支持策略隐藏且密文长度恒定的可搜索加密方案

杨小东*① 李 婷① 麻婷春① 陈桂兰① 王彩芬①②

①(西北师范大学计算机科学与工程学院 兰州 730070)

②(深圳技术大学大数据与互联网学院 深圳 518118)

摘 要：属性加密体制是实现云存储中数据灵活访问控制的关键技术之一，但已有的属性加密方案存在密文存储开销过大和用户隐私泄露等问题，并且不能同时支持云端数据的公开审计。为了解决这些问题，该文提出一个新的可搜索属性加密方案，其安全性可归约到q-BDHE问题和CDH问题的困难性。该方案在支持关键词搜索的基础上，实现了密文长度恒定；引入策略隐藏思想，防止攻击者获取敏感信息，确保了用户的隐私性；通过数据公开审计机制，实现了云存储中数据的完整性验证。与已有的同类方案相比较，该方案有效地降低了数据的加密开销、关键词的搜索开销、密文的存储成本与解密开销，在云存储环境中具有较好的应用前景。

关键词：云存储；属性加密；密文长度恒定；关键词搜索；公开审计

中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2021)04-0900-08

DOI: 10.11999/JEIT200083

Searchable Encryption Scheme Supporting Policy Hiding and Constant Ciphertext Length

YANG Xiaodong① LI Ting① MA Tingchun① CHEN Guilan① WANG Caifen①②

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

②(*College of Big Data and Internet, Shenzhen Technology University, Shenzhen* 518118, *China*)

Abstract: The Attribute-Based Encryption (ABE) mechanism is one of the key technologies for implementing flexible access control of data in cloud storage. However, the existing ABE schemes have some problems, such as too much ciphertext storage overhead and user privacy leakage, and unsupported public auditing of cloud data. To solve these problems, a new searchable ABE scheme is proposed, and its security can be reduced to the difficulty of q-BDHE (q –decisional Bilinear Diffie-Hellman Exponent) problem and CDH (Computational Diffie-Hellman) problem. The proposed scheme achieves a constant ciphertext length on the basis of supporting keyword search. By introducing strategies to hide ideas, it prevents attackers from obtaining sensitive information and ensures the privacy of users. And the integrity of the data in cloud storage is verified through data public audit mechanism. Compared with the existing similar schemes, this scheme greatly reduces the data encryption overhead, keyword search overhead, ciphertext storage cost and decryption cost, which has a good application prospect to the cloud storage environment.

Key words: Cloud storage; Attribute-Based Encryption (ABE); Constant ciphertext length; Keyword search; Public audit

收稿日期：2020-01-20；改回日期：2021-10-21；网络出版：2020-11-16

*通信作者： 杨小东 y200888@163.com

基金项目：国家自然科学基金(61662069, 61562077)，中国博士后科学基金(2017M610817)，兰州市科技计划项目(2013-4-22)，西北师范大学青年教师科研能力提升计划(NWNU-LKQN-14-7)

Foundation Items: The National Natural Science Foundation of China (61662069, 61562077), The Postdoctoral Science Foundation of China (2017M610817), The Science and Technology Project of Lanzhou City (2013-4-22), The Foundation of Northwest Normal University (NWNU-LKQN-14-7)

1　引言

云存储具有较高的存储效率和较低的存储成本，给个人和企业提供了便利的存储服务[1]。然而，云存储安全策略还未形成标准、规范的体系结构，导致云端数据面临隐私泄露、数据损坏等安全问题[2]。基于密文策略的属性加密方案(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)[3]确保了云端数据的机密性和完整性，并且支持灵活、细粒度的访问控制，提高了云端数据的安全性。为了保护用户隐私，节省密文存储开销，国内外学者从策略隐藏、密文长度恒定等方面对CP-ABE方案进行了研究和拓展。

传统的CP-ABE方案[4,5]通常以明文的形式公布访问策略，任何获得密文的人(包括云服务提供商)都可以推断出密文的部分秘密信息，导致解密用户面临私密信息泄露的风险。为解决此问题，文献[6,7]提出了带有部分隐藏策略的CP-ABE方案，隐藏访问策略中的属性值以保护私密信息，但面临离线字典攻击的安全问题。文献[8,9]将属性分为属性名和属性值两部分，采用隐藏属性值的思想设计了支持部分策略隐藏的CP-ABE方案。尽管这些方案在某种程度上能够保护策略隐私，但存在部分属性信息泄露的问题。针对使用部分隐藏策略的CP-ABE方案引起的安全性和隐私问题，一系列可完全隐藏访问策略的CP-ABE方案[10–13]相继被提出，确保了数据的完整性和私密性。但文献[10–13]使用隐藏的访问策略加密数据，使得解密者需要执行若干配对操作来解密密文，存在计算开销较大的问题。此外，上述方案均没有考虑密文长度这一重要技术指标，都存在密文长度随属性个数正向增长的问题。

为了降低密文存储开销，Emura等人[14]提出了一种密文长度恒定的CP-ABE方案，但该方案的访问结构单一。Herranz等人[15]采用多项式重构的思想，构造了一种密文长度恒定的CP-ABE方案；Ge等人[16]提出了选择明文攻击下可证安全且密文长度恒定的CP-ABE方案。然而，文献[15,16]加密和解密涉及的配对运算较多，存在计算开销大的问题。Zhang等人[17]基于多值通配符的AND门访问策略，提出了一种密文长度恒定的CP-ABE方案，有效地提升了计算效率，但安全性较低。文献[18–21]构造了一种策略隐藏且密文长度恒定的属性加密方案，确保了用户隐私信息的安全，并且节省了密文存储开销。然而，随着云存储中加密文件数量的增多，已有的同类方案[22,23]未能同时支持云端数据的公开审计、关键词搜索，这已成为云存储中一个重要且具有挑战性的问题。

