支持访问策略部分隐藏的CP-ABE方案

刘霞[1,2,3]，王馨族[2]，张涛[1]，陈盈阁[1]，王荣[1]，冯朝胜[1,3]，秦志光[3]
（1. 四川师范大学计算机科学学院，四川 成都 610101；2. 成都东软学院数字艺术与设计学院，四川 成都 611844；
3. 电子科技大学网络与数据安全四川省重点实验室，四川 成都 610054）

摘　要：针对现有支持外包解密的基于密文策略的属性加密（CP-ABE）方案大多未考虑对密文访问策略的隐私保护，而部分支持策略隐藏的方案又存在访问策略匹配效率低的问题，提出一种支持访问策略隐藏且访问策略匹配效率较高的CP-ABE方案。该方案对属性值进行盲化处理并构造隐藏策略访问树，实现了访问策略的隐私保护；采用布隆过滤器对属性进行过滤与成员认证，从而快速找到满足访问策略的最小属性集，减少解密测试中的大量无效计算；利用强算力的云服务器进行外包计算，减少本地的解密开销。理论分析和实验结果分析均表明，所提方案可兼顾计算效率与策略隐私保护，访问策略匹配效率和加解密速度显著提升，本地解密时间被减少至常数级。安全性分析表明，所提方案不仅保护了外包访问策略的隐私性，还能抵御选择明文攻击。

关键词：基于密文策略的属性加密；隐藏策略访问树；外包解密；布隆过滤器
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024179

CP-ABE scheme supporting partially hidden access policy

LIU Xia[1,2,3], WANG Xinzu[2], ZHANG Tao[1], CHEN Yingge[1], WANG Rong[1],
FENG Chaosheng[1,3], QIN Zhiguang[3]
1. Department of Computer Science, Sichuan Normal University, Chengdu 610101, China
2. College of Digital Art and Design, Chengdu Neusoft University, Chengdu 611844, China
3. Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China

Abstract: Most of the existing ciphertext-policy attribute-based encryption (CP-ABE) schemes that support outsourced decryption do not consider the privacy protection of the ciphertext access policy, while some schemes that support policy hidden have the problem of low access policy matching efficiency. Therefore, a CP-ABE scheme was proposed that supported access policy hidden and had high efficiency in access policy matching. In this scheme, the attribute values were blinded and a policy hidden access tree was constructed to realize the privacy protection of the access policy. Bloom filter was used to filter attributes and authenticate members, so as to quickly find the minimum set of attributes that meet the access policy and reduce a large number of invalid calculations in the decryption test. Finally, cloud servers with strong computing power for outsourced computing were used to reduce local decryption costs. Theoretical analysis and experimental results show that the proposed scheme can take into account both computational efficiency and policy privacy protection, significantly improving access policy matching efficiency, encryption and decryption speed, and local decryption time is reduced to a constant level. Security analysis demonstrates that the proposed scheme not only protects the privacy of outsourced access policies but also can resist chosen plaintext attacks.

Keywords: CP-ABE, hidden policy access tree, outsourced decryption, bloom filter

收稿日期：2024–04–26；修回日期：2024–09–24
通信作者：冯朝胜，csfenggy@126.com
基金项目：国家自然科学基金资助项目（No.61373163）；四川省自然科学基金资助项目（No.2022NSFSC0552, No.2023NSFSC1397）
Foundation Items: The National Natural Science Foundation of China (No.61373163), The Natural Science Foundation of Sichuan Province (No.2022NSFSC0552, No.2023NSFSC1397)

0　引言

随着云计算的发展日趋成熟，越来越多的企业享受着云服务带来的便捷，他们不仅能够将本地数据存储在云服务器上实现数据资源共享，还能以较低的成本获取云提供的强大算力，极大地解决了本地设备计算及存储性能不足的问题。与此同时，云计算的广泛使用也为用户带来了一系列安全问题，如云中密文共享的问题。为此，Bethencourt等[1]率先提出基于密文策略的属性加密（CP-ABE, ciphertext-policy attribute-based encryption）方案（又叫BSW方案），通过密文与访问策略绑定，用户私钥与一组属性相对应来实现外包数据的安全存储和秘密共享。该方案因其在CP-ABE[2]研究领域的基础性地位，成为后续研究重要的理论基础。尽管CP-ABE以其灵活的细粒度访问控制机制被广泛应用于云环境下的安全数据共享，但现有的CP-ABE方案[3-5]依然面临很多挑战，如解密计算效率较低、访问策略与用户属性未被保护等。

针对解密开销过高问题，目前主流的解决方式是采用外包解密技术。Green等[6]首次提出支持外包解密CP-ABE和基于密钥策略的属性加密（KP-ABE, key-policy attribute-based encryption）方案，基本原理是需要外包解密服务的用户将其外包解密私钥与密文发送给云服务器，利用云服务器的强大算力为用户执行复杂的幂指数与双线性配对计算。文献[7-8]提出了一些外包解密方案，将大量解密计算外包给云服务器，虽然大大减少了用户的计算量，但在实际应用场景中云服务器并不完全可信，用户如何判断云服务器的外包计算结果是否正确成为难题。针对该问题，一系列支持外包验证的CP-ABE方案被提出。Hwang等[9]提出了一个基于CP-ABE的数据共享系统，设计了基于签名的可验证外包方法，满足了CP-ABE所要求的可验证的计算外包和固定大小的密文输出，使多个用户在云环境中安全高效地共享数据。Liu等[10]提出了一种安全且高效的车辆雾计算外包计算方案，通过雾车执行外包计算，基于双线性映射的数字签名技术BLS（Boneh Lynn Shacham）和组签名，实现雾车的批量匿名认证，并验证了外包计算结果的正确性。Wang等[11]提出一种面向CP-ABE的外包解密验证方法，利用哈希函数和指数运算生成验证码，并对解密后的共享文件进行验证。

