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

张克君[1,2,3]，王文彬[1]，徐少飞[2]，于新颖[1]，王钧[2]，李鹏程[3]，钱榕[2]
（1.北京邮电大学网络空间安全学院，北京 100876；2.北京电子科技学院网络空间安全系，北京 100071；
3.中国科学技术大学网络空间安全学院，安徽 合肥 230026）

摘　要：针对一对多模型下共享数据细粒度访问控制、密文密钥的安全共享和更新等问题，提出了一种面向云存储且支持代理重加密的多关键词属性基可搜索加密方案。增加节点信息改进访问树结构，实现对密文数据读写权限的细粒度访问控制；对查询关键词进行属性基加密优化处理，实现陷门信息不可区分性和限制不同用户的检索能力；利用重加密方法更新密文及密钥，解决已撤销用户恶意访问隐私数据带来的系统安全问题；设计了一种基于区块链的安全性验证算法来识别第三方托管隐私数据被攻击篡改的问题。基于DBDH困难问题和DDH困难问题，推理证明了所提方案能够满足自适应关键词密文安全和陷门安全。实验结果表明，该方案在密钥生成、陷门生成、关键词索引生成和正确性验证阶段能够保证隐私数据及密钥安全，同时相比于同类方案，在时间开销方面具有更高效率。

关键词：可搜索加密；属性基加密；读/写节点；代理重加密；访问控制
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024150

Multi-keyword attribute-based searchable encryption scheme supporting re-encryption for cloud storage

ZHANG Kejun[1,2,3], WANG Wenbin[1], XU Shaofei[2], YU Xinying[1], WANG Jun[2],
LI Pengcheng[3], QIAN Rong[2]
1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100071, China
3. School of Cyberspace Security, University of Science and Technology of China, Hefei 230026, China

Abstract: To address fine-grained access control, secure sharing, and encrypted key updates in a one-to-many model, a multi-keyword attribute-based searchable encryption scheme with proxy re-encryption for cloud storage was proposed. The access tree was enhanced with node information for fine-grained control over ciphertext read and write permissions. The keyword encryption process was optimized for trapdoor indistinguishability and restricted user search capabilities. Re-encryption updated ciphertext and keys, preventing malicious access by revoked users. A blockchain-based verification algorithm was designed to detect tampering of third-party data. The DBDH and DDH hard problems proved the scheme's keyword ciphertext security and trapdoor security. Experiments show the proposed scheme secures data and keys during key generation, trapdoor, and index generation, and correctness verification. It also demonstrates higher efficiency in time overhead, ensuring privacy and key safety while maintaining high efficiency.

Keywords: searchable encryption, attribute-based encryption, read/write node, proxy re-encryption, access control

收稿日期：2023–11–01；修回日期：2024–02–02
通信作者：王文彬，20212923@mail.besti.edu.cn
基金项目：中央高校基本科研业务费资金资助项目（No.3282023033）；北京高校“高精尖”学科建设基金资助项目（No.20210086Z0401）
Foundation Items: The Fundamental Research Funds for the Central Universities (No.3282023033), Advanced Discipline Construction Project of Beijing Universities (No.20210086Z0401)

0　引言

随着云存储外包服务的日益普及，越来越多的个人隐私和政企敏感数据被存储至云服务器，这不仅能够解决本地存储资源和计算资源匮乏问题，而且方便用户在多个终端中灵活使用和共享访问数据。然而，数据持有者将数据的管理权完全授予云服务器后，数据的安全性将无法保证。为了保证隐私数据安全，提出密文托管方案，但用户对密文的检索利用变得困难，可搜索加密技术[1]应运而生。

Song 等[1]基于对称加密算法首次提出可搜索加密方案，解决加密数据的有效检索问题，但该方案仅支持单关键词检索并且检索效率较低。Boneh 等[2]首次实现适用于邮件路由系统的公钥可搜索加密方案，并在 bilinear Diffie-Hellman 困难问题下证明了方案的安全性，但该方案计算开销大，效率低，不适用于大批量隐私数据的检索查询，并且陷门生成算法不满足陷门不可区分要求，因此无法抵抗关键词猜测攻击。Rhee 等[3]在上述方案的基础上提出了基于关键词搜索的公钥可搜索加密方案，该方案使用关键词检索并引入指定服务器来增强模型的安全性。以上方案均采用单关键词的检索方式，并且用户的数据检索能力覆盖了云服务器中的全部隐私数据，这将导致网络带宽和计算资源的浪费。Golle 等[4]为了解决单关键词检索机制带来的效率问题，提出了支持连接关键词搜索的可搜索加密方案，但该方案使用固定网络开销优化检索效率，不再适用于当前网络环境。Li 等[5]引入相似度和首选项的概念，实现了基于连接词的多功能关键词可搜索加密方案，该方案在检索结果正确性和效率等方面取得了重要成果。

文献[1-5]在一定程度上解决了单关键词导致的检索效率问题，但数据持有者在实施对隐私数据的细粒度访问控制方面存在一定的困难。因此，研究人员广泛关注将属性策略融入加密方案，以实现对隐私数据的细粒度访问控制技术。Sahai 等[6]首次将属性应用到隐私数据共享方案中，提出了基于属性的加密（ABE, attribute-based encryption）方案，该方案中数据持有者利用布尔表达式制定隐私数据的访问控制策略，只有拥有访问策略的用户才能够解密相关密文。基于属性的加密方案主要分为 2 种，分别为基于密钥策略的属性加密方案（KP-ABE, key-policy attribute-based encryption）和基于密文策略的属性加密方案（CP-ABE, ciphertext-policy attribute-based encryption）。CP-ABE 方案中，访问策略与密文数据相关联，数据持有者通过设置访问策略对隐私数据进行加密，生成与访问策略相关联的用户密钥。Waters 等[7]基于线性秘密共享矩阵（LSSS, linear secret sharing scheme），提出了一种 CP-ABE 方案，该方案中基于 LSSS 访问结构既可以实现“与”和“或”的操作，同时也可以实现门限操作，使得方案更加灵活。高诗尧等[8]和 Sravanthi 等[9]基于属性加密算法与可搜索加密进行结合，在医疗数据领域解决了患者隐私数据细粒度访问控制的问题。Li 等[10]提出了多授权机构属性加密的概念，该方案主要解决了数据删除操作的验证问题。但以上方案均未解决访问结构未隐藏的问题，攻击者可以通过访问结构推断出用户的隐私信息。为了防止访问结构泄露导致的个人隐私安全问题，Nishide 等[11]首次提出了部分隐藏访问结构的属性基加密方案。文献[12-15]也提出了几种支持隐藏访问结构的 CP-ABE 方案，其中，文献[14]的方案能够有效避免用户的隐私信息被泄露给其他第三方。基于大用户群体下的属性基数据共享方案中，为了解决已撤销用户对系统的恶意访问问题，Yu 等[16]提出沿用外包来解决属性撤销问题；Wang 等[17]提出一种支持用户撤销的属性基密文共享方案，该方案采用版本控制的方式来实现属性撤销；Sultan 等[18]和 Luo 等[19]等设计实现了支持用户和属性的动态撤销的属性更新策略，保证当某个用户或属性被撤销后，不影响其他用户的访问权限。在基于物联网的医疗保健系统中，Das 等[20]提出了一种支持属性撤销的细粒度访问控制方案，该方案能够减少传统 CP-ABE 方案中使用单个权限的工作开销。

以上方案均未解决任意用户在访问云服务器所带来的身份验证问题，区块链技术能够为系统提供平台支撑，生成不可更改且可追踪的记录，使数据持有者和用户能够安全地使用和共享数据。文献[21]从系统设计的角度介绍了当前区块链存在的安全问题以及发展前景。Li 等[22]基于区块链提出了一种与可搜索加密相结合的方案，该方案使用区块链保证用户公平并且可减少用户计算量。Lu 等[23]和 Wu 等[24]基于区块链可追踪的特点，提出了

一种针对隐私泄露和密钥滥用问题的属性基可搜索加密方案，该方案确保数据持有者和用户的数据在传递过程中的完整和不可篡改。牛淑芬等[25]基于区块链提出一种属性基可搜索加密方案，该方案利用区块链技术保证用户和云服务器之间的公平性，设计用户与区块链多次交易获取正确检索结果。但方案基于单关键词进行设计，检索效率较低。Zheng等[26]基于属性加密算法设计并验证了云服务器是否按照用户需求安全运行检索算法，但该方案未对各个实体的行为进行监督，存在安全风险。闫玺玺等[27]在保证用户隐私数据安全的基础上，利用区块链验证检索数据正确性，减少用户计算开销，但该方案对用户检索能力未进行限制，用户仍旧对云服务器中所有与检索关键词有关的隐私数据具有检索能力。Hu等[28]提出一种支持代理重加密的属性基可搜索加密方案，实现了离线用户可授权检索权限给其他用户，从而对关键词和密文进行有效共享，但该方案基于单关键词进行设计，并且不能验证检索结果的正确性。