针对上述问题，本文设计了一种支持策略隐藏且密文长度恒定的可搜索属性加密方案。该方案基于可搜索加密机制，实现了密文长度的恒定。将访问策略隐藏在密文和关键词中，确保了数据的隐私性。采用数据公开审计的思想，实现了云端数据的完整性验证。相比于现有的同类方案，本文方案不仅从加密、解密和搜索3方面提升了计算效率，而且大大降低了云端数据的存储成本。通过对相关领域的文献搜索，本文方案是第1个同时具备策略隐藏、密文长度恒定、关键词搜索和公开审计的属性加密方案。

2　预备知识

2.1　双线性映射

设G_1和G_T分别是两个阶为素数p的乘法循环群，其中g为G_1的一个生成元，$e:G_1\times G_1\to G_T$是满足以下条件的双线性映射[24]。

(1) 双线性：对于任意的$a,b\in Z_p^*$，有$e(g^a,g^b)=e(g,g)^{ab}$；

(2) 非退化性：$e(g,g)\neq 1$；

(3) 可计算性：对于群G_1中的任意两个元素g_1,g_2，存在一个有效算法计算$e(g_1,g_2)$。

2.2　决策性q-BDHE假设

决策性q-BDHE(q –Decisional Bilinear Diffie-Hellman Exponent)问题：假设T为群G_T中的一个随机数，给定$y_{g,\alpha,q}=(g_1,g_2,\cdots,g_q,g_{q+1},\cdots,g_{2q},g^r)$，其中$\alpha,r\in Z_P^*$，$g_i=g^{\alpha^i}$，区分$(g,y_{g,\alpha,q},e(g_{q+1},g^r))$和$(g,y_{g,\alpha,q},T)$。

定义1　决策性q-BDHE假设。如果攻击者在多项式时间内无法以不可忽略的优势区分元组$(g,y_{g,\alpha,q},e(g_{q+1},g^r))$和$(g,y_{g,\alpha,q},T)$，则表明$G_1$和$G_T$上的$q$-BDHE问题是困难的[20]。

2.3　CDH假设

CDH(Computational Diffie-Hellman)问题：给定$(g,g^x,g^y)\in G_1^3$，其中$x,y\in Z_P^*$是未知的，计算$g^{xy}\in G_1$。

定义2　CDH假设。如果攻击者在多项式时间内无法以不可忽略的优势计算出g^{xy}，则表明G_1上的CDH问题是困难的[25]。

3　支持策略隐藏且密文长度恒定的可搜索属性加密方案

3.1　系统模型

本文方案的系统模型如图1所示，包含数据拥有者(Data Owner, DO)、云服务提供商(Cloud Service Provider, CSP)、属性权威中心(Attribute Authority Center, AAC)、访问用户(Accessing

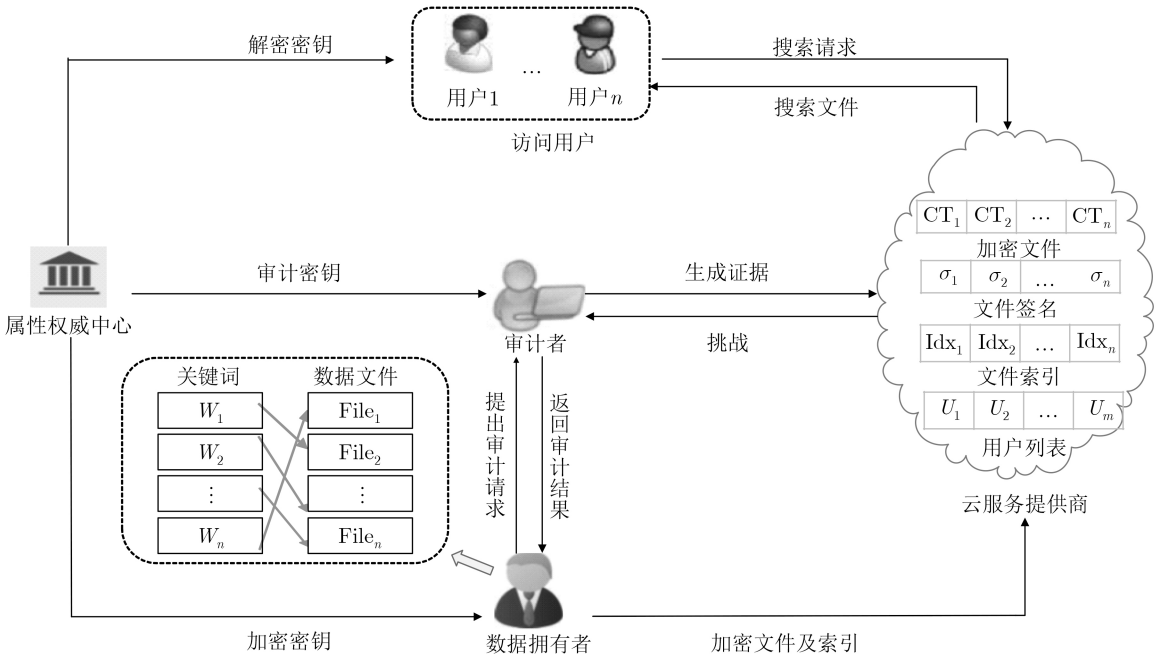


图 1 系统模型

Users, AU)和第三方审计者(Third-Party Auditors, TPA)5个实体。各实体的功能介绍如下：

(1) DO：根据数据文件和关键词生成对应的关键词索引，并将数据文件和索引加密后上传至CSP。

(2) CSP：存储数据拥有者上传的密文数据，并处理访问用户的搜索请求。

(3) AAC：负责生成系统公共参数和系统中各个实体的私钥。

(4) AU：向云服务提供商发送密文的搜索请求，并解密云服务提供商返回的密文数据文件。

(5) TPA：负责验证云端数据的完整性，并将审计结果返回给数据拥有者。

3.2 具体方案

(1) 系统建立(Setup(k))：输入安全参数k，令G_1和G_T为阶为素数p的乘法循环群，g为G_1的生成元，$e:G_1\times G_1\to G_T$是一个双线性映射。假定$U=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\}$为系统属性集，$S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,j}\}$表示属性$\mathrm{att}_i$的取值集合。AAC按照如下步骤生成系统参数PP和主密钥msk。

