基于区块链且支持验证的属性基搜索加密方案

闫玺玺，原笑含，汤永利，陈艳丽
（河南理工大学计算机科学与技术学院，河南 焦作 454003）

摘 要：针对一对多搜索模型下共享解密密钥缺乏细粒度访问控制且搜索结果缺乏正确性验证的问题，提出了一种基于区块链且支持验证的属性基搜索加密方案。通过对共享密钥采用密文策略属性加密机制，实现细粒度访问控制。结合以太坊区块链技术，解决半诚实且好奇的云服务器模型下返回搜索结果不正确的问题，在按需付费的云环境下，实现用户和云服务器之间服务−支付公平，使各方诚实地按照合约规则执行。另外，依据区块链的不可篡改性，保证云服务器得到服务费，用户得到正确的检索结果，而不需要额外验证，减少用户计算开销。安全性分析表明，所提方案满足自适应选择关键词语义安全，能很好地保护用户的隐私以及数据的安全。性能对比及实验结果表明，所提方案在安全索引产生、搜索令牌生成、检索效率以及交易数量方面有一定的优化，更加适用于智慧医疗等一对多搜索场景。

关键词：对称可搜索加密；属性基加密；以太坊智能合约；可验证
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020011

Verifiable attribute-based searchable encryption scheme based on blockchain

YAN Xixi, YUAN Xiaohan, TANG Yongli, CHEN Yanli
School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China

Abstract: For the problem that the shared decryption key lacks of fine-grained access control and the search results lacks of correctness verification under one-to-many search model, a verifiable attribute-based searchable encryption scheme based on blockchain was proposed. The ciphertext policy attribute-based encryption mechanism was used on the shared key to achieve fine-grained access control. Ethereum blockchain technology was combined to solve the problem of incorrect search results returned by the semi-honest and curious cloud server model, so it could prompt both the cloud server and the user to follow the rules of the contract honestly and achieved service-payment fairness between the user and the cloud server in the pay-per-use cloud environment. In addition, based on the irreversible modification of the blockchain, the cloud server was guaranteed to receive the service fee, and the user was assured to obtain the correct retrieval results without additional verification which reduced the computational overhead of the user. The security analysis shows that the scheme satisfies the semantic security against adaptive chosen keyword attack and can protect the privacy of users and the security of data. The performance comparison and experimental results show that the scheme has certain optimizations in security index generation, search token generation, retrieval efficiency and transaction quantity, so it is more suitable for one-to-many search scenarios such as smart medical.

Key words: symmetric searchable encryption, attribute-based encryption, ethereum smart contract, verifiable

收稿日期：2019−09−04；**修回日期**：2019−11−26
通信作者：陈艳丽，yanlichen@hpu.edu.cn
基金项目：国家自然科学基金资助项目（No.61802117）；河南省高校科技创新团队基金资助项目（No.20IRTSTHN013）；河南省科技攻关基金资助项目（No.192102210280）；河南省高等学校青年骨干教师基金资助项目（No.2018GGJS058）；河南省高等学校重点科研基金资助项目（No.20A413005, No.19A520025）

Foundation Items: The National Natural Science Foundation of China (No.61802117), The Innovative Scientists and Technicians Team of Henan Provincial High Education (No.20IRTSTHN013), Projects of Henan Provincial Department of Science and Technology (No.192102210280), Research Foundation of Young Core Instructor in Henan province (No.2018GGJS058), Key Scientific Research Project of Henan Higher Education Institutions (No.20A413005, No.19A520025)

1 引言

云环境下“一切即服务”的商业模式和按需付费的特点，使用户支付一定的服务费便能享受到云端提供的各种服务，云存储模式下廉价的计算和巨大的容量吸引越来越多的用户为节约本地存储和维护开销将私人数据外包至云端服务器。但由于用户失去了对数据的实际控制，考虑到云服务器的不可信以及保障用户数据的隐私安全，数据需要在用户上传前进行加密处理，然而加密操作使基于明文的关键词检索技术无法使用。可搜索加密（SE, searchable encryption）技术的提出[1]实现了在不泄露用户数据隐私的条件下完成对加密数据的搜索。

社交网络、智慧医疗等云环境下，常常采用一对多的搜索模型，因此密文策略属性基加密（CP-ABE, ciphertext-policy attribute-based encryption）机制和可搜索加密机制的结合是目前的研究热点。基于密文策略属性基加密方案[2]使数据拥有者可以指定访问策略，实现细粒度访问控制。Yin 等[3]结合 CP-ABE 方案实现了可搜索加密方案，在安全索引上指定访问结构，只有用户的属性满足访问策略时才可以进行搜索。刘振华等[4]提出了支持关键词搜索的属性代理重加密方案，将密钥分为搜索密钥和属性密钥，实现密文检索和数据安全共享，并有效地隐藏搜索模式。孙瑾等[5]提出支持属性撤销的可验证多关键词密文检索方案，在密文中捆绑撤销信息，当属性撤销后无法检索和解密密文消息。Curtmola 等[6]将可搜索加密应用在多用户场景中，然而解密密钥被多个用户共享会增加其泄露的风险。因此，将属性基加密技术应用到搜索加密机制中，能够解决一对多搜索模式下数据拥有者和多用户之间共享搜索密钥导致密钥管理难度大的问题，且支持数据拥有者对搜索结果进行细粒度访问控制。

另外，在云环境的实际应用中，云服务器是半诚实且好奇的实体，存在为了节省计算或骗取服务费返回部分或不正确搜索结果的情况，这就需要用户验证搜索结果的正确性和完整性。Chai 等[7]首次提出可验证的对称密文检索方案，用户根据检索路径的散列序列对结果进行验证。Jiang 等[8]提出可验证的多关键词排序搜索方案，用户端采用消息验证码验证返回结果的正确性。杜瑞忠等[9]基于倒排索引提出可验证混淆关键词的搜索方案，该方案需要数据拥有者和用户事先通过安全信道共享验证集合，用户端先利用双线性映射确定返回的结果是否包含查询关键词，再验证返回结果正确性。以上方案均需要用户本地进行验证，计算开销较大。为了减轻用户的计算负担，伍祈应等[10]引入第三方可信审计机构对结果进行验证，验证时间与返回密文集合的大小有关。但是，现有的大多数可验证 SE 方案中，重点在于检测恶意行为，缺乏某种机制去惩罚不诚实执行者。

在按需付费的云环境下，云服务器想在返回搜索结果前得到服务费，用户想在验证正确后支付服务费，同时云服务器可能在得到服务费后返回不正确的结果，用户可能在得到正确结果后声称不正确而不支付服务费，导致服务−支付不公平的现象。这就需要一种可靠的密文检索方案，不仅能够有效地检测出恶意操作，而且支持公平支付机制，惩罚恶意行为。服务−支付不公平问题的解决，往往依赖于可信第三方，如银行，当发生冲突时需要银行耗费时间来解决。为了消除第三方机构，在点对点网络中快速实现公平支付，区块链技术受到了广泛的关注。由于区块链不可篡改的性质，引入区块链公平机制到可搜索加密机制中，实现服务−支付公平，保证用户和云服务器只要诚实地按照协议执行，云服务器就可以得到相应的服务费，同时用户得到正确的搜索结果。一旦云服务器被检测到不诚实，就得不到服务费并且会受到损失保证金的惩罚。此外，用户在搜索结果正确的前提下，不可否认云服务器提供的结果以拒绝支付服务费。Cai 等[11]在分布式存储中实现动态的关键词检索，结合区块链技术，在客户端和服务器之间进行公平搜索。Zhang 等[12]以在区块链中临时冻结押金的形式实现手续费的公平支付而不需要可信机构，保证参与方诚实执行就能得到搜索结果以及服务费，但是在验证结果正确性过程中需要用户端进行大量的签名验证计算，用户开销较大。Wang 等[13]结合区块链技术实现公平支付，采用智能合约存储安全索引并执行搜索，解决云服务器返回不正确结果的情况，保证用户只要支付了手续费就总能得到正确的结果，虽有效地进行细粒度访问控制，但只支持“与”门访问策略，表达不灵活。Chen 等[14]提出支持逻辑表达式查询的公平可搜索加密方案，该方案采用智能合约取代云服务器，但是该方案密文数据库和