聚焦构建细粒度访问控制需求的可搜索加密机制，本文主要工作如下。

1) 本文将属性加密技术与可搜索加密技术相结合，设计了一个基于密文策略的多关键词属性基可搜索加密方案，并基于安全模型进行验证，证明其安全性。

2) 基于属性的加密技术在构造访问结构中不能进一步对加密数据的读/写状态进行控制，针对这一问题，本文对访问结构进行改造，通过在访问结构中增加读/写节点实现对用户访问请求的控制。

3) 为了防止系统已撤销用户再次使用授予密钥对加密数据进行检索，本文引用代理重加密的思想，在加密文件密钥过程和用户访问密钥生成过程中融入重加密密钥，对加密文件密钥以及访问密钥进行更新。

4) 为了检测隐私数据在传输过程和存储阶段是否存在恶意篡改问题，本文利用区块链去中心化、不可篡改、可验证及可追踪的特性，将区块链技术应用于该方案。本文设计一系列安全验证算法，将加密关键词密文索引结构和密文消息验证码存储在区块链上，为用户提供查询服务和数据正确性验证服务。

1 相关知识

1.1 双线性映射

令G_1和G_2为阶是素数p的乘法循环群，定义一个双线性映射$e:G_1 \times G_1 \to G_2$满足如下性质。

1）双线性。对任意的$u,v \in G_1$，存储$a,b \in Z_p^*$，使得$e\left(u^a,v^b\right)=e(u,v)^{ab}$。

2）非退化性。存在$u,v \in G_1$，使得$e\left(u,v\right) \neq 1$。

3）可计算性。对任意的$u,v \in G_1$，存在有效算法计算$u,v \in G_1$。

1.2 困难问题

定义1 判定性双线性DBDH假设。假设G_1和G_2是阶为素数p的循环群,$e:G_1 \times G_1 \to G_2$为一个双线性映射，g为G_1的生成元，给定2个元组$(g,g^a,g^b,g^c,e(g,g)^{abc})$和$(g,g^a,g^b,g^c,e(g,g)^z)$。对随机的$a,b,c,z \in Z_q^*$，不存在概率多项式时间攻击者以不可忽略的优势区分$(g,g^a,g^b,g^c,e(g,g)^{abc})$和$(g,g^a,g^b,g^c,e(g,g)^z)$。

定义2 判定性Diffie-Hellman（decisional Diffie-Hellman, DDH）假设。g为G_1的生成元，给定2个三元组$\left(g^a,g^b,g^z\right)$和$\left(g^a,g^b,g^{ab}\right)$，对随机的$a,b,z \in Z_q^*$，不存在概率多项式时间攻击者以不可忽略的优势区分$\left(g^a,g^b,g^z\right)$和$\left(g^a,g^b,g^{ab}\right)$。

1.3 访问结构

一个实体集$I=\left\{I_1,I_2,\cdots,I_n\right\}$，对于集合$A \in 2^I$是$2^I$上的一个非空子集。$\forall B,C$，如果$B \in A$且$B \subseteq C$时，则有$C \in A$，那么称集合$A \in 2^I$是单调的，一个访问结构$A$是$I=\left\{I_1,I_2,\cdots,I_n\right\}$的一个非空子集合，即$A \subseteq 2^I \backslash \{\phi\}$。包含于$A$中的集合称为授权集合，而不包含在$A$中的集合称为非授权集合。只有得到授权的用户密钥才可以解密密文。

1.4 访问树

Γ表示一个访问树，其中Γ的每个非叶子节点X都可以代表一个关系函数，关系函数可以是AND$(n \text{ of } n)$、OR$(1 \text{ of } n)$和$n \text{ of } m(m>n)$门限等。Γ中叶子节点x用来描述属性。

2 算法与安全模型定义

2.1 系统模型

围绕隐私数据第三方安全托管需求，本文设计了面向云储存支持重加密的多关键词属性基可搜索加密

方案。在一对多检索场景下，重点解决了隐私数据细粒度访问控制中用户检索能力、访问权限规范不足问题和识别隐私数据被攻击篡改的问题。方案主要包含数据持有者（DO, data owner）、数据用户（DU, data user）、云服务器、区块链、可信的属性授权中心5个实体。实体间交互协作的系统模型如图1所示。

1) 属性授权中心。其功能主要是为系统各实体生成参数，并为系统内所有用户进行注册生成授权密钥。

2) 数据持有者。数据持有者使用密钥生成算法生成文件加密密钥K_f，使用关键词提取算法形成关键词索引CI，并使用相应的访问策略对关键词索引CI以及文件加密密钥K_f进行加密，将加密密钥密文随密文文件集$C=\{C_1,C_2,\cdots,C_n\}$一同上传至云服务器，将加密索引嵌入交易并上传至区块链，构成新区块并进行广播。

3) 数据用户。数据用户使用其授权查询密钥及查询关键词生成检索陷门，以加密陷门的形式构成交易上传至智能合约。通过智能合约进行检索，若检索正确，返回相应数据密文地址传输至云服务器，服务器依据地址进行数据验证，验证通过，则查询对应的数据密文，服务器将数据密文和文件加密密钥密文返回给用户。数据用户通过向属性授权中心申请数据持有者授权的访问密钥，从而对数据密文解密后进行读/写操作。

4) 云服务器。云服务器为系统内所有用户提供数据存储服务。云服务器存储数据持有者上传的数据密文文件和加密密钥密文。当用户通过陷门查询成功得到存储在云服务器上的密文数据地址后，向云服务器发出请求，云服务器根据地址为用户返回相应的数据密文和加密密钥密文。

5) 区块链。区块链为数据持有者提供存储服务，同时智能合约为用户提供数据检索服务。数据持有者将关键词索引密文和密文消息验证码存储在链上，利用智能合约技术，检索节点自动执行合约函数，并依托其不可篡改等特性，确保各实体间诚实地执行安全交易协议。

2.2　形式化定义

本文提出的方案包括以下8个概率多项式时间算法。

1) 系统初始化算法

$\text{Setup}\left(1^l\right)\rightarrow \text{PK,MK,RK}$。该算法由属性授权中心执行。输入安全参数$\lambda$，输出公开参数PK，主密钥MK，重加密密钥RK。

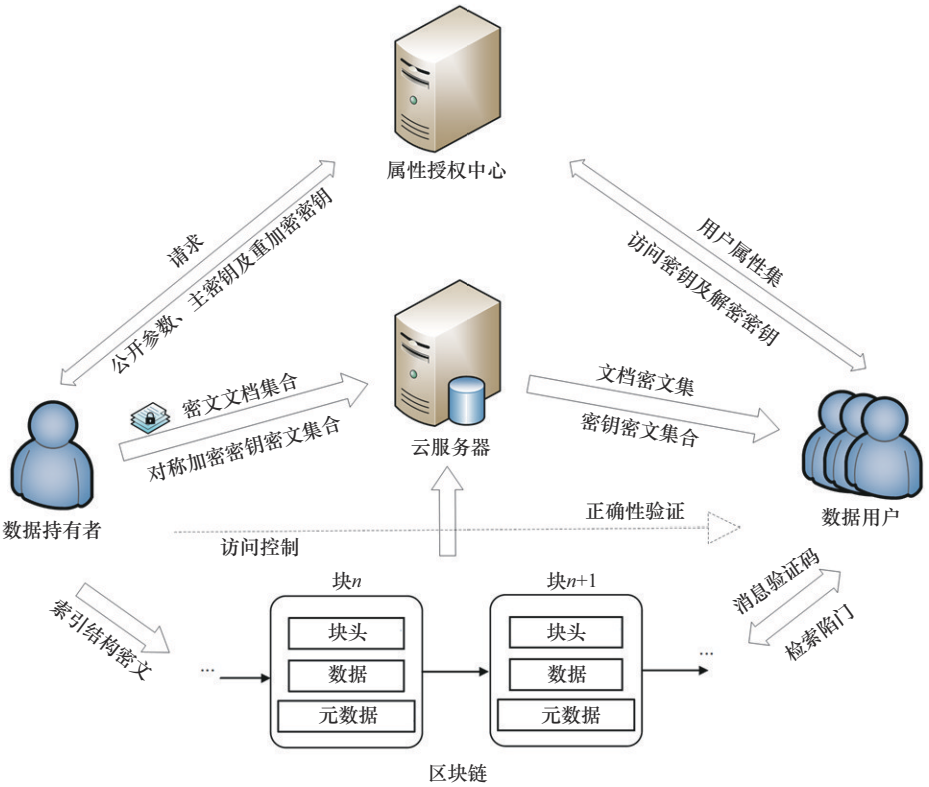


图1　系统模型

2) 密钥生成算法

$\mathrm{KeyGen}(\mathrm{PK},\mathrm{MK},\mathrm{RK},S_{\mathrm{uid}}) \to \mathrm{SK}_u,\mathrm{SK}_s$。该算法由属性授权中心执行，DO输入公开参数PK、系统主密钥MK、重加密密钥RK以及用户属性集合S_{uid}，输出用户授权查询密钥SK_s和用户授权访问密钥SK_u。