上述方案均侧重于减轻用户端本地解密计算负担，忽略了对访问策略中属性隐私的保护。针对访问策略的隐私泄露问题，Nishide等[12]通过多值属性的布尔公式表示访问策略，实现了与门访问结构的隐私保护，但其策略表达性受限，且计算开销较大。Lai等[13]提出一种灵活的策略隐藏方案，虽然该方案在标准模型中完全安全，但其安全性依赖非标准的复杂性假设，此外，在解密测试阶段，计算开销随着策略的复杂性呈线性增加。Han等[14]提出了一种可实现撤销、白盒跟踪和隐藏策略的CP-ABE方案，然而该方案需要生成冗余的密文或密钥组件。Zhang等[15]提出在标准模型下安全的策略隐藏方案，通过增加冗余密文子项，减少属性匹配检测中涉及的配对操作次数，降低了解密测试开销，但该方案依然面临较大的解密性能瓶颈。Zhang等[16]针对隐藏策略CP-ABE方案中普遍存在的属性值猜测攻击和解密测试算法时间复杂度过高两大问题，设计了一种在线隐私保护解密测试算法，将用户解密测试安全地外包给云服务器。但该方案的判断算法需要花费用户大量的计算时间，从而加重用户的计算负担。Nasiraee等[17]提出了一种在物联网环境下支持隐私保护的分布式数据访问控制（PDAC, privacy-preserving distributed data access control）方案，通过设计3种辅助树结构来实现隐私保护，但该方案在解密时需要抵消用户密钥中绑定的匿名凭据，导致加解密开销较大。Zhang等[18]提出了一种基于线性秘密共享方案（LSSS, linear secret sharing scheme）访问结构的实现部分隐藏的CP-ABE方案，并支持高效的密钥撤销，但验证算法占用大量时间，加重了用户的计算负担。MahdaviOliaee等[19]提出第一个基于多线性映射的算术电路访问策略的CP-ABE方案，定义了基于隐藏结果属性的加密概念，算术函数的结果不会透露给用户。

支持外包解密或策略隐藏的CP-ABE方案对比如表1所示，其中√表示支持，×表示不支持。

现有的支持外包解密的CP-ABE方案仍然存在用户属性与访问策略隐私未保护、外包解密正确性难验证等问题，而支持策略隐藏的CP-ABE方案存在访问策略匹配效率低（要解密完成才知道用户属性是否满足访问策略）的问题。鉴于此，本文提出一种支持访问策略隐藏且访问策略匹配效率较高的CP-ABE方案。

表1　支持外包解密或策略隐藏的CP-ABE方案对比

方案	访问结构	群阶	策略隐藏	外包解密算法	外包解密验证	属性匹配
文献[8]	LSSS	p	×	√	×	×
文献[9]	树型	p	×	√	√	×
文献[10]	LSSS	p	×	√	√	×
文献[12]	与门	p	√	×	×	×
文献[13]	LSSS	pqr	√	×	×	√
文献[14]	LSSS	p	√	×	×	√
文献[15]	LSSS	pqr	√	×	×	√
文献[17]	树形	p	√	√	×	√
所提方案	树形	p	√	√	√	√

本文主要的工作和贡献如下。

1) 提出一种面向访问树的部分访问策略隐藏方法。将一般访问树改进为隐藏策略访问树W与$\overline{W}$。用W加密信息后将其叶子节点删除以构成新的隐藏策略访问树$\overline{W}$，再与密文一同上传给云服务提供商，无论授权还是非授权用户都无法得到具体的属性值，在节省存储空间的同时实现访问策略的隐藏。

2) 基于所提的部分访问策略隐藏方法并以BSW方案[1]为基础，设计一个支持外包解密和部分策略隐藏的CP-ABE方案。提出一种具有筛选功能的外包解密方法，在加密与解密测试阶段引入布隆过滤器，对属性进行过滤与组合后找到满足策略的最小属性集，减少解密测试中的无效计算；利用云服务器进行外包解密计算，减少用户端解密开销，兼顾计算效率与策略隐私保护。

3) 分析了所设计方案的安全性和性能。安全性分析表明，属性经过盲化后进行外包保证了访问策略的隐私性，通过密文中的验证子项确保了外包解密的正确性，以BSW方案为基础确保了所提出方案的机密性。性能分析与实验结果均表明，仅对属性值进行隐藏与筛选可在较低计算开销的情况下实现策略隐私保护，经过属性的成员认证和外包解密后，本地解密时间被减少至常数级。

1　访问策略的部分隐藏

1.1　隐藏策略访问树

一般的访问树T由叶子节点和内部节点组成，如图1所示，叶子节点用来表示用户属性，内部节点为and、or或阈值门。所提方案通过将一般访问树T转换为图1所示的隐藏策略访问树W与$\overline{W}$，从而实现访问结构部分隐藏。将属性划分为属性名和属性值，设置父节点表示属性名，其子节点表示属性值。一个访问策略中有n个不同的属性名，记为$N=\{\varphi_1,\cdots,\varphi_i,\cdots,\varphi_n\}$；每一个属性名$\varphi_i$下又划分了2级节点，表示有$n_i$个不同的属性值，记为$A_i=\{v_{i,1},\cdots,v_{i,j},\cdots,v_{i,n_i}\}$，因此用户$u$的属性集合表示为$A_u=\{\varphi_1{:}v_{1,n_1},\varphi_2{:}v_{2,n_2},\cdots,\varphi_n{:}v_{n,n_i}\}$，其中，$v_{i,j}\in A_i$。例如，某医院的患者采用所提方案加密电子病历上传至云服务器，设置访问策略为{科室：肿瘤科 and 地区：成华 and 身份：患者}，则其属性名节点有3个，分别为{φ_1=科室}、{φ_2=地区}和{φ_4=身份}，其下对应的属性值节点分别为{v_{1,n_1}=肿瘤科}、{v_{2,n_2}=成华}和{v_{4,n_4}=患者}。

从树W根节点开始，自上而下为每个非叶子节点x定义一个次数为其门限值减1的多项式q_x，设置$q_R(0)=s$；此外，为每个属性值节点x选择对应的秘密值$b_x=q_{\mathrm{parent}(x)}(\mathrm{index}(x))$。数据拥有者使用上述访问结构$W$加密信息后，将访问树$W$的叶子节点删除，构成新的隐藏策略访问树$\overline{W}$和密文一起上传

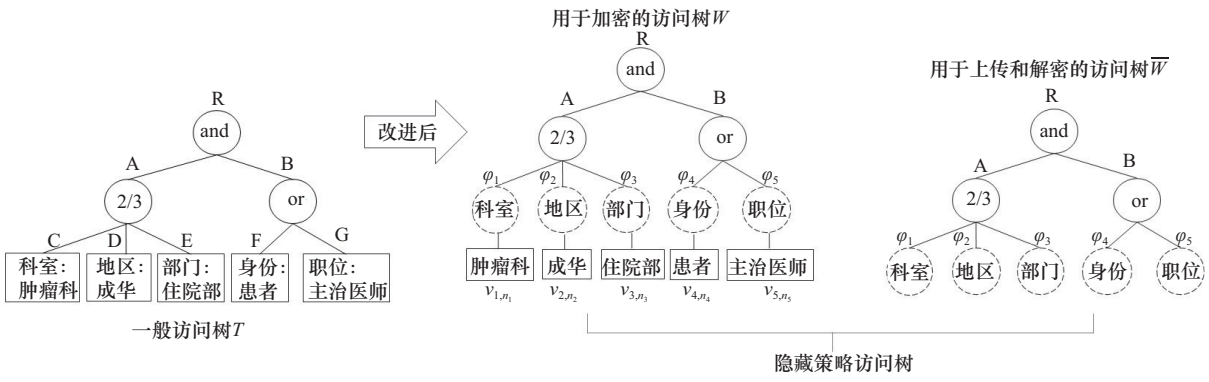

图1　改进后的隐藏策略访问树

至云服务提供商（CSP, cloud service provider）。由于所提方案中属性名是公开的，而属性值被嵌入到了密文中。因此，授权和非授权用户均无法获得具体的属性值与具体的取值要求，从而在节省存储空间和提高加解密效率的基础上，实现了访问结构的隐藏。

