基于属性加密的区块链数据溯源算法

田有亮[1,2,3]，杨科迪[1,3,4]，王缵[1,2,3]，冯涛[5]

（1. 公共大数据国家重点实验室（贵州大学），贵州 贵阳 550025；2. 贵州大学计算机科学与技术学院，贵州 贵阳 550025；
3. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025；4. 贵州大学数学与统计学院，贵州 贵阳 550025；
5. 兰州理工大学计算机与通信学院，甘肃 兰州 730050）

摘 要：针对目前基于区块链的溯源算法主要通过同态加密及零知识证明进行隐私保护，使溯源信息难于实现动态共享这一问题，提出基于属性加密的区块链数据溯源算法。为实现交易隐私的动态保护，基于 Waters 所提 CP-ABE 方案设计适用于区块链的策略更新算法，完成交易隐私的动态保护。为实现区块内容可见性的动态更新，基于策略更新算法设计区块结构，实现区块内容可见性的动态更新。通过安全性及实验仿真分析表明，所提算法可以在完成保护交易隐私的同时，实现溯源信息动态共享。

关键词：数据溯源；区块链；属性加密；隐私保护；数据共享

中图分类号：TP309.7

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019222

Algorithm of blockchain data provenance based on ABE

TIAN Youliang[1,2,3], YANG Kedi[1,3,4], WANG Zuan[1,2,3], FENG Tao[5]

1. State Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China
4. College of Mathematics and Statistics, Guizhou University, Guiyang 550025, China
5. School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: To solve the problem that the blockchain-based traceability algorithm mainly used homomorphic encryption and zero-knowledge proof for privacy protection, making it difficult to achieve dynamic sharing of traceability information, a blockchain data traceability algorithm based on attribute encryption was proposed. In order to realize the dynamic protection of transaction privacy, the strategy update algorithm applicable to block chain was designed based on the CP-ABE scheme proposed by Waters to achieve dynamic protection of transaction privacy. In order to realize the dynamic update of the visibility about block content, based on the strategy update algorithm, the block structure was designed to achieve the dynamic update about the content visibility of the block. The security and experimental simulation analysis show that the proposed algorithm can realize the dynamic sharing of traceability information while completing the protection transaction privacy.

Key words: data provenance, blockchain, attribute-based encryption, privacy protection, data sharing

---

收稿日期：2019–07–18；**修回日期**：2019–09–26

基金项目：教育部—中国移动科研基金资助项目（No.MCM20170401）；国家自然科学基金资助项目（No.61772008, No.U1836205）；贵州省科技重大专项计划基金资助项目（No.20183001）；贵州省科技计划基金资助项目（黔科合基础 No.[2019]1098, 黔科合平台人才 No.[2017]5788）

Foundation Items: Ministry of Education-China Mobile Research Fund Project (No.MCM20170401), The National Natural Science Foundation of China (No.61772008, No.U1836205), Science and Technology Major Support Program of Guizhou Province (No.20183001), Guizhou Provincial Science and Technology Plan Project (No.[2019]1098, No.[2017]5788)

1 引言

数据是继物质、能源之后的第三大基础性战略资源，各行各业的发展越来越离不开数据。数据开放、共享和交易是解决“数据孤岛”的重要手段，但随着大数据的开放与共享，数据盗卖转售及隐私泄露等问题尤为突出，给数据安全和隐私安全带来前所未有的挑战。

数据溯源是对原始数据及其演变过程的追溯、重现与展示。通过数据溯源，用户可以了解数据生命周期变化过程，回溯数据相关来源。区块链技术具有去中心化和去信任化等特点，能够在陌生节点之间建立点对点的可信账本，形成具有唯一性和不可篡改的区块，非常适合应用于溯源，但区块链的公开透明性严重威胁着用户隐私。针对这一问题，Ramachandran 等[1]及 Tosh 等[2]分别在区块链数据溯源框架中，通过散列函数对用户 ID 进行处理实现隐私保护。Wu 等[3]引入数据脱敏技术，提出一种基于区块链的电子病历安全共享模型，该模型在不破坏数据统计特性的前提下，以牺牲某些数据的准确性为代价解决交易隐私泄露问题。Wang 等[4]利用智能合约和同态加密技术对用户进行隐私保护，但该方案中交易信息的可见性仅限于交易双方，并不利于数据高效共享。Lei 等[5]以零知识证明方法对交易隐私进行保护，但在频繁交易和扩展性要求较高的场景下，交易信息共享性难于满足需要。Zhang 等[6]通过群签名技术对群用户进行隐私保护，但流转信息的公开性仅限于事先设定的群内成员，无法实现溯源信息共享性的动态更新。Bhuiyan 等[7]根据场景不同设置智能合约限制用户访问权限，并根据特定条件授予和撤销访问权以确保数据动态共享，然而细粒度的交易隐私保护却难于实现。Neisse 等[8]基于智能合约设计 3 种具有不同粒度的可扩展性访问控制模型，实现数据细粒度访问控制和流转信息有效跟踪。从以上方案可知，目前基于区块链的数据溯源方案主要采用数据脱敏、数字签名、零知识证明、同态加密等加密技术并结合智能合约实现隐私保护，使溯源信息共享性局限于事先设定的交易群体，无法实现高效扩展，难以满足实际溯源需要。

属性基加密（ABE, attribute-based encryption）作为一种新兴的加密技术，将用户身份与一系列属性绑定，通过对用户私钥或密文设置属性集与访问结构，只有属性集与访问结构相匹配时才能解密，从而实现一对多的加密通信以及对文件的细粒度访问控制，因此更适用于具有数据共享和隐私保护的加密处理。属性加密思想最早由 Sahai 等[9]于 2005 年提出，根据密文、密钥表现形式以及访问策略绑定位置不同，属性加密可分为基于密钥策略的属性加密（KP-ABE, key-policy attribute-based encryption）[10]和基于密文策略的属性加密（CP-ABE, ciphertext-policy attribute-based encryption）。在 CP-ABE 中，密文和访问策略相关联，用户密钥和属性集合相对应。因此，CP-ABE 方案更适合应用于溯源场景。2007 年，Bethencourt 等[11]给出了第一个基于密文策略的属性加密构造。2011 年，Waters[12]首次在标准模型下证明了 CP-ABE 的安全性，并于 2012 年提出支持动态证书和密文授权的 ABE 方案[13]，该方案首次提出策略更新的思想，但其新策略比原策略更严格。此后，Yang 等[14]通过策略动态更新对云环境中的数据进行访问控制，Liu 等[15]提出一种智能电网多权限访问控制的高效属性撤销方案，Huang 等[16]提出一种多权限可撤销的 ABE 方案。上述具有策略更新的 ABE 方案[14-16]主要将密文存储于云环境或大数据平台中，通过修改密文实现访问策略的动态更新。但区块数据具有不可更改、不可删除等特性，无法通过修改区块内容实现策略更新。因此设计一种访问策略可更新的区块链溯源算法，是实现溯源信息安全动态共享的重要手段之一。

鉴于上述分析，本文提出一种基于属性加密的区块链数据溯源算法。通过改进的属性加密算法完成交易隐私保护，利用设计的策略可更新溯源链实现溯源信息动态共享。本文的主要贡献如下。

1) 形成适用于区块链的访问策略可更新属性加密算法。改进 Waters 所提 CP-ABE 方案[12]，设计访问策略更新算法，并确保攻击者无法通过策略更新对交易内容发起攻击。