安全索引均存储在智能合约中，需要消耗大量的燃料。Li 等[15]采用时间锁技术和比特币区块链，实现公平的单关键词可搜索加密，但是需要矿工进行解密操作，违背了比特币区块链的特性。

针对以上应用问题，为了实现在一对多搜索模式下云服务器和用户之间公平安全的搜索交易，且支持搜索结果的验证，本文提出了一种基于区块链且支持验证的属性基搜索加密方案，主要贡献如下。1) 结合对称可搜索加密和 CP-ABE，对共享解密密钥指定树形访问结构，实现细粒度访问控制，适合一对多搜索场景，只有属性密钥满足访问策略时才可以获得解密密钥。2) 基于以太坊区块链，设计 2 个智能合约——搜索合约和验证合约，将安全索引存储在搜索合约中，减轻云服务器的存储空间和搜索代价，验证合约检测云服务器搜索结果的正确性。同时，将区块链公平机制引入可搜索加密方案中，实现服务−支付公平，只要用户和云服务器诚实按照合约规则执行，用户就能得到正确的检索结果，而不需要本地额外验证，减轻数据使用者的计算开销，同时云服务器收到相应的服务费。3) 安全性分析表明，本文方案满足自适应选择关键词语义安全，能有效防止隐私数据的泄露，实现密文检索。基于真实数据集在以太坊测试网络中实现本文方案，性能对比与实验分析表明，本文方案在索引产生、搜索令牌生成、检索效率、验证正确性以及交易数量方面具有一定的优势，适用于智慧医疗等一对多搜索场景。

2　以太坊区块链相关知识

以太坊是智能合约的分布式应用平台，扩展了比特币的功能，支持图灵完备脚本语言，是可编程的区块链系统。

智能合约是一套控制着数字资产并包含了合约参与方约定的权利和义务，由计算机自动执行而不需要人为参与的协议，总是按照事先约定的规则执行操作。将智能合约以数字化的形式写入以太坊区块链中，由区块链的不可篡改性以及密码学散列算法保障存储、读取、执行的整个过程透明、可跟踪、不可篡改、不可否认。在以太坊中，智能合约是特殊的账户，由账户地址、脚本代码、余额以及存储空间构成。

在以太坊中，有 2 种不同类型的账户：外部拥有账户和合约账户。外部拥有账户由私钥控制，地址对应于公钥，可以发起消息通信交易进行转账或者创建合约交易触发合约代码的执行。合约账户被合约代码控制，一经创建便存在于区块链中不可更改，其代码将被激活并运行。

矿工处理交易而产生的每一次计算都会产生费用，这个费用以指令操作所消耗的燃料（gas）量来支付，不同的指令消耗的 gas 值不同。gasLimit 表示发送方最多支出的燃料量，gasPrice 表示发送方愿意在每个燃料上支付的费用。对于每个交易，gasLimit×gasPrice 表示发送方愿意为执行交易支付的最大费用。如果发送方账户余额中有足够的以太币来支付最大费用，那么该交易会被成功打包提交给区块链；否则，交易被认为是无效的。

以太坊中有 2 种类型的交易：通信交易和合约创建交易。通信交易通常指从一个外部账户到另一个外部账户进行转账的交易，合约创建交易表示产生一个新的以太坊智能合约并触发智能合约中相关代码执行的交易。交易的数据结构如下所示。

```
type Transaction struct {
    nonce uint    // 发送方发送交易数的计数。
    gasPrice    *bit.Int    // 单位燃料价格，发送方愿意支付执行交易所需的每个燃料的单价
    gasLimit    uint64    // 发送方愿意为本交易支付的最大燃料量
    to    address    //接收账户地址。在通信交易中，表示接收方外部拥有账户的公钥地址。在创建合约交易中，该字段为 0。
    value    *big.Int    // 转账金额
    v,r,s    *big.Int    // 发送方签名值
    data    []byte    //data 域。在通信交易中，表示通信中的输入数据。在合约创建交易中，表示用来初始化新合约账户的以太坊虚拟机代码片段。
}
```

3　算法与安全模型定义

3.1　系统模型

基于区块链的密文检索系统如图 1 所示，适用于一对多的搜索模型，数据拥有者将密文集合上传至云端，只有用户的属性私钥满足访问结构时才可以解密文档，包含 6 个参与方，分别是数据拥有者（DO, data owner）、数据使用者（DU, data user）、云服务提供商（CSP, cloud service provider）、可信授权机构（TA, trusted authority）、区块链（BC,

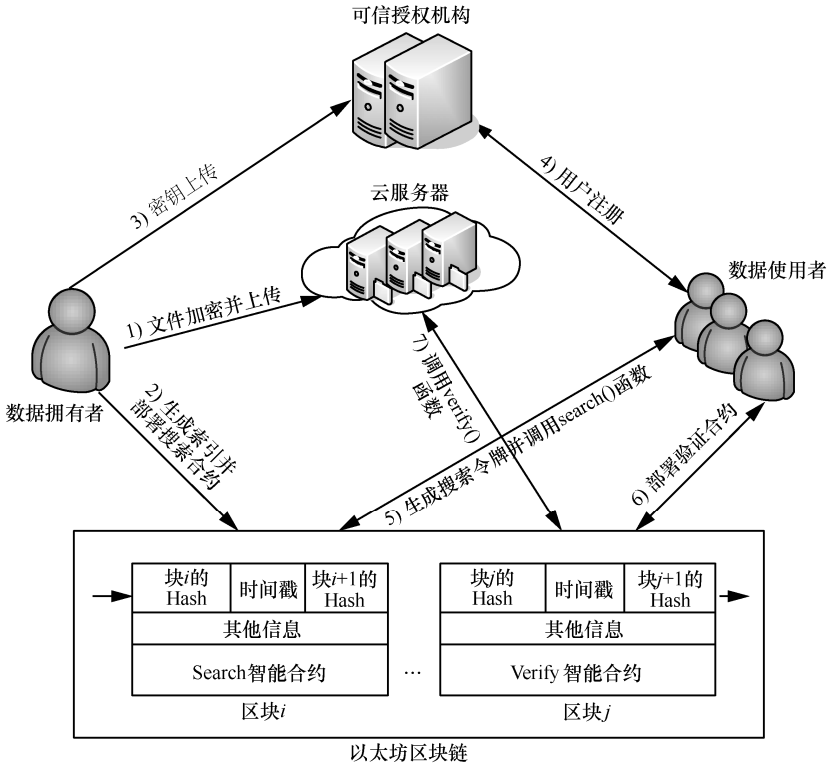

图 1 系统模型

blockchain）、智能合约（SC, smart contract）。

3.2 算法定义

基于文献[2]的 CP-ABE 方案、文献[6]的 SE 方案以及文献[13]的区块链数据共享方案，构建一种基于区块链且支持细粒度访问控制的可验证密文检索方案，该方案由 7 个多项式时间算法的元组构成，即

$$\pi=(\text{Setup},\text{Enc},\text{UserRegist},\text{TokenGen},\text{Search},\text{Verify},\text{Dec})$$

1) 初始化算法。$\text{Setup}(1^{\lambda})\rightarrow \text{PK},\text{MK}$，可信授权机构 TA 输入安全参数 λ，输出系统公共参数 PK 和主私钥 MK。

