随机选择$\alpha_k\in Z_p^*\,(k\in(1,2,\cdots,N))$，计算$Y_k=e(\mathrm{g},\mathrm{g})^{\alpha_k}$并发送给所有其他的属性授权机构，每个属性授权机构都可以计算$Y=\prod_{k\in(1,2,\cdots,N)}Y_k=e(g,g)^{\sum_{k\in(1,2,\cdots,N)}\alpha_k}$。$\mathrm{AA}_i$为属性集合中的属性$\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_i,\cdots,\mathrm{att}_n$选择随机值$t_{i,j}\in Z_p(i\in(1,n),j\in(1,n_i))$，计算$T_{i,j}=g^{t_{i,j}}$ $(i\in(1,n),j\in(1,n_i))$。数据拥有者DO随机选择$r\in Z_p^*$，计算$d_1=g^r$并通过安全信道将d_1传输给数据用户。公布系统参数$\mathrm{pa}=\{Y,e,g,G_0,G_1,T_{i,j}$ $(i\in(1,n),j\in(1,n_i))\}$，系统主密钥$\mathrm{msk}=\{\alpha_k,r\}$由每个$\mathrm{AA}_i$保存。

(2) SkeyGen: CFS和CSS′分别随机选择$s,t\in Z_p^*$作为其私钥，生成公钥$\mathrm{PK_s}$，即公私钥对为$(\mathrm{SK_s},\mathrm{PK_s})=(st,g^{st})$。

(3) UkeyGen：该算法由DU运行，输入pa，令用户属性列表$L=(L_1,L_2,\cdots,L_i,\cdots,L_n)$，$\mathrm{AA}_i$计算${d_0}^k=g^{\alpha_k}$，随机选择$\lambda_i\in Z_P^*$，并计算$d_{i,j,1}=g^{r+\lambda_i t_{i,j}}$，$d_{i,j,2}=g^{\lambda_i}\,(i\in(1,n),\ j\in(1,n_i))$。当DU收到$\mathrm{AA}_i$反馈的属性私钥组件后，计算$d_0=\prod_{k\in(1,2,\cdots,N)}d_0^k=g^{\sum_{k\in(1,2,\cdots,N)}\alpha_k}$，最后生成DU的私钥$\mathrm{SK_L}=\left(d_0,\forall\mathrm{att}_i\in L:\{d_{i,j,1},d_{i,j,2}\}_{i\in(1,n),j\in(1,n_i)},d_1\right)$。

(4) Encrypt: DO选择消息$m\in G_1$和访问策略$W=(W_1,W_2,\cdots,W_n)$，随机选择$\beta\in Z_p^*$用于计算密文$C_0=g^{\beta}$，$C_1=mY^{\beta}=me(g,g)^{\sum_{k\in(1,2,\cdots,N)}\alpha_k\beta}$。

将树形访问结构的根节点设为β并进行“标记”，将其儿子节点设为“未标记”，并将所有“未标记”的非叶子节点进行递归运算。执行递归算法时，当递归到“未标记”的非叶子节点是“与”门，则DO随机选择$\beta_i\in Z_p(1\le\beta_i\le p-1)$，设置最后一个儿子节点的值为$\beta_j=\beta-\sum_{i=1}^{j-1}\beta_i \bmod p$，并将该节点标记为“已标记”；当递归到“未标记”的非叶子节点为“或”门时，将根节点β标记为“已标记”，并设该节点的值为该节点下任意节点的值。

对于访问结构的叶子节点，数据拥有者计算$C_{i,j,1}=g^{\beta_i}$，$C_{i,j,2}=T_{i,j}{}^{\beta_i}$，并返回密文$\mathrm{CT}=\left\{C_0,C_1,\{C_{i,j,1},C_{i,j,2}\}_{i\in(1,n),j\in(1,n_i)}\right\}$，将CT上传至CSS。