2) 实现区块内容可见性动态更新。通过改进的属性加密算法生成交易区块和访问策略区块，基于访问策略更新算法追加策略区块，实现区块内容可见性的动态调整。

3) 确保交易隐私不发生泄露的同时，实现溯源信息动态共享。利用属性加密算法完成交易隐私保护，通过适用于区块链的策略更新算法实现溯源信息动态共享。

2　准备知识

2.1　参数定义

本文中改进的属性算法及策略可更新溯源算法所涉及的主要参数如表 1 所示。

表 1　　主要参数

参数	含义
k	属性加密算法的系统安全参数
U	系统属性集
PK	系统主公钥
MSK	系统主私钥
S	用户属性集
SK	用户属性私钥
$\boldsymbol{M}_i$	$l\times n$ 型访问矩阵 $\boldsymbol{M}$ 的第 i 行
$\rho(i)$	函数 ρ 将矩阵 $\boldsymbol{M}$ 的第 i 行映射到属性
s	秘密共享密钥
λ	秘密共享份额
$\boldsymbol{v}$	加密算法所选择随机向量
m	待加密的明文
δ	策略更新者身份标识
CT	密文结构 $\mathrm{CT}=\{C,\ C_\delta,\ (C_i,\ D_i)_{i\in[1,l]}\}$
C	含明文部分
C_δ	含共享密钥部分
$(C_i,\ D_i)$	含访问控制策略部分
En(s)	保留加密信息
GID	溯源参与者的身份唯一标识
R	数据资源
P	版权区块
tx	交易信息
TX	交易区块
A	策略区块

2.2　单调张成方案

改进的 CP-ABE 算法采用单调张成方案[17]完成访问结构向访问矩阵的转化。转换过程中，对于系统属性 a,b,c,d 及其访问结构 $F=(a\cap(b\cup(c\cap d)))$，方案首先将“∩”格式化为“2”、将“∪”格式化为“1”，然后将属性元素自左向右依次展开。故 $(a\cap b)$ 格式化为 $(a,b,2)$，表示在属性 a,b 中需满足 2 个；$(c\cup d)$ 格式化为 $(c,d,1)$，表示在属性 c,d 中需满足一个。则 F 格式化为 $L=(a,(b,(c,d,2),1),2)$，访问结构 L 转换为访问矩阵 $\boldsymbol{M}$ 的详细过程如表 2 所示。若 F 更新为 $F'=(a\cap(b\cup(c\cap d\cap e)))$，则 L 更新为 $L'=(a,(b,(c,d,e,3),1),2)$，更新后访问矩阵 $\boldsymbol{M'}$ 的转换过程如表 3 所示。

表 2　　原访问结构与访问矩阵转换

访问结构（L）	访问矩阵（$\boldsymbol{M}$）
$(a,(b,(c,d,2),1),2)$	(1)
$\begin{pmatrix} a \\ (b,(c,d,2),1) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ (c,d,2) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ (c,d,2) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix}$

表 3　　新访问结构与访问矩阵转换

访问结构(L')	访问矩阵（$\boldsymbol{M'}$）
$(a,(b,(c,d,e,3),1),2)$	(1)
$\begin{pmatrix} a \\ (b,(c,d,e,3),1) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ (c,d,e,3) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ (c,d,e,3) \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 1 & 2 & 2 & 4 \\ 1 & 2 & 3 & 9 \end{pmatrix}$

根据线性秘密共享方案[18]可知，对于满足访问结构 F 的授权集 $S=\{a,c,d\}$ 在访问策略 $(\boldsymbol{M},\rho)$ 中可以找到一组向量 $\{\boldsymbol{w}_i\}_{\rho(i)\in S}=\{2,-2,1\}$，使 $\sum_{\rho(i)\in S}\boldsymbol{w}_i\boldsymbol{M}_i=(1,0,0)$。同理，对于更新后的访问结构 F'，满足该结构的授权集 $S'=\{a,c,d,e\}$，在访问策略 (M',ρ') 中可以找到向量 $\{\boldsymbol{w}_i'\}_{\rho(i)\in S'}=\{2,-3,3,-1\}$，使 $\sum_{\rho(i)\in S'}\boldsymbol{w}_i'\boldsymbol{M}_i=(1,0,0,0)$。

3　改进的属性加密算法

本文算法对 Waters 所提的 CP-ABE 进行改进，

改进后的算法总体流程如图 1 所示，其中虚线框为修改或新增部分。

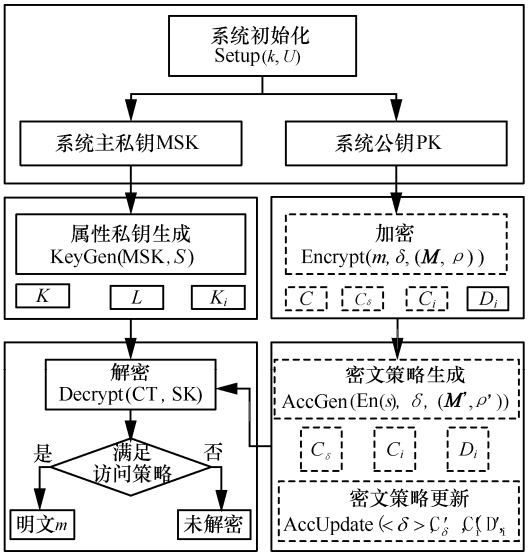

图 1 改进的 CP-ABE 属性加密流程

3.1 算法描述

改进的 CP-ABE 算法主要由系统初始化、属性私钥生成、加密、解密、密文策略生成及密文策略更新 6 个部分组成，具体如下。

1) $\text{Setup}(k,U)\rightarrow(\text{PK},\text{MSK})$。系统初始化算法通过输入安全参数 k 和系统属性集 U，输出系统公私钥对 (PK,MSK)。

设 G_1 为 q 阶循环群，g 为 G_1 的生成元，双线性映射 $e:G_1\times G_1\rightarrow G_2$。随机选择 $\alpha,\beta\in Z_p$ 及群 G_1 的元素 $h_1,h_2,\cdots,h_u$，其中 $\{1,2,\cdots,u\}$ 表示属性集 U 中对应的属性标号，输出系统密钥对 (PK,MSK) 为

$$\text{PK}=\{g,\ e(g,g)^{\alpha},g^{\beta},\ h_1,\ h_2,\cdots,\ h_u\}$$

$$\text{MSK}=g^{\alpha}$$

2) $\text{KeyGen}(\text{MSK},S)\rightarrow\text{SK}$。属性私钥生成算法通过输入系统私钥 MSK 和用户属性集合 S，输出用户的属性私钥 SK。

密钥中心输入系统私钥 $\text{MSK}=g^{\alpha}$ 和用户属性集 $S=\{x_1,x_2,\cdots,x_n\}$，选择随机参数 $t\in Z_p$，输出用户的属性私钥 SK 为

$$\text{SK}=\{K=g^{\alpha}g^{\beta t},L=g^{t},K_x=h_x^{t},\forall x\in S\}$$

3) $\text{Encrypt}(m,\delta,(\boldsymbol{M},\rho))\rightarrow\text{CT}$。加密算法通过输入明文 m、策略更新者身份标识 δ 及访问控制策略 $(\boldsymbol{M},\rho)$，输出密文 CT。