3) 加密算法

$\mathrm{Encrypt}(\Gamma,\mathrm{PK},F,W,\mathrm{FK},\mathrm{RK}) \to \mathrm{CI}_w,\mathrm{CF}_i,\mathrm{CK},\mathrm{MAC}_i$。该算法由DO执行，数据持有者输入访问策略$\Gamma$、公开参数PK、明文数据集合$F$、关键词集合$W$、加密密钥FK、重加密密钥RK，输出安全索引$\mathrm{CI}_w$、密文数据集合$\mathrm{CF}_i$、加密密钥密文CK以及数据消息验证码$\mathrm{MAC}_i$。数据持有者将密文数据集合$\mathrm{CF}_i$和加密密钥密文CK上传至云服务器，将安全索引$\mathrm{CI}_w$和消息验证码$\mathrm{MAC}_i$发送至区块链。

4) 陷门生成算法

$\mathrm{TrapdoorGen}(\mathrm{PK},\mathrm{SK}_s,W) \to T_w$。该算法由数据用户执行，数据用户输入公开参数PK、用户授权查询密钥SK_s以及查询的关键词集合W，输出用户查询陷门T_w，数据用户将生成的陷门发送给查询合约函数。

5) 检索算法

$\mathrm{Search}(\mathrm{PK},\mathrm{CI}_w,T_w) \to \mathrm{ID}_f,\mathrm{MAC}_f$。该算法由智能合约执行，智能合约输入公开参数PK、安全索引CI_w以及查询陷门T_w，输出包含有查询关键词的密文数据标识符集合ID_f和消息验证码集合MAC_f。

6) 验证算法

$\mathrm{Verify}(\mathrm{ID}_f,\mathrm{CF},\mathrm{MAC}_f) \to \mathrm{CF}_i,\mathrm{CK}$。该算法由云服务器和数据用户执行，云服务器将检索结果返回给数据用户，数据用户验证查询合约结果，输入查询密文数据标识符ID_f、密文数据集合CF、消息验证码集合MAC_f。若验证成功，输出正确的包含有查询关键词的密文数据集CF_i和密文数据密钥的密文CK。

7) 解密算法

$\mathrm{Dec}(\mathrm{SK}_u,\mathrm{CK},\mathrm{CF}_i) \to F_i$。该算法由数据用户执行，数据用户输入授权访问密钥$\mathrm{SK}_u$，包含有查询关键词的密文数据集$\mathrm{CF}_i$和加密密钥密文CK，如果用户授权访问密钥满足DO定义的访问策略，则可以恢复出对称加密密钥FK，解密密文文档集合CF_i，输出包含有查询关键词的明文数据集合F_i。

8) 密文属性更新算法

$\mathrm{CTUpdate}(\mathrm{CK},\mathrm{RK},\mathrm{SK}_u,\mathrm{Ver}^k) \to \mathrm{CK}^{k+1},\mathrm{SK}_u^{vk+1}$。该算法由云服务器和属性授权中心执行，输入当前版本的加密密钥密文CK和重加密密钥RK、用户授权访问密钥SK_u，输出更新版本后的加密密钥密文CK^{k+1}以及用户授权访问密钥SK_u^{k+1}。

2.3 安全模型

本文基于在概率多项式时间攻击者A和挑战者B的挑战方案定义本文方案在选择明文攻击下具备关键词不可区分性安全和陷门不可区分性安全。

挑战I 关键词不可区分性。

初始阶段。挑战者B运行系统初始化算法，生成公开参数，攻击者A运行访问树构造算法，定义一个访问树Γ^*。

阶段1。该阶段中，攻击者A进行以下多项式数量下的自适应询问。

1) 查询密钥生成询问。攻击者A自适应地向挑战者B发起对属性集的询问。

2) 关键词密文询问。攻击者A自适应地向挑战者B发起对应关键词密文的请求，在该过程中攻击者A向挑战者B发起询问得到的授权查询密钥SK_s都不满足设定的访问树Γ^*。

挑战。攻击者A向挑战者B提交2个关键词w_0,w_1，挑战者B随机选取$\mu \in \{0,1\}$，并且加密关键词得到关键词密文索引CI_w返回给攻击者A。

阶段2。攻击者A自适应地向挑战者B发起对属性集的询问，询问得到的查询密钥SK_s均不满足访问树。

猜测。攻击者A输出$\mu' \in \{0,1\}$，若$\mu' = \mu$，则攻击者A赢得挑战。

攻击者A挑战成功的概率被定义为$\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda) = \left| \Pr[\mu' = \mu] - \frac{1}{2} \right|$。

假设在该多项式时间内的攻击者A赢得挑战的概率$\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)$可忽略，则描述该方案满足关键词密文不可区分性。

挑战II 陷门不可区分性。

假设A是一个企图攻破陷门不可区分性安全的概率多项式时间攻击者，挑战者B通过设计建立算

法解决 DDH 问题，挑战者 B 获得参数 Para = $(G_1,G_2,e,p,g,a,b,g^{ab})$。

初始阶段。挑战者 B 运行系统初始化算法输出公共参数。

阶段 1。该阶段中，攻击者 A 进行以下多项式数量下的自适应询问。

1) 查询密钥生成询问。挑战者 B 运行密钥生成算法计算用户授权密钥，返回给攻击者 A。

2) 陷门询问。计算一个给定关键词 w，计算相应关键词的陷门 T_w，并将其返回给攻击者 A。

挑战。攻击者 A 向挑战者 B 提交 2 个挑战关键词 w_0,w_1，挑战者 B 随机选取 $\mu \in \{0,1\}$，基于关键词 w_μ 生成陷门 T_μ，将其返回给攻击者 A。

阶段 2。攻击者 A 仍旧发起查询密钥生成询问和陷门询问，但不能询问与挑战关键词相关的信息。

猜测。攻击者 A 输出 $\mu' \in \{0,1\}$，若 $\mu' = \mu$，则攻击者 A 赢得挑战。

攻击者 A 成功挑战的概率被定义为 $\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda) = \left| \Pr[\mu' = \mu] - \frac{1}{2} \right|$。

若对于在该多项式时间内的攻击者 A，赢得挑战的概率 $\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)$ 可忽略，则描述该方案满足陷门不可区分性。

3　方案构造

面向云存储且支持用户撤销的多关键词属性基可搜索加密方案可以分为 5 个阶段：系统建立、数据加密、数据检索、数据解密和用户撤销及密钥更新。

3.1　系统建立

本阶段包括系统初始化和密钥生成 2 个部分。

系统初始化。$\mathrm{Setup}(1^\lambda) \to \mathrm{PK,MK,RK}$。属性授权中心 AA 执行该算法，输入安全参数 λ，生成系统公开参数 PK、主密钥 MK 和重加密密钥 RK。

1) 定义一个双线性映射 $e: G_1 \times G_1 \to G_2$，其中 G_1 和 G_2 是以素数 p 为阶的循环乘法群，g 是 G_1 的生成元。

2) 定义 2 个抗碰撞 Hash 函数。$H: \{0,1\}^* \to G_1, H_1: \{0,1\}^* \to G_1$。

3) 随机选择 $\alpha,\beta \in Z_q^*$，输出公开参数 $\mathrm{PK} = \left(G_1,G_2,g,h = g^\beta,e(g,g)^\alpha\right)$，系统主密钥 $\mathrm{MK} = (\alpha,\beta)$。

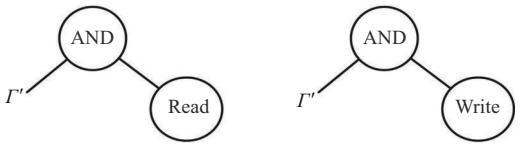
4) 在预设重加密密钥版本号最大值为 m 的范围内，对第 i 个版本 Ver^i，其中 $1 \leqslant i \leqslant m$，随机选择随机数 $\mathrm{rk}_i \in Z_q^*$，生成重加密密钥。

密钥生成。$\mathrm{KeyGen}(\mathrm{PK,MK,RK},S_{\mathrm{uid}}) \to \mathrm{SK}_u,\mathrm{SK}_s$。属性授权中心执行该算法，为用户产生授权查询密钥 SK_s 和授权访问密钥 SK_u。随机选择 $r \in Z_q^*$，对属性集中每个属性 $j \in S_{\mathrm{uid}}$，随机选择 $r_j \in Z_q^*$，计算得到用户访问密钥 $\mathrm{SK}_u = \left\{ D = g^{\frac{\alpha + r + \mathrm{rk}^i}{\beta}}, \forall \mathrm{att} \in S_{\mathrm{uid}}: D_{\mathrm{att}} = g^{r+\mathrm{rk}^i} H_1(\mathrm{att})^{r_j \mathrm{rk}_j^i}, D_j' = g^{r_j} \right\}$ 和用户查询密钥 $\mathrm{SK}_S = \left\{ D = g^{\frac{\alpha + r}{\beta}}, \forall \mathrm{att} \in S_{\mathrm{uid}}: D_{\mathrm{att}} = g^r H_1(\mathrm{att})^{r_j}, D_j' = g^{r_j} \right\}$。属性授权中心 AA 为数据用户颁发授权查询密钥 SK_s 和授权访问密钥 SK_u。

