Journal of System Simulation

Volume 32 | Issue 6 Article 4

6-25-2020

Attribute Proxy Re-encryption for Ciphertext Storage Sharing Scheme on Blockchain

Xiaohong Zhang
1. School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China;;

Lanlan Sun
1. School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China;;2. Henan University Minsheng College, Kaifeng 475001, China;

Attribute Proxy Re-encryption for Ciphertext Storage Sharing Scheme on Blockchain

Abstract

Abstract: In order to implement the information storage sharing service safely and efficiently, a blockchain storage sharing scheme supporting the attribute proxy re-encryption and keyword retrieval is proposed. By the nodes classification and ciphertext storage separation, the anti-collusion attack is better implemented. The smart contract design of the information transaction is introduced and the information sharing parties can communicate spontaneously without the participation of the central organization. By the attribute-based proxy re-encryption algorithm, the information owner can share the information with other users without re-encrypting, uploading, and downloading information, and relieves the burden of the high-frequency access of the cloud to some extent. Comparing with the other schemes, the scheme is more secure and efficient.

Keywords

attribute-based proxy re-encryption, blockchain, anti-collusion attack, smart contract

Recommended Citation

Zhang Xiaohong, Sun Lanlan. Attribute Proxy Re-encryption for Ciphertext Storage Sharing Scheme on Blockchain[J]. Journal of System Simulation, 2020, 32(6): 1009-1020.

第 32 卷第 6 期 系统仿真学报© Vol. 32 No. 6
2020 年 6 月 Journal of System Simulation Jun., 2020

属性代理重加密的区块链密文云存储共享研究

张小红[1]，孙岚岚[1,2]
（1. 江西理工大学信息工程学院，江西 赣州 341000；2. 河南大学民生学院，河南 开封 475001）

摘要：*为了更安全高效地实现信息存储共享服务，提出一种支持关键词检索及属性代理重加密的区块链存储共享方案。采用节点分类和密文存储分离的方式，更好地实现了抗共谋攻击；引入信息交互智能合约，使信息共享双方无需中心机构参与就可以自发地进行通信。利用属性代理重加密算法，信息属主不需要重新加密、上传、下载就可以向其他用户共享信息，在一定程度上减轻云存储器高频访问的压力。通过与现有的属性代理重加密方案进行对比，结果验证了方案的安全性和高效性。*

关键词：*属性代理重加密；区块链；抗共谋攻击；智能合约*
中图分类号：TP309.7 文献标识码：A 文章编号：1004-731X (2020) 06-1009-12
DOI: 10.16182/j.issn1004731x.joss.18-0658

Attribute Proxy Re-encryption for Ciphertext Storage Sharing Scheme on Blockchain

Zhang Xiaohong[1], *Sun Lanlan*[1,2]
（1. School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China；
2. Henan University Minsheng College, Kaifeng 475001, China)

Abstract: In order to implement the information storage sharing service safely and efficiently, *a blockchain storage sharing scheme supporting the attribute proxy re-encryption and keyword retrieval is proposed. By the nodes classification and ciphertext storage separation, the anti-collusion attack is better implemented. The smart contract design of the information transaction is introduced and the information sharing parties can communicate spontaneously without the participation of the central organization. By the attribute-based proxy re-encryption algorithm, the information owner can share the information with other users without re-encrypting, uploading, and downloading information, and relieves the burden of the high-frequency access of the cloud to some extent.* Comparing with the other schemes, the scheme is more secure and efficient.

Keywords: attribute-based proxy re-encryption; blockchain; anti-collusion attack; smart contract

引言

随着云计算、物联网(Internet Of Things，IOT)技术的飞速发展，用户信息呈现爆炸式增长[1]，越来越多的用户选择将隐私信息转移到云中，云存储成为了最常用的一种网络存储服务。目前，云存储共享系统大多是中心化的，在第三方云服务提供商(Cloud Service Provider，CSP)的帮助下管理个人信息，但这种方法不仅需要大量的通信开销、高额的计算成本，而且物联网的公开透明化使信息的完整性、准确性、机密性面临着严重威胁。2009 年 Google 隐私文件外泄[2]；2010 年 6 月苹果公司 iPad 用户的隐私信息泄露[3]；2013 年云笔记应用 Evemote 的 5 000 万用户数据遭到黑客攻击[4]；2017

收稿日期：2018-10-03 修回日期：2018-11-22；
基金项目：国家自然科学基金(51665019, 61763017)，江西省自然科学基金(20161BAB206145)；
作者简介：张小红(1966-)，女，河北昌黎，博士，教授，研究方向为非线性动力学，信息安全，视频保密通信。

年 Dell 公司旗下的 BOX 提供的“云协作”文件在共享过程中敏感信息泄露。如何保护用户信息隐私和敏感数据的机密性已经成为了当前云存储共享技术的亟需解决的问题。

Hong 等[5]提出一种基于属性加密的混合云重加密的秘密共享方案，从降低信息属主管理复杂度的角度出发，实现更为高效的动态密文访问控制。Seo 等[6]设计一种基于属性的代理重加密方案，该方案将传统的代理重加密与属性基加密相结合，使信息属主能够授权指定的用户根据用户的属性来解密重新加密的密文。以上方案对保证信息的机密性，实现信息的安全交互均起到积极作用，但均不支持关键词检索功能，高效的信息共享仍然存在一定的阻碍。Shi 等[7]提出一种基于公钥可检索关键词的属性代理重加密方案，并不支持原始密文和重加密密文的解密。Liang 等[8]在随机预言机模型下证明其提出的基于密钥策略的支持关键词检索的属性代理重加密模型的可行性，但是该方案的计算代价较大。以上提出的所有方案均是采用中心化管理模式，所有用户的信息集中在资源池内，由第三方 CSP 使用特定的软件对信息强制进行统一管理，CSP 的软硬件一旦出现故障或受到攻击，可能会造成信息丢失、泄露，甚至服务中断等意外。

区块链(Blockchain，BC)技术的出现为人们提供了一种去中心化、不可篡改、不可伪造、集体维护的分布式管理方法[9]。2008 年美籍日裔学者中本聪[10]提出一个可以作为公共账本的区块链概念，它是分布式数据存储、点对点传输、共识机制[11]、加密算法等技术相融合的新型应用模式。区块链技术利用块链式数据结构来验证与存储数据，采用分布式节点共识算法来生成和更新数据，结合密码学的方式保证数据传输和访问的安全，并由自动化脚本代码组成的智能合约[12]来编程和操作数据的一种全新的分布式基础架构与计算范式。它是一种符合物联网时代的共享开放、公平竞争、真实完整、安全可靠等基本特性的比特币底层技术架构。

本文结合区块链技术设计了一种与传统信息存储共享兼容的，同时支持关键词检索的区块链密文信息存储共享模型，通过属性代理重加密技术，使信息共享具有更灵活的共享控制特性。当信息属主下线时，节点依然可以按照智能合约规则完成信息交互工作，实现信息的不间断共享。关键词作为元数据的一部分存在区块链上，便于信息检索，提高了信息共享的效率，在一定程度上节约了通信成本，减轻了云存储器高频访问的压力。

1 预备知识

1.1 Pool 验证池共识机制

在去中心化的区块链系统中，节点之间是相互独立的，通过共识机制算法达成“信任”，各节点在满足自身收益的前提下，实现系统内部信息的统一。本设计中按照 Pool 验证池共识机制的工作原理，以及实际需要将所有节点分为两类：存储节点、传输节点。

