区块链上基于云辅助的密文策略属性基数据共享加密方案

牛淑芬[①] 杨平平*[①] 谢亚亚[①] 杜小妮[②]
[①](西北师范大学计算机科学与工程学院 兰州 730070)
[②](西北师范大学数学与统计学院 兰州 730070)

摘 要：针对云存储的集中化带来的数据安全和隐私保护问题，该文提出一种区块链上基于云辅助的密文策略属性基(CP-ABE)数据共享加密方案。该方案采用基于属性加密技术对加密数据文件的对称密钥进行加密，并上传到云服务器，实现了数据安全以及细粒度访问控制；采用可搜索加密技术对关键字进行加密，并将关键字密文上传到区块链(BC)中，由区块链进行关键字搜索保证了关键字密文的安全，有效地解决现有的云存储共享系统所存在的安全问题。该方案能够满足选择明文攻击下的不可区分性、陷门不可区分性和抗串联性。最后，通过性能评估，验证了该方案的有效性。

关键词：区块链；属性基加密；可搜索加密；细粒度访问控制
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2021)07-1864-08
DOI: 10.11999/JEIT200124

Cloud-Assisted Ciphertext Policy Attribute Based Eencryption Data Sharing Encryption Scheme Based on BlockChain

NIU Shufen[①] YANG Pingping[①] XIE Yaya[①] DU Xiaoni[②]
[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)
[②](*College of Computer Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: To solve the problem of data security and privacy preservation brought by the centralization of cloud storage, a cloud-assisted Ciphertext Policy Attribute Based Eencryption(CP-ABE) data sharing encryption scheme based on BlockChain(BC) is proposed. In this scheme, the symmetric key of the encrypted file is encrypted by attribute-based encryption and the encrypted file is uploaded to cloud server for realizing the data security and fine-grained access control. Searchable encryption technology is adopted to encrypt the keyword, and the keyword ciphertext is uploaded to the BlockChain. Keyword search is executed by the BlockChain to ensure the security of keyword ciphertext, which effectively solves the security problems existing in the cloud storage and sharing system. This scheme can satisfy the indiscernibility, trap indiscernibility and series resistance under the selective plaintext attack. Finally, the effectiveness of the scheme is verified by performance evaluation.

Key words: BlockChain(BC); Attribute-based encryption; Searchable encryption; Fine-grained access control

1 引言

为了节省本地的数据管理开销和系统维护开销，数据拥有者会选择将数据上传到云端服务器中，云存储数据共享技术就成为信息交互的一种重要方式[1]。但云存储在给用户带来便利的同时也会造成用户隐私泄露问题[2]。

可搜索加密技术[3,4]实现了数据用户利用关键字搜索陷门对密文数据进行检索，同时也不会泄露关键字。基于属性加密技术[5–7]在实现数据隐私的同时还能够实现细粒度访问控制。尽管如此，基于云存储的数据共享模式大多数依赖第三方，一旦受到攻击或缺乏监控，第三方可能会窃取、泄露、篡改或滥用数据。还有传统的云存储模式以集中存储方式运行，存在单点故障等可能导致系统崩溃的问题[8]。

区块链技术[9]的发展能够解决云存储中数据可

收稿日期：2020-02-21；改回日期：2020-12-08；网络出版：2020-12-23
*通信作者： 杨平平 862558924@qq.com
基金项目：国家自然科学基金(61562077, 61662069, 61662071, 61772022)，西北师范大学青年教师科研提升计划(NWNU-LKQN-13-12)
Foundation Items: The National Natural Science Foundation of China (61562077, 61662069, 61662071, 61772022), The Young Teacher's Scientific Research Ability Promotion Program of Northwest Normal University (NWNU-LKQN-13-12)

能被篡改、完整性得不到保证的问题。区块链技术是一种特定的数据结构，这种数据结构按照时间顺序将数据区块组合成链条，由此来保证其不可篡改性和不可伪造性[10]；区块链也是一种去中心化的分布式数据库，它由区块链网络中的所有节点共同维护数据，每一个节点都会对数据进行备份。但是，如何在区块链中实现数据隐私保护以及如何实现只有授权数据用户才能访问数据是目前所要面临的一个挑战[4]。

针对以上问题，本文提出一种区块链上基于云辅助的密文策略属性基(Ciphertext Policy Attribute Based Eencryption, CP-ABE)数据共享加密方案，将基于属性加密技术和可搜索加密技术相结合，实现了数据共享的隐私保护和数据安全。在本方案中，使用对称加密算法对数据文件进行加密，将加密的数据文件存储在云服务器上。基于属性加密算法则对对称密钥进行加密，并且将访问策略与关键字加密结合，密文存储在区块链上，由区块链完成搜索。保证了只有当数据用户的属性集满足密文中的访问策略并且关键字匹配时，区块链才能够返回搜索结果。本文方案中访问策略使用的是线性秘密共享矩阵[11](Linear Secret Sharing Scheme, LSSS)，不仅能够实现细粒度访问控制，而且具有较高的计算效率。

2　基础知识

2.1　区块链

区块链技术起源于文献[9]发表的论文《比特币:一种点对点电子现金系统》，是一种去中心化、不可篡改、可信的分布式账本。根据不同的应用场景，区块链可分为公有链、联盟链和私有链。本文方案中所使用的区块链为联盟链，是指由特定的组织或个人参与建立的，由该群体内部共同许可的多个节点作为记账人，所有区块的产生也由这些节点之间的共识规则决定。

本文中区块的数据结构由块头和有效负载组成。块头包括块标识(Block ID)、块的大小(Block size)、前一个区块的哈希值(Pre-block hash)和时间戳(Timestamp)；有效负载包括块产生者的身份(Block producer ID)、块产生者的签名(Block producer signature)和交易单(Transaction)。数据结构如表1所示。

2.2　共识机制

共识机制的作用就是验证无中心的分布式网络环境中数据的真实性和一致性。共识机制保证了所有节点在不依赖中心协调的情况下使得所有交易以可靠方式进行。目前，区块链在联盟链环境下最常用的是实用拜占庭容错(Practical Byzantine Fault Tolerant, PBFT)共识算法[12]。PBFT算法过程[13]如下：客户端负责将交易上传至主节点，主节点对全网交易单进行打包并广播给从节点；从节点执行验证操作，并将验证结果返回给客户端；客户端接收从节点返回的结果，若验证正确结果数大于f+1，则表示上链存储成功。