1.2　基于布隆过滤器的策略隐藏

布隆过滤器（BF, bloom filter）的设计初衷是测试某一元素是否属于某一个集合，本质是一种空间维度概率数据结构。其空间大小与所存储的元素自身大小无关，仅由用到的哈希函数个数决定，具备查询效率高、空间利用率高及计算复杂度低等优点。其构成包括一组m位数组和f个独立哈希函数$H=\{h_j\}_{i\in[f]}$，其中h_j:$\{0,1\}^*\rightarrow[1,m],1\leqslant j\leqslant f$。BF构造原理如图2所示，假设BF有3个独立哈希函数，数组中元素集合为$\{x,y\}\subseteq S$，BF构造算法将$h_1(x)$、$h_2(x)$、$h_3(x)$、$h_1(y)$、$h_2(y)$、$h_3(y)$在BF数组中的索引位置的值均设置为1。若想测试给定的元素x是否属于集合S，则利用BF查询算法计算元素x的所有哈希值$\{h_i(x)\}_{i\in[1,3]}$以获得其在数组的3个位置，若所有位都是1，则可认为x属于集合S。反之，若元素在数组位置上的任何一位是0，那么该元素一定不在集合S中。

基于BF的策略隐藏具备高查询效率和低内存消耗等优点，所提方案先将用户属性值进行盲化处理后构造BF，再在解密测试阶段，利用BF对数据使用者的属性进行过滤和成员认证，找到满足访问策略的最小属性集，进而实现高效的属性匹配。

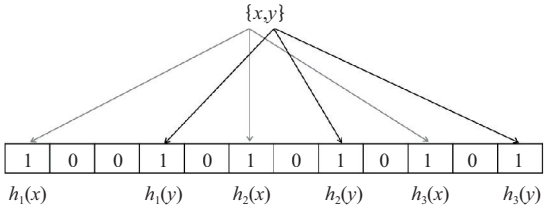

图2　BF构造原理

2　系统模型

2.1　系统框架

支持访问策略部分隐藏的CP-ABE方案的系统框架如图3所示，包含4类实体。

1) 授权机构（TA, trusted authority）：完全可信实体，负责生成系统公钥、系统主密钥和用户私钥。

2) CSP：半可信实体，负责存储密文、通过BF完成属性匹配，并利用转换密钥半解密，但不能保证解密结果的正确性。

3) 数据拥有者（DO, data owner）：负责定义访问策略，执行加密，创建隐藏策略访问树，构造用于隐藏属性的BF、生成外包验证子项并将其嵌入密文一同上传至CSP。

4) 数据使用者（DU, data user）：从TA获取用户私钥进而生成转换密钥和解密密钥，从CSP下载

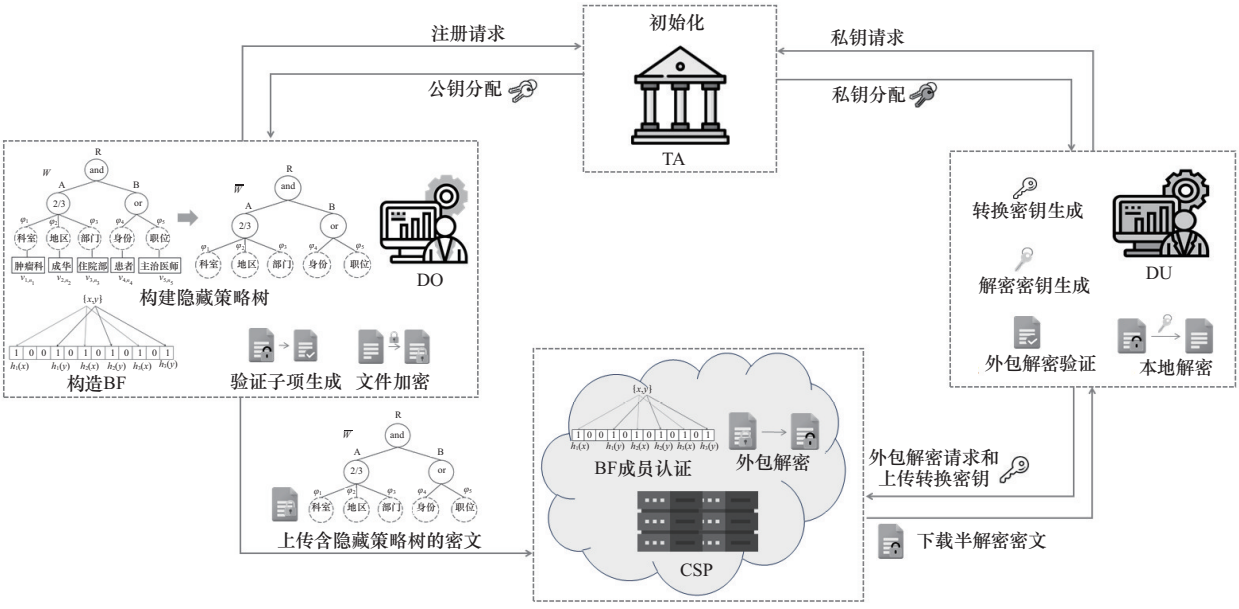

图3　支持访问策略部分隐藏的CP-ABE方案的系统框架

半解密密文，执行本地解密并对解密结果的正确性进行验证。

2.2 选择明文攻击CPA安全模型

支持访问策略部分隐藏的CP-ABE方案的CPA（chosen plaintext attack）安全模型定义如下。

初始化：挑战者C运行Setup算法，生成系统公钥PK和主密钥MSK，并将PK发送给A，MSK秘密保存。

查询阶段1：对于属性集$\{S_1,\cdots,S_{q_1}\}$的私钥，A向C发起属性密钥和外包解密密钥查询。

属性密钥查询：A将属性集合$\{S_1,\cdots,S_{q_1}\}$发送至C，然后对属性密钥询问。C执行KeyGen算法产生属性密钥SK^*作为A询问的回应。

外包解密密钥查询：A把属性集合$\{S_1,\cdots,S_{q_1}\}$发送到C以查询解密密钥。C回应A的询问时，先执行tk_KeyGen算法，生成外包解密密钥TK^*返回至A，同时在本地保留最终解密密钥DK^*。