(a) 选择哈希函数$H_0:Z_p^*\times\{0,1\}^{\log_2 n}\times\{0,1\}^{\log_2 m}\to Z_p^*$, $H_1:\{0,1\}^*\to G_1$, $H_3:Z_p\to G_1$和一个带密钥的哈希函数$H_k:\{0,1\}^*\to Z_p$。随机选取$a,b,c\in Z_p$，计算$\phi=e(g,g)^a$,$\gamma=g^b$ 和$\mathrm{pk}=g^c$ 。

(b) 对任意属性$\mathrm{att_i}\,(\mathrm{att}\in U)$，随机选取$x_{i,j}\in Z_p$，计算$a_{i,j}=H_0(a||x_{i,j})$, $A_{i,j}=g^{-a_{i,j}}$和$Y_{i,j}=e(g,g)^{a_{i,j}}$，其中$i,j\in(1,2,\cdots,n)$，“||”表示连接符。

(c) 公开系统参数$\mathrm{PP}=\Big(G_1,G_T,e,p,g,\phi,\gamma,\mathrm{pk},H_0,H_1,H_2,H_3,\{A_{i,j},Y_{i,j}\}_{1\le i\le n,1\le j\le n_i}\Big)$，秘密保存主密钥$\mathrm{msk}=(a,b,a_{i,j})$。

(2) 密钥生成(KeyGen): AAC收到用户发送的属性列表$L=\{L_1,L_2,\cdots,L_u\}$后，按照以下步骤生成L对应的私钥。

(a) 随机选取$\mathrm{sk},\alpha,\beta\in Z_p$，计算$\tau_i=(g\cdot H_3(\mathrm{sk}))^{-a_{i,j}}$, $X=\phi^{\alpha}$和$K=g^{(a+\beta)/b}$。对任意属性att_i, AAC随机选择$\lambda_i\in Z_p$，计算$\mathrm{sk}_{i,1}=g^{\beta-\lambda_i||a_{i,j}}$，得到私钥$\mathrm{SK}_L$，即$\mathrm{SK}_L=\Big(\mathrm{sk},K,\{\tau_i,\mathrm{sk}_{i,1}\}_{1\le i\le n}\Big)$。

(b) 随机选取$\mathrm{ssk}_F\in Z_p$作为任意数据文件块$F(1\le F\le m)$的签名私钥，通过安全信道将ssk_F发送给用户。计算$\mathrm{pk}=g^{\mathrm{ssk}_F}$，并将pk作为公钥。

(3) 数据文件加密(Encrypt): DO在访问策略W下对数据文件M执行如下的加密操作。

(a) 计算$A_\omega=\prod_{v_{i,j}\in W}A_{i,j}$和$Y_\omega=\prod_{v_{i,j}\in W}Y_{i,j}$。随机选取$r\in Z_p$，计算$C_1=g^r$, $C_2={A_\omega}^r$及$C_3=M\cdot {Y_\omega}^r$。

(b) 将密文数据CT划分为m块，即$\mathrm{CT}=(\mathrm{CT}_1,\mathrm{CT}_2,\cdots,\mathrm{CT}_m)$。

(c) 为每个密文数据块CT_j计算标签$\delta_j=(H_2(j)g^{\mathrm{CT_j}})^{\mathrm{ssk}_F}$。

(d) 输出文件M的密文$C_T=(C_1,C_2,C_3)$和相应的标签δ_j，将其发送给CSP。

(4) 关键词索引生成(Encind)：DO首先创建数据文件M的关键词集合$\mathrm{kw}=\{\mathrm{kw}_1,\mathrm{kw}_2,\cdots,\mathrm{kw}_n\}$，然后基于访问策略$W$计算$\hat{C}=\phi^r$, $I=\gamma^{r/H_k(\mathrm{kw}_i)}$和$U=X^{-r}$，最后将关键词索引$\mathrm{WI}=\Big(\hat{C},I,U\Big)$发送给CSP。

(5) 陷门生成(Trapdoor): AU随机选取$s \in Z_p$，计算$\hat{T}=\alpha+s$，$T_0=K^{H_k(\mathrm{kw}_i)s}$，$T_{i,1}=\mathrm{sk}_{i,1}{}^s$和$T_{i,2}=\mathrm{sk}_{i,2}{}^s$，其中$i \in \{1,2,\cdots,n\}$。将身份标识符$\mathrm{ID}_i$和陷门$T=\left(\hat{T},T_0,T_{i,1},T_{i,1}\right)$发送给CSP。

(6)搜索(Search)：CSP收到身份标识符和陷门后，验证该用户是否在用户列表L_u中。如果该用户不在列表L_u或该用户的属性集不满足访问控制策略W，终止搜索；否则，按照如下步骤搜索文件。

(a) 计算$T_1=\prod_{i=1}^{n}T_{i,1}$, $T_2=\prod_{i=2}^{n}T_{i,2}$, $E_1=e(C_1,T_1)$和$E_2=e(C_2,T_2)$。

(b) 验证$e(I,T_0)\cdot E=\hat{C}^{\hat{T}}\cdot U$是否成立，其中$E=E_2/E_1$。如果等式成立，云服务器向访问用户发送相应的数据搜索文件；否则，返回$\perp$。

(7) 解密(Decrypt)：访问用户得到密文$C_T=(C_1,C_2,C_3)$后，计算$\prod_{v_{i,j}\in W}\tau_i$恢复出数据文件$M=\dfrac{C_3}{e(\tau_\omega,C_1)e(H_3(\mathrm{sk}),C_2)}$。