2.3　困难问题假设

令$(G,\times)$和$(G_{\mathrm{T}},\times)$是两个阶均为大素数p的循环群，g是群G的生成元。

定义1(判定性q-BDHE假设[14])　循环群上线性映射是指具有下列性质的映射$e:G\times G\to G_{\mathrm{T}}$:随机选取$\alpha,s\in Z_p$，计算$Q=(g,g^s,g^{\alpha},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}})$。若不存在一个算法可以在多项式时间内以不可忽略的优势区分$e(g,g)^{\alpha^{q+1}s}$与G_{T}中的随机元素，则称q-BDHE假设成立。

定义2(判定性DDH假设)　给定$g,g^a,g^b,g^c\in G$，其中$a,b,c\in Z_p$，判断g^{ab}是否等于g^c。如果在多项式时间内，没有一个攻击者$\mathcal{A}$能够以一个不可忽略的优势将上述两个元组区分开来，则攻击者$\mathcal{A}$的优势定义为：$\mathrm{Adv}_{\mathrm{DDH}}(\mathcal{A})=\left|\Pr[\mathcal{A}(g^a,g^b,g^{ab})=1]\right|-\left|\Pr[\mathcal{A}(g^a,g^b,g^c)=1]\right|$。

3　系统模型与安全模型

3.1　系统模型

本方案的系统模型如图1所示，主要包括以下5个实体：

(1) 属性授权中心 (Attribute Authority, AA)：AA是一个可信机构，主要生成系统参数、系统主密钥以及数据用户DU和云服务器CS的私钥。定义属性集合，当DU加入系统时，属性授权中心AA为其分配一个唯一标识uid和一个属性集Suid。

(2) 云服务器 (Cloud Server, CS)：CS负责存储数据拥有者DO提供的加密的数据文件F以及将文件存储位置F_{id}发送到DO在区块链的账户。如果数据用户DU满足访问策略，CS则进行部分解密并将部分解密的密文A和相应加密的数据文件$E_k(F)$发送到DU在区块链的账户。

表 1　区块数据结构

Block Head				Payload		
Block ID ID	Block size size	Pre-block hash hash	Timestamp t	Block producer ID Data Owner	Block producer signature δ	Transaction TX

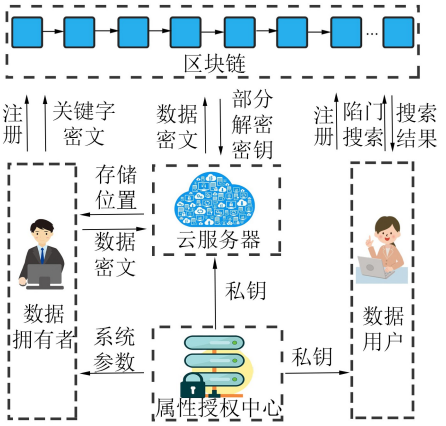

图 1 系统模型

(3) 区块链 (BlockChain, BC)：区块链上DO将关键字索引作为交易存储在BC上，前提是这一交易需要经过区块链验证者的验证。本文中区块链采用PBFT共识算法，该算法在全网节点不超过1/3的情况下，保证分布式节点网络的一致性。DU将搜索陷门上传到BC上，BC进行关键字密文搜索。当搜索成功后，BC将与对称密钥k有关的密文返回给CS，云服务器CS进行部分解密运算。

(4) 数据拥有者 (Data Owner, DO)：DO从数据文件中提取关键字，使用对称密钥加密数据文件得到C_F，然后建立关键字索引。DO定义数据文件的访问策略，并对访问策略下的对称密钥进行加密从而获得相应的密文C以及对关键字和每个属性加密得到C_i。最后，DO将加密的数据文件C_F和密文C上传到CS上并且将关键字密文C_i和存储地址F_{id}构成的交易上传至区块链BC上形成新的区块。

(5) 数据用户 (Data User, DU)：数据用户DU搜索陷门上传到区块链上，验证通过后，区块链将加密的数据文件$E_k(F)$与部分解密的密文A返回到DU在区块链的账户上，DU使用自己的私钥对A解密得到对称密钥k，从而能够对加密的数据文件进行解密，得到数据文件明文。

3.2 算法模型

本文方案由以下6个概率多项式时间算法组成。

系统建立$\mathrm{Setup}(\lambda)$：给定一个安全参数λ，AA产生系统主密钥MSK和系统公共参数Params以及属性集合$\boldsymbol{U}$。

密钥生成$\mathrm{KeyGen}(\mathrm{Params}, \mathrm{MSK})$：以MSK为输入，AA计算出$\mathrm{SK}_{\mathrm{CS}}$,$\mathrm{SK}_{\mathrm{uid}}$，然后将$\mathrm{SK}_{\mathrm{uid}}$发送给DU，将$\mathrm{SK}_{\mathrm{CS}}$发送给CS。AA还为DU分配一个属性集Suid。

加密阶段$\mathrm{Encryption}(\mathrm{Params}, w, \boldsymbol{U}, k, T)$：这一阶段由DO执行。使用对称密钥$k$对数据文件进行加密，输入Params,$w$，属性集合$\boldsymbol{U}$以及访问策略$T$，输出CT。

陷门生成$\mathrm{Trapdoor}(w', \mathrm{Suid})$：对于关键字$w'$，DU结合自身属性集Suid中的属性，生成陷门$T_i, T_i'$。

测试阶段$\mathrm{Test}(\mathrm{CT}, T, T_i, T_i')$：DU所搜索的关键字$w'$和拥有的属性集Suid满足访问结构$T$时，输出"True"，并将CT中的$B$返回给CS；否则，输出"False"。

解密阶段$\mathrm{Decryption}(\mathrm{Params}, \mathrm{SK}_{\mathrm{CS}}, \mathrm{SK}_{\mathrm{uid}}, B)$：CS根据$\mathrm{SK}_{\mathrm{CS}}$，$B$计算得出$A$，并将$A$返回给DU，DU利用自身私钥$\mathrm{SK}_{\mathrm{uid}}$和$A$得出对称密钥$k$，对加密的数据文件进行解密，从而得到数据文件明文。

3.3 安全模型

3.3.1 选择明文攻击下的不可区分性

定义3 为证明选择明文攻击下的不可区分性，我们定义了攻击者$\mathcal{A}_1$和挑战者$\mathcal{B}$之间的交互性游戏Game_1。如果在多项式时间内，攻击者$\mathcal{A}_1$赢得游戏的概率是可忽略的，则称方案是适应性选择明文安全的。

初始化阶段: 挑战者$\mathcal{B}$运行系统建立算法输出公共参数并定义访问策略，攻击者$\mathcal{A}_1$输出挑战身份ID。

哈希询问阶段: 挑战者$\mathcal{B}$建立如下哈希询问：

$O_{H_1}(w)$：攻击者$\mathcal{A}_1$输入关键字w，挑战者$\mathcal{B}$返回$H_1(w)$。

$O_{H_2}(\rho(i))$：攻击者$\mathcal{A}_1$输入属性$\rho(i)$，挑战者$\mathcal{B}$返回$H_2(\rho(i))$。

