研究论文

面向云数据访问控制的认证密文检索方案

曹艺博[1],徐仕远[2],陈雪[2],奚雨新[3],郭宇[3*]

摘要 可搜索加密作为实现密文检索的关键技术,在云存储领域具有重要应用价值。然而,现有方案普遍采用单一用户模型,且不能抵抗内部关键字猜测攻击,导致云数据面临隐私泄露风险。因此,亟需面向云数据的隐私保护需求,设计支持多用户模型且具备更高安全性的可搜索加密方案。鉴于此,提出了一种面向云数据访问控制的认证密文检索方案。在访问控制方面,通过将属性嵌入用户私钥并以此生成检索陷门,将访问策略嵌入关键字密文,通过门限秘密共享技术实现属性和访问策略的匹配,从而构建细粒度的检索权限控制机制。在安全性增强方面,数据拥有者的私钥被嵌入到关键字密文中实现密文认证,有效抵御内部关键字猜测攻击。性能分析表明,本文方案的陷门生成算法具有计算高效性,同时用户私钥具备较低的存储开销,适用于云存储领域。

关键词 云存储;隐私保护;密文检索;访问控制

云计算技术的广泛应用推动了云存储服务的高效部署,海量数据以加密形式集中托管于云端服务器,显著提升了资源利用率和跨域协作能力[1]。然而,云存储的开放性与数据所有权的分离特性,使得数据的隐私保护面临严峻挑战[2]。2024 年全球网络安全态势显示,数据安全已成为网络空间安全体系建设的重点领域,各国纷纷出台政策法规以应对数据泄露、非法访问等安全风险[3]。在电力行业智能化转型中,基于边缘计算与区块链的智慧用电平台通过去中心化架构实现了数据安全共享[4-5],但云端数据的细粒度访问控制仍需强化。传统密码学技术(如加密、签名[6-9]、签密[10]等原语)虽能确保数据静态安全性,却阻碍了授权用户对密文数据的检索与共享,导致用户需频繁下载并解密数据以进行本地检索,极大削弱了云存储的实用价值。为此,可搜索加密(searchable encryption, SE)技术应运而生,其允许用户在加密数据上直接执行关键字搜索操作,既保障了数据隐私,又满足了实际应用中的检索需求[11-13]。然而,随着数据共享场景的复杂化,如何在多用户协作环境下实现安全高效的密文检索成为亟待突破的挑战[14]。

云存储环境下,多用户协同场景对 SE 技术提出了更高的动态访问控制需求[15-16]。传统单用户 SE 方案通常假设数据所有者独立管理密钥与检索权限[17-18],但在实际云数据共享中,不同用户(如医疗机构中的医生、护士、研究人员)须基于角色或属性获取差异化的数据访问权限。例如,在跨机构联合数据分析场景中,参与方可能动态加入或退出,且需根据数据敏感性分级授权检索能力。现有基于单用户的 SE 方案难以支持灵活的权限分配与动态更新,导致检索效率低下或安全隐患加剧等问题,制约了 SE 技术在实际

1. 北京邮电大学网络空间安全学院,北京 100876

2. 香港大学计算机科学系,香港 999077

3. 北京师范大学人工智能学院,北京 100875

收稿日期:2025-05-06;修回日期:2025-05-30

基金项目:国家自然科学基金项目(62102035);国家重点研发计划项目(2022ZD0115901);北京市科技计划项目(Z241100001324011);CCF-蚂蚁科研基金项目(CCF-AFSG RF20240403)

作者简介:曹艺博,博士研究生,研究方向为云数据安全、隐私保护和密码学,电子信箱:yibocaobupt@gmail.com;郭宇(通信作者),副教授,研究方向为人工智能安全、数据安全和隐私保护,电子信箱:yuguo@bnu.edu.cn

引用格式:曹艺博,徐仕远,陈雪,等. 面向云数据访问控制的认证密文检索方案[J]. 科技导报,2025,43(12):161-170;doi:10.3981/j.issn.1000-7857.2025.05.00015

跨机构数据共享中的应用。

当前可搜索加密技术还面临内部关键字猜测攻击(insider keyword guessing attacks, IKGAs)的威胁,攻击手段为:攻击者(云服务器或其他授权用户)可通过遍历有限的关键字空间,反复调用密文计算算法,将生成的密文与用户提交的检索陷门进行匹配,进而推断出关键字的信息。此类攻击一旦成功,将直接泄露用户的搜索意图,破坏方案的陷门安全性。在云存储场景中,攻击者甚至可进一步推断用户身份、数据关联关系等高价值信息,导致严重的隐私泄露风险。因此,设计抗 IKGAs 的可搜索加密方案,已成为提升方案实际部署能力的关键研究方向,这将对电力物联网[19]、智能电网[20]等关键领域的云数据安全管理具有重要实践价值。

鉴于此,提出了一种面向云数据访问控制的认证密文检索(attribute-based authenticated searchable encryption, ABASE)方案,实现云数据的密文检索与访问控制,并且抵抗 IKGAs。具体而言,将属性嵌入用户私钥并以此生成检索陷门,将访问策略嵌入关键字密文,通过门限秘密共享技术实现属性和访问策略的匹配,实现用户的检索权限控制。另外,在关键字密文中加入数据拥有者的私钥实现认证,因此,只有拥有这一私钥的实体(即数据拥有者本身)才能执行密文计算算法,抵抗了 IKGAs。性能分析表明,ABASE 相对于其他 SE 方案在陷门生成过程中具有明显的效率优势,且具有较短的用户私钥大小,适用于云存储领域。