2) 加密算法。$\text{Enc}(\text{PK},D,W,\text{SK}_S,\Gamma,K_1,K_2)\rightarrow C,\text{MAC},I$，数据拥有者 DO 输入系统公共密钥 PK、明文文档集合 D、关键词集合 W、搜索密钥 SK_S、访问策略 Γ、加密密钥 K_1、验证密钥 K_2，输出密文文档 C、消息验证码集合 MAC、安全索引 I，数据拥有者将 C 发送给 CSP，将索引 I 发送给搜索合约，将 SK_S、MAC、K_2 上传到授权机构 TA。

3) 用户注册算法。$\text{UserRegist}(\text{PK},\text{MK},S)\rightarrow \text{SK}_U,\text{SK}_S,K_2,\text{MAC}$，TA 输入公共参数 PK、主私钥 MK 以及用户属性集合 S，输出属性私钥 SK_U、搜索密钥 SK_S、验证密钥 K_2、消息验证码集合 MAC，TA 收到用户的注册请求，为用户颁发相应的密钥和集合。

4) 搜索令牌生成算法。$\text{TokenGen}(\text{PK},\text{kw},\text{SK}_S)\rightarrow T_{\text{kw}}$，数据使用者 DU 输入公共参数 PK、所查询的关键词 kw、搜索密钥 SK_S，输出搜索令牌 T_{kw}，DU 将 T_{kw} 发送给搜索合约。

5) 搜索算法。$\text{Search}(I,T_{\text{kw}})\rightarrow C_{K_1},\text{DB}(\text{kw})$，搜索智能合约输入安全索引 I、搜索令牌 T_{kw}，输出包含访问策略的密钥密文 C_{K_1} 和包含关键词的数组 DB(kw)。

6) 验证算法。$\text{Verify}(\text{DB}(\text{kw}),C,K_2,\text{MAC})\rightarrow C_{\text{kw}}/\perp$，验证智能合约输入数组 DB(kw)、密文集合 C、验证密钥 K_2、消息验证码集合 MAC，如果验证通过，输出正确的包含查询关键词的密文文档集合 C_{kw}；否则，算法输出 $\perp$，而不需要用户本地验证 CSP 返回的结果是否正确，减轻用户计算开销。

7) 解密算法。$\text{Dec}(\text{SK}_U,C_{K_1},C_{\text{kw}})\rightarrow D_{\text{kw}}/\perp$，数据使用者 DU 输入属性私钥 SK_U、包含访问策略的密钥密文 C_{K_1}、包含关键词的密文文档集合 C_{kw}，如果属性私钥满足 DO 定义的访问结构，则可以恢复对称密钥 K_1，解密密文文档集合，输出包含查询

关键词的明文文档集合 D_{kw}；否则，输出 $\perp$。

3.3 安全模型定义

本文采用文献[7]的安全模型，在有状态的模拟器 B 和攻击者 A 之间采用基于模拟的游戏，允许泄露访问模式和搜索模式来证明安全。信息泄露情况采用 2 个泄露函数进行描述，即 $L=(L_1,L_2)$。L_1 定义为 $L_1(D)=\{|D|,n,\{|D_i|,\mathrm{id}(D_i)\}_{i\in[1,n]}\}$，输入文档集合 D，输出文档集合的大小、文档数量、每个文档的大小和标识符；L_2 定义为 $L_2(D,w)=(\mathrm{AP}(w),T_w)$，输入文档集合和查询关键词 w，输出关键词的访问模式 AP(w) 和搜索令牌。在挑战者 C、敌手 A 以及模拟器 B 之间进行的游戏定义如下。

$\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)$。挑战者根据安全参数 λ 初始化系统，敌手 A 给挑战者文件集合 D，挑战者根据 Enc 算法生成安全索引 I 和加密文档 C，并发送给攻击者，攻击者进行多项式数量的自适应查询 $Q=(w_1,w_2,\cdots,w_q)$，挑战者对每个查询的关键词产生搜索令牌并发送给攻击者，最后攻击者返回一个比特 b 作为游戏的输出。

$\mathrm{Ideal}_{\mathrm{A,B}}^{\pi}(\lambda)$。敌手 A 输入数据文件 D，给定泄露函数 L_1 和 L_2，模拟器 B 产生并发送 (I^*,C^*) 给 A，然后攻击者进行多项式数量的自适应查询 $Q=(w_1,w_2,\cdots,w_q)$，对每个查询对应的关键词，模拟器 B 根据泄露函数 L_2 返回对应的搜索令牌 T_w^*，最后攻击者返回一个比特 b 作为游戏的输出。

4 方案构造

1) 系统初始化阶段

$\mathrm{Setup}(1^{\lambda})\rightarrow \mathrm{PK,MK}$。输入安全参数 λ，TA 定义 G_0、G_1 是 $\mathbb{Z}_p$ 上的 2 个乘法循环群，阶 p 为一个大安全素数，令 g 为群 G_0 的生成元，定义双线性映射 $e:G_0\times G_0\rightarrow G_1$，选取抗碰撞散列函数 $H_1:\{0,1\}^*\rightarrow G_0$，定义伪随机函数 $H_2:\{0,1\}^k\times\{0,1\}^*\rightarrow\{0,1\}^l$，$F:\{0,1\}^k\times\{0,1\}^*\rightarrow\{0,1\}^l$，TA 随机选择 $\alpha,\beta\xleftarrow{R}\mathbb{Z}_p$，输出系统公共参数 PK = ($G_0$, G_1, p, g, $h=g^{\beta}$, $e(g,g)^{\alpha}$, F, H_1, H_2)，系统主私钥 MK = (α, β)。其中，$e(g,g)$ 表示双线性映射在群 G_1 中的值。

2) 加密阶段

$\mathrm{Enc}(\mathrm{PK},D,W,\mathrm{SK}_S,\Gamma,K_1,K_2)\rightarrow C,\mathrm{MAC},I$。假设 DO 有 n 个明文文档，即 $D=\{D_1,D_2,\cdots,D_n\}$ 需要加密上传到 CSP 中。

步骤 1　文档加密，$\mathrm{FileEnc}(D,K_1,K_2)\rightarrow C,\mathrm{MAC}$。数据拥有者 DO 随机选取 $K_1\leftarrow\{0,1\}^k$ 作为明文文档的对称加密密钥。DO 使用 K_1 加密文档 D_i ($i\in[1,n]$)，得到 $C_i=\{\varepsilon.\mathrm{Enc}_{K_1}(D_i)\,|\,i\in[1,n]\}$，其中，$\varepsilon$ 表示安全的对称加密方案，ε.Enc 表示加密过程，ε.Dec 表示解密过程。DO 选取验证密钥 $K_2\leftarrow\{0,1\}^k$ 对密文文档 C_i ($i\in[1,n]$) 生成消息验证码集合 $\mathrm{MAC}_{C_i}=\{H_2(K_2,C_i)\,|\,i\in[1,n]\}$，DO 将密文文档集合 $C=\{C_1,C_2,\cdots,C_n\}$ 发送给 CSP。

步骤 2　密钥加密，$\mathrm{KeyEnc}(\mathrm{PK},K_1,\Gamma)\rightarrow C_{K_1}$。对于密钥 K_1，数据拥有者 DO 定义访问结构 Γ，首先从树的根节点 r 开始为树 Γ 的每一个节点 x 分配一个阶为 d_x 的多项式 q_x（叶子节点的 q_x 为常数），令 k_x 表示节点 x 的门限值，设置 $\deg(q_x)=d_x=k_x-1$，从树的根节点 r 开始，DO 随机选择 $s\xleftarrow{R}\mathbb{Z}_p$，并设置 $q_r(0)=s$，接着从 $\mathbb{Z}_p$ 中选取 $\deg(q_r)$ 个随机系数来确定多项式 q_r；对于其他任意节点 x，设置 $q_x(0)=q_{\mathrm{parent}(x)}(\mathrm{index}(x))$，并从 $\mathbb{Z}_p$ 中随机选取 $\deg(q_x)$ 个系数来确定多项式 q_x。令 Y 表示树 Γ 中所有叶子节点，DO 计算得到密钥 K_1 加密后的密文，如式(1)所示。

$$C_{K_1}=\{\Gamma,\bar{C}=K_1e(g,g)^{\alpha s},C=h^s,\{C_y=g^{q_y(0)},$$
$$C_y'=H_1(\mathrm{att}(y))^{q_y(0)}\}_{\forall y\in Y}\} \tag{1}$$