挑战：敌手A向C提交两等长消息M_0、M_1和访问树T^*，C随机选择$\tilde{b}\in\{0,1\}$，并计算密文$\mathrm{CT}^*=\mathrm{Encrypt}(\mathrm{PK},M_{\tilde{b}},T^*)$，将密文$\mathrm{CT}^*$交给A。

查询阶段2：如查询阶段1，敌手发起其他查询，挑战者响应。限制条件是没有一组属性$\{S_1,\cdots,S_{q_1}\}$满足挑战访问结构T^*。

猜测：敌手输出关于$\tilde{b}$的猜测$\tilde{b}'$，如果$\tilde{b}=\tilde{b}'$则获胜。在本游戏中，敌手的优势被定义为

$$\mathrm{Adv}_{\mathrm{A}}=\left|\Pr[\tilde{b}=\tilde{b}']-\frac{1}{2}\right| \tag{1}$$

3 方案构造

支持访问策略部分隐藏的CP-ABE方案主要包括初始化、私钥生成、转换密钥生成、属性隐藏、加密、外包解密和本地解密7个阶段，涉及的算法及工作流程如图4所示，初始化阶段生成系统公钥和系统主密钥，在属性隐藏阶段构建隐藏策略树，对属性值进行盲化，同时创建BF并与加密阶段生成的共享密文及外包解密验证子项一起上传至CSP，实现对用户访问策略的隐藏。CSP收到DU下载请求后，先用BF进行属性匹配，再完成外包解密，最后DU下载半解密密文进行本地解密，验证外包解密结果的正确性并获得最终明文。

支持访问策略部分隐藏的CP-ABE方案的算法及详细过程如下。

3.1 初始化阶段

$\mathrm{Setup}(\lambda)\rightarrow(\mathrm{PK},\mathrm{MSK})$。该算法由TA初始化并调用，$\lambda$为安全参数，输出为系统公钥PK和系统主密钥MSK。G_0和G_T是2个阶为素数p的乘法循环群，g为群G_0的生成元，$e:G_0\times G_0\rightarrow G_T$是一组对称双线性映射。$U=\{\varphi_1,\cdots,\varphi_i,\cdots,\varphi_n\}$为系统中的属性名全集，为每个属性名$\varphi_i$下的属性取值集合$A_i=\{v_{i,1},\cdots,v_{i,j},\cdots,v_{i,n_i}\}$，对于每个属性值$v_{i,j}$随机选择$b_{i,j}\in Z_p^*$，计算$B_{i,j}=g^{b_{i,j}}$，然后生成$T=\{\varphi_i,v_{i,j},B_{i,j}\}_{i\in[1,n],j\in[1,n_j]}$。TA定义哈希函数$H_1$:$G_T\rightarrow Z_p^*$,$H_2$:$\{0,1\}^*\rightarrow\{0,1\}^\eta$,$H_3$:$G_T\rightarrow\{0,1\}^m$,$H_4$:$G_0\rightarrow\{0,1\}^m$。随机选择$\alpha,\beta\in Z_p^*$，$u,v\in G_0$，生成PK和MSK。

$$\mathrm{PK}=\{p,G_0,G_T,g,e(g,g)^\alpha,g^\beta,H_1,H_2,H_3,H_4,u,v\} \tag{2}$$

$$\mathrm{MSK}=\{g^\alpha,\beta,T,\{b_{i,j}\}_{i\in[1,n],j\in[1,n_i]}\} \tag{3}$$

3.2 私钥生成阶段

$\mathrm{KeyGen}(\mathrm{PK},\mathrm{MSK},L)\rightarrow\mathrm{SK}$。该算法由TA调用，输入系统公钥PK、主密钥MSK和用户属性集$L=\{\varphi_1{:}v_{1,n_1},\varphi_2{:}v_{2,n_2},\cdots,\varphi_n{:}v_{n,n_i}\}$。为DU随机选择$r\in Z_p^*$，对于$\forall v_{i,j}\in L(i\in[1,n],j\in[1,n_i])$，选择$r_i\in Z_p^*$，计算$D_{i,j}=g^r\cdot B_{i,j}{}^{r_i}$，$D'_{i,j}=g^{r_i}$，最后生成式(4)所示的用户私钥。

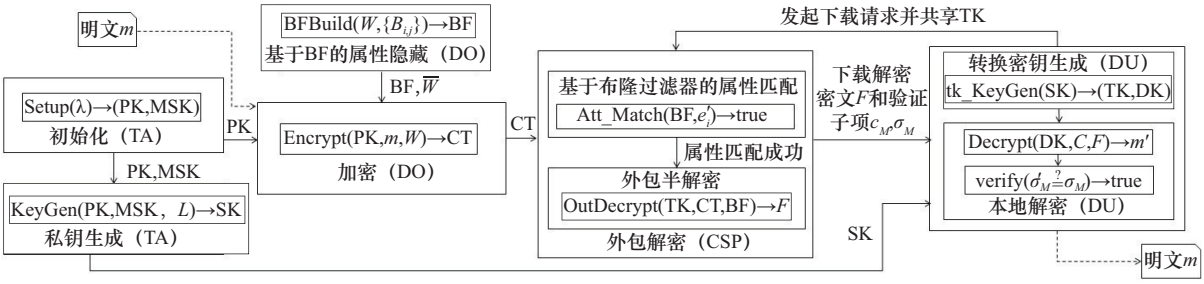

图4 支持访问策略部分隐藏的CP-ABE方案的算法及工作流程

$$\mathrm{SK}=\{D=g^{\frac{\alpha+r}{\beta}};\forall v_{i,j}\in L,D_{i,j}=g^{r}B_{i,j}{}^{r_i},D'_{i,j}=g^{r_i}\} \tag{4}$$

TA 还要为 DU 的每个属性计算对应的 $H_4(B_{i,j})$，并将之与生成的私钥一并通过安全通道发给DU。

3.3　转换密钥生成阶段

tk_KeyGen(SK) → (TK,DK)：由私钥所有者调用，输入其私钥SK，接着随机选择 $\delta\in Z_p^*$，生成的转换密钥TK为

$$\mathrm{TK}=\{D=g^{\frac{\delta\alpha+r}{\beta}};\forall v_{i,j}\in L,D_{i,j}=g^{\delta r}B_{i,j}{}^{\delta r_i},D'_{i,j}=g^{\delta r_i}\} \tag{5}$$