询问阶段1：$O_{\mathrm{SK}}(\mathrm{Params})$：挑战者$\mathcal{B}$运行密钥生成算法输出私钥。

挑战阶段：当询问阶段1完毕，攻击者$\mathcal{A}_1$选择两个明文(m_0, m_1)、挑战身份ID$*$和访问控制策略$(\boldsymbol{M}*, \rho*)$一起发送给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$输出挑战密文给攻击者$\mathcal{A}_1$。

询问阶段2：攻击者$\mathcal{A}_1$进行询问，除挑战密文及其衍生不能询问外，其他同询问阶段1一致。

猜测阶段：最后攻击者$\mathcal{A}_1$返回猜测δ'，如果$\delta'=\delta$，则挑战成功，输出1；否则输出0。

3.3.2 陷门不可区分性

定义4 为证明满足陷门不可区分性，我们定义了攻击者$\mathcal{A}_2$和挑战者$\mathcal{B}$之间的交互性游戏Game_2。如果在多项式时间内，攻击者$\mathcal{A}_2$赢得游戏的概率是可忽略的，则称方案是满足陷门不可区分性。

初始化阶段：挑战者$\mathcal{B}$运行系统建立算法输出公共参数，攻击者$\mathcal{A}_2$选择挑战身份ID。

询问阶段1：攻击者$\mathcal{A}_2$发起了多项式次数的私钥询问和陷门询问。

$O_{\mathrm{SK}}(\mathrm{Params}, \mathrm{L})$：$\mathcal{A}_2$选择用户的ID和公共参数

Params给挑战者$\mathcal{B}$。$\mathcal{B}$运行密钥生成算法输出私钥。

$O_{\text{Trapdoor}}(w)$：攻击者$\mathcal{A}_2$输入关键字w，挑战者$\mathcal{B}$设置陷门发送给攻击者$\mathcal{A}_2$。

挑战阶段: 询问阶段1完毕，攻击者$\mathcal{A}_2$选择两个关键字(w_0, w_1)和挑战身份ID*发送给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$回应挑战陷门。

询问阶段2：攻击者$\mathcal{A}_2$进行询问，除挑战密文及其衍生不能询问外，其他同询问阶段1一致。

猜测阶段：最后敌手返回猜测δ'，如果δ'=δ，则挑战成功，输出1；否则输出0。

4　具体方案

本文所提出的方案由以下6个概率多项式时间算法组成，算法模型如图2所示，具体设计如下：

系统建立(Setup)：AA随机选取一个安全参数λ，输入系统安全参数后，输出系统公共参数Params和主密钥MSK。设G和G_{T}分别是两个阶为素数q的循环群，g是G的一个生成元，$e: G \times G \to G_{\text{T}}$是一个双线性映射。AA定义属性集合$\boldsymbol{U}$，每个属性$x \in \boldsymbol{U}$。随机选取$\alpha, \beta, a \in Z_p$，将$\alpha$作为系统主密钥MSK；然后选择两个哈希函数：$H_1: \{0,1\}^* \to G$, $H_2: \{0,1\}^* \to G$；最后，AA公布Params = $\{G, G_{\text{T}}, e(g,g)^{\alpha}, g^{\beta}, g^{a}, H_1, H_2\}$。

密钥生成(KeyGen)：DU加入系统时，AA为其分配一个唯一标识符uid和一个属性集Suid。AA随机选取$\alpha_1, \alpha_2 \in Z_p^*$, α_1, α_2满足α= $(\alpha_1 + \alpha_2) \bmod p$，计算$\text{SK}_{\text{uid}} = g^{\alpha_1} \cdot g^{a\beta}$, $\text{SK}_{\text{CS}} = g^{\alpha_2}$。然后将$\text{SK}_{\text{uid}}$发送给DU，将$\text{SK}_{\text{CS}}$发送CS。

加密阶段(Encryption)：数据加密：数据拥有者DO随机选取一个对称密钥k，使用DES对称加密算法对数据文件F进行加密，得到加密的数据文件C_F=$E_k(F)$。

关键字加密：DO从数据文件F中提取关键字w，然后定义LSSS访问策略$(\boldsymbol{M}, \rho)$将对称密钥k和关键字w进行加密。其中，$\boldsymbol{M}$是$l \times n$的矩阵，ρ为内映射函数，是矩阵$\boldsymbol{M}$的每一行$\boldsymbol{M}_x$到属性集合中属性$\rho(x)$的映射，每个属性在矩阵$\boldsymbol{M}$中都有唯一的行与之对应。随机选取向量$\boldsymbol{v} = (s, y_2, \cdots, y_n) \in Z_q$,$s$为要分享的秘密值。对于矩阵的每一行$i \in [1, l]$，计算$\lambda_i = \boldsymbol{M}_i \cdot \boldsymbol{v}$，其中$\boldsymbol{M}_i$为矩阵$\boldsymbol{M}$的第$i$行向量。DO计算

$$\begin{aligned}&\text{CT} = \{(\boldsymbol{M}, \rho), C = e(g,g)^{\alpha s} \cdot k, C' = g^{s},\\ &B = e(g^{as}, g^{\beta})\\ &\forall_{i=1,2,\cdots,l}: C_i = [H_1(w) \cdot H_2(\rho(i))]^{\lambda_i},\\ &C_i' = (g^{a})^{\lambda_i}\}\end{aligned}$$

DO将$(C, C', E_k(F))$上传到CS上，CS返回给DO文件存储位置F_{id}。然后再将$(B, C_i, C_i', F_{\text{id}})$构成块上的交易单TX = $(B, C_i, C_i', F_{\text{id}})$，并对交易单进行签名得到$\delta$，然后向主节点提交验证请求。区块链全网节点执行PBFT共识算法，主节点对一个时间段接收到的交易单打包后，发送给从节点进行验证。DO接收验证节点的验证结果，若验证结果正确数大于f+1，则表明新区块已经添加到区块链上。新区块的结构如表1所示。

陷门生成(Trapdoor)：对于属性集Suid中的每一个属性a_i, DU随机选取$r_i \in Z_p^*$，计算$T_i = [H_1(w') \cdot H_2(a_i)]^{r_i}$。DU将三元组$(\text{uid}, T_i, T_i')$上传到BC上。