(5) Delegate: DU输入$\mathrm{PK_s}$和$\mathrm{SK_L}$，随机选择$v\in Z_p^*$，计算$T_0=g^{stv}$，$T_1=g^{\lambda_i v}$，$T_2=T_{i,j}{}^{v}=g^{vt_{i,j}}$，$d_{i,j,1}{}'=g^{(r+\lambda_i t_{i,j})v}$和$d_{i,j,2}{}'=g^{\lambda_i vr}$，输出生成的授权信息$t_{\omega,s}=\left(T_0,T_1,T_2,\forall\mathrm{att}_i\in L:\left\{d_{i,j,1}{}',d_{i,j,2}{}'\right\}_{i\in(1,n),j\in(1,n_i)}\right)$。

(6) TrapGen: DU输入$\mathrm{SK_L}$，随机选择$\mu\in Z_p^*$，计算$T_3=d_0^{\mu}$，$T_4=d_1^{\mu}$和$T_5=g^{\lambda_i\mu t_{i,j}}$，输出为CSS′生成的陷门信息$t_{m,s}=(T_3,T_4,T_5)$。

(7) Test1: CFS根据DU在Delegate阶段生成的$t_{\omega,s}$和DO在Encrypt阶段生成的CT来进行信息检测。输入CFS私钥$\mathrm{SK_s}$和CT检测$t_{\omega,s}$是否满足CT中定义的访问结构，若满足，则返回1，否则返回0。

判断$t_{\omega,s}$是否满足CT定义的访问结构，通过递归函数DecryptNode(x)执行。

当节点x为叶子节点时，i是叶子节点x对应的属性，若$i \in U$，则$\mathrm{DecryptNode}(x)=\dfrac{e\left(c_{i,j,1}, d_{i,j,1}{}'\right)}{e\left(c_{i.i.2}, d_{i.i.2}{}'\right)}=\dfrac{e\left(g^{\beta_i}, g^{(r+\lambda_i t_{i,j})v}\right)}{e\left(g^{\beta_i t_{i,j}}, g^{\lambda_i v r}\right)}=\dfrac{e(g,g)^{\beta_i v(r+\lambda_i t_{i,j})}}{e(g,g)^{\beta_i t_{i,j}\lambda_i v r}}=e(g,g)^{\beta v}$。否则，DecryptNode($x$)输出为空。

当节点x为非叶子节点时，对节点x的子节点进行计算，即：$F_{x'}=\mathrm{DecryptNode}(x')$假设$S_{x'}$是$F_{x'}$不为空的子节点$x'$的一个任意$k_x$大小的集合，若不存在这样的集合$S_{x'}$，则DecryptNode($x$)为空。否则计算$F_x=\prod_{x'\in S_{x'}} F_{x'}{}^{\Delta i S_{x'}}=\prod_{x'\in S_{x'}} e(g,g)^{\beta_i v \Delta i S_{x'}}=e(g,g)^{\beta_i v}$，其中$\Delta i S_{x'}$是拉格朗日系数。

利用拉格朗日插值定理可得$D=\mathrm{DecryptNode}(x')=e(g,g)^{\beta v}$。

验证等式如下：计算$T_2'=T_2^{st}$, $A=e(T_1,T_2')$, $B=e(T_0,T_2)$, $C=A/B$, $F=e(C_0,T_1)$和$E=F/C$。根据$E=D$得出返回值b, $b\in(0,1)$。

(8) Test2：该算法由CSS′执行，当Test1算法阶段返回值为1时，CSS′将产生搜索数据，计算$M'=\dfrac{e(C_0,T_4T_5)\,C_1}{e(C_0,T_3)}$将生成结果返回给DU。

(9) Decrypt：该算法由DU执行，当DU得到从CSS′返回的加密信息M'，利用$\mathrm{SK_L}$和CT进行解密得到密文m。即计算$m=\dfrac{M'}{e(C_0,d_{i,j,1})}$。