(1) 存储节点(memory node，M_i)：负责记录存储、下载工作，记录新的交易，保证信息的有效、准确的存储；

(2) 传输节点(transmission node，T_n)：负责安全传递信息以及验证工作，实现信息的安全、高效的传输。

每个节点可处于 3 种状态：领导节点、竞选节点和群众节点。在初始状态下，信息属主发送存储请求之前，所有参与节点都是群众节点，在没有接收到领导节点命令之前，所有群众节点均有可能成为竞选节点，在 150~300 ms 的时间内得票最多者竞选节点被选为领导节点。一旦竞选成功，领导节点会根据 Raft 协议[13]的组织集群内部所有群众节点对系统内部最新的交易信息进行传输、存储。在 Raft 协议中，其依赖于领导节点的可用性来确保集群数据的一致性，交易流向只能从领导节点向群众节点转移。所以在进行存储时，所有节点在竞选节点通过民主投票的形式选取领导节点，选取成功后，其余节点自动变回群众节点，服从领导节点的

https://dc-china-simulation.researchcommons.org/journal/vol32/iss6/4
DOI: 10.16182/j.issn1004731x.joss.18-0658

指令完成指定工作。

1.2 属性代理重加密算法

1998 年，Blaze 等[14]在欧洲密码学会议上提出了“代理重加密”(Proxy Re-Encryption，PRE)的概念，PRE 是代理者在不透露任何关键词以及明文信息的前提下，允许半可信的代理者将信息属主的密文转换为共享者的密文得到明文信息的过程。本文利用这种属性代理重加密算法[7-8]方案解决信息的存储及共享的安全问题。

属性代理重加密算法方案由以下 7 个算法构成，如图 1 所示。

(1) 系统初始化

$setup(k,U)\rightarrow(GP,MSK,PK)$：给定系统的安全参数 k、系统属性集合 U，生成公共参数 GP，系统主密钥 MSK，系统公钥 PK。

(2) 密钥生成

$KeyGen(MSK,PK,S_A,S_B)\rightarrow((SK_A,PK_A),(SK_B,PK_B))$：输入系统公共参数 GP、主密钥 MSK、系统公钥 PK、用户 Alan 属性集合 $S_A\subseteq U$ 以及用户 Bill 的属性集合 $S_B\subseteq U$，分别生成用户 Alan 的私钥/公钥 (SK_A,PK_A) 和用户 Bill 的私钥/公钥 (SK_B,PK_B)。

(3) 重加密密钥生成

$ReKeyGen(SK_A,S_A,PK_B,GP,(M',\rho'))\rightarrow rk_{A\rightarrow B}$：假设信息属主为 Alan，请求者为 Bill，输入 Alan 的私钥 SK_A 及其对应的属性集合 S_A、公共参数 GP、Bill 的公钥 PK_B，以及新的共享结构 (M',ρ')，生成对应的重加密密钥 $rk_{A\rightarrow B}$，其中 M' 是一个 $l\times n$ 的矩阵，行标号函数 ρ' 将矩阵 M' 的行映射成属性且 $\rho':\{1,2,...,l\}\rightarrow S_B$。

(4) 加密

$Encrypt(m,(M,\rho),GP,PK_A)\rightarrow CT_A$：给定公钥 PK_A、公共参数 GP、信息的共享结构 (M,ρ) [15]以及明文 m 生成密文 CT_A。密文 CT_A 可以通过 $rk_{A\rightarrow B}$ 转换成 CT_B 且仅能被满足共享结构 (M,ρ) 的用户正确解密。

(5) 重加密

$ReEncrypt(PK,GP,CT_A,rk_{A\rightarrow B})\rightarrow CT_B$：根据系统公钥 PK，密文 CT_A 和重加密密钥 $rk_{A\rightarrow B}$ 输出重加密密文 CT_B。

(6) 密文解密

$Decrypt(PK,CT_A,SK_A)\rightarrow m$：由系统公钥 PK、密文 CT_A 和私钥 SK_A 解密得到明文 m。

(7) 重加密解密

$ReDecrypt(CT_B,SK_B)\rightarrow m$：针对重加密密文 CT_B，利用私钥 SK_B 进行解密从而得到明文 m。

1.3 双线性映射

设阶数为 p 的循环群 G_1，G_2，存在相同阶数 p 且满足的双线性映射 $\hat{e}:G_1\times G_2\rightarrow G_T$ 的乘法循环群 G_T，满足以下性质：

(1) 双线性：对于 $J\in G_1$，$L\in G_2$，$a,b\in Z_p$，存在 $\hat{e}(J^a,L^b)=\hat{e}(J,L)^{ab}$。

(2) 可计算性：任意 $c\in G_1$，$d\in G_2$ 则 $\hat{e}(c,d)$ 在时间上均可以进行有效计算。

(3) 非退化性：存在 $c\in G_1$，$d\in G_2$ 满足 $\hat{e}(c,d)\neq 1$。

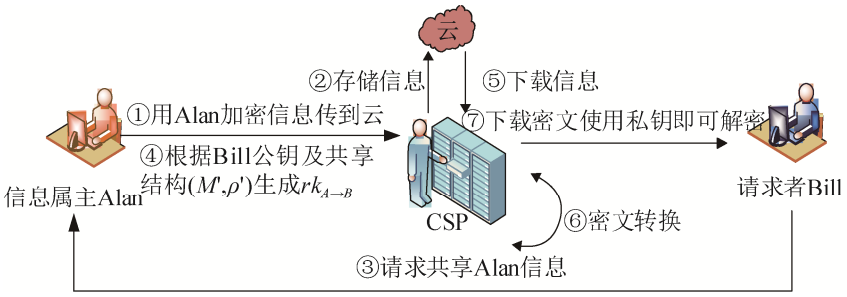


图 1 属性代理重加密过程示意图
Fig. 1 Attribute-based proxy re-encryption

1.4 安全性假设

判定性 q–并行双线性迪菲-赫尔曼指数(Decisional q–parallel Bilinear Diffie-Hellman Exponent，q–parallel BDHE)假设[16]。根据系统安全参数选取阶数为大素数 p 的加法循环群 G_1，g 为 G_1 的生成元，随机选取 $a,s,b_1,...,b_q \in Z_p$，则攻击者 ℓ 根据给定的元组 y：

$$\begin{aligned}&\vec{y}=g,g^{s},g^{a},...,g^{(a^{q})},g^{(a^{q+2})},...,g^{(a^{2q})}\\&\forall_{1\le j\le q}g^{s\cdot b_j},g^{\frac{a}{b_j}},...,g^{\left(\frac{a^{q}}{b_j}\right)},g^{\left(\frac{a^{q+1}}{b_j}\right)},...,g^{\left(\frac{a^{2q}}{b_j}\right)}\\&\forall_{1\le j,k\le q,k\ne 1}g^{\frac{a\cdot s\cdot b_k}{b_j}},...,g^{\left(\frac{a^{q}\cdot s\cdot b_k}{b_j}\right)}\end{aligned} \tag{1}$$