测试阶段(Test)：当数据用户DU所搜索的关键字w'和拥有的属性集Suid满足访问结构$(\boldsymbol{M}, \rho)$时，区块链节点进行以下操作：选择$I \subset \{1, 2, \cdots, l\}$，并定义$I = \{i : \rho(i) \in S\}$。那么，根据LSSS协议，可以在多项式时间内找出一个常数集$\{\omega_i \in Z_p\}_{i \in I}$，使得$\sum_{i \in I} \omega_i \cdot \lambda_i = s$。测试如下

$$\frac{\prod_{i \in I} e(g^{\beta} \cdot T_i, C_i')^{\omega_i}}{\prod_{i \in I} e(T'_i, C_i)^{\omega_i}} = B$$

如果等式不成立，则输出错误符号"⊥"；如果等式成立，区块链节点则根据数据文件位置F_{id}将B以及数据用户DU在区块链上的账户发送到云服务器CS上。

解密阶段(Decryption)：(1)云服务器CS利用私钥SK_{CS}进行部分解密计算：$A = \dfrac{B}{e(C', \text{SK}_{\text{CS}})} = \dfrac{e(g,g)^{a\beta s}}{e(g,g)^{\alpha_2 s}}$计算完成后，云服务器将部分解密的密文$A$以及加密的数据文件$E_k(F)$发送给数据用户DU。

(2) 数据用户DU利用私钥SK_{uid}以及部分解密的密文A计算得出对称密钥k，从而对加密的数据文件$E_k(F)$进行解密，获得数据文件F

$$k = \frac{C \cdot A}{e(C', \text{SK}_{\text{uid}})}, \quad F = \text{Dec}_k(C_F)$$

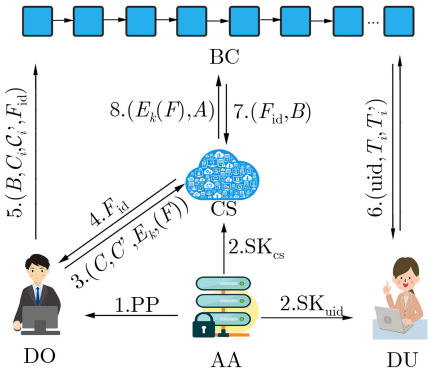

图 2 算法模型

正确性证明：

(1) 测试阶段的正确性：$\dfrac{\prod_{i\in I} e(g^{\beta}\cdot T_i, C_i')^{\omega_i}}{\prod_{i\in I} e(T'_i, C_i)^{\omega_i}}=$

$$\frac{\prod_{i\in I} e(g^{\beta}\cdot[H_1(w')\cdot H_2(a_i)]^{r_i}, (g^{a})^{\lambda_i})^{\omega_i}}{\prod_{i\in I} e((g^{a})^{r_i}, [H_1(w)\cdot H_2(\rho(i))]^{\lambda_i})^{\omega_i}}$$

$$=\frac{\prod_{i\in I} e([H_1(w')\cdot H_2(a_i)]^{r_i}, g^{a\lambda_i\omega_i})\prod_{i\in I} e(g^{\beta}, g^{a\lambda_i\omega_i})}{\prod_{i\in I} e(g^{a\omega_i\lambda_i}{}_i, [H_1(w)\cdot H_2(\rho(i))]^{r_i})}$$

$$=\prod_{i\in I} e(g^{\beta}, g^{a\lambda_i\omega_i})=e(g^{\beta}, g^{as})$$

(2) 解密阶段的正确性：$\dfrac{C\cdot A}{e(C', \mathrm{SK}_{\mathrm{uid}})}=$

$$\frac{e(g,g)^{\alpha s}\cdot k\cdot e(g,g)^{a\beta s}}{e(g^{s}, g^{\alpha_1}\cdot g^{a\beta})e(g,g)^{\alpha_2 s}}=\frac{e(g,g)^{\alpha s}\cdot k\cdot e(g,g)^{a\beta s}}{e(g^{s}, g^{\alpha_1+\alpha_2})e(g,g)^{a\beta s}}=k。$$

证毕

5 安全性证明

5.1 选择明文攻击下的不可区分性

定理1 若攻击者$\mathcal{A}_1$在一个概率多项式时间内能以不可忽略的优势ε赢得游戏，则证明挑战者$\mathcal{B}$能够以不可忽略的优势$\varepsilon/2$解决q-BDHE困难问题。

证明 假设给挑战者$\mathcal{B}$一个q-BDHE实例$\left(g, g^{s}, g^{a}, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{a^{2q}}, T\right)$，挑战者$\mathcal{B}$的目的是确定$T=e(g,g)^{a^{q+1}s}$是否成立。游戏过程如下：挑战者$\mathcal{B}$选择$(G,\times)$和$(G_{\mathrm{T}},\times)$两个阶均为大素数$p$的循环群，$g$是群$G$的生成元，则双线性对为$e: G\times G\to G_{\mathrm{T}}$。

初始化阶段：$\mathcal{B}$选取随机数$\alpha', \beta\in Z_p^*$，计算$\alpha=\alpha'+a^{q+1}$则$e(g,g)^{\alpha}=e(g,g)^{\alpha'+a^{q+1}}=e\left(g^{a}, g^{a^{q}}\right)e(g,g)^{\alpha'}$。$\mathcal{B}$输出公共参数Params=$\{G, G_{\mathrm{T}}, e\left(g^{a}, g^{a^{q}}\right)e(g,g)^{\alpha'}, g^{\beta}, g^{a}, H_1, H_2\}$。挑战者$\mathcal{B}$定义LSSS访问策略$(\boldsymbol{M},\rho)$。最后，攻击者$\mathcal{A}_1$输出挑战身份ID，挑战者$\mathcal{B}$设置数组$(\mathrm{ID}, \rho(i), R^{(2)}, \mathrm{SK}, \mathrm{coin})$放入列表$L^{\mathrm{list}}$中，此时$\rho(i), R^{(2)}$为空值。

哈希询问阶段: 挑战者$\mathcal{B}$建立如下哈希询问：

$O_{H_1}(w)$：攻击者$\mathcal{A}_1$输入关键字w，挑战者$\mathcal{B}$从列表$L_{\mathrm{H_1}}$中恢复数组$(w, r, R^{(1)}, \mathrm{coin})$，若$w, R^{(1)}$不为空值，挑战者$\mathcal{B}$提取$R^{(1)}$发送给攻击者$\mathcal{A}_1$。否则，挑战者$\mathcal{B}$选择随机数$r^{(1)}\in Z_p^*$，挑战者$\mathcal{B}$设置$R^{(1)}=g^{r^{(1)}}g^{aM_{i.1}}g^{a^2M_{i.2}}\cdots g^{a^nM_{i.n}}$记入数组$(w, r, R^{(1)}, \mathrm{coin})$。