3.2 方案的安全分析

限于篇幅，本文略去对用户抗共谋性、数据保密性和服务器返回结果安全性的理论分析。

(1) 密文不可区分性：指敌手A要想从密文中学习到任何消息是不可行的。

证明　若敌手A在一个概率多项式时间内能以不可忽略的优势ε赢得游戏，则证明挑战者B能够以不可忽略的优势$\varepsilon/2$解决CDH困难问题。

在游戏过程中，由于v, μ是随机元素，因此，设DU^*私钥，$t_{\omega,s}$和$t_{m,s}$的生成方式和本方案中生成方式一致。

(a) Setup：设G_1是阶为素数p，生成元为g的乘法循环群；B随机选择$s,t\in Z_p^*$，将服务器的公私钥对设置为$(\mathrm{SK_s},\mathrm{PK_s})=(st,g^{st})$，输入安全参数$\tau$，生成系统公共参数pa。

(b) UkeyGen to $\mathrm{O_1}$: B输入pa，为DU^*计算私钥。B既不知道a的值也不知道具体的私钥。$\mathrm{SK_L}^*=\left(d_0,\forall \mathrm{att}_i\in L:\{d_{i,j,1}{}^*,d_{i,j,2}\}_{i\in(1,n),j\in(1,n_i)},d_1{}^*\right)$其中，$d_0=\prod_{k\in(1,\cdots,N)} d_0^k=g^{\sum_{k\in(1,2,\cdots,N)}\alpha_k}$, $d_1{}^*=g^a$, $d_{i,j,1}{}^*=g^{a+\lambda_i t_{i,j}}$和$d_{i,j,2}=g^{\lambda_i}(i\in(1,n),j\in(1,n_i))$。

(c) Delegate Query to $\mathrm{O_2}$：为DU请求一个$t_{\omega,s}$，若DU=DU^*, B停止模拟返回猜测值u'；若$\mathrm{DU}\neq\mathrm{DU}^*$, B进行模拟，随机选择$v\in Z_p^*$输出$t_{\omega,s}=\left(T_0,T_1,T_2,\forall \mathrm{att}_i\in L:\left\{d_{i,j,1}{}',d_{i,j,2}{}'\right\}_{i\in(1,n),j\in(1,n_i)}\right)$。

(d) TrapGen Query to $\mathrm{O_3}$: A向B请求一个$t_{m,s}$，若DU=DU^*, B停止模拟返回猜测值u'；若DU≠DU^*, B随机选择$\mu\in Z_p^*$输出$t_{m,s}=(T_3,T_4,T_5)$。其中，$T_3=d_0^{\mu}$, $T_4=d_1^{\mu}$和$T_5=g^{\lambda_i\mu t_{i,j}}$。

(e) Challenge：A向B发送两个消息m_0和m_1，并请求由DO生成一个消息密文。若$\mathrm{DU}\neq\mathrm{DU}^*$, B停止模拟返回猜测值$u'$；若DU=$\mathrm{DU}^*$, B随机抛硬币得到$\xi\in_R\{0,1\}$并设置$\beta=b$，返回密文$\mathrm{CT}'=\left\{C_0',C_1',\left\{C_{i,j,1}{}',C_{i,j,2}{}'\right\}_{i\in(1,n),j\in(1,n_i)}\right\}$。其中，$C_0'=g^b$, $C_1'=mY^b=me(g,g)^{\sum_{k\in(1,2,\cdots,N)}\alpha_k b}$，$C_{i,j,1}{}'=g^{b_i}$和$C_{i,j,2}{}'=T_{i,j}{}^{b_i}$。若$\xi=0$，则令$T_\xi=g^{ab}$，否则令$T_\xi\in G_1$。

(f) Guess：在游戏结束时，假设A可以向每个用户索取密文并能对$\mathrm{O_2}$, $\mathrm{O_3}$进行陷门请求。因此，在非中断模拟的情况下，A应该有所有用户生成的密文，至少有一个由DU^*产生的一个有效或无效的挑战密文CT′，但A不具有相对应的陷门。最后，A输出猜测u'，若猜测正确$u'=u$，则B设置$\xi'=0$，令$T_{\xi_0}=g^{ab}$，否则设置$\xi'=1$，令$T_{\xi_1}\in G_1$。