同时生成最终解密密钥 $DK=\delta$，用于本地解密。

3.4　属性隐藏阶段

属性隐藏阶段包含隐藏策略树的构建和布隆过滤器的构造，具体过程如下。

1) 隐藏策略树的构建Att_Hide:$W\rightarrow\overline{W}$

DO按图1将一般访问树 W 的属性分为属性名和属性值，将属性值去掉，只保留属性名来构建隐藏策略树 $\overline{W}$，实现对访问策略的部分隐藏。

2) BF构造BFBuild($\varphi_i,v_{i,j}$,MF) → BF

DO向TA提交共享文件访问策略所包含的所有属性，TA查询 T（$T=\{\varphi_i,v_{i,j},B_{i,j}\}_{i\in[1,n],j\in[1,n_j]}$）表获得每个属性对应的 $B_{i,j}$，并返回给DO，DO计算盲化属性集 $e=\{H_2(H_2(\mathrm{MF})\|H_4(B_{i,j}))\}$（其中MF为共享文件元数据）来构造BF，用于数据使用者在解密时进行属性的存在性判定。BF的构造如下。

① 定义BF的参数(n,η,H,k)，其中 n 为要添加的属性数量，k 为哈希函数的数量，η 表示插入元素的最大位长，$H=\{h_j\}_{j\in[1,k]}$ 是 k 个独立哈希函数，并将过滤器中所有位置的值初始化为0。

② 用BF的独立哈希函数 $H=\{h_j\}_{j\in[1,k]}$ 将DO盲化后的属性 $e_{i,j}$ 分别散列到 k 个位置索引 $\{h_1(e_{i,j}),h_2(e_{i,j}),\cdots,h_k(e_{i,j})\}$，最后将所有位置索引上的值置为1，即BF[$h_i(e)$] = 1。

③ 对于访问树 W 中的每个属性，重复上述过程以完成BF的构造。

3.5　加密阶段

Encrypt(PK,m,W) → CT。该加密算法由数据拥有者执行，输入公共参数PK、消息 m 和访问策略树 W，输出包含隐藏策略树 $\overline{W}$ 的密文CT。

自根节点 R 开始，逐一为树 W 中的节点 x 选取一个多项式 q_x，次数 $d_x=k_x-1$，其中 k_x 为门限值。首先，DO设置根节点 $q_R(0)=s$，并选择 d_R 个剩余节点完全定义多项式。对于其他节点，设置为 $q_x(0)=q_{\mathrm{parent}(x)}(\mathrm{index}(x))$，并随机选择其余系数完全定义它，对于 W 中叶子节点的父节点，其表示属性值 $v_{i,j}$ 所属的属性名 φ_i。接着，调用BFBuild($\varphi_i,v_{i,j}$,MF) → BF，并随机选择 $R\in\{0,1\}^m$，生成外包解密验证子项 $C_M=H_3(m)\oplus R$，$\sigma_M=u^{H_1(m)}v^{H_2(R)}$ 并输出式(6)所示密文。

$$\begin{aligned}\mathrm{CT}=\{&\overline{W},\mathrm{BF},C=me(g,g)^{\alpha s},C'=g^{\beta s},C_M,\sigma_M,\\&\forall y\in Y,C_{i,j}=g^{q_y(0)},C'_{i,j}=B_{i,j}{}^{q_y(0)}\}\end{aligned} \tag{6}$$

最后，DO将 H_2(MF)与CT一并发给CSP。其中，$\overline{W}$ 为不含属性值信息的访问策略，确保了用户策略隐私安全。

3.6　外包解密阶段

OutDecrypt(TK, CT, BF) → F。该阶段包括属性匹配和半解密。

1) 属性匹配

用户DU首先检查自己属性名是否满足 $\overline{W}$。若满足，则计算最小属性集 $S_{\min}$，对于每个属性 φ_i:$v_{i,j}\in S_{\min}$，获取对应 $H_4(B_{i,j})$，从CSP获取 H_2(MF)，计算得到盲化后的属性集 $e'=\{H_2(H_2(\mathrm{MF})\|H_4(B_{i,j}))\}$，连同转换密钥TK及最小属性集相关部分一起上传至CSP。本文所提的支持访问策略部分隐藏的CP-ABE方案采用先验证后解密，云服务器在收到DU的解密请求和转换密钥TK后，对盲化后的用户属性集 e' 进行成员认证，流程如下。

云服务器通过BF中的独立哈希函数 H 计算出 $e'_{i,j}$ 的 k 个位置索引 $\{h_1(e'_{i,j}),h_2(e'_{i,j}),\cdots,h_k(e'_{i,j})\}$；接着，查找BF中 k 个位置索引，判断BF[$h_i(e'_{i,j})$]是否全为1，若不全为1，则说明该属性不在布隆过滤器中，输出⊥；若全为1，则说明该属性 $v_{i,j}$ 满足访问树 $\overline{W}$。重复上述过程，直至确定用户所提供的最小属性集是否满足 $\overline{W}$，若不满足，则拒绝DU的解密请求，避免无效解密；若属性匹配成功，则进行外包解密。

2) 外包解密：OutDecrypt(TK, CT) → F

CSP通过DU解密请求发来的TK对共享密文

CT进行半解密。定义递归的解密函数DecNode(x)，半解密操作如下。

若x为叶子节点，则计算

$$\mathrm{DecNode}(v_{i,j})=\frac{e(D_{i,j},C_{i,j})}{e(D'_{i,j},C'_{i,j})}$$

$$=\frac{e(g^{\delta r}B_{i,j}{}^{\delta r_i},g^{q_x(0)})}{e(g^{\delta r_i},B_{i,j}{}^{q_x(0)})}=e(g,g)^{\delta r q_x(0)} \tag{7}$$

若x为非叶子节点，S_x为其任意k_x大小的子节点集合，则计算

$$\begin{aligned}F_x&=\prod_{Z\in S_x}F_Z{}^{\Delta_{i,S'_x}(0)}\\&=\prod_{Z\in S_x}(e(g,g)^{\delta r q_z(0)})^{\Delta_{i,S'_x}(0)}\\&=\prod_{Z\in S_x}(e(g,g)^{\delta r q_{\mathrm{parent}(z)}(\mathrm{index}(z))})^{\Delta_{i,S'_x}(0)}\\&=e(g,g)^{\delta r q_x(0)}\end{aligned} \tag{8}$$

解密至根节点时$q_R(0)=s$，可得$A=e(g,g)^{\delta r s}$，最后向数据使用者输出F

$$F=\frac{e(C',D)}{A}=\frac{e(g^{\beta s},g^{\delta\frac{\alpha+r}{\beta}})}{e(g,g)^{\delta r s}}=e(g,g)^{\delta\alpha s} \tag{9}$$

3.7 本地解密阶段

Decrypt(DK,C,F)$\rightarrow m'$：数据使用者将半解密密文F以及解密相关信息包括验证子项、密文子项C等下载至本地，计算$m'=\dfrac{C}{F^{\delta-1}}$。接着，计算外包验证子项$R'=C_M\oplus H_3(m')$，$\sigma'_M=u^{H_1(m')}\cdot v^{H_2(R')}$。仅当$\sigma'_M=\sigma_M$时，$m'$作为正确结果被接受。