判别 T 是一个随机值或者是 $e(g,g)^{a^{q+1}s}$。

攻击者 ℓ 在 q–parallel BDHE 问题上取得的优势可以用概率表示为：

$$Adv_{\ell}(k)=\left|\begin{matrix}Pr[B(\vec{y},T=e(g,g)^{a^{q+1}s})=0]\\-Pr[B(\vec{y},T=R)=0]\end{matrix}\right|\ge\xi \tag{2}$$

则不存在一个不可忽略的优势 ξ 用于区分判别 $e(g,g)^{a^{q+1}s}$ 与 G_T 中的随机元 T，则称假设成立。

2 区块链存储共享方案

2.1 方案角色预设

本方案主要围绕 3 个角色：云存储器、信息属主、共享请求者进行设计，其基本职责设计如下：

(1) 云存储器：负责提供存储空间，用户可以向 CSP 购买相应的存储空间，便于存储记录信息。

(2) 信息属主：系统内所有用户拥有记录存储信息的权限，可对信息进行加密并预先设置共享权限，只有共享请求者满足共享权限的前提下才能解密获取密钥，从而获取信息属主共享的原始明文信息，假设信息属主是 Alan。

(3) 共享请求者：系统内用户可以向信息属主或本地节点发起共享信息请求，假设共享请求者为 Bill。

在本方案中，假设信息交互双方均是具有有效身份的用户，且所有的信息属主都是可信任的，共享请求者是非可信的，即共享请求者之间可以串通共谋，非法访问未授权的用户信息。

2.2 系统存储架构模型

基于区块链技术的存储架构如图 2 所示，不同于经典的集中式虚拟化存储，在存储阶段，Alan 发送存储请求时，集群中的传输领导节点 T 向自己集群内广播验证 Alan 签名的有效性。若有效，则由传输领导节点 T 将基于属性加密后的数据暂时存储到自己的日志内，然后向所有集群内的群众节点 T_n 复制信息并等待响应，在确定至少集群内部已经超过一半数量的节点已经接受到了信息后再向 Alan 确认信息已经接收，一旦用户收到确认信息后就表明此时信息处于已提交状态，T 再向 T_n 发通知告知该数据状态已提交。然后传输节点向存储节点发送存储信息，由负责存储的节点 M 向自己集群内的 M_i 广播存储请求，在确定多于半数节点完成存储后，向请求者反馈信息，此次存储工作完成。若无效，则反馈“无效用户”。

使用公钥 PK 及预先设定好的阅览、共享权限 (M,ρ)，对原信息密文解密密钥 k' 和文件存储位置 LC 以及信息关键词 w 进行加密，IN 为信息的项目编号，作为元数据 $Data$ 的一部分存储在区块链上，原始信息由用户加密后存储在云中。在系统中，所有节点共同完成信息存储共享工作，为了保证系统的稳定性及系统内存储信息的有效性和准确性，系统内部节点每记录一笔交易，将获取相应的信用币作为劳动报酬，这是区块链系统保证各节点在系统内部记录信息的真实性，有效性的激励方式。其中，采用信息提取关键词作为信息摘要的方式便于信息检索，以提高信息共享的效率。

2.3 云安全密文共享设计

在区块链存储共享结构中如图 3 所示，为了实现高效率、高安全的信息共享，原始信息密文 CT_A 通过公共渠道传输，解密密钥 k' 通过安全渠道传输。在信息共享阶段，Bill 发送共享请求需要缴纳相应的共享费用，集群中的存储领导节点 M 向自

DOI: 10.16182/j.issn1004731x.joss.18-0658

已集群内的群众节点广播验证用户身份，判定其是否符合密文共享权限 (M,ρ)。若符合，则由领导节点 M 向自己集群内的节点 M_i 通过关键词的形式对信息进行检索广播共享请求，获取元数据后，由 Bill 自主选择需要的信息，系统判断 Bill 的信用币与信息报价的关系，若大于等于信息报价，则将其使用代理重加密技术转换成符合 Bill 的共享权限 $(M^{'},\rho^{'})$ 密文 CT_B，然后传输领导节点 T 向所有集群内 T_n 节点复制信息并等待响应，在确定至少集群内部已经超过一半数量的节点已经接受到了信息后，向存储节点确认信息后就表明此时信息处于已传输状态。然后传输节点向 Bill 发送通过关键词密文检索获取的元数据密文 CT，通过解密后获取信息的存储位置 LC，从而在相应位置下载解密原信息密文 CT_A，获取信息明文 m；若小于信息报价，则反馈“余额不足”。若不符合共享权限，输出“访问无效”。在共享过程中，为了保证共享后的信息安全，Alan 可以通过重加密技术随时撤销共享信息。