1 研究现状

Boneh 等[21]基于身份基加密和双线性 Diffie-Hellman 困难假设,首次提出公钥可搜索加密的概念,受到研究者的广泛关注。随着云存储多用户访问控制需求的激增,研究者将可搜索加密与属性基加密技术深度融合,构造一系列属性可搜索加密方案。Zheng 等[22]设计可验证的密文策略属性基可搜索加密方案,通过引入验证机制确保云服务器搜索操作的可信执行。Yu 等[23]提出基于密钥策略的属性可搜索加密方案,其核心在于将访问策略嵌入加密索引,仅当用户属性集满足预设策略时方可生成有效的陷门进行检索。Miao 等[24]提出了一种多授权中心的属性可搜索加密(multi-authority attribute-based keyword search, MABKS)方案,最大限度地减少云系统中资源有限设备的计算和存储开销,并且支持恶意属性权限跟踪和属性更新。随后,Miao 等[25]构建了面向多数据拥有者场景的属性可搜索加密(attribute-based encryption with keyword search in shared multi-owner setting, ABKSSM)方案,实现了选择安全性并且抵御离线关键字猜测攻击。Yang 等[26]提出了一种高效且安全的数据选择性共享与获取(data selective sharing and acquisition, DSA)方案,使数据拥有者能够以细粒度的方式控制数据的访问,并使用户能够在不暴露其利益的情况下完成数据获取。李红等[27]借助线性秘密共享方案构建检索陷门生成机制,支持以任意单调布尔公式表达的复杂策略检索。针对传统方案中明文策略泄露敏感信息的问题,刘晨旭等[28]创新性地提出具有前向安全、后向安全与动态撤销能力的部分策略隐藏方案,通过公开属性类别但隐藏属性值的策略构造方法实现隐私保护,同时优化了恶意用户撤销流程。此外,张克君等[29]基于代理重加密机制设计了多关键词属性基可搜索方案,通过重构访问树节点信息实现数据读写权限的细粒度控制,并利用属性基加密实现陷门不可区分性。为缓解资源受限设备的计算压力,郭瑞等[30]结合了密文策略属性加密与在线/离线加密技术,提出一种完全策略隐藏属性可搜索加密方案与外包解密机制,实现计算负载的分布式迁移。上述方案虽然能够实现数据检索过程中的用户访问控制,但没有考虑 IKGAs。

Byun 等[31]揭示了文献[21]方案的安全隐患,由于关键词熵值远低于传统密钥空间,攻击者可利用用户习惯性选取有限语义关键词的特性,对密文索引发起离线关键字猜测攻击(keyword guessing attacks, KGAs)。为应对此类威胁,Huang 等[32]开创性提出公钥认证可搜索加密方案,要求数据所有者对关键字同时执行加密与认证操作,确保密文关键词的真实性与来源可验证。张玉磊等[33]通过融合无证书公钥密码体制与代理重加密技术,构建多用户环境下抗 IKGAs 的可搜索加密方案,在随机预言模型下实现其选择密文安全性。胡震宇等[34]在强安全模型下构建了一种指定验证者的高效公钥认证可搜索加密方案,一定程度上避免

了双线性配对操作,提升了计算效率。随后,刘永志等[35]引入可信执行环境,在云端部署飞地程序隔离关键字匹配过程,通过硬件级安全隔离抵御恶意服务器攻击。肖心雨等[36]设计了具有严格陷门不可区分性的公钥认证密文检索方案,通过消除陷门生成过程中的统计特征关联,显著降低检索过程的信息泄露风险。Xu 等[37]提供了具有前向安全特性的公钥认证可搜索加密方案的一般结构,并提出了一个基于格密码的实现方式。面向实际部署需求,蒲浪等[38]基于国密 SM9 算法重构了公钥认证可搜索加密架构,将双线性映射运算等复杂操作迁移至云端,在抵抗 IKGAs 的同时优化用户端计算效率。

当前可搜索加密领域尚缺乏同时实现用户访问控制与抵抗内部关键字猜测攻击的可行架构,这一缺陷严重制约了该技术在云存储场景中的实际应用。因此,针对上述问题,提出一种面向云数据访问控制的认证密文检索方案。

2　问题描述

2.1　系统架构

系统模型如图 1 所示,包含 4 个实体,分别是可信权威中心、数据拥有者、数据用户和云服务器,各个实体的主要功能如下。

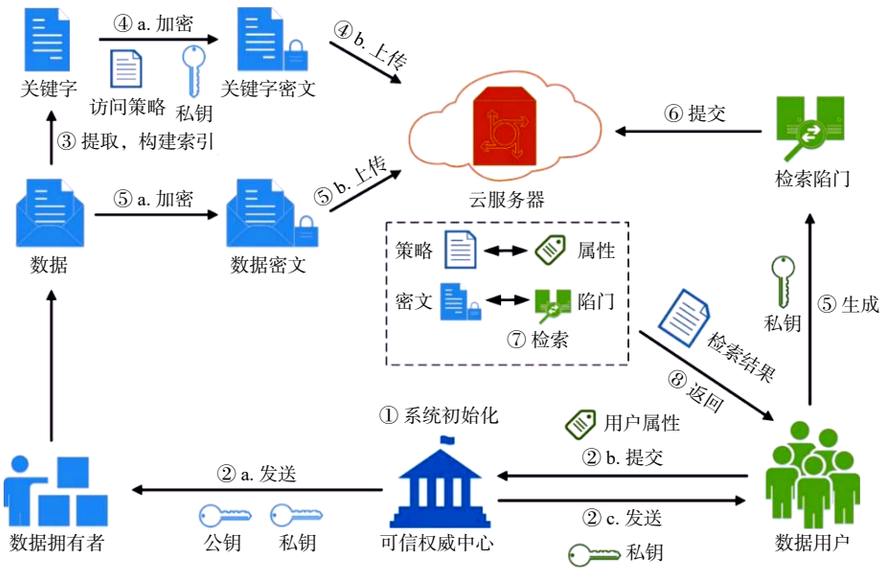

图 1　系统模型

1) 可信权威中心:可信权威中心负责初始化整个系统,并为数据拥有者和数据用户生成执行算法所需的密钥。具体而言,当接收到公共参数后,可信权威中心为数据拥有者生成公钥和私钥;当接收到公共参数和属性后,可信权威中心为数据用户生成包含用户属性的私钥。