4 安全性证明

由于文献[1]证明了BSW方案在一般群模型和随机预言模型下能抵御选择明文攻击，本文所提的支持访问策略部分隐藏的CP-ABE方案基于BSW方案提出，安全性可规约为BSW方案的安全性。

定理1 在随机预言模型和一般群模型下，本文所提出的支持访问策略部分隐藏的CP-ABE方案可抵御选择明文攻击。

证明 假设敌手A在一般群模型和随机预言模型下能以不可忽略的优势攻破所提方案，那么可以构建模拟器B，使得其能在同样的模型下攻破BSW方案[1]。这与在一般群模型和随机预言模型下BSW方案[1]可抵御选择明文攻击相矛盾，故所提方案在一般群模型和随机预言模型下能够抵御选择明文攻击。以下为模拟器B的构建过程。

初始化：挑战者C执行文献[1]中的Setup算法，生成MSK=$\{g^{\alpha},\beta,T,\{b_{i,j}\}_{i\in[1,n],j\in[1,n_i]}\}$和PK=$\{p,G_0,G_T,g,e(g,g)^{\alpha},g^{\beta},H_1,H_2,H_3,H_4,u,v\}$，将PK发送到模拟器B，MSK由挑战者C秘密保存，模拟器B选择随机的哈希函数用于生成改进后布隆过滤器，将其作为公开参数连同PK发送给敌手A。

查询阶段1：模拟器B构造密钥查询空表W和空集D。敌手A发起以下查询。

1) 私钥查询。模拟器B将待查询属性集S_u发送给挑战者C，挑战者C调用KeyGen算法生成对应私钥SK。模拟器B令空集$D=D\cup\{S_u\}$并将私钥SK返给敌手A，将(S_u,SK)存入W。

2) 转换密钥查询。模拟器B查询W，若查询不到，执行步骤1)以获得私钥，随后选择随机数$n\in Z_p^*$并计算转换密钥TK。接着，模拟器B将DK=n与TK返回敌手A，并将(S_u,SK, DK, TK)存入W。

挑战：敌手A向模拟器B提交明文消息M_0、M_1以及访问树T^*，并确保已经查询过的表W中属性集合S_u均不满足T^*。然后，模拟器B将M_0、M_1和T^*发送给文献[1]的挑战者C，挑战者C选择一个随机值$b\in\{0,1\}$，生成明文M_b与挑战访问树T^*相关联的密文CT*发给模拟器B。根据敌手A提交的挑战访问树T^*选择恰当的BF参数(n,η,H,k)构造BF$_{T^*}$，叶子节点属性值集合S_{T^*}被BF$_{T^*}$代替。模拟器B先从密钥询问表中查询布隆过滤器的参数(n,η,H,k)，然后构造相同的布隆过滤器，最后将CT**=$\{\mathrm{BF}_u,C,C_0,\forall i\in[1,l],C_i,C'_i\}$作为挑战密文发送给敌手A。

查询阶段2：敌手A重复查询阶段1的私钥查询，查询分为以下2种情况。

①S_u不满足T^*，进行的操作同查询阶段1。

②S_u满足T^*，该情况下无法查询属性集合S_u对应的私钥，而是按照如下方法生成伪转换密钥。模拟器B随机选择$d\in Z_p^*$，$t\in G_0$，运行KeyGen((d,t,PK),S_u)算法，生成私钥SK*。令TK=SK*，DK=d，根据S_u选择恰当的BF参数(n,η,H,k)构造BF$_u$，将DK、TK和BF$_u$返回给敌手A，并把(S_u,SK, DK, TK, BF$_u$)存入表W中。

猜测：若敌手A输出随机值b的猜想为b'，那么模拟器B输出的猜想也为b'。

考虑到属性BF的构造仅取决于T^*，所以游戏中额外构造出的BF不受所选择加密消息的影响，即BF不会扩大敌手A在此安全游戏中的优势。并且，在密钥生成阶段中，DO使用哈希函数计算了属性在BF中的位置序号，并采用BF代替属性集合S_u。外包时提供的用户属性经过了一系列盲化操作，所以外包解密的云服务器只能获得BF、改进后访问树以及盲化后的属性，敏感的属性值被替换为一串长为$n \times \eta$的比特串，仅当抗碰撞的哈希函数被云服务器所攻破时才可获得相关隐私数据。

综上，若敌手A能够以不可忽略的优势攻破本文提出的方案，那么模拟器B也能以不可忽略的优势攻破BSW方案[1]。但是BSW方案[1]已被证明在一般群模型和随机预言模型下是安全的，因此本文提出的支持访问策略部分隐藏的CP-ABE能达到CPA安全，并且可以实现安全的外包解密，具备访问策略的隐私保护功能。证毕。

定理2　在椭圆曲线离散对数难题成立的假设下，所提出的支持访问策略部分隐藏的CP-ABE方案能抵御选择明文攻击。

证明　假设敌手A能采用密钥密文篡改或伪造攻击以不可忽略的优势攻破所提出的支持访问策略部分隐藏的CP-ABE方案，那么就能够构造模拟器B，使得模拟器B能以不可忽略的优势解决椭圆曲线离散对数难题，给定六元组(p,G_0,G_T,e,g,g^x)，模拟器B的构建过程如下。

初始化：同定理1。

查询阶段1：敌手发起查询。查询内容包括私钥、加密和解密。

挑战：敌手A提交消息m和访问树T^*。模拟器B随机选择R，加密m得$C=\text{Encrypt}(\text{PK},T^*,m)$。计算验证码：$\hat{C}=u^{H_1(m)}v^{H_2(R)}$。将密文$(C,\hat{C})$返回给敌手A。

查询阶段2：敌手A重复查询阶段1的私钥查询。

输出密文：敌手A输出密文$(\bar{C},\hat{C})$。

模拟器B解密$\bar{C}$得到$\bar{m}||\bar{R}$。如果敌手A赢得游戏，有

$$u^{H_1(m)}v^{H_2(R)}=u^{H_1(\bar{m})}v^{H_2(\bar{R})} \tag{10}$$

$$g^{xH_1(m)}g^{yH_2(R)}=g^{xH_1(\bar{m})}g^{yH_2(\bar{R})} \tag{11}$$

$$x=\frac{y(H_2(\bar{R})-H_2(R))}{H_1(m)-H_1(\bar{m})} \tag{12}$$

对于六元组(p,G_0,G_T,e,g,g^x)，基于使用上面验证方法的ABE方案，通过在初始化阶段令$u=g^x$，选择$\forall y\in Z_p^*$，计算$v=g^y$，模拟器B就能利用式(12)计算出指数x，即意味着破解了椭圆曲线离散对数难题。故一旦密钥密文被篡改或伪造，就无法通过式(10)验证。证毕。