加密过程中，$\boldsymbol{M}$ 是 $l\times n$ 的访问矩阵，$\boldsymbol{M}_i$ 表示矩阵中的第 i 行，$i\in[1,2,\cdots,l]$。函数 ρ 将 $\boldsymbol{M}_i$ 映射到属性，记为 $\rho:\{1,2,\cdots,l\}\rightarrow\{1,2,\cdots,u\}$。加密算法选择随机向量 $\boldsymbol{v}=(s,t_2,\cdots,t_n)\in Z_p^n$ 生成密文信息 (C,C_{δ})，s 为秘密共享密钥，$t_2,\cdots,t_n$ 为随机值，以 $\lambda_i=\boldsymbol{v}\boldsymbol{M}_i$ 表示秘密共享密钥份额，随机选取 $r_1,r_2,\cdots,r_l\in Z_p$ 在密文中添加附加信息 $(C_i,D_i)_{i\in[1,l]}$，以此作为访问控制策略。最终创建密文 CT 为

$$\text{CT}=\Big\{C=\text{me}(g,g)^{\alpha s\delta},\ C_{\delta}=g^{s\delta},$$

$$(C_i=g^{\beta\lambda_i\delta}h_{\rho(i)}^{-r_i},\ D_i=g^{r_i})_{i\in[1,l]}\Big\}$$

为实现访问控制策略动态更新，加密完成后，属性加密算法根据安全加密算法（如 SM9）对 s 进行加密，以此作为保留加密信息 $\text{En}(s)$。

4) $\text{Decrypt}(\text{CT},\text{SK})\rightarrow m$。解密算法输入关于访问策略 $(\boldsymbol{M},\rho)$ 的密文 CT，以及关于用户属性集 S 的私钥 SK。如果解密者的属性集 S 满足访问策略 $(\boldsymbol{M},\rho)$，则输出明文 m，否则解密失败。

设索引集为 $I=\{i:\rho(i)\in S\}$，目标向量为 $(1,0,\cdots,0)$。根据单调张成方案知，如果用户属性满足访问矩阵 $(\boldsymbol{M}_i)_{i\in I}$，则能够找到一组向量 $\{\boldsymbol{w}_i\}_{i\in I}$ 使得 $\sum_{i\in I}\boldsymbol{w}_i\boldsymbol{M}_i=(1,0,\cdots,0)$。根据线性秘密共享方案知 $\sum_{i\in I}\boldsymbol{w}_i\lambda_i=\sum_{i\in I}\boldsymbol{w}_i\boldsymbol{v}\boldsymbol{M}_i=\boldsymbol{v}\sum_{i\in I}w_i\boldsymbol{M}_i=s$。则解密计算式为

$$\frac{e(C_{\delta},K)}{\prod_{i\in I}(e(C_i,L)e(D_i,K_{\rho(i)}))^{w_i}}=$$

$$\frac{e(g,g)^{\alpha s\delta}\,e(g,g)^{s\delta\beta t}}{\prod_{i\in I}e(g,g)^{\delta\beta t\lambda_i w_i}}=e(g,g)^{\alpha s\delta}$$

最终得到密文信息 $m=\dfrac{C}{e(g,g)^{\alpha s\delta}}$。

5) $\text{AccGen}(\text{En}(s),\delta,(\boldsymbol{M}',\rho'))\rightarrow\{C_{\delta}',(C_i',D_i')\}$。密文策略生成算法输入更新者身份 δ、保留加密信息 $\text{En}(s)$ 及新访问策略 $(\boldsymbol{M}',\rho')$，输出新的策略密文 $\{C_{\delta}',(C_i',D_i')_{i\in[1,l']}\}$。

密文策略生成算法通过更新者身份 δ 对 $\text{En}(s)$ 解密获取 s' 作为第一个输入值，根据新访问策略 $(\boldsymbol{M}',\rho')$ 选择随机向量 $\boldsymbol{v}'=(s',t_2',\cdots,t_{n'}')\in Z_p^{n'}$ 计算 $\lambda_i'=\boldsymbol{v}'\boldsymbol{M}_i'$，其中 $\boldsymbol{M}'$ 是一个 $l'\times n'$ 矩阵，s' 仍为秘密共享密钥，$t_2',\cdots,t_{n'}'$ 为随机值。然后，随机选取 $r_1',r_2',\cdots,r_{l'}'\in Z_p$，对 $i\in[1,2,\cdots,l']$ 计算更新后的策略密文信息为

$$C'_{\delta}=g^{s'\delta},\ C'_i=g^{\beta\lambda'_i\delta}h_{\rho'(i)}^{-r'_i},\ D'_i=g^{r'_i}$$

6) $\text{AccUpdate}(<\delta>,C'_{\delta},(C'_i,D'_i)_{i\in[1,l']})\rightarrow \text{CT}'$。

密文策略更新算法输入更新者身份签名消息$<\delta>$及策略密文信息$\{C'_{\delta},(C'_i,D'_i)_{i\in[1,l']}\}$，进行访问策略更新。算法首先验证签名消息$<\delta>$，然后判断等式$C_{\delta}=C'_{\delta}$是否成立。通过上述验证后输出更新后的密文$\text{CT}'=\{C,C_{\delta},(C'_i,D'_i)_{i\in[1,l']}\}$。

3.2　安全模型

改进的CP-ABE方案安全模型是选择属性和选择明文攻击下的不可区分性（IND-SAS-CPA, indistinguish ability against selective access structure and chosen plaintext attack）游戏，游戏中包含一个挑战者和一个敌手，挑战者模拟系统运行并回答敌手的询问。具体游戏如下。

1) 系统建立。挑战者运行系统初始化算法$\text{Setup}(k,U)$，将生成的系统公共参数PK发给敌手，敌手宣布要挑战的旧访问策略$(\boldsymbol{M},\rho)$和新访问策略$(\boldsymbol{M}^*,\rho^*)$。

2) 私钥询问。敌手向挑战者发送多个属性集合$S_1,S_2,\cdots,S_n$，且这些属性集合不能满足访问策略$(\boldsymbol{M},\rho)$和$(\boldsymbol{M}^*,\rho^*)$，挑战者运行私钥生成算法$\text{KeyGen}(\text{MSK},S)$生成相应属性私钥并发给敌手。

3) 挑战明文。①敌手发送2个等长的消息m_0、m_1给挑战者，挑战者随机选取$c\in\{0,1\}$使用旧访问策略$(\boldsymbol{M},\rho)$对m_c加密；②挑战者根据$(\boldsymbol{M}^*,\rho^*)$对访问策略进行更新，生成相应的更新密文$\text{CT}^*$；③挑战者将更新密文$\text{CT}^*$发送给敌手。

4) 重复步骤2)，敌手再度向挑战者发送属性集合$S_{n+1},S_{n+2},\cdots,S_{n+m}$申请相应私钥，但规定以上属性集合不能满足访问结构$(\boldsymbol{M}^*,\rho^*)$。

5) 猜测阶段。敌手输出对c的猜想$c'\in\{0,1\}$。

定义 1　若多项式时间敌手赢得以上安全模型游戏的优势$\varepsilon=\left|\Pr[c=c']-\frac{1}{2}\right|$是可忽略的，则改进的CP-ABE方案是安全的（CPA）。