(8) 审计(Audit): TPA收到DO对文件CT_F做出的验证请求后，随机选择d个数，生成数据的索引集合$I=\{\mathrm{CT}_1,\mathrm{CT}_2,\cdots,\mathrm{CT}_d\}$。对任意$j \in I$，随机选取$\rho_j \in Z_p$，生成挑战信息$\mathrm{chal}=(j,\rho_j)_{j\in I}$，并向CSP发送挑战信息chal及文件标签$\delta_j$。TPA和CSP进行交互，按照以下两个步骤对云端数据文件进行审计。

(a) 证据生成(ProofGen): CSP收到TPA的审计请求后，计算聚合证据$\delta=\prod_{j\in I}\delta_j{}^{\rho_j}$和聚合密文$\theta=\prod_{(j,\rho_j)\in I}C_j\rho_j$，并将证明信息$P=(\delta,\theta)$发送给TPA。

(b) 证据验证(VerifyProof): TPA收到证明信息后，验证$e(\delta,g)=e\left(\prod_{(j,\rho_j)\in I}H_2(j)^{\rho_j}\cdot g^{\theta},\mathrm{pk}\right)$是否成立。如果等式成立，则表明存储在云端的密文数据块CT_j完整；否则，意味着数据块CT_j损坏，并将验证结果反馈给DO。

4　安全性分析

4.1 机密性

定理1　如果q-BDHE假设成立，则没有任何多项式敌手$\mathcal{A}$能够以不可忽略的优势攻破本文方案。

证明：假设在多项式时间t内，存在一个敌手$\mathcal{A}$以不可忽略的优势ε_A攻破本文方案，则可以构建一个挑战者$\mathcal{B}$以不可忽略的优势ε_B解决q-BDHE问题。给定q-BDHE挑战元组$(g,y_{g,\alpha,q},T)$，其中$y_{g,\alpha.q}=(g_1,g_2,\cdots,g_q,g_{q+1},\cdots,g_{2q},g^s)$, $T \in G_T$, $\mathcal{B}$和$\mathcal{A}$进行如下的模拟游戏。

系统建立：$\mathcal{A}$向$\mathcal{B}$发送一个访问策略$W^*=\{W_1,W_2,\cdots,W_n\}=\Lambda_{i\in I_{W^*}}W_i$，其中$I_{W^*}=\{1,2,\cdots,n\}$表示$W^*$中属性的索引。$\mathcal{B}$随机选择$i^* \in I_{W^*}$, $a,a' \in \mathrm{Z}_P$以及$x_{i,j} \in \mathrm{Z}_P$，计算$A_{i^*\ j}$和$Y_{i^*,j}$，将产生的系统公共参数$\mathrm{PP}=\left(G_1,G_T,e,p,g,\phi,\gamma,pk,H_0,H_1,H_2,H_3,(A_{i,j},Y_{i,j})_{1\le i\le n,1\le j\le n_i}\right)$发送给$\mathcal{A}$。

询问阶段1：$\mathcal{A}$可以自适应性地向$\mathcal{B}$进行以下两类哈希询问。

(1) $O_{H_0}(a_{i,j})$询问：$\mathcal{A}$输入属性att_i向$\mathcal{B}$发起H_0询问，$\mathcal{B}$维护初始列表$L_0=[\mathrm{att}_i,a,a_{i,j}]$，先在列表$L_0$中查询$\mathrm{att}_i$是否存在，如果存在，将对应的值返回给$\mathcal{A}$；否则，随机选择$x_{i',j} \in Z_P$，令$a_{i',j}=H_0(a||x_{i',j})$，其中$a \in Z_P$。然后，在列表$L_0$中添加$(\mathrm{att}_i,a,a_{i',j})$，并将$a_{i',j}$返回给$\mathcal{A}$。

(2) $O_{H_3}(\mathrm{sk})$询问：$\mathcal{A}$输入属性att_i进行私钥询问，$\mathcal{B}$收到询问请求后，先查询sk是否存在于列表L_3。如果列表L_3中已经记录此值，则$\mathcal{B}$将此值返回给$\mathcal{A}$；否则，随机选择$\mu \in Z_p$，将$(\mathrm{sk},g_l g^{\mu})$添加至列表$L_3$并返回$g_l g^{\mu}$，其中$l$表示$L_3$的索引值。

(3) 密钥询问：$\mathcal{A}$输入ID_i及属性集合$L=\{L_1,L_2,\cdots,L_u\}$向$\mathcal{B}$进行密钥询问。为不失一般性，假设一定存在属性$\mathrm{att}_{i'} \in L$，且$v_{i',j} \ne W_{i'}$。当$i \ne l$时，$\mathcal{B}$随机选取$\mu \in Z_p$，计算$\tau_i=g_i{}^{H_0(a||x_{i,j})}\cdot g^{H_0(a||x_{i,j})}g_{q+1-i+i'}(A_{i,t_i})^{-\mu}$，并返回给$\mathcal{A}$。

挑战阶段：$\mathcal{A}$向$\mathcal{B}$发送明文消息M_0和M_1(M_0和M_1等长)，$\mathcal{B}$计算$a_{W^*}=\sum_{i=1}^{n}\sum_{j=1}^{j=n_i}a_{i,j}$，通过抛硬币游戏选择$\xi \in \{0,1\}$，计算得到密文$\mathrm{CT}'=\left(C_1',C_2',C_3'\right)$，其中$C_1'=g^r=h$，$C_2'=\left(\prod_{v_{i,j}\in W}g^{-a_{i,j}}\right)^r=\left(g^{-a_{i^*,j}}\prod_{i\in I_W-\{i^*\}}g_{q+1-i}\prod_{i\in I_W-\{i^*\}}g^{a_{i,j}}g_{q+1-i}^{-1}\right)^r=h^{-a_{W^*}}$；当$T=e(g_{q+1},h)$时，密文$\mathrm{CT}'=\left(C_1',C_2',C_3'\right)$是明文$M_\xi$的合法密文；否则，$\mathrm{CT}'$是随机密文。