2) 数据拥有者:数据拥有者设定访问策略,并从数据中提取关键字,构建索引列表。随后,数据拥有者利用自己的私钥和预设的访问策略对关键字进行加密,生成关键字密文。对于数据本身,数据拥有者调用属性加密算法进行加密生成数据密文。最后,将关键字密文和数据密文上传至云服务器。

3) 数据用户:数据用户选取待检索关键字,通过私钥为其生成检索陷门,提交给云服务器。此外,若检索到匹配的密文,数据用户利用自己的私钥解密搜索结果后得到原始云数据。

4) 云服务器:在接收到检索陷门后,云服务器对关键字密文进行逐一检索。若存在与此陷门匹配的关键字密文,则云服务器将其对应的数据密文作为搜索结果返回给数据用户。否则,云服务器向数据用户返回⊥,表示不存在匹配的关键字密文。

2.2　威胁模型

方案的威胁模型定义如下:(1) 可信权威中心被视作完全可信的,能够诚实地为各个实体生成所需要的参数,并通过安全保密的信道进行参数分发;(2) 数据拥有者是完全可信的,它能够生成有效的数据密文

和关键字密文,上传至云服务器;(3)数据用户被认为是恶意的,它会对存储在云服务器上的云数据进行未经授权的访问;(4)云服务器是半诚实的,它会诚实地执行检索操作并向数据用户返回正确的结果,但它会尝试获取有关云数据和关键字的信息。此外,云服务器通过遍历有限的关键字空间,反复调用密文计算算法,将生成的密文与用户提交的检索陷门进行匹配,能够推断出关键字的信息,破坏了陷门的不可区分性,发起内部关键字猜测攻击。

2.3 设计目标

根据上述威胁模型,方案具有3个设计目标。

1)实现云数据密文检索:对于任意待检索关键字,数据用户能够利用自己的私钥生成对应的检索陷门,提交给云服务器。云服务器能够在无须解密的前提下检索到匹配的关键字密文。

2)支持用户访问控制:引入密文策略属性加密的思想,将用户属性嵌入私钥,访问策略嵌入关键字密文,当且仅当属性满足访问策略时,用户才具有对这一关键字密文的检索权限,实现用户层面的访问控制。

3)抵抗内部关键字猜测攻击:在关键字密文计算过程中输入数据拥有者的私钥,实现对关键字的认证,保证只有数据拥有者才能执行密文计算算法。

2.4 算法定义

方案由6个算法组成,具体定义如下。

1)$(pp,MSK)\leftarrow \mathrm{Setup}(\lambda)$:输入安全参数$\lambda$,算法输出公共参数$pp$和主私钥$MSK$,将$pp$分发给其他实体,$MSK$由自己保存。

2)$(PK_S,SK_S)\leftarrow \mathrm{KeyGen_S}(pp)$:输入公共参数$pp$,算法输出公钥$PK_S$和私钥$SK_S$,发送给数据拥有者。

3)$SK_R\leftarrow \mathrm{KeyGen_R}(pp,R)$:输入公共参数$pp$和用户属性$R$,算法输出私钥$SK_R$,发送给数据用户。

4)$CT\leftarrow \mathrm{Encrypt}(pp,ck,SK_S,(W,t))$:输入公共参数$pp$、关键字$ck$、数据拥有者的私钥$SK_S$和访问策略$(W,t)$,算法输出关键字密文$CT$,上传至云服务器。

5)$TD\leftarrow \mathrm{Trapdoor}(pp,tk,PK_S,SK_R,R)$:输入公共参数$pp$、待搜索关键字$tk$、数据拥有者的公钥$PK_S$、数据用户的私钥$SK_R$和用户属性$R$,算法输出检索陷门$TD$,提交至云服务器。

6)$CT_M/\perp\leftarrow \mathrm{Search}(pp,CT,TD,R,(W,t))$:输入公共参数$pp$、关键字密文$CT$、检索陷门$TD$、用户属性$R$和访问策略$(W,t)$,算法输出搜索结果$CT_M/\perp$,发送给数据用户。

3 算法设计

3.1 预备知识

算法设计过程中所需要的预备知识如下。

定义1(双线性映射):设$\mathbb{G}$和$\mathbb{G}_T$是阶为p的乘法循环群,p是一个素数,a和b是2个整数,定义双线性映射$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$满足以下3个条件。

1)双线性:对于任意的群元素$g_1,g_2\in\mathbb{G}$和整数$a,b\in\mathbb{Z}_p$,$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

2)非退化性:存在群元素$g_1,g_2\in\mathbb{G}$,$e(g_1,g_2)\neq 1$。

3)可计算性:对于任意的群元素$g_1,g_2\in\mathbb{G}$,存在多项式时间算法计算$e(g_1,g_2)$。

定义2(属性加密):属性加密(attribute-based encryption, ABE)是一种基于属性实现细粒度访问控制的公钥加密方案,允许数据所有者根据数据接收者的属性或数据属性动态控制解密权限,可分为2类。