4　访问策略可更新的溯源链

区块链是以区块结构存储数据，同时使用密码技术保证安全传输和多方访问的分布式数据存储技术体系。区块链因其去中心化、防篡改、高透明和可追溯等特性，成为各专家学者研究的热点。但区块链的公开透明性严重威胁着交易隐私，并且写到链上的数据不可更改，更不可销毁，使管理者难以对链上的非法数据进行有效管理。

针对上述问题，本文溯源算法基于访问策略更新算法对区块结构进行设计，实现区块内容可见性的动态更新。如图2所示，大数据平台中每一个数据资源块R_i在区块链中都有唯一版权区块P_i与之对应。数据交易过程中，大数据平台对上链前的每一笔交易信息tx进行属性加密处理，形成交易密文结构$\text{CT}=\{C,C_{\delta},(C_i,D_i)_{i\in[1,2,\cdots,l]}\}$，共识节点通过如下过程完成交易的上链、查询及策略更新。

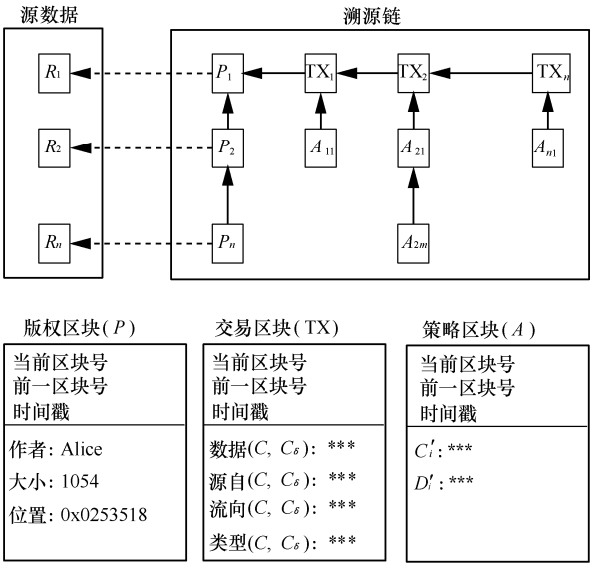

图 2　溯源链及区块结构

写入交易过程中，共识节点首先以(C,C_{δ})生成交易区块TX，以$(C_i,D_i)_{i\in[1,2,\cdots,l]}$生成访问控制策略区块$A$，得到新交易策略区块组$\{\text{TX},A\}$；然后根据$R_i$找到其$P_i$交易链的最后一个交易策略区块组$\{\text{TX}_j,A_j\}$，将$\{\text{TX},A\}$追加到链上形成新的交易记录$\{\text{TX}_{j+1},A_{j+1}\}$。

溯源信息查询过程中，共识节点从TX中获取交易信息(C,C_{δ})，从TX对应的最后一个策略区块A中，获取相应访问控制策略$(C_i,D_i)_{i\in[1,2,\cdots,l]}$。将$\{\text{TX},A\}$构成的交易记录完整密文$\text{CT}=\{C,C_{\delta},(C_i,D_i)_{i\in[1,2,\cdots,l]}\}$返回给溯源用户，用户通过属性私钥SK解密CT得到交易信息m。

为更新链上某笔交易的访问控制策略，首先共识节点对签名消息$<\delta>$进行验证，以此确定更新者身份是否真实；然后通过判断等式$C_{\delta}=C'_{\delta}$是否

成立，以此判别更新者是否有交易 TX 的更新权限且更新前后所使用的共享密钥 s 是否一致；最后将 $(C_i', D_i')_{i\in[1,2,\cdots,l']}$ 生成的新策略区块 A' 追加到 TX 的最后一个访问策略区块之后，得到含新访问策略的交易策略区块组 $\{\mathrm{TX}, A'\}$，以此完成策略更新。

5 数据流转溯源算法

本节将讲述如何通过改进的属性加密算法及策略可更新的溯源链，实现流转信息的隐私保护及溯源信息的动态共享。

5.1 系统模型

为实现大数据平台中的数据高效溯源，平台将数据供应商发布的数据资源分割为数据块，以此作为流转溯源的基本单位。数据的上传、交易、共享、修改及其他流转操作都视为一笔交易写到区块链中，形成溯源信息。溯源用户可通过持有的属性密钥访问链上的授权信息，完成权限范围内的数据追踪溯源，以此实现交易隐私保护。溯源管理者过身份信息及保留加密信息对交易的访问策略进行更新，完成交易信息的细粒度访问控制，从而实现溯源信息动态共享。本模型主体单元如图 3 所示。

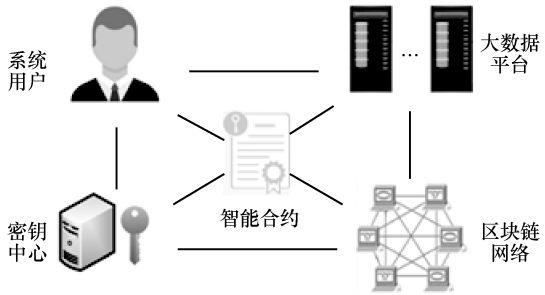

图 3 溯源系统主体单元

1) 系统用户。可以是溯源管理者、数据供应商或消费者，也可以是大数据平台的其他参与人，每个系统用户都有一个身份唯一标识符 GID。

2) 大数据平台。提供大数据存储及交易服务，并将版权信息及历史交易记录存入区块链中。

3) 区块链网络。由各验证节点组成，负责存储版权信息及数据交易记录，各交易信息上链都需经过属性加密处理。

4) 密钥中心。通过用户身份信息生成 GID，根据用户属性生成属性私钥 SK，并对 GID 及 SK 进行管理。

5) 智能合约。为上述主体提供交互接口。

5.2 算法构造

本节利用第 3 节改进的属性加密算法和第 4 节设计的溯源链，完成数据流转信息上链、查询及访问策略动态更新，算法具体步骤如下。

1) 系统初始化。密钥中心首先通过安全散列算法对用户身份信息进行散列处理，生成身份唯一标识符 GID；然后选取安全参数 k 和系统属性集 U，通过 3.1 节的算法 $\mathrm{Setup}(k,U)$ 生成系统主密钥对 $(\mathrm{PK},\mathrm{MSK}) \leftarrow \mathrm{Setup}(k,U)$。

2) 用户属性私钥生成。为产生用户的属性私钥，密钥中心首先将用户发来的 GID 提交给大数据平台审核，以获取用户属性集 S；然后利用 3.1 节的密钥生成算法输入主私钥 MSK 生成用户属性私钥 $\mathrm{SK} \leftarrow \mathrm{KeyGen}(\mathrm{MSK}, S)$；最后将 SK 返回给用户。

3) 上传版权数据。数据供应商将数据资源 Resource 上传至大数据平台，平台首先对数据进行分割，形成数据块 $\{R_1, R_2, \cdots, R_n\}$ 及其版权信息；然后将生成的版权信息记录到区块链中，得到对应的版权区块 $\{P_1, P_2, \cdots, P_n\}$。由于版权信息公开可查阅，故不作属性加密处理。

4) 存入交易信息。若数据供应商 GID_p 想将数据块 R_i 共享给某一数据使用者 GID_u 或某一数据消费者 GID_u 欲购买该数据块 R_i，则大数据平台对上述操作生成一笔交易 $\mathrm{tx} = \{R_i, \mathrm{From}, \mathrm{To}, \mathrm{Time}\}$，形成交易明文信息 $m = \{\mathrm{tx}.R_i, \mathrm{tx.From}, \mathrm{tx.To}, \mathrm{tx.Time}\}$。