其中，s 为随机数，att(y) 表示属性值。

步骤 3　索引生成，$\mathrm{IndexGen}(\mathrm{PK},W,\mathrm{SK}_S)\rightarrow I$。DO 首先从文档集合 $D=\{D_1,D_2,\cdots,D_n\}$ 中提取关键词。假设关键词集合 $W=\{w_1,w_2,\cdots,w_m\}$。对于每一个关键词 $w_i\in W$，DO 选择一个大小为 n 的空数组 $\mathrm{DB}(w_i)$，该数组按如下方法构造：如果第 j 个文档包含关键词 w_i，那么 $\mathrm{DB}(w_i)[j]=1$；否则 $\mathrm{DB}(w_i)[j]=0$。例如，假设有 3 个文件 D_1、D_2、D_3，其中，D_1 包含关键词 w_1、w_2，D_2 包含关键词 w_2、w_3，D_3 包含关键词 w_1、w_2，可以得到 $\mathrm{DB}(w_1)=\{101\}$，$\mathrm{DB}(w_2)=\{111\}$，$\mathrm{DB}(w_3)=\{010\}$。

接着，DO 对于关键词集合 $W=\{w_1,w_2,\cdots,w_m\}$ 中的每一个关键词 $w_i\in W$，随机选取搜索密钥 $\mathrm{SK}_S\leftarrow\{0,1\}^k$ 并计算 $T_{w_i}=F_{\mathrm{SK}_S}(w_i)$，DO 将 T_{w_i} 和 $C_{K_1}\,\|\,\mathrm{DB}(w_i)$ ($i\in[1,m]$)通过交易 TX_s 发送给搜索智能合约地址 Add_S，调用智能合约的 addIndex()函数

存储安全索引，如果 DO 账户中没有足够的余额来支付 $cost，系统回滚，其中，$cost 表示矿工收取的燃料费。

智能合约定义一个查找表 I，其包含了 m 个条目，允许高效定位并查找密文信息，查找表的每一个条目与一个关键词相关并包含一个键值对 $<\text{address},\text{value}>$，其中，address 字段用于定位查找表的条目，value 字段用于获得密文信息。在查找表中，当给定一个 address 时，会立刻返回相应的 value 域，令 $\text{address}=T_{w_i}$，$\text{value}=C_{K_1}\|\text{DB}(w_i)$，可得 $I[T_{w_i}]=C_{K_1}\|\text{DB}(w_i)$，其中，$1\leqslant i\leqslant m$。

步骤 4 数据上传。DO 将 $\text{MAC}=\{\text{MAC}_{C_1},\text{MAC}_{C_2},\cdots,\text{MAC}_{C_n}\}$、$\text{SK}_S$ 和 K_2 通过安全信道传输给 TA。

3) 用户注册阶段

$\text{UserRegist}(\text{PK},\text{MK},S)\rightarrow \text{SK}_U,\text{SK}_S,K_2,\text{MAC}$。用户注册阶段由 TA 执行。当一个用户 DU 发送注册请求后，TA 认证用户的身份并通过安全信道颁发相应的密钥。TA 为用户的相应属性集合 S 生成属性私钥，对 $\forall u\in U$，TA 选择 $r\xleftarrow{R}\mathbb{Z}_p$，并且对 $\forall j\in S$，TA 取 $r_j\xleftarrow{R}\mathbb{Z}_p$，计算相应的属性私钥，如式(2)所示。

$$\text{SK}_U=\{E=g^{\frac{\alpha+r}{\beta}},\{E_j=g^r H_1(j)^{r_j},E_j^{'}=g^{r_j}\}_{\forall j\in S}\} \quad (2)$$

TA 为 DU 颁发搜索密钥 SK_S、验证密钥 K_2 以及消息验证码集合 $\text{MAC}=\{\text{MAC}_{C_1},\text{MAC}_{C_2},\cdots,\text{MAC}_{C_n}\}$。对于不同的 DU 来说，属性私钥 SK_U 是不同的，但是 MAC 集合、SK_S 和 K_2 都是相同的。

4) 搜索令牌生成阶段

$\text{TokenGen}(\text{PK},\text{kw},\text{SK}_S)\rightarrow T_{\text{kw}}$。搜索令牌由 DU 生成。在用户注册阶段，DU 得到相应的密钥 SK_S，根据要查询的关键词 kw 计算出搜索令牌 $T_{\text{kw}}=F_{\text{SK}_S}(\text{kw})$。

5) 搜索阶段

$\text{Search}(I,T_{\text{kw}})\rightarrow C_{K_1},\text{DB}(\text{kw})$。数据使用者 DU 将搜索令牌 T_{kw} 通过交易 TX_T 发送给搜索合约地址 Add_S，调用智能合约的 search()函数并传入搜索令牌 T_{kw}，使用智能合约进行搜索，如果 DU 账户中没有足够的余额来支付 $cost，系统回滚。搜索合约的设计在第 5 节介绍。

智能合约搜索得到 C_{K_1} 和 DB(kw)，将 C_{K_1} 发送给调用合约的 DU。由于在区块链中所有的数据都是公开的，云服务器和数据使用者可以公开读取到 DB(kw)。通过智能合约进行搜索，减轻了云服务器的存储负担和计算开销。

6) 验证阶段

$\text{Verify}(\text{DB}(\text{kw}),C,K_2,\text{MAC})\rightarrow C_{\text{kw}}/\perp$。数据使用者 DU 读取到 DB(kw)后，初始化集合 ID_{MAC}，遍历 DB(kw)，如果 $\text{DB}(\text{kw})[j]=1$，将 j 添加到集合 ID_{MAC} 中，得到 $\text{ID}_{\text{MAC}}=\{\text{id}_1,\text{id}_2,\cdots,\text{id}_j\}$，根据集合 ID_{MAC} 遍历 MAC 集合，返回所有包含查询关键词 kw 的消息验证码集合 $\text{MAC}_{\text{kw}}=\{\text{MAC}_{C_1},\text{MAC}_{C_2},\cdots,\text{MAC}_{C_j}\}$。

DU 将 MAC_{kw} 和 K_2 通过交易 TX_C 发送给验证合约地址 Add_V，调用验证合约中的 addMac()函数并传入参数 MAC_{kw} 和 K_2，方便合约进行验证，令 $serFee 表示数据使用者 DU 支付给云服务器的手续费，被临时保存在验证合约账户中。验证合约的设计在第 5 节介绍。

云服务器读取到 DB(kw)后，初始化集合 ID_{kw}，遍历 DB(kw)，如果第 j 个文档包含关键词 kw，即 $\text{DB}(\text{kw})[j]=1$，将 j 添加到集合 ID_{kw} 中，得到 $\text{ID}_{\text{kw}}=\{\text{id}_1,\text{id}_2,\cdots,\text{id}_j\}$，根据集合 ID_{kw} 查询密文数据库，返回所有匹配的密文文档 $C_{\text{kw}}=\{C_1,C_2,\cdots,C_j\}$。

CSP 将包含查询关键词 kw 的密文文档 $C_{\text{kw}}=\{C_1,C_2,\cdots,C_j\}$ 通过交易 TX_V 发送给验证合约地址 Add_V，调用智能合约中的 verify()函数并传入参数 C_{kw}，使用智能合约验证云服务器返回结果的正确性，令 $Guranty 表示云服务器 CSP 支付给验证合约的保证金。

借助验证合约验证云服务器返回结果的正确性，使数据使用者 DU 总能得到正确的密文文档 $C_{\text{kw}}=\{C_1,C_2,\cdots,C_j\}$，而不需要本地进行再次验证，减轻用户的计算开销。