$O_{H_2}(\rho(i))$：攻击者$\mathcal{A}_1$输入属性$\rho(i)$。挑战者$\mathcal{B}$从列表L^{list}中恢复数组$(\mathrm{ID}, \rho(x), R^{(2)}, \mathrm{SK}, \mathrm{coin})$，若$\rho(i), R^{(2)}$不为空值，挑战者$\mathcal{B}$提取$R^{(2)}$发送给攻击者$\mathcal{A}_1$。否则，挑战者$\mathcal{B}$选择随机数$z_x\in Z_p^*$并抛掷一个硬币$\mathrm{coin}\in\{0,1\}$。若正面朝上，则$\mathrm{coin}=0$，挑战者$\mathcal{B}$设置$R^{(2)}=g^{z_x}g^{aM_{i.1}}g^{a^2M_{i.2}}\cdots g^{a^nM_{i.n}}$记入数组$(\mathrm{ID},\rho(i),R^{(2)},\mathrm{SK},\mathrm{coin})$。否则$\mathrm{coin}=1$，挑战者设置$R^{(2)}=g^{z_x}$记入数组$(\mathrm{ID},\rho(i),R^{(2)},\mathrm{SK},\mathrm{coin})$。

询问阶段1:$O_{\mathrm{SK}}(\mathrm{Params})$：攻击者$\mathcal{A}_1$选择用户ID和公共参数Params给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$从列表$L^{\mathrm{list}}$中恢复数组$(\mathrm{ID},\rho(i),R^{(2)},\mathrm{SK},\mathrm{coin})$，若$\rho(i),\mathrm{SK}$不为空值，挑战者$\mathcal{B}$提取私钥发送给攻击者$\mathcal{A}_1$。否则，挑战者$\mathcal{B}$随机选择$\alpha_1'\in Z_p^*$，计算$\alpha_1=\alpha_1'+a^{q+1}$，$\alpha_2=\alpha_2'=\alpha'-\alpha_1'$，并查看coin值。若$\mathrm{coin}=1$，挑战者$\mathcal{B}$输出$\mathrm{SK}_{\mathrm{CS}}=g^{\alpha_2}=g^{\alpha_2'}$, $\mathrm{SK}_{\mathrm{uid}}=g^{\alpha_1'+a^{q+1}}\cdot g^{a\beta}=g^{\alpha_1}\cdot g^{a\beta}$。否则$\mathrm{coin}=0$，挑战者$\mathcal{B}$输出失败。

挑战阶段：当询问阶段1完毕，攻击者$\mathcal{A}_1$选择两个明文(m_0,m_1)、挑战身份ID$*$和访问控制策略$(\boldsymbol{M}*,\rho*)$一起发送给挑战者$\mathcal{B}$。挑战者B从列表L^{list}中恢复数组$(\mathrm{ID}*,\rho(i)*,R^{(2)}*,\mathrm{SK}*,\mathrm{coin}*)$，若$\mathrm{coin}*=1$，挑战者$\mathcal{B}$输出失败(该事件用$E$表示)；否则挑战者$\mathcal{B}$随机选择$y_2',\cdots,y_n'\in Z_p^*$，则向量$\boldsymbol{v}=(s, y_2'/sa, y_3'/sa^2,\cdots,y_n'/sa^{n*-1})\in Z_q$，对于矩阵的每一行$i\in[1,l]$，计算$\lambda_i=\boldsymbol{M}_i\boldsymbol{v}$。挑战者$\mathcal{B}$随机选取$\delta\in\{0,1\}$，设置：$\mathrm{CT}*=\{(\boldsymbol{M}*,\rho*), C*=e(g,g)^{\alpha s}\cdot k=e(g,g)^{a^{q+1}s}e(g,g)^{\alpha' s}\cdot k=T\cdot e(g,g)^{\alpha' s}\cdot k, C'*=g^{s}, B*=e(g^{as},g^{\beta})$

$$\forall_{i=1,2,\cdots,n}: C_i*=[H_1(w)\cdot H_2(\rho(i))]^{\lambda_i}=\prod_{j=1,2,\cdots,n}\left(g^{r^{(1)}}g^{z_x}\right)^{\boldsymbol{M}_{i,j}y_j},$$

$$C_i'*=(g^{a})^{\lambda_i}=\prod_{j=1,2\cdots,n} g^{M_{i,j}y_j/a^{j+1}}\}$$

最后挑战者$\mathcal{B}$输出挑战密文$(C*, C'*, C_i*, C_i'*, B*, E_k(F))$给攻击者$\mathcal{A}_1$。

询问阶段2: 攻击者$\mathcal{A}_1$进行询问，除挑战密文及其衍生不能询问外，其他同询问阶段1一致。

猜测阶段：最后攻击者$\mathcal{A}_1$返回猜测δ'，如果$\delta'=\delta$，则挑战成功，输出1；否则输出0。

分析：若事件E没有发生，攻击者$\mathcal{A}_1$能攻破方案，则挑战者$\mathcal{B}$能解决q-BDHE困难问题。若$\mathrm{coin}=0$，则密文$C=e(g,g)^{\alpha s}\cdot k=T\cdot e(g,g)^{\alpha' s}\cdot k$是一个$q$-BDHE实例，攻击者$\mathcal{A}_1$的优势为$\varepsilon=\Pr[\delta'=\delta]-1/2$，挑战者$\mathcal{B}$获胜的概率$\Pr[\delta'=\delta|\beta=1]=\Pr[\delta'=\delta]=\varepsilon+1/2$。否则，事件$E$发生，挑战者$\mathcal{B}$获胜的概率$\Pr[\delta'=\delta|\beta=0]=\Pr[\delta'\neq\delta]=1/2$。那么挑战者能解决$q$-BDHE困难问题的优势

$$\mathrm{Adv}=\Pr[\delta'=\delta]-1/2=1/2\left(\Pr[\delta'=\delta|\beta=1]+\Pr[\delta'=\delta|\beta=0]\right)-1/2=\varepsilon/2$$

证毕

5.2 陷门不可区分性

定理2 若攻击者$\mathcal{A}_2$在一个概率多项式时间内能以不可忽略的优势ε赢得游戏，则证明挑战者$\mathcal{B}$能够以不可忽略的优势$\dfrac{\varepsilon}{e\left(q_{\mathrm{T}}+1\right)}$解决DDH困难问题。

证明　假设给挑战者$\mathcal{B}$一个DDH实例(g^a, g^b, g^c)，挑战者$\mathcal{B}$的目的是确定$g^c = g^{ab}$是否成立。游戏过程如下：