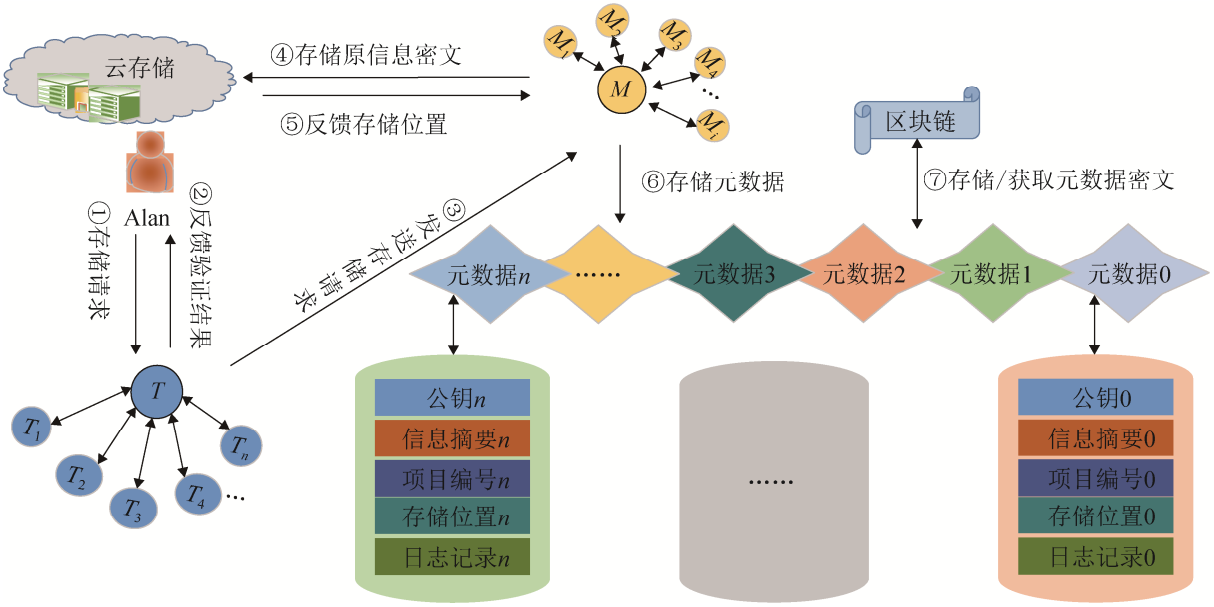


图 2　区块链密文云存储系统模型

Fig. 2　Blockchain ciphertext storage system model2.3 云安全密文共享设计

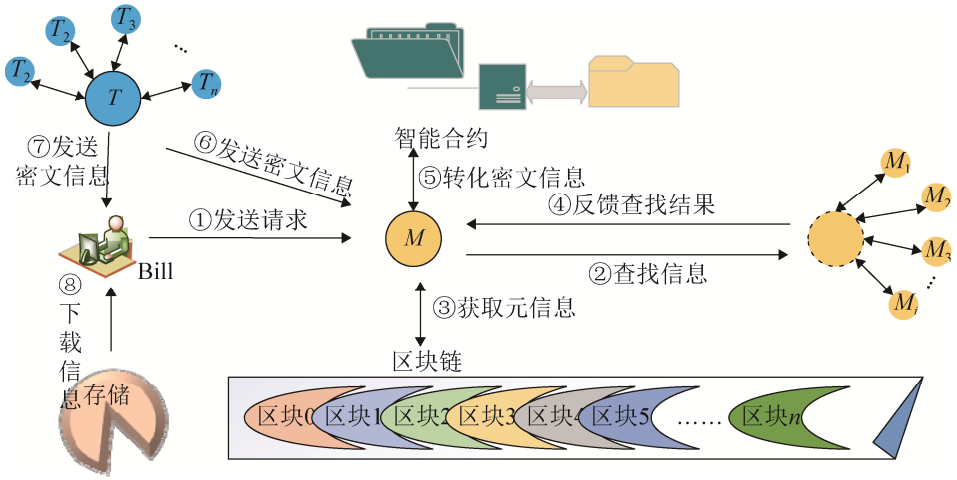


图 3　区块链密文信息共享过程模型

Fig. 3　Blockchain ciphertext information sharing system model

2.4 信息交易合约设计

智能合约是区块链的重要组成部分之一，本设计智能合约的设计符合以下几个原则：(1) 系统内部的所有用户均可自愿发布及参与信息存储及共享交易；(2) 所有用户的信息在实行共享之前处于保密状态；(3) 合约执行结果自动结算。

本节中的交易处理按照时间顺序划分为以下几个阶段：合约发布，发布存储交易，发布共享交易，权限审核，安全校核，交易结算。具体表述如图 4 所示。

(1) 制定合约：合约创建者使用高级语言将带有用户属性集合特性的合约转化为二进制合约码，记录在本地网中，同时召集所有本地用户对合约进行签名，由节点确认签名后，通过以太坊虚拟机部署在以太坊区块链中，并向用户反馈合约地址及调用指令。

(2) 发布存储交易：信息属主 Alan 根据预先设置好的共享权限 (M,ρ) 存储明文信息 m 以及密文 CT，同时，Alan 提交信息报价及自定义的随机字符串以便于用户获取信息共享报酬，在此过程中，Alan 还需要向合约地址提供一定的信用币作为保证金，以避免虚假、抄袭等现象。

(3) 发布共享交易：共享请求者 Bill 发送共享请求，同时需要缴纳相应的共享保证金，以保证请求的真实性、有效性。

(4) 权限审核：在权限审核阶段，系统根据请求者 Bill 的属性集合 S_B 与共享权限 (M,ρ) 进行权限匹配，并将结果提交给智能合约。系统根据公钥 PK、关键词 w 生成相应的搜索口令 TK 获取检索结果信息及各信息对应的报价。

(5) 安全校核：在安全校核阶段，Bill 根据筛选结果选择自己所需要的信息，同时系统审核请求者信用币数量和用户请求共享的信息价格，若信用币大于等于信息价格，则进入密文转换阶段；否则，反馈“余额不足”。

(6) 交易结算：系统根据信息交互结果，对用户的信用币作相应的调整并确认信息的更新变化情况，然后根据反馈的数据进行信用币结算。首先返还未成功交互的用户保证金，然后根据交易完成情况，结算用户交互信息费用。

2.5 具体方案执行步骤

本文给出了一种支持关键词检索的密文策略属性代理重加密方案，该方案涉及到的变量符号如表 1 所示。

本方案由以下 8 种算法构成，算法表示如下：

(1) 系统初始化：

$$Setup(\lambda,U)\rightarrow(GP,MSK,PK)$$

给定系统安全参数 λ，系统属性集合 U，然后构造阶数为 p 的加法循环群 G，g 为 G 的生成元，

且存在满足双线性映射 e：$G\times G\rightarrow G_T$，随机选取一个整数且满足 $g_1\in G$，并设置以下目标散列哈希函数 $H_1:(0,1)^{2k}\rightarrow Z_p$，$H_2:(0,1)^{2k}\rightarrow G_T$，$H_3:(0,1)^*\rightarrow G$，$H_4:(0,1)^*\rightarrow G$，$H_5:(0,1)^k\rightarrow Z_p$，$H_6:(0,1)^*\rightarrow G$ 随机选取不同的整数 $\alpha,a\in Z_p,Z=e(g,g)$，随机选取整数 $h_x\in Z_p$ 计算 $H_x=g^{h_x}$，其中 $x\in U$。

$$\begin{cases} GP=\begin{pmatrix} p,g,g_1,g^a,e(g,g)^\alpha, \\ H_1,H_2,H_3,H_4,H_5,H_6 \end{pmatrix} \\ PK=(g,g_1,g^a,e(g,g)^\alpha,H_x) \\ MSK=(g^\alpha,a) \end{cases} \tag{3}$$

式中：GP 为系统公共参数；MSK 为系统主密钥；PK 为系统公钥。

(2) 密钥生成阶段：$KeyGen(GP,PK,MSK,S_A)\rightarrow(SK_A,PK_A)$

输入公共参数 GP，系统主密钥 MSK，信息属主 Alan 属性集合 $S_A\subseteq U$，随机选择整数 $t\in Z_p$，以及生成 Alan 对应的私钥 SK_A，PK_A。

$$\begin{cases} SK_A=\begin{pmatrix} S_A,K_A=g^\alpha g^{at},L_A=g^t, \\ (K_X=H_3(x)^t)_{x\in S_A} \end{pmatrix} \\ PK_A=g^{SK_A} \end{cases} \tag{4}$$

同理，生成共享请求者 Bill 的私钥 SK_B，PK_B。

https://dc-china-simulation.researchcommons.org/journal/vol32/iss6/4
DOI: 10.16182/j.issn1004731x.joss.18-0658

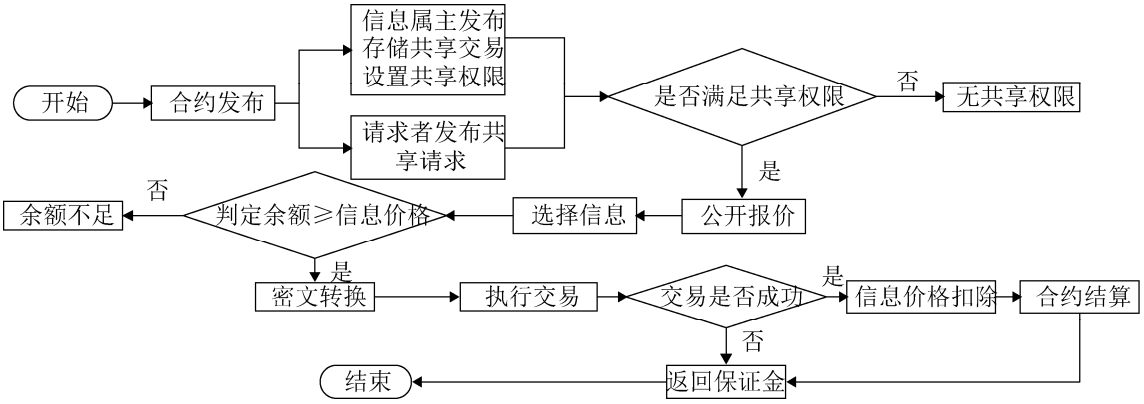


图 4 信息交互双方合约执行流程示意图

Fig. 4 Information exchange execution flow diagram of smart contract

表 1 符号描述

Tab. 1 Scheme design symbol description

符号	描述
m、λ	信息明文、系统安全参数
U、S_*	系统通用属性集合、用户*的属性集合
GP、MSK、PK	公共参数、系统主密钥、系统公钥
G	阶数为大素数 p 的加法循环群
SK_*、PK_*	用户*的私钥、公钥
w	存储信息的关键词
(M^*,ρ^*)	共享结构
CT_A	原始信息密钥密文
CT_B	重加密密钥密文
$rk_{A\to B}$	代理重加密密钥
CT	元数据密文
LC	原始信息密文在云中的存储位置
IN	信息的项目编号