7) 解密阶段

$\text{Dec}(\text{SK}_U,C_{K_1},C_{\text{kw}})\rightarrow D_{\text{kw}}/\perp$。DU 收到正确的密文文档 $C_{\text{kw}}=\{C_1,C_2,\cdots,C_j\}$ 后，需要本地验证是否具有解密权限。验证通过，则可以进行解密得到明文文档；如果验证不通过，即使搜索到相应的文档但由于不具有解密权限，故得不到明文文档。

步骤 1 验证密钥 $\text{Test}(\text{SK}_U,C_{K_1})\rightarrow K_1/\perp$。DU

收到密文C_{K_1}后，检查属性私钥SK_U和访问策略Γ是否匹配，如果不匹配，返回⊥；否则，根据文献[2]采用自下而上的递归算法，得到$A=e(g,g)^{rs}$。由此DU可以恢复出对称密钥

$$K_1=\frac{\bar{C}}{\frac{e(C,E)}{A}}=\frac{K_1e(g,g)^{\alpha s}}{\frac{e(h^s,g^{\frac{\alpha+r}{\beta}})}{e(g,g)^{rs}}}=$$

$$\frac{K_1e(g,g)^{\alpha s}e(g,g)^{rs}}{e(g,g)^{s(\alpha+r)}} \tag{3}$$

步骤 2　用户解密$\mathrm{Dec}(C_{\mathrm{kw}},K_1)\to D_{\mathrm{kw}}$。利用解密得到的对称密钥$K_1$，解密读取到的密文文档$C_{\mathrm{kw}}=\{C_1,C_2,\cdots,C_j\}$，得到包含查询关键词 kw 的明文文档$D_{\mathrm{kw}}=\{D_1,D_2,\cdots,D_j\}$，即$D_i=\{\varepsilon.\mathrm{Dec}(K_1,C_i)\,|\,i\in[1,j]\}$。

5　智能合约设计

智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪并且不可逆转。本节引入搜索合约和验证合约的相关变量和函数。

1) 搜索合约

搜索合约由数据拥有者 DO 部署。搜索合约中用到的变量如表 1 所示。

表 1　搜索合约变量

变量	描述
owner	地址类型，合约创建者 DO 地址
Index	映射类型，由键值对组成，通过给定键找到相应值，本文中索引包含 m 个条目，键值对一一对应，键为T_{w_i}，值为$C_{K_1}\|\mathrm{DB}(w_i)$。其中，键是唯一的
result	整数类型，存储搜索结果
miner	地址类型，当前区块的矿工地址

搜索合约中用到的函数如表 2 所示。

表 2　搜索合约函数

函数	描述
searchTest()	构造函数，无参函数，进行初始化操作，判断合约部署者是否是数据拥有者 DO
addIndex()	添加索引函数，输入安全索引，数据拥有者 DO 调用该函数，用在智能合约中存储安全索引
search()	搜索函数，数据使用者 DU 调用该函数并传入搜索令牌T_{kw}，输出搜索结果C_{K_1}和 DB(kw) 存储在 result 中

2) 验证合约

验证合约由数据使用者 DU 部署。验证合约中用到的变量如表 3 所示。

表 3　验证合约变量

变量	描述
key	整数类型，存储验证密钥K_2
contract	地址类型，合约地址
$\mathrm{Mac}_{\mathrm{kw}}$	数组类型，存放包含查询关键词的消息验证码集合$\mathrm{MAC}_{\mathrm{kw}}=\{\mathrm{MAC}_{C_1},\mathrm{MAC}_{C_2},\cdots,\mathrm{MAC}_{C_j}\}$
cipher	数组类型，存放密文文档$C_{\mathrm{kw}}=\{C_1,C_2,\cdots,C_j\}$

验证合约中定义的函数如表 4 所示。

表 4　验证合约函数

函数	描述
verifyTest()	构造函数，无参函数，进行初始化操作，判断合约部署者是否是数据使用者 DU
addMac()	添加消息验证码函数，数据使用者 DU 调用该函数用于存储$\mathrm{MAC}_{\mathrm{kw}}$和验证密钥$K_2$
verify()	验证函数，云服务器 CSP 调用该函数并传入参数C_{kw}，验证合约验证结果的正确性和完整性：$H_2(K_2,C_i)==\mathrm{MAC}_{C_i}$，其中$1\leqslant i\leqslant j$，当验证不通过时，表明云服务器返回的结果不正确，云服务器受到惩罚，将 $ Guranty 和 $ serFee 支付给 DU；当验证通过时，DU 得到正确结果，CSP 获得应收的服务费，将 $ Guranty 和 $ serFee 支付给 CSP。通过智能合约，使用户支付了手续费就一定能得到正确的搜索结果，云服务器提供了正确的结果就一定可以获得服务费，同时用户不能否认结果而不支付手续费，各方均诚实按照合约的规则执行，很好地解决了不公平的问题，实现服务–支付公平，并且不需要用户本地额外验证

6　方案分析

6.1　正确性分析

当 DU 收到包含访问结构的密钥密文C_{K_1}后，用属性私钥检测是否满足访问结构，如果属性私钥满足访问结构，则可以恢复出对称密钥，正确性如下。

$$K_1=\frac{\bar{C}}{\frac{e(C,E)}{A}}=\frac{K_1e(g,g)^{\alpha s}}{\frac{e(h^s,g^{\frac{\alpha+r}{\beta}})}{e(g,g)^{rs}}}=$$

$$\frac{K_1e(g,g)^{\alpha s}e(g,g)^{rs}}{e(g,g)^{s(\alpha+r)}}=K_1 \tag{4}$$

6.2　安全性分析

定理 1　本文方案π是适应性选择关键词语义安全的，CSP 和外部攻击者除搜索模式和访问模式外，不会获取任何额外信息。

证明　如果对于任意敌手 A，存在一个模拟器 B，满足条件$|\Pr[\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)]-\Pr[\mathrm{Ideal}_{\mathrm{A,B}}^{\pi}(\lambda)]|\leqslant\mathrm{negl}(\lambda)$，其中，$\mathrm{negl}(\lambda)$是可忽略函数，那么本文方案是适应

性选择关键词语义安全。由文献[7]的证明等价可知，基于模拟的游戏证明等价于不可区分游戏证明，敌手 A 将通过分析模拟器产生的密文、索引以及搜索令牌的区分性赢得游戏，因此，要证方案是安全的，即 $\Pr[\mathrm{Ind}_{\mathrm{A}}^{\pi}(\lambda)=1]\leqslant\frac{1}{2}+\mathrm{negl}(\lambda)$。

模拟器自适应生成模拟密文文档 C^*、模拟索引 I^* 和模拟令牌 $T_w{}^*$ 的过程如下。

1) 模拟密文文档 C^*。根据泄露函数 $L_1(D)=\{|D|,n,\{|D_i|,\mathrm{id}(D_i)\}_{i\in[1,n]}\}$，模拟器均匀随机地生成 n 个长度为 $|D_i|_{i\in[1,n]}$ 比特的模拟加密文档 $C^*=\{C_1,C_2,\cdots,C_n\}$。由于 ε 是安全的对称加密方案，可保证 $\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)$ 中的 C 和 $\mathrm{Ideal}_{\mathrm{A,B}}^{\pi}(\lambda)$ 中的 C^* 在计算上是不可区分的，即

$$|\Pr[\mathrm{FileEnc}(D,K_1)\to C]-\Pr[\mathrm{Random}\to C^*]|\leqslant\mathrm{negl}_1(\lambda)$$