挑战者$\mathcal{B}$选择$(G,\times)$和$(G_{\mathrm{T}},\times)$两个阶均为大素数p的循环群，g是群G的生成元，则双线性对为$e: G\times G\to G_{\mathrm{T}}$，哈希函数为$H_1:\{0,1\}^*\to G$, $H_2:\{0,1\}^*\to G$。

初始化阶段：挑战者$\mathcal{B}$选取随机数$\alpha,\beta\in Z_p^*$，则输出公共参数$\mathrm{Params}=\{G, G_{\mathrm{T}}, e(g,g)^{\alpha}, g^{\beta}, g^{a}, H_1, H_2\}$。挑战者$\mathcal{B}$定义LSSS访问策略$(\boldsymbol{M},\rho)$。最后，攻击者$\mathcal{A}_2$输出挑战身份ID，挑战者$\mathcal{B}$设置数组$(\mathrm{ID}, w, a_j, \mathrm{SK}, \mathrm{coin})$放入列表$L^{\mathrm{list}}$中，此时$w, a_j, \mathrm{SK}$为空值。

询问阶段1：攻击者$\mathcal{A}_2$发起了多项式次数的私钥询问和陷门询问。

$O_{\mathrm{SK}}\left(\mathrm{Params}, L^{\mathrm{list}}\right)$：攻击者$\mathcal{A}_2$选择用户的ID和公共参数Params给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$从列表$L^{\mathrm{list}}$中恢复数组$(\mathrm{ID}, w, a_j, \mathrm{SK}, \mathrm{coin})$，若$a_j, \mathrm{SK}$不为空值，挑战者$\mathcal{B}$提取私钥发送给攻击者$\mathcal{A}_2$。否则，挑战者$\mathcal{B}$随机选取$\alpha_1,\alpha_2\in Z_p^*$，$\alpha_1,\alpha_2$满足$\alpha=(\alpha_1+\alpha_2)\bmod p$，计算$\mathrm{SK}_{\mathrm{uid}}=g^{\alpha_1}\cdot g^{a\beta}$，$\mathrm{SK}_{\mathrm{CS}}=g^{\alpha_2}$。

$O_{\mathrm{Trapdoor}}(w)$：攻击者$\mathcal{A}_2$输入关键字$\mathcal{B}$，挑战者$\mathcal{B}$从列表L^{list}中恢复数组$(\mathrm{ID}, w, a_j, \mathrm{SK}, \mathrm{coin})$。若$\mathrm{coin}=1$，挑战者$\mathcal{B}$输出失败。若$\mathrm{coin}=0$，挑战者设置陷门$T_i=[H_1(w)\cdot H_2(a_i)]^b, T_i'=(g^a)^b=g^c$发送给攻击者$\mathcal{A}_2$。

挑战阶段：当询问阶段1完毕，攻击者$\mathcal{A}_2$选择两个关键字(w_0, w_1)和挑战身份ID*发送给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$从列表L^{list}中恢复数组$(\mathrm{ID}*, w*, a_j*, \mathrm{SK}*, \mathrm{coin}*)$。若$\mathrm{coin}*=0$，挑战者$\mathcal{B}$输出失败；否则挑战者$\mathcal{B}$随机选取$\delta\in\{0,1\}$并回应陷门$T_i*=[H_1(w)\cdot H_2(a_i)]^b$, $T_i'*=(g^a)^b=g^c$。

询问阶段2：攻击者$\mathcal{A}_2$进行询问，除挑战密文及其衍生不能询问外，其他同询问阶段1一致。

猜测阶段：最后攻击者$\mathcal{A}_2$返回猜测δ'，如果$\delta'=\delta$，则挑战成功，输出1；否则输出0。

分析：若事件E没有发生，攻击者$\mathcal{A}_2$能攻破方案，则挑战者$\mathcal{B}$能解决DDH困难问题。若$\mathrm{coin}=0$，则密文$T_i'=(g^a)^b=g^c$是一个DDH实例，攻击者$\mathcal{A}_2$的优势为$\varepsilon=\Pr[\delta'=\delta]-1/2$，挑战者$\mathcal{B}$获胜的概率$\Pr[\delta'=\delta|\beta=1]=\Pr[\delta'=\delta]=\varepsilon+1/2$。否则，事件$E$发生，挑战者$\mathcal{B}$获胜的概率$\Pr[\delta'=\delta|\beta=0]=\Pr[\delta'\neq\delta]=1/2$。那么挑战者$\mathcal{B}$能解决DDH困难问题的优势

$$\begin{aligned}\mathrm{Adv}&=\Pr[\delta'=\delta]-1/2=1/2\left(\Pr[\delta'=\delta|\beta=1]\right.\\&\quad\left.+\Pr[\delta'=\delta|\beta=0]\right)-1/2=\varepsilon/2\end{aligned}$$

证毕

6　性能分析

6.1　理论分析比较

本节从理论角度分析本文方案与文献[15,16]在计算效率上的优劣。其中，主要比较的运算有双线性运算T_{P}、指数运算T_{E}、点乘运算T_{M}和哈希运算T_{H}。n_{U}为系统属性值数量、n_{S}为数据用户属性值数量。比较结果如表2所示。

由表2可知，本文方案在系统建立阶段的计算量与文献[15]一样；本文方案在密钥生成阶段、加密阶段以及解密阶段的计算量均小于文献[15]方案；本文方案在陷门生成阶段和测试阶段的计算量大于文献[15]方案。本文方案在系统建立阶段、密钥生成阶段、测试阶段以及解密阶段的计算量均小于文献[16]方案；本文方案在加密阶段和陷门生成阶段的计算量大于文献[16]方案。

6.2　数值实验分析

本节对方案算法进行数值模拟实验。数值模拟实验是在Windows10操作系统下使用C语言的PBC (Pairing-Based Cryptography)库[17]实现的。在PC机(华硕电脑，3.1 GHz CPU, 4 GB RAM)的VC++6.0中运行。通过改变属性的数量分析本文方案的计算效率，属性的数量n分别取1, 4, 8, 12, 16。实验结果是算法运行50次的平均值，如图3所示。

图3(a)、图3(b)、图3(c)分别表示系统建立算法、密钥生成算法和加密算法的运行时间与属性数量的关系。由图3(a)可知，本文方案在系统建立阶段的计算效率高于文献[16]，系统建立算法的运行时间不会随着属性个数的增加而改变。由图3(b)可知，