(3) 重加密密钥生成算法：$RekeyGen(GP, SK_A,(M^{'},\rho^{'}),PK_B)\to rk_{A\to B}$

信息属主 Alan 随机取一个整数 $\theta\in Z_p$，并计算 g^{θ}、g_1^{θ}，根据 Bill 的属性集合 S_B 构造共享结构 $(M^{'},\rho^{'})$，结合公共参数 GP，Alan 对应的私钥 SK_A，请求者 Bill 的私钥 PK_B，计算重加密密钥 $rk_{A\to B}$。

$$\begin{cases} rk_1 = K^{H_5(\delta)} g_1{}^{\theta} = g^{\alpha} g^{at} g_1^{\theta} \\ rk_2 = g^{\theta} \\ rk_3 = L^{H_5(\delta)} \\ rk_4 = C^{'}_{(M^{'},\rho^{'})} \\ R_x = K_x{}^{H_5(\delta)} \end{cases} \tag{5}$$

$$rk_{A\to B} = (S_A, rk_1, rk_2, rk_3, rk_4, R_x) \tag{6}$$

式中：$M^{'}$ 是一个 $l^{'}\times n^{'}$ 的矩阵，函数 $\rho^{'}$ 将矩阵 $M^{'}$ 的行映射成属性。随机选取整数 $s, y_2, ..., y_n\in Z_p$ 构成 Z_p 一个列向量 $\vec{\upsilon}=(s, y_1, y_2, ..., y_n)$ 计算 $\varepsilon_i=\vec{\upsilon}M_i$，其中 s 表示信息属主共享的秘密，$M_i^{'}$ 对应矩阵 $M^{'}$ 第 i 行的矢量，$\{\varepsilon_i\}$ 为 $M_i^{'}$ 的 $\vec{\upsilon}$ 的有效部分，$I=\{i:\rho^{'}(i)\in S_A, 1\le i\le l^{'}\}$ 表示共享结构 $(M^{'},\rho^{'})$ 中用到的属性。

(4) 信息加密：

$$\begin{cases} Encrypt_1(m,(M,\rho),\ PK_A)\to CT_A \\ Encrypt_2(PK, Data,(M,\rho),k^{'})\to CT \end{cases}$$

第 1 步原信息加密：输入公钥 PK_A，信息属主输入信息明文 m，预先设定好的设置阅览、共享权限 (M,ρ)，计算密文 CT_A，并将密文信息存储在云服务器中。

第 2 步元数据加密：输入系统公钥 PK，以及预先设定好的阅览、共享权限 (M,ρ)，元数据 $Data\to\{LC, w, IN\}$，其中，LC 表示原始信息密文在云中的存储位置，w 为信息的关键词，IN 为信息的项目编号，原始信息密文解密密钥 $k^{'}$，输出密文 CT，并存储在区块链中。

$$\begin{cases} A_1 = Data\cdot e(g,g)^{\alpha s}, A_2 = g^s, A_3 = g_1^s \\ B_1 = (g^{\alpha})^{\varepsilon_1} H_1(\rho(1))^{-\gamma_1}, ..., B_l = (g^{\alpha})^{\varepsilon_l} H_l(\rho(1))^{-\gamma_l} \\ C_1 = g^{r_1}, ..., C_l = g^{r_l} \end{cases} \tag{7}$$

(5) 密文重加密算法：$ReEncrypt(rk_{A\to B}, CT, PK_{B},(M^{'},\rho^{'}))\to CT_B$

节点首先判断 Bill 是否为系统合约用户，若是，随机选择 $\delta \in G_T$ 并计算。

$$CT' = ((M', \rho'), A_1', A_2', A_3', (B_i', C_i')_{i=1}^{l}) \tag{8}$$

$$\begin{cases} A_1' = \delta \cdot e(g,g)^{\alpha s'}, A_2' = g^{s'}, A_3' = g_1^{s'} \\ B_1' = (g^{\alpha})^{\varepsilon_1'} H_1(\rho'(1))^{-\gamma_1'}, ..., B_l' = (g^{\alpha})^{\varepsilon_1'} H_l(\rho'(l'))^{-\gamma_l'} \\ C_1' = g^{r_1'}, ..., C_{l'}' = g^{r_l'} \end{cases} \tag{9}$$

然后根据重加密密钥 $rk_{A \to B}$，密文 CT，计算出密文的重要分量 ϕ，最终输出重加密后的密文 CT_B。

$$\phi = \frac{e(A_2', rk_1) / e(A_3', rk_2)}{\prod_{i \in I} (e(B_i', rk_3) e(C_i', R'_{\rho(1)}))^{\omega_i}} \tag{10}$$

$$CT_B = (A_1', A_3', (M', \rho'), (B_i', C_i')_{i=1}^{l'}, \ \phi) \tag{11}$$

式中：$\omega_i \in Z_p$ 且满足 $\sum_{i \in I} \omega_i \varepsilon_i = s$。

(6) 索引生成及关键词检索：

$$\begin{cases} Index(GP, w) \to ID、ID' \\ StokenGen(SK_B, w_B', kw') \to TK \end{cases}$$

第 1 步索引生成：输入公共参数 GP，信息 m 的关键词 w，节点计算原始信息中关键词 w_A 对应的消息认证码 kw，以及重加密信息密文的 CT_B 中 w_B' 对应的认证码 kw'，生成索引码 ID、ID'；

第 2 步关键词检索：根据输入用户 Bill 对应的私钥 SK_B，关键词 w_B 及其对应的搜索密钥 kw'，输出关键词 w_A 对应的搜索口令 TK。

(7) 代理重加密解密算法：$ReDecrypt(SK_B, CT_B) \to CT$

系统核对请求用户 Bill 的属性集合 S_B 是否满足重加密后的密文 CT_B 中的共享结构 (M', ρ')，若满足，Bill 可以使用私钥 SK_B 解密通过密文策略属性基加密的解密方法恢复出密文的重要分量 ϕ，得到 CT 恢复出 k'、$Data$。

$$k' = \frac{A_1}{(\phi)^{\frac{1}{H(\delta)}}} \tag{12}$$

用户根据元数据 $Data$ 获取原信息存储位置 LC 及解密密钥 k'，对 CT_A 解密恢复明文信息 m。

$$m = \frac{A_1 \cdot e(A_3, g^{\theta})}{\phi} \tag{13}$$

(8) 原信息密文解密：$Decrypt(CT_A, k', GP) \to m$

解密密钥 k' 仅由区块链与信息属主 Alan 掌握，未授权的情况下，仅有信息属主 Alan 可以对云存储器上的原始信息密文 CT_A，利用式(14)解密获取原始明文信息 m。

$$m = \frac{A_1}{\prod_{i \in I} (e(B_i, L_A) e(A_2, R_{\rho(1)}))^{\omega_i}} \tag{14}$$