5　性能分析

性能分析包含了理论分析与实验分析。本节将所提方案与文献[12]方案、文献[13]方案、文献[15]方案以及文献[17]方案进行了特性和计算开销的对比分析。

5.1　理论分析

1) 特性对比

根据表1可知，所提方案与对比方案均实现了访问策略隐藏，但文献[12]方案的访问结构为多值“与门”，无法实现细粒度的灵活访问控制。文献[13]方案和文献[15]方案的群阶为耗时更多的合数阶，计算效率过低，且不支持外包解密和外包解密验证。文献[17]方案通过构造辅助树进行属性的匹配测试，建立属性累加器对属性进行成员认证，虽支持外包解密，但不支持外包解密验证。综上，本文提出的支持访问策略部分隐藏的CP-ABE方案提供了外包解密与高效的属性匹配，实现了访问策略的隐藏。

2) 计算开销对比

将所提方案与对比方案在加密、解密测试与本地解密计算开销方面进行理论分析，用到的符号及其定义如表2所示，计算开销对比结果如表3所示。

表2　符号及其定义

符号	定义
E_{G_0}	一次群G_0上的指数运算时间开销
E_{G_T}	一次群G_T上的指数运算时间开销
$\|I\|$	表示叶子节点个数或矩阵的行数
$\|I_{\min}\|$	最小访问树叶子节点个数
E_h	哈希函数计算时间
k	布隆过滤器中哈希函数的数量
pair	一次双线性配对运算的时间开销

表3 计算开销对比结果

方案	加密	解密测试	本地解密
文献[13]方案	$(7\|I\|+2)E_{G_0}+2E_{G_T}$	$(\|I_{\min}\|+2)\text{pair}+\|I_{\min}\|E_{G_0}+\|I_{\min}\|E_{G_T}$	$(\|I_{\min}\|+2)\text{pair}+\|I_{\min}\|E_{G_0}+\|I_{\min}\|E_{G_T}$
文献[15]方案	$(6\|I\|+2)E_{G_0}+2E_{G_T}$	$2\text{pair}+2\|I_{\min}\|E_{G_0}$	$(\|I_{\min}\|+2)\text{pair}+\|I_{\min}\|E_{G_0}+\|I_{\min}\|E_{G_T}$
文献[17]方案	$(5\|I\|-1)E_{G_0}+3E_{G_T}$	$2(\|I_{\min}\|-1)E_{G_T}$	E_{G_T}
所提方案	$(2\|I\|+3)E_{G_0}+E_{G_T}+(k+1)\|I\|E_h$	$(k+1)\|I_{\min}\|E_h$	$2E_{G_0}+E_{G_T}$

从表3可以看出，所提方案的加密阶段需要将用户盲化后的属性$\{B_{i,j}\}$添加至布隆过滤器中，用于数据使用者在解密时进行属性的存在性判定及过滤，因此相比其他方案增加了哈希运算开销$(k+1)|I|E_h$，并且为了后续外包解密时进行正确性验证，需要多计算2个密文验证子项，所以加密总开销为$(2|I|+3)E_{G_0}+E_{G_T}+(k+1)|I|E_h$。其他3个对比方案在密文中增加了冗余的密文子项或密钥组件，导致加密开销增大，它们之间在加密量上仅相差一个$|I|$。与其他3个对比方案加密计算量最少的文献[17]所提方案比较，所提方案加密计算量仅为其$\frac{2}{5}$。

所提方案在进行解密测试时，利用布隆过滤器筛选出满足访问树的属性，解密测试时间至多为$(k+1)|I_{\min}|E_h$。由于布隆过滤器的哈希计算耗时为微秒级，映射耗时为纳秒级，相对于群中的指数运算和双线性配对运算的毫秒级耗时，几乎可以忽略不计，故所提方案解密测试优势非常明显。

在本地解密部分，文献[13]方案和文献[15]方案都只实现了策略隐藏，并未进行解密外包，解密开销均包含大量复杂的配对运算和幂指数运算，解密开销与访问策略中属性数量成正比或线性关系。所提方案在本地解密时，先进行一次G_T上的指数运算得到解密结果，再进行2次G_0上的指数运算以完成外包解密的正确性验证，本地解密总开销为$2E_{G_0}+E_{G_T}$。由于文献[17]方案和所提方案将大量复杂的运算外包给云计算，因此本地解密开销减少为常数级。文献[17]方案虽然在本地解密上计算量略低于所提方案，但其未对外包解密进行验证。

在不支持解密外包的情况下，总解密计算量=解密测试计算量+本地解密计算量；在支持解密外包情况下，总解密计算量=解密测试计算量+外包解密计算量+本地解密计算量。所提方案和文献[17]方案的外包解密计算量均约为$2|I_{\min}|\text{pair}+2(|I_{\min}|-1)E_{G_T}$。不难发现，由于解密测试时间显著低于其他方案，所提方案的总解密量也显著低于其他方案。

通过上述理论分析可知，在综合考虑计算成本和策略隐私的情况下，所提方案实现了不降低系统安全性下的访问策略的隐私保护以及加解密速度和策略匹配效率的大幅提升。

5.2 实验分析

本文基于CP-ABE工具包以及基于双线性配对的Java语言的密码学库（JPBC），使用Java编程语言在IDEA集成开发工具上构建实验平台。所提到的布隆过滤器基于Spookyhash哈希技术来构造，哈希函数为128位。实验环境配置：CPU为Intel(R)Core(TM)i5-12490F(3.0 GHz)、内存为16 GB、操作系统为Windows10×64位的台式计算机。本次仿真实验对比分析了文献[13]方案、文献[15]方案、文献[17]方案和本文所提方案在加密、解密过程中的计算开销。设属性空间$|U|=50$，访问策略中的用户属性数$|S_u|$以5为间隔从5个逐次递增到50个。为降低测算误差，对每组实验进行50次测算求平均作为结果，计算开销对比如图5和图6所示。