1)密文策略属性加密:将访问策略嵌入数据密文,将属性嵌入数据接收者的私钥。

2)密钥策略属性加密:将访问策略嵌入数据接收者的私钥,将属性嵌入数据密文。

ABE通过逻辑表达式(如“财务 AND 职位”)灵活定义访问权限,适用于云存储场景,在保护数据隐私的同时实现访问控制。

定义3(门限秘密共享):门限秘密共享(threshold secret sharing, TSS)是一种将秘密信息分散为多个份额并分发给不同参与者的密码学技术,其核心思想是只有达到预设门限值才能重构原始秘密,而少于门限值则无法获取任何有效信息。最经典的TSS方案是Shamir秘密共享,基于拉格朗日插值多项式实现,其秘密拆分和恢复过程如下。

1)秘密拆分:对于秘密值$s\in\mathbb{Z}_p$,设参与者数量为n,门限值为k。选择一个多项式$p[x]\in\mathbb{Z}_p[x]$,且令$p[0]=s$。生成n个秘密份额$p[1],p[2],\cdots,p[n]$,分别发送给n个参与者。

2)秘密恢复:收集至少k个秘密份额,利用拉格朗日插值公式$p[x]=\sum_{i=1}^{k}p[i]\cdot\prod_{j=1,j\neq i}^{k}\frac{x-j}{i-j}$重构多项式$p[x]$,进

而计算$p[0]=s$,即可恢复秘密值s。

3.2 系统初始化

系统初始化算法$Setup(\lambda)$由可信权威中心执行,负责初始化整个系统,并生成公共参数和主私钥。首先,可信权威中心选择一个大素数p和2个乘法循环群$\mathbb{G}$和$\mathbb{G}_T$,其中g是$\mathbb{G}$的生成元,初始化双线性映射$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$。其次,可信权威中心设定3个哈希函数$H_1:\{0,1\}^*\to\mathbb{G}$,$H_2:\mathbb{Z}_p\to\mathbb{G}$和$H_3:\mathbb{Z}_p\to\mathbb{Z}_p$,随机选择一个整数$v\in\mathbb{Z}_p$。最后,可信权威中心返回如下公共参数$pp$和主私钥$MSK$,将其发送给系统中的各个参与实体。

$$pp:=\left(p,\mathbb{G},\mathbb{G}_T,g,e,H_1,H_2,H_3,g^{H_3(v)}\right) \tag{1}$$

$$MSK:=v \tag{2}$$

3.3 密钥生成

密钥生成算法$KeyGen_S(pp)$和$KeyGen_R(pp,R)$由可信权威中心执行,负责为数据拥有者和数据用户生成密钥。对于数据拥有者,输入公共参数pp,可信权威中心随机选择一个整数$s\in\mathbb{Z}_p$,返回数据拥有者的公钥$PK_S:=g^s$和私钥$SK_S:=s$,并将其发送给数据拥有者。

对于数据用户,输入公共参数pp、主私钥MSK和用户属性$R=\{1,2,\cdots,r\}$,可信权威中心随机选择一个多项式$p[x]\in\mathbb{Z}_p[x]$,其中$p[0]=H_3(v)$。对于$j\in R$,计算$\hat{v}_j=p[j]$。最后,可信权威中心将私钥$SK_R:=\{\hat{v}_j\}_{j\in R}$返回给数据用户。

3.4 密文计算

密文计算算法$\mathrm{Encrypt}(pp,ck,SK_S,(W,t))$旨在为关键字计算密文,由数据拥有者执行。对于云数据M,数据拥有者设定关键字$ck\in\{0,1\}^*$,并且构建索引列表,记录云数据和关键字的对应关系。然后,数据拥有者输入访问策略并调用属性基加密算法$ABE-\mathrm{Encrypt}(pp,M,(W,t))$生成云数据密文$CT_M$,上传至云服务器。

具体来说,数据拥有者输入公共参数pp、关键字$ck\in\{0,1\}^*$,自己的私钥SK_S和访问策略(W,t),其中$W=\{1,2,\cdots w\}$是访问集合,t是门限值。对于$j\in W$,随机选择一个整数$r_j\in\mathbb{Z}_p$,计算

$$C_{1,j}=H_1(ck)^{r_j s}\cdot H_2(j) \tag{3}$$

$$C_{2,j}=H_1(ck)\cdot H_2(j) \tag{4}$$

$$C_{3,j}=g^s\cdot g^{H_3(v)}\cdot(g^s)^{r_j} \tag{5}$$

最后,数据拥有者设定关键字密文$CT:=\{C_{1,j},C_{2,j},C_{3,j}\}_{j\in W}$,上传至云服务器。

3.5 陷门生成

陷门生成算法$\mathrm{Trapdoor}(pp,tk,PK_S,SK_R,R)$由数据用户调用,输入公共参数$pp$、待检索关键字$tk\in\{0,1\}^*$、数据发送者的公钥$PK_S$、数据用户的私钥$SK_R$和用户属性$R$,输出对应的检索陷门$TD$,上传至云服务器。具体来说,数据用户计算:

$$T_1=H_1(tk) \tag{6}$$

$$T_2=g^s \tag{7}$$

$$T_{3,j}=g^{\hat{v}_j},\ j\in R \tag{8}$$

最后,数据用户设定检索陷门为$TD:=(T_1,T_2,\{T_{3,j}\}_{j\in R})$。

3.6 密文检索

云服务器接收到公共参数pp、关键字密文CT、检索陷门TD、访问策略(W,t)和用户属性R,将其输入到密文检索算法$\mathrm{Search}(pp,CT,TD,R,(W,t))$中。如果$|R\cap W|<t$,云服务器返回表示$\perp$关键字密文和检索陷门不匹配。否则,云服务器选择子集$J\subseteq R\cap W$使得$|J|=t$,计算$T_{1,2}=e(T_1,T_2)$和$T_{1,3}=\prod_{j\in J}e(T_1,T_{3,j})^{L_j}$。对于$j\in J$,云服务器计算拉格朗日系数$L_j=\prod_{j\in J,j\neq i}\frac{-j}{i-j}$,并判断如下等式

$$T_{1,2}\cdot T_{1,3}\cdot e(C_{1,j},g)/e(T_1,C_{3,j})\stackrel{?}{=}e(C_{2,j},g) \tag{9}$$