假设B在不中止模拟期间，若$\xi=0$，则CT′是由DU^*产生的一个有效密文，那么说明A游戏成功，这种情况发生的概率为$1/2+\varepsilon$。若$\xi=1$，则CT′是由DU^*产生的一个随机密文，说明A没有获取任何消息密文，这种情况发生的概率为1/2。在所有的游戏过程中A和B的优势一致。

假设B在TrapGen Query或Challenge阶段中止模拟期间，B独立于A的猜测阶段输出猜测u'。因此，B在中止模拟期间的优势为1/2，定义总体优势为$\varepsilon/2$。

假设A在TrapGen Query阶段最多进行q次询问，系统中有n个用户，由于有且仅有一个用户在TrapGen Query阶段不能回答B，因此导致B查询中止的概率最多为$1/n$。A能够进行q次询问，在TrapGen Query阶段中止的总概率为q/n，因此B不中止模拟的概率为$1-q/n$, B在Challenge阶段不中止的概率为$1/n$。

综上所述，B挑战成功的总体优势为$1/n(1-q/n)\cdot\varepsilon/2$。根据CDH数学困难问题，A在一个概率多项式时间内无法计算g^{ab}解出密文，故

本方案满足密文不可区分性。

(2) 陷门不可区分性：本方案中DU利用CFS和CSS′的公钥$\mathrm{PK_s}$和$\mathrm{SK_L}$生成$t_{\omega,s}$, $t_{m,s}$，由于CFS拥有私钥$\mathrm{SK_s}$，所以只有CFS检测通过才能对加密的数据进行检测。

证明 敌手A在一个概率多项式时间内能以不可忽略的优势ε赢得游戏，则证明挑战者B能够以不可忽略的优势$\varepsilon/2$解决CDH困难问题。

在游戏过程中，由于v, μ是随机元素，因此，设用户私钥，$t_{\omega,s}$和$t_{m,s}$的生成方式和本方案中生成方式一致。

(a) Setup：设G_1是阶为素数p，生成元是g的乘法循环群；B随机选择$a\in Z_p$，将CFS的公钥设为$\mathrm{PK_s}=g^a$，输出pa。B随机抛硬币得$\xi\in\{0,1\}$，若$\xi=0$，令$T_\xi=g^{ab}$，否则$T_\xi\in G_1$。

(b) UkeyGen to $\mathrm{O_1}$: B为DU计算私钥$\mathrm{SK_L}=\left(d_0,\forall \mathrm{att}_i\in L:\{d_{i,j,1},d_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]},d_1\right)$。其中，$d_0=\prod_{k\in(1,2,\cdots,N)}d_0^k=g^{\sum_{k\in(1,2,\cdots,N)}\alpha_k}$，$d_1=g^r$，$d_{i,j,1}=g^{r+\lambda_i t_{i,j}}$ 和 $d_{i,j,2}=g^{\lambda_i}\ (i\in(1,n),j\in(1,n_i))$ 。

(c) Delegate Query to $\mathrm{O_2}$：为DU请求一个$t_{\omega,s}$，若DU=DU*, B停止模拟返回猜测值u'；若DU≠DU*，B进行模拟，随机选择$v\in Z_p^*$，输出$t_{\omega,s}=\left(T_0,T_1,T_2,\forall \mathrm{att}_i\in L:\left\{d_{i,j,1}',d_{i,j,2}'\right\}_{i\in(1,n),j\in(1,n_i)}\right)$。其中，$T_0=g^{stv}$，$T_1=g^{\lambda_i v}$，$T_2={T_{i,j}}^v=g^{vt_{i,j}}$，$d_{i,j,1}'=g^{(r+\lambda_i t_{i,j})v}$ 和$d_{i,j,2}'=g^{\lambda_i vr}$ 。

