基于区块链的多授权密文策略属性基等值测试加密方案

杨小东[1],陈艾佳[1],汪志松[1],廖泽帆[1],王彩芬[2]
(1. 西北师范大学计算机科学与工程学院,甘肃兰州 730070;2. 深圳技术大学大数据与互联网学院,广东深圳 518118)

摘 要: 针对云环境下密文策略属性基加密方案中存在的密文检索分类困难与依赖可信第三方等问题,本文提出了一种基于区块链的多授权密文策略属性基等值测试加密方案. 利用基于属性的等值测试技术,实现了支持属性级灵活授权的云端数据检索和分类机制,降低了数据用户对重复数据解密的计算开销. 结合多授权属性基加密机制和区块链技术,实现了去中心化用户密钥生成. 采用多属性授权机构联合分发密钥,有效抵抗用户和属性授权机构的合谋攻击. 引入区块链和智能合约技术,消除了现有密文策略属性基密文等值测试方案中等值测试、数据存储与外包解密操作对可信云服务器的依赖. 利用外包服务器执行部分解密计算,降低了用户本地的计算开销. 将原始数据哈希和验证参数上传至区块链,保障外包服务器解密结果正确性和云端数据完整性. 在随机预言模型下,基于判定性q-parallel Bilinear Diffie-Hellman Exponent困难问题证明了本文方案在选择密文攻击下的单向性. 与同类方案相比较,本文方案支持更多的安全属性,并具有较低的计算开销.

关键词: 云存储;等值测试;区块链;密文策略属性基加密;多授权机构;完整性验证
基金项目: 国家自然科学基金(No.62172337)
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0898-11
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220950

Blockchain-Based Multi-Authority Ciphertext-Policy Attribute-Based Encryption Scheme with Equality Test

YANG Xiao-dong[1], CHEN Ai-jia[1], WANG Zhi-song[1], LIAO Ze-fan[1], WANG Cai-fen[2]
(1. *College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou*, *Gansu* 730070, *China*;
2. *College of Big Data and Internet*, *Shenzhen Technology University*, *Shenzhen*, *Guangdong* 518118, *China*)

Abstract: Aiming at the problems of ciphertext retrieval classification difficulty and dependence on trusted third party in the ciphertext-policy attribute-based encryption schemes within cloud environment, a blockchain-based multi-authority ciphertext-policy attribute-based encryption scheme with equality test is proposed. The attribute-based encryption with equality test technology is used to retrieve and classify ciphertexts that supports attribute-level flexible authorization, which reduces the computational cost of data users to decrypt duplicate data. Combined with multi-authority attribute-based encryption and blockchain technology to achieve decentralized user key generation. Meanwhile, the key is jointly distributed by different authorized institutions can effectively resist collusive attacks by users and attribute authorization agencies. Blockchain and smart contract technology are introduced to eliminate the dependence of trusted cloud servers in the outsourcing decryption, data storage and equivalence test operation in the existing ciphertext-policy attribute-based encryption with equality testing schemes. Outsourced server is used to perform part of the decryption computation, which reduces the user's local calculation overhead. The original data hash and verification parameters are uploaded to the blockchain, which ensures the correctness of the outsourcing server's decryption results and the integrity of cloud data. Under the random oracle model, the one-way property of the proposed scheme under chosen-ciphertext attack is proved based on the decision q-parallel BDHE hard problem. Compared with similar schemes, the proposed scheme supports more security properties and has lower computational overhead.

Key words: cloud storage; equality test; blockchain; ciphertext-policy attribute-based encryption; multi-authority; in-

收稿日期:2022-08-10;修回日期:2023-06-06;责任编辑:梅志强

tegrity verification
Foundation Item(s): National Natural Science Foundation of China (No.62172337)

1 引言

云存储技术利用云端服务器的巨大存储空间降低用户本地存储负担,在各行各业得到了广泛使用. 然而,云服务器通常对上传和存储的用户敏感数据保持好奇,有特权的用户如云服务提供商作为能够绕过监管机制获取或访问存储的敏感信息. 因此,用户享受云存储提供便利的同时,数据的隐私保护和访问控制问题亟待解决[1].

数据加密技术能够对数据在上传到云服务器之前进行加密,保护了用户隐私,保证了云存储数据机密性. 其中,密文策略属性基加密(Ciphertext-Policy Attribute-Based Encryption,CP-ABE)[2]是一种支持灵活访问控制功能的加密技术,从而成为云存储数据访问控制的关键技术之一. 然而,传统CP-ABE方案[3~6]在云存储实际应用中仍存在着一些不足,例如单授权机构面临单点失效、加密后的数据很难被高效检索以及数据检索和密文存储对可信云服务器的依赖等.

针对传统CP-ABE方案中存在的问题,本文提出了一种基于区块链的多授权密文策略属性基等值测试加密方案,实现了去中心化的灵活授权密文检索、去中心化属性授权,同时保证了云存储数据的机密性和完整性. 本文方案的特点总结如下:

(1)支持授权密文检索:通过将CP-ABE与等值测试技术结合,实现了对特定属性用户的测试授权,同时实现了授权用户无需解密条件下,对云端数据的有效检索和比较.

(2)支持去中心化的多授权CP-ABE机制:基于多授权CP-ABE机制,将系统参数和公钥上传至区块链来消除对单一属性授权方的单点失效和可信依赖. 每个属性机构将用户属性集合和全局身份标识绑定在生成的用户密钥中,有效抵抗了用户和授权机构的合谋攻击.

(3)去中心化:引入区块链和智能合约技术,由部署在联盟区块链平台上的智能合约执行密文等值测试和数据验证操作,消除了对云服务器的可信依赖,实现了去中心化的密文检索方式,保证了云存储数据的完整性.

目前,一系列CP-ABE方案[5,6]被提出,能有效实现云环境下数据的机密性和灵活访问控制. 然而,这些方案都采用单个属性授权中心生成所有用户私钥,存在着一定的安全和性能问题[7]. 在单授权机构的属性基系统模型中,由于单个属性授权中心管理着系统中所有属性和用户私钥,一旦授权中心遭到恶意攻击或授权机构不可信,则可能导致数据安全受到严重威胁. 同时,随着系统用户数量及用户拥有属性个数增加,单一授权中心容易存在性能受限的问题. 为提升单授权机构密钥分发效率,Chase提出了一个多授权中心Attribute-Based Encryption (ABE)方案[8],但由于该方案存在一个中央授权机构,系统依然面临依赖可信第三方的问题. 为了提升属性授权的安全性,Lewko等提出无中心授权机构的分布式CP-ABE方案[9]. 通过多属性中心分别独立负责部分任务,实现去中心化的授权方式,但该方案无法保证数据完整性和不可篡改性. 针对分布式CP-ABE无法防篡改的缺陷,Gao等人利用区块链构造了一种去中心化策略隐藏CP-ABE方案[10],但计算开销较大,未考虑加密操作降低了数据可用性.

随着大量被加密的数据上传云端,上述方案[7~10]都没有考虑如何实现密文的有效检索或分类. 为了避免下载完整加密文件进行解密,Boneh等提出公钥可搜索加密技术[11]满足了对加密数据的搜索需求. 然而,公钥可搜索加密技术只针对数据接收方公钥加密的数据执行搜索,在多公钥应用场景中存在一定的局限性. 2010年,Yang等提出密文等值测试加密方案[12],云服务器能够直接利用陷门对任意公钥加密数据进行快速检索. 相较于公钥可搜索加密方案,该方案能够对比不同公钥加密的两段密文数据是否对应相同明文,实现了云环境中多公钥加密下对密文数据的检索分类. 但同时,文献[12]仍存在着一些安全缺陷,例如由于系统公开所有输入,导致任何拥有密文的用户都能对密文等值测试发起猜测攻击. 另外,基于传统公钥加密的密文等值测试方案也存在固有的数字证书管理负担问题. 为解决上述问题,各国学者相继提出支持授权的密文等值测试方案[13~16]、基于身份[17~19]和无证书的密文等值测试方案[20]. 尽管上述方案改进了用户的密钥管理方式,但都缺乏灵活高效的授权方式.