如果对于任意的$j\in J$,等式两边均相等,则云服务器将关键字对应的云数据密文CT_M返回给数据用户,数据用户调用解密算法$ABE-\mathrm{Decrypt}(pp,CT_M,SK_R)$恢复云数据$M'$。

3.7 正确性分析

本文面向云数据访问控制的认证密文检索算法的正确性在于解密算法的正确性,当云服务器接收到ck对应的关键字密文$CT=\{C_{j,1},C_{j,2},C_{3,j}\}_{j\in W}$和$tk$对应的检索陷门$TD:=\left(T_1,T_2,\{T_{3,j}\}_{j\in R}\right)$后,若$ck=tk$,则有:

$$\begin{aligned}
&T_{1,2}\cdot T_{1,3}\cdot e(C_{1,j},g)/e(T_1,C_{3,j})\\
&=e(H_1(tk),g^s)\cdot\prod_{j\in J}e(H_1(tk),g^{\hat{v}_j})^{L_j}\cdot\\
&\quad e(H_1(ck)^{r_j s},g)\cdot e(H_2(j),g)/e(T_1,C_{3,j})\\
&=e(H_1(tk),g^s)\cdot e(H_1(tk),g)^{\sum_{j\in J}L_j\hat{v}_j}\cdot\\
&\quad e(H_1(ck)^{r_j s},g)\cdot e(H_2(j),g)/e\left(H_1(tk),g^{(s+H_3(v))+r_j s}\right)\\
&=e\left(H_1(tk),g^{s+H_3(v)}\right)\cdot e(H_1(ck)^{r_j s},g)\cdot
\end{aligned}$$

$$e(H_2(j),g)/e(H_1(tk),g)^{(s+H_3(v))+r_js}$$
$$=e(H_1(ck),g)^{(s+H_3(v))+r_js}\cdot e(H_2(j),g)/$$
$$e(H_1(ck),g)^{(s+H_3(v))+r_js}$$
$$=e(H_2(j),g) \quad (10)$$
$$e(C_{2,j},g)=e(H_2(j),g) \quad (11)$$

因此,本文构造的算法满足正确性。

3.8 安全性分析

定理:本文提出的 ABASE 方案能够抵御内部关键字猜测攻击。

证明:在密文计算算法中,关键字$ck\in\{0,1\}^*$通过哈希函数$H_1:\{0,1\}^*\to\mathbb{G}$和随机数$r_j\in\mathbb{Z}_p$被隐藏在$C_{1,j}$和$C_{2,j}$中,由于$H_1(ck)$和$H_2(j)$是群$\mathbb{G}$中的元素,且$r_j$是随机选择的,敌手无法从$C_{1,j}$和$C_{2,j}$中直接获取$ck$的信息。另外,在计算关键字密文时,数据拥有者需要输入自己的私钥$SK_S=s$,参与$C_{1,j}$的计算,即$C_{1,j}=H_1(ck)^{r_js}\cdot H_2(j)$。若敌手不知道$s$,则无法构造$H_1(ck)^{r_js}$。即使敌手是内部实体(如云服务器),也无法调用密文生成算法生成关键字密文。综上所述,内部敌手即使拥有陷门,因缺乏数据拥有者的私钥SK_S,无法得到关键字密文,故本文提出的 ABASE 方案可抵御内部关键字猜测攻击,证毕。

4 性能分析

从计算开销和存储开销的角度对提出的方案进行性能分析。本实验在搭载第 12 代 Intel Core i7−12800HX 处理器与 16 GB 内存的笔记本电脑上进行,所有方案均基于 Java JPBC 密码学库实现。通过控制变量法,分别对本文提出的 ABASE 方案与 MABKS 方案[24]、ABKSSM 方案[25]和 DSA 方案[26]的密文计算、陷门生成、密文检索算法的计算开销和用户私钥、关键字密文、检索陷门的通信开销进行对比分析,自变量分别设置为关键字数量(10~100)和属性数量(10~50),实验结果以秒(s)和千字节(KB)为单位。为了确保公平性,本文的测试过程保持一致的硬件配置与软件环境,选择 Type A 型曲线$y^2=x^3+x$,并且设置$|\mathbb{Z}_p|=1024$ bits,$|\mathbb{G}|=1024$ bits和$|\mathbb{G}_T|=1024$ bits。

4.1 计算开销分析

算法设计过程中所需要的基础知识如下。表 1 展示了 MABKS、ABKSSM、DSA 和 ABASE 的理论计算开销对比。考虑如下操作,T_H表示哈希操作时间,T_E表示群$\mathbb{G}$上的模幂操作时间,T_{ET}表示群$\mathbb{G}_T$上的模幂操作时间,T_P表示双线性配对操作时间。此外,r表示属性数量,r_i表示 ABKSSM 方案中每个属性授权中心所掌管的属性数量,d表示访问策略矩阵的行数,w表示访问集合中的元素数量,t表示子集$J=R\cap W$中的元素数量。