2) 模拟安全索引 I^*。模拟器将 I^* 设置为具有 q 个条目的查找表，在 $\{0,1\}^l$ 中随机均匀选择 q 个元素 $a_i{}^*$，其中 $i\in[1,q]$，根据泄露函数 L_1 和 L_2，模拟器生成 $\mathrm{DB}(w_i{}^*)$，模拟索引 $I^*[a_i{}^*]=C_{K_1}\|\mathrm{DB}(w_i{}^*)$，在 $\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)$ 中构造索引的过程采用伪随机函数 F，模拟 I^* 就是使用随机字符串取代相同长度输出的 $F_{\mathrm{SK}_S}(w_i)$。由伪随机函数的安全性可知，在不知道密钥 SK_S 的情况下，敌手 A 无法区分伪随机函数 F 的输出和相同大小的随机字符串，因此，敌手在计算上无法区分 I 和 I^*，即

$$|\Pr[\mathrm{IndexGen}(\mathrm{PK},W,\mathrm{SK}_S)\to I]-\Pr[\mathrm{Random}\to I^*]|\leqslant\mathrm{negl}_2(\lambda)$$

3) 模拟搜索令牌 $T_w{}^*$。根据泄露函数 $L_2(D,w)=(\mathrm{AP}(w),T_w)$ 获得模拟搜索令牌 $T_{w_i}{}^*$。在没有分配搜索密钥的情况下，模拟器生成有效的搜索令牌的概率是可忽略的，对 $\forall w_i\in Q$，搜索令牌的定义为 $T_{w_i}=F_{\mathrm{SK}_S}(w_i)$，且 F 是伪随机函数，由于模拟器不知道 SK_S，那么随机选择 $\mathrm{SK}_S{}^*$ 并且构造出有效搜索令牌的概率为

$$\Pr[T_{w_i}{}^*=T_{w_i};T_{w_i}{}^*=F_{\mathrm{SK}_S{}^*}(w_i);T_{w_i}=F_{\mathrm{SK}_S}(w_i);$$
$$\mathrm{SK}_S{}^*\leftarrow\{0,1\}^k]\approx\Pr[\mathrm{SK}_S=\mathrm{SK}_S{}^*|\mathrm{SK}_S{}^*\leftarrow\{0,1\}^k]\approx\frac{1}{2^k}$$

因此，由可忽略函数的定义可知，针对伪随机函数 F，在不具有搜索密钥 SK_S 的情况下，可保证 $\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)$ 中的搜索令牌和 $\mathrm{Ideal}_{\mathrm{A,B}}^{\pi}(\lambda)$ 中的搜索令牌的不可区分性，即

$$|\Pr[\mathrm{TokenGen}(\mathrm{PK},w_i,\mathrm{SK}_S)\to T_{w_i}]-\Pr[\mathrm{Random}\to T_{w_i}{}^*]|\leqslant\mathrm{negl}_3(\lambda)$$

由于敌手 A 试图通过分析密文、索引以及搜索令牌来赢得不可区分性游戏，即 $\mathrm{Adv}(\mathrm{A}(C))$ 表示敌手 A 区分真实密文文档和随机密文文档的优势，$\mathrm{Adv}(\mathrm{A}(I))$ 表示敌手 A 区分真实索引和随机字符串的优势，$\mathrm{Adv}(\mathrm{A}(T_w))$ 表示敌手 A 区分真实搜索令牌和随机搜索令牌的优势，则

$$\Pr[\mathrm{Ind}_{\mathrm{A}}^{\pi}(\lambda)=1]=\frac{1}{2}+\mathrm{Adv}(\mathrm{A}(C))+\mathrm{Adv}(\mathrm{A}(I))+\mathrm{Adv}(\mathrm{A}(T_w))=\frac{1}{2}+|\Pr[\mathrm{FileEnc}(D,K_1)\to C]-\Pr[\mathrm{Random}\to C^*]|+|\Pr[\mathrm{IndexGen}(\mathrm{PK},W,\mathrm{SK}_S)\to I]-\Pr[\mathrm{Random}\to I^*]|+|\Pr[\mathrm{TokenGen}(\mathrm{PK},w_i,\mathrm{SK}_S)\to T_{w_i}]-\Pr[\mathrm{Random}\to T_{w_i}{}^*]|\leqslant\frac{1}{2}+\mathrm{negl}_1(\lambda)+\mathrm{negl}_2(\lambda)+\mathrm{negl}_3(\lambda)$$

令 $\mathrm{negl}(\lambda)=\mathrm{negl}_1(\lambda)+\mathrm{negl}_2(\lambda)+\mathrm{negl}_3(\lambda)$，有 $\Pr[\mathrm{Ind}_{\mathrm{A}}^{\pi}(\lambda)=1]\leqslant\frac{1}{2}+\mathrm{negl}(\lambda)$。

综上所述，对于任意多项式时间敌手 A，$\mathrm{Real}_{\mathrm{A}}^{\pi}(\lambda)$ 和 $\mathrm{Ideal}_{\mathrm{A,B}}^{\pi}(\lambda)$ 的输出是不可区分的，本文方案 π 满足适应性选择关键词语义安全。证毕。

定理 2 对于 CSP 和其他外部敌手，除密文文档外，学习不到明文文档的任何信息。

证明 在本方案中，文档 D_i 在被上传至 CSP 前采用对称密钥 K_1 加密，并且 DO 基于 CP-ABE 将 K_1 加密为 C_{K_1} 存放在安全索引中，也就是说，即使 CSP 和外部敌手窃听到信道中的密文文档，但是得到明文信息的难度等同于解密 C_{K_1} 的难度。在 C_{K_1} 中，$\overline{C}=K_1e(g,g)^{\alpha s}$，所以想要解密得到 K_1，就必须计算出 $e(g,g)^{\alpha s}$。基于离散对数问题，对 CSP 和外部攻击者而言，由 $e(g,g)^{\alpha}$ 和 $C=h^s$ 计算求得 $e(g,g)^{\alpha s}$ 是困难的。同样，基于计算性迪菲–赫尔曼问题，由于攻击者没有符合访问策略的属性密钥，无法利用拉格朗日插值公式向上递归计算出根节点的值 $e(g,g)^{rs}$，进而不能计算出 K_1。因此，当且仅当属性私钥满足访问结构时才可以计算出 K_1，从而解密出明文文档。但由于属性私钥是由 DU 私藏，因此对 CSP 和外部攻击者而言，除密文文档外，学

习不到明文文档的任何信息。

6.3　公平性分析

本文利用智能合约，在点对点服务中快速实现公平支付，由以太坊区块链保证合约执行的不可篡改、不可否认以及可追踪，确保 CSP 和 DU 诚实地按照合约规则执行。借助验证合约验证 CSP 返回结果的正确性，使 DU 总能得到正确的密文文档 $C_{\mathrm{kw}}=\{C_1,C_2,\cdots,C_j\}$，而不需要本地验证，减轻用户计算负担。由于区块链的不可篡改性，使智能合约一经部署便不可修改并全网共识，只能按照合约的逻辑执行，只要 DU 得到正确的结果，CSP 才能得到手续费并赎回保证金，只要 DU 支付了手续费，那么一定会得到正确的结果，在 CSP 返回不正确的结果时，会受到惩罚并损失保证金，DU 同时收回手续费并得到保证金作为对 CSP 的惩罚。此外，DU 不可否认 CSP 提供的服务以拒绝支付服务费，因为 DU 需要使用唯一的外部拥有账户来产生交易以调用合约，并且将手续费临时存储在合约账户中，一旦交易被确认并记录在区块链中便不可修改、不可否认。将区块链公平机制引入可搜索加密方案中，实现服务−支付公平。