3.2　数据加密

本阶段可划分为访问树构建、索引生成、文档加密和密钥加密 4 个部分。

1) 访问树构建。数据持有者在加密文档密钥前首先要按照以下规则构建访问树 Γ'。首先对访问树 Γ' 中每一个节点 x，从根节点 root 开始选择一个阶为 d_x 的多项式 q_x，令 k_x 表示为节点 x 的门限值，定义 $d_x = k_x - 1$，从 Γ' 根节点 root 开始，DO 随机选择 $s \in Z_q^*$，并定义 $q_{\mathrm{root}}(0) = s$，接着选取 d_{root} 个随机系数来确定多项式 q_{root}。对其他节点 x，定义 $q_{\mathrm{root}}(0) = q_{\mathrm{parent}(x)}(\mathrm{index}(x))$，并随机选择 d_x 个点定义多项式 q_x，完成对访问树 Γ' 的建立。本文方案通过增加读/写节点进一步控制 DU 对检索密文的读写请求，定义 DO 构建的访问树为 Γ'，将关系函数 AND 定义为完整访问树 Γ 的根节点，Γ' 设置为 Γ 的左子树，将用户的读写请求分为 Read 和 Write 节点，设置为根节点的叶子节点，读写权限访问树如图 2 所示。



(a) 读权限访问树　　(b) 写权限访问树

图 2　访问树构建

2) 索引生成。$\mathrm{IndexGen}(\Gamma',W,\mathrm{PK}) \to \mathrm{CI}_w$。数据持有者对于每一个明文文档$f \in F$提取关键词集合$W$，建立一个大小为$m \times n$的二维数组$\mathrm{DB}[H(w_i)][j]$，若第$j$个文档包含有关键词$w_i$，则令$\mathrm{DB}[H(w_i)][j]=1$，否则为0。数据持有者在完成访问树$\Gamma'$的构造后，令$X$为$\Gamma$中叶子节点集合，最后将关键词进行加密并生成索引为$\mathrm{CI}_w = \{\Gamma',\tilde{C}_{w_i} = H(w_i)e(g,g)^{\alpha s},i \in [1,m],C_w' = g^{\beta s},\{C_x = g^{q_x(0)},C_x' = H_1(\mathrm{att}(x))^{q_x(0)}\}_{\forall x \in X}\}$，DO将$\mathrm{CI}_w$通过形成交易$T_x$发送给区块链，调用智能合约中的索引添加函数addIndex()存储安全索引。智能合约中定义一个二维查找表，允许快速定位与关键词有关的密文信息。其中，二维查找表中每一维度的一对键值<$\tilde{C}_{w_i}$,value>由一个关键词密文和一个与关键词有关的密文文件0/1检索符构成。当确定一个$\tilde{C}_{w_i}$，能够快速返回检索符value用于确认当前密文是否包含该关键词。

3) 文档加密。$\mathrm{FileEnc}(F,\mathrm{FK}) \to \mathrm{CF}_i$。数据持有者随机生成$\mathrm{FK} \leftarrow \{0,1\}^k$作为加密明文文档集合的对称加密密钥。假设明文文档集合上限为n，DO使用$\mathrm{FK} \leftarrow \{0,1\}^k$加密明文文档$F_i(i \in [1,n])$，得到$\mathrm{CF}_i = \{\xi.\mathrm{Enc}(F_i)|i \in [1,n]\}$，其中，$\xi$.Enc算法表示安全的对称加密算法，例如AES加密算法。

4) 密钥加密。$\mathrm{KeyEnc}(\Gamma,\mathrm{FK},\mathrm{RK},\mathrm{PK}) \to \mathrm{CK}$。当数据持有者完成对访问树的构建后，令$Y$为$\Gamma$中叶子节点集合，DO计算得到加密密钥密文$\mathrm{CK} = \{\Gamma,\tilde{C}=(\mathrm{FK}\|\delta_{\mathrm{DO1}}/*)e(g,g)^{\alpha s},C=h^s,\{C_y = g^{q_y(0)},C_y' = H_1(\mathrm{att}(y))^{q_y(0)\mathrm{rk}_y^i}\}_{\forall y \in Y}\}$。对于允许用户执行写操作的文件加密密钥，DO在加密密钥末尾添加数据持有者数字签名δ_{DO1}，该签名作为数据用户在执行写操作时验证。对于只允许用户执行读操作的文件加密密钥，DO在加密密钥末尾添加*，定义为无写权限。

5) 消息验证码生成。$\mathrm{MacGen}(\mathrm{CF}_i,\mathrm{CK}) \to \mathrm{MAC}_i$。令$H_2$: $\{0,1\}^k \times \{0,1\}^* \to \{0,1\}^l$，DO对密文文档集合$\mathrm{CF}_i$计算，生成消息验证码集合$\mathrm{MAC}_i = \{H_2(\mathrm{CF}_i\|\mathrm{CK}),i \in [1,n]\}$。最后数据持有者将密文文档集合$\mathrm{CF}_i$连同加密密钥CK上传至云服务器CS，将关键词索引$\mathrm{CI}_w$和消息验证码$\mathrm{MAC}_i$上传至区块链。

3.3 数据检索

本阶段可划分为陷门生成和数据检索2个部分。

1) 陷门生成。$\mathrm{TrapdoorGen}(\mathrm{PK},\mathrm{SK}_s,w) \to T_w$。数据用户使用授权访问密钥$\mathrm{SK}_s$和拟查询的关键词集合$w' = \{w_1',w_2',\cdots,w_m'\}$，计算检索陷门$T_w$。

DU随机选择$r_1 \in Z_q^*$，计算$T_{1,i} = H(w_i')g^{\frac{\alpha + r + r_1}{\beta}},i \in [1,m],\forall \mathrm{att} \in S_{\mathrm{uid}}$。用户计算$T_{\mathrm{att}}' = D_{\mathrm{att}}'$和$T_{\mathrm{att}} = D_{\mathrm{att}} \times g^{r_1} = g^{r+r_1}H_1(\mathrm{att})^{r_{\mathrm{att}}}$最后得到检索陷门$T_w = \{T_{1,i},\{T_{\mathrm{att}}',T_{\mathrm{att}}\}\}$。

2) 数据检索。$\mathrm{Search}(\mathrm{PK},\mathrm{CI}_w,T_w) \to \mathrm{ID}_f,\mathrm{MAC}_f$。智能合约运行检索算法，输入加密关键词索引$\mathrm{CI}_w$和检索陷门$T_w$，$x$表示访问树中的节点，算法运行主要分为以下2种情况。

① 当前节点x是叶子节点时，令$\mathrm{att} = \mathrm{att}(x)$，当$\mathrm{att} \in S_{\mathrm{uid}}$，进行计算。

$$F_x = \frac{e(T_{\mathrm{att}},D_x)}{e(T_{\mathrm{att}}',D_x')} = \frac{e(g^{r+r_1}H_1(\mathrm{att})^{r_a},g^{q_x(0)})}{e(g^{r_a},H_1(\mathrm{att}(x))^{q_x(0)})} = \frac{e(g^{r+r_1},g^{q_x(0)})e(H_1(\mathrm{att})^{r_a},g^{q_x(0)})}{e(g^{r_a},H_1(\mathrm{att}(x))^{q_x(0)})} = e(g,g)^{(r+r_1)q_x(0)}$$

若$\mathrm{att} \notin S_{\mathrm{uid}}$，令$F_x = \perp$。

② 若当前节点x是非叶子节点，输入当前节点x的所有孩子节点z，运行该算法后的结果定义为F_z，集合U_x中保留$F_x \neq \perp$的所有值。若集合$|U_x| < k_x$，说明当前节点x的孩子节点属性集合不满足该节点的门限值k_x，算法终止并输出$\perp$；若集合$|U_x| \geqslant k_x$，则说明当前节点x的孩子节点包含的属性集合满足该节点的门限值k_x，并从集合U_x中随机挑选k_x个F_z的值，利用拉格朗日系数计算其隐藏的值。

$$F_x = \prod_{z \in U_x} F_z^{\triangle_{,S_x}(0)} = \prod_{z \in U_x} e\left(\left(g,g^{(r+r_1)q_z(0)}\right)\right)^{\triangle_{i,S_x}(0)} = \prod_{z \in U_x}\left(e\left(g,g^{(r+r_1)q_{\mathrm{parent}(z)}(\mathrm{index}(z))}\right)\right)^{\triangle_{i,S_x}(0)} = \prod_{z \in U_x} e(g,g)^{(r+r_1)q_x(i)\triangle_{i,S_x}(0)} = e(g,g)^{(r+r_i)q_x(0)}$$