接下来,通过仿真这 4 个方案,对比了它们在密文计算、陷门生成和密文检索算法的计算开销。如图 2 所示,当关键字数量从 10 增至 100 时,MABKS 的计算时间从 20.6 s 增至 206.0 s,ABKSSM 的计算时间从 13.3 s 增至 133.0 s,DSA 的计算时间从 16.5 s 增至 165.0 s,而从 ABASE 的计算时间从 19.7 s 线性增长至 197.0 s。可见,面对关键字的增长,本文提出的 ABASE 在密文计算过程中避免了冗余的双线性配对操作,其计算开销相对于 MABKS 具有优势,但没有 ABKSSM 和 DSA 高效。图 3 展示了 4 个方案陷门生成算法的计算开销对比,由于减少了陷门生成算法中模幂运算次数,ABASE 的陷门生成时间始终低于另外 3 个方案,增长趋势平缓。同时,随着关键字数量的增加,另外 3 个方案陷门生成时间的增长速度远高于 ABASE。具体而言,当关键字数量为 100 时,ABASE 方案的陷门生成时间仅为另外 3 个方案的 76.19%、46.38% 和 18.82%。

表 1 理论计算开销

方案	密文计算算法	陷门生成算法	密文检索算法
MABKS[24]	$T_H+(4r+3)T_E+2T_{ET}+T_P$	$T_H+(2r+2)T_E$	$2T_P$
ABKSSM[25]	$T_H+\left(\sum_{i=1}^{n}r_i+r+2d+2\right)T_E+3T_{ET}$	$T_H+(2r+1)T_E$	$T_{ET}+(2r+1)T_P$
DSA[26]	$(d+6)T_H+(3d+5)T_E+2T_{ET}+2T_P$	T_H+10T_E	$3T_H+rT_{ET}+(2r+7)T_P$
ABASE	$(w+1)T_H+3wT_E$	T_H+rT_E	$tT_{ET}+(4t+1)T_P$

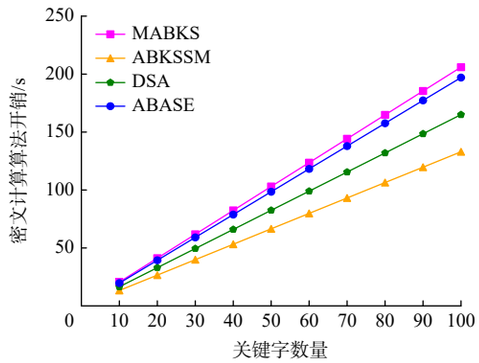

图 2 密文计算算法开销对比

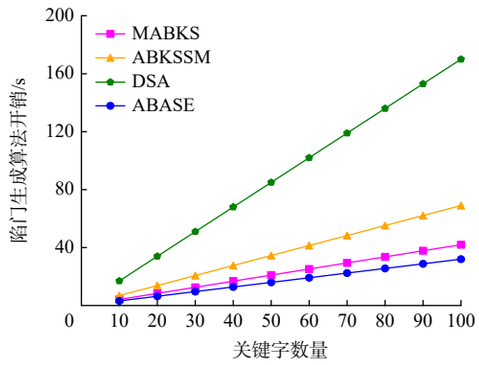

图 3 陷门生成算法开销对比

在密文检索算法中，如图 4 所示，4 个方案均呈现线性增长趋势。然而，由于 ABASE 在检索过程中所需的双线性配对操作的数量远高于 MABKS，所以 ABASE 呈现了较高的计算开销，但相对于 ABKSSM 和 DSA 具有较为明显的优势。具体而言，当关键字数量增加时，MABKS 的检索时间由 0.6 s 增至 6.0 s，ABKSSM 的检索时间由 6.6 s 增至 66.0 s，DSA 的检索时间由 8.7 s 增至 87.0 s，而 ABASE 的检索时间仅由 4.3 s 增至 43.0 s。

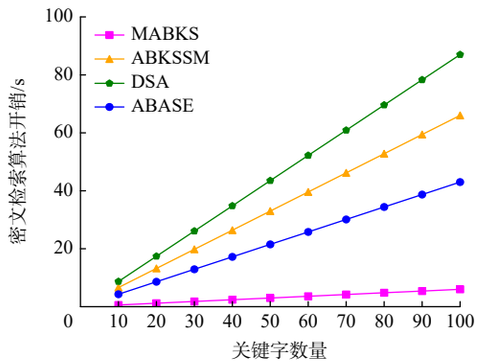

图 4 密文检索算法开销对比

4.2 存储开销分析

提出的 ABASE 方案和其他 3 个方案的理论存储开销对比如表 2 所示，其中$|\mathbb{G}|$、$|\mathbb{G}_T|$和$|\mathbb{Z}_p|$分别表示群$\mathbb{G}$、$\mathbb{G}_T$和$\mathbb{Z}_p$中的元素长度，λ表示字符串$\{0,1\}^{\lambda}$的长度。可见，ABASE 在用户私钥的存储开销显著低于其他 3 个方案。

表 2 理论存储开销

方案	用户私钥	关键字密文	检索陷门
MABKS[24]	$(3r+4)\|\mathbb{G}\|+3\|\mathbb{Z}_p\|$	$(3w+3)\|\mathbb{G}\|+2\|\mathbb{G}_T\|+w\|\mathbb{Z}_p\|$	$2\|\mathbb{G}\|$
ABKSSM[25]	$(2r+3)\|\mathbb{G}\|+\|\mathbb{Z}_p\|$	$\left(\sum_{i=1}^{n} r_i+r+d+2\right)\|\mathbb{G}\|+3\|\mathbb{G}_T\|+(r+2)\|\mathbb{Z}_p\|$	$(2r+1)\|\mathbb{G}\|+2\|\mathbb{Z}_p\|$
DSA[26]	$(r+4)\|\mathbb{G}\|+2\|\mathbb{Z}_p\|$	$(2d+4)\|\mathbb{G}\|+\|\mathbb{G}_T\|+\|\mathbb{Z}_p\|+4\lambda$	$6\|\mathbb{G}\|$
ABASE	$r\|\mathbb{Z}_p\|$	$3w\|\mathbb{G}\|$	$(r+2)\|\mathbb{G}\|$