加密交易明文 m 时，平台输入溯源管理者提供的身份标识 δ 及访问控制策略 (M,ρ)，利用 3.1 节的属性加密算法 $\mathrm{Encrypt}(m,\delta,(M,\rho))$ 对 m 进行加密，得到交易密文信息 $\mathrm{CT} = \{C, C_\delta, (C_i, D_i)_{i\in p[1,2,\cdots,l]}\}$。同时，属性加密算法还将通过安全加密算法 SM9，对加密过程中产生的共享密钥 s 进行加密，形成保留加密信息 $\mathrm{En}(s)$，为策略更新提供条件。

交易密文 CT 上链过程中，共识节点首先基于第 4 节的策略可更新溯源链，生成交易区块 TX 及其访问控制策略区块 A；然后将 $\{\mathrm{TX}, A\}$ 追加到链上形成 R_i 的一条溯源信息。

5) 读取溯源信息。若溯源用户欲获取数据资源 R_i 的所有流转信息 $\{\mathrm{tx}_i\}_{i\in[1,2,\cdots,n]}$，共识节点从 R_i 对应的交易链 P_i 中提取 tx_i 对应的交易策略区块组 $\{\mathrm{TX}, A\}$，以此构建一条完整交易密文结构 $\mathrm{CT} = \{C, C_\delta, (C_i, D_i)_{i\in[1,2,\cdots,l]}\}$ 返回给用户。如果用户属性集 S 满足密文策略 $\{C_\delta, (C_i, D_i)_{i\in[1,2,\cdots,l]}\}$，则解密得到交

易信息 $\mathrm{tx}=m$，否则解密失败。通过上述方式提取 P_i 链的所有交易区块组 $\{\mathrm{TX}_i, A_i\}_{i\in[1,2,\cdots,n]}$，从中获取交易密文结构 $\mathrm{CT}_{i\in[1,2,\cdots,n]}$ 并解密，得到所有交易信息 $\{\mathrm{tx}_i\}_{i\in[1,2,\cdots,n]}$ 形成完整溯源信息。

6) 更新访问策略。策略更新过程分为策略密文生成和策略区块上链两步。其中，策略密文生成由更新者执行，策略区块上链由共识节点执行。

①更新者输入身份信息 δ、保留加密信息 $\mathrm{En}(s)$ 及新访问策略 $(\boldsymbol{M}', \rho')$，通过 3.1 节的策略密文生成算法 $\mathrm{AccGen}(\mathrm{En}(s), \delta, (\boldsymbol{M}', \rho'))$ 生成新的策略密文 $\{C'_\delta, (C'_i, D'_i)_{i\in[1,2,\cdots,l']}\}$；然后将身份签名消息 $<\delta>$ 及 $\{C'_\delta, (C'_i, D'_i)_{i\in[1,2,\cdots,l']}\}$ 发送给共识节点。

②共识节点基于第 4 节的策略验证过程对 $<\delta>$ 及 C'_δ 进行审核。通过后以 $(C'_i, D'_i)_{i\in[1,2,\cdots,l']}$ 生成新策略区块 A' 并追加到 TX 对应的策略区块后，形成新交易策略区块组 $\{\mathrm{TX}, A'\}$。

6　方案分析

6.1　安全性分析

定理 1　若判定性 $q-$PBDHE 假设[12]成立，则不存在多项式时间敌手能够选择挑战访问结构 $(\boldsymbol{M}^{\#}, \rho^{\#})$ 攻破改进的 CP-ABE 方案。

证明　若存在一个多项式时间敌手 $\mathcal{A}$ 选择一个挑战访问结构 $(\boldsymbol{M}^{\#}, \rho^{\#})$，以不可忽略的优势 ε 赢得游戏，则存在一个模拟器以不可忽略的优势 ε 解决判定性 $q-$PBDHE 假设。

1) 系统建立。模拟器加载 $q-$PBDHE 参数 $\mathcal{Y}$、$\mathcal{T}$，敌手提交要挑战的旧访问策略 $(\boldsymbol{M}^*, \rho^*)$ 和新访问策略 $(\boldsymbol{M}^{\#}, \rho^{\#})$。其中，$\boldsymbol{M}^*$ 是 $l^*\times n^*$ 的矩阵，$\boldsymbol{M}^{\#}$ 是 $l^{\#}\times n^{\#}$ 的矩阵，且 $l^*, n^*, l^{\#}, n^{\#}\leqslant q$。模拟器随机选择 $\alpha=\alpha'+\beta^{q+1}$，$\alpha'\in Z_p$，使系统公钥 $e(g,g)^{\alpha}=e(g,g)^{\alpha'+\beta^{q+1}}=e(g^{\beta}, g)^{\beta^q}e(g,g)^{\alpha'}$。对系统属性集合 U 中的每一个元素 $x\in U$，令索引集 $X=\{i:\rho^*(i)=x\}$ 选择一个随机的参数 $z_x\in Z_p$，并执行以下运算。若 $x\in U$，则 $h_x=g^{z_x}\prod_{i\in X}\left(g^{\frac{\beta \boldsymbol{M}^*_{i,1}}{b_i}}\cdot g^{\frac{\beta^2 \boldsymbol{M}^*_{i,2}}{b_i}}\cdots g^{\frac{\beta^n \boldsymbol{M}^*_{i,n}}{b_i}}\right)$，否则 $h_x=g^{z_x}$。

2) 私钥询问。敌手通过提交不满足访问策略 $(\boldsymbol{M}^*, \rho^*)$ 和 $(\boldsymbol{M}^{\#}, \rho^{\#})$ 的属性集 S 询问私钥，挑战者运行私钥生成算法 $\mathrm{KeyGen}(\mathrm{MSK}, S)$ 生成相应属性私钥 $\mathrm{SK}=\{L, K, K_x\}$ 发给敌手。私钥构造过程如下。

根据线性重构特性知，可以找到一组向量 $\boldsymbol{w}=(w_1, w_2, \cdots, w_{n^*})\in Z_p^{n^*}$，$w_1=-1$，使 $\boldsymbol{w}\boldsymbol{M}^*_i=0$，其中，$i:\rho^*(i)\in S$。设置参数 $t=k+w_1\beta^q+w_2\beta^{q-1}+\cdots+w_{n^*}\beta^{q-n^*+1}$，$k\in Z_p$，则 $L=g^t=g^k\prod_{i=1,\cdots,n^*}\left(g^{\beta^{q+1-i}}\right)^{w_i}$。

计算 K 值时包含参数 $g^{\beta^{q+1}}$，该参数不能通过判定性 $q-$PBDHE 提供的参数计算出来，其可以利用步骤 1)中等式 $\alpha=\alpha'+\beta^{q+1}$ 经过指数运算来消除。

$$K=g^{\alpha}g^{\beta t}=g^{\alpha'+\beta^{q+1}}g^{\beta t}=g^{\alpha'}L^{\sigma}=g^{\alpha'}g^{\beta k}\prod_{i=2,\cdots,n^*}\left(g^{\beta^{q+2-i}}\right)^{w_i}$$