基于属性的密文等值测试方案结合了属性基加密机制和等值测试技术的优点,通过对一群拥有特定属性的用户进行密文等值测试权限的授权,避免向测试者逐个分发授权陷门,实现了更加灵活的授权模式. 2017年,Wang等首次提出了基于CP-ABE的等值测试方案[21],委托半可信云服务器对不同策略下加密的CP-ABE密文进行等值测试,利用访问策略实现属性级的等值测试授权机制. 随后,Cui等设计了一个基于密文策略属性的数据等值测试和分类方案[22],具有更短的用户私钥和更高的安全性. 为了提高用户端的解密计

算效率,Cui等利用外包解密技术设计了支持外包解密的密文策略属性基等值测试加密方案[23],降低了等值测试和解密过程中的计算开销. 尽管上述方案[21~23]实现了密文检索的属性级授权,但忽略了系统存在可信中央授权和密文检索及外包解密过程对云服务器的可信依赖问题. 一旦云服务器遭到恶意攻击或云服务器自身对数据出于好奇篡改数据,测试结果正确性和云端数据完整性都面临严峻挑战.

针对现有云环境下CP-ABE加密方案中存在的问题,本文提出了一种基于区块链的多授权密文策略属性基等值测试加密方案. 该方案首次设计了基于多机构CP-ABE的多授权密文等值测试机制,将用户密钥与用户身份绑定和系统参数上链,消除了传统多授权CP-ABE方案对中央授权方的可信依赖,实现了去中心化的密文检索灵活授权. 利用部署在联盟区块链中的智能合约执行测试操作,消除了对测试服务器的可信依赖. 将部分计算开销大的解密运算过程外包给第三方服务器,降低了用户本地计算开销. 此外,采用链上存储验证信息、云端存储完整密文的方式,确保了外包解密结果的正确性和云存储数据的完整性. 分析结果表明,本文方案满足云存储数据的机密性和灵活访问控制、支持属性授权的等值测试、外包解密结果的可验证性、等值测试结果的可信性与测试陷门的单向性.

2 预备知识

2.1 双线性映射

设G和G_T是阶为素数p的循环群,G_1的一个生成元为g,$e: G\times G\to G_T$是一个满足以下性质的双线性映射:

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

(2)非退化性:$e\left(g,g\right)\neq 1$,其中1为G_T中的单位元;

(3)可计算性:对任意$g_1,g_2\in G$,存在有效的算法计算$e(g_1,g_2)$.

可除计算性(Divisible Computation Diffie-Hellman, DCDH)问题:设G是阶为素数p的循环乘法群,g是G的生成元,$a,b\in Z_p^*$,已知$\left(g,g^a,g^b\right)$,计算$g^{b/a}$.

在群G中,CDH(Computational Diffie-Hellman)问题与DCDH问题等价[18].

2.2 判定性q-parallel BDHE假设

设G和G_T是阶为素数p的循环群,生成元$g\in G$,随机选取元素$a,s,b_1,\cdots,b_q\in Z_p$,判定性$q$-parallel BDHE(Bilinear Diffie-Hellman Exponent)问题[24]:给定一个多元组

$$y=\{g,g^s,g^a,\cdots,g^{\left(a^q\right)},g^{\left(q+2\right)},\cdots,g^{\left(a^{2q}\right)},\forall_{1\leqslant j\leqslant q},\\ g^{s\cdot b_j},g^{a/b_j},\cdots,g^{\left(a^q/b_j\right)},g^{\left(a^{q+2}/b_j\right)},\cdots,g^{\left(a^{2q/b_j}\right)},\forall_{1\leqslant j,k\leqslant q,k\neq j},\\ g^{a\cdot s\cdot b_k/b_j},\cdots,g^{\left(a^q\cdot s\cdot b_k/b_j\right)}\}.$$

判断T的输出为$T=e(g,g)^{a^{q+1}s}$还是G_T中的一个随机值. 如果不存在一个多项式时间算法能以一个不可忽略的概率解决判定性q-parallel BDHE问题,则称判定性q-parallel BDHE问题是困难的.

2.3 区块链与智能合约

区块链[25]技术的本质功能是一种不可篡改和伪造的分布式账本,能够通过参与节点达成共识来实现去中心化,并保证交易的公平性. 将数据区块按照时间顺序相连结合而成的链式数据结构,并且以密码学方式保证链上数据的不变性和安全性,同时通过设立激励机制奖励来鼓励网络节点参与并共同维护链式数据. 依据开放程度不同,区块链分为公有链、私有链和联盟链. 其中公有链是一种对所有人公开的部署形式,允许所有人在链上读取数据、发布并确认交易. 私有链由于多受中心化机构掌控,只能对拥有权限的人员开放,使其信任度相比于公有链较低,但权限的设置也使得私有链更具灵活性. 联盟链指由多个组织共同构建与维护的区块链,各个参与者之间通过契约构建共识机制以实现部分去中心化,且相比于公有链,联盟链有更强的可控性.

智能合约[26]是一段部署于区块链上的自动代码,具有唯一的地址. 初始者可以创建一个智能合约,以交易的形式存储在区块链平台. 当合约中某一事务被触发,该合约会自动根据脚本执行预定义内容,例如执行相关计算. 最后将该事务的输出、状态信息等作为交易记录在区块链中. 智能合约为区块链应用层提供了各种处理外部数据和负责存储的接口,使区块链技术能够代替半可信云服务器执行诸如密文检索[27]等操作.

2.4 线性秘密共享

设参与者的集合为$P=\{P_1,\cdots,P_k\}$,访问结构表示为$(\boldsymbol{M},\rho)$,其中$\boldsymbol{M}$是一个l行m列的矩阵,ρ是一个从$\{1,2,\cdots,l\}$到P的映射,一个线性秘密共享方案[23](Linear Secret Sharing Scheme,LSSS)包含以下两个算法.

(1)秘密分发:假设$s\in Z_p$是共享的秘密值,算法随机选择$r_2,\cdots,r_m\in Z_p$,构造一个向量$\boldsymbol{v}=(s,r_2,\cdots,r_m)$,则$\rho(i)$分享的子秘密值为$\lambda_i=\boldsymbol{M}_i\times\boldsymbol{v}^{\mathrm{T}}$,其中$\boldsymbol{M}_i$为矩阵$\boldsymbol{M}$的第$i$行.

(2)秘密重构:假设S表示一个授权集,$I=\{i|\rho(i)\in S\}$且$I\subseteq\{1,\cdots,l\}$,则存在多项式时间算法得到系数$\{w_i\in Z_p^*\}_{i\in I}$,其中$\{w_i\in Z_p^*\}_{i\in I}$满足

$\sum_{i\in I} w_i\lambda_i=(1,0,\cdots,0)$,因此可以恢复秘密 $s=\sum_{i\in I} w_i\lambda_i\cdot v=\sum_{i\in I} w_i\lambda_i$.

3　系统模型及安全目标

3.1　系统模型

本文提出的基于区块链的多授权可验证密文策略属性基等值测试加密方案的系统模型如图1所示,包括6个实体:属性授权机构(Attribute Authority, AA)、云服务提供商、区块链平台、外包服务器、数据拥有者和数据用户.

(1)属性授权机构:负责初始化系统,生成系统参数上传至区块链. 多个授权中心共同为数据拥有者和数据用户生成用户私钥.

(2)云存储提供商:半可信云服务提供商,负责存储数据拥有者上传的数据密文.

(3)区块链平台:部署了智能合约的联盟区块链. 区块链作为不可篡改的数据库,存储了验证参数,智能合约从云端下载密文数据,根据用户的陷门对两个密文进行等值测试. 验证智能合约根据数据用户上传的计算结果和区块链中存储的验证参数对数据进行完整性验证.

(4)外包服务器:半可信的第三方服务器,负责代替数据用户对开销较大的数据解密操作进行外包运算.

(5)数据拥有者:负责指定一个满足用户属性的访问结构并加密数据,将数据密文和测试陷门分别上传至云服务器和区块链平台存储.

(6)数据用户:负责计算并上传测试陷门至区块链平台存储,只有满足数据拥有者指定访问策略的数据用户才能被授权利用智能合约执行密文等值测试.