其中，$i=\mathrm{index}(z),S_x=\{\forall z\in U_x:\mathrm{index}(z)\},\Delta_{i,S_x}$ 为拉格朗日系数。

③ 若数据用户的属性集合满足访问树，通过递归计算可以得到最终结果 $F_t=e(g,g)^{(r+r_i)s}$。

④ 正确性验证。智能合约计算 $A=\dfrac{e\left(C_w',T_{1,i}\right)}{F_t}$，验证 $A=\sum_{i=1}^{n}C_{w_i}$ 是否成立，若等式成立，则数据用户检索成功，其表明数据用户的属性集满足嵌入在中的访问树且对关键词 w 拥有检索权限。因为 $\sum_{i=1}^{n}C_{w_i}=\sum_{i=1}^{n}H(w_i)e(g,g)^{\alpha s}$，计算

$$A=\frac{e\left(C_w',T_{1,i}\right)}{F_t}=\frac{\sum_{i=1}^{n}H(w_i)e\left(g^{\beta s},g^{\frac{\alpha+r+r_i}{\beta}}\right)}{e(g,g)^{(r+r_1)s}}=$$

$$\frac{\sum_{i=1}^{n}H(w_i)e\left(g^{s},g^{r+r_1}\right)e\left(g^{s},g^{\alpha}\right)}{e(g,g)^{(r+r_1)s}}=$$

$$\sum_{i=1}^{n}H(w_i)e\left(g^{s},g^{\alpha}\right)=$$

$$\sum_{i=1}^{n}H(w_i)e(g,g)^{\alpha s}$$

定义集合 ID_f，若检索成功，满足 $A=\dfrac{e\left(C_w',T_{1,i}\right)}{F_t}$ 的检索关键词所关联的密文文档 f_{id_j} 添加到集合 ID_f，得到 $\mathrm{ID}_f=\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_j\}$。根据集合 ID_f 遍历消息验证码 MAC 集合，得到包含有查询关键词的密文文档验证码集合

$$\mathrm{MAC}_f=\left\{\mathrm{MAC}_{c_1},\mathrm{MAC}_{c_2},\cdots,\mathrm{MAC}_{c_j}\right\}$$

3.4　数据解密

本阶段可划分为数据验证、密钥验证和文档密文解密 3 个部分。

数据验证。$\mathrm{Verify}(\mathrm{ID}_f,\mathrm{CF},\mathrm{MAC}_f)\rightarrow 0/1$。云服务器输入智能合约检索出的密文文档标识符 ID_f，输出相应的密文数据文件集合 CF_i 和相应密文的加密密钥密文 CK。云服务器收到密文文档标识符 ID_f 后，在数据集中检索密文文档，将密文数据 ID_f、检索得到的密文数据文件集合 CF_f 以及相应密文的加密密钥 CK 打包发送给数据用户，数据用户在收到上述数据后，向智能合约请求密文数据 ID_f 对应的消息验证码 $\mathrm{MAC}_{\mathrm{fid}}$，计算 $\mathrm{MAC}_{\mathrm{fid}}'=H_2(\mathrm{CF}_{\mathrm{fid}}\|\mathrm{CK})$。

判断 $\mathrm{MAC}_{\mathrm{fid}}'=\mathrm{MAC}_{\mathrm{fid}}$，若等式不成立，则表明当前文件返回结果不正确，云服务器存在篡改嫌疑。若等式成立，DU 将获得正确结果。

密钥解密。$\mathrm{CKDec}(\mathrm{SK}_u,\mathrm{CK})\rightarrow \mathrm{FK}$。DU 收到对应密文文档的加密密钥，使用用户的授权访问密钥对其进行解密。

检查数据用户属性集是否满足访问树 Γ，算法过程与数据检索算法验证访问树 Γ' 相同，但增加了对读/写叶子节点的验证，若数据用户属性集满足访问树 Γ，则可以通过递归计算得到最终结果 $F_t=e(g,g)^{(r+r_i+\mathrm{rk}_y^i)s}$。由此可以恢复加密文件密钥

$$\mathrm{FK}\|(\delta_{\mathrm{DO1}}/*)=\frac{\tilde{C}*F_t}{e(C,D)}=$$

$$\frac{(\mathrm{FK}\|\delta_{\mathrm{DO1}}/*)e(g,g)^{\alpha s}e(g,g)^{\left(r+r_i+\mathrm{rk}_y^i\right)s}}{e\left(h^s,g^{\frac{\alpha+r+\mathrm{rk}^i}{\beta}}\right)}=$$

$$\frac{(\mathrm{FK}\|\delta_{\mathrm{DO1}}/*)e(g,g)^{\alpha s}e(g,g)^{\left(r+r_i+\mathrm{rk}_y^i\right)s}}{e\left(g^{\beta s},g^{\frac{\alpha+r+\mathrm{rk}^i}{\beta}}\right)}=$$

$$\frac{(\mathrm{FK}\|\delta_{\mathrm{DO1}}/*)e(g,g)^{\alpha s}e(g,g)^{\left(r+r_i+\mathrm{rk}_y^i\right)s}}{e(g,g)^{s\left(a+r+r_i+\mathrm{rk}_y^i\right)}}$$

文档密文解密。$\mathrm{CFDec}(\mathrm{FK},\mathrm{CF}_i)\rightarrow F_i$。数据用户利用解密得到的加密密钥 FK，解密获得包含查询关键词的明文文档 F_i，检查随加密密钥解密得到的 DO 数字签名 $\delta_{\mathrm{DO1}}/*$ 获取明文文档的读/写权。

3.5　用户撤销及密钥更新

本阶段可划分为加密密钥密文重加密和授权访问密钥重加密 2 个部分。

1) 加密密钥密文重加密。$\mathrm{CK\_ReEncrypt}(\mathrm{CK},\mathrm{RK})\rightarrow \mathrm{CK}^{k+1}$。加密密钥密文重加密主要是对密文中访问树属性进行重加密，由云服务器 CS 执行，输入加密密钥密文 CK={ $\Gamma,\tilde{C}=(\mathrm{FK}\|\delta_{\mathrm{DO1}}/*)e(g,g)^{\alpha s}$;

$C=h^s,\left\{C_y=g^{q_y(0)},C_y'=H_1(\mathrm{att}(y))^{q_y(0)\mathrm{rk}_y^i}\right\}_{\forall y\in Y}$以及各个属性$i$的重加密密钥$\mathrm{RK}_i$。对于当前加密密钥的访问树的叶子节点$x$，执行算法后将每一个节点的属性版本号$\mathrm{Ver}_i^k$更新为$\mathrm{Ver}_i^{k+1}$，密文CK的版本号$C_y'^k$更新为$C_y'^{k+1}$。计算方法为$C'^{k+1}_y=C'^{k\frac{\mathrm{rk}_i^{k+1}}{\mathrm{rk}_i^k}}_y=H_1\left(\mathrm{att}(y)^{q_y(0)\mathrm{rk}_i^k}\right)^{\frac{\mathrm{rk}_i^{k+1}}{\mathrm{rk}_i^k}}=H(i)^{q_y(0)\mathrm{rk}_i^{k+1}}$。

2) 授权访问密钥重加密。$\mathrm{SK\_ReEncrypt}(\mathrm{SK}_u,\mathrm{Ver}),\mathrm{RK}\rightarrow\mathrm{SK}_u^{\mathrm{ver}+1}$。该算法由属性授权中心AA执行，输入属性集$S$的授权访问密钥$\mathrm{SK}_u=\{D=g^{\frac{\alpha+r+\mathrm{rk}^i}{\beta}},\forall\mathrm{att}\in S_{\mathrm{uid}}:D_{\mathrm{att}}=g^{r+\mathrm{rk}^i}H_1(\mathrm{att})^{r_j\mathrm{rk}_j^i},D_j'=g^{r_j}\}$以及需要重加密的属性$i$的重加密密钥，输出更新后的授权访问密钥$\mathrm{SK}_u^{\mathrm{ver}+1}$。对于任意属性$j$，计算方法为

$$D_j^{k+1}=D_j^kH_1(j)^{r_j\left(\mathrm{rk}_j^{k+1}-\mathrm{rk}_j^k\right)}g^{r+\mathrm{rk}_j^{k+1}-\mathrm{rk}_j^k}=$$
$$g^{r+\mathrm{rk}^k}H_1(j)^{r_j\mathrm{rk}_j^k}H_1(j)^{r_j\left(\mathrm{rk}_j^{k+1}-\mathrm{rk}_j^k\right)}g^{r+\mathrm{rk}^{k+1}-\mathrm{rk}^k}=$$
$$g^{r+\mathrm{rk}^{k+1}}H_1(j)^{q_x(0)\mathrm{rk}_i^{k+1}}$$

4 安全性证明

4.1 关键词密文安全

本文通过建立算法解决DBDH问题，保证关键词密文安全，模拟一个试图攻破关键词密文安全的攻击者A与挑战者B之间的安全游戏以证明本文算法。

初始阶段。挑战者随机选取$v\in\{0,1\},a,b,c,d\in Z_q^*$,得到

$$t_0=(g,A'=g^a,B'=g^b,C=g^c,Z=e(g,g)^{abc}),t_1=(g,A'=g^a,B'=g^b,C=g^c,Z=e(g,g)^z)。$$