对于方案的通信开销对比，如图 5 所示，相对于 MABKS、ABKSSM 和 DSA，ABASE 在用户私钥的通信开销方面具有显著的优势，从而印证了表 2 中所得到的结论。尤其是，当属性数量为 50 时，ABASE 的用户私钥大小仅为另外 3 个方案的 31.84%、48.08% 和 89.29%。图 6 展示了 4 个方案的关键字密文大小，可见 DSA 的密文大小与属性数量无关，ABASE 的密文大小随着属性数量的增加而线性增大，显著低于 MABKS 和 ABKSSM 方案的开销。对于检索陷门大

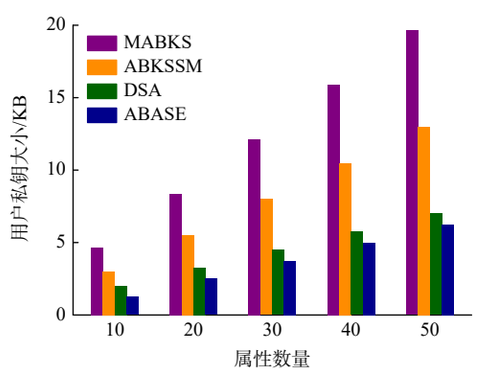

图 5 用户私钥大小对比

小,如图 7 所示,虽然 ABASE 方案的开销没有明显优势,但其具有关键字认证功能,可以抵御来自内部敌手的关键字猜测攻击,具有更高的安全性。

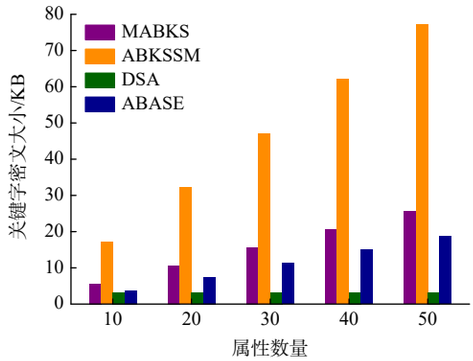

图 6 关键字密文大小对比

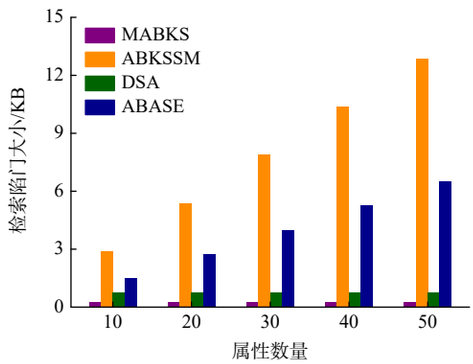

图 7 检索陷门大小对比

5 结论

提出了一种面向云数据访问控制的认证密文检索方案,有效解决了云存储环境下多用户安全检索的关键问题。通过将属性基加密与门限秘密共享技术相结合,构建了密文策略的细粒度访问控制机制,确保检索权限的精确管控。在关键字密文中嵌入数据所有者的私钥实现密文认证,从根本上阻断了云服务器发起内部关键字猜测攻击的途径。性能分析表明,本文提出方案的陷门生成算法相对于其他可搜索加密方案是高效的,同时具有较短的用户私钥大小,适用于云数据隐私保护。未来,本方案可进一步结合前向安全与后向安全机制以缓解密钥泄露问题,使得方案可以在保持密文检索效率的前提下,构建具有时序约束的动态访问控制体系,以适配更复杂的云存储需求。

参考文献(References)

[1] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328−1348.

[2] 张海阔, 陆忠华, 陈闻宇, 等. 基于隐私保护技术的DNS通信协议[J]. 科技导报, 2019, 37(8): 97−103.

[3] 苏璞睿, 冯登国. 2024年网络空间安全科技热点回眸[J]. 科技导报, 2025, 43(1): 102−117.

[4] 冯登国. 数据安全: 保障数据高效合理开发利用的基石[J]. 科技导报, 2021, 39(8): 1.

[5] 杨开兴, 满红任, 刘秀, 等. 基于边缘计算与区块链融合的智慧用电平台的研究与设计[J]. 科技导报, 2024, 42(9): 26−38.

[6] Chen X, Xu S Y, Gao S, et al. FS−LLRS: Lattice−based linkable ring signature with forward security for cloud−assisted electronic medical records[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 8875−8891.

[7] Cao Y B, Xu S Y, Chen X, et al. A forward−secure and efficient authentication protocol through lattice−based group signature in VANETs scenarios[J]. Computer Networks, 2022, 214: 109149.

[8] Chen X, Gao S, Xu S Y, et al. From Σ−protocol−based signatures to ring signatures: General construction and applications[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 3646−3661.

[9] Cao Y B, Chen X B, He Y F, et al. A post−quantum cross−domain authentication scheme based on multi−chain architecture[J]. Computers, Materials & Continua, 2024, 78(2): 2813−2827.

[10] Xu S Y, Chen X, Guo Y, et al. Efficient and secure post−quantum certificateless signcryption with linkability for IoMT[J]. IEEE Transactions on Information Forensics and Security, 2024, 20: 1119−1134.

[11] 肖人毅. 云计算中数据隐私保护研究进展[J]. 通信学报, 2014, 35(12): 168−177.

[12] Xu S Y, Cao Y B, Chen X, et al. Post−quantum searchable encryption supporting user−authorization for outsourced data management[C]//Proceedings of the 33rd ACM International Conference on Information and Knowledge Management. New York: ACM, 2024: 2702−2711.

[13] 秦志光, 徐骏, 聂旭云, 等. 公钥可搜索加密体制综述[J]. 信息安全学报, 2017, 2(3): 1−12.

[14] 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.