表 2　效率分析

	文献[15]方案	文献[16]方案	本文方案
Setup	$T_{\mathrm{P}}+3T_{\mathrm{E}}$	$T_{\mathrm{P}}+4T_{\mathrm{E}}+T_{\mathrm{M}}$	$T_{\mathrm{P}}+3T_{\mathrm{E}}$
KeyGen	$4T_{\mathrm{E}}+3T_{\mathrm{M}}$	$(2+n_{\mathrm{S}})T_{\mathrm{E}}+(2+n_{\mathrm{S}})T_{\mathrm{M}}$	$3T_{\mathrm{E}}+2T_{\mathrm{M}}$
Encryption	$2T_{\mathrm{P}}+(3n_{\mathrm{U}}+5)T_{\mathrm{E}}+(2n_{\mathrm{U}}+2)T_{\mathrm{M}}$ $+(2+n_{\mathrm{U}})T_{\mathrm{H}}$	$T_{\mathrm{P}}+(4n_{\mathrm{U}}+6)T_{\mathrm{E}}+(4n_{\mathrm{U}}+8)T_{\mathrm{M}}+T_{\mathrm{H}}$	$2T_{\mathrm{P}}+(2n_{\mathrm{U}}+3)T_{\mathrm{E}}+(n_{\mathrm{U}}+3)T_{\mathrm{M}}$ $+(1+n_{\mathrm{U}})T_{\mathrm{H}}$
Trapdoor	$T_{\mathrm{E}}+T_{\mathrm{H}}$	$(n_{\mathrm{S}}+5)T_{\mathrm{E}}+3T_{\mathrm{M}}+T_{\mathrm{H}}$	$(2n_{\mathrm{S}}+1)T_{\mathrm{E}}+n_{\mathrm{S}}T_{\mathrm{M}}+(1+n_{\mathrm{S}})T_{\mathrm{H}}$
Test	$T_{\mathrm{P}}+T_{\mathrm{E}}+T_{\mathrm{H}}$	$(2n_{\mathrm{S}}+3)T_{\mathrm{P}}+n_{\mathrm{S}}T_{\mathrm{E}}+(2n_{\mathrm{S}}+1)T_{\mathrm{M}}$	$2n_{\mathrm{S}}T_{\mathrm{P}}+(2n_{\mathrm{S}}-2)T_{\mathrm{E}}+(2n_{\mathrm{S}}-1)T_{\mathrm{M}}$
Decryption	$(2+2n_{\mathrm{S}})T_{\mathrm{P}}+2n_{\mathrm{S}}T_{\mathrm{E}}+(2n_{\mathrm{S}}+3)T_{\mathrm{M}}$	$(2n_{\mathrm{S}}+1)T_{\mathrm{P}}+n_{\mathrm{S}}T_{\mathrm{E}}+(2n_{\mathrm{S}}+1)T_{\mathrm{M}}$	$3T_{\mathrm{P}}+2T_{\mathrm{E}}+4T_{\mathrm{M}}$

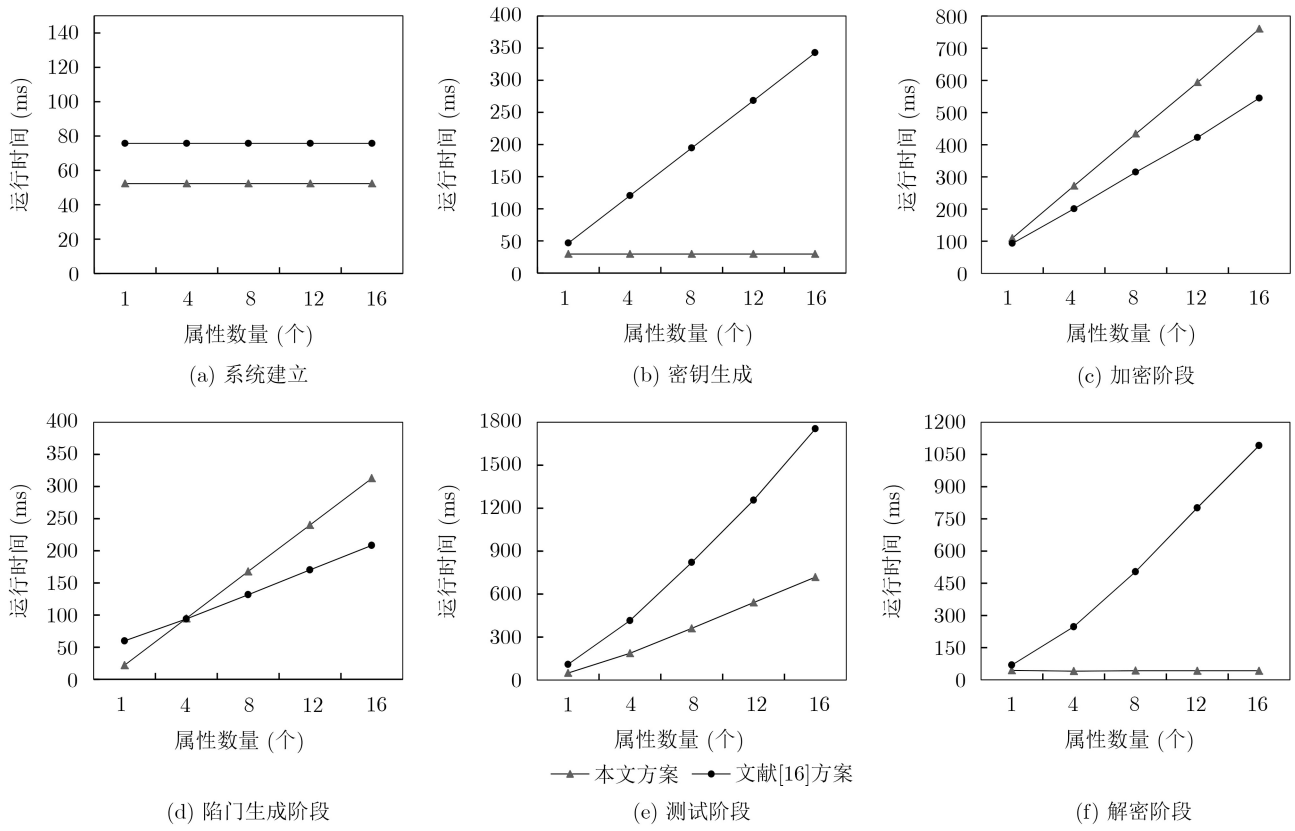

图 3 属性数量与运行时间

本文方案在密钥生成阶段的计算效率高于文献[16]。文献[16]密钥生成算法的运行时间随着属性个数的增加呈线性增长，而本文方案密钥生成算法的运行时间不会随着属性个数的增加而改变。由图3(c)可知，本文方案在加密阶段的计算效率低于文献[16]。