询问阶段1。攻击者A自适应地向挑战者B的随机预言机发起询问，挑战者B执行初始化算法并公开参数$Y=e(B',C)=e(g,g)^{bc}$发送给攻击者A，攻击者A同时定义被挑战的访问树Γ^*。

密钥询问。攻击者A自适应地询问各个属性集$S_1,S_2,\cdots,S_m$并得到对应的用户查询密钥$\mathrm{SK}_{AS}^{S_1},\mathrm{SK}_{AS}^{S_2},\cdots,\mathrm{SK}_{AS}^{S_n}$。询问要求得到嵌入在查询私钥中对应的属性集合均不满足挑战访问树且均能成功生成检索陷门。

关键词询问。攻击者A自适应地询问关键词$\mathrm{kw}_1,\mathrm{kw}_2,\cdots,\mathrm{kw}_m$，得到对应密文$\mathrm{CI}_{w_1},\mathrm{CI}_{w_2},\cdots,\mathrm{CI}_{w_m}$。询问过程要求攻击者给定一个查询密钥$\mathrm{SK}_{AS}^{S_i}\{i\in[1,n]\}$和一个关键词$w$，计算得到的检索陷门$\mathrm{CI}_{w_i}$满足存在$\mathrm{Search}(\mathrm{PK},\mathrm{CI}_w,T_w)\neq\perp$，使得检索算法成立。

挑战阶段。攻击者A向挑战者B提交2个关键词w_0,w_1以及挑战访问树Γ^*，挑战者B随机选择$\mu\in\{0,1\}$，运行加密算法并返回密文$\mathrm{CI}_{W_\mu}=\{\Gamma^*,C_\mu^*=H(w_\mu)Z,\ C_w^*=A'^\beta,\{C_x=g^{q_x(0)},\ C_x'=H_1(\mathrm{att}(x))^{q_x(0)}\}_{\forall x\in X}\}$给攻击者$A$。

询问阶段2。攻击者A自适应地询问属性集$S_{n+1},S_{n+2},\cdots$，并得到对应的查询密钥$\mathrm{SK}_{AS}^{S_{n+1}},\mathrm{SK}_{AS}^{S_{n+2}},\cdots$，同时，自适应地询问关键词$\mathrm{kw}_{m+1},\mathrm{kw}_{m+2},\cdots$，得到对应的关键词密文索引$\mathrm{CI}_{w_{m+1}},\mathrm{CI}_{w_{m+2}},\cdots$，询问要求得到嵌入在查询密钥中对应的属性集合均不满足挑战访问树Γ^*。

猜测阶段。攻击者A输出猜测比特μ'。因为询问过程中要求攻击者A得到嵌入在查询密钥中的属性集均不满足访问树Γ^*，故攻击者A通过检索算法$\mathrm{Search}(\mathrm{PK},\mathrm{CI}_w,T_w)\neq\perp$无法判断出$\mu=0/1$。攻击者$A$只能通过恢复出索引结构中的关键词信息来判断$\mu=0/1$。

当$v=0$，加密关键词索引可以表示为$\mathrm{CI}_{w_\mu}=\{\Gamma^*,C_\mu^*=H(w_\mu)e(g,g)^{\alpha bc},C_w^*=g^{a\beta},\ \{C_x=g^{q_x(0)},C_x'=H_1(\mathrm{att}(x))^{q_x(0)}\}_{\forall x\in X}\}$。因为$a,b,c$均为随机选取，因此令$a=s,bc=\alpha$，即加密关键词索引描述为$\mathrm{CI}_{w_\mu}=\{\Gamma^*,C_\mu^*=H(w_\mu)e(g,g)^{s\alpha},C_w^*=g^{s\beta},\{C_x=g^{q_x(0)},C_x'=H_1(\mathrm{att}(x))^{q_x(0)}\}_{\forall x\in X}\}$；同理，当$v=1$时，加密关键词索引可以表示为$\mathrm{CI}_{w_\mu}=\{\Gamma^*,C_\mu^*=H(w_\mu)e(g,g)^z,C_w^*=g^{s\beta},\{C_x=g^{q_x(0)},C_x'=H_1(\mathrm{att}(x))^{q_x(0)}\}_{\forall x\in X}\}$。

攻击者A输出猜测。若$\mu=\mu'$，则挑战者B输出v'。假设攻击者A从关键词密文索引中恢复出关键词信息的概率为$\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)$，则攻击者$A$赢得安全游戏的概率为$\frac{1}{2}+\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)$。若$\mu\neq\mu'$，则挑战者$B$输出$\mu'=1$，攻击者$A$赢得安全游戏的概率为$\frac{1}{2}$。

因此挑战者 B 在以上挑战中解决DBDH问题的概率为

$$\mathrm{Adv}_A^{\mathrm{DBDH}}(\lambda)=\left|\frac{1}{2}\Pr[v=v'|v=0]+\frac{1}{2}\Pr[v=v'|v=1]-\frac{1}{2}\right|=\left|\left[\frac{1}{2}\times\left(\frac{1}{2}+\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)\right)+\frac{1}{2}\times\frac{1}{2}\right]-\frac{1}{2}\right|=\frac{1}{2}\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)$$

假设 $\mathrm{Adv}_A^{\mathrm{CIP}}(\lambda)$ 不可忽略，则 $\mathrm{Adv}_A^{\mathrm{DBDH}}(\lambda)$ 不可忽略，与DBDH问题中的困难假设矛盾。

4.2　陷门安全

本文通过建立算法解决DDH问题保证陷门安全，通过模拟一个试图攻破陷门安全的攻击者 A 与挑战者 B 之间的安全游戏来证明，挑战者 B 获得参数 $\mathrm{Para}=(G_1,G_2,e,p,g,a,b,g^{ab})$。

初始阶段。挑战者随机选择 $a,r,r_1\in Z_q^*$，生成 $\mathrm{PK}=\left(G_1,G_2,g,h=g^{\beta}=g^{b},e(g,g)^{\alpha}=e(g,g)^{a-r-r_1}\right)$，将PK返回给攻击者 A。随机选择1个比特 $v\in\{0,1\}$，若 $v=1$，令 $g^{\beta}=g^{b}$。若 $v=0$，随机选择 $y\in Z_q^*$，得到 $g^{\beta}=g^{y}$。挑战者维护一个空列表 $L=\{<\cdot,\cdot,\cdot,\cdot>\}$。

询问阶段1。在此阶段攻击者 A 适应性地进行如下询问，并且假设攻击者 A 不会执行重复的询问。

1) Hash询问。挑战者 B 从 L 中查找 $\{<w,\alpha,P,v>\}$，若 L 不为空，挑战者 B 将私钥发送给攻击者 $\mathcal{A}$。否则，若 $v=1$，计算 $P=a-\alpha-r_1$，并写入 L；若 $v=0$，计算 $P=g^{y}$，并写入 L。

2) 密钥询问。若 $v=1$，则中止。否则，查看列表 L，挑战者 B 执行密钥生成算法计算 SK_S，并将其返回给攻击者 A。其中，$\mathrm{SK}_S=\{D=g^{\frac{\alpha+r}{\beta}},\forall\mathrm{att}\in S_{\mathrm{uid}}:D_{\mathrm{att}}=g^{r}H_1(\mathrm{att})^{r_j},D_j'=g^{r_j}\}$。

3) 陷门询问。若 $v=1$，查看列表 L，计算 T_w 并返回给攻击者 A，其中，$T_w=\{T_{1,i}=H(w)^{\frac{\alpha+r+r_1}{\beta}}=g^{ab};\forall\mathrm{att}\in S_{\mathrm{uid}},r_1\in Z_q^*,T_{\mathrm{att}}'=D_{\mathrm{att}}',\ T_{\mathrm{att}}=D_{\mathrm{att}}\times g^{r_1}=g^{r+r_1}H_1(\mathrm{att})^{r_{\mathrm{att}}}=g^{a-P-\alpha}\times H_1(\mathrm{att})^{r_{\mathrm{att}}}\}$。否则，$v=0$，则中止。

挑战阶段。攻击者 A 向挑战者 B 提交2个挑战关键字 w_0,w_1。挑战者随机选择 $\mu\in\{0,1\}$，计算陷门 $T_{w_u}^*=\{T_{1,i}=H(w)^{\frac{\alpha+r+r_1}{\beta}}=g^{ab};\forall\mathrm{att}\in S_{\mathrm{uid}},r_1\in Z_q^*,T_{\mathrm{att}}'=D_{\mathrm{att}}',T_{\mathrm{att}}=D_{\mathrm{att}}g^{r_1}=g^{r+r_1}H_1(\mathrm{att})^{r_{\mathrm{att}}}=g^{a-P-\alpha}H_1(\mathrm{att})^{r_{\mathrm{att}}}\}$ 并返回给攻击者 A。

