



基于属性加密的联盟区块链数据共享方法

朱丽丽

(金陵科技学院 软件工程学院, 江苏 南京 211169)

摘要:在保证区块链内数据安全的前提下,数据共享的速度通常较慢,为减少数据共享所需时间,基于属性加密算法设计联盟区块链数据共享方法。构建分层访问树,在无密钥托管模式中完成对用户代理加密的分类,使用哈希函数简单处理分层模型;基于属性加密构造数据访问共享模型,定义数据库域值,设置系统公共参数,建立主密钥与公密钥,完成集中式的数据共享管理;设计区块链数据共享算法,依据公钥格式生成用户私钥,完成区块链内的数据共享。分别计算数据共享过程中安全索引、陷门生成、关键字搜索三个步骤的用时,由数据可知,在安全索引与关键字搜索时,属性加密算法的运算效率更高,在陷门生成过程中,属性加密算法的运算效率相对较高。该方法的数据共享总用时为 991 ms,共享时间更短,速度更快。

关键词:属性加密;区块链数据;数据共享;优化算法;分层访问;访问权限

中图分类号: TP309.7

文献标识码: A

文章编号: 1671-931X(2024)01-0115-06

DOI: 10.19899/j.cnki.42-1669/Z.2024.01.019

在电子技术的发展下,现代社会的信息数据共享已经是一个非常普遍的现象,但是数据在共享过程中经常会出现隐私泄露、单点故障等问题,而且很容易受到黑客的攻击,因此对于共享数据的访问控制与加密也成了备受关注的问題^[1]。为减少服务器内数据共享过程中可能存在的被伪造、被篡改的风险,需要设计一种对数据共享加密的方法。通过基于区块链的轻量级协议——基于有向无环图的 V2G 网络(DV2G),可提高交易数据共享的吞吐量,实现高速率的交易数据共享^[2]。在代理重加密算法下,可以通过多权限的云数据进行分类共享,结

合属性加密算法,提出双线性的粒度细化准则,并在第三方的数据云中继续降低重加密阶段的用户计算需求。因此该方法可以针对云环境下的细粒度进行安全共享,并大幅度提高计算效率^[3]。也可以通过一个安全且可验证的一对多数据共享方案来实现数据安全传输。使用区块链记录访问策略,实现用户自认证和云不可否认性。结合认证方案和策略隐藏方案,提高了数据传输的安全性和有效性^[4]。结合以上文献研究,设计了一种基于属性加密的联盟区块链数据共享方法,属性加密方法可以根据数据类型进行加密,进一步提高共享数据的安全性。

收稿日期: 2023-02-21

基金项目:2021 年度江苏省现代教育技术智慧校园专项课题“基于 5G 背景下智慧校园建设研究”(项目编号:2021-R-96613);2022 年度江苏省现代教育技术课题“智慧教育平台个性化课程推荐系统的研究与应用”(项目编号:2022-R-98782);2022 年教育部产学合作协同育人项目“高校智慧教室应用现状及优化策略研究”(项目编号:220503175115959);2022 年度江苏省现代教育技术智慧校园专项课题“基于区块链的在线教育系统的研究与实现”(项目编号:2022-R-107212)。

作者简介:朱丽丽(1980—),女,江苏淮安人,金陵科技学院软件工程学院副研究员,研究方向:计算机技术、教育信息化。

一、基于属性加密设计联盟区块链数据共享方法

(一) 构建分层访问树

在互联网中,数据的在线共享已经成为一种流行的趋势,为了保证数据共享的稳定性与安全性,因此从两方面优化存储结构,一方面提高数据的外部存储容量,以在硬件方面为区块链技术提供大量的存储空间,并加大存储访问的效率,另一方面保

证数据在云存储方面的分层结构稳定性,以建立安全的访问机制^[5]。为了保证用户在密文模型中访问机制的安全性,可以通过无密钥托管的模式完成对用户代理加密的分类操作,并基于层次结构的方式建立访问控制树,以提前完成节点数据的运输与分级。通过层次文件的读取,获得访问控制平台的处理与解密,尽量降低用户的开销,提高数据共享的效率。基于以上理念,建立如图1所示分层树。