询问阶段2：重复询问阶段1的工作，但不能继续询问明文消息M_0和M_1。

猜测阶段：$\mathcal{A}$输出对M_ξ的猜测结果$\xi' \in \{0,1\}$。如果$\xi=\xi'$, $\mathcal{B}$输出1，表示猜测结果为$T=e(g_{q+1},g^r)$。$\mathcal{A}$猜中$n_a|G_1|+|Z_P|$的概率为$\varepsilon_A=\Pr[\xi'=\xi|T=e(g_{q+1},g^r)]=\dfrac{1}{2}+\varepsilon$。如果$\xi' \ne \xi$, $\mathcal{B}$输出0，意味着T为一个随机值，$\mathcal{A}$猜中ξ'的概率为$\varepsilon_A=\Pr[\xi'=\xi|T \in G_T]=\dfrac{1}{2}$。则$\mathcal{B}$解决$q$-DBHE问题的概率为$\varepsilon_B=\dfrac{1}{2}\Pr[\xi'=\xi|T=e(g_{q+1},g^r)]+\dfrac{1}{2}\Pr[\xi'=\xi|T \in G_T]-\dfrac{1}{2}=\dfrac{\varepsilon}{2}$。

因此，如果$\mathcal{A}$以不可忽略的优势$\dfrac{1}{2}+\varepsilon$攻破本文

方案的机密性，那么$\mathcal{B}$能以$\frac{\varepsilon}{2}$的概率解决q-BDHE问题。 证毕

4.2 索引的不可区分性

定理2 如果CDH假设成立，则本文提出的方案满足索引不可区分性。

证明：假设在多项式时间t内，存在一个敌手$\mathcal{F}$能够以不可忽略的优势ε_F攻破本文方案，则存在一个挑战者$\mathcal{C}$能够以不可忽略的优势ε_C解决CDH问题。给定CDH问题元组(g, g^a, g^b), $\mathcal{F}$与$\mathcal{C}$的模拟游戏如下。

系统建立：$\mathcal{F}$向$\mathcal{C}$发送要挑战的访问策略$W^*=\{W_1, W_2, \cdots, W_n\}=\Lambda_{i\in I_{W^*}} W_i$, $\mathcal{C}$生成公共参数PP并发送给$\mathcal{F}$，其中$\mathrm{PP}=\left(G_1, G_T, e, p, g, \phi, \gamma, pk, H_0, H_1, H_2, H_3, (A_{i,j}, Y_{i,j})_{1\le i\le n, 1\le j\le n_i}\right)$。

询问阶段1：$\mathcal{F}$选择属性集合$L=\{L_1, L_2, \cdots, L_u\}$发送给$\mathcal{C}$，向$\mathcal{C}$发起如下的哈希询问和陷门询问。

(1) $O_{H_0}(a_{i,j})$询问：$\mathcal{C}$输入属性att_i向$\mathcal{F}$发起H_0询问，$\mathcal{C}$维护初始列表$L_{H_0}=[\mathrm{att}_i, a, a_{i,j}]$，先在列表$L_{H_0}$中查询$\mathrm{att}_i$是否存在，如果存在，则将对应值返回给$\mathcal{C}$；否则，为属性$\mathrm{att}_i$随机选择$x_{i',j}\in Z_P$，令$a_{i',j}=H_0(a||x_{i',j})$，其中$a\in Z_P$，并在列表$L_{H_0}$中添加$(\mathrm{att}_i, a, a_{i',j})$，将$a_{i',j}$返回给$\mathcal{F}$。

(2) $O_{H_3}(\mathrm{sk})$询问：$\mathcal{F}$输入属性att_i向$\mathcal{C}$发起H_3询问，$\mathcal{C}$维护初始列表$L_{H_3}=[\mathrm{att}_i, a_{i,j}, \mathrm{sk}, \tau_i]$，先查询sk是否存在于列表$L_3$。如果存在，则$\mathcal{C}$将对应值返回给$\mathcal{F}$；否则，$\mathcal{C}$随机选取$\mathrm{sk}'\in Z_P$，对于每个属性$\mathrm{att}_i$，随机选择$x_{i',j}\in Z_P$，计算$\tau_i=(g\cdot H_3(\mathrm{sk}'))^{-a_{i',j}}$，将其添加至列表$L_{H_3}$并发送给$\mathcal{F}$。

(3) 陷门查询：$\mathcal{F}$向$\mathcal{C}$发送属性列表L和关键词集合$\mathrm{kw}=\{\mathrm{kw}_1, \mathrm{kw}_2, \cdots, \mathrm{kw}_n\}$，如果属性集合$L$满足访问控制结构$W^*$, $\mathcal{C}$不响应此次询问。否则，$\mathcal{C}$随机选择$s\in Z_p$，计算$\hat{T}=\mathrm{sk}+s$, $T_0=K^{H_k(W_i)s}$, $T_{i,1}=\mathrm{sk}_{i,1}{}^s$和$T_{i,2}=\mathrm{sk}_{i,2}{}^s$，向敌手发送陷门$\mathrm{Trap}=(\hat{T}, T_0, T_{i,1}, T_{i,2})$，更新关键词列表$L_W=L_W\cup\mathrm{kw}$。

挑战阶段：$\mathcal{C}$向$\mathcal{F}$发送要挑战的关键词集合kw_1和kw_2，挑战者通过投掷硬币的游戏选择$\xi\in\{0,1\}$，记作关键词kw_ξ。随机选取$r'\in Z_p$，计算$\hat{C}=\phi^{r'}$，$I=\gamma^{r'/H_k(\mathrm{kw}_{i'})}$和$U=X^{-r'}$，并将计算得出的关键词索引$\mathrm{WI}=\left(\hat{C}, I, U\right)$发送给$\mathcal{F}$。