(d)TrapGen Query to $\mathrm{O_3}$: A向B请求一个$t_{m,s}$，若DU=DU*，则B停止模拟返回猜测值u'；若DU≠DU*,B随机选择$\mu\in Z_p^*$，输出$t_{m,s}=(T_3,T_4,T_5)$。其中，$T_3=d_0^\mu$，$T_4=d_1^\mu$和$T_5=g^{\lambda_i\mu t_{i,j}}$。

(e) Challenge: A向B发送两个消息m_0, m_1，并请求由DU*生成授权信息，返回$t_{\omega,s}{}^*=\left(T_0,T_1,T_2,\forall \mathrm{att}_i\in L:\left\{d_{i,j,1}',d_{i,j,2}'\right\}_{i\in(1,n),j\in(1,n_i)}\right)$ 。其中，$T_0=T_\xi$, $T_1=g^{\lambda_i b}$, $T_2={T_{i,j}}^b=g^{bt_{i,j}}$, $d_{i,j,1}'=g^{(r+\lambda_i t_{i,j})b}$和$d_{i,j,2}'=g^{\lambda_i br}$。B随机抛硬币得到$\xi\in_R\{0,1\}$并设置$v=b$。

(f) Guess: A输出猜测u'，若$u=0$，则$T_\xi=g^{ab}$，表示生成的挑战授权信息$t_{\omega,s}{}^*$是一个由DU*生成的有效授权信息，A挑战成功，这种情况发生的概率为$1/2+\varepsilon$；若$u=1$，则$T_\xi\in G_1$，表示生成的挑战授权信息$t_{\omega,s}{}^*$是一个无效授权信息，这种情况发生的概率为1/2。

综上所述，A挑战成功赢得游戏的总体优势为$\varepsilon/2$。故本文方案满足陷门不可区分性。

4 性能分析

本小节将本文方案与文献[16,17]进行比较，从表1可以看出，本文方案无须中央授权机构，支持多属性授权机构分发用户私钥，满足用户私钥抗合谋性，保证用户私钥的安全性。具有更多的功能和更好的灵活性，如表1所示。

与文献[16]方案相比，二者均能实现细粒度访问的可搜索加密，但本文方案利用多属性授权机构能够抵御用户的合谋攻击。通过理论数值分析，本文方案降低了加解密的计算开销，具有较高的加解密运行效率。由于本文方案为了实现对所有密文信息进行搜索，在检测阶段利用多服务器增加了运算量。但是，在多服务器模型下对数据密文进行检测时，数据检测效率会随着参与检测的服务器数量的增加而提高。因此，本文方案在数据量较大的情况下，检索速率更快灵活性更高，如表2所示。

为证明上述理论分析的正确性，对本文方案与文献[16]方案的加密算法及解密算法进行仿真实验。实验环境为戴尔笔记本(I7-4700 CPU @ 3.20 GHz, 16 GB内存和Ubuntu Linux操作系统)。使用基于双线性对的密码函数库[18](Pairing-Based Cryptography, PBC)，并选用了160位阶的A类椭圆曲线。令系统中的属性值最多为30个，如图2所示，其中横轴为属性个数，纵轴为算法的执行时间。

表 1 不同方案功能对比

方案	支持细粒度访问	中央授权机构	属性授权机构	支持多服务器	支持授权服务器
文献[16]	是	有	单	否	否
文献[17]	否	无	无	是	否
本文方案	是	无	多	是	是

表 2 计算开销表

方案	加密运算量	陷门检测运算量	解密运算量
文献[16]	$3+P(2n+5)E+(3n+3)M$	$4P+6E+6M$	$(n+5)P+(3n+3)E+(5n+4)M$
本文方案	$+P+(2n+1)E+(2n+1)M$	①$3+P+(4n+2)E+(4n+2)M$②$4+P+(8n+4)E+(2n+3)M$	$2+P+(2n+5)E+(n+1)M$