3 系统性能分析

3.1 安全性分析

本设计是基于 q–parallel BDHE 困难性问题进行安全性证明的，判断双线性困难性问题，如果假设成立，即在随机预言模型下的敌手 ℓ 的优势 $Adv_{\ell}(k)$ 忽略不计，则说明该方案是选择明文安全(CPA，Chosen Plaintext Attack)的。

定理：如果方案在 (G, G_T) 上解决 q–parallel BDHE 问题的优势是可以忽略不计的，那么不可以找到任意的概率多项式挑战 (M^*, ρ^*) 攻破本方案，即称 q–parallel BDHE 假设在 (G, G_T) 成立，该方案在随机预言模型下是 CPA 安全的。

证明：假设存在一个攻击者 ℓ 在 CPA 游戏中，以不能够忽略的优势 $\xi = Adv_{\ell}(k)$ 赢得游戏。那么我们可以构造一个游戏挑战者 $\Re$ 实现对 q–parallel BDHE 的判断，从而判别 $T = e(g,g)^{a^{q+1}s}$ 还是 $T \in G_T$。具体实施过程如下：

初始化阶段：游戏挑战者 $\Re$ 将会收到来自攻击者 ℓ 发送的共享权限结构 (M^*, ρ^*)。

(1) 系统建立阶段：挑战者 $\Re$ 随机选择一个值 α，$\chi' \in Z_p$，目标哈希函数 H_1，H_2，H_3，H_4，H_5，H_6 计算：$e(g,g)^{\alpha} = e(g,g)^{\chi'} e(g,g^{\alpha})$ 并发送 $GP = (p, g, g_1, g^a, e(g,g)^{\alpha}, H_1, H_2, H_3, H_4, H_5, H_6)$ 和 $PK = (g, g_1, g^a, e(g,g)^{\alpha}, H_x)$ 给攻击者 ℓ。

(2) 查询阶段 1：

攻击者 ℓ 对挑战者 $\Re$ 进行一系列的提问，挑战者 $\Re$ 做相应应答。

情况 1：私钥提取阶段：攻击者 ℓ 按照属性集

合 S 构造私钥 SK_s，若 S 满足 (M^*,ρ^*)，则挑战者 $\Re$ 就在{0,1}中随机选择一个输出，游戏终止；若不满足，则挑战者 $\Re$ 随机选取 $r_S \in Z_p$，$\lambda=(\lambda_1,\lambda_2,...,\lambda_n)\in Z_p$，其中 $\lambda_1=-1$ 且满足 $\lambda M^*=0$；

情况 2：重加密密钥提取阶段：用一个属性集 S_i 和一个共享权限结构 (M',ρ') 进行密钥提取，首先判定 S 是否满足 (M^*,ρ^*)，若满足，则挑战者 $\Re$ 就在{0,1}中随机选择一个输出，游戏终止；否则，获取私钥 SK，然后计算 $rk_{A\to B}=(S,rk_1,rk_2,rk_3,rk_4,R_x)$，反馈给攻击者 ℓ。

(3) 挑战阶段：攻击者 ℓ 随机发送两段相等长度的消息 m_0 和 m_1 给挑战者 $\Re$，挑战者 $\Re$ 随机抽取一个比特属性 $b\in(0,1)$，利用 (M^*,ρ^*) 对 m_b 加密得到密文 CT^* 并发送给 ℓ。若 $T=e(g,g)^{a^{q+1}s}$，则 CT^* 是一个有效的密文。

(4) 查询阶段 2：重复查询阶段 1 的操作。

(5) 猜测阶段：ℓ 输出猜测比特 $b'\in(0,1)$，挑战者 $\Re$ 的根据 ℓ 的结果做出相应的猜测，若 ℓ 给出了猜测 $b'=b$，即挑战者 $\Re$ 在猜想游戏中得到的是 $T=e(g,g)^{a^{q+1}s}$。若攻击者 ℓ 猜测结果 $b'\neq b$，则 $T\in G_T$。我们定义挑战者 $\Re$ 的优势：

$$\xi=Adv_\ell(k)=|Pr[b'=b]-\frac{1}{2}| \tag{15}$$

当输出为 0 时，即 ℓ 得不到任何关于 m_b 的任何信息，不能恢复明文，因此猜测正确得的概率为 $\frac{1}{2}$。当输出为 1 时，即 ℓ 得到任何关于 m_b 的有关密文信息，并能恢复明文，由定理不难得出猜测正确得的概率为 $\frac{1}{2}+\xi$。

因此，在本方案中 $q-paralle\ BDHE$ 猜测准确，即 $b'=b$ 的优势为

$$Adv_\ell(k)=|Pr[b'=b]-\frac{1}{2}|=\frac{1}{2}Pr[b'=b|b=0]+\frac{1}{2}Pr[b'=b|b=1]-\frac{1}{2}=\frac{\xi}{2} \tag{16}$$

因此，如果攻击者 ℓ 能攻破方案的概率为 ξ，则解决 q–parallel BDHE 问题的优势为 $\frac{\xi}{2}$，这与目前的已知是相互矛盾的，因此在多项式时间内不存在一种算法是能够以不可忽略的概率 ξ 解决此问题，即本方案可以达到挑战明文攻击的目的。

3.2 抗共谋攻击性

在重加密密钥生成阶段，用户属性集 $S_A\subseteq U$ 和共享结构 (M,ρ) 通过 A_2 进行验证，rk_1，rk_3，rk_4，与 R_x 通过 $\delta\in G_T$ 关联，rk_1，rk_2 和 rk_4 通过 $\theta\in Z_p$ 紧密相连，rk_4 在 $\theta\in Z_p$ 及共享权限结构 (M,ρ) 下对 $\delta\in G_T$ 进行加密，所以当 rk_1，rk_2，rk_3，R_x 的值被攻击者篡改其对应的重加密密文也就无效，如果 $S_A\subseteq U$、(M,ρ) 和 rk_4 被篡改，可以通过

$$e(A_2,H_6(A_1,A_2,(B_i,C_i)_{i=1}^l,S_A,(M,\rho)))=e(g,g)$$

检验出来。

由于该系统的特殊构造，将传输节点及存储节点分离开，引用了 Pool 验证池共识机制，存储节点与传输节点均是通过民主选举的方式产生，因此保证了执行节点的随机性及位置的不定性。即存储节点既不知道下一个传输节点位置，更不了解共享者信息，节点的随机性决定了 3 者串通的难度，因此存储节点、传输节点、共享者 3 者之间串通的可能性也极低。

3.3 属性代理重加密方案比较

本节主要结合 Seo 方案[6], Tiwari 方案[17], Luo 方案[18]对属性代理重加密方案特征做出了以下对比分析如表 2 所示。

由表 2 可见，Seo 方案、Luo 方案和 Tiwari 方案均采用了属性代理重加密技术，但是均依赖于第三方实现信息交互，尤其是 Seo 方案需要多个数据中心分层管理信息，故在信息传输及存储过程中很难保证信息不被篡改，而且以上 3 个方案均不支持信息检索功能，在一定程度上造成了信息共享阻塞；本方案可以同时实现表上的所有功能，根据实际情况自主选择所需信息，因此更适用于云存储共享的实际应用。