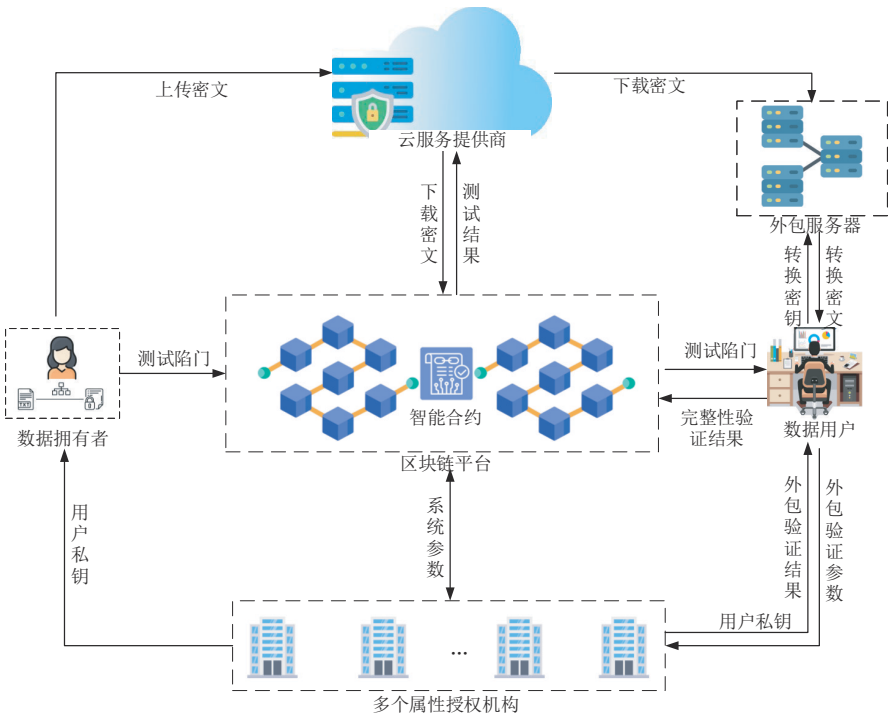


图1　系统模型

3.2　安全目标

对于本文提出的基于区块链的多授权密文策略属性基等值测试加密方案的安全性,需要考虑两类敌手[22]:

I类敌手 $\mathcal{A}_1$:拥有与挑战密文有关的测试陷门但不能从中判断对应哪个消息.

II类敌手 $\mathcal{A}_2$:无法获得与挑战密文有关的测试陷门,且不能区别挑战密文对应哪个消息.

在随机预言机模型下,本文模拟了敌手 $\mathcal{A}_1$ 与挑战者 $\mathcal{C}_1$ 之间的单向安全游戏和敌手 $\mathcal{A}_2$ 与挑战者 $\mathcal{C}_2$ 之间的判定性安全游戏,分别满足测试陷门的单向性和云端数据机密性. 该类模型在文献[23]已有详细的证明,此处不再赘述.

4　本文方案

(1)　系统初始化

算法输入安全参数,第一个属性授权机构 AA_1 执行全局初始化算法输出全局参数. 定义一个双线性映

射 e 为 $G_0\times G_0\to G_1$ 和两个阶为素数 P 的双线性群 G_0 和 G_1，生成元为 g. 属性机构 AA_1 选择 3 个哈希函数：$H_1\colon G_1\to G_0$，$H_2\colon\{0,1\}^*\to Z_p^*$ 和 $H_3\colon\{0,1\}^*\to\{0,1\}^{l_0+l_1}$，其中 l_0 和 l_1 分别表示 G_0 和 G_1 中的元素长度，输出全局参数 $\mathrm{params}=\left(e,G_0,G_1,p,g,H_1,H_2,H_3\right)$ 并上传至区块链供其他用户访问.

（2） 属性初始化算法

每个属性授权机构 AA_u 管理用户的不同属性，根据全局参数计算系统公钥和主密钥. 给定系统属性集合为 US，AA_u 表示第 u 个属性授权机构，负责的属性集合为 U_u. 对每个属性 $i\in U_u$，AA_u 随机选取 $\mathrm{att}_1,\cdots,\mathrm{att}_N\in G_0$ 和 $\alpha_i,\alpha_i',b_i\in Z_p^*$，秘密保存主密钥 $\mathrm{msk}=(g^{\alpha_i},g^{\alpha_i'},b_i)$，计算公钥 $\mathrm{mpk}=(g^{b_i},e(g,g)^{\alpha_i},e(g,g)^{\alpha_i'},\mathrm{att}_1,\cdots,\mathrm{att}_N)$，上传至区块链.

（3） 密钥生成

属性授权机构根据用户属性集合 U 和对应身份标识 gid，生成用户私钥. AA_u 在生成用户密钥时将用户 gid 与属性绑定，防止属性授权机构之间的合谋攻击. AA_u 具体操作如下：

①选择随机数 $t,t',a\in Z_p$，计算私钥组件 $\mathrm{sk}_0=\{K=g^{\alpha_i}g^{a_it},\ L=g^t,\ \{k_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^t\}_{i\in U}\}$ 和 $\mathrm{sk}_1=\{K'=g^{\alpha_i'}g^{a_it},L'=g^{t'},\{k'_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^{t'}\}_{i\in U}$；

②设置并发送私钥 $\mathrm{sk}_U=(\mathrm{sk}_0,\mathrm{sk}_1)$ 给用户.

（4） 数据加密

给定主公钥 mpk，消息 m 和访问策略 $(\boldsymbol{M},\rho)$，其中 $\boldsymbol{M}$ 是 $l\times n$ 矩阵，函数 ρ 将矩阵的每一行 $\boldsymbol{M}_i$ 映射为一个属性. 数据拥有者执行如下操作对 m 进行加密：

①随机选择一个向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)\in Z_p^n$，并计算份额 $\lambda_i=\boldsymbol{M}_i\cdot\boldsymbol{v}\,(i=1,\cdots,l)$；

② 随机选择 $u,y_1,\cdots,y_l\in Z_p$，并计算 $\tilde{C}=m^{\varepsilon}\cdot H_1(e(g,g)^{\alpha_i s})$，$C_0=g^s$，$C'=g^{\varepsilon}$，$\{C_i=g^{a_i\lambda_i}h_{\rho(i)}^{-y_i},D_i=g^{y_i}\}_{\forall 1\leqslant i\leqslant l}$，$\hat{C}=(m\|\varepsilon)\oplus H_3(e(g,g)^{\alpha_i's},\ \tilde{C},C_0,C',\boldsymbol{B})$ 和 $V=g^{H_4(e(g,g)^{\alpha_i s})}$，其中 $\boldsymbol{B}=(C_1,D_1,\cdots,\ C_l,D_l)$；

③ 输出密文 $\mathrm{CT}=(\tilde{C},C_0,C',\{C_i,D_i\}_{\forall 1\leqslant i\leqslant l},\hat{C})$ 上传到云服务器存储，同时将 V 和元组 $(\tilde{C},C')$ 作为参数上传至区块链平台保存，以验证外包解密正确性和数据完整性.

（5） 转换密文生成

为生成外包服务器用于解密的转换密钥，数据用户执行具体操作如下：

①随机选择盲化因子 $k,k'\in Z_p$，计算 $\tilde{t}=t/k,\tilde{t}'=t'/k'$；

② 计算转换密钥组件 $\mathrm{tk}_0=\{T=g^{\alpha_i/k}g^{a_i\tilde{t}},\ \tilde{L}=g^{\tilde{t}},\{\tilde{T}_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^{\tilde{t}}\}_{i\in U}\}$ 和 $\mathrm{tk}_1=\{T'=g^{\alpha_i'/k'}\cdot\ g^{a_i\tilde{t}'},\ \tilde{L}'=g^{\tilde{t}'},\{\tilde{T}'_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^{\tilde{t}'}\}_{i\in U}\}$；

③设置并发送转换密钥 $\mathrm{tk}=(\mathrm{tk}_0,\mathrm{tk}_1)$ 给外包服务器.

（6） 外包解密

收到用户发送的转换密钥 tk 后，外包服务器对云端下载的密文进行解密运算输出转换密文. 假设用户属性集合 U 满足 CT 中的策略 $(\boldsymbol{M},\rho)$，设置集合 $I=\{i\colon\rho(i)\in U\}$ 和 $\{\rho(i)\in Z_p\}_{i\in I}$. 根据拉格朗日插值多项式可知，如果 $\{\lambda_i\}$ 是依据矩阵 $\boldsymbol{M}$ 生成的隐私值 s 的合法秘密共享，则存在系数集 $\{\omega_i|i\in I\}$ 使等式 $\sum_{i\in I}\omega_i\cdot\lambda_i=s$ 成立. 外包服务器执行解密操作，分别计算 $X_{\mathrm{tra}}=\dfrac{e(C_0,T)}{\prod_{i\in I}(e(C_i,\tilde{L})e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}$ 和 $X'_{\mathrm{tra}}=\dfrac{e(C_0,T')}{\prod_{i\in I}(e(C_i,\tilde{L}')e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}$，将转换密文 $(X_{\mathrm{tra}},X'_{\mathrm{tra}})$ 上传到区块链平台存储.