计算 K_x 时包含参数 $g^{\beta^{q+1}}$，根据线性重构特性，当用户属性集 S 不满足访问结构时，有 $\boldsymbol{w}\boldsymbol{M}^*_i=0$。根据这一特性可以消除 K_x 中包含的参数 $g^{\frac{\beta^{q+1}}{b_i}}$，令 X 为 i 的索引集且 $\rho^*(i)=x$。用户提交的属性集 S 分为两部分，属于系统属性 U 的元素集合命名为 S_1，记作 $S_1=\{x:\rho(i)\in S\bigcap U\}$；不属于系统属性 U 的元素命名为 S_2，记作 $S_2=\{x:\rho(i)\in S\text{且}\rho(i)\notin U\}$。$K_x$ 计算的具体方法为

$$K_x=h_x^t=L^{z_x}\prod_{i\in X}\prod_{j=1,\cdots,n}\left(g^{\frac{\beta^j}{b_i}k}\prod_{\substack{m=1,\cdots,n^*\\ m\neq j}}\left(g^{\beta^{q+1+j-m}}\right)^{w_m}\right)^{\boldsymbol{M}^*_{ij}},\ x\in S_1$$

$$K_x=h_x^t=g^{z_x t}=L^{z_x},\ x\in S_2$$

3) 挑战明文。敌手发送 2 个等长的消息 m_0、m_1 给挑战者，挑战者随机选取 $c\in\{0,1\}$ 使用旧的访问结构 $(\boldsymbol{M}^*, \rho^*)$ 对 m_c 进行加密。

①挑战者计算 $C=m_c\mathcal{T}e(g,g)^{\alpha s\delta}$ 和 $C_\delta=g^{s\delta}$，随机选择 $y'_2, y'_3, \cdots, y'_{n^*}$，通过 $\boldsymbol{v}=(s, s\beta+y^*_2, s\beta^2+y^*_3, \cdots, s\beta^{n-1}+y^*_{n^*})\in Z_p^{n^*}$ 共享密钥，随机选择 $r_1, \cdots, r_{l^*}\in Z_p$ 对 $i=1,\cdots,n^*$ 定义 H_i 为 $m\neq i$ 时 $\rho^*(i)=\rho^*(m)$ 的集合，则密文元素为

$$C_i=h^{r'_i}_{\rho^*(i)}\left(\prod_{j=2,\cdots,n^*}\left(g^{\delta\beta}\right)^{\boldsymbol{M}^*_{i,j}y'_j}\right)\left(g^{b_i s}\right)^{-z_{\rho^*(i)}}\cdot\left(\prod_{m\in H_i}\prod_{j=1,\cdots,n^*}\left(g^{\beta^j s\frac{b_i}{b_m}}\right)^{\boldsymbol{M}^*_{m,j}}\right)$$

$$D_i=g^{-r'_i}g^{-sb_i}$$

② 挑战者根据敌手提供的新问策略 $(\boldsymbol{M}^{\#},\rho^{\#})$ 及保留加密共享密钥 s' 对 (C_i,D_i) 进行更新计算。随机选择 $\boldsymbol{v}=(s',s'\beta+y_2^{'},s'\beta^2+y_3^{'},\cdots,s'\beta^{n-1}+y_{n^{\#}}^{'})\in Z_p^{n^{\#}}$，随机选择 $r_1,\cdots,r_{l^{\#}}\in Z_p$ 对 $i=1,\cdots,n^{\#}$ 定义 H_i 为 $m\neq i$ 时 $\rho^{\#}(i)=\rho^{\#}(m)$ 的集合，则新策略元素为

$$C_i^{\#}=h_{\rho^{\#}(i)}^{r_i^{'}}\left(\prod_{j=2,\cdots,n^{\#}}\left(g^{\delta\beta}\right)^{\boldsymbol{M}_{i,j}^{\#}y_j^{'}}\right)\left(g^{b_i s}\right)^{-z_{\rho^{\#}(i)}}\cdot$$

$$\left(\prod_{m\in H_i}\prod_{j=1,\cdots,n^{\#}}\left(g^{\beta^j s\frac{b_i}{b_m}}\right)^{\boldsymbol{M}_{m,j}^{\#}}\right)$$

$$D_i^{\#}=g^{-r_i^{'}}g^{-sb_i}$$

③ 挑战者将密文 $\mathrm{CT}=\{C,C_\delta,(C_i^{\#},D_i^{\#})_{i\in\{1,2,\cdots,l^{\#}\}}\}$ 发给敌手 $\mathcal{A}$。

4) 重复步骤 2)，敌手再次向挑战者发送任意次的属性集合 $S_{n+1},S_{n+2},\cdots,S_{n+m}$ 申请相应私钥，但规定以上属性集合不能满足访问结构 $(\boldsymbol{M}^{\#},\rho^{\#})$。

5) 猜测阶段。敌手输出对的 c 猜想 $c'=\{0,1\}$，如果 $c'=c$，则挑战者输出 $\theta=0$，表示 $\mathcal{T}=e(g,g)^{a^{q+1}s}$，此时敌手的优势 $\Pr[c=c'|\theta=0]=\frac{1}{2}+\varepsilon$；如果 $c'\neq c$，则输出 $\theta=1$，表示 $\mathcal{T}$ 是群 G_T 中的一个随机元素，此时敌手的优势 $\Pr[c=c'|\theta=0]=\frac{1}{2}$。因此，敌手 $\mathcal{A}$ 攻击 $q-$PBDHE 假设的优势为

$$\mathrm{Adv}_{\mathcal{A}}=\left|\frac{1}{2}\Pr[c=c'|\theta=0]+\frac{1}{2}\Pr[c=c'|\theta=1]-\frac{1}{2}\right|=\frac{1}{2}\varepsilon$$

故任何多项式时间敌手赢得 IND-SAS-CPA 游戏的优势是可忽略的。

证毕。

定义 2 若敌手可以通过策略更新算法任意更新访问控制策略从而非法访问交易数据，则敌手可以成功发起访问策略更新攻击。

定理 2 若数字签名算法满足不可伪造性，则溯源算法可以抵抗策略更新攻击。

证明 由溯源算法执行主体构成知，策略更新算法攻击者可分为溯源管理者、溯源用户及区块链网络中的共识验证节点。根据策略更新算法 $\mathrm{AccUpdate}(<\delta>,C_\delta^{'},(C_i^{'},D_i^{'})_{i\in[1,l']})$ 可知，若恶意管理者欲发起访问策略攻击，即不解密 $\mathrm{En}(s)$ 而直接计算 $C_\delta^{'}=g^{s'\delta}$，则 $C_\delta^{'}=g^{s'\delta}\neq g^{s\delta}$ 将无法通过验证，故恶意管理者无法成功更新访问策略；若恶意溯源用户欲发起攻击，则需提供管理者的身份签名消息 $<\delta>$ 和策略密文 $C_\delta^{'}$，由于签名算法具有不可伪造性且恶意溯源用户无法提供有效的 $C_\delta^{'}$，故恶意用户无法通过验证。即恶意用户无法成功更新访问策略；同理，恶意共识节点无法提供有效签名消息 $<\delta>$，故恶意节点亦无法成功更新访问策略。综上，溯源算法可以抵抗策略更新攻击。