6.4　性能分析

1) 功能对比

将本文方案的功能特征与文献[10,12-13]中的方案进行对比，如表 5 所示。文献[10]方案支持多关键搜索，并支持细粒度访问控制，同时引入一个可信审计机构验证来返回结果的正确性，对用户不具有公平性。文献[12-13]方案都是支持单关键词的可搜索加密方案，且采用区块链技术实现服务−支付公平，文献[12]方案在验证搜索结果是否正确时不需要引入可信审计机构，由用户进行本地验证，增加了用户的计算开销。另外，与本文方案相比，文献[12]方案并不支持细粒度的访问控制策略。而本文方案使用智能合约验证结果，不需要用户本地验证，使用户始终得到正确的搜索结果，减轻用户本地计算开销。文献[13]方案和本文方案都采用属性基加密机制实现对用户的细粒度访问控制，但是文献[13]方案仅支持“与”门访问策略，而本文方案支持访问树结构，策略表达更加灵活。另外，文献[13]方案并不支持用户验证，而本文方案通过智能合约技术实现搜索结果的正确性验证，同时支持公平支付。

从功能方面来看，本文方案既扩展了实际应用中对数据的细粒度访问控制功能，又保证了云计算中搜索的安全性和正确性，同时实现服务−支付公平。

2) 性能对比

将本文方案与相关方案在索引、搜索令牌、搜索、验证方面的计算代价进行对比，对基于区块链的可搜索加密方案在交易数量上进行对比，如表 6 所示。其中，E_0 和 E_1 分别表示群 G 和 G_1 上的指数运算；M 表示模乘运算；P 表示双线性对操作；H 表示散列运算；F 表示伪随机函数；$|m|$ 表示 DO 提取关键词个数；$|j|$ 表示包含关键词 w 的文件数；$|l|$ 表示 DU 查询关键词的个数；$|U|$ 表示系统的属性个数；$|S|$ 表示 DU 拥有的属性个数；$|R|$ 表示返回密文文件个数；$|N|$ 表示文档的数量；I_p 表示与门访问策略 P 的下标；$|Y|$ 表示树型访问策略 Γ 的叶子节点个数；SIG 表示签名算法，包含签名和验证 2 个过程；PK 表示公钥加密算法，包含加密和解密 2 个过程；—表示不参与此项操作。

索引生成阶段，文献[10]方案需要进行复杂的指数运算，且指数操作次数和系统属性个数$|U|$相关。一般情况下，$|U|$要远远大于加密访问策略中属性数量$|Y|$，可见文献[10]方案计算代价是最大的。文献[12]方案需要在每个关键词以及每个关键词的文档集合上进行一次 F、一次 H、一次SIG 运算，计算量较大。本文方案和文献[13]方案虽也涉及耗时的指数和模乘运算，但都是一次性操作，数据使用者只需要计算一次，同时，文献[13]方案需要在每个关键词上进行 2 次 F，本文方案进行一次

表 5　　**功能对比**

方案	关键词类型	基于区块链	细粒度访问控制	访问策略	可信审计机构	结果可验证	公平支付
文献[10]方案	多关键词	×	√	访问树	√	审计机构	×
文献[12]方案	单关键词	√	×	×	×	用户端	√
文献[13]方案	单关键词	√	√	与门	×	—	√
本文方案	单关键词	√	√	访问树	×	智能合约	√

F，减少了索引生成时间。

搜索令牌生成过程中，文献[10]方案主要依靠指数运算，且指数的计算代价随$|S|$线性变化。文献[12]方案主要依靠伪随机函数生成运算，且计算代价随$|N|$线性增加。文献[13]方案需要先进行公钥解密操作获得搜索密钥，然后通过一次伪随机函数生成搜索令牌。而本文方案只需进行一次伪随机函数就可以产生搜索令牌。

搜索阶段，本文方案和文献[13]方案都是常数级别，搜索时间快，因为构建索引时采用基于键−值对的查找表方式，具有$O(1)$的搜索效率，使当给定一个搜索令牌时会立刻返回相应的值。此外，文献[10,12]方案都需要 CSP 进行搜索，CSP 存储密文文档和安全索引，而本文方案将密文文档存储在 CSP，安全索引存储在智能合约，使用智能合约进行搜索，减少占用 CSP 的存储空间并减轻 CSP 的计算负担。

验证结果的正确性阶段，文献[10]方案需要由可信审计机构进行$3|R|$次双线性对计算才可以检测出是否正确，随着$|R|$增大，验证时间增加。文献[12]方案移除可信审计机构，但是需要用户在本地进行$|N|$次散列运算和$|N|$次签名验证操作，随着文档数量的增加，验证时间增加。本文方案不需要用户本地验证就可以得到正确的结果，使用智能合约进行$|R|!$次散列运算，降低了用户的工作量，减轻用户计算开销。

本文方案与文献[12-13]方案都是基于区块链技术的，文献[12]方案需要进行 13 次交易，文献[13]方案需要进行 7 次，而本文方案的交易只有 4 次，减少了交易在区块链中上传、打包以及确认过程中的时延，使系统具有较高的响应速度。

综上所述，从索引生成、搜索令牌生成、搜索阶段、验证阶段、交易数量 5 个方面来看，本文方案在性能上是最优的，采用智能合约实现外包搜索，降低了 CSP 的存储空间和计算开销，同时支持搜索结果正确性的验证，移除可信审计机构而且不需要用户本地额外验证就能得到正确的搜索结果，降低了用户的计算开销，减少了交易数量以获得更高的响应速率，并实现服务−支付公平。

3) 实验分析

为了更准确地评估方案的实际性能，本文使用真实数据集和 PBC（pairing-based cryptography）库在索引生成时间、搜索令牌生成时间、搜索时间方面进行仿真测试。本实验采用 IEEE 数据库中的英文论文作为测试数据集，选取 PBC 库中提供的 A 类椭圆曲线，散列算法采用 SHA-256，2 个伪随机函数采用 HMAC-SHA256，对称加密算法采用 AES-256，智能合约采用 solidity 语言，运行在以太坊虚拟机中，区块链的实现基于以太坊官方测试网络 Rinkeby，账户采用以太坊钱包 MetaMask。本实验的硬件环境为 Intel(R) Core(TM) i5-4200 CPU(2.3 GHz)，RAM 为 4 GB。由于以太坊账户余额的限制，因此在实验中设置参数如下：访问树中叶子节点个数$|Y|=10$，每个用户拥有的属性$|S|\in[0,10]$，文档的数量$|N|\in[0,100]$，提取出的关键词个数$|m|\in[0,20]$。实验结果如图 2 所示。

如图 2(a)所示，在叶子节点个数固定为 10 的情况下，索引生成时间与关键词数量成正比。当关键词数量为 0 时，纵坐标不为 0，因为需要在索引中为共享密钥指定访问策略，是一次性运算，时间为 319.8 ms。此外，在索引生成阶段，数据拥有者为每个关键词调用一次 HMAC-SHA256 算法。当关键词数量为 20 时，数据拥有者生成索引的时间为 917.5 ms。安全索引由数据拥有者生成，并发送给智能合约存储，不会影响用户的搜索体验。

如图 2(b)所示，搜索令牌生成时间并不会随着用户属性的增加而剧烈变化。在用户属性为 6 的情况下，用户想要搜索关键词“Blockchain”，由于采

表 6 性能对比

方案	索引生成阶段	搜索令牌生成阶段	搜索阶段	验证阶段	交易数量
文献[10]方案	$2(\|U\|+\|m\|+6)E_0+E_1+\|U\|H$	$(2\|S\|+\|l\|+4)E_0$	$2\|S\|E_0+E_1+5P$	$3\|R\|P$	—
文献[12]方案	$\|m\|\|j\|(F+H+\mathrm{SIG})$	$\|N\|F$	$\|N\|(H+\mathrm{SIG})$	$\|N\|(H+\mathrm{SIG})$	13
文献[13]方案	$(2I_P+2)M+2E_0+E_1+2\|m\|F$	$\mathrm{PK}+F$	1	—	7
本文方案	$M+(2Y+1)E_0+E_1+\|m\|F$	F	1	$\|R\|!H$	4