询问阶段2。与阶段1相同，并且要求攻击者不能询问与挑战关键词相关的信息。

猜测阶段。攻击者 A 输出猜测比特 μ'，若 $\mu'=\mu$，则表示挑战者 B 挑战成功，输出1，否则输出0。

攻击者 A 输出猜测。若 $\mu=\mu'$，则挑战者 B 输出 v'。假设攻击者 A 从成功赢得这个游戏的概率为 $\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)$，则攻击者 A 赢得安全游戏的概率为 $\frac{1}{2}+\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)$。若 $\mu\neq\mu'$，则挑战者 B 输出 $\mu'=1$。攻击者 A 赢得安全游戏的概率为 $\frac{1}{2}$。

因此挑战者 B 在以上挑战中解决DDH问题的概率为

$$\mathrm{Adv}_A^{\mathrm{DDH}}(\lambda)=\left|\frac{1}{2}\Pr[v=v'|v=0]+\frac{1}{2}\Pr[v=v'|v=1]-\frac{1}{2}\right|=\left|\left[\frac{1}{2}\times\left(\frac{1}{2}+\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)\right)+\frac{1}{2}\times\frac{1}{2}\right]-\frac{1}{2}\right|=\frac{1}{2}\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)$$

假设 $\mathrm{Adv}_A^{\mathrm{TRA}}(\lambda)$ 不可忽略，则 $\mathrm{Adv}_A^{\mathrm{DDH}}(\lambda)$ 不可忽略，与DDH问题中的困难假设矛盾。

5　性能分析

5.1　功能对比

如表1所示，从功能方面而言，本文方案扩展了数据持有者对隐私数据的访问控制，又在数据安全性和正确性方面为用户提供足够的保障服务，并且为系统内各个角色提供密钥及密文的重加密服务，实现了用户和服务器之间的支付公平。

5.2　性能对比

将本文方案与文献[17,25]方案在密钥生成、索引生成、陷门生成、查询过程和解密过程中的计算进行对比，如表2所示；与文献[29-30]方案在密钥更新和密文更新中的计算进行对比，如表3所示。

表 1 功能对比

方案	关键词类型	区块链	关键词查询细粒度控制	读写控制	结果可验证	密钥更新
文献[25]方案	单关键词	√	√	×	×	×
文献[26]方案	单关键词	√	√	×	×	×
文献[28]方案	多关键词	×	√	×	×	√
本文方案	多关键词	√	√	√	√	√

表 2 性能对比

方案	密钥生成	索引生成	陷门生成	查询过程	解密过程
文献[17]方案	$(4\|S\|+8)G+\|S\|H_1$	$(2\|N\|+2)G+\|N\|H_1+2G_T$	—	$2G_e$	$(2\|N\|+1)G_e+3G+\|N+3\|G_T$
文献[25]方案	$(2\|S\|+3)G+\|S\|H_1$	$(2\|N\|+3)G+\|N\|H_1+G_e$	$(\|S\|+1)G+H_1$	$(2\|N\|+3)G_e+\|N\|G_T$	—
本文方案	$(2\|S\|+2)G+\|S\|H_1$	$(2\|N\|+2)G+\|N\|H_1+G_e$	$\|S\|G+H_1$	$(2\|N\|+3)G_e+\|N\|G_T$	$(2\|N\|+2)G_e+\|N+5\|G_T$

表 3 密钥更新及密文更新性能对比

方案	密钥更新	密文更新
文献[29]方案	G_m+2m	$\|N\|(G_m+m)$
文献[30]方案	$2G_m+2m$	$\|N\|(G_m+m)$
本文方案	m	$\|N\|m$

表 2 和表 3 中，G 和 G_T 分别表示为群 G_1 和 G_2 上的指数运算，G_e 表示双线性运算，H_1 表示由群 G_1 生成的散列运算，G_m 表示群上的一次幂乘运算，m 表示一次乘法运算，$|S|$ 表示属性集中的属性个数，$|N|$ 表示访问策略中的属性的数量。

与文献[17]方案相比，本文方案在密钥生成阶段同样也使用“版本控制”的方式实现密钥重加密，但通过减少指数模乘来节省运算时间，比文献[17]方案更优；在索引生成阶段，由于文献[17]方案直接对密文密钥进行加密实现密文共享，其方案中所使用的加密计算开销为 $(2|N|+2)G+|N|H_1+2G_T$，本文方案与其基本一致；在查询过程中，由于方案[17]方案并没有对用户检索能力进行限制，因此检索过程的计算开销仅在与索引结构进行对比。在解密过程中，文献[17]方案因版本控制密钥参与解密模乘运算，计算开销为 $(2|N|+1)G_e+3G+|N+3|G_T$，本文方案相比于文献[17]方案更优。

与文献[25]方案相比，本文方案通过减少双线性运算和指数运算来节省结算成本。在密钥生成、索引生成和陷门生成阶段中，文献[25]方案为了节省检索阶段带来的计算消耗，为用户提前计算群 G_1 上的逆运算，本文方案因为在加密时并不考虑逆运算，因此可以节省此类计算带来的时间消耗。本文方案在查询过程的计算开销与文献[25]方案一致。

与文献[29-30]方案相比，本文方案时间开销相当甚至更优。密钥更新时本文方案只需执行一次乘法运算，文献[29]方案需多执行一次幂乘运算，文献[30]方案需多执行 2 次幂乘运算。密文更新时，针对每个待撤销属性，只需执行一次乘法运算，而文献[29-30]方案需多执行一次幂乘运算。

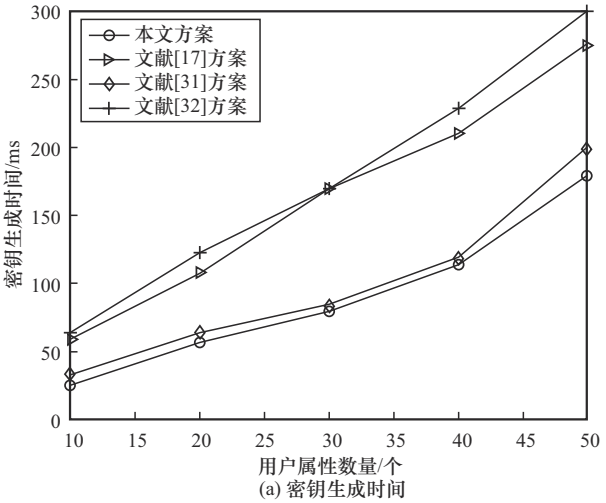
综上所述，从密钥生成、索引生成、陷门生成、查询过程、解密过程、密钥更新和密文更新 7 个方面来看，本文方案在性能上是最优的，将检索服务部署在智能合约上，很大程度上降低了用户和服务器的存储和计算开销。

5.3 实验分析

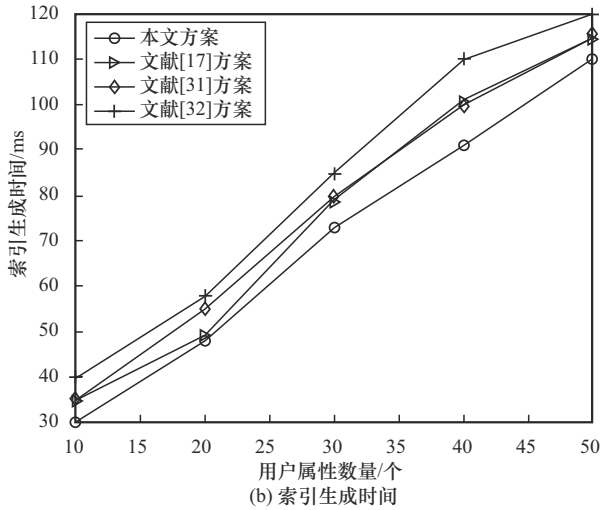
为了更加准确全面地评估本文方案在实际运行中的性能，本节通过模拟实验对本文方案与文献[17,31-32]方案的运行时间进行统计，实验结果如图 3 所示。本文方案基于 Charm-dev 框架，使用 Python3 语言进行编程实现所有算法，其中选取“SS512”曲线作为双线性映射曲线，所使用的平台基于 Linux 系统、Inter Core i7 (2.7 GHz)、2 GB RAM 虚拟环境运行。

从图 3 可以看出，相比于文献[17]方案，本文方案在密钥生成阶段中的时间开销有了较好改善，但是在加密和查询过程中，本文方案与文献[17]方案开销基本一致，这是因为本文方案为关键词增加了访问策略，在与索引结构进行对比查询前需要进行验证，因此在该阶段存在一定的时间开销，但本文方案能够为数据持有者提供增强的访问控制策略。文献[31-32]方案虽然与本文方案同