证毕。

定理 3 若通过 $\mathrm{En}(s)$ 解密得到的 s' 与加密时使用的 s 一致，则更新算法具有正确性。

证明 根据加密算法 $\mathrm{Encrypt}(m,\delta,(M,\rho))$ 及其生成的密文结构 $\mathrm{CT}=\{C,C_\delta,(C_i,D_i)_{i\in[1,2,\cdots,l]}\}$ 知，若要对 CT 的访问控制策略进行更新，则对 CT 解密获取 m 后重新加密即可。即通过旧属性私钥 SK 解密 CT 获取 m 后，更新者输入 δ 和欲更新的访问控制策略 $(\boldsymbol{M}',\rho')$，算法选取新秘密共享值 s' 和随机参数 $t_2^{'},\cdots,t_n^{'}$，对 m 再次加密生成全新密文 $\mathrm{CT}^{'}=\{C^{'},C_\delta^{'},(C_i^{'},D_i^{'})_{i\in[1,2,\cdots,l']}\}$ 即可。根据解密算法 $\mathrm{Decrypt(CT,SK)}$ 知，满足新策略的用户可以借助属性密钥 $\mathrm{SK}^{'}$ 通过解密 $C_\delta^{'}$ 及 $(C_i^{'},D_i^{'})_{i\in[1,2,\cdots,l']}$ 得到 $e(g,g)^{\alpha s\delta}$，从而解出 $m=\frac{C^{'}}{e(g,g)^{\alpha s\delta}}$。由于更新过程中，通过 $\mathrm{En}(s)$ 获取到的 s' 与加密时使用的 s 一致，故 $C^{'}=C$，$C_\delta^{'}=C_\delta$，则重加密后的密文结构可表示为 $\mathrm{CT}^{'}=\{C,C_\delta,(C_i^{'},D_i^{'})_{i\in[1,2,\cdots,l']}\}$。因此，$\mathrm{SK}^{'}$ 可以通过 C_δ 及 $(C_i^{'},D_i^{'})_{i\in[1,2,\cdots,l']}$ 解密得到 $e(g,g)^{\alpha s\delta}$，从而解出 $m=\frac{C}{e(g,g)^{\alpha s\delta}}$，即 $\mathrm{SK}^{'}$ 可以正确解密更新后的密文 $\mathrm{CT}^{'}=\{C,C_\delta,(C_i^{'},D_i^{'})_{i\in[1,2,\cdots,l']}\}$。

证毕。

定理 4 若改进的属性加密算法满足 IND-SAS- CPA，则溯源方案具有隐私保护性。

证明 首先，交易记录 tx 生成过程中，由于交易双方都通过各自的 GID 进行匿名交易，使攻击者即便获取到交易记录，也无法通过交易密文提取到有效的交易者身份信息，故溯源方案可以保护用户身份隐私。其次，由于数据上链过程中，每条交易记录都将经过属性加密处理。根据改进的属性加密算法满足 IND-SAS-CPA 知，即便多项式时间敌手获取到交易密文 CT，也无法从密文中获取到关于

明文的有效信息，故溯源方案可以保护交易隐私。综上，溯源方案具有保护身份隐私和交易隐私的隐私保护性。

证毕。

定理 5　若溯源方案可以抵抗访问策略更新攻击，则溯源信息具有动态共享性。

证明　由于交易信息上链前都将基于访问策略 $(\boldsymbol{M},\rho)$ 进行属性加密处理，故满足策略要求的溯源用户可以通过属性私钥 SK 从溯源信息 CT 中共享到交易信息。当溯源信息的访问权限发生改变时，由于溯源管理者可以通过有效的管理身份信息 δ 及新的访问策略 $(\boldsymbol{M}',\rho')$ 对访问权限进行动态更新，并且溯源方案可以抵抗访问策略更新攻击，故旧策略用户无法以 SK 对溯源信息 CT' 进行有效共享，而新用户可以通过 SK' 对 CT' 进行有效访问。故溯源信息具有动态共享性。

证毕。

6.2　实验仿真分析

基于属性加密的数据溯源算法实验采用一台主机（其中，CPU 为 Intel Core i3 2120，内存为 4 GB，操作系统为 Windows 7），并选用 C++作为主要编程语言模拟实现 Waters 属性加密方案和改进的 CP-ABE 算法。

如图 4 所示，当访问策略的属性个数设置为 4，数据大小分别为 128 B、256 B、512 B 和 1 024 B 时，从 Waters 方案与本文方案的加解密时间曲线可以看出，由于本文方案中引入身份参数，使双线性映射的计算量有所增加，导致加密时间和解密时间代价平均比 Waters 方案约高出 400 ms 和 300 ms。

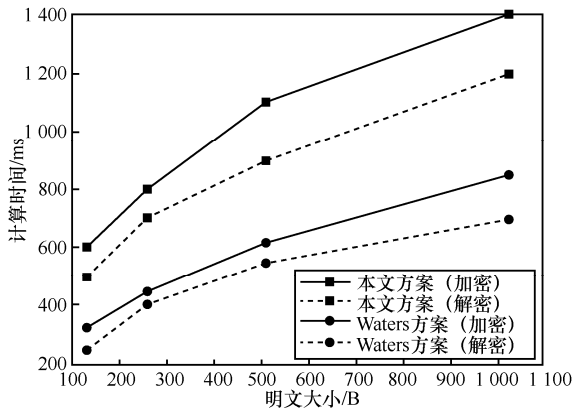

图 4　同属性个数下的加解密时间对比

如图 5 所示，当加解密数据大小设置为 128 B，访问属性分别为 4、8、12 和 16 个时，随着属性个数的增加，本文方案加解密时间代价总体高于 Waters 方案。其中加密执行时间平均约高出 Waters 方案 500 ms，而解密时间平均约高出 300 ms。

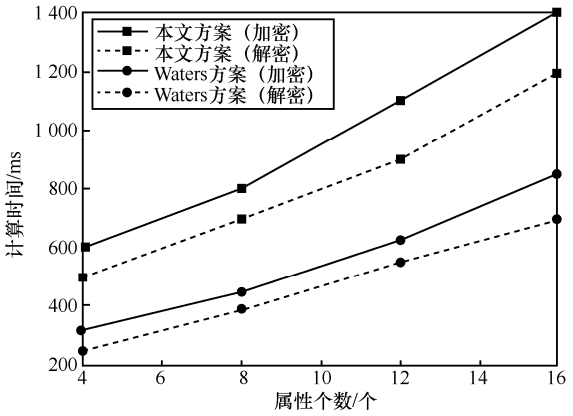

图 5　同文件下的加解密时间对比

由定理 2 知，要实现溯源信息访问权限的更改，可以通过重加密方式和策略更新方式完成。重加密过程分为解密原密文和生成新密文两步，策略更新分为新策略生成和新策略上链两步。通过模拟上述算法步骤得到各部分时间代价如图 6 所示，当更新算法的属性个数依次递增为 4、8、12 和 16 时，策略更新总时间消耗比重加密总时间消耗节约 100~700 ms，故本文方案在满足溯源信息动态共享的同时，访问策略更新算法有一定优势。