询问阶段2：重复询问阶段1，但$\mathcal{F}$不能继续询问关键词集合kw_1和kw_2或者kw_1和kw_2的子集。

猜测阶段：$\mathcal{F}$输出对kw_ξ的猜测结果$\mathrm{kw}_{\xi'}$，其中$\xi'\in\{0,1\}$。如果$\xi'=\xi$, $\mathcal{C}$输出1，意味着$T=g^{ab}$，敌手猜测成功。$\mathcal{F}$猜中正确ξ'的概率为：$\varepsilon_A=\Pr[\xi'=\xi|T=e(g_{q+1}, g^r)]=\varepsilon+\frac{1}{2}$。如果$\xi'\neq\xi$, $\mathcal{C}$输出0，意味着T为群G_1的一个随机值，猜测失败。$\mathcal{F}$猜错ξ'的概率为：$\varepsilon_A=\Pr[\xi'=\xi|T\in G_T]=1/2$。

根据上述推理得出$\varepsilon_B=\frac{1}{2}\Pr[\xi'=\xi|T=g^{ab}]+\frac{1}{2}\Pr[\xi'=\xi|T\in G_1]-\frac{1}{2}=\frac{\varepsilon}{2}$。因此，在多项式时间$t$内，如果敌手$\mathcal{F}$能以$\frac{1}{2}$的优势攻破该方案，则挑战者$\mathcal{C}$能够以不可忽略的优势$\frac{\varepsilon}{2}$解决CDH问题。 证毕

5 性能分析

5.1 理论分析

本节从计算开销和存储开销两个方面将本文方案与支持关键词搜索的属性加密方案[20,26,27]进行比较。为便于表述，用n_a表示系统中属性总个数，n_ω表示包含在访问控制策略中的属性个数，n_d表示解密时所需要的属性个数，n_s表示搜索时所需属性个数，n_k表示密钥中的属性个数，$|G_1|$和$|G_T|$分别表示群G_1和G_T中的元素长度，$|Z_p|$表示Z_p中元素长度，指数运算和对数运算分别用T_e和T_p表示。

5.1.1 计算成本

在表1中，文献[20]的解密开销，文献[26]的加密开销、关键词搜索开销以及文献[27]的加密开销、解密开销和关键词搜索开销均与属性个数呈线性增长关系。本文方案具有密文长度恒定，加密开销、解密开销和关键词搜索开销均与属性个数无关，具有较小的计算量。因此，本文方案具有更高的计算效率。

5.1.2 存储成本

在属性加密方案中，属性权威中心承担主密钥的存储开销，数据拥有者和访问用户分别用来存储公钥和私钥，云服务提供商的存储开销主要源于密文。由表2可知，本文方案与文献[20,26,27]的属性权威中心、数据拥有者和访问用户的存储开销相

表 1 计算开销对比

方案	加密开销	解密开销	关键词搜索开销
文献[20]	$3T_E$	$(n_d+2)T_P+n_dT_E$	/
文献[26]	$(n_\omega+6)T_E$	/	$(2n_s+1)T_P+T_E$
文献[27]	$(3n_\omega+4)T_E$	$T_P+n_dT_E$	$(2n_s+1)T_P+n_sT_E$
本文方案	$3T_E$	$2T_P$	$3T_P+T_E$

当。文献[26,27]密文存储开销与访问策略中的属性个数呈正相关关系，未实现密文长度恒定。虽然文献[20]方案的密文长度恒定，但该方案将密文分为密文头和中间密文两部分，存储开销高于本文方案。因此，本文方案具有较低的存储开销。

5.2 实验仿真分析

以Intel(R) Core(TM) i5-2400 @ 3.10 GHz的处理器、4 GB的内存、Windows10 X64专业版的操作系统以及jpbc-2.0.0密码库为实验环境，将本文方案与已有的支持关键词搜索的属性加密方案[26,27]进行搜索开销、加密开销和解密开销比较。在相同设备条件下进行多次实验，得到图2比较结果。

图2(a)表明，在数据文件搜索阶段，文献[26,27]的搜索时间与访问策略中属性个数呈正相关关系。由于本文方案实现了关键词索引的长度恒定，所以搜索时间不会随属性个数的增加而线性增长，始终保持在0.023 s左右。因此，本文方案具有较高的搜索效率。

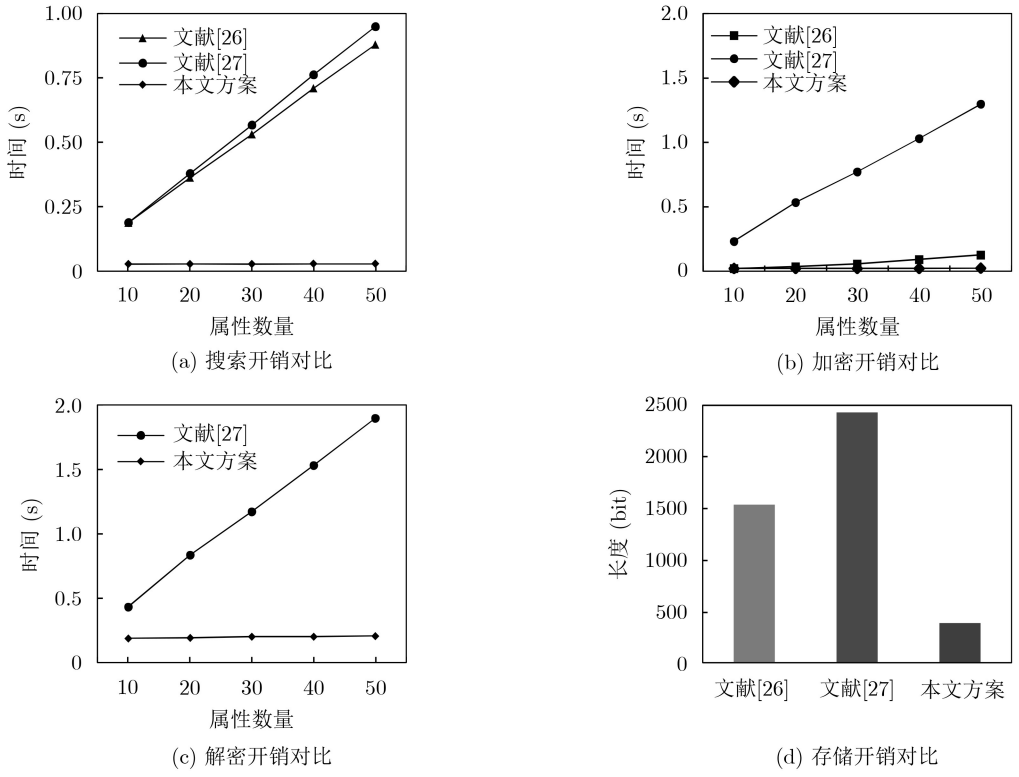
由图2(b)所示，当属性数量为10～30时，文献[26]和本文方案加密时间接近。随着属性数量的增加，文献[26]花费的加密时间缓慢增长；而本文方案的密文长度恒定，加密时间和属性数量无关，加密时间始终保持在0.02 s左右；文献[27]的加密开销一直高于本文方案。综上所述，本文方案具有较低的加密开销。