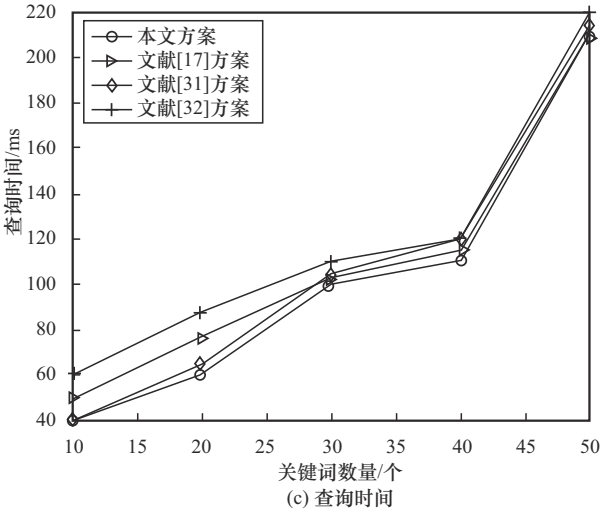
样对关键词增加了访问策略，但是在密钥生成阶段和索引生成阶段，相比于本文方案需要进行更多的逆运算和模乘运算，因此需要更多的时间消耗。



(a) 密钥生成时间



(b) 索引生成时间



(c) 查询时间

图3　实验结果

综合以上分析，本文方案测试性能与理论性能分析相一致，同时在密钥生成、索引加密和查询过程的响应速度均在毫秒级别，证明了本文方案具有较高效率。

6　结束语

本文基于属性加密、代理重加密和智能合约等技术，提出了一种面向云存储且支持密钥更新的属性基可搜索加密方案，解决了一对多模型下存在的共享密文密钥和关键词密文细粒度访问控制问题，并且通过增加读/写节点来强化数据持有者对共享密文的访问控制，进一步保证密文数据的安全,且在DBDH困难问题和DDH困难问题下验证了本文方案满足关键词不可区分性和陷门不可区分性。同时，使用代理重加密技术解决了用户撤销后的共享密钥密文重加密问题以及用户授权访问密钥更新问题，防止已撤销用户使用其授权密钥对系统中的密文数据再次访问，提高了方案的实用性和安全性。性能分析和实验数据表明，本文方案在功能性和计算效率上与同类方案相比具有一定优势，未来将重点研究用户访问和查询密钥在分发过程中的存储及传输安全问题。

参考文献：

[1] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2000: 44-55.

[2] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.

[3] RHEE H S, SUSILO W, KIM H J. Secure searchable public key encryption scheme against keyword guessing attacks[J]. IEICE Electronics Express, 2009, 6(5): 237-243.

[4] GOLLE P, STADDON J, WATERS B. Secure conjunctive keyword search over encrypted data[C]//Applied Cryptography and Network Security: Second International Conference. Berlin: Springer, 2004: 31-45.

[5] LI H W, YANG Y, LUAN T H, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(3): 312-325.

[6] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Ber-

lin: Springer, 2005: 457-473.

[7] 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.

[8] 高诗尧, 陈燕俐, 许玉岚. 云环境下基于属性的多关键字可搜索加密方案[J]. 计算机科学, 2022, 49(3): 313-321.
GAO S Y, CHEN Y L, XU Y L. Expressive attribute-based searchable encryption scheme in cloud computing[J]. Computer Science, 2022, 49 (3): 313-321.

[9] SRAVANTHI K, CHANDRASEKHAR P. An efficient multi-user group-wise integrity CP-ABE(GI-CPABE) for homogeneous and heterogeneous cloud blockchain transactions[J]. Journal of Electrical Systems, 2024, 20(1): 326-349.

[10] LI J G, ZHANG R Y, LU Y, et al. Multiauthority attribute-based encryption for assuring data deletion[J]. IEEE Systems Journal, 2023, 17 (2): 2029-2038.

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

[12] LAI J, DENG R H, LI Y. Fully secure ciphertext-policy hiding CP-ABE[C]//International Conference of Information Security Practice and Experience. Berlin: Springer, 2011: 24-39.

[13] QIU S, LIU J Q, SHI Y F, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack[J]. Science China Information Sciences, 2016, 60(5): 052105.

[14] MENG F, CHENG L X, WANG M Q. Ciphertext-policy attribute-based encryption with hidden sensitive policy from keyword search techniques in smart city[J]. EURASIP Journal on Wireless Communications and Networking, 2021(1): 20.

[15] ZHOU Y S, PENG R D, LIU Y N, et al. TRE-DSP: a traceable and revocable CP-ABE based data sharing scheme for IoV with partially hidden policy[J]. Digital Communications and Networks, 2024: doi. org/10.1016/j.dcan.2024.03.005.

[16] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//Proceedings of the IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2010: 1-9.

[17] WANG J, YIN X, NING J, et al. Attribute-based encryption with efficient keyword search and user revocation[C]//International Conference of Information Security and Cryptology. Berlin: Springer, 2019: 490-509.

[18] SULTAN N H, KAANICHE N, LAURENT M, et al. Authorized keyword search over outsourced encrypted data in cloud environment[J]. IEEE Transactions on Cloud Computing, 2022, 10(1): 216-233.

[19] LUO F C, AL-KUWARI S, WANG H Y, et al. Revocable attribute-based encryption from standard lattices[J]. Computer Standards & Interfaces, 2023, 84: 103698.

[20] DAS S, NAMASUDRA S. MACPABE: multi-authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure[J]. International Journal of Network Management, 2023, 33(3): e2200.

[21] 胡甜媛, 李泽成, 李必信, 等. 智能合约的合约安全和隐私安全研究综述[J]. 计算机学报, 2021, 44(12): 2485-2514.
HU T Y, LI Z C, LI B X, et al. Contractual security and privacy security of smart contract: a system mapping study[J]. Chinese Journal of Computers, 2021, 44(12): 2485-2514.

[22] LI H G, TIAN H B, ZHANG F G, et al. Blockchain-based searchable symmetric encryption scheme[J]. Computers & Electrical Engineering, 2019, 73: 32-45.

[23] LU Y, FENG T, LIU C Y, et al. A blockchain and CP-ABE based access control scheme with fine-grained revocation of attributes in cloud health[J]. Computers, Materials & Continua, 2024, 78(2): 2787-2811.

[24] WU A X, ZHANG Y H, ZHENG X K, et al. Efficient and privacy-preserving traceable attribute-based encryption in blockchain[J]. Annals of Telecommunications, 2019, 74(7): 401-411.

[25] 牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案[J]. 计算机研究与发展, 2021, 58(4): 811-821.
NIU S F, XIE Y Y, YANG P P, et al. Cloud-assisted attribute-based searchable encryption scheme on blockchain[J]. Journal of Computer Research and Development, 2021, 58(4): 811-821.

[26] ZHENG Q J, XU S H, ATENIESE G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data[C]//Proceedings of the IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 522-530.

[27] 闫玺玺, 原笑含, 汤永利, 等. 基于区块链且支持验证的属性基搜索加密方案[J]. 通信学报, 2020, 41(2): 187-198.
YAN X X, YUAN X H, TANG Y L, et al. Verifiable attribute-based searchable encryption scheme based on blockchain[J]. Journal on Communications, 2020, 41(2): 187-198.

[28] HU Y Y, CHEN Y L, ZHU M H. Privacy protection attribute-based ciphertext search scheme[J]. Application Research of Computers, 2019, 36(4): 1158-1164.

[29] YANG K, JIA X H, REN K, et al. DAC-MACS: effective data access control for multiauthority cloud storage systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1790-1801.

[30] XIONG S M, NI Q, WANG L M, et al. SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage[J]. IEEE Internet of Things Journal, 2020, 7(4): 2914-2927.

[31] 周艺华, 扈新宇, 李美奇, 等. 云环境下基于属性策略隐藏的可搜索加密方案[J]. 网络与信息安全学报, 2022, 8(2): 112-121.

ZHOU Y H, HU X Y, LI M Q, et al. Searchable encryption scheme based on attribute policy hiding in cloud environment[J]. Journal of Network and Information Security, 2022, 8(2): 112-121.

[32] LIU X, LU T, HE X, et al. Verifiable attribute-based keyword search over encrypted cloud data supporting data deduplication[J]. IEEE Access, 2020, 8: 52062-52074.

[作者简介]

张克君（1972– ），男，山东临沂人，博士，北京电子科技学院教授、博士生导师，北京邮电大学、中国科学技术大学兼职博士生导师，主要研究方向为网络安全、隐私保护等。

王文彬（1999– ），男，青海海晏人，北京邮电大学博士生，主要研究方向为认知信息安全、密文检索等。

徐少飞（1999– ），男，陕西汉中人，北京电子科技学院硕士生，主要研究方向为隐私保护、可搜索加密等。

于新颖（1997– ），女，山东泰安人，北京邮电大学博士生，主要研究方向为网络安全、隐私保护。

王钧（1998– ），男，河北保定人，北京电子科技学院博士生，主要研究方向为网络主动防御、隐私保护机器学习。

李鹏程（1998– ），男，河北邯郸人，中国科学技术大学博士生，主要研究方向为自然语言处理、隐私保护。

钱榕（1970– ），男，福建福州人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为复杂网络、数据挖掘、云计算安全等。