（7） 密文等值测试

数据用户生成各自的测试陷门并上传到区块链平台，触发智能合约对从云端下载的两段密文 CT_A 和 CT_B 执行等值测试操作如下：

①数据用户根据密钥组件参数 k' 和 $\tilde{t}'$，计算测试陷门 $\mathrm{td}=(k',T'=g^{a_i'/k'}g^{a_i\tilde{t}'},\tilde{L}=g^{\tilde{t}'},\ \{\tilde{T}'_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^{\tilde{t}'}\}_{i\in U})$ 提交到区块链平台；

②智能合约接收到两段转换密文组件 $X_{\mathrm{tra}A}$，$X_{\mathrm{tra}B}$ 和陷门 $\mathrm{td}_A,\mathrm{td}_B$，计算 $X_A=\dfrac{\tilde{C}_A}{H_1((X_{\mathrm{tra}A})^{k_A})}$ 和 $X_B=\dfrac{\tilde{C}_B}{H_1((X_{\mathrm{tra}B})^{k_B})}$；

③智能合约检查 $e(C'_A,X_B)=e(C'_B,X_A)$ 是否成立. 若等式成立，向云服务器输出测试结果为“1”，代表两段密文 CT_A 和 CT_B 对应相同明文；否则，输出“0”表示 CT_A 和 CT_B 对应不同明文.

（8） 用户解密

①验证 $V=g^{H_4((X_{\mathrm{tra}})^k)}$ 是否成立，若成立则计算 $m\|\varepsilon=\hat{C}\oplus H_3((X'_{\mathrm{tra}A})^{k'},\tilde{C},C_0,C',\boldsymbol{B})$；否则输出“⊥”；

②计算 $\bar{C}=m^{\varepsilon}\cdot H_1(X_{\mathrm{tra}A})$ 和 $C_0'=g^{\varepsilon}$，上传验证参数 $\bar{C}$ 和 C_0' 到区块链平台，调用验证智能合约执行完整性验证算法；

③若完整性验证算法返回结果为“1”，代表云端数据通过完整性验证，数据用户接受并输出 m.

（9） 转换密文生成

当数据用户的验证参数 $\bar{C}$ 和 C_0' 被上传至区块链存储后，验证智能合约按预置规则执行验证操作. 验证智能合约检查 $\bar{C}=\tilde{C}$ 和 $C_0'=C_0$ 是否均成立，若成立则输出完整性验证结果为“1”；否则返回“⊥”.

5　方案分析与安全性证明

5.1　正确性分析

5.1.1　外包解密结果的正确性

外包服务器接收到数据用户属性集相关的转换密钥tk后,通过计算

$$X_{\text{tra}}=\frac{e(C_0,T)}{\prod_{i\in I}(e(C_i,\tilde{L})e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}$$

$$X'_{\text{tra}}=\frac{e(C_0,T')}{\prod_{i\in I}(e(C_i,\tilde{L}')e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}$$

对云端密文进行解密. 当tk满足密文中的访问结构,外包服务器才能计算出秘密值s的合法秘密共享,从而计算得到X_{tra}和X'_{tra}的值:

$$\begin{aligned}X_{\text{tra}}&=\frac{e(C_0,T)}{\prod_{i\in I}(e(C_i,\tilde{L})e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}\\&=\frac{e(g^s,g^{\alpha_i/k}g^{a\tilde{t}})}{\prod_{i\in I}(e(g^{a\lambda_i}H_2(\text{gid})^{b_i(-y_i)},g^{\tilde{t}})e(g^{y_i},H_2(\text{gid})^{b_i\tilde{t}}))^{\omega_i}}\\&=\frac{e(g,g)^{\alpha_i s/k}e(g,g)^{as\tilde{t}}}{(e(\prod_{i\in I}g^{a\lambda_i},g^{\tilde{t}})e(\prod_{i\in I}H_2(\text{gid})^{b_i(-y_i)}g^{\tilde{t}}))^{\omega_i}}\\&=\frac{e(g,g)^{\alpha_i s/k}e(g,g)^{as\tilde{t}}}{\prod_{i\in I}e(g,g)^{a\tilde{t}\lambda_i\omega_i}}\\&=e(g,g)^{\alpha_i s/k}\end{aligned}$$

$$\begin{aligned}X'_{\text{tra}}&=\frac{e(C_0,T')}{\prod_{i\in I}(e(C_i,\tilde{L}')e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}\\&=\frac{e(g^s,g^{\alpha'_i/k'}g^{a\tilde{t}'})}{\prod_{i\in I}(e(g^{a\lambda_i}H_2(\text{gid})^{b_i(-y_i)},g^{\tilde{t}'})e(g^{y_i},H_2(\text{gid})^{b_i\tilde{t}'}))^{\omega_i}}\\&=\frac{e(g,g)^{\alpha'_i s/k'}e(g,g)^{as\tilde{t}'}}{(e(\prod_{i\in I}g^{a\lambda_i},g^{\tilde{t}'})e(\prod_{i\in I}H_2(\text{gid})^{b_i(-y_i)}g^{\tilde{t}'}))^{\omega_i}}\\&=\frac{e(g,g)^{\alpha'_i s/k'}e(g,g)^{as\tilde{t}'}}{\prod_{i\in I}e(g,g)^{a\tilde{t}'\lambda_i\omega_i}}\\&=e(g,g)^{\alpha'_i s/k'}\end{aligned}$$

数据用户通过检查等式$V=g^{H_1((X_{\text{tra}})^k)}$是否成立以验证转化密文的正确性,其中$X_{\text{tra}}=e(g,g)^{\alpha_i s/k}$,则有$g^{H_1((X_{\text{tra}})^k)}=g^{H_1((e(g,g)^{\alpha_i s/k})^k)}=g^{H_1(e(g,g)^{\alpha_i s})}=V$. 因此,本文方案满足外包解密结果的正确性.

5.1.2　密文解密的正确性

数据用户通过计算$m\|\varepsilon=\hat{C}\oplus H_3((X'_{\text{tra}})^{k'},\tilde{C},C_0,C',\boldsymbol{B})$对密文进行解密,其中$k'$是盲化因子. 由于$X'_{\text{tra}}=e(g,g)^{\alpha'_i s/k'}$且$\boldsymbol{B}=(C_1,D_1,\cdots,C_l,D_l)$,则有:

$$\begin{aligned}&\hat{C}\oplus H_3((X'_{\text{tra}})^{k'},\tilde{C},C_0,C',\boldsymbol{B})\\&=(m\|\varepsilon)\oplus H_3(e(g,g)^{\alpha'_i s/k'})^{k'},\tilde{C},C_0,C',\boldsymbol{B})\\&=m\|\varepsilon\end{aligned}$$

数据用户计算并上传验证组件$\bar{C}=m^{\varepsilon}\cdot H_1(X_{\text{tra}A})$和$C'_0=g^{\varepsilon}$到区块链平台,智能合约验证$\bar{C}=\tilde{C}$和$C'_0=C_0$是否均成立来验证用户解密结果. 因此,本文方案满足签名验证等式的正确性.

5.1.3　等值测试结果的正确性

智能合约验证等式$e(C'_A,X_B)=e(C'_B,X_A)$是否成立来判断双方密文是否对应同一明文,等式中X_A与X_B的计算结果如下:

$$X_A=\frac{\text{CT}_A}{H_1((X_{\text{tra}A})^{k_A})}=\frac{m_A^{\varepsilon_A}H_1(e(g,g)^{\alpha_i k_A})}{H_1(e(g,g)^{\alpha_i k_A})}=m_A^{\varepsilon_A}$$

$$X_B=\frac{CT_B}{H_1((X_{\text{tra}B})^{k_B})}=\frac{m_B^{\varepsilon_B}H_1(e(g,g)^{\alpha_i k_B})}{H_1(e(g,g)^{\alpha_i k_B})}=m_B^{\varepsilon_B}$$

若消息$m_A^{\varepsilon_A}=m_B^{\varepsilon_B}$,则有:

$$e(C'_A,X_B)=e(g^{\varepsilon},m_B^{\varepsilon_B})=e(g^{\varepsilon_B},m_A^{\varepsilon_A})=e(C'_B,X_A)$$

即$e(C'_A,X_B)=e(C'_B,X_A)$. 由智能合约输出的密文等值测试结果可知,当$e(C'_A,X_B)=e(C'_B,X_A)$成立时,代表$m_A^{\varepsilon_A}=m_B^{\varepsilon_B}$,因此,本文方案满足等值测试结果的正确性.