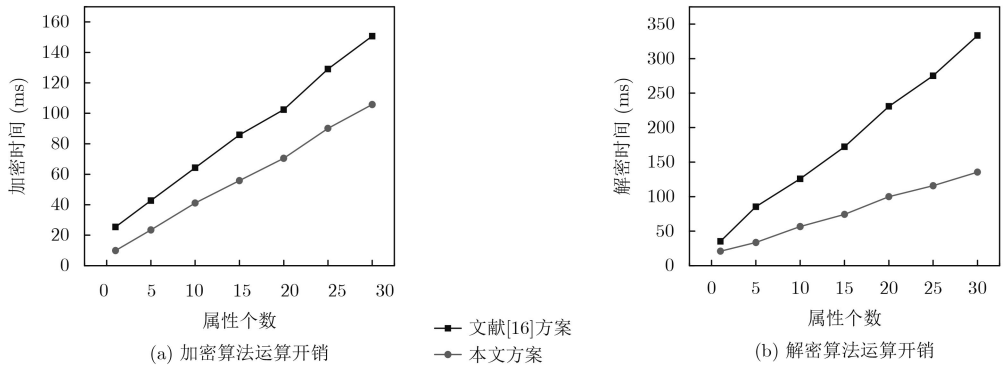

图 2 加密算法及解密算法运算开销

由图2可以看出，文献[16]和本文方案加密算法部分虽然都是线性增长，且增幅也大致相似，但本文方案时间消耗明显低于文献[16]方案。解密阶段本文方案无论在单位时间还是增幅各项都要优于文献[16]方案。降低了加解密的计算开销，具有较高的运行效率。通过仿真实验可得出，本文方案可以更好地适用于大规模的云环境数据存储系统中。

5　结束语

本文提出了一种基于授权的多服务器可搜索CP-ABE方案。在不需要对密文解密的情况下，通过云过滤服务器进行恶意信息检测，有效地保护数据用户的隐私。建立访问树结构，管理不同授权机构颁发的属性，抵抗多个属性授权机构的联合攻击，实现用户的细粒度访问。通过安全性分析，证明方案满足密文不可区分性和陷门不可区分性。

参 考 文 献

[1] BONEH D, DI CRESCENZO G, OSTROVSKY R, *et al*. Public key encryption with keyword search[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 506–522. doi: 10.1007/978-3-540-24676-3_30.

[2] 李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. 软件学报, 2015, 26(1): 109–128. doi: 10.13328/j.cnki.jos.004700.
LI Jingwei, JIA Chunfu, LIU Zheli, *et al*. Survey on the searchable encryption[J]. *Journal of Software*, 2015, 26(1): 109–128. doi: 10.13328/j.cnki.jos.004700.

[3] BAEK J, SAFAVI-NAINI R, and SUSILO W. On the integration of public key data encryption and public key encryption with keyword search[C]. The 9th International Conference on Information Security, Samos Island, Greece, 2006: 217–232. doi: 10.1007/11836810_16.

[4] BAEK J, SAFAVI-NAINI R, and SUSILO W. Public key encryption with keyword search revisited[C]. Computational Science and Its Applications – ICCSA 2008, Berlin, Heidelberg, 2008: 1249–1259. doi: 10.1007/978-3-540-69839-5_96.

[5] YANG Ce, ZHANG Weiming, XU Jun, *et al*. A fast privacy-preserving multi-keyword search scheme on cloud data[C]. 2012 International Conference on Cloud and Service Computing, Shanghai, China, 2012: 104–110. doi: 10.1109/CSC.2012.23.

[6] 王保民, 何智灵, 罗文俊. 基于云存储的多用户可搜索加密方案[J]. 信息网络安全, 2013(12): 33–36.
WANG Baomin, HE Zhiling, and LUO Wenjun. An efficient scheme of multi-user searchable encryption with keyword in cloud storage[J]. *Netinfo Security*, 2013(12): 33–36.