表 2 属性代理重加密方案的功能对比
Tab. 2 Functional comparison of attribute-based proxy re-encryption scheme

方案	关键词检索	属性加密	代理重加密	可解密密文	区块链技术	不依赖第三方	防篡改
Seo 方案	×	✓	✓	✓	×	×	×
Luo 方案	×	✓	✓	✓	×	×	×
Tiwari 方案	×	✓	✓	✓	×	×	×
本方案	✓	✓	✓	✓	✓	✓	✓

3.4 算法复杂性分析

结合 Seo 方案，Tiwari 方案，Luo 方案，本节将对与现有的属性代理重加密的方案进行效率及通信开销(密文长度)分析对比。为了便于描述，文中的 n 表示属性个数，L_G，L_{G_T}分别表示 G，G_T中的元素的比特长度。

本节中，通过与以下 3 种方案的系统公钥 *PK*，*MSK* 长度，用户私钥 *SK* 长度和 *CT* 长度进行对比，结果如表 3 所示。由表可知，相比于 Tiwari 方案，Luo 方案，本方案的系统公钥 *PK* 随着属性个数的增加，长度逐渐增长，用户私钥 *SK* 长度增长率大于其他三个方案，故本方案的密钥具有更高的抗攻击能力。将用户的属性作为每个用户私钥 *SK* 生成的依据之一，能够更加灵活的实现共享权限的控制，在密文中将用户属性转化为共享结构，对密文进行了定向的更有效的保护。

表 3 通信开销对比
Tab. 3 Comparison of communication overhead of attribute-based proxy re-encryption scheme

方案	*PK* 长度	*MSK* 长度	*SK* 长度	*CT* 长度
Seo	$(n+2)L_G+L_{G_T}$	L_G	$(n+2)L_G$	$(n+2)L_G+L_{G_T}$
Luo	L_{G_T}	L_G	$(n+2)L_G$	$nL_G+L_{G_T}$
Tiwari	$2L_G+L_{G_T}$	$3L_{Z_p}$	$(2n+1)L_G$	$(n+2)L_G+L_{G_T}$
本方案	$(n+3)L_G+L_{G_T}$	$L_G+L_{Z_p}$	$(2n+2)L_G$	$(2n+2)L_G+L_{G_T}$

3.5 执行效率分析

本节针对算法中的加密、重加密、密文解密及重加密密文解密过程所需要的计算量，并与现有的 3 种典型方案进行对比，结果如表 4 所示。其中，E 用于描述群 G，G_T幂运算的时长，而 P 表示双线性的对数运算时长，n 表示属性个数。

表 4 计算开销对比
Tab. 4 Comparison of computational cost of attribute proxy re-encryption scheme

方案	加密	原始密文解密	重加密	重加密解密
Seo	$(2n+2)E+2P$	$(2n+1)E+4P$	$(5n+2)E+4P$	$(6n+4)E+6P$
Luo	$(5n+2)E+P$	$(4n+4)E+5P$	$(10n+2)E+8P$	$(5n+2)E+5P$
Tiwari	$(4n+4)E+2P$	$4E+(n+3)P$	$(3n+12)E+8P$	$(5n+7)E+P$
本方案	$(3n+2)E+2P$	$(3n+2)E+3P$	$(3n+1)E+5P$	$(4n+6)E+3P$

由表 4 可知，Seo 方案中的双线性实现的是与门访问结构仅支持属性间的“与”关系操作，而本方案的却支持任意共享权限公式，更加灵活的便捷。本方案与 Tiwari 方案相比，利用增加乘法运算使减少了所需要的双线性对数运算，故本方案的运算成本要远小于以上 2 个方案的运算量，从而达到了降低计算开销的目的。相比于 Luo 方案，本文的执行效率也有明显下降。

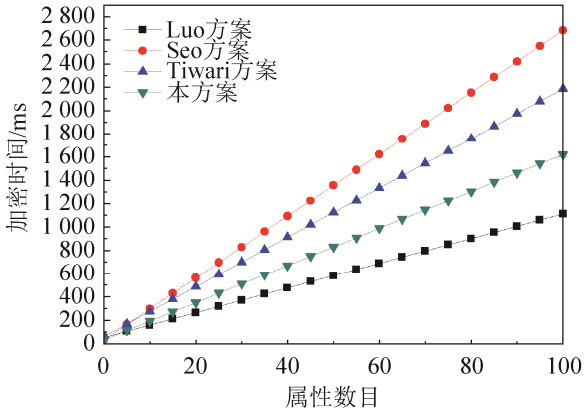
4 模拟实验

为了进一步评估系统中的效率，本文对 Seo 方案，Tiwari 方案，Luo 方案 3 个方案做了对比实验，4 个方案均是采用了 Tate 双线性配对，根据上文提出的计算操作方案，对其性能进行了测试，以便进行理论分析。评估是在配备 Intel Core i5-3337U、CPU 2.40 GHz 和 4GB RAM 的笔记本电脑上进行的，执行一次 Tate 双线性配对操作用时为 20.04 ms，执行一次幂指数运算 5.31 ms。本文的实验过程是根据用户持有的属性数目作为变量，分别对加密、解密、重加密、重解密运算时间进行了仿真。

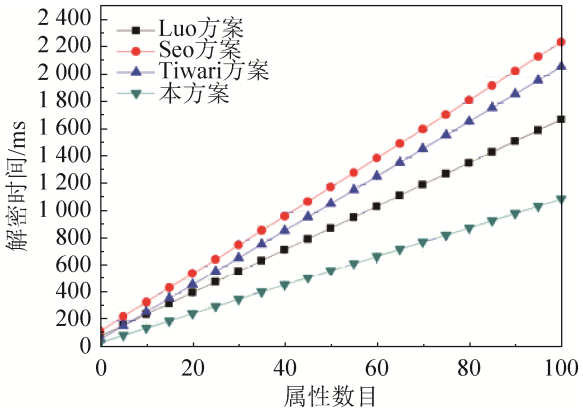
图 5(a)说明随着属性数目递增，加密的计算时

https://dc-china-simulation.researchcommons.org/journal/vol32/iss6/4
DOI: 10.16182/j.issn1004731x.joss.18-0658