5.2　安全性分析

5.2.1　等值测试结果可信性分析

验证智能合约按照预置规则执行密文等值测试操作,将测试结果生成交易发布在联盟区块链中,联盟链上的所有参与者对发布的测试结果进行验证. 因此,本文所提方案具有等值测试结果可信性.

5.2.2　数据完整性分析

验证智能合约通过检查$\bar{C}=\tilde{C}$和$C'_0=C_0$是否均成立来验证从云端数据的完整性,由于验证参数$\tilde{C}$和C_0采用链上存储方式,基于区块链的不可篡改特性,云存储服务器无法伪造或篡改云端数据. 因此,本文所提方案保证云服务提供商在执行存储密文过程中无法破坏数据完整性.

5.2.3　抗合谋攻击分析

合谋攻击分为未授权用户合谋和未授权用户与AA_u合谋两种情况. 针对未授权用户间的合谋情况,在用户私钥$\text{sk}_U=(\text{sk}_0,\text{sk}_1)$中,$k_{i,\text{gid}}=(H_2(\text{gid})^{b_i})^t{}_{i\in U}$和$k'_{i,\text{gid}}=(H_2(\text{gid})^{b_i})^{t'}{}_{i\in U}$将用户身份标识gid和每个属性$i\in U$进行了绑定,防止用户之间合谋构造属性组合恢复正确解密私钥. 针对用户与属性授权机构的合谋情况,AA_u为每个用户选择的随机元素t,t'. 因此,本文所提方案能抵抗未授权用户间的合谋攻击.

5.3　安全性证明

本文所提方案满足面对I类敌手时选择访问结构

下抗选择密文攻击的单向安全性(One-Way against Selective Access Structure and Chosen Ciphertext Attacks, OW-SAS-CCA),同时满足面对II类敌手时选择访问结构下抗选择密文攻击的不可区分性(Indistinguishable against Selective Access Structure and Chosen Ciphertext Attacks, IND-SAS-CCA).

定理1 假设q-parallel BDHE问题困难,则本文方案在随机预言模型下对I类敌手是OW-SAS-CCA安全的.

证明 假定I类敌手$\mathcal{A}_1$能以不可忽略的优势在概率多项式时间内在本节方案的单向安全游戏中获胜,则存在算法$\mathcal{C}_1$具有成功解决判定性q-parallel BDHE问题的能力. 随机给定一个q-parallel BDHE实例(y,Z),选取$\mu\in\{0,1\}$,若$\mu=0$,设置$Z=e(g,g)^{a^{q+1}s}$;若$\mu=1$,设置Z为G_1中的随机值.$\mathcal{C}_1$为了猜测出μ的值,与$\mathcal{A}_1$进行如下交互游戏.

初始化阶段:$\mathcal{A}_1$选取一个挑战访问结构$(\boldsymbol{M}^*,\rho^*)$,发送给$\mathcal{C}_1$.

建立阶段:$\mathcal{C}_1$随机选择元素α_1和α_1',通过计算$e(g,g)^{\alpha}=e(g,g)^{\alpha_1}\cdot e(g,g^{\alpha'})$和$e(g,g)^{\alpha'}=e(g,\ g)^{\alpha_1'}\cdot e(g,g^{\alpha'})$,设置$\alpha=\alpha_1+a^{q+1}$和$\alpha'=\alpha_1'+a^{q+1}$. 接着$\mathcal{C}_1$为每一个属性$h\in\{1,\cdots,n\}$选取对应的$\kappa_h$,令集合$U$满足$\{i:\rho(i)=h\}$,设置$\mathrm{att}_h=g^{\kappa_h}\prod_{i\in U^*}g^{aM^*_{i,1}/b_i}\cdot g^{a^2M^*_{i,2}/b_i}\cdot\cdots\cdot g^{a^{n^*}M^*_{i,n}/b_i}$. 若$U=\phi$,则有$\mathrm{att}_h=g^{\kappa_h}$为随机值.$\mathcal{C}_1$返回$\mathrm{mpk}=(g,g^a,e(g,g)^{\alpha_i},e(g,g)^{\alpha_i'},\mathrm{att}_1,\cdots,\mathrm{att}_n)$给$\mathcal{A}_1$.

询问阶段1:为了响应$\mathcal{A}_1$的询问,$\mathcal{C}_1$维持初始为空的列表L_{H_1}、L_{H_2}、L_{H_3},$\mathcal{C}_1$通过以下方式响应:.

(1)H_1哈希询问:给定一个群元素$R=G_1$,$\mathcal{C}_1$收到$\mathcal{A}_1$的H_1预言机询问后,遍历表L_{H_1},若存在元组(R,h_1),则返回h_1给$\mathcal{A}_1$;否则,$\mathcal{C}_1$选取$h_1\in G_1$,将(R,h_1)加入到L_{H_1}中并输出.

(2)H_2哈希询问:给定一个用户身份信息gid,$\mathcal{C}_1$收到$\mathcal{A}_1$的$H_2(\mathrm{gid},h_2)$预言机询问后,遍历表L_{H_2},若存在元组(gid,h_2),则返回h_1给$\mathcal{A}_1$;否则,$\mathcal{C}_1$选取$h_2\in Z_p^*$,将(gid,h_2)加入到L_{H_2}中并输出.

(3)H_3哈希询问:给定$R=(R,\tilde{C},C_0,C',\{C_i,D_i\}_{1\leqslant i\leqslant l})$,$\mathcal{C}_1$遍历表$L_{H_3}$,若存在元组$(R,h_3)$,则返回$h_3$给$\mathcal{A}_1$;否则,$\mathcal{C}_1$选取$h_3\in\{0,1\}^{l_1+l_2}$,将$(R,h_3)$加入到$L_{H_3}$中并输出.

(4)秘密提取询问:收到属性集合U后,$\mathcal{C}_1$首先计算tk. $\mathcal{C}_1$随机选择$\delta,k'\in Z_q^*$,并挑选一个向量$\boldsymbol{\omega}=(\omega_1,\omega_2,\cdots,\omega_{n^*})\in Z_q^*$,其满足$\omega_1=-1$,能够对所有$i\in I=\{i:\rho^*(i)\in U\}$有$\boldsymbol{\omega}\cdot\boldsymbol{M}_i^*=0$成立.$\mathcal{C}_1$通过计算$\tilde{L}'=g^{\delta/k'}\prod_{i=1}^{n^*}(g^{a^{q+1-i}})^{\omega_i/k'}=g^{\tilde{t}'}$,定义$\tilde{t}'=(\delta+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_na^{q-n+1})/k'$,这样定义使得$g^{a_i\tilde{t}'}$包含项$g^{a^{q+1}/k'}$,在构造$T'$时可以与$g^{\alpha_i'/k'}$的$g^{a^{q+1}/k'}$消除.$\mathcal{C}_1$设置$T'=g^{\alpha'/k'}g^{a_i\tilde{t}'}=g^{(\alpha_1'+a_i^{q+1})/k'}g^{a_i\tilde{t}'}=g^{a_1'/k'}g^{a\delta/k'}\cdot\prod_{i=2}^{n^*}(g^{a^{q+2-i}})^{\omega_i/k'}$. 对所有$h\in U$,如果不存在使$\rho^*(i)=h$成立的$i$,$\mathcal{C}_1$设置$T_h'=\mathrm{att}_h^{\tilde{t}'}=(g^{\kappa_h})^{\tilde{t}'}=(g^{\tilde{t}'})^{\kappa_h}=(\tilde{L}')^{\kappa_h}$. 如果$U=\{i:\rho^*(i)=h\}$,$\mathcal{C}_1$构造$T_h'$如下:

$$T_h'=\mathrm{att}_h^{\tilde{t}'}=(g^{\kappa_h})^{\tilde{t}'}=(g^{\tilde{t}'})^{\kappa_h}$$
$$=(\tilde{L}')^{\kappa_h}\prod_{i\in U}\prod_{j=1}^{n^*}(g^{(a^j/\mu_i)r}\prod_{v=1,v\neq j}^{n^*}(g^{a^{q+1+j-v}/\mu_i})^{\omega_v})^{M^*_{i,j}/k'}$$