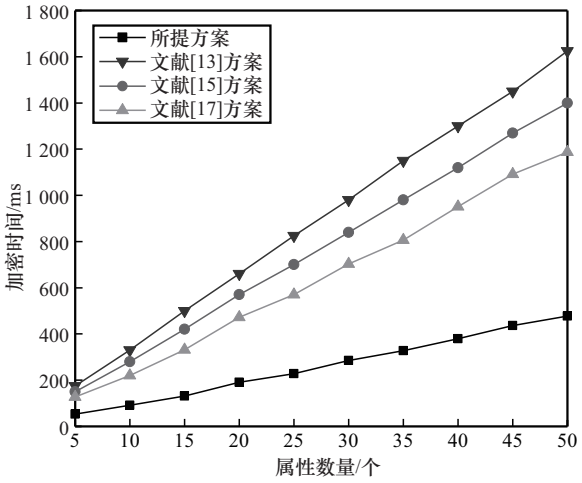

图5 加密时间开销对比

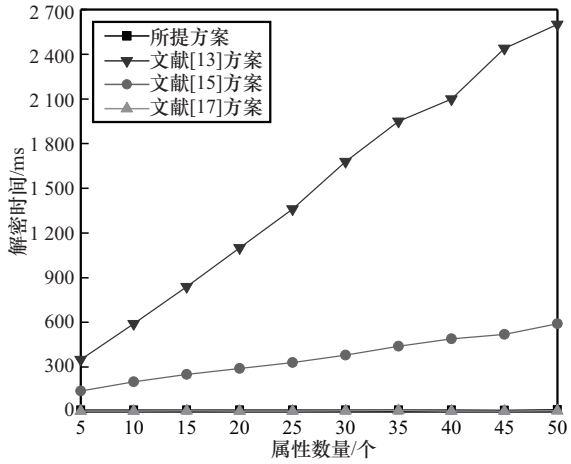

图6　本地解密时间开销对比

从图5中可以看出，包含所提方案在内的4个方案的加密时间均与访问策略中属性个数成正比或线性关系，但在属性个数相同的情况下，所提方案的加密耗时明显要少得多，而且随着属性个数的增加，加密耗时的差距愈加明显。从图6中可以容易看出，文献[13]方案和文献[15]方案的本地解密时间（含解密测试时间）均与最小属性集对应的最小访问树的叶子节点数量或最小访问矩阵行数成正比或线性关系，但文献[15]方案的增长速度要慢得多，这是因为文献[15]方案解密测试时进行的双线性配对数量固定。所提方案与文献[17]方案的解密耗时均为一个很小的常量。无论是加密还是解密，实验结果均与前面的理论分析结果是一致的。

6　结束语

本文提出一种支持访问策略部分隐藏的CP-ABE方案，该方案利用布隆过滤器对访问树的属性值进行隐藏，将一般访问树改进为访问策略部分隐藏访问树，实现对访问策略属性隐私保护；在解密测试阶段采用布隆过滤器对数据使用者的属性进行过滤与成员认证，找到满足访问策略的最小属性集，减少解密测试中的无效计算，提升访问策略匹配效率。利用强算力的云服务器完成外包解密，在减少本地解密开销的同时实现外包解密的正确性验证。安全性分析表明，所提方案在一般群模型和随机预言模型下能对抗选择明文攻击。理论分析和实验结果分析表明，所提方案在支持访问策略部分隐藏和可验证外包解密的同时，加解密时间更短，访问策略匹配效率更高。

参考文献：

[1] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07). Piscataway: IEEE Press, 2007: 321-334.

[2] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[3] FENG C S, YU K P, ALOQAILY M, et al. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13784-13795.

[4] LI H, YU K P, LIU B, et al. An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things[J]. IEEE Journal of Biomedical and Health Informatics, 2022, 26(5): 1949-1960.

[5] LI Q, ZHANG Q Q, HUANG H P, et al. Secure, efficient, and weighted access control for cloud-assisted industrial IoT[J]. IEEE Internet of Things Journal, 2022, 9(18): 16917-16927.

[6] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//Proceedings of the 20th USENIX Security Symposium. Berkeley: USENIX Association, 2011: 523-538.

[7] SANCHOL P, FUGKEAW S, SATO H. A mobile cloud-based access control with efficiently outsourced decryption[C]//Proceedings of the 2022 10th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). Piscataway: IEEE Press, 2022: 1-8.

[8] TU S S, HUANG F M, ZHANG S J, et al. Ciphertext-policy attribute-based encryption for securing IoT devices in fog computing[C]//Proceedings of the 2022 International Conference on Computer, Information and Telecommunication Systems (CITS). Piscataway: IEEE Press, 2022: 1-7.

[9] HWANG Y W, LEE I Y. A study on CP-ABE based data sharing system that provides signature-based verifiable outsourcing[C]//Proceedings of the 2021 International Conference on Advanced Enterprise Information System (AEIS). Piscataway: IEEE Press, 2021: 1-5.

[10] LIU X J, CHEN W, XIA Y J, et al. SE-VFC: secure and efficient outsourcing computing in vehicular fog computing[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 3389-3399.

[11] WANG H Q, HE D B, HAN J G. VOD-ADAC: anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud[J]. IEEE Transactions on Services Computing, 2020, 13(3): 572-583.

[12] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encrypttion with partially hidden encryptor-specified access structures[C]//International Conference on Applied Cryptography & Network Security. Berlin: Springer, 2008: 111-129.

[13] LAI J Z, DENG R H, LI Y J. Expressive CP-ABE with partially hidden access structures[C]//Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2012: 146-162.

[14] HAN D Z, PAN N N, LI K C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 316-327.

[15] ZHANG Y H, ZHENG D, DENG R H. Security and privacy in smart health: efficient policy-hiding attribute-based access control[J]. IEEE Internet of Things Journal, 2018, 5(3): 2130-2145.

[16] ZHANG Z S, ZHANG W, QIN Z G. A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy- protective decryption testing in IoT assisted cloud computing[J]. Future Generation Computer Systems, 2021, 123: 181-195.

[17] NASIRAEE H, ASHOURI-TALOUKI M. Privacy-preserving distributed data access control for CloudIoT[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(4): 2476-2487.

[18] ZHANG W, ZHANG Z S, XIONG H, et al. PHAS-HEKR-CP-ABE: partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system[J]. Journal of Ambient Intelligence and Humanized Computing, 2022, 13(1): 613-627.

[19] MAHDAVIOLIAEE M, AHMADIAN Z. Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits[J]. Journal of Computer Virology and Hacking Techniques, 2023, 19(4): 515-528.

[作者简介]

刘霞（1978– ），女，四川都江堰人，四川师范大学讲师，主要研究方向为网络安全、访问控制、隐私保护和区块链等。

王馨族（1997– ），女，四川苍溪人，成都东软学院助教，主要研究方向为区块链、信息安全等。

张涛（2000– ），男，四川德阳人，四川师范大学硕士生，主要研究方向为隐私保护与访问控制等。

陈盈阁（2000– ），男，四川成都人，四川师范大学硕士生，主要研究方向为云环境下的隐私保护、数据安全等。

王荣（1989– ），女，四川资阳人，博士，四川师范大学讲师，主要研究方向为隐私保护、联邦学习等。

冯朝胜（1971– ），男，四川广元人，博士，四川师范大学教授、博士生导师，主要研究方向为网络与信息安全。

秦志光（1956– ），男，四川荣昌人，博士，电子科技大学教授、博士生导师，主要研究方向为密码学、网络与信息安全。