[15] Xu G, Xu S Y, Cao Y B, et al. AAQ−PEKS: An attribute−based anti−quantum PublicKey encryption scheme with keyword search for E−healthcare scenarios[J]. Peer−to−Peer Networking and Applications, 2025, 18(2): 64.

[16] Xu S Y, Chen X, Guo Y, et al. Lattice−based forward secure

multi-user authenticated searchable encryption for cloud storage systems[J]. IEEE Transactions on Computers, 2025, 74(5): 1663-1677.
[17] 刘源龙, 戴华, 李张晨, 等. 云环境中语义感知密文检索研究综述[J]. 计算机科学, 2024, 51(11): 298-306.
[18] 李颖, 马春光. 可搜索加密研究进展综述[J]. 网络与信息安全学报, 2018, 4(7): 13-21.
[19] 衡星辰, 普钢, 李零, 等. 运行于边侧物联网设备的区块链轻型应用研究与实现[J]. 科技导报, 2024, 42(9): 60-66.
[20] 李申章, 杨铮宇, 李力, 等. 云边协同与区块链融合架构研究与设计[J]. 科技导报, 2024, 42(9): 39-50.
[21] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[M]//Advances in Cryptology-EUROCRYPT 2004. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 506-522.
[22] Zheng Q J, Xu S H, Ateniese G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data[C]//Proceedings of IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Piscataway, NJ: IEEE, 2014: 522-530.
[23] Yu Y, Shi J B, Li H L, et al. Key-policy attribute-based encryption with keyword search in virtualized environments [J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6): 1242-1251.
[24] Miao Y B, Deng R H, Liu X M, et al. Multi-authority attribute-based keyword search over encrypted cloud data[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 1667-1680.
[25] Miao Y B, Liu X M, Choo K R, et al. Privacy-preserving attribute-based keyword search in shared multi-owner setting[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1080-1094.
[26] Yang K, Shu J G, Xie R T. Efficient and provably secure data selective sharing and acquisition in cloud-based systems[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 71-84.
[27] 李红, 汪学明. 支持策略检索的属性基可搜索加密方案[J]. 计算机工程与设计, 2024, 45(11): 3209-3215.
[28] 刘晨旭, 曹素珍, 刘静洁, 等. 策略隐藏的可撤销属性基可搜索加密方案[J/OL]. 计算机工程, (2024-12-13). [2025-04-29]. https://doi.org/10.19678/j.issn.1000-3428.0069806.
[29] 张克君, 王文彬, 徐少飞, 等. 面向云存储且支持重加密的多关键词属性基可搜索加密方案[J]. 通信学报, 2024, 45(9): 244-257.
[30] 郭瑞, 杨鑫, 贾晨阳, 等. 云辅助医疗物联网中支持策略隐藏的可搜索属性加密方案[J]. 密码学报(中英文), 2025, 12(1): 49-68.
[31] Byun J W, Rhee H S, Park H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[M]//Secure Data Management. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 75-83.
[32] Huang Q, Li H B. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks[J]. Information Sciences, 2017, 403: 1-14.
[33] 张玉磊, 文龙, 王浩浩, 等. 多用户环境下无证书认证可搜索加密方案[J]. 电子与信息学报, 2020, 42(5): 1094-1101.
[34] 胡震宇, 邓伦治, 高岩, 等. 一个指定验证者的基于身份可搜索认证加密方案[J]. 贵州师范大学学报(自然科学版), 2022, 40(3): 56-63, 101.
[35] 刘永志, 秦桂云, 刘蓬涛, 等. 可证明安全的基于SGX的公钥认证可搜索加密方案[J]. 计算机研究与发展, 2023, 60(12): 2709-2724.
[36] 肖心雨, 李高燕, 孙文涛, 等. 一种陷门随机生成的公钥认证可搜索加密方案[J]. 智能计算机与应用, 2024, 14(7): 136-139.
[37] Xu S Y, Cao Y B, Chen X, et al. Post-quantum public-key authenticated searchable encryption with forward security: General construction, and applications[M]//Information Security and Cryptology. Singapore: Springer Nature Singapore, 2024: 274-298.
[38] 蒲浪, 林超, 伍玮, 等. 基于国密SM9的公钥认证可搜索加密方案[J/OL]. 软件学报, (2024-12-12)[2025-04-29]. https://doi.org/10.13328/j.cnki.jos.007271.

An authenticated ciphertext retrieval scheme for cloud data access control

CAO Yibo[1], XU Shiyuan[2], CHEN Xue[2], XI Yuxin[3], GUO Yu[3*]

1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Department of Computer Science, The University of Hong Kong, Hong Kong 999077, China
3. School of Artificial Intelligence, Beijing Normal University, Beijing 100875, China

Abstract Searchable encryption is a key technology for enabling data encrypted search, and it has significant application value for cloud storage. However, existing schemes generally adopt a single−user model and are vulnerable to insider keyword guessing attacks, which exposes cloud data to the risk of privacy leakage. Therefore, there is an urgent need to design a searchable encryption scheme that support multi−user models and provide higher security to meet the privacy−preserving of cloud data. In response, this paper proposes an authenticated ciphertext retrieval scheme for cloud data access control. In terms of access control, the scheme embeds attributes into users' secret key to generate search trapdoor and incorporates access policies into the keyword ciphertext. The matching of attributes and access policies is achieved through threshold secret sharing techniques, thus establishing a fine−grained retrieval permission control mechanism. To enhance security, the secret key of the data owner is embedded into the keyword ciphertext to provide ciphertext authentication, effectively preventing insider keyword guessing attacks. Performance analysis shows that the trapdoor generation algorithm in our proposed scheme are computationally efficient, while the user secret key has relatively low storage overhead, making our scheme suitable for cloud storage applications.

Keywords cloud storage; privacy preserving; ciphertext retrieval; access control

（责任编辑 王微）