由于构造的T_h'要求不包含$\mathcal{C}_1$不能模拟的项g^{a^{q+1}/μ_i},所以能够防止g^{a^{q+1}/μ_i}项由于满足$\boldsymbol{\omega}\cdot\boldsymbol{M}_i^*=0$性质而被抵消. 至此,$\mathcal{C}_1$计算得到$\mathrm{tk}=(T,\tilde{L},\tilde{T}_{i,\mathrm{gid}})$,随后计算tk'如下:

$\mathcal{C}_1$随机选取新元素$\tilde{t},k\in Z_p$,计算$T=g^{\alpha/k}g^{\tilde{t}}=g^{(\alpha_1+a_i^q)/k}g^{\tilde{t}}=g^{\alpha_1/k}g^{a_i^q}g^{\tilde{t}}$,$\tilde{L}=g^{\tilde{t}}$和$\{\tilde{T}_{i,\mathrm{gid}}=(H_2(\mathrm{gid})^{b_i})^{\tilde{t}}\}_{i\in U}$,返回私钥$\mathrm{sk}_U=\{\mathrm{sk}_0,\mathrm{sk}_1\}$.

(5)测试陷门询问:给定一个属性集合U,当$\mathcal{C}_1$收到$\mathcal{A}_1$对U对应的陷门td_U询问后,若U满足挑战矩阵$(\boldsymbol{M}^*,\rho^*)$,$\mathcal{C}_1$随机选择新$k,\tilde{t}$并执行秘密提取询问计算对应$\mathrm{td}_U=(k,\mathrm{tk}_0)$;否则,有上述方式得到并返回$\mathrm{td}_U=(k,\mathrm{tk}_0)$.

(6)解密询问:给定$\mathrm{CT}=(\tilde{C},C_0,C',\{C_i,D_i\}_{\forall 1\leqslant i\leqslant l},\hat{C})$,当$\mathcal{A}_1$以$(U,\mathrm{CT})$作为输入发起询问后,$\mathcal{C}_1$执行如下操作:

①若U不满足$(\boldsymbol{M}^*,\rho^*)$,$\mathcal{C}_1$采用秘密提取的方式计算得到对应私钥$\mathrm{sk}_U$. 接着,$\mathcal{C}_1$运行解密算法输出CT解密结果发送给$\mathcal{A}_1$.

②若U满足$(\boldsymbol{M}^*,\rho^*)$,$\mathcal{A}_1$没有直接获得私钥$\mathrm{sk}_U$的能力.$\mathcal{C}_1$首先通过上述方式计算陷门$\mathrm{td}_U=(k,\mathrm{tk}_0)$,并执行外包解密算法计算

$$X_{\mathrm{tra}}=\frac{e(C_0,T)}{\prod_{i\in I}(e(C_i,\tilde{L})e(D_i,\tilde{T}_{\rho(i)}))^{\omega_i}}.$$

然后,$\mathcal{C}_1$遍历表L_{H_1},若不存在元组$((X_{\mathrm{tra}})^k,h_1)$,$\mathcal{C}_1$输出"$\perp$";否则,$\mathcal{C}_1$遍历表$L_{H_3}$,若表$L_{H_3}$中不存在元组$((X'_{\mathrm{tra}})^{k'},\tilde{C},C_0,C',\{C_i,\ D_i\}_{1\leqslant i\leqslant l},h_3)$,$\mathcal{C}_1$输出"$\perp$";否则,对在表$L_{H_3}$中找到的该形式元组,计算$m\|\varepsilon=\hat{C}\oplus h_3$. 并且,若$C'=g^{\varepsilon}$和$\bar{C}=m^{\varepsilon}\cdot H_1((X_{\mathrm{traA}})^k)$均成立,输出对应明文消息.

挑战阶段:$\mathcal{A}_1$向$\mathcal{C}_1$提交两个等长的挑战消息m_0和m_1,$\mathcal{C}_1$执行以下操作:

(1)随机选择$\beta\in\{0,1\}$和元素$\varepsilon^*\in Z_p$,计算$\tilde{C}^*=$

$(m_\beta^*)^{\varepsilon^*}\cdot H_1(Z\cdot e(g^s,g^{\alpha_i}))$，$C_0^*=g^s$ 和 $C'^*=g^{\varepsilon^*}$.

（2）选择 $r_2',\cdots,r_n'\in Z_p^{n^*}$，通过向量 $\boldsymbol{v}=(s,\ sa+r_2',sa^2+r_3',\cdots,sa^{n-1}+y_{n^*}')\in Z_p^{n^*}$ 对秘密值 s 进行分割共享．定义集合 X_i 中包含所有满足 $\{x: x\neq i\wedge\rho^*(i)=\rho^*(x)\}$ 的 x 值.

（3）随机选择 $y_1',\cdots,y_l'\in Z_p$，计算挑战密文中的密文组件如下：

$$C_i^*=h_{\rho(i)}^{-y_i'}\Big(\prod_{j=2}^{n^*}(g^{a_i})^{M_{i,j}^*r_i'}\Big)(g^{\mu_i s})^{-k\rho^*(i)}\Big(\prod_{x\in X_i}\prod_{j=1}^{n^*}g^{a_i^j s(\mu_i/\mu_x)}\Big)^{M_{x,j}^*}$$

$$D_i^*=g^{-y_i'}g^{-s\mu_i}$$

$$\hat{C}^*=(m^*\|\varepsilon)\oplus H_3(Z\cdot e(g^s,g^{\alpha_i'}),\tilde{C}^*,C_0^*,C'^*,C_1^*,D_1^*,\cdots,C_l^*,D_l^*)$$

并返回 $\mathrm{CT}^*=(\tilde{C}^*,C_0^*,C'^*,C_1^*,D_1^*,\cdots,C_l^*,D_l^*,\hat{C}^*)$ 给 $\mathcal{A}_1$.

询问阶段 2：与询问阶段 1 类似，区别在于此阶段限制 $\mathcal{A}_1$ 提交满足 $(\boldsymbol{M}^*,\rho^*)$ 的 U，并以 (U,CT^*) 为输入进行任何秘密提取查询和解密查询.

猜测阶段：$\mathcal{A}_1$ 输出一个对 β 的猜测 $\beta'\in\{0,1\}$，若 $\beta=\beta'$，$\mathcal{C}_1$ 输出 $\mu'=0$，则有 $Z=e(g,g)^{a^{q+1}s}$，说明 $\mathcal{A}_1$ 在游戏中获胜；否则，$\mathcal{C}_1$ 输出 $\mu'=1$，表示 Z 是群 G_1 中的随机元素．若 $\mu'=0$，$\mathcal{C}_1$ 提供的模拟是完善的，此时 $\mathcal{A}_1$ 赢的优势为 $\Pr[\mu'=0,\mu=0]=\frac{1}{2}$；若 $\mu'=1$，密文 CT′会由于 Z 是随机元素被隐藏，$\mathcal{A}_1$ 成功猜测出 $\beta=\beta'$ 的概率是可忽略的．若 $\mathcal{A}_1$ 能够以不可忽略的概率打破该方案的 OW-SAS-CCA 安全，则 $\mathcal{C}_1$ 能够以不可忽略的大于 $\frac{1}{2}$ 的概率求解出判定性 q-parallel BDHE 问题的解．然而，判定性 q-parallel BDHE 在多项式时间内是难以解决的．因此，本文方案在面对 I 类敌手时，满足 OW-SAS-CCA 安全．证毕.

定理 2　假设 q-parallel BDHE 问题困难，则本文方案在随机预言模型下对 II 类敌手是 IND-SAS-CCA 安全的.

证明　假设 II 类敌手 $\mathcal{A}_2$ 能以不可忽略的优势在 PPT 时间内在本节方案的判定性安全游戏中获胜，则存在算法 $\mathcal{C}_2$ 能成功解决判定性 q-parallel BDHE 问题．随机给定输入为 (y,Z) 的困难问题实例，若 $\mu=0$，则 $Z=e(g,g)^{a^{q+1}s}$；若 $\mu=1$，则 Z 为 G_1 中的随机元素．$\mathcal{C}_2$ 的目标是给出 μ 值的猜测作为对困难问题的解.

初始化阶段：$\mathcal{A}_2$ 选取一个挑战访问结构 $(\boldsymbol{M}^*,\rho^*)$，发送给 $\mathcal{C}_2$.