用单关键词搜索，同时搜索令牌的生成只需要调用一次 HMAC-SHA256 算法，测试可得搜索令牌的生成时间为 29.6 ms。在用户属性为 10 的情况下，搜索相同的关键词，测试可得令牌生成时间为 29.9 ms。通过 10 次实验可以得出结论，在 C 语言环境下测试搜索令牌平均生成时间约为 30 ms，用户的属性数量并不会影响搜索令牌的生成时间。在用户想要搜索某个关键词时，只需要通过约 30 ms 时间提交搜索令牌，因此具有较高的效率。

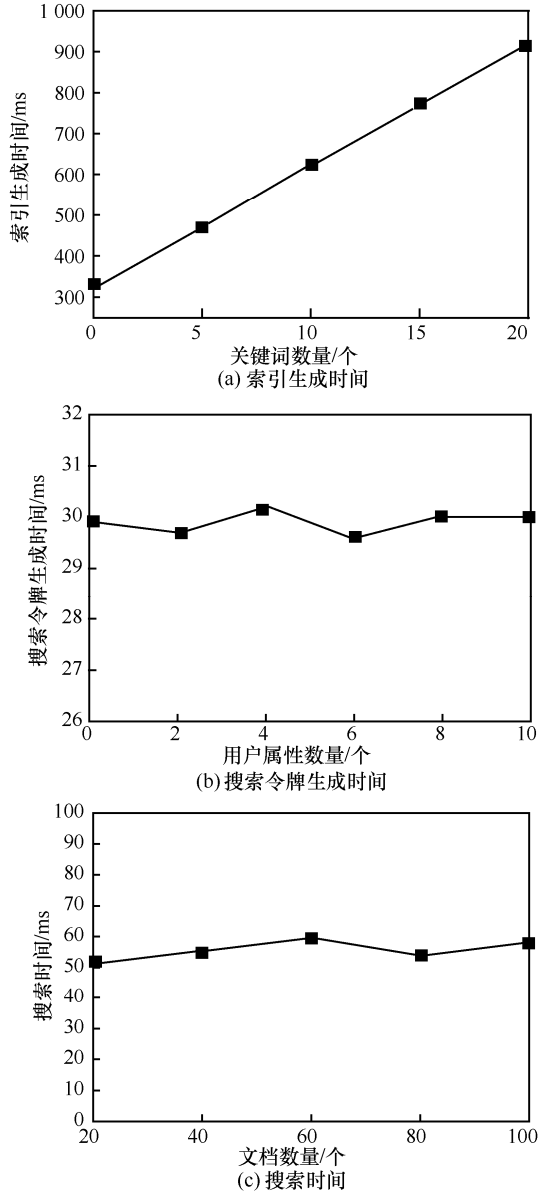

图 2　实验结果

如图 2(c)所示，当文档数量为 20 时，用户搜索关键词“Blockchain”的时间为 51 ms；当文档数量为 60 时，搜索时间为 60 ms；当文档数量为 100 时，搜索效率为 58 ms。在搜索效率方面，由于构建索引时采用基于键值对的查找表方式，因此随着文件数量的增加，检索效率保持不变，平均测试检索时间为 56 ms。在用户支付一定的手续费后，只需大约 56 ms 便可得到正确的搜索结果，而不需要额外步骤对结果正确性进行验证。搜索效率表明，本文方案具有实时性，满足云存储环境下搜索应用需求。

综合以上分析，本文方案实际性能测试和理论性能分析一致，且安全索引生成阶段、搜索令牌生成阶段以及搜索阶段响应时间都处于毫秒级别，在实际应用过程中不需要用户过长的等待，不会影响用户的操作习惯，因此本文方案在智慧医疗等一对多搜索环境中具有实用性。

7　结束语

本文方案在对称可搜索加密的基础上，采用密文策略属性加密机制和以太坊智能合约技术，构造了一种基于区块链且支持验证的属性可搜索加密方案，实现一对多搜索模型下对共享解密密钥的细粒度访问控制，并且在半诚实且好奇的云服务器模型下验证返回结果的正确性，而不需要用户本地验证就能得到正确的结果，减轻用户计算开销。同时由于区块链的不可篡改性，保证用户和云服务器之间的服务–支付公平，使用户支付手续费就一定得到正确的检索结果，同时云服务器在提供正确结果后收到相应的服务费，并且用户不可否认云服务器提供的正确结果而拒绝支付服务费，使各参与方均诚实地按照合约的规则执行操作。实际性能测试和理论性能分析表明，本文方案与相关方案相比，在安全索引产生、搜索令牌生成、检索效率以及交易数量方面有一定的性能提升，在保障数据隐私的同时，提高了检索效率并验证结果的正确性。下一步将考虑多关键词搜索等灵活的查询方式，以提高查询的精确度，避免带宽的浪费。

参考文献：

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

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

[3] YIN H, ZHANG J, XIONG Y, et al. CP-ABSE: a ciphertext-policy attribute-based searchable encryption scheme[J]. IEEE Access, 2019, 7(99): 5682-5694.

[4] 刘振华, 周佩琳, 段淑红. 支持关键词搜索的属性代理重加密方案[J]. 电子与信息学报, 2018, 40(3):683-689.
LIU Z H, ZHOU P L, DUAN S H. Attribute proxy re-encryption scheme supporting keyword search[J]. Journal of Electronics & Information Technology, 2018,40(3):683-689.

[5] 孙瑾, 王小静, 王尚平, 等. 支持属性撤销的可验证多关键词搜索加密方案[J]. 电子与信息学报, 2019, 41(1):53-60.
SUN J, WANG X J, WANG S P, et al. Verifiable multi-keyword search encryption scheme supporting attribute revocation[J]. Journal of Electronics & Information Technology, 2019, 41(1):53-60.

[6] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[C]//The 13th ACM Conference on Computer and Communications Security. Alexandria, 2006: 79-88.

[7] CHAI Q, GONG G. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers[C]//The 2012 IEEE International Conference on Communications. Ottawa, 2012: 917-922.

[8] JIANG X, YU J, YAN J, et al. Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data[J]. Information Sciences, 2017, 40(3):22-41.

[9] 杜瑞忠, 李明月, 田俊峰, 等. 基于倒排索引的可验证混淆关键字密文检索方案[J]. 软件学报, 2019, 30(8): 2362-2374.
DU R Z, LI M Y, TIAN J F, et al. A ciphertext retrieval scheme for verifiable confusing keywords based on inverted index[J]. Journal of Software, 2019, 30(8): 2362-2374.

[10] 伍祈应, 马建峰, 李辉, 等. 支持用户撤销的多关键字密文查询方案[J]. 通信学报, 2017, 38(8):183-193.
WU Q Y, MA J F, LI H, et al. Multi-keyword ciphertext query scheme supporting user revocation[J]. Journal on Communications, 2017, 38(8): 183-193.

[11] CAI C, WENG J, YUAN X, et al. Enabling reliable keyword search in encrypted decentralized storage with fairness[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 1(99): 1.

[12] ZHANG Y H, DENG R H, SHU J, et al. TKSE: trustworthy keyword search over encrypted data with two-side verifiability via blockchain[J]. IEEE Access, 2018(6): 31077-31087.

[13] WANG S P, ZHANG Y L, ZHANG Y L. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018(6): 38437-38450.

[14] CHEN L X, LEE W K, CHANG C C, et al. Blockchain based searchable encryption for electronic health record sharing[J]. Future Generation Computer Systems, 2019, 95: 420-429.

[15] 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.

[作者简介]

闫玺玺（1985− ），女，河南灵宝人，博士，河南理工大学副教授，主要研究方向为网络与信息安全、数字版权管理、数字内容安全和密码学。

原笑含（1995− ），女，河南焦作人，河南理工大学硕士生，主要研究方向为密码学、网络与信息安全。

汤永利（1972− ），男，河南焦作人，博士，河南理工大学教授，主要研究方向为现代密码学、网络与信息安全。

陈艳丽（1981− ），女，河南洛阳人，河南理工大学讲师，主要研究方向为人工智能、计算机应用、网络与信息安全。