由图2(c)可知，访问策略中的属性数量为10时，本文方案与文献[27]的解密开销相当。但随着属性数量的增加，文献[27]的解密时间增幅较大，和属性数量呈正相关关系。本文方案中采用密文长度恒定技术，解密时间保持在0.2 s左右。因此，用户需要负担较小的解密花费。

如图2(d)所示，假设属性数量为5，本文方案与同类方案[26,27]在存储开销上相比具有明显优势。影响存储开销最关键的因素是密文的大小，所以图2显示了本文方案与文献[26,27]的密文尺寸，文献[26]和文献[27]密文大小分别为1536 bit和2432 bit，而

表 2　存储开销对比

方案	属性权威中心	数据拥有者	访问用户	云服务提供商
文献[20]	$2\|Z_P\|$	$(2n_a+1)\|G_1\|$	$n_k\|G_1\|+\|Z_p\|$	$3\|G_1\|+\|G_T\|$
文献[26]	$(n_\omega+2)\|Z_P\|$	$(n_a+1)\|G_1\|$	$(2n_k+1)\|G_1\|+\|Z_P\|$	$(2n_\omega+1)\|G_1\|+\|G_T\|$
文献[27]	$\|G_1\|+\|Z_P\|$	$n_a\|G_1\|+\|Z_P\|$	$(n_k+1)\|G_1\|+\|G_T\|$	$(n_\omega+2)\|G_1\|+\|G_T\|$
本文方案	$(n_\omega+2)\|Z_P\|$	$n_a\|G_1\|+n_a\|G_T\|$	$n_k\|G_1\|+\|G_T\|$	$2\|G_1\|+\|G_T\|$



(a) 搜索开销对比　(b) 加密开销对比

(c) 解密开销对比　(d) 存储开销对比

图 2 计算和存储开销对比

本文方案密文长度恒定，仅需要花费384 bit来存储密文。

6 结束语

针对现有方案面临的存储开销随属性数量正向增长、用户隐私泄露及数据可用性较低等安全性问题，本文面向云存储提出一种支持策略隐藏且密文长度恒定的可搜索属性加密方案。该方案在支持关键词搜索的前提下，实现了密文长度恒定，降低了云服务提供商的存储开销。通过对密文数据和关键词中的访问策略进行隐藏，提高了数据安全性。引入公开审计功能，确保了数据的完整性。分析结果表明：该方案在实现数据隐私性和完整性的同时，降低了云服务提供商的存储成本，提高了计算性能，在云存储环境中具有更好的应用性。然而，该方案仅满足CPA安全，下一步将对满足选择密文安全的属性加密方案进行探究。

参 考 文 献

[1] ZHANG Jindan, WANG Baocang, HE Debiao, *et al*. Improved secure fuzzy auditing protocol for cloud data storage[J]. *Soft Computing*, 2019, 23(10): 3411–3422. doi: 10.1007/s00500-017-3000-1.

[2] ZHANG Yinghui, YANG Menglei, ZHENG Dong, *et al*. Efficient and secure big data storage system with leakage resilience in cloud computing[J]. *Soft Computing*, 2018, 22(23): 7763–7772. doi: 10.1007/s00500-018-3435-z.

[3] BETHENCOURT J, SAHAI A, and WATERS B. Ciphertext-policy attribute-based encryption[C]. The 2007 IEEE Symposium on Security and Privacy, Berkeley, USA, 2007: 321–334. doi: 10.1109/SP.2007.11.

[4] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]. The 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography, Taormina, Italy, 2011: 53–70. doi: 10.1007/978-3-642-19379-8_4.

[5] ROUSELAKIS Y and WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]. The 2013 ACM SIGSAC Conference on Computer & Communications Security, New York, USA, 2013: 463–474. doi: 10.1145/2508859.2516672.

[6] CHEUNG L and NEWPORT C. Provably secure ciphertext policy abe[C]. The 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 2007: 456–465. doi: 10.1145/1315245.1315302.

[7] LAI Junzuo, DENG R H, and LI Yingjiu. Expressive CP-ABE with partially hidden access structures[C]. The 7th ACM Symposium on Information, Computer and Communications Security, New York, USA, 2012: 18–19. doi: 10.1145/2414456.2414465.

[8] NISHIDE T, YONEYAMA K, and OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]. The 6th International Conference on Applied Cryptography and Network Security, New York, USA, 2008: 111–129. doi: 10.1007/978-3-540-68914-0_7.

[9] 应作斌, 马建峰, 崔江涛. 支持动态策略更新的半策略隐藏属性加密方案[J]. 通信学报, 2015, 36(12): 178–189. doi: 10.11959/j.issn.1000-436x.2015327.
YING Zuobin, MA Jianfeng, and CUI Jiangtao. Partially policy hidden CP-ABE supporting dynamic policy updating[J]. *Journal on Communications*, 2015, 36(12): 178–189. doi: 10.11959/j.issn.1000-436x.2015327.

[10] PHUONG T V X, YANG Guomin, and SUSILO W. Hidden ciphertext policy attribute-based encryption under standard assumptions[J]. *IEEE transactions on Information Forensics and Security*, 2016, 11(1): 35–45. doi: 10.1109/TIFS.2015.2475723.