[7] 张楠, 陈兰香. 一种高效的支持排序的关键词可搜索加密系统研究[J]. 信息网络安全, 2017(2): 43–50. doi: 10.3969/j.issn.1671-1122.2017.02.007.
ZHANG Nan and CHEN Lanxiang. Research on an efficient ranked keywords searchable encryption system[J]. *Netinfo Security*, 2017(2): 43–50. doi: 10.3969/j.issn.1671-1122.2017.02.007.

[8] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[9] WANG Hao, ZHENG Zhihua, WU Lei, *et al*. New directly revocable attribute-based encryption scheme and its application in cloud storage environment[J]. *Cluster Computing*, 2017, 20(3): 2385–2392. doi: 10.1007/s10586-016-0701-7.

[10] 李双, 徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报, 2014, 37(5): 1017–1024.
LI Shuang and XU Maozhi. Attribute-based public encryption with keyword search[J]. *Chinese Journal of Computers*, 2014, 37(5): 1017–1024.

[11] ZHENG Qingji, XU Shouhuai, and ATENIESE G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data[C]. 2014 IEEE Conference on Computer Communications, Toronto, Canada, 2014: 522–530. doi:

10.1109/INFOCOM.2014.6847976.

[12] SUN Wenhai, YU Shucheng, LOU Wenjing, *et al*. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2016, 27(4): 1187–1198. doi: 10.1109/TPDS.2014.2355202.

[13] IBRAIMI L, NIKOVA S, HARTEL P, *et al*. Public-key encryption with delegated search[C]. The 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, 2011: 532–549. doi: 10.1007/978-3-642-21554-4_31.

[14] 林鹏, 江颉, 陈铁明. 云环境下关键词搜索加密算法研究[J]. 通信学报, 2015, 36(S1): 259–265.
LIN Peng, JIANG Jie, and CHEN Tieming. Application of keyword searchable encryption in cloud[J]. *Journal on Communications*, 2015, 36(S1): 259–265.

[15] 苏航, 朱智强, 孙磊. 移动云存储中基于属性的搜索加密方案研究[J]. 计算机应用研究, 2017, 34(12): 3753–3757, 3766. doi: 10.3969/j.issn.1001-3695.2017.12.053.
SU Hang, ZHU Zhiqiang, and SUN Lei. Research on searchable attribute based encryption in mobile cloud storage[J]. *Application Research of Computers*, 2017, 34(12): 3753–3757, 3766. doi: 10.3969/j.issn.1001-3695.2017.12.053.

[16] 伍祈应, 马建峰, 苗银宾, 等. 多数据拥有者认证的密文检索方案[J]. 通信学报, 2017, 38(11): 161–170.
WU Qiying, MA Jianfeng, Miao Yinbin, *et al*. Multi-owner accredited keyword search over encrypted data[J]. *Journal on Communications*, 2017, 38(11): 161–170.

[17] 黄海平, 杜建澎, 戴华, 等. 一种基于云存储的多服务器多关键词可搜索加密方案[J]. 电子与信息学报, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.
HUANG Haiping, DU Jianpeng, DAI Hua, *et al*. Multi-sever multi-keyword searchable encryption scheme based on cloud storage[J]. *Journal of Electronics & Information Technology*, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.

[18] PBC Library. The pairing-based cryptography library[EB/OL]. http://crypto.stanford.edu/pbc/, 2010.

张玉磊：男，1979年生，博士，副教授，研究方向为密码学与信息安全.

刘文静：女，1994年生，硕士生，研究方向为密码学与信息安全.

刘祥震：男，1994年生，硕士生，研究方向为密码学与信息安全.

张永洁：女，1978年生，硕士，副教授，研究方向为密码学与信息安全.

王彩芬：女，1963年生，博士，教授，博士生导师，研究方向为密码学与信息安全.