询问阶段 1：$\mathcal{A}_2$ 可以模拟定理 1 证明过程中定义的“H_1 哈希询问”、“H_2 哈希询问”、“H_3 哈希询问”和“测试陷门询问”游戏操作．另外，需要对“测试陷门询问”增加“$\mathcal{A}_2$ 不得提交满足挑战矩阵的属性集进行询问”的限制.

秘密提取询问：收到属性集合 U 后，$\mathcal{C}_2$ 采用定理 1 中的方式计算 tk_1，随后计算 tk_0 如下：

① $\mathcal{C}_2$ 随机选择 $\delta,k\in Z_q^*$，并挑选一个向量 $\boldsymbol{\omega}=(\omega_1,\omega_2,\cdots,\omega_{n^*})\in Z_q^*$，其中 $\omega_1=-1$，能够对所有 $i\in I=\{i:\rho^*(i)\in U\}$ 有 $\boldsymbol{\omega}\cdot\boldsymbol{M}_i^*=0$ 成立 $\mathcal{A}_1$.

② $\mathcal{C}_2$ 通过计算 $\tilde{L}=g^{\delta/k}\prod_{i=1}^{n^*}(g^{a^{q+1-i}})^{\omega_i/k}=g^{\tilde{t}}$，定义 $\tilde{t}=(\delta+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_na^{q-n+1})/k$.

③ $\mathcal{C}_2$ 计算 $T=g^{\alpha/k}g^{a_i\tilde{t}}=g^{(\alpha_1+a_i^{q+1})/k}g^{a_i\tilde{t}}=g^{\alpha_1/k}g^{a\delta/k}\prod_{i=2}^{n^*}(g^{a^{q+2-i}})^{\omega_i/k}$.

由于 $\mathcal{C}_2$ 无法成功模拟出 $g^{a_i\tilde{t}}$ 中的 $g^{a^{q+1}/k}$ 项，只能通过计算与 $g^{\alpha_i/k}$ 中的 $g^{a^{q+1}/k}$ 项相抵.

解密询问：解密询问与定理 1 解密询问在 U 不满足 $(\boldsymbol{M}^*,\rho^*)$ 情况下证明的过程一致．当 U 满足 $(\boldsymbol{M}^*,\rho^*)$ 时，$\mathcal{A}_2$ 没有直接获得 U 相关的陷门或私钥的能力．$\mathcal{C}_2$ 遍历表 L_{H_3}，若未找到元组 $((X_{\mathrm{tra}}')^{k'},\tilde{C},C_0,C',\{C_i,D_i\}_{1\leqslant i\leqslant l},h_3)$，$\mathcal{C}_2$ 输出“⊥”；否则，对每个找到的相同形式元组，$\mathcal{C}_2$ 计算 $m\|\varepsilon=\hat{C}\oplus h_3$．若 $C'=g^{\varepsilon}$ 成立，$\mathcal{C}_2$ 计算 $h_1=\bar{C}/m^{\varepsilon}$，同时在表 L_{H_1} 中查找 $((X_{\mathrm{tra}})^k,h_1)$．若表 L_{H_1} 存在该元组，返回明文消息 m.

挑战阶段：与定理 1 的证明过程类似.

询问阶段 2：$\mathcal{C}_2$ 模拟过程类似定理 1，并限制 $\mathcal{A}_2$ 不得提交任何满足 $(\boldsymbol{M}^*,\rho^*)$ 的 U 以进行测试陷门询问.

猜测阶段：$\mathcal{A}_2$ 输出一个 $\beta'\in\{0,1\}$ 进行猜测，若 $\beta=\beta'$，则 $\mathcal{C}_2$ 输出 $\mu'=0$，则有 $Z=e(g,g)^{a^{q+1}s}$，说明 $\mathcal{A}_2$ 在游戏中获胜；否则，$\mathcal{C}_2$ 输出 $\mu'=1$，表示 Z 是群 G_1 中的随机元素．若 $\mu'=0$，$\mathcal{C}_1$ 提供的模拟是完善的，则有 $\Pr[\mu'=0,\mu=0]=\frac{1}{2}+\mathrm{Adv}_{\mathcal{A}_2}^{\mathrm{IND-SAS-CCA}}(x)$；若 $\mu'=1$，密文 CT^* 会通过随机隐藏消息明文，$\mathcal{A}_2$ 成功猜测出 $\beta=\beta'$ 的概率为 $\frac{1}{2}$．若 $\mathcal{A}_2$ 能够以不可忽略的概率打破该方案的 IND-SAS-CCA 安全，则 $\mathcal{C}_2$ 能够以大于 $\frac{1}{2}$ 的不可忽略优势求出判定性 q-parallel BDHE 问题的解．然而，判定性 q-parallel BDHE 在多项式时间内是难以解决的．因此，本文方案在面对 II 类敌手时，满足 IND-SAS-CCA 安全．证毕.

6　性能分析

6.1　特性分析

将本文所提方案与已有的支持密文等值测试的 CP-ABE 方案[21~23]在功能特性方面进行对比，对比结果如表 1 所示．与文献[21~23]相比，所提方案利用多授权机构，解决了单授权机构存在的性能瓶颈和单点失效问题；通过引入区块链技术，消除了已有方案中测试

操作对可信云服务器的依赖. 与文献[23]相比,本文方案利用区块链存储验证信息,具有对外包解密结果正确和云端数据完整的可验证性.

表1 特性对比

方案	多授权属性机构	区块链	去中心化测试	外包可验证	完整性验证
文献[21]	×	×	×	×	√
文献[22]	×	×	√	√	×
文献[23]	×	×	×	×	×
本文方案	√	√	√	√	√

6.2 效率分析

将本文提出的新方案在计算性能方面与文献[21~23]方案进行比较,使用i5-8250U CPU 1.80 GHz处理器,8 GB内存和win10 64位操作系统. 在VC6.0环境下,通过调用基于配对的密码学(Pairing-Based Cryptography, PBC)库对新方案和其他对比方案进行了仿真模拟,对比结果如表2和图2所示.

表2主要探讨了方案中时间开销较大的幂运算和双线性对运算,其中T_e为群G上的幂运算时间;T_p是双线性配对时间. 令$|U|$表示属性集大小;$|AA|$表示本文方案中属性授权机构数量. 由表2可知,本文方案在私钥生成阶段的计算开销与授权机构个数相关,降低了其他文献中与属性个数相关的计算成本. 等值测试过程中,本文方案通过部署在区块链上的智能合约代替用户执行密文等值测试操作,相比其他方案消除了双线性对的计算开销. 外包可验证思想的引入,使得新方案在用户解密阶段的计算开销略高于文献[23],但通过验证外包解密结果正确性,确保了解密结果的正确性.

表2 计算开销对比

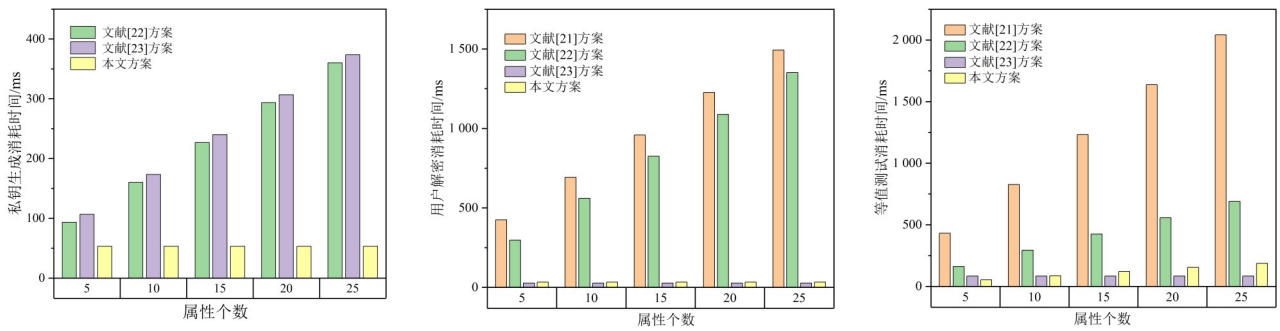
方案	私钥生成	等值测试	用户解密
文献[21]	$(4+6\|U\|+12\|U\|^2)T_e$	$(8\|U\|+4)T_e+14T_p$	$(8\|U\|+6)T_e+12T_p$
文献[22]	$(4+2\|U\|)T_e$	$\|U\|T_e+(2\|U\|+3)T_p$	$(2\|U\|+2)T_e+(4\|U\|+2)T_p$
文献[23]	$(6+2\|U\|)T_e$	$2T_e+2T_p$	$4T_e$
本文方案	$(4+2\|AA\|)T_e$	$(\|U\|+3)T_e$	$5T_e$

在图2(a)中,设置本文属性授权机构数量为2. 文献[22,23]生成私钥消耗时间均与属性个数相关,而本文方案的花费时间恒定. 当属性数量为5时,本文所提新方案在私钥生成阶段的计算开销分别比文献[22,23]方案减少了42.86%和50.13%;随着属性个数增多,新方案在私钥生成阶段的性能优势更加明显.