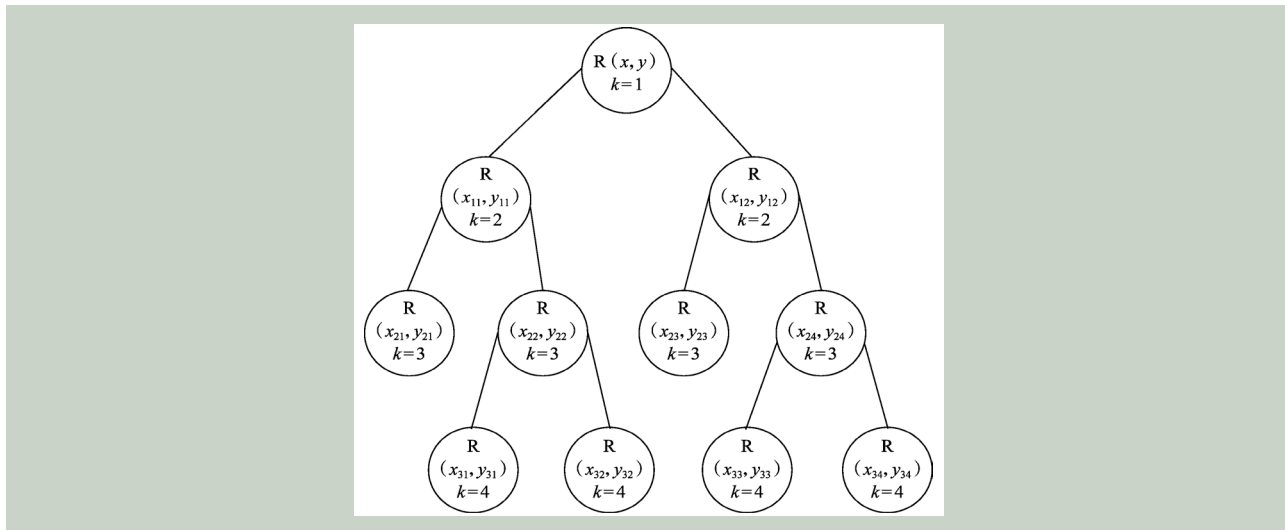


图1 访问树结构模型

如图1所示,访问树中共分为四个层次,分别使用 $k=1, k=2, \dots$ 表示,其中R表示访问树中的节点标识, (x, y) 的坐标表示子节点中行、列的属性。如 (x_{12}, y_{12}) 表示第2个横子节点中第1个坐标值^[6-7]。在这些结构模型中,需要对哈希函数进行简单处理,基于不可逆性定理可以得到公式:

$$h_k = \text{Hash}(x_{mn}, y_{mn}) \quad (1)$$

式中, h_k 表示经过简单的访问树处理后所能得到的哈希函数值; (x_{mn}, y_{mn}) 则表示访问树中的子节点坐标; m 表示第 m 个坐标值; n 表示第 n 个子节点。通常情况下可以在任意哈希函数中获取固定的函数值,从而得到较为稳定的数据分层结果。

(二) 基于属性加密构造数据访问共享模型

在设计数据访问共享模型前,需要首先建立基于属性加密的区块链哈希函数,一旦能够寻找到一个可以满足区块结构的工作量,就能够在节点完成资源消耗的同时,对工作进行完美执行^[8-9]。将共享数据存储区块链上,需要根据已有的关键词,建立候选共享数据的信息数据库,该域值可以定义为:

$$G = \{g | g \in \theta\} \quad (2)$$

式中, G 表示共享数据库中关键词的数据集; g 表示某一个关键词; θ 表示通过数据检索机制得到的目标数据域^[10]。在初始化身份系统的过程中,可以在系统内设置安全参数,并生成相应的密钥公式,此时系统的公共参数可以表示为:

$$H_{par} = (F_1, T_g, m_e, f_g, K_1, K_2, P_n) \quad (3)$$

式中, H_{par} 表示系统内的密钥公式的主要参数; F_1 表示系统内公共参数的生成元; T_g 表示生成元的阶乘; m_e 表示双线性映射特征的向量区间; f_g 表示生成元的总数量; K_1 和 K_2 分别表示哈希函数的共享多项分量; P_n 表示系统内权威中心的数量。通过权威中心建立主密钥和公密钥,公式为:

$$\begin{cases} d_z = \sum_{i=1}^n f_{im} \pmod{Q_m} \\ d_g = \prod_{i=1}^n Q^{d_n} = q^d \end{cases} \quad (4)$$

式中, d_z 表示权威中心的主密钥, d_g 则表示公密钥; f_{im} 表示随机多项式的第 m 个分量值; Q_m 表示区块连接点依据公共参数获取的身份私钥; Q^{d_n} 表示经过错误提示返回的私钥分量; q^d 表示私人身

份标识参数^[11-12]。结合主密钥与公密钥,可以建立数据共享发送者与数据共享接受者的数据共享模

型,在数据源以及哈希函数的参与下,可以得到如图 2 所示的数据共享模型。

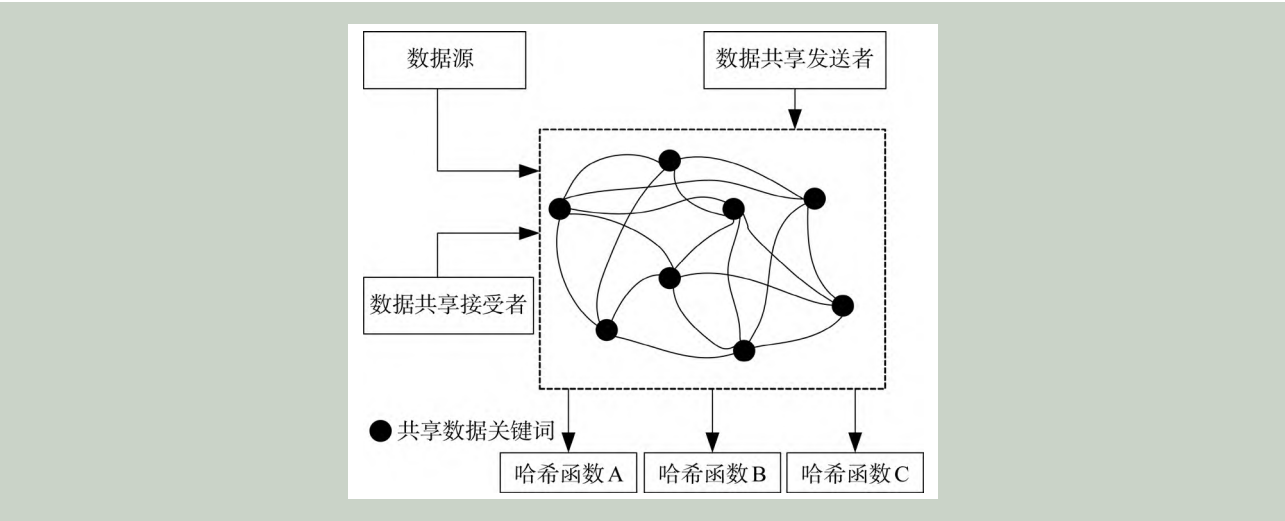


图 2 数据共享模型

如图 2 所示,通过数据源接收数据的原始信息,并在经过处理后,得到共享数据关键词的访问路径。在数据共享发送者与数据共享接受者之间建立解密访问路径,结合不同的数据存储形式,重新设计哈希表对公钥地址内的存储结构^[13]。在所有返回函数的输出转换项中,将不同的地址节点作为

一个以业务逻辑为核心的区块链加密场景,并集中进行数据的共享管理。

(三)设计区块链数据共享算法

通过以上方法,可以得到联盟区块链的数据共享算法,如图 3 所示。

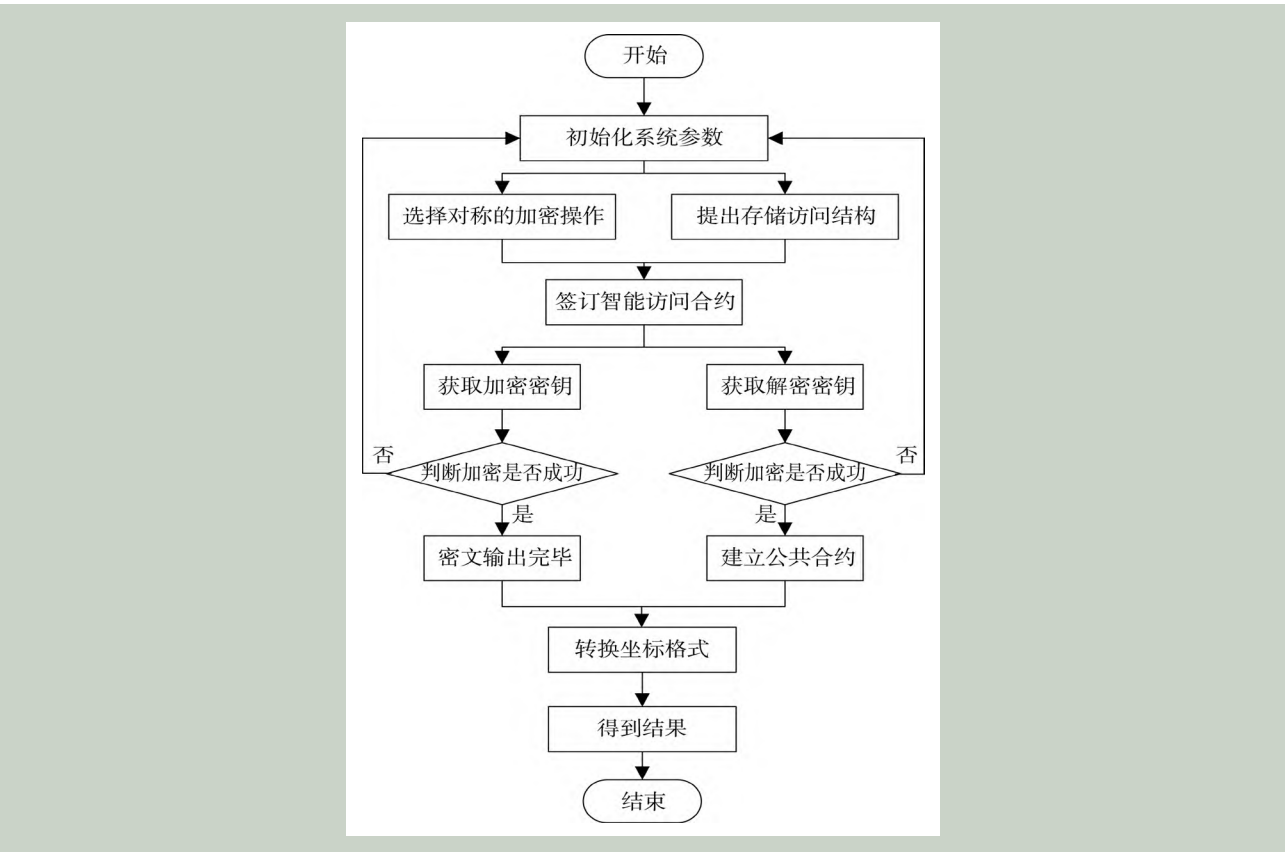


图 3 算法流程

如图3所示,在初始化系统参数以后,可以依据双线性的生成定理,定义哈希函数:

$$\begin{cases} H_1: \{0,1\}^* \rightarrow h_p \\ H_2: \{0,1\}^* \rightarrow f_t \end{cases} \quad (5)$$

式中, H_1 和 H_2 分别表示数据加密与数据解密两个哈希函数; h_p 表示系统公钥的安全参数; f_t 则表示用户私钥的安全参数^[14-15]。在生成公钥并计算私钥时,可以依据公式:

$$Y_s = \left\{ \frac{G_p \times t_{dv}}{h_k} \right\} \quad (6)$$

式中, Y_s 表示用户私钥; G_p 表示分层访问树中由内容形成的密文格式; t_{dv} 表示输出的集成随机多项式; h_k 表示系统内各等级节点的数量。通过以上公式,判断数据的加密或解密是否成功,并建立密文输出的公共合约,从而得到转换后的坐标格式,此时即可对联盟区块链的数据进行共享。

二、实验研究

(一) 联盟区块链数据共享流程

为测试上文中联盟区块链数据共享方法的安全性能,设计以下实验。初始化整个区块链系统,并在往外完成机制函数执行步骤的同时,生成初始化的函数,在其中加入系统公钥以及密钥请求。在发布数字用户的属性信息之后,通过请求者上传的数据文件,可以得到数据的共享流程,如图4所示。

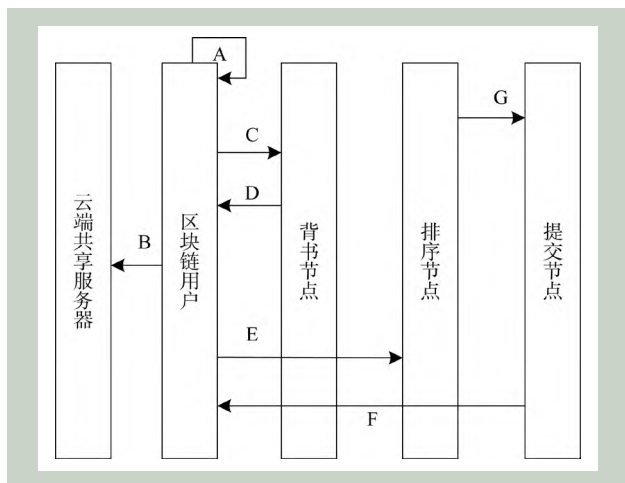


图4 数据共享流程

在如图4所示的数据共享流程中,用户至少需要对四个共享节点进行操作。其中流程A为用户自身对数据信息的详细描述,在访问过程中,需要首先生成共享数据的明文 M_w ,并在明文中填写必要的描述信息 X_{xi} ,此时的数据哈希值可以表示为

S_{hash} 。同时,在流程B、C、E中,区块链数据还可以同步上传至云端共享服务器、背书节点以及排序节点。用户通过流程D将数据指向明文的描述信息 X_{xi} 与哈希值 S_{hash} 发送到背书节点,并结合验证签名将其重新返回到客户端。在客户端中若监听网络传递出数据存储已经成功上链的消息,则数据的共享已经成功。这时候,就需要经过流程F,将信息由提交节点返回到区块链用户。

(二) 数据加密开销计算

在本实验中,使用属性加密的方法对联盟区块链数据进行共享,此时的加密共分为三个步骤,分别为安全索引、陷门生成、关键字搜索,第一个步骤安全索引的计算公式为:

$$T_{aq} = \frac{2F_1 + t_p + t_{h1} + t_{h2}}{\sqrt{\frac{F_1 + C_{m1}}{t_p}}} \quad (7)$$

式中, T_{aq} 表示属性加密算法内联盟区块链数据共享中安全索引所需时间; F_1 表示区块链横向群体中幂运算的时间长度; t_p 表示加密数据共享映射的时间长度; t_{h1} 和 t_{h2} 分别表示哈希函数 H_1 和哈希函数 H_2 的运算时间; C_{m1} 表示区块链群体的传输运算时长。第二步陷门生成所需时间的计算公式为:

$$T_{xm} = \frac{F_1 + t_{h1}}{3F_1 + F_2 + 4t_{h1}} \quad (8)$$

式中, T_{xm} 表示属性加密算法内联盟区块链数据共享中陷门生成所需时间; F_2 表示区块链纵向生成的群体中幂运算运行时间;第三步关键字搜索运算的整体时间计算公式为:

$$T_{ss} = \frac{\sqrt{t_p + t_{h2}}}{F_2 + 2t_p + t_{h2}} \quad (9)$$

式中, T_{ss} 表示区块链数据共享所需的关键字搜索。将以上三个公式叠加计算,可以得到数据共享的总时间,计算公式为:

$$T_z = T_{aq} + T_{xm} + T_{ss} \quad (10)$$

式中, T_z 表示数据共享的总用时。在以下的实验中,通过公式(10),可以获取实验数据结果,并对其进行分析。

(三) 数据共享时间测试

基于上述公式,计算数据的安全索引、陷门生成、关键字搜索三个步骤的时间,并与有向无环图方法、代理重加密算法和多数据共享方案进行对比,得到如图5所示的数据结果。

如图5所示,为安全索引、陷门生成以及关键字搜索三个共享过程在不同关键字数量下的时间。当关键字数量为60时,四种共享方法在安全索引步骤中的用时分别为183 ms、312 ms、339 ms、487 ms;其在陷门生成步骤所需要的时间分别为451 ms、386 ms、526 ms、765 ms;在关键字搜索步骤需要的时间差进一步扩大,分别为357 ms、571 ms、392 ms、940 ms。其中,属性加密方法在安全索引步骤与

关键字搜索步骤,均在四种方法中速度最快,但是在陷门生成步骤中,其速度略小于代理密码公钥方法。通过求和公式获取的共享总时间对比中,四种方法的用时分别为991 ms、1269 ms、1257 ms、1992 ms,由此可见,本文设计的属性加密共享方法在速度测试中优于其他方法。

本文设计了一种基于属性加密的联盟区块链数据共享方法,在建立了分层访问树以后,通过哈希函数的不可逆性定理,得到了较为有效的分层结果。在属性加密算法下构造数据共享模型,模型中详细论述了数据分享者与数据接受者之间的数据传输过程,并结合以上方法,设计了新的算法实现数据共享。在实验中以安全索引、陷门生成、关键字搜索三个步骤,分别测试数据的共享时间,结合数据结果可知,本文设计的共享方法可以以更快的速度完成数据共享工作。

参考文献:

- [1] 侯雨桐, 马兆丰, 罗守山. 基于区块链的数据安全共享与受控分发技术研究[*J*]. 信息安全学报, 2022(2): 55-63.
- [2] Hassija V, Chamola V, Garg S, et al. A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network[*J*]. IEEE Transactions on Vehicular Technology, 2020(6): 5799-5812.
- [3] 文鹏程, 沈济南, 梁芳, 等. 云环境中细粒度的数据安全共享方案[*J*]. 武汉大学学报(理学版), 2022(1): 93-101.
- [4] Fan K, Pan Q, Zhang K, et al. A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks[*J*]. IEEE Transactions on Vehicular Technology, 2020(6): 5826-5835.
- [5] 牛淑芬, 宋蜜, 方丽芝, 等. 智慧医疗中基于属性加密的云存储数据共享[*J*]. 电子与信息学报, 2022(1): 107-117.
- [6] 冯景瑜, 汪涛, 于婷婷, 等. 基于多云多链协同的医疗数据安全共享机制[*J*]. 信息安全学报, 2022(1): 9-18.
- [7] 杨学成, 李业勤. 区块链视角下供应链多主体数据共享意愿博弈研究[*J*]. 科技管理研究, 2021(23): 181-192.
- [8] 杨业平, 林德威, 黄芳芳, 等. 基于区块链的物联网安全数据共享系统[*J*]. 福州大学学报(自然科学版), 2021(6): 739-746.
- [9] 于克辰, 郭莉, 姚萌萌. 基于区块链的高价值数据共享系统设计[*J*]. 信息安全学报, 2021(11): 75-84.
- [10] 林孟晨, 冯勇, 付晓东. 一种基于联盟区块链的电子医疗记录安全共享模型[*J*]. 小型微型计算机系统, 2021(10): 2161-2166.
- [11] Zhen Z, Fg B, JI C, et al. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts-ScienceDirect[*J*]. Theoretical Computer Science, 2020(809): 73-87.

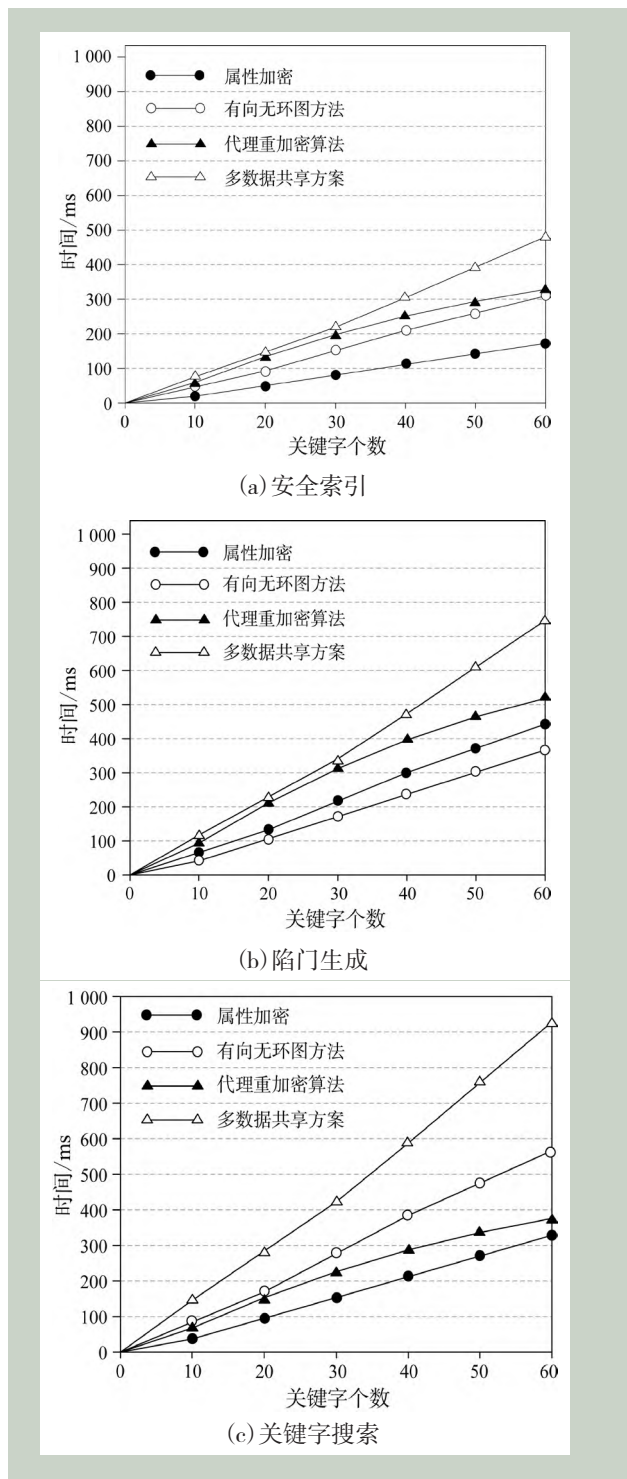


图5 数据共享所需时间对比结果

- [12] 刘玉红, 杨亮, 朴春慧, 等. 基于区块链的铁路工程施工安全监测数据共享关键技术研究[J]. 通信学报, 2021(8): 206-216.
- [13] 周正强, 陈玉玲, 李涛, 等. 基于联盟链的医疗数据安全共享方案[J]. 应用科学学报, 2021(1): 123-134.
- [14] Yza B, Bo Y, Tao W A, et al. Novel updatable identity-

based hash proof system and its applications[J]. Theoretical Computer Science, 2020(804): 1-28.

- [15] 邢海龙, 高长元, 翟丽丽, 等. 大数据联盟成员间数据资源共享动态演化博弈模型研究——基于共享积极性视角[J]. 管理评论, 2020(8): 155-165.

[责任编辑: 胡大威]

Data Sharing Method of Alliance Blockchain based on Attribute Encryption

Zhu Lili

(Software Engineering Institute, Jinling Institute of Technology, Nanjing, Jiangsu 211169, China)

Abstract: On the premise of ensuring the data security in the blockchain, the speed of data sharing is usually slow. In order to reduce the time required for data sharing, the alliance blockchain data sharing method is designed based on attribute encryption algorithm. Build a hierarchical access tree, complete the classification of user agent encryption in the keyless hosting mode, and use the hash function to simply deal with the hierarchical model. Construct data access and sharing model based on attribute encryption, define database domain value, set system public parameters, establish master key and public key, and complete centralized data sharing management. Design the blockchain data sharing algorithm, generate the user's private key according to the public key format, and complete the data sharing in the blockchain. Calculate the time of security index, trap generation and keyword search in the process of data sharing. It can be seen from the data that the operation efficiency of attribute encryption algorithm is higher in the process of security index and keyword search, and the operation efficiency of attribute encryption algorithm is relatively higher in the process of trap generation. The total data sharing time of this method is 991ms, so the sharing time is shorter and the speed is faster.

Key words: attribute encryption; blockchain data; data sharing; optimization algorithm; hierarchical access; access rights