图3(d)、图3(e)、图3(f)分别表示陷门生成算法、测试算法和解密算法的运行时间与属性数量的关系。由图3(d)可知，当属性个数>4时，本文方案在陷门生成阶段的计算效率低于文献[16]。由图3(e)可知，本文方案在测试阶段的计算效率高于文献[16]。本文方案与文献[16]密钥生成算法的运行时间都在随着属性个数的增加呈线性增长，而本文方案在这一阶段运行时间增长较为缓慢。由图3(f)可知，本文方案在解密阶段的计算效率高于文献[16]。文献[16]解密算法的运行时间随着属性个数的增加呈线性增长，而本文方案解密算法的运行时间不会随着属性个数的增加而改变，这在一定程度上减少了数据用户的计算量。

7 结束语

本文提出了一种区块链上基于云辅助的CP-ABE数据共享加密方案，该方案使用基于属性加密技术和可搜索加密技术实现了细粒度访问控制以及关键字密文搜索。搜索过程在区块链上进行，窃听者无法猜出关键字，保证了搜索的安全性。本文所提方案中还是存在一些问题有待解决：如何设计更高效的访问结构；细化区块链上对新区块的验证。在未来的工作中，将对本文方案进行改进，解决这些存在的难题。

参 考 文 献

[1] 牛淑芬, 王金风, 王伯彬, 等. 区块链上基于B+树索引结构的密文排序搜索方案[J]. 电子与信息学报, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.
NIU Shufen, WANG Jinfeng, WANG Bobin, *et al*. Ciphertext sorting search scheme based on B+ tree index structure on blockchain[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.

[2] 黄穗, 陈丽炜, 范冰冰. 基于CP-ABE和区块链的数据安全共享方法[J]. 计算机系统应用, 2019, 28(11): 79–86. doi: 10.15888/j.cnki.csa.007144.
HUANG Sui, CHEN Liwei, and FAN Bingbing. Data security sharing method based on CP-ABE and blockchain[J]. *Computer Systems and Applications*, 2019, 28(11): 79–86. doi: 10.15888/j.cnki.csa.007144.

[3] 牛淑芬, 谢亚亚, 杨平平, 等. 加密邮件系统中基于身份的可搜索加密方案[J]. 电子与信息学报, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.

NIU Shufen, XIE Yaya, YANG Pingping, *et al*. Identity-based searchable encryption scheme for encrypted email system[J]. *Journal of Electronics & Information Technology*, 2020, 42(7): 1803–1810. doi: 10.11999/JEIT190578.

[4] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th annual international conference on Theory and Applications of Cryptographic Techniques, Berlin Germany, 2005. doi: 10.1007/11426639_27.

[5] 张玉磊, 文龙, 王浩浩, 等. 多用户环境下无证书认证可搜索加密方案[J]. 电子与信息学报, 2020, 42(5): 1094–1101. doi: 10.11999/JEIT190437.

ZHANG Yulei, WEN Long, WANG Haohao, *et al*. Certificateless authentication searchable encryption scheme for multi-user[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1094–1101. doi: 10.11999/JEIT190437.

[6] SONG D X, WAGNER D, and PERRIG A. Practical techniques for searches on encrypted data[C]. 2020 IEEE Symposium on Security and Privacy. S&P 2000, Berkeley, USA, 2000. doi: 10.1109/SECPRI.2000.848445.

[7] 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, Interlaken, Switzerland, 2004: 506–522. doi: 10.1007/978-3-540-24676-3_30.

[8] WANG Yong, ZHANG Aiqing, ZHANG Peiyun, *et al*. Cloud-assisted EHR sharing with security and privacy preservation via consortium Blockchain[J]. *IEEE Access*, 2019, 7: 136704–136719. doi: 10.1109/ACCESS.2019.2943153.

[9] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/en/bitcoin-paper, 2016.

[10] ZHENG Zibin, XIE Shaoan, DAI Hongning, *et al*. An overview of Blockchain technology: Architecture, consensus, and future trends[C]. 2017 IEEE International Congress on Big Data, Honolulu, USA, 2017. doi: 10.1109/BigDataCongress.2017.85.

[11] ZHENG Dong, WU Axin, and ZHANG Yinghui. Efficient and privacy-preserving medical data sharing in internet of things with limited computing power[J]. *IEEE Access*, 2018, 6: 28019–28027. doi: 10.1109/ACCESS.2018.2840504.

[12] 张良嵩. 基于拜占庭容错的区块链共识算法研究[D]. [硕士论文], 电子科技大学, 2020.

ZHANG Liangsong. Research of blockchain consensus algorithm based on byzantine fault tolerance[D]. [Master dissertation], University of Electronic Science and Technology of China, 2020.

[13] 刘格昌, 李强. 基于可搜索加密的区块链数据隐私保护机制[J]. 计算机应用, 2019, 39(S2): 140–146.

LIU Gechang and LI Qiang. BlockChain data privacy protection mechanism based on searchable encryption[J]. *Journal of Computer Applications*, 2019, 39(S2): 140–146.

[14] 齐芳, 李艳梅, 汤哲. 可撤销和可追踪的密钥策略属性基加密方案[J]. 通信学报, 2018, 39(11): 63–69. doi: 10.11959/j.issn.1000-436x.2018231.

QI Fang, LI Yanmei, and TANG Zhe. Revocable and traceable key-policy attribute-based encryption scheme[J]. *Journal on Communications*, 2018, 39(11): 63–69. doi: 10.11959/j.issn.1000-436x.2018231.

[15] WANG Shangping, ZHANG Duo, ZHANG Yaling, *et al*. Efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage[J]. *IEEE Access*, 2018, 6: 30444–30457. doi: 10.1109/ACCESS.2018.2846037.

[16] 胡媛媛, 陈燕俐, 朱敏惠. 可实现隐私保护的基于属性密文可搜索方案[J]. 计算机应用研究, 2019, 36(4): 1158–1164. doi: 10.19734/j.issn.1001-3695.2017.12.0760.

HU Yuanyuan, CHEN Yanli, and ZHU Minhui. Privacy protection attribute-based ciphertext search scheme[J]. *Application Research of Computers*, 2019, 36(4): 1158–1164. doi: 10.19734/j.issn.1001-3695.2017.12.0760.

[17] The pairing-based cryptography library[EB/OL]. http://crypto.stanford.edu/pbc/, 2015.

牛淑芬：女，1976年生，博士，副教授，研究方向为云计算和大数据网络的隐私保护.

杨平平：女，1995 年生，硕士生，研究方向为网络与信息安全.

谢亚亚：女，1996 年生，硕士生，研究方向为网络与信息安全.

杜小妮：女，1972 年生，博士，教授，研究方向为信息安全.

责任编辑：马秀强