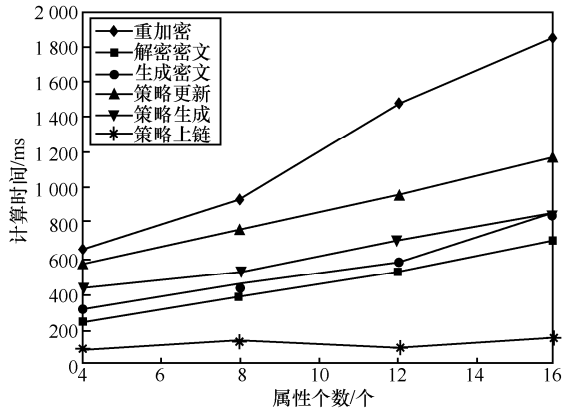

图 6　重加密与策略更新时间对比

为完整模拟整个溯源信息的上链、查询以及策略动态更新，本文实验利用 4 台主机采用 C++编写 PBFT 共识算法对数据流转操作进行模拟。为提高区块存储及查询效率，共识节点以 SQL Server 2008 存储本地区块数据。数据上链过程分为属性加密、共识验证及写入本地区块 3 个阶段，溯源信息查询过程分为交易策略区块组查询和交易密文解密 2 个

阶段，策略更新过程分为策略密文生成和追加新策略区块 2 个阶段。从图 7 中可以看出，当属性个数在 16 个以内时，上述操作的执行时间代价维持在 2 s 以内，并且时间代价随属性个数的增加呈线性增长关系。

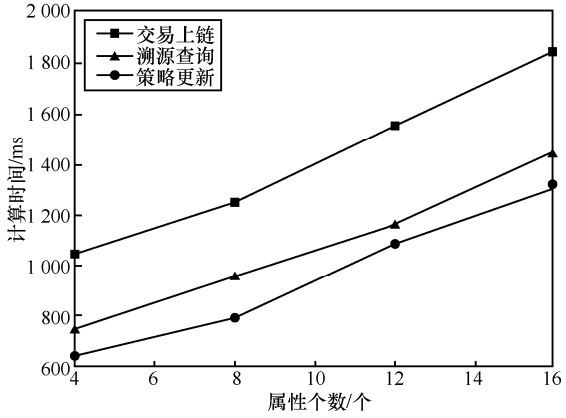

图 7 溯源操作执行时间代价

相较于传统区块链的“完全去中心化”，数据上链过程中，为实现溯源信息访问权限的细粒度控制，第三方需对交易进行属性加密并对加密过程中产生的共享密钥信息进行保存，甚至对访问策略进行更新；而共识节点需将每笔交易的密文分为 2 个区块存储。以上处理虽在一定程度上加大了第三方的计算代价及溯源链的存储代价，但为链上数据访问策略的动态更新提供有利条件。第三方计算代价如图 8 所示，当交易的数据大小为 128 B 时，随着属性个数的增加，整个交易信息的加密时间代价约为 800~1800 ms，解密时间约为 600~1400 ms，而新策略生成时间约为 400~900 ms，保留加密信息的解密 En(s) 时间约为 200 ms（与属性个数无关）。

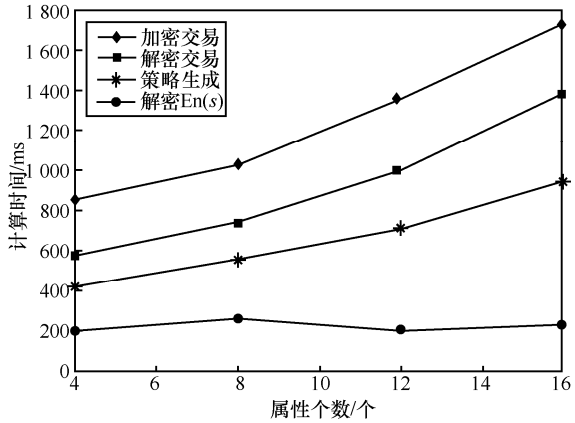

图 8 第三方计算时间代价

7 结束语

数据共享和隐私保护一直是评价区块链溯源系统的重要因素，本文基于属性加密算法提出一种具有保护用户隐私和数据动态共享的区块链数据溯源算法。数据上链过程中，基于 Waters 所提的 CP-ABE 方案设计适用于区块链的策略可更新属性加密算法，以此实现溯源信息的隐私保护。溯源信息查阅过程中，基于策略更新算法设计区块结构，完成交易区块访问策略的动态更新。最后，通过安全性及实验仿真分析表明，所提方案可以在保护用户隐私的同时实现溯源信息共享性的动态调整。本文方案具有广阔的应用场景，不仅能够为数据溯源提供具体的思路和方法，还能够为区块内容可见性的调整提供有效的解决方案。

参考文献：

[1] RAMACHANDRAN A, KANTARCIOGLU M. Smart provenance: a distributed, blockchain based data provenance system[C]//Eighth ACM Conference on Data and Application Security and Privacy. ACM, 2018: 35-42.

[2] TOSH D K, SHETTY S, LIANG X, et al. Consensus protocols for blockchain-based data provenance: challenges and opportunities[C]//Ubiquitous Computing, Electronics & Mobile Communication Conference. IEEE, 2018.

[3] WU S H, DU J. Electronic medical record security sharing model based on blockchain[C]//International Conference on Cryptography, Security and Privacy. ACM, 2019: 3-17.

[4] WANG R, TSAI W T, HE J, et al. A medical data sharing platform based on permissioned blockchains[C]//International Conference on Blockchain Technology and Application. ACM, 2018: 12-16.

[5] LEI X, SHAH N, LIN C, et al. Enabling the sharing economy: privacy respecting contract based on public blockchain[C]//ACM Workshop on Blockchain. ACM, 2017.

[6] ZHANG Y, WU S, JIN B, et al. A blockchain-based process provenance for cloud forensics[C]//International Conference on Computer and Communications. IEEE, 2017: 2470-2473.

[7] BHUIYAN M Z A, ZAMAN A, WANG T, et al. Blockchain and big data to transform the healthcare[C]//International Conference on Data Processing and Applications. ACM, 2018: 62-68.

[8] NEISSE R, STERI G, NAI-FOVINO I. A blockchain-based approach for data accountability and provenance tracking[C]//International Conference on Availability, Reliability and Security. ACM, 2017: 1-10.

[9] SAHAI A, WATERS B R. Fuzzy identity based encryption[C]//24th

Annual International Conference on Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2004: 457-473.

[10] GOYAL V, PANDEY O, SAHAI A , et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//13th ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

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

[12] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography. Heidelberg, 2011: 53-70.

[13] SAHAI A, SEYALIOGLU H, WATERS B. Dynamic credentials and ciphertext delegation for attribute-based encryption[J]. Lecture Notes in Computer Science, 2012: 199-217.

[14] YANG K, JIA X, REN K. Secure and verifiable policy update outsourcing for big data access control in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12): 3461-3470.

[15] LIU D, LI H, YANG Y, et al. Achieving multi-authority access control with efficient attribute revocation in smart grid[C]//IEEE International Conference on Communications. IEEE, 2014.

[16] HUANG X F, TAO Q, QIN B D, et al. Multi-authority attribute based encryption scheme with revocation[C]//IEEE International Conference on Computer Communication & Networks. IEEE, 2015: 1-5.

[17] LIU Z, CAO Z. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption[J]. IACR Cryptology ePrint Archive, 2010.

[18] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Haifa, Israel: Institute of Technology, 1996.

[作者简介]

田有亮（1982− ），男，贵州盘县人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护等。

杨科迪（1990− ），男，贵州安顺人，贵州大学硕士生，主要研究方向为数据溯源、区块链应用、数字水印等。

王缵（1992− ），男，安徽安庆人，贵州大学硕士生，主要研究方向为信息安全、区块链应用与共识机制、机器学习。

冯涛（1970− ），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全、密码学。