[11] XU Runhua and LANG Bo. A CP-ABE scheme with hidden policy and its application in cloud computing[J]. *International Journal of Cloud Computing*, 2015, 4(4): 279–298. doi: 10.1504/IJCC.2015.074224.

[12] ZHOU Zhibin, HUANG Dijiang, and WANG Zhijie. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. *IEEE Transactions on Computers*, 2015, 64(1): 126–138. doi: 10.1109/TC.2013.200.

[13] LAI Junzuo, DENG R H, and LI Yingjiu. Fully secure cipertext-policy hiding CP-ABE[C]. The 7th International Conference on Information Security Practice and Experience, Guangzhou, China, 2011: 24–39. doi: 10.1007/978-3-642-21031-0_3.

[14] EMURA K, MIYAJI A, NOMURA A, *et al*. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]. The 5th International Conference on Information Security Practice and Experience, Xi'an, China, 2009: 13–23. doi: 10.1007/978-3-642-00843-6_2.

[15] HERRANZ J, LAGUILLAUMIE F, and RÀFOLS C. Constant size ciphertexts in threshold attribute-based encryption[C]. The 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 2010: 19–34. doi: 10.1007/978-3-642-13013-7_2.

[16] GE Aijun, ZHANG Rui, CHEN Cheng, *et al*. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts[C]. The 17th Australasian Conference on Information Security and Privacy, Wollongong, Australia, 2012: 336–349. doi: 10.1007/978-3-642-31448-3_25.

[17] ZHANG Yinghui, ZHENG Dong, CHEN Xiaofeng, *et al*. Computationally efficient ciphertext-policy attribute-based

encryption with constant-size ciphertexts[C]. The 8th International Conference on Provable Security, Hong Kong, China, 2014: 259–273. doi: 10.1007/978-3-319-12475-9_18.

[18] 安立峰, 范运东, 付钰. 支持策略隐藏且固定密文长度的属性基加密方案[J]. 通信技术, 2018, 51(1): 156–164. doi: 10.3969/j.issn.1002-0802.2018.01.028.
AN Lifeng, FAN Yundong, and FU Yu. Attribute-based encryption scheme with hidden policy and constant length ciphertext[J]. *Communications Technology*, 2018, 51(1): 156–164. doi: 10.3969/j.issn.1002-0802.2018.01.028.

[19] KUMAR G S and KRISHNA A S. Privacy Sustaining Constant Length Ciphertext-policy Attribute-based Broadcast Encryption[M]. WANG J, REDDY G, PRASAD V, *et al*. Soft Computing and Signal Processing. Singapore: Springer, 2019: 313–324.

[20] 赵志远, 朱智强, 王建华, 等. 属性可撤销且密文长度恒定的属性基加密方案[J]. 电子学报, 2018, 46(10): 2391–2399. doi: 10.3969/j.issn.0372-2112.2018.10.012.
ZHAO Zhiyuan, ZHU Zhiqiang, WANG Jianhua, *et al*. Attribute-based encryption with attribute revocation and constant-size ciphertext[J]. *Acta Electronica Sinica*, 2018, 46(10): 2391–2399. doi: 10.3969/j.issn.0372-2112.2018.10.012.

[21] SUSILO W, YANG Guomin, GUO Fuchun, *et al*. Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes[J]. *Information Sciences*, 2018, 429: 349–360. doi: 10.1016/j.ins.2017.11.037.

[22] 孙瑾, 王小静, 王尚平, 等. 支持属性撤销的可验证多关键词搜索加密方案[J]. 电子与信息学报, 2019, 41(1): 53–60. doi: 10.11999/JEIT180237.
SUN Jin, WANG Xiaojing, WANG Shangping, *et al*. Verifiable multi-keyword search encryption scheme with attribute revocation[J]. *Journal of Electronics & Information Technology*, 2019, 41(1): 53–60. doi: 10.11999/JEIT180237.

[23] 牛淑芬, 谢亚亚, 杨平平, 等. 加密邮件系统中基于身份的可搜索加密方案[J]. 电子与信息学报, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.
NIU Shufen, XIE Yaya, YANG Pingping, *et al*. Identity-based searchable encryption scheme for encrypted email system[J]. *Journal of Electronics & Information Technology*, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.

[24] BELGUITH S, KAANICHE N, LAURENT M, *et al*. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IOT[J]. *Computer Networks*, 2018, 133: 141–156. doi: 10.1016/j.comnet.2018.01.036.

[25] 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. doi: 10.3724/SP.J.1001.2011.03993.
SU Jinshu, CAO Dan, WANG Xiaofeng, *et al*. Attribute-based encryption schemes[J]. *Journal of Software*, 2011, 22(6): 1299–1315. doi: 10.3724/SP.J.1001.2011.03993.

[26] QIU Shuo, LIU Jiqiang, SHI Yanfeng, *et al*. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack[J]. *Science China Information Sciences*, 2017, 60(5): 052105. doi: 10.1007/s11432-015-5449-9.

[27] 刘振华, 周佩琳, 段淑红. 支持关键词搜索的属性代理重加密方案[J]. 电子与信息学报, 2018, 40(3): 683–689. doi: 10.11999/JEIT170448.
LIU Zhenhua, ZHOU Peilin, and DUAN Shuhong. Attribute-based proxy re-encryption scheme with keyword search[J]. *Journal of Electronics & Information Technology*, 2018, 40(3): 683–689. doi: 10.11999/JEIT170448.

杨小东：男，1981年生，博士，教授，研究方向为代理重签名和云计算安全.
李　婷：女，1995年生，硕士生，研究方向为云审计安全.
麻婷春：女，1992年生，硕士生，研究方向为属性加密.
陈桂兰：女，1995年生，硕士生，研究方向为可搜索加密.
王彩芬：女，1963年生，博士，教授，研究方向为信息安全协议与网络安全.

责任编辑：马秀强