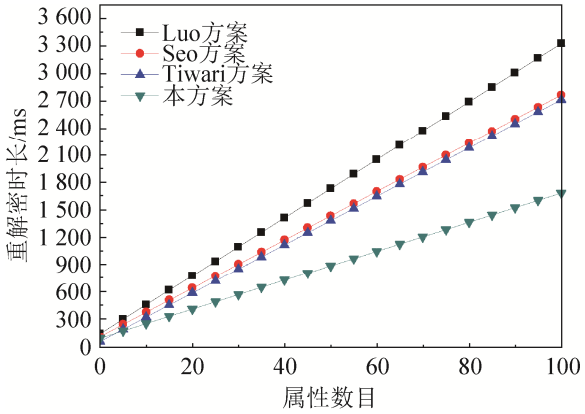
间也在增长，为了更好地保证信息的安全性，在加密过程中本文增加了属性匹配的次数，故运算时耗略高于 Seo 方案。图 5(b)是原信息解密时长，本方案相对于 Tiwari 方案，Luo 方案有绝对的优势。本方案利用区块链技术由不同的节点分担数据中心计算任务，减少了可信中心的双线性配对的计算次数，因此在计算开销上更具有优势。图 5(c)是重加密阶段计算时间的变化情况，4 个方案均需要共享权限匹配，本方案中对于持有 100 个特征属性的信息重加密仅需 1.70 s 左右，相比于其他 3 种方案效率平均提高了 37.89%。图 5(d)表示随着属性数目的增加重解密信息时耗，随着属性数目的增加，100 个特征属性的信息重加密仅需 1.68 s，相比于其他 3 个方案，本方案的解密时长的增长率最小平均速率提高了 42.1%。



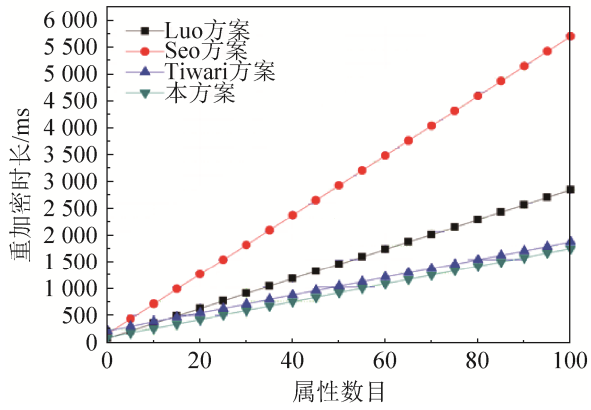
(a) 加密时间



(b) 解密时间



(c) 重加密时间



(d) 重解密时间

图 5 属性数目对执行性能的影响

Fig. 5 Effect of number of attributes on system performance

5 结论

结合区块链技术的去中心化、智能合约模式和分布式存储等特点，提出的区块链密文存储共享模型，打破了传统集中分布式云存储模式，既实现了中心化与去中心化存储共享模型的过渡，又满足现有的信息安全存储共享的技术需求。通过使用 Pool 验证池共识机制使每个节点出于对自身利益最大化的考虑，都会自发、诚实地遵守协议中预先设定的规则，判断每一笔记录的真实性，最终将判断为真的记录记入区块链之中，在很大程度上提高了信息存储共享的效率；明文信息采用属性加密方式，一定程度上避免了信息共享请求者的二次销售现象；利用属性代理重加密算法，将原信息密文与重加密密文分离存储，具有一定的抗共谋攻击性；采

用智能合约取代第三方的信息管理中心，实现了自主化的密钥转换，提高了信息存储、共享的效率节约了成本。通过功能分析、效率对比、通信开销对比显示，本方案更具有适用性。

参考文献：

[1] 王涛. 信息数据服务平台虚拟资源调度算法设计与分析 [D]. 南京: 南京邮电大学, 2016.
Wang Tao. Design and Analysis of Virtual Resource Scheduling Algorithm on Data Service PlatformNanjing [D]. Nanjing: University of Posts and Telecommunications, 2016.

[2] Kaufman L M. Data Security in the World of Cloud Computing [J]. IEEE Security & Privacy (S1540-7993), 2009, 7(4): 61-64.

[3] Takabi H, Joshi J B D, G J. Security and Privacy Challenges in Cloud Computing Environments [J]. IEEE Security & Privacy (S1540-7993), 2010, 8(6): 24-31.

[4] 崔光耀. 2013 年国际十大信息安全热点事件 [J]. 中国信息安全, 2014, 1: 79-80.
Cui Guangyao. Ten international information security hotspots in 2013[J]. China Information Security, 2014, 1: 79-80.

[5] Cheng H, Min Z, Feng D G. Achieving efficient dynamic cryptographic access control in cloud storage [J]. Journal on Communications (S1000-436X), 2011, 32(7): 125-132.

[6] Seo H J, Kim H. Attribute-based Proxy Re-encryption with a Constant Number of Pairing Operations [J]. Journal of Information & Communication Convergence Engineering (S2234-8883), 2012, 10(1): 53-60.

[7] Shi Y, Liu J, Han Z, et al. Attribute-based proxy re-encryption with keyword search[J]. PLoS ONE (S1932-6203), 2014, 9(12): e116325.

[8] Liang K, Susilo W. Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage [J]. IEEE Transactions on Information Forensics & Security (S1556-6013), 2017, 10(9): 1981-1992.

[9] 唐长兵, 杨珍, 郑忠龙, 等. PoW 共识算法中的博弈困境分析与优化 [J]. 自动化学报, 2017, 43(9): 1520-1531.
Tang Changbing, Yang Zhen, Zheng Zhonglong, et al. Game Dilemma Analysis and Optimization of PoW Consensus Algorithm [J]. Journal of Automation, 2017, 43(9): 1520-1531.

[10] 韩裕光. 互联网金融演化：比特币研究[D]. 安徽大学博士学位论文, 2016.
Yuguang Han. Internet Financial Evolution: The Study of Bitcoin[D]. Doctoral dissertation of Anhui University, 2016.

[11] Li K, Li H, Hou H, et al. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain[C]// IEEE, International Conference on High PERFORMANCE Computing and Communications; IEEE, International Conference on Smart City; IEEE, International Conference on Data Science and Systems. Bangkok, Thailand: IEEE, 2017: 466-473.

[12] 平健, 陈思捷, 张宁, 等. 基于智能合约的配电网去中心化交易机制 [J]. 中国电机工程学报, 2017, 37(13): 3682-3690.
Ping Jian, Chen Sijie, Zhang Ning, et al. Decentralized Transactive Mechanism in Distribution Network Based on Smart Contract [J]. Proceedings of the CSEE, 2017, 37(13): 3682-3690.

[13] Nakagawa T, Hayashibara N. Energy Efficient Raft Consensus Algorithm[C]// International Conference on Network-Based Information Systems. Toronto, Canada: Springer, Cham, 2017: 719-727.

[14] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography [J]. Lecture Notes in Computer Science (S0302-9743), 1998, 1403: 127-144.

[15] 刘梦君, 刘树波, 王颖, 等. 基于 LSSS 共享矩阵无授权策略的属性密码解密效率提高方案 [J]. 电子学报, 2015, 43(6): 1065-1072.
Liu Mengjun, Liu Shubo, Wang Ying, et al. Optimizaing the decrytion efficiency in LSSS matrix-based attribute-based encryption without given policy [J]. Chinese Journal of Electronics, 2015, 43(6): 1065-1072.

[16] Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization [J]. Lecture Notes in Computer Science (S0302-9743), 2011, 2008: 321-334.

[17] Tiwari D, Gangadharan G R. SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation [J]. International Journal of Communication Systems (S1099-1131), 2017, 31(4): e3494.

[18] 罗恩韬, 王国军, 陈淑红, 等. 移动社交网络中跨域代理重加密朋友发现隐私保护方案研究 [J]. 通信学报, 2017, 38(10): 81-93.
Luo Entao, Wang Guojun, Chen Shuhong, et al. Privacy preserving friend discovery cross domain scheme using re-encryption in mobile social networks [J]. Journal on Communications, 2017, 38(10): 81-93.