由图2(b)可知,在等值测试阶段,本文方案与文献[21, 22]所需测试时间随属性增加,文献[23]测试时间固定. 与文献[21,22]相比,本文方案测试时间增幅较小. 当属性数量为5时,本文方案在等值测试阶段的时间开销比文献[21,22]分别降低85.48%和78.82%,且随着属性个数增加性能优势更加明显. 本文方案的测试开销略高于文献[23],但采用智能合约执行密文等值测试操作,实现了去中心化授权检索.

由图2(c)可知,本文方案与文献[23]在解密时将大部分解密操作外包给服务器,具有比文献[21,22]高的解密性能. 与文献[23]相比较,本文方案增加一次指数运算来验证外包解密结果正确性,但消除了对外包服务器的可信依赖.

通过上述分析可以看出,新方案在私钥生成阶段的具有较高计算性能,尽管在等值测试和解密阶段的开销略高于文献[23],但引入区块链技术消除了依赖可信第三方的问题,具有更高的安全性能.



(a) 私钥生成时间对比 (b) 等值测试时间对比 (c) 用户解密时间对比

图2 时间开销对比

7 结束语

云存储技术拥有降低本地开销、可扩展存储空间等优点,具有十分广阔的应用前景. 针对现有云存储环境下CP-ABE方案中密文授权检索分类困难和对第三方服务器的可信依赖问题,本文提出了一种基于区块链的多授权密文策略属性基等值测试加密方案. 基于多授权的密文策略属性基密码体制对云端数据进行加密,确保了云端数据的机密性. 利用部署在区块链

中的智能合约执行等值测试和数据完整性验证操作，消除了对半可信云服务器的依赖．采用外包服务器执行复杂部分的解密运算，降低了数据用户解密和测试的计算开销．通过与现有支持等值测试功能的加密方案对比分析，本文所提方案满足更多安全属性，同时降低了部分操作的计算开销．在未来的工作中，将尝试设计支持多密文等值测试的密文策略属性基加密方案．

参考文献

[1] 冯朝胜, 秦志光, 袁丁, 等. 云计算环境下访问控制关键技术[J]. 电子学报, 2015, 43(2): 312-319.
FENG C S, QIN Z G, YUAN D, et al. Key techniques of access control for cloud computing[J]. Acta Electronica Sinica, 2015, 43(2): 312-319. (in Chinese)

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

[3] LI J, ZHANG Y H, CHEN X F, et al. Secure attribute-based data sharing for resource-limited users in cloud computing[J]. Computers & Security, 2018, 72: 1-12.

[4] 赵志远, 王建华, 朱智强, 等. 面向物联网数据安全共享的属性基加密方案[J]. 计算机研究与发展, 2019, 56(6): 1290-1301.
ZHAO Z Y, WANG J H, ZHU Z Q, et al. Attribute-based encryption for data security sharing of Internet of Things [J]. Journal of Computer Research and Development, 2019, 56(6): 1290-1301. (in Chinese)

[5] CHEN N Y, LI J G, ZHANG Y C, et al. Efficient CP-ABE scheme with shared decryption in cloud storage[J]. IEEE Transactions on Computers, 2022, 71(1): 175-184.

[6] ZHANG L Y, CUI Y L, MU Y. Improving security and privacy attribute based data sharing in cloud computing[J]. IEEE Systems Journal, 2020, 14(1): 387-397.

[7] 关志涛, 杨亭亭, 徐茹枝, 等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报, 2015, 36(6): 120-130.
GUAN Z T, YANG T T, XU R Z, et al. Multi-authority attribute-based encryption access control model for cloud storage[J]. Journal on Communications, 2015, 36(6): 120-130. (in Chinese)

[8] CHASE M. Multi-authority attribute based encryption[M]// Theory of Cryptography. Berlin: Springer, 2007: 515-534.

[9] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//Advances in Cryptology—EUROCRYPT 2011. Berlin: Springer, 2011: 568-588.

[10] GAO S, PIAO G R, ZHU J M, et al. TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5784-5798.

[11] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//Advances in Cryptology—EUROCRYPT 2004. Berlin: Springer, 2004: 506-522.

[12] YANG G M, TAN C H, HUANG Q, et al. Probabilistic public key encryption with equality test[C]//Topics in Cryptology—CT-RSA 2010. Berlin: Springer, 2010: 119-131.

[13] TANG Q. Towards public key encryption scheme supporting equality test with fine-grained authorization[C]// Information Security and Privacy. Berlin: Springer, 2011: 389-406.

[14] TANG Q. Public key encryption schemes supporting equality test with authorisation of different granularity[J]. International Journal of Applied Cryptography, 2012, 2(4): 304-321.

[15] MA S, ZHANG M W, HUANG Q, et al. Public key encryption with delegated equality test in a multi-user setting[J]. The Computer Journal, 2015, 58(4): 986-1002.

[16] HUANG K B, TSO R, CHEN Y C, et al. PKE-AET: Public key encryption with authorized equality test[J]. The Computer Journal, 2015, 58(10): 2686-2697.

[17] LIN X J, SUN L, QU H P. Generic construction of public key encryption, identity-based encryption and signcryption with equality test[J]. Information Sciences, 2018, 453: 111-126.

[18] MA S. Identity-based encryption with outsourced equality test in cloud computing[J]. Information Sciences, 2016, 328: 389-402.

[19] MING Y, WANG E X. Identity-based encryption with filtered equality test for smart city applications[J]. Sensors, 2019, 19(14): 3046.

[20] QU H P, YAN Z, LIN X J, et al. Certificateless public key encryption with equality test[J]. Information Sciences, 2018, 462: 76-92.

[21] WANG Q, PENG L, XIONG H, et al. Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing[J]. IEEE Access, 2018, 6: 760-771.

[22] CUI Y Z, HUANG Q, HUANG J Y, et al. Ciphertext-policy attribute-based encrypted data equality test and classifi-

cation[J]. The Computer Journal, 2019, 62(8): 1166-1177.
[23] CUI Y Z, HUANG Q, HUANG J Y, et al. Outsourced ciphertext-policy attribute-based encryption with equality test[C]//Information Security and Cryptology. Cham: Springer International Publishing, 2019: 448-467.
[24] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Public Key Cryptography—PKC 2011. Berlin: Springer, 2011: 53-70.
[25] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008-08-21) [2022-08-10]. http://bitcoin.org/bitcoin.pdf, 2009.
[26] 朱健, 胡凯, 张伯钧. 智能合约的形式化验证方法研究综述[J]. 电子学报, 2021, 49(4): 792-804.
ZHU J, HU K, ZHANG B J. Review on formal verification of smart contract[J]. Acta Electronica Sinica, 2021, 49(4): 792-804. (in Chinese)
[27] CHEN B W, HE D B, KUMAR N, et al. A blockchain-based proxy re-encryption with equality test for vehicular communication systems[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(3): 2048-2059.

作者简介

杨小东 男, 1981 年出生于甘肃甘谷. 现为西北师范大学教授、硕士生导师. 主要研究方向为现代密码学和云计算安全.
E-mail: y200888@163.com

陈艾佳 女, 1995 年出生于甘肃兰州. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为属性基加密.
E-mail: papchen217@163.com

汪志松 男, 1998 年出生于江苏盐城. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为代理重签名.
E-mail: 1216053764@qq.com

廖泽帆 男, 1997 年出生于甘肃兰州. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为电力数据安全.
E-mail: lzf0097@163.com

王彩芬 女, 1963 年出生于河北安国. 现为深圳技术大学大数据与互联网学院教授、博士生导师. 主要研究方向为大数据安全.
E-mail: wangcaifen